Radware DefensePro DDoS Mitigation User Guide

Software Version 8.22.2
Last Updated: July 2020
Document ID: RDWR-DPCSCOFP-V082220_UG2007

Important Notices

The following important notices are presented in English, French, and German.

Important Notices

This guide is delivered subject to the following conditions and restrictions: Copyright

Radware Ltd. 2020. All rights reserved.

The copyright and all other intellectual property rights and trade secrets included in this guide are owned by Radware Ltd.

The guide is provided to Radware customers for the sole purpose of obtaining information with respect to the installation and use of the Radware products described in this document, and may not be used for any other purpose.

The information contained in this guide is proprietary to Radware and must be kept in strict confidence.

It is strictly forbidden to copy, duplicate, reproduce or disclose this guide or any part thereof without the prior written consent of Radware.

Notice importante

Ce guide est sujet aux conditions et restrictions suivantes:

Copyright Radware Ltd. 2020. Tous droits réservés.

Le copyright ainsi que tout autre droit lié à la propriété intellectuelle et aux secrets industriels contenus dans ce guide sont la propriété de Radware Ltd.

Ce guide d'informations est fourni à nos clients dans le cadre de l'installation et de l'usage des produits de Radware décrits dans ce document et ne pourra être utilisé dans un but autre que celui pour lequel il a été conçu.

Les informations répertoriées dans ce document restent la propriété de Radware et doivent être conservées de manière confidentielle.

Il est strictement interdit de copier, reproduire ou divulguer des informations contenues dans ce manuel sans avoir obtenu le consentement préalable écrit de Radware.

Wichtige Anmerkung

Dieses Handbuch wird vorbehaltlich folgender Bedingungen und Einschränkungenausgeliefert: Copyright

Radware Ltd. 2020. Alle Rechte vorbehalten.

Das Urheberrecht und alle anderen in diesem Handbuch enthaltenen Eigentumsrechteund Geschäftsgeheimnisse sind Eigentum von Radware Ltd.

Dieses Handbuch wird Kunden von Radware mit dem ausschließlichen Zweck ausgehändigt, Informationen zu Montage und Benutzung der in diesem Dokument beschriebene Produkte von Radware bereitzustellen. Es darf für keinen anderen Zweck verwendet werden.

Die in diesem Handbuch enthaltenen Informationen sind Eigentum von Radware und müssen streng vertraulich behandelt werden.

Es ist streng verboten, dieses Handbuch oder Teile daraus ohne vorherige schriftliche Zustimmung von Radware zu kopieren, vervielfältigen, reproduzieren oder offen zu legen.

Copyright Notices

The following copyright notices are presented in English, French, and German.

Copyright Notices

The programs included in this product are subject to a restricted use license and can only be used in conjunction with this application.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL, please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display thefollowing acknowledgement:

   This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All

rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions andthe following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display thefollowing acknowledgement:

   " This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the appsdirectory (application code) you must include an acknowledgment:

   " This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS”' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

This product contains the Rijndael cipher

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimized ANSI C code for the Rijndael cipher (now AES) @author

Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be> @author

Paulo Barreto <paulo.barreto@terra.com.br>

The OnDemand Switch may use software components licensed under the GNU General Public License Agreement Version 2 (GPL v.2) including LinuxBios and Filo open source projects. The source code of the LinuxBios and Filo is available from Radware upon request. A copy of the license can be viewed at: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

This code is hereby placed in the public domain.

This product contains code developed by the OpenBSD Project Copyright ©1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This product includes software developed by Markus Friedl. This

product includes software developed by Theo de Raadt. This

product includes software developed by Niels Provos This

product includes software developed by Dug Song

This product includes software developed by Aaron Campbell This

product includes software developed by Damien Miller This

product includes software developed by Kevin Steves This product

includes software developed by Daniel Kouril This product

includes software developed by Wesley Griffin This product

includes software developed by Per Allansson This product

includes software developed by Nils Nordman This product

includes software developed by Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

This product contains work derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. RSA Data Security, Inc. makes no representations concerning either the merchantability of the MD5 Message - Digest Algorithm or the suitability of the MD5 Message - Digest Algorithm for any particular purpose. It is provided “as is” without express or implied warranty of any kind.

Notice traitant du copyright

Les programmes intégrés dans ce produit sont soumis à une licence d’utilisation limitée et ne peuvent être utilisés qu’en lien avec cette application.

L'implémentation de Rijindael par Vincent Rijmen, Antoon Bosselaers et Paulo Barreto est du domaine public et distribuée sous les termes de la licence suivante:

@version 3.0 (Décembre 2000)

Code ANSI C code pour Rijndael (actuellement AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be> @author

Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be> @author Paulo

Barreto <paulo.barreto@terra.com.br>

Le commutateur OnDemand peut utiliser les composants logiciels sous

licence, en vertu des termes de la licence GNU General Public License

Agreement Version 2 (GPL v.2), y compris les projets à source ouverte

LinuxBios et Filo. Le code source de LinuxBios et Filo est disponible sur

demande auprès de Radware. Une copie de la licence est répertoriée sur:

http://www.gnu.org/licenses/old- licenses/gpl-2.0.html.

Ce code est également placé dans le domaine public.

Ce produit renferme des codes développés dans le cadre du projet OpenSSL. Copyright

©1983, 1990, 1992, 1993, 1995

Les membres du conseil de l'Université de Californie. Tous droits réservés.

La distribution et l'usage sous une forme source et binaire, avec ou sans modifications, est autorisée pour autant que les conditions suivantes soient remplies:

1. La distribution d'un code source doit inclure la notice de copyright mentionnée ci-dessus,cette liste de conditions et l'avis de non-responsabilité suivant.
2. La distribution, sous une forme binaire, doit reproduire dans la documentation et/ou danstout autre matériel fourni la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.
3. Le nom de l'université, ainsi que le nom des contributeurs ne seront en aucun cas utiliséspour approuver ou promouvoir un produit dérivé de ce programme sans l'obtention préalable d'une autorisation écrite.

Ce produit inclut un logiciel développé par Markus Friedl. Ce

produit inclut un logiciel développé par Theo de Raadt. Ce

produit inclut un logiciel développé par Niels Provos.

Ce produit inclut un logiciel développé par Dug Song.

Ce produit inclut un logiciel développé par AaronCampbell. Ce

produit inclut un logiciel développé par DamienMiller.

Ce produit inclut un logiciel développé par Kevin Steves. Ce

produit inclut un logiciel développé par Daniel Kouril. Ce

produit inclut un logiciel développé par WesleyGriffin. Ce

produit inclut un logiciel développé par Per Allansson. Ce

produit inclut un logiciel développé par NilsNordman.

Ce produit inclut un logiciel développé par Simon Wilkinson.

La distribution et l'usage sous une forme source et binaire, avec ou sans modifications, est autorisée pour autant que les conditions suivantes soient remplies:

1. La distribution d'un code source doit inclure la notice de copyright mentionnée ci-dessus,cette liste de conditions et l'avis de non-responsabilité suivant.
2. La distribution, sous une forme binaire, doit reproduire dans la documentation et/ou danstout autre matériel fourni la notice de copyright mentionnée ci-dessus, cette liste de conditions et l'avis de non-responsabilité suivant.

LE LOGICIEL MENTIONNÉ CI-DESSUS EST FOURNI TEL QUEL PAR LE DÉVELOPPEUR ET TOUTE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER EST EXCLUE.

EN AUCUN CAS L'AUTEUR NE POURRA ÊTRE TENU RESPONSABLE DES DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, SPÉCIAUX, EXEMPLAIRES OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS S'Y LIMITER, L'ACQUISITION DE BIENS OU DE SERVICES DE REMPLACEMENT, LA PERTE D'USAGE, DE DONNÉES OU DE PROFITS OU L'INTERRUPTION DES AFFAIRES), QUELLE QU'EN SOIT LA CAUSE ET LA THÉORIE DE RESPONSABILITÉ, QU'IL S'AGISSE D'UN CONTRAT, DE RESPONSABILITÉ STRICTE OU D'UN ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE), DÉCOULANT DE QUELLE QUE FAÇON QUE CE SOIT DE L'USAGE DE CE LOGICIEL, MÊME S'IL A ÉTÉ AVERTI DE LA POSSIBILITÉ D'UN TEL DOMMAGE.

Copyrightvermerke

Die in diesem Produkt enthalten Programme unterliegen einer eingeschränkten Nutzungslizenz und können nur in Verbindung mit dieser Anwendung benutzt werden.

Die Rijndael-Implementierung von Vincent Rijndael, Anton Bosselaers und Paulo Barreto ist öffentlich zugänglich und wird unter folgender Lizenz vertrieben:

@version 3.0 (December 2000)

Optimierter ANSI C Code für den Rijndael cipher (jetzt AES) @author

Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be> @author

Paulo Barreto <paulo.barreto@terra.com.br>

Der OnDemand Switch verwendet möglicherweise Software, die im Rahmen der DNU Allgemeine Öffentliche Lizenzvereinbarung Version 2 (GPL v.2) lizensiert sind, einschließlich LinuxBios und Filo Open Source-Projekte. Der Quellcode von LinuxBios und Filo ist bei Radware auf Anfrage erhältlich. Eine Kopie dieser Lizenz kann eingesehen werden unter http://www.gnu.org/licenses/old-licenses/ gpl-2.0.html.

Dieser Code wird hiermit allgemein zugänglich gemacht.

Dieses Produkt enthält einen vom OpenBSD-Projekt entwickelten Code Copyright

©1983, 1990, 1992, 1993, 1995

The Regents of the University of California. Alle Rechte vorbehalten.

Die Verbreitung und Verwendung in Quell- und binärem Format, mit oder ohne Veränderungen, sind unter folgenden Bedingungen erlaubt:

1. Die Verbreitung von Quellcodes muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss beibehalten.
2. Die Verbreitung in binärem Format muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder andere Materialien, die mit verteilt werden, reproduzieren.
3. Weder der Name der Universität noch die Namen der Beitragenden dürfen ohneausdrückliche vorherige schriftliche Genehmigung verwendet werden, um von dieser Software abgeleitete Produkte zu empfehlen oder zu bewerben.

Dieses Produkt enthält von Markus Friedl entwickelte Software. Dieses Produkt enthält von Theo de Raadt entwickelte Software. Dieses Produkt enthält von Niels Provos entwickelte Software.

Dieses Produkt enthält von Dug Song entwickelte Software. Dieses Produkt enthält von Aaron Campbell entwickelte Software. Dieses Produkt enthält von Damien Miller entwickelte Software. Dieses Produkt enthält von Kevin Steves entwickelte Software.

Dieses Produkt enthält von Daniel Kouril entwickelte Software. Dieses Produkt enthält von Wesley Griffin entwickelte Software. Dieses Produkt enthält von Per Allansson entwickelte Software. Dieses Produkt enthält von Nils Nordman entwickelte Software. Dieses Produkt enthält von Simon Wilkinson entwickelte Software.

Die Verbreitung und Verwendung in Quell- und binärem Format, mit oder ohne Veränderungen, sind unter folgenden Bedingungen erlaubt:

1. Die Verbreitung von Quellcodes muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss beibehalten.
2. Die Verbreitung in binärem Format muss den voranstehenden Copyrightvermerk, diese Liste von Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder andere Materialien, die mit verteilt werden, reproduzieren.

SÄMTLICHE VORGENANNTE SOFTWARE WIRD VOM AUTOR IM IST-ZUSTAND (“AS IS”) BEREITGESTELLT. JEGLICHE AUSDRÜCKLICHEN ODER IMPLIZITEN GARANTIEN, EINSCHLIESSLICH, DOCH NICHT BESCHRÄNKT AUF DIE IMPLIZIERTEN GARANTIEN DER MARKTGÄNGIGKEIT UND DER ANWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK, SIND AUSGESCHLOSSEN.

UNTER KEINEN UMSTÄNDEN HAFTET DER AUTOR FÜR DIREKTE ODER INDIREKTE SCHÄDEN, FÜR BEI VERTRAGSERFÜLLUNG ENTSTANDENE SCHÄDEN, FÜR BESONDERE SCHÄDEN, FÜR SCHADENSERSATZ MIT STRAFCHARAKTER, ODER FÜR FOLGESCHÄDEN EINSCHLIESSLICH, DOCH NICHT BESCHRÄNKT AUF, ERWERB VON ERSATZGÜTERN ODER ERSATZLEISTUNGEN; VERLUST AN NUTZUNG, DATEN ODER GEWINN; ODER GESCHÄFTSUNTERBRECHUNGEN) GLEICH, WIE SIE ENTSTANDEN SIND, UND FÜR JEGLICHE ART VON HAFTUNG, SEI ES VERTRÄGE, GEFÄHRDUNGSHAFTUNG, ODER DELIKTISCHE HAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER ANDERE), DIE IN JEGLICHER FORM FOLGE DER BENUTZUNG DIESER SOFTWARE IST, SELBST WENN AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WURDE.

Standard Warranty

The following standard warranty is presented in English, French, and German.

Standard Warranty

Radware offers a limited warranty for all its products (“Products”). Radware hardware products are warranted against defects in material and workmanship for a period of one year from date of shipment. Radware software carries a standard warranty that provides bug fixes for up to 90 days after date of purchase. Should a Product unit fail anytime during the said period(s), Radware will, at its discretion, repair or replace the Product.

For hardware warranty service or repair, the product must be returned to a service facility designated by Radware. Customer shall pay the shipping charges to Radware and Radware shall pay the shipping charges in

returning the product to the customer. Please see specific details outlined in the Standard Warranty section of the customer's purchase order.

Radware shall be released from all obligations under its Standard Warranty in the event that the Product and/or the defective component has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than Radware authorized service personnel, unless such repairs by others were made with the written consent of Radware.

EXCEPT AS SET FORTH ABOVE, ALL RADWARE PRODUCTS (HARDWARE AND SOFTWARE) ARE PROVIDED BY "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

Garantie standard

Radware octroie une garantie limitée pour l'ensemble de ses produits ("Produits"). Le matériel informatique (hardware) Radware est garanti contre tout défaut matériel et de fabrication pendant une durée d'un an à compter de la date d'expédition. Les logiciels (software) Radware sont fournis avec une garantie standard consistant en la fourniture de correctifs des dysfonctionnements du logiciels (bugs) pendant une durée maximum de 90 jours à compter de la date d'achat. Dans l'hypothèse où un Produit présenterait un défaut pendant ladite (lesdites) période(s), Radware procédera, à sa discrétion, à la réparation ou à l'échange du Produit.

S'agissant de la garantie d'échange ou de réparation du matériel informatique, le Produit doit être retourné chez un réparateur désigné par Radware. Le Client aura à sa charge les frais d'envoi du Produit à Radware et Radware supportera les frais de retour du Produit au client. Veuillez consulter les conditions spécifiques décrites dans la partie "Garantie Standard" du bon de commande client.

Radware est libérée de toutes obligations liées à la Garantie Standard dans l'hypothèse où le Produit et/ou le composant défectueux a fait l'objet d'un mauvais usage, d'une négligence, d'un accident ou d'une installation non conforme, ou si les réparations ou les modifications qu'il a subi ont été effectuées par d'autres personnes que le personnel de maintenance autorisé par Radware, sauf si Radware a donné son consentement écrit à ce que de telles réparations soient effectuées par ces personnes.

SAUF DANS LES CAS PREVUS CI-DESSUS, L'ENSEMBLE DES PRODUITS RADWARE (MATERIELS ET LOGICIELS) SONT FOURNIS "TELS QUELS" ET TOUTES GARANTIES EXPRESSES OU IMPLICITES SONT EXCLUES, EN CE COMPRIS, MAIS SANS S'Y RESTREINDRE, LES GARANTIES IMPLICITES DE QUALITE MARCHANDE ET D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE.

Standard Garantie

Radware bietet eine begrenzte Garantie für alle seine Produkte ("Produkte") an. Hardware Produkte von Radware haben eine Garantie gegen Material- und Verarbeitungsfehler für einen Zeitraum von einem Jahr ab Lieferdatum. Radware Software verfügt über eine Standard Garantie zur Fehlerbereinigung für einen Zeitraum von bis zu 90 Tagen nach Erwerbsdatum. Sollte ein Produkt innerhalb des angegebenen Garantiezeitraumes einen Defekt aufweisen, wird Radware das Produkt nach eigenem Ermessen entweder reparieren oder ersetzen.

Für den Hardware Garantieservice oder die Reparatur ist das Produkt an eine von Radware bezeichnete Serviceeinrichtung zurückzugeben. Der Kunde hat die Versandkosten für den Transport des Produktes zu Radware zu tragen, Radware übernimmt die Kosten der Rückversendung des Produktes an den Kunden. Genauere Angaben entnehmen Sie bitte dem Abschnitt zur Standard Garantie im Bestellformular für Kunden.

Radware ist von sämtlichen Verpflichtungen unter seiner Standard Garantie befreit, sofern das Produkt oder der fehlerhafte Teil zweckentfremdet genutzt, in der Pflege vernachlässigt, einem Unfall ausgesetzt oder unsachgemäß installiert wurde oder sofern Reparaturen oder Modifikationen von anderen Personen als durch Radware autorisierten Kundendienstmitarbeitern vorgenommen wurden, es sei denn, diese Reparatur

durch besagte andere Personen wurden mit schriftlicher Genehmigung seitens Radware durchgeführt.

MIT AUSNAHME DES OBEN DARGESTELLTEN, SIND ALLE RADWARE PRODUKTE (HARDWARE UND SOFTWARE) GELIEFERT “WIE GESEHEN” UND JEGLICHE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN, EINSCHLIESSLICH ABER NICHT BEGRENZT AUF STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUSGESCHLOSSEN.

Limitations on Warranty and Liability

The following limitations on warranty and liability are presented in English, French, and German.

Limitations on Warranty and Liability

IN NO EVENT SHALL RADWARE LTD. OR ANY OF ITS AFFILIATED ENTITIES BE LIABLE FOR ANY DAMAGES INCURRED BY THE USE OF THE PRODUCTS (INCLUDING BOTH HARDWARE AND SOFTWARE) DESCRIBED IN THIS USER GUIDE, OR BY ANY DEFECT OR INACCURACY IN THIS USER GUIDE ITSELF. THIS INCLUDES BUT IS NOT LIMITED TO ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION). THE ABOVE LIMITATIONS WILL APPLY EVEN IF RADWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES OR LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Limitations de la Garantie et Responsabilité

RADWARE LTD. OU SES ENTITIES AFFILIES NE POURRONT EN AUCUN CAS ETRE TENUES RESPONSABLES DES DOMMAGES SUBIS DU FAIT DE L’UTILISATION DES PRODUITS (EN CE COMPRIS LES MATERIELS ET LES LOGICIELS) DECRITS DANS CE MANUEL D’UTILISATION, OU DU FAIT DE DEFAUT OU D’IMPRECISIONS DANS CE MANUEL D’UTILISATION, EN CE COMPRIS, SANS TOUTEFOIS QUE CETTE ENUMERATION SOIT CONSIDEREE COMME LIMITATIVE, TOUS DOMMAGES DIRECTS, INDIRECTS, ACCIDENTELS, SPECIAUX, EXEMPLAIRES, OU ACCESSOIRES (INCLUANT, MAIS SANS S’Y RESTREINDRE, LA FOURNITURE DE PRODUITS OU DE SERVICES DE REMPLACEMENT; LA PERTE D’UTILISATION, DE DONNEES OU DE PROFITS; OU L’INTERRUPTION DES AFFAIRES). LES LIMITATIONS CI-DESSUS S’APPLIQUERONT QUAND BIEN MEME RADWARE A ETE INFORMEE DE LA POSSIBLE EXISTENCE DE CES DOMMAGES. CERTAINES JURIDICTIONS N’ADMETTANT PAS LES EXCLUSIONS OU LIMITATIONS DE GARANTIES IMPLICITES OU DE RESPONSABILITE EN CAS DE DOMMAGES ACCESSOIRES OU INDIRECTS, LESDITES LIMITATIONS OU EXCLUSIONS POURRAIENT NE PAS ETRE APPLICABLE DANS VOTRE CAS.

Haftungs- und Gewährleistungsausschluss

IN KEINEM FALL IST RADWARE LTD. ODER EIN IHR VERBUNDENES UNTERNEHMEN HAFTBAR FÜR SCHÄDEN, WELCHE BEIM GEBRAUCH DES PRODUKTES (HARDWARE UND SOFTWARE) WIE IM BENUTZERHANDBUCH BESCHRIEBEN, ODER AUFGRUND EINES FEHLERS ODER EINER UNGENAUIGKEIT IN DIESEM BENUTZERHANDBUCH SELBST ENTSTANDEN SIND. DAZU GEHÖREN UNTER ANDEREM (OHNE DARAUF BEGRENZT ZU SEIN) JEGLICHE DIREKTEN; IDIREKTEN; NEBEN; SPEZIELLEN, BELEGTEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH ABER NICHT BEGRENZT AUF BESCHAFFUNG ODER ERSATZ VON WAREN ODER DIENSTEN, NUTZUNGSAUSFALL, DATEN- ODER GEWINNVERLUST ODER BETRIEBSUNTERBRECHUNGEN). DIE OBEN GENANNTEN BEGRENZUNGEN GREIFEN AUCH, SOFERN RADWARE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SEIN SOLLTE. EINIGE RECHTSORDNUNGEN LASSEN EINEN AUSSCHLUSS ODER EINE BEGRENZUNG STILLSCHWEIGENDER GARANTIEN ODER HAFTUNGEN BEZÜGLICH NEBEN- ODER FOLGESCHÄDEN NICHT

ZU, SO DASS DIE OBEN DARGESTELLTE BEGRENZUNG ODER DER AUSSCHLUSS SIE UNTER UMSTÄNDEN NICHT BETREFFEN WIRD.

Safety Instructions

The following safety instructions are presented in English, French, and German.

Safety Instructions

CAUTION

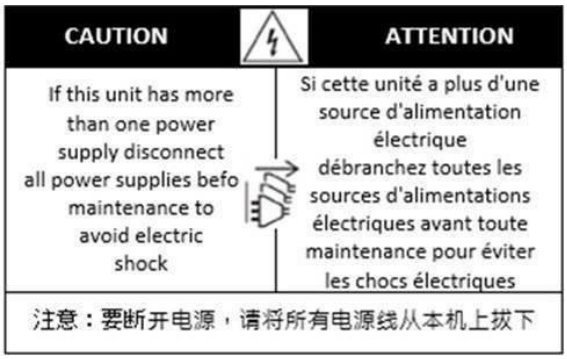
A readily accessible disconnect device shall be incorporated in the building installation wiring.

Due to the risks of electrical shock, and energy, mechanical, and fire hazards, any procedures that involve opening panels or changing components must be performed by qualified service personnel only.

To reduce the risk of fire and electrical shock, disconnect the device from the power line before removing cover or panels.

The following figure shows the caution label that is attached to Radware platforms with dual power supplies.

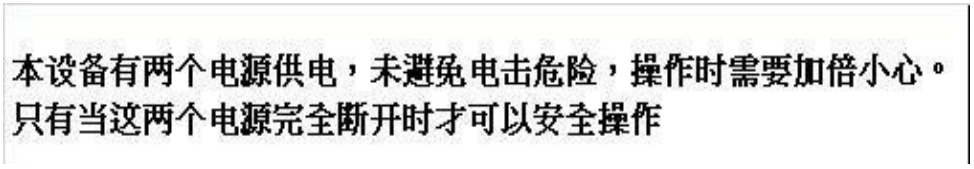
Figure 1: Electrical Shock Hazard Label



DUAL-POWER-SUPPLY-SYSTEM SAFETY WARNING IN CHINESE

The following figure is the warning for Radware platforms with dual power supplies.

Figure 2: Dual-Power-Supply-System Safety Warning in Chinese



Translation of Dual-Power-Supply-System Safety Warning in Chinese:

This unit has more than one power supply. Disconnect all power supplies before maintenance to avoid electric shock.

SERVICING

Do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so. There are no serviceable parts inside the unit.

HIGH VOLTAGE

Any adjustment, maintenance, and repair of the opened instrument under voltage must be avoided as much as possible and, when inevitable, must be carried out only by a skilled person who is aware of the hazard involved.

Capacitors inside the instrument may still be charged even if the instrument has been disconnected from its source of supply.

GROUNDING

Before connecting this device to the power line, the protective earth terminal screws of thisdevice must be connected to the protective earth in the building installation.

LASER

This equipment is a Class 1 Laser Product in accordance with IEC60825 - 1: 1993 + A1:1997 + A2:2001 Standard.

FUSES

Make sure that only fuses with the required rated current and of the specified type are used for replacement. The use of repaired fuses and the short-circuiting of fuse holders must be avoided. Whenever it is likely that the protection offered by fuses has been impaired, the instrument must be made inoperative and be secured against any unintended operation.

LINE VOLTAGE

Before connecting this instrument to the power line, make sure the voltage of the power source matches the requirements of the instrument. Refer to the Specifications for information about the correct power rating for the device.

48V DC-powered platforms have an input tolerance of 36-72V DC.

SPECIFICATION CHANGES

Specifications are subject to change without notice.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15B of the FCC Rules and EN55022 Class A, EN 55024; EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8 and IEC 61000-4-11For CE MARK Compliance.
These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

SPECIAL NOTICE FOR NORTH AMERICAN USERS

For North American power connection, select a power supply cord that is UL Listed and CSA Certified 3 - conductor, [18 AWG], terminated in a molded on plug cap rated 125 V, [10 A], with a minimum length of 1.5m [six feet] but no longer than 4.5m...For European connection, select a power supply cord that is internationally harmonized and marked “<HAR>”, 3 - conductor, 0,75 mm2 minimum mm2 wire, rated 300 V, with a PVC insulated jacket. The cord must have a molded on plug cap rated 250 V, 3 A.

RESTRICT AREA ACCESS

The DC powered equipment should only be installed in a Restricted Access Area.

INSTALLATION CODES

This device must be installed according to country national electrical codes. For North America, equipment must be installed in accordance with the US National Electrical Code, Articles 110 - 16, 110 -17, and 110 - 18 and the Canadian Electrical Code, Section 12.

INTERCONNECTION OF UNITS

Cables for connecting to the unit RS232 and Ethernet Interfaces must be UL certified type DP-1 or DP-2. (Note- when residing in non LPS circuit)

OVERCURRENT PROTECTION

A readily accessible listed branch-circuit over current protective device rated 15 A must be incorporated in the building wiring for each power input.

REPLACEABLE BATTERIES

If equipment is provided with a replaceable battery, and is replaced by an incorrect battery type, then an explosion may occur. This is the case for some Lithium batteries and the following is applicable:

- If the battery is placed in an **Operator Access Area**, there is a marking close to the battery or a statement in both the operating and service instructions.
- If the battery is placed elsewhere in the equipment, there is a marking close to the battery or a statement in the service instructions.

This marking or statement includes the following text warning:

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT BATTERY TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

Caution – To Reduce the Risk of Electrical Shock and Fire

1. This equipment is designed to permit connection between the earthed conductor of the DC supply circuit and the earthing conductor equipment. See Installation Instructions.
2. All servicing must be undertaken only by qualified service personnel. There are not user serviceable parts inside the unit.
3. DO NOT plug in, turn on or attempt to operate an obviously damaged unit.
4. Ensure that the chassis ventilation openings in the unit are NOT BLOCKED.
5. Replace a blown fuse ONLY with the same type and rating as is marked on the safety label adjacent to the power inlet, housing the fuse.
6. Do not operate the device in a location where the maximum ambient temperature exceeds 40° C/104° F.
7. Be sure to unplug the power supply cord from the wall socket BEFORE attempting to remove and/or check the main power fuse.

CLASS 1 LASER PRODUCT AND REFERENCE TO THE MOST RECENT LASER STANDARDS IEC 60 825-1:1993 + A1:1997 + A2:2001 AND EN 60825-1:1994+A1:1996+ A2:2001

AC units for Denmark, Finland, Norway, Sweden (marked on product):

- Denmark - “Unit is class I – unit to be used with an AC cord set suitable with Denmark deviations. The cord includes an earthing conductor. The Unit is to be plugged into a wall socket outlet which is connected to a protective earth. Socket outlets which are not connected to earth are not to be used!”
- Finland – (Marking label and in manual) - “Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan”
- Norway (Marking label and in manual) - “Apparatet må tilkoples jordet stikkontakt”
- Unit is intended for connection to IT power systems for Norway only.
- Sweden (Marking label and in manual) - “Apparaten skall anslutas till jordat uttag.”

To connect the power connection:

1. Connect the power cable to the main socket, located on the rear panel of the device.
2. Connect the power cable to the grounded AC outlet.

CAUTION

Risk of electric shock and energy hazard. Disconnecting one power supply disconnects only one power supply module. To isolate the unit completely, disconnect all power supplies.

Instructions de sécurité

AVERTISSEMENT

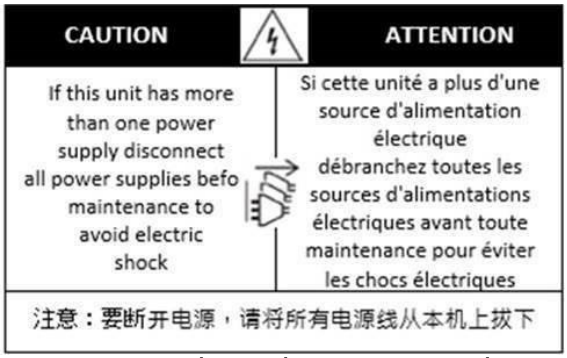
Un dispositif de déconnexion facilement accessible sera incorporé au câblage du bâtiment.

En raison des risques de chocs électriques et des dangers énergétiques, mécaniques et d'incendie, chaque procédure impliquant l'ouverture des panneaux ou le remplacement de composants sera exécutée par du personnel qualifié.

Pour réduire les risques d'incendie et de chocs électriques, déconnectez le dispositif du bloc d'alimentation avant de retirer le couvercle ou les panneaux.

La figure suivante montre l'étiquette d'avertissement apposée sur les plateformes Radware dotées de plus d'une source d'alimentation électrique.

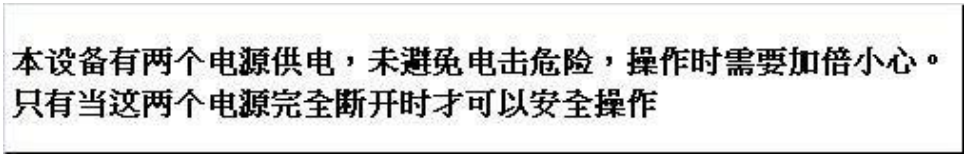
Figure 3: Étiquette d'avertissement de danger de chocs électriques



AVERTISSEMENT DE SÉCURITÉ POUR LES SYSTÈMES DOTÉS DE DEUX SOURCES D'ALIMENTATION ÉLECTRIQUE (EN CHINOIS)

La figure suivante représente l'étiquette d'avertissement pour les plateformes Radware dotées de deux sources d'alimentation électrique.

Figure 4: Avertissement de sécurité pour les systèmes dotes de deux sources d'alimentation électrique (en chinois)



Traduction de la Avertissement de sécurité pour les systèmes dotes de deux sources d'alimentation électrique (en chinois):

Cette unité est dotée de plus d'une source d'alimentation électrique. Déconnectez toutes les sources d'alimentation électrique avant d'entretenir l'appareil ceci pour éviter tout choc électrique.

ENTRETIEN

N'effectuez aucun entretien autre que ceux répertoriés dans le manuel d'instructions, à moins d'être qualifié en la matière. Aucune pièce à l'intérieur de l'unité ne peut être remplacée ou réparée.

HAUTE TENSION

Tout réglage, opération d'entretien et réparation de l'instrument ouvert sous tension doit être évité. Si cela

s'avère indispensable, confiez cette opération à une personne qualifiée et consciente des dangers impliqués.

Les condensateurs au sein de l'unité risquent d'être chargés même si l'unité a été déconnectée de la source d'alimentation électrique.

MISE A LA TERRE

Avant de connecter ce dispositif à la ligne électrique, les vis de protection de la borne de terre de cette unité doivent être reliées au système de mise à la terre du bâtiment.

LASER

Cet équipement est un produit laser de classe 1, conforme à la norme IEC60825 - 1: 1993 + A1: 1997 + A2: 2001.

FUSIBLES

Assurez-vous que, seuls les fusibles à courant nominal requis et de type spécifié sont utilisés en remplacement. L'usage de fusibles réparés et le court-circuitage des porte-fusibles doivent être évités. Lorsqu'il est pratiquement certain que la protection offerte par les fusibles a été détériorée, l'instrument doit être désactivé et sécurisé contre toute opération involontaire.

TENSION DE LIGNE

Avant de connecter cet instrument à la ligne électrique, vérifiez que la tension de la source d'alimentation correspond aux exigences de l'instrument. Consultez les spécifications propres à l'alimentation nominale correcte du dispositif.

Les plateformes alimentées en 48 CC ont une tolérance d'entrée comprise entre 36 et 72 V CC.
MODIFICATIONS DES SPÉCIFICATIONS

Les spécifications sont sujettes à changement sans notice préalable.

Remarque: Cet équipement a été testé et déclaré conforme aux limites définies pour un appareil numérique de classe A, conformément au paragraphe 15B de la réglementation FCC et EN55022 Classe A, EN 55024, EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8, et IEC 61000-4-11, pour la marque de conformité de la CE. Ces limites sont fixées pour fournir une protection raisonnable contre les interférences nuisibles, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément au manuel d'instructions, peut entraîner des interférences nuisibles aux communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l'utilisateur devra corriger le problème à ses propres frais.

NOTICE SPÉCIALE POUR LES UTILISATEURS NORD-AMÉRICAINS

Pour un raccordement électrique en Amérique du Nord, sélectionnez un cordon d'alimentation homologué UL et certifié CSA 3 - conducteur, [18 AWG], muni d'une prise moulée à son extrémité, de 125 V, [10 A], d'une longueur minimale de 1,5 m [six pieds] et maximale de 4,5m...Pour la connexion européenne, choisissez un cordon d'alimentation mondialement homologué et marqué "<HAR>", 3 - conducteur, câble de 0,75 mm2 minimum, de 300 V, avec une gaine en PVC isolée. La prise à l'extrémité du cordon, sera dotée d'un sceau moulé indiquant: 250 V, 3 A.

ZONE A ACCÈS RESTREINT

L'équipement alimenté en CC ne pourra être installé que dans une zone à accès restreint. CODES

D'INSTALLATION

Ce dispositif doit être installé en conformité avec les codes électriques nationaux. En Amérique du Nord, l'équipement sera installé en conformité avec le code électrique national américain, articles 110-16, 110 - 17, et 110 -18 et le code électrique canadien, Section 12.

INTERCONNEXION DES UNÎTES

Les câbles de connexion à l'unité RS232 et aux interfaces Ethernet seront certifiés UL, type DP-1 ou DP-2.

(Remarque- s'ils ne résident pas dans un circuit LPS).

PROTECTION CONTRE LES SURCHARGES

Un circuit de dérivation, facilement accessible, sur le dispositif de protection du courant de 15 A doit être intégré au câblage du bâtiment pour chaque puissance consommée.

BATTERIES REMPLAÇABLES

Si l'équipement est fourni avec une batterie, et qu'elle est remplacée par un type de batterie incorrect, elle est susceptible d'exploser. C'est le cas pour certaines batteries au lithium, les éléments suivants sont donc applicables:

- Si la batterie est placée dans une zone d'accès opérateur, une marque est indiquée sur la batterie ou une remarque est insérée, aussi bien dans les instructions d'exploitation que d'entretien.
- Si la batterie est placée ailleurs dans l'équipement, une marque est indiquée sur la batterieou une remarque est insérée dans les instructions d'entretien.

Cette marque ou remarque inclut l'avertissement textuel suivant:

AVERTISSEMENT

RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UN MODÈLE INCORRECT. METTRE AU REBUT LES BATTERIES CONFORMÉMENT AUX INSTRUCTIONS.

Attention – Pour réduire les risques de chocs électriques et d'incendie

1. Cet équipement est conçu pour permettre la connexion entre le conducteur de mise à la terre du circuit électrique CC et l'équipement de mise à la terre. Voir les instructions d'installation.
2. Tout entretien sera entrepris par du personnel qualifié. Aucune pièce à l'intérieur de l'uniténe peut être remplacée ou réparée.
3. NE branchez pas, n'allumez pas ou n'essayez pas d'utiliser une unitémanifestement endommagée.
4. Vérifiez que l'orifice de ventilation du châssis dans l'unité n'est PAS OBSTRUE.
5. Remplacez le fusible endommagé par un modèle similaire de même puissance, tel qu'indiqué sur l'étiquette de sécurité adjacente à l'arrivée électrique hébergeant le fusible.
6. Ne faites pas fonctionner l'appareil dans un endroit, où la température ambiante dépassela valeur maximale autorisée. 40° C/104° F.
7. Débranchez le cordon électrique de la prise murale AVANT d'essayer de retirer et/ou devérifier le fusible d'alimentation principal.

   PRODUIT LASER DE CLASSE 1 ET RÉFÉRENCE AUX NORMES LASER LES PLUS RÉCENTES: IEC 60 825-1: 1993 + A1: 1997 + A2: 2001 ET EN 60825-1: 1994+A1: 1996+ A2: 2001

   Unités à CA pour le Danemark, la Finlande, la Norvège, la Suède (indiqué sur le produit):

   - Danemark – Unité de classe 1 – qui doit être utilisée avec un cordon CA compatible avec les déviations du Danemark. Le cordon inclut un conducteur de mise à la terre. L'unité sera branchée à une prise murale, mise à la terre. Les prises non-mises à la terre ne seront pas utilisées!
   - Finlande (Étiquette et inscription dans le manuel) – Laite onliitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan
   - Norvège (Étiquette et inscription dans le manuel) – Apparatet må tilkoples jordetstikkontakt
   - L'unité peut être connectée à un système électrique IT (en Norvège uniquement).
   - Suède (Étiquette et inscription dans le manuel) – Apparaten skall anslutas till jordatuttag.

   Pour brancher à l'alimentation électrique:

   1. Branchez le câble d'alimentation à la prise principale, située sur le panneau arrière del'unité.

2. Connectez le câble d'alimentation à la prise CA mise à la terre.

AVERTISSEMENT

Risque de choc électrique et danger énergétique. La déconnexion d'une source d'alimentation électrique ne débranche qu'un seul module électrique. Pour isoler complètement l'unité, débranchez toutes les sources d'alimentation électrique.

ATTENTION

Risque de choc et de danger électriques. Le débranchement d'une seule alimentation stabilisée ne débranche qu'un module "Alimentation Stabilisée". Pour Isoler complètement le module en cause, il faut débrancher toutes les alimentations stabilisées.

Attention: Pour Réduire Les Risques d'Électrocution et d'Incendie

1. Toutes les opérations d'entretien seront effectuées UNIQUEMENT par du personnel d'entretien qualifié. Aucun composant ne peut être entretenu ou remplacée par l'utilisateur.
2. NE PAS connecter, mettre sous tension ou essayer d'utiliser une unité visiblement défectueuse.
3. Assurez-vous que les ouvertures de ventilation du châssis NE SONT PAS OBSTRUÉES.
4. Remplacez un fusible qui a sauté SEULEMENT par un fusible du même type et de même capacité, comme indiqué sur l'étiquette de sécurité proche de l'entrée de l'alimentation qui contient le fusible.
5. NE PAS UTILISER l'équipement dans des locaux dont la température maximale dépasse 40 degrés Centigrades.
6. Assurez vous que le cordon d'alimentation a été déconnecté AVANT d'essayer de l'enlever et/ou vérifier le fusible de l'alimentation générale.

Sicherheitsanweisungen

VORSICHT

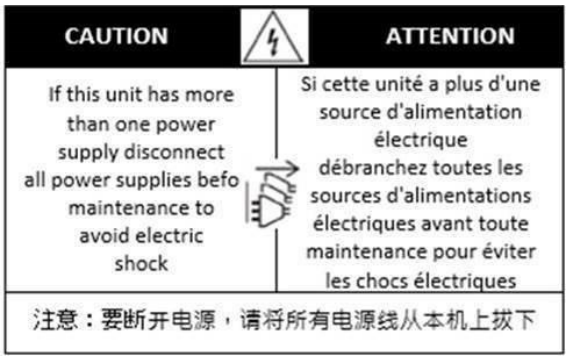
Die Elektroinstallation des Gebäudes muss ein unverzüglich zugängliches Stromunterbrechungsgerät integrieren.

Aufgrund des Stromschlagrisikos und der Energie-, mechanische und Feuergefahr dürfen Vorgänge, in deren Verlauf Abdeckungen entfernt oder Elemente ausgetauscht werden, ausschließlich von qualifiziertem Servicepersonal durchgeführt werden.

Zur Reduzierung der Feuer- und Stromschlaggefahr muss das Gerät vor der Entfernung der Abdeckung oder der Paneele von der Stromversorgung getrennt werden.

Folgende Abbildung zeigt das VORSICHT-Etikett, das auf die Radware-Plattformen mit Doppelspeisung angebracht ist.

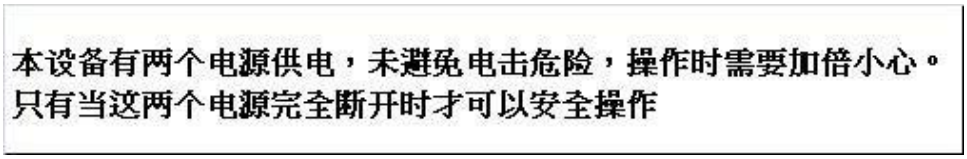
Figure 5: Warnetikett Stromschlaggefahr



SICHERHEITSHINWEIS IN CHINESISCHER SPRACHE FÜR SYSTEME MIT DOPPELSPEISUNG

Die folgende Abbildung ist die Warnung für Radware-Plattformen mit Doppelspeisung.

Figure 6: Sicherheitshinweis in chinesischer Sprache für Systeme mit Doppelspeisung



Übersetzung von Sicherheitshinweis in chinesischer Sprache für Systeme mit Doppelspeisung:

Die Einheit verfügt über mehr als eine Stromversorgungsquelle. Ziehen Sie zur Verhinderung von Stromschlag vor Wartungsarbeiten sämtliche Stromversorgungsleitungen ab.

WARTUNG

Führen Sie keinerlei Wartungsarbeiten aus, die nicht in der Betriebsanleitung angeführt sind, es sei denn, Sie sind dafür qualifiziert. Es gibt innerhalb des Gerätes keine wartungsfähigen Teile.

HOCHSPANNUNG

Jegliche Einstellungs-, Instandhaltungs- und Reparaturarbeiten am geöffneten Gerät unter Spannung müssen so weit wie möglich vermieden werden. Sind sie nicht vermeidbar, dürfen sie ausschließlich von qualifizierten Personen ausgeführt werden, die sich der Gefahr bewusst sind.

Innerhalb des Gerätes befindliche Kondensatoren können auch dann noch Ladung enthalten, wenn das Gerät von der Stromversorgung abgeschnitten wurde.

ERDUNG

Bevor das Gerät an die Stromversorgung angeschlossen wird, müssen die Schrauben der Erdungsleitung des Gerätes an die Erdung der Gebäudeverkabelung angeschlossen werden.

LASER

Dieses Gerät ist ein Laser-Produkt der Klasse 1 in Übereinstimmung mit IEC60825 - 1: 1993 + A1:1997 + A2:2001 Standard.

SICHERUNGEN

Vergewissern Sie sich, dass nur Sicherungen mit der erforderlichen Stromstärke und der angeführten Art verwendet werden. Die Verwendung reparierter Sicherungen sowie die Kurzschließung von Sicherungsfassungen muss vermieden werden. In Fällen, in denen wahrscheinlich ist, dass der von den Sicherungen gebotene Schutz beeinträchtigt ist, muss das Gerät abgeschaltet und gegen unbeabsichtigten Betrieb gesichert werden.

LEITUNGSSPANNUNG

Vor Anschluss dieses Gerätes an die Stromversorgung ist zu gewährleisten, dass die Spannung der Stromquelle den Anforderungen des Gerätes entspricht. Beachten Sie die technischen Angaben bezüglich der korrekten elektrischen Werte des Gerätes.

Plattformen mit 48 V DC verfügen über eine Eingangstoleranz von 36-72 V DC.

ÄNDERUNGEN DER TECHNISCHEN ANGABEN

Änderungen der technischen Spezifikationen bleiben vorbehalten.

Hinweis: Dieses Gerät wurde geprüft und entspricht den Beschränkungen von digitalen Geräten der Klasse 1 gemäß Teil 15B FCC-Vorschriften und EN55022 Klasse A, EN55024; EN 61000-3-2; EN; IEC 61000 4-2 to4-6, IEC 61000 4-8 und IEC 61000-4- 11 für Konformität mit der CE-Bezeichnung.
Diese Beschränkungen dienen dem angemessenen Schutz vor schädlichen Interferenzen bei Betrieb des Gerätes in kommerziellem Umfeld. Dieses Gerät erzeugt, verwendet und strahlt elektromagnetische Hochfrequenzstrahlung aus. Wird es nicht entsprechend den Anweisungen im Handbuch montiert und benutzt, könnte es mit dem Funkverkehr interferieren und ihn beeinträchtigen. Der Betrieb dieses Gerätes in Wohnbereichen wird höchstwahrscheinlich zu schädlichen Interferenzen führen. In einem solchen Fall wäre der Benutzer verpflichtet, diese Interferenzen auf eigene Kosten zu korrigieren.

BESONDERER HINWEIS FÜR BENUTZER IN NORDAMERIKA

Wählen Sie für den Netzstromanschluss in Nordamerika ein Stromkabel, das in der UL aufgeführt und CSA-zertifiziert ist 3 Leiter, [18 AWG], endend in einem gegossenen Stecker, für 125 V, [10 A], mit einer Mindestlänge von 1,5 m [sechs Fuß], doch nicht länger als 4,5 m. Für europäische Anschlüsse verwenden Sie ein international harmonisiertes, mit “<HAR>” markiertes Stromkabel, mit 3 Leitern von mindestens 0,75 mm2, für 300 V, mit PVC-Umkleidung. Das Kabel muss in einem gegossenen Stecker für 250 V, 3 A enden.

BEREICH MIT EINGESCHRÄNKTEM ZUGANG

Das mit Gleichstrom betriebene Gerät darf nur in einem Bereich mit eingeschränktem Zugang montiert werden.

INSTALLATIONSCODES

Dieses Gerät muss gemäß der landesspezifischen elektrischen Codes montiert werden. In Nordamerika müssen Geräte entsprechend dem US National Electrical Code, Artikel 110 - 16, 110 - 17 und 110 - 18, sowie dem Canadian Electrical Code, Abschnitt 12, montiert werden.
VERKOPPLUNG VON GERÄTEN Kabel für die Verbindung des Gerätes mit RS232- und Ethernet- müssen UL-zertifiziert und vom Typ DP-1 oder DP-2 sein. (Anmerkung: bei Aufenthalt in einem nicht-LPS-Stromkreis)

ÜBERSTROMSCHUTZ

Ein gut zugänglicher aufgeführter Überstromschutz mit Abzweigstromkreis und 15 A Stärke muss für jede Stromeingabe in der Gebäudeverkabelung integriert sein.

AUSTAUSCHBARE BATTERIEN

Wird ein Gerät mit einer austauschbaren Batterie geliefert und für diese Batterie durch einen falschen Batterietyp ersetzt, könnte dies zu einer Explosion führen. Dies trifft zu für manche Arten von Lithiumsbatterien zu, und das folgende gilt es zu beachten:

- Wird die Batterie in einem Bereich für Bediener eingesetzt, findet sich in der Nähe der Batterie eine Markierung oder Erklärung sowohl im Betriebshandbuch als auch in der Wartungsanleitung.
- Ist die Batterie an einer anderen Stelle im Gerät eingesetzt, findet sich in der Nähe der Batterie eine

Markierung oder einer Erklärung in der Wartungsanleitung.

Diese Markierung oder Erklärung enthält den folgenden Warntext: VORSICHT

EXPLOSIONSGEFAHR, FALLS BATTERIE DURCH EINEN FALSCHEN BATTERIETYP ERSETZT WIRD. GEBRAUCHTE BATTERIEN DEN ANWEISUNGEN ENTSPRECHEND ENTSORGEN.

- Denmark - “Unit is class I - mit Wechselstromkabel benutzen, dass für die Abweichungen in Dänemark eingestellt ist. Das Kabel ist mit einem Erdungsdraht versehen. Das Kabel wird in eine geerdete Wandsteckdose angeschlossen. Keine Steckdosen ohne Erdungsleitungverwenden!”
- Finland - (Markierungsetikett und im Handbuch) - Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan
- Norway - (Markierungsetikett und im Handbuch) - Apparatet må tilkoples jordet stikkontakt Ausschließlich für Anschluss an IT-Netzstromsysteme in Norwegen vorgesehen
- Sweden - (Markierungsetikett und im Handbuch) - Apparaten skall anslutas till jordatuttag.

Anschluss des Stromkabels:

1. Schließen Sie das Stromkabel an den Hauptanschluss auf der Rückseite des Gerätes an.
2. Schließen Sie das Stromkabel an den geerdeten Wechselstromanschlussan.

VORSICHT

Stromschlag- und Energiegefahr Die Trennung einer Stromquelle trennt nur ein Stromversorgungsmodul von der Stromversorgung. Um das Gerät komplett zu isolieren, muss es von der gesamten Stromversorgung getrennt werden.

Vorsicht - Zur Reduzierung der Stromschlag- und Feuergefahr

1. Dieses Gerät ist dazu ausgelegt, die Verbindung zwischen der geerdeten Leitungdes Gleichstromkreises und dem Erdungsleiter des Gerätes zu ermöglichen. Siehe Montageanleitung.
2. Wartungsarbeiten jeglicher Art dürfen nur von qualifiziertem Servicepersonalausgeführt werden. Es gibt innerhalb des Gerätes keine vom Benutzer zu wartenden Teile.
3. Versuchen Sie nicht, ein offensichtlich beschädigtes Gerät an den Stromkreis anzuschließen, einzuschalten oder zu betreiben.
4. Vergewissern Sie sich, dass sie Lüftungsöffnungen im Gehäuse des GerätesNICHT BLOCKIERT SIND.
5. Ersetzen Sie eine durchgebrannte Sicherung ausschließlich mit dem selben Typ und von der selben Stärke, die auf dem Sicherheitsetikett angeführt sind, das sich neben dem Stromkabelanschluss, am Sicherungsgehäuse.
6. Betreiben Sie das Gerät nicht an einem Standort, an dem die Höchsttemperatur der Umgebung 40° C überschreitet.
7. Vergewissern Sie sich, das Stromkabel aus dem Wandstecker zu ziehen, BEVOR Siedie Hauptsicherung entfernen und/oder prüfen.

Electromagnetic-Interference Statements

The following statements are presented in English, French, and German.

Electromagnetic-Interference Statements

SPECIFICATION CHANGES

Specifications are subject to change without notice.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15B of the FCC Rules and EN55022 Class A, EN 55024; EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8 and IEC 61000-4-11For CE MARK Compliance.
These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

VCCI ELECTROMAGNETIC-INTERFERENCE STATEMENTS

Figure 7: Statement for Class A VCCI-certified Equipment

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Translation of Statement for Class A VCCI-certified Equipment:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

KCC KOREA

Figure 8: KCC–Korea Communications Commission Certificate of Broadcasting and Communication Equipment

Figure 9: Statement For Class A KCC-certified Equipment in Korean

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Translation of Statement For Class A KCC-certified Equipment in Korean:

This equipment is Industrial (Class A) electromagnetic wave suitability equipment and seller or user should take notice of it, and this equipment is to be used in the places except for home.

BSMI

Figure 10: Statement for Class A BSMI-certified Equipment

這是甲類的資訊產品，在居住的環境使用中時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Translation of Statement for Class A BSMI-certified Equipment:

This is a Class A product, in use in a residential environment, it may cause radio interference in which case the user will be required to take adequate measures.

Déclarations sur les Interférences Électromagnétiques

MODIFICATIONS DES SPÉCIFICATIONS

Les spécifications sont sujettes à changement sans notice préalable.

Remarque: Cet équipement a été testé et déclaré conforme aux limites définies pour un appareil numérique de classe A, conformément au paragraphe 15B de la réglementation FCC et EN55022 Classe A, EN 55024, EN 61000-3-2; EN 61000-3-3; IEC 61000 4-2 to 4-6, IEC 61000 4-8, et IEC 61000-4-11, pour la marque de conformité de la CE. Ces limites sont fixées pour fournir une protection raisonnable contre les interférences nuisibles, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément au manuel d'instructions, peut entraîner des interférences nuisibles aux communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l'utilisateur devra corriger le problème à ses propres frais.

DÉCLARATIONS SUR LES INTERFÉRENCES ÉLECTROMAGNÉTIQUES VCCI

Figure 11: Déclaration pour l'équipement de classe A certifié VCCI

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Traduction de la Déclaration pour l'équipement de classe A certifié VCCI:

Il s'agit d'un produit de classe A, basé sur la norme du Voluntary Control Council for Interference by Information Technology Equipment (VCCI). Si cet équipement est utilisé dans un environnement domestique, des perturbations radioélectriques sont susceptibles d'apparaître. Si tel est le cas, l'utilisateur sera tenu de prendre des mesures correctives.

KCC Corée

Figure 12: KCC–Certificat de la commission des communications de Corée pour les equipements de radiodiffusion et communication.

Figure 13: Déclaration pour l'équipement de classe A certifié KCC en langue coréenne

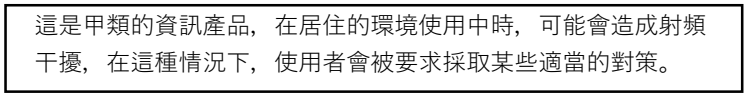
이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Translation de la Déclaration pour l'équipement de classe A certifié KCC en langue coréenne:

Cet équipement est un matériel (classe A) en adéquation aux ondes électromagnétiques et le vendeur ou l'utilisateur doit prendre cela en compte. Ce matériel est donc fait pour être utilisé ailleurs qu' á la maison.

BSMI

Figure 14: Déclaration pour l'équipement de classe A certifié BSMI



Translation de la Déclaration pour l'équipement de classe A certifié BSMI:

Il s'agit d'un produit de Classe A; utilisé dans un environnement résidentiel il peut provoquer des interférences, l'utilisateur devra alors prendre les mesures adéquates.

Erklärungen zu Elektromagnetischer Interferenz

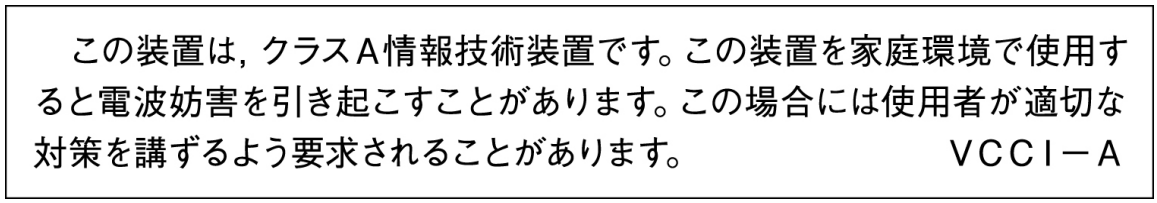
ÄNDERUNGEN DER TECHNISCHEN ANGABEN

Änderungen der technischen Spezifikationen bleiben vorbehalten.

Hinweis: Dieses Gerät wurde geprüft und entspricht den Beschränkungen von digitalen Geräten der Klasse 1 gemäß Teil 15B FCC-Vorschriften und EN55022 Klasse A, EN55024; EN 61000-3-2; EN; IEC 61000 4-2 to4-6, IEC 61000 4-8 und IEC 61000-4- 11 für Konformität mit der CE-Bezeichnung.
Diese Beschränkungen dienen dem angemessenen Schutz vor schädlichen Interferenzen bei Betrieb des Gerätes in kommerziellem Umfeld. Dieses Gerät erzeugt, verwendet und strahlt elektromagnetische Hochfrequenzstrahlung aus. Wird es nicht entsprechend den Anweisungen im Handbuch montiert und benutzt, könnte es mit dem Funkverkehr interferieren und ihn beeinträchtigen. Der Betrieb dieses Gerätes in Wohnbereichen wird höchstwahrscheinlich zu schädlichen Interferenzen führen. In einem solchen Fall wäre der Benutzer verpflichtet, diese Interferenzen auf eigene Kosten zu korrigieren.

ERKLÄRUNG DER VCCI ZU ELEKTROMAGNETISCHER INTERFERENZ

Figure 15: Erklärung zu VCCI-zertifizierten Geräten der Klasse A



Übersetzung von Erklärung zu VCCI-zertifizierten Geräten der Klasse A:

Dies ist ein Produkt der Klasse A gemäß den Normen des Voluntary Control Council for Interference by Information Technology Equipment (VCCI). Wird dieses Gerät in einem Wohnbereich benutzt, können

elektromagnetische Störungen auftreten. In einem solchen Fall wäre der Benutzer verpflichtet, korrigierend einzugreifen.

KCC KOREA

Figure 16: KCC–Korea Communications Commission Zertifikat für Rundfunk-und Nachrichtentechnik

Figure 17: Erklärung zu KCC-zertifizierten Geräten der Klasse A

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Übersetzung von Erklärung zu KCC-zertifizierten Geräten der Klasse A:

Verkäufer oder Nutzer sollten davon Kenntnis nehmen, daß dieses Gerät der Klasse A für industriell elektromagnetische Wellen geeignete Geräten angehört und dass diese Geräte nicht für den heimischen Gebrauch bestimmt sind.

BSMI

Figure 18: Erklärung zu BSMI-zertifizierten Geräten der Klasse A

這是甲類的資訊產品，在居住的環境使用中時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Übersetzung von Erklärung zu BSMI-zertifizierten Geräten der Klasse A:

Dies ist ein Class A Produkt, bei Gebrauch in einer Wohnumgebung kann es zu Funkstörungen kommen, in diesem Fall ist der Benutzer verpflichtet, angemessene Maßnahmen zu ergreifen.

Altitude and Climate Warning

This warning only applies to The People's Republic of China.

1. 对于在非热带气候条件下运行的设备而言，Tma：为制造商规范允许的最大环境温度，或者为 25°C，采用两者中的较大者。
2. 关于在海拔不超过 2000m 或者在非热带气候地区使用的设备，附加警告要求如下：

关于在海拔不超过 2000m 的地区使用的设备，必须在随时可见的位置处粘贴包含如下内容或者类似用语的警告标记、或者附件 DD 中的符号。

“ 只可在海拔不超过 2000m 的位置使用。”

关于在非热带气候地区使用的设备，必须在随时可见的位置处粘贴包含如下内容的警告标记：

附件 DD：有关新安全警告标记的说明

。DD.1 海拔警告标记

标记含义：设备的评估仅基于 2000m 以下的海拔高度，因此设备只适用于该运行条件。如果在海拔超过 2000m 的位置使用设备，可能会存在某些安全隐患。

DD.2 气候警告标记

标记含义：设备的评估仅基于温带气候条件，因此设备只适用于该运行条件。如果在热带气候地区使用设备，可能会存在某些安全隐患。

Document Conventions

The following describes the conventions and symbols that this guide uses:

Item	Description	Description	Beschreibung
Example	An example scenario	Un scénario d’exemple	Ein Beispielszenarium
Caution:	Possible damage to equipment, software, or data	Endommagement possible de l’équipement, des données ou du logiciel	Mögliche Schäden an Gerät, Software oder Daten
Note:	Additional information	Informations complémentaires	Zusätzliche Informationen
To	A statement and instructions	Références et instructions	Eine Erklärung und Anweisungen
Tip:	A suggestion or workaround	Une suggestion ou solution	Ein Vorschlag oder eine Umgehung

 **Warning:**	Possible physical harm to the operator	Blessure possible de l'opérateur	Verletzungsgefahr des Bedieners

TABLE OF CONTENTS

IMPORTANT NOTICES 3
COPYRIGHT NOTICES 4
STANDARD WARRANTY 9
LIMITATIONS ON WARRANTY AND LIABILITY 11
SAFETY INSTRUCTIONS 12
ELECTROMAGNETIC-INTERFERENCE STATEMENTS 21
ALTITUDE AND CLIMATE WARNING 25
DOCUMENT CONVENTIONS 26

TABLE OF CONTENTS 28

CHAPTER 1 - INTRODUCTION 34

RADWARE DEFENSEPRO DDOS MITIGATION–OVERVIEW 34
RADWARE DEFENSEPRO DDOS MITIGATION SYSTEM COMPONENTS 35
SUBSCRIPTION SERVICES 36
ERT Security Update Service (SUS) 36
ERT Active Attackers Feed (EAAF) 37
Geolocation Feed 37
NETWORK CONNECTIVITY 38
MANAGEMENT INTERFACES–APSOLUTE VISION AND OTHERS 38
RADWARE DEFENSEPRO DDOS MITIGATION FEATURES 39
Security Protections 39
Inspection of Tunneled Traffic 40
Real-Time Security Reporting 41
Historical Security Reporting–APSolute Vision Reporter 41
Real-time and Historical Reporting–APSolute Vision Analytics 41
RELATED DOCUMENTATION 42
Radware DefensePro DDoS Mitigation Release Notes 42
APSolute Vision Documentation 42
APSolute Vision Reporter Documentation 43
APSolute Vision Analytics Documentation 43

CHAPTER 2 - GETTING STARTED 44

LOGGING IN TO APSOLUTE VISION 44
CHANGING THE PASSWORD FOR LOCAL APSOLUTE VISION USERS 46
APSOLUTE VISION USER INTERFACE OVERVIEW 46
APSolute Vision Toolbar and Sidebar Menu 47
APSolute Vision Settings View 49
Device Pane 52
Device-Properties Pane 53
Configuration Perspective 54
Monitoring Perspective 56
Security Monitoring Perspective 56
SELECTING YOUR LANDING PAGE 57
USING COMMON GUI ELEMENTS IN APSOLUTE VISION 58
Icons/Buttons and Commands for Managing Table Entries 58
Filtering Table Rows 59

MANAGING RADWARE DEFENSEPRO DDOS MITIGATION DEVICES, APSOLUTE VISION SITES, AND LOGICAL GROUPS.. 60
Using the Device Pane *60*
Managing Individual Radware DefensePro DDoS Mitigation Devices in APSolute Vision *63*
APSolute Vision Server Registered for Device Events–Radware DefensePro DDoS Mitigation *68*
Locking and Unlocking Devices *69*
Using the Multi-Device View and the Multiple Devices Summary *70*
Using Logical Groups of Devices *73*
After You Set Up Your Managed Devices *77*

CHAPTER 3 – MANAGING THE RADWARE DEFENSEPRO DDOS MITIGATION SETUP 78

MANAGING SOFTWARE VERSIONS 78
Uploading Radware DefensePro DDoS Mitigation Software *80*
CONFIGURING THE GLOBAL PARAMETERS 82
Viewing and Configuring Basic Global Parameters *82*
Upgrading Licenses for Radware DefensePro DDoS Mitigation Devices *83*
CONFIGURING DATE AND TIME PARAMETERS 84
CONFIGURING THE NETWORKING SETUP 84
Configuring the General Parameters of the Radware DefensePro DDoS Mitigation Networking Setup *84*
Configuring IP Interface Management in the Networking Setup *85*
Configuring DNS for the Radware DefensePro DDoS Mitigation Networking Setup *88*
CONFIGURING THE DEVICE-SECURITY SETUP 89
Configuring Access Protocols for the Radware DefensePro DDoS Mitigation Device-Security Setup *89*
Configuring Authentication Protocols for Device Management *91*
Configuring SNMP in the Radware DefensePro DDoS Mitigation Device- Security Setup *95*
Configuring Device Users in the Radware DefensePro DDoS Mitigation Device-Security Setup *105*
Configuring Advanced Parameters in the Radware DefensePro DDoS Mitigation Device-Security

Setup *107*
CONFIGURING THE SSL-SETTINGS SETUP 107
Configuring the SSL-Decryption-and-Encryption Option *108*
Managing SSL/TLS Certificates *110*
Managing Protected SSL Objects *119*
CONFIGURING THE SECURITY-SETTINGS SETUP 122
Configuring Global Anti-Scanning Protection Settings *122*
Configuring Global Behavioral DoS Protection *123*
Configuring Global DNS Flood Protection *126*
Configuring Global HTTPS Flood Protection *130*
Configuring Global Out-of-State Protection *130*
Configuring Global Signature Protection *134*
Configuring Global SYN Flood Protection *136*
Configuring Global Packet Anomaly Protection *136*
CONFIGURING THE ADVANCED-PARAMETERS SETUP 141
Configuring Radware DefensePro DDoS Mitigation Session Table Settings *141*
Configuring Radware DefensePro DDoS Mitigation Suspend Table Settings *143*
Configuring CPU-Load Alerts Parameters *144*
CONFIGURING THE REPORTING-SETTINGS SETUP 148
Configuring Radware DefensePro DDoS Mitigation Syslog Settings *148*
Enabling Configuration Auditing on the Radware DefensePro DDoS Mitigation Device *150*
Configuring Security Reporting Settings *150*
CONFIGURING THE CLUSTERING SETUP 153

CHAPTER 4 – MANAGING CLASSES 155

MANAGING NETWORK CLASSES 155
MANAGING CONTEXT GROUP CLASSES 156
MANAGING APPLICATION CLASSES 157
MANAGING SGT CLASSES 158

CHAPTER 5 – MANAGING PROTECTION POLICIES 161

CONFIGURING PROTECTION POLICIES 162
CONFIGURING ANTI-SCANNING PROTECTION PROFILES 170
CONFIGURING BDOS PROFILES 174
Radware DefensePro DDoS Mitigation CLI Command for BDoS Learning Suppression Threshold

..... 183
CONFIGURING CONNECTION LIMIT PROFILES 183
Configuring Connection Limit Protections 185
CONFIGURING CONNECTION PPS PROFILES 187
CONFIGURING DNS FLOOD PROTECTION PROFILES 190
Radware DefensePro DDoS Mitigation CLI Command for DNS Learning Suppression Threshold 197
CONFIGURING ERT ACTIVE ATTACKERS FEED PROFILES 198
CONFIGURING GEOLOCATION PROFILES 201
CONFIGURING HTTPS FLOOD PROTECTION PROFILES 204
CONFIGURING OUT-OF-STATE PROTECTION PROFILES 208
CONFIGURING SIGNATURE PROTECTION 210
Signature Protection in Radware DefensePro DDoS Mitigation 210
Configuration Considerations with Signature Protection 211
Configuring Signature Protection Profiles 212
Managing Signature Protection Signatures 215
Managing Signature Protection Attributes 234
Viewing and Modifying Attribute Type Properties 235
CONFIGURING SYN FLOOD PROTECTION PROFILES 237
Defining SYN Flood Protections 238
Managing SYN Flood Protection Profile Parameters 240
CONFIGURING TRAFFIC FILTERS PROFILES 247

CHAPTER 6 – MANAGING ACCESS CONTROL 263

CONFIGURING THE ACL GLOBAL PARAMETER—LIST PRECEDENCE 263
CONFIGURING BLACK LISTS 263
Configuring Black List Rules 264
CONFIGURING WHITE LISTS 267
Configuring White Lists in Radware DefensePro DDoS Mitigation 268

CHAPTER 7 – MANAGING OPERATIONS AND MAINTENANCE 273

UPDATING POLICY CONFIGURATIONS 273
REBOOTING OR SHUTTING DOWN A RADWARE DEFENSEPRO DDOS MITIGATION DEVICE 274
USING CONFIGURATION TEMPLATES FOR SECURITY POLICIES 274
CONFIGURING MULTIPLE DEVICES 283
DOWNLOADING A DEVICE'S LOG FILE TO APSOLUTE VISION 284
UPDATING A RADWARE SIGNATURE FILE 285
DOWNLOADING TECHNICAL-SUPPORT AND CONFIGURATION FILES 286
Downloading a Technical Support File Using APSolute Vision 286
Downloading a Technical Support File Using CLI 287
User Credentials in Radware DefensePro DDoS Mitigation Technical Support Files 287
MANAGING RADWARE DEFENSEPRO DDOS MITIGATION DEVICE CONFIGURATIONS 288
Radware DefensePro DDoS Mitigation Configuration File Content 288
Downloading a Device-Configuration File 289
Restoring a Device Configuration 290
RESETTING THE BASELINE FOR RADWARE DEFENSEPRO DDOS MITIGATION 291
SCHEDULING APSOLUTE VISION AND DEVICE TASKS 292
Overview of Scheduling 292
Configuring Tasks in the Scheduler 293

Task Parameters *295*
UPDATING THE ATTACK DESCRIPTION FILE 310

CHAPTER 8 – MONITORING AND CONTROLLING THE OPERATIONAL STATUS 311

MONITORING THE GENERAL RADWARE DEFENSEPRO DDOS MITIGATION DEVICE INFORMATION 311
MONITORING AND CONTROLLING RADWARE DEFENSEPRO DDOS MITIGATION PORTS 312
MONITORING RADWARE DEFENSEPRO DDOS MITIGATION RESOURCE UTILIZATION 315
Monitoring Radware DefensePro DDoS Mitigation CPU Utilization *315*
Monitoring Radware DefensePro DDoS Mitigation RAM and Disk Utilization *316*
Monitoring and Clearing Radware DefensePro DDoS Mitigation Authentication Tables *318*
Monitoring Radware DefensePro DDoS Mitigation Syslog Information *319*
MONITORING SECURITY GROUP TAGS (SGTS) 319

CHAPTER 9 – MONITORING CLUSTERING 322

CHAPTER 10 – MONITORING RADWARE DEFENSEPRO DDOS MITIGATION STATISTICS 324

MONITORING RADWARE DEFENSEPRO DDOS MITIGATION SNMP STATISTICS 324
MONITORING RADWARE DEFENSEPRO DDOS MITIGATION IP STATISTICS 325

CHAPTER 11 – MONITORING AND CONTROLLING NETWORKING 328

MONITORING THE SESSION TABLE 328
MONITORING ROUTING TABLE INFORMATION 329
MONITORING RADWARE DEFENSEPRO DDOS MITIGATION ARP TABLE INFORMATION 329
MONITORING THE RADWARE DEFENSEPRO DDOS MITIGATION SUSPEND TABLE 330
LOCATION-BASED SUSPENDED TRAFFIC 331

CHAPTER 12 – USING REAL-TIME SECURITY MONITORING 332

RISK LEVELS 333
USING THE DASHBOARD VIEWS FOR REAL-TIME SECURITY MONITORING 333
Configuring the Display Parameters of a Dashboard View *334*
Using the Current Attacks Table *335*
Using the Ongoing Attacks Monitor *339*
Attack Details *341*
Sampled Data Tab *352*
VIEWING REAL-TIME TRAFFIC REPORTS 354
Viewing the Traffic Utilization Report *354*
Viewing the Connection Rate Report *358*
Viewing the Concurrent Connections Report *360*
Viewing the Top Queried Domain Names Report *361*
PROTECTION MONITORING 363
Displaying Attack Status Information *363*
Monitoring the Traffic Under BDoS Protection *364*
Monitoring the Traffic Under DNS Flood Protection *366*
HTTP REPORTS 370
Monitoring Continuous Learning Statistics *370*
Monitoring Hour-Specific Learning Statistics *370*
HTTP Request Size Distribution *370*
ALERTS FOR NEW SECURITY ATTACKS 370

CHAPTER 13 – ADMINISTERING RADWARE DEFENSEPRO DDOS MITIGATION ERROR! BOOKMARK NOT

DEFINED.

COMMAND LINE INTERFACE 373
CLI Command Restrictions *374*
CLI Session Time-Out *374*
CLI Capabilities *375*
CLI Traps *375*
Send Traps To All CLI Users *376*
WEB SERVICES 376
API STRUCTURE 376
APSOLUTE API SOFTWARE DEVELOPMENT KIT (SDK) 377

APPENDIX A – FOOTPRINT BYPASS FIELDS AND VALUES 379

BDOS FOOTPRINT BYPASS FIELDS AND VALUES 380
DNS FOOTPRINT BYPASS FIELDS AND VALUES 387

APPENDIX B – PREDEFINED BASIC FILTERS 389

APPENDIX C – ATTACK-PROTECTION ID NUMBERS 400

APPENDIX D – SUPPORTED PROTOCOLS 411

APPENDIX E – TROUBLESHOOTING 413

TECHNICAL SUPPORT FILE 413

APPENDIX F – GLOSSARY 415

RADWARE LTD. END USER LICENSE AGREEMENT 423

CHAPTER 1 – INTRODUCTION

This guide describes Radware DefensePro DDoS Mitigation version 8.22.2 and how to use it.

Note: This guide may use the short term *DefensePro* to refer to the *Radware DefensePro DDoS Mitigation* product.

Unless specifically stated otherwise, the procedures described in this guide are performedusing APSolute Vision™ version 4.60.

This chapter introduces Radware DefensePro DDoS Mitigation and provides a general explanation of its main features and modules.

This chapter contains the following sections:

- Radware DefensePro DDoS Mitigation System Components, page 34
- Subscription Services, page 35
- Network Connectivity, page 37
- Management Interfaces–APSolute Vision and Others, page 37
- Radware DefensePro DDoS Mitigation Features, page 38
- Related Documentation, page 41

Radware DefensePro DDoS Mitigation–Overview

Radware DefensePro DDoS Mitigation is a service that provides distributed denial-of-service (DDoS) detection and mitigation capabilities on Cisco Firepower platforms. The Firepower platform is Cisco's new approach for delivering security services. The Firepower platform can host several applications, for example, a DDoS protector, an intrusion prevention system (IPS), and a firewall. Applications or services can be chained to enable applications to serve other security-platform applications and end customers. The Firepower platform can be deployed in various deployment scenarios to support different customer use cases.

The Radware DefensePro DDoS Mitigation for Cisco Firepower service can run on up to three compute blades.

Each compute blade hosts the following components:

- **An instance of the Firepower software infrastructure** –Contains a Linux-based operating environment with a set of generic services, for example, logging, software image management, and so on, which is accessible through various APIs.
- **One or more security applications on top of the infrastructure**–These applications can be provided either by Cisco or a third party. Radware's Radware DefensePro DDoS Mitigation for Cisco Firepower is one such third-party application. Radware DefensePro DDoS Mitigation for Cisco Firepower runs on a KVM-based virtual machine. Multiple services (for example, DefensePro for Cisco Firepower, an IPS, and a firewall) can co-exist on a blade. The services can be chained. For example, the Radware DefensePro DDoS Mitigation for Cisco Firepower can be first in line-and protect customers and other applications from denial-of-serviceattacks.

Chassis management for the Firepower is performed by the Cisco Unified Manager, whereas Radware APSolute Vision manages the Radware DefensePro DDoS Mitigation application.

Initial startup configuration is performed using an XML file that provisions Radware DefensePro DDoS Mitigation.

Notes

- For information about Cisco Firepower platforms that support Radware DefensePro DDoS Mitigation, please consult your Cisco sales representative.
- For information on installation, maintenance, and upgrade of Radware DefensePro DDoS Mitigation, please consult Cisco Technical Support.

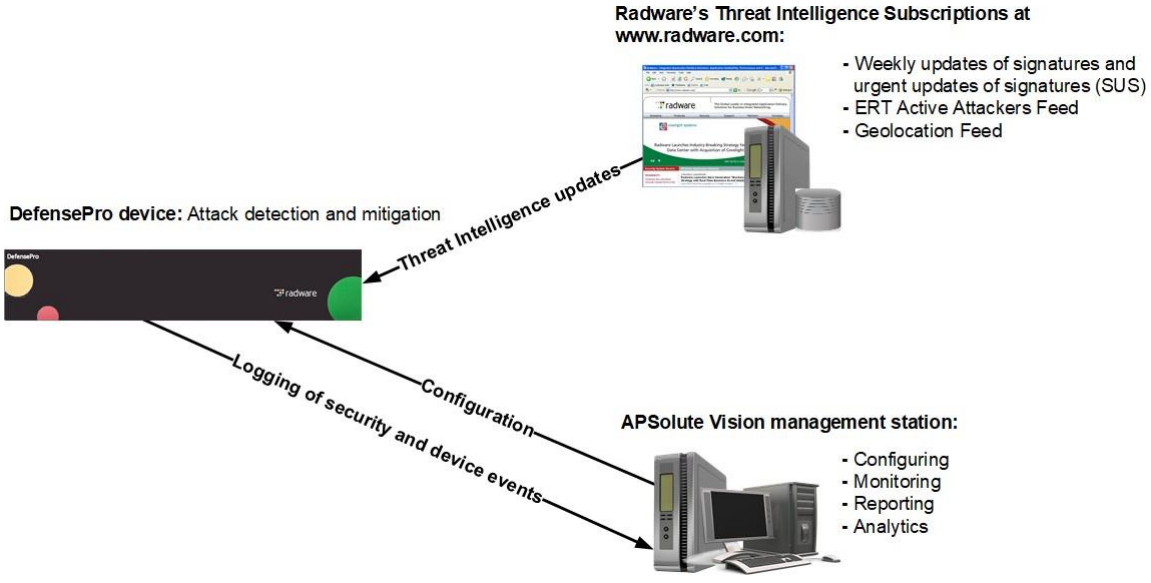
Radware DefensePro DDoS Mitigation System Components

Radware DefensePro DDoS Mitigation is an in-line intrusion-prevention and denial-of-service protection system that detects and prevents network threats in real-time. Radware DefensePro DDoS Mitigation inspects incoming and outgoing traffic for potential attacks, clearing the network from unwanted malicious traffic.

The Radware DefensePro DDoS Mitigation system contains the following components:

- **Radware DefensePro DDoS Mitigation device**—The term *device* refers to the virtual platform and the Radware DefensePro DDoS Mitigation product.
- **Management interface**—APSolute Vision and others.
- **Subscription Services**—Radware DefensePro DDoS Mitigation can use the following subscription services:
  - ERT Security Update Subscription (SUS)
  - ERT Active Attackers Feed (EAAF)
  - Geolocation Feed

Figure 19: Radware DefensePro DDoS Mitigation System Components



Subscription Services

Radware DefensePro DDoS Mitigation may use the following subscription services:

- ERT Security Update Service (SUS), page 35
- ERT Active Attackers Feed (EAAF), page 36
- Geolocation Feed, page 36

ERT Security Update Service (SUS)

Radware's *Emergency Response Team* (ERT) *Security Update Service* (SUS) is a subscription-based security-advisory and managed-monitoring/detection system dedicated to protecting network elements, hosts, and applications against the latest security vulnerabilities and threats. The ERT is a group of security experts that provides 24/7 security support services for customers facing a denial- of-service (DoS) attack or malware outbreak. SUS delivers rapid and continuous updates to current subscribers. SUS provides periodic updates to signature files, rapid response to high impact security events, and development and distribution of custom filters. These updates can be done in a fully automated way or manually, depending on the your choice.

The SUS consists of the following key service elements:

- **Weekly updates**—Scheduled periodic updates (typically weekly) to the signature files, with automatic distribution through APSolute Vision, or on-demand download from https://www.radware.com/products/threat-intelligence/. Radware's SUS provides protection for most known attack tools and recent vulnerabilities, sourced directly from Radware's ERT. SUS leverages the ERT's unique visibility into new attacks in the wild—as well as independent and external research utilizing Radware's threat expertise. SUS updates include DoS flooding tools, slow DoS attacks and tools, DoS single packet vulnerabilities, and critical data-center- applications vulnerabilities. Periodic updates are typically available on a weekly basis and include all new filters, including those previously released as an *Emergency* update.
- **Emergency updates** —For cases where an immediate response is necessary, Radware issues an emergency signature-file update. Emergency updates are released outside of the weekly release when there are critical vulnerabilities that put customers at risk, based on ERT analysis. These updates are accompanied by an ERT threat alert, which also provides guidance for preventive actions in addition to the signature update. Registered customers are notified via email once the emergency update is available for download from radware.com.
- **Custom signatures**—SUS also allows you to contact Radware to report environment-specific or newly discovered threats and request signatures to mitigate those threats. Custom signatures are generated according to relevance and risk according to Radware's *Vulnerability Research Team* (VRT). Threats are assessed, and for those threats for which a filter is appropriate, Radware either issues an emergency update to all customers or provides a custom filter specifically to the customer reporting the threat. Custom signatures are subsequently analyzed and incorporated through periodic updates when appropriate.

For up-to-date security information, go to https://www.radware.com/products/threat-intelligence/.

To view and monitor various SUS statistics, go to the *Radware Security Signatures (SUS)* node of the Security Control Center.

To view whether Radware DefensePro DDoS Mitigation devices have an *ERT Active Attackers Feed* subscription or the expiration date of the subscription, go to the APSolute Vision *Device Subscriptions* pane.

ERT Active Attackers Feed (EAAF)

The *ERT Active Attackers Feed* (EAAF) is a subscription service, which draws intelligence data from three main sources:

- Radware's Cloud Security Services
- Radware's Global Deception Network, which is a global network of honeypots designedto monitor and track malicious traffic
- Radware's *Emergency Response Team* (*ERT*), which deploys proprietary algorithms and manual research techniques to identify threats

The data from these sources are automatically analyzed, cleaned, and correlated by Radware's *Threat Research Center* (TRC) to generate a validated list of IP addresses involved in active attacks.

In real-time, the list is used to update the entries in the Radware DefensePro DDoS Mitigation *ERT Active Attackers Feed* module, enabling Radware DefensePro DDoS Mitigation to block known attackers before they target the network. For more information, see Configuring ERT Active Attackers Feed Profiles, page 195.

The service continuously monitors the suspect IP addresses, removing them from the feed when attacks have subsided, to decrease the risk of false positives.

For more information on the ERT Active Attackers Feed, go to https://www.radware.com/products/threat-intelligence/.

To view and monitor statistics on attacks and attackers that Radware DefensePro DDoS Mitigation devices blocked using the ERT Active Attackers Feed, you can use the APSolute Vision *EAAF Dashboard*.

To view and monitor statistics relevant to feed itself (for example, the time that APSolute Vision received the last feed), go to the *ERT Active Attackers Feed* node of the Security Control Center. The *ERT Active Attackers Feed* node also displays statistics on the updates of the feed on Radware DefensePro DDoS Mitigation devices.

To view whether Radware DefensePro DDoS Mitigation devices have an *ERT Active Attackers Feed* subscription or the expiration date of the subscription, go to the APSolute Vision *Device Subscriptions* pane.

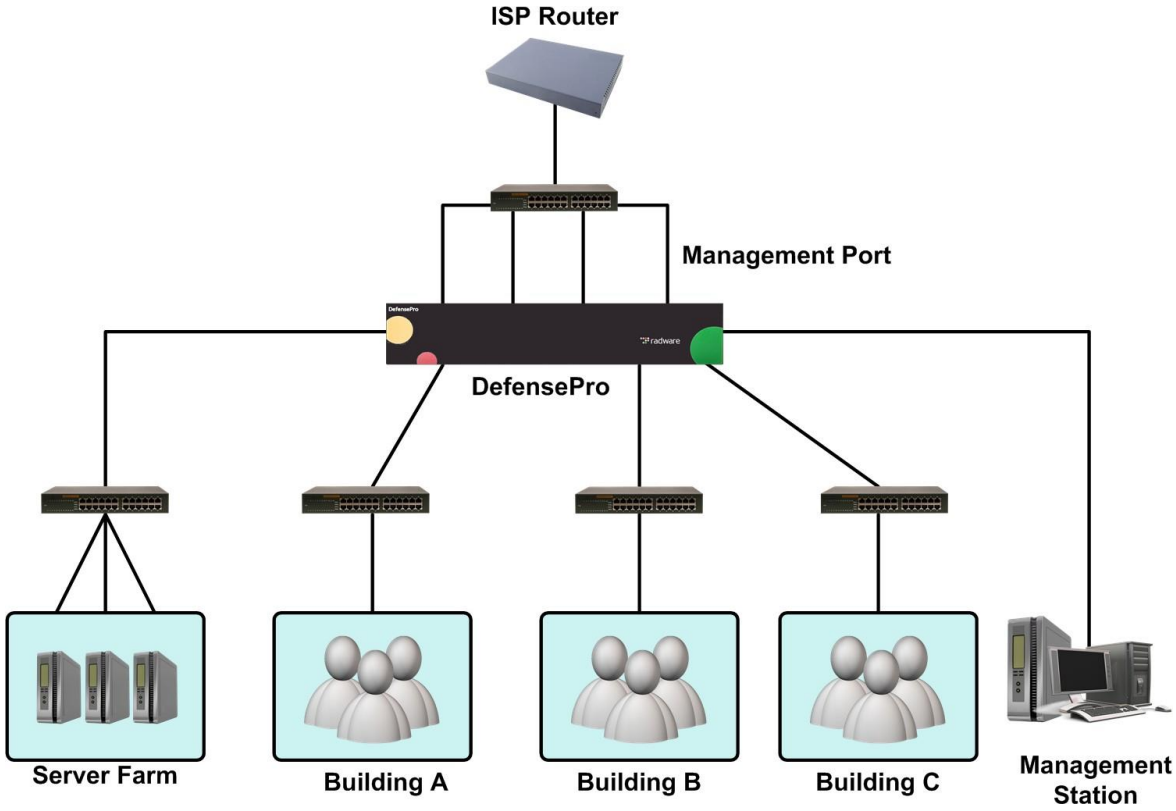
Geolocation Feed

The Geolocation Feed enables the *Geolocation* features in Radware DefensePro DDoS Mitigation and in *APSolute Vision Analytics* (AVA). The *Geolocation* module in Radware DefensePro DDoS Mitigation can permanently block all traffic from selected countries. You can use the AVA *Geolocation Map* to *temporarily* block traffic from selected countries.

Network Connectivity

The following figure shows the typical network topology of Radware DefensePro DDoS Mitigation.

Figure 20: Typical Network Connectivity



Management Interfaces–APSolute Vision and Others

APSolute Vision is the main management interface for Radware DefensePro DDoS Mitigation. Radware DefensePro DDoS Mitigation also supports a command-line interface (CLI).

You can perform most tasks using any of the management systems. However, for the most part, this guide describes management tasks using APSolute Vision.

APSolute Vision is a graphical application that enables you to configure, modify, monitor, and generate reports centrally for single or multiple Radware DefensePro DDoS Mitigation deployments.

Radware DefensePro DDoS Mitigation Features

This section provides a brief description of the main Radware DefensePro DDoS Mitigation features and includes the following topics:

- Security Protections, page 38
- Inspection of Tunneled Traffic, page 39
- Real-Time Security Reporting, page 40
- Historical Security Reporting—APSolute Vision Reporter, page 40
- Real-time and Historical Reporting—APSolute Vision Analytics, page 40

Security Protections

You can use APSolute Vision or the CLI to configure Radware DefensePro DDoS Mitigation security policies.

Note: The Radware DefensePro DDoS Mitigation version and platform may affect the types of the security policies that the device supports.

A security policy in an organization is a set of rules and regulations that defines what constitutes a secure network and how it reacts to security violations.You implement a security policy for your organization by configuring the global security settings and protection policies. You can adjust a security policy to suit the security needs of different network segments down to a single server, providing comprehensive protection for your organization.

Each policy consists of multiple rules. Each rule in a policy defines a network segment or server, one or more protection profiles to be applied, and the action to be taken when the device detects an attack.

Each protection profile defines the security defenses that provide protection against a specific network threat. For example, the Signature Protection profile prevents intrusion attempts, and the Behavioral DoS profile prevents flood attacks aimed at creating denial of service.

Notes

- In this book, unless specifically noted, the procedures to configure security policies relateto using APSolute Vision.
- All the configuration procedures assume that the relevant device is selected in theAPSolute Vision *device pane* and that the device is locked.
- Some protections are not supported on management interfaces.

Radware DefensePro DDoS Mitigation's multi-layer security approach combines features for detecting and mitigating a wide range of network and server attacks.

Radware DefensePro DDoS Mitigation supports *network-wide protections*.

Network-wide protections include the following:

- **Anti-Scanning Protection (Scanning and worm-propagation protection)**—Provides zero- day protection against self-propagating worms, horizontal and vertical TCP and UDP scanning, and ping sweeps.
- **Behavioral DoS (BDoS) Protection**—Protects against zero-day flood attacks, including SYN floods, TCP floods, UDP floods, ICMP and IGMP floods. BDoS Protection also mitigates *burst attacks*.
- **Connection Limit Protection**—Protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks.

- **Connection PPS Protection**—Protects against attacks that use a high PPS rates on one or several connections to flood a server.
- **DNS Flood Protection**—Protects against zero-day DNS query floods. DNS query floods can impact not only the DNS servers, but also the entire network infrastructure. It is therefore crucial to protect the DNS infrastructure from these threats. DNS query floods overwhelm the DNS servers with queries, denying service to legitimate users. DNS query floods can target an authoritative DNS server or a recursive DNS server. In the case of an authoritative DNS server, queries originate from either commercial or public recursive DNS servers. In the case of a recursive DNS server, queries originate from hosts (for example, subscribed hosts of a commercial recursive resolver or any host using an open resolver). A basic query flood may be composed of a single Fully Qualified Domain Name (FQDN) or multiple FQDNs. A sophisticated query flood, also known as a *recursive flood* or *random-subdomains flood*, is composed of fake, random subdomains of a targeted domain. The goal of the random-subdomains attack is to overload the DNS resolver's resources and also target an authoritative DNS server in charge of the targeted domain. In this attack, both legitimate ("good") subdomains and attack ("bad") subdomains appear as legitimate queries to the DNS server. In Radware DefensePro DDoS Mitigation 8.*x* versions 8.13 and later, the DNS Flood Protection engine is able to detect all types of DNS query floods, automatically identify the attack FQDNs and/or targeted domain, and allow only the "good" queries to the protected DNS servers.
- **ERT Active Attackers Feed**—Uses the ERT Active Attackers Feed subscription service to identify and block IP addresses actively involved in major attacks in real-time to provide preemptive protection from known attackers.
- **Geolocation**—Permanently blocks all traffic from selected countries. The Geolocation feature uses the subscription Geolocation Feed to identify the source country of the traffic.
- **HTTPS-Flood Protection**—Mitigates HTTPS-flood attacks.
- **Out-of-State Protection**—Ensures that TCP connections are established based on the protocol RFCs.
- **Packet-Anomaly Protection**—Detects and provides protection against packet anomalies.
- **Signature-based Protection**—Protects against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. Signature-based Protection uses the *Emergency Response Team* (ERT) *Security Update Service* (SUS), which is a subscription-based system. Signature-based Protection includes *DoS Shield* protection, which protects against known flood attacks and flood attack tools that cause a denial-of-service effect.
- **SYN Flood Protection** —Protects against any type of SYN-flood attack using SYN cookies. A SYN-flood attack is usually aimed at specific servers with the intention of consuming the server's resources. However, you configure SYN Flood Protection as a network protection to allow easier protection of multiple network elements.
- **Traffic Filters**—Block or rate-limit traffic that matches specified values or traffic not matching specified values. Traffic Filters enable you to specify network addresses, ports, packet size, TTL, and additional parameters for filtering packets within the Protection policy.

Black List rules and White List rules block or allow traffic to or from specified networks, based on protocols, applications, and other criteria.

Inspection of Tunneled Traffic

Carriers, service providers, and large organizations use various tunneling protocols to transmit data from one location to another. This is done using the IP network so that network elements are unaware of the data encapsulated in the tunnel.

