



Radware DefensePro DDoS Mitigation User Guide

Software Version 8.13.01

Last Updated: September, 2017



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. 2017. 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. 2017. 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 Einschränkungen ausgeliefert:

Copyright Radware Ltd. 2017. Alle Rechte vorbehalten.

Das Urheberrecht und alle anderen in diesem Handbuch enthaltenen Eigentumsrechte und 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 the following 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 adhered 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 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 the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (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 Rijndael 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 dans tout 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 utilisés pour 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 Aaron Campbell.

Ce produit inclut un logiciel développé par Damien Miller.

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 Wesley Griffin. Ce

produit inclut un logiciel développé par Per Allansson. Ce

produit inclut un logiciel développé par Nils Nordman. 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 dans tout 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 enthaltenen 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) lizenziert 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 ohne ausdrückliche 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 VORGENANNTEN 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 Garantienzeitraumes 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 JEDLICHE 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) JEDLICHE 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

CAUTION	ATTENTION
This unit has more than one power supply. Disconnect all power supplies before maintenance to avoid electric shock.	Cette unité a plus d'une source d'alimentation électrique. Débranchez toutes les sources d'alimentations électriques avant toute maintenance pour éviter les chocs électriques.

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

本设备有两个电源供电，未避免电击危险，操作时需要加倍小心。
只有当这两个电源完全断开时才可以安全操作

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 this device 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 61000-4-11 For 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 60825-1:1993 + 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

CAUTION	ATTENTION
<p>This unit has more than one power supply. Disconnect all power supplies before maintenance to avoid electric shock.</p>	<p>Cette unité a plus d'une source d'alimentation électrique. Débranchez toutes les sources d'alimentations électriques avant toute maintenance pour éviter les chocs électriques.</p>

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 dotés de deux sources d'alimentation électrique (en chinois)

本设备有两个电源供电，未避免电击危险，操作时需要加倍小心。
只有当这两个电源完全断开时才可以安全操作

Traduction de la [Avertissement de sécurité pour les systèmes dotés 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 batterie ou 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'unité ne peut être remplacée ou réparée.
3. NE branchez pas, n'allumez pas ou n'essayez pas d'utiliser une unité manifestement 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 dépasse la valeur maximale autorisée. 40°C/104°F.
7. Débranchez le cordon électrique de la prise murale AVANT d'essayer de retirer et/ou de vérifier le fusible d'alimentation principal.

PRODUIT LASER DE CLASSE 1 ET RÉFÉRENCE AUX NORMES LASER LES PLUS RÉCENTES: IEC 60825-1: 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 on liitettävä suojavaadoituskoskettimilla varustettuun pistorasiaan
- Norvège (Étiquette et inscription dans le manuel) - Apparatet må tilkoples jordet stikkontakt
- L'unité peut être connectée à un système électrique IT (en Norvège uniquement).
- Suède (Étiquette et inscription dans le manuel) - Apparatens skall anslutas till jordat uttag.

Pour brancher à l'alimentation électrique:

1. Branchez le câble d'alimentation à la prise principale, située sur le panneau arrière de l'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 remplacé 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

CAUTION	ATTENTION
This unit has more than one power supply. Disconnect all power supplies before maintenance to avoid electric shock.	Cette unité a plus d'une source d'alimentation électrique. Débranchez toutes les sources d'alimentations électriques avant toute maintenance pour éviter les chocs électriques.

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

本设备有两个电源供电，未避免电击危险，操作时需要加倍小心。
只有当这两个电源完全断开时才可以安全操作

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 to 4-6, 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 Ethernetmüssen 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 Lithiumbatterien 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 Erdungsleitung verwenden!"
- 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 jordat uttag.

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 Wechselstromanschluss an.

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 Leitung des Gleichstromkreises und dem Erdungsleiter des Gerätes zu ermöglichen. Siehe Montageanleitung.
2. Wartungsarbeiten jeglicher Art dürfen nur von qualifiziertem Servicepersonal ausgeführt 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 Gerätes NICHT 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 Sie die 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 61000-4-11 For 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 équipements 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' à la maison.