When tunneling is used, IPS devices and load balancers cannot locate the relevant routing information because their decisions are based on information located inside the packet at a known offset, and the original IP packet is encapsulated in the tunnel.

You can install Radware DefensePro DDoS Mitigation in different environments, which might include

encapsulated traffic using different tunneling protocols. In general, wireline operators deploy MPLS and L2TP for their tunneling, and mobile operators deploy GRE and GTP.

Radware DefensePro DDoS Mitigation 8.*x* versions can inspect traffic that may use various encapsulation protocols. In some cases, the outer header (tunnel data) is the data that Radware DefensePro DDoS Mitigation needs to inspect. In other cases, Radware DefensePro DDoS Mitigation needs to inspect the inner data (IP header and even the payload).

Radware DefensePro DDoS Mitigation always *processes* IPsec traffic, which uses protocol type 50 and 51.

Caution: Radware DefensePro DDoS Mitigation devices identify blacklisted traffic and whitelisted traffic based only on the *outer* address of tunneled traffic.

Real-Time Security Reporting

APSolute Vision provides real-time attack views and security service alarms for Radware DefensePro DDoS Mitigation devices.

When Radware DefensePro DDoS Mitigation detects an attack, the attack is reported as a security event.

When Radware DefensePro DDoS Mitigation detects an attack, it automatically generates counter-measures that you can observe and analyze using various monitoring tools. Radware DefensePro DDoS Mitigation provides you with monitoring tools that show real-time network traffic and application-behavior parameters. Security monitoring also provides statistical parameters that represent normal behavior baselines, which are generated using advanced statistical algorithms.

Historical Security Reporting—APSolute Vision Reporter

APSolute Vision supports APSolute Vision Reporter (AVR) for Radware DefensePro DDoS Mitigation. APSolute Vision Reporter is a historical security reporting engine, which provides the following:

- Customizable dashboards, reports, and notifications
- Advanced incident handling for security operating centers (SOCs) and network operating centers (NOCs)
- Standard security reports
- In-depth forensics capabilities
- Ticket workflow management

Real-time and Historical Reporting—APSolute Vision Analytics

APSolute Vision supports APSolute Vision Analytics (AVA), which provides real-time attack views and security service alarms for Radware DefensePro DDoS Mitigation devices as well as features for historical reporting.

AVA for Radware DefensePro DDoS Mitigation supports the following main modules:

- **Dashboards** –Dashboards display near real-time and historical monitoring and reporting metrics. You can use the dashboards to track the security throughout the network that your Radware DefensePro DDoS Mitigation devices are protecting. Dashboards summarize the existing network infrastructure in panels of graphs, charts, and tables. You can perform adeep analysis wherever necessary by drilling down into the event details.
- **Reports**–You can use the *Reports* module to create and generate reports of a single query.
- **Forensics**–Forensics analysis involves recording and analyzing historical security events. You can use the APSolute Vision Analytics *Forensics* module to discover the source of the attack, attack trends, and analyze the risk associated with each incident.

AVA opens through the APSolute Vision Web interface–by clicking the **Analytics** button on the APSolute Vision toolbar.

Full functionality of APSolute Vision Analytics requires a *Vision Reporting Module - AMS* license, which must be installed on the APSolute Vision server.

For more information, see the *APSolute Vision Analytics User Guide* or the APSolute Vision online help.

Related Documentation

See the following documents for information related to Radware DefensePro DDoS Mitigation:

- Radware DefensePro DDoS Mitigation Release Notes, page 41
- APSolute Vision Documentation, page 41
- APSolute Vision Reporter Documentation, page 42
- APSolute Vision Analytics Documentation, page 42

Note: For information on installing and maintaining *Radware DefensePro DDoS Mitigation*, see your Cisco documentation.

Radware DefensePro DDoS Mitigation Release Notes

See the *Radware DefensePro DDoS Mitigation Release Notes* for information about this Radware DefensePro DDoS Mitigation version.

APSolute Vision Documentation

APSolute Vision documentation includes the following:

- **APSolute Vision Installation and Maintenance Guide**–See this for information about:
  - Installing APSolute Vision.
  - Initializing APSolute Vision.
- **APSolute Vision User Guide**–See this for information about:
  - APSolute Vision features.
  - APSolute Vision interface navigation.
  - User management–for example, adding users and defining their permissions.
  - Adding and removing Radware DefensePro DDoS Mitigation devices.
  - Configuring Sites–a *Site* is a physical or logical representation of a group of managed devices.
  - Administration and maintenance tasks on managed devices–such as, scheduling APSolute Vision and device tasks, making backups, and so on.
  - APSolute Vision CLI.
  - Monitoring APSolute Vision–for example, version, server, database, device-configuration files, controlling APSolute Vision operations, backing up the APSolute Vision database.
  - Managing auditing and alerts.
  - Monitoring managed Radware DefensePro DDoS Mitigation devices.
- **APSolute Vision online help**–See this for information about configuring and monitoring managed Radware DefensePro DDoS Mitigation devices.

APSolute Vision Reporter Documentation

See the APSolute Vision Reporter online help and *APSolute Vision Reporter User Guide* for information about APSolute Vision Reporter and how to use it.

APSolute Vision Analytics Documentation

See the APSolute Vision online help or the *APSolute Vision Analytics User Guide* for information about APSolute Vision Analytics and how to use it.

CHAPTER 2 – GETTING STARTED

This chapter describes what to do before you set up and configure Radware DefensePro DDoS Mitigation with security policies.

For information on installation, maintenance, and upgrade of Radware DefensePro DDoS Mitigation, please consult Cisco Technical Support.

For information and procedures related to the physical specifications and basic setup of the APSolute Vision server, read the relevant information and follow the instructions in the *APSolute Vision Installation and Maintenance Guide* before you perform the other tasks described in this chapter.

This chapter contains the following sections:

- Logging In to APSolute Vision, page 43
- Changing the Password for Local APSolute Vision Users, page 45
- APSolute Vision User Interface Overview, page 45
- Selecting Your Landing Page, page 56
- Using Common GUI Elements in APSolute Vision, page 57
- Managing Radware DefensePro DDoS Mitigation Devices, APSolute Vision Sites, and Logical Groups, page 59

Logging In to APSolute Vision

To start working with APSolute Vision, you log in to the APSolute Vision Web application, which is referred to as *Web Based Management* (WBM).

The first login to APSolute Vision WBM requires an *APSolute Vision Activation License* (which has the prefix **vision-activation**). When APSolute Vision is running as a virtual appliance (VA), the activation-license is based on the MAC address of the APSolute Vision G1 or G2 port. When APSolute Vision is running on an OnDemand Switch VL2 (ODS-VL2) platform, the activation-license is based on the MAC address of the APSolute Vision G3 or G5 port.

You can request the activation-license from Technical Support.

Note: The CLI command net ip get displays the ports and the MAC addresses. Up to 50

users can access the APSolute Vision server concurrently.

APSolute Vision supports role-based access control (RBAC) to manage user privileges. Your credentials and privileges may be managed through an authentication server or through the local APSolute Vision user database.

For RBAC users, after successful authentication of your username and password, your role is determined together with the devices that you are authorized to manage. The assigned role remains fixed throughout your user session, and you can access only the content panes, menus, and operations that the role allows.

Depending on the configuration of the APSolute Vision server, you may be prompted to change your user password when you log in for the first time.

If you enter the credentials incorrectly, you are is prompted to re-enter the information. After a globally defined number of consecutive failures, the APSolute Vision server locks you out of the system. If you use *local* user credentials, a user administrator can release the lockout by resetting the password to the global default password. If you use credentials from an authentication server (for example, a RADIUS server), you must contact the administrator of that authentication server.

To log in to APSolute Vision as an existing user

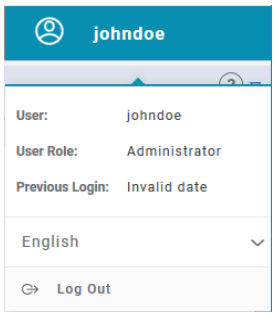
1. In a Web browser, enter the hostname or IP address of the APSolute Vision server.
2. In the login dialog box, specify the following:
   - **User Name** –Your username.
   - **Password**–Your user password. Depending on the configuration of the server, youmay be required to change your password immediately.
   - The language of the APSolute Vision graphical user interface. Click the arrow next to the name of the current language to open the language drop-down list and select thelanguage that you require.

3. Click **Log In**.

Caution: Cisco recommends increasing the SNMP **Timeout** to 180 seconds (*APSolute Vision Settings* view *System* perspective, **General Settings** > **Connectivity > Timeout**).

To log out of APSolute Vision

1. In the APSolute Vision toolbar, click the **User** ribbon at the at the far right. A drop-down dialog box opens.



2. Click **Log Out**.

Changing the Password for Local APSolute Vision Users

If your user credentials are managed through the APSolute Vision *Local Users* table (not through an authentication server, such as RADIUS), you can change your user password at the login or in the *APSolute Vision Settings* view *Preferences* perspective.

If your password has expired, you must change it in the *APSolute Vision Login* dialog box.

Note: For more information about password requirements and APSolute Vision users, see the *APSolute Vision User Guide*.

To change a password for a local user

1. In the *APSolute Vision Settings* view *Preferences* perspective, select **User Preferences > User Password Settings**.
2. Configure the parameters, and click **Update Password**.

Table 1: User Password Settings Parameters

Parameter	Description
Current Username	(Read-only) The current username.
Current Password	Your current password.
New Password	Your new password.
Confirm New Password	Your new password.

APSolute Vision User Interface Overview

This section contains the following topics:

- APSolute Vision Toolbar and Sidebar Menu, page 46
- APSolute Vision Settings View, page 48
- Device Pane, page 51
- Configuration Perspective, page 53
- Monitoring Perspective, page 55
- Security Monitoring Perspective, page 55

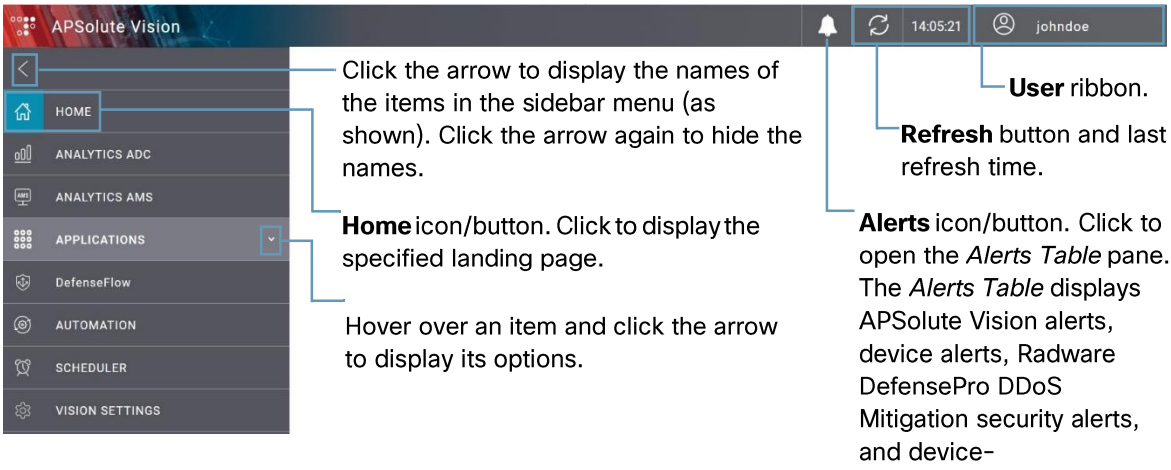
The APSolute Vision interface follows a consistent hierarchical structure, organized functionally to enable easy access to options. You start at a high functional level and drill down to a specific module, function, or object.

Note: Access to and privileges in APSolute Vision interface elements is determined by Role-Based Access Control (RBAC). For more information, see the APSolute Vision documentation.

APSolute Vision Toolbar and Sidebar Menu

The following figure shows the APSolute Vision (horizontal) toolbar and (vertical) sidebar menu.

Figure 21: APSolute Vision Toolbar and Sidebar Menu

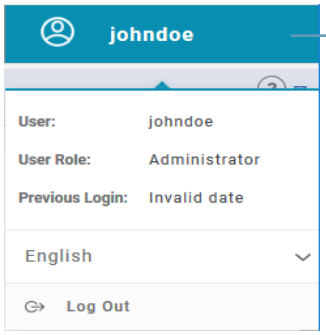


The APSolute Vision toolbar contains the following items:

- **Alerts icon/button**–Click the button to open the *Alerts Table* pane. The *Alerts Table* displays APSolute Vision alerts, device alerts, Radware DefensePro DDoS Mitigation security alerts, and device-configuration messages.
- **Refresh button and last refresh time**.
- **User ribbon**–Clicking in the ribbon opens a drop-down dialog box. Use

  the dialog box to do the following:
  - View the user name, RBAC role, and previous login time.
  - Change the UI language by selecting another value from the **Language** drop-down list.
  - Log out of the session and log in as another user.

Figure 22: User Dialog Box



Clicking the user name opens the drop-down dialog box.

The APSolute Vision sidebar menu contains the following items:

- **Home**–Returns the display to the landing page, which is specified for the server.
- **Analytics ADC**–Opens a drop-down list with options for *APSolute Vision Analytics* (AVA) for Radware application-delivery-control (ADC) products.

  Note: For more information about AVA and how to use it, see the *APSolute Vision Analytics User Guide*.

- **Analytics AMS**–Opens a drop-down list with the following options for *APSolute Vision Analytics* (AVA) for Radware Attack Mitigation Solution (AMS) products:
  - **Radware DefensePro DDoS Mitigation Monitoring**–Opens the *Radware DefensePro DDoS Mitigation Monitoring* dashboard.
  - **Radware DefensePro DDoS Mitigation Attacks**–Opens the *Radware DefensePro DDoS Mitigation Attacks* dashboard.
  - **HTTPS Flood**–Opens the Radware DefensePro DDoS Mitigation *HTTPS Flood dashboard.*
  - **Radware DefensePro DDoS Mitigation Analytics**–Opens the *Radware DefensePro DDoS Mitigation Analytics dashboard.*
  - **Radware DefensePro DDoS Mitigation Behavioral Protections**–Opens the *Radware DefensePro DDoS Mitigation Behavioral Protections* dashboard.
  - **DefenseFlow Analytics**–Opens the *DefenseFlow Analytics dashboard.*
  - **AppWall** –Opens the *AppWalldashboard.*
  - **Reports** –Opens the AVA AMS *Reports*module.

- **Forensics**–Opens the AVA AMS *Forensics* module.
- **Alerts**–Opens the AVA AMS *Alerts* module.

Note: AVA AMS can provide real-time and historical information from your Radware DefensePro DDoS Mitigation devices. For more information about AVA and how to use it, see the *APSolute Vision Analytics User Guide*.

- **Applications**–Opens a drop-down list with buttons to open or connect to various apps and services, including the following:
  - **AVR**–APSolute Vision Reporter, which is historical security reporting for Radware DefensePro DDoS Mitigation and AppWall.
  - **Cloud DDoS Portal** –Connects you to the to the associated Radware Cloud DDoS Protection service interface. For more information on Radware Cloud DDoS Protection services, see the *Cloud DDoS Protection Services User Guide*.
  - **vDirect**–Opens the vDirect interface in the APSolute Vision server.
  - **Security Control Center**–Opens the Security Control Center.
  - **GEL**–Opens the *Global Elastic License (GEL) Dashboard* to activate a new *Global Elastic License* (GEL) *Entitlement*, allocate throughput to Alteon servers using GELEntitlements, and to view the Entitlement-utilization state.
  - **EAAF**–Opens the *ERT Active Attackers Dashboard*.
  - **Operation**–Opens the *DefenseFlow Attack Mitigation Operation dashboard*.
  - **Configuration** –Opens the DefenseFlow interface (when the DefenseFlow IP address is configured in the APSolute Vision CLI).
- **Automation**–Opens the *Toolbox* pane, which includes the *Toolbox* tab and the *Advanced* tab. By default, the *Toolbox* tab displays predefined Toolbox scripts. From the adjacent *Workflows* tab, you can manage and use vDirect workflows. From the *Advanced* tab, you can manage Toolbox scripts, use AppShape templates, and manage Radware DefensePro DDoS Mitigation configuration templates. For more information, see Managing Radware DefensePro DDoS Mitigation Configuration Templates, page 270.
- **Scheduler**–Opens the Scheduler to schedule various operations for the APSolute Vision server and managed devices. For more information, see Scheduling APSolute Vision and Device Tasks, page 284.
- **Vision Settings**–Opens the *APSolute Vision Settings* view. For more information, see APSolute Vision Settings View, page 48.

APSolute Vision Settings View

Select the **Vision Settings** item () from the APSolute Vision sidebar menu to display the *APSolute Vision Settings* view.

The *APSolute Vision Settings* view includes the following perspectives:

- **System**–For more information, see Settings View–System Perspective, page 50. Access to the *APSolute Vision Settings* view *System* perspective is restricted to administrators.
- **Dashboards**–For more information, see Settings View–Dashboards Perspective, page 50.
- **Preferences**–For more information, see Settings View–Preferences Perspective, page 50.

Click the relevant button (**System**, **Dashboards**, or **Preferences**) to display the perspective that you require.

At the upper-left of the *APSolute Vision Settings* view, APSolute Vision displays the *APSolute Vision device-properties pane*. For more information, see Device-Properties Pane, page 52.

When you hover over a device node in the device pane, a popup displays. For more information, see Device-

Properties Hover Popup, page 52.

Figure 23: Vision Settings View (Showing the System Perspective)

Vision Settings button—Switches to the *APSolute Vision Settings* view.

Displays the *device pane*.

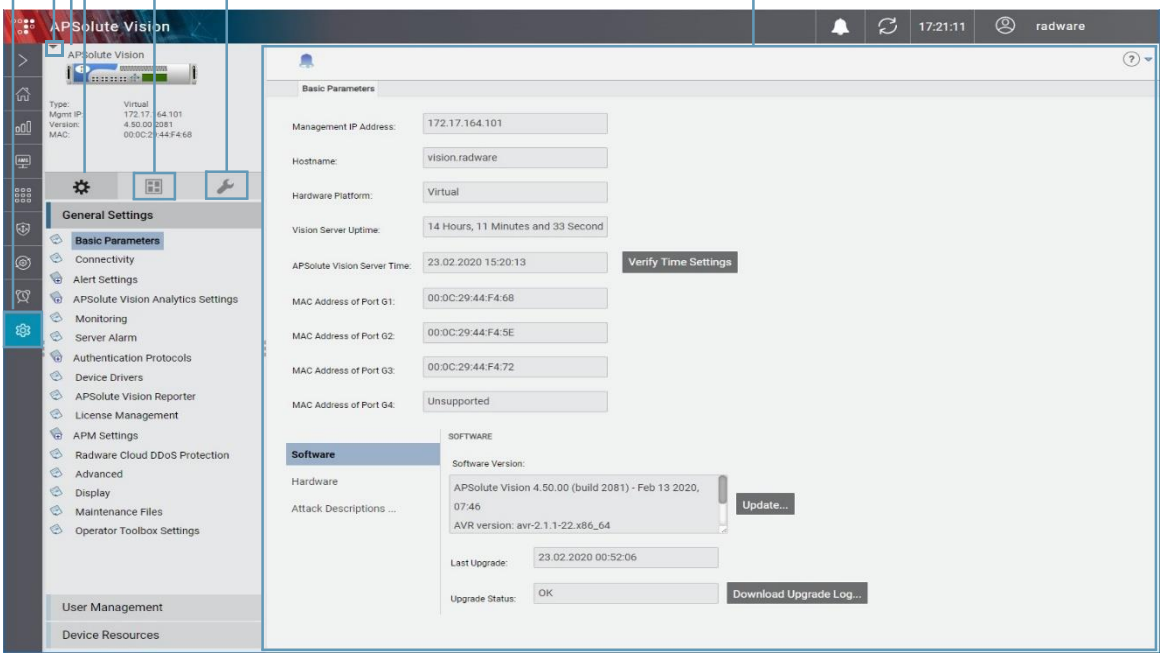
APSolute Vision device-properties pane.

The *System* perspective in the *APSolute Vision Settings* view is being displayed.

Dashboards button—Displays the *Dashboards* perspective in the *APSolute Vision Settings* view.

Preferences button—Displays the *Preferences* perspective in the *APSolute Vision Settings* view.

Content area.



Settings View–System Perspective

Administrators can use the *APSolute Vision Settings* view *System* perspective to do the following:

- **Monitor or manage the general settings of the APSolute Vision server**–Monitoring and managing the general settings of the APSolute Vision server include the following:
  - General properties, details, and statistics of the APSolute Vision server
  - Statistics of the APSolute Vision server
  - Connectivity
  - Alert browser and security alerts
  - Monitoring parameters
  - Server alarm thresholds
  - Authentication protocols
  - Device drivers
  - APSolute Vision Reporter for Radware DefensePro DDoS Mitigation
  - Licenses
  - Advanced general parameters
  - Display formats
  - Maintenance files
  - Operator Toolbox settings
- **Manage and monitor users**–Users can, in turn, manage multiple devices concurrently. Using APSolute Vision RBAC, administrators can allow the users various access control levels on devices. RBAC provides a set of predefined roles, which you can assign per user and per working scope (device or group of devices). RBAC definition is supported both internally (in APSolute Vision) and through remote authentication.
- **Manage device resources** –For device backup files and device subscriptions.

Note: For more information on operations that are exposed in the *APSolute Vision Settings* view *System* perspective, see the *APSolute Vision User Guide*.

Settings View–Dashboards Perspective

Users with a proper role can use the *APSolute Vision Settings* view *Dashboards* perspective to access the following:

- **Application SLA Dashboard**–For more information, see the *APSolute Vision User Guide*.
- **Security Control Center**–For more information, see the *APSolute Vision User Guide*.

Settings View–Preferences Perspective

Use the *Preferences* perspective to change your password or select the landing page (that is, the page that APSolute Vision displays when you open APSolute Vision WBM).

Device Pane

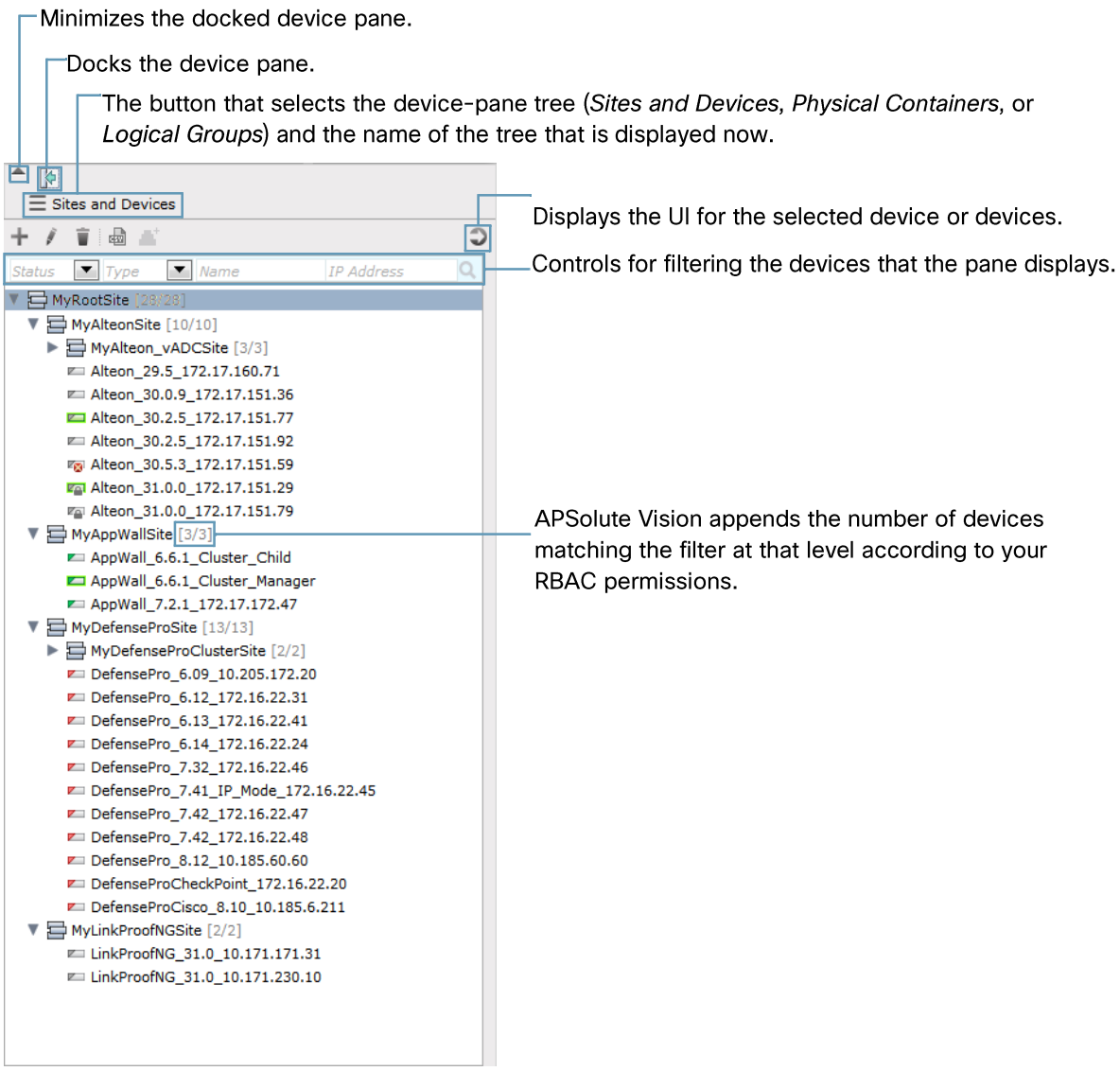
Users with a proper role can use the *device pane* to add or delete the devices that the APSolute Vision server manages.

If the device pane is not being displayed, to display it, click the little downward-pointing arrow ( ) close to the upper-left corner of the APSolute Vision main screen.

To organize and manage devices, the device pane includes the following three different trees:

- **Sites and Devices**—The *Sites and Devices* tree can contain user-defined *Sites* and Radware DefensePro DDoS Mitigation devices (*instances*).
- **Physical Containers**—The *Physical Containers* tree is not relevant for Radware DefensePro DDoS Mitigation.
- **Logical Groups**—The *Logical Groups* tree contains user-defined Logical Groups. A Logical Group is a group of devices of the same type, which you manage as a single entity.

Figure 24: Device Pane (Not Docked)—Showing the Sites and Devices Tree



Notes

- For information on how to add or delete the devices that the APSolute Vision server manages, see Managing Radware DefensePro DDoS Mitigation Devices, APSolute Vision Sites, andLogical Groups, page 59.
- For more information on the device pane, see Using the Device Pane, page 59.
- When you double-click a device in the *Sites and Devices* tree, APSolute Vision displays the device-properties pane and the last perspective that you viewed on the device along withthe corresponding content area.
- In the context of role-based access control (RBAC) RBAC, Sites and Logical Groups enable administrators to define the scope of each user. For more information on RBAC, see the *APSolute Vision User Guide*.
- For more information on Logical Groups, see, see Using Logical Groups of Devices, page 72.

Device-Properties Hover Popup

When you hover over a device node in the device pane, a popup displays the following parameters:

- **Device Name**–The user-defined device name.
- **Status**–The device general status: **Up**, **Down**, or **Maintenance**.
- **Locked By**–If the device is locked, the user who locked it.
- **Management IP Address**–The host or IP address of the device.
- **Device Type**–The device type, that is, **Radware DefensePro DDoS Mitigation**.
- **Version**–The device version.
- **MAC**–The MAC address.
- **Form Factor**–This form factor of the device.
- **Platform**–The platform type.
- **HA Status**–The high-availability status of the device: **Standalone**, **Primary**, or **Secondary**.
- **Device Driver** –The device drivername.
- **RTU License**–The status of the *Right to Use* license: **Valid** or **Invalid**.

Note: If the status of the *Right to Use* license is **Invalid**, the device icon in the device pane has a red slash through it– for Radware DefensePro DDoS Mitigation.

Logical-Group-Properties Hover Popup

When you hover over a Logical Group in the device pane *Logical Groups* tree, a popup opens. For more information, see Logical Group User Interface, page 73.

Device-Properties Pane

When you select a single device in the device pane, all APSolute Vision perspectives display the *device-properties pane* (see Figure 23 - Vision Settings View (Showing the System Perspective), page 49,Figure 27 - Monitoring Perspective–Radware DefensePro DDoS Mitigation, page 55, Figure 28 - Radware DefensePro DDoS Mitigation Security Monitoring Perspective–Showing the Security Dashboard, page 56).

When you select *multiple* devices in the device pane, APSolute Vision displays the multi-device view.

When you select a single device in the device pane, the device-properties pane displays the following parameters:

- *The device type (Alteon, AppWall, Radware DefensePro DDoS Mitigation, or LinkProof NG)and the user-defined device name.*
- *An icon showing whether the device is locked.*
- *A picture of the device front panel. When the device is locked, you can click the*  *button to reset or shut down the device.*
- **Status**—The device general status: **Up**, **Down**, or **Maintenance**.
- **Locked By**—If the device is locked, the user who locked it.
- **Type**—The platform and form-factor.
- **Platform** (displayed only for Radware DefensePro DDoS Mitigation devices)—The platform type, for example **x420**.
- **Mngt IP** —The host or IP address of thedevices.
- **Version**—The device version.
- **MAC** —TheMAC address.
- **HA Status**—The high-availability status of the device: **Standalone**, **Primary**, or **Secondary**.
- **Device Driver** —Thedevice driver name.
- **User Role**—The RBAC role that the user has for the selected device. The **User Role** parameter clarifies situations where the configuration of a user includes multiple devices (scopes) and differing roles. For more information on RBAC users and role-scope pairs, see the *APSolute Vision User Guide*.

Configuration Perspective

Use the *Configuration* perspective to configure devices.

Choose the device to configure in the device pane.

You can view and modify device configurations in the *content pane*.

The following points apply to all configuration tasks in the *Configuration* perspective:

- To configure a device, you must lock it. For more information, see the APSoluteVision documentation.
- When you change a field value (and there is configuration that is pending **Submit** action), the tab title changes to in italics with an asterisk (*).
- By default, tables display up to 20 rows per table page.
- You can perform one or more of the following operations on table entries:
  - Add a new entry to the table, and define its parameters.
  - Edit one or more parameters of an existing table entry.
  - Delete a table entry.
  - Device configuration information is saved only on the managed device, not in theAPSolute Vision database.

To commit information to the device, you must click **Submit** when you modify settings in a configuration dialog box or configuration page.

Some configuration changes require an immediate device reboot. When you submit the configuration change the device will reboot immediately.

Some configuration changes require a device reboot to take effect, but you can save the change without an immediate reboot. When you submit a change without a reboot, the *Properties* pane displays a "Reboot Required" notification until you reboot the device.

Click **Update Policies** to implement policy-configuration changes if necessary. Policy-configuration changes for a device are saved on the Radware DefensePro DDoS Mitigation device, but the device does not apply the changes until you perform a device configuration update. If the new configuration requires an Update Policies operation to take effect, the button is displayed with an orangeicon.

Figure 25: Update Policies Button

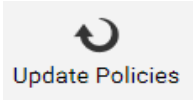
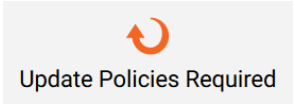


Figure 26: Update Policies Required Button



Example Device selection in the *Configuration* perspective

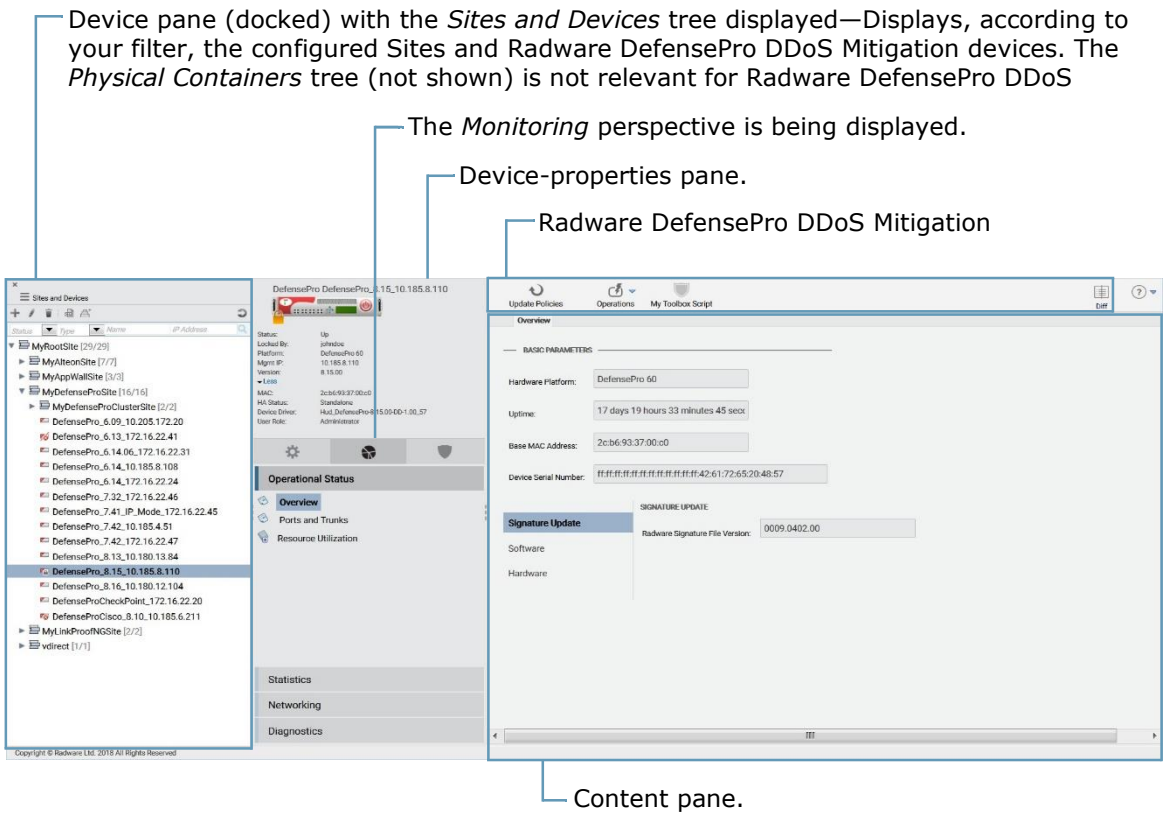
The following example shows the selections you would make to view or change configuration parameters for a device:

1. Select the required device in the device pane by drilling down through the Sites and child Sites.
2. Lock the device by clicking the icon in the device-properties pane. The icon changes to (a picture of a locked padlock).
3. Click **Configuration** ( ) to open the *Configuration* perspective.
4. Navigate to the configuration objects in the content pane.

Monitoring Perspective

In the *Monitoring* perspective, you can monitor physical devices and interfaces, and logical objects.

Figure 27: Monitoring Perspective–Radware DefensePro DDoS Mitigation



Security Monitoring Perspective

APSolute Vision displays the *Security Monitoring* perspective to view and analyze real-time security information of managed devices.

The *Security Monitoring* perspective is available for single devices and also for multiple devices. Security monitoring for multiple devices supports two report categories: the *Dashboard View* and *Traffic Monitoring*. Security monitoring for single devices supports two additional report categories: *Protection Monitoring* and *HTTP Reports*.

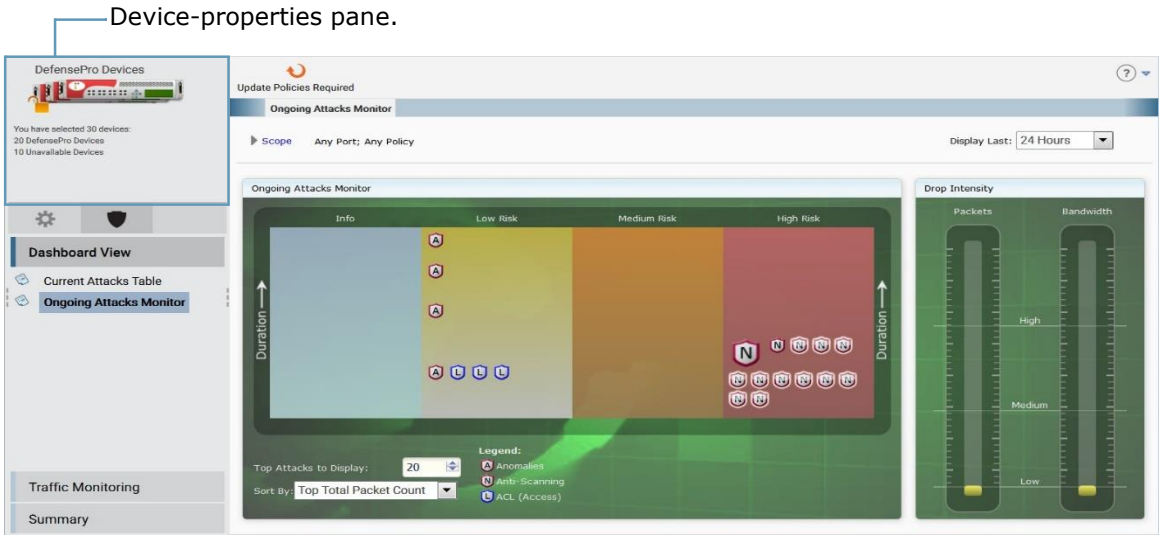
You can filter the Sites and devices that APSolute Vision displays. The filter does not change the contents of the tree, only how APSolute Vision displays the tree to you.

For DefenseFlow and Radware DefensePro DDoS Mitigation, the *Security Monitoring* perspective includes the following tabs:

- **Dashboard View**–Comprises the following:
  - **Security Dashboard** –A graphical summary view of all current active attacks in the network with color-coded attack-category identification, graphical threat-level indication, and instant drill-down to attack details.
  - **Current Attacks**–A view of the current attacks in a tabular format with graphical notations of attack categories, threat-level indication, drill-down to attack details, and easy access to the protecting policies for immediate fine-tuning.
- **Traffic Monitoring**–A real-time graph and table displaying network information, with the attack traffic and legitimate traffic filtered according to specified traffic direction and protocol.

- **Protection Monitoring**—Real-time graphs and tables with statistics on policies, protections according to specified traffic direction and protocol, along with learned traffic baselines.
- **HTTP Reports**—Real-time graphs and tables with statistics on policies, protections according to specified traffic direction and protocol, along with learned traffic baselines.

Figure 28: Radware DefensePro DDoS Mitigation Security Monitoring Perspective—Showing the Security Dashboard



Note: For more information on the *Security Monitoring* perspective, see Using Real-Time Security Monitoring, page 323.

Selecting Your Landing Page

You can select the page that APSolute Vision displays when you open APSolute Vision WBM.

To select your landing page

1. In the *APSolute Vision Settings* view *Preferences* perspective, select **User Preferences> Display**.
2. Configure the parameter, and click **Submit**.

Table 2: Display Parameter

Parameter	Description
Default Landing Page	The page that APSolute Vision displays when you open APSolute Vision WBM. Values: • None–When you open APSolute Vision WBM, you land in the default page configured on the APSolute Vision server. • Application SLA Dashboard–When you open APSolute Vision WBM, you land on the Application SLA Dashboard. • Security Control Center–When you open APSolute Vision WBM, you land on the Security Control Center. • Operator Toolbox–When you open APSolute Vision WBM, you land on the Toolbox. • Service Status Dashboard–When you open APSolute Vision WBM, you land on the Service Status Dashboard. Default: None **Note:** Your user role and scope determines the available options. If you do not have permission to view the default page configured on the APSolute Vision server, you land in the first permitted tab of the APSolute Vision *Settings* view.

Using Common GUI Elements in APSolute Vision

This section contains the following:

- Icons/Buttons and Commands for Managing Table Entries, page 57
- Filtering Table Rows, page 58

Icons/Buttons and Commands for Managing Table Entries

The following table describes icons/buttons and corresponding commands that are available when you manage table entries (rows) using APSolute Vision Web Based Management. The commands that are available depend on the feature. The icons/buttons are always above a table on the left side. When the cursor (pointer) hovers over an icon/button, the display changes from monochrome (gray) to colored.

Notes

- You can configure and control a managed device only when the device is locked (see Locking and Unlocking Devices, page 68).

- The APSolute Vision documentation shows icons/buttons in their colored state.

Table 3: Icons/Buttons and Commands for Managing Table Entries

Icon/Button	Command	Description
	Add	Opens an “Add New...” tab to configure a new entry.
	Edit	Opens an “Edit...” tab to modify the selected existing entry.
	Duplicate	Opens an “Add New...” tab, which is populated with the values from the selected entry, except for the indexes.
	Delete	Deletes the selection.
	Export	Exports the selected entry.
	View	Opens a “View...” tab to view the values of the selected entry.

Filtering Table Rows

For many tables in APSolute Vision and managed devices, you can filter table rows accordingto values in the table columns.

The filter uses a Boolean AND operator for the filter criteria that you specify. That is, the filtered table displays the rows that match *all* the search parameters, not *any* of the search parameters. For example, if the table includes the columns *Policy* and *Port*, and you filter for the policy value **ser**, and the port value **80**, the filtered table displays rows where the value of the Policy parameter includes **ser** AND the value of the Port parameter includes **80**.

To filter table rows

1. Do the following:
   - If a table column displays a drop-down list (with an arrow, like this, 

), click the arrow and select the value to filter by.
   - If the table column displays a white, text box (like this, 

), type the value to filter by.

   Notes

   - For text boxes, the filter uses a *contains* algorithm. That is, the filter considers it to be a match if the string that you enter is merely *contained* in a value. For example, if youenter **ser** in the text box, the filter returns rows with the values **ser**, **service1**, and**service2**.
   - If the box at the top of a column is gray (like this,), you cannot filter according to that parameter.
2. Click the  (Filter) button or press **Enter**.

Managing Radware DefensePro DDoS Mitigation Devices, APSolute Vision Sites, and Logical Groups

Before you can configure a Radware DefensePro DDoS Mitigation device and security policies through APSolute Vision, the Radware DefensePro DDoS Mitigation device must exist on and be connected to the APSolute Vision server. Only users with the proper permissions can add Radware DefensePro DDoS Mitigation devices to an APSolute Vision server.

Note: For more information on APSolute Vision permissions, see the *APSolute Vision User Guide*.

Before you can configure Radware devices through APSolute Vision, you add devices to the APSolute Vision server configuration. You can group devices into *Sites* and/or *Logical Groups*.

This section contains the following topics:

- Using the Device Pane, page 59
- Configuring Sites, page 60
- Managing Individual Radware DefensePro DDoS Mitigation Devices in APSolute Vision, page 62
- Locking and Unlocking Devices, page 68
- Using the Multi-Device View and the Multiple Devices Summary, page 69
- Using Logical Groups of Devices, page 72
- After You Set Up Your Managed Devices, page 76

Note: To add Radware DefensePro DDoS Mitigation devices to APSolute Vision or remove them, you can also use vDirect with APSolute Vision. For more information, see the *APSolute Vision User Guide*.

Using the Device Pane

You organize the devices that APSolute Vision manages in the *device pane*. The

following topics describe using the device pane:

- Device Pane Trees, page 60
- Configuring Sites, page 60
- Tree Nodes, page 61
- Exporting a CSV File with the Devices in the Sites and Devices Tree, page 61
- Filtering Entities in the Device Pane, page 61

Note: For a picture of the device pane, see Figure 24 – Device Pane (Not Docked)–Showing the Sites and Devices Tree, page 51.

Device Pane Trees

To organize and manage devices, the device pane includes the following three different trees:

- **Sites and Devices**–The *Sites and Devices* tree can contain Radware DefensePro DDoS Mitigation devices.
- **Physical Containers**–The *Physical Containers* tree is not relevant for Radware DefensePro DDoS Mitigation.
- **Logical Groups**–The *Logical Groups* tree contains user-defined Logical Groups. A Logical Group is a group of devices of the same type, which you manage as a single entity. For more information on Logical Groups, see, see Using Logical Groups of Devices, page 72.

To display another tree, click the ☰ button, and select the name of the tree that you require.

Configuring Sites

You can configure Sites in the *Sites and Devices* tree and in the *Physical Containers* tree. You may configure Sites according to a geographical location, administrative function, or device type. You can nest Sites; that is, each Site can contain child Sites and devices. By default, the root Site is called *Default*. You can rename this Site, and add nested Sites and devices. You can add, rename, and delete Sites. When you delete a Site, you must first remove all its child Sites anddevices.

Notes

- To move a device between Sites, you must first delete the device from the tree and then add the device in the required Site.
- A Site cannot have the same name as a device, and Sites nested under different parentSites cannot have the same name.
- You cannot delete the *Default* Site, but you can rename it.

To add a new Site

1. In the device pane, click the ☰ icon, and select **Sites and Devices** or **Physical Containers**.
2. In the device pane *Sites and Devices* tree or *Physical Containers* tree, select the Site nodein which you want to create the new Site.
3. Click the ➕ (Add) button in the tab toolbar.
4. From the **Type** drop-down list, select **Site**.
5. In the **Name** text box, type the name of the Site.
6. Click **Submit**.

Caution: With remote authentication, if a user definition explicitly mentions the name of a Site and the Site name changes, the user definition in the authentication server must be updated accordingly. For more information, see the *APSolute Vision User Guide*.

If the name of an APSolute Vision Site changes and APSolute Vision authenticates the userslocally, APSolute Vision updates the relevant scopes for the users.

To rename a Site

1. In the device pane, click the ☰ icon, and select **Sites and Devices** or **Physical Containers**.
2. Select the Site.
3. Click the  (Edit) button.
4. In the **Name** text box, type the name of the Site.
5. Click **Submit**.

To delete a Site

1. In the device pane, click the ☰ icon, and select **Sites and Devices** or **Physical Containers**.
2. Select the Site.
3. Click the  (Delete) button and confirm your action.

Tree Nodes

Tree nodes are arranged alphabetically in the tree within each level.

All nested Sites appear before devices at the same level, regardless of their alphanumerical order.

All node names in a tree must be unique. For example, you cannot give a Site and a device the same name, and you cannot give devices in different Sites the same name.

Node names are case-sensitive.

Exporting a CSV File with the Devices in the Sites and Devices Tree

You can export a CSV file with the devices in the *Sites and Devices* tree. The CSV file includes information on each device. The file does not include information regarding associated Sites.

For more information, see the procedure To export a CSV file with the devices in the Sites and Devices tree, page 67.

Filtering Entities in the Device Pane

You can filter the Sites, devices, and Logical Groups that APSolute Vision displays. The filter applies to all the Sites, devices, and Logical Groups in the tree. The filter does not change the contents of the tree, only how APSolute Vision displays the tree to you. By default, APSolute Vision displays all the Sites, devices, and Logical Groups that you have permission to view. To each node in the tree, APSolute Vision appends the number of devices matching the filter at that level according to your RBAC permissions.

You can filter the Sites, devices, and Logical Groups that APSolute Vision displays according to the following criteria:

- **Status**—**Up**, **Down**, **Maintenance**, or **Unknown**. The *Logical Groups* tab includes the criteria **Valid** and **Invalid**.
- **Type**—**Alteon**, **AppWall**, **Radware DefensePro DDoS Mitigation**, or **LinkProof NG**. The *Physical Containers* tab does not display this field.
- **Name**—The name of a device, Site, Logical Group, or string contained in the name (for example, the value **aRy** matches an element named **Primary1** and **SecondaryABC**).

- **IP Address**–The IP address or portion of the IP address.

After you configure the filter criteria, to apply the filter, click the button to apply the filter.

Click the button to cancel the filter.

Managing Individual Radware DefensePro DDoS Mitigation Devices in APSolute Vision

Before you can manage a device in APSolute Vision, you need to add the device to the appropriate Site tree in the device pane.

The number of devices that APSolute Vision can manage depends on the *Right to Use* (RTU) license. For information on managing licenses in APSolute Vision, see the *APSolute Vision User Guide*.

When you add a device, you can define a name for it. You also provide the device-connection information, including authentication parameters (credentials) for communication between the device and the APSolute Vision server.

After APSolute Vision connects to the device, basic device information is displayed in the content pane, and device properties information is displayed in the device-properties pane.

After submitting device-connection information, the APSolute Vision server verifies that it can connect to the device. APSolute Vision then retrieves and stores the device information and licensing information.

After the connection has been established, you can modify some of the connection information and configure the device.

When you add a device or modify device properties, you can specify whether the APSolute Vision server configures itself as a target of the device events and whether the APSolute Vision server removes from the device all recipients of device events except for its own address. For more, important information, see APSolute Vision Server Registered for Device Events–Radware DefensePro DDoS Mitigation, page 67.

After adding devices, you can create clusters of the main and backup devices, or the primary and secondary devices (according to the device *type*).

Notes

- A device cannot have the same name as a Site.
- Devices in different Sites cannot have the same name.
- You can change the name of a device after you have added it to the APSolute Vision configuration.
- To move a device between Sites, you must first delete the device from the tree and then add it to the required target Site.
- If you replace a device with a new device to which you want to assign the same management IP address, you must delete the device from the Site and then recreate it for the replacement.
- When you delete a device, you can no longer view historical reports for that device.
- When you delete a device, the device alarms and security monitoring information are removed also.
- You can export a CSV file with the devices in the *Sites and Devices* tab. The CSV file includes information on each device. The file does not include information regarding associated Sites. For more information, see the procedure To export a CSV file with the devices in the Sites and Devices tree, page 67.

- HTTPS is used for downloading/uploading various files from/to managed devices, including: configuration files, certificate and key files, attack-signature files, device-software files, and so on. For this version of Radware DefensePro DDoS Mitigation, APSolute Vision uses Transport Layer Security (TLS) protocol version 1.1 or later. In the CLI, you can disable the TLS version 1.1 to use only version 1.2, using the **manage ssl version** command.

Caution: If a Radware DefensePro DDoS Mitigation device was added to APSolute Vision using vDirect (that is, *registered* on APSolute Vision), and the device Web (HTTPS) credentials are different from the CLI (SSH) credentials, you must update the Web credentials of the device in the APSolute Vision Device Properties dialog box. For the procedure, see To add a new device or edit device-connection information, page 63. For more information on vDirect, see the *APSolute Vision User Guide*.

This section includes the procedures to do the following:

- To add a new device or edit device-connection information, page 63
- To delete a device, page 66

To add a new device or edit device-connection information

1. In the device pane, click the ☰ icon, and select **Sites and Devices**.
2. In the device pane *Sites and Devices* tree, do one of the following:
   - To add a new device:
     a. Navigate to and select the Site name to which you want to add the device.
     b. Click the + (Add) button in the tab toolbar.
     c. From the **Type** drop-down list, select the device type that you require.
   - To edit device-connection information:
     a. Select the device name.
     b. Click the (Edit) button.
3. Configure the parameters, and click **Submit**.

   After APSolute Vision connects to the device, basic device information is displayed in the content pane, and device properties information is displayed in the device-properties pane.

Table 4: Device Properties: General Parameters

Parameter	Description
Type	The type of the object. Choose **DefensePro**.
Name	The name of the device. **Notes:** • There are some reserved words (for example, *DefenseFlow*) that APSolute Vision does not allow as names. • You can change the name of a device after you have added it to the APSolute Vision configuration.

Table 5: Device Properties: SNMP Parameters

Parameter	Description
Management IP	The management IP address as it is defined on the managed device. **Note:** Once you add the device to the APSolute Vision configuration, you cannot change its IP address.
SNMP Version	The SNMP version used for the connection.
SNMP Read Community (This parameter is displayed only when **SNMP Version** is **SNMPv1** or **SNMPv2**.)	The SNMP read community name.
SNMP Write Community (This parameter is displayed only when **SNMP Version** is **SNMPv1** or **SNMPv2**.)	The SNMP write community name.
User Name (This parameter is displayed only when **SNMP Version** is **SNMPv3**.)	The username for the SNMP connection. Maximum characters: 18
Use Authentication (This parameter is displayed only when **SNMP Version** is **SNMPv3**.)	Specifies whether the device authenticates the user for a successful connection. Default: Disabled
Authentication Protocol (This parameter is available only when the **Use Authentication** checkbox is selected.)	The protocol used for authentication. Values: MD5, SHA Default: SHA
Authentication Password (This parameter is available only when the **Use Authentication** checkbox is selected.)	The password used for authentication. **Caution:** The password *should* be at least eight characters. vDirect requires that password be at least eight characters.
Use Privacy (This parameter is available only when and the **Use Authentication** checkbox is selected.)	Specifies whether the device encrypts SNMPv3 traffic for additional security. Default: Disabled
Privacy Protocol (This parameter is available only when and the **Use Privacy** checkbox is selected.)	This version of Radware DefensePro DDoS Mitigation supports only the DES privacy protocol. Value: DES, AES128 Default: DES
Privacy Password (This parameter is available only when the **Use Privacy** checkbox is selected.)	The password used for the Privacy facility. **Caution:** The password *should* be at least eight characters. vDirect requires that password be at least eight characters.

Table 6: Device Properties: HTTP/S Access Parameters

Parameter	Description
Verify HTTP Access	Specifies whether APSolute Vision verifies HTTP access to the managed device. Default: Enabled
Verify HTTPS Access	Specifies whether APSolute Vision verifies HTTPS access to the managed device. Default: Enabled
User Name	The username for HTTP and HTTPS communication. Maximum characters: 32
Password	The password used for HTTP and HTTPS communication.
HTTP Port	The port for HTTP communication with the device. Default: 80
HTTPS Port	The port for HTTPS communication with the device. Default: 443

Table 7: Device Properties: SSH Access Parameters

Parameter	Description
User Name	The username for SSH access to the device. Maximum characters: 32 Default: admin
Password	The password for SSH access to the device. Maximum characters: 32 Default: admin
SSH Port	The port for SSH communication with the device. Default: 22 **Note:** This value should be the same as the value for the SSH port configured in the device (*Configuration* perspective, **System> Management Access > Management Protocols > SSH**).

Table 8: Device Properties: Event Notification Parameters

Parameter	Description
Register This APSolute Vision Server for Device Events	Specifies whether the APSolute Vision server configures itself as a target of the device events. Values: • Enabled–The APSolute Vision server configures itself as a target of the device events (for example, traps, alerts, IRP messages, and packet-reporting data). • Disabled–*For a new device,* the APSolute Vision server adds the device without registering itself as a target for events. *For an existing device,* the APSolute Vision removes itself as a target of the device events. Default: Enabled **Notes:** • APSolute Vision runs this action each time you click **Submit** in the dialog box. • For more, important information, see APSolute Vision Server Registered for Device Events–Radware DefensePro DDoS Mitigation, page 67.
Register APSolute Vision Server IP (This parameter is available only when the **Register This APSolute Vision Server for Device Events** checkbox is selected.)	The port and IP address of the APSolute Vision server to which the managed device sends events. Select an APSolute Vision server interface that is used as the APSolute Vision server data port, and is configured to have a route to the managed devices.
Remove All Other Targets of Device Events (This parameter is available only when the **Register This APSolute Vision Server for Device Events** checkbox is selected.)	Specifies whether the APSolute Vision server removes from the device all recipients of device events (for example, traps, and IRP messages) except for its own address. Default: Disabled **Note:** APSolute Vision runs this action each time you click **Submit** in the dialog box. For example, if you select the checkbox and click **Submit**–and later, a trap target is added to the trap target-address table–APSolute Vision removes the additional address the next time you click **Submit** in the dialog box.

To delete a device

1. In the device pane, click the ☰ icon, and select **Sites and Devices**.
2. Select the device name, and click the (Delete) button.
3. Click **Yes** in the confirmation box. The device is deleted from the list of managed devices.

To export a CSV file with the devices in the Sites and Devices tree

1. In the device pane, click the ☰ icon, and select **Sites and Devices**.
2. Click (Export Device List to CSV).
3. View the file or specify the location and file name, and then, click **Save**. The CSV file includes the following columns:
   - Device Name
   - Device Type
   - Status
   - Management IP Address
   - Software Version
   - MAC Address
   - License
   - Platform
   - Form Factor
   - HA Status
   - Device Driver

Note: The file does not include information regarding Sites or Logical Groups.

APSolute Vision Server Registered for Device Events–Radware DefensePro DDoS Mitigation

In the **Device Properties** dialog box, you can specify the following actions–which APSolute Vision runs each time you click **Submit** in the dialog box:

- Whether the APSolute Vision server configures itself as a target of the device events (**Register This APSolute Vision Server for Device Events** checkbox)
- Whether the APSolute Vision server removes from the device all recipients of deviceevents except for its own address (**Remove All Other Targets of Device Events** checkbox)

Caution: If the **Register This APSolute Vision Server for Device Events** checkbox is cleared, the Alert browser, security reporting, and APSolute Vision Reporter (AVR) might not collect and display information about the device.

Radware DefensePro DDoS Mitigation supports a device being managed by multiple APSolute Vision servers.

When multiple APSolute Vision servers manage the same Radware DefensePro DDoS Mitigation device, the device sends the following:

- Traps to all the APSolute Vision servers that manage it. The Target Address table and the Target Parameters table contain entries for all APSolute Vision servers.
- Packet-reporting data *only to the last APSolute Vision server that registered on the device*.

Locking and Unlocking Devices

When you have permission to perform device configuration on a specific device, you must lock the device before you can configure it. Locking the device ensures that other users cannot make configuration changes at the same time. The device remains locked until you unlock the device, you disconnect, until the *Device Lock Timeout* elapses, or an *Administrator* unlocks it.

Locking a device does not apply to the same device that is configured on another APSolute Vision server, using Web Based Management, or using the CLI.

Note: Only one APSolute Vision server should manage any one device. While the device is locked:

- The device icon in the device pane includes a small lock symbol– for Radware DefensePro DDoS Mitigation.
- Configuration panes are displayed in read-only mode to other users withconfiguration permissions for the device.
- If applicable, the **Submit** button is available.
- If applicable, the (Add) button is displayed.

To lock a single device

1. In the device pane, click the icon, and select **Sites and Devices** or **Physical Containers**.
2. Select the device.
3. In the device-properties pane, click (the drawing of the unlocked padlock at the lower-left corner of the device drawing). The drawing changes to (a picture of a locked padlock).

To unlock a single device

1. In the device pane, click the icon, and select **Sites and Devices** or **Physical Containers**.
2. Select the device.
3. In the device-properties pane, click (the drawing of the locked padlock at the lower-left corner of the device drawing). The drawing changes to (a picture of an unlocked padlock).

To lock multiple devices

1. In the device pane, click the icon, and select **Sites and Devices** or **Physical Containers**.

2. Select the devices to lock. You can select a Site or select multiple devices (usingstandard, mouse click/keyboard combinations) whether or not the devices are in the same Site.
3. Click the (View) button.
4. In the device-properties pane, click (the drawing of the unlocked padlock at the lower-left corner of the device drawing). The drawing changes to (a picture of a locked padlock).

To unlock multiple devices

1. In the device pane, click the icon, and select **Sites and Devices** or **Physical Containers**.
2. Select the devices to unlock. You can select a Site or select multiple devices (usingstandard, mouse click/keyboard combinations) whether or not the devices are in the same Site.
3. Click the (View) button.
4. In the device-properties pane, click (the drawing of the locked padlock at the lower-left corner of the device drawing). The drawing changes to (a picture of an unlocked padlock).

Tip: If you APSolute Vision setup uses Logical Groups, you can select a Logical Group to lock or unlock the devices in it.

Using the Multi-Device View and the Multiple Devices Summary

APSolute Vision displays the multi-device view when you do one of the following:

- Select a Logical Group in the *Logical Groups* tree in the device pane. For information about managing and configuring Logical Groups, see Using Logical Groups of Devices, page 72.
- Select multiple devices in the *Sites and Devices* tree or the *Physical Containers* tree in the device pane and then click the (View) button.

Use the multi-device view to do the following:

- **Lock multiple devices to configure them**.
- **View the *Multiple Devices Summary* table**. The table contains all the relevant devices and comprises the following columns: *Lock State*, *Device Type*, *Device Name*, *IP Address*, *Locked by User*, and *Status*.
- **Run configuration-management actions for the relevant devices**–You can run the Update Policies action on multiple Radware DefensePro DDoS Mitigation devices.
- **Use a Logical Group to configure the devices in it**–For information aboutconfiguring multiple devices simultaneously, see Configuring Multiple Devices, page 275.
- **Open the Multi-Device Configuration dialog box to configure simultaneously multiple devices of the same type and major version** –For information about configuring multiple devices simultaneously, see Configuring Multiple Devices, page 275.
- **Open the *Security Monitoring* perspective**–In the multi-device view, the *Security Monitoring* perspective displays the *Dashboard View* and *Traffic Utilization* tabs–with the data aggregated for all the selected devices. For more information, see Using Real-Time Security Monitoring, page 323.

Figure 29: Multi-Device View from the Site and Devices Tree

Multiple devices are selected. You can select a site or select multiple devices (using standard, mouse click/keyboard combinations) whether or not the devices are in the same site.

View button.

Configuration button—Opens the Multi-Device Configuration dialog box.

Security Monitoring button — Opens the *Security Monitoring* perspective.

The relevant configuration-management buttons display for the selected devices.

Multiple Devices Summary pane.

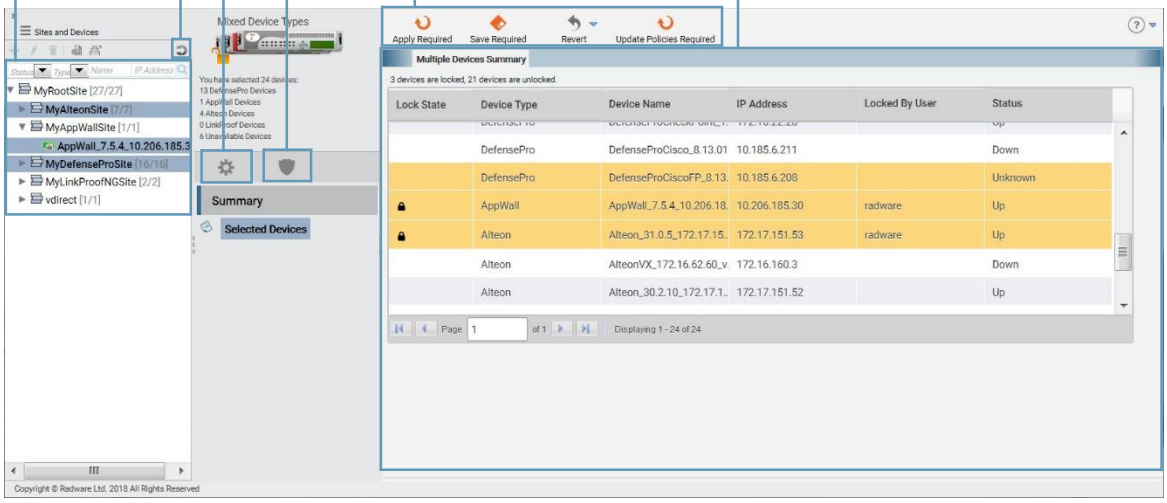


Figure 30: Multi-Device View from the Logical Groups Tree

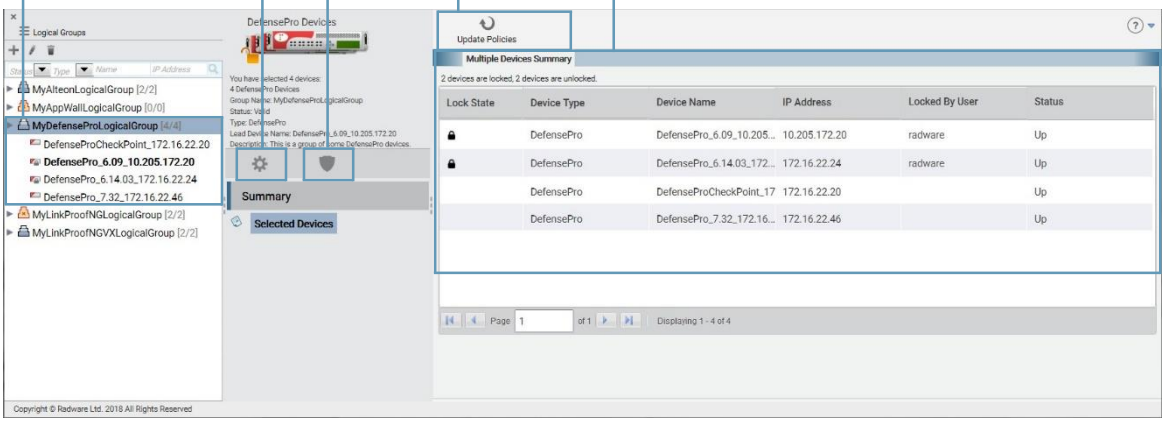
A Logical Group is selected, which automatically opens the multi-device view. APSolute Vision displays the name of the *lead device* with **bold lettering**. APSolute Vision dynamically chooses the lead device of the Logical Group. The lead device is always the device in the group that is available and running the earliest software version.

Configuration button—Opens the Multi-Device Configuration dialog box.

Security Monitoring button— Opens the *Security Monitoring* perspective.

The relevant configuration-management buttons display for the selected devices.

Multiple Devices Summary pane.



To open the multi-device view from the Sites and Devices tree

1. In the device pane, click the ☰ button, and select **Sites and Devices**.
2. Select the devices. You can select a Site or select multiple devices (using standard, mouse click/ keyboard combinations) whether or not the devices are in the same site.
3. Click the (View) button.

To open the multi-device view from the Logical Groups tree

1. In the device pane, click the ☰ button, and select **Logical Groups**.
2. Select the Logical Group.

Using Logical Groups of Devices

This section contains the following main topics:

- Logical Groups–General Information, page 72
- Logical Group User Interface, page 73
- Managing Logical Groups, page 74

Logical Groups—General Information

A Logical Group is a user-defined group of one or more devices of the same device type.

To be valid, a Logical Device group must contain at least one accessible device, and all the devices in the group must be the same device type.

The devices in a Logical Group do not need to be running the same software version. The

same device can exist in more than one Logical Group.

You can use a Logical Group to help you perform the following:

- **Define the scope of APSolute Vision users**–The **Scope** value of a user's RBAC role/scope pair can be a Logical Group. The user's scope dynamically updates, according to the devicesin the Logical Group. That is, when the device-set of a Logical Group changes, the user's scope changes accordingly. For more information on Role-Based Access Control (RBAC), see the *APSolute Vision User Guide* or online help.
- **Manage multiple devices simultaneously**–When you configure the devices in a Logical Group, you use the multi-device view (see Using the Multi-Device View and the Multiple Devices Summary, page 69) to do the following:
  - **View the *Multiple Devices Summary* table**. The table contains all the relevant devices and comprises the following columns: *Lock State*, *Device Type*, *Device Name*, *IPAddress*, *Locked by User*, and *Status*.
  - **Lock multiple devices to configure them**.
  - **Make configuration changes to the *lead device* and apply the changes to the other devices in the Logical Group**–APSolute Vision dynamically chooses the lead device of the Logical Group. The lead device is always the device in the group that is available, and running the earliest software version. APSolute Vision displays the name of the lead device with bold lettering. After you make a valid change and click **Submit All**, APSolute Vision attempts to change the value for the submitted parameters on the lead device and all the other devices in the Logical Group. APSolute Vision submits only modified values; APSolute Vision does not submit values that were not modified. For more information, see the Configuring Multiple Devices, page 275.
  - **Run configuration-management actions for the relevant devices**–You can run the Update Policies action on multiple Radware DefensePro DDoS Mitigation devices.
  - **Open the *Security Monitoring* perspective**–In the multi-device view, the *Security Monitoring* perspective displays the *Dashboard View* and *Traffic Utilization* tabs–with the data aggregated for all the selected devices. For more information, see Using Real-Time Security Monitoring, page 323.
- **Specify devices for scheduled tasks** –In addition to selecting individual devices, you can specify one or more relevant Logical Groups. For more information on scheduled tasks, seethe Scheduling APSolute Vision and Device Tasks, page 284.
- **Specify devices for Operator Toolbox scripts** –In addition to selecting individual devices, you can specify one or more relevant Logical Groups. APSolute Vision provides many predefined *Toolbox* scripts for Radware DefensePro DDoS Mitigation, which automate and streamline common configuration and management actions. For more information, see the *APSolute Vision User Guide* or online help.

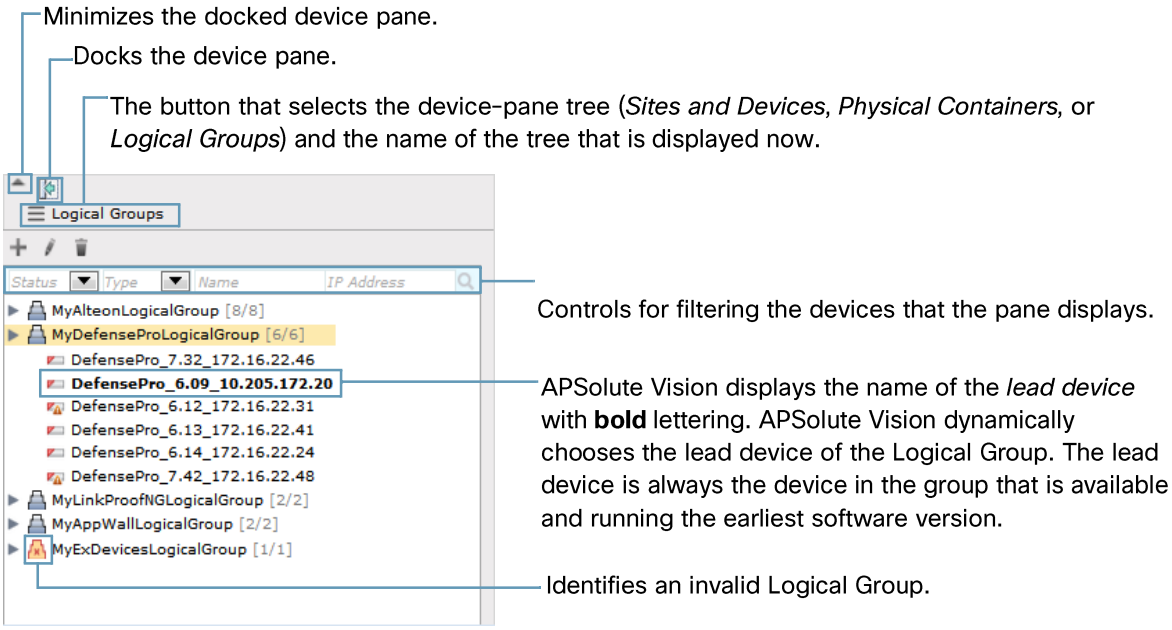
- **Specify devices for sending or deleting Radware DefensePro DDoS Mitigation configuration templates**–In addition to selecting individual devices, you can specify one or more Logical Groups of Radware DefensePro DDoS Mitigation devices. For more informationon Radware DefensePro DDoS Mitigation configuration templates, see Using Configuration Templates for Security Policies, page 266.
- **Specify devices for Alert Profile**–In addition to selecting individualdevices, you can specify one or more relevant Logical Groups. For more information on Alert Profiles, see the *APSolute Vision User Guide* or online help.
- **Specify devices for the Alerts Table Filter**–In addition to selecting individual devices, you can specify one or more relevant Logical Groups. For more information on the Alerts Filter,see the *APSolute Vision User Guide* or online help.
- **Specify devices for REST API operations**–For information on the REST API, see the APSolute Vision REST API documentation.

Logical Group User Interface

The user interface for existing Logical Groups comprises the following:

- The *Logical Groups* tree in the device pane and the popup displays information for eachLogical Group node.
- The multi-device view, which is displayed when you click a Logical Group node in the *Logical Groups* tree. For more information, see Using the Multi-Device View and the Multiple Devices Summary, page 69.

Figure 31: Device Pane (Not Docked)–Showing the Logical Groups Tree with a Logical Group of Radware DefensePro DDoS Mitigation Devices

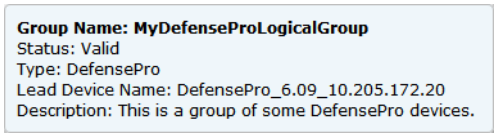


Note: For information on filtering the display of the tree, see Filtering Entities in the Device Pane, page 61.

When you hover over a Logical Group node in the device pane, a popup displays the following parameters:

- **Group Name**–The user-defined name of the Logical Group.
- **Status**–The status of the group: **Valid** or **Invalid**.
- **Invalid Reason** (displayed only when **Status** is **Invalid**)–The reason that the Logical Group is invalid.
- **Type**–The device type of the group, that is: **Alteon**, **AppWall**, **Radware DefenseProDDoS Mitigation**, or **LinkProof NG**.
- **Lead Device Name**–The name of the lead device of the Logical Group, select the *lead* device– that is, the device whose configuration changes will be applied to the select devices.
- **Description**–The user-defined description of the Logical Group.

Figure 32: Popup for Logical Group Node in the Device Pane



Managing Logical Groups

Only users with a proper RBAC roles can manage Logical Groups (Administrator, Vision Administrator, and System User).

To be valid, a Logical Device group must contain at least one accessible device, and all the devices in the group must be the same device type.

You can create a new Logical Group in any of the three trees that the device pane can display. However, you cannot *modify* Logical Groups in the device pane *Sites and Devices* tree or *Physical Containers* tree.

Caution: With RADIUS or TACACS+ authentication, if a user definition explicitly mentions the name of a Logical Group and the Logical Group name changes, the user definition in the RADIUS or TACACS+ server must be updated accordingly. For more information, see the *APSolute Vision User Guide*.

If the name of Logical Group changes and APSolute Vision authenticates the users locally, APSolute Vision updates the relevant scopes for the users.

In the device pane *Logical Groups* tree, you can configure and modify Logical Groups.

To configure a Logical Group from the Logical Groups tree

1. In the device pane, click the ☰ button, and select **Logical Groups**.
2. Do one of the following:
   - To create a new Logical Group, click the + (Add) button.
   - To edit a Logical Group, select the Logical Group node and click the ✎ (Edit) button.
3. Configure the parameters, and click **Submit**.

Table 9: Logical Groups Parameters

Parameter	Description
Type	The device type. When you are creating a new Logical Group, the **Type** value determines the devices that the *Device* lists display. When you are editing a Logical Group, the **Type** value is read-only. Values: • Alteon • AppWall • Radware DefensePro DDoS Mitigation • LinkProof NG Default: Alteon
Name	The name of the Logical Group. Maximum characters: 255
Devices	The **Available** list and the **Selected** list. The **Available** list displays the available devices. The **Selected** list displays the devices in the Logical Group.
Description	The description of the Logical Group. Maximum characters: 255

In the device pane *Sites and Devices* tree and *Physical Containers* tree, you can select devices and create a new Logical Group.

To create a new Logical Group from the Sites and Devices tree or Physical Containers tree

1. In the device pane, click the button, and select **Sites and Devices** or **Physical Containers**.
2. In the *Sites and Devices* or *Physical Containers* tree, select the devices, which must be ofthe same type. You can select multiple devices (using standard, mouse click/keyboard combinations) whether or not the devices are in the same Site.
3. Click the (Add Group) button.
4. Configure the parameters, and click **Submit**.

Table 10: Logical Groups Parameters

Parameter	Description
Type	(Read-only) The device type.
Name	The name of the Logical Group. Maximum characters: 255
Devices	The **Available** list and the **Selected** list. The **Available** list displays the available devices. The **Selected** list displays the devices in the Logical Group.
Description	The description of the Logical Group. Maximum characters: 255

You cannot delete a Logical Group if it is the used in a user role-scope pair.

To delete a Logical Group

1. In the device pane, click the ☰ button, and select **Logical Groups**.
2. In the device pane *Logical Groups* tree, click the Logical Group node, and click the (Delete) button.
3. Click **Yes** in the confirmation box. The Logical Group is deleted from the *Logical Groups*tree.

After You Set Up Your Managed Devices

After you set up your network of managed devices, and establish a connection to the devices, APSolute Vision obtains the network configuration and displays the settings in the device configuration tabs.

You can then do the following:

- Set and change the device configuration through APSolute Vision.
- Perform administration and maintenance tasks on managed devices such as schedulingtasks, making backups, and so on.
- Monitor managed devices through APSolute Vision.

CHAPTER 3 – MANAGING THE RADWARE DEFENSEPRO DDOS MITIGATION SETUP

You can configure the following setup parameters for a selected Radware DefensePro DDoS Mitigation device:

- Managing Software Versions, page 77
- Configuring the Global Parameters, page 81
- Configuring Date and Time Parameters 83
- Configuring the Networking Setup, page 83
- Configuring the Device-Security Setup, page 88
- Configuring the SSL-Settings Setup, page 107
- Configuring the Security-Settings Setup, page 120
- Configuring the Advanced-Parameters Setup, page 139
- Configuring the Reporting-Settings Setup, page 146
- Configuring the Clustering Setup, page 151

Managing Software Versions

You can use the *Software Version Management* pane to manage up to eight *software-version packages*, which are stored on the Radware DefensePro DDoS Mitigation device. There is one *active* version, and there can be up to seven non-active (*idle*) versions. Activating a software-version does not alter the existing configuration. Activating a software-version *may* constitute a device upgrade (to enable new features and functions on the device) and/or a minor-version or hotfix-version upgrade for specific components only.

You can use the *Upload Software Version* pane to upload software-version packages (see Uploading Radware DefensePro DDoS Mitigation Software, page 79).

The Software Version Management feature and the associated upload process enables your certification process of a Radware DefensePro DDoS Mitigation release to be simpler, because less testing is required following hotfix upgrades. Radware DefensePro DDoS Mitigation *hotfix* versions are identified by the number after the third dot in version number. For example, 8.17.3.4 is a hotfix version for version 8.17.3.

A software-version package of a *hotfix* version may comprise any combination of the device components (for example, only the DME and operating system):

- Radware DefensePro DDoS Mitigation application
- DME
- Device driver
- Operating system

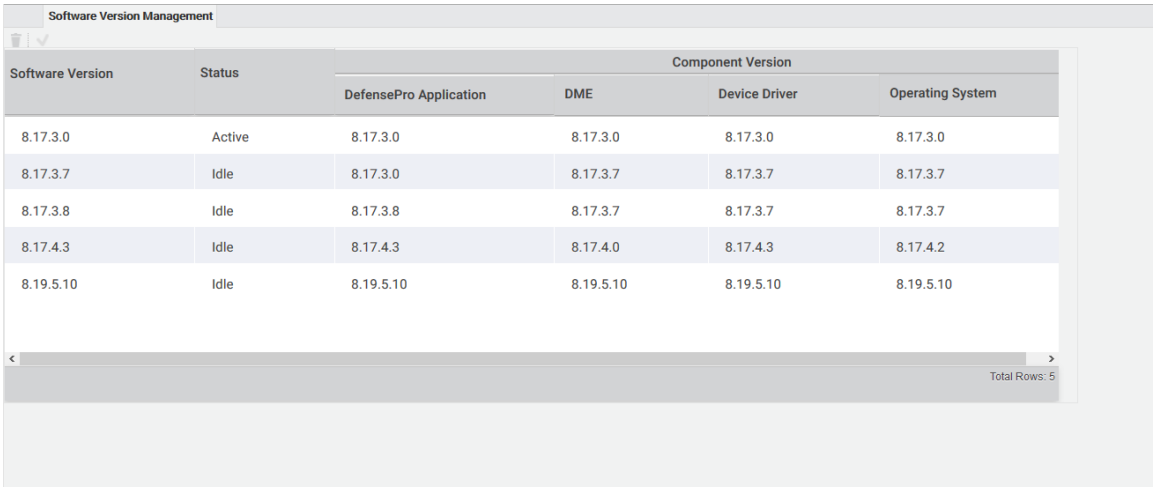
When you upload a software-version package of a hotfix version that does not contain the full installation (all four components), there needs to be a full installation already on the device.

If the Radware DefensePro DDoS Mitigation device is already storing the maximum eight software- version packages, you must first delete at least one, *idle* software-version package (see the procedure To delete a software-version package stored on the Radware DefensePro DDoS Mitigation device, page 79 below).

The table in the *Software Version Management* pane displays all the stored software-version packages, the status (**Idle** or **Active**), and the versions of the components. You can select a row in the table with the software-version package that comprises the component versions you require and

click the (Activate Selected Version) button to activate it. To delete a software-version package, select the row, and click the (Delete Selected Version) button.

Figure 33: Software Version Management Pane



Notes

- You cannot delete the *active* software version.
- The table in the *Software Version Management* pane displays the versions of thecomponents version 8.17.3.0 and later. For earlier versions, the table displays **N/A**.
- The version of a component cannot be later than the software versions that it isassociated with—that is, the value in the *Software Version* column of the table row.

Caution: If you activate a software-version package of a version earlier than the current *active* version, all configurations changes since you upgraded will be lost.

Caution: If you activate a software-version package of a version earlier than 8.17.3, *all* previous configurations and other software-version packages will be lost.

Caution: Before upgrading to a newer software version, do the following:

- Back up the existing configuration file. For more information, see Downloading a Device-Configuration File, page 281.
- Ensure that you have configured on the device the authentication details for the protocol used to upload the file.

To activate a software-version package stored on the Radware DefensePro DDoS Mitigation device

1. In the *Configuration* perspective, select **Setup > Software Version Management**.
2. Select the row with the required software-version package and click the (Activate Selected Version) button. The devices reboots, the value in the *Status* column of the active software- version package changes to **Idle**, and the value in the *Status* column of the software-version package that you selected changes to **Active**.

To delete a software-version package stored on the Radware DefensePro DDoS Mitigation device

1. In the *Configuration* perspective, select **Setup > Software Version Management**.
2. Select the row with the required software-version package and click the (Delete Selected Version) button.

Uploading Radware DefensePro DDoS Mitigation Software

You can use the *Upload Software Version* pane to upload *software-version packages*, which include release-specific *components* (see Managing Software Versions, page 77).

If the Radware DefensePro DDoS Mitigation device is already storing the maximum eight software- version packages, you must first delete at least one *idle* software-version package (see the procedure To delete a software-version package stored on the Radware DefensePro DDoS Mitigation device, page 79).

The software-version-package file must be accessible from your PC. APSolute Vision transfers the file, over HTTPS, to the APSolute Vision server and uploads it to the Radware DefensePro DDoS Mitigation device.

For minor-version or hotfix-version upgrades, a password is not required.

New major versions require a password. If the device has a valid support agreement, APSolute Vision can generate a new password automatically.

Notes

- Use the *Software Version Management* pane to *manage* the software-version packages.For more information, see Managing Software Versions, page 77.
- If the Radware DefensePro DDoS Mitigation platform is very far away from the machine with the software-version-package file, upload may take a very long time. Besides distance, the line quality may further increase the upload time.

To upload a software-version package onto a Radware DefensePro DDoS Mitigation device

1. In the *Configuration* perspective, select **Setup > Software Version Management >Upload Software Version**.
2. Configure the parameters, and click **Upload and Activate** or **Upload Without Activating**.

Table 11: Software Upgrade Parameters

Parameter	Description
Generate Password Automatically	Specifies whether APSolute Vision generates the password automatically–after verifying that the device has a valid support agreement. Default: Enabled **Caution:** The functionality of the **Generate Password Automatically** button requires connectivity to radware.com or the proxy server that is configured in the APSolute Vision settings (*APSolute Vision Settings* view *System* perspective, **General Settings > Connectivity > Proxy Server Parameters**).
Password (This parameter is available only when the **Generate Password Automatically** checkbox is cleared.)	The password received with the new software version. The password is case-sensitive.
Upload and Activate New Version Immediately (option button)	The software-version-package is uploaded and activated immediately. Default: Enabled
Upload Without Activating (option button)	The software-version-package is uploaded but not activated. Default: Disabled
Browse for File	The name of the file to upload. **Caution:** You must use the original filename.
Upload and Activate (This button is displayed only when the **Upload and Activate New Version Immediately** option button is selected.)	Radware DefensePro DDoS Mitigation uploads the software-version-package, activates the software with all the associated components, and reboots. The *Status* column in the table displays **Active** for this version.
Upload Without Activating (This button is displayed only when the **Install Without Activating** option button is selected.)	Radware DefensePro DDoS Mitigation uploads the software-version-package, but does not activate the new software. The *Status* column in the table displays **Idle** for this version.

Configuring the Global Parameters

This section contains the following topics:

- Viewing and Configuring Basic Global Parameters, page 81
- Upgrading Licenses for Radware DefensePro DDoS Mitigation Devices, page 82

Viewing and Configuring Basic Global Parameters

You can view and configure the following:

- Basic device-setup parameters
- The date and time settings on the device
- Device hardware and software versions

To view and configure basic global parameters

1. In the *Configuration* perspective, select **Setup > Global Parameters**.
2. Configure the parameters, if required, and then, click **Submit**.

Table 12: Global Parameters: General Parameters

Parameter	Description
Device Name	(Read-only) The device name configured on the device.
Device Description	(Read-only) The device description configured on the device.
Location	The device location, if required.
Contact Information	Contact information, if required.
System Uptime	(Read-only) The length of time since that the device has been up since last device reboot.
Base MAC Address	(Read-only) The MAC address of the first port on the device.

Table 13: Global Parameters: Date and Time Parameters

Parameter	Description
Device Date	The date setting on the device. Click in the field to modify the date.
Device Time	The time setting on the device. Click in the field to modify the time.

Table 14: Global Parameters: Version Information Parameters

Parameter	Description
Software Version	(Read-only) The version of the product software on the device.

Upgrading Licenses for Radware DefensePro DDoS Mitigation Devices

You can upgrade the capabilities of a Radware DefensePro DDoS Mitigation for Cisco Firepower device using the licensing procedure.

Upgrading a License on a Radware DefensePro DDoS Mitigation Instance

Radware DefensePro DDoS Mitigation requires a valid throughput license. The throughput license determines the maximum throughput of legitimate traffic that Radware DefensePro DDoS Mitigation inspects.

After an initial Radware DefensePro DDoS Mitigation deployment, there is a 60-day grace period. After the grace period, Radware DefensePro DDoS Mitigation passes traffic through the device, without inspection.

There is a *default* license, which supports up to 10 vCPUs.

Note: For information about purchasing an upgrade for a throughput license for Radware DefensePro DDoS Mitigation for Cisco Firepower, please contact your Cisco representative or refer to the Cisco documentation.

Caution: If you change the IP address that was used to generate a license, the license will not work after the subsequent reboot. Radware DefensePro DDoS Mitigation will issue an appropriate error message.

To upgrade a license after receiving a new license key

1. In the *Configuration* perspective, select **Setup > Global Parameters > LicenseUpgrade**.
2. In the **Throughput License Key** field, enter the new key, and then, click **Submit**.

Table 15: License Upgrade Parameters for Radware DefensePro DDoS Mitigation

Parameter	Description
Throughput License ID	(Read-only) The device throughput-license ID that was provided when requesting the new throughput license.
Throughput License Key	The key for the device throughput license.
Throughput License Method	(Read-only) The method used to generate the license. Values: • IP—The license generator used an IP address of the device to generate the license. • MAC—The license generator used the MAC address of the device to generate the license.
Throughput License IP Address	(Read-only) Values: • *The IP address that was used to generate the throughput license.* • None—The license generator used the MAC address of the device to generate the throughput license.

Configuring Date and Time Parameters

This section describes configuring Radware DefensePro DDoS Mitigation date and time parameters.

Radware DefensePro DDoS Mitigation for Cisco Firepower does *not* support Network Time Protocol (NTP) synchronization. Radware DefensePro DDoS Mitigation for Cisco Firepower synchronizes with the time and date of the host. You cannot change the time or date on Radware DefensePro DDoS Mitigation for Cisco Firepower. However you *can* set Daylight Saving time parameters. Additionally, in the CLI, you can set the timezone, with the command services ntp time-zone.

Configuring the Networking Setup

This section contains the following topics:

- Configuring the General Parameters of the Radware DefensePro DDoS MitigationNetworking Setup, page 83
- Configuring IP Interface Management in the Networking Setup, page 84
- Configuring DNS for the Radware DefensePro DDoS Mitigation Networking Setup, page 87

Configuring the General Parameters of the Radware DefensePro DDoS Mitigation Networking Setup

Use the *Networking* pane to configure the IP Fragmentation parameters.

IPv4 and IPv6 Support

Radware DefensePro DDoS Mitigation supports IPv6 and IPv4 protocols and provides a fully functional IPS and DoS prevention solution for IPv6/IPv4 packets. Management works only in IPv4.

Radware DefensePro DDoS Mitigation supports processing of IPv6 packets and ICMPv6 packets, including the following:

- Setting networks with IPv6 addresses
- Applying security policies
- Blocking attacks
- Security reporting

Maximum Transmission Unit

For this version of Radware DefensePro DDoS Mitigation, the MTU value is 1542 bytes.

IP Fragmentation

When the length of the IP packet is too long to be transmitted, the originator of the packet or one of the routers transmitting the packet must fragment the packet to multiple shorter packets.

Using IP fragmentation, Radware DefensePro DDoS Mitigation can classify the Layer 4 information of IP fragments. Radware DefensePro DDoS Mitigation identifies all the fragments belong to same datagram, then classifies and forwards them accordingly. Radware DefensePro DDoS Mitigation does not reassemble the original IP packet, but forwards the fragmented datagrams to their destination, even if the datagrams arrive at the device out of order.

Traffic Exclusion

Traffic Exclusion is when Radware DefensePro DDoS Mitigation passes through all traffic that matches no network policy configured on the device.

In Radware DefensePro DDoS Mitigation, the Traffic Exclusion behavior is always enabled. That is, the device always passes through all traffic that matches no Protection policy configured on the device.

Configuring the General Networking Parameters

The following procedure describes how to configure the general networking parameters.

To configure the general networking parameters

1. In the *Configuration* perspective, select **Setup > Networking**.
2. Configure the parameters, and then, click **Submit**.

Table 16: Networking: IP Fragmentation Parameters

Parameter	Description
Queuing Limit	The percentage of IP packets the device allocates for out-of- sequence fragmented IP datagrams. Values: 0–100 Default: 25
Aging Time	The time, in seconds, that the device keeps the fragmented datagrams in the queue. Values: 1–255 Default: 1

Configuring IP Interface Management in the Networking Setup

Use the *IP Management* tab to change the network prefix of the device's management port. You can also configure a label for the port.

To configure an IP interface

1. In the *Configuration* perspective, select **Setup > Networking > IP Management**.
2. Do one of the following:
   - To add an IP interface, click the  (Add) button.
   - To edit an IP interface, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 17: IP Interface Parameters

Parameter	Description
Network Type	(Read-only) The IP version of the network interface. Value: IPv4
IP Address	The IP address of the interface.

Table 17: IP Interface Parameters (cont.)

Parameter	Description
Prefix	The prefix length that defines the subnet attached to this IP interface. Values for IPv4: 1 –32
Port	The interface identifier. The only valid value is **MNG-1**. Value: MNG-1
Label	A name for the interface. Maximum characters: 19

Configuring IP Routing in Radware DefensePro DDoS Mitigation

This section describes IP routing in Radware DefensePro DDoS Mitigation.

Radware DefensePro DDoS Mitigation devices forward management IP packets to their destination using an IP routing table. This table stores information about the destinations and how they can be reached. By default, all networks directly attached to the device are registered in the IP routing table. Other entries can be statically configured.

To configure IP routing for management in Radware DefensePro DDoS Mitigation

1. In the *Configuration* perspective, select **Setup > Networking > IP Management >IP Routing**.
2. Do one of the following:
   - To add a static route, click the  (Add) button.
   - To edit a static route, double-click the row.
3. Configure the static-route parameters, and then, click **Submit**.
4. Configure the global advanced parameters.
5. Click **Submit**.

Notes

- When editing a static route, you can modify only the **Metric** field.
- The **Type** field is displayed only in the *Static Routes* table. It cannot be configured.

Table 18: IP Routing: General (Static Route) Parameters

Parameter	Description
Destination Network	The destination network to which the route is defined.
Netmask	The network mask of the destination subnet.
Next Hop	The IP address of the next hop toward the Destination subnet. (The next hop always resides on the subnet local to the device.)
Via Interface	(Read-only) The value **3** (read-only), which is the value of the management interface.

Table 18: IP Routing: General (Static Route) Parameters (cont.)

Parameter	Description
Type	(Read-only) This field is displayed in the Static Routes table. Values: • Local–The subnet is directly reachable from the device. • Remote–The subnet is not directly reachable from the device.
Metric	The metric value defined or calculated for this route.

Table 19: IP Routing: Advanced Parameters

Parameter	Description
Enable Sending Trap on ICMP Error	Specifies whether Radware DefensePro DDoS Mitigation sends a trap if there is an ICMP error message. Default: Enabled **Note:** The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite and is used by networked computers' operating systems to send error messages–indicating, for example, that a requested service is not available, or that a host or router could not be reached.

Configuring the ARP Table

When Proxy ARP is enabled, a network host answers ARP queries for the network address that is not configured on the receiving interface. Proxying ARP requests on behalf of another host effectively directs all LAN traffic destined for that host to the proxying host. The captured traffic is then routed to the destination host via another interface.

You can configure and manage the static ARP entries on the local router.

To configure the ARP table

1. In the *Configuration* perspective, select **Setup > Networking > IP Management >ARP Table**.
2. Do one of the following:
   - To add a new entry, click the (Add) button.
   - To edit an entry, double-click the row.
3. Configure the ARP parameters and click **Submit**.
4. Modify advanced parameters, if required; and then, click **Submit**.

Table 20: ARP: Entry Parameters

Parameter	Description
Port	The interface number where the station resides.
IP Address	The station's IP address.
MAC Address	The station's MAC address.

Table 20: ARP: Entry Parameters (cont.)

Parameter	Description
Type	The entry type. Values: • Other–Not Dynamic or Static. • Invalid–Invalidates the ARP entry and effectively deletes it. • Dynamic–The entry is learned from ARP protocol. If the entry is not active for a predetermined time, the node is deleted from the table. • Static–The entry was configured by the network management station and is permanent.

Table 21: ARP: Advanced Parameters

Parameter	Description
Inactive ARP Timeout	The time, in seconds, that inactive ARP cache entries can remain in the ARP table before the device deletes them. If an ARP cache entry is not refreshed within a specified period, it is assumed that there is a problem with that address. Values: 10-86,400 Default: 3,600

Configuring DNS for the Radware DefensePro DDoS Mitigation Networking Setup

You can configure Radware DefensePro DDoS Mitigation to operate as a Domain Name Service (DNS) client. When the DNS client is disabled, IP addresses cannot be resolved. When the DNS client is enabled, you must configure servers to which Radware DefensePro DDoS Mitigation will send out queries for host name resolving.

You can set the DNS parameters and define the primary and the alternate DNS servers for dynamic DNS. In addition, you can set static DNS parameters.

To configure DNS settings

1. In the *Configuration* perspective, select **Setup > Networking > DNS**.
2. Configure basic DNS client parameters, and click **Submit**.
3. To add or modify static DNS entries, do one of the following:
   - To add an entry, click the (Add) button.
   - To modify an entry, double-click the entry in the table.
4. Configure the parameters, and click **Submit**.

Table 22: DNS Client Parameters

Parameter	Description
Enable DNS Client	Specifies whether the Radware DefensePro DDoS Mitigation device operates as a DNS client to resolve IP addresses. Values: Enable, Disable Default: Disable
Primary DNS Server	The IP address of the primary DNS server that Radware DefensePro DDoS Mitigation uses for domain-name resolution.
Alternative DNS Server	The IP address of the alternative DNS server that Radware DefensePro DDoS Mitigation uses for domain-name resolution.
Static DNS Table The static DNS hosts. Click the (Add) button to add a new static DNS. The configuration of each static DNS comprises the following parameters: • Host Name–The domain name for the specified IP address • IP Address–The IP address for the specified domain name	

Configuring the Device-Security Setup

This section contains the following topics:

- Configuring Access Protocols for the Radware DefensePro DDoS MitigationDevice-Security Setup, page 88
- Configuring Authentication Protocols for Device Management, page 90
- Configuring SNMP in the Radware DefensePro DDoS Mitigation Device-Security Setup, page 94
- Configuring Device Users in the Radware DefensePro DDoS Mitigation Device-SecuritySetup, page 104
- Configuring Advanced Parameters in the Radware DefensePro DDoS MitigationDevice-Security Setup, page 106

Configuring Access Protocols for the Radware DefensePro DDoS Mitigation Device-Security Setup

Radware DefensePro DDoS Mitigation supports the following access protocols:

- **HTTPS**–For APSolute Vision communication with Radware DefensePro DDoS Mitigation.
- **Telnet**–For the command-line interface.
- **SSH**–For the command-line interface.
- **Web services**–For the Radware DefensePro DDoS Mitigation SOAP interface.

To configure access protocols for APSolute Vision and CLI

1. In the *Configuration* perspective, select **Setup > Device Security > Access Protocols**.
2. Configure the parameters, and then, click **Submit**.

Table 23: Access Protocols: Secured Web Access Parameters

Parameter	Description
Enable Secured Web Access	Specifies whether to enable HTTPS access to Radware DefensePro DDoS Mitigation. Default: Enabled **Caution:** The **Enable Secured Web Access** checkbox must be selected to enable full communication between APSolute Vision and Radware DefensePro DDoS Mitigation.
L4 Port	The port for HTTPS communications with the management interface of the device. Default: 443
Certificate	The SSL certificate used by the HTTPS server for encryption. **Caution:** For security reasons, Radware advises replacing the out- of-the-box certificate issued by Radware with a certificate issued by a Certificate Authority (CA) of your choice. **Caution:** Changing the certificate requires a reboot to take effect.

Table 24: Access Protocols: Telnet Parameters

Parameter	Description
Enable Telnet	Specifies whether to enable Telnet access to Radware DefensePro DDoS Mitigation. Default: Disabled
L4 Port	The TCP port used by the Telnet. Default: 23
Session Timeout	The time, in minutes, that Radware DefensePro DDoS Mitigation maintains a connection during periods of inactivity. If the session is still inactive when the predefined period ends, the session terminates. Values: 1-120 Default: 5 **Note:** To avoid affecting device performance, the timeout is checked every 10 seconds. Therefore, the actual timeout can be up to 10 seconds longer than the configured time.
Authentication Timeout	The timeout, in seconds, required to complete the authentication process. Values: 10-60 Default: 30

Table 25: Access Protocols: SSH Parameters

Parameter	Description
Enable SSH	Specifies whether to enable SSH access to Radware DefensePro DDoS Mitigation. Default: Disabled **Note:** When SSH is enabled, Radware DefensePro DDoS Mitigation uses various SSH algorithms. The list of SSH algorithms is configurable in the Radware DefensePro DDoS Mitigation CLI.
L4 Port	The source port for the SSH server connection. Default: 22
Session Timeout	The time, in minutes, that Radware DefensePro DDoS Mitigation maintains a connection during periods of inactivity. If the session is still inactive when the predefined period ends, the session terminates. Values: 1–120 Default: 5 **Note:** To avoid affecting device performance, the timeout is checked every 10 seconds. Therefore, the actual timeout can be up to 10 seconds longer than the configured time.
Authentication Timeout	The timeout, in seconds, required to complete the authentication process. Values: 10–60 Default: 10

Table 26: Access Protocols: Web Services Parameter

Parameter	Description
Enable Web Services	Specifies whether to enable access to Web services. Default: Enabled

Configuring Authentication Protocols for Device Management

This section comprises the following:

- Configuring RADIUS Authentication for Device Management, page 90
- Configuring TACACS+ Authentication for Device Management, page 92

Configuring RADIUS Authentication for Device Management

Radware DefensePro DDoS Mitigation provides additional security by authenticating the users who access a device for management purposes. With RADIUS authentication, you can use RADIUS servers to determine whether a user is allowed to access device management using APSolute Vision, the CLI, Telnet, SSH and the SOAP interface.

Notes

- The default **Authentication Mode** is **Local User Table** –*without* RADIUS. To modify the configuration, in the *Configuration* perspective, select **Device Security > Users Table**. Then, in the *Advanced Parameters* tab, from the **Authentication Mode** drop-down list, select the option you require, and click **Submit**.

- The Radware DefensePro DDoS Mitigation devices must have access to the RADIUS server.
- Radware DefensePro DDoS Mitigation uses Password Authentication Protocol (PAP) when connecting to the RADIUS server.

With RADIUS authentication for device management, Radware DefensePro DDoS Mitigation searches Service Type attribute (AVP 6) (which is built into all RADIUS servers), in Access Accept response. The Read Write (administrator) user privilege is built into all RADIUS servers (Service Type value 6). The Read Only user privilege is given to the Service Type value 7 and must be defined in the RADIUS dictionary. If Radware DefensePro DDoS Mitigation does not find the attribute,Radware DefensePro DDoS Mitigation sets the default value to Read Only.

To configure RADIUS authentication for device management

1. In the *Configuration* perspective, select **Setup > Device Security >Authentication Protocols > RADIUS Authentication**.
2. Configure RADIUS authentication parameters for the managed Radware DefenseProDDoS Mitigation device, and then, click **Submit**.

Table 27: RADIUS Authentication: General Parameters

Parameter	Description
Timeout	The length of time Radware DefensePro DDoS Mitigation waits for a reply from the RADIUS server before a retry, or, if the **Retries** value is exceeded, before Radware DefensePro DDoS Mitigation acknowledges that the server is offline. Default: 1
Retries	The number of connection retries to the RADIUS server, after the RADIUS server does not respond to the first connection attempt. After the specified number of retries, if all connection attempts have failed (**Timeout**), the backup RADIUS server is used. Default: 2
Client Lifetime	The duration, in seconds, of client authentication. If the client logs in again during the lifetime, Radware DefensePro DDoS Mitigation will not re-authenticate the client with the RADIUS server. If the client logs in again after the lifetime expires, Radware DefensePro DDoS Mitigation re-authenticates the client. Default: 30

Table 28: RADIUS Authentication: Main Parameters

Parameter	Description
L4 Port	The access port number of the primary RADIUS server. Values: 1645, 1812 Default: 1645
Secret	The authentication password for the primary RADIUS server. Maximum characters: 64 **Note:** When Radware DefensePro DDoS Mitigation stores the **Secret**, it is encrypted. Therefore, the length of the **Secret** in the configuration file is longer than the number of characters that you configured.

Table 28: RADIUS Authentication: Main Parameters (cont.)

Parameter	Description
Verify Secret	The authentication password for the primary RADIUS server.
Server IP Address Type	Values: IPv4, IPv6
Server IP Address	The IP address of the primary RADIUS server.

Table 29: RADIUS Authentication: Backup Parameters

Parameter	Description
L4 Port	The access port number of the backup RADIUS server. Values: 1645, 1812 Default: 1645
Secret	The authentication password for the backup RADIUS server. Maximum characters: 64 **Note:** When Radware DefensePro DDoS Mitigation stores the **Secret**, it is encrypted. Therefore, the length of the **Secret** in the configuration file is longer than the number of characters that you configured.
Verify Secret	The authentication password for the backup RADIUS server.
Server IP Address Type	Values: IPv4, IPv6
Server IP Address	The IP address of the backup RADIUS server.

Configuring TACACS+ Authentication for Device Management

Radware DefensePro DDoS Mitigation provides additional security by authenticating the users who access a device for management purposes. With TACACS+ authentication, you can use TACACS+ servers to determine whether a user is allowed to access device management using APSolute Vision, the CLI, Telnet, SSH, and the SOAP interface.

Notes

- The default **Authentication Mode** is **Local User Table** –*without* TACACS+. To modify the configuration, in the *Configuration* perspective, select **Device Security > Users Table.** Then, in the *Advanced Parameters* tab, from the **Authentication Mode** drop-down list, select the option you require, and click **Submit**.
- The Radware DefensePro DDoS Mitigation devices must have access to the TACACS+ server.
- Radware DefensePro DDoS Mitigation uses Password Authentication Protocol (PAP) when connecting to the TACACS+ server.

With TACACS+ authentication for device management, Radware DefensePro DDoS Mitigation searches for the privilege level (which is built into all TACACS+ servers), in the Start message. The Read Write user privilege is built into all TACACS+ servers (Privilege level 15). The Read Only user privilege is given for privilege levels 0 through 14.

To configure TACACS+ authentication for device management

1. In the *Configuration* perspective, select **Setup > Device Security >Authentication Protocols > TACACS+ Authentication.**
2. Configure the parameters, and then, click **Submit**.

Table 30: TACACS+ Authentication: General Parameters

Parameter	Description
Timeout	The time, in seconds, that Radware DefensePro DDoS Mitigation waits for a reply from the TACACS+ server before a retry, or, if the **Retries** value is exceeded, before Radware DefensePro DDoS Mitigation acknowledges that the server is offline. Values: 1–10 Default: 1
Retries	The number of connection retries to the TACACS+ server, after the TACACS+ server does not respond to the first connection attempt. After the specified number of retries, if all connection attempts have failed (**Timeout**), the backup TACACS+ server is used. Values: 1, 2, 3 Default: 2
Client Lifetime	The duration, in seconds, of client authentication. If the client logs in again during the lifetime, Radware DefensePro DDoS Mitigation will not re-authenticate the client with the TACACS+ server. If the client logs in again after the lifetime expires, Radware DefensePro DDoS Mitigation re-authenticates the client. Default: 30

Table 31: TACACS+ Authentication: Main Parameters

Parameter	Description
Server IP Address	The IP address of the primary TACACS+ server.
L4 Port	The access port number of the primary TACACS+ server. Values: 1–65,000 Default: 49
Secret	The authentication password for the primary TACACS+ server. Maximum characters: 64 **Note:** When Radware DefensePro DDoS Mitigation stores the **Secret**, it is encrypted. Therefore, the length of the **Secret** in the configuration file is longer than the number of characters that you configured.
Verify Secret	The authentication password for the primary TACACS+ server.

Table 32: TACACS+ Authentication: Backup Parameters

Parameter	Description
Server IP Address	The IP address of the backup TACACS+ server.
L4 Port	The access port number of the backup TACACS+ server. Values: 1-65,000 Default: 49
Secret	The authentication password for the backup TACACS+ server. Maximum characters: 64 **Note:** When Radware DefensePro DDoS Mitigation stores the **Secret**, it is encrypted. Therefore, the length of the **Secret** in the configuration file is longer than the number of characters that you configured.
Verify Secret	The authentication password for the backup TACACS+ server.

Configuring SNMP in the Radware DefensePro DDoS Mitigation Device- Security Setup

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between APSolute Vision and network devices.

Radware DefensePro DDoS Mitigation devices can work with all versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3.

The default user is configured in SNMPv1.

Caution: APSolute Vision does *not* support SNMPv2c traps. SNMPv2c traps that arrive at the APSolute Vision are discarded.

Note: When you add a Radware DefensePro DDoS Mitigation device to APSolute Vision using SNMPv3, the username and authentication details must match one of the users configured on the device.

The following topics describe the procedures to configure SNMP on a selected device:

- Configuring SNMP Supported Versions, page 95
- Configuring Radware DefensePro DDoS Mitigation SNMP Users, page 95
- Configuring SNMP Community Settings, page 97
- Configuring the SNMP Group Table, page 98
- Configuring SNMP Access Settings, page 99
- Configuring SNMP Notify Settings, page 100
- Configuring SNMP View Settings, page 101
- Configuring the SNMP Target Parameters Table, page 101
- Configuring SNMP Target Addresses, page 103

Configuring SNMP Supported Versions

To configure SNMP supported versions

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP > SNMP Versions**.
2. Configure the parameters, and then, click **Submit**.

Table 33: SNMP Supported Version Parameters

Parameter	Description
Supported SNMP Versions	The currently supported SNMP versions.
Supported SNMP Versions after Reset	The SNMP versions supported by the SNMP agent after resetting the device. Select the SNMP version to support. Clear the versions that are not supported.

Configuring Radware DefensePro DDoS Mitigation SNMP Users

With SNMPv3 user-based management, each user can have different permissions based on the username and authentication method. You define the users who can connect to the device, and store the access parameters for each SNMP user.

To configure an SNMPv3 Radware DefensePro DDoS Mitigation user, the Radware DefensePro DDoS Mitigation device must be configured to support SNMPv3 (*Configuration* perspective, select **Setup > Device Security > SNMP > SNMP Versions > V3**).

Configuring an SNMPv3 Radware DefensePro DDoS Mitigation user for APSolute Vision involves the following:

1. Using the default Radware DefensePro DDoS Mitigation user and connected to APSoluteVision over SNMPv3 configured with Authentication and Privacy.
2. Adding the new user to the SNMP *Group* table.

Note: In the SNMP configuration, a username is also known as a *security name*.

To configure an SNMPv3 Radware DefensePro DDoS Mitigation user

1. In the APSolute Vision device pane *Sites and Devices* tree, select the Radware DefensePro DDoS Mitigation device.
2. Do the following:
   a. Click the  (Edit) button.
   b. Verify the following:
      - **SNMP Version** is **SNMPv3**.
      - **User Name** is **radware**.
      - The **Use Authentication** checkbox is selected and the associated parameters are configured (**Authentication Protocol** and **Authentication Password**).
      - The **Use Privacy** checkbox is selected and the associated parameters are configured (**Privacy Protocol** and **Privacy Password**).
   c. If any of the verification criteria in step b is *false*, modify the parameters accordingly, and then, click **Submit**.

3. In the *Configuration* perspective, select **Setup > Device Security > SNMP > SNMPUser Table**.
4. Do one of the following:
   - To add a user, click (Add).
   - To edit an entry, double-click the row.
5. Configure the SNMP user parameters (see Table 34 - SNMP User Parameters, page 96), and then, click **Submit**.
6. In the *Configuration* perspective, select **Setup > Device Security > SNMP > GroupTable**.
7. Configure the user in an SNMP Group with the following values, and then, click **Submit**.
   - **Security Model**–Select **User Based**, which represents SNMPv3.
   - **Security Name**–Select the username that you created in step 5.
   - **Group Name**–Select **initial**.

   Note: For general information on the SNMP *Group* table, see Configuring the SNMP Group Table, page 98.
8. In the *Configuration* perspective, select **Setup > Device Security > SNMP >Access**.
9. Do the following:
   a. Verify the following that there is a row in the table with the following values:
      - **Group Name** is **initial**.
      - **Security Model** is **User Based**.
      - **Security Level** is **Authentication and Privacy**.
      - **Read View Name** is **iso**.
      - **Write View Name** is **iso**.

   b. If any of the verification criteria in step a is *false*, and an entry accordingly, and then, click **Submit**.

   Note: For general information on the Access configuration, see Configuring SNMP Access Settings, page 99.

Table 34: SNMP User Parameters

Parameter	Description
User Name	The username, also known as a *security name*. Maximum characters: 32
Authentication Protocol	The protocol used during authentication process. The option that you select must match the configuration in the Device Properties dialog box. For example, if **Authentication Protocol** is **MD5** in the device properties, the option here must be **MD5**–and, if **Authentication Protocol** is **SHA** in the device properties, the option here must be **SHA**. Values: • MD5 • SHA • None Default: None

Table 34: SNMP User Parameters (cont.)

Parameter	Description
Authentication Password	The authentication password.
Privacy Protocol	The algorithm used for encryption. Values: • DES–The device uses Data Encryption Standard. • AES–The device uses Advanced Encryption Standard. • None Default: None
Privacy Password	The user privacy password.

Configuring SNMP Community Settings

The SNMP *Community* table is used only for SNMP versions 1 and 2 to associate community strings to users. When a user is connected to a device with SNMPv1 or SNMPv2, the device checks the community string sent in the SNMP packet. Based on a specific community string, the device maps the community string to a predefined user, which belongs to a group with certain access rights.
Therefore, when working with SNMPv1 or SNMPv2, users, groups, and access must be defined.

Use the SNMP *Community* table to associate community strings with usernames and vice versa, and to restrict the range of addresses from which SNMP requests are accepted and to which traps can be sent.

Note: You cannot change the community string associated with the username that you are currently using.

To configure SNMP community settings

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP > Community**.
2. Do one of the following:
   - To add an SNMP community entry, click (Add).
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 35: SNMP Community Parameters

Parameter	Description
Index	A descriptive name for this entry. This name cannot be modified after creation. Default: public
Community Name	The community string. Default: public
Security Name	The security name identifies the SNMP community used when the notification is generated. Default: public

Table 35: SNMP Community Parameters (cont.)

Parameter	Description
Transport Tag	Specifies a set of target addresses from which the SNMP accepts SNMP requests and to which traps can be sent. The target addresses identified by this tag are defined in the SNMP *Target Address* table. At least one entry in the SNMP *Target Address* table must include the specified transport tag. If no tag is specified, addresses are not checked when an SNMP request is received or when a trap is sent.

Configuring the SNMP Group Table

SNMPv3 permissions are defined for groups of users. If, based on the connection method, there is a need to grant different permissions to the same user, you can associate a user to more than one group. You can create multiple entries with the same group name for different users and security models.

Note: Access rights are defined for groups of users in the SNMP *Access* table (see Configuring SNMP Access Settings, page 99).

To configure SNMP group settings

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP > GroupTable**.
2. Do one of the following:
   - To add a group entry, click (Add).
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 36: SNMP Group Parameters

Parameter	Description
Group Name	The name of the SNMP group.
Security Model	The SNMP version that represents the required **security model**. Security models are predefined sets of permissions that can be used by the groups. These sets are defined according to the SNMP versions. By selecting the SNMP version for this parameter, you determine the permissions set to be used. Values: • SNMPv1 • SNMPv2c • User Based (SNMPv3) Default: SNMPv1
Security Name	If the User Based security model is used, the security name identifies the user that is used when the notification is generated. For other security models, the security name identifies the SNMP community used when the notification is generated.

Configuring SNMP Access Settings

The *SNMP Access* table binds groups and security models with SNMP views, which define subsets of MIB objects. You can define which MIB objects can be accessed for each group and security model. MIB objects can be accessed for a read, write, or notify action based on the **Read View Name**, **Write View Name**, and **Notify View Name** parameters.

Note: Views are defined in the SNMP *View* table (see Configuring SNMP View Settings, page 101).

To configure SNMP access settings

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP >Access**.
2. Do one of the following:
   - To add an access entry, click (Add).
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 37: SNMP Access Parameters

Parameter	Description
Group Name	The name of the group.
Security Model	Security models are predefined sets of permissions that can be used by the groups. These sets are defined according to the SNMP versions. Select the SNMP version that represents the required Security Model to determine the permissions set to be used. Values: • SNMPv1 • SNMPv2c • User Based–That is, SNMPv3 Default: SNMPv1
Security Level	The security level required for access. Values: • No Authentication–No authentication or privacy are required. • Authentication and No Privacy–Authentication is required, but privacy is not required. • Authentication and Privacy–Both authentication and privacy are required. Default: No Authentication
Read View Name	The name of the View that specifies which objects in the MIB tree are readable by this group.
Write View Name	The name of the View that specifies which objects in the MIB tree are writable by this group.

Table 37: SNMP Access Parameters (cont.)

Parameter	Description
Notify View Name	The name of the View that specifies which objects in the MIB tree can be accessed in notifications (traps) by this group. **Caution:** In typical environments and scenarios, the value of this field should *not* be **None** or empty. Radware DefensePro DDoS Mitigation does not send notifications (traps) to APSolute Vision in the following setup: • The value of **Notify View Name** field is **None** or empty. • The (SNMP) **User Name** in the Device Properties *SNMP* tab (see To add a new device or edit device-connection information, page 63) is associated with an SNMP user using this *Access* group (according to **Group Name** and **Security Model** and **Security Level**).

Configuring SNMP Notify Settings

You can select management targets that receive notifications and the type of notification to be sent to each selected management target. The **Tag** parameter identifies a set of target addresses. An entry in the *Target Address* table that contains a tag specified in the *Notify* table receives notifications.

To configure SNMP notification settings

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP >Notify**.
2. Do one of the following:
   - To add an SNMP notify entry, click  (Add).
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 38: SNMP Notify Parameters

Parameter	Description
Name	A descriptive name for this entry, for example, the type of notification.
Tag	A string that defines the target addresses that are sent this notification. All the target addresses that have this tag in their tag list are sent this notification.

Configuring SNMP View Settings

You can define subsets of the MIB tree for use in the SNMP *Access* table. Different entries may have the same name. The union of all entries with the same name defines the subset of the MIB tree and can be referenced in the *Access* table through its name.

To configure SNMP view settings

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP >View**.
2. Do one of the following:
   - To add an SNMP view entry, click  (Add).
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 39: SNMP View Parameters

Parameter	Description
View Name	The name of this entry.
Sub-Tree	The Object ID of a subtree of the MIB.
Type	Specifies whether the object defined in the entry is included or excluded in the MIB view. Values: Included, Excluded Default: Included

Configuring the SNMP Target Parameters Table

The *Target Parameters Table* defines message-processing and security parameters that are used in sending notifications to a particular management target. Entries in the *Target Parameters Table* are referenced in the *Target Address* table.

To configure SNMP target parameters

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP >Target Parameters Table**.
2. Do one of the following:
   - To add a target parameters entry, click  (Add).
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 40: SNMP Target Parameters

Parameter	Description
Name	The name of the target parameters entry. Maximum characters: 32
Message Processing Model	The SNMP version to use when generating SNMP notifications. Values: SNMPv1, SNMPv2c, SNMPv3 Default: SNMPv1 **Caution:** APSolute Vision does not support SNMPv2c traps. SNMPv2c traps that arrive at the APSolute Vision are discarded.
Security Model	The SNMP version that represents the required Security Model. Security models are predefined sets of permissions that can be used by the groups. These sets are defined according to the SNMP versions. By selecting the SNMP version for this parameter, you determine the permissions set to be used. Values: • SNMPv1 • SNMPv2c • User Based–That is, SNMPv3 Default: SNMPv1 **Caution:** APSolute Vision does not support SNMPv2c traps. SNMPv2c traps that arrive at the APSolute Vision are discarded.
Security Name	If the **User Based** security model is used, the **Security Name** identifies the user that is used when a notification is generated. For other security models, the **Security Name** identifies the SNMP community used when a notification is generated.
Security Level	Specifies whether the trap is authenticated and encrypted before it is sent. Values: • No Authentication–No authentication or privacy are required. • Authentication and No Privacy–Authentication is required, but privacy is not required. • Authentication and Privacy–Both authentication and privacy are required. Default: No Authentication

Configuring SNMP Target Addresses

In SNMPv3, the *Target Address* table contains transport addresses to be used in the generation of traps. If the tag list of an entry contains a tag from the SNMP *Notify* table, this target is selected for reception of notifications. For SNMP versions 1 and 2, this table is used to restrict the range of addresses from which SNMP requests are accepted and to which SNMP traps may be sent. If the **Transport Tag** of an entry in the *Community* table is not empty, it must be included in one or more entries in the *Target Address* table.

To configure SNMP target addresses

1. In the *Configuration* perspective, select **Setup > Device Security > SNMP >Target Address**.
2. Do one of the following:
   - To add a target address, click  (Add).
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 41: SNMP Target Address Parameters

Parameter	Description
Name	The name of the target address entry.
IP Address and L4 Port [IP-port number]	The IP address of the management station (APSolute Vision server) and TCP port to be used as the target of SNMP traps. The format of the values is <IP address >-<TCP port>, where <TCP port>must be 162. For example, if the value for **IP Address and L4 Port** is 1.2.3.4-162, 1.2.3.4 is the IP address of the APSolute Vision server and 162 is the port number for SNMP traps. **Note:** APSolute Vision listens for traps only on port 162.
Mask	A subnet mask of the management station.
Tag List	Specifies sets of target addresses. Tags are separated by spaces. The tags contained in the list may be either tags from the *Notify* table or Transport tags from the *Community* table. Each tag can appear in more than one tag list. When a significant event occurs on the network device, the tag list identifies the targets to which a notification is sent. Default: v3Traps
Target Parameters Name	The set of target parameters to be used when sending SNMP traps. Target parameters are defined in the *Target Parameters Table*.
Report the Following Event Types	
Security Events	Specifies whether Radware DefensePro DDoS Mitigation sends security-event traps to the target address. *Security events* include all events related to attack detection and mitigation: start, ongoing, occurred, sampled, and terminated. Default: Enabled

Table 41: SNMP Target Address Parameters (cont.)

Parameter	Description
Device-Health Event	Specifies whether Radware DefensePro DDoS Mitigation sends device-health-event traps to the target address. *Device-health events* include all events related to device health, for example, temperature, fan failure, CPU, tables, resources, and so on. Default: Enabled
Configuration-Auditing Events	Specifies whether Radware DefensePro DDoS Mitigation sends configuration-auditing-event traps to the target address. *Configuration-auditing events* include all events related to user operations, for example, login attempts and configuration changes. Default: Enabled

Configuring Device Users in the Radware DefensePro DDoS Mitigation Device-Security Setup

For each Radware DefensePro DDoS Mitigation device, you can configure a list of users who are authorized to access that device through any enabled access method (Web, Telnet, SSH, HTTPS). When configuration tracing is enabled, users can receive e-mail notifications of changes made to the device.

To configure a device user for a selected device

1. In the *Configuration* perspective, select **Setup > Device Security > Users Table**.
2. Do one of the following:
   - To add a user, the  (Add) button.
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 42: Users Table: General Parameters

Parameter	Description
User Name	The name of the user.
Password	The password of the user.
Confirm Password	The password of the user.
Email Address	The e-mail address of the user to which notifications will be sent.
Minimal Severity for Sending Traps	The minimum severity level of traps sent to this user. Values: • None—The user receives no traps. • Info—The user receives traps with severity Info or higher. • Warning—The user receives Warning, Error, and Fatal traps. • Error—The user receives Error and Fatal traps. • Fatal—The user receives Fatal traps only. Default: None

Table 42: Users Table: General Parameters (cont.)

Parameter	Description
Enable Configuration Tracing	When selected, the specified user receives notifications of configuration changes made to the device. Every time the value of a configurable variable changes, information about all the variables in the same MIB entry is reported to the specified users. Radware DefensePro DDoS Mitigation gathers reports and sends them in a single notification message when the buffer is full or when the timeout of 60 seconds expires. The notification message contains the following details: • Name of the MIB variable that was changed. • New value of the variable. • Time of configuration change. • Configuration tool that was used (APSolute Vision, Telnet, SSH). • User name, when applicable.
Access Level	The user's level of access through APSolute Vision and CLI. Default: Read-Write

To configure the advanced parameter for the device users

1. In the *Configuration* perspective, select **Setup > Device Security > Users Table**.
2. In the *Advanced Parameters* tab, configure the parameter, and then, click **Submit**.

Table 43: Users Table: Advanced Parameters

Parameter	Description
Authentication Mode	The method for authenticating a user's access to the device. Values: • Local User Table–Radware DefensePro DDoS Mitigation uses the User Table to authenticate access. • RADIUS and Local User Table–Radware DefensePro DDoS Mitigation uses the RADIUS servers to authenticate access. If the request to the RADIUS server times out, Radware DefensePro DDoS Mitigation uses the User Table to authenticate access. • TACACS+ and Local User Table –Radware DefensePro DDoS Mitigation uses the TACACS+ servers to authenticate access. If the request to the TACACS+ server times out, Radware DefensePro DDoS Mitigation uses the User Table to authenticate access. Default: Local User Table

Configuring Advanced Parameters in the Radware DefensePro DDoS Mitigation Device-Security Setup

Access to devices can be limited to specified physical interfaces. Interfaces connected to insecure network segments can be configured to discard some or all management traffic directed at the device itself. Administrators can allow certain types of management traffic to a device (for example, SSH), while denying others such as SNMP. If an intruder attempts to access the device through a disabled port, the device denies access, and generates syslog and CLI traps as notification.

To configure access permissions for a selected device

1. In the *Configuration* perspective, select **Setup > Device Security > Advanced**.
2. To edit permissions for a port, double-click the relevant row.
3. Select or clear the checkboxes to allow or deny access, and then, click **Submit**.

Table 44: Port Permission Parameters

Parameter	Description
Port	(Read-only) The name of the physical port.
SNMP Access	When selected, allows access to the port using SNMP.
Telnet Access	When selected, allows access to the port using Telnet.
SSH Access	When selected, allows access to the port using SSH.

Configuring Port Pinging

You can define which physical interfaces can be pinged. When a ping is sent to an interface for which ping is not allowed, the packet is discarded. By default, all the interfaces of the device allowpings.

To define the ports to be pinged

1. In the *Configuration* perspective, select **Setup > Device Security > Advanced > PingPorts**.
2. To edit port ping settings, double-click the relevant row.
3. Select or clear the checkbox to allow or not allow pinging, then click **Submit**.

Configuring the SSL-Settings Setup

This section contains information related to the management of the SSL Settings, which are used for the following:

- *HTTPS mitigation methods* in HTTPS Flood Protection
- The *SSL Mitigation* feature in SYN Flood Protection

This section contains the following main topics:

- Configuring the SSL-Decryption-and-Encryption Option, page 107
- Managing SSL/TLS Certificates, page 109
- Managing Protected SSL Objects, page 117

Configuring the SSL-Decryption-and-Encryption Option

SSL-decryption-and-encryption requires a DefenseSSL license.

Radware DefensePro DDoS Mitigation uses *SSL-decryption-and-encryption* for the following:

- **HTTPS mitigation methods in HTTPS Flood Protection** –In HTTPS Flood Protection, with SSL-decryption-and-encryption *enabled*, Radware DefensePro DDoS Mitigation can authenticate HTTPS traffic that is suspected as malicious and mitigate HTTPS-flood attacks when needed. That is, when SSL-decryption-and-encryption is *enabled* and HTTPS Flood Protection is triggered, Radware DefensePro DDoS Mitigation can challenge SSL/TLS connections by decrypting and re-encrypting the SSL/TLS packets during application-level challenges; and Radware DefensePro DDoS Mitigation can allow traffic from validated clients to pass through the Radware DefensePro DDoS Mitigation device to the protected server.

  Note: With SSL-decryption-and-encryption *disabled*, mitigation of HTTPS-flood attacks with HTTPS Flood Protection is limited to *rate-limiting* traffic from sources suspected as malicious.

- **The SSL Mitigation feature in SYN Flood Protection**–In SYN Flood Protection, Radware DefensePro DDoS Mitigation can mitigate SSL/TLS SYN-flood attacks using the *SSL Mitigation* feature. When SYN Flood Protection is triggered on a configured SSL/TLS port (usually port 443) and the **Use SSL Mitigation** option is enabled in the SYN Flood Protection profile, Radware DefensePro DDoS Mitigation challenges new SSL/TLS connections–first at the network level. Then, to decrypt and re-encrypt the SSL/TLS packets during the application-level challenge, Radware DefensePro DDoS Mitigation uses the specified *SSL-decryption-and-encryption* option. Finally, Radware DefensePro DDoS Mitigation allows traffic from validated clients to pass through the Radware DefensePro DDoS Mitigation device to the protected server.

This section contains the procedure to specify the *SSL-decryption-and-encryption* option, and the following topics:

- Radware DefensePro DDoS Mitigation Platforms and SSL/TLSDecryption-and-Encryption Components, page 108
- SYN Flood Protection with SSL Mitigation Using the On-Device Component forSSL/TLS Decryption and Encryption, page 108

Notes

- For information on the configuration of HTTPS Flood Protection profiles, see Configuring HTTPS Flood Protection Profiles, page 201.
- For information on the configuration of a SYN Flood Protection profile and the **UseSSL Mitigation** option, see Managing SYN Flood Protection Profile Parameters, page235.

Caution: Changing the configuration of the SSL-decryption-and-encryption option requires resetting the device to take effect.

To specify the SSL-decryption-and-encryption option

1. In the *Configuration* perspective, select **Setup > SSL Settings**.
2. Select one of the following:
   — **Disabled**–The Radware DefensePro DDoS Mitigation device does not useSSL-decryption- and-

encryption.

- **Enabled, Using the On-Device Component** (available only on devices with a DefenseSSL license)– The Radware DefensePro DDoS Mitigation device decrypts and encrypts SSL/TLS traffic using the on-device SSL/TLS component.

3. Click **Submit**.

Radware DefensePro DDoS Mitigation Platforms and SSL/TLS Decryption-and-Encryption Components

Radware DefensePro DDoS Mitigation can decrypt and re-encrypt the SSL/TLS packets using the on- device SSL/TLS component, which is a software module.

Notes

- In SYN Flood Protection, when you must configure Protected SSL Objects only when you use the on-device SSL/TLS component. In HTTPS Flood Protection, you must always configure Protected SSL Objects. For more information on configuring Protected SSL Objects, see Managing Protected SSL Objects, page 117.
- For more information about the on-device component for SSL/TLS decryption and encryptionin SYN Flood Protection with the SSL Mitigation feature, see SYN Flood Protection with SSL Mitigation Using the On-Device Component for SSL/TLS Decryption and Encryption.

SYN Flood Protection with SSL Mitigation Using the On-Device Component for SSL/TLS Decryption and Encryption

In SYN Flood Protection, using the on-device component for SSL/TLS decryption and encryption, the Radware DefensePro DDoS Mitigation SSL Mitigation feature works as follows during an active HTTPS SYN-flood attack on a protected server, which is defined by an enabled *Protected SSL Object*:

1. The Layer 4 challenge on an HTTPS port is successful.
2. Radware DefensePro DDoS Mitigation passes the next SYN packet from the same source tothe on-device SSL/TLS component.
3. The on-device SSL/TLS component, via the Radware DefensePro DDoS Mitigationnetwork interface, performs the SSL/TLS handshake with the client.
4. Radware DefensePro DDoS Mitigation passes the subsequent HTTPS request from the same source to the on-device SSL/TLS component.
5. The on-device SSL/TLS component decrypts the request and sends it to the Radware DefensePro DDoS Mitigation SYN Flood Protection module.
6. The Radware DefensePro DDoS Mitigation SYN Flood Protection module generates the HTTP response including the L7 challenge, and sends it to the on-device SSL/TLScomponent.

7. The on-device SSL/TLS component encrypts the response from Radware DefensePro DDoS Mitigation SYN Flood Protection module and sends the encrypted HTTPS challenge to theclient via the Radware DefensePro DDoS Mitigation network interface.
8. Radware DefensePro DDoS Mitigation passes the subsequent HTTPS request to the on-device SSL/TLS component.
9. The on-device SSL/TLS component decrypts the request and sends it to the Radware DefensePro DDoS Mitigation SYN Flood Protection module.
10. Radware DefensePro DDoS Mitigation validates the request, and considers the connection to be legitimate or not.
11. If successfully validated, Radware DefensePro DDoS Mitigation adds the source IP address to the HTTP Authentication Table.
12. Radware DefensePro DDoS Mitigation terminates the HTTPS connection using theon-device SSL/TLS component.
13. The next SYN packet from the validated source passes through Radware DefenseProDDoS Mitigation to the protected server.

Notes

- For more information on Protected SSL Objects, see Managing Protected SSL Objects, page 117.
- For Radware DefensePro DDoS Mitigation to perform SSL Mitigation (in SYN Flood Protection) on an active HTTPS SYN-flood attack for a protected server, the server IP address and port must be defined as an enabled Protected SSL Object.

Managing SSL/TLS Certificates

This section describes managing the repository for SSL/TLS certificates for Radware DefensePro DDoS Mitigation, and how to manage the certificates using APSolute Vision.

This section contains the following main topics:

- Certificates, Keys, and Self-Signed Certificates, page 109
- Managing the SSL Certificates Repository, page 110
- Configuring Default Certificate Attributes, page 117

Certificates, Keys, and Self-Signed Certificates

Certificates are digitally signed indicators that identify the server or user. Certificates are usually provided in the form of an electronic key or value. The digital certificate represents the certification of an individual business or organizational public key, but can also be used to show the privileges and roles for which the holder has been certified. The digital certificate can also include information from a third-party verifying identity. Authentication is needed to ensure that users in a communication or transaction are who they claim to be.

A basic certificate includes the following:

- The certificate holder's identity
- The certificate's serial number
- The certificate expiry date
- A copy of the certificate holder's public key
- The identity of the Certificate Authority (CA) and its digital signature to affirm thedigital certificate was issued by a valid agency

A key is a variable set of numbers that the sender applies to encrypt data to be sent via the Internet. Usually a pair of public and private keys is used. A private key is kept secret and used only by its owner to encrypt and decrypt data. A public key has a wide distribution and is not secret. It is used for encrypting data and for verifying signatures. One key is used by the sender to encrypt or interpret the data. The recipient also uses the key to authenticate that the data comes from the sender.

The use of keys ensures that unauthorized entities cannot decipher the data. Only with the appropriate key can the information be easily deciphered or understood. Stolen or copied data would be incomprehensible without the appropriate key to decipher it and prevent forgery.

Radware DefensePro DDoS Mitigation supports RSA private keys, self-signed certificates, server certificates, and intermediate CA certificates.

Self-signed certificates do not include third-party verification.

When you open an HTTPS session for Radware DefensePro DDoS Mitigation management (such as using APSolute Vision), the Radware DefensePro DDoS Mitigation device uses a certificate for identification. By default, the device has a self-signed SSL/TLS certificate named **radware**. You can also create and use your own self-signed SSL/TLS certificates.

Radware DefensePro DDoS Mitigation supports the following key size lengths: 1024, 2048, and 4096 bytes.

Radware DefensePro DDoS Mitigation supports the following types of certificates:

- Server certificates with no wildcard in the common name and with no *Subject Alternative Name* (SAN).
- Server certificates with a wildcard in the common name.
- Server certificates with SANs.

Radware DefensePro DDoS Mitigation also supports Server Name Indication (SNI) using *Protected SSL Objects*. For more information, see Managing Protected SSL Objects, page 117.

Managing the SSL Certificates Repository

This section includes the following procedures and subsections:

- To add a private key certificate, page 111
- To add a server certificate, page 111
- To view the configuration of a certificate or key, page 113
- Importing Certificates, page 114
- Exporting Certificates, page 115

The *SSL Certificates Repository* table displays information for each SSL/TLS certificate stored on the Radware DefensePro DDoS Mitigation device.

Radware DefensePro DDoS Mitigation can store up to 1024 distinct, SSL/TLS server certificates. This allows the protection of up to 1024 distinct servers (IP addresses), where each server uses a different certificate.

In addition, Radware DefensePro DDoS Mitigation can store up to 2048 Intermediate CA certificates.

When APSolute Vision is connected to Radware DefensePro DDoS Mitigation using SNMPv3, you can do the following:

- Create and delete self-signed server certificates.
- Create and delete private keys for new certificates.
- Import and export certificates and private keys.

You can view—*read-only*—the configuration of a server certificate or private key as follows:

- After you have added (created) a server certificate or private key

- When APSolute Vision is connected to Radware DefensePro DDoS Mitigation not using SNMPv3
- When the Radware DefensePro DDoS Mitigation device is unlocked

To add a private key certificate

1. In the *Configuration* perspective, select **Setup > SSL Settings > SSL Certificates Repository**.
2. Click (Add).
3. From the **Certificate Type** drop-down list, select **Private Key**.

   Note: After you create a **Private Key** object, you can change **Certificate Type** to **Server Certificate**. No other modification is allowed.
4. Configure the following parameters:
   - **Certificate Friendly Name**–The friendly name that identifies the key or certificate. Maximum characters: 50
   - **Key Size**–The key size, in bytes. Values: 1024 Bytes, 2048 Bytes, 4096 Bytes. Default: 2048 Bytes
5. Click **Submit**.

To add a server certificate

1. In the *Configuration* perspective, select **Setup > SSL Settings > SSL Certificates Repository**.
2. Click (Add).
3. From the **Certificate Type** drop-down list, select **Server Certificate**.

   Note: After you create a **Server Certificate** object, you cannot modify it.
4. Configure the remaining available parameters and click **Submit**.

Table 45: Certificate Parameters–When Adding a Certificate

Parameter	Description
Certificate Friendly Name	The friendly name that identifies the key or certificate. Maximum characters: 50
Certificate Issuer	(Read-only) The issuer specified in the certificate. This field is empty when you are creating the certificate. After you create the certificate, the **Certificate Issuer** field displays the value from the **Common Name** field.
Serial Number	(Read-only) The serial number specified in the certificate. This field is empty when you are creating the certificate. After you create the certificate, the field displays the generated value.
Key Size	The key size, in bytes. Values: 1024 Bytes, 2048 Bytes, 4096 Bytes Default: 2048 Bytes

Table 45: Certificate Parameters–When Adding a Certificate (cont.)

Parameter	Description
Certificate Lifetime	
Valid From	(Read-only) The time, in DDD MMM dd HH:mm:ss yyyyformat, that the certificate became valid. This field is empty when you are creating the certificate. After you create the certificate, the field displays the value based on the value that you specified in the **Certificate Expiration**field. Example: Wed Jul 19 09:18:27 2017
Valid To	(Read-only) The time, in DDD MMM dd HH:mm:ss yyyyformat, that the certificate will become (or *became*) invalid. This field is empty when you are creating the certificate. After you create the certificate, the field displays the value based on the value that you specified in the **Certificate Expiration**field. Example: Wed Jul 19 09:18:27 2018
Certificate Expiration	The duration, in days, that the certificate remains valid. Default: 365
Common and Alternative Names	
Common Name	The domain name (Fully Qualified Domain Name, FQDN) of the Web site for which this certificate is intended. This value should match the Web address that clients (human or machine) use to connect to the Web site–for example www.mysite.com, MyInternalSite (typically, only when connecting within the corporate network), or 10.20.30.40. When you are creating the certificate, the default value is determined by the corresponding value in the *Default Attributes* table (see Configuring Default Certificate Attributes, page 117).
Subject Alternative Name (SAN) (Read-only) The *Subject Alternative Name (SAN)* table lists the SANs in the certificate. The table is empty when you create a certificate. When you create a certificate, there are no SANs.	
Organization Details When you are creating the certificate, the default value for each field in the *Organization Details* group is determined by the corresponding value in the *Default Attributes* table (see Configuring Default Certificate Attributes, page 117).	
Organization	The name of the organization.
Email Address	Any e-mail address that you want to include within the certificate.
Organization Unit	The department or unit within the organization.
City or Locality	The name of the city or locality of the organization.
State or Province	The state or province of the organization.
Country or Region	The country or region of the organization.

To view the configuration of a certificate or key

1. In the *Configuration* perspective, select **Setup > SSL Settings > SSLCertificates Repository**.
2. Do one of the following:
   - When APSolute Vision is connected to Radware DefensePro DDoS Mitigation usingSNMPv3, double-click the certificate name.
   - When APSolute Vision is connected to Radware DefensePro DDoS Mitigation *not*using SNMPv3 or the Radware DefensePro DDoS Mitigation device is unlocked, selectthe certificate name and click  (View Certificate).

Table 46: Certificate / Private-Key Parameters–Read-only, Viewing the Configuration

Parameter	Description
Certificate Friendly Name	The friendly name that identifies the key or certificate.
Certificate Type	Values: • Private Key • Server Certificate • Intermediate CA–The intermediate CA that is defined in an imported certificate.
Certificate Issuer	The issuer specified in the certificate. If the certificate was created using APSolute Vision, the **Certificate Issuer** field is the value from the **Common Name** field.
Serial Number	The serial number specified in the certificate. If the certificate was created using APSolute Vision, the field value is a generated value.
Key Size	The key size, in bytes.
Certificate Lifetime	
Valid From	The time, in DDD MMM dd HH:mm:ss yyyyformat, that the certificate became valid. If the certificate was created using APSolute Vision, the field value is based on the value that was specified in the **Certificate Expiration** field. Example: Wed Jul 19 09:18:27 2017
Valid To	The time, in DDD MMM dd HH:mm:ss yyyyformat, that the certificate will become–or *became*–invalid. If the certificate was created using APSolute Vision, the field value is based on the value in the **Certificate Expiration** field. Example: Wed Jul 19 09:18:27 2018
Certificate Expiration	The duration, in days, that the certificate remains valid.

Table 46: Certificate / Private-Key Parameters–Read-only, Viewing the Configuration (cont.)

Parameter	Description
Common and Alternative Names	
Common Name	The domain name (Fully Qualified Domain Name, FQDN) of the Web site for which this certificate is (supposedly) issued. This should match the Web address that clients (human or machine) use to connect to the website–for example www.mysite.com, MyCorporation-wideApp (typically, only when connecting within the corporate network), or 10.20.1.172.
Subject Alternative Name (SAN) The *Subject Alternative Name (SAN)* table lists all the SANs in the certificate.	
Organization Details The parameters in the *Organization Details* group are relevant only when **Certificate Type** is **Server Certificate**.	
Organization	The name of the organization.
Email Address	Any e-mail address that you want to include within the certificate.
Organization Unit	The department or unit within the organization.
City or Locality	The name of the city or locality of the organization.
State or Province	The state or province of the organization.
Country or Region	The country or region of the organization.

Importing Certificates

To import keys and certificates, the connection between the APSolute Vision server and the relevant device must use SNMPv3.

Keys and certificates are imported in PEM format. If you have separate PEM files for keys and for certificates, you must import them consecutively with the same **Certificate Friendly Name**.

To import a certificate or key

1. In the *Configuration* perspective, select **Setup > SSL Settings > SSL Certificates Repository**.
2. Click the  (Import Certificate) button.
3. Configure the parameters, and then, click **Upload**.

Table 47: Importing Certificates Parameters

Parameter	Description
Certificate Friendly Name	A new friendly name to create by import, or an existing entry name to overwrite or complete a key.

Table 47: Importing Certificates Parameters (cont.)

Parameter	Description
Certificate Type	Values: • Private Key–Imports a key from backup or exported from another system. To complete the configuration, you will need to import a server certificate into this key. • Server Certificate–Imports a server certificate from backup or exported from another machine. The certificate must be imported onto a matching private key. • Intermediate CA–Imports an intermediate CA certificate. Default: Private Key
Private Key Passphrase (This parameter is available only when the **Certificate Type** is **Private Key**.)	The passphrase for the encryption of the private key. Minimum characters: 4 Maximum characters: 64 **Notes:** • When you are importing a private key, the **Private Key Passphrase** parameter is mandatory if a passphrase was set when it was exported. • Radware DefensePro DDoS Mitigation can import a certificate that was not exported by Radware DefensePro DDoS Mitigation. Therefore, there is a scenario where import is not possible if the certificate has a passphrase longer than 64 characters.
File Name	The certificate file to import.

Exporting Certificates

You can export private keys and server certificates for backup purposes, moving existing configurations to another system.

You can export certificates from a device by copying and pasting a certificate or by downloading a file. Keys and certificates are exported to PEM format.

To export a certificate or key

1. In the *Configuration* perspective, select **Setup > SSL Settings > SSL Certificates Repository**.
2. Select the relevant certificate.
3. Click the  (Export Certificate) button.
4. Configure the parameters, and do one of the following:
   - Click **Show** (when **Export To** is **Text**) to display the certificate content, which you can copy and paste as appropriate.
   - Click **Export** (when **Export To** is **File**) to export the certificate as a file to a specified location.

Table 48: Export Certificate Parameters

Parameter	Description
Certificate Friendly Name	The friendly name of the certificate to export.
Certificate Type	The certificate type that Radware DefensePro DDoS Mitigation exports. Values: • Private Key–Exports a server certificate or private key from the device as a private key. • Server Certificate–Exports a server certificate from the device. • Intermediate CA–Exports an intermediate CA certificate from the device. **Note:** The option or options that are available depend on the certificate type that you selected in step 2 of this procedure. If you selected an Intermediate CA, **Intermediate CA** is the only option. If you selected a private key, **Private Key** is the only option. If you selected a server certificate, the options are **Server Certificate** and **Private Key**.
Private Key Passphrase (This parameter is available only when the **Certificate Type** is **Private Key**.)	The passphrase that encrypts the key while in transit, and to only allow it to be imported (later) only by someone who knows the passphrase. Minimum characters: 4 Maximum characters: 64
Confirm Private Key Passphrase (This parameter is available only when the **Certificate Type** is **Private Key**.)	The passphrase that was entered when the private key was created or imported. You must enter the key passphrase to validate that you are authorized to export the key. Minimum characters: 4 Maximum characters: 64
Export To	The target type of the certificate. Values: • Text–Displays the certificate content, which you can copy and paste as appropriate. • File–Exports the certificate as a file to the location you specify. The filename is in the following format: — <CertificateFriendlyName>.key–for a private key — <CertificateFriendlyName>.cert–for a server certificate — <CertificateFriendlyName>.interm–for an intermediate CA certificate Default: Text

Configuring Default Certificate Attributes

Use certificate defaults to define your organization's default parameters to be used when creating server certificates (see the procedure To add a server certificate, page 111).

To configure default attributes, the connection between the APSolute Vision server and the relevant device must use SNMPv3.

To configure the default certificate attributes

1. In the *Configuration* perspective, select **Setup > SSL Settings > SSL Certificates Repository > Default Attributes**.
2. Configure the parameters, and then, click **Submit**.

Table 49: Default Certificate Parameters

Parameter	Description
Common Name	The domain name of the organization. For example, www.mydomain.com.
Locality	The name of the city.
State / Province	The state or province.
Organization	The name of the organization.
Organization Unit	The department or unit within the organization.
Country Name	The organization country.
Email Address	Any e-mail address to include in the certificate.

Managing Protected SSL Objects

Each *Protected SSL Object* in the *Protected SSL Objects* pane represents one or both of the following:

- A protected HTTPS server in an HTTPS Flood Protection profile
- A server that the SSL Mitigation feature can protect in a SYN Flood Protection profile

Notes

- *SSL-decryption-and-encryption* requires a DefenseSSL license.
- For information on HTTPS Flood Protection, see Configuring HTTPS Flood ProtectionProfiles, page 201.
- For information on the configuration of a SYN Flood Protection profile and the **UseSSL Mitigation** option, see Managing SYN Flood Protection Profile Parameters, page235.
- You can configure up to 1024 Protected SSL Objects.
- Up to 1024 Protected SSL Objects can be associated to a single Protection policy.
- For more information on Protection policies, see Configuring Protection Policies, page160. An

HTTPS Flood Protection profile uses a Protected SSL Object under the following conditions:

- The Protected SSL Object is *enabled*.
- The IP address specified in the Protected SSL Object matches an IP address of the**DST Network** parameter in the Protection policy.

- For HTTPS mitigation methods, when:
  - The **SSL Decryption and Encryption** option is **Enabled, Using theOn-Device Component**.
  - The Protection policy includes a HTTPS Flood Protection profile with the mitigation method **Use HTTPS Authentication on Suspect Sources** enabled and/or with the mitigation method **Use HTTPS Authentication on All Sources** enabled.

A SYN Flood Protection profile uses a Protected SSL Object during the SSL Mitigation challenge process under the following conditions:

- The Protected SSL Object is *enabled*.
- The IP address specified in the Protected SSL Object matches an IP address of the**DST Network** parameter in the Protection policy.
- The Protection policy includes a SYN Flood Protection profile with **Use SSL Mitigation**enabled.
- The *Protection Name* list in the SYN Flood Protection profile includes **HTTPS**.

Note: For information on how SSL Mitigation works in the scenario using Protected SSL Objects, see SYN Flood Protection with SSL Mitigation Using the On-Device Component for SSL/TLS Decryption and Encryption, page 108.

To configure a Protected SSL Object

1. In the *Configuration* perspective, select **Setup > SSL Settings > Protected SSLObjects**.
2. Do one of the following:
   - To add an entry, click the  (Add) button.
   - To edit an entry, double-click the row.
3. Configure the parameters, and then click **Submit**.

Table 50: Protected SSL Objects Parameters

Parameter	Description
Enabled	Specifies whether Radware DefensePro DDoS Mitigation implements the object, that is, tries to match this object to the destination IP addresses defined by a Protection policy.
Object Name	Maximum characters: 60
IP Address Type	Values: IPv4, IPv6 Default: IPv4
IP Address	The IPv4 or IPv6 address. **Note:** The IP address *can* represent a virtual IP address (VIP) of a cluster of servers.
Application Port	The port on which the server in the Protection policy listens for HTTPS traffic. Values: 0–65,534 Default: 443

Table 50: Protected SSL Objects Parameters (cont.)

Parameter	Description
SSL Server Certificates	
The **Certificates Available** list and the **Certificates Selected** list together contain all the server certificates stored on the Radware DefensePro DDoS Mitigation devices. The **Certificates Selected** list displays the server certificates included in the Protected SSL Object. Select entries from the lists and use the arrows to move the entries to the other lists as required. If the **Certificates Selected** list contains multiple entries, Radware DefensePro DDoS Mitigation treats the certificates as a group of certificates, to be used for *Server Name Indication* (SNI). **Note:** For information on configuring server certificates, see Managing the SSL Certificates Repository, page 110.	
Default Certificate (This parameter is available only if the **Certificates Selected** list contains more than one entry.)	Specifies one of the following: • if more than one server certificate is selected from the SSL Certificates Repository, specifies the default SNI certificate. • When the field is empty, specifies that the Protected SSL Object uses no default SNI certificate.
Encryption Protocol and Ciphers	
Allowed SSL Protocol Version	
SSL 3.0	Specifies which SSL-protocol version the Protected SSL Object allows. Default: TLS 1.1, TLS 1.2, TLS 1.3
TLS 1.0	
TLS 1.1	
TLS 1.2	
TLS 1.3	
SSL Cipher Suites	The SSL/TLS cipher suites that Radware DefensePro DDoS Mitigation uses for the SSL/TLS connection. Values: • System Defined–Comprises the cipher suites defined by the following string: kEECDH+ECDSA:kEECDH:kEDH:RSA:kECDH:+CAMELLIA:+SHA:+SEED:!NULL:!aNULL:!EXPORT:!RC4:!3DES:!DES:!DSS:!SRP:!PSK:!AESCCM • User Defined–Comprises the cipher suites defined in the **User-defined Cipher-Suite List** field Default: System Defined
User-Defined SSL Cipher-Suite List (This parameter is available only when the option for **SSL Cipher Suites** is **User Defined**.)	Any specified set of cipher suites supported by the accepted OpenSSL format. For more information, see the OpenSSL documentation. Maximum characters: 256

Configuring the Security-Settings Setup

Before you configure a Protection policy and its protection profiles, you must enable the protection features you want to use and configure the global parameters for the protection features.

This section contains the following topics:

- Configuring Global Anti-Scanning Protection Settings, page 120
- Configuring Global Behavioral DoS Protection, page 121
- Configuring Global DNS Flood Protection, page 124
- Configuring Global HTTPS Flood Protection, page 128
- Configuring Global Out-of-State Protection, page 128
- Configuring Global Signature Protection, page 132
- Configuring Global SYN Flood Protection, page 134
- Configuring Global Packet Anomaly Protection, page 134

Notes

- When you enable or disable a protection feature—except for Signature Protection, the device requires a reboot to take effect. However, you need to reboot only once after enablingfeatures within the same navigation branch.
- When you enable or disable Signature Protection, the device requires an Update Policies action to take effect.

Configuring Global Anti-Scanning Protection Settings

Anti-Scanning protects against malicious scanning activity, which includes the following:

- **Zero-day self-propagating network worms**—A self-propagating worm is an attack that spreads by itself using network resources. This worm uses a random-IP-address-generation technique (that is, network scanning) to locate a vulnerable host to infect. When a vulnerable host is identified, the worm immediately executes its code on this host, thereby infecting the computer with the worm's malicious code. Then, the infected hosts initiate similar scanning techniques and infect other hosts, propagating exponentially.
- **Horizontal scans, also referred to *IP scans* or *IP-address scans***—These scans scan fora specific port or ports across a range of IP addresses. There are several random-IP-address- generation techniques, commonly characterized with horizontal scanning schemes.
- **Vertical scans, also referred to *port scans***—These scans scan multiple ports on a specific IP address or IP addresses. Prior to launching an attack, hackers try to identify what TCP and UDP ports are open on the victim machine. An open port represents a service, an application or a back door. Ports left open unintentionally can create serious security problems. These scanning techniques commonly utilize a vertical scanning scheme

When Anti-Scanning Protection is enabled, upon detecting an attack, the Anti-Scanning profile in a Protection policy implements the blocking-footprint rule for a predefined, initial *blocking duration*.

Anti-Scanning Protection does the following when it identifies repeated scanning activities from the same source:

- Extends the blocking duration.
- Uses the Suspend Table to store source information. When the Suspend Table is full, and the policy/profile **Action** is **Block and Report**, Radware DefensePro DDoS Mitigation drops all packets from new sessions that are suspected to be involved in a scanning attack andissues appropriate, periodic alerts.

Note: For information on the Suspend Table, see Configuring Radware DefensePro DDoS Mitigation Suspend Table Settings, page 141.

Note: For information on configuring Anti-Scanning profiles, see Configuring Anti-Scanning Protection Profiles, page 168.

To enable or disable Anti-Scanning Protection

1. In the *Configuration* perspective, select **Setup > Security Settings >Anti-Scanning Protection**.
2. Select or clear the **Enable Anti-Scanning Protection** checkbox. Default: Disabled.

Caution: Changing the setting of this parameter requires an Update Policies action to take effect.

3. Click **Submit**.

Configuring Global Behavioral DoS Protection

Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Protection policy, defends your network from zero-day network-flood attacks. These attacks fill available network bandwidth with irrelevant traffic, denying use of network resources to legitimate users. The attacks originate in the public network and threaten Internet-connected organizations.

The Behavioral DoS profiles detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic.

Network-flood protection types include the following:

- TCP floods–which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN +ACK Flood, and TCP Fragmentation Flood
- UDP floods–which includes UDP Fragmentation Flood
- ICMP flood
- IGMP flood

The main advantage of BDoS Protection is the ability to detect statistical traffic anomalies and generate an accurate DoS-attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

Note: This feature is *not* supported on management interfaces.

Enabling BDoS Protection

Before you configure BDoS Protection profiles, enable BDoS Protection. You can also change the default global device settings for BDoS Protection. The BDoS Protection global settings apply to all the Protection policies with BDoS profiles on the device.

To enable BDoS Protection and configure global settings

1. In the *Configuration* perspective, select **Setup > Security Settings > BDoSProtection**.
2. Configure the parameters, and then, click **Submit**.

Table 51: BDoS Protection (Global): General Parameters

Parameter	Description
Enable BDoS Protection	Specifies whether BDoS Protection is enabled. **Caution:** Changing the setting of this parameter requires a reboot to take effect.
Learning Response Period	The initial period from which baselines are primarily weighted. The default and recommended learning response period is one week. If traffic rates legitimately fluctuate (for example, TCP or UDP traffic baselines change more than 50% daily), set thelearning response to one month. Use a one-day period for testing purposes only. Values: Day, Week, Month Default: Week
Enable Traffic Statistics Sampling	Specifies whether the BDoS module uses traffic-statistics sampling during the creation phase of the real-time signature. Default: Enabled **Note:** For accurate mitigation and best performance, Cisco recommends that the parameter be *enabled*.
Enable Overblocking Prevention	Specifies whether the Radware DefensePro DDoS Mitigation device allows enabling Overblocking Prevention in BDoS profiles. *Overblocking* is a situation where the BDOS profile creates a signature that meets all required criteria–blocking the attack and matching the specified strictness level, but blocks too much legitimate traffic. **Note:** For more information, see Configuring BDoS Profiles, page 172.

Table 52: BDoS Protection (Global): Advanced Parameters

Parameter	Description
These settings affect periodic attack behavior. The settings are used to effectively detect and block these attack types.	
Duration of Non-Attack Traffic in Blocking State	The time, in seconds, at which the *degree of attack* falls below and stays below the hard-coded threshold in the Blocking state. When the time elapses, Radware DefensePro DDoS Mitigation declares the attack to be terminated. Values: 45–300 Default: 45 **Note:** When a BDoS profile has Burst-Attack Protection *enabled*, Radware DefensePro DDoS Mitigation ignores the **Duration of Non-Attack Traffic in Blocking State** parameter. With Burst- Attack Protection, Radware DefensePro DDoS Mitigation calculates the duration of non-attack traffic in the Blocking state using internal parameters and the configuration of the BDoS profile. For more information on Burst-Attack Protection, see Configuring BDoS Profiles, page 172.
Duration of Non-Attack Traffic in Anomaly or Non- Strictness State	The time, in seconds, at which the *degree of attack* falls below and stays below the hard-coded threshold in the Anomaly state or the Non-strictness state. When the time elapses, Radware DefensePro DDoS Mitigation declares the attack to be terminated. Values: 45–300 Default: 45
Reset BDoS Baseline	Click to reset the BDoS baseline. Then, select whether to reset the baseline for all Protection policies that contain a BDoS profile, or for a specific Protection policy that contains a BDoS profile; and then, click **Submit**. Resetting baseline-learned statistics clears the baseline traffic statistics and resets default normal baselines. Reset the baseline statistics only when the characteristics of the protected network have changed entirely and bandwidth quotas need to be changed to accommodate the network changes.

Configuring BDoS Footprint Bypass

You can define footprint bypass types and values that will not be used as part of a real-time signature. The types and values that you define will not be used in OR or in AND operations within the blocking rule (real-time signature) even when the protection-engine suggests that the traffic is a real-time signature candidate.

To configure BDoS footprint bypass

1. In the *Configuration* perspective, select **Setup > Security Settings > BDoS Protection> BDoS Footprint Bypass**.
2. From the drop-down list of the *Footprint Controller* column, select the controller for which you want to configure footprint bypass, and click the  (Search) button. The table displays the bypass types and values for the selected controller.
3. To edit bypass type settings, double-click the corresponding row.
4. Configure the footprint bypass parameters for the selected bypass type, and then, click **Submit**.

Table 53: BDoS Footprint Bypass Parameters

Parameter	Description
Footprint Controller	(Read-only) The controller for which you are configuring footprint bypass.
Bypass Field	(Read-only) The selected bypass type to configure.
Bypass Status	The bypass option. Values: • Bypass All Values–The Behavioral DoS module bypasses all possible values of the selected Bypass Field when generating a footprint. • Bypass Defined Values–The Behavioral DoS module bypasses only the specified values (if such a value exists) of theselected **Bypass Field** when generating a footprint.
Bypass Values	The value(s) that the Behavioral DoS mechanism does not use for the selected **Bypass Field** when generating the footprint. Radware DefensePro DDoS Mitigation uses the **Bypass Values** parameter only when the value of the **Bypass Status** parameter is **Bypass Defined Values**. The valid values for the **Bypass Values** parameter vary according to the selected **Bypass Field**. Multiple values in the **Bypass Values** field must be comma-delimited.

Configuring Global DNS Flood Protection

DNS Flood Protection, which you can use in your Protection policy, defends your network against zero-day DNS query floods. These floods overwhelm the DNS servers with queries, denying service to legitimate users. DNS query floods can impact not only the DNS servers, but also the entire network infrastructure.

DNS query floods can target an authoritative DNS server or a recursive DNS server. In the case of an authoritative DNS server, queries originate from either commercial or public recursive DNSservers. In the case of a recursive DNS server, queries originate from hosts (for example, subscribed hosts of a commercial recursive resolver or any host using an open resolver). A basic query flood may be composed of a single Fully Qualified Domain Name (FQDN) or multiple FQDNs. A sophisticated query flood, also known as a *recursive flood* or *random-subdomains flood*, is composed of fake, random subdomains of a targeted domain. The goal of the random-subdomains attack is to overload the DNS resolver's resources and also target an authoritative DNS server in charge of the targeted domain. In this attack, both legitimate (“good”) subdomains and attack (“bad”) subdomains appear as legitimate queries to the DNS server.

In Radware DefensePro DDoS Mitigation 8.*x* versions 8.13 and later, the DNS Flood Protection engine is able to detect all types of DNS query floods, automatically identify the attack FQDNs and/ or targeted domain, and allow only the “good” queries to the protected DNS servers.

DNS Flood Protection monitors DNS queries with query-type granularity. That is, Radware DefensePro DDoS Mitigation examines each query type rather than handling all DNS queries equally. Radware DefensePro DDoS Mitigation is thus able to detect a flood on a specific query type.

DNS Flood Protection types can include the following DNS query types:

- A
- MX
- PTR
- AAAA
- Text
- SOA
- NAPTR
- SRV
- Other

DNS Flood Protection can detect statistical anomalies in DNS traffic and generate an accurate attack footprint based on a heuristic protocol information analysis. This ensures accurate attack filtering with minimal risk of false positives. The default average time for a new signature creation is between 10 and 18 seconds. This is a relatively short time, because flood attacks can last for minutes and sometimes hours.

Before you configure DNS Flood Protection *profiles,* ensure that DNS Flood Protection is enabled. You can also change the default global device settings for DNS Flood Protection. The DNS Flood Protection global settings apply to all the Protection policies with DNS Flood Protection profiles on the Radware DefensePro DDoS Mitigation device.

To enable DNS Flood Protection and configure global settings

1. In the *Configuration* perspective, select **Setup > Security Settings > DNS FloodProtection**.
2. Configure the parameters, and then, click **Submit**.

Table 54: DNS Flood Protection: General Parameters

Parameter	Description
Enable DNS Flood Protection	Specifies whether DNS Flood Protection is enabled. **Caution:** Changing the setting of this parameter requires a reboot to take effect.
Learning Response Period	The initial period from which baselines are primarily weighted. The default and recommended learning response period is one week. If traffic rates legitimately fluctuate (for example, TCP or UDP traffic baselines change more than 50% daily), set the learning response to one month. Use a one day period for testing purposes only. Values: Day, Week, Month Default: Week

Table 55: DNS Flood Protection: Mitigation Actions Parameters

Parameter	Description
When the protection is enabled and the device detects that a DNS-flood attack has started, the device implements the Mitigation Actions in escalating order–in the order that they appear in the tab. If the first enabled Mitigation Action does not mitigate the attack satisfactorily (after a certain *Escalation Period*), the device implements the next more-severe enabled Mitigation Action–and so on. As the most severe Mitigation Action, the device always implements the *Collective Rate Limit*, which limits the rate of all DNS queries to the protected server.	
Enable Signature Rate Limit	Specifies whether the device limits the rate of DNS queries that match the real-time signature. Default: Enabled
Enable Collective Rate Limit	(Read-only) The device limits the rate of all DNS queries to the protected server. Value: Enabled

Table 56: DNS Flood Protection: Advanced Parameters

Parameter	Description
These settings affect periodic attack behavior. The settings are used to effectively detect and block these attack types.	
Duration of Non-Attack Traffic in Blocking State	The time, in seconds, at which the *degree of attack* falls below and stays below the hard-coded threshold in the Blocking state. When the time elapses, Radware DefensePro DDoS Mitigation declares the attack to be terminated. Values: 45-300 Default: 45
Duration of Non-Attack Traffic in Anomaly or Non- Strictness State	The time, in seconds, at which the *degree of attack* falls below and stays below the hard-coded threshold in the Anomaly state or the Non-strictness state. When the time elapses, Radware DefensePro DDoS Mitigation declares the attack to be terminated. Values: 45-300 Default: 45
Enable DNS Protocol Compliance Checks	Specifies whether the device checks each DNS query for DNS protocol compliance and drops the non-compliant queries. Default: Enabled
Allow Large EDNS Packets (This checkbox is active only when the **Enable DNS Protocol Compliance Checks** checkbox is selected.)	Specifies whether, when checking for DNS protocol compliance, the device allows DNS packets larger than 512 bytes. In the *extension mechanisms for DNS* (EDNS) specification, DNS packets larger than 512 bytes *are* allowed. In the original DNS specification, the maximum UDP packet size is 512 bytes. Default: Enabled

Table 56: DNS Flood Protection: Advanced Parameters (cont.)

Parameter	Description
Reset DNS Baseline (button)	Click to reset the DNS baseline. Then, select whether to reset the baseline for all Protection policies that contain a DNS profile, or for a specific Protection policy that contains a DNS profile; and then, click **Submit**. Resetting baseline-learned statistics clears the baseline traffic statistics and resets default normal baselines. Reset the baseline statistics only when the characteristics of the protected network have changed entirely and bandwidth quotas need to be changed to accommodate the network changes.

Table 57: DNS Footprint Strictness Examples

Footprint Example	Low Strictness	Medium Strictness	High Strictness
DNS Query	Yes	No	No
DNS Query AND DNS ID	Yes	Yes	No
DNS Query AND DNS ID AND Packet Size	Yes	Yes	Yes

Configuring DNS Footprint Bypass

You can define footprint bypass types and values that will not be used as part of a real-time signature. The types and values that you define will not be used in OR or in AND operations within the blocking rule (real-time signature) even when the protection-engine suggests that the traffic is a real-time signature candidate.

To configure DNS footprint bypass

1. In the *Configuration* perspective, select **Setup > Security Settings > DNSFlood Protection > DNS Footprint Bypass**.
2. From the drop-down list of the *Footprint Controller* column, select the DNS query type for which you want to configure footprint bypass, and click the  (Search) button. The table displays the bypass fields for the selected DNS query type.
3. To edit bypass type settings, double-click the corresponding row.
4. Configure the footprint bypass parameters for the selected bypass field, and then, click **Submit**.

Table 58: DNS Footprint Bypass Parameters

Parameter	Description
Footprint Controller	(Read-only) The selected DNS query type for which you are configuring footprint bypass.
Bypass Field	(Read-only) The selected **Bypass Field** to configure.

Table 58: DNS Footprint Bypass Parameters (cont.)

Parameter	Description
Bypass Status	The bypass option. Values: • Bypass All Values–The DNS Flood Protection module bypasses all possible values of the selected **Bypass Field** when generating a footprint. • Bypass Defined Values–The DNS Flood Protection module bypasses only the specified values (if such a value exists) of the selected **Bypass Field** when generating a footprint.
Bypass Values	The value(s) that the DNS Flood Protection mechanism does not use for the selected Bypass Field when generating the footprint. Radware DefensePro DDoS Mitigation uses the Bypass Values parameter only when the value of the Bypass Status parameter is Bypass Defined Values. The valid values for the Bypass Values parameter vary according to the selected Bypass Field. Multiple values in the Bypass Values field must be comma-delimited.

Configuring Global HTTPS Flood Protection

This feature requires a DefenseSSL license.

HTTPS Flood Protection protects against HTTPS flood attacks, and effectively handles large amounts of HTTPS traffic, with the minimum possible need to decrypt traffic.

You configure HTTPS Flood Protection *globally* using the procedure below.

For the requirements and information about configuring HTTPS Flood Protection profiles, see Configuring HTTPS Flood Protection Profiles, page 201.

To enable or disable global HTTPS Flood Protection

1. In the *Configuration* perspective, select**Setup > Security Settings > HTTPS Flood Protection**.
2. Select or clear the **Enable HTTPS Flood Protection** checkbox to specify whether Radware DefensePro DDoS Mitigation enables HTTPS Flood Protection configuration and learning, and then, click **Submit**. Default: Enabled (if the device has a DefenseSSL license)

Configuring Global Out-of-State Protection

Out-of-State Protection detects out-of-state packets to provide additional protection for TCP- session-based attacks.

You configure Out-of-State Protection *globally* using the procedure below. For information about configuring Out-of-State Protection profiles, see Configuring Out-of-State Protection Profiles, page 205.

Radware DefensePro DDoS Mitigation implements several different *grace periods* for Out-of-State Protection actions for different scenarios. During any one of these grace periods, Radware DefensePro DDoS Mitigation delays Out-of-State Protection actions and only registers all sessions in the Session table, including sessions whose initiation was not registered.

Note: The Radware DefensePro DDoS Mitigation CLI includes commands for configuring Out-of- State Protection and viewing the state. For example, the CLI includes commands for viewingthe status of grace periods. For more information, refer to the relevant *CLI Reference Manual*.

Caution: Some CLI commands are intended for internal use only–for example, for use by Technical Support.

Radware DefensePro DDoS Mitigation implements a grace period for Out-of-State Protection actions for the following scenarios:

- **After startup or reboot when the selected Startup Mode is Graceful**–This *graceful- startup* period (**Startup Timer**) is configurable in the Out-of-State Protection global parameters (in the procedure below). Default: 1800 seconds (30 minutes).
- **When an Update Policies action finishes**–This grace period is configurable in the Out-of- State Protection global parameters (in the procedure below). Default: 30 seconds.
- **When the Session table is no longer full**–This grace period is configurable in the Out-of- State Protection global parameters (in the procedure below). Default: 1800 seconds (30 minutes).

To configure global Out-of-State Protection

1. In the *Configuration* perspective, select **Setup > Security Settings >Out-of-State Protection**.
2. Configure the parameters, and then, click **Submit**.

Table 59: Out-of-State Protection Global Parameters

Parameter	Description
Enable Out-of-State Protection	Specifies whether Radware DefensePro DDoS Mitigation enables Out-of-State Protection configuration and learning. Default: Enabled

Table 59: Out-of-State Protection Global Parameters (cont.)

Parameter	Description
Activate Out-of-State Protection (Without Reboot) (This parameter is available only after selecting the **Enable Out-of-State Protection** checkbox.)	Values: • Enabled–Activate Out-of-State Protection actions immediately. • Disabled–Deactivate Out-of-State Protection actions immediately. Default: Enabled When the selected **Startup Mode** is **Off** or **Graceful**, to start Out- of-State Protection after startup *immediately* (with no learning of traffic and sessions), select the **Activate Out-of-State Protection (Without Reboot)** checkbox. When the **Activate Out-of-State Protection (Without Reboot)** checkbox is selected and the Update Policies action starts, Radware DefensePro DDoS Mitigation clears the checkbox and suspends Out-of-State Protection actions for 30 seconds. These 30 seconds give Radware DefensePro DDoS Mitigation some time to learn traffic and sessions, thereby reducing the chances of false positives. When the **Activate Out-of-State Protection (Without Reboot)** checkbox is selected and the selected **Startup Mode** is **Graceful**, after startup, the **Activate Out-of-State Protection (Without Reboot)** checkbox is cleared for the duration of the **Startup Timer**. After the **Startup Timer** has elapsed, the **Activate Out- of-State Protection (Without Reboot)** checkbox is automatically selected (that is, *enabled* again). When the **Activate Out-of-State Protection (Without Reboot)** checkbox is selected and the selected **Startup Mode** is **Off**, after startup, the **Activate Out-of-State Protection (Without Reboot)** checkbox is cleared.
Startup Mode (This parameter is available only after selecting the **Enable Out-of-State Protection** checkbox.)	The behavior of the device after startup. Values: • On–Start Out-of-State Protection action immediately after startup (with no time to learn traffic and sessions). Sessions that started before startup get dropped. Only new, valid sessions are allowed. • Off–Do not start Out-of-State Protection after startup or reboot. • Graceful–After startup, start learning sessions (and updating the Session table) for the time specified by the **Startup Timer** parameter. Then, begin Out-of-State Protection actions. Default: Graceful **Note:** When the value is **Off** or **Graceful**, to start Out-of-State Protection *immediately* after startup (with no learning of traffic and sessions), select the **Activate Out-of-State Protection (Without Reboot)** checkbox.

Table 59: Out-of-State Protection Global Parameters (cont.)

Parameter	Description
Grace Period on Device Startup (This parameter is available only after selecting the **Enable Out-of-State Protection** checkbox.)	When the selected **Startup Mode** is **Graceful**, this parameter specifies the time, in seconds, after startup or reboot, that the Radware DefensePro DDoS Mitigation device delays Out-of-State Protection actions and only registers all sessions in the Session table, including sessions whose initiation was not registered. After this time, the Out-of-State Protection module inspects packets and decides whether a packet is out of state. Radware DefensePro DDoS Mitigation then takes action according to the configuration of the matching Protection policy and Out-of-State Protectionprofile. Values: 0–65,535 Default: 1800 (30 minutes)
Grace Period on Update Policies (This parameter is available only after selecting the **Enable Out-of-State Protection** checkbox.)	This parameter specifies the time, in seconds, after an Update Policies action, that the Radware DefensePro DDoS Mitigation device delays Out-of-State Protection actions and only registers all sessions in the Session table, including sessions whose initiation was not registered. After this time, the Out-of-State Protection module inspects packets and decides whether a packet is out of state. Radware DefensePro DDoS Mitigation then takes action according to the configuration of the matching Protection policy and Out-of-State Protection profile. Values: 0–65,535 Default: 30
Grace Period After Session Table No Longer Full (This parameter is available only after selecting the **Enable Out-of-State Protection** checkbox.)	This parameter specifies the time, in seconds, after the Session table was full and is no longer full, that the Radware DefensePro DDoS Mitigation device delays Out-of-State Protection actions and only registers all sessions in the Session table, including sessions whose initiation was not registered. After this time, the Out-of- State Protection module inspects packets and decides whether a packet is out of state. Radware DefensePro DDoS Mitigation then takes action according to the configuration of the matching Protection policy and Out-of-State Protection profile. Values: 0–65,535 Default: 1800 (30 minutes)
Sampling Frequency	The time, in seconds, that the out-of-state PPS is below the specified **Termination Threshold** in the Out-of-State Protection profile before Radware DefensePro DDoS Mitigation considers the TCP-session-based attack to have stopped. For example, if the value is 10, Radware DefensePro DDoS Mitigation considers the TCP-session-based attack to have stopped only if the out-of-state PPS is below the **Termination Threshold** for 10 consecutive seconds. Values: 4–10 Default: 10 **Note:** For more information on the **Termination Threshold** parameter (*Configuration* perspective, **Protections > Outof State Protection Profiles > Termination Threshold**), see Configuring Out-of-State Protection Profiles, page 205.

Configuring Global Signature Protection

Signature Protection is enabled by default.

When Radware DefensePro DDoS Mitigation detects a signature in a TCP session, Radware DefensePro DDoS Mitigation drops all packets of the session.

Caution: When Radware DefensePro DDoS Mitigation is dropping packets of an existing TCP session, and then, certain changes are made to the configuration of the Signature Protection profile, reports relating to that session might include unexpected results.

To configure Signature Protection

1. In the *Configuration* perspective, select **Setup > Security Settings > SignatureProtection**.
2. Select or clear the **Enable Application Security Protection** checkbox to specifywhether Radware DefensePro DDoS Mitigation uses Application Security Protection.

   If the protection is disabled, enable it before setting up the protection profiles.

   Caution: Changing the setting of this parameter requires an Update Policies action to take effect.
3. Click **Submit**.

Configuring Global DoS Shield Protection

The DoS Shield mechanism protects against known flood attacks and flood-attack tools that cause a denial-of-service effect, making computer resources unavailable to the intended users.

Notes

- DoS Shield protection is enabled by default.
- This feature is also supported on managementinterfaces. DoS

Shield profiles prevent the following:

- Known TCP, UDP, and ICMP floods
- Known attack tools available over the Internet
- Known floods created by bots, which are automated attacks

DoS Shield protection uses signatures from the Radware *Signatures* database. This database is continuously updated and protects against all known threats.

Radware Signature profiles include all DoS Shield signatures as part of the signature database and Radware predefined profiles that already include DoS Shield protection. To create a profile that includes DoS Shield protection, you configure a profile with the **Threat Type** attribute set to **Floods**.

Radware also supplies a predefined profile, the **All-DoS-Shield** profile, which provides protection against all known DoS attacks. The **All-DoS-Shield** profile is applied when a DoS-only solution is required. Note that if the DoS Shield Radware -defined profile is applied, you cannot apply other Signature profiles in the same security policy.

To prevent denial of service, DoS Shield samples traffic flowing through the device and limits the bandwidth of traffic recognized as a DoS attack with predefined actions.

Most networks can tolerate sporadic attacks that consume negligible amounts of bandwidth. Such attacks do not require any counteraction. An attack becomes a threat to the network when it starts to consume large amounts of the network's bandwidth. DoS Shield detects such events using an advanced sampling algorithm for optimized performance, acting automatically to solve the problem.

The DoS Shield considers two protection states:

- **Dormant state**–Indicates that Sampling mechanism is used for recognition prior to active intervention. A protection in Dormant state becomes active only if the number of packets entering the network exceeds the predefined limit.
- **Active state**–Indicates that the action is implemented on each packet matching the attack signature, without sampling.

DoS Shield counts packets matching Dormant and Active states. In the Dormant state, DoSShield compares samples of the traffic with the list of protections. When a specified number of packets is reached, the state of the protection changes to Active.

The DoS Shield module uses two processes working in parallel. One process statistically monitors traffic to check if any dormant protection has become active. Then, when DoS Shield detects the protection as active, the module compares each packet that passes through the device to the list of *Currently Active Protections*. The module compares some of the packets that do not match the Active signature with the Dormant protections list. The module forwards the rest of the packets to the network without inspection.

To configure DoS Shield protection

1. In the *Configuration* perspective, select **Setup > Security Settings > Signature Protection> DoS Shield**.
2. Configure the parameters, and then, click **Submit**.

Table 60: DoS Shield Parameters

Parameter	Description
Enable DoS Shield	Specifies whether the DoS Shield feature is enabled. **Note:** If the protection is disabled, enable it before configuring the protection profiles.
Sampling Frequency	How often, in seconds, DoS Shield compares the predefined thresholds for each dormant attack to the current value of packet counters matching the attack. Values: 1–15 Default: 5 **Note:** If the sampling time is very short, there are frequent comparisons of counters to thresholds, so regular traffic bursts might be considered attacks. If the sampling time is too long, the DoS Shield mechanism cannot detect real attacks quickly enough.
Sampling Rate	The packet-sampling rate. For example, if the specified value is 5001, the DoS Shield mechanism checks 1 out of 5001 packets. Values: 1–50,000 Default: 5001

To include DoS Shield protection in the Protection policy

> In the *Configuration* perspective, select **Protections > Protection Policies >** **(Add) > Action > Signature Protection Profile > All-DoS-Shield**.
>
> For more information, see Managing Protection Policies, page 159.

Configuring Global SYN Flood Protection

A SYN-flood attack is usually aimed at specific *servers* with the intention of consuming the server's resources. However, you configure SYN Flood Protection as a *network* Protection to allow easier protection of multiple network elements.

Before you configure SYN profiles for the Protection policy, ensure that SYN Flood Protection is enabled and the SYN Flood Protection global parameters are configured.

Note: Some Radware DefensePro DDoS Mitigation versions have all the global SYN Flood Protection parameters on the *SYN Flood Protection* pane.

To configure global SYN Flood Protection

1. In the *Configuration* perspective, select **Setup > Security Settings > SYN FloodProtection**.
2. Configure the parameters, and then, click **Submit**.

Table 61: SYN Flood Protection Parameters: Advanced Parameters

Parameter	Description
Enable SYN Flood Protection	Specifies whether SYN Flood Protection is enabled on the device. Default: Enabled **Caution:** Changing the setting of this parameter requires a reboot to take effect.
Tracking Time	The time, in seconds, during which the number of SYN packets directed to a single protected destination must be lower than the Termination Threshold to cause the attack state to terminate for that destination. Values: 1–10 Default: 5

Configuring Global Packet Anomaly Protection

This feature is *not* supported on management interfaces.

Packet Anomaly Protection detects and provides protection against packet anomalies.

Note: The Packet Anomaly Protection module inspects traffic before the BDoS Protection module. Therefore, the BDoS Protection module is unaware of anomalous packets that the Packet Anomaly module detects and drops (when the specified **Action** is **Drop**) or passes through (when the specified **Report Action** is **Bypass**). For more information on the **Action** and **Report Action** parameters, see Table 62 - Packet-

Anomaly Protection Parameters, page 135.

Configuring Packet Anomaly Protection

Use the following procedure to configure Packet Anomaly Protection.

To configure Packet Anomaly Protection

1. In the *Configuration* perspective, select **Setup > Security Settings > PacketAnomaly**.
2. Double-click the relevant row.
3. Configure the parameters, and then, click **Submit**.

   For more information about these parameters and their default configurations, see Table 62 - Packet-Anomaly Protection Parameters, page 135.

Table 62: Packet-Anomaly Protection Parameters

Parameter	Description
ID	(Read-only) The ID number for the packet-anomaly protection. The ID is appears in the trap sent to APSolute Vision Security logs.
Protection Name	(Read-only) The name of the packet-anomaly protection.
Action	The action that the device takes when the packet anomaly is detected. The action is only for the specified packet-anomaly protection. Values: • Drop–The device discards the anomalous packets and issues a trap. • Report–The device issues a trap for anomalous packets. If the **Report Action** is **Process**, the packet goes to the rest of the device modules. If the **Report Action** is **Bypass**, the packet bypasses the rest of the device modules. • No Report–The device issues no trap for anomalous packets. If the **Report Action** is **Process**, the packet goes to the rest of the device modules. If the **Report Action** is **Bypass**, the packet bypasses the rest of the device modules. **Note:** Click **Drop All** to set the **Action** for all packet-anomaly protections to **Drop**. Click **Report All** to set the **Action** for all packet-anomaly protections to **Report**. Click **No Report All** to set the **Action** for all packet-anomaly protections to **No Report**.

Table 62: Packet-Anomaly Protection Parameters (cont.)

Parameter	Description
Report Action	The action that the Radware DefensePro DDoS Mitigation device takes on the anomalous packets when the specified **Action** is **Report** or **No Report**. The **Report Action** option is only for the specified packet- anomaly protection. Values: • Bypass–The anomalous packets bypass the device. • Process–The Radware DefensePro DDoS Mitigation modules process the anomalous packets. If the anomalous packets are part of an attack, Radware DefensePro DDoS Mitigation can mitigate the attack. **Note:** You cannot select **Process** for the following packet-anomaly protections: • 100–Unrecognized L2 Format • 104–Invalid IP Header or Total Length • 107–Inconsistent IPv6 Headers • 126–Incorrect GRE Version • 128–Invalid GRE Header • 131–Invalid L4 Header Length
Risk	The risk associated with the trap for the packet-anomaly protection. Values: Info, Low, Medium, High Default: Low

Table 63: Packet-Anomaly Protections

Anomaly	Description
Invalid IPv4 Header or Total Length	This packet-anomaly protection matches packets that fulfill any of the following criteria: • The IP packet header length does not match the actual header length. • The IP packet total length does not match the actual packet length. ID: 104 Default **Action**: Drop Default **Risk**: Low **Report Action**: Bypass[1]
TTL Equal to 0	This packet-anomaly protection matches packets whose fulfill TTL field value is equal to 0. ID: 105 Default **Action**: Report Default **Risk**: Low Default **Report Action**: Process

Table 63: Packet-Anomaly Protections (cont.)