BSMI

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

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 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 to 4-6, 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

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

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， T_{ma} ：为制造商规范允许的最大环境温度，或者为 $25^{\circ}C$ ，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	10
Safety Instructions	11
Electromagnetic-Interference Statements.....	20
Altitude and Climate Warning.....	24
Document Conventions.....	25
Chapter 1 – Introduction.....	33
Radware DefensePro DDoS Mitigation—Overview	33
Radware DefensePro DDoS Mitigation System Components	34
Typical Deployment	34
Network Connectivity	35
Management Interfaces—APSolute Vision and Others.....	35
Radware DefensePro DDoS Mitigation Features	36
Security Protections	36
Inspection of Tunneled Traffic	37
Real-time Security Reporting for DefensePro	37
Historical Security Reporting—APSolute Vision Reporter	38
Related Documentation	38
Radware DefensePro DDoS Mitigation Release Notes	38
APSolute Vision Documentation	38
APSolute Vision Reporter Documentation	39
Chapter 2 – Getting Started	41
Logging In to APSolute Vision.....	41
Changing the Password for Local APSolute Vision Users	42
APSolute Vision User Interface Overview	43
APSolute Vision Toolbar	44
APSolute Vision Settings View	45
Device Pane.....	47
Device-Properties Pane	49
Configuration Perspective	50
Monitoring Perspective	51
Security Monitoring Perspective.....	52
Selecting Your Landing Page.....	53

Using Common GUI Elements in APSolute Vision	54
Icons/Buttons and Commands for Managing Table Entries.....	54
Filtering Table Rows.....	55
Managing Radware DefensePro DDoS Mitigation Devices and APSolute Vision Sites and Logical Groups	55
Using the Device Pane	56
Managing Individual DefensePro Devices in APSolute Vision	58
APSolute Vision Server Registered for Device Events—DefensePro.....	64
Locking and Unlocking Devices	64
Using the Multi-Device View and the Multiple Devices Summary	66
Using Logical Groups of Devices	69
After You Set Up Your Managed Devices.....	73
Chapter 3 – Managing the DefensePro Setup.....	75
Configuring the DefensePro Global Parameters	75
Viewing and Configuring Basic Global Parameters.....	75
Managing Certificates.....	76
Upgrading Licenses for DefensePro Devices.....	81
Configuring Date and Time Settings in DefensePro	83
Configuring the DefensePro Networking Setup	84
Configuring the Basic Parameters of the DefensePro Networking Setup	84
Configuring IP Interface Management in the Networking Setup.....	85
Configuring DNS for the DefensePro Networking Setup.....	88
Configuring the DefensePro Device-Security Setup.....	89
Configuring Access Protocols for the DefensePro Device-Security Setup.....	89
Configuring Advanced Parameters in the DefensePro Device-Security Setup	91
Configuring SNMP in the DefensePro Device-Security Setup	93
Configuring Device Users in the DefensePro Device-Security Setup	103
Configuring the DefensePro Security-Settings Setup.....	104
Configuring Global Signature Protection	104
Configuring Global DoS Shield Protection	105
Configuring Global Behavioral DoS Protection.....	107
Configuring Global SYN Flood Protection.....	111
Configuring Global Out-of-State Protection.....	112
Configuring Global Packet Anomaly Protection	115
Configuring Global DNS Flood Protection	118
Configuring the DefensePro Advanced-Parameters Setup	123
Configuring Authentication Tables Settings	123
Configuring DefensePro Session Table Settings	124
Configuring the DefensePro Reporting-Settings Setup	126
Configuring DefensePro Syslog Settings	126
Enabling Configuration Auditing on the DefensePro Device.....	127
Configuring Security Reporting Settings.....	127
Configuring the Radware DefensePro DDoS Mitigation Clustering Setup	130

Chapter 4 – Managing Classes	133
Managing Network Classes	133
Managing Context Group Classes.....	134
Managing Application Classes	135
Managing MAC Address Classes.....	136
Managing SGT Classes	137
Chapter 5 – Managing DefensePro Network Protection Policies	139
Configuring Network Protection Policies.....	140
Configuring Signature Protection for Network Protection.....	144
Signature Protection in DefensePro	144
Configuration Considerations with Signature Protection	145
Configuring Signature Protection Profiles	146
Managing Signature Protection Signatures.....	148
Managing Signature Protection Filters	158
Configuring Signature Protection Attributes	161
Viewing and Modifying Attribute Type Properties	163
Configuring BDoS Profiles for Network Protection.....	164
Configuring Connection Limit Profiles for Network Protection	167
Configuring Connection Limit Protections	169
Configuring SYN Protection Profiles for Network Protection	170
Defining SYN Flood Protections	171
Managing SYN Protection Profile Parameters.....	173
Configuring DNS Protection Profiles for Network Protection.....	177
Configuring Out of State Protection Profiles for Network Protection	181
Chapter 6 – Managing DefensePro Operations and Maintenance	183
Updating Policy Configurations on a DefensePro Device	183
Rebooting or Shutting Down a DefensePro Device	184
Using Configuration Templates for Security Policies	184
Configuring Multiple Devices	191
Downloading a Device’s Log File to APSolute Vision	193
Updating a Radware Signature File.....	193
Downloading Technical-Support and Configuration Files.....	195
Downloading a Technical Support File Using APSolute Vision	195
Downloading a Technical Support File Using CLI.....	195
Managing DefensePro Device Configurations	196
DefensePro Configuration File Content.....	196
Downloading a Device-Configuration File.....	196
Restoring a Device Configuration	197
Resetting the Baseline for DefensePro.....	198