Anomaly	Description
Inconsistent IPv6 Headers	This packet-anomaly protection matches packets with inconsistent IPv6 headers. ID: 107 Default **Action**: Drop Default **Risk**: Low **Report Action**: Bypass[1]
IPv6 Hop Limit Reached	This packet-anomaly protection matches packets whose IPv6 hop limit is not be greater than 1. ID: 108 Default **Action**: Report Default **Risk**: Low Default **Report Action**: Process
Unsupported L4 Protocol	This packet-anomaly protection matches traffic other than UDP, TCP, ICMP, or IGMP. ID: 110 Default **Action**: No Report Default **Risk**: Low Default **Report Action**: Process
Invalid TCP Flags	This packet-anomaly protection matches packets whose TCP flags combination is not according to the standard. ID: 113 Default **Action**: Drop Default **Risk**: Low Default **Report Action**: Bypass
Source or Dest. Address same as Local Host	This packet-anomaly protection matches packets whose IP packet source address or destination address is equal to the local host. ID: 119 Default **Action**: Drop Default **Risk**: Low Default **Report Action**: Bypass
Source Address same as Dest Address (Land Attack)	This packet-anomaly protection matches packets whose source IP address and the destination IP address in the packet header are the same. This is referred to as a LAND, Land, or LanD attack. ID: 120 Default **Action**: Drop Default **Risk**: Low Default **Report Action**: Bypass

Table 63: Packet-Anomaly Protections (cont.)

Anomaly	Description
L4 Source or Dest. Port Zero	This packet-anomaly protection matches packets whose Layer 4 source port or destination port equals zero. ID: 125 Default **Action**: Drop Default **Risk**: Low Default **Report Action**: Bypass
Incorrect GRE Version	This packet-anomaly protection matches packets whose GRE version is not 0 or 1. ID: 126 Default **Action**: Report Default **Risk**: Low **Report Action**: Bypass[1]
Invalid GRE Header	This packet-anomaly protection matches packets that fulfill any of the following criteria: • One or more flags are not RFC compliant, that is: — If version ID is 0, bit 8–12 are not 0. — If version ID is 1, bit 9–12 are not 0. • Partial or sliced packets—that is, any of the following: — The GRE header size is less than the minimum (four bytes). — If version ID is 0, the GRE header length is not in accordance with the optional bits (0–3). — If version ID is 1, the GRE header length is not in accordance with the optional bits (0–3 and 8). — The SRE header length is improper. ID: 128 Default **Action**: Report Default **Risk**: Low **Report Action**: Bypass[1]
Invalid L4 Header Length	This packet-anomaly protection matches packets with an invalid Layer 4 TCP/UDP/SCTP header length. ID: 131 Default **Action**: Drop Default **Risk**: Low **Report Action**: Bypass[1]

1 – You cannot select **Process** for this packet-anomaly protection.

Configuring the Advanced-Parameters Setup

This section contains the following topic: Configuring Radware DefensePro DDoS Mitigation Session Table Settings, page 139.

Configuring Radware DefensePro DDoS Mitigation Session Table Settings

Radware DefensePro DDoS Mitigation includes a *Session* table, which tracks sessions that Radware DefensePro DDoS Mitigation bridges and forwards.

Note: There is one Session table for each core.

To configure Session table settings

1. In the *Configuration* perspective, select **Setup > Advanced Parameters > SessionTable Settings**.
2. Configure the parameters, and then, click **Submit**.

Table 64: Session Table: Session Aging Parameters

Parameter	Description
Idle TCP-Session Aging Time	The time, in seconds, that the Session table keeps idle TCP sessions. Values: 1-7200 Default: 100
Idle UDP-Session Aging Time	The time, in seconds, that the Session table keeps idle UDP sessions. Values: 1-7200 Default: 100
Idle SCTP-Session Aging Time	The time, in seconds, that the Session table keeps idle SCTP sessions. Values: 1-7200 Default: 100
Idle ICMP-Session Aging Time	The time, in seconds, that the Session table keeps idle ICMP sessions. Values: 1-7200 Default: 100
Idle GRE-Session Aging Time	The time, in seconds, that the Session table keeps idle GRE sessions. Values: 1-7200 Default: 100

Table 64: Session Table: Session Aging Parameters (cont.)

Parameter	Description
Idle Other-Protocol-Session Aging Time	The time, in seconds, that the Session table keeps idle sessions of protocols other than TCP, UDP, SCTP, ICMP, or GRE. Values: 1-7200 Default: 100
Non-Established-Session Aging Time	How long, in seconds, the device waits for the session to be *established*. When the aging time elapses, the device deletes the session. Radware DefensePro DDoS Mitigation considers a session to be established after the three-way handshake completes–and, depending on the configuration, if data is sent after the TCP handshake (see **Consider Session Established Only If Data Sent After TCP Handshake**). Values: • 0–When SYN Flood Protection is disabled and you specify **0**, the device ages sessions TCP sessions immediately. Zero (**0**) is a valid value only when SYN Flood Protection is disabled (that is, when the **Enable SYN Flood Protection** checkbox is cleared). • 1-10 Default: 10 **Note:** The device can send a TCP Reset (RST) packet to the destination when the timeout elapses. For more information, see the *Advanced Parameters* tab.

Table 65: Session Table: Advanced Parameters

Parameter	Description
Session Establishment	
Consider Session Established Only If Data Sent After TCP Handshake	Specifies whether the device considers a session to be incomplete when– after the three-way handshake–there is no data sent in the session, within the specified **Non-Established- Session Aging Time** (see the *Session Aging Parameters* tab). Default: Enabled
Send Reset to Destination of Aged Unestablished Sessions	Specifies whether the device sends a TCP Reset (RST) packet to the destination of aged, unestablished sessions. Radware DefensePro DDoS Mitigation considers an incomplete session to be a session whose three-way handshake did not complete after the specified **Non-Established-Session Aging Time** (see the *Session Aging Parameters* tab). Default: Disabled **Caution:** This feature does *not* work on sessions that use any tunneling protocol (such as GRE, GTP, L2TP, and IPinIP).

Table 65: Session Table: Advanced Parameters (cont.)

Parameter	Description
At Session End	
Remove Session Entry at Session End	Specifies whether the device removes sessions from the Session table after receiving a FIN or RST packet if no additional packets are received on the same session within the *Remove Session Entry at Session End Timeout* period. Default: Enabled
Remove Session Entry at Session End Timeout (This parameter is available only if **Remove Session Entry at Session End** is enabled.)	When **Remove Session Entry at Session End** is enabled, the time, in seconds, after which the device removes sessions from the Session table after receiving a FIN or RST packet if no additional packets are received on the same session. Values: 0–60 Default: 5
Session Table Full	
Session-Table-Full Action	The action that the device takes when the Session table is at full capacity. Values: • Allow new traffic—New sessions bypass the device until the Session table has room for new entries. • Block new traffic—The device blocks new sessions until the Session table has room for new entries. Default: Allow new traffic
Alert-Start Threshold	The percentage of capacity of the Session table when the device starts issuing alerts. Default: 95
Alert-Stop Threshold	The percentage of full capacity of the Session table when the device stops issuing alerts. Default: 90

Configuring Radware DefensePro DDoS Mitigation Suspend Table Settings

Various Radware DefensePro DDoS Mitigation security modules can suspend (that is, *block*) traffic from an attack source for a defined period of time. The *Suspend table* stores the entries that define the suspended traffic.

Note: In the Connection Limit module, the specified **Suspend Action** parameter determines the traffic that Radware DefensePro DDoS Mitigation suspends. For more information on the **Suspend Action** parameter, see Configuring Connection Limit Protections, page 183.

If, within 60 seconds after the end of a suspension period, Radware DefensePro DDoS Mitigation suspends the same traffic, the suspension period increases. Each additional time that Radware DefensePro DDoS Mitigation suspends the same traffic, the suspension period increases until it reaches the specified maximum period.

When the suspension period reaches the specified maximum period, the period remains constant for each additional suspension.

To configure Suspend-table parameters

1. In the *Configuration* perspective, select **Setup > Advanced Parameters > Suspend Table Settings**.
2. Configure the parameters, and then, click **Submit**.

Table 66: Suspend Table Parameters

Parameter	Description
Minimum Aging Period	The time, in seconds, the *first time* that Radware DefensePro DDoS Mitigation suspends the traffic that the **Suspend Action** value defines. Default: 10 **Note:** Each *subsequent* time that Radware DefensePro DDoS Mitigation suspends the same traffic, the suspension period doubles.
Maximum Aging Period	The maximal time, in seconds, for which Radware DefensePro DDoS Mitigation suspends traffic that the **Suspend Action** value defines. Default: 600 **Note:** Each time Radware DefensePro DDoS Mitigation suspends the same traffic, the suspension period doubles until it reaches the **Maximum Aging Period**.

Configuring CPU-Load Alerts Parameters

Use the following procedure to configure the settings for issuing the following *device-health-event* messages:

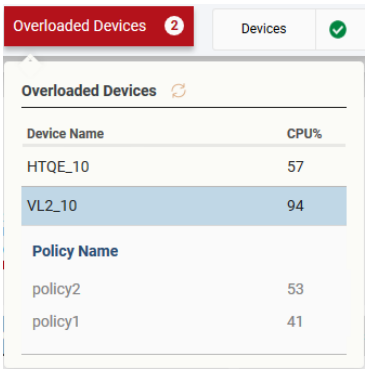
- **Device CPU load alerts**–That is, high utilization of the Radware DefensePro DDoS Mitigation flow-engine CPUs, referred to as *CPU Overload*. The mechanism polls the utilization of all the flow-engine CPUs every five seconds and uses the *average*. The information in thesemessages is broken down according to Protection policy. This information is especially useful for service providers. In attack scenarios or peacetime scenarios, service providers can take measures to avoid impacting *many* customers when the Protection policies of only *certain* customers are consuming inordinate CPU resources.
- **Controller CPU load alerts** –That is, high utilization of the Radware DefensePro DDoS Mitigation *controller CPU*. High CPU utilization (load) may lead to a degradation of the service in your network.
- **Flow-engine CPU load alerts**–That is, high utilization of single Radware DefensePro DDoS Mitigation *flow-engine CPUs*. High CPU utilization (load) may lead to a degradation of the service in your network.

Notes

- Radware DefensePro DDoS Mitigation issues *device-health-event* messages as SNMP traps and syslog messages. The configuration of each syslog server includes the **Device-Health Events** checkbox, which determines whether Radware DefensePro DDoS Mitigation sends messages for device-health events. For more information, see Configuring Radware DefensePro DDoS Mitigation Syslog Settings, page 146.

- Radware DefensePro DDoS Mitigation sends *CPU Overload* messages to *APSolute Vision Analytics* (AVA) AMS, where the toolbar of the *Radware DefensePro DDoS Mitigation Monitoring* dashboard displays the **Overloaded Devices** indicator. If there is a *CPU Overload* happening currently, the indicator is red, and you can click on it to view more information in a drop-down table. The table shows devices sending *CPU Overload* messages and the Protection policies (up to five) that are consuming the most CPU resources. For more information, see the *APSolute Vision Analytics User Guide*.

Figure 34: Overloaded Devices Indicator on the Radware DefensePro DDoS Mitigation Monitoring Dashboard



- You can monitor the current information for *controller CPU load alerts* and *flow-engine CPU load alerts* in the Radware DefensePro DDoS Mitigation *Monitoring* perspective. The **Cores** parameter (*Monitoring* perspective, **Operational Status > Overview > Hardware**) displays the number of flow-engine CPUs/cores in the device. The *CPU Utilization* pane includes controller-utilization and flow-engine–utilization, parameters (*Monitoring* perspective, **Operational Status > Resource Utilization > CPU Utilization**). Additionally, you can monitor information relating to the syslog mechanism (*Monitoring* perspective, select **Operational Status > Resource Utilization > Syslog Monitor**).

To configure CPU-load alerts parameters

1. In the *Configuration* perspective, select **Setup > Advanced Parameters > CPULoad Settings**.
2. Configure the parameters, and then, click **Submit**.

Table 67: CPU-Load Alert Parameters

Parameter	Description
Device CPU Load-Alert Thresholds	
CPU Overload Activation Threshold	The utilization percentage of the Radware DefensePro DDoS Mitigation CPUs–after rising to this level for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation starts issuing *CPU Overload* messages. Radware DefensePro DDoS Mitigation issues the first three *CPU Overload* messages at five-second intervals. Radware DefensePro DDoS Mitigation issues the subsequent *CPU overload* messages at 120- second intervals. Values: 50–98 Default: 95 **Note:** Radware DefensePro DDoS Mitigation sends *CPU overload* messages to *APSolute Vision Analytics* (AVA) AMS, where the toolbar of the *Radware DefensePro DDoS Mitigation Monitoring* dashboard displays the **Overloaded Devices** indicator with the related information.
CPU Overload Termination Threshold	The utilization percentage of the Radware DefensePro DDoS Mitigation CPUs–after dropping to this level or below for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation issues one *CPU Overload* message. Example message: INFO Device CPU Overload terminated. Overall CPU utilization: 46% (termination threshold: 50%). Values: 50–98 Default: 75
Enable CPU Load Alerts	Specifies whether Radware DefensePro DDoS Mitigation issues SNMP traps and syslog messages for high utilization of the *controller* CPU and/or for high utilization of *flow-engine* CPUs. Default: Disabled
Controller CPU Load-Alert Thresholds	
Load Error-Start Threshold	The utilization percentage of the controller CPU–after rising to this level for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation starts issuing *device-health-event* messages. Radware DefensePro DDoS Mitigation issues these messages at 60-second intervals, as long as the CPU utilization value does not go below the error-start threshold for at least five consecutive seconds. Values: 0–100 Default: 90
Load Warning-Start Threshold	The utilization percentage of the controller CPU–after rising to this level for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation issues one *device-health-event* message. Values: 0–100 Default: 80

Table 67: CPU-Load Alert Parameters (cont.)

Parameter	Description
Load Error-Stop Threshold	The utilization percentage of the controller CPU–after dropping to this level or below for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation issues one *device- health-event* message. Example message: Controller utilization has decreased to 85%. (The specified error alert-stop threshold is 85%.) Values: 0–100 Default: 85
Load Warning-Stop Threshold	The utilization percentage of the controller CPU–after dropping to this level or below for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation issues one *device- health-event* message. The message states that the CPU utilization is no longer at the *Warning* status. Values: 0–100 Default: 75
Flow Engines CPU Load-Alert Thresholds	
Load Error-Start Threshold	The utilization percentage of the flow-engine CPUs–after rising to this level for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation starts issuing *device- health-event* messages. Radware DefensePro DDoS Mitigation issues these messages at 60-second intervals, as long as the CPU utilization value does not go below the error-start threshold for at least five consecutive seconds. Values: 0–100 Default: 90
Load Warning-Start Threshold	The utilization percentage of the flow-engine CPUs–after rising to this level for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation issues one *device-health- event* message. Values: 0–100 Default: 80
Load Error-Stop Threshold	The utilization percentage of the flow-engine CPUs CPU–after dropping to this level or below for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation issues one *device-health-event* message. Example message: Flow Engine utilization has decreased to 85%. (The specified error alert-stop threshold is 85%.) Values: 0–100 Default: 85

Table 67: CPU-Load Alert Parameters (cont.)

Parameter	Description
Load Warning-Stop Threshold	The utilization percentage of the flow-engine CPUs–after dropping to this level or below for at least five consecutive seconds, at which Radware DefensePro DDoS Mitigation issues one *device-health-event* message. The message states that the CPU utilization is no longer at the *Warning* status. Values: 0–100 Default: 75

Configuring the Reporting-Settings Setup

This section contains the following topics:

- Configuring Radware DefensePro DDoS Mitigation Syslog Settings, page 146
- Enabling Configuration Auditing on the Radware DefensePro DDoS Mitigation Device, page 148
- Configuring Security Reporting Settings, page 148

Configuring Radware DefensePro DDoS Mitigation Syslog Settings

Radware DefensePro DDoS Mitigation can send event traps to up to five syslog servers. For each Radware DefensePro DDoS Mitigation instance, you can configure the relevant information.

Note: Instead of configuring each individual device, Cisco recommends configuring the APSolute Vision server to convey the syslog messages from all devices. For information about configuring syslog reporting on the APSolute Vision server, see the *APSolute Vision User Guide* or the APSolute Vision online help.

To configure syslog settings

1. In the *Configuration* perspective, select **Setup > Reporting Settings > Syslog**.
2. Do one of the following:
   - To enable the syslog feature, select the **Enable Syslog** checkbox.
   - To disable the syslog feature, clear the **Enable Syslog** checkbox.

   Default: Enabled
3. Do one of the following:
   - To add an entry, click the (Add) button.
   - To modify an entry, double-click the entry in the table.
4. Configure the parameters, and then, click **Submit**.

Table 68: Syslog Parameters

Parameter	Description
Enable Syslog Server	Specifies whether the syslog server is enabled. Default: Enabled **Note:** The device sends syslog messages using UDP. That is, the device sends syslog messages with no verification of message delivery. The *Status* is **N/R** in the Radware DefensePro DDoS Mitigation Syslog Monitor (*Monitoring* perspective, *Resource Utilization* pane > **Syslog Monitor**).
Syslog Server	The IP address or hostname of the device running the syslog service (syslogd).
Source Port	The syslog source port. Values: 1–65535 Default: 514
Destination Port	The syslog destination port. Values: 1–65535 Default: 514
Facility	The type of device of the sender. This is sent with syslog messages. You can use this parameter to distinguish between different devices and define rules that split messages. Values: • Authorization Messages • Clock Daemon • Clock Daemon2 • FTP Daemon • Kernel Messages • Line Printer Subsystem • Local Use 0 • Local Use 1 • Local Use 2 • Local Use 3 • Local Use 4 • Local Use 5 ▪ Local Use 6 ▪ Local Use 7 ▪ Log Alert ▪ Log Audit ▪ Mail System ▪ Network News Subsystem ▪ NTP Daemon ▪ Syslogd Messages ▪ System Daemons ▪ User Level Messages ▪ UUCP Default: Local Use 6
Report the Following Event Types	
Security Events	Specifies whether the device sends security-event messages to the syslog server. *Security events* include all events related to attack detection and mitigation: *start*, *ongoing*, *occurred*, *sampled*, and *terminated*. Default: Enabled
Device-Health Events	Specifies whether the device sends device-health-event messages to the syslog server. *Device-health events* include all events related to device health, for example, temperature, fan failure, CPU, tables, resources, and so on. Default: Enabled

Table 68: Syslog Parameters (cont.)

Parameter	Description
Configuration-Auditing Events	Specifies whether the device sends audit-event messages to the syslog server. *Audit events* include all events related to user operations, for example, login attempts and configuration changes. Default: Enabled

Enabling Configuration Auditing on the Radware DefensePro DDoS Mitigation Device

When configuration auditing for devices is enabled on the APSolute Vision server and on the device, any configuration change on a device using APSolute Vision creates two records in the Audit database, one from the APSolute Vision server, and one from the device audit message.

Note: To prevent overloading the managed device and prevent degraded performance, the feature is disabled by default.

To enable configuration auditing for a managed device

1. In the *Configuration* perspective, select**Setup > Advanced Parameters > Configuration Audit**.
2. Select the **Enable Configuration Auditing** checkbox, and click **Submit**.

Configuring Security Reporting Settings

To support historical and real-time security-monitoring capabilities and provide in-depth attack information for each attack event, Radware DefensePro DDoS Mitigation establishes a data-reporting protocol between the device and APSolute Vision. This protocol, called Statistical Real-time Protocol (SRP), uses UDP packets to send attack information.

You can enable the reporting channels used by Radware DefensePro DDoS Mitigation to receive information about attacks, and to report detected attacks based on their various risk levels.

You can also specify the minimal severity of the traps and syslog messages for device-health and audit events.

In addition, Radware DefensePro DDoS Mitigation can provide the APSolute Vision server sampled captured packets that were identified by the Radware DefensePro DDoS Mitigation device as part of the specific attack. Radware DefensePro DDoS Mitigation sends these packets to the specified IP address, encapsulated in UDP packets.

You can also configure Radware DefensePro DDoS Mitigation devices to send captured attack packets along with the attack event for further offline analysis. Packet reporting and SRP use the same default port, 2088.

Notes

- Radware DefensePro DDoS Mitigation does *not* provide sampled captured packets from suspicious sources that Radware DefensePro DDoS Mitigation challenged. (Radware DefensePro DDoS Mitigation supports an option to challenge sources in HTTPS Flood Protection, SYN Flood Protection, and DNS Flood Protection.)
- Radware DefensePro DDoS Mitigation does *not* provide sampled GRE-encapsulatedcaptured packets.
- When the **Enable Session Drop Mechanism** checkbox is not selected (see Configuring Global Signature Protection, page 132), captured HTTP-request packets from the Signature Protection module will not necessarily include the footprint. This is due to the fact that HTTP requests may comprise multiple packets, and Radware DefensePro DDoS Mitigation blocks only the last packet when the Session Drop Mechanism is *not* enabled.

To configure security reporting settings

1. In the *Configuration* perspective, select **Setup > Reporting Settings > Advanced Reporting Settings**.
2. Configure the parameters, and then, click **Submit**.

Table 69: Advanced Reporting Settings: Security Reporting Parameters

Parameter	Description
Report Interval	The frequency, in seconds, Radware DefensePro DDoS Mitigation sends reports though the reporting channels. Values: 1-65,535 Default: 5
Maximal Number of Alerts per Report	The maximum number of attack events that can appear in each report (sent within the reporting interval). Values: 1-2000 Default: 1000
Report per Attack Aggregation Threshold	The number of events for a specific attack during a reporting interval, before the events are aggregated to a report. When the number of the generated events exceeds the Aggregation Threshold value, the IP address value for the event is displayed as 0.0.0.0, which specifies *any IP address*. Values: 1-50 Default: 5
L4 Port for Reporting	The port used for packet reporting and SRP. Values: 1-65,535 Default: 2088
Enable Sending Traps	Specifies whether Radware DefensePro DDoS Mitigation uses the traps reporting channel. Default: Enabled
Minimal Risk Level for Sending Traps	The minimal risk level for the reporting channel. Attacks with the specified risk value or higher are reported. Default: Low

Table 69: Advanced Reporting Settings: Security Reporting Parameters(cont.)

Parameter	Description
Enable Sending Syslog	Specifies whether Radware DefensePro DDoS Mitigation uses the syslog reporting channel. Default: Enabled
Minimal Risk Level for Sending Syslog	The minimal risk level for the reporting channel. Attacks with the specified risk value or higher are reported. Default: Low
Enable Sending Terminal Echo	Specifies whether Radware DefensePro DDoS Mitigation uses the Terminal Echo reporting channel. Default: Disabled
Minimal Risk Level for Sending Terminal Echo	The minimal risk level for the reporting channel. Attacks with the specified risk value or higher are reported. Default: Low
Enable Security Logging	Specifies whether Radware DefensePro DDoS Mitigation uses the security logging reporting channel.

Table 70: Advanced Reporting: Packet Reporting and Packet Trace Parameters

Parameter	Description
Note: The parameters in this tab apply only to Packet Reporting. This version does not support the Packet Trace feature.	
Enable Packet Reporting	Specifies whether Radware DefensePro DDoS Mitigation sends sampled attack packets along with the attack event. Default: Enabled
Maximum Packets per Report	The maximum number of packets that the device can send within the Report Interval. Values: 1-65,535 Default: 100
Destination IP Address	The destination IP address for the packet reports. Default: 0.0.0.0 **Note:** Only one destination IP address can be configured for packet reporting, even when more than one APSolute Vision server manages the device.

Table 71: Advanced Reporting Settings: netForensics Parameters

Parameter	Description
Enable netForensics Reporting	Specifies whether Radware DefensePro DDoS Mitigation sends reports using the netForensics reporting agent. Default: Disabled
Agent IP Address	The IP address of the netForensics agent.
L4 Port	The port used for netForensics reporting. Values: 1-65,535 Default: 555

Table 72: Advanced Reporting Settings: Data Reporting Destinations Parameters

Parameter	Description
Destination IP Address	The target addresses for data reporting. The table can contain up to 10 addresses. By default, when there is room in the table, addresses are added automatically when you add a Radware DefensePro DDoS Mitigation device to the tree in the device pane. To add an address, click the (Add) button. Enter the destination IP address, and click **Submit**.

Configuring the Clustering Setup

Use the *Clustering* pane to configure clustering multiple Radware DefensePro DDoS Mitigation instances.

Clustering enables multiple Radware DefensePro DDoS Mitigation instances to support SYN Flood Protection among the cluster members.

Running several separate Radware DefensePro DDoS Mitigation instances on the same virtual platform, each instance configured with the same protections and networks, enables increasing the protection capacity of a protected network. The internal switch of the virtual platform can share the traffic load among the instances. Each instance is configured separately and operates as a stand- alone instance. Thus, activating a protection on some or all instances, which are defined on the same protected network, enables load-sharing traffic among the instances (based on the switch's load-sharing mechanism), and thereby achieves increased device capacity.

Web-cookies authentication involves a challenge-response process where, per-instance, HTTP- session persistency is required. Since the load-sharing switch distributes traffic based on L4 parameters, HTTP-session persistency issues might occur. Multi-instance clustering enables verifying that web-cookies persistency is maintained among Radware DefensePro DDoS Mitigation instances on the same virtual platform. This is achieved by an internal mechanism, which uses one cluster instance, defined as the *cluster master*, to periodically synchronize cookies among the instances.

Note: For information on the installation of Radware DefensePro DDoS Mitigation for Cisco Firepower, see the related Cisco documentation.

To configure clustering

1. In the *Configuration* perspective, select **Setup > Advanced Parameters > Clustering**.
2. Configure the parameters, and then, click **Submit**.

Table 73: Clustering Parameters

Parameter	Description
Device-Management-Channel IP Address	(Read-only) The IP address of the management channel of the Radware DefensePro DDoS Mitigation instance.[1]
Device-Management-Channel Default Gateway	(Read-only) The default gateway of the device management channel.[1]

Table 73: Clustering Parameters (cont.)

Parameter	Description
Device-Management-Channel Netmask	(Read-only) The network mask of the device management channel.[1]
Cluster-Master IP Address	The IP address of the cluster master. That is, the IP address to which cluster members connect. For this Radware DefensePro DDoS Mitigation instance to be the cluster *master*, specify the value in the **Device-Management-Channel IP Address** field. For this Radware DefensePro DDoS Mitigation instance to be a cluster *member*, specify the **Device-Management-Channel IP Address** of the master Radware DefensePro DDoS Mitigation instance. **Caution:** You can change the value only when the **Cluster State** is **Disabled**, after you have clicked **Submit**.
Cluster State	The state of the cluster or cluster membership. Values: • Enabled–One of the following: — When this Radware DefensePro DDoS Mitigation instance is the master–Enables the cluster. — When this Radware DefensePro DDoS Mitigation instance is a cluster member–Joins the cluster. • Disabled–One of the following: — When this Radware DefensePro DDoS Mitigation instance is the master–Disables the cluster and breaks the relationship with the cluster. — When this Radware DefensePro DDoS Mitigation instance is a cluster member–Leaves the cluster. Default: Disabled

1 – In Radware DefensePro DDoS Mitigation for Cisco Firepower, the Firepower bootstrap XML file defines this value. The Radware DefensePro DDoS Mitigation instance reads the bootstrap XML file every time that it initializes.

CHAPTER 4 – MANAGING CLASSES

Classes define groups of elements of the same type of entity in Radware DefensePro DDoS Mitigation.

This chapter contains the following sections:

- Managing Network Classes, page 153
- Managing Context Group Classes, page 154
- Managing Application Classes, page 155
- Managing SGT Classes, page 156

You can configure classes based on the following:

- **Networks**–To classify traffic in a Protection policy.
- **Context Groups**–To classify traffic in a Protection policy or in a Traffic Filter.
- **Application ports**–To define or modify applications based on Layer 4 destination ports.
- **SGTs** –To configure the Security Group Tags(SGTs).

After you create or modify a class, the configuration is saved in the APSolute Vision database. You must activate the configuration to download it to the device. You can also view the current class configurations on your device. After creation, you cannot modify the name of a class, or the configuration of application classes.

Managing Network Classes

In Radware DefensePro DDoS Mitigation for Cisco Firepower, you can use Network classes in Protection policies to match source or destination traffic. A Network class is identified by a name and defined by a network address and IPv4 mask or IPv6 prefix.

Note: Radware DefensePro DDoS Mitigation always configures the following default Network classes, which you cannot modify or delete:

- **any**–Specifies any IPv4 or IPv6 network. IPv6 notation is displayed for the class.
- **any_ipv4**–Specifies any IPv4 network.

To configure a Network class

1. In the *Configuration* perspective, select **Classes > Networks**.
2. To add or modify a Network class, do one of the following:
   - To add a class, click the  (Add) button.
   - To edit a class, double-click the entry in the table.
3. Configure the Network class parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ().

Table 74: Network Class Parameters

Parameter	Description
Network Name	The name of the Network class. The network name is case-sensitive. The network name cannot be an IP address. Maximum characters: 19 **Caution:** If the name was configured in a user interface other than APSolute Vision, and the name includes any leading or trailing spaces, APSolute Vision displays this text box *empty*. If the name was configured in a user interface other than APSolute Vision, and the name includes more than one space within the name, APSolute Vision displays the *multiple* spaces as *one* space.
Entry Type	Specifies whether the network is defined by a subnet and mask, or by an IP range. Value: IP Mask
Network Type	Values: IPv4, IPv6
Network Address	The network address.
Prefix	The mask of the subnet, which you can enter in either of the following ways: • A subnet mask in dotted decimal notation–for example, 255.0.0.0or 255.255.0.0. • An IP prefix, that is, the number of mask bits–for example, 8or 16. **Caution:** When a Network class contains no mask, the Radware DefensePro DDoS Mitigation CLI always displays IPv6 notation for the class.

Managing Context Group Classes

You can define network segments using Context Group classes. Use them to classify traffic in security policies or Traffic Filters.

Each Radware DefensePro DDoS Mitigation instance supports a maximum 64 Context Group classes. Each Context Group class can contain a maximum 32 discrete tags and 32 ranges. That is, in effect, each Radware DefensePro DDoS Mitigation device supports up to 64^2 definitions.

Caution: If you use a Context Group class in a Traffic Filter (see Configuring Traffic Filters Profiles, page 242), the Context Group class can represent a maximum of 50 Context tags.

To configure a Context Group class

1. In the *Configuration* perspective, select **Classes > Context Groups**.
2. Do one of the following:
   - To add an entry, click the (Add) button.
   - To edit an entry, double-click the entry in the table.

3. Configure the parameters, and then, click **Submit**.

4. To activate your configuration changes on the device, click **Update Policies** ().

Table 75: Context Groups Class Parameters

Parameter	Description
Context Group Name	The name of the group. Maximum characters: 19 **Caution:** If the name was configured in a user interface other than APSolute Vision, and the name includes any leading or trailing spaces, APSolute Vision displays this text box *empty*. If the name was configured in a user interface other than APSolute Vision, and the name includes more than one space within the name, APSolute Vision displays the *multiple* spaces as *one* space.
Group Mode	Values: • Discrete—An individual Context Group, as defined in the interface parameters of the device. • Range—A group of sequential Context Group numbers, as defined in the interface parameters of the device. Default: Discrete
Tag (This parameter is available only for the **Discrete** mode.)	The Context Group number. Values: 0–4095
Range From (This parameter is available only for the **Range** mode.)	The first Context Group in the range. Values: 0–4095 **Note:** You cannot modify the value after creating the Context Group.
Range To (This parameter is available only for the **Range** mode.)	The last Context Group in the range. Values: 0–4095

Managing Application Classes

Application classes are groups of Layer-4 ports for UDP and TCP traffic. Each class is identified by its unique name, and you can define multiple Layer-4 ports in a single class. You cannot modify the predefined (**System Defined**) application classes for standard applications; however, you can add entries for the class. You can add and modify user-defined (**User Defined**) classes to the *Application Port Group* table.

Note: In some (legacy) Radware DefensePro DDoS Mitigation versions, the CLI refers to **System Defined** entries as **static**, and **User Defined** entries as **regular**.

To configure an application class

1. In the *Configuration* perspective, select **Classes > Applications**.
2. Do one of the following:
   - To add a class entry, click the (Add) button.
   - To edit a class, double-click the entry in the table.
3. Configure the application class parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ( ).

Table 76: Application Class Parameters

Parameter	Description
Ports Group Name	The name of the Application Port Group. To associate a number of ranges with the same port group, use the same name for all the ranges that you want to include in the group. Each range appears as a separate row with the same name in the Application Port Group table. **Caution:** If the name was configured in a user interface other than APSolute Vision, and the name includes any leading or trailing spaces, APSolute Vision displays this text box *empty*. If the name was configured in a user interface other than APSolute Vision, and the name includes more than one space within the name, APSolute Vision displays the *multiple* spaces as *one* space.
Type of Entry	(Read-only) Values: System Defined, User Defined
From L4 Port	The first port in the range.
To L4 Port	The last port in the range. To define a group with a single port, set the same value for the **From L4 Port** and **To L4 Port** parameters.

Managing SGT Classes

Each Radware DefensePro DDoS Mitigation can have zero or one enabled Security Group Tag (SGT).

When the SYN Flood Protection module receives a packet to challenge, and the packet includes an SGT, Radware DefensePro DDoS Mitigation replaces the SGT in the packet with the SGT that is enabled in the Radware DefensePro DDoS Mitigation configuration. When Radware DefensePro DDoS Mitigation has *no* enabled SGT or a packet to challenge includes *no* SGT, Radware DefensePro DDoS Mitigation challenges the packet as is.

Notes

- Each Radware DefensePro DDoS Mitigation supports up to 16 SGTs.
- Only one SGT value can be enabled at any given time.
- A change to the status of the SGT (enabled/disabled), requires the Update Policies action to take effect.

To configure an SGT

1. In the *Configuration* perspective, select **Classes > SGTs**.
2. Do one of the following:
   - To add an entry, click the (Add) button.
   - To edit an entry, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ( ).

Table 77: SGT Class Parameters

Parameter	Description
Name	The name of the SGT. Maximum characters: 20 **Caution:** If the name was configured in a user interface other than APSolute Vision, and the name includes any leading or trailing spaces, APSolute Vision displays this text box *empty*. If the name was configured in a user interface other than APSolute Vision, and the name includes more than one space within the name, APSolute Vision displays the *multiple* spaces as *one* space.
Value	The numerical SGT value. Values: 0–65534 Default: 0
Status	Values: Enabled, Disabled Default: Disabled **Note:** If there is an enabled SGT value in the Radware DefensePro DDoS Mitigation configuration, if you enable another, Radware DefensePro DDoS Mitigation automatically disables the previously enabled one, and issues an appropriate message.

CHAPTER 5 – MANAGING PROTECTION POLICIES

Protection *policies* protect your configured networks using *protection profiles*. Each Protection policy uses one or more protection profiles that are applied on a predefined network segment. Each Protection includes the action to take when an attack is detected.

Before you configure Protection policies and profiles, ensure that you have enabled all the required protections and configured the corresponding global protection parameters under **Setup > Security Settings**.

The following table describes protections that Radware DefensePro DDoS Mitigation supports. The set of supported protections depends on the Radware DefensePro DDoS Mitigation version and platform.

Table 78: Radware DefensePro DDoS Mitigation Protection Types

Protection	Description
Anti-Scanning	Prevents zero-day self-propagating network worms, horizontal scans, and vertical scans. For more information, see Configuring Anti-Scanning Protection Profiles, page 168.
Behavioral DoS (BDoS)	Protects against zero-day DoS/DDoS-flood attacks. For more information, see Configuring BDoS Profiles, page 172.
Connection Limit	Protects against connection-flood attacks. For more information, see Configuring Connection Limit Profiles, page 181.
Connection PPS	Protects against DoS attacks that use a high PPS rate in a certain connection. For more information, see Configuring Connection PPS Profiles, page 185.
DNS Flood Protection	Protects against zero-day DNS-flood attacks and can also detect various types of recursive attacks. For more information, see Configuring DNS Flood Protection Profiles, page 187.
ERT Active Attackers Feed	Uses the ERT Active Attackers Feed subscription service to identify and block IP addresses actively involved in major attacks in real-time to provide preemptive protection from known attackers. For more information, see Configuring ERT Active Attackers Feed Profiles, page 195.
Geolocation	Permanently blocks all traffic from selected geolocations. The Geolocation feature uses the subscription Geolocation Feed to identify the source geolocation of the traffic. For more information, see Configuring Geolocation Profiles, page 198. **Note:** If you have an *APSolute Vision Analytics - AMS* license installed on the APSolute Vision server, you can block traffic from selected geolocations for a selected duration—for example, 24 hours.

Table 78: Radware DefensePro DDoS Mitigation Protection Types (cont.)

Protection	Description
HTTPS Flood Protection	Protects against HTTPS-flood attacks. For more information, see Configuring HTTPS Flood Protection Profiles, page 201.
Out-of-State Protection	Detects out-of-state packets to provide additional protection for TCP-session-based attacks. For more information, see Configuring Out-of-State Protection Profiles, page 205.
Signature Protection	Signature Protection includes two mechanisms: *DoS Shield* and *Application Security*. DoS Shield protects against known flood attacks and flood-attack tools that can also cause a denial-of-service effect. Application Security prevents known application vulnerabilities and exploitation attempts, and protects against known DoS/DDoS flood attacks. For more information, see Configuring Signature Protection, page 207.
SYN Flood Protection	Protects against SYN-flood attacks using SYN cookies. For more information, see Configuring SYN Flood Protection Profiles, page 232.
Traffic Filters	Provides control over mitigation or processing of traffic by means of filtering or rate-limiting capabilities. For more information, see Configuring Traffic Filters Profiles, page 242.

Configuring Protection Policies

Each Protection policy consists of the following two parts:

- The classification that defines the protected network segment.

  Note: The classification includes the source and destination configuration, which defines the inbound traffic and outbound traffic. If the packet data matches the source-to-destination configuration, Radware DefensePro DDoS Mitigation considers the packet to be *inbound*. If the packet data matches the destination-to-source configuration, Radware DefensePro DDoS Mitigation considers the packet to be *outbound*.

- The action that Radware DefensePro DDoS Mitigation applies when it detects an attack on the matching network segment. The action defines the protection profiles that Radware DefensePro DDoS Mitigation applies to the network segment, and whether to block the malicious traffic. Radware DefensePro DDoS Mitigation always *reports* malicious traffic.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Protection policies.

You can export, edit, and import policies. The information of an exported policy is referred to as a *template*. A template may also include baselines. For more information, see Using Configuration Templates for Security Policies, page 266.

Before you configure a policy, ensure that you have configured the following:

- The Classes that will be required to define the protected network segment. Formore information, see Managing Classes, page 153.

- The Protection profiles–for more information see:
  - Configuring Anti-Scanning Protection Profiles, page 168
  - Configuring BDoS Profiles, page 172
  - Configuring Connection Limit Profiles, page 181
  - Configuring Connection PPS Profiles, page 185
  - Configuring DNS Flood Protection Profiles, page 187
  - Configuring ERT Active Attackers Feed Profiles, page 195
  - Configuring Geolocation Profiles, page 198
  - Configuring HTTPS Flood Protection Profiles, page 201
  - Configuring Out-of-State Protection Profiles, page 205
  - Configuring Signature Protection, page 207
  - Configuring SYN Flood Protection Profiles, page 232
  - Configuring Traffic Filters Profiles, page 242

Caution: When you configure the policy, APSolute Vision stores your configuration changes, but it does not download your configuration changes to the device. To apply changes onto the device, you must activate the configuration changes. *Activating the latest changes* is also referred to as *Update Policies*.

Caution: When using the Radware DefensePro DDoS Mitigation SOAP interface, to remove a protection profile from a Protection policy, you must enter the value **none** for the profile.

To configure a Protection policy

1. In the *Configuration* perspective, select **Protection > Protection Policies**.
2. Do one of the following:
   - To add an entry, click the (Add) button.
   - To edit an entry in the table, double-click the entry.
3. Configure the Protection policy parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ( ).

Table 79: Protection Policy: General Parameters

Parameter	Description
Enabled	Specifies whether the policy is enabled.

Table 79: Protection Policy: General Parameters (cont.)

Parameter	Description
Policy Name	The name of the Protection policy. Maximum characters: 64 **Caution:** The name must not include a comma (,). **Caution:** If the name was configured in a user interface other than APSolute Vision, and the name includes any leading or trailing spaces, APSolute Vision displays this text box *empty*. If the name was configured in a user interface other than APSolute Vision, and the name includes more than one space within the name, APSolute Vision displays the *multiple* spaces as *one* space.
Action	The default action for all attacks under this policy. Values: • Block and Report–The malicious traffic is terminated and a security event is generated and logged. • Report Only–The malicious traffic is forwarded to itsdestination and a security event is generated and logged. Default: Block and Report **Caution:** Generally, the **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in a particular profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in a particular profile, the action behavior of all the Protection policy is *block and report* except for that particular profile whose action behavior is *report only*. However, signature-specific actions override the **Action** for the policy. That is, any option that you specify for the *action parameter* in an enabled, associated *signature* always overrides the specified action in the policy. (The label of the *action parameter* may be **Action**, **Action Mode**, or **Profile Action** depending on the profile type.)

Table 80: Protection Policy: Classification Parameters

Parameter	Description
Priority	The unique priority of the Protection policy. The highest value is the highest priority. Radware DefensePro DDoS Mitigation processes each packet using *one* Protection policy. When there are multiple policies whose classification specification overlap, only the policy with the highest Priority processes the packet. Values: • 0–Specifies that Radware DefensePro DDoS Mitigation automatically sets the priority by adding 10 to the highest existing value. • 1-63,999 Default: 0 **Caution:** Radware DefensePro DDoS Mitigation uses the specified **Priority** for *all* actions. That is, the specified **Priority** takes precedence over all other Protection parameters. For example, if you configure multiple policies that include the same network addresses (sometimes referred to as *overlapping policies*), Radware DefensePro DDoS Mitigation performs all actions according to the specified **Priority**, even if the policies are configured for different directions. **Caution:** If a policy exists with a priority greater than or equal to 63,990, you cannot create a new policy using APSolute Vision.
SRC Network	The IP address or predefined class object that defines the source of the packets that the policy uses. To specify *any* network, the field may contain the value **any** or be empty.
DST Network	The IP address or predefined class object that defines the destination of the packets that the policy uses. To specify *any* network, the field may contain the value **any** or be empty.
Port Group	The Physical Port class or physical port that the policy uses. Values: • *A Physical Port class displayed in the Classes tab* • *The physical ports on the device* • None **Caution:** If you specify a management port or a Physical Port class with a management port, the Protection policy can support only Signature Protection and BDoS Protection.
Direction	The direction of the traffic to which the policy relates. Values: • One Way–The protection applies to sessions originating from sources to destinations that match the network definitions of the policy. • Two Way–The protection applies to sessions that match the network definitions of the policy regardless of their direction. Default: One Way

Table 80: Protection Policy: Classification Parameters (cont.)

Parameter	Description
Context	The Context Group class that the policy uses. Values: • *A Context Group class displayed in the Classes tab* • None

Table 81: Protection Policy: Profiles Parameters

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
Anti-Scanning Profile	The Anti-Scanning profile applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy.
Connection PPS Profile	The Connection PPS profile applied to the network segment defined in this policy.
DNS Flood Protection Profile	The DNS Flood Protection profile applied to the network segment defined in this policy.
ERT Active Attackers Feed Profile	The ERT Active Attackers Feed profile applied to the network segment defined in this policy.
Geolocation Profile	The Geolocation profile applied to the network segment defined in this policy.
HTTPS Flood Protection Profile	The HTTPS Flood Protection profile applied to the Protected SSL Objects within the network segment defined in this policy.
Out-of-State Profile	The Out-of-State Protection profile to apply to the network segment defined in this policy.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy.
SYN Flood Protection Profile	The SYN Flood Protection profile applied to the network segment defined in this policy.
Traffic Filters Profile	The Traffic Filters profile applied to the network segment defined in this policy.

Table 82: Protection Policy: CDN Handling Parameters

Parameter	Description
Policy Handles Traffic Received Through a CDN	Specifies whether the Protection policy handles traffic from a content delivery network (CDN) with special treatment at the Protection policy level. Radware DefensePro DDoS Mitigation uses the following criteria to determines what *traffic received through a CDN* is: • The **Action** in the Protection policy is **Block and Report**. • The packet is a TCP packet. • The packet is not the first packet in the session. • The selected **Signature Protection Profile** is an Application Security (AppSec) signature that includes the following: — An **Action** other than **Report Only**. — An entry in the *Attributes Table* whose **Attribute Type** is **Services** whose **Attribute Value** is **Web-HTTP**. **Note:** For more information on Signature Protection profiles, see Configuring Signature Protection, page 207.

Table 82: Protection Policy: CDN Handling Parameters (cont.)

Parameter	Description
Override Action	The action that Radware DefensePro DDoS Mitigation takes on *traffic received through a CDN*, overriding the specified **Action** in the selected **Signature Protection Profile**. The **Override Action** options (other than **No Override**) enable Radware DefensePro DDoS Mitigation to respond gracefully to the CDN, using a standard HTTP response. Radware DefensePro DDoSMitigation performs a legal termination of the connection over HTTP (including termination at the TCP level)—as opposed to a *Drop* or *Reset* at the TCP level. Using an **Override Action**, Radware DefensePro DDoS Mitigation can handle CDN traffic in such a way as to avoid caching in the CDN. For all the HTTP actions, Radware DefensePro DDoS Mitigation sends the Connection: Closeheader in the HTTP response. Values: ● No Override—Radware DefensePro DDoS Mitigation uses the **Action** that is specified in the Application Security (AppSec) signature. ● HTTP 200 OK—Radware DefensePro DDoS Mitigation sends a 200 OK response using an empty page and leaves the server-side connection open. ● HTTP 200 OK and Reset Destination—Radware DefensePro DDoS Mitigation sends a 200 OK response using an empty page and sends a TCP-Reset packet to the server side to close the connection. ● HTTP 403 Forbidden—Radware DefensePro DDoS Mitigation sends a 403 Forbidden response using an empty page and leaves the server-side connection open. ● HTTP 403 Forbidden and Reset Destination—Radware DefensePro DDoS Mitigation sends a 403 Forbidden response using an empty page and sends a TCP-Reset packet to the server side to closethe connection. Default: No Override **Note:** Signatures in the **Signature Protection Profile** selected in the Protection policy may be configured to drop the matching packets from the client or reset the destination. This causes a reset of the TCP connection to the *server* (not to the client). When HTTP connections (legitimate *or* non-legitimate) to a protected server come from a CDN proxy, the Radware DefensePro DDoS Mitigation Action should not be just *drop* or *destination reset*. A *drop* or *destination reset* **Action** will lead to a broken session between CDN and the server. After multiple retries, the CDN proxy may decide that the server is down and return responses from cache or stop serving the page altogether. Configuring the Protection policy with an *HTTP...* **Override Action** handles the issue, because instead of just dropping the packet, Radware DefensePro DDoS Mitigation sends an HTTP reply back to the client (CDN proxy) with the request to close the connection gracefully.

Table 83: Protection Policy: Associated Protected SSL Objects

Parameter	Description
	Radware DefensePro DDoS Mitigation displays the *Associated Protected SSL Objects* tab only after the Protection policy has been configured, and only when the **DST Network** (see DST Network, page 163) of the Protection policy includes the IP address of at least one enabled *Protected SSL Object* in a SYN Flood Protection profile or an HTTPS Flood Protection profile specified in the policy. The tab contains a read-only table with the following columns: • **Object Name**–The name of the Protected SSL Object. • **IP Address**–The IP address of the Protected SSL Object. • **Application Port**–The application port of the Protected SSL Object. • **Includes SSL Server Certificate**–Specifies whether the Protected SSL Object includes a valid SSL/TLS certificate. • **Applicable to SYN Protection**–When the selected option is **Enabled, Using the On-Device Component**, this field displays **Yes** when the Protection policy includes a SYN Flood Protection profile with SSL Mitigation enabled, and the Protected SSL Object includes a validcertificate. • **Applicable to HTTPS Flood Protection**–When the selected option is **Enabled, Using the On-Device Component**, this field displays **Yes** when the Protection policy includes an HTTPS Flood Protection profile that uses SSL Mitigation enabled, and the Protected SSL Object includes a valid certificate. **Notes:** • For more information on Protected SSL Objects, see Managing Protected SSL Objects, page 117. • For more information on SYN Flood Protection, see Configuring SYN Flood ProtectionProfiles, page 232. • For more information on HTTPS Flood Protection, see Configuring HTTPS Flood Protection Profiles, page 201.

Table 84: Protection Policy: Packet Reporting Parameters

Parameter	Description
Packet Reporting	Specifies whether the device sends sampled attack packets to APSolute Vision for offline analysis. Default: Disabled **Caution:** When this feature is enabled here, for the packet- reporting to take effect, the global setting must be enabled (*Configuration* perspective, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting > Enable Packet Reporting**).
Packet Reporting Configuration on Policy Takes Precedence	Specifies whether the configuration of the Packet Reporting feature here, on this policy, takes precedence over the configuration of the Packet Reporting feature in the associated profiles.

When deleting one or more Protection policies, you have two options: **Delete Policy Only**, and **Delete Policy and Related Elements**.

To delete one or more Protection policies

1. In the *Configuration* perspective, select **Protection > Protection Policies**.

2. Select the row or rows.

3. Click the  button, and select one of the following:
   - **Delete Policy Only**–Deletes the selected policy or policies, without the related objects.
   - **Delete Policy and Related Elements**–Deletes the selected policy or policies and all other policy-related configurations (Network Classes, Context Classes, profile definitions) as long as the other policies on the device are not using those objects.

Caution: When you select multiple rows and select **Delete Policy and Related Elements**, Radware DefensePro DDoS Mitigation performs an Update Policies action after each policy deletion. Therefore, it might take a long time for all the deletions to complete–depending on the number of selected rows and the complexity of the policies. You might not be able to perform any other actions until the whole deletion process is complete.

Configuring Anti-Scanning Protection Profiles

Anti-Scanning protects against malicious scanning activity.

For general information on Radware DefensePro DDoS Mitigation Anti-Scanning Protection, see Configuring Global Anti-Scanning Protection Settings, page 120.

You can configure up to 200 Anti-Scanning profiles on Radware DefensePro DDoS Mitigation 60, 110, 200, 220, and 400 devices–and up to 50 Anti-Scanning profiles on Radware DefensePro DDoS Mitigation 6 and 20 devices.

Note: You can configure an Anti-Scanning profile even when Anti-Scanning Protection is disabled (*Configuration* perspective, **Setup > Security Settings > Anti-Scanning**). For more information, see Configuring Global Anti-Scanning Protection Settings, page 120.

Caution: In some cases, you may find that network elements perform legitimate scans as part of their normal operation. To avoid interruption or network operation, you can configure a list of *whitelisted* IP addresses and a list of *whitelisted* Layer 4 ports on which the profile allows scanning. That is, when Anti-Scanning is configured and enabled, there is no blocking of scans that target these addresses or ports.

The following describes the recommended settings for Protection policies that include an Anti- Scanning profile:

- Configure a policy that contains an Anti-Scanning profile using networks with *source network= any*, that is, the public network–and *destination = protected network*. This ensures optimized attack-detection sensitivity. To facilitate this, you can configure policies using a Context Group or physical ports.
- Cisco recommends *not* to define a network in which the source and destination are set to*any*, because it results in lower detection sensitivity.
- When the **Direction** of a policy is set to **One Way**, Radware DefensePro DDoS Mitigation prevents incoming attacks only. When the **Direction** of a policy is set to **Two Way**, the device prevents both incoming and outgoing attacks. In either case, the device inspects incomingand outgoing traffic for connection scoring.

To configure an Anti-Scanning profile

1. In the *Configuration* perspective, select **Protection > Anti-Scanning Profiles**.
2. To add or modify an Anti-Scanning profile, do one of the following:
   - To add a profile, click the (Add) button.
   - To edit a profile, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 85: Anti-Scanning Profile–General Parameters

Parameter	Description
Profile Name	The name of the profile. Maximum characters: 29
TCP	Specifies whether the profile protects against horizontal and vertical TCP scans, including worm propagation activity, over TCP. Default: Enabled
UDP	Specifies whether the profile protects against horizontal and vertical UDP scans, including worm propagation activity, over UDP. Default: Disabled
ICMP	Specifies whether the profile protects against ping sweeps. Default: Disabled
Action	The action that the profile takes when it encounters malicious scanning. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.
Packet Reporting	Specifies whether the device sends sampled attack packets to APSolute Vision for offline analysis. Default: Disabled **Caution:** When this feature is enabled here, for the packet- reporting to take effect, the global setting must be enabled (*Configuration* perspective, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting > Enable Packet Reporting**).

Table 86: Anti-Scanning Profile–Whitelisted Source IP Addresses Parameters

Parameter	Description
To add a whitelisted source IP address, click the *Whitelisted Source IP Addresses* tab and click the (Add) button. After you have configured the parameters, click **Submit**.	
Profile Name	(Read-only) The name of the profile.
Address Type	The IP version of the address. Values: IPv4, IPv6 Default: IPv4
Source IP Address	The IP address on which the profile allows scanning.

Table 87: Anti-Scanning Profile–Whitelisted L4 Ports Parameters

Parameter	Description
To add a whitelisted L4 port, click the *Whitelisted L4 Ports* tab and click the (Add) button. After you have configured the parameters, click **Submit**. **Note:** The *Whitelisted L4 Ports* table can contain up to 50 entries.	
Profile Name	(Read-only) The name of the profile.
L4 Port Number	Values: 1-65,535
L4 Port Type	Values: Source, Destination, Source and Destination Default: Source and Destination
L4 Protocol	Values: TCP, UDP, TCP and UDP Default: TCP and UDP

Table 88: Anti-Scanning Profile–Advanced Parameters

Parameter	Description
Scanning Sensitivity Level	The level of sensitivity to scanning activities before the profile activates Anti-Scanning protection. The higher the sensitivity, the fewer scanning attempts (*probes*) to trigger the Anti-Scanning protection. The lower the sensitivity, the more scanning attempts (*probes*) to trigger the Anti-Scanning protection. Values: • Low • Medium • High • Very High • User-Defined Default: Medium **Note:** Choose a lower **Scanning Sensitivity Level** for scans with higher rates. Choose a higher **Scanning Sensitivity Level** for scans with lower rates.

Table 88: Anti-Scanning Profile–Advanced Parameters (cont.)

Parameter	Description
Number of Probes (This parameter is available only when the specified **Scanning Sensitivity Level** is **User- Defined**.)	The number of scanning attempts (*probes*) within the specified **Tracking Time** that triggers the Anti-Scanning protection. Values: 5–50,000 Default: 90
Tracking Time (This parameter is available only when the specified **Scanning Sensitivity Level** is **User- Defined**.)	The number of consecutive seconds with the specified **Number of Probes** per second that triggers the Anti-Scanning protection. Values: 1–2,400 (40 minutes) Default: 5
Bypass Connections Originating from System Ports to Non-System Ports	Specifies how the Anti-Scanning profile handles connections originating from system ports (ports numbered 1–1023) to non- system ports (port numbered 1024 and higher). Values: • Disable—The Anti-Scanning module inspects packets also from system ports to non-system ports (except for the whitelisted L4 ports). • TCP and UDP—All TCP packets and UDP packets from system ports to non-system ports bypass the Anti-Scanning module. • TCP—All TCP packets from system ports to non-system ports bypass the Anti-Scanning module. • UDP—All UDP packets from system ports to non-system ports bypass the Anti-Scanning module. Default: TCP and UDP
Increase the Sensitivity for Non-System Ports	Specifies whether Anti-Scanning profile emphasizes inspecting scans aimed at port numbers greater than 1023. Values: • Enabled—The Anti-Scanning profile emphasizes inspecting scans aimed at ports greater than 1023. Select this checkbox when using applications that utilize standard system ports (that is, port 1023 and lower). • Disabled—The Anti-Scanning profile treats all the scan activities equally. Clear this checkbox when using applications utilizing non-system ports (that is, port numbers greater than 1023). Default: Disabled **Notes:** • Port numbers greater than 1023 may be referred to as *high ports*. • When the parameter is enabled and you have legitimate applications using ports greater than 1023, the device is prone to more false positives.

Table 88: Anti-Scanning Profile–Advanced Parameters (cont.)

Parameter	Description
Monitor but Do Not Block Port Scans	Values: • Enabled–Radware DefensePro DDoS Mitigation detects and reports on *IP-address scans* that use a single port, but does not block these scans. (Radware DefensePro DDoS Mitigation continues to detect and block scans on multiple L4 ports.) • Disabled–Radware DefensePro DDoS Mitigation detects, reports, and blocks scans on multiple L4 ports and *IP-address scans* that use a single port. Default: Disabled **Note:** Scans on a single L4 port are usually network worms.
Include in the Footprint More than Source IP Address and Protocol	Values: • Enabled–A footprint requires at least one attack-source parameter (using the Boolean AND operator) in addition to the *source-IP-address* and *protocol* attack-source parameters. If Radware DefensePro DDoS Mitigation is unable to find a footprint with the additional attack-source parameter, Radware DefensePro DDoS Mitigation does not block the attack. • Disabled–A footprint requires only the *source-IP-address* and *protocol* (using the Boolean AND operator) as attack-source parameters. Default: Disabled

Configuring BDoS Profiles

To configure BDoS profiles, BDoS Protection must be enabled (*Configuration* perspective, **Setup > Security Settings > BDoS Protection**).

When you configure Behavioral DoS profiles, you need to configure the bandwidth and quota settings. Setting the bandwidth and quota values properly and accurately is important, because Radware DefensePro DDoS Mitigation uses these values to derive the initial baselines and attack- detection sensitivity.

Radware DefensePro DDoS Mitigation for Cisco Firepower version 8.22.2 supports a maximum of 50 BDoS profiles.

Recommended settings for policies that include Behavioral DoS profiles are as follows:

- Configure rules containing Behavioral DoS profiles using Networks with source = Any, the public network, and destination = Protected Network. It is recommended to create multiple Behavioral DoS rules, each one protecting a specific servers segment (for example, Web server segments, Mail servers segments, and so on). This assures optimized learning of normaltraffic baselines.
- It is not recommended to define a network with the Source and Destination set to *Any*, because the device collects statistics globally, with no respect to inbound and outbound directions. This may result in lowered sensitivity to detecting attacks.
- When a rule's Direction is set to *One Way*, the rule prevents incoming attacks only. When a rule's Direction is set to *Two Way*, the rule prevents both incoming and outgoing attacks. In both cases, the traffic statistics are collected for incoming and outgoing patterns to achieve optimal detection.

You can configure footprint bypass to bypass specified footprint types or values. For more information, see Configuring BDoS Footprint Bypass, page 123.

To configure a BDoS profile

1. In the *Configuration* perspective, select **Protections > BDoS Profiles**.
2. Do one of the following:
   - To add a profile, click the (Add) button.
   - To edit a profile, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 89: BDoS Profile: General Parameters

Parameter	Description
Profile Name	The name of the BDoS profile.
Packet Reporting	Specifies whether the profile sends sampled attack packets to APSolute Vision for offline analysis. Default: Enabled **Notes:** • When this feature is enabled, for the packet-reporting to take effect, the global setting must be enabled (*Configuration* perspective, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting > EnablePacket Reporting**). • Packets can be sampled even when **Enable Transparent Optimization** is selected. Values in packets that are sampled before the final footprint is generated may not match thefinal footprint.

Table 89: BDoS Profile: General Parameters (cont.)

Parameter	Description
Enable Transparent Optimization	Values: • Enabled–Radware DefensePro DDoS Mitigation does not mitigate new BDoS attacks until the final footprint is generated. Some network environments are more sensitive to dropping packets (for example, VoIP). Enabling the Transparent Optimization option minimizes the probability that Radware DefensePro DDoS Mitigation drops legitimate traffic. • Disabled–Radware DefensePro DDoS Mitigation starts mitigating new BDoS attacks as soon as an initial footprint is generated. Default: Disabled **Notes:** • It may take several seconds (and multiple BDoS closed-feedback iterations) for the final footprint to be generated. • Packets can be sampled even when **Enable Transparent Optimization** is selected. Values in packets that are sampled before the final footprint is generated may not match the final footprint.
Profile Action	The action that the profile takes on traffic matching the attack footprint during an attack. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.

Table 90: BDoS Profile: Flood Protection Settings Parameters

Parameter	Description
Select All Flood Protection Types	Specifies whether the profile protects all the listednetwork-flood protection types. Default: Disabled
SYN Flood	Select the network-flood protection types to apply.
TCP ACK + FIN Flood	
TCP RST Flood	
TCP SYN + ACK Flood	
TCP Fragmentation Flood	
UDP Flood	
UDP Fragmentation Flood	
ICMP Flood	
IGMP Flood	

Table 91: BDoS Profile: Bandwidth Settings Parameters

Parameter	Description
Inbound Traffic	The maximum inbound traffic bandwidth, in Kbit/s, expected on your links. Radware DefensePro DDoS Mitigation derives the initial baselines from the bandwidth and quota settings. Values: 1–1,342,177,280 **Caution:** You must configure this setting to start Behavioral DoS protection. **Caution:** When you change a bandwidth setting (**Inbound Traffic** or **Outbound Traffic**), the quota settings automatically change to the default values appropriate for the bandwidth. There is no alert message for this automatic action, however the user interface does show the actual values. **Note:** For the definition of inbound traffic and outbound traffic, see Configuring Protection Policies, page 160.
Outbound Traffic	The maximum outbound traffic bandwidth, in Kbit/s, expected on your links. Radware DefensePro DDoS Mitigation derives the initial baselines from the bandwidth and quota settings. Values: 1–1,342,177,280 **Caution:** You must configure this setting to start Behavioral DoS protection. **Caution:** When you change a bandwidth setting (**Inbound Traffic** or **Outbound Traffic**), the quota settings automatically change to the default values appropriate for the bandwidth. There is no alert message for this automatic action, however the user interface does show the actual values. **Note:** For the definition of inbound traffic and outbound traffic, see Configuring Protection Policies, page 160.

Table 92: BDoS Profile: Quota Settings Parameters

Parameter	Description
Revert to Default Quotas (button) (This button is active only when the **Inbound Traffic** and **Outbound Traffic** parameters–in the *Bandwidth Settings* tab–are set.)	Restores the default values to all the quotas. Radware DefensePro DDoS Mitigation calculates the default values according to the values of the **Inbound Traffic** and **Outbound Traffic** parameters.

Table 92: BDoS Profile: Quota Settings Parameters (cont.)

Parameter	Description
TCP UDP Fragmented UDP ICMP IGMP	For each traffic type, specify the quota–the maximum expected percentage of incoming and outgoing traffic out of the total traffic. Cisco recommends that you initially leave these fields empty, so that the default values will automatically be used. To view default values after creating the profile, double-click the entry in the table. You can then adjust quota values based on your network performance. **Caution:** After you enter quota values and click **Submit**, Radware DefensePro DDoS Mitigation calculates the required minimum value for each type. (The calculation uses various parameters, which include **Inbound Traffic** and **Outbound Traffic**.) If you enter a value that is less than the required minimum, the actual value automatically changes to the required minimum. There is no alert message for this automatic action, however the user interface does show the actual values. **Note:** The total quota values may exceed 100%, because each value represents the maximum volume per protocol.

Table 93: BDoS Profile: Detection Sensitivity Parameter

Parameter	Description
UDP Packet Rate Detection Sensitivity	The packet-rate detection sensitivity–that is, to what extent the BDoS engine considers the UDP PPS-rate values (baseline and current). This parameter is relevant only for only for BDoS UDP protection. Values: • Ignore or Disable • Low • Medium • High Default: Low

Table 94: BDoS Profile: Burst-Attack Protection Settings Parameters

Parameter	Description
Note: The Radware DefensePro DDoS Mitigation CLI exposes two additional parameters for *advanced* configuration of Burst-Attack Protection.[1]	
Enable Burst-Attack Protection	Specifies whether Burst-Attack Protection is enabled. Enabling and configuring Burst-Attack Protection lets Radware DefensePro DDoS Mitigation identify repeated bursts of malicious traffic with the same footprint as belonging to the same attack. Pauses between bursts sometimes last hours, and some burst attack last days. Using Burst- Attack Protection, Radware DefensePro DDoS Mitigation does not need to regenerate the attack footprint every time a new burst occurs. Rather, Radware DefensePro DDoS Mitigation can identify a new burst in an attack and mitigate the attack immediately. Default: Enabled **Caution:** When Burst-Attack Protection is enabled, the BDoS profile may block some legitimate traffic if that traffic matches the BDoS footprint–even between bursts.
Maximum Interval Between Bursts	The time, in minutes, without any burst, that causes the BDoS profile to consider the attack to be terminated. Values: 10–10,080 (seven days) Default: 30

1 – The Radware DefensePro DDoS Mitigation CLI exposes the following CLI commands for *advanced* configuration of Burst-Attack Protection:

- **dp behavioral-DoS profiles-bt**–The number of bursts that causes the BDoS profile to identify the attack as a burst attack. Values: 2–50. Default: 5.
- **dp behavioral-DoS profiles -bl**–The time, in hours, after which the BDoS profile returns to *footprint analysis* state to refresh the generated footprint. If there is no burst in progress, the BDoS profile enters the *non-attack* state and will generate a new footprint if and when another attack is detected. Values: 1–336(14 days). Default: 10. For more information on the BDoS states, see Table 217 - BDoS Attack Details: Info Parameters, page 335.

Table 95: BDoS Profile: Overblocking Settings Parameters

Parameter	Description
Enable Overblocking Prevention	Specifies whether the BDoS profile prevents blocking too much legitimate traffic. *Overblocking* is a situation where the BDoS profile has created a signature that meets all required criteria (blocking the suspicious traffic and matching the specified strictness level), but the profile is blocking too much legitimate traffic. When Overblocking Prevention is enabled, and Radware DefensePro DDoS Mitigation identifies an overblocking situation, the profile returns to *footprint analysis* state to refresh the generated footprint. If BDoS protection started blocking the attack but stopped three times after identifying an overblocking situation, the profile enters the *over-blocking- footprint* state. This state remains for 10 minutes, after which, BDoS protection generates and implements a new footprint. Default: Disabled **Caution:** When Overblocking Prevention is enabled, if the profile repeatedly enters the *over-blocking-footprint* state, the BDoS profile may still block traffic (possibly legitimate), especially when Transparent Optimization is enabled (see Table 89 - BDoS Profile: General Parameters, page 173). **Note:** For more information on the BDoS states, see Table 217 - BDoS Attack Details: Info Parameters, page 335.
Overblocking Prevention Threshold	The percentage of the traffic rate–after beginning the blocking of the attack traffic–below the *recent baseline* that is considered as overblocking. The *recent baseline* is separate from the normal baseline. The *recent baseline* is based on recent, peacetime traffic, whereas the normal baseline is learned over a much longer period. Values: 1–100 Default: 25

Table 96: BDoS Profile: Advanced Settings Parameters

Parameter	Description
Learning Suppression Threshold	The percentage of the *specified bandwidth*, below which, Radware DefensePro DDoS Mitigation suppresses BDoS-baseline learning. The *specified bandwidth* refers to the **Outbound Traffic** and **Inbound Traffic** parameters specified in the *Bandwidth Parameters* tab above. Radware DefensePro DDoS Mitigation calculates the threshold per Protection policy and specified *Direction* (*Network Protection* tab, **Network Protection Policy > Direction**). For *One Way* policies, the Learning Suppression Threshold considers the inbound bandwidth. Radware DefensePro DDoS Mitigation treats *Two Way* policies as two policies, so the Learning Suppression Threshold calculates the bandwidth for each policy (inbound/outbound). The Learning Suppression Threshold feature helps preserve a good BDoS-baseline value in scenarios where, at times, Radware DefensePro DDoS Mitigation handles very little traffic. There are two typical scenarios where, at times, Radware DefensePro DDoS Mitigation handles very little traffic: • Out-of-path deployments–In an out-of-path deployment, when traffic is diverted through Radware DefensePro DDoS Mitigation for mitigation. During an attack, the traffic is diverted and routed through Radware DefensePro DDoS Mitigation. During peacetime, no traffic passes through Radware DefensePro DDoS Mitigation (except for maintenance messages). When no traffic is diverted to Radware DefensePro DDoS Mitigation, the BDoS learning mustbe suppressed to prevent extremely low values affecting the baseline and ultimately increasing the susceptibility to false positives. • Environments where traffic rates change dramaticallythroughout the day. Values: • 0–The BDoS profile uses *no* Learning Suppression Threshold. • 1–50 Default: 0 **Note:** Using the Radware DefensePro DDoS Mitigation CLI, you can view the Protection policies with a BDoS profile and the runtime status of the BDoS Learning Suppression feature per Protection policy. For more information, see the Radware DefensePro DDoS Mitigation CLI Command for BDoS Learning Suppression Threshold, page 181.

Table 96: BDoS Profile: Advanced Settings Parameters (cont.)

Parameter	Description
BDoS Rate Limit	Specifies whether/how the profile limits the rate of traffic–only a fallback measure–when BDoS protection fails to generate the real- time signature. The rate-limit applies to each *flood protection type* separately. (The *flood protection types* are selected in the BDoS Profile *Flood Protection Settings* tab.) Traffic below the rate-limit threshold bypasses the BDoS module. (Traffic that bypasses the BDoS module *may* be handled by other Radware DefensePro DDoS Mitigation modules. Traffic above the rate- limit threshold is dropped.) Having a BDoS Rate Limit insures the uptime of the network that the Protection policy protects during volumetric attacks. Note however, that when implementing the BDoS Rate Limit, legitimate traffic may also be dropped. Values: • Disabled–While in the *Anomaly* state or *Non-strictness* state, the traffic bypasses the BDoS module. • Limit to Normal Edge–While in the *Anomaly* state or *Non- strictness* state, the profile limits the traffic rate according to the current *Normal* baseline. • Limit to Suspect Edge–While in the *Anomaly* state or *Non- strictness* state, the profile limits the traffic rate according to the current *Suspect* baseline. • Limit to User-defined Rate–While in the *Anomaly* state or *Non-strictness* state, the profile limits the traffic rate according to the user-defined rate. The user-defined rate is determined by the number entered in the adjacent text box and the selected unit– **Kbps**, **Mbps**, or **Gbps**. Default: Disabled

Table 97: BDoS Footprint Strictness Examples

Footprint Example	Low Strictness	Medium Strictness	High Strictness
TTL	Yes	No	No
TTL AND Packet Size	Yes	Yes	No
TTL AND Packet Size AND Destination Port	Yes	Yes	Yes

Radware DefensePro DDoS Mitigation CLI Command for BDoS Learning Suppression Threshold

To view the Protection policies with a BDoS profile and the runtime status of the BDoS Learning Suppression feature per Protection policy

> Open the Radware DefensePro DDoS Mitigation CLI, and enter the following command:

dp behavioral-DoS global advanced learning suppression status

The CLI displays a table like this:

```
+-----------------------------------------------------+
| Policy Name              | Direction    | IP Ver    |   Status    |
+-----------------------------------------------------+
| Policy_1                 | Inbound      | IPv4      |     OFF     |
| Policy_1                 | Inbound      | IPv6      |     OFF     |
| Policy_1                 | Outbound     | IPv4      |     OFF     |
| Policy_1                 | Outbound     | IPv6      |     OFF     |
+-----------------------------------------------------+
```

The Status value specifies the status of BDoS Learning Suppression. When the Status value is ON, BDoS Learning Suppression is active, and BDoS-baseline learning is *not* active. When the Status value is OFF, BDoS Learning Suppression is not active, and BDoS-baseline learning *is* active.

Configuring Connection Limit Profiles

Connection Limit profiles defend against session-based attacks, such as half-open SYN attacks, request attacks, and full-connection attacks.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Connection Limit profiles.

Connection Limit profiles contain attack definitions for groups of TCP or UDP application ports. Radware DefensePro DDoS Mitigation counts the number of TCP connections, or UDP sessions, opened per client, per server, or per client plus server combination, for traffic that matches a Connection Limit policy attack definition. Once the number of connections per second reaches the specified threshold, any session/connection over the threshold is dropped, unless the **Action Mode** defined for this attack is **Report Only**.

You can also define whether to suspend specified traffic (**Suspend Action**). That is, Radware DefensePro DDoS Mitigation can drop specified traffic for a number of seconds according to the *Suspend table* parameters.

Recommended settings for policies that include Connection Limit profiles:

- Configure policies containing Connection Limit profiles using Networks only with **Source** being **Any**, the public network, and **Destination** being **Protected Network**. You can define segments using VLAN tags and physical ports.
- It is not recommended to define networks when the **Source** and **Destination** are set to **Any**.
- You can configure policies containing Connection Limit profiles with **Direction** set to either **One Way** or **Two Way**.

Before you configure a Connection Limit profile, you should configure the required Connection Limit protections.

To configure a Connection Limit profile

1. In the *Configuration* perspective, select **Protections > Connection Limit Profiles**.
2. To add or modify a profile, do one of the following:
   - To add a profile, enter the profile name, click the (Add) button, and then, click **Submit**.
   - To edit a profile, double-click the entry in the table.
3. To add Connection Limit protections to the profile, in the *Edit Connection Limit Profile* dialog box protections table, do the following:
   a. Click the (Add) button.
   b. Select the **Protection Name**, and then, click **Submit**.
4. To define additional Connection Limit protections for the profile, click **Go to Protection Table**. For more information, see Configuring Connection Limit Protections, page 183.

Note: A Connection Limit profile should include all the Connection Limit *protections* that you want to apply in a Protection policy.

Table 98: Connection Limit Profile Parameters

Parameter	Description
Profile Name	(Read-only) The name of the Connection Limit profile.
Connection Limit Protection Table	Lists the Connection Limit *Protection Name* and *Protection ID* for each protection applied for the selected profile. **To add a protection** 1. In the table, click the (Add) button. 2. From the **Protection Name** drop-down list, select the protection, and then, click **Submit**. **Note:** In each Protection policy, you can use only one Connection Limit profile. Therefore, ensure that all the protections that you want to apply to a rule are contained in the profile specified for that policy.
Go to Protection Table	Opens the *Connection Limit Protection* dialog box in which you can add and modify Connection Limit protections.

Configuring Connection Limit Protections

Configure Connection Limit protections to add to Connection Limit profiles.

To configure a Connection Limit protection

1. In the *Configuration* perspective, select **Protections > Connection Limit Profiles> Connection Limit Protections**.
2. To add or modify a protection, do one of the following:
   - To add a protection, click the  (Add) button.
   - To edit a protection, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 99: Connection Limit Protection Parameters

Parameter	Description
Protection Name	A descriptive name for easy identification when configuring and reporting.
Protection ID	(Read-only) The ID number assigned to the Connection Limit protection.
Application Port Group	The Layer 4 port or class object that defines the application you want to protect. Having the field empty specifies *any* port.
Protocol	The Layer 4 protocol of the application you want to protect. Values: TCP, UDP Default: TCP
Number of New Connections	The maximum number of new TCP connections, or new UDP sessions, per second, allowed for each source, destination orsource- and-destination pair. All additional sessions are dropped. When the threshold is reached, attacks are identified, and Radware DefensePro DDoS Mitigation generates a security event. Values: 0–100,000,000 Default: 50
Tracking Type	The counting rule for tracking sessions. Values: • Source Count–Sessions are counted per source IP address. • Destination Count–Sessions are counted per destination IP address. • Source and Destination Count–Sessions are counted per source IP and destination IP address combination. • TBDddd 8.23 Default: Source Count **Note:** When **Tracking Type** is **Destination Count**, the **Suspend Action** can only be **None**.

Table 99: Connection Limit Protection Parameters (cont.)

Parameter	Description
Action Mode	The action that Radware DefensePro DDoS Mitigation takes when an attack is detected. Values: • Drop–The packet is discarded. • Report-only–The packet is forwarded to the destination IP address. Default: Drop **Caution:** The **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Drop** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report-only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.
Risk	The risk assigned to this attack for reporting purposes. Values: Info, Low, Medium, High Default: Medium
Suspend Action	Specifies which session traffic the device suspends for the attack duration. Values: • None–Suspend action is disabled for this attack. • Source IP–All traffic from the IP address identified as the source of this attack is suspended. • Source IP + Destination IP–Traffic from the IP address identified as the source of this attack to the destination IP address under attack is suspended. • Source IP + Destination Port–Traffic from the IP address identified as the source of this attack to the application (Destination port) under attack is suspended. • Source IP + Destination IP and Port–Traffic from the IP address identified as the source of this attack to the destination IP address and port under attack is suspended. Default: None **Note:** When **Tracking Type** is **Destination Count**, the **Suspend Action** can only be **None**.
Packet Reporting	Specifies whether the device sends sampled attack packets to APSolute Vision for offline analysis. Default: Disabled **Caution:** When this feature is enabled here, for the packet- reporting to take effect, the global setting must be enabled (*Configuration* perspective, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting and Packet Trace > Enable Packet Reporting**).

Configuring Connection PPS Profiles

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Connection PPS profiles.

Each Connection PPS profile can contain up to 50 *PPS Protections*.

Each PPS Protection tracks the PPS rate in sessions matching the specified values of the following parameters:

- **Protocol** (TCP, UDP, or TCP or UDP)
- **Destination Port**
- **Destination Network**
- **Threshold**, in packets per second

As soon as a session matches the criteria of a PPS Protection in the profile, the profile declares a Connection PPS attack and applies the specified **Action** on matching packets that exceed the threshold.

The first matching PPS Protection in the profile remains associated with the session for as long as the attack continues.

When the packets-per-second rate falls below the threshold for a certain number of seconds, the profile declares the attack to be ended (*terminated*).

Ensure that all the PPS Protections that you want to apply to a Protection policy are contained in the Connection PPS profile selected for that policy.

Note: In APSolute Vision features other than AVA AMS, security reporting and security monitoring for Connection PPS profiles is minimal.

To configure a Connection PPS profile

1. In the *Configuration* perspective, select **Protections > Connection PPS Profiles**.
2. Do one of the following:
   - To add a profile, click the  (Add Connection PPS Profile) button. Enter the profile name, and then, click **Submit**.
   - To edit a profile, double-click the entry in the table.
3. Do one of the following:
   - To add a PPS Protection, at the top of the table, click the  (Add PPS Protection) button.
   - To edit a PPS Protection, double-click the entry in the table.
4. Configure the PPS Protection parameters, and then, click **Submit**.
5. Repeat the previous two steps, as required, to define additional PPS Protections for the profile.
6. Click **Submit**.

Tip: You can click the **Drop All** or **Report All** button at the top of the table to change the **Action** value of all the PPS Protections in the table to **Block and Report** or **Report Only**.

Table 100: Connection PPS Profile Parameters

Parameter	Description
Profile Name	The name of the Connection PPS profile. Maximum characters: 29
Number of PPS Protections	(Read-only) The number of PPS Protections configured in the profile.

Table 101: PPS Protection Parameters

Parameter	Description
Protection Name	A descriptive name of the PPS Protection, for easy identification when configuring and reporting.
Protocol	The protocol to which the PPS Protection applies. Values: TCP, UDP, TCP or UDP Default: TCP
Destination Port	The port or predefined Application Port Group class object that defines the destination of the packets to which the PPS Protection applies. You can specify a specific value, a comma-separated list, a range (in the format **a- b**), a mixture, or use an Application Port Group. Values: • Any—The PPS Protection matches *any* destination application port. • *A specific application-port number.* • *A list of comma-separated application-port numbers.* • *An Application Port Group class displayed in the Classes tab.* • TCP-reset-ACK • TCP-reset-Data • dcerpc • dns • ftp • h225 • http • https • imap • irc • ldap • ms-sql-m • ms-sql-s ▪ msn ▪ my-sql ▪ ntp ▪ oracle ▪ pop3 ▪ privileged-services ▪ radius ▪ rexec ▪ rshell ▪ rtsp ▪ sccp (skinny) ▪ sip ▪ smb ▪ smtp ▪ snmp ▪ ssh ▪ ssl ▪ sunrpc ▪ telnet ▪ tftp Default: Any Maximum characters: 255 **Caution:** You can specify up to 50 ranges/values, in a comma- separated list or in the Application Port Group class. However, each port range is unlimited,

	for example, 1-10, 50-65535is valid.

Table 101: PPS Protection Parameters (cont.)

Parameter	Description
Destination Network	The destination network of the packets to which the PPS Protection applies. Values: • As in Policy–The PPS Protection matches only destination networks that match the Protection policy. • any–The PPS Protection matches any destination network. • any_ipv4–The PPS Protection matches any IPv4 destination network. • *A discrete IP address*–The PPS Protection matches the IP address. • *A Network class displayed in the Classes tab*–The PPS Protection matches the configuration of the Network class. Default: As in Policy **Caution:** If you specify a Network class, the class can represent up to 50 discrete IP addresses.
Threshold	The packets-per-second rate on a single session that activates the PPS Protection. For rate-limiting, enter a packet-per-session-per-second value, for rate-limiting. To apply the specified **Action** to all matching traffic, enter **0** (zero). Values: 0–1,000,000,000
Risk	The risk assigned to this attack for reporting purposes. Values: High, Info, Low, Medium Default: Medium
Action	The action that the profile takes when an attack is detected. Values: Report Only, Block and Report Default: Report Only **Caution:** The **Report Only** option takes precedence–in the Network Protection *policy* or the PPS Protection *in the profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the PPS Protection, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the PPS Protection, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.

Configuring DNS Flood Protection Profiles

To configure DNS Flood Protection profiles, *DNS Flood Protection* must be enabled (*Configuration* perspective, **Setup > Security Settings > DNS Flood Protection**).

When you configure a DNS Flood Protection profile, you need to configure the query and quota settings. Setting the query and quota values properly and accurately is important, because Radware DefensePro DDoS Mitigation uses these values to derive the initial baselines and attack-detection sensitivity.

Radware DefensePro DDoS Mitigation version 8.22.2 supports a maximum of 50 DNS Flood Protection profiles.

Cisco recommends configuring Protection policies that include DNS Flood Protection profiles using networks with **SRC Network** set to **any** (that is, the public network) and **DST Network** set to the protected network.

DNS Flood Protection profiles operate only on ingress traffic. However, you can use a DNS Flood Protection profile in one-way *or* two-way policies (that is, policies where **Direction** can be **One Way** or **Two Way**).

You can configure footprint bypass to bypass specified footprint types or values. For more information, see Configuring DNS Footprint Bypass, page 127.

To configure a DNS Flood Protection profile

1. In the *Configuration* perspective, select **Protections > DNS Flood ProtectionProfiles**.
2. Do one of the following:
   - To add a profile, click the  (Add) button.
   - To edit a profile, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 102: DNS Flood Protection Profile: General Parameters

Parameter	Description
Name	The name of the profile.
Profile Action	The action that the profile takes on DNS traffic during an attack. The device implements this parameter only when the **Use Manual Triggers** checkbox is cleared. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence—in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.
Packet Reporting	Specifies whether the profile sends sampled attack packets to APSolute Vision for offline analysis. Default: Enabled **Notes:** • When this feature is enabled, for the packet-reporting to take effect, the global setting must be enabled (*Configuration* perspective, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting > Enable Packet Reporting**). • Packets can be sampled even when **Enable Transparent Optimization** is selected. Values in packets that are sampled before the final footprint is generated may not match the final footprint.

Table 103: DNS Flood Protection Profile: Query Protections and Quotas Parameters

Parameter	Description
Revert to Default Quotas (button) (This button is active only when the **Expected DNS Query Rate** and **Max Allowed QPS** parameters– in the *Rate Settings* tab–are set.)	Restores the default values to all the quotas. Radware DefensePro DDoS Mitigation calculates the default values according to the values of the **Expected DNS Query Rate** and **Max Allowed QPS** parameters.
Select All Query Types	Specifies whether the profile protects all the listed DNS query types. Default: Disabled
A Query MX Query PTR Query AAAA Query Text Query SOA Query NAPTR Query SRV Query Other Queries	For each DNS query type to protect, specify the quota–the maximum expected percentage of DNS traffic out of the total DNS traffic–and select the checkbox in the row. Cisco recommends that you initially leave these fields empty so that the default values will automatically be used. To view default values after creating the profile, double-click the entry in the table. You can then adjust quota values based on your network performance. **Caution:** After you enter quota values and click **Submit**, Radware DefensePro DDoS Mitigation calculates the required minimum value for each type. (The calculation uses various parameters, which include **Expected DNS Query Rate**.) If you enter a value that is less than the required minimum, the actual value automatically changes to the required minimum. There is no alert message for this automatic action, however the user interface does show the actual values. **Note:** The total quota values may exceed 100%, because each value represents the maximum volume per query type.

Table 104: DNS Flood Protection Profile: Rate Settings Parameters

Parameter	Description
Note: The device implements the parameters in this tab only when the **Use Manual Triggers** option is *disabled*.	
Expected DNS Query Rate	The expected rate, in queries per second, of DNS queries. **Caution:** After you change the **Expected DNS Query Rate** and click **Submit**, the quota settings (see Table 103 - DNS Flood Protection Profile: Query Protections and Quotas Parameters, page 189) automatically change to the default values appropriate for the query rate. There is no alert message for this automatic action, however the user interface does show the actual values.
Max Allowed QPS	The maximum allowed rate of DNS queries per second, when the *Manual Triggers* option is *not* enabled (that is, when the **Use Manual Triggers** checkbox is cleared in the *Manual Triggers* tab). Values: 0–4,000,000 Default: 0 **Caution:** If the **Max Allowed QPS** is lower than the DNS baseline, the profile drops every packet that matches the real- time signature.

Table 104: DNS Flood Protection Profile: Rate Settings Parameters (cont.)

Parameter	Description
Signature Rate-Limit Target	The maximum level of DNS traffic, in percent, relative to the DNS baseline, that the profile allows during a DNS-flood attack. This is relevant to the traffic that matches the real-time signature. Values: 0–100 Default: 0 **Note:** If the DNS baseline plus the added **Signature Rate-Limit Target** proportion is greater than the **Max Allowed QPS**, Radware DefensePro DDoS Mitigation will not allow traffic to exceed the **Max Allowed QPS**.

Table 105: DNS Flood Protection Profile: Manual Triggers Parameters

Parameter	Description
Use Manual Triggers	Specifies whether the profile uses user-defined DNS QPS thresholds instead of the learned baselines. Default: Disabled
Activation Threshold	The number of total queries per second, per protected destination network–after the specified **Activation Period**–above which, Radware DefensePro DDoS Mitigation considers there to be an ongoing attack. When Radware DefensePro DDoS Mitigation detects an attack, it starts challenging all sources. Radware DefensePro DDoS Mitigation continues the challenges unless the specified **Max QPS** (see below) is reached. Above the specified **Max QPS**, Radware DefensePro DDoS Mitigation limits the rate of total QPS towards the protected network. Values: 0–4,000,000 Default: 0
Activation Period	The number of consecutive seconds that the DNS traffic exceeds the **Activation Threshold** that determines when Radware DefensePro DDoS Mitigation considers an attack to be in progress. Values: 1–30 Default: 3
Termination Threshold	The maximum number of queries per second–after the specified **Termination Period**–that causes Radware DefensePro DDoS Mitigation to consider the attack to have ended. Values: 0–4,000,000 Default: 0 **Note:** The **Termination Threshold** must be less than or equal to the **Activation Threshold**.
Termination Period	The time, in seconds, that the DNS traffic is continuously below the **Termination Threshold**, which causes Radware DefensePro DDoS Mitigation to consider the attack to have ended. Values: 1–30 Default: 3

Max QPS	The maximum allowed rate of DNS queries per second. Values: 0–4,000,000 Default: 0

Table 105: DNS Flood Protection Profile: Manual Triggers Parameters (cont.)

Parameter	Description
Escalation Period	The time, in seconds, that Radware DefensePro DDoS Mitigation waits before escalating to the next enabled *Mitigation Action*. Values: 0–30 Default: 3

Table 106: DNS Flood Protection Profile: Subdomains Whitelist Parameters

Parameter	Description
The *Subdomains Whitelist* is an aggregated list of the *top-n* FQDNs (by occurrence) seen in the DNS traffic. A single Radware DefensePro DDoS Mitigation device is able to process and analyze tens of millions of FQDNs for detection and mitigation purposes. For visibility and management purposes, Radware DefensePro DDoS Mitigation aggregates these FQDNs into the Subdomains Whitelist. There is one Subdomains Whitelist per DNS Flood Protection profile per Protection policy. You can export and import the Subdomains Whitelist as a text file. The Subdomains Whitelist file can include the following types of FQDNs: • Automatic entries–Radware DefensePro DDoS Mitigation populates these entries automatically. An automatic entry has the letter *a* appended to the FQDN, after a comma (for example, www.website1.com,a). Radware DefensePro DDoS Mitigation uses an aging mechanism to update the list of automatic entries in the Subdomains Whitelist. **Note:** You can manually add this entry type, and it will age as part of the aging mechanism. • Manual entries–A manual entry has the letter *m* appended to the FQDN, after a comma (for example, www.website2.com,m). Manual entries may remain in the Subdomains Whitelist indefinitely. You can add manual entries to prepare for random-subdomain attacks, specifying subdomains that you know to be legitimate. You can export a Subdomains Whitelist file, and examine or modify the file as required. Radware DefensePro DDoS Mitigation names exported Subdomains Whitelist files using the format <DeviceName>_<PolicyName>_dns_whitelist_<ddMMyyyy>_<hhmmss>.txt. You can import a Subdomains Whitelist file into the current profile that is configured in the specified Protection policy.	
Protection Policy	The Protection policy for which you want to apply actions on the Subdomains Whitelist. A DNS Flood Protection profile can be used in multiple Protection policies, so you need to choose the policy for which you want to modify the Subdomains Whitelist.
Subdomains Whitelist File to Import	The Subdomains Whitelist file to import into the current DNS profile that is configured in the selected **Protection Policy**. You can click **Browse** to navigate to the required file and select the file. The file must be a text file with the **.txt** extension.
Import (button)	Imports the file specified in the **Subdomains Whitelist File to Import** text box.

Table 106: DNS Flood Protection Profile: Subdomains Whitelist Parameters (cont.)

Parameter	Description
Clear Subdomains Whitelist Before Importing	Values: • Enabled–When you click **Import**, the profile clears the existing Subdomains Whitelist entries before importing the Subdomains Whitelist file. • Disabled–When you click **Import**, the entries in the imported Subdomains Whitelist file merge with the existing entries. Default: Disabled
Export Whitelist File (button)	Exports a file with the current Subdomains Whitelist of the profile that is configured in the selected **Protection Policy**.[1]
Clear Manual Entries (button)	Clears the manual entries from the current Subdomains Whitelist of the profile that is configured in the selected **Protection Policy**.[1]
Clear All Entries (button)	Clears all entries from the current Subdomains Whitelist of the profile that is configured in the selected **Protection Policy**.[1]

1 – The profile must be configured in the selected **Protection Policy**.

Table 107: DNS Profile: Advanced Settings Parameters

Parameter	Description

Learning Suppression Threshold	The percentage of the specified **Expected DNS Query Rate** below which, Radware DefensePro DDoS Mitigation suppresses DNS-baseline learning. Radware DefensePro DDoS Mitigation calculates the threshold per Network Protection policy, per IP version (IPv4 or IPv6). **Example:** Consider a Protection policy, Policy1. Policy1 has a DNS profile with the **Expected DNS Query Rate** value **1000**, and the DNS **Learning Suppression Threshold** is **5**(%). The baseline for Policy1 will not change (that is, learning is suppressed) if the traffic rate drops below 50 QPS. The Learning Suppression Threshold feature helps preserve a good DNS-baseline value in scenarios where, at times, Radware DefensePro DDoS Mitigation handles very little traffic. There are two typical scenarios where, at times, RadwareDefensePro DDoS Mitigation handles very little traffic: • Out-of-path deployments–In an out-of-path deployment, when traffic is diverted through Radware DefensePro DDoS Mitigation for mitigation. During an attack, the traffic is diverted and routed through Radware DefensePro DDoS Mitigation. During peacetime, no traffic passes through Radware DefensePro DDoS Mitigation (except for maintenance messages). When no traffic is diverted to Radware DefensePro DDoS Mitigation, the DNS learning must be suppressed to prevent extremely low values affecting the baseline and ultimately increasing the susceptibility to false positives. • Environments where traffic rates change dramaticallythroughout the day. Values: • 0–Specifies that the DNS-baseline learning is always active. • 1-100 Default: 0 **Note:** Using the Radware DefensePro DDoS Mitigation CLI, you can view the Protection policies with a DNS Flood Protection profile and the runtime status of the DNS Learning Suppression feature per Protection policy. For more information, see the Radware DefensePro DDoS Mitigation CLI Command for DNS Learning Suppression Threshold, page 195.

rameters (cont.)

Parameter	Description

	When the DNS Flood Protection profile detects a new attack, the profile generates an attack footprint to block the attack traffic. If the profile is unable to generate a footprint that meets the footprint- strictness condition, the profile issues a notification for the attack but does not block it. The higher the strictness, the more accurate the footprint. However, higher strictness increases the probability that the profile cannot generate a footprint. Values: • High–Requires at least two Boolean AND conditions and no Boolean OR condition in the footprint. This level lowers the probability for false positives but increases the probability for *false negatives* (that is, increases the probability of not identifying attack traffic). • Medium–Comprises the following: — At least one Boolean AND condition in the top-level expression. — No OR condition in the top-level expression. — Up to two Boolean OR conditions in a nested expression. Examples: — A AND B — (A OR B OR C) AND D [where "(A OR B OR C)" is a *nested expression*] • Low–Allows any footprint suggested by the DNS Flood Protection profile. This level achieves the best attack blocking but increases the probability of false positives. Default: Low **Notes:** • The DNS Flood Protection profile always considers the Checksum field and the Sequence Number fields as *High* **Footprint Strictness** fields. Therefore, a footprint with only a checksum or sequence number is always considered as *High* **Footprint Strictness**. • Table 108 - DNS Footprint Strictness Examples, page 194 shows examples of footprint strictness requirements.

Table 108: DNS Footprint Strictness Examples

Footprint Example	Low Strictness	Medium Strictness	High Strictness
DNS Query	Yes	No	No
DNS Query AND DNS ID	Yes	Yes	No
DNS Query AND DNS ID AND Packet Size	Yes	Yes	Yes

Radware DefensePro DDoS Mitigation CLI Command for DNS Learning Suppression Threshold

To view the Protection policies with a DNS Flood Protection profile and the runtime status of the DNS Learning Suppression feature per Protection policy

> Open the Radware DefensePro DDoS Mitigation CLI, and enter the following command:

dp dns global advanced learning suppression status

The CLI displays a table like this:

```
+-------------------------------------------------------+
| Policy Name | IP Ver          |    Status     |
+-------------------------------------------------------+
| Policy1          | IPv4       |    ON       |
| Policy1          | IPv6       |    OFF      |
+-------------------------------------------------------+
```

The Status value specifies the status of DNS Learning Suppression. When the Status value is ON, DNS Learning Suppression is active, and DNS-baseline learning is *not* active. When the Status value is OFF, DNS Learning Suppression is not active, and DNS-baseline learning *is* active.

Configuring ERT Active Attackers Feed Profiles

ERT Active Attackers Feed (EAAF) profiles use the EAAF subscription service to identify andblock source IP addresses involved in major attacksin real-time to provide preemptive protection from known attackers. The feed is generated by Radware's Threat Research Center.

Each IP address in the EAAF may belong to one, two, or all three of the following categories:

- **ERT Active Attackers**—An IP address that has been correlated and determined to be malicious from multiple sources. Reported events use **ERT**to identify an *ERT Active Attackers* address.
- **Tor Exit Nodes**—An IP address that is a Tor exit node, regardless of whether it has been seen performing malicious activity. Block these only if you wish to block all Tor exit nodes by default. Note that *ERT Active Attackers* category will contain Tor exit nodes that have recently been seen performing malicious activities. Reported events use **TOR**to identify a *Tor Exit Nodes* address.
- **Web Attackers**—An IP address that has been seen performing Web violations. Note that the *ERT Active Attackers* category will contain Web attackers that have recently been seen performing other malicious activities in addition to Web violations. Reported events use **WEB**to identify a *Web Attackers* address.

The configuration of each EAAF profile specifies the action that the profile takes (**Block and Report**, **Report Only**, or **No Action**) per category and per *risk-score level* (**High**, **Medium**, and**Low**).

This feature requires a valid *ERT Active Attackers Feed subscription*. You can view subscription information in the APSolute Vision *Device Subscriptions* table (*APSolute Vision Settings* view *System* perspective, **Device Resources > Device Subscriptions**). For more information on the *Device Subscriptions* table, see the APSolute Vision online help or the *APSolute Vision User Guide*.

APSolute Vision manages the EAAF subscription and the EAAF data.

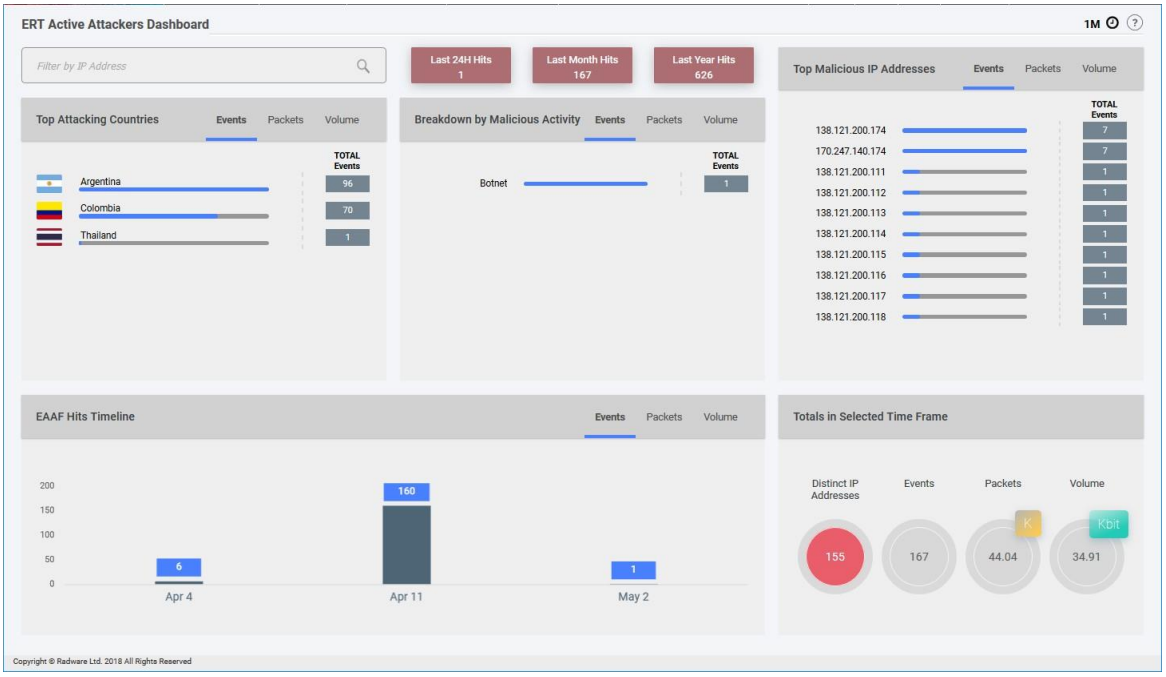
To upload the EAAF data from APSolute Vision to the Radware DefensePro DDoS Mitigation device, you need to configure a scheduled task of type *ERT Active Attackers Feed for DefensePro*. For information on how to configure the scheduled task,

Caution: ERT Active Attackers Feed profiles are ineffective without an *ERT Active Attackers Feed for DefensePro* task that is properly configured and running.

Notes

- If you select an EAAF profile in the configuration of a Protection policy (*Configuration* perspective, **Protection > Protection Policies**), the feed must be available to the Radware DefensePro DDoS Mitigation device. You *can*, however, configure an EAAF profile even if the feed is currently unavailable–for example, if the *ERT Active Attackers Feed subscription* is not yet installed.
- In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 EAAF profiles.
- The *ERT Active Attackers Feed* node of the Security Control Center shows information about DefensePro devices that were updated with the ERT Active Attackers Feed in the last run of the *ERT Active Attackers Feed for DefensePro* scheduled task. To open the Security Control Center, in the APSolute Vision sidebar menu, select **Applications** () **> Security Control Center > ERT Active Attackers Feed**)–or, select **Vision Settings** (), and in the *Dashboards* perspective, select **Security Control Center > ERT Active Attackers Feed**.
- APSolute Vision Analytics (AVA) uses the term **Malicious IP Addresses** to identify attacks that *ERT Active Attackers Feed* profiles handle. For more information, see the *APSolute Vision Analytics User Guide* or the APSolute Vision online help.
- In APSolute Vision features other than AVA AMS, security reporting and security monitoring for ERT Active Attackers Feed profiles is minimal.
- You can use the *EAAF Dashboard* (*ERT Active Attackers* dashboard) to view and monitor statistics on attacks and attackers that Radware DefensePro DDoS Mitigation devices blocked using the ERT Active Attackers Feed. To open the dashboard, in the APSolute Vision sidebar menu, select **Applications** () **> EAAF**. For more information, see the section "Using the EAAF Dashboard" in the *APSolute Vision User Guide* or the APSolute Vision online help.

Figure 35: EAAF Dashboard



To configure an ERT Active Attackers Feed profile

1. In the *Configuration* perspective, select **Protections > ERT Active Attackers FeedProfiles**.
2. Do one of the following:
   - To add a profile, click the (Add) button.
   - To edit a profile, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 109: ERT Active Attackers Feed Profile Parameters

Parameter	Description
Profile Name	The name of the profile. Maximum characters: 29
Feed Categories and Action per Level If an IP address in the EAAF exists in more than one Feed Category, the **Block and Report** option takes precedence over the **Report Only** option, and the **Report Only** option takes precedence over the No Action option. That is, the profile blocks an IP address if it matches the selected risk- score level whose action is **Block and Report**, even if the IP address exists in another Feed Category and matches the selected risk-score level whose action is **Report Only**. **Caution:** However, the **Report Only** option takes precedence on the Protection *policy* level. For example, if an IP address matches a Feed Category and risk-score level whose action is **Block and Report**, but in the configuration of the Protection policy itself, **Report Only** is the selected **Action** option, the action behavior of *all* the Protection policy is *report only*.	
ERT Active Attackers	The action that the profile takes per risk-score level on source IP addresses marked in the EAAF as an *ERT Active Attacker*. Values: Block and Report, Report Only, No Action Default action for risk-score level **High**: Block andReport Default action for risk-score level **Medium**: No Action Default action for risk-score level **Low**: No Action
Tor Exit Nodes	The action that the profile takes per risk-score level on source IP addresses marked in the EAAF as a *Tor Exit Node*. Values: Block and Report, Report Only, No Action Default action for risk-score level **High**: Report Only Default action for risk-score level **Medium**: Report Only Default action for **risk-score level Low**: Report Only
Web Attackers	The action that the profile takes per risk-score level on source IP addresses marked in the EAAF as a *Web Attacker*. Values: Block and Report, Report Only, No Action Default action for risk-score level **High**: Report Only Default action for risk-score level **Medium**: No Action Default action for risk-score level **Low**: No Action

Configuring Geolocation Profiles

This feature requires a *Geolocation subscription*. For more information, contact Technical Support. A Geolocation profile can do one of the following:

- Permanently block traffic from/to selected geolocations.
- Permanently allow traffic from/to selected geolocations, and block all other geolocations.

To identify the geolocation that traffic originates from, the Geolocation feature uses the *Geolocation feed*. APSolute Vision manages the Geolocation subscription and the Geolocation feed.

If the Radware DefensePro DDoS Mitigation device has a valid Geolocation subscription and a user- defined scheduled task of type *Geolocation Feed*, the task uploads the feed to the Geolocation database on the Radware DefensePro DDoS Mitigation device.

Caution: Before you can configure a Geolocation profile, you must configure and run a *Geolocation Feed* task that targets the Radware DefensePro DDoS Mitigation device.

Note: DefenseFlow can use an associated Radware DefensePro DDoS Mitigation device for the Geolocation feed.

For information on how to configure the scheduled task, see Configuring Tasks in the Scheduler, page 285 and Geolocation Feed–Parameters, page 300.

Caution: If the specified **Action** option is **Block and Report**, the Geolocation profile will *not* block the traffic as expected if the specified action of *another* profile type in the Protection policy is **Report Only** and matches the same traffic.

Notes

- In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Geolocation profiles.
- If you have an *APSolute Vision Analytics - AMS* license installed on the APSolute Vision server, you can do the following:
  - Block traffic from selected geolocations for a selected duration–You can open the *Radware DefensePro DDoS Mitigation Monitoring Dashboard*, select a row from the *Protection Policies* table, click a geolocation in the *Geolocation Map* and select one of the following **Block Duration** values (in hours): **1H**, **3H**, **6H**, **12H**, **24H**, **36H**, **72H**. To unblock a geolocation that is being blocked temporarily, click on the geolocation in the *Geolocation Map* and click the selected **Block Duration** value. To change the block duration of a geolocation that is being blocked temporarily, click on the geolocation in the *Geolocation Map* and click the **Block Duration** value that you require. You cannot (temporarily) block a geolocation that the Geolocation *profile* blocks (permanently).
  - View the following (according to the map display):
    - Top Unblocked Attacking Geolocations–That is, geolocations without Geolocation blocking that are identified as being the top origins of attacks.
    - Temporarily Blocked Geolocations–That is, geolocations blocked temporarily (using the Geolocation Map).
    - Permanently Blocked Geolocations–That is, geolocations blocked permanently (by means of the Geolocation profile in the Protection policy).
    - Allowed Geolocations–That is, geolocations without Geolocation blocking that are not top attackers.

    To open the Geolocation Map, open the Radware DefensePro DDoS Mitigation Monitoring Dashboard, select a row from the *Protection Policies* table, and then, select the *Geolocation Map* tab.
  - Use the *Location-Based Suspended Traffic* pane to view a list of temporarily blocked geolocations (*Monitoring* perspective, **Networking > Location-Based Suspended Traffic**). The *Location-Based Suspended Traffic* pane shows the Protection policy name, geolocation code, the start time and date of the temporary blocking, and the end time and date of the temporary blocking.

- Use Radware DefensePro DDoS Mitigation CLI dp geo-feed temporary-rules commands to do the following:
  - Unblock geolocations that are temporarily blocked.
  - View a list of temporarily blocked geolocations in a table. The table shows the Protection policy name, geolocation code, duration (in minutes), the start time and date of the temporary blocking, and the end time and date of the temporary blocking.

For more information on APSolute Vision Analytics (AVA), see the *APSolute Vision Analytics User Guide* or the APSolute Vision online help.

Figure 36: Geolocation Map in APSolute Vision Analytics

- In APSolute Vision features other than AVA AMS, security reporting and security monitoring for Geolocation profiles is minimal.

To configure a Geolocation profile

1. In the *Configuration* perspective, select **Protections > Geolocation Profiles**.
2. Do one of the following:
   - To add a profile, click the (Add) button.
   - To edit a profile, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 110: Geolocation Profile Parameters

Parameter	Description
Profile Name	The name of the profile. Maximum characters: 29

Table 110: Geolocation Profile Parameters (cont.)

Parameter	Description
Geolocation Action	
	Values: • Block Selected Geolocations–The profile blocks traffic from/to the selected regions and geolocations. • Allow Only Selected Geolocations–The profile allows traffic from/to the selected regions and blocks all the rest. Default: Block Selected Geolocations
Regions and Geolocations	
	The **Available** list and the **Selected** list together contain all the and geolocations defined in the Geolocation feed. The **Selected** list displays the geolocations that the profile matches. To filter the **Available** list, enter a value at the top of the *Region* and/or *Geolocation* column,and then click the button. The filter is case-insensitive and uses a Boolean AND operator. Select entries from the lists and use the arrows to move the entries to the other lists as required.
Action	
	The action that the profile takes on the matching traffic. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.

Configuring HTTPS Flood Protection Profiles

This feature requires a DefenseSSL license.

HTTPS Flood Protection profiles efficiently and effectively defend against HTTPS-flood attacks that send malicious HTTPS requests to *protected HTTPS servers*.

HTTPS Flood Protection can detect HTTPS floods without decryption of the traffic. Decryption introduces latency and increases resource consumption.

HTTPS Flood Protection is available only on platforms with an *on-device SSL/TLS component* (*Configuration* perspective, **Setup > SSL Settings > SSL Decryption and Encryption > Enabled, Using the On-Device Component**).

Each *protected HTTPS server* is a *Protected SSL Object* (see Managing Protected SSL Objects, page 117). The Protection policy automatically associates each enabled Protected SSL Object configured on the device whose IP address matches the specified **DST Network** (see DST Network, page 163) of the Protection policy.

When there is no attack (referred to as *peacetime*), HTTPS Flood Protection profiles generate baselines, learning the characteristics of HTTPS traffic for each Protected SSL Object. HTTPS Flood Protection profiles detect attacks based on significant increases in the HTTPS requests from the baselines–increases which are not due to legitimate *flash-event/flash-crowd* traffic.

During the characterization phase of an HTTPS-flood attack, Radware DefensePro DDoS Mitigation creates a list of suspected attacker sources.

To mitigate attacks, HTTPS Flood Protection can use *HTTPS mitigation* and/or *rate-limiting* methods. HTTPS mitigation methods require SSL-decryption-and-encryption that are properly and fully configured. The *rate-limiting* method does not require SSL-decryption-and-encryption.

Tip: You can use *APSolute Vision Analytics* (AVA) to monitor HTTPS Flood Protection. During peacetime, you can use AVA to monitor the characteristics of the traffic learned, such as baselines and statistics. You can also use AVA to monitor real-time and historical information about attack characteristics, such as the HTTPS traffic levels vs. baselines, suspected attacker sources characteristics, and so on. Without any special license, you can open the AVA AMS *Attacks* dashboard and view the statistics of the last 24 hours. All other use of AVA AMS requires an *APSolute Vision Analytics - AMS* license, which must be installed on the APSolute Vision server. For more information on AVA, see the *APSolute Vision Analytics User Guide*.

Note: In APSolute Vision features other than AVA AMS, security reporting and security monitoring for HTTPS Flood Protection is minimal.

You can configure up to 50 HTTPS Flood Protection profiles on a Radware DefensePro DDoS Mitigation instance.

Before you configure an HTTPS Flood Protection profile, ensure the following:

- HTTPS Flood Protection is enabled and the global parameters are configured (*Configuration* perspective, **Setup > Security Settings > HTTPS Flood Protection**).
- The SSL Protected Objects are configured as required. Each SSL Protected Object definesa protected HTTPS server.
- To use an *HTTPS mitigation method* (and not merely a rate-limiting method), and the **Profile Action** is **Block and Report** (not **Report Only**), ensure that the **SSL Decryption and Encryption** option (*Configuration* perspective, **Setup > SSL Settings**) is **Enabled, Using the On-Device Component**, and the Protected SSL Objects are configured fully–with valid SSL server certificates, encryption protocols, and ciphers.

  Caution: If SSL/TLS-decryption-and-encryption is not properly and fully configured (for example, lacking the SSL certificates, encryption protocols, and ciphers), the HTTPS mitigation methods will not work, and only rate-limiting is possible.

To configure an HTTPS Flood Protection profile

1. In the *Configuration* perspective, select **Protections > HTTPS Flood Protection Profiles**.
2. Do one of the following:
   - To add a profile, click the  (Add) button.
   - To edit a profile, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 111: HTTPS Flood Protection Profile Parameters

Parameter	Description
Profile Name	The name of the profile. Maximum characters: 29
Profile Action	The action that the profile takes on HTTPS traffic during an attack. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence—in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.
Mitigation Methods When the profile detects that an HTTPS-flood attack has started, the device implements the mitigation actions in escalating order—in the order that they appear in this tab. Radware DefensePro DDoS Mitigation applies the mitigation methods in an escalating manner. That is, the first mitigation method is applied, and the Degree of Attack (DoA) is evaluated. If, after a certain *escalation period*, the DoA is still high, Radware DefensePro DDoS Mitigation applies the next, more-severe enabled mitigation action—and so on. **Notes:** • Escalation periods are not configurable. • The *HTTPS mitigation* options are available only when SSL-decryption-and-encryption is enabled in the *SSL Settings* node (*Configuration* perspective, **Setup > SSL Settings**). IfSSL- decryption-and-encryption is disabled, features in the *HTTPS mitigation* options are inactive and not operational (even if a grayed-out checkbox appears to be selected).For more information, see Configuring the SSL-Settings Setup, page 107.	
Use HTTPS Authentication on Suspect Sources	Specifies whether Radware DefensePro DDoS Mitigation sends traffic from *the sources suspected to be malicious* to the specified SSL-decryption-and-encryption component—and then authenticates the source using the selected **HTTPS Authentication Method**. Default: Enabled
Rate-Limit Traffic from Suspect Sources	Specifies whether Radware DefensePro DDoS Mitigation limits the rate of packets from sources suspected to be malicious. Default: Disabled
Rate-Limit Threshold (This parameter is available only when the **Rate-Limit Traffic from Suspect Sources** checkbox is selected.)	The number of packets per second per source-suspected-to-be-malicious that Radware DefensePro DDoS Mitigation does *not* block. Values: 0–100,000 Default: 100
Use HTTPS Authentication on All Sources	Specifies whether Radware DefensePro DDoS Mitigation sends traffic from *all* sources to the specified SSL-decryption-and-encryption component—and then authenticates the source using the selected **HTTPS Authentication Method**. Default: Disabled

Table 111: HTTPS Flood Protection Profile Parameters (cont.)

Parameter	Description
Authentication Methods	
HTTPS Authentication Method	The method that the profile uses to authenticate HTTPS traffic at the application layer. Values: • 302 Redirect–Radware DefensePro DDoS Mitigation authenticates HTTPS traffic using a 302 Redirectmessage. • JavaScript–Radware DefensePro DDoS Mitigation authenticates HTTPS traffic using a JavaScriptobject. Default: 302 Redirect **Notes:** • Some attack tools are capable of handling 302 Redirect responses. The **302 Redirect** option for **HTTPS Authentication Method** is not effective against attacks that use those tools. The **JavaScript** option for **HTTPS Authentication Method** requires an engine on the client side that supports JavaScript, and therefore, the **JavaScript** option is considered stronger. However, the **JavaScript** option has some limitations, which are relevant in certain scenarios. • Limitations when using the *JavaScript* **HTTPS Authentication Method**: — If the browser does not support JavaScript calls, the browser will not answer the challenge. — When the protected server is accessed as a sub-page through another (main) page *only* using JavaScript, the user session will fail (that is, the browser will not answer the challenge).[1]
Packet Reporting	
Packet Reporting	Specifies whether the profile reports out-of-state packets. Default: Disabled **Caution:** When this feature is enabled here, for the packet- reporting to take effect, the global setting must be enabled (*Configuration perspective*, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting and Packet Trace > Enable Packet Reporting**). In addition, a change to this parameter takes effect only after you update policies.

1 – For example, if the protected server supplies content that is requested using a JavaS- cript tag, the Radware DefensePro DDoS Mitigation JavaScript is enclosed within the original JavaScript block. This violates JavaScript rules, which results in a challenge fail- ure. In the following example, the request accesses an HTTPS server. The returned chal- lenge page contains the <script> tag again, which is illegal, and therefore, it is dropped by the browser without making the redirect.

```
<script> setTimeout(function(){
   var js=document.createElement(“script”);
   js.src=”http://mysite.site.com.domain/service/
appMy.jsp?dlid=12345”;
   document.getElementsByTagName(“head”)[0].appendChild(js);
   },1000);
</script>
```

Configuring Out-of-State Protection Profiles

Out-of-State Protection profiles detect out-of-state packets to provide additional protection against application-level attacks.

To configure Out-of-State Protection profiles, Out-of-State Protection must be enabled (*Configuration* perspective, **Setup > Security Settings > Out-of-State Protection**).

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Out-of-State Protection profiles.

Caution: In cases of overlapping Protection policies configured with Out-of-State Protection profiles, attacks triggered on both policies are reported twice, once per policy. As a consequence, in traffic monitoring, there might be some inconsistencies in the value for discarded traffic, because the value is the sum of all detected attacks.

To configure an Out-of-State Protection profile

1. In the *Configuration* perspective, select **Protections > Out-of-State ProtectionProfiles.**
2. Do one of the following:
   - To add a profile, click the (Add) button.
   - To edit a profile, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.

Table 112: Out-of-State Protection Profile Parameters

Parameter	Description
Profile Name	The name of the profile.
Activation Threshold	The rate, in PPS, of out-of-state packets above which the profile considers the packets to be part of a flood attack. When Radware DefensePro DDoS Mitigation detects an attack, it issues an appropriate alert and drops the out-of-state packets that exceed the threshold. Packets that do not exceed the threshold bypass the Radware DefensePro DDoS Mitigation device. Values: 1–250,000 Default: 5000
Termination Threshold	The rate, in PPS, of out-of-state packets below which the profile considers the flood attack to have stopped; and Radware DefensePro DDoS Mitigation resumes normal operation. Values: 0–249,999 Default: 4000
Allow SYN-ACK	Values: • Enabled–Radware DefensePro DDoS Mitigation opens a session and processes a SYN-ACK packet even when Radware DefensePro DDoS Mitigation has identified no SYN packet for the session. This option supports asymmetric environments, when the first packet that Radware DefensePro DDoS Mitigation receives is the SYN-ACK. • Disabled–When Radware DefensePro DDoS Mitigation receives a SYN-ACK packet and has identified no SYN packet for the session, Radware DefensePro DDoS Mitigation passes through the SYN-ACK packet (unprocessed) if the packet is below the specified activation threshold, and Radware DefensePro DDoS Mitigation drops the packet if it is above the specified activation threshold. Default: Enabled
Profile Action	The action that the profile takes when it encounters out-of-state packets. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.
Risk Level	The risk–for reporting purposes–assigned to the attack that the profile detects. Values: Info, Low, Medium, High Default: Low

Table 112: Out-of-State Protection Profile Parameters (cont.)

Parameter	Description
Packet Reporting	Specifies whether the profile reports out-of-state packets. Default: Disabled **Caution:** When this feature is enabled here, for the packet-reporting to take effect, the global setting must be enabled (*Configuration perspective*, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting and Packet Trace > Enable Packet Reporting**). In addition, a change to this parameter takes effect only after you update policies.

Configuring Signature Protection

Signature Protection detects and prevents network-oriented attacks, operating-system-oriented attacks, and application-oriented attacks by comparing each packet to the set of signatures stored in the Signatures database.

The Signatures database is updated using the *Security Update Service* (SUS). For information on the SUS, see ERT Security Update Service (SUS), page 35. For information on updating the Signatures database see Updating a Radware Signature File, page 277 and/or Scheduling APSolute Vision and Device Tasks, page 284/Update Security Signature Files—Parameters, page 289. To view statistics on the SUS, go to the Security Control Center interface in APSolute Vision.

This section contains the following topics:

- Signature Protection in Radware DefensePro DDoS Mitigation, page 207
- Configuration Considerations with Signature Protection, page 208
- Configuring Signature Protection Profiles, page 209
- Managing Signature Protection Signatures, page 212
- Managing Signature Protection Filters, page 218
- Managing Signature Protection Attributes, page 230

Signature Protection in Radware DefensePro DDoS Mitigation

The Signature Protection module handles attacks of the following types:

- Server-based vulnerabilities:
  - Web-amplification vulnerabilities
  - Mail server vulnerabilities
  - FTP server vulnerabilities
  - SQL server vulnerabilities
  - DNS server vulnerabilities
  - SIP server vulnerabilities
- Worms and viruses
- Trojans and backdoors
- IRC bots
- Spyware
- Phishing

- Anonymizers
- Client-side vulnerabilities

Caution: Signatures for client-side vulnerabilities are prone to cause significant performance degradation.

You can configure Signature Protection using a set of *predefined signature profiles* for field installation or using user-defined signature profiles. The set of predefined signature profiles include protections for a corporate gateway, for a LAN DMZ, for carrier links, and so on.

You cannot edit the *predefined signature profiles*, but you can create a new profile according to the needs of your environment. For example, if you need to use only a small set of custom (that is, *user-defined*) signatures, you can create a new profile with those signatures and a new **Threat Type** attribute (see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231).

Notes

- If you require assistance creating a new signature, you can contact the relevantRadware department–according to your service agreement.
- The differences between the system-defined, Signature Protection profiles *All-DoS-Shield* and *DoS-All* are as follows:
  - The *All-DoS-Shield* profile includes all DoS-flood signatures that have low complexity–that is, without Application Security signatures. This profile provides protection against DoS floods (high-rate and/or high-volume attacks).
  - The *DoS-All* profile includes all types of DoS signatures: DoS-Shield signatures and Application Security signatures. This profile provides the same protection as the *All-DoS- Shield* profile with additional protection against application-level vulnerabilities and attack tools including low-and-slow DoS attacks.

Configuration Considerations with Signature Protection

Cisco recommends that you configure policies containing Signature Protection profiles using Networks with Source = *Any*, the public network, and Destination = Protected Network.

You can configure policies to use Context Groups, application ports, and physical ports.

For implications of direction settings for policies and protections, see Table 113 - Implications of Policy Directions, page 209.

You can configure policies containing Signature Protection profiles with **Direction** set to either **One Way** or **Two Way**.

You can configure protections with the **Direction** values **Inbound**, **Outbound**, or **In-Outbound**.

While most of the attacks (such as worm infections) are detected through their inbound pattern, some attacks require inspecting outbound patterns initiated by infected hosts. For example, trojans require inspecting outbound patterns initiated by infected hosts.

Policies configured with **Source = Any** and **Destination = Any** inspect only *In-Outbound* attacks.

Table 113: Implications of Policy Directions

Policy Direction	Policy Action	Packet Direction	Signature Direction		
			Inbound	Outbound	Inbound or Outbound
From To	One way	Ex to in	Inspect	Ignore	Inspect
		In to ex	Ignore	Ignore	Ignore
From To	Two way	Ex to in	Inspect	Ignore	Inspect
		In to ex	Ignore	Inspect	Inspect
Any to any	N/A	N/A	Inspect	Ignore	Inspect

Configuring Signature Protection Profiles

A Signature Protection profile contains one or more *rules* for the network segment that you want to protect. Each rule defines a query on the Signatures database. Radware DefensePro DDoS Mitigation activates protections from the Signatures database that matches the set of rules. User-defined profiles are updated each time you download an updated Signatures database.

To configure Signature Protection profiles, Signature Protection must be enabled, and global DoS Shield parameters must be configured. For more information, see Configuring Global Signature Protection, page 132 and Configuring Global DoS Shield Protection, page 132.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Signature Protection profiles.

Each rule in the profile can include one or more entries from the various *attribute types* (see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231).

Rules define a query on the Signatures database based on the following logic:

- Values from the same *type* are combined with logical OR.
- Values from different *types* are combined with logical AND.

The rules are combined in the profile with a logical OR.

The relationship inside a signature between all filters is a logical AND.

Caution: Use as few characters as possible for the Signature Protection profile name and attributes. Otherwise, Radware DefensePro DDoS Mitigation might not be able to add the profile to the device configuration. The maximum size of a Radware DefensePro DDoS Mitigation management packet is 1500 bytes. So, for example, if a management packet includes a Signature Protection profile name and long attribute-type names, the command will fail and Radware DefensePro DDoS Mitigation will not add the profile to the device configuration.

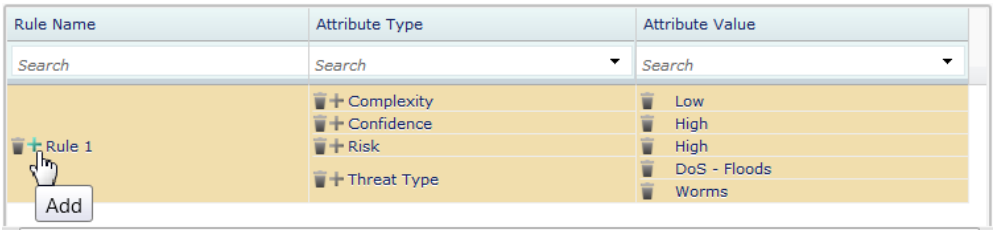
Notes

- Rules in the profile are *implicit*. That is, when you define a value, the rule includes all signatures that match a specific selected attribute *plus* all the signatures that have *no* attribute of that type. This logic ensures that signatures that *may* be relevant to the protected network are included—even if they are not associated explicitly with the application in the network.

- The difference between the system-defined, Signature Protection profiles *All-DoS-Shield* and *DoS-All* are as follows:
  - The *All-DoS-Shield* profile includes all DoS-flood signatures that have low complexity–that is, without Application Security signatures. This profile provides protection against DoS floods (high-rate. high-volume attacks).
  - The *DoS-All* profile includes all types of DoS signatures: DoS-Shield signatures and Application Security signatures. This profile provides the same protection as the *All-DoS- Shield* profile with additional protection against slow-rate attacks and DoS vulnerability.

To configure a Signature Protection profile

1. In the *Configuration* perspective, select **Protections > Signature Protection >Profiles**.
2. Do one of the following:
   - To add a profile, click the (Add) button, and in the **Profile Name** text box, type the name of the profile.
   - To edit a profile, double-click the entry in the table.
   - To display the list of signatures associated with the configured protections for the profile, double-click the entry in the table, and then, click **Show Matching Signatures**.
3. Configure a rule for the profile as follows:
   - To configure a new rule:
     a. Click the (Add) button above the rules table.
     b. In the **Rule Name** text box, type the name of the new rule.
     c. From the **Attribute Type** drop-down list, select the required value.
     d. In the **Attribute Value** drop-down list, type the required value.
     e. Click **Submit**.
   - To edit the attribute type and/or attribute value of a rule:
     a. In the *Rule Name* column of the table, move your cursor (pointer) to the name of the relevant rule and click the little (Add) button. The *Add Signature Profile Rule* tab opens, populated with the name of the selected rule.

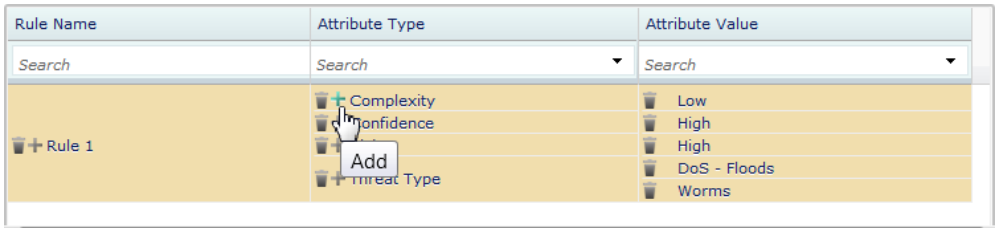


     b. From the **Attribute Type** drop-down list, select the required value.
     c. In the **Attribute Value** drop-down list, select or type the required value.
     d. Click **Submit**.

Note: For more information, see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231.

– To edit the **Attribute Value** of a rule:

a. In the *Attribute Type* column of the table, move your cursor (pointer) to the relevant attribute type of the relevant rule and click the little (Add) button. The *Add Signature Profile Rule* tab opens, populated with the name of the rule and the name of the selected attribute type.



b. In the **Attribute Value** drop-down list, select or type the required value.

c. Click **Submit**.

Note: For more information, see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231.

Note: Alternatively, to edit the **Attribute Type** and/or the **Attribute Value** of an existing profile, you can do the following:

a. Click the (Add) button above the rules table.

b. In the **Rule Name** text field, type the name of the rule that you are modifying.

c. From the **Attribute Type** drop-down list, select the required value.

d. In the **Attribute Value** drop-down list, type the required value.

e. Click **Submit**.

4. Repeat step 3 as required–to configure more rules for the profile, more attributes for rules, or more values for existing attribute types.

5. To save the signature profile configuration, click **Submit**.

Table 114: Signature Protection Profiles Parameters

Parameter	Description
Profile Name	The name of the signature profile.
Number of Matching Signatures	(Read-only) The number of signatures that match the profile. The number of matching signatures depends on the **Match Method** of the **Attribute Type** (see Viewing and Modifying Attribute Type Properties, page 231). The **Match Method** *Minimum* is relevant only for the attribute types **Complexity**, **Confidence**, and **Risk**, which have Attribute Values with ascending-descending levels. **Minimum** specifies that the *attribute value* includes the results for the lower-level Attribute Values. For example, for the attribute type **Risk** when the **Match Method** is **Minimum**, the *attribute value* **High** matches only *High*, not *Info*, *Low*, or *Medium*. **Minimum** is the default for **Complexity**, **Confidence**, and **Risk**.

Table 114: Signature Protection Profiles Parameters (cont.)

Parameter	Description
Show Matching Signatures	This button appears only when editing a profile. Click to display the list of signatures associated with the configured protections for the profile.

Table 115: Signature Profile Rules Table Parameters

Parameter	Description
The table displays details of the configured rules for the selected profile. Each rule can contain more than one attribute. Each rule can contain multiple *attribute types* and values. **Note:** For more information, see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231.	
Rule Name	The name of the signature profile rule.
Attribute Type	The list of predefined attribute types, which are based on the various aspects taken into consideration when defining a new attack.
Attribute Value	The value for the defined attribute type.

Managing Signature Protection Signatures

A signature is a building block of the Signature Protection profile. Each signature contains one or more protection *filters* and *attributes*, which determine which packets are malicious and how they are treated. The general parameters of a signature define how Radware DefensePro DDoS Mitigation tracks and treats malicious packets once Radware DefensePro DDoS Mitigation recognizes the signature in the traffic. Each attack is bound to a *tracking* function, which defines how Radware DefensePro DDoS Mitigation handles the packet when it is matched with a signature. The main purpose of these functions is to determine whether the packet is harmful and to apply an appropriate action.

Radware DefensePro DDoS Mitigation divides signatures into the followingtypes:

- **Application Security signatures**–Use the Application Security mechanism. Application Security signatures support high complexity and string matching.
- **DoS Shield signatures**–Use the DoS Shield mechanism. DoS Shield samples traffic flowing through the device and limits the bandwidth of traffic recognized as a DoS attack. DoS Shield signatures have low complexity; they do not support string matching. For more information, see Configuring Global DoS Shield Protection, page 132.

Radware DefensePro DDoS Mitigation provides predefined signatures, which are also referred to as *static* signatures. You can also define your own signatures as necessary. You can edit and remove only these *user-defined* signatures. For static signatures, you can edit only the general parameters. Any change that you make to a static signature causes Radware DefensePro DDoS Mitigation to identify that signature as a user-defined signature.

The *Signature Source Type* column in the table in the *Signatures / Application Security* or *Signatures / DoS Shield* tab displays **static** for static signatures and displays **user** for user-defined signatures. You can filter the table as you as you require.

The table that displays the signatures provide filters that enable viewing static and user-defined signatures most efficiently. You can define filtering criteria, so that all signatures that match the criteria are displayed in the Signatures table.

Caution: Radware DefensePro DDoS Mitigation may automatically add user-defined signatures to existing profiles even without a full attribute match. If you configure any user-defined signature, you must specify attributes in addition to the *default* attributes–the more the better. The default attributes of user-defined signatures are only Risk and Confidence. Unless you specify additional attributes, all other attributes in a user-defined signature are NULL. If all other attributes in a user- defined signature are NULL, Radware DefensePro DDoS Mitigation matches the signature against existing *static* profiles (such as DoS-ALL, DoS-SSL, and All-DoS-Shield), and treats the missing attributes in it (which are NULL) as existing, with default values. This causes Radware DefensePro DDoS Mitigation to add the user-defined signature to static profiles, which is improper. Therefore, Cisco recommends that you specify as many additional attributes as possible, and prevent Radware DefensePro DDoS Mitigation using your user-defined signature improperly.

To locate all the policies and profiles that use a specific signature

1. In the *Configuration* perspective, select **Protections > Signature Protection >Signatures**.
2. Select the relevant node: the **DoS Shield** node or the **Application Security** node.
3. Select the signature.
4. Click **Find Usages**.

To view Signature Protection signatures

> In the *Configuration* perspective, select**Protections > Signature Protection > Signatures**, and then, select the relevant node: the **DoS Shield** node or the **Application Security**node.

Note: To view all signatures, clear the text boxes at the top of the table columns, and then, click the (Filter) button.

To view Signature Protection signatures and filter the table by signature parameters

1. In the *Configuration* perspective, select **Protections > Signature Protection >Signatures**.
2. Select the relevant node: the **DoS Shield** node or the **Application Security** node.
3. Select the **Filter by ID** option button.
4. Enter the search criteria in the boxes under the column headings.
5. Click the (Filter) button.

To view Signature Protection signatures and filter the table by attribute parameters

1. In the *Configuration* perspective, select **Protections > Signature Protection >Signatures**.
2. Select the relevant node: the **DoS Shield** node or the **Application Security** node.
3. Select the **Filter by Attribute** option button.

4. Enter the search criteria in the boxes under the column headings.

Note: For example, for **Attribute Type**, select from the list of predefined attribute types, which are based on the various aspects taken into consideration when defining a new attack. For more information, see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231.

5. Click the  (Filter) button.

Managing Application Security Signatures

The table in the *Application Security* pane displays all the Application Security (AppSec) signatures stored on the device. You can create new signatures as necessary.

To configure an Application Security signature

1. In the *Configuration* perspective, select **Protections > Signature Protection > Signatures > Application Security**.
2. To add or edit a signature, do one of the following:
   - To add a signature, click the  (Add) button.
   - To edit a signature, display the required signature, then double-click the signature.
3. Configure the parameters, and then, click **Submit**.

Table 116: Signature: General Parameters

Parameter	Description
Enabled	Specifies whether the signature can be used in protection profiles.
Signature Name	The name of the signature. Maximum characters: 29
Signature ID	(Read-only) The ID assigned to the signature by the system.
Direction	The protection inspection path. The protections can inspect the incoming traffic only, the outgoing traffic only, or both. Values: Inbound, Outbound, Inbound and Outbound Default: Inbound and Outbound

Table 116: Signature: General Parameters (cont.)

Parameter	Description
Tracking Type	Specifies how Radware DefensePro DDoS Mitigation determines which traffic to block or drop when under attack. Values: • Track All–Select this option when each packet of the defined attack is harmful, for example, Code Red and Nimda attacks. • Source Count–Select this option when the defined attack is source- based–that is, the attack can be recognized by its source address, for example, a *horizontal port scan*, where the hacker scans a certain application port (TCP or UDP) to detect which servers are available in the network. • Destination Count–Select this option when the defined attack is destination-based–that is, the hacker is attacking a specific destination, such as a Web server, for example, Ping Floods or DDoS attacks. • Source and Destination Count–Select this option when the attack type is a source- and destination-based attack–that is, the hacker is attacking from a specific source IP to a specific destination IP address, for example, port-scan attacks.
Tracking Period (This parameter is active only whenthe **Tracking Type** is *not* **Track All**.)	The time, in seconds, for measuring the **Active Threshold**. When a number of packets exceeding the **Active Threshold** passes through the device within the configured **Tracking Period**, Radware DefensePro DDoS Mitigation considers the attack to be active. Values: 1–300 Default: 1 **Note:** When the value for **Tracking Type** is **Track All**, the value is read- only, and Radware DefensePro DDoS Mitigation ignores the parameter.
Activation Threshold (This parameter is active only when the **Tracking Type** is *not* **Track All**.)	The number of attack packets per **Tracking Period** that pass through the device on to their destination. Values: 2–1,000,000 Default: 50 **Note:** When the value for **Tracking Type** is **Track All**, the value is read- only, and Radware DefensePro DDoS Mitigation ignores the parameter.
Drop Threshold (This parameter is active only whenthe **Tracking Type** is *not* **Track All**.)	The attack packets per **Tracking Period** after an attack is considered to be active above which Radware DefensePro DDoS Mitigation starts dropping excessive traffic. The value must be higher than the value for the **Termination Threshold** parameter. Values: 0–1,000,000 Default: 50 **Note:** When the value for **Tracking Type** is **Track All**, the value is read- only, and Radware DefensePro DDoS Mitigation ignores the parameter.
Termination Threshold (This parameter is active only when the **Tracking Type** is *not* **Track All**.)	The number of attack packets per **Tracking Period** below which the profile changes the attack from active mode to inactive mode. Values: 0–1,000,000 Default: 50 **Note:** When the value for **Tracking Type** is **Track All**, the value is read- only, and Radware DefensePro DDoS Mitigation ignores the parameter.

Table 116: Signature: General Parameters (cont.)

Parameter	Description
Action	The action that Radware DefensePro DDoS Mitigation takes when an attack is detected. Values: • Drop–Radware DefensePro DDoS Mitigation discards the packet. • Reset Destination–Radware DefensePro DDoS Mitigation sends a TCP- Reset packet to the destination address. This action works only when the filter for the signature has **TCP** specified for the **Protocol** (see Managing Signature Protection Filters, page 218). • Report Only–Radware DefensePro DDoS Mitigation forwards the packet to the defined destination. • HTTP 200 OK–Radware DefensePro DDoS Mitigation sends a 200 OK response using an empty page and leaves the server-side connection open. • HTTP 200 OK and Reset Destination–Radware DefensePro DDoS Mitigation sends a 200 OK response using an empty page and sends a TCP-Reset packet to the server side to close the connection. • HTTP 403 Forbidden–Radware DefensePro DDoS Mitigation sends a 403 Forbidden response using an empty page and leaves the server-side connection open. • HTTP 403 Forbidden and Reset Destination–Radware DefensePro DDoS Mitigation sends a 403 Forbidden response using an empty page and sends a TCP-Reset packet to the server side to close the connection. Default: Drop **Caution:** The **Action** option that you specify in the signature always overrides the specified action behavior in the Protection policy. For example, if you specify **Report Only** in the policy, and you specify **Drop** in the signature, the action behavior of the Protection policy is *report only*, but the behavior for traffic matching the signature is *drop*. **Note:** The *HTTP...* options (that is, **HTTP 200 OK**, and so on) perform a legal termination of the connection over HTTP (including termination at the TCP level)–as opposed to a *drop* or *reset* at the TCP level. The *HTTP...* options are designed especially for content-delivery-network (CDN) environments. In a CDN environment, the real source IP address is typically found in the X-Forwarded-For (XFF) HTTP header. Radware DefensePro DDoS Mitigation can use a user-defined signature (sometimes referred to as a *custom signature*) for the accurate identification and blocking of a malicious source IP address. The signature is based on the real source of an HTTP attack–using the XFF header. A CDN may perceive common Drop or Reset actions as an indication of a server problem. The *HTTP...* options overcome this problem. Furthermore, Radware DefensePro DDoS Mitigation creates the messages of the *HTTP...* options in such a way as to avoid caching in the CDN.
Packet Reporting	Enables the sending of sampled attack packets to APSolute Vision for offline analysis. Default: Disabled

Table 117: Signature: Attack Description

Parameter	Description
	(Read-only) A description of the static signature. You cannot configure a description for a user-defined signature.

Table 118: Signature: Filter Table

Parameter	Description
	The *Filter Table* contains the filters for the signature. Filters match scanned packets with attack signatures in the Signatures database. An Application Security signature must include at least one *filter* to scan and classify traffic. Application Security signatures use a logical AND between the filters. **Caution:** Each time that you configure a new signature or edit an existing signature, after you click **Submit** for the *filter*, click **Submit** on the *Add New Signature* / *Edit Signature* pane. This is necessary to ensure that the filter is valid and added to the configuration of the signature. **Note:** For more information, see Managing Signature Protection Filters, page 218.

Table 119: Signature: Attributes Table

Parameter	Description
	The attributes for the signature determine the attack characteristics used in the rule creation process. The attributes in the *Attributes Table* tab are defined in the *Attributes* tab (see Managing Signature Protection Attributes, page 230). To add an attribute, in the table, click the (Add) button. **Note:** For more information, see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231.

To locate all the policies and profiles that use a specific signature

1. In the *Configuration* perspective, select **Protections > Signature Protection > Signatures > Application Security**.
2. Select the signature.
3. Click **Find Usages**.

Managing Signature Protection Filters

Filters match scanned packets with attack signatures in the Signatures database.

An Application Security signature must include at least one *filter* to scan and classify traffic. A signature *may* include multiple *filters*.

Application Security signatures use a logical AND between the selected filters.

To configure a filter for an Application Security signature

1. In the *Configuration* perspective, select **Protections > Signature Protection > Signatures > Application Security**.
2. Do one of the following:
   - To add a signature, click the (Add) button.
   - To edit a signature, double-click the entry in the table.
3. If you are configuring a new signature, in the **Signature Name** field, type the name forthe signature.
4. Select the *Filter Table* tab, and do one of the following:
   - To add a filter, click the (Add) button.
   - To edit a filter, double-click the entry in the table.
5. Configure the filter parameters, and then, click **Submit**. The *Add New Signature* / *Edit Signature* pane is displayed.
6. Configure other parameters for the signature, as you require.
7. In the *Add New Signature* or *Edit Signature* pane, click **Submit**. If the filter is valid, Radware DefensePro DDoS Mitigation adds the filter to the configuration of the signature.

Table 120: Filter: General Parameters

Parameter	Description
Each filter has a specified name and specified protocol-properties parameters.	
Filter Name	The name of the signature filter.
Protocol	Values: • ICMP • ICMPv6 • IP • TCP • UDP Default: IP
Source Application Port (This parameter is available only when the **Protocol** is **UDP** or **TCP**.)	The *source* application port or Application port-group class that the filter applies on UDP or TCP traffic. **Note:** For information on Application port-group classes, see Managing Application Classes, page 155.

Table 120: Filter: General Parameters (cont.)

Parameter	Description
Destination Application Port (This parameter is available only when the **Protocol** is **UDP** or **TCP**.)	The *destination* application port or Application port-group class that the filter applies on UDP or TCP traffic. **Note:** For information on Application port-group classes, see Managing Application Classes, page 155.

Table 121: Filter: Packet Parameters

Parameter	Description
Packet parameters are used to match the correct packet length in different layers.	
Packet Size Type	Specifies whether the length is measured for Layer 7 content. Values: • L7—The L4 data part of the packet is measured (excluding the Layer 2/Layer 3/Layer 4 headers). • None Default: None
Packet Size Length	The range of values for packet length. The size is measured per packet only. The size is not applied on reassembled packets. Fragmentation of Layer 7 packets may result in tails that do not contain the Layer 7 headers. The check is bypassed, because no match with Type = L7 is detected.

Table 122: Filter Parameters for Signatures: OMPC Parameters

Parameter	Description
Offset Mask Pattern Condition (OMPC) parameters are a set of attack parameters that definerules for pattern lookups. The OMPC rules look for a fixed size pattern of up to four bytes that uses fixed offset masking. This is useful for attack recognition, when the attack signature is a TCP/IP header field or a pattern in the data/payload in a fixed offset.	
OMPC Condition	The OMPC condition. Values: • Equal • Greater Than • Not Applicable • Less Than • Not Equal Default: Not Applicable

Table 122: Filter Parameters for Signatures: OMPC Parameters (cont.)

Parameter	Description
OMPC Length	The length of the OMPC (Offset Mask Pattern Condition) data. Values: • Not Applicable • 1 Byte • 2 Bytes • 3 Bytes • 4 Bytes Default: 1 Byte
OMPC Offset	The location in the packet, in bytes, from where data checking starts looking for specific bits in the IP/TCP header. Values: 0–65,535 Default: 0
OMPC Offset Relative to	Specifies to which OMPC offset the selected offset is relative. Values: • Ethernet • IP Data • IP Header • IPv6 Header • L4 Data • L4 Header • None Default: None
OMPC Pattern	The fixed size pattern within the packet that OMPC rules attempt to find. Values: A combination of hexadecimal numbers (0 –9, a–f). The value is defined by the **OMPC Length** parameter. The **OMPC Pattern** definition contain eight symbols. When the **OMPC Length** is less than four bytes, complete it with zeros. For example, when the **OMPC Length** is two bytes, the **OMPC Pattern** can be abcd0000. Default: 00000000
OMPC Mask	The mask for the OMPC data. Values: A combination of hexadecimal numbers (0 –9, a–f). The value is defined by the **OMPC Length** parameter. The **OMPC Mask** definition contains eight symbols. When the **OMPC Length** value is less than four bytes, complete it with zeros. For example, When the **OMPC Length** is two bytes, the OMPC Mask can be abcd0000. Default: 00000000

Table 123: Filter Parameters for Signatures: Content Parameters

Parameter	Description
The Content parameters are available only when the **Protocol** specified for the filter is **ICMP**, **ICMPv6**, **TCP**, or **UDP** (that is, any **Protocol** option except for **IP**). The Content parameters define the rule for a text/content string lookup for attack recognition, when the attack signature is a text/content string within the packet payload. For convenience, refer to Table 124 - Content Parameters per Content Type, page 224.	
Content Type	The content type that the filter tries to match. When **Content Type** is *not* **None**, the **Content to Match** field becomes available, and other Content parameters may be supported or required. When the **Protocol** for the filter is **TCP**, RadwareDefensePro DDoS Mitigation allows a filter *Content* configuration with any **Content Type** option. When the **Protocol** for the filter is **ICMP**, **ICMPv6**, or **UDP**, Radware DefensePro DDoS Mitigation allows a filter Content configuration only when the **Content Type** option is **Text**. Values: • None—The filter does not try to match the content of the packet based on type. • Text—Anywhere from the beginning of the Layer 7 header. • HTTP Request Header • HTTP Request Data • HTTP URL—The URL found in the very first header of each HTTP request, in its non-canonicalized, *as-is* format. • Normalized HTTP URL—The URL found in the very first header of each HTTP request, after Radware DefensePro DDoS Mitigation has canonicalized it. To avoid evasion techniques when classifying HTTP requests, the URL content is transformed into its canonical representation, interpreting the URL the same way the server would. • HTTP Host Name • HTTP Cookie Header • HTTP Response Header • HTTP Response Data The canonicalization (normalization) procedure supports the following: — Directory referencing by reducing /./into /or A/B/../ to A/. — Changing backslash (\) to slash (/). — Changing HEX encoding to ASCII characters. For example, the hex value %20is changed to a space. — Unicode support, UTF-8 and IIS encoding. Default: None

Table 123: Filter Parameters for Signatures: Content Parameters (cont.)

Parameter	Description
Search Settings for the Content	
Content to Match	The content name to search for (for example, the *key* name) according to the selected **Content Type**. Values: <space> ! " # $ % & ' ( ) * + , -. / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~ Maximum characters: 255 **Caution:** A value is required when **Content Type** is not **None**. Example: The **Protocol** for the filter is **TCP**. **Content Type** is **HTTP Cookie Header**. **Content to Match** is **qwerty**. **Content Value to Match** is empty. The filter searches HTTP-cookie- header keys up to the equals sign (=). A packet with **qwerty=** anywhere in the HTTP cookie header matches the filter.
Search Using Regular Expression	Specifies whether the **Content to Match** field value is formatted as a regular expression (and not as free text to search). You can set a regex search for all content types.
Encoding for the Content	The encoding of the content specified in the **Content Type** field. Values: • Not Applicable • Case Insensitive • Case Sensitive • Hex Default: Not Applicable **Caution:** This field cannot be **Not Applicable** when **Content to Match** has a value.
Start Search at Offset (This parameter is available only when **Content Type** is **Text**.)	The location in the packet from which the content is checked. The location is measured from the beginning of the L7 header. Values: 0–65,535 Default: 0
Stop Search at Offset (This parameter is available only when **Content Type** is **Text**.)	The maximum length to be searched within the selected **Content Type**. The location is measured from the beginning of the L7 header. Values: 0–65,535 Default: 0 **Caution:** The value for this field must be equal to or greater than the **Start Search at Offset** value.

Table 123: Filter Parameters for Signatures: Content Parameters (cont.)

Parameter	Description
Search Settings for the Content Value	
Content Value to Match (This parameter is available only when **Content Type** is **HTTP Cookie Header**, **HTTP Request Data**, **HTTP Request Header**, **HTTP Response Data**, **HTTP Response Header**, or **Text**.)	The value associated with the specified **Content to Match** for the selected **Content Type**. The filter searches for the specified **Content Value to Match** only after finding a match for the **Content to Match** value. Maximum characters: 255 **Caution:** This field requires a value when **Distance from Content to Content Value** has a value. Examples: • The **Protocol** for the filter is **TCP**. **Content Type** is **HTTP Request Data**. **Content to Match** is **ip_addr**. **Content Value to Match** is **10.0.0.1**. The filter searches HTTP- request-data and finds **ip_addr**. **Distance from Content to Content Value** is empty. A packet with **ip_addrs!@#$%10.0.0.1** anywhere in the HTTP request data matches the filter. • **Content Type** is **Text**. **Content to Match** is **qwerty**. **Content Value to Match** is **10.0.0.1**. **Distance from Content to Content Value** is **0**. A packet with **ip_addr10.0.0.1** anywhere packet matches the filter.
Search Using Regular Expression	Specifies whether the **Content Value to Match** field value is formatted as a regular expression (and not as free text to search).
Encoding for Content Value	The encoding of the content specified in the **Content Value to Match** field. Values: • Not Applicable • Case Insensitive • Case Sensitive • Hex Default: Not Applicable **Caution:** This field cannot be **Not Applicable** when **Content Value to Match** has a value.

Table 123: Filter Parameters for Signatures: Content Parameters (cont.)

Parameter	Description
Distance from Content to Content Value (This parameter is available only when **Content Type** is **HTTP Request Data**, **HTTP Response Data**, or **Text**.)	The number of bytes or range of bytes between the location of the **Content to Match** and the location of the **Content Value to Match** within the specified **Content Type**. To specify a range, use a hyphen (-) between the start and end values. Values: • *empty*—The filter searches for the **Content Value to Match** anywhere after the **Content to Match** within the specified **Content Type**. • 0–1000 —The filter searches for the **Content Value to Match** at the exact number of byte after the **Content to Match** within the specified **Content Type**. • *A range, 0–1000, using a hyphen (-) between a start and end value* —The filter searches for the **Content Value to Match** in the specified range after the **Content toMatch** within the specified **Content Type**. Example: 3-1000

The following table lists the *available* or *required* Content-parameter values for each **Content Type**.

Table 124: Content Parameters per Content Type

Content Type	Content to Match	Start Search at Offset	Stop Search at Offset	Content Value to Match	Distance from Content to Content Value
HTTP Cookie Header	Required	-	-	Available	-
HTTP Host Name	Required	-	-	-	-
HTTP Request Data	Required	-	-	Available	Available when **Content Value to Match** is specified.
HTTP Request Header	Required	-	-	Available	-
HTTP Response Data	Required	-	-	Available	Available when **Content Value to Match** is specified.
HTTP Response Header	Required	-	-	Available	-
HTTP URL	Required	-	-	-	-
Normalized HTTP URL	Required	-	-	-	-
Text	Required	Available	Available	Available	Available when **Content Value to Match** is specified.

Managing DoS Shield Signatures

The table in the *DoS Shield* pane displays all the DoS Shield signatures stored on the device. The names of the default DoS Shield signature usually start with *DOSS*. You can modify the DoS Shield signatures and create new ones as necessary.

To configure a DoS Shield signature

1. In the *Configuration* perspective, select **Protections > Signature Protection > Signatures > DoS Shield**.
2. To add or edit a signature, do one of the following:
   - To add a signature, click the  (Add) button.
   - To edit a signature, display the required signature, then double-click the signature.
3. Configure the parameters, and then, click **Submit**.

Table 125: Signature (DoS Shield): General Parameters

Parameter	Description
Signature Name	The name of the signature. Maximum characters: 29
Signature ID	(Read-only) The ID assigned to the signature by the system.
Enabled	Specifies whether the signature can be used in protection profiles.
Direction	The protection inspection path. The protections can inspect the incoming traffic only, the outgoing traffic only, or both. Values: Inbound, Outbound, Inbound and Outbound Default: Inbound and Outbound
Tracking Type	(Read-only) Specifies how Radware DefensePro DDoS Mitigation determines which traffic to block or drop when under attack. Value: Sampling–This option is geared to the DoS Shield mechanism.
Tracking Period	The time, in seconds, for measuring the **Activation Threshold**. When a number of packets exceeding the Activation Threshold passes through the device within the configured **Tracking Period**, Radware DefensePro DDoS Mitigation considers the attack to be active. Values: 1–300 Default: 1
Activation Threshold	The number of attack packets per **Tracking Period** that pass through the device on to their destination. Values: 2–1,000,000 Default: 50
Drop Threshold	The number of attack packets per **Tracking Period** after an attack is considered to be active above which Radware DefensePro DDoS Mitigation starts dropping excessive traffic. The value must be higher than the value for the **Termination Threshold** parameter. Values: 0–1,000,000 Default: 50

Table 125: Signature (DoS Shield): General Parameters (cont.)

Parameter	Description
Termination Threshold	The number of attack packets per **Tracking Period** below which the profile changes the attack from active mode to inactive mode. Values: 0–1,000,000 Default: 50
Action	The action that Radware DefensePro DDoS Mitigation takes when an attack is detected. Values: • Drop–Radware DefensePro DDoS Mitigation discards the packet. • Report Only–Radware DefensePro DDoS Mitigation forwards the packet to the defined destination. Default: Drop **Caution:** The **Action** option that you specify in the signature always overrides the specified action behavior in the Protection policy. For example, if you specify **Report Only** in the policy, and you specify **Drop** in the signature, the action behavior of the Protection policy is *report only*, but the behavior for traffic matching the signature is *drop*.
Packet Reporting	Enables the sending of sampled attack packets to APSolute Vision for offline analysis. Default: Disabled

Table 126: Signature (DoS Shield): Attack Description

Parameter	Description
(Read-only) A description of the static signature. You cannot configure a description for a user-defined signature.	

Table 127: Signature (DoS Shield): Filter Table

Parameter	Description
A DoS Shield signature can include one or more simple filters to scan and classify predefined traffic. Filters match scanned packets with attack signatures in the Signatures database. To add a filter, in the table, click the (Add) button. For more information, see Configuring Filters for a DoS Shield Signature, page 227.	

Table 128: Signature (DoS Shield): Attributes Table

Parameter	Description
The attributes for the signature determine the attack characteristics used in the rule creation process. The attributes in the *Attributes Table* tab are defined in the *Attributes* tab (see Managing Signature Protection Attributes, page 230). To add an attribute, in the table, click the (Add) button. **Note:** For more information, see Managing Signature Protection Attributes, page 230 and Viewing and Modifying Attribute Type Properties, page 231.	

To locate all the policies and profiles that use a specific DoS Shield signature

1. In the *Configuration* perspective, select **Protections > Signature Protection > Signatures > DoS Shield**.
2. Select the signature.
3. Click **Find Usages**.

Configuring Filters for a DoS Shield Signature

A DoS Shield signature can include one or more simple filters to scan and classify predefined traffic. Filters match scanned packets with attack signatures in the Signatures database.

To configure a filter for a DoS Shield signature

1. In the *Configuration* perspective, select **Protections > Signature Protection > Signatures > DoS Shield**.
2. In the *Filter Table* tab, do one of the following:
   - To add an entry, click the (Add) button.
   - To edit an entry, double-click the row.
3. Configure the parameters, and then, click **Submit**.

Table 129: Filter Parameters for DoS Shield Signatures: General Parameters

Parameter	Description
Each filter has a specified name and specified protocol-properties parameters.	
Filter Name	The name of the signature filter.
Protocol	The protocol used. Values: • ICMP • ICMPv6 • IP • TCP • UDP Default: IP

Table 129: Filter Parameters for DoS Shield Signatures: General Parameters (cont.)

Parameter	Description
Source Application Port (This parameter is available only when the **Protocol** is **UDP** or **TCP**.)	The *source* application port or Application port-group class that the filter applies on UDP or TCP traffic. **Note:** For information on Application port-group classes, see Managing Application Classes, page 155.
Destination Application Port (This parameter is available only when the **Protocol** is **UDP** or **TCP**.)	The *destination* application port or Application port-group class that the filter applies on UDP or TCP traffic. **Note:** For information on Application port-group classes, see Managing Application Classes, page 155.

Table 130: Filter Parameters for DoS Shield Signatures: PacketParameters

Parameter	Description
Packet parameters are used to match the correct packet length in different layers.	
Packet Size Type	Specifies whether the length is measured for Layer 7 content. Values: • L7—The L4 data part of the packet is measured (excluding the Layer 2/Layer 3/Layer 4 headers). • None Default: None
Packet Size Length	The range of values for packet length. The size is measured per packet only. In non-first IP-fragmented frames, Radware DefensePro DDoS Mitigation uses the L3 content size as the packet size.

Table 131: Filter Parameters for DoS Shield Signatures: OMPCParameters

Parameter	Description
Offset Mask Pattern Condition (OMPC) parameters are a set of attack parameters that definerules for pattern lookups. The OMPC rules look for a fixed size pattern of up to four bytes that uses fixed offset masking. This is useful for attack recognition, when the attack signature is a TCP/IP header field or a pattern in the data/payload in a fixed offset. **Note:** If the value for **OMPC Condition** is **Not Applicable**, the other parameters in this tab must use the default values.	
OMPC Condition	The OMPC condition. Values: • Equal • Greater Than • Not Applicable • Less Than • Not Equal

	Default: Not Applicable

Table 131: Filter Parameters for DoS Shield Signatures: OMPC Parameters (cont.)

Parameter	Description
OMPC Length	The length of the OMPC data. Values: • Not Applicable • 1 Byte • 2 Bytes • 3 Bytes • 4 Bytes Default: 1 Byte
OMPC Offset	The offset location, in bytes, in the packet from where data checking starts looking for specific bits in the IP/TCP header. Values: 0–65,535 Default: 0
OMPC Offset Relative to	Specifies to which OMPC offset the selected offset is relative. Values: • Ethernet • IP Data • IP Header • IPv6 Header • L4 Data • L4 Header • None Default: None
OMPC Pattern	The fixed size pattern within the packet that OMPC rules attempt to find. Values: A combination of hexadecimal numbers (0 –9, a–f). The value is defined by the **OMPC Length** parameter. The **OMPC Pattern** definition contain eight symbols. When the **OMPC Length** is less than four bytes, complete it with zeros. For example, when the **OMPC Length** is two bytes, the **OMPC Pattern** can be abcd0000. Default: 00000000
OMPC Mask	The mask for the OMPC data. Values: A combination of hexadecimal numbers (0 –9, a–f). The value is defined by the OMPC Length parameter. The **OMPC Mask** definition contains eight symbols. When the **OMPC Length** value is less than four bytes, complete it with zeros. For example, When the **OMPC Length** is two bytes, the OMPC Mask can be abcd0000. Default: 00000000

Managing Signature Protection Attributes

Attributes are components of the protection policies set in the process of *rule-based* profile configuration. Attributes are organized according to types, based on the various aspects taken into consideration when defining a new attack—such as environment, applications, threat level, risk levels, and so on.

Each signature is assigned with attributes of different types.

You can use the existing attribute types and attribute values, add new attribute values, and remove user-defined attribute values from the list.

Attribute values are derived from the Signatures database and are added dynamically with any update.

The following table describes the attribute types. To view the properties of each attribute type, in the *Configuration* perspective, select **Protections > Signature Protection > Attributes > Attribute Type Properties**. For more information, see Viewing and Modifying Attribute Type Properties, page 231.

Table 132: Attribute Types

Attribute Type	Description
Applications	The applications that are vulnerable to this exploit. Attribute values include, for example: Web servers, mail servers, browsers
Complexity	The level of analysis performed as part of the attack lookup mechanism. Default attribute values: • Low—This signature has negligible impact on device performance. • High—This signature has stronger impact on the device performance. **Note:** For this attribute type, you can specify the **Match Method** (**Minimum** or **Exact**). For more information, see Viewing and Modifying Attribute Type Properties, page 231.
Confidence	The level of certainty with which a signature match can be trusted. The confidence level is the opposite of the false-positive level associated with a signature. For example, if **Confidence** is set to **High**, there is a *low* expectation of false positives. Values: Low, High, Medium **Notes:** • For this attribute type, you can specify the **Match Method** (**Minimum** or **Exact**). For more information, see Viewing and Modifying Attribute Type Properties, page 231. • In user-defined signatures, this attribute type is configured by default, but you can change the attribute value or delete the attribute type.
Groups	Enables you to create customized attack groups.
Platforms	The operating systems that are vulnerable to this exploit. Attribute values include, for example: Windows, Linux, Unix

Table 132: Attribute Types (cont.)

Attribute Type	Description
Risk	The risk associated with the attack. For example, attacks that impact the network are very severe and are defined as high-risk attacks. Values: Info, Low, Medium, High **Notes:** • For this attribute type, you can specify the **Match Method** (**Minimum** or **Exact**). For more information, see Viewing and Modifying Attribute Type Properties, page 231. • In user-defined signatures, this attribute type is configured by default, but you can change the attribute value or delete the attribute type.
Services	The protocol that is vulnerable to this exploit. Attribute values include, for example: FTP, HTTP, DNS
Target	The target of the threat–client side or server side.
Threat Type	The threats that best describe the signature. Attribute values include, for example: floods, worms

To configure a Signature Protection attribute value

1. In the *Configuration* perspective, select **Protections > Signature Protection >Attributes**.
2. Click the (Add) button.
3. Select the attribute type, and enter the attribute value.
4. Click **Submit**.

Viewing and Modifying Attribute Type Properties

Use the *Attribute Type Properties* pane to view the properties of the attribute types that the device supports. You can also change the **Match Method** for the attribute types **Complexity**, **Confidence**, and **Risk**.

You can view the following properties of the attribute types:

- **Multiple Values in Signature**–Specifies whether the attribute type may contain multiple values in any one signature.
- **Multiple Values in Rule**–Specifies whether the attribute type may contain multiple values in any one signature profile rule.
- **Configurable in Static**–Specifies whether the attribute type may contain multiple values in signatures from the signature file.
- **Match Method**–Relevant only for the attribute types **Complexity**, **Confidence**, and **Risk**, which have *attribute values* with ascending-descending levels.

  Values:

  — **Minimum**–Specifies that the attribute value includes the results for the lower-level attribute values.

  For example, when the **Match Method** is **Minimum**:

  • For the attribute type **Complexity**, the attribute value *Medium* matches only **Low** and

Medium—not **High**.

- For the attribute type **Confidence**, the attribute value *Medium* matches only **Medium** and **High**—not **Low**.

- For the attribute type **Risk**, the attribute value *Medium* matches only **Medium** and **High** —not **Info** or **Low**.

– **Exact** —Specifies that the attribute value uses only its own results. For example, when the attribute type is **Risk** and the **Match Method** is **Exact**, the attribute value **High** uses only High-risk results.

Caution: If the **Match Method** for the **Complexity** attribute type is **Minimum**, there must be no user-defined attribute value.

To view the properties of the attribute types that the device supports

> In the *Configuration* perspective, select **Protections > Signature Protection > Attributes > Attribute Type Properties**.

Use the following procedure to change the **Match Method** for the attribute types **Complexity**, **Confidence**, and **Risk**. The default **Match Method** option is **Minimum**.

To change the Match Method for Complexity, Confidence, or Risk attribute types

1. In the *Configuration* perspective, select **Protections > Signature Protection > Attributes > Attribute Type Properties**.
2. Double-click the attribute type.
3. From the **Match Method** drop-down list, select **Minimum** or **Exact**.
4. Click **Submit**.

Configuring SYN Flood Protection Profiles

SYN Flood Protection profiles defend against SYN-flood attacks.

You can configure up to 50 SYN Flood Protection profiles on a Radware DefensePro DDoS Mitigation instance.

During a SYN-flood attack, the attacker sends a volume of TCP SYN packets requesting new TCP connections without completing the TCP handshake, or completing the TCP handshake, but not requesting data. This fills up the server connection queues, which denies service to legitimate TCP users.

Before you configure a SYN Flood Protection profile, ensure the following:

- The Session Table **Lookup Mode** is **Full L4**.
- SYN Flood Protection is enabled and the global parameters are configured (*Configuration* perspective, **Setup > Security Settings > SYN Flood Protection**).
- You can change the global settings. The SYN Flood Protection global settings apply to all the profiles on the device. For more information, see Configuring Global SYN Flood Protection, page 134.

To configure a SYN Flood Protection profile

1. In the *Configuration* perspective, select **Protections > SYN Flood ProtectionProfiles**.
2. Do one of the following:
   - To add a profile, click the (Add) button. Enter the profile name, and then, click **Submit**.
   - To edit a profile, double-click the entry in the table.
3. To add a SYN-flood protection to the profile, do the following:
   a. Click the (Add) button.
   b. From the *Profile Name* drop-down list, select the protection.
   c. Click **Submit**.
4. To define additional SYN-flood protections for the profile, click **Go to SYN FloodProtections Table**.

Note: A SYN Flood Protection profile should contain all the *SYN-flood protections* that you want to apply in a Protection policy.

Table 133: SYN Flood Protection Profile Parameters

Parameter	Description
Profile Name	(Read-only) The name of the profile.
SYN Flood Protection Table	Contains the protections applied for the selected profile. To add a protection, in the table, click the (Add) button, select the protection name, and then, click **Submit**. **Note:** In each Protection policy, you can use only one SYN profile. Therefore, ensure that all the protections that you want to apply to a rule are contained in the profile the policy.
Go to SYN Flood Protections Table (button)	Opens the *SYN Flood Protections* pane in which you can add and modify SYN-flood protections.
Go to Profile Parameters (button)	Opens the *Profile Parameters* pane in which you can view and modify the configuration of the SYN Flood Protection profiles.

Defining SYN Flood Protections

After you define SYN-flood protections, you can add them to SYN Flood Protection profiles.

To define a SYN-flood protection

1. In the *Configuration* perspective, select **Protections > SYN Flood Protection Profiles > SYN Flood Protections**.
2. To add or modify a protection, do one of the following:
   - To add a protection, click the (Add) button.
   - To edit a protection, double-click the entry in the table.

3. Configure the parameters, and then, click **Submit**.

Table 134: SYN Flood Protection Parameters

Parameter	Description
Protection Name	A name for easy identification of the attack for configuration and reporting. **Note:** Predefined SYN-flood protections are available for the most common applications: FTP, HTTP, HTTPS, IMAP, POP3, RPS, RTSP, SMTP, and Telnet. The thresholds are predefined by Radware. You can change the thresholds for these attacks.
Protection ID	(Read-only) The ID number assigned to the protection.
Protection Defined By	(Read-only) Specifies whether the SYN-flood protection is a predefined (static) or user-defined (user) protection.
Application Port Group	The group of TCP ports that represent the application that you want to protect. Select from the list predefined port groups, or leave the field empty to select any port.
Activation Threshold	The behavior of the threshold differs depending on the connection protocol, as follows: • For HTTP and HTTPS–This parameter specifies the number of total SYN packets minus the number of total first data packets received per second at a certain destination above which Radware DefensePro DDoS Mitigation starts the challenge actions. • For all protocols other than HTTTP and HTTPS–This parameter specifies the number of SYN packets minus the number of first ACK packets received per second at a certain destination above which Radware DefensePro DDoS Mitigation starts the challenge actions. Values: 1–150,000 Default: 2500
Termination Threshold	The number of total SYN packets minus the total number of verified RST packets received per second at a certain destination for specified **Tracking Time**[1] below which Radware DefensePro DDoS Mitigation stops the challenge actions. Values: 0–150,000 Default: 1500
Risk Level	The risk level assigned to this attack for reporting purposes. Values: Info, Low, Medium, High Default: Low

1 – You can configure this value at **Setup > Security Settings > SYN Flood Protection> Tracking Time**.

Recommended Verification Type Values

The following table lists the Verification Type values that Cisco recommends.

Table 135: Verification Type Values Parameters

Protocol	Destination Port	Verification Type
FTP_CNTL	21	ack

Table 135: Verification Type Values Parameters (cont.)

Protocol	Destination Port	Verification Type
HTTP	80	request
HTTPS	443	request
IMAP	143	ack
POP3	110	ack
RPC	135	ack
RTSP	554	request
SMTP	25	ack
TELNET	23	ack

Managing SYN Flood Protection Profile Parameters

After you define a SYN Flood Protection profile, you can configure the authentication parameters for it.

To configure SYN Flood Protection profile parameters

1. In the *Configuration* perspective, select **Protections > SYN Flood Protection Profiles> Profiles Parameters**.
2. Double-click the relevant profile.
3. Configure the parameters, and then, click **Submit**.

Table 136: SYN Flood Protection Profile Parameters

Parameter	Description
Profile Name	(Read-only) The name of the profile.
Profile Action	The action that the profile takes on traffic matching the attack footprint during an attack. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.

Table 136: SYN Flood Protection Profile Parameters (cont.)

Parameter	Description
Tracking Method	
Tracking Method	Values: • Tracking per Destination IP Address—The profile tracks SYN packets individually for each pair composed of the destination IP address and port. • Spoofed SYN Attack Protection - Aggregated Tracking for All Destination IP Addresses in Policy—The profile tracks and counts traffic by aggregating the SYN packets sent toward any and all IP addresses included in the **DST Network** configured in the Protection policy. (For more information, see *Spoofed SYN Attack Protection* below.) Default: Tracking per Destination IP Address
Spoofed SYN Attack Protection (These parameters are available only when the **Tracking Method** is **Spoofed SYN Attack Protection**.) Radware DefensePro DDoS Mitigation's *Spoofed SYN Attack Protection* handles attacks that use multiple, spoofed, source subnets and/or CIDRs. Spoofed-SYN-flood attacks are not the "usual/typical" SYN-flood attack. Spoofed-SYN-flood attacks are slow-rate SYN-flood attacks, sourcing from multiple subnets (/22-/24) to multiple destination subnets (/22-/24). A spoofed-SYN-flood attack resembles a highly distributed scan attack, originating from many source subnets to many destination subnets. These attacks are also called *carpet-bombing attacks*. If you observe a drastic increase in the number of incomplete three-way TCP handshakes, over various protocols (such as DNS, HTTP, HTTPS, C-LDAP, and so on)—where the source of the SYN packets is distributed across a wide range of subnets, you may be facing a spoofed-SYN-flood attack, where your system is the *reflector*. As the reflector, your system generates a flood of SYN- ACK-packets towards the spoofed destination.	
Destination Ports	Values: • All Traffic Matching Policy Regardless of Destination Port—The profile tracks all traffic that matches the destination IP addresses of the Protection policy, *regardless of the destination port*. • Traffic Matching Destination Ports Included in SYN Protections in Profile—The profile tracks traffic whose destination port is included in the **Application Port Group** configured for one of the *SYN Flood Protections* in the SYN Flood Protection *profile*. Default: All Traffic Matching Policy Regardless of Destination Port
Activation Mode	Values: • Continuous—The profile applies the authentication methods configured in the profile immediately. The profile authenticates all SYN packets received by the associated Protection policy. • Threshold-Based—The profile applies the authentication methods configured in the profile after reaching the configured **Activation Threshold** value (of SYN packets per second). The profile authenticates all *subsequent* SYN packets received by the associated Protection policy. Default: Threshold-Based

Table 136: SYN Flood Protection Profile Parameters (cont.)

Parameter	Description
Activation Threshold (This parameter is available only when the **Activation Mode** is **Threshold-Based**.)	The number of SYN packets per second that triggers the SYN Flood Protection. Values: 1–10,000 Default: 1500
Network Level Authentication	
Authentication Method	The authentication method that Radware DefensePro DDoS Mitigation uses at the transport layer. When Radware DefensePro DDoS Mitigation is installed in an ingress- only topology, select the **Safe Reset** option. Values: • Transparent Proxy–When Radware DefensePro DDoS Mitigation receives a SYN packet, Radware DefensePro DDoS Mitigation replies with a SYN ACK packet with a cookie in the Sequence Number field. If the response is an ACK packet that contains the cookie, Radware DefensePro DDoS Mitigation considers the session to be legitimate. Then, Radware DefensePro DDoS Mitigation opens a connection with the destination and acts as transparent proxy between the source and the destination. • Safe Reset–When Radware DefensePro DDoS Mitigation receives a SYN packet, Radware DefensePro DDoS Mitigation responds with an ACK packet with an invalid Sequence Number field as a cookie. If the client responds with the RST packet with the cookie and retransmits the original SYN packet within the specified time range (**Minimum Allowed SYN Retransmission Time** and **Maximum Allowed SYN Retransmission Time**), Radware DefensePro DDoS Mitigation discards the RST packet, and adds the source IP address to the TCP Authentication Table. The next SYN packet from the same source passes through Radware DefensePro DDoS Mitigation, and the session is approved for the server. Radware DefensePro DDoS Mitigation saves the source IP address for a specified time. Default: Safe Reset **Notes:** • If you select **Transparent Proxy**, **Use HTTP Authentication**, and **Use SSL Mitigation**, Radware DefensePro DDoS Mitigation uses the TCP-Reset method for HTTP, HTTPS, SMTP, and *custom-protocol* traffic rather than the *Transparent-Proxy* method. • If you select **Transparent Proxy** and **Use HTTP Authentication** (*without* **Use SSL Mitigation**), Radware DefensePro DDoS Mitigation performs the HTTP Authentication before performing the Transparent-Proxy actions. • To configure **Minimum Allowed SYN Retransmission Time** and **Maximum Allowed SYN Retransmission Time**, in the *Configuration* perspective, select **Setup > Security Settings > SYN Flood Protection**.

Table 136: SYN Flood Protection Profile Parameters (cont.)

Parameter	Description
Use TCP Reset for Supported Protocols (This option is available only when the **Authentication Method** is **Safe Reset**.)	Specifies whether Radware DefensePro DDoS Mitigation uses the TCP- Reset method for HTTP, HTTPS, SMTP, and *custom-protocol* traffic rather than the default Authentication Method: *Safe Reset*. Cisco recommends enabling the **Use TCP Reset for Supported Protocols** option in symmetric and ingress-only environments that include HTTP, HTTPS, and SMTP traffic. Default: Disabled **Notes:** • For more information on the TCP-Reset method, see TCP Reset, page 240. • Using the Safe-Reset method, when Radware DefensePro DDoS Mitigation receives a SYN packet, Radware DefensePro DDoS Mitigation responds with an ACK packet with an invalid Sequence Number field as a cookie. If the client responds with RST and the cookie, Radware DefensePro DDoS Mitigation discards the RST packet, and adds the source IP address to the TCP Authentication Table. The next SYN packet from the same source (normally, a retransmit of the previous SYN packet) passes through Radware DefensePro DDoS Mitigation, and the session is approved for the server. Radware DefensePro DDoS Mitigation saves the source IP address for a specified time.
Application Level Authentication	
Use HTTP Authentication	Specifies whether Radware DefensePro DDoS Mitigation authenticates the transport layer of HTTP traffic using SYN cookies and then authenticates the HTTP application layer using the specified **HTTP Authentication Method**. Values: • Enabled–Radware DefensePro DDoS Mitigation authenticates the transport layer of HTTP traffic using SYN cookies, and then, authenticates the HTTP application layer using the specified **HTTP Authentication Method**. • Disabled–Radware DefensePro DDoS Mitigation handles HTTP traffic using the specified TCP **Authentication Method**. Default: Disabled
Use SSL Mitigation (This parameter is available only when SSL-decryption-and-encryption is enabled in *SSL Settings* node.)	Specifies whether Radware DefensePro DDoS Mitigation sends traffic to the specified SSL-decryption-and-encryption component and uses the SSL Mitigation mechanism. SSL Mitigation works with HTTP Authentication. If you select the **Use SSL Mitigation** checkbox, Radware DefensePro DDoS Mitigation selects the **Use HTTP Authentication** checkbox automatically. **Note:** You configure the SSL Mitigation mechanism in the *SSL Settings* node (*Configuration* perspective, **Setup > SSL Settings**). For more information, see Configuring the SSL-Settings Setup, page 107).

Table 136: SYN Flood Protection Profile Parameters (cont.)

Parameter	Description
HTTP Authentication Method	The method that the profile uses to authenticate HTTP traffic at the application layer. Values: • 302-Redirect–Radware DefensePro DDoS Mitigation authenticates HTTP traffic using a 302-redirect response code. • JavaScript–Radware DefensePro DDoS Mitigation authenticates HTTP trafficusing a JavaScript object, which Radware DefensePro DDoS Mitigation generates. Default: 302-Redirect **Notes:** • Some attack tools are capable of handling 302-redirectresponses. The *302-Redirect* HTTP Authentication Method is not effective against attacks that use those tools. The *JavaScript* HTTP Authentication Method requires an engine on the client side that supports JavaScript, and therefore, the JavaScript option is considered stronger. However, the *JavaScript* option has some limitations, which are relevant in certain scenarios. • Limitations when using the *JavaScript* HTTP AuthenticationMethod: — If the browser does not support JavaScript calls, thebrowser will not answer the challenge. — When the protected server is accessed as a sub-page through another (main) page *only* using JavaScript, the user session will fail (that is, the browser will not answer the challenge).[1]

1 – For example, if the protected server supplies content that is requested using a JavaS- cript tag, the Radware DefensePro DDoS Mitigation JavaScript is enclosed within the original JavaScript block. This violates JavaScript rules, which results in a challenge fail- ure. In the following example, the request accesses an HTTPS server. The returned chal- lenge page contains the <script> tag again, which is illegal, and therefore, it is dropped by the browser without making the redirect.

```
<script> setTimeout(function(){
   var js=document.createElement(“script”);
   js.src=”http://mysite.site.com.domain/service/
appMy.jsp?dlid=12345”;
   document.getElementsByTagName(“head”)[0].appendChild(js);
   },1000);
</script>
```

TCP Reset

Cisco recommends enabling the TCP-Reset option in symmetric and ingress-only environments that include HTTP, HTTPS, and SMTP traffic.

Caution: When Radware DefensePro DDoS Mitigation implements the TCP-Reset mechanism, according to the relevant RFCs (for HTTP, HTTPS, and SMTP), a new connection must be initiated automatically when the original connection is reset (in this case, by the TCP-Reset mechanism). For browsers that fully comply with this aspect of the RFCs, the connection will be re-initiated automatically, and the user will experience a delay of approximately three seconds with no additional latency expected during the *authentication period*. (The authentication period is determined by the **TCP Authentication Table Aging** parameter, which, by default, is 20 minutes.) For browsers that do not fully comply with this aspect of the RFCs, legitimate users will receive a notification that the connection is reset and will need to manually retry the connection. After the retry, the users will be able to browse with no additional latency expected during the authentication period.

When the **Use TCP Reset for Supported Protocols** checkbox is selected, Radware DefensePro DDoS Mitigation uses the TCP-Reset authentication method for HTTP, HTTPS, SMTP, and *custom- protocol* traffic instead of the authentication method, which, for Radware DefensePro DDoS Mitigation version 8.22.2, is Safe-Reset).

Custom-protocol refers to traffic that you define for the TCP-Reset method to handle. To enable you to do this, Radware DefensePro DDoS Mitigation exposes two, system-defined Application Port Groups: **TCPReset-ACK** and **TCPReset-Data**. These Application Port Groups are dummy groups, which are defined with Layer 4 port 0 (zero). (For the procedure to define custom-protocol traffic, see the procedure To define custom-protocol traffic for the TCP-Reset method, page 241.)

When Radware DefensePro DDoS Mitigation implements the TCP-Reset method, Radware DefensePro DDoS Mitigation tries to match packets to a relevant Application Port Group according to the following order:

1. HTTP
2. HTTPS
3. SMTP
4. TCPReset-Data
5. TCPReset-ACK

Radware DefensePro DDoS Mitigation handles packets in a session according to the first packet that matched one of the relevant Application Port Groups.

When the TCP-Reset option is enabled, Radware DefensePro DDoS Mitigation does the following:

1. When it receives a SYN packet, Radware DefensePro DDoS Mitigation replies with a SYN-ACK packet with a cookie in the Sequence Number field using the original destination IP address and MAC, without any additional authentication parameters (cookies).
2. If the response is an ACK with the cookie:
   - In HTTP or HTTPS traffic or *custom-protocol* traffic with the **TCPReset-Data** Application Port Group, Radware DefensePro DDoS Mitigation waits for the first data packet from the client. (If Radware DefensePro DDoS Mitigation receives an ACK with no data before the first data packet, Radware DefensePro DDoS Mitigation drops the packet.) When the Radware DefensePro DDoS Mitigation device receives data, it replies with a RST packet, and saves the source IP address in the TCP Authentication table.

– For SMTP or *custom-protocol* traffic with the **TCPReset-ACK** Application Port Group, Radware DefensePro DDoS Mitigation replies with a RST packet, and saves the source IP address in the TCP Authentication table.

Note: HTTP, HTTPS, and SMTP sources respond automatically to a RST packet by re- sending a SYN–that is, the source automatically retries to open the connection with the protected server. Legitimate clients are expected to retry and open a new connection towards the protected server.

3. Radware DefensePro DDoS Mitigation checks each SYN packet against the entries in the TCP Authentication table. If there is a match, Radware DefensePro DDoS Mitigation forwards the packet to the other Radware DefensePro DDoS Mitigation inspection modules and later forwards the SYN packet to the destination as-is, so the protected server will open a connection withthe source.
4. Once Radware DefensePro DDoS Mitigation has authenticated a source, Radware DefensePro DDoS Mitigation does not challenge the source again during the *authentication period*. (The authentication period is determined by the **TCP Authentication Table Aging** parameter, which, by default, is 20 minutes).

Notes

- If Radware DefensePro DDoS Mitigation receives multiple SYNs from the same source, Radware DefensePro DDoS Mitigation implements the TCP-Reset authentication process per SYN packet, until one of the connections is authenticated.
- Radware DefensePro DDoS Mitigation always uses the TCPReset-Data behavior (step 2 above) for traffic through ports included in **HTTP** Application Port Group and **HTTPS** Application Port Group.
- Radware DefensePro DDoS Mitigation always uses the TCPReset-ACK behavior (step 2 above) for traffic through ports included in **SMTP** Application Port Group.
- When you select both the **Use HTTP Authentication** and the **Use TCP Reset ForSupported Protocols** checkboxes, Radware DefensePro DDoS Mitigation uses the HTTP Authentication method, not the TCP-Reset method–except for when SSL Mitigation is enabled.
- When SSL Mitigation is enabled (see Configuring Global SYN Flood Protection, page 134), Radware DefensePro DDoS Mitigation always uses the TCP-Reset method, regardless of other SYN Flood Protection profile configuration parameters.

To define custom-protocol traffic for the TCP-Reset method

1. Create a new Application Port Group as follows:
   a. In the *Configuration* perspective, select **Classes > Applications**.
   b. Click the (Add) button.
   c. In the *Ports Group Name* text box, type **TCPReset-ACK** or **TCPReset-Data**–according to the TCP-Reset behavior that you require (see step 2 above).
   d. In the **From L4 Port** text box, type the first port in the range.
   e. In the **To L4 Port** text box, type the last port in the range. To define a group with asingle port, type the same value in the **From L4 Port** and **To L4 Port** text boxes.
   f. To activate your configuration changes on the device, click **Update Policies** ( ).
2. Configure a SYN Flood Protection profile (see To configure a SYN Flood Protectionprofile, page 233).