Scheduling APSolute Vision and Device Tasks.....	199
Overview of Scheduling	199
Configuring Tasks in the Scheduler	200
Task Parameters	202
Updating the Attack Description File.....	212
Chapter 7 – Monitoring and Controlling the DefensePro Operational Status.	215
Monitoring the General DefensePro Device Information	215
Monitoring and Controlling DefensePro Ports and Trunks.....	216
Monitoring DefensePro Resource Utilization.....	218
Monitoring DefensePro CPU Utilization.....	218
Monitoring and Clearing DefensePro Authentication Tables	219
Monitoring DME Utilization According to Configured Policies	220
Monitoring DefensePro Syslog Information	220
Monitoring Security Group Tags (SGTs).....	220
Chapter 8 – Monitoring DefensePro Clustering.....	221
Chapter 9 – Monitoring DefensePro Statistics.....	223
Monitoring DefensePro SNMP Statistics.....	223
Monitoring DefensePro IP Statistics.....	224
Chapter 10 – Monitoring and Controlling DefensePro Networking	227
Monitoring and Controlling the DefensePro Session Table.....	227
Monitoring Session Table Information.....	227
Monitoring Routing Table Information	228
Monitoring DefensePro ARP Table Information	228
Chapter 11 – Using Real-Time Security Monitoring.....	231
Risk Levels	231
Using the Dashboard Views for Real-Time Security Monitoring	232
Configuring the Display Parameters of a Dashboard View.....	233
Using the Current Attacks Table	234
Using the Ongoing Attacks Monitor	239
Attack Details	240
Sampled Data Tab	248
Viewing Real-Time Traffic Reports.....	249
Viewing the Traffic Utilization Report	249
Viewing the Connection Rate Report	252
Viewing the Concurrent Connections Report	254
Viewing the Top Queried Domain Names Report	255

Protection Monitoring	257
Displaying Attack Status Information	257
Monitoring the Traffic Under BDoS Protection.....	257
Monitoring the Traffic Under DNS Flood Protection	260
HTTP Reports.....	264
Monitoring Continuous Learning Statistics.....	264
Monitoring Hour-Specific Learning Statistics.....	264
HTTP Request Size Distribution	264
Alerts for New Security Attacks	264
Chapter 12 – Administering Radware DefensePro DDoS Mitigation	267
Command Line Interface	267
CLI Command Restrictions	268
CLI Session Time-Out	268
CLI Capabilities	269
CLI Traps.....	269
Send Traps To All CLI Users	270
Web Services.....	270
API Structure	270
APSolute API Software Development Kit (SDK).....	271
Appendix A – Footprint Bypass Fields and Values	273
BDoS Footprint Bypass Fields and Values	274
DNS Footprint Bypass Fields and Values.....	281
Appendix B – Predefined Basic Filters.....	283
Appendix C – DefensePro Attack-Protection IDs.....	293
Appendix D – Protocols Supported by DefensePro	307
Appendix E – Troubleshooting	309
Technical Support File	309
Appendix F – Glossary.....	311
Radware Ltd. End User License Agreement.....	319

Chapter 1 – Introduction

This guide describes Radware DefensePro DDoS Mitigation version 8.13 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 performed using APSolute Vision™ version 3.90.

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—Overview, page 33](#)
- [Radware DefensePro DDoS Mitigation System Components, page 34](#)
- [Typical Deployment, page 34](#)
- [Network Connectivity, page 35](#)
- [Management Interfaces—APSolute Vision and Others, page 35](#)
- [Radware DefensePro DDoS Mitigation Features, page 36](#)
- [Related Documentation, page 38](#)

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-service attacks.