3. Configure a SYN-flood protection (see To define a SYN-flood protection, page 233) for theSYN Flood Protection Profile in the previous step, and, from the *Application Port Group* drop-down list, select **TCPReset-ACK** or **TCPReset-Data** as you require.

Configuring Traffic Filters Profiles

Use a *Traffic Filters profile* to implement control over processing traffic through Radware DefensePro DDoS Mitigation at the Protection policy level. Traffic Filters complement other Radware DefensePro DDoS Mitigation protections with additional manual control.

With Traffic Filters, you can block or rate-limit traffic that matches specified values or traffic not matching specified values. Traffic Filters enable you to specify network addresses, ports, packet size, TTL, and additional parameters for filtering packets within the Protection policy.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 200 Traffic Filters profiles on a Radware DefensePro DDoS Mitigation device.

You can configure up to 200 Traffic Filters profiles on a Radware DefensePro DDoS Mitigation platform.

Use Cases for Traffic Filters

Use cases for Traffic Filters include the following:

- **Defining a maximum rate** –You can configure a Traffic Filter for all the traffic towards a specific Protection policy with the maximum rate (in packets per second or kilobitsper second) of the protected network and servers. This predefined Traffic Filter can help cap the maximum rate from Radware DefensePro DDoS Mitigation towards the protected network at any given time.
- **Whitelisting when under attack** –You can configure a Traffic Filter for the traffic that Radware DefensePro DDoS Mitigation inspects towards the protected network and block all other traffic that might match the Protection policy. This way, you can inspect only the expected legitimate traffic and block the rest of the traffic that reaches the policy. You can achieve this by selecting the **Non-Matching Traffic** option in **Filter Mode** in the configuration of the Traffic Filters.
- **Blocking traffic when under attack**–You can configure a Traffic Filter for blocking or rate- limiting specific traffic or all traffic towards the Protection policy.

Traffic Filters in a Traffic Filters Profile

Each Traffic Filters profile can include up to 15 individual *Traffic Filters*. An

individual Traffic Filter is composed of the following main parts:

- **Filter Mode**–Specifies the way to apply the filter. You can choose to apply the filter to traffic that matches all parameters in the Filter Criteria or to apply the filter to traffic that does not match all the parameters in the Filter Criteria.
- **Filter criteria**–Specify traffic characteristics based on network parameters and packet parameters. You can configure up to 10 criteria parameters in a Traffic Filter.
- **Filter Action parameters**–Specify the following:
  - **The threshold units**–You can specify the threshold in packets per second or kilobits per second.
  - **The threshold that triggers the Traffic Filter**–Enter zero (**0**) to block all matching, or enter a value greater than zero to limit the rate of the matching traffic.
  - **The Tracking Mode**–You specify what traffic to track after the Traffic Filter matches traffic to the specified filter criteria. You can choose to track all traffic, traffic per source IP address, traffic per destination IP address, and traffic per source-IP-address-source-IP-address pair. Additionally, there is a special option **Track Returning Traffic from Destination and Suspend Corresponding Sources**, which tracks the specific direction of the traffic and applies the action on the *reverse* direction.

Notes

  - The **Track Returning Traffic from Destination and Suspend Corresponding Sources** option enables handling attacks such as brute-force attacks, dictionary attacks, and application reconnaissance.
  - To use the **Track Returning Traffic from Destination and Suspend Corresponding Sources** option, you must define a value for the **Destination Port** parameter and entera pattern to track in the **Regular Expression** field.
  - For more information, see Example Traffic Filter Configurations Showing Tracking Mode Behavior, page 253 and Example Traffic Filters for Various Attack Types, page 254.

The order of the individual *Traffic Filters* in the *Traffic Filters profile* determines *priority*. When a packet is handled by a Traffic Filters profile, the profile determines which of the Traffic Filters have matching criteria–and updates the rate counters for all of them. The profile applies the **Profile Action** (**Report Only** or **Block and Report**) of the matching Traffic Filter with the highest priority if the packet exceeds the rate threshold. The best practice for prioritization is to give the Traffic Filter with the narrowest criteria the highest priority.

Configuring a Traffic Filters Profile

This section describes how to configure a Traffic Filters profile in Radware DefensePro DDoS Mitigation 8.x versions 8.17 and later

Notes

- You can configure up to a total 200 Traffic Filters on a Radware DefensePro DDoSMitigation device.
- For information on the details that the APSolute Vision *Security Monitoring* perspectivedisplays for Traffic Filters, see Traffic Filters Attack Details, page 342.
- A Traffic Filters profile is applied on an inspected Protection policy. The classification of a Protection policy includes the **Direction** (**One Way** or **Two Way**) and can include aspecific source network (**SRC Network**) and/or destination network (**DST Network**).

Take the following into consideration:

- The Traffic Filters profile applies exactly according to your configuration: on *one* directionin one-way policies or on *both* directions in two-way policies.
- Using the **Tracking Mode** option **Track Returning Traffic from Destination and Suspend Corresponding Sources**, the "reverse" option will work as defined in the Traffic Filter, regardless of whether the policy he **Direction** is **One Way** or **Two Way**. That is, you can use the **Track Returning Traffic from Destination and Suspend Corresponding Sources** option to track responses from the protected servers and block "bad" sources, or track incoming traffic and block "misbehaving" hosts within the protected network.

- The configuration of individual Traffic Filter and the order of the Traffic Filters in a Traffic Filters profile may reduce performance, depending on the configured filter criteria and platforms–for example:
  - Traffic Filters with a regular expression and/or a **Tracking Mode** (other than **All**) affect performance more than Traffic Filters that do not use those parameters.
  - On Radware DefensePro DDoS Mitigation 110, 200, 220, and 400 devices, a Traffic Filter with a regular expression and/or a **Tracking Mode** (other than **All**) reduces performance. Therefore, Cisco recommends placing such Traffic Filters at the *bottom* of the Traffic Filters list–to ensure that the Traffic Filters profile processes the Traffic Filters at the *top* of the list with maximal performance.

To configure a Traffic Filters profile

1. In the *Configuration* perspective, select **Protections > Traffic Filters Profiles**.
2. Do one of the following:
   - To add a profile, click the (Add) button. Configure the profile parameters, and then, click **Submit**.
   - To edit a profile, double-click the entry in the table, configure the parameter, and then, click **Submit**.
3. Do one of the following to configure an individual Traffic Filter:
   - To add a Traffic Filter, click the (Add) button. Configure the Traffic Filter parameters, and then, click **Submit**.
   - To edit a Traffic Filter, double-click the entry in the table, configure the Traffic Filter parameters, and then, click **Submit**.
4. Repeat step 3 to edit or add additional Traffic Filters as required.
5. Do the following:
   - Set the processing order of the Traffic Filters in the table by selecting an entry and clicking the (Move the selection up) button or the (Move the selection down) button.
   - Enable or disable Traffic Filters in the table by selecting one or more entries (using standard Windows mouse commands) and clicking **Enable** or **Disable**.

Table 137: Traffic Filters Profile Parameters

Parameter	Description
Profile Name	The name of the Traffic Filters profile. Maximum characters: 29
Number of Traffic Filters	(Read-only) The number of Traffic Filters in the profile.

Table 137: Traffic Filters Profile Parameters (cont.)

Parameter	Description
Profile Action	The action that the profile takes when it detects traffic matching a Traffic Filter configuration. Values: Block and Report, Report Only Default: Block and Report **Caution:** The **Report Only** option takes precedence–in the Protection *policy* or the Protection *profile*. For example, if you specify **Report Only** in the policy, and you specify **Block and Report** in the profile, the action behavior of all the Protection policy is *report only*. If you specify **Block and Report** in the policy, but you specify **Report Only** in the profile, the action behavior of all the Protection policy is *block and report* except for the profile whose action behavior is *report only*.

Table 138: Traffic Filter: General Parameters

Parameter	Description
Enabled	Specifies whether the filter is enabled. Default: Enabled
Filter Name	The name of the Traffic Filter. Maximum characters: 29
Filter ID	(Read-only) The Radware DefensePro DDoS Mitigation Attack- Protection ID of the Traffic Filter. Radware DefensePro DDoS Mitigation automatically generates the Filter IDs. Each Filter ID is unique to each Radware DefensePro DDoS Mitigation device. The range for Filter IDs is 700,000–1,000,000. **Notes:** • When you import a Protection policy (see Using Configuration Templates for Security Policies, page 266) with the Traffic Filters profile, Radware DefensePro DDoS Mitigation always regenerates the Filter IDs to ensure uniqueness. • The *Security Monitoring* perspective displays the Filter ID as a hyperlink, which you can click to open the relevant *Traffic Filters* configuration pane. The *Current Attacks Table* in the *Security Monitoring* perspective displays the Filter ID as the *Radware ID* (see Using the Current Attacks Table, page 326). The *Attack Details* (Characteristics) tab in the *Security Monitoring* perspective also displays the Filter ID (see Traffic Filters Attack Details, page 342).

Table 139: Traffic Filter: Filter Mode Parameter

Parameter	Description
Apply Traffic Filter	Values: • Matching Traffic–Apply the filter to traffic that matches all the parameters in the *Filter Criteria*. • Non-Matching Traffic–Apply the filter to traffic that does not match all the parameters in the *Filter Criteria*. Default: Matching Traffic

Table 140: Traffic Filter: Basic Filter Criteria Parameters

Parameter	Description
Source Network	The IP address or predefined Network class object that defines the source of the packets to match to the Traffic Filter. Values: • As in Policy–The filter matches only source networks that match the Protection policy. • *A discrete IP address.* • *A Network class displayed in the Classes tab.* Default: As in Policy **Caution:** If you specify a Network class, the class can represent up to 50 discrete IP addresses.
Source Port (This parameter is available only when the value for the **Protocol** parameter is **Any Supported Protocol**, **TCP**, or **UDP**.)	The port or predefined Application Port Group class object that defines the source of the packets that the Traffic Filter applies to. Values: • Any–The filter matches *any* source application port. • *A specific application-port number.* • *A list of comma-separated application-port numbers.* • *An Application Port Group class displayed in the Classes tab.* Default: Any Maximum characters in version 8.19 and later: 255 **Caution:** You can specify up to 50 ranges/values, in the comma-separated list or in the Application Port Group class. However, each port range is unlimited, for example, 1-10, 50-65535is valid.
Destination Network	The IP address or predefined Network class object that defines the destination of the packets that the policy applies to. Values: • As in Policy–The filter matches only destination networks that match the Protection policy. • *A discrete IP address.* • *A Network class displayed in the Classes tab.* Default: As in Policy **Caution:** If you specify a Network class, the class can represent up to 50 discrete IP addresses.

Table 140: Traffic Filter: Basic Filter Criteria Parameters (cont.)

Parameter	Description
Destination Port (This parameter is available only when the value for the **Protocol** parameter is **Any Supported Protocol**, **TCP**, or **UDP**.)	The port or predefined Application Port Group class object that defines the destination of the packets that the Traffic Filter applies to. Values: • Any–The filter matches *any* destination application port. • *A specific application-port number*. • *A list of comma-separated application-port numbers*. • *An Application Port Group class displayed in the Classes tab*. Default: Any Maximum characters in version 8.19 and later: 255 **Caution:** You can specify up to 50 ranges/values, in the comma-separated list or in the Application Port Group class. However, each port range is unlimited, for example, 1-10, 50-65535is valid.
Protocol	The protocol that defines the packets that the Traffic Filter applies to. Values: • Any Supported Protocol–The filter matches *any* supported protocol. • TCP • UDP • ICMP • IGMP • ICMPv6 • Other Protocol(s)–The filter matches the protocol number or numbers specified in the **Other Protocol Number(s)** textbox. Default: Any Supported Protocol **Caution:** If **Protocol** is **Any Supported Protocol** and a checkbox for **TCP Flags** is selected, the effective value for **Protocol** is **TCP**.
Other Protocol Number(s) (This parameter is available only when the value for the **Protocol** parameter is **Other Protocol(s)**.)	The IANA-assigned number or numbers that identify the protocol or protocols that define the packets that the Traffic Filter applies to. Values: • 0-255 • *A list of comma-separated values in the range 0-255* • *A range of values 0-255, in the format a-b* **Caution:** When the selected **Protocol** value is **Other Protocol(s)**, for the Traffic Filter to apply, the **Report Action** for Packet Anomaly *Unsupported L4 Protocol* (ID 110) must be **Process**. To verify this, in the *Configuration* perspective, select **Setup > Security Settings > Packet Anomaly**. **Note:** You can enter a list with a combination of numbers and ranges. Example: 1-20,47,48,58-62

Table 140: Traffic Filter: Basic Filter Criteria Parameters (cont.)

Parameter	Description
Packet Size	The size, in bytes, of the packets that the Traffic Filter applies to. Values: • *None* • 64-1542 • *A list of comma-separated values in the range 64-1542* • *A range of values 64-1542, in the format a-b* Default: *None* Maximum characters: 255 **Caution:** You can specify up to a total of 50 packet-size values. **Notes:** • You can enter a list with a combination of specific packet sizes and packet-size ranges. Example: 64-80,90,92,101-130 • The **Packet Size** value does not account for the CRC.

Table 141: Traffic Filter: Advanced Filter Criteria Parameters

Parameter	Description
TCP Flags (The checkboxes for TCP flags are available only when the value for the **Protocol** parameter is **Any Supported Protocol** or **TCP**.)	
SYN	Select the TCP flags to match toward the Traffic Filter. Radware DefensePro DDoS Mitigation combines multiple values using a Boolean OR operator. Default: *None* **Caution:** If you select a TCP flag, you cannot specify a value for the **Fragment Offset** or **Fragment ID** parameter.
ACK	
RST	
SYN+ACK	
FIN+ACK	
PSH+ACK	
Time to Live	The time-to-live (TTL) value in the packet header. Values: • *None* • *A specific value* • *A list of comma-separated values* • *A range of values, in the format a-b* Default: *None* Maximum characters: 255 **Caution:** You can specify up to 50 TTL values, in the comma- separated list or in the range. **Note:** You can enter a list with a combination of values and ranges. Example: 6-10,12,13,15-64

Table 141: Traffic Filter: Advanced Filter Criteria Parameters (cont.)

Parameter	Description
TCP Sequence (This parameter is available only when the value for the **Protocol** parameter is **Any Supported Protocol** or **TCP**.)	The TCP-sequence value in the packet header. Values: • Any • *A specific value* • *A list of comma-separated values* • *A range of values, in the format a-b* Default: *None* Maximum characters: 255 **Caution:** You can specify up to a total of 50 TCP-sequence values, in the comma-separated list or in the range. **Caution:** If you specify a value for this parameter, you cannot specify a value for the **Fragment Offset** or **Fragment ID** parameter. **Note:** You can enter a list with a combination of values and ranges. Example: 6-10,12,13,15-64
Context Tag	The context tag in the packet header. Values: • *None* • *A context-tag value* • *A list of comma-separated context-tag values* • *A Context Group class displayed in the Classes tab* **Caution:** You can specify up to 50 tags, in the comma-separated list or in the class.
Type of Service (ToS) / DSCP	The type-of-service (ToS) value or Differentiated Services Code Point (DSCP) value in the packet header. Values: • *None* • *A specific value* • *A list of comma-separated values* • *A range of values, in the format a-b* Default: *None* Maximum characters: 255 **Caution:** You can specify up to a total of 50 ToS/DSCP values, in the comma-separated list or in the range. **Note:** You can enter a list with a combination of values and ranges. Example: 8-14,24,26,32-38

Table 141: Traffic Filter: Advanced Filter Criteria Parameters (cont.)

Parameter	Description
Fragment Offset	The fragment offset value in the packet header. Values: • *None* • *A specific value* • *A list of comma-separated values* • *A range of values, in the format a-b* Default: *None* Maximum characters: 255 **Caution:** You can specify up to a total of 50 fragment-offset values, in the comma-separated list or in the range. **Caution:** If you specify a value for this parameter, you cannot select a TCP flag or specify a value for the **TCP Sequence** parameter. **Note:** You can enter a list with a combination of values and ranges. Example: 0-8,16,32,64-100
Fragment ID	The fragment identifier value in the packet header. Values: • *None* • *A specific value* • *A list of comma-separated values* • *A range of values, in the format a-b* Default: *None* Maximum characters: 255 **Caution:** You can specify up to a total of 50 fragment-ID values, in the comma-separated list or in the range. **Caution:** If you specify a value for this parameter, you cannot select a TCP flag or specify a value for the **TCP Sequence** parameter. **Note:** You can enter a list with a combination of values and ranges. Example: 0-3,5,7,9-20
Regular Expression	The regular expression that the filter tries to match to the contents of the packet payload. This field supports only *text* represented by the specified regular expression—anywhere in the packet payload. Maximum characters: 255 **Caution:** Configuring a regular expression in this field may reduce performance.

Table 142: Traffic Filter: Filter Action Parameters

Parameter	Description
Threshold Units	Values: Packets per Second, Kbits per Second, Default: Packets per Second

Table 142: Traffic Filter: Filter Action Parameters (cont.)

Parameter	Description
Threshold	The rate, in the specified units, at which Radware DefensePro DDoS Mitigation triggers the Traffic Filter. Values: • 0—The filter blocks all traffic. • For Packets per Second: 1–200,000,000 • For Kilobits per Second: 1–156,250,000
Tracking Mode	The traffic, matching the specified criteria, that the Traffic Filter tracks, counts, and acts upon. Options: • All—The Traffic Filter applies the specified **Filter Action** on all the traffic above the specified **Threshold**. • Per Source—The Traffic Filter applies the specified **Filter Action** on the traffic above the specified **Threshold**, per source. The source can be a discrete IP address or a subnet, according to the specified **Source Prefix Length**. For example, if the specified **Source Prefix Length** for **IPv4** is **32**, *per source* is per discrete source IPv4 address. • Per Destination—The Traffic Filter applies the specified **Filter Action** on the traffic, above the specified **Threshold**, per destination. The destination can be a discrete IP address or a subnet, according to the specified **Destination Prefix Length**. For example, if the specified **Destination Prefix Length** for **IPv4** is **32**, *per destination* is per discrete destination IPv4 address. You may select this option in a Traffic Filter for HTTP-flood protection. For more information, see Example Traffic Filters for Various Attack Types, page 254. • Per Source and Destination Pair—The Traffic Filter applies the specified **Filter Action** on the traffic, above the specified **Threshold**, per source-and-destination pair. Each source and destination can be a discrete IP address or a subnet, according to the specified **Source Prefix Length** and Destination Prefix Length. For example, if the specified **Source Prefix Length** for **IPv4** is **32**, the *per source* part of the source-and-destination pair is per discrete source IPv4 address. • Track Returning Traffic from Destination and Suspend Corresponding Sources—The Traffic Filter tracks the traffic that matches the specified **Regular Expression**, per *destination* IP address, from the specified **Destination Port**—and when the traffic rate is above the specified **Threshold**, the filter places the corresponding *source* IP address into the *Suspend Table*, and drops *all* subsequent packets from that IP address, until the *aging period* expires. When you select this option: — You must enter a **Regular Expression**. — The **Destination Port** field must *not* be **Any**. For more information, see Example Traffic Filters for Various Attack Types, page 254. **Note:** For information on the Suspend Table, see Configuring Radware DefensePro DDoS Mitigation Suspend Table Settings, page

	141. **Caution:** Except for the **All** option, specifying any of these options may reduce performance.

Table 142: Traffic Filter: Filter Action Parameters (cont.)

Parameter	Description
Source Prefix Length (The *Source Prefix Length* parameters are available only when the value for the **Tracking Mode** parameter is **Per Source** or **Per Source and Destination Pair**.) The prefix length that specifies the subnet-size for tracking, without classifying a specific network. This avoids a rate limit that is too low per discrete IP address, while still mitigating floods received from sequential subnets. Specifying the prefix length is useful against certain attack types (such as *carpet-bombing* and *carpet-bombing-reflection* attacks). These attacks may be able to evade a Traffic Filter by sending a small number of packets from each IP address while using large networks/subnets. The result is malicious traffic passing into the protected network, because no single source reaches the thresholds.	
IPv4	The IPv4 prefix length that specifies the subnet size for tracking source addresses. Values: 1–32 Default: 32
IPv6	The IPv6 prefix length that specifies the subnet size for tracking source addresses. Values: 1–128 Default: 128
Destination Prefix Length (The *Destination Prefix Length* parameters are available only when the value for the **Tracking Mode** parameter is **Per Destination** or **Per Source and Destination Pair**.) The prefix length that specifies the subnet-size for tracking, without classifying a specific network. This avoids a rate limit that is too low per discrete IP address, while still mitigating floods sent to sequential subnets. Specifying the prefix length is useful against certain attack types (such as *carpet-bombing* and *carpet-bombing-reflection* attacks). These attacks may be able to evade a Traffic Filter by sending a small number of packets to each IP address while using large networks/subnets. The result is malicious traffic passing into the protected network, because no single destination reaches the thresholds.	
IPv4	The IPv4 prefix length that specifies the subnet size for tracking destination addresses. Values: 1–32 Default: 32
IPv6	The IPv6 prefix length that specifies the subnet size for tracking destination addresses. Values: 1–128 Default: 128

Table 143: Traffic Filter: Reporting Setting Parameters

Parameter	Description
Packet Reporting	Specifies whether the profile sends sampled attack packets to APSolute Vision for offline analysis. Default: Disabled **Note:** When this feature is enabled, for the packet-reporting to take effect, the global setting must be enabled (*Configuration* perspective, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting > Enable Packet Reporting**).

Example Traffic Filter Configurations Showing Tracking Mode Behavior

This section contains an example Traffic Filter configuration with **Tracking Mode**, **All** and one with **Tracking Mode**, **Per Source**.

Example Configuration and Behavior of a Traffic Filter Profile with Tracking Mode = All

Consider a Protection policy named NetProtPol1, which includes a Traffic Filters profile named TFProf1. The **Filter action** on TFProf1 is **Block and Report**, that is block (drop) and report the relevant traffic. TFProf1 contains one enabled Traffic Filter named TF1.

TF1 has the following configuration:

- **Filter Mode > Apply Traffic Filter To > Matching Traffic**—That is, apply the filter to traffic that matches all the filter criteria.
- **Advanced Filter Criteria> Type of Service (ToS) / DSCP > 2**—And no other criteria specified.
- **Filter Action**:
  - **Threshold Units > Kbits per Second**
  - **Threshold > 1000**
  - **Tracking Mode > All**

NetProtPol1 passes traffic to TFProf1. The traffic is matches the filter criteria. The traffic contains source IP address 1.1.1.1 at 1000 Kbit/s and source IP address 1.1.1.2 at 2000 Kbit/s. NetProtPol1 drops all traffic from 1.1.1.1 and 1.1.1.2 over 1000 Kbit/s.

Example Configuration and Behavior of a Traffic Filter Profile with Tracking Mode = Per Source

Consider a Protection policy named NetProtPol2, which includes a Traffic Filters profile named TFProf2. The **Filter action** on TFProf2 is **Block and Report**, that is block (drop) and report the relevant traffic. TFProf2 contains one enabled Traffic Filter named TF2.

TF2 has the following configuration:

- **Filter Mode > Apply Traffic Filter To > Matching Traffic**—That is, apply the filter to traffic that matches all the filter criteria.
- **Advanced Filter Criteria> Type of Service (ToS) / DSCP > 2**—And no other criteria specified.
- **Filter Action**:
  - **Threshold Units > Kbits per Second**
  - **Threshold > 1000**
  - **Tracking Mode > Per Source**—Thatis per source IP address.

NetProtPol2 passes traffic to TFProf2. The traffic is matches the filter criteria. The traffic contains source IP address 1.1.1.1 at 1000 Kbit/s and source IP address 1.1.1.2 at 2000 Kbit/s. NetProtPol2 track the traffic rates of 1.1.1.1 and 1.1.1.2 separately, and drops all traffic from 1.1.1.1 over 1000 Kbit/s and all traffic from 1.1.1.2 over 1000 Kbit/s.

Example Traffic Filters for Various Attack Types

This section describes example Traffic Filter configurations for mitigating the following types of attacks:

- Example Traffic Filter for HTTP Flood Protection, page 254
- Example Traffic Filter for SIP Flood Protection, page 254
- Example Traffic Filter for HTTP Brute Force Protection, page 255
- Example Traffic Filter for DNS Brute Force Protection, page 255

Example Traffic Filter for HTTP Flood Protection

Consider a Protection policy named Policy1, which includes a Traffic Filters profile named TF-Profile1. TF-Profile1 contains a Traffic Filter TF1.

TF1 has the following configuration:

- **Filter Mode > Apply Traffic Filter To > Matching Traffic**—That is, apply the filter to traffic that matches all the filter criteria.
- **Basic Filter Criteria**:
  - **Source Network > As in Policy**—That is, the default.
  - **Destination Network > As in Policy**—That is, the default.
  - **Destination Port > HTTP**
  - **Protocol > TCP**
- **Advanced Filter Criteria> Regular Expression > GET | POST**
- **Filter Action**:
  - **Threshold Units > Packets per Second**
  - **Threshold > 1000**
  - **Tracking Mode > Per Destination**

The specified **Tracking Mode** rate-limits HTTP requests towards each HTTP server in the protected network in Policy1.

Example Traffic Filter for SIP Flood Protection

Consider a Protection policy named Policy1, which includes a Traffic Filters profile named TF-Profile1. TF-Profile1 contains a Traffic Filter TF1.

TF1 has the following configuration:

- **Filter Mode > Apply Traffic Filter To > Matching Traffic**—That is, apply the filter to traffic that matches all the filter criteria.
- **Basic Filter Criteria**:
  - **Source Network > As in Policy**—That is, the default.
  - **Destination Network > As in Policy**—That is, the default.
  - **Destination Port > SIP**
  - **Protocol > UDP**

- **Advanced Filter Criteria> Regular Expression > INVITE**
- **Filter Action**:
  - **Threshold Units > Packets per Second**
  - **Threshold > 1000**
  - **Tracking Mode > Per Destination**

The specified **Tracking Mode** rate-limits SIP requests towards each SIP server in the protected network in Policy1.

Example Traffic Filter for HTTP Brute Force Protection

Consider a Protection policy named Policy1, which includes a Traffic Filters profile named TF-Profile1. TF-Profile1 contains a Traffic Filter TF1.

TF1 has the following configuration:

- **Filter Mode > Apply Traffic Filter To > Matching Traffic**–That is, apply the filter to traffic that matches all the filter criteria.
- **Basic Filter Criteria**:
  - **Source Network > As in Policy**–That is, the default.
  - **Destination Network > As in Policy**–That is, the default.
  - **Destination Port > HTTP**
  - **Protocol > TCP**
- **Advanced Filter Criteria> Regular Expression > 404 Not Found**
- **Filter Action**:
  - **Threshold Units > Packets per Second**
  - **Threshold > 20**
  - **Tracking Mode > Track Returning Traffic from Destination andSuspend Corresponding Sources**

The specified **Tracking Mode** suspends sources that send HTTP requests that lead to HTTP-error responses from each HTTP server in the protected network in Policy1.

Example Traffic Filter for DNS Brute Force Protection

Consider a Protection policy named Policy1, which includes a Traffic Filters profile named TF-Profile1. TF-Profile1 contains a Traffic Filter TF1.

TF1 has the following configuration:

- **Filter Mode > Apply Traffic Filter To > Matching Traffic**–That is, apply the filter to traffic that matches all the filter criteria.
- **Basic Filter Criteria**:
  - **Source Network > As in Policy**–That is, the default.
  - **Destination Network > As in Policy**–That is, the default.
  - **Destination Port > DNS**
  - **Protocol > UDP**
- **Advanced Filter Criteria**:
  - **Fragment Offset > 0**
  - **Regular Expression > ^.{3}[\x03\x83\x93\x13\x23\x33\xb3\xa3]\x00\x01\x00\x00**–Matches NXDOMAIN within a stream of binary traffic.

- **Filter Action**:
  - **Threshold Units > Packets per Second**
  - **Threshold > 20**
  - **Tracking Mode > Track Returning Traffic from Destination andSuspend Corresponding Sources**

The specified **Tracking Mode** suspends sources that send DNS queries that lead to DNS-error responses from each DNS server in the protected network in Policy1.

CHAPTER 6 – MANAGING ACCESS CONTROL

Managing black lists and white lists comprises the following main topics:

- Configuring Black Lists, page 257
- Configuring White Lists, page 260

Configuring the ACL Global Parameter–List Precedence

Use the following procedure to configure whether a Black List rule or a White List rule processes the packet when the packet matches both a White List rule and a Black List rule.

To configure the Black or White List Precedence parameter

1. In the *Configuration* perspective, select **Access Control > Black List and White List**.
2. Choose one of the following **Black or White List Precedence** options:

   Values:

   - **White List Takes Precedence**–If a packet matches both a White List rule and a Black List rule, Radware DefensePro DDoS Mitigation processes the packet as belonging to the White List rule.
   - **Black List Takes Precedence**–If a packet matches both a White List rule and a Black List rule, Radware DefensePro DDoS Mitigation processes the packet as belonging to the Black List rule.

   Default: White List Takes Precedence
3. Click **Submit**.

Configuring Black Lists

The Black List comprises the traffic that the device always blocks without inspection. You use the Black List as policy exceptions for security policies.

Notes

- This feature is *not* supported on management interfaces.
- Radware DefensePro DDoS Mitigation identifies blacklisted traffic based on the *external* address of tunneled traffic.
- In captured packets that the Black List module blocked, the MAC address is not the MAC address of the packet source.

This section contains the following topics:

- Black List and White List Entries and Storage Capabilities, page 258
- Configuring Black List Rules, page 258

Black List and White List Entries and Storage Capabilities

Radware DefensePro DDoS Mitigation defines Black List and White List entries using rules and entries. Rules are user-defined. Entries are single-network entries or subnets derived from the classes in the user-defined rule.

On Radware DefensePro DDoS Mitigation 110, 200, 220, and 400 devices:

- Radware DefensePro DDoS Mitigation can store up to 64,000 hardware entries.
- Radware DefensePro DDoS Mitigation can store up to 10,000 rules, where each rule may include up to 256 network blocks.

On Radware DefensePro DDoS Mitigation 20 and 60 devices:

- Radware DefensePro DDoS Mitigation can store up to 32,000 hardware entries.
- Radware DefensePro DDoS Mitigation can store up to 10,000 rules, where each rule may include up to 256 network blocks.

On a Radware DefensePro DDoS Mitigation 6 device:

- Radware DefensePro DDoS Mitigation can store up to 20,000 software entries.
- Radware DefensePro DDoS Mitigation can store up to 5,000 rules, where each rule mayinclude up to 256 network blocks.

Note: To utilize the full capacity with the highest performance, Cisco recommends that you configure Black List and White List rules using network masks rather than network ranges.

Configuring Black List Rules

This section describers configuring Black List rules.

Note: You can recreate a Black List rule with the same name only after you update policies.

To configure a Black List rule

1. In the *Configuration* perspective, select **Access Control > Black List and White List > Black List**.
2. To add or modify a black list rule, do one of the following:
   - To add a rule, click the  (Add) button.
   - To edit a rule, double-click the entry in the table.
3. Configure the parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ().

Table 144: Black List Rule: General Parameters

Parameter	Description
Enabled	When selected, the rule is active. Default: Enabled
Name	The name of the rule. Maximum characters: 64
Description	The user-defined description of the rule.
Action	(Read-only) The action for a Black List rule is always **Drop**.

Table 145: Black List Rule: Classification Parameters

Parameter	Description
Source Network	The source of the packets that the rule uses. Values: • *A Network class displayed in the Classes tab* • *An IP address* • None • any Default: any
Source Port	The source Application Port class or application-port number that the rule uses. Values: • *An Application Port class displayed in the Classes tab* • *An application-port number* • None
Destination Network	The destination of the packets that the rule uses. Values: • *A Network class displayed in the Classes tab* • *An IP address* • None • any Default: any
Destination Port	The destination Application Port class or application-port number that the rule uses. Values: • *An Application Port class displayed in the Classes tab* • *An application-port number* • None
Physical Ports	The Physical Port class that the rule uses. Values: • *A Physical Port class displayed in the Classes tab* • None

Table 145: Black List Rule: Classification Parameters (cont.)

Parameter	Description
Context	The Context Group class that the rule uses. Values: • *A Context Group class displayed in the Classes tab* • None
Protocol	The protocol of the traffic that the rule uses. Values: • Any • TCP • UDP • ICMP • SCTP • ICMPv6 Default: Any
Direction	The direction to which the rule relates. Values: • One-directional–The protection applies to sessions originating from sources to destinations that match the network definitions of the policy. • Bi-directional–The protection applies to all traffic that matches the network definitions of the policy, regardless of which is defined as source and which is defined as destination. Default: One-directional

Table 146: Black List Rule: Reporting Parameters

Parameter	Description
Report	Specifies whether the device issues traps for the rule.
Packet Reporting	Specifies whether the device sends sampled attack packets to APSolute Vision for offline analysis. Default: Disabled **Caution:** When this feature is enabled here, for the feature to take effect, the global setting must be enabled (*Configuration* perspective, **Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting > Enable Packet Reporting**).

Configuring White Lists

The White List determines the traffic that is exempt from security inspection. For each protection, you can set different White List rules.

Note: Radware DefensePro DDoS Mitigation identifies whitelisted traffic based on the *external* address of tunneled traffic.

Configuring White Lists in Radware DefensePro DDoS Mitigation

This section contains the following topics:

- White List and Black List Entries and Storage Capabilities, page 261
- Configuring a White List in Radware DefensePro DDoS Mitigation, page 261

White List and Black List Entries and Storage Capabilities

Radware DefensePro DDoS Mitigation defines Black List and White List entries using rules and entries. Rules are user-defined. Entries are single-network entries or subnets derived from the classes in the user-defined rule.

On Radware DefensePro DDoS Mitigation 110, 200, 220, and 400 devices:

- Radware DefensePro DDoS Mitigation can store up to 64,000 hardware entries.
- Radware DefensePro DDoS Mitigation can store up to 10,000 rules, where each rule may include up to 256 network blocks.

On Radware DefensePro DDoS Mitigation 20 and 60 devices:

- Radware DefensePro DDoS Mitigation can store up to 32,000 hardware entries.
- Radware DefensePro DDoS Mitigation can store up to 10,000 rules, where each rule may include up to 256 network blocks.

On a Radware DefensePro DDoS Mitigation 6 device:

- Radware DefensePro DDoS Mitigation can store up to 20,000 software entries.
- Radware DefensePro DDoS Mitigation can store up to 5,000 rules, where each rule may include up to 256 network blocks.

Note: To utilize the full capacity with the highest performance, Cisco recommends that you configure Black List and White List rules using network masks rather than network ranges.

Configuring a White List in Radware DefensePro DDoS Mitigation

In Radware DefensePro DDoS Mitigation, a White List rule can use explicit values or predefined *classes* to classify the traffic. The classes are displayed in the *Classes* tab.

Notes

- Since networks on the White List are not inspected, certain protections are not applied to sessions in the opposite direction. For example, with SYN Flood Protection, this cancause servers not to be added to known destinations due to ACK packets not beinginspected.
- You can recreate a White List rule with the same name only after you update policies.

To configure a White List rule

1. In the *Configuration* perspective, select **Access Control > Black List and White List > White List**.
2. To add or modify a white list rule, do one of the following:
   - To add a rule, click the  (Add) button.
   - To edit a rule, double-click the entry in the table.

3. Configure white list rule parameters.

4. To activate your configuration changes on the device, click **Update Policies** ().

Table 147: White List Rule: General Parameters

Parameter	Description
Enabled	When selected, the rule is active. Default: Enabled
Name	The name of the rule. Maximum characters: 64
Description	The user-defined description of the rule.
Action	(Read-only) The action for a White List rule is always **Bypass**.

Table 148: White List Rule: Classification Parameters

Parameter	Description
Source Network	The source of the packets that the rule uses. Values: • *A Network class displayed in the Classes tab* • *An IP address*
Source Port	The source Application Port class or application-port number that the rule uses. Values: • *An Application Port class displayed in the Classes tab* • *An application-port number* • None
Destination Network	The destination of the packets that the rule uses. Values: • *A Network class displayed in the Classes tab* • *An IP address* • any
Destination Port	The destination Application Port class or application-port number that the rule uses. Values: • *An Application Port class displayed in the Classes tab* • *An application-port number* • None
Physical Ports	The Physical Port class that the rule uses. Values: • *A Physical Port class displayed in the Classes tab* • None
Context	The Context Group class that the rule uses. Values: • *A Context Group class displayed in the Classes tab* • None

Table 148: White List Rule: Classification Parameters (cont.)

Parameter	Description
Protocol	The protocol of the traffic that the rule uses. Values: • Any • GRE • ICMP • ICMPv6 • IGMP • SCTP • TCP • UDP • L2TP • GTP • IP in IP Default: Any
Direction	The direction of the traffic to which the rule relates. Values: • One-directional–The protection applies to sessions originating from sources to destinations that match the network definitions of the policy. • Bi-directional–The protection applies to sessions that match the network definitions of the policy regardless of their direction. Default: One-directional

CHAPTER 7 – MANAGING OPERATIONS AND MAINTENANCE

This chapter describes the following operation and maintenance tasks:

- Updating Policy Configurations, page 265
- Rebooting or Shutting Down a Radware DefensePro DDoS Mitigation Device, page 266
- Using Configuration Templates for Security Policies, page 266
- Configuring Multiple Devices, page 275
- Downloading a Device's Log File to APSolute Vision, page 276
- Updating a Radware Signature File, page 277
- Downloading Technical-Support and Configuration Files, page 278
- Managing Radware DefensePro DDoS Mitigation Device Configurations, page 280
- Resetting the Baseline for Radware DefensePro DDoS Mitigation, page 283
- Scheduling APSolute Vision and Device Tasks, page 284
- Updating the Attack Description File, page 302

Notes

- When you have permissions to perform device configuration on a specific device, you must lock the device before you can configure it. For more information, see Locking and Unlocking Devices, page 68.
- You cannot use APSolute Vision to upgrade Radware DefensePro DDoS Mitigation. For information on device upgrade for Radware DefensePro DDoS Mitigation, see the relevant release notes.
- Updating signature files using APSolute Vision is not relevant to Radware DefensePro DDoS Mitigation.

Tip: APSolute Vision provides many predefined *Toolbox* scripts for Radware DefensePro DDoS Mitigation, which automate and streamline common configuration and management actions. For more information, see the *APSolute Vision User Guide* or online help.

Updating Policy Configurations

You can apply the following configuration changes to a Radware DefensePro DDoS Mitigation device in a single operation:

- Protection policy
- Classes

To update policy configurations on a Radware DefensePro DDoS Mitigation device

> In the device pane, select the device, and then, click **Update Policies** ().

Rebooting or Shutting Down a Radware DefensePro DDoS Mitigation Device

You can activate a device reboot (reset) or device shutdown from APSolute Vision.

Some configuration changes on the device require a device reboot for the configuration to take effect. You can activate the device reboot from APSolute Vision.

To reboot a device

1. Lock the device.
2. In the *Properties* pane, click the  (On-Off) button, which is part of the device picture.
3. Select **Reset**.

To shut down a device

1. Lock the device.
2. In the *Properties* pane, click the  (On-Off) button, which is part of the device picture.
3. Select **Shut Down**.

Using Configuration Templates for Security Policies

You can export and import *Radware DefensePro DDoS Mitigation configuration templates*.

A Radware DefensePro DDoS Mitigation configuration template can include the configuration (the definitions and security settings) and/or baselines of a Protection policy.

A template from a Protection policy can include the baselines from the associated DNS and/or BDoS profiles.

Radware DefensePro DDoS Mitigation configuration templates do *not* include the following information:

- **Radware DefensePro DDoS Mitigation setup and network configuration**–For example, device time, physical ports, and so on.
- **Radware DefensePro DDoS Mitigation security settings**–The protections that a policy template uses must be supported and enabled globally in the target Radware DefensePro DDoS Mitigation device (that is, the target Radware DefensePro DDoS Mitigation device into which you are importing the policy template). For example, if you export a Protection policy that includes a BDoS Protection profile, the Radware DefensePro DDoS Mitigation device into which you are importing the policy template must have BDoS Protection enabled globally (*Configuration* perspective, **Setup > Security Settings > BDoS Protection > Enable BDoSProtection**).
- **User-defined signatures**.

- **The configuration of user-defined SYN Flood Protections in the SYN Flood Protection profile.**

  Caution: If you export a configuration that includes any user-defined *SYN Flood Protection* in the SYN Flood Protection profile, the configuration template will include the value(s) of the **Protection Name** parameter, but will *not* include the associated *configuration(s)*. Importing such a configuration template will fail if the target DefensePro device does not include the user- defined *SYN Flood Protections* with the same names.

Caution: If the imported BDoS baseline or DNS baseline is below the minimum value in the configuration of the corresponding profile, after an Update Policies action, Radware DefensePro DDoS Mitigation recalculates the baseline or baselines according to the configuration of the *profile*. (For information on the configuration of profiles, see Configuring BDoS Profiles, page 172 and Configuring DNS Flood Protection Profiles, page 187.)

Notes

- The terms *Protection policy*, *Network Protection policy*, and *network policy* may be used interchangeably in APSolute Vision and in the documentation.
- You can import Protection policies from Radware DefensePro DDoS Mitigation platforms running supported 8.*x* versions only into other platforms running supported 8.*x* versions.
- APSolute Vision provides a predefined Toolbox script for exporting and importing Radware DefensePro DDoS Mitigation configurations, *DefensePro Export/Import Policies*. For more information, see the *APSolute Vision User Guide* or online help.

Exporting a Protection Policy as a Template

Use the following procedure to export a Protection policy as a template.

To export a Protection policy as a template

1. In the *Configuration* perspective, select **Protections > Protection Policies**.
2. Select the Protection policy that you want to export, and click (Export).
3. Configure the parameters, and then click **Submit**.

Table 149: Export Protection Parameters

Parameter	Description
Download To	Values: • APSolute Vision Client–Radware DefensePro DDoS Mitigation exports the template to the location specified (in the dialog box that opens after you click **Submit**) in the filepath or by browsing to the location with the **Browse** button. • APSolute Vision Server–Radware DefensePro DDoS Mitigation exports the template to the APSolute Vision database. Default: Server

Table 149: Export Protection Parameters (cont.)

Parameter	Description
Save As	The filepath when **Download To** is **APSolute Vision Client** or the filename when **Download To** is **APSolute Vision Server**. The default filename uses the following format (with no extension): <DeviceName>_<PolicyName>_<date>_<time> Example: MyRadware DefensePro DDoS Mitigation_MyPolicy_2016.03.19_13.45.59 The date-time format is determined in the *APSolute Vision Settings* view *Preferences* perspective, under **General Settings > Display**. The file is saved on the server as a ZIP file; and on the local host, the file is saved as a TXT file.
Export Policy and Profiles	
Policy Configuration	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the configuration of the policy. Default: Enabled
Anti-Scanning Whitelisted Objects	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current whitelisted objects of the Anti-Scanning profile of the policy. Default: Enabled
Custom Signature Profile	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current custom (user-defined) Signature Protection profile of the policy. Default: Enabled
Traffic Filters Profile	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current Traffic Filters profile of the policy. Default: Enabled
Export Baselines	
BDoS Baseline	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current BDoS baseline of the policy. Default: Enabled
DNS Flood Protection Baseline	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current DNS Flood Protection baseline of the policy. Default: Enabled
HTTPS Flood Protection Baselines	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current HTTPS Flood Protection baselines of the policy. Default: Enabled

To export a Network Protection policy as a template

1. In the *Configuration* perspective, select **Network Protection > Network Protection Policies**.
2. Select the Network Protection policy that you want to export, and click  (Export).
3. Configure the parameters, and then click **Submit**.

Table 150: Export Network Protection Parameters

Parameter	Description
Download To	Values: • Client–Radware DefensePro DDoS Mitigation exports the templateto the location specified (in the dialog box that opens after you click **Submit**) in the filepath or by browsing to the location with the **Browse** button. • Server–Radware DefensePro DDoS Mitigation exports the template to the APSolute Vision database. Default: Server
Configuration	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the configuration of the policy. Default: Enabled
DNS Baseline	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current DNS baseline of the policy. Default: Enabled
BDoS Baseline	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current BDoS baseline of the policy. Default: Enabled
Custom Signature Profile	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current custom (user-defined) Signature Protection profile of the policy. Default: Enabled
Traffic Filters Profile	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current Traffic Filters profile of the policy. Default: Enabled
Anti-Scanning Whitelisted Objects	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current whitelisted objects of the Anti-Scanning profile of the policy. Default: Enabled
Save As	The filepath when **Download To** is **Client** or the filename when **Download To** is **Server**. The default filename uses the following format (with no extension): <DeviceName>_<PolicyName>_<date>_<time> Example: MyRadware DefensePro DDoS Mitigation_MyPolicy_2016.03.19_13.45.59 The date-time format is determined in the *APSolute Vision Settings* view *Preferences* perspective, under **General Settings > Display**. The file is saved on the server as a ZIP file; and on the local host, the file is saved as a TXT file.

Managing Radware DefensePro DDoS Mitigation Configuration Templates

Use the *Radware DefensePro DDoS Mitigation Configuration Templates* pane to manage security- protection templates.

The *Radware DefensePro DDoS Mitigation Configuration Templates* pane contains the table of templates, which comprises the following columns:

- **Source Device Name** –Displays one of thefollowing:
  - The name of the device from which the template was exported.
  - **Local**–The template was uploaded from the local PC.
  - **System**–The template is a predefined template.
- **File Name**–Displays the filename of the template.
- **File Type**–Displays **Network Protection** for a template from a Protection policy.
- **Export Date**–Displays the date and time that the template was added to the *Template List*. The date-time format is determined in the *APSolute Vision Settings* view *Preferences* perspective, under **General Settings > Date and Time Format**.

The template table can contain up to 2000 entries.

You can filter the display of the list for convenience and efficiency, and clear the filter as necessary. You can select one or multiple rows, using standard key combinations.

You can do the following:

- **Send the templates to one or more Radware DefensePro DDoS Mitigationdevices**.
- **Delete the templates from one or more Radware DefensePro DDoSMitigation devices**– The delete command does the following:
  - Removes the selected templates from the table.
  - Removes, from the Radware DefensePro DDoS Mitigation *devices*, the policy definitions and all other policy-related configurations (Network Classes, profile definitions) as long as the other policies on the devices are not using those objects.
- **Add (upload) templates from another location to the templatetable**.
- **Download the templates to another location**.
- **Delete the rows**–This action deletes the policy or policies, without the related objects.

To filter the display of the template list

1. Select the **Automation** item () from the APSolute Vision sidebar menu. The Toolbox dashboard opens.
2. Select **Advanced > Radware DefensePro DDoS Mitigation Configuration Templates**.
3. Configure the parameters, and then, click the  (Search) button.

Table 151: Template-List Filter Parameters

Parameter	Description
Source Device Name	Values: • Device name–Shows only the templates downloaded from the selected device. • Local–Shows only the templates uploaded from the local PC. • System–Shows only the predefined templates. Default: All
File Type	Values: • Server Protection (not relevant for Radware DefensePro DDoS Mitigation 8.*x* versions)–Shows the templates from Server Protection policies. • Network Protection–Shows the templates Protection policies.
File Name	The filename that the filter uses. The value supports one or two wildcards (*). Examples: • *pol*–Shows any filename containing the string pol. • *pol–Shows any filename ending with the string pol. • pol*–Shows any filename starting with the string pol.

To clear the template-list filter and show all of the stored templates

1. Select the **Automation** item () from the APSolute Vision sidebar menu. The Toolbox dashboard opens.
2. Select **Advanced > Radware DefensePro DDoS Mitigation Configuration Templates**.
3. Click **Clear**.

To send templates to Radware DefensePro DDoS Mitigation devices

1. Select the **Automation** item () from the APSolute Vision sidebar menu. The Toolbox dashboard opens.
2. Select **Advanced > Radware DefensePro DDoS Mitigation Configuration Templates**.
3. Configure the filter as necessary (see the procedure To filter the display of the template list, page 270).
4. Select the rows with the required templates (using standard Windows key combinations).
5. Select **Send to Devices**.
6. Configure the parameters, and then click **Submit**.

Table 152: Send to Devices: Select Devices to Update Parameters

Parameter	Description
The **Available** lists and the **Selected** lists of Radware DefensePro DDoS Mitigation devices and Logical Groups (of Radware DefensePro DDoS Mitigation devices). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices to update. The **Selected** *Logical Group* list displays the Logical Groups with the devices to update. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Notes:** • The **Available** *device* list can contain only the devices that support the templates features. • When a Logical Group is selected, the effective *Target Device List* dynamically updates, according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.	
Update Method	Values: • Append to Existing Configuration–The template adds the policy and profile configurations, and any baselines, to the devices in the **Selected** lists. The template does not overwrite any existing configuration. For example, if a policy name exists in a target device, the policy on the target device does not get changed. • Overwrite Existing Configuration–The template adds the policy and profile configurations, and any baselines, to the devices in the **Selected** lists. If a policy or profile with the same name exists in a target device, the template overwrites it. Default: Overwrite Existing Configuration **Caution:** For the update behavior when the policy template includes a user-defined profile (**User-Defined Signature Protection Profile**, **Custom Signature Profile**, or **Traffic Filters Profile**), see Update Behavior Using Radware DefensePro DDoS Mitigation Configuration Templates with User-Defined Profiles, page 273.
Install on Instance (This parameter is relevant only for Radware DefensePro DDoS Mitigation x420 platforms.)	The identifier or the Radware DefensePro DDoS Mitigation hardware instance onto which to add the template. Values: 0, 1 Default: 0
Update Policies After Sending Configuration	Values: • Enabled–After successfully uploading a template to a device, an Update Policies (activate latest changes) action is automatically initiated. • Disabled–After successfully uploading a template to a device, an Update Policies (activate latest changes) action is required for the configuration to take effect. Default: Disabled

Update Behavior Using Radware DefensePro DDoS Mitigation Configuration Templates with User-Defined Profiles

This section describes the update behavior when one of the following **Export** options was enabled when a security-protection policy template was created:

- Custom Signature Profile
- Traffic Filters Profile

To delete templates and associated configuration objects from Radware DefensePro DDoS Mitigation devices

1. Select the **Automation** item () from the APSolute Vision sidebar menu. The Toolbox dashboard opens.
2. Select **Advanced > Radware DefensePro DDoS Mitigation Configuration Templates**.
3. Configure the filter as necessary (see the procedure To filter the display of the template list, page 270).
4. Select the rows with the required templates (using standard Windows key combinations).
5. Select **Delete from Devices**.
6. Configure the parameters, and then click **Submit**.

Table 153: Delete from Devices: Select Devices to Update Parameters

Parameter	Description
The **Available** lists and the **Selected** lists of Radware DefensePro DDoS Mitigation devices and Logical Groups (of Radware DefensePro DDoS Mitigation devices). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices to update. The **Selected** *Logical Group* list displays the Logical Groups with the devices to update. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Notes:** • The **Available** *device* list can contain only the devices that support the templates features. • The **Selected** *device* list can contain only Radware DefensePro DDoS Mitigation devices running 6.*x* versions 6.14 and later, 7.*x* versions 7.41.02 and later, or 8.*x* versions 8.10 and later. • When a Logical Group is selected, the effective *Target Device List* dynamically updates, according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.	
Update Policies After Sending Configuration	Values: • Enabled–After successfully deleting the templates and associated configuration objects from a device, an Update Policies (activate latest changes) action is automatically initiated. • Disabled–After successfully deleting the templates and associated configuration objects from the devices, an Update Policies (activate latest changes) action is required for the configuration to take effect. Default: Disabled

To add (upload) templates from another location to the template list

1. Select the **Automation** item () from the APSolute Vision sidebar menu. The Toolbox dashboard opens.
2. Select **Advanced > Radware DefensePro DDoS Mitigation Configuration Templates**.
3. Click the  (Add) button.
4. Configure the parameters, and then click **Submit**.

Table 154: Upload File to Server Parameters

Parameter	Description
File Type	Values: • Server Protection–The template defines a Server Protection policy (not relevant for Radware DefensePro DDoS Mitigation 8.*x* versions). • Network Protection–The template defines a Protection policy.
Upload From	The filepath of the template. Click **Browse** to browse to the directory and select the file.

To download templates to another location

1. Select the **Automation** item () from the APSolute Vision sidebar menu. The Toolbox dashboard opens.
2. Select **Advanced > Radware DefensePro DDoS Mitigation Configuration Templates**.
3. Configure the filter as necessary (see the procedure To filter the display of the templatelist, page 270).
4. Select the rows with the required templates (using standard Windows key combinations).
5. Click the  (Download Selected File) button.
6. In the **Save As** text box, type the path to the target directory or click **Browse** to browse to the directory.
7. Click **Save**.

To delete stored templates

1. Select the **Automation** item () from the APSolute Vision sidebar menu. The Toolbox dashboard opens.
2. Select **Advanced > Radware DefensePro DDoS Mitigation Configuration Templates**.
3. Configure the filter as necessary (see the procedure To filter the display of the templatelist, page 270).

4. Select the rows with the required templates (using standard Windows key combinations).

5. Click the (Delete) button in the pane.

Configuring Multiple Devices

Use the Multi-Device Configuration feature to make changes to multiple devices. You can use the Multi-Device Configuration feature in the following ways:

- Using a Logical Group. The devices in Logical Group are of the same type, but may run different software versions. For more information on Logical Groups, see Using Logical Groups of Devices, page 72.
- Selecting a site or multiple devices from the *Sites and Clusters* tree or the *Physical Containers* tree. The devices must be of the same type and same major version. You can select devices from different Sites. For more information, see Configuring Sites, page 60.

To configure multiple devices using a Logical Group

1. In the device pane, open the *Logical Groups* tree, and click the Logical Group. The Multi-Device View opens.

   Note: For more information, see Using the Multi-Device View and the Multiple Devices Summary, page 69.

2. Click the (Configuration) button. The configuration GUI of the lead device opens.

   Notes

   - The tabs of the configuration GUI include the *Summary* tab, which comprises the Multi- Device View.
   - The lead device is the device whose configuration changes will be applied to the selected additional devices. For more information on the lead device of a Logical Group, see Using Logical Groups of Devices, page 72.

3. Lock the devices if necessary.
4. Make a required change in the GUI of the lead device.
5. After you make a valid change, click **Submit All**. APSolute Vision attempts to change the value for the submitted parameter on the lead device and all the other devices in the Logical Group.

   Notes

   - APSolute Vision submits only modified values. APSolute Vision does *not* submit values that were not modified.
   - APSolute Vision issues detailed message for unsuccessful attempts to change the value of a parameter on other devices in the Logical Group.

6. Repeat step 4 and step 5 as necessary.

To configure the multiple devices by selecting a site or multiple devices

1. In the device pane, open the *Sites and Clusters* tree, and select the devices. You can select a site or select multiple devices (using standard, mouse click/keyboard combinations) whetheror not the devices are in the same site.
2. Click the  (View) button.
3. Click the  (Configuration) button. The Multi-Device Configuration dialog box opens.

   Note: The top table, which you can filter, contains all the selected devices and comprises the following columns: *Device Type*, *Device Name*, *IP Address*, and *Version*.
4. From the top table, select the *lead* device–that is, the device whose configuration changes will be applied to the selected additional devices. The bottom table, which you can filter, displays the selected devices of the same type and major version.
5. From the bottom table, select the checkbox next to each device that the lead device will tryto change.
6. Click **Go**. The GUI of the lead device opens. The device pane shows the lead device andthe selected additional devices as selected.
7. Lock the devices if necessary.
8. Make a required change in the GUI of the lead device.
9. After you make a valid change, click **Submit All**. APSolute Vision attempts to change the value for the submitted parameter on the lead device and all the selected additional devices.

   Notes

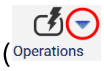
   — APSolute Vision submits only modified values. APSolute Vision does *not* submit values that were not modified.

   — APSolute Vision issues detailed message for unsuccessful attempts to change the value of a parameter on selected additional devices.
10. Repeat step 8 and step 9 as necessary.

Downloading a Device's Log File to APSolute Vision

You can download a Radware DefensePro DDoS Mitigation log file to the APSolute Vision system. Radware DefensePro DDoS Mitigation automatically generates a log file, which contains a report of configuration errors.

To download a device log file

1. In the device pane, select the device.
2. Click the arrow next to the **Operations** icon (

).

3. Click **Export Configuration Log File**.
4. Configure the download parameters, and click **Submit**.

Updating a Radware Signature File

This section describes how to upload an updated Radware signature file to a Radware DefensePro DDoS Mitigation device using the **Update Security Signatures** option in the **Operations** menu.

Notes

- You can *schedule* signature-file updates using the APSolute Vision scheduler. For more information, see Configuring Tasks in the Scheduler, page 285.
- Signatures files are supplied by the SUS. For more information, see ERT Security Update Service (SUS), page 35. For more information, see ERT Security Update Service (SUS), page 1364.
- A signature file on a Radware DefensePro DDoS Mitigation device may also be referred to as the *attack database*.

You can upload an updated Radware signature file to a Radware DefensePro DDoS Mitigation device from the following sources:

- **Radware.com or the proxy file server that is configured in the APSolute Vision settings**–The *Alerts* pane displays a success or failure notification and whether the operation was performed using a proxy server. The configuration of the proxy server in the *APSolute Vision Settings* view *System* perspective, under **General Settings > Connectivity > Proxy Server Parameters**.
- **APSolute Vision client system**–The name of the signature file must be one of the following:
  - <Device-MAC-address>.sig–For Radware DefensePro DDoS Mitigation physical platforms.
  - <Device-IP-address>.sig–For Radware DefensePro DDoS Mitigation virtual platforms.

Caution: Updating the signature file consumes large amounts of resources, which may cause the device to go temporarily into an *overload* state. Cisco recommends updating the signature file during hours of low activity.

To update the signature file of a device

1. In the device pane, select the device.
2. Click the arrow next to the **Operations** icon (

).
3. Select **Update Security Signatures**.
4. Configure the parameters, and click **Update**.

Table 155: Update Device Signature File Parameters

Parameter	Description
Signature Type	The type of the signature file to upload to the device. Values: • Radware Signatures • Fraud Signatures
Update From	The location of the signature file to upload. Values: • Radware.com–APSolute Vision uploads the signature file directly from Radware.com or from the proxy server that is configured in the Vision Server Connection configuration. • Client–APSolute Vision uploads the signature file from the APSolute Vision client system. This option is only availablefor Radware signatures.
File Name (This parameter is displayed only when **Update From Client** is selected)	Name of the signature file on the client system.

Downloading Technical-Support and Configuration Files

For debugging purposes, a Radware DefensePro DDoS Mitigation device can generate a TAR file containing the technical information that Technical Support requires. The file includes output of various CLI commands, for example, a printout of the Client table.

You can download a Radware DefensePro DDoS Mitigation technical support file and send it to Technical Support.

Downloading a Technical Support File Using APSolute Vision

Use the following procedure to download a technical support file using APSolute Vision.

To download a technical support file using APSolute Vision

1. In the device pane, select the device.
2. Click the arrow next to the **Operations** icon (

).
3. Select **Export Technical Support File**.
4. Configure download parameters, and click **Submit**.

Table 156: Device Technical Support File Download Parameters

Parameter	Description
Download Via	(Read-only) The protocol used to download the technical support file. Value: HTTPS
Save As	Save the downloaded technical support file as a text file on the client system. Enter or browse to the location of the saved file, and select or enter a file name.

Downloading a Technical Support File Using CLI

Using the CLI, you can save a technical support file to the Radware DefensePro DDoS Mitigation device under the
/mnt/cf/downloadsdirectory.

The name of the support file is support.tar. You can

copy the file using SCP.

To download a technical support file using CLI

> In the CLI, run the following command:

manage support save-file

User Credentials in Radware DefensePro DDoS Mitigation Technical Support Files

By default, the passwords in the Radware DefensePro DDoS Mitigation technical support files are encrypted or hashed. However, you can use a CLI command to specify that Radware DefensePro DDoS Mitigation generates its technical support files without any user credentials (that is, files without even encrypted or hashed passwords). The command affects all subsequent technical support files that the device generates.

The syntax of the command is:
system internal config-file remove-credentials-info {0|1}

where:

- **0**(default) specifies that the feature is disabled. That is, generated technical support files include user credentials (but they *are* encrypted or hashed)
- **1**specifies that the feature is enabled. That is, generated technical support files contain no user credentials.

When the feature is enabled, the following items are not included in the iterations of the generated technical support files:

- All users and passwords in the *Local User Table* for Web, Telnet, SSH, and HTTPS access (*Configuration* perspective, **Setup > Device Security > Users Table**)
- The SNMPv3 users and associated values, such as **Authentication Password** and**Privacy Password**.
- All secrets (both primary and secondary) of RADIUS users.
- All secrets (both primary and secondary) of TACACS+ users.

Managing Radware DefensePro DDoS Mitigation Device Configurations

This section describes how to manage configurations of the Radware DefensePro DDoS Mitigation devices that are configured on APSolute Vision.

Radware DefensePro DDoS Mitigation Configuration File Content

The configuration file content is divided into two sections:

- **Commands that require rebooting the device** –These include Application Security status, and so on. Copying and pasting a command from this section takes effect only after the device is rebooted. The section has the heading: The following commands will take effect only once the device has been rebooted!
- **Commands that do not require rebooting the device** –Copying and pasting a command from this section takes effect immediately after pasting. The commands in the section arenot bound to SNMP. The section has the heading: The following commands take effect immediately upon execution!

The commands are printed within each section–in the order of implementation.

At the end of the file, the device prints the signature of the configuration file. This signature is used to verify the authenticity of the file and that it has not been corrupted. The signature is validated each time the configuration file is uploaded to the device. If the validity check fails, the device accepts the configuration, but a notification is sent to the user that the configuration file has been tampered with and there is no guarantee that it works. The signature looks like File Signature: 063390ed2ce0e9dfc98c78266a90a7e4.

User Credentials in Radware DefensePro DDoS Mitigation Configuration Files

By default, the passwords in the Radware DefensePro DDoS Mitigation configuration files are encrypted or hashed. However, you can use a CLI command to specify that Radware DefensePro DDoS Mitigation generates its configuration files without any user credentials (that is, files without even encrypted or hashed passwords). The command affects all subsequent configuration files that the device generates.

The syntax of the command is:

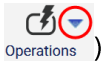
system internal config-file remove-credentials-info {0|1}

where

- **0**(default) specifies that the feature is disabled. That is, generated configuration files include user credentials (but they *are* encrypted or hashed)
- **1**specifies that the feature is enabled. That is, generated configuration files and contain no user credentials.

When the feature is enabled:

- The following items are not included in the iterations of the generated configurationfiles:
  - All users and passwords in the *Local User Table* for Web, Telnet, SSH, and HTTPSaccess (*Configuration* perspective, **Setup > Device Security > UsersTable**)
  - The SNMPv3 users and associated values, such as **Authentication Password** and **Privacy Password**.
  - All secrets (both primary and secondary) of RADIUS users.
  - All secrets (both primary and secondary) of TACACS+ users.

- After selecting the **Operations**icon (

) > **Export Configuration File**, if the user enables **Include Private Keys** (default: disabled) there is no effect.
- If the user uploads a configuration file that was generated without the credentials-info, the device is accessible only with the default user through the console or over SNMPv1 orSNMPv2.

Downloading a Device-Configuration File

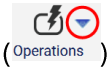
You can download a configuration file from a managed device to APSolute Vision, for backup. If you choose to download to the APSolute Vision server, a copy is always saved in the APSolute Vision database.

Downloading a Device-Configuration File Using APSolute Vision

By default, you can save up to five (5) configuration files per device on the APSolute Vision server. You can change this number in the APSolute Vision Setup page–up to a maximum of 10. When the limit is reached, you are prompted to delete the oldest file.

Note: You can schedule configuration file backups in the APSolute Vision scheduler. For more information, see Configuring Tasks in the Scheduler, page 285.

To download a device-configuration file

1. In the device pane, select the device.
2. Click the arrow next to the **Operations** icon (

).
3. Select **Export Configuration File**.
4. Configure the download parameters, and then, click **OK**.

Table 157: Device Configuration File Download Parameters

Parameter	Description
Destination	The destination of the device configuration file. Values: Client, Server
Include Private Keys	Specifies whether the certificate private key information is included in the downloaded file. Default: Disabled
Passphrase (This parameter is available only when the **Include Private Keys** checkbox is selected.)	The user-defined passphrase for the encryption of the private keys. Minimum characters: 4 Maximum characters: 64

Table 157: Device Configuration File Download Parameters (cont.)

Parameter	Description
Confirm Passphrase (This parameter is available only when the **Include Private Keys** checkbox is selected.)	The user-defined passphrase for the encryption of the private keys. Minimum characters: 4 Maximum characters: 64
Save As (This parameter is displayed only when **Destination** is **Server**.)	On the server, the default name is a combination of the device name and backup date and time. You can change the default name.

Downloading a Device-Configuration File Using CLI

Using the CLI, Radware DefensePro DDoS Mitigation can print the configuration file to screen or download the configuration as a file.

Radware DefensePro DDoS Mitigation saves configuration files under the /mnt/cf/downloads directory.

The name of the configuration file is DeviceConfigurationFile<yyy-MM-dd-hh-mm-ss>. For example, DeviceConfigurationFile2014-08-18-15-41-38.

You can copy the file using SCP.

To download a device-configuration file using CLI

> Run the following command:

```
system config save-file
```

Restoring a Device Configuration

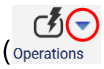
You can restore a Radware DefensePro DDoS Mitigation configuration from a backup configuration file on the APSolute Vision server or client system to the Radware DefensePro DDoS Mitigation device. When you upload the configuration file to the device, it overwrites the existing device configuration.

After the restore operation is complete, you must reboot the device.

Caution: Importing a configuration file that has been edited is not supported.

Caution: Importing a configuration file from a different version is not supported.

To restore a device's configuration

1. In the device pane, select the device.
2. Click the arrow next to the **Operations** icon (

).

3. Click **Import Configuration File**.
4. Configure upload parameters, and then, do one of the following:
   - If you select **Upload From Client**, click **Import**.
   - If you select **Upload From Server**, click **Update**.
5. When the upload completes, reboot the device.

Table 158: Device Configuration File Upload Parameters

Parameter	Description
Upload From	The location of the backup device-configuration file to send. Values: Client, Server
File Name (This parameter is available only when **Upload From** is **Client**.)	When uploading from the computer running the APSolute Vision client– that is, the browser, enter or browse to the name of the configuration file to upload.
File for Upload (This parameter is available only when **Upload From** is **Server**.)	When uploading from the APSolute Vision server, select the configuration to upload.
Passphrase	The passphrase for the decryption of the private keys–if a passphrase was used to encrypt the file when it was exported (see Downloading a Device-Configuration File, page 281). Minimum characters: 4 Maximum characters: 64

Resetting the Baseline for Radware DefensePro DDoS Mitigation

Resetting baseline-learned statistics clears the baseline traffic statistics and resets default normal baselines. Reset the baseline statistics only when the characteristics of the protected network have changed entirely and bandwidth quotas need to be changed to accommodate the network changes.

You can reset the baseline for all the Protection policies that contain a BDoS or DNS Flood Protection profile, or for a selected Protection policy that contains a BDoS or DNS Flood Protection profile.

For information about managing Protection policies, see Managing Protection Policies, page 159.

To reset BDoS baseline statistics

1. In the *Configuration* perspective, select **Setup > Security Settings > BDoS Protection> Reset BDoS Baseline**.
2. Select whether to reset the baseline for all Protection policies that contain a BDoS profile, or for a specific Protection policy that contains a BDoS profile.
3. Click **Submit**.

To reset DNS baseline statistics

1. In the *Configuration* perspective, select **Setup > Security Settings > BDoS Protection > Reset DNS Baseline**.
2. Select whether to reset the baseline for all Protection policies that contain a DNS profile, or for a specific Protection policy that contains a DNS profile.
3. Click **Submit**.

Note: APSolute Vision provides a predefined Toolbox script for exporting and importing Radware DefensePro DDoS Mitigation configurations, *DefensePro Export/Import Policies*. For more information, see the *APSolute Vision User Guide* or online help.

Scheduling APSolute Vision and Device Tasks

The following topics describe how to schedule operations in the APSolute Vision Scheduler:

- Overview of Scheduling, page 284
- Configuring Tasks in the Scheduler, page 285
- Task Parameters, page 287

Note: For information on how to schedule operations in the APSolute Vision server, see the *APSolute Vision User Guide* or APSolute Vision online help.

Overview of Scheduling

You can schedule various operations for the APSolute Vision server and managed devices. Scheduled operations are called *tasks*.

The APSolute Vision scheduler tracks when tasks were last performed and when they are due to be performed next. When you configure a task for multiple devices, the task runs on each device sequentially. After the task completes on one device, it begins on the next. If the task fails to complete on a device, the Scheduler will activate the task on the next listed device.

Select the **Scheduler** item () from the APSolute Vision sidebar menu to display the *Scheduler* pane.

When you create a task and specify the time to run it, the time is according to your local OS. APSolute Vision then stores the time, translated to the timezone of the of the APSolute Vision server, and then runs it accordingly. That is, once you configure a task, it runs according to the APSolute Vision time settings, disregarding any changes made to the local OS time settings.

Caution: If the APSolute Vision client timezone differs from the timezone of the APSolute Vision server or the managed device, take the time offset into consideration.

When you define a task, you can choose whether to enable or disable the task. All configured tasks are stored in the APSolute Vision database.

You can define the following types of Radware DefensePro DDoS Mitigation-related scheduled tasks:

- Back up a device configuration
- Back up the APSolute Vision Reporter data
- Reboot a device
- Update the Radware security signature file onto a Radware DefensePro DDoS Mitigation device from radware.com or the proxy server
- Run an Operator Toolbox script
- Retrieve the ERT Active Attackers Feed (EAAF) for Radware DefensePro DDoS Mitigation from radware.com, and upload the feed to selected Radware DefensePro DDoS Mitigationdevices.
- Retrieve the Geolocation feed for Radware DefensePro DDoS Mitigation from radware.com, and upload the feed to selected Radware DefensePro DDoS Mitigation devices.

Notes

- Some tasks that APSolute Vision exposes are non-operational/irrelevant for certain Radware DefensePro DDoS Mitigation versions.
- You can perform some of the operations manually, for example, from the *APSolute Vision Settings* view *System* perspective, or from the Operations options (

).

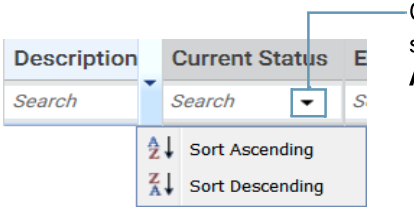
For more information, see:

- Rebooting or Shutting Down a Radware DefensePro DDoS Mitigation Device, page 266
- Updating a Radware Signature File, page 277
- Downloading a Device-Configuration File, page 281

Configuring Tasks in the Scheduler

The *Task List* table is the starting point for viewing and configuring tasks, which are scheduled operations. The table displays the information for each configured task. You can sort and filter the table rows according to your needs. You can also drag the bottom of *Task List* pane to lengthen the table.

Figure 37: Sorting Rows in the Task List



Click the far-right side of the title of the column with the values to sort by. Then, select the option that you require, for example, **Sort Ascending** or **Sort Descending**.

Note: For more information on filtering table rows, see Filtering Table Rows, page 58.

Table 159: Tasks Table Parameters

Parameter	Description

Task Type	The type of task to be performed.
Name	The name of the configured task.

Table 159: Tasks Table Parameters (cont.)

Parameter	Description
Description	The user-defined description of the task.
Current Status	The current status of the task. Values: Waiting, In progress
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task is saved in the database.
Last Execution Status	Whether the last task run was successful. When the task is disabled or has not yet started, the status is **Never Executed**. Values: • Failure • Never Executed • Success • Warning
Last Execution Time	The date and time of the last task run. When the task is disabled or has not yet started, this field is empty.
Next Execution Time	The date and time of the next task run. When the task is disabled, this field is empty.
Run	The frequency at which the task runs; for example, daily or weekly. The schedule start date is displayed, if it has been defined. Values: • Daily • Minutes • Once • Weekly

To configure a scheduled task

1. Select the **Scheduler** item () from the APSolute Vision sidebar menu. The *Scheduler* pane opens. The *Task List* table displays information for each scheduled task.
2. Do one of the following:
   - To add an entry to the table, click the  (Add) button. Then, select the type of task, and click **Submit**. The dialog box for the selected task type is displayed.
   - To edit an entry in the table, select the entry and click the  (Edit) button.
3. Configure task parameters, and click **Submit**. All task configurations include basic parameters and scheduling parameters. Other parameters depend on the task type that you select. Some tasks that APSolute Vision exposes are non-operational/irrelevant for certain products and/or versions. For more information, see the description of the relevant task parameters in Task Parameters, page 287.

To run an existing task

1. Select the **Scheduler** item ( ) from the APSolute Vision sidebar menu. The *Scheduler* pane opens. The *Task List* table displays information for each scheduled task.
2. Select the required task, and click the (Run Now) button.

Task Parameters

The following sections describe the parameters for Scheduler tasks that relate to Radware DefensePro DDoS Mitigation:

The following sections describe the parameters for Scheduler tasks:

- APSolute Vision Reporter Backup–Parameters, page 287
- Update Security Signature Files–Parameters, page 289
- Device Configuration Backup–Parameters, page 291
- Device Reboot Task–Parameters, page 293
- Operator Toolbox Task–Parameters, page 295
- ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation–Parameters, page 297
- Geolocation Feed–Parameters, page 300

APSolute Vision Reporter Backup–Parameters

The *APSolute Vision Reporter Backup* task creates a backup of the APSolute Vision Reporter data in the *storage location* and exports the date to a specified destination. The backup includes all the APSolute Vision Reporter data.

Notes

- APSolute Vision stores up to three iterations of the APSolute Vision Reporter data in the *storage location*. After the third reporter-backup, the system deletes the oldest one.
- The backup filenames in the *storage location* are the first five characters of the specified filename plus a 10-character timestamp. When the task exports the backup file, the filename is as specified in the task configuration.
- The backup file in the storage location includes the hard-coded descriptionScheduler-generated.

Table 160: APSolute Vision Reporter Backup: General Parameters

Parameter	Description
Name	A name for the task.
Description	A user-defined description of the task.
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task configuration is saved in the database.

Table 161: APSolute Vision Reporter Backup: Schedule Parameters

Parameter	Description
Run	The frequency at which the task runs. Select a frequency, then configure the related time and day/date parameters. Values: • Once–The task runs one time only at the specified date and time. • Minutes–The task runs at intervals of the specified number of minutes between task starts. • Daily–The task runs daily at the specified time. • Weekly–The task runs every week on the specified day or days, at the specified time. **Note:** Tasks run according to the time as configured on the APSolute Vision client.
Time[1]	The time at which the task runs.
Date[2]	The date on which the task runs.
Minutes[3]	The interval, in minutes, at which the task runs.
Run Always[4]	Specifies whether the task always runs or only during the defined period. Values: • Enabled–The task is activated immediately and runs indefinitely, with no start or end time. It runs at the first Time configured with the Frequency in the *Schedule* tab. • Disabled–The task runs (at the time and frequency specified in the *Schedule* tab) from the specified **Start Date** at the **Start Time** until the **End Date** at the **End Time**. Default: Enabled
Start Date[5]	The date and time at which the task is activated.
Start Time[5]	
End Date[5]	The date and time after which the task no longer runs.
End Time[5]	

1 – This parameter is available only when the specified **Run** value is **Once**, **Daily**, or **Weekly**.
2 – This parameter is available only when the specified **Run** value is **Once**.
3 – This parameter is available only when the specified **Run** value is **Minutes**.
4 – This parameter is available only when the specified **Run** value is **Minutes**, **Daily**, or **Weekly**.
5 – This parameter is available only when the **Run Always** checkbox is cleared.

Table 162: APSolute Vision Reporter Backup: Destination Parameters

Parameter	Description
Backup Configuration To	The destination of the backup configuration files. Values: • APSolute Vision Server • APSolute Vision and External Location Default: APSolute Vision Server
Protocol[1]	The protocol that APSolute Vision uses for this task. Values: • FTP • SCP • SFTP • SSH
IP Address[1]	The IP address of the external location. **Note:** By default, the selected **Protocol** determines the port of the external location. You can *specify* a port by adding a colon and the port number after the IP address–for example, **172.16.254.1:8022**or **[2001:db8:0:1234:0:567:8:1]:8022**.
Directory[1]	The path to the export directory with no spaces. Only alphanumeric characters and underscores (_) are allowed.
Backup File Name[1]	The name of the backup, up to 64 characters, with no spaces. Only alphanumeric characters and underscores (_) are allowed.
User[1]	The username.
Password[1]	The user password.
Confirm Password[1]	The user password.

1 – This parameter is available only when **Backup Configuration To** is **APSolute Vision Server and External Location**.

Update Security Signature Files–Parameters

The *Update Security Signature Files* task updates the Radware security signature files on the selected Radware DefensePro DDoS Mitigation devices. This action uses the Radware *Security Update Service* (SUS).

Caution: The Security Update Service (SUS) requires APSolute Vision communication with services.radware.com. You may configure APSolute Vision communication with services.radware.com through your own proxy server.

Table 163: Update Security Signature Files: General Parameters

Parameter	Description
Name	A name for the task.
Description	A user-defined description of the task.

Table 163: Update Security Signature Files: General Parameters (cont.)

Parameter	Description
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task configuration is saved in the database.

Table 164: Update Security Signature Files: Schedule Parameters

Parameter	Description
Run	The frequency at which the task runs. Select a frequency, then configure the related time and day/date parameters. Values: • Once–The task runs one time only at the specified date and time. • Minutes–The task runs at intervals of the specified number of minutes between task starts. • Daily–The task runs daily at the specified time. • Weekly–The task runs every week on the specified day or days, at the specified time. **Note:** Tasks run according to the time as configured on the APSolute Vision client.
Time[1]	The time at which the task runs.
Date[2]	The date on which the task runs.
Minutes[3]	The interval, in minutes, at which the task runs.
Run Always[4]	Specifies whether the task always runs or only during the defined period. Values: • Enabled–The task is activated immediately and runs indefinitely, with no start or end time. It runs at the first Time configured with the Frequency in the *Schedule* tab. • Disabled–The task runs (at the time and frequency specified in the *Schedule* tab) from the specified **Start Date** at the **Start Time** until the **End Date** at the **End Time**. Default: Enabled
Start Date[5]	The date and time at which the task is activated.
Start Time[5]	
End Date[5]	The date and time after which the task no longer runs.
End Time[5]	

1 – This parameter is available only when the specified **Run** value is **Once**, **Daily**, or **Weekly**.
2 – This parameter is available only when the specified **Run** value is **Once**.
3 – This parameter is available only when the specified **Run** value is **Minutes**.
4 – This parameter is available only when the specified **Run** value is **Minutes**, **Daily**, or **Weekly**.
5 – This parameter is available only when the **Run Always** checkbox is cleared.

Table 165: Update Security Signature Files: Target Device List

Parameter	Description
	The **Available** lists and the **Selected** lists of Radware DefensePro DDoS Mitigation devices and Logical Groups (of Radware DefensePro DDoS Mitigation devices). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices whose Radware signature files this task updates. The **Selected** *Logical Group* list displays the Logical Groups with the devices whose Radware signature files this task updates. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Note:** When a Logical Group is selected, the effective *Target Device List* dynamically updates–according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.

Device Configuration Backup–Parameters

The *Device Configuration Backup* task saves a configuration backup of the specified devices.

Note: By default, you can save up to five (5) configuration files per device on the APSolute Vision server. You can change this parameter in the APSolute Vision *Setup* tab.

Table 166: Device Configuration Backup: General Parameters

Parameter	Description
Name	A name for the task.
Description	A user-defined description of the task.
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task configuration is saved in the database.

Table 167: Device Configuration Backup: Schedule Parameters

Parameter	Description
Run	The frequency at which the task runs. Select a frequency, then configure the related time and day/date parameters. Values: • Once–The task runs one time only at the specified date and time. • Minutes–The task runs at intervals of the specified number of minutes between task starts. • Daily–The task runs daily at the specified time. • Weekly–The task runs every week on the specified day or days, at the specified time. **Note:** Tasks run according to the time as configured on the APSolute Vision client.
Time[1]	The time at which the task runs.
Date[2]	The date on which the task runs.
Minutes[3]	The interval, in minutes, at which the task runs.

Table 167: Device Configuration Backup: Schedule Parameters (cont.)

Parameter	Description
Run Always[4]	Specifies whether the task always runs or only during the defined period. Values: • Enabled–The task is activated immediately and runs indefinitely, with no start or end time. It runs at the first Time configured with the Frequency in the *Schedule* tab. • Disabled–The task runs (at the time and frequency specified in the *Schedule* tab) from the specified **Start Date** at the **Start Time** until the **End Date** at the **End Time**. Default: Enabled
Start Date[5]	The date and time at which the task is activated.
Start Time[5]	
End Date[5]	The date and time after which the task no longer runs.
End Time[5]	

1 – This parameter is available only when the specified **Run** value is **Once**, **Daily**, or **Weekly**.
2 – This parameter is available only when the specified **Run** value is **Once**.
3 – This parameter is available only when the specified **Run** value is **Minutes**.
4 – This parameter is available only when the specified **Run** value is **Minutes**, **Daily**, or **Weekly**.
5 – This parameter is available only when the **Run Always** checkbox is cleared.

Table 168: Device Configuration Backup: Parameters Parameters

Parameter	Description
Include Private Keys	Specifies whether to include the certificate private key information in the configuration file in devices that support private keys. Default: Disabled

Table 169: Device Configuration Backup: Destination Parameters

Parameter	Description
Backup Configuration To	The destination of the backup configuration files. Values: • APSolute Vision Server • External Location Default: APSolute Vision Server
Protocol[1]	The protocol that APSolute Vision uses for this task. Values: • FTP • SCP • SFTP • SSH

Table 169: Device Configuration Backup: Destination Parameters

Parameter	Description
IP Address[1]	The IP address of the external location. **Note:** By default, the selected **Protocol** determines the port of the external location. You can *specify* a port by adding a colon and the port number after the IP address–for example, **172.16.254.1:8022** or **[2001:db8:0:1234:0:567:8:1]:8022**.
Directory[1]	The path to the export directory with no spaces. Only alphanumeric characters and underscores (_) are allowed.
Backup File Name[1]	The name of the backup, up to 64 characters, with no spaces. Only alphanumeric characters and underscores (_) are allowed.
User[1]	The username.
Password[1]	The user password.
Confirm Password[1]	The user password.

1 – This parameter is available only when **Backup Configuration To** is **External Location**.

Table 170: Device Configuration Backup: Target Device List

Parameter	Description
The **Available** lists and the **Selected** lists of devices and Logical Groups (of devices). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices whose configurations this task backs up. The **Selected** *Logical Group* list displays the Logical Groups with the devices whose configurations this task backs up. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Note:** When a Logical Group is selected, the effective *Target Device List* dynamically updates–according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.	

Device Reboot Task–Parameters

The *Device Reboot* task reboots the specified devices.

Table 171: Device Reboot: General Parameters

Parameter	Description
Name	A name for the task.
Description	A user-defined description of the task.
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task configuration is saved in the database.

Table 172: Device Reboot: Schedule Parameters

Parameter	Description
Run	The frequency at which the task runs. Select a frequency, then configure the related time and day/date parameters. Values: • Once–The task runs one time only at the specified date and time. • Minutes–The task runs at intervals of the specified number of minutes between task starts. • Daily–The task runs daily at the specified time. • Weekly–The task runs every week on the specified day or days, at the specified time. **Note:** Tasks run according to the time as configured on the APSolute Vision client.
Time[1]	The time at which the task runs.
Date[2]	The date on which the task runs.
Minutes[3]	The interval, in minutes, at which the task runs.
Run Always[4]	Specifies whether the task always runs or only during the defined period. Values: • Enabled–The task is activated immediately and runs indefinitely, with no start or end time. It runs at the first Time configured with the Frequency in the *Schedule* tab. • Disabled–The task runs (at the time and frequency specified in the *Schedule* tab) from the specified **Start Date** at the **Start Time** until the **End Date** at the **End Time**. Default: Enabled
Start Date[5]	The date and time at which the task is activated.
Start Time[5]	
End Date[5]	The date and time after which the task no longer runs.
End Time[5]	

1 – This parameter is available only when the specified **Run** value is **Once**, **Daily**, or **Weekly**.
2 – This parameter is available only when the specified **Run** value is **Once**.
3 – This parameter is available only when the specified **Run** value is **Minutes**.
4 – This parameter is available only when the specified **Run** value is **Minutes**, **Daily**, or **Weekly**.
5 – This parameter is available only when the **Run Always** checkbox is cleared.

Table 173: Device Reboot: Target Device List

Parameter	Description
	The **Available** lists and the **Selected** lists of devices and Logical Groups (of devices). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices that this task reboots. The **Selected** *Logical Group* list displays the Logical Groups with the devices that this task reboots. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Note:** When a Logical Group is selected, the effective *Target Device List* dynamically updates–according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.

Operator Toolbox Task–Parameters

The *Operator Toolbox* task can run a Toolbox script on selected devices.

Notes

- For more information on Toolbox scripts, see the *APSolute Vision User Guide* or online help.
- The *scope* configured for an APSolute Vision user determines the managed devices that the *Operator Toolbox* task displays. (For more information, see the *APSolute Vision User Guide*.)
- APSolute Vision issues a failure message if any task action is not successful. The failure message includes the result of each action–that is, whether the action succeeded or failed for each target device.
- The configuration of the Toolbox script determines whether the target device must be locked for the script to run. If the script requires device locking, when an *Operator Toolbox* task runs the script, APSolute Vision tries to lock the device. If the locking action is successful, the script runs, and then, APSolute Vision unlocks the device. If the locking action fails, the *Operator Toolbox* task fails.
- If a device in the **Target Device List** is deleted from APSolute Vision, APSolute Vision deletes the device from the **Target Device List** and continues running the task.
- If all the devices inthe **Target Device List** are deleted from APSolute Vision, APSolute Vision disables the task.

Table 174: Operator Toolbox: General Parameters

Parameter	Description
Name	The name of the task.
Description	A user-defined description of the task.
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task configuration is saved in the database.

Table 175: Operator Toolbox: Schedule Parameters

Parameter	Description
Run	The frequency at which the task runs. Select a frequency, then configure the related time and day/date parameters. Values: • Once–The task runs one time only at the specified date and time. • Minutes–The task runs at intervals of the specified number of minutes between task starts. • Daily–The task runs daily at the specified time. • Weekly–The task runs every week on the specified day or days, at the specified time. **Note:** Tasks run according to the time as configured on the APSolute Vision client.
Time[1]	The time at which the task runs.
Date[2]	The date on which the task runs.
Minutes[3]	The interval, in minutes, at which the task runs.
Run Always[4]	Specifies whether the task always runs or only during the defined period. Values: • Enabled–The task is activated immediately and runs indefinitely, with no start or end time. It runs at the first Time configured with the Frequency in the *Schedule* tab. • Disabled–The task runs (at the time and frequency specified in the *Schedule* tab) from the specified **Start Date** at the **Start Time** until the **End Date** at the **End Time**. Default: Enabled
Start Date[5]	The date and time at which the task is activated.
Start Time[5]	
End Date[5]	The date and time after which the task no longer runs.
End Time[5]	

1 – This parameter is available only when the specified **Run** value is **Once**, **Daily**, or **Weekly**.
2 – This parameter is available only when the specified **Run** value is **Once**.
3 – This parameter is available only when the specified **Run** value is **Minutes**.
4 – This parameter is available only when the specified **Run** value is **Minutes**, **Daily**, or **Weekly**.
5 – This parameter is available only when the **Run Always** checkbox is cleared.

Table 176: Operator Toolbox: Configuration Template

Parameter	Description
Selected Script	(Read-only) The script that is selected in the table—with the file name.
To select the script, click the script from the *Action Title* column. The table contains all the Toolbox scripts that you have permission to run. The table comprises the following columns: *Action Title*, *File Name*, and *Category*. **Note:** When you change a selection, the parameters in the *Parameters* tab change accordingly.	

Table 177: Operator Toolbox: Parameters Parameters

Parameter	Description
Note: This tab is available only when the script that is selected in the *Configuration Template* tab includes configuration parameters.	
The parameters for the selected script.	

Table 178: Operator Toolbox: Target Device List

Parameter	Description
Note: This tab is available only when the script that is selected in the *Configuration Template* tab includes configuration parameters.	
The **Available** lists and the **Selected** lists of devices and Logical Groups (of devices of the appropriate type). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices that the Toolbox script runs on. The **Selected** *Logical Group* list displays the Logical Groups that the Toolbox script runs on. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Note:** When a Logical Group is selected, the effective *Target Device List* dynamically updates—according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.	

ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation—Parameters

The *ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation* task updates thedatabase of *ERT Active Attackers Feed* profiles in the selected Radware DefensePro DDoS Mitigation devices.

Using the *ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation* task requires a valid *ERT Active Attackers Feed subscription*. You can view subscription information in the APSolute Vision *Device Subscriptions* table (*APSolute Vision Settings* view *System* perspective, **DeviceResources > Device Subscriptions**). For more information on the *Device Subscriptions* table, seethe APSolute Vision online help or the *APSolute Vision User Guide*.

Caution: The ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation requires APSolute Vision communication with services.radware.com *and also with* radwareti.s3.amazonaws.com—that is Amazon Simple Storage Service (Amazon S3). You may configure APSolute Vision communication with services.radware.com through your own proxy server.

Caution: SSH must be enabled on the selected Radware DefensePro DDoS Mitigation devices for the *ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation* task to run. (You can enable SSH on Radware DefensePro DDoS Mitigation in the *Configuration* perspective, under **Setup > Device Security >**

Access Protocols> SSH Parameters > Enable SSH.)

Caution: The task updates each selected Radware DefensePro DDoS Mitigation device *sequentially*, and if the task fails on one device, the task-run does not continue. For example, suppose the task is configured with three selected Radware DefensePro DDoS Mitigation devices, A, B, and C. The task succeeds on device A. The task fails on device B, and stops. The task does not try to update device C.

Notes

- The *ERT Active Attackers Feed* node of the Security Control Center shows information about DefensePro devices that were updated with the ERT Active Attackers Feed in the last run of the *ERT Active Attackers Feed for DefensePro* scheduled task. To open the Security Control Center,

  in the APSolute Vision sidebar menu, click  , and then select **Security Control Center > ERT Active Attackers Feed**. For more information, see the section "Using the Security Control Center" in the *APSolute Vision User Guide* or the APSolute Vision online help.

Table 179: ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation: General Parameters

Parameter	Description
Name	A name for the task.
Description	A user-defined description of the task.
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task configuration is saved in the database.

Table 180: ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation: Schedule Parameters

Parameter	Description
Run	The frequency at which the task runs. Select a frequency, then configure the related time and day/date parameters. Values: • 1 Hour • 3 Hours • 6 Hours • 12 Hours • Daily Default: 3 Hours **Note:** Tasks run according to the time as configured on the APSolute Vision client.

Table 180: ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation: Schedule Parameters (cont.)

Parameter	Description
Run Always	Specifies whether the task always runs or only during the defined period. Values: • Enabled–The task is activated immediately and runs indefinitely, with no start or end time, at the frequency specified in **Run** box. • Disabled–The task runs (at the frequency specified in the **Run** box tab) from the specified **Start Date** at the **Start Time** until the **End Date** at the **End Time**. Default: Enabled
Start Date[1]	The date and time at which the task is activated.
Start Time[1]	
End Date[1]	The date and time after which the task no longer runs.
End Time[1]	

1 – This parameter is available only when the **Run Always** checkbox is cleared.

Table 181: ERT Active Attackers Feed for Radware DefensePro DDoS Mitigation: Target Device List

Parameter	Description
Allow Device Updates During Attacks	Specifies whether the task tries to update a device also when the device is mitigating an attack. Default: Disabled **Caution:** Updating a device with the ERT Active Attackers Feed includes running the Update Policies action. Therefore, updating a device with the ERT Active Attackers Feed when Radware DefensePro DDoS Mitigation is handling an attack may cause attack leakage.
The **Available** lists and the **Selected** lists of Radware DefensePro DDoS Mitigation devices and Logical Groups (of Radware DefensePro DDoS Mitigation devices). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices whose Black List rules this task updates. The **Selected** *Logical Group* list displays the Logical Groups with the devices whose Black List rule files this task updates. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Note:** When a Logical Group is selected, the effective *Target Device List* dynamically updates–according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.	

Geolocation Feed–Parameters

The *Geolocation Feed* task retrieves the Geolocation feed from radware.com, and uploads the feed to selected Radware DefensePro DDoS Mitigation devices.

Note: DefenseFlow can use an associated Radware DefensePro DDoS Mitigation device for the Geolocation feed.

Using the *Geolocation Feed* task requires a valid subscription to the *Location-Based Mitigation (GeoIP)* service.

Caution: The Location-Based Mitigation (GeoIP) service requires APSolute Vision communication with services.radware.com *and also with* radwareti.s3.amazonaws.com–that is Amazon Simple Storage Service (Amazon S3). You may configure APSolute Vision communication with services.radware.com through your own proxy server.

Caution: SSH must be enabled on the selected Radware DefensePro DDoS Mitigation devices for the *Geolocation Feed* task to run. (You can enable SSH on Radware DefensePro DDoS Mitigation in the *Configuration* perspective, under **Setup > Device Security > Access Protocols> SSH Parameters > Enable SSH**.)

Caution: The task updates the entries in the Geolocation module in each selected Radware DefensePro DDoS Mitigation device *sequentially*, and if the task fails on one device, the task-run does not continue. For example, suppose the task is configured with three selected Radware DefensePro DDoS Mitigation devices, A, B, and C. The task succeeds on device A. The task fails on device B, and stops. The task does not try to update device C.

Table 182: Geolocation Feed: General Parameters

Parameter	Description
Name	A name for the task.
Description	A user-defined description of the task.
Enabled	When selected, the task runs according to the defined schedule. Disabled tasks are not activated, but the task configuration is saved in the database.

Table 183: Geolocation Feed: Schedule Parameters

Parameter	Description

Run	The frequency at which the task runs. Select a frequency, then configure the related time and day/date parameters. Values: • Daily–The task runs daily at the specified time. • Weekly–The task runs every week on the specified day or days, at the specified time. **Note:** Tasks run according to the time as configured on the APSolute Vision client.

Table 183: Geolocation Feed: Schedule Parameters (cont.)

Parameter	Description
Time[1]	The time at which the task runs.
Run Always[2]	Specifies whether the task always runs or only during the defined period. Values: • Enabled–The task is activated immediately and runs indefinitely, with no start or end time. It runs at the first Time configured with the Frequency in the *Schedule* tab. • Disabled–The task runs (at the time and frequency specified in the *Schedule* tab) from the specified **Start Date** at the **Start Time** until the **End Date** at the **End Time**. Default: Enabled
Start Date[3]	The date and time at which the task is activated.
Start Time[3]	
End Date[3]	The date and time after which the task no longer runs.
End Time[3]	

1 – This parameter is available only when the specified **Run** value is **Daily** or **Weekly**. 2 – This parameter is available only when the specified **Run** value is **Daily** or **Weekly**. 3 – This parameter is available only when the **Run Always** checkbox is cleared.

Table 184: Geolocation Feed: Target Device List

Parameter	Description
Allow Device Updates During Attacks	Specifies whether the task tries to update a device also when the device is mitigating an attack. Default: Disabled
The **Available** lists and the **Selected** lists of Radware DefensePro DDoS Mitigation devices and Logical Groups (of Radware DefensePro DDoS Mitigation devices). The **Available** lists display the available devices and available Logical Groups. The **Selected** *device* list displays the devices whose Geolocation profiles this task updates. The **Selected** *Logical Group* list displays the Logical Groups with the devices whose Geolocation profiles this task updates. Select entries from the lists and use the arrows to move the entries to the other lists as required. **Note:** When a Logical Group is selected, the effective *Target Device List* dynamically updates–according to the devices in the Logical Group. That is, when the device-set of a Logical Group changes, the effective *Target Device List* changes accordingly. For more information, see Using Logical Groups of Devices, page 72.	

Updating the Attack Description File

You can view the time of the latest update of the Attack Description file on the APSolute Vision server, and you can update the file.

The Attack Description file contains descriptions of all the different attacks that Radware DefensePro DDoS Mitigation can handle. You can view a specific description by entering the attack name. When you first configure APSolute Vision, you should download the latest Attack Description file to the APSolute Vision server. The file is used for real-time and historical reports to show attack descriptions for attacks coming from Radware DefensePro DDoS Mitigation devices.

The file versions on APSolute Vision and on the Radware DefensePro DDoS Mitigation devices should be identical. Cisco recommends synchronizing regular updates of the file at regular intervals on APSolute Vision and on the individual devices.

Note: Cisco recommends updating the Attack Description file each time you update the Signature files on Radware DefensePro DDoS Mitigation devices.

When you update the Attack Description file, APSolute Vision downloads the file directly from Radware.com or from the enabled proxy file server.

To view the date and time of the last update of the Attack Description file

1. In the *APSolute Vision Settings* view *System* perspective, select **GeneralSettings > Basic Parameters**.
2. Select the *Attack Descriptions File* tab. The **Attack Descriptions Last Update** text box displays the time of the latest update of the Attack Description file on the APSolute Vision server.

To update the Attack Description file

1. In the *APSolute Vision Settings* view *System* perspective, select **GeneralSettings > Basic Parameters**.
2. Do one of the following:
   - To update the Attack Description file from Radware.com, select the **Radware.com** radio button.
   - To update the files from the APSolute Vision client host:
     a. Select the **Client** radio button.
     b. In the **File Name** text box, enter the file path of the Attack Description file or click **Browse** to navigate to and select the file.
3. Click **Update**. The *Alerts* pane displays a success or failure notification and whether the operation was performed using a proxy server.

CHAPTER 8 – MONITORING AND CONTROLLING THE OPERATIONAL STATUS

APSolute Vision's online monitoring for Radware DefensePro DDoS Mitigation can serve as part of a Network Operating Center (NOC) that monitors and analyzes the network and connected devices for changes in conditions that may impact network performance.

This section contains the following topics:

- Monitoring the General Radware DefensePro DDoS Mitigation Device Information, page 303
- Monitoring and Controlling Radware DefensePro DDoS Mitigation Ports, page 304
- Monitoring Radware DefensePro DDoS Mitigation Resource Utilization, page 306
- Monitoring Security Group Tags (SGTs), page 310

Monitoring the General Radware DefensePro DDoS Mitigation Device Information

The *Overview* pane displays general device information, including the information about the software version on the device and the hardware version of the device.

To display general device information for a selected device

> In the *Monitoring* perspective, select **Operational Status > Overview**.

Table 185: Overview: Basic Parameters

Parameter	Description
Hardware Platform	The type of hardware platform for this device.
Uptime	The system up time in days, hours, minutes, and seconds.
Base MAC Address	The MAC address of the first port on the device.
Device Serial Number	

Table 186: Overview: Signature Update Parameters

Parameter	Description
Radware Signature File Version	The version of the Radware Signature File installed on the device.

Table 187: Overview: Software Parameters

Parameter	Description
Software Version	The version of the product software installed on the device.

Table 187: Overview: Software Parameters (cont.)

Parameter	Description
Build	The build number of the current software version.
Version Status	The state of this software version. Values: • Open–Not yet released • Final–Released version
Throughput License	Values: • *The maximum throughput that the license allows.* • Unlimited

Table 188: Overview: Hardware Parameters

Parameter	Description
RAM Size	The amount of RAM, in megabytes.
Flash Size	The size of flash (permanent) memory, in megabytes.
Cores	The number of CPUs/cores that the device uses for processing traffic. That is, the value does *not* include the CPUs/cores for Radware DefensePro DDoS Mitigation management. **Note:** On virtual Radware DefensePro DDoS Mitigation platforms, you can specify the number of virtual cores in the initial setup of the virtual instance.
CPU Speed	The CPU speed, in GHz.

Monitoring and Controlling Radware DefensePro DDoS Mitigation Ports

A Layer 2 interface is defined as any interface that has its own MAC address, physical port, trunk, and VLAN.

You can also change the administrative status of a port, from *Up* to *Down* or vice versa.

To change the administrative status of a port or trunk

1. In the *Monitoring* perspective, select **Operational Status > Ports and Trunks**.
2. Select the rows with the relevant ports, and click the (Disable Selected Ports) button (for a port currently Up) or the (Enable Selected Ports) button (for a port that is currently *Down*).

To display L2 interface statistics for a selected device

1. In the *Monitoring* perspective, select **Operational Status > Ports and Trunks**.
2. To view the statistics for a specific port all in one dialog box, double-click the row.

Table 189: L2 Interface Statistics Basic Parameters

Parameter	Description
Port Name	The interface name or index number.
Port Family	A hard-coded description of the interface.
Port Description	A user-defined description of the interface.
Port Speed	The current bandwidth of the interface, in megabits per second.
MAC Address	The MAC address of the interface.
Admin Status	The administrative status of the interface, **Up** or **Down**.
Operational Status	The operational status of the interface, **Up** or **Down**.
Last Change Time	The value of System Up time at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is zero (**0**).

Table 190: L2 Interface Statistics Parameters

Parameter	Description
Incoming Bytes	The number of incoming octets (bytes) through the interface including framing characters.
Incoming Unicast Packets	The number of packets delivered by this sub-layer to a higher sub- layer, which were not addressed to a multicast or broadcast address at this sub-layer.
Incoming Non-Unicast Packets	The number of packets delivered by this sub-layer to a highersub- layer, which were addressed to a multicast or broadcast address at this sub-layer.
Incoming Discards	The number of inbound packets chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Incoming Errors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher- layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
Outgoing Bytes	The total number of octets (bytes) transmitted out of the interface, including framing characters.
Outgoing Unicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
Outgoing Non-Unicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those discarded or not sent.

Outgoing Discards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

Table 190: L2 Interface Statistics Parameters (cont.)

Parameter	Description
Outgoing Errors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Monitoring Radware DefensePro DDoS Mitigation Resource Utilization

This section contains the following topics:

- Monitoring Radware DefensePro DDoS Mitigation CPU Utilization, page 306
- Monitoring Radware DefensePro DDoS Mitigation RAM and Disk Utilization, page 307
- Monitoring and Clearing Radware DefensePro DDoS Mitigation Authentication Tables, page 309
- Monitoring Radware DefensePro DDoS Mitigation Syslog Information, page 310

Note: On virtual platforms, like Radware DefensePro DDoS Mitigation, the *Policies* pane in the *Monitoring* perspective (**Operational Status > Resource Utilization > Policies**) shows no information.

Monitoring Radware DefensePro DDoS Mitigation CPU Utilization

You can view statistics for the device's average resource utilization and the utilization for each accelerator.

Tip: You can configure Radware DefensePro DDoS Mitigation to issue *Device-Health Event* messages (SNMP traps and syslog messages) for high *controller CPU* utilization and/or high *flow- engine CPUs* utilization (*Configuration* perspective, **Setup > Advanced Parameters > CPU Load Settings**). For more information, see Configuring CPU-Load Alerts Parameters, page 142.

To monitor device utilization for a selected Radware DefensePro DDoS Mitigation device

> In the *Monitoring* perspective, select **Operational Status > Resource Utilization > CPU Utilization**.

Table 191: CPU Utilization: Controller Utilization Parameters

Parameter	Description
Controller Utilization	The percentage of the controller's resources currently utilized.
Average Controller Utilization - Last 5 Seconds	The average utilization of controller's resources in the last 5 seconds.
Average Controller Utilization - Last 60 Seconds	The average utilization of controller's resources in the last 60 seconds.

Table 192: CPU Utilization: Engines Utilization Parameters

Parameter	Description
Engine ID	The name of the flow engine.
Forwarding Task	The percentage of CPU cycles used for traffic processing.
Other Tasks	The percentage of CPU resources used for other tasks such as aging and so on.
Idle Task	The percentage of free CPU resources.

Monitoring Radware DefensePro DDoS Mitigation RAM and Disk Utilization

Use the *RAM and Disk Utilization* page to do the following:

- View statistics for the device's RAM utilization and disk utilization.
- Configure the device to issue alerts about RAM utilization and disk utilization. Radware DefensePro DDoS Mitigation issues these alerts as SNMP traps, which are also displayed in the APSolute Vision *Alerts Table*. In the context of Radware DefensePro DDoS Mitigation, these alerts are *Device-Health Events*. In the context of APSolute Vision, these alerts are *Device Health Errors*.

Notes

— APSolute Vision can convey *Device Health Error* messages from the APSolute Vision *Alerts Table* (*APSolute Vision Settings* view *System* perspective, **General Settings > Alert Settings > Alert Browser**). APSolute Vision can convey the messages in various formats, including syslog messages. For information, see the *APSolute Vision User Guide* or the APSolute Vision online help.

— If you require *Device-Health Events* (also) as syslog messages directly from the Radware DefensePro DDoS Mitigation device, make sure that the **Device-Health Events** checkbox is selected in the configuration of the syslog server(s) (*Configuration* perspective, **Setup > Reporting Settings > Syslog**). For information, see Configuring Radware DefensePro DDoS Mitigation Syslog Settings, page 146.

To configure alert settings for RAM utilization and disk utilization

1. In the *Monitoring* perspective, select **Operational Status > Resource Utilization > RAM and Disk Utilization**.
2. Configure the parameters, and then, click **Submit**.

Table 193: RAM and Disk Utilization–Alert Parameters

Parameter	Description
Enable RAM Utilization Alerts	Specifies whether the device issues alerts about RAM utilization. Default: Enabled

Table 193: RAM and Disk Utilization–Alert Parameters (cont.)

Parameter	Description
RAM Utilization Alert Level (This parameter is available only when the **Enable RAM Utilization Alerts** is selected.)	The percentage of the device's RAM utilization above which the device sends an alert. The device issues another message when the utilization level returns to below the specified percentage. Values: 50–99 Default: 85
Enable Disk-Space Utilization Alerts	Specifies whether the device sends alerts about disk-space utilization. Default: Enabled
Disk-Space Utilization Alert Level (This parameter is available only when the **Enable Disk-Space Utilization Alerts** is selected.)	The percentage of the device's disk-space utilization above which the device sends alerts. The device issues another message when the utilization level returns to below the specified percentage. Values: 30–99 Default: 50

To monitor RAM utilization and disk utilization

> In the *Monitoring* perspective, select **Operational Status > Resource Utilization > RAM and Disk Utilization**.

Table 194: RAM and Disk Utilization–Monitoring Parameters

Parameter	Description
RAM Utilization	
RAM Capacity	The device's total RAM capacity, in GB.
Used RAM	The amount, in GB, of the device's RAM currently used.
RAM Used	The percentage of the device's RAM currently utilized.
Disk Utilization	
Hard Disk Capacity	The device's hard disk capacity, in GB.
Used Disk Space	The amount, in GB, of the device's hard disk currently used.
Disk Space Utilization	The percentage of the device's hard-disk space currently utilized.

Monitoring and Clearing Radware DefensePro DDoS Mitigation Authentication Tables

You can view statistics for the device's Authentication Tables. You can also clear the contents of each table.

To monitor Authentication Tables for a selected Radware DefensePro DDoS Mitigation device

> In the *Monitoring* perspective, select **Operational Status > Resource Utilization> Authentication Tables**.

Table 195: TCP Authentication Table: Monitoring Parameters

Parameter	Description
Table Size	The number of source addresses that the table can hold.
Table Utilization	Percent of the table that is currently utilized.
Aging Time	The aging time, in seconds, for the table.

Table 196: Radware DefensePro DDoS Mitigation HTTP Authentication Table: Monitoring Parameters

Parameter	Description
Table Size	The number of source-destination couples for protected HTTP servers. For example, if there are two attacks towards two HTTP servers and the source addresses are the same, for those two servers, there will be two entries for the source in the table.
Table Utilization	Percent of the table that is currently utilized.
Aging Time	The aging time, in seconds, for the table. Values: 60–3600 Default: 1200

To clean an Authentication Table for a selected Radware DefensePro DDoS Mitigation device

1. In the *Monitoring* perspective, select **Operational Status > Resource Utilization> Authentication Tables**.
2. In the relevant tab (that is, **TCP Authentication Table**, **HTTP Authentication Table**, or **DNS Authentication Table**), click **Clean Table**.

Note: For the TCP Authentication Table and the HTTP Authentication Table, the **Clean Table** action can take up to 10 seconds.

Monitoring Radware DefensePro DDoS Mitigation Syslog Information

You can view information relating to the syslog mechanism.

Note: Radware DefensePro DDoS Mitigation can send event traps to syslog servers which are specified in the device configuration (*Configuration* perspective, **Setup > Reporting Settings > Syslog**). For more information, see Configuring Radware DefensePro DDoS Mitigation Syslog Settings, page 146.

To monitor Radware DefensePro DDoS Mitigation syslog information

> In the *Monitoring* perspective, select **Operational Status > Resource Utilization > Syslog Monitor**.

Table 197: Radware DefensePro DDoS Mitigation Syslog Monitoring Parameters

Parameter	Description
Syslog Server	The name of the syslog server.
Status	The status of the syslog server. Values: • Reachable–The server is reachable. • Unreachable–The server is unreachable. • N/R–Specifies *not relevant*, because traffic towards the Syslog server is over UDP–as specified (*Configuration* perspective, **Setup > Syslog Server > Protocol >UDP**).
Messages in Backlog	The number of messages in the backlog to the syslog server.

Monitoring Security Group Tags (SGTs)

You can monitor the name and value of the enabled SGT, if one exists.

Note: For more information on SGTs in Radware DefensePro DDoS Mitigation, see Managing SGT Classes, page 156.

Note: For more information on SGTs in Radware DefensePro DDoS Mitigation, see Managing SGT Classes, page 1688.

To monitor SGTs

> In the *Monitoring* perspective, select **Operational Status > SGT**.

Table 198: SGT Monitoring Parameters

Parameter	Description
Name	The name of the SGT.
Value	The value of the SGT.

CHAPTER 9 – MONITORING CLUSTERING

Use the *Clustering Status* pane to monitor cluster nodes in Radware DefensePro DDoS Mitigation for Cisco Firepower.

To monitor clustering

> In the *Monitoring* perspective, select **Clustering > Cluster Status**.

Table 199: Clustering Monitoring Parameters

Parameter	Description
IP Address	The IP address of the cluster node.
Status	The state of the cluster node.

CHAPTER 10 – MONITORING RADWARE DEFENSEPRO DDOS MITIGATION STATISTICS

Monitoring Radware DefensePro DDoS Mitigation statistics comprises the following topics:

- Monitoring Radware DefensePro DDoS Mitigation SNMP Statistics, page 315
- Monitoring Radware DefensePro DDoS Mitigation IP Statistics, page 316

Monitoring Radware DefensePro DDoS Mitigation SNMP Statistics

You can view statistics for the SNMP layer of the device.

To monitor Radware DefensePro DDoS Mitigation SNMP statistics

> In the *Monitoring* perspective, select **Statistics > SNMP Statistics**.

Table 200: Radware DefensePro DDoS Mitigation SNMP Statistics

Parameter	Description
Number of SNMP Received Packets	The total number of messages delivered to the SNMP entity from the transport service.
Number of SNMP Sent Packets	The total number of SNMP messages passed from the SNMP protocol entity to the transport service.
Number of SNMP Successful 'GET' Requests	The total number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP GET-Request and GET-Next PDUs.
Number of SNMP Successful 'SET' Requests	The total number of MIB objects modified successfully by the SNMP protocol entity as the result of receiving valid SNMP SET-Request PDUs.
Number of SNMP 'GET' Requests	The total number of SNMP GET-Request PDUs accepted and processed by the SNMP protocol entity.
Number of SNMP 'GET-Next' Requests	The total number of SNMP GET-Next Request PDUs accepted and processed by the SNMP protocol entity.
Number of SNMP 'SET' Requests	The total number of SNMP SET-Request PDUs accepted and processed by the SNMP protocol entity.
Number of SNMP Error “Too Big” Received	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is ‘tooBig.’
Number of SNMP Error “No Such Name” Received	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status is ‘noSuchName’.

Table 200: Radware DefensePro DDoS Mitigation SNMP Statistics (cont.)

Parameter	Description
Number of SNMP Error “Bad Value” Received	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is ‘badValue’.
Number of SNMP Error “Generic Error” Received	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is ‘genErr’.
Number of SNMP 'GET' Responses Sent	The total number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
Number of SNMP Traps Sent	The total number of SNMP Trap PDUs generated by the SNMP protocol entity.

Monitoring Radware DefensePro DDoS Mitigation IP Statistics

You can monitor statistics for the IP layer of the device, including the number of packets discarded and ignored. This enables you to quickly summarize the state of network congestion from a given interface.

To display IP statistics information for a selected Radware DefensePro DDoS Mitigation device

> In the *Monitoring* perspective, select **Statistics > IP Statistics**.

Table 201: IP Statistics Parameters

Parameter	Description
Number of IP Packets Received	The total number of input datagrams received from interfaces, including those received in error.
Number of IP Header Errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
Number of Discarded IP Packets	The total number of input datagrams for management that were discarded. This counter does not include any datagrams discarded while awaiting re-assembly.
Number of Valid IP Packets Received	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Number of Transmitted Packets (Inc. Discards)	The total number of IP datagrams which local IP user-protocols, including ICMP supplied to IP in requests for transmission. This counter does not include any datagrams counted in the Number of IP Packets Forwarded.

Table 201: IP Statistics Parameters (cont.)

Parameter	Description
Number of Discarded Packets on TX	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded, for example, the lack of buffer space. This counter includes any datagrams counted in the Number of IP Packets Forwarded if those packets meet this (discretionary) discard criterion.

Table 202: Router Statistics Parameters

Parameter	Description
Number of IP Packets Forwarded	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP Gateways, this counter includes only those packets which were Source – Routed via this entity, and the Source – Route option processing was successful.
Number of IP Packets Discarded Due to 'Unknown Protocol'	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Number of IP Packets Discarded Due to 'No Route'	The number of IP datagrams discarded because no route could be found to transmit them to their destination. **Note:** This counter includes any packets counted in the Number of IP Packets Forwarded that meet the no-route criterion. This includes any datagrams which a host cannot route because all of its default gateways are down.
Number of IP Fragments Received	The number of IP fragments received which needed to be reassembled at this entity.
Number of IP Fragments Successfully Reassembled	The number of IP datagrams successfully re-assembled.
Number of IP Fragments Failed Reassembly	The number of failures detected by the IP re-assembly algorithm, such as timed out, errors, and so on. Note: This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Number of IP Datagrams Successfully Reassembled	The number of IP datagrams that have been successfully re- assembled at this entity.
Number of IP Datagrams Discarded Due to Fragmentation Failure	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.
Number of IP Datagrams Fragments Generated	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
Valid Routing Entries Discarded	Number of valid routing entries discarded.

CHAPTER 11 – MONITORING AND CONTROLLING NETWORKING

Monitoring and controlling Radware DefensePro DDoS Mitigation networking comprises the following topics:

- Monitoring the Session Table, page 319
- Monitoring Routing Table Information, page 320
- Monitoring Radware DefensePro DDoS Mitigation ARP Table Information, page 320
- Monitoring the Radware DefensePro DDoS Mitigation Suspend Table, page 321
- Location-Based Suspended Traffic, page 322

Monitoring the Session Table

Each Radware DefensePro DDoS Mitigation device includes a Session table to keep track of sessions bridged and forwarded by the device.

Note: Radware DefensePro DDoS Mitigation issues alerts for high utilization alerts of the Session table. Radware DefensePro DDoS Mitigation sends alerts to APSolute Vision when table utilization reaches 90% and 100%.

To view Session table information

> In the *Monitoring* perspective, select **Networking > Session Table > SessionTable**.

Table 203: Session-Table Monitoring Parameters

Parameter	Description
Source IP	The source IP address within the defined subnet.
Destination IP	The destination IP address within the defined subnet.
Source L4 Port	The session source port.
Destination L4 Port	The session destination port.
Context Group Tag	The **Tag** value of the Context Group class associated with the entry.
Protocol	The session protocol.
Lifetime (Sec.)	The time, in seconds, following the arrival of the last packet, that the entry remains in the table before it is deleted.

Monitoring Routing Table Information

The Routing table stores information about destinations and how they can be reached.

By default, all networks directly attached to the Radware DefensePro DDoS Mitigation device are registered in this table. Other entries can be statically configured or dynamically created through the routing protocol.

Note: The Routing table is not automatically refreshed periodically. The information is loaded when you select to display the *Routing Table* pane, and when you manually refresh the display.

To display Routing Table information for a selected device

> In the *Monitoring* perspective, select **Networking > Routing**.

Table 204: Routing-Table Monitoring Parameters

Parameter	Description
Destination Network	The destination network to which the route is defined.
Netmask	The network mask of the destination subnet.
Next Hop	The IP address of the next hop toward the Destination subnet. (The next hop always resides on the subnet local to the device.)
Via Interface	In Radware DefensePro DDoS Mitigation, the value is **MNG-1** (read-only), which is the value of the management interface.
Type	This field is displayed only in the Static Routes table. The type of routing. Values: • Local–The subnet is directly reachable from the device. • Remote–The subnet is not directly reachable from the device.
Metric	The metric value defined or calculated for this route.

Monitoring Radware DefensePro DDoS Mitigation ARP Table Information

You can view the device's ARP table, which contains both static and dynamic entries. You can change an entry type from dynamic to static.

Note: The ARP table is not automatically refreshed periodically. The information is loaded when you select to display the ARP Table pane, and when you manually refresh the display.

To display ARP Table information for a selected Radware DefensePro DDoS Mitigation device

> In the *Monitoring* perspective, select **Networking > ARP**.

Table 205: Radware DefensePro DDoS Mitigation ARP-Table Monitoring Parameters

Parameter	Heading
Port	The interface number where the station resides.
IP Address	The station's IP address.
MAC Address	The station's MAC address.
Type	The entry type. Values: • Other–Not Dynamic or Static. • Dynamic–Entry is learned from ARP protocol. If the entry is not active for a predetermined time, the node is deleted from the table. • Static–Entry has been configured by the network management station and is permanent.

To change an entry type from dynamic to static

1. In the *Monitoring* perspective, select **Networking > ARP**.
2. Select the entry, and select **Change Entry to Static**.

Monitoring the Radware DefensePro DDoS Mitigation Suspend Table

When a Connection Limit profile detects an attack, Radware DefensePro DDoS Mitigation can suspend traffic according to the specified **Suspend Action** for a defined time period. The Suspend table stores the entries that define the suspended traffic.

To view the real-time Suspend table for a selected Radware DefensePro DDoS Mitigation device

> In the *Monitoring* perspective, select **Networking > Suspend Table**.

Table 206: Radware DefensePro DDoS Mitigation Suspend-Table Monitoring Parameters

Parameter	Description
Source IP	The IP address from which traffic was suspended.
Destination IP	The IP address to which traffic was suspended. The value **0.0.0.0** specifies *all* destinations.
Destination Port	The application port to which traffic was suspended.
Protocol	The network protocol of the suspended traffic.
Module	The security module that activated the traffic suspension. Values: Anti-Scanning, Connection Limit, Traffic Filters
Classification Type	Value: Policy–A Protection policy suspended the traffic.
Policy Name	The name of the Protection policy that suspended the traffic.

Table 206: Radware DefensePro DDoS Mitigation Suspend-Table Monitoring Parameters (cont.)

Parameter	Description
Expiration Type	The method of determining the expiration. Value: Dynamic Timeout
Expiration Time	The number of seconds until the entry is aged from the Suspend table.

Location-Based Suspended Traffic

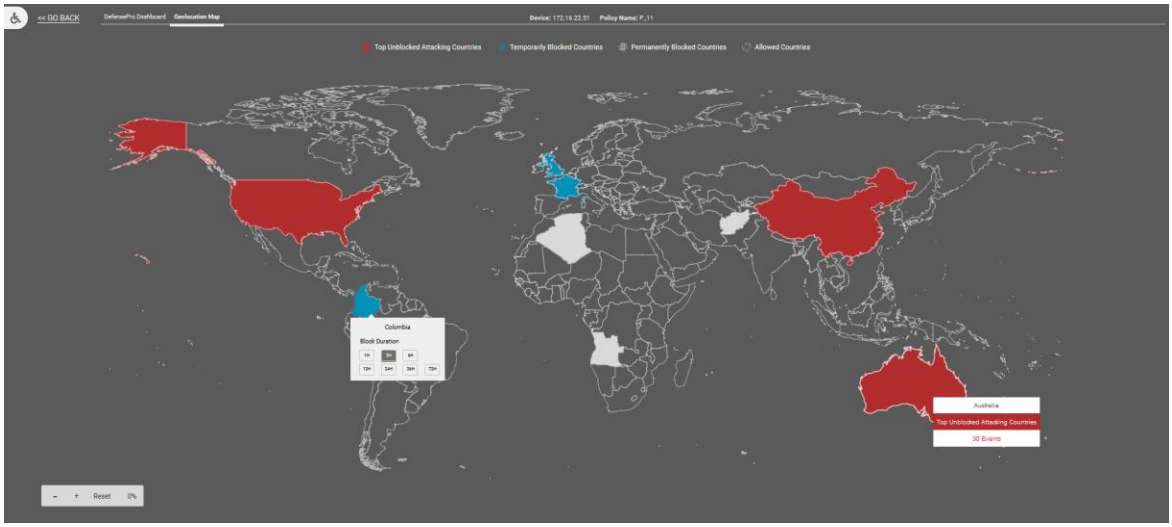
This feature requires a *Geolocation subscription*. For more information, contact Technical Support.

This feature requires a *Geolocation subscription*. and an *APSolute Vision Analytics - AMS* license installed on the APSolute Vision server. For more information, contact Technical Support.

You can use the *Location-Based Suspended Traffic* pane to view the list of geolocations that are temporarily blocked (that is, suspended) using the using the *Geolocation Map* in APSolute Vision Analytics.

For more information on APSolute Vision Analytics (AVA), see the *APSolute Vision Analytics User Guide* or the APSolute Vision online help.

Figure 38: Geolocation Map in APSolute Vision Analytics



To view the list of temporarily blocked geolocations

> In the *Monitoring* perspective, select **Networking > Location-Based SuspendedTraffic**.

Table 207: Location-Based Suspended Traffic Parameters

Parameter	Description
Policy Name	The name of the Protection policy with the temporarily blocked geolocation.
Geolocation	The geolocation code.
Suspended At	The time that the geolocation was blocked.
Suspension Expires At	The time that the block expires.

CHAPTER 12 – USING REAL-TIME SECURITY MONITORING

When an attack is detected, Radware DefensePro DDoS Mitigation creates and reports a *security event*, which includes the information relevant to the specific attack. The *Security Monitoring* perspective displays information relevant to the specific attack along with real-time network traffic and statistical parameters. Use the *Security Monitoring* perspective to observe and analyze the attacks that the device detected and the countermeasures that the device implemented.

The following main topics describe security monitoring in APSolute Vision:

- Risk Levels, page 324
- Using the Dashboard Views for Real-Time Security Monitoring, page 324
- Viewing Real-Time Traffic Reports, page 344
- Protection Monitoring, page 353
- HTTP Reports, page 360

Notes

- Your user permissions (your *RBAC user definition)* determine the Radware DefensePro DDoS Mitigation devices and policies that the *Security Monitoring* perspective displays to you. You can view and monitor only the attacks blocked by the Radware DefensePro DDoS Mitigation devices and policies that are available to you.
- APSolute Vision also manages and issues alerts for new security attacks.
- Radware DefensePro DDoS Mitigation calculates traffic baselines, and uses the baselines to identify abnormalities in traffic levels.
- At the time of writing, APSolute Vision collects the sampled attack data that Radware DefensePro DDoS Mitigation sends to it at the rate of two samples per two minutes per attack. Please note that the rate is subject to change without notice.
- When calculating the real-time network traffic and statistical parameters, Radware DefensePro DDoS Mitigation does not include traffic that exceeded the throughput license.
- You can use *APSolute Vision Analytics* to view and analyze real-time and historical security information from Radware DefensePro DDoS Mitigation version-8.*x* devices. APSolute Vision Analytics includes dashboards for Radware DefensePro DDoS Mitigation security monitoring and analytics, customizable reports, and in-depth forensics capabilities. Full functionality of APSolute Vision Analytics requires a license. For more information, see the APSolute Vision online helpor the *APSolute Vision Analytics User Guide*.
- You can use the APSolute Vision REST API to view security events from Radware DefensePro DDoS Mitigation devices. For more information, see the APSolute Vision REST API documentation.
- You can use the APSolute Vision CLI to export security events from Radware DefenseProDDoS Mitigation devices. For more information, see the *APSolute Vision User Guide*.

Risk Levels

The following table describes the risk levels that Radware DefensePro DDoS Mitigation supports to classify security events.

Note: For some protections, the user can specify the risk level for an event. For these protections, the descriptions in the following table are recommendations, and specifying the risk level is the user's responsibility.

Table 208: Risk Levels

Risk Level	Description
Info	The risk does not pose a threat to normal service operation.
Low	The risk does not pose a threat to normal service operation, but may be part of a preliminary action for malicious behavior.
Medium	The risk may pose a threat to normal service operation, but is not likely to cause complete service outage, remote code execution, or unauthorized access.
High	The risk is very likely to pose a threat to normal service availability, and may cause complete service outage, remote code execution, or unauthorized access.

Using the Dashboard Views for Real-Time Security Monitoring

This section includes the following topics:

- Configuring the Display Parameters of a Dashboard View, page 325
- Using the Current Attacks Table, page 326
- Using the Ongoing Attacks Monitor, page 330
- Attack Details, page 332
- Sampled Data Tab, page 343
- Viewing Real-Time Traffic Reports, page 344
- Viewing the Traffic Utilization Report, page 344

Use a *Dashboard View* in the *Security Monitoring* perspective to analyze activity and security events in the network, identify security trends, and analyze risks.

You can view information for individual devices, all devices in a Site, all devices in a Logical Group, or all devices in the network. The dashboard monitoring display automatically refreshes providing ongoing real-time analysis of the system.

The *Dashboard View* node comprises the following tabs, which display the same summary information:

- **Current Attacks Table**–which is a table display (see Figure 39 - Current Attacks Table, page 327).
- **Ongoing Attacks Monitor**–which includes a graphical, chart display (see Figure 40 - Ongoing Attacks Monitor, page 331).

The **Scope** and other display parameters that you configure apply to the*Current Attacks Table* and to the *Ongoing Attacks Monitor*. For more information, see Configuring the Display Parameters of a Dashboard View, page 325.

When you double-click an attack in the *Current Attacks Table* or *Ongoing Attacks Monitor*, APSolute Vision displays the details in an *Attack Details* tab. There, you can display the *Sampled Data* dialog box for the all attack types that support sampled data.

By default, the display of the *Dashboard View* refreshes every 15 seconds. Administrators can configure the refresh rate (*APSolute Vision Settings* view *System* perspective, **General Settings > Monitoring > Polling Interval for Reports**).

Configuring the Display Parameters of a Dashboard View

The following table describes the display parameters of the *Dashboard View* in the *Security Monitoring* perspective. The **Scope** and **Display Last** parameters that you configure in the *Current Attacks Table* applies to the *Ongoing Attacks Monitor* and vice versa.

Table 209: Security Monitor Dashboard View–Display Parameters

Parameter	Description
Scope	The physical ports and the Protection policies that the dashboard displays. By default, the Scope is **Any Port; Any Policy**. That is, by default, the dashboard displays all the information. To control the scope of the information that the dashboard displays in Radware DefensePro DDoS Mitigation, see the procedure To control the scope of the information that the Dashboard View displays, page 326.
Display Last	How long the dashboard displays attacks after the attack terminates. That is, the dashboard displays all attacks that are currently ongoing or that terminated within the selected period. Values: • 10 Minutes • 20 Minutes • 30 Minutes • 1 Hour • 2 Hours • 6 Hours • 12 Hours • 24 Hours Default: 10 Minutes
Top Attacks to Display (This parameter is available only in the Ongoing Attacks Monitor.)	The number of attacks that the Ongoing Attacks Monitor displays. Values: 1–50 Default: 20

Table 209: Security Monitor Dashboard View–Display Parameters (cont.)

Parameter	Description
Sort By (This parameter is available only in the Ongoing Attacks Monitor.)	Values: • Top Total Packet Count–The Ongoing Attacks Monitor displays the attacks with the highest number of packets. • Top Volume–The Ongoing Attacks Monitor displays the attacks with the highest volume. • Most Recent–The Ongoing Attacks Monitor displays the most recent attacks. • Attack Risk–The Ongoing Attacks Monitor displays the attacks according to attack risk. Default: Top Packet Count

To control the scope of the information that the Dashboard View displays

1. Click Scope. Two tables open. One table has the *Device Name* and *Port* columns, and the other table has the *Device Name* and *Policy* columns.
2. Do one of the following:
   - To limit the Protection policies that the dashboard displays, select the corresponding checkboxes.
   - To display the information for all the currently relevant Protection policies, click in the top- left table cell, and then, select **Select All**.
   - To display all the information in the database, even information that is not associated with a specific port or specific Protection policy, click in the top-left table cell, and then, select **Select None**.

Using the Current Attacks Table

The *Current Attacks Table* displays information on current and recent attacks. The configuration of the display parameters determine the information that the *Current Attacks Table* displays (see Configuring the Display Parameters of a Dashboard View, page 325).

Note: For certain attacks, once Radware DefensePro DDoS Mitigation reports the attack, the **Status** value **Occurred** and the **Start Time** value remain indefinitely. Such attacks include *Packet Anomaly* attacks and DNS Flood attacks with ID 470. For example, suppose a new Radware DefensePro DDoS Mitigation device starts identifying and handling a Packet Anomaly attack with **Radware ID** 105 with the start time **20.02.2017 15:19:09**. The attack subsides. One month later, the Radware DefensePro DDoS Mitigation device starts identifying and handling another Packet Anomaly attack with **Radware ID** 105. The **Start Time** value **20.02.2017 15:19:09** is reported. (For more information on Packet Anomaly protection, see Configuring Global Packet Anomaly Protection, page 134. For more information on the DNS Flood attack with ID 470, see Attack- Protection ID Numbers, page 389.)

To display the Current Attacks Table

1. In the *Security Monitoring* perspective, select the Radware DefensePro DDoS Mitigationdevice, Site, or Logical Group for which to display data.
2. Select **Dashboard View > Current AttacksTable**. You

can do the following in the Current Attacks Table:

- **Filter the rows**–You can filter table rows according to values in the table columns. For more information on filtering table rows, see Filtering Table Rows, page 58.
- **Sort the rows**–You can change the row order from ascending to descending or vice versa. To do this, hover the cursor (pointer) over the column to display the arrow and change theorder.
- **View additional information for a specific attack**–To do this, select the relevant row, and click (View Attack Details). For more information, see Attack Details, page 332.
- **Go to the policy that handled attack**–To do this, click (Go to Policy).
- **Export the information in the table to a CSV file**–To do this, click (CSV). Then, you can view the file or specify the location and file name.
- **Pause the refresh of the table display**–To do this, click (Pause). When the table display is *not* paused, it refreshes approximately every 15 seconds.

Figure 39: Current Attacks Table

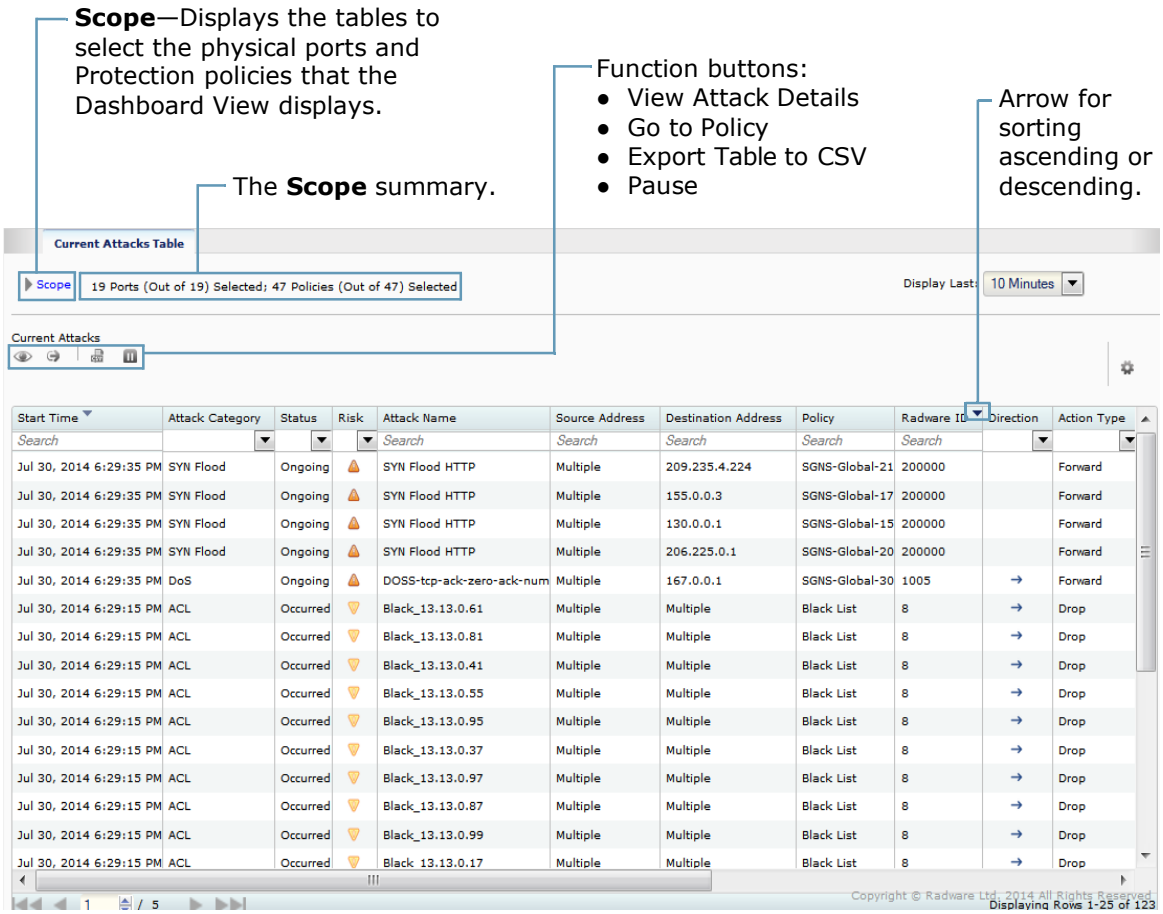


Table 210: Current Attacks Table Parameters

Parameter	Description
Start Time	The date and time that the attack started.[1]
Attack Category	The threat type to which this attack belongs. Values: • ACL • Anomalies[1] • Behavioral DoS • DNS Flood [1] • DoS • Intrusions • SYN Flood • Traffic Filters
Status	The last-reported status of the attack.[1] Values: • Started–An attack containing more than one security event has been detected. (Some attacks contain multiple security events, such as DoS, Scans, and so on.) • Occurred (Signature-based attacks)–Each packet matched with signatures was reported as an attack and dropped. • Ongoing–The attack is currently taking place, that is, the time between Started and Terminated (for attacks that contain multiple security events, such as DoS, Scans, and so on). • Terminated–There are no more packets matching the characteristics of the attack, and the device reports that the attack has ended.
Risk	The predefined attack severity level (see Risk Levels, page 324). Values: ▪  –High ▪  –Medium ▪  –Low ▪  –Info
Attack Name	The name of the detected attack.
Source Address	The source IP address of the attack. If there are multiple IP sources for an attack, this field displays **Multiple**. The multiple IP addresses are displayed in the *Attack Details* window. **Multiple** may also refer to cases when Radware DefensePro DDoS Mitigation cannot report a specific value. The **Search** string can be any legal IPv4 or IPv6 address, and can include a wildcard (*).
Destination Address	The destination IP address of the attack. If there are multiple IP sources for an attack, this field displays **Multiple**. The multiple IP addresses are displayed in the *Attack Details* window. **Multiple** may also refer to cases when Radware DefensePro DDoS Mitigation cannot report a specific value.

Table 210: Current Attacks Table Parameters (cont.)

Parameter	Description
Policy	The name of the configured Protection policy that was violated by this attack. To view or edit the policy for a specific attack, select the attack entry and click the (Go to Policy) button.
Radware ID	The Radware DefensePro DDoS Mitigation Attack-Protection identifier issued by the device.
Direction	The direction of the attack, inbound or outbound. Values: in, out
Action Type	The reported action against the attack. The actions are specified in the protection profile, which may or may not be available or relevant for your system. Values: • Bypass–Radware DefensePro DDoS Mitigation does not protect against this attack, but rather, sends its data out of the device, and may report it. • Challenge–Radware DefensePro DDoS Mitigation challenges the packet. • Destination Reset–Radware DefensePro DDoS Mitigation sends a TCP-Reset packet to the destination IP address and port. • Drop–Radware DefensePro DDoS Mitigation discards the packet. • Forward–Radware DefensePro DDoS Mitigation continues to process the traffic and eventually forwards the packet to its destination. • Proxy • Source Destination Reset–Radware DefensePro DDoS Mitigation sends a TCP-Reset packet to both the packet source IP and the packet destination IP address. • Source Reset–Radware DefensePro DDoS Mitigation sends a TCP-Reset packet to the packet source IP address. • Http 200 Ok–Radware DefensePro DDoS Mitigation sends a 200 OK response using a predefined page and leaves the server-side connection open. • Http 200 Ok Reset Dest–Radware DefensePro DDoS Mitigation sends a 200 OK response using a predefined page and sends a TCP-Reset packet to the server side to close the connection. • Http 403 Forbidden–Radware DefensePro DDoS Mitigation sends a 403 Forbidden response using a predefined page and leaves the server-side connection open. • Http 403 Forbidden Reset Dest–Radware DefensePro DDoS Mitigation sends a 403 Forbidden response using a predefined page and sends a TCP-Reset packet to the server side to close the connection.
Total Packet Count	The number of identified attack packets from the beginning of the attack.
Volume	For most protections, this value is the volume of the attack, in kilobits, from when the attack started. For SYN Flood Protection (SYN cookies), this value is the number of SYN packets dropped, multiplied by 60 bytes (the SYN packet size).
Device IP	The IP address of the attacked device.

Table 210: Current Attacks Table Parameters (cont.)

Parameter	Description
Application Protocol[2]	The transmission protocol used to send the attack. Values: • TCP • UDP • ICMP • IP
MPLS RD[2]	The Multi-protocol Label Switching Route Distinguisher in the policy that handled the attack. The value **N/A** or **0** (zero) in this field indicatesthat the MPLS RD is not available.
VLAN Tag / Context[2]	The VLAN tag value or Context Group in the policy that handled the attack. The value **N/A** or **0** (zero) in this field indicates that the VLAN tag or Context Group is not available.
Source Port[2]	The Layer 4 source port of the attack.
Destination Port[2]	The Layer 4 destination port of the attack. If there are multiple destination L4 ports, this field displays **Multiple**. In cases when Radware DefensePro DDoS Mitigation cannot report a specific value, the field displays **0** (zero).
Physical Port[2]	The port on the device at which the attack packets arrived. In cases when Radware DefensePro DDoS Mitigation cannot report a specific value, the field displays **0** (zero) or **Multiple**.

1 – For certain attacks, once Radware DefensePro DDoS Mitigation reports the attack, the **Status** value **Occurred** and the **Start Time** value remain indefinitely. Such attacks include *Packet Anomaly* attacks and DNS Flood attacks with ID 470. For example, suppose a new Radware DefensePro DDoS Mitigation device starts identifying and handling a Packet Anomaly attack with **Radware ID** 105 with the start time **20.02.2017 15:19:09**. The attack subsides. One month later, the Radware DefensePro DDoS Mitigation device starts identifying and handling another Packet Anomaly attack with **Radware ID** 105. The **Start Time** value **20.02.2017 15:19:09** is reported. (For more information on Packet Anomaly protection, see Configuring Global Packet Anomaly Protection, page 134. For more information on the DNS Flood attack with ID 470, see Attack-Protection ID Numbers, page 389.)

2 – This column is not displayed by default in the *Current Attacks* tab.

To display the column, click the (Table Settings) button and then select therelevant checkbox. Click the button again to close the *Table Settings* list.

Using the Ongoing Attacks Monitor

The *Ongoing Attacks Monitor* comprises two charts: the *Ongoing Attacks Monitor* and *Drop Intensity* gauges. The information that the charts display is according to the configuration of the display parameters (see Configuring the Display Parameters of a Dashboard View, page 325).

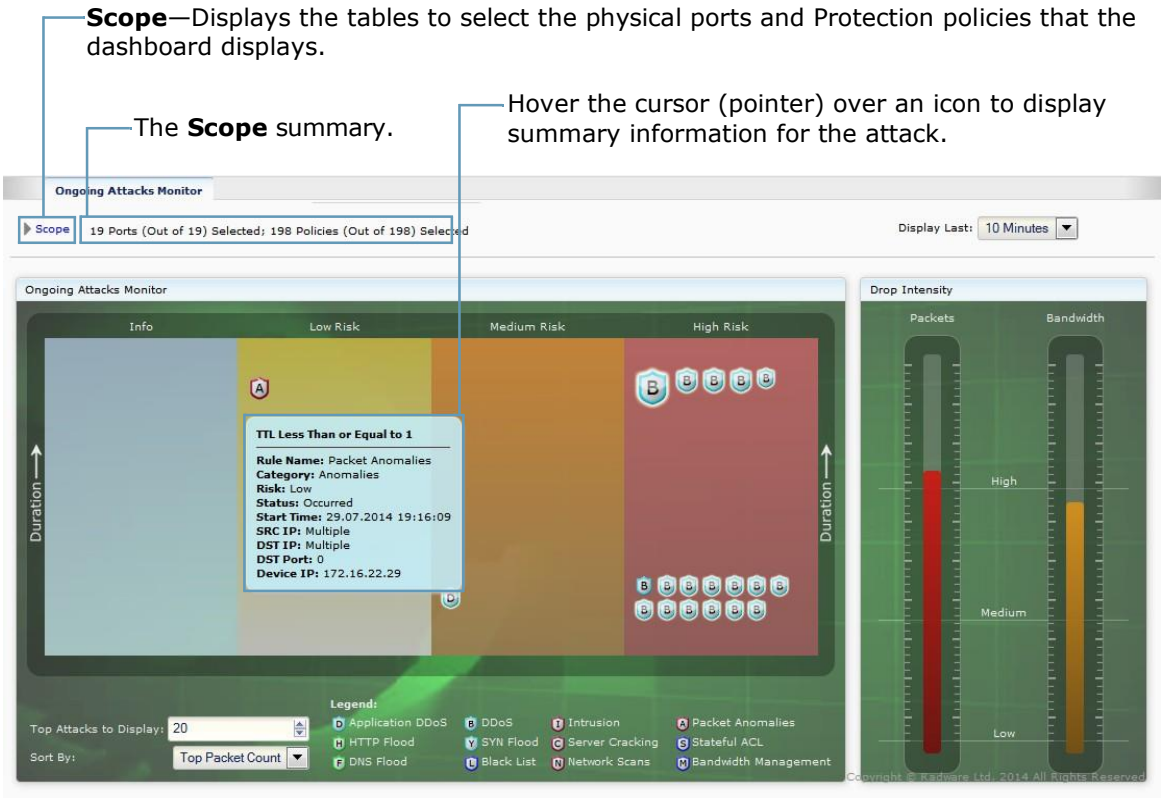
To display the Ongoing Attacks Monitor

1. In the *Security Monitoring* perspective, select the Radware DefensePro DDoS Mitigationdevice, Site, or Logical Group for which to display data.
2. Select **Dashboard View > Ongoing Attacks Monitor**.

The *Ongoing Attacks Monitor* is a graphical representation of current and recent attacks. Each icon in the monitor represents a separate attack. The icon type (see the legend) represents the type of protection that the attack violates. A flashing icon represents an ongoing attack. The horizontal position of each icon in the chart indicates the attack risk (see Risk Levels, page 324). The vertical position of the icon in the chart indicates the attack duration; the higher in the chart, the longer the attack has existed. Attacks that have started recently are lower in the monitor. The icon size indicates the amount of dropped data for the attack type relative to other attacks of the same type. Hover the cursor (pointer) over an icon to display summary information for the attack. Double-click an icon to display detailed information for the attack. For more information, see Attack Details, page 332.

There are two *Drop Intensity* gauges: *Packets* and *Bandwidth*. The *Packets* gauge indicates the proportion of dropped packets relative to the total packets. The *Bandwidth* gauge indicates the proportion of dropped bandwidth relative to the total bandwidth (according to the license). The gauges show the calculated ranges Low (up to 30% dropped), Medium (up to 70% dropped), and High (more than 70% dropped).

Figure 40: Ongoing Attacks Monitor



Attack Details

APSolute Vision displays an *Attack Details* tab when you double-click an attack in a Security Monitoring *Dashboard View*.

APSolute Vision displays attack details for the following attacks:

- Anti-Scanning Details, page 333
- BDoS Attack Details, page 334
- DNS Flood Attack Details, page 337
- DoS Attack Details, page 339
- Intrusions Attack Details, page 340
- Packet Anomalies Attack Details, page 340
- SYN Flood Attack Details, page 341
- Traffic Filters Attack Details, page 342

Each *Attack Details* tab includes two or more sub-tabs, which provide details on the attack. All *Attack Details* tabs include the sub-tabs *Attack Characteristics* and the *Attack Description*. The *Attack Characteristics* tab displays information that is also available in the hidden columns of the *Current Attacks Table*. The *Attack Description* tab displays the information from the Attack Descriptions file. An attack description is displayed only if the Attacks Description file has been uploaded on the APSolute Vision server.

Notes

- To display hidden columns of the *Current Attacks Table*, click the (Table Settings) button and then select the relevant checkbox. Click the button again to close the *Table Settings* list.
- For information about uploading the Attacks Description file, see Updating the Attack Description File, page 302.

In addition to viewing the details of the attack, in each *Attack Details* tab, you can do the following:

- **View sampled data from the attack**–To do this, click the (View Sampled Data) button. For more information, see Sampled Data Tab, page 343.
- **Go to the policy that handled attack** – To do this, click the (Go to Policy) button.
- **Export the information in the in the Attack Details tab to a CSV file**–To do this, click the (CSV) button. Then, you can view the file or specify the location and file name.
- **For DNS recursive attacks, view the list of relevant whitelisted subdomains**–To do this, click the (View Subdomains Whitelist) button.
- **Export the** DoS Attack Details, page 339 **files related to the selected attack to a ZIP file**–

  To do this, click the (Export Attack Capture Files) button, and enter a file name in the file selection dialog box.

  Notes

  — You can send the CAP file to a packet analyzer.

  — Up to 255 bytes of packet information is saved in the CAP file. That is, Radware DefensePro DDoS Mitigation exports full packets but APSolute Vision trims them to 255 bytes.

  — The file is available only as long as it is displayed in the *Current Attacks* table.

- The file is created only if packet reporting is enabled in the protection configuration forthe profile that was violated.
- Radware DefensePro DDoS Mitigation exports only the last packet in a sequence that matches the filter. Furthermore, if traffic matches a signature that consists of more than one packet, the reported packet will not include the whole expression in the filter.
- For DoS attacks of very short duration, there might be no sampling or *ongoing* traps. Consequently, for such attacks, there might be no sampled data or capture files. (For more information, see DoS Attack Details, page 339.)

Anti-Scanning Details

Table 211: Anti-Scanning Attack Details: Characteristics Parameters

Parameter	Description
Source L4 Port	The source L4 port that the attack uses or used.
Protocol	The protocol that the attack uses or used.
Physical Port	The physical port that the attack uses or used.
Total Packet Count	The packet count that the attack uses or used.
VLAN Tag / Context	The Context Group that the attack uses or used.
MPLS RD	*N/A*
Device IP Address	The device IP address that the attack uses or used.
Avg. Time Between Probes	The average time, in seconds, between scan events.
Number of Probes	The number of scan events from the time the attack started.
Volume (Kbits)	The volume, in Kbits, that the attack uses or used.

Table 212: Anti-Scanning Attack Details: Info Parameters

Parameter	Description
Action	The protection Action taken.
Action Reason	Values: • Configuration–The action is (or was) according to the value in the **Action** field in the Anti-Scanningprofile. • Footprint-accuracy-level–There is (or was) insufficient data for a footprint, because the **Include in the Footprint More than Source IP Address and Protocol** option is enabled in the Anti-Scanningprofile. • Multiple-probed-ports–Port scans are (or were) *monitored* only (not blocked), because the **Monitor but Do Not Block Port Scans** option is enabled in the Anti- Scanning profile.
Blocking Duration	The blocking duration, in seconds, of the attacker source IP address.
Estimated Release Time (Local)	The estimated release time of attacker in local time.

Table 213: Anti-Scanning Attack Details: Scan Details Parameters

Parameter	Description
DST IP	The destination IP address of the scan.

Table 213: Anti-Scanning Attack Details: Scan Details Parameters (cont.)

Parameter	Description
DST L4 Port	The destination port of the scan.
TCP Flag / Protocol	Values: • *The TCP flag, for example, "ACK"*–Displayed for TCP scans. • UDP–Displayed for UDP scans. • ICMP–Displayed for ICMP scans.

Table 214: Anti-Scanning Attack Details: Footprint

Parameter	Description
The footprint-blocking rule generated by the Anti-Scanning protection, which provides the narrowest effective blocking rule against the scanning attack.	

Table 215: Anti-Scanning Attack Details: Attack Description

Parameter	Description
The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

BDoS Attack Details

Table 216: BDoS Attack Details: Characteristics Parameters

Parameter	Description
Note: Some fields can display multiple values, when relevant and available. The values that these field display depend on the current stage of the attack. If a field is part of the dynamic signature (that is, a specific value or values appear in all the attack traffic), the field displays the relevant value or values.	
Protocol	The protocol that the attack uses or used.
Source L4 Port	The source L4 port that the attack uses or used.
Physical Port	The physical port that the attack uses or used.
Packet Count	The packet count of the attack.
Volume (Kbits)	The volume, in Kbits, that the attack uses or used.
VLAN Tag / Context	The VLAN tag value or Context Group in the policy that handled the attack. **Note:** The VLAN tag or Context Group identifies similar information in this field. Radware DefensePro DDoS Mitigation 6.*x* and 7.*x* versions support VLAN tags. Radware DefensePro DDoS Mitigation 8.*x* versions support Context Groups.
MPLS RD	The MPLS RD that the attack uses or used.
Device IP	The device IP address that the attack uses or used.
TTL	The TTL that the attack uses or used.
L4 Checksum	The L4 checksum that the attack uses or used.
TCP Sequence Number	The TCP sequence number that the attack uses or used.

Table 216: BDoS Attack Details: Characteristics Parameters (cont.)

Parameter	Description
IP ID Number	The IP ID number that the attack uses or used.
Fragmentation Offset	The fragmentation offset that the attack uses or used.
Fragmentation Flag	The fragmentation flag that the attack uses or used. **0** indicates that fragmentation is allowed. **1** indicates that fragmentation is not allowed.
Flow Label	(IPv6 only) The flow label that the attack uses or used.
ToS	The ToS that the attack uses or used.
Packet Size	The packet size that the attack uses or used.
ICMP Message Type (This is displayed only if the protocol is ICMP.)	The ICMP message type that the attack uses or used.
Source IP	The source IP address that the attack uses or used.
Destination IP	The destination IP address that the attack uses or used.
Source Ports	The source ports that the attack uses or used.
Destination Ports	The destination port that the attack uses or used.
DNS ID	The DNS ID that the attack uses or used.
DNS Query	The DNS query that the attack uses or used.
DNS Query Count	The DNS query count that the attack uses or used.

Table 217: BDoS Attack Details: Info Parameters

Parameter	Description
Packet Size Anomaly Region	The statistical region of the attack packets. The formula for the packet-size baseline for a policy is as follows: {(AnomalyBandwidth/AnomalyPPS)/(NormalBandwidth/NormalPPS)} Values: • Large Packets–The attack packets are approximately 15% larger than the normal packet-size baseline for the policy. • Normal Packets–The attack packets are within approximately 15% either side of the normal packet-size baseline for the policy. • Small Packets–The attack packets are approximately 15% smaller than the normal packet-size baseline for the policy.

Table 217: BDoS Attack Details: Info Parameters (cont.)

Parameter	Description
State	The state of the protection process. Values: • footprint analysis–BDoS protection has detected an attack and is currently generating an attack footprint. • footprint-applied–BDoS protection is blocking the attack based on the generated footprint. Through a closed-feedback loop operation, BDoS protection optimizes the footprint rule, achieving the narrowest effective mitigation rule. • burst-footprint-blocking–BDoS protection is blocking the burst attack based on the footprint generated by the previous states. This state remains until the burst attack terminates or the specified **Maximum Burst-Attack Period** is reached. • footprint-is-overblocking–BDoS protection started blocking the attack but stopped three times after identifying an overblocking situation. This state remains for 10 minutes, after which, BDoS protection generates and implements a new footprint. • non-attack–Nothing was blocked because the traffic was not an attack. That is, no footprint was detected or the blocking strictness level was not met.

Table 218: BDoS Attack Details: Footprint Parameters

Parameter	Description
The footprint-blocking rule generated by the Behavioral DoS Protection, which provides the narrowest effective blocking rule against the flood attack.	

Table 219: BDoS Attack Details: Attack-Identification Statistics Table

Parameter	Description
This table displays attack traffic (Anomaly) and normal traffic information. Red indicates real-time values identified as suspicious in the 15 seconds prior to when the attack was triggered. Black indicates the learned normal traffic baselines. Table columns are displayed according to the protocols: TCP (includes all flags), UDP, or ICMP.	

Table 220: BDoS Attack Details: Attack-Identification Statistics Graph

Parameter	Description
The graph displays a snapshot of the relevant traffic type for the 15-second period during which the attack was triggered. For example, during a UDP flood, just UDP traffic is represented. The blue line represents the normal adapted traffic baseline.	

Table 221: BDoS Attack Details: Burst Attack Statistics

Parameter	Description
This tab displays data only when the value of the **State** parameter in the *Info* tab (see above) is **burst-footprint-blocking**. **Note:** For information on Burst-Attack Protection, see Table 94 - BDoS Profile: Burst-Attack Protection Settings Parameters, page 177.	
Burst Occurring Now	Values: Yes, No
Current Burst Number	The number of bursts since start of the attack.
Average Burst Duration	The average duration, in hh:mm:ssformat, of the bursts.
Average Time Between Bursts	The average time, in hh:mm:ssformat, between separate bursts.
Average Burst Rate	The average rate, in Kbps, of the bursts.
Max. Burst Rate	The rate, in Kbps, of the biggest burst in this attack.

Table 222: BDoS Attack Details: Attack Description

Parameter	Description
The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

DNS Flood Attack Details

The *Attack Details* tab includes the  (View Subdomains Whitelist) button. When the attack is a recursive attack, clicking the button opens a table with the subdomains that match the attack footprint but Radware DefensePro DDoS Mitigation identifies as legitimate.

Note: Radware DefensePro DDoS Mitigation can identify a subdomain as legitimate through automatic learning and by using manual entries in the Subdomains Whitelist. For more information, see Configuring DNS Flood Protection Profiles, page 187.

Table 223: DNS Flood Attack Details: Characteristics Parameters

Parameter	Description
Note: Some fields can display multiple values, when relevant and available. The values that these field display depend on the current stage of the attack. If a field is part of the dynamic signature (that is, a specific value or values appear in all the attack traffic), the field displays the relevant value or values.	
Protocol	The protocol that the attack uses or used.
Source L4 Port	The source L4 port that the attack uses or used.
Physical Port	The physical port that the attack uses or used.
Packet Count	The packet count of the attack.
Volume (Kbits)	The volume, in Kbits, that the attack uses or used.

Table 223: DNS Flood Attack Details: Characteristics Parameters (cont.)

Parameter	Description
VLAN Tag / Context	The VLAN tag value or Context Group in the policy that handled the attack. **Note:** The VLAN tag or Context Group identifies similar information in this field. Radware DefensePro DDoS Mitigation 6.*x* and 7.*x* versions support VLAN tags. Radware DefensePro DDoS Mitigation 8.*x* versions support Context Groups.
MPLS RD	The MPLS RD that the attack uses or used.
Device IP	The device IP address that the attack uses or used.
TTL	The TTL that the attack uses or used.
L4 Checksum	The L4 checksum that the attack uses or used.
IP ID Number	The IP ID number that the attack uses or used.
Packet Size	The packet size that the attack uses or used.
Destination IP	The destination IP address that the attack uses or used.
Destination Ports	The destination ports that the attack uses or used.
DNS ID	The DNS ID that the attack uses or used.
DNS Query	The DNS query that the attack uses or used.
DNS Query Count	The DNS query count that the attack uses or used.
DNS An Query Count	The DNS An query count that the attack uses or used.

Table 224: DNS Flood Attack Details: Info Parameters

Parameter	Description
State	The state of the protection process.
Mitigation Action	The mitigation action. Values: • Signature Challenge • Signature Rate Limit • Collective Challenge • Collective Rate Limit

Table 225: DNS Flood Attack: Footprint

Parameter	Description
The footprint-blocking rule that the Behavioral DoS Protection generated. The footprint-blocking rule provides the narrowest effective blocking rule against the flood attack.	

Table 226: DNS Flood Attack Details: Attack-Identification Statistics Table

Parameter	Description
This table displays attack traffic (Anomaly) and normal traffic information. Red indicates real-time values identified as suspicious in the 15 seconds prior to when the attack was triggered. Black indicates the learned normal traffic baselines. Table columns are displayed according to the DNS query types: A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV, Other.	

Table 227: DNS Flood Attack Details: Attack-Identification Statistics Graph

Parameter	Description
The graph displays a snapshot of the relevant traffic type for the 15-second period during which the attack was triggered. For example, during a UDP flood, just UDP traffic is represented. The blue line represents the normal adapted traffic baseline.	

Table 228: DNS Flood Attack Details: Attack Description

Parameter	Description
The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

DoS Attack Details

Note: For DoS attacks of very short duration, there might be no sampling or ongoing traps. Consequently, for such attacks, there might be no sampled data or capture files.

Table 229: DoS Attack Details: CharacteristicsParameters

Parameter	Description
Protocol	The protocol that the attack uses or used.
Physical Port	The physical port that the attack uses or used.
Packet Count	The packet count of the attack.
VLAN Tag / Context	The VLAN tag value or Context Group in the policy that handled the attack. **Note:** The VLAN tag or Context Group identifies similar information in this field. Radware DefensePro DDoS Mitigation 6.*x* and 7.*x* versions support VLAN tags. Radware DefensePro DDoS Mitigation 8.*x* versions support Context Groups.
MPLS RD	The MPLS RD that the attack uses or used.
Device IP	The device IP address that the attack uses or used.

Table 230: DoS Attack Details: Info Parameters

Parameter	Description
Action	The Action that the protection took for the attack traffic, for example: **Drop**.
Attacker IP	The IP address of the attacker.
Protected Host	The protected host.
Protected Port	The protected port.
Attack Duration	The duration of the attack.
Current Packet Rate	The current packet rate.
Average Packet Rate	The average packet rate.

Table 231: DoS Attack Details: Attack Description

Parameter	Description
The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

Intrusions Attack Details

Table 232: Intrusions Attack Details: CharacteristicsParameters

Parameter	Description
Protocol	The protocol that the attack uses or used.
Physical Port[1]	The physical port that the attack uses or used.
Packet Count	The packet count of the attack.
Volume (Kbits)	The volume, in Kbits, that the attack uses or used.
VLAN[1]	The VLAN that the attack uses or used.
MPLS RD[1]	The MPLS RD that the attack uses or used.
Device IP	The device IP address that the attack uses or used.

1 – This parameter is not resolved, and the value **Multiple** is alwaysdisplayed.

Table 233: Intrusions Attack Details: Attack Description

Parameter	Description
The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

Packet Anomalies Attack Details

Table 234: Packet Anomalies Attack Details: Characteristics Parameters

Parameter	Description
Protocol	The protocol that the attack uses or used.
Physical Port[1]	The physical port that the attack uses or used.
Packet Count	The packet count of the attack.
VLAN Tag / Context	The VLAN tag value or Context Group in the policy that handled the attack. **Note:** The VLAN tag or Context Group identifies similar information in this field. Radware DefensePro DDoS Mitigation 6.*x* and 7.*x* versions support VLAN tags. Radware DefensePro DDoS Mitigation 8.*x* versions support Context Groups.
MPLS RD	The MPLS RD that the attack uses or used.
Device IP	The device IP address that the attack uses or used.
Attack Description The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

1 – This parameter is not resolved, and the value **Multiple** is always displayed.

Table 235: Packet Anomalies Attack Details: Attack Description

Parameter	Description
The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

SYN Flood Attack Details

Table 236: SYN Flood Attack Details: Characteristics Parameters

Parameter	Description
Protocol	The protocol that the attack uses or used.
Physical Port	The physical port that the attack uses or used. If the configuration of the Protection policy includes no value for **Port Group**, the field displays **Multiple**.
Packet Count	The packet count of the attack.
Volume (Kbits)	The volume, in Kbits, that the attack uses or used.
VLAN Tag / Context	The VLAN tag value or Context Group in the policy that handled the attack. **Note:** The VLAN tag or Context Group identifies similar information in this field. Radware DefensePro DDoS Mitigation 6.*x* and 7.*x* versions support VLAN tags. Radware DefensePro DDoS Mitigation 8.*x* versions support Context Groups.
MPLS RD	The MPLS RD that the attack uses or used.

Table 237: SYN Flood Attack Details: Info Parameters

Parameter	Description
The information is displayed when the protection action is blocking mode. **Caution:** If SYN Flood Protection is configured with report-only mode, the fields **Average Attack Rate**, **Attack Threshold**, and **Attack Volume** display **0** (zero).	
Average Attack Rate	The average rate of spoofed SYNs and data connection attempts per second, calculated every 10 seconds.
Attack Threshold	The configured attack trigger threshold, in half connections per second.
Attack Volume	The number of packets from spoofed TCP connections during the attack life cycle (aggregated). These packets are from the sessions that were established through the SYN-cookies mechanism or were passed through the SYN Flood Protection trusted list.
Attack Duration	The duration, in hh:mm:ssformat, of the attack on the protected port.
TCP Challenge	The *Authentication Method* that identified the attack: *Transparent Proxy* or *Safe-Reset*.
HTTP Challenge	The *HTTP Authentication Method* that identified the attack: *302-Redirect* or *JavaScript*.

Table 238: SYN Flood Attack Details: Authentication Lists Utilization Parameters

Parameter	Description
TCP Auth. List	The current utilization, in percent, of the TCP Authentication table.
HTTP Auth. List	The current utilization, in percent, of the HTTP Authentication table.

Table 239: SYN Flood Attack Details: Attack Description

Parameter	Description
The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.	

Traffic Filters Attack Details

Note: For information on Traffic Filters, see Configuring Traffic Filters Profiles, page 242.

Table 240: Traffic Filters Attack Details: Characteristics Parameters

Parameter	Description
Filter Name	The name of the Traffic Filter that matched the traffic.
Filter ID	The *Radware ID* of the Traffic Filter that matched the traffic. **Note:** The ID is a hyperlink to the configuration of the Traffic Filter.
Protocol	The protocol of the traffic that the Traffic Filter matched.
Source Network	The source network of the traffic that the Traffic Filter matched.
Source Port	The source port of the traffic that the Traffic Filter matched.
Destination Network	The destination network of the traffic that the Traffic Filter matched.
Destination Port	The destination port of the traffic that the Traffic Filter matched.
Device IP	The IP address of the Radware DefensePro DDoS Mitigation device with the Traffic Filter that matched the traffic.

Table 241: Traffic Filters Attack Details: Info Parameters

Parameter	Description
Total Attack Packets	The total number of packets that match or matched the Traffic Filter.
Attack Packets Rate (pps)	The rate, in packets/second, of packets that match or matched the Traffic Filter.
Total Attack Data (Kbits)	The total volume, in Kbits, of traffic that matches or matched the Traffic Filter.
Attack Bandwidth (Kbps)	The bandwidth, in Kbits/second, of traffic that matches or matched the Traffic Filter.

Table 242: Traffic Filters Attack Details: Attack Description

Parameter	Description
	The description of the attack from the Attack Descriptions file, if it is uploaded on the APSolute Vision server.

Sampled Data Tab

You can display the *Sampled Data* dialog box for the all attack types that support sampled data.

The *Sampled Data* tab contains a table with data on sampled attack packets. Each row in the table displays the data for one sampled attack packet. The title bar includes the category of the data–for example, *Behavioral DoS*.

Note: APSolute Vision stores sampled attack data, which includes the source and destination addresses of the sampled packets. This information reflects a sampling of the attack packets; it does not reflect the full attack data. For example, it is possible that the source IP addresses of the sampled data do not include all of the source addresses of the attack.

The table in the *Sampled Data* tab comprises the following columns:

- Time
- Source Address
- Source L4 Port
- Destination Address
- Destination L4 Port
- Protocol
- VLAN / Context
- MPLS RD
- Physical Port

To display the Sampled Data tab

1. In the *Security Monitoring* perspective, select the Radware DefensePro DDoS Mitigationdevice, Site, or Logical Group for which to display data.
2. Select **Dashboard View**.
3. Do one of the following to open the *Attack Details* tab:
   - Select **Current Attacks Table**, and then, double-click the relevant row.
   - Select **Ongoing Attacks Monitor**, and then, double-click the icon.
4. Click the  (View Sampled Data) button.

You can export some rows of the table in the *Sampled Data* dialog box to a CSV file.

To save sampled data to a CSV file

1. In the *Security Monitoring* perspective, select the Radware DefensePro DDoS Mitigationdevice, Site, or Logical Group for which to display data.

2. Select **Dashboard View**.

3. Do one of the following to open the *Attack Details* tab:
   - Select **Current Attacks Table**, and then, double-click the relevant row.
   - Select **Ongoing Attacks Monitor**, and then, double-click the icon.
4. Click the  (View Sampled Data) button.
5. Select the row with which you want the data rows in the file to start.
6. Click the  (CSV) button.
7. View the file or specify the location and file name.

Viewing Real-Time Traffic Reports

You can view real-time traffic reports over time for the IP traffic passing through the Radware DefensePro DDoS Mitigation devices. The information includes data on overall IP traffic, protocol mix, and packet discards. You can display the data in graph or table format. The traffic is calculated according to the port pair. When you are viewing multiple Radware DefensePro DDoS Mitigation devices in the *Security Monitoring* perspective, the table displays both port pairs and the selected ports as appropriate.

You can also view graphs of connection rates and concurrent connections based on data from the Session table.

By default, all traffic is presented in these graphs and tables. In each graph, you can filter the display by protocol or traffic direction, but not for concurrent connections.

You can monitor the following traffic information in the *Traffic Monitoring* tab:

- Viewing the Traffic Utilization Report, page 344
- Viewing the Connection Rate Report, page 348
- Viewing the Concurrent Connections Report, page 350
- Viewing the Top Queried Domain Names Report, page 351

Viewing the Traffic Utilization Report

The Traffic Utilization Report displays statistics for the following:

- **Traffic Statistics**–Displays information for the selected port pairs as a graph. The graph contains information for a selected protocol or the total for all protocols over a period oftime.

  There is a curve on the graph for each the following:
  - Inbound IP traffic
  - Outbound IP traffic
  - Discarded inbound traffic
  - Discarded outbound traffic
  - Excluded inbound traffic
  - Excluded outbound traffic

  To hide or show a curve for a particular traffic type, click the corresponding colored square in the legend.
- **Traffic Authentication Statistics (Challenge/Response)** –Displays statistics for the Challenge-Response mechanism when the relevant option is enabled in the protection modules that support the Challenge-Response mechanism. For more information, see Configuring Global DNS Flood Protection, page 124.

- **Last Sample Statistics**–Displays the last reading for each protocol and provides totals for all protocols, for a single device. (This information is only available when viewing a single device.)

  To view or save a CSV file, click (CSV).

  Caution: When the **Scope** is **Devices/Policies**, the *Last Sample Statistics* table displays Outbound statistics only when the **Direction** of the Protection policy is **Two Way**.

Tip: To get the current traffic rate in packets or bytes per second (calculated as the average rate in 15 seconds), you can use the following CLI command on the Radware DefensePro DDoS Mitigation device:
dp rtm-stats get [port number]

Caution: When the **Scope** is **Devices/Policies**, the Traffic Utilization Report does not include inbound traffic that the Black List module blocked. This is because the Black List module processes traffic before the classification of a Protection policy.

Notes

- For packets received through the 1G, 10G, or 40G ports, packet-size information andcounters do not account for the CRC.
- The *Traffic Utilization Report* and the statistical traffic information that *Protection Monitoring* provides are based on different counters. (For information on the *statistical trafficinformation that Protection Monitoring provides*, see Protection Monitoring, page 353.)

To view the Traffic Utilization Report

1. In the *Security Monitoring* perspective, select the RadwareDefensePro DDoS Mitigation device, Site, or Logical Group for which to display data.
2. Select **Traffic Monitoring > Traffic Utilization Report**.
3. Change display settings for the graph and table, as required.
4. For the *Statistics Graph* and *Last Sample Statistics*, set filter options for the displayedtraffic data, as required. The displayed information refreshes automatically.

Table 243: Traffic Utilization Report: Display Parameters for Graph and Table

Parameter	Description
Scope (link, which displays the table)	The Protection policies that the Traffic Utilization Report displays. By default, the Scope is **Any Port** or **Any Policy** (depending on the specified value in the **Scope** drop-down list). That is, by default, the Traffic Utilization Report displays all the information. To control the scope of the information that the report shows, see the procedure To control the scope of the information that the report shows, page 346.

Table 243: Traffic Utilization Report: Display Parameters for Graph and Table (cont.)

Parameter	Description
Display Last	How long the graph displays attacks after the attack terminates. That is, the graph displays all attacks that are currently ongoing or that terminated within the selected period. Values: • 10 Minutes • 20 Minutes • 30 Minutes • 1 Hour Default: 10 Minutes
Scope (drop-down list)	The scope of the graph view. Values: • Devices/Physical Ports–The graph shows traffic according tophysical ports on the specified device. • Devices/Policies–The graph shows traffic according to Protection policies on the specified device. Default: Devices/Physical Ports
Units	The units for the traffic rate. Values: • Kbps–Kilobits per second • Packet/Sec–Packets per second

To control the scope of the information that the report shows

1. Click Scope. A table opens. The table has either the *Device Name* and *Port* columns or the *Device Name* and *Policy columns*–according to the specified value in the **Scope** drop-down list: **Devices/Physical Ports** or **Devices/Policies**.
2. Do one of the following:
   - To limit the physical ports or Protection policies that the report displays, select the corresponding checkboxes.
   - To display the information for all the currently relevant physical ports or Protection policies, click in the top-left table cell, and then, select **Select All**.
   - To display all the information in the database, even information that is not associated with a specific port or specific Protection policy, click in the top-left table cell, and then, select **Select None**.

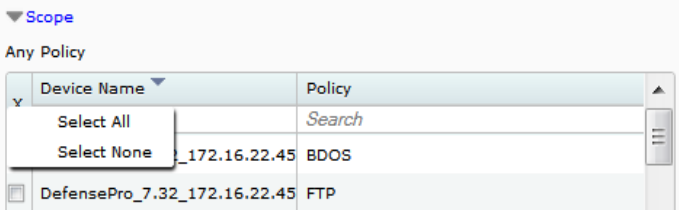


Table 244: Traffic Utilization Report: Filter Parameters for the Traffic Statistics Graph

Parameter	Description
Direction	The traffic that the graph shows. Values: • Inbound–Show inbound traffic. • Outbound–Show outbound traffic. • Both–Show inbound and outbound traffic. Data for inbound and outbound are displayed as separate lines, not as totals. **Note:** The direction of traffic between a pair of ports is defined by the **In Port** setting in the port pair configuration.
Protocol	The traffic protocol to display. Values: • TCP–Show the statistics of the TCP traffic. • UDP–Show the statistics of the UDP traffic. • ICMP–Show the statistics of the ICMP traffic. • IGMP–Show the statistics of the IGMP traffic. • SCTP–Show the statistics of the SCTP traffic. • Other–Show the statistics of the traffic that is not TCP, UDP, ICMP, IGMP, or SCTP. • All–Show total traffic statistics. **Caution:** When the **Scope** is **Devices/Policies**, the *Other* traffic does not include IPsec traffic.

Table 245: Traffic Utilization Report: Traffic Authentication Statistics (Challenge/Response) Parameters

Parameter	Description
Protocol	The protocol of the statistics displayed in the row. Values: HTTP, TCP, DNS
Current Attacks	The number of attacks currently in the device.
Authentication Table Utilization %	The percentage of the Authentication Table that is full.
Challenges Rate	The rate, in PPS, that the device is sending challenges.

Table 246: Traffic Utilization Report: Last Sample Statistics Parameters

Parameter	Description
Protocol	The traffic protocol. Values: • TCP • UDP • ICMP • IGMP • SCTP • Other–The statistics of the traffic that is not TCP, UDP, ICMP, IGMP, or SCTP. • All–Total traffic statistics. **Caution:** When the **Scope** is **Devices/Policies**, the *Other* traffic does not include IPsec traffic.
Inbound	The amount of inbound traffic for the protocol identified in the row.
Outbound	The amount of outbound traffic for the protocol identified in the row.
Discarded Inbound	The amount of discarded inbound traffic for the protocol identified in the row.
Discarded Outbound	The amount of discarded outbound traffic for the protocol identified in the row.
Discard %	The percentage of discarded traffic for the protocol identified in the row.
Excluded Inbound	The amount of excluded inbound traffic for the protocol identified in the row.
Excluded Outbound	The amount of excluded outbound traffic for the protocol identified in the row.

Viewing the Connection Rate Report

The Connection Rate Report displays a graph showing connection rate statistics of inbound and outbound traffic.

To view the Connection Rate Report

1. In the *Security Monitoring* perspective, select the Radware DefensePro DDoS Mitigationdevice, Site, or Logical Group for which to display data.
2. Select **Traffic Monitoring > Connections Rate Report**.
3. Change display settings for the graph, as required.

Table 247: Connection Rate Report: Display Parameters

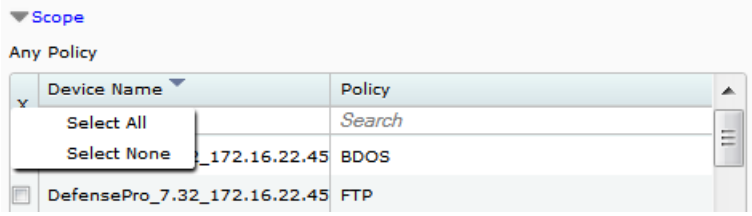
Parameter	Description
Scope (link, which displays the table)	The physical ports and the Protection policies that the ConnectionRate Report shows. By default, the Scope is **Any Port** or **Any Policy** (depending on the specified value in the **Scope** drop-down list). That is, by default,the Connection Rate Report displays all the information. To control the scope of the information that the report shows, see the procedure To control the scope of the information that the report shows, page 350.
Display Last	How long the graph displays attacks after the attack terminates. That is, the graph displays all attacks that are currently ongoing or that terminated within the selected period. Values: • 10 Minutes • 20 Minutes • 30 Minutes • 1 Hour Default: 10 Minutes
Scope (link, which displays the table)	The scope of the graph view. Values: • Devices/Physical Ports–The graph shows traffic according tophysical ports on the specified device. • Devices/Network Policies–The graph shows traffic according to Protection policies on the specified device. Default: Devices/Physical Ports **Caution:** In this version of Radware DefensePro DDoS Mitigation, the Connection Rate Report works *only* when the **Scope** is **Devices/ Network Policies**.
Direction	Values: • Both–Show both inbound traffic and outbound traffic. Data forinbound and outbound are displayed as separate lines, not as totals. • Inbound–Show only inbound traffic. • Outbound–Show only outbound traffic. **Note:** The direction of traffic between a pair of ports is defined by the **In Port** setting in the port pair configuration.
Protocol	The traffic protocol to display. When you select **All**, total traffic statistics are displayed.
Select Port Pair (button) (This button is displayed only when the **Scope** is **Devices/Physical Ports**.)	Opens the *Select Port Pairs* dialog box. Select the port pairs relevant for the network topology by moving the required port pairs to the *Selected Port Pairs* list. All other port pairs should be in the *Available Port Pairs* list. **Note:** You can select port pairs for each direction; however, Cisco recommends that you select a port pair in one direction only, and display traffic for both directions, if required. If you select port pairs in both directions, and traffic for both directions, the graph will display the same traffic twice.

Table 247: Connection Rate Report: Display Parameters (cont.)

Parameter	Description
Select Policies (This button is displayed only when the **Scope** is **Devices/Policies**.)	Opens the *Select Policies* dialog box. Select the Protection policies relevant for the network topology by moving the required policies the *Selected Policies* list.

To control the scope of the information that the report shows

1. Click Scope. A table opens. The table has either the *Device Name* and *Port* columns or the *Device Name* and *Policy columns*—according to the specified value in the **Scope** drop-down list: **Devices/Physical Ports** or **Devices/Policies**.
2. Do one of the following:
   - To limit the physical ports or Protection policies that the report displays, select the corresponding checkboxes.
   - To display the information for all the currently relevant physical ports or Protection policies, click in the top-left table cell, and then, select **Select All**.
   - To display all the information in the database, even information that is not associated with a specific port or specific Protection policy, click in the top-left table cell, and then, select **Select None**.



Viewing the Concurrent Connections Report

The Concurrent Connections Report displays a graph showing the rate of current connections for selected port pairs. You can display the information for a selected protocol or the total for all protocols over the last 10, 20, 30, or 60 minutes.

Note: For packets received through the 1G, 10G, or 40G ports, packet-size information and counters do not account for the CRC.

To view the Concurrent Connections Report

1. In the *Security Monitoring* perspective, select the device, Site, or Logical Group for which to display data.
2. Select **Traffic Monitoring > Concurrent Connections Report**.
3. Change display settings for the graph, as required.

Table 248: Concurrent Connections Report: Display Parameters

Parameter	Description
Display Last	How long the graph displays attacks after the attack terminates. That is, the graph displays all attacks that are currently ongoing or that terminated within the selected period. Values: • 10 Minutes • 20 Minutes • 30 Minutes • 1 Hour Default: 10 Minutes
Protocol	The traffic protocol to display. When you select **All**, total traffic statistics are displayed.

Viewing the Top Queried Domain Names Report

This feature is available only when viewing a single device.

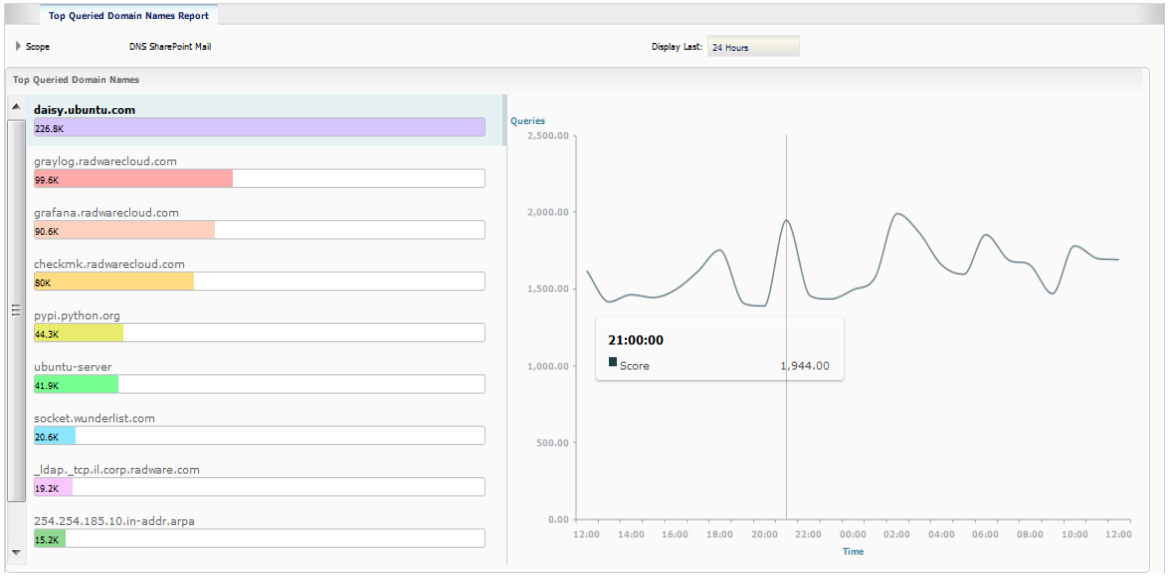
Note: For more information, see Configuring DNS Flood Protection Profiles, page 187.

Every 10 minutes, Radware DefensePro DDoS Mitigation sends APSolute Vision data about *sampled* DNS packets, and APSolute Vision recalculates the values and the display of the *Top Queried Domain Names Report*.

The *Top Queried Domain Names Report* shows the following:

- **The 10 most-queried DNS domain names under the specified Protection policy**—The list is in descending order; that is, the most-queried domain name is at the top of the list.
- **A colored bar beneath each domain name**—The width of the colored bar represents the ranking of the domain name. The most-queried domain name is at the top of the list and the colored bar always fills the box. The sequence of the *colors* of the bars is static; that is, the actual colors have no significance. Inside each colored bar, a number displays the approximate total number of queries from the samples, for the specified period (according to the selected **Display Last** option). The displayed value is based on a sampling of up to 1000 DNS queries per second.
- **A line graph for a selected domain**—The graph shows the number of queries—and trend— for the specified period (according to the selected **Display Last** option). Hovering the cursor (pointer) on the line opens a popup that shows the sample time (hh:mm:ss) and a **Score** with the number of queries for that domain name, for that sample.

Figure 41: Top Queried Domain Names Report



To view the Top Queried Domain Names Report

1. In the *Security Monitoring* perspective, select the device for which to display data.
2. Select **Traffic Monitoring > Top Queried Domain Names Report**.
3. Change display settings, as required.