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 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.

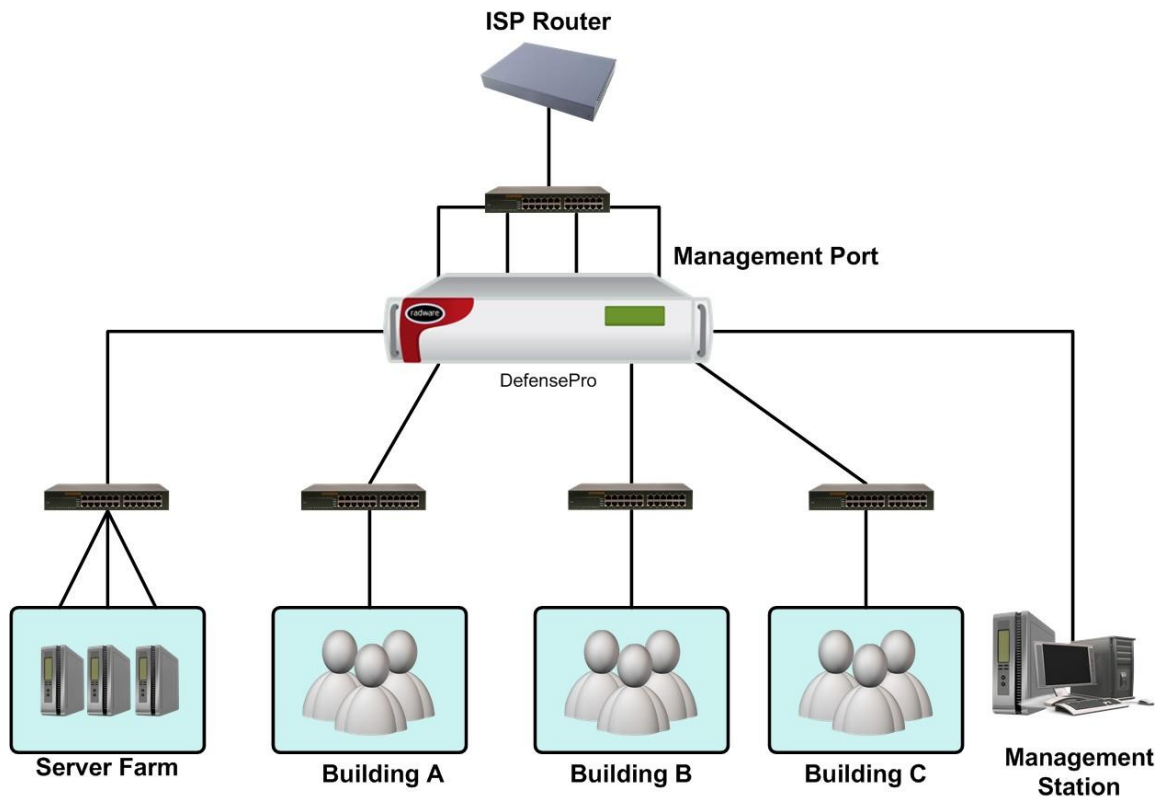
Typical Deployment

The following illustration shows an in-line installation of Radware DefensePro DDoS Mitigation in an enterprise. In this deployment, Radware DefensePro DDoS Mitigation is located at the gateway, protecting hosts, servers, and network resources against incoming network attacks. Radware DefensePro DDoS Mitigation also protects DMZ servers against attacks targeting Web, e-mail, VoIP and other services. This Radware deployment is at the enterprise gateway, in front of the DMZ servers, where Radware DefensePro DDoS Mitigation provides perimeter protection for the enterprise servers, users, routers and firewalls.

Network Connectivity

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

Figure 19: Typical Network Connectivity



Management Interfaces—APSSolute Vision and Others

APSSolute 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 APSSolute Vision.

APSSolute 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 36](#)
- [Inspection of Tunneled Traffic, page 37](#)
- [Real-time Security Reporting for DefensePro, page 37](#)
- [Historical Security Reporting—APSolute Vision Reporter, page 38](#)

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 DefensePro 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 using the global security settings and Network Protection policy. 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

- Unless specifically noted, the procedures to configure security policies in this book relate to using APSolute Vision.
- Some protections are not supported on management interfaces.

DefensePro'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:

- **Behavioral DoS (BDoS) Protection**—Protects against zero-day flood attacks, including SYN Floods, TCP Floods, UDP floods, ICMP and IGMP floods.
- **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 Protection as a Network Protection to allow easier protection of multiple network elements.
- **DNS 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 DefensePro 8.x versions 8.13 and later, the DNS 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.

- **Signature-based Protection**—Protects against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. Signature-based Protection includes DoS Shield protection, which protects against known flood attacks and flood attack tools that cause a denial-of-service effect.
- **Packet-Anomaly Protection.**
- **Out-of-State Protection**—Ensures that TCP connections are established based on the protocol RFCs.
- **Connection Limit Protection**—Protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks.

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.

Tunneling implies that traffic routing is based on source and destination IP addresses. When tunneling is used, IPS devices and load balancers cannot locate the relevant information because their decisions are based on information located inside the IP packet in 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.

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

Radware DefensePro DDoS Mitigation always bypasses (passes-through) IPsec traffic.

Real-time Security Reporting for DefensePro

APolute 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.

Radware DefensePro DDoS Mitigation's security monitoring enables you to analyze real-time and historical attacks.

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 the APSolute Vision Reporter 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

Related Documentation

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

- [Radware DefensePro DDoS Mitigation Release Notes, page 38](#)
- [APSolute Vision Documentation, page 38](#)
- [APSolute Vision Reporter Documentation, page 39](#)



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 the relevant 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—which 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.
 - **APSolute Vision online help**—See this for information about monitoring managed 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.

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 41](#)
- [Changing the Password for Local APSolute Vision Users, page 42](#)
- [APSolute Vision User Interface Overview, page 43](#)
- [Selecting Your Landing Page, page 53](#)
- [Using Common GUI Elements in APSolute Vision, page 54](#)
- [Managing Radware DefensePro DDoS Mitigation Devices and APSolute Vision Sites and Logical Groups, page 55](#)

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 a **vision-activation** prefix). When APSolute Vision is running as a virtual appliance (VA) or on an OnDemand Switch VL (ODS-VL) platform, the 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 license is based on the MAC address of the APSolute Vision G3 or G5 port.



Note: The CLI command `net ip getdisplays` the ports and the MAC addresses.

You can request the license from Radware Technical Support. The license is also available using the license generator at radware.com.

Up to 50 concurrent 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 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 user name.
 - **Password**—Your user password. Depending on the configuration of the server, you may be required to change your password immediately. Default: radware.
 - The language of the APSolute Vision graphical user interface. Click the  (globe) icon to set the value.
3. Click **Log In**.

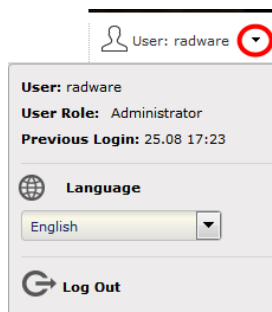


Caution: Radware recommends increasing the SNMP **Timeout** to 180 seconds (APSolute Vision Settings view System perspective, **General Settings > Connectivity > Timeout**).



To log out of APSolute Vision

1. In the APSolute Vision toolbar, in the **User** ribbon at the at the far right, click the arrow. 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, page 44](#)
- [APSolute Vision Settings View, page 45](#)
- [Device Pane, page 47](#)
- [Configuration Perspective, page 50](#)
- [Monitoring Perspective, page 51](#)
- [Security Monitoring Perspective, page 52](#)

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

The following figure shows the APSolute Vision toolbar.

Figure 20: APSolute Vision Toolbar



The the APSolute Vision toolbar contains the following items:


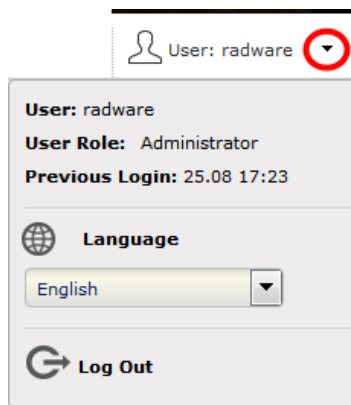

- **AVR button**—Opens the APSolute Vision Reporter, which is historical security reporting for DefensePro and AppWall.
- **APM button**—Opens Application Performance Monitoring for Alteon and LinkProof NG.
- **DPM button**—Opens Device Performance Monitoring for Alteon and LinkProof NG.
- **DefensePipe button**—Connects you to the associated DefensePipe interface. For more information on DefensePipe, see