Table 249: Top Queried Domain Names Report: Display Parameters

Parameter	Description
Scope (drop-down list)	The Protection policy whose 10 most-queried DNS domain names the tab displays.
Display Last	Determines the following: • The period for the calculation of the 10 most-queried DNS domain names (the bar graphs and the displayed values) • The time range of the x-axis in the line graph (for a selected domain) Values: • 10 Minutes • 1 Hour • 12 Hours • 24 Hour Default: 10 Minutes

Protection Monitoring

Protection Monitoring provides the real-time traffic monitoring per network policy, either for the network as a whole–if BDoS Protection is configured, or for DNS traffic–if DNS Flood Protection is configured. The statistical traffic information that Protection Monitoring provides can help you better understand the traffic that flows through the protected network, how the configured protection is working, and, most importantly, how anomalous traffic is detected.

For information about displaying protection information for a selected device, see the following:

- Displaying Attack Status Information, page 353
- Monitoring the Traffic Under BDoS Protection, page 354
- Monitoring the Traffic Under DNS Flood Protection, page 356

Note: The statistical traffic information that *Protection Monitoring* provides and *Traffic Utilization Report* are based on different counters. (For information on the *Traffic Utilization Report*, see Viewing the Traffic Utilization Report, page 344.)

Displaying Attack Status Information

You can display summary status information for attacks for each configured and enabled protection policy. When there is an attack that violates a Protection policy, the table displays an icon indicating the status of the attack in the corresponding row for the relevant attack traffic.

To display attack status information

1. In the *Security Monitoring* perspective, select the Radware DefensePro DDoS Mitigationdevice to monitor.
2. Select **Protection Monitoring > Attack StatusReport**. The

   table comprises the following columns:

   - Policy Name
   - IPv4-TCP
   - IPv4-UDP
   - IPv4-ICMP
   - IPv4-DNS
   - IPv6-TCP
   - IPv6-UDP
   - IPv6-ICMP
   - IPv6-DNS
3. When an attack icon is displayed in the table, click the icon to display the corresponding attack traffic information.

Monitoring the Traffic Under BDoS Protection

You can monitor the traffic for a Protection policy that includes BDoS protection. Traffic information is displayed in the following tabs:

- BDoS Traffic Statistics, page 355
- Last Sample Statistics, page 356

Caution: When traffic matches multiple Protection policies with Out-of-State protection, the value that APSolute Vision displays for the total dropped traffic represents the sum of all dropped traffic for all relevant Protection policies. This is because when traffic matches multiple Protection policies with Out-of-State protection, all those Protection policies count the same dropped traffic.

Note: APSolute Vision displays the Protection Monitoring graphs using averaged values, and therefore, points on the curves might diverge from the exact values.

To display traffic information for a Protection policy that includes BDoS protection

1. In the *Security Monitoring* perspective, select the device to monitor.
2. Select **Protection Monitoring > BDoS Traffic MonitoringReports**.
3. Configure the general parameters for the display of the *BDoS TrafficStatistics* graph and *Last Sample Statistics* table.

Table 250: BDoS Traffic Monitoring Reports: General Parameters

Parameter	Description
Scope	The Protection policy. The list only displays policies that are configured with a BDoS profile.
Display Last	How long the graph displays attacks after the attack terminates. That is, the graph displays all attacks that are currently ongoing or that terminated within the selected period. Values: • 10 Minutes • 20 Minutes • 30 Minutes • 1 Hour Default: 10 Minutes
Direction	The direction of the traffic that the *Statistics Graph* and *Last Sample Statistics* table display. Values: Inbound, Outbound
Units	The unit according to which the *Statistics Graph* and *Last Sample Statistics* table display the traffic. Values: • Kbps–Kilobits per second • Packets/Sec–Packets per second

BDoS Traffic Statistics

The graph displays the traffic rates for the selected Protection policy according to the specified parameters.

Table 251: BDoS Traffic Statistics Parameters

Parameter	Description
IP Version	The IP version of the traffic that the graph displays. Values: IPv4, IPv6
Protection Type	The protection type to monitor. Values: • TCP ACK FIN • TCP FRAG • TCP RST • TCP SYN • TCP SYN ACK • UDP • UDP FRAG • ICMP • IGMP
Scale	The scale for the presentation of the information along the Y-axis. Values: Linear, Logarithmic
Attack Status	(Read-only) The status of the attack.

Table 252: Statistics Graph Legend

Line	Description
Total Traffic (dark blue)	The total traffic that the device sees for the specific protection type and direction.
Legitimate Traffic (light blue)	The actual forwarded traffic rate, after Radware DefensePro DDoS Mitigation managed to block the attack. When there is no attack, the Total Traffic and Legitimate Traffic are equal.
Normal Edge (dashed green)	The statistically calculated baseline traffic rate.
Suspected Edge (dashed orange)	The traffic rate that indicates a change in traffic that might be an attack. **Caution:** Radware DefensePro DDoS Mitigation reports the Suspected Edge in Kbps only. The graph displays the Suspected Edge only when the Scope parameter **Units** is **Kbps** (see Table 254 - DNS Traffic Monitoring Reports: General Parameters, page 357). When the Scope parameter **Units** is **Packets/Sec**, the graph does not display the Suspected Edge.

Table 252: Statistics Graph Legend (cont.)

Line	Description
Attack Edge (dashed red)	The traffic rate that indicates an attack. **Caution:** Radware DefensePro DDoS Mitigation reports the Attack Edge in Kbps only. The graph displays the Attack Edge only when the Scope parameter **Units** is **Kbps** (see Table 254 - DNS Traffic Monitoring Reports: General Parameters, page 357). When the Scope parameter **Units** is **Packets/Sec**, the graph does not display the Attack Edge.

Last Sample Statistics

Use the *Last Sample Statistics* table to view information about last relevant sample.

Table 253: Last Sample Statistics Parameters

Parameter	Description
Traffic Type	The protection type. Each specific traffic type and direction has a baseline that the device learns automatically.
Baseline	The normal traffic rate expected by the device.
Total Traffic	The total traffic rate that the Radware DefensePro DDoS Mitigation device sees for the specific traffic type and direction.
Baseline Portion %	An indication for the rate invariant baseline–that is, the normal percentage of the specific traffic type to all other traffic in the same direction.
RT Portion %	The actual percentage of the specific traffic type relative to all other traffic in the same direction.
Legitimate Traffic	The actual forwarded traffic rate, after the device blocked the attack. When there is no attack, the RT Rate and Legitimate Rate are equal.
Legitimate Portion %	The actual percentage of the forwarded traffic rate of the specified type relative to other types of traffic, after the device blocked the attack.
Degree of Attack	A numeric value that evaluates the current level of attack. A value of 8 or greater signifies an attack.

Monitoring the Traffic Under DNS Flood Protection

You can monitor the traffic for a Protection policy that includes DNS Flood Protection.

APSolute Vision displays traffic information in the following tabs:

- DNS Traffic Statistics, page 357
- Last Sample Statistics, page 358

Note: APSolute Vision displays the Protection Monitoring graphs using averaged values, and therefore, points on the curves might diverge from the exact values.

To display traffic information for a Protection policy that includes DNS Flood Protection

1. In the *Security Monitoring* perspective, select the device to monitor.
2. Select **Protection Monitoring > DNS Traffic Monitoring Reports**.

3. Configure the general parameters for the display of the *Statistics Graph* and *LastSample Statistics* table.

Table 254: DNS Traffic Monitoring Reports: General Parameters

Parameter	Description
Scope	The Protection policy. The list only displays rules configured with a DNS profile.
Direction	(Read-only) The direction of the traffic that the *Statistics Graph* and *Last Sample Statistics* table display. Value: Inbound
Units	(Read-only) The unit according to which the *Statistics Graph* and *Last Sample Statistics* table display the traffic. Value: QPS–Queries per second

DNS Traffic Statistics

The graph displays the traffic rates for the selected Protection policy according to the specified parameters.

Table 255: DNS Traffic Statistics Graph Parameters

Parameter	Description
IP Version	The IP version of the traffic that the graph displays. Values: IPv4, IPv6
Protection Type	The DNS query type to monitor. Values: • Other • Text • A • AAAA • MX • NAPTR • PTR • SOA • SRV
Scale	The scale for the presentation of the information along the Y-axis. Values: Linear, Logarithmic
Attack Status	(Read-only) The status of the attack.

Table 256: Statistics Graph Legend

Line	Description
Total Traffic (dark blue)	The total traffic that the device sees for the specific protection type and direction.

Table 256: Statistics Graph Legend (cont.)

Line	Description
Legitimate Traffic (light blue)	The actual forwarded traffic rate, after Radware DefensePro DDoS Mitigation managed to block the attack. When there is no attack, the Total Traffic and Legitimate Traffic are equal.
Normal Edge[1] (dashed green)	The statistically calculated baseline traffic rate.
Suspected Edge[1] (dashed orange)	The traffic rate that indicates a change in traffic that might be an attack.
Attack Edge[1] (dashed red)	The traffic rate that indicates an attack.

1 – This line is not displayed if the protection is configured to use a footprint bypass or manual triggers.

Last Sample Statistics

Use the *Last Sample Statistics* tab to view information about the last relevant sample of DNS query statistics.

The *Last Sample Statistics* tab is divided into panels for each of the DNS query types.

Note: For more information, see Configuring DNS Flood Protection Profiles, page 187.

Figure 42: DNS Last Sample Statistics–Example Showing the "A" Panel

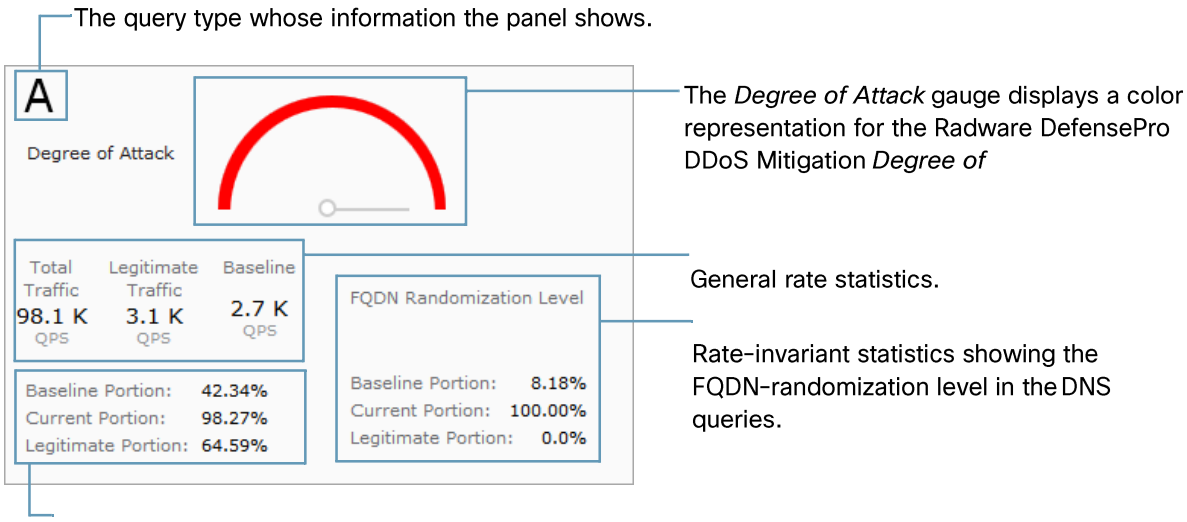


Table 257: Last Sample Statistics Parameters

Parameter	Description
Query Type	The DNS query type. Values: • A • AAAA • MX • NAPTR • Other • PTR • SOA • SRV • Text
Degree of Attack (gauge)	A gauge with a color representation of the Radware DefensePro DDoS Mitigation *Degree of Attack* (DoA) value for the specific query type. Green represents the *Normal* status. Orange represents the *Suspect* status. Red represents the *Attack* status.
General rate statistics	
Total Traffic	The total rate of traffic, in QPS, that the Radware DefensePro DDoS Mitigation device sees for the specific query type.
Legitimate Traffic	The actual forwarded traffic rate, in QPS, for the specific query type, after the device blocked the attack. **Note:** When there is no attack, the **Total Traffic** and **Legitimate Traffic** values are equal.
Baseline	The normal rate of traffic, in QPS, expected by the Radware DefensePro DDoS Mitigation device for the specific query type. Each query type has a baseline that the device learns automatically.
Rate-invariant statistics–query-type distribution (on the left side of the panel)	
Baseline Portion %	An indication of the rate-invariant baseline—that is, the normal percentage of the specific query type out of all other DNS traffic in the same direction.
Current Portion %	The actual percentage of the specific traffic type relative to all other DNS traffic in the same direction.
Legitimate Portion %	The actual percentage of the forwarded traffic rate of the specified query type relative to other types of queries, after the device blocked the attack.
Rate-invariant statistics–FQDN Randomization Level (on the right side of the panel)	
Baseline Portion %	An indication of the FQDN Randomization Level baseline—that is, the normal randomness level, in percent, of FQDNs i the DNS queries of the specific query type.
Current Portion %	The actual percentage, representing the FQDN Randomization Level within the DNS queries of the specific query type.
Legitimate Portion %	The actual FQDN Randomization Level, in the forwarded traffic after the device blocked the attack.

HTTP Reports

This feature is not functional in Radware DefensePro DDoS Mitigation.

You can monitor real-time and historical (normal baseline) values, and analyze HTTP traffic anomalies using the following reports:

- Monitoring Continuous Learning Statistics, page 360
- Monitoring Hour-Specific Learning Statistics, page 360
- HTTP Request Size Distribution, page 360

Monitoring Continuous Learning Statistics

This feature is not functional in Radware DefensePro DDoS Mitigation.

Monitoring Hour-Specific Learning Statistics

This feature is not functional in Radware DefensePro DDoS Mitigation.

HTTP Request Size Distribution

This feature is not functional in Radware DefensePro DDoS Mitigation.

Alerts for New Security Attacks

APSolute Vision triggers an alert when a new attack is displayed in the *Current Attacks* table (which is part of the *Security Monitoring* perspective).

The value in the *Module* column in the *Alerts* pane is *Security Reporting*.

Each Radware DefensePro DDoS Mitigation device triggers separate security alerts.

The security alerts are either for a single security event (that is, a single attack event) or aggregated from multiple security events. The format is similar for alerts for single attacks and multiple attacks.

Table 258: Information in Security Alerts

String in a Security Alert for a Single Attack	String in a Security Alert Aggregated Attack Information
An attack of type: <attack category>[1] started.	<number of attacks> attacks of type: <attack category>[1] started between <start time of first attack> and <start time of last attack>.[2]
Detected by rule: <Protection policy>;	Detected by rule: <Protection policy>;[3]
Attack name: <attack name>;	Attack name: <attack name>;[3]
Source IP: <attacker IP address>;	Source IP: <attacker IP address>;[4]
Destination IP: <attacked IP address>;	Destination IP: <attacked IP address>;[4]
Destination port: <attacked port>;	Destination port: <attacked port>;[4]
Action: <action>.	Action: <action>.[4]

1 – For more information, see *Attack Category* in Table 210 - Current Attacks Table Parameters, page 328.

2 – Times are in the format dd.MM.yy hh:mm.
3 – When there are differences in the field values for the attacks, the values arecomma-separated.
4 – When there are differences in the field values for the attacks, the value is **multiple**. The value **multiple** may also refer to cases when Radware DefensePro DDoS Mitigation cannot report a specific value.

An APSolute Vision administrator can limit the parameters that are included in security alerts. This is option useful, because security alerts, which are often received by e-mail, are often viewed on a smartphone. To compensate for the small screen size, an administrator can select parameters to include in the alerts.

To select parameters to include in security alerts

1. In the *APSolute Vision Settings* view *System* perspective, select **General Settings >Alert Browser > Security Alerts**.
2. Select the check box next to each parameter you want to include in the alerts. By default, all the checkboxes are selected.

   You can choose any combination of the following parameters:

   - Policy Name
   - Attack Name
   - Source IP Address
   - Destination IP Address
   - Destination Port
   - Action
3. Click **Submit**.

   Note: Changes to the settings take effect on alerts generated from the time of the change and forward.

CHAPTER 13 - ADMINISTERING RADWARE DEFENSEPRO DDOS MITIGATION

This chapter describes administering Radware DefensePro DDoS Mitigation and contains the following sections:

- Command Line Interface, page 363
- Web Services, page 366
- API Structure, page 366
- APSolute API Software Development Kit (SDK), page 367

Command Line Interface

Access to the Command Line Interface (CLI) requires a serial-cable connection and a terminal emulation application.

Radware DefensePro DDoS Mitigation supports up to five simultaneous Telnet or SSH sessions.

Caution: In production environments, Radware recommends disabling CLI traps. In production environments, you can view all traps using APSolute Vision.

Note: When troubleshooting is required, Radware DefensePro DDoS Mitigation can generate a text file that includes the output of various CLI commands, such as printouts of the *Client* table, *ARP* table, and so on. You can download this file using APSolute Vision and send it to Technical Support (see Downloading a Device-Configuration File, page 281).

Table 259: Radware DefensePro DDoS Mitigation CLI Commands and Menus

Command	Description
acl	Access control list.
classes	Configures traffic attributes used for classification.
device	Device settings.
dp	Radware DefensePro DDoS Mitigation security settings.
help	Displays help for the specified command.
login	Log in to the device.
logout	Log out of the device.
manage	Device management configuration.
net	Network configuration.
ping	Ping a remote host.
reboot	Reboot the device.

Table 259: Radware DefensePro DDoS Mitigation CLI Commands and Menus (cont.)

Command	Description
security	Device security.
services	General networking services.
shutdown	Shut down.
ssh	Connect via SSH to a remote host.
statistics	Device statistics configuration.
system	Set system parameters.
telnet	Connect to a remote host via Telnet.
trace-route	Measure hops and latency to a given destination.

CLI Command Restrictions

Radware DefensePro DDoS Mitigation version 8.22.2 imposes the following restrictions on CLI commands:

- Maximum simultaneous commands: Approximately 120
- Maximum characters per command: 256

Example

manage terminal buffer-size set 16000000

CLI Session Time-Out

When you log on to CLI through Telnet or SSH, there is a predefined time-out for completing the authentication procedure. After establishing a CLI session with the device, the user name and password must be inserted within the period defined by the *Authentication Time-out* parameter. After three incorrect login attempts, the terminal is locked for 10 minutes and no further login attempts are accepted from that IP address.

For Telnet or SSH sessions, you define the period of time the connection with the device is maintained despite session inactivity with the Session Time-out parameter. If the session is still inactive when the predefined period ends, the session automatically terminates.

You can define the period of time the connection with the device via the console remains open despite the session's inactivity with the Session Time-out parameter. After the predefined time, the session is automatically terminated.

To configure the session time-out

> Do one of the following:

- For the console, use the following command:

  manage terminal session-timeout

- For the SSH session, use the following command:

  manage ssh session-timeout

- For the Telnet session, use the following command:

manage telnet session-timeout

- For the Telnet authentication, use the following command:

  manage telnet auth-timeout

- For the SSH authentication, use the following command:

  manage ssh auth-timeout

CLI Capabilities

You can use Radware DefensePro DDoS Mitigation CLI through console access, Telnet, or SSH. The CLI provides the following capabilities:

- Consistent, logically structured and intuitive command syntax.
- A system configcommand to view the current configuration of the device, formatted as CLI command lines.
- Pasting the output of system config, or part of it, to the CLI of another device, usingthe system configset command. This option can be used for easy configuration replication.
- Help and command completion keys.
- Command line editing keys.
- Command history.
- Configurable prompt.
- Configurable banner for Telnet and SSH.
- Ping–Ping other hosts on the network to test availability of the otherhosts.
- Traceroute–Use the following command:

  trace-route <destination IP address>

  Output format:

  trace-route to host 209.218.228.203:

  1: 50ms 50ms 50ms 212.150.43.130
  2: 50ms 50ms 50ms 80.74.101.129
  3: 50ms 50ms 50ms 192.116.214.2
  4: * * *
  5: 50ms 50ms 50ms 80.74.96.40

- Telnet client–To initiate a Telnet session to remote hosts, use the following CLI command:

  telnet <IP address>

- SSH client–To initiate a SSH session to remote hosts, use the following CLI command:

  ssh <IP address>

CLI Traps

When connected to a physical Radware DefensePro DDoS Mitigation platform via a serial cable, the device generates traps when events occur.

To send traps by CLI, Telnet, and SSH, the command is:

manage terminal traps-outputs set-on

For console only:

```
manage terminal traps-outputs set normal
```

Send Traps To All CLI Users

This option enables you to configure whether traps are sent only to the serial terminal or to SSH and Telnet clients as well.

Web Services

Radware DefensePro DDoS Mitigation devices can be managed through SNMP, a serial port, Telnet, SSH, HTTP (via internal Web application), and HTTPS. To provide customers with the capability to develop enhanced application monitoring, customized application-delivery, network-management applications and advanced automation tools, Radware provides Web Service interfaces on Radware DefensePro DDoS Mitigation with APSolute API, an open standards-based SOAP (XML) API.

Integration with APSolute API allows customers a comprehensive view of device performance, including historical data analysis and trending, performance diagnostics, availability reports and the automation of maintenance operations and fine-tuning of Radware DefensePro DDoS Mitigation for optimal application delivery based on external parameters.

Key features:

- Control of Radware product features and functions from any external application.
- API enabled network devices appear as software for applications, resulting in true, software- native integration.
- Comprehensive SDK for multiple development platforms and languages.
- Extensive sample application code, documentation, and configuration guidance.
- Over 1,700 methods available through a Web Services-based API.
- Support for SOAP/XML over HTTPS ensures flexible and secure communications.

The Radware DefensePro DDoS Mitigation Web services operate via HTTP or HTTPS requests, like a regular Web browser. Web Services are by default disabled on Radware DefensePro DDoS Mitigation.

You can enable Radware DefensePro DDoS Mitigation Web services using the following:

- CLI—manage Web-services status
- APSolute Vision—*Configuration* perspective, **Setup > Device Security > Access Protocols**

You can enable Web Services only if either the Web or secure Web management interface is enabled on the device.

API Structure

The APSolute API is a SOAP/XML interface that provides full access to Radware DefensePro DDoS Mitigation devices for third-party applications utilizing common development languages, including Java, Visual Basic/C#, and Perl. This interface enables both device configuration and monitoring status and performance statistics.

APSolute API offers two approaches to interacting with Radware DefensePro DDoS Mitigation devices:

- **Issuing CLI commands**—Note, however, that this interface does *not* provide support for:
  - Commands that are not configuration commands or monitoring, such as ping, telnetand trace-route.
  - Commands that have asynchronous output (such as accelerator related CLI commands).

  - The response to a CLI command is limited to the first 1000 rows.
- **Configuring and monitoring the devices via SOAPcommands that mirror SNMP MIB**– The following types of commands are available:
  - For scalar MIB parameter, retrieve (GET) the value and change (SET) the value.
  - For a MIB table entry, create an entry, delete an entry, update one or more parameters of an entry, retrieve (GET) an entry, retrieve (GET) the entire table, walk through the table (*get first entry* and *get next*).

APSolute API Software Development Kit (SDK)

The APSolute API SDK for Radware DefensePro DDoS Mitigation comprises Web Service Description Language (WSDL) files for all interfaces and modules. The SDK enables you to develop control and monitoring capabilities in custom-developed applications.

To start working with the APSolute API SDK, install a SOAP client tool kit (supporting SOAP version 1.1 and later) and a development environment for the tool kit on the workstation.

APPENDIX A – FOOTPRINT BYPASS FIELDS AND VALUES

This appendix describes *footprint bypass* fields in BDoS Protection and DNS Flood protection and contains the following main sections:

- BDoS Footprint Bypass Fields and Values, page 370
- DNS Footprint Bypass Fields and Values, page 377

BDoS Footprint Bypass Fields and Values

This section contains the following tables:

- BDoS Footprint Bypass Fields and Values for UDP, ICMP, and IGMP Controllers, page 370
- BDoS Footprint Bypass Fields and Values for All TCP Controllers, page 373 For

more information, see Configuring BDoS Footprint Bypass, page 123.

Table 260: BDoS Footprint Bypass Fields and Values for UDP, ICMP, and IGMP Controllers

Controller	Field	Default Status	Default Value or "N/A"[1]	Remark
UDP ICMP IGMP	checksum	Accept	For UDP: 0 For ICMP and IGMP: N/A	The checksum value in the UDP header of the packet.
UDP UDP FRAG[2] ICMP IGMP	id-num	Accept	For UDP: 0 UDP FRAG: N/A For ICMP and IGMP: N/A	The ID number from the IP packet header.
UDP UDP FRAG[2] ICMP IGMP	id-num-ipv6[3]	Accept	For UDP: 0 UDP FRAG: N/A For ICMP and IGMP: N/A	The ID number from the IPv6 packet head.
UDP ICMP IGMP	dns-id-num	Accept	For UDP: 0 For ICMP and IGMP: N/A	The ID number of a DNS query.
UDP	dns-qname	Accept	N/A	The domain name requested by a DNS query.
UDP	dns-qcount	Accept	1	The number of DNS queries in a single DNS session.
UDP	source-port	Accept	N/A	The source port of the attack.

Table 260: BDoS Footprint Bypass Fields and Values for UDP, ICMP, and IGMP Controllers (cont.)

Controller	Field	Default Status	Default Value or "N/A"[1]	Remark
UDP UDP FRAG[2] ICMP IGMP	frag-offset	Accept	UDP: 0,185 UDP FRAG: N/A ICMP: 0,185 IGMP: 0,185	Indicates where this fragment belongs in the datagram. The fragment offset is measured in units of 8 bytes (64 bits).
UDP UDP FRAG[2] ICMP	frag-offset-ipv6[3]	Accept	UDP: 0,181 UDP FRAG: N/A ICMP: 0,181 IGMP: 0,181	Indicates where this IPv6 fragment belongs in the datagram. The IPv6 fragment offset is measured in units of 8 bytes (64 bits).
UDP UDP FRAG[2] ICMP	flow-label[3]	Accept	0	Used by a source to label those products for which it requests special handling by the IPv6 router. The flow is uniquely identified by the combination of a Source address and a non-zero flow label.
UDP UDP FRAG[2] ICMP IGMP	source-ip	Accept	N/A	The source IP address of the attack.
UDP UDP FRAG[2] ICMP	source-ip-ipv6[3]	Accept	N/A	The source IPv6 address of the attack.
UDP UDP FRAG[2]7 ICMP IGMP	tos	Accept	N/A	The type of Service value from the IP packet header.

Table 260: BDoS Footprint Bypass Fields and Values for UDP, ICMP, and IGMP Controllers (cont.)

Controller	Field	Default Status	Default Value or "N/A"[1]	Remark
UDP UDP FRAG[2] ICMP IGMP	packet-size	Accept	For UDP, UDP FRAG, and IGMP: N/A For ICMP: 74	The size of the packet in bytes, including data- link header.
UDP UDP FRAG[2] ICMP	packet-size-ipv6[3]	Accept	For UDP and UDP FRAG: N/A For ICMP: 118	The size of the IPv6 packet in bytes, including data-link header.
UDP	destination-port	Accept	N/A	The destination port from the packet header.
UDP UDP FRAG[2] ICMP IGMP	destination-ip	Accept	N/A	The destination IP address.
UDP UDP FRAG[2] ICMP	destination-ip-ipv6[3]	Accept	N/A	The destination IPv6 address.
UDP UDP FRAG[2] ICMP IGMP	fragment	Accept	N/A	The protocol fragmented packet.
UDP UDP FRAG[2] ICMP IGMP	ttl	Accept	N/A	The Time-To-Live value in the IP packet header.

Table 260: BDoS Footprint Bypass Fields and Values for UDP, ICMP, and IGMP Controllers (cont.)

Controller	Field	Default Status	Default Value or "N/A"[1]	Remark
UDP UDP FRAG[2] ICMP IGMP	vlan-tag	Accept	N/A	The VLAN tag value (external).
ICMP IGMP	icmp-igmp-message-type	Accept	N/A	The protocol Message Type value.
ICMP	icmp-message-type-ipv6[3]	Accept	N/A	The ICMP IPv6 Message Type value.

1 – "N/A" (that is, "not applicable") means that no specific values can be used with the field; only the general status, **Accept** or **Bypass**, applies.
2 – This controller is available only in Radware DefensePro DDoS Mitigation 7.*x* versions 7.40 and later, and 8.*x*versions.
3 – This field is displayed only when the **IP Version Mode** on the device is set to **IPv4 and IPv6** (*Configuration* perspective > **Setup > Networking > Basic**).

Table 261: BDoS Footprint Bypass Fields and Values for All TCP Controllers

Controllers	Field	Default Status	Default Value or "N/A"[1]	Remark
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	sequence-num	Accept	N/A	The sequence number value from the relevant TCP packet header.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	id-num	Accept	N/A	The ID number from the IP packet header.

Table 261: BDoS Footprint Bypass Fields and Values for All TCP Controllers (cont.)

Controllers	Field	Default Status	Default Value or "N/A"[1]	Remark
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-port	Accept	N/A	The source port of the generated attack.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-ip	Bypass		The source IP address of the generated attack.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	source-ip-ipv6[2]	Bypass		The source IPv6 address of the generated attack.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	tos	Accept		The type of Service value from the IP packet header.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	packet-size	Accept	For TCP-SYN, TCP-SYN-ACK: 60, 62, 66, 74 For TCP-RST, TCP-ACK-FIN: 60 For TCP-Frag: N/A	The size of the packet in bytes, including the data- link header.

Table 261: BDoS Footprint Bypass Fields and Values for All TCP Controllers (cont.)

Controllers	Field	Default Status	Default Value or "N/A"[1]	Remark
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	packet-size-ipv6[2]	Accept	For TCP-SYN, TCP-SYN-ACK: 80, 82, 86, 94 For TCP-RST, TCP-ACK-FIN: 74 For TCP-Frag: N/A	The size of theIPv6 packet in bytes, including the data-link header.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-port	Accept		The destination TCP port of the attack.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-ip	Accept		The destination IP address of the attack.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	destination-ip-ipv6[2]	Accept		The destination IPv6 address of the attack.
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	ttl	Accept		The Time-To-Live value in the IP packet header.

Table 261: BDoS Footprint Bypass Fields and Values for All TCP Controllers (cont.)

Controllers	Field	Default Status	Default Value or "N/A"[1]	Remark
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	vlan-tag	Accept		The VLAN tag value (external).
TCP-FRAG	frag-offset	Accept	0, 185	Indicates where this fragment belongs in the datagram. The fragment offset is measured in units of 8 bytes (64 bits).
TCP-FRAG	frag-offset-ipv6[2]	Accept	0, 181	Indicates where this IPv6 fragment belongs in the datagram. The IPv6 fragment offset is measured in units of 8 bytes (64 bits).
TCP-SYN TCP-RST TCP-ACK-FIN TCP-SYN-ACK TCP-Frag	flow-label[2]	Accept	0	Used by a source to label those products for which it requests special handling by the IPv6 router. The flow is uniquely identified by the combination of a Source address and a non-zero flow label.

1 – "N/A" (that is, "not applicable") means that no specific values can be used with the field; only the general status, **Accept** or **Bypass**, applies.

2 – This field is displayed only when the **IP Version Mode** on the device is set to **IPv4 and IPv6** (*Configuration* perspective > **Setup > Networking > Basic**).

DNS Footprint Bypass Fields and Values

DNS footprint bypass types relate to the following controllers, all of which support the same fields, default status, and default values:

- A
- AAAA
- MX
- NAPTR
- Others
- PTR
- SOA2
- SRV
- Text

For more information, see Configuring DNS Footprint Bypass, page 127.

Table 262: DNS Footprint Bypass Fields and Values

Field	Default Status	Default Value or "N/A"[1]	Remark
checksum	Accept	For UDP: 0 For ICMP and IGMP: N/A	The checksum value in the UDP header of the packet.
id-num	Accept	For UDP: 0 For ICMP and IGMP: N/A	The ID number from the IP packet header.
id-num-ipv6[2]	Accept	For UDP: 0 For ICMP and IGMP: N/A	The ID number from the IPv6 packet head.
dns-id-num	Accept	For UDP: 0 For ICMP and IGMP: N/A	The ID number of a DNS query.
dns-qname	Accept	N/A	The domain name requested by a DNS query.
dns-subdomain	Accept	N/A	The subdomain name requested by a DNS query.
dns-qcount	Accept	1	The number of DNS queries in a single DNS session.
source-port	Accept	N/A	The source port of the attack.

Table 262: DNS Footprint Bypass Fields and Values (cont.)

Field	Default Status	Default Value or "N/A"[1]	Remark
flow-label[2]	Accept	0,181	Used by a source to label those products for which it requests special handling by the IPv6 router. The flow is uniquely identified by the combination of a Source address and a non-zero flow label.
source-ip	Accept	N/A	The source IP address of the attack.
source-ip-ipv6[2]	Accept	N/A	The source IPv6 address of the attack.
tos	Accept	N/A	The type of Service value from the IP packet header.
packet-size	Accept	For UDP and IGMP: N/A For ICMP: 74	The size of the packet in bytes, including data-link header.
packet-size-ipv6[2]	Accept	For UDP: N/A For ICMP: 118	The size of the IPv6 packet in bytes, including data-link header.
destination-ip	Accept	N/A	The destination IP address.
destination-ip-ipv6[2]	Accept	N/A	The destination IPv6 address.
fragment	Accept	N/A	The protocol fragmented packet.
ttl	Accept	N/A	The Time-To-Live value in the IP packet header.
vlan-tag	Accept	N/A	The VLAN tag value (external).
dns-ancount	Accept	0	The number of DNS answers in a single DNS session.
flags	Accept	N/A	The DNS header flags field (AA, TC, RD, and so on).

1 – "N/A" (that is, "not applicable") means that no specific values can be used with the field; only the general status, **Accept** or **Bypass**, applies.
2 – This field is displayed only when the **IP Version Mode** on the device is set to **IPv4 and IPv6** (*Configuration* perspective > **Setup > Networking > Basic**).

APPENDIX B – PREDEFINED BASIC FILTERS

The following table lists predefined basic filters that Radware DefensePro DDoS Mitigation supports. The list may vary depending on the product version.

Table 263: Predefined Basic Filters

Name	Description	Protocol	OMPC Offset	OMPC Mask
000	Routine	IP	1	e0000000
001	Priority	IP	1	e0000000
010	Immediate	IP	1	e0000000
011	Flash	IP	1	e0000000
100	ToS Flash Override	IP	1	e0000000
101	CRITIC/ECP	IP	1	e0000000
110	Internetwork Control	IP	1	e0000000
111	Network Control	IP	1	e0000000
aim-aol-any	AIM/AOL Instant Messenger	TCP	0	ffff0000
aol-msg	AOL Instant	TCP	0	0
ares_ft_udp_0	Ares_FT_udp	UDP	36	ffffffff
ares_ft_udp_1	Ares_FT_udp	UDP	40	ff000000
bearshare_download_tcp_0	BearShare_Download_tcp	TCP	0	ffffffff
bearshare_download_tcp_1	BearShare_Download_tcp	TCP	4	ffffffff
bearshare_request_file_udp_0	BearShare_Request_File_udp	UDP	0	ffffffff
bearshare_request_file_udp_1	BearShare_Request_File_udp	UDP	4	00ffffff
bittorrent_command_1_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_1_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_1_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_1_3	BitTorrent	TCP	12	ffffffff
bittorrent_command_1_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_2_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_2_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_2_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_2_3	BitTorrent	TCP	12	ffffffff

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
bittorrent_command_2_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_2_5	BitTorrent	TCP	20	ffffffff
bittorrent_command_3_0	BitTorrent	TCP	0	ffffffff
bittorrent_command_3_1	BitTorrent	TCP	4	ffffffff
bittorrent_command_3_2	BitTorrent	TCP	8	ffffffff
bittorrent_command_3_3	BitTorrent	TCP	12	ffffffff
bittorrent_command_3_4	BitTorrent	TCP	16	ffffffff
bittorrent_command_3_5	BitTorrent	TCP	20	ffff0000
bittorrent_command_4_0	BitTorrent	TCP	8	ffffff00
bittorrent_command_4_1	BitTorrent	TCP	11	ff000000
bittorrent_command_4_2	BitTorrent	TCP	11	ff000000
bittorrent_udp_1_0	BitTorrent_UDP_1	UDP	8	ffffff00
bittorrent_udp_1_1	BitTorrent_UDP_1	UDP	12	ffff0000
citrix-admin	Citrix Admin	TCP	0	0
citrix-ica	Citrix ICA	TCP	0	0
citrix-ima	Citrix IMA	TCP	0	0
citrix-ma-client	Citrix MA client	TCP	0	0
citrix-rtmp	Citrix RTMP	TCP	0	0
diameter	Diameter	TCP	0	0
directconnect_file_transfer_0	DirectConnect_File_transfer	TCP	0	ff000000
directconnect_file_transfer_1	DirectConnect_File_transfer	TCP	21	ffffffff
directconnect_file_transfer_2	DirectConnect_File_transfer	TCP	25	ffffffff
dns	Session for DNS	UDP	0	0
emule_tcp_file_request_0	eMule	TCP	0	ff000000
emule_tcp_file_request_1	eMule	TCP	4	ffff0000
emule_tcp_hello_message_0	eMule	TCP	0	ff000000

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
emule_tcp_hello_message_1	eMule	TCP	4	ffff0000
emule_tcp_secure_handshake_0	eMule	TCP	0	ff000000
emule_tcp_secure_handshake_1	eMule	TCP	4	ffff0000
ftp-session	Session for FTP	TCP	0	0
gnutella_tcp_1_0	Gnutella_TCP_1	TCP	0	ffffff00
gnutella_tcp_2_0	Gnutella_TCP_2	TCP	0	ffffffff
gnutella_tcp_2_1	Gnutella_TCP_2	TCP	4	ffffffff
gnutella_tcp_3_0	Gnutella_TCP_3	TCP	0	ffffff00
googletalk_ft_1_0	GoogleTalk_FT_1	UDP	24	ffffffff
googletalk_ft_1_1	GoogleTalk_FT_1	UDP	28	ffffffff
googletalk_ft_1_2	GoogleTalk_FT_1	UDP	32	ffffffff
googletalk_ft_1_3	GoogleTalk_FT_1	UDP	36	ffff0000
googletalk_ft_2_0	GoogleTalk_FT_2	UDP	24	ffffffff
googletalk_ft_2_1	GoogleTalk_FT_2	UDP	28	ffffffff
googletalk_ft_4_0	GoogleTalk_FT_4	UDP	67	ffffffff
googletalk_ft_4_1	GoogleTalk_FT_4	UDP	71	ffffffff
groove_command_1_0	Groove	TCP	6	ffffffff
groove_command_1_1	Groove	TCP	10	ffffffff
groove_command_1_2	Groove	TCP	14	ffffffff
groove_command_2_0	Groove	TCP	6	ffffffff
groove_command_2_1	Groove	TCP	10	ffff0000
groove_command_3_0	Groove	TCP	7	ffffffff
groove_command_3_1	Groove	TCP	11	ffffffff
groove_command_3_2	Groove	TCP	15	ffffffff
groove_command_3_3	Groove	TCP	19	ffffffff
h.225-session	Session Of H225	TCP	0	0

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
hdc1	High Drop Class 1	IP	1	fc000000
hdc2	High Drop Class 2	IP	1	fc000000
hdc3	High Drop Class 3	IP	1	fc000000
hdc4	High Drop Class 4	IP	1	fc000000
http	World Wide Web HTTP	TCP	0	0
http-alt	HTTP alternate	TCP	0	0
https	HTTP over SSL	TCP	0	0
icecast_1	IceCast_Stream	TCP	0	ffffffff
icecast_2	IceCast_Stream	TCP	4	ffffffff
icecast_3	IceCast_Stream	TCP	8	ffff0000
icmp	ICMP	ICMP	0	0
icq	ICQ	TCP	0	0
icq_aol_ft_0	ICQ_AOL_FT	TCP	0	ffffffff
icq_aol_ft_1	ICQ_AOL_FT	TCP	0	ffffffff
icq_aol_ft_2	ICQ_AOL_FT	TCP	2	ffff0000
imap	Internet Message Access	TCP	0	0
imesh_download_tcp_0	iMesh_Download_tcp	TCP	0	ffffffff
imesh_download_tcp_1	iMesh_Download_tcp	TCP	4	ffffffff
imesh_request_file_udp_0	iMesh_Request_File_udp	UDP	0	ffffffff
imesh_request_file_udp_1	iMesh_Request_File_udp	UDP	4	00ffffff
ip	IP Traffic	IP	0	0
itunesdaap_ft_0	iTunesDaap_FT	TCP	0	ffffffff
itunesdaap_ft_1	iTunesDaap_FT	TCP	4	ffffffff
itunesdaap_ft_2	iTunesDaap_FT	TCP	8	ffffff00
itunesdaap_ft_3	iTunesDaap_FT	TCP	2	ffff0000
kazaa_request_file_0	Kazaa_Request_File	TCP	0	ffffffff

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
kazaa_request_file_1	Kazaa_Request_File	TCP	4	ffffffff
kazaa_request_file_2	Kazaa_Request_File	TCP	8	ffff0000
kazaa_udp_packet_0	Kazaa_UDP_Packet	UDP	6	ffffffff
kazaa_udp_packet_1	Kazaa_UDP_Packet	UDP	4	ffff0000
ldap	LDAP	TCP	0	0
ldaps	LDAPS	TCP	0	0
ldc1	Low Drop Class 1	IP	1	fc000000
ldc2	Low Drop Class 2	IP	1	fc000000
ldc3	Low Drop Class 3	IP	1	fc000000
ldc4	Low Drop Class 4	IP	1	fc000000
lrp	Load Report Protocol	UDP	0	0
manolito_file_transfer_0_0	Manolito	TCP	0	ffffffff
manolito_file_transfer_0_1	Manolito	TCP	0	ffffffff
manolito_file_transfer_0_2	Manolito	TCP	0	ffffffff
manolito_file_transfer_1_0	Manolito	TCP	4	ff000000
manolito_file_transfer_1_1	Manolito	TCP	4	ff000000
manolito_file_transfer_2_0	Manolito	TCP	4	ff000000
manolito_file_transfer_2_1	Manolito	TCP	4	ff000000
mdc1	Medium Drop Class 1	IP	1	fc000000
mdc2	Medium Drop Class 2	IP	1	fc000000
mdc3	Medium Drop Class 3	IP	1	fc000000
mdc4	Medium Drop Class 4	IP	1	fc000000
meebo_get_0	MEEBO_GET	TCP	0	ffffffff
meebo_get_1	MEEBO_GET	TCP	4	ffffffff
meebo_get_2	MEEBO_GET	TCP	8	ffffffff
meebo_get_3	MEEBO_GET	TCP	12	ffffffff

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
meebo_get_4	MEEBO_GET	TCP	16	ffffffff
meebo_get_5	MEEBO_GET	TCP	20	ffffffff
meebo_get_6	MEEBO_GET	TCP	24	ffffffff
meebo_get_7	MEEBO_GET	TCP	28	ffffffff
meebo_get_8	MEEBO_GET	TCP	32	ff000000
meebo_post_0	MEEBO_POST	TCP	0	ffffffff
meebo_post_1	MEEBO_POST	TCP	4	ffffffff
meebo_post_2	MEEBO_POST	TCP	8	ffffffff
meebo_post_3	MEEBO_POST	TCP	12	ffffffff
meebo_post_4	MEEBO_POST	TCP	16	ffffffff
meebo_post_5	MEEBO_POST	TCP	20	ffffffff
meebo_post_6	MEEBO_POST	TCP	24	ffffffff
meebo_post_7	MEEBO_POST	TCP	28	ffffff00
msn-any	MSN Messenger Chat	TCP	0	ffffffff
msn-msg	MSN Messenger Chat	TCP	0	0
msn_msgr_ft_0	MSN_MSGR_FT	TCP	0	ffffffff
msn_msgr_ft_1	MSN_MSGR_FT	TCP	48	ffffffff
mssql-monitor	Microsoft SQL traffic-monitor	TCP	0	0
mssql-server	Microsoft SQL server traffic	TCP	0	0
nntp	Network News	TCP	0	0
nonip	Non IP Traffic	NonIP	0	0
oracle-server1	Oracle server	TCP	0	0
oracle-server2	Oracle server	TCP	0	0
oracle-server3	Oracle server	TCP	0	0
oracle-v1	Oracle SQL *Net version 1	TCP	0	0
oracle-v2	Oracle SQL *Net version 2	TCP	0	0

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
pop3	Post Office Protocol 3	TCP	0	0
prp	PRP	UDP	0	0
radius	RADIUS protocol	TCP	0	0
rexec	Remote Process Execution	TCP	0	0
rshell	Remote Shell	TCP	0	0
rtp_ft_0	RTP_FT	UDP	0	ffff0000
rtp_ft_1	RTP_FT	UDP	0	ffff0000
rtp_ft_2	RTP_FT	UDP	16	ffff0000
rtsp	RTSP	TCP	0	0
sap	SAP	TCP	0	0
sctp	SCTP Traffic	SCTP	0	0
skype-443-handshake	Skype signature for port 443	TCP	0	ff000000
skype-443-s-hello	Skype signature for port 443	TCP	11	ffffffff
skype-80-l-56	Skype signature for port 80	TCP	2	ffff0000
skype-80-proxy	Skype signature for port 80	TCP	0	ffffffff
skype-80-pshack	Skype signature for port 80	TCP	13	ff000000
skype-ext-l-54	Skype signature	TCP	2	ffff0000
skype-ext-pshack	Skype signature	TCP	13	ff000000
smtp	Simple Mail Transfer	TCP	0	0
snmp	SNMP	UDP	0	0
snmp-trap	SNMP Trap	UDP	0	0
softethervpn443	SoftEther Ethernet System	TCP	0	ffffff00
softethervpn8888	SoftEther Ethernet System	TCP	0	ffffff00
soulseek_pierce_fw_0	SoulSeek_Pierce_FW	TCP	0	ffffffff
soulseek_pierce_fw_1	SoulSeek_Pierce_FW	TCP	4	ff000000
soulseek_pierce_fw_2	SoulSeek_Pierce_FW	TCP	2	ffff0000

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
ssh	Secure Shell	TCP	0	0
tcp	TCP Traffic	TCP	0	0
telnet	Telnet	TCP	0	0
tftp	Trivial File Transfer	UDP	0	0
udp	UDP Traffic	UDP	0	0
voip_sign_1	VOIP signature	UDP	28	c03f0000
voip_sign_10	VOIP signature	UDP	28	c03f0000
voip_sign_11	VOIP signature	UDP	28	c03f0000
voip_sign_12	VOIP signature	UDP	28	c03f0000
voip_sign_13	VOIP signature	UDP	28	c03f0000
voip_sign_2	VOIP signature	UDP	28	c03f0000
voip_sign_3	VOIP signature	UDP	28	c03f0000
voip_sign_4	VOIP signature	UDP	28	c03f0000
voip_sign_5	VOIP signature	UDP	28	c03f0000
voip_sign_6	VOIP signature	UDP	28	c03f0000
voip_sign_7	VOIP signature	UDP	28	c03f0000
voip_sign_8	VOIP signature	UDP	28	c03f0000
voip_sign_9	VOIP signature	UDP	28	c03f0000
yahoo_ft_0	YAHOO_FT	TCP	0	ffffffff
yahoo_ft_1	YAHOO_FT	TCP	10	ffff0000
yahoo_get_0	YAHOO_GET	TCP	0	ffffffff
yahoo_get_1	YAHOO_GET	TCP	4	ffffffff
yahoo_get_2	YAHOO_GET	TCP	8	ffffffff
yahoo_get_3	YAHOO_GET	TCP	12	ffffffff
yahoo_get_4	YAHOO_GET	TCP	16	ff000000
yahoo_post_0	YAHOO_POST	TCP	0	ffffffff

Table 263: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
yahoo_post_1	YAHOO_POST	TCP	4	ffffffff
yahoo_post_2	YAHOO_POST	TCP	8	ffffffff
yahoo_post_3	YAHOO_POST	TCP	12	ffffffff
yahoo_post_4	YAHOO_POST	TCP	16	ffff0000

APPENDIX C – ATTACK-PROTECTION ID NUMBERS

This appendix describes the Radware DefensePro DDoS Mitigation Attack-Protection IDs.

Table 264: Radware DefensePro DDoS Mitigation Attack-Protection IDs

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report Action	Description
8	Black List	Access				Black-list access violation.
9	White List	N/A				White-list encounters are not reported as security events.
70	Network flood IPv4 UDP	Behavioral-DoS				Network flood IPv4 UDP.
71	Network flood IPv4 ICMP	Behavioral-DoS				Network flood IPv4 ICMP.
72	Network flood IPv4 IGMP	Behavioral-DoS				Network flood IPv4 IGMP.
73	Network flood IPv4 TCP- SYN	Behavioral-DoS				Network flood IPv4 TCP with SYN flag.
74	Network flood IPv4 TCP-RST	Behavioral-DoS				Network flood IPv4 TCP with RST flag.
76	Network flood IPv4 TCP- PSH	Behavioral-DoS				Network flood IPv4 TCP with PSH flag.
77	Network flood IPv4 TCP- FIN	Behavioral-DoS				Network flood IPv4 TCP with FIN flag.
78	Network flood IPv4 TCP-SYN-ACK	Behavioral-DoS				Network flood IPv4 TCP with SYN and ACK flags
79	Network flood IPv4 TCP-FRAG	Behavioral-DoS				Network flood IPv4 TCP with FRAG flag.
80	Network flood IPv6 UDP	Behavioral-DoS				Network flood IPv6 UDP.
81	Network flood IPv6 ICMP	Behavioral-DoS				Network flood IPv6 ICMP.
83	Network flood IPv6 TCP- SYN	Behavioral-DoS				Network flood IPv6 TCP with SYN flag.
84	Network flood IPv6 TCP-RST	Behavioral-DoS				Network flood IPv6 TCP with RST flag.
86	Network flood IPv6 TCP- PSH	Behavioral-DoS				Network flood IPv6 TCP with PSH flag.
87	Network flood IPv6 TCP- FIN	Behavioral-DoS				Network flood IPv6 TCP with FIN flag.

Table 264: Radware DefensePro DDoS Mitigation Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report Action	Description
88	Network flood IPv6 TCP-SYN-ACK	Behavioral-DoS				Network flood IPv6 TCP with SYN and ACK flags.
89	Network flood IPv6 TCP-FRAG	Behavioral-DoS				Network flood IPv6 TCP with FRAG flag.
90	Network flood IPv4 UDP-FRAG	Behavioral-DoS				Network flood IPv4 UDP with FRAG flag.
100	Unrecognized L2 Format	Anomalies	Low	No-report	Process	Unrecognized L2 format.
103	Incorrect IPv4 checksum	Anomalies	Low	Block	Bypass	Incorrect IPv4 checksum.
104	Invalid IPv4 Header or Total Length	Anomalies	Low	Block	Bypass	Invalid IPv4 header or total length.
105	TTL Less Than or Equal to 1	Anomalies	Low	Report	Process	TTL less than or equal to 1.
107	Inconsistent IPv6 Headers	Anomalies	Low	Block	Bypass	Inconsistent IPv6 headers.
108	IPv6 Hop Limit Reached	Anomalies	Low	Report	Process	IPv6 hop limit reached.
110	Unsupported L4 Protocol	Anomalies	Low	No-report	Process	Unsupported L4 protocol.
113	Invalid TCP Flags	Anomalies	Low	Block	Bypass	Invalid TCP flags.
119	Source or Dest Address same as Local Host	Anomalies	Low	Block	Bypass	Source or destination IP address same as local host.
120	Source Address same as Dest Address (Land Attack)	Anomalies	Low	Block	Bypass	Source IP address same as destination IP address (Land Attack). The common vulnerability enumerator (CVE) for this signature is CVE-1999-0016.
125	L4 Source or Dest Port Zero	Anomalies	Low	Block	Bypass	Layer 4 source or destination port are zero.
126	Incorrect GRE Version	Anomalies	Low	Report	Bypass	Matches packets whose GRE version is not 0 or 1.

128	Invalid GRE Header	Anomalies	Low	Report	Bypass	Matches packets where one or more flags are not RFC compliant or there are partial or sliced packets.

Table 264: Radware DefensePro DDoS Mitigation Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report Action	Description
131	Invalid L4 Header Length	Anomalies	Low	Block	Bypass	Invalid L4 header length
240	TCP Out-of-State	Anomalies				TCP Out-of-State floods.
350	SCAN_TCP_SCAN	Anti Scan				TCP scanning attempt.
351	SCAN_UDP_SCAN	Anti Scan				UDP scanning attempt.
352	SCAN_ICMP_SCAN	Anti Scan				ICMP scanning attempt.
450	DNS flood IPv4 DNS-A	DNS-Protection				DNS A query flood over IPv4.
451	DNS flood IPv4 DNS-MX	DNS-Protection				DNS MX query flood over IPv4.
452	DNS flood IPv4 DNS-PTR	DNS-Protection				DNS PTR query flood over IPv4.
453	DNS flood IPv4 DNS-AAAA	DNS-Protection				DNS AAAA query flood over IPv4.
454	DNS flood IPv4 DNS-Text	DNS-Protection				DNS Text query flood over IPv4.
455	DNS flood IPv4 DNS-SOA	DNS-Protection				DNS SOA query flood over IPv4.
456	DNS flood IPv4 DNS-NAPTR	DNS-Protection				DNS NAPTR query flood over IPv4.
457	DNS flood IPv4 DNS-SRV	DNS-Protection				DNS SRV query flood over IPv4.
458	DNS flood IPv4 DNS-Other	DNS-Protection				DNS Other queries flood over IPv4.
459	DNS flood IPv4 DNS-ALL	DNS-Protection				DNS query flood over IPv4.
460	DNS flood IPv6 DNS-A	DNS-Protection				DNS A query flood over IPv6.
461	DNS flood IPv6 DNS-MX	DNS-Protection				DNS MX query flood over IPv6.
462	DNS flood IPv6 DNS-PTR	DNS-Protection				DNS PTR query flood over IPv6.
463	DNS flood IPv6 DNS-AAAA	DNS-Protection				DNS AAAA query flood over IPv6.
464	DNS flood IPv6 DNS-Text	DNS-Protection				DNS Text query flood over IPv6.
465	DNS flood IPv6 DNS-SOA	DNS-Protection				DNS SOA query flood over IPv6.
466	DNS flood IPv6 DNS-NAPTR	DNS-Protection				DNS NAPTR query flood over IPv6.
467	DNS flood IPv6 DNS-SRV	DNS-Protection				DNS SRV query flood over IPv6.
468	DNS flood IPv6 DNS-Other	DNS-Protection				DNS Other queries flood over IPv6.
469	DNS flood IPv6 DNS-ALL	DNS-Protection				DNS query flood over IPv6.

Table 264: Radware DefensePro DDoS Mitigation Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report Action	Description
470	DNS RFC-compliance violation	DNS-Protection	Low	Drop		DNS RFC-compliance violation for DNS queries.
700	HTTPS Flood protection	Https				HTTPS Flood Protection defends against HTTPS-flood attacks that send malicious HTTPS requests to protected HTTPS servers.
720	SYN Flood protection		High	According to policy Action		Start, ongoing, and termination of attacks per protection policy.
727	SYN Protect full table		Medium	According to policy Action		Used when the SYN Flood Protection table is full and the module cannot handle more concurrent authentication processes. New verified ACK (or data) packets will be discarded as long as the table is full.
800	GEO Protection	GeoFeed				Geolocation protection blocks all traffic from selected geolocations. Customers can configure specific permanently blocked locations or use the Geolocation Map to temporarily block traffic from selected geolocations
1282	EAAF Protection	ErtFeed				ERT Active Attackers Feed (EAAF) profiles use the EAAF subscription service to identify and block source IP addresses involved in major attacks in real-time to provide preemptive protection from known attackers.

1,000–100,000	DoS Shield signatures or intrusion-protection signatures	DoS				Range for signatures, from the Security Operations Center (SOC) signature file. Odd ID numbers are DoS shield signatures. Even ID numbers are Intrusion signatures.

Table 264: Radware DefensePro DDoS Mitigation Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report Action	Description
200,000	HTTP	SynFlood	Medium	According to policy Action		Predefined HTTP-SYN-flood attack protection.
200,001	HTTPS	SynFlood	Medium	According to policy Action		Predefined HTTPS-SYN-flood attack protection.
200,002	RTSP	SynFlood	Medium	According to policy Action		Predefined RTSP-SYN-flood attack protection.
200,003	FTP_CTRL	SynFlood	Medium	According to policy Action		Predefined FTP_CTRL-SYN-flood attack protection.
200,004	POP3	SynFlood	Medium	According to policy Action		Predefined POP3-SYN-flood attack protection.
200,005	IMAP	SynFlood	Medium	According to policy Action		Predefined IMAP-SYN-flood attack protection.
200,006	SMTP	SynFlood	Medium	According to policy Action		Predefined SMTP-SYN-flood attack protection.
200,007	TELNET	SynFlood	Medium	According to policy Action		Predefined TELNET-SYN-flood attack protection.
200,008	RPC	SynFlood	Medium	According to policy Action		Predefined RPC-SYN-flood attack protection.
300,000–449,999	User-defined custom signatures	DoS				Range for user-defined protections. The device generates the ID number sequentially when the user creates the signature.

Table 264: Radware DefensePro DDoS Mitigation Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report Action	Description
450,000–475,000	User-defined Connection Limit protections	DoS				Range for user-defined Connection Limit protections. The device generates the ID number sequentially when the user creates the protection.
500,000–599,999	User-defined SYN-flood protections	SYNFlood	Low	According to policy Action		Range for user-defined SYN-flood protections device generates the ID number sequentially when the user creates the protection.
600,000–675,000	User-defined Connection PPS protections	DoS				Range for user-defined *Connection PPS / Connection PPS Limit* protections device generates the ID number sequentially when the user creates the protection.
700,000–1,000,000	User-defined Traffic Filters	Traffic Filters	High	Drop		Range for user-defined Traffic Filters. The device generates the ID number sequentially when the user creates the Traffic Filter.

APPENDIX D – SUPPORTED PROTOCOLS

This appendix lists the protocols and operating systems that Radware DefensePro DDoS Mitigation signatures can protect.

Radware DefensePro DDoS Mitigation signatures can protect the following protocols:

- BGP
- BOOTP
- Borland Interbase Protocol
- CA License Client Protocol
- CVS
- DCERPC
- DHCP
- DNP3 (SCADA)
- DNS
- EIGRP
- Finger
- FTP
- HTTP
- HTTPS
- ICCP (SCADA)
- ICMP
- Ident
- IGAP
- IGMP
- IP
- IPP
- IRC
- ISAKMP
- LDAP
- LPR
- MaxDB
- MODBUS (SCADA)
- Motorola Timbuktu
- NBT
- NDAP
- NDMP
- NetBIOS
- NetFlow
- NFS
- NHRP
- NMAP
- NNTP
- Ntalk
- NTP
- ORACLE
- Overnet
- PCAnywhere
- POP2
- POP3
- PP
- RADIUS
- RDP
- Retrospect
- RFB (VNC)
- RIP
- Rlogin
- RTSP
- SCCP (SKINNY)
- SCTP
- Secure IMAP
- Secure SMTP
- SIP
- SMB
- SMS Remote Control
- SMTP
- SNMP
- SOAP
- SOCKS4
- SOCKS5
- SQL
- SSH
- SSL
- SUN-RPC
- TACACS
- TCP
- TELNET
- TFTP
- UDP
- UPNP
- WebDAV
- WHOIS
- Winny
- WINS
- XD

Radware DefensePro DDoS Mitigation signatures can protect the following operating systems:

- 3COM
- Cisco
- Juniper
- Linux
- MAC OS
- MS Windows
- MS Windows Server

- Unix

APPENDIX E – TROUBLESHOOTING

If the device does not operate as expected, you can diagnose the system or provide Technical Support with relevant information.

For troubleshooting hardware-related issues, please consult Cisco Technical Support.

Technical Support File

A Radware DefensePro DDoS Mitigation device can generate a technical-support file, which you can save to a specified location and send to Technical Support to help diagnose problems.

Using the CLI, the technical-support file includes the following:

- **The data that Radware Technical Support typically needs to diagnose a problem with a Radware DefensePro DDoS Mitigation device**–The data comprises the collected output from various CLI commands.
- **A record of each configuration change to the device (by any management interface)**– A device begins storing these records when the device receives its first command. The records are sorted by date in ascending order. When the size of the data exceeds the maximum allowed size (2 MB), the oldest record is overwritten. The entire data is never cleared unless you erase the device configuration.
- **support.txt**–Contains the data that Technical Support typically needs to diagnose a problem with a Radware DefensePro DDoS Mitigation device. The data comprises the collected output from various CLI commands.
- **auditLog.log** –Contains record of each configuration change to the device (by any management interface). A device begins storing these records when the device receives its first command. The records are sorted by date in ascending order. When the size of the data exceeds the maximum allowed size (2 MB), the oldest record is overwritten. The entire data is never cleared unless you erase the device configuration.

  The structure of each record in the auditLog.logfile is as follows:

  <dd>-<MM>-<yyyy> <hh>:<mm>:<ss> <Event description>

  Example:

  06-12-2016 19:16:11 COMMAND: “logout” by user radware via Console
- NTFLD.tar–Contains data on network floods.

To generate and display the output of a technical-support file on the terminal using the CLI

> Enter the following command:

manage support display

To generate a technical-support file and send it to a TFTP server using the CLI

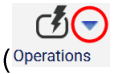
> Enter the following command:

manage support tftp put <file name> <TFTP server IP address> [-v]

where:

-vdisplays also the output of the command.

To generate and download a technical-support file using APSolute Vision

1. In the device pane, select the device.
2. Click the arrow next to the **Operations** icon (

).
3. Select **Export Technical Support File**.
4. Configure the download parameters, and click **Submit**.

Table 265: Device Technical Support File Download Parameters

Parameter	Description
Download Via	(Read-only) The protocol used to download the technical support file. Value: HTTPS
Save As	Save the downloaded technical support file as a text file on the APSolute Vision system. Enter or browse to the location of the saved file, and select or enter a file name.

Caution: If you run the following procedure using Internet Explorer, the file downloads successfully, however, an error occurs, and the connection resets.

APPENDIX F – GLOSSARY

Table 266: Glossary Terms

Term	Definition
AMS	Attack Mitigation Service. AMS is a solution offering from Radware, which comprises the following products: • DefensePro • Cloud DDoS Protection (previously DefensePipe) • DefenseFlow • AppWall • Cloud WAF • APSolute Vision • ERT–Emergency Response Team
Anomaly	An anomaly is unusual or unexpected behavior of traffic patterns or a protocol.
Attack	An attack is a realization of a threat, a malicious action taken against a network, host, or service.
Attack Signatures Database / Signatures Database	Radware's Attack Signatures database contains signatures of known attacks. These signatures are included in the predefined groups and profiles supplied by Radware to create security protection policies. Each profile consists of attack signatures with common characteristics intended to protect a specific application or range of IP addresses.
Behavioral DoS (BDoS)	Behavioral DoS (Behavioral Denial of Service) protection defends networks from zero day network-flood attacks that jam available network bandwidth with spurious traffic, denying use of network resources for legitimate users. BDoS profiles do this by identifying the footprint of the anomalous traffic. Network-flood protection types include: • SYN Flood • TCP Flood, including TCP Fin + Ack Flood, TCP Reset Flood • TCP Syn + Ack Flood, TCP Fragmentation Flood • UDP Flood • ICMP Flood • IGMP Flood
Black List	You can define Radware DefensePro DDoS Mitigation Black List rules to block certain traffic. Black List rules are used as exceptions for Radware DefensePro DDoS Mitigation *security policies* (see Security policy). You can define Black List rules for a single IP address or using a Network class.

Table 266: Glossary Terms (cont.)

Term	Definition
Certificate	Certificates are digitally signed indicators which identify the server or user. They are usually provided in the form of an electronic key or value. The digital certificate represents the certification of an individual business or organizational public key but can also be used to show the privileges and roles for which the holder has been certified. It can also include information from a third-party verifying identity. Authentication is needed to ensure that users in a communication or transaction are who they claim to be.
Class	In Radware DefensePro DDoS Mitigation, *classes* define groups of elements of the same type of entity.
DDoS	Distributed denial-of-service attack on a DNS server. A typical attack involves numerous compromised zombie systems (botnets) sending spoofed domain-name requests to DNS servers, which process the “legitimate” request and send replies to the spoofed victims. When the DNS server is configured to provide recursion, if the requested domain name is not available locally, the DNS server will query the root name servers for the IP address. The traffic then traverses the Internet backbone, affecting the Internet Service Provider and any upstream provider to reach the intended target. Radware DefensePro DDoS Mitigation’s adaptive behavior-based DoS Protection learns the characteristics of DNS traffic and re-establishes normal traffic behavior baselines. An embedded decision engine, based on fuzzy logic, constantly analyzes DNS traffic and detects when deviations from the normal baselines occur. Upon detection, the system performs an in-depth analysis of the suspicious DNS packets in order to identify abnormal appearances of parameters in the packet headers and payload.
Deep Packet Inspection	Inspection of the packet’s payload as opposed to only its header. This enables the security device to perform inspection at the application level.
DME	DoS/DDoS mitigation engine.
DoS	Denial of service is an attack intended to consume system resources and create a temporary loss of service.
ERT	Emergency Response Team. Radware’s ERT is an emergency DDoS service that can stop DDoS attacks fast. This unique emergency DDoS service is designed to provide 24/7 security services for customers facing a denial-of-service (DoS) or a distributed denial-of-service (DDoS) attack, or a malware outbreak. Often, these attacks require immediate assistance and specialized DDoS prevention techniques.
Exploit	An exploit is a program or technique that takes advantage of a software vulnerability. The program can be used for breaking security, or otherwise attacking a host over the network.
Filter	In the context of the Radware DefensePro DDoS Mitigation Signature Protection module, filters are components of a signature. Each filter contains the exact pattern of the attack. Radware DefensePro DDoS Mitigation scans, classifies and matches packets to the filters in the Signatures database. Upon a match, the Signature Protection module takes the configured action.

Table 266: Glossary Terms (cont.)

Term	Definition
Heuristic analysis	Heuristic analysis is behavior-based analysis, targeted to provide a filter blocking the abnormal phenomena. Heuristic analysis is the ability of a virus scanner to identify a potential virus by analyzing the behavior of the program, rather than looking for a known virus signature.
Historical security reporting	The Attack Mitigation Service (AMS), using APSolute Vision, offers a built-in security information and event management (SIEM) for historical security reporting of Radware DefensePro DDoS Mitigation security events.
Inspection port	An inspection port is a port on a Radware DefensePro DDoS Mitigation device that you can configure to receive, inspect, and transmit traffic.
Intrusion	An intrusion is an attempted or successful access to system resources in any unauthorized manner.
Intrusion Detection System (IDS)	Intrusion Detection System. An IDS applies the latest security or attack expertise to filter out potentially destructive/malicious events from a much larger amount of legitimate activity. There are two system-monitoring approaches: • NIDS—network-based IDS—monitors all network traffic passing on the segment where the agent is installed, acting upon suspicious anomalies or signature-based activity. • HIDS—host-based IDS—is confined to the local host and monitor activity in detail, such as, command execution, file access, or system calls. Organizations generally choose a combination of these approaches, based on known vulnerabilities.
IPS	Intrusion prevention system. That is, a network security appliance that monitors network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. Intrusion prevention systems are considered extensions of Intrusion Detection Systems (IDS) because they both monitor network traffic and/ or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are supposed to be able to actively prevent/block intrusions that are detected.

Table 266: Glossary Terms (cont.)

Term	Definition
IP interface	An IP interface in Radware DefensePro DDoS Mitigation is comprised of two components: an IP address and an associated interface. The associated interface can be a physical interface or a virtual interface (VLAN). IP routing is performed between Radware DefensePro DDoS Mitigation IP interfaces, while bridging is performed within an IP interface that contains an IP address associated with a VLAN. Radware DefensePro DDoS Mitigation is designed to intercept HTTP requests and to redirect them to a content inspection server farm. The first assumption in designing a Radware DefensePro DDoS Mitigation network is that the Radware DefensePro DDoS Mitigation device resides on the path between the clients and both the Internet and the content inspection servers. This is required since Radware DefensePro DDoS Mitigation needs to intercept the clients' requests going to the Internet and to manipulate the packets returning from the content inspection servers to the clients. Except when using local triangulation or transparent proxy, all traffic must physically travel through the Radware DefensePro DDoS Mitigation device. This includes traffic from the users to the Internet and from the content inspection server farm back to the users. If there are users statically configured to use a content inspection server, they should be configured to the Radware DefensePro DDoS Mitigation virtual address. This address is the access IP address for the content inspection servers. This address is used only for statically configured users.
Network class	A Network class is a type of class in the Radware DefensePro DDoS Mitigation configuration (see Class). A Network class is identified by a name and defined by a network address and mask, or by a range of IP addresses (from-to).
NHR	A Next-Hop Router (NHR) is a network element with an IP address through which traffic is routed.
Protection policy	Another term for a Radware DefensePro DDoS Mitigation *security policy* (see Security policy).
Security event reporting	Radware DefensePro DDoS Mitigation security events include all events related to attack detection and mitigation. When an attack is detected, Radware DefensePro DDoS Mitigation creates and reports a *security event*, which includes the information relevant to the specific attack.
Security policy	A security policy in an organization is a set of rules that defines what constitutes a secure network and how Radware DefensePro DDoS Mitigation reacts to security violations. You implement a security policy for your organization by using the global security settings, network classification and protection profiles. You can define the security policy to suit different network segments down to a single server, providing comprehensive protection for your organization. Each policy consists of multiple profiles and the action to be taken when the device detects an attack.
Server, Reporting	A reporting server is the component responsible for running the required services to display reports to the end user. It may contain a Web server and provide services for both Eclipse and Web interfaces.
Service	A feature that provides protection against a set of attacks.

Table 266: Glossary Terms (cont.)

Term	Definition
Signature	A signature is a pattern-based analysis, used to search for packets generated by known network vulnerabilities, application vulnerabilities, exploitation attempts, and DoS/DDoS attack tools.
Signature Protection module	The Radware DefensePro DDoS Mitigation Signature Protection module protects against known network vulnerabilities, application vulnerabilities, exploitation attempts, and DoS/DDoS flood attacks.
SME	String-matching engine.
Spoof	A spoof is when one system entity poses as or assumes the identity of another entity.
SYN cookie	SYN cookies are particular choices of initial TCP sequence numbers by TCP servers. The difference between the server's initial sequence number and the client's initial sequence number is: • Top 5 bits: t mod 32, where t is a 32-bit time counter that increases every 64 seconds. • Next 3 bits: an encoding of an MSS selected by the server in response to the client's MSS. • Bottom 24 bits: a server-selected secret function of the client IP address and port number, the server IP address and port number, and t. This choice of sequence number complies with the basic TCP requirement that sequence numbers increase slowly; the server's initial sequence number increases slightly faster than the client's initial sequence number. A server that uses SYN cookies does not have to drop connections when its SYN queue fills up. Instead it sends back a SYN+ACK, exactly as if the SYN queue had been larger. (Exceptions: the server must reject TCP options such as large windows, and it must use one of the eight MSS values that it can encode.) When the server receives an ACK, it checks that the secret function works for a recent value of t, and then rebuilds the SYN queue entry from the encoded MSS. A SYN flood is simply a series of SYN packets from forged IP addresses. The IP addresses are chosen randomly and don't provide any hint of where the attacker is. The SYN flood keeps the server's SYN queue full. Normally this would force the server to drop connections. A server that uses SYN cookies, however, will continue operating normally. The biggest effect of the SYN flood is to disable large windows.

Table 266: Glossary Terms (cont.)

Term	Definition
SYN flood	A SYN attack/flood is a type of DoS (denial-of-service) attack. SYN-flood attacks are performed by sending a SYN packet without completing the TCP three-way handshake, referred as single packet attack. Alternatively, the TCP three-way handshake can be completed, but no data packets are sent afterwards. Such attacks are known as connection flood attacks. A SYN packet notifies a server of a new connection. The server then allocates some memory in order to handle the incoming connection, sends back an acknowledgment, then waits for the client to complete the connection and start sending data. By spoofing large numbers of SYN requests, an attacker can fill up memory on the server, which waits for more data that never arrives. Once memory has filled up, the server is unable to accept connections from legitimate clients. This effectively disables the server. Key point: SYN floods exploit a flaw in the core of the TCP/IP technology itself. There is no complete defense against this attack. There are, however, partial defenses. Servers can be configured to reserve more memory and decrease the amount of time they wait for connections to complete. Likewise, routers and firewalls can filter out some of the spoofed SYN packets. Finally, there are techniques (such as “SYN cookies”) that can play tricks with the protocol in order to help distinguish good SYNs from bad ones.
SYN-ACK Reflection Attack Prevention	SYN-ACK Reflection Attack Prevention is intended to prevent reflection of SYN attacks and reduce SYN-ACK packet storms that are created as a response to DoS attacks. When a device is under SYN attack, it sends a SYN-ACK packet with an embedded Cookie, in order to prompt the client to continue the session.
Threat	A threat, in Internet security terms, is a person, thing, event, or idea, that poses a danger to an asset. A fundamental threat can be any of the following: information leakage, Denial of Service, integrity violation, and illegitimate use.
Trojan Horse	A Trojan horse (also known as a *Trojan*) is a computer program that appears benign, but is actually designed to harm or compromise the system. It is usually designed to provide unrestricted access into internal systems, bypassing security monitoring and auditing policies.
Virus	A virus is a malicious program code written with the intention to damage computer systems and to replicate itself to extend the possible damage.
Web application attack	A category of attacks, which are crafted to take advantage of vulnerabilities found in Web servers, vulnerabilities in HTTP, or application-specific vulnerabilities. Examples of Web application attacks include cross-site scripting (XSS), SQL injection, and code injection.
White List	Radware DefensePro DDoS Mitigation White List rules allow certain traffic without inspection. White List are rules are used as exceptions for Radware DefensePro DDoS Mitigation security policies (see Security policy). You can define White List rules for a single IP address or using a Network class.
Worm	A worm is a type of computer virus that uses the Internet or local networks to spread itself by sending copies of itself to other hosts.

Table 266: Glossary Terms (cont.)

Term	Definition
Zero-day attack / zero-minute attack	A zero-day attack (0-day) or zero-minute attack is an attack on a vulnerability that no one knows about except for those who discovered it. A zero-day attack is carried out by exploiting a non-public, unknown vulnerability. Since there are no known signatures, the attack penetrates any signature-based security defenses (for example, an intrusion prevention system). If the exploit passes through a common port and there are no other defenses, such as behavioral-based or impact-based techniques, the attack is hard or impossible to stop.

RADWARE LTD. END USER LICENSE AGREEMENT

By accepting this End User License Agreement (this "License Agreement") you agree to be contacted by Radware Ltd.'s ("Radware") sales personnel.

If you would like to receive license rights different from the rights granted below or if you wish to acquire warranty or support services beyond the scope provided herein (if any), please contact Radware's sales team.

THIS LICENSE AGREEMENT GOVERNS YOUR USE OF ANY SOFTWARE DEVELOPED AND/OR DISTRIBUTED BY RADWARE AND ANY UPGRADES, MODIFIED VERSIONS, UPDATES, ADDITIONS, AND COPIES OF THE SOFTWARE FURNISHED TO YOU DURING THE TERM OF THE LICENSE GRANTED HEREIN (THE "SOFTWARE"). THIS LICENSE AGREEMENT APPLIES REGARDLESS OF WHETHER THE SOFTWARE IS DELIVERED TO YOU AS AN EMBEDDED COMPONENT OF A RADWARE PRODUCT ("PRODUCT"), OR WHETHER IT IS DELIVERED AS A STANDALONE SOFTWARE PRODUCT. FOR THE AVOIDANCE OF DOUBT IT IS HEREBY CLARIFIED THAT THIS LICENSE AGREEMENT APPLIES TO PLUG-INS, CONNECTORS, EXTENSIONS AND SIMILAR SOFTWARE COMPONENTS DEVELOPED BY RADWARE THAT CONNECT OR INTEGRATE A RADWARE PRODUCT WITH THE PRODUCT OF A THIRD PARTY (COLLECTIVELY, "CONNECTORS") FOR PROVISIONING, DECOMMISSIONING, MANAGING, CONFIGURING OR MONITORING RADWARE PRODUCTS. THE APPLICABILITY OF THIS LICENSE AGREEMENT TO CONNECTORS IS REGARDLESS OF WHETHER SUCH CONNECTORS ARE DISTRIBUTED TO YOU BY RADWARE OR BY A THIRD PARTY PRODUCT VENDOR. IN CASE A CONNECTOR IS DISTRIBUTED TO YOU BY A THIRD PARTY PRODUCT VENDOR PURSUANT TO THE TERMS OF AN AGREEMENT BETWEEN YOU AND THE THIRD PARTY PRODUCT VENDOR, THEN, AS BETWEEN RADWARE AND YOURSELF, TO THE EXTENT THERE IS ANY DISCREPANCY OR INCONSISTENCY BETWEEN THE TERMS OF THIS LICENSE AGREEMENT AND THE TERMS OF THE AGREEMENT BETWEEN YOU AND THE THIRD PARTY PRODUCT VENDOR, THE TERMS OF THIS LICENSE AGREEMENT WILL GOVERN AND PREVAIL. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE CONTAINING RADWARE'S PRODUCT, OR BEFORE DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING RADWARE'S STANDALONE SOFTWARE (AS APPLICABLE). THE SOFTWARE IS LICENSED (NOT SOLD). BY OPENING THE PACKAGE CONTAINING RADWARE'S PRODUCT, OR BY DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE (AS APPLICABLE), YOU CONFIRM THAT YOU HAVE READ AND UNDERSTAND THIS LICENSE AGREEMENT AND YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT. FURTHERMORE, YOU HEREBY WAIVE ANY CLAIM OR RIGHT THAT YOU MAY HAVE TO ASSERT THAT YOUR ACCEPTANCE AS STATED HEREINABOVE IS NOT THE EQUIVALENT OF, OR DEEMED AS, A VALID SIGNATURE TO THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE UNOPENED PRODUCT PACKAGE OR YOU SHOULD NOT DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE (AS APPLICABLE). THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND RADWARE, AND SUPERSEDES ANY AND ALL PRIOR PROPOSALS, REPRESENTATIONS, OR UNDERSTANDINGS BETWEEN THE PARTIES. "YOU" MEANS THE NATURAL PERSON OR THE ENTITY THAT IS AGREEING TO BE BOUND BY THIS LICENSE AGREEMENT, THEIR EMPLOYEES AND THIRD PARTY CONTRACTORS. YOU SHALL BE LIABLE FOR ANY FAILURE BY SUCH EMPLOYEES AND THIRD PARTY CONTRACTORS TO COMPLY WITH THE TERMS OF THIS LICENSE AGREEMENT.

1. **License Grant.** Subject to the terms of this Agreement, Radware hereby grants to you, and you accept, a limited, nonexclusive, nontransferable license to install and use the Software in machine-readable, object code form only and solely for your internal business purposes ("Commercial License"). If the Software is distributed to you with a software development kit (the "SDK"), then, solely with regard to the SDK, the Commercial License above also includes a limited, nonexclusive, nontransferable license to install and use the SDK solely on computers within your organization, and solely for your internal development of an integration or interoperation of the Software and/or other Radware Products with software or hardware products owned, licensed and/or controlled by you (the "SDK Purpose"). To the extent an SDK is

distributed to you together with code samples in source code format (the "Code Samples")that are meant to illustrate and teach you how to configure, monitor and/or control the Software and/or any other Radware Products, the Commercial License above further includes a limited, nonexclusive, nontransferable license to copy and modify the Code Samples and create derivative works based thereon solely for the SDK Purpose and solely on computers within your organization. The SDK shall be considered part of the term "Software" for all purposes of this License Agreement. You agree that you will not sell, assign, license, sublicense, transfer, pledge, lease, rent or share your rights under this License Agreement nor will you distribute copies of the Software or any parts thereof. Rights not specifically granted herein, are specifically prohibited.

2. **Evaluation Use**. Notwithstanding anything to the contrary in this License Agreement, if the Software is provided to you for evaluation purposes, as indicated in your purchase order or sales receipt, on the website from which you download the Software, as inferred from any time- limited evaluation license keys that you are provided with to activate the Software, or otherwise, then You may use the Software only for internal evaluation purposes ("Evaluation Use") for a maximum of 30 days or such other duration as may specified by Radware in writing at its sole discretion (the "Evaluation Period"). The evaluation copy of the Software contains a feature that will automatically disable it after expiration of the Evaluation Period. You agree not to disable, destroy, or remove this feature of the Software, and any attempt to do so will be a material breach of this License Agreement. During or at the end of the evaluation period, you may contact Radware sales team to purchase a Commercial License to continue using the Software pursuant to the terms of this License Agreement. If you elect not to purchase a Commercial License, you agree to stop using the Software and to delete the evaluation copy received hereunder from all computers under your possession or control at the end of the Evaluation Period. In any event, your continued use of the Software beyond the Evaluation Period (if possible) shall be deemed your acceptance of a Commercial License to the Software pursuant to the terms of this License Agreement, and you agree to pay Radware any amounts due for any applicable license fees at Radware's then-current list prices.

3. **Lab/Development License**. Notwithstanding anything to the contrary in this License Agreement, if the Software is provided to you for use in your lab or for development purposes, as indicated in your purchase order, sales receipt, the part number description for the Software, the Web page from which you download the Software, or otherwise, then You may use the Software only in your lab and only in connection with Radware Products that you purchased or will purchase (in case of a lab license) or for internal testing and development purposes (in case of a development license) but not for any production use purposes.

4. **Subscription Software**. If you licensed the Software on a subscription basis, your rights to use the Software are limited to the subscription period. You have the option to extend your subscription. If you extend your subscription, you may continue using the Software until the end of your extended subscription period. If you do not extend your subscription, after the expiration of your subscription, you are legally obligated to discontinue your use of the Software and completely remove the Software from your system.

5. **Feedback**. Any feedback concerning the Software including, without limitation, identifying potential errors and improvements, recommended changes or suggestions ("**Feedback**"), provided by you to Radware will be owned exclusively by Radware and considered Radware's confidential information. By providing Feedback to Radware, you hereby assign to Radware all of your right, title and interest in any such Feedback, including all intellectual property rights therein. With regard to any rights in such Feedback that cannot, under applicable law, be assigned to Radware, you hereby irrevocably waives such rights in favor of Radware and grants Radware under such rights in the Feedback, a worldwide, perpetual royalty-free, irrevocable, sub-licensable and non-exclusive license, to use, reproduce, disclose, sublicense, modify, make, have made, distribute, sell, offer for sale, display, perform, create derivative works of and otherwise exploit the Feedback without restriction. The provisions of this Section 5 will survive the termination or expiration of this Agreement.

6. **Limitations on Use**. You agree that you will not: (a) copy, modify, translate, adapt or create any derivative works based on the Software; or (b) sublicense or transfer the Software, or include the Software or any portion thereof in any product; or (b) reverse assemble, disassemble, decompile,

reverse engineer or otherwise attempt to derive source code (orthe

underlying ideas, algorithms, structure or organization) from the Software, in whole or in part, except and only to the extent: (i) applicable law expressly permits any such action despite this limitation, in which case you agree to provide Radware at least ninety (90) days advance written notice of your belief that such action is warranted and permitted and to provide Radware with an opportunity to evaluate if the law's requirements necessitate such action, or (ii) required to debug changes to any third party LGPL-libraries linked to by the Software; or (c) create, develop, license, install, use, or deploy any software or services to circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Software;
(d) in the event the Software is provided as an embedded or bundled component of another Radware Product, you shall not use the Software other than as part of the combined Product and for the purposes for which the combined Product is intended; (e) remove any copyright notices, identification or any other proprietary notices from the Software (including any notices of Third Party Software (as defined below); or (f) copy the Software onto any public or distributed network or use the Software to operate in or as a time-sharing, outsourcing, service bureau, application service provider, or managed service provider environment. Notwithstanding the foregoing, if you provide hosting or cloud computing services to your customers, you are entitled to use and include the Software in your IT infrastructure on which you provide your services. Lastly, if you acquire Software under Radware's Global Elastic License (GEL) model, you commit to use any such Software only as an Alteon VA on COTS server or on GEL-dedicated hardware platforms as indicated in the part description of such hardware (be it hardware originally purchased as GEL-dedicated or later upgraded to be GEL-dedicated). Use of Software under a GEL model on a non-GEL-dedicated hardware platform is prohibited. If you deploy GEL model Software on a virtual platform, you can do so without the virtual platform being GEL-dedicated. It is hereby clarified that the prohibitions on modifying, or creating derivative works based on, any Software provided by Radware, apply whether the Software is provided in a machine or in a human readable form. Human readable Software to which this prohibition applies includes (without limitation) “Radware AppShape++ Script Files” that contain “Special License Terms”. It is acknowledged that examples provided in a human readable form may be modified by a user.

7. **Intellectual Property Rights**. You acknowledge and agree that this License Agreement does not convey to you any interest in the Software except for the limited right to use the Software, and that all right, title, and interest in and to the Software, including any and all associated intellectual property rights, are and shall remain with Radware or its third party licensors. You further acknowledge and agree that the Software is a proprietary product of Radware and/or its licensors and is protected under applicable copyright law.

8. **No Warranty**. The Software, and any and all accompanying software, files, libraries, data and materials, are distributed and provided “AS IS” by Radware or by its third party licensors (as applicable) and with no warranty of any kind, whether express or implied, including, without limitation, any non-infringement warranty or warranty of merchantability or fitness for a particular purpose. Neither Radware nor any of its affiliates or licensors warrants, guarantees, or makes any representation regarding the title in the Software, the use of, or the results of the use of the Software. Neither Radware nor any of its affiliates or licensors warrants that the operation of the Software will be uninterrupted or error-free, or that the use of any passwords, license keys and/or encryption features will be effective in preventing the unintentional disclosure of information contained in any file. You acknowledge that good data processing procedure dictates that any program, including the Software, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of the Software covered by this License. Radware does not make any representation or warranty, nor does Radware assume any responsibility or liability or provide any license or technical maintenance and support for any operating systems, databases, migration tools or any other software component provided by a third party supplier and with which the Software is meant to interoperate.

   This disclaimer of warranty constitutes an essential and material part of this License.

   In the event that, notwithstanding the disclaimer of warranty above, Radware is held liable under any warranty provision, Radware shall be released from all such obligations in the event that the Software shall have been subject to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than by Radware's authorized service personnel.

9. **Limitation of Liability**. Except to the extent expressly prohibited by applicable statutes, in no event shall Radware, or its principals, shareholders, officers, employees, affiliates, licensors, contractors, subsidiaries, or parent organizations (together, the "Radware Parties"), be liable for any direct, indirect, incidental, consequential, special, or punitive damages whatsoever relating to the use of, or the inability to use, the Software, or to your relationship with, Radware or any of the Radware Parties (including, without limitation, loss or disclosure of data or information, and/or loss of profit, revenue, business opportunity or business advantage, and/or business interruption), whether based upon a claim or action of contract, warranty, negligence, strict liability, contribution, indemnity, or any other legal theory or cause of action, even if advised of the possibility of such damages. If any Radware Party is found to be liable to You or to any third- party under any applicable law despite the explicit disclaimers and limitations under these terms, then any liability of such Radware Party, will be limited exclusively to refund of any license or registration or subscription fees paid by you to Radware.

10. **Third Party Software**. The Software includes software portions developed and owned by third parties (the "Third Party Software"). Third Party Software shall be deemed part of the Software for all intents and purposes of this License Agreement; provided, however, that in the event that a Third Party Software is a software for which the source code is made available under an open source software license agreement, then, to the extent there is any discrepancy or inconsistency between the terms of this License Agreement and the terms of any such open source license agreement (including, for example, license rights in the open source license agreement that are broader than the license rights set forth in Section 1 above and/or no limitation in the open source license agreement on the actions set forth in Section 6 above), the terms of any such open source license agreement will govern and prevail. The terms of open source license agreements and copyright notices under which Third Party Software is being licensed to Radware or a link thereto, are included with the Software documentation or in the header or readme files of the Software. Third Party licensors and suppliers retain all right, title and interest in and to the Third Party Software and all copies thereof, including all copyright and other intellectual property associated therewith. In addition to the use limitations applicable to Third Party Software pursuant to Section 6 above, you agree and undertake not to use the Third Party Software as a general SQL server, as a stand-alone application or with applications other than the Software under this License Agreement.

11. **Term and Termination**. This License Agreement is effective upon the first to occur of your opening the package of the Product, purchasing, downloading, installing, copying or using the Software or any portion thereof, and shall continue until terminated. However, sections 5-15 shall survive any termination of this License Agreement. The Licenses granted under this License Agreement are not transferable and will terminate upon: (i) termination of this License Agreement, or (ii) transfer of the Software, or (iii) in the event the Software is provided as an embedded or bundled component of another Radware Product, when the Software is unbundled from such Product or otherwise used other than as part of such Product. If the Software is licensed on subscription basis, this Agreement will automatically terminate upon the termination of your subscription period if it is not extended.

12. **Export**. The Software or any part thereof may be subject to export or import controls under applicable export/import control laws and regulations including such laws and regulations of the United States and/or Israel. You agree to comply with such laws and regulations, and, agree not to knowingly export, re-export, import or re-import, or transfer products without firstobtaining all required Government authorizations or licenses therefor. Furthermore, You hereby covenant and agree to ensure that your use of the Software is in compliance with all other foreign, federal, state, and local laws and regulations, including without limitation all laws and regulations relating to privacy rights, and data protection. You shall have in place a privacy policy and obtain all of the permissions, authorizations and consents required by applicable law for use of cookies and processing of users' data (including without limitation pursuant to Directives 95/46/EC, 2002/58/EC and 2009/136/EC of the EU if applicable) for the purpose of provision of any services.

13. **US Government**. To the extent you are the U.S. government or any agency or instrumentality thereof, you acknowledge and agree that the Software is a "commercial computer software" and "commercial computer software documentation" pursuant to applicable regulations and your use of the Software is subject to the terms of this License Agreement.

14. **Federal Acquisition Regulation (FAR)/Data Rights Notice**. Radware's commercial computer software is created solely at private expense and is subject to Radware's commercial license rights.
15. **Governing Law**. This License Agreement shall be construed and governed in accordancewith the laws of the State of Israel.
16. **Miscellaneous**. If a judicial determination is made that any of the provisions contained in this License Agreement is unreasonable, illegal or otherwise unenforceable, such provision or provisions shall be rendered void or invalid only to the extent that such judicial determination finds such provisions to be unreasonable, illegal or otherwise unenforceable, and the remainder of this License Agreement shall remain operative and in full force and effect. In any event a party breaches or threatens to commit a breach of this License Agreement, the other party will, in addition to any other remedies available to, be entitled to injunction relief. This License Agreement constitutes the entire agreement between the parties hereto and supersedes all prior agreements between the parties hereto with respect to the subject matter hereof. The failure of any party hereto to require the performance of any provisions of this License Agreement shall in no manner affect the right to enforce the same. No waiver by any party hereto of any provisions or of any breach of any provisions of this License Agreement shall be deemed or construed either as a further or continuing waiver of any such provisions or breach waiver or as a waiver of any other provision or breach of any other provision of this License Agreement.

IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE YOU MUST REMOVE THE SOFTWARE FROM ANY DEVICE OWNED BY YOU AND IMMEDIATELY CEASE USING THE SOFTWARE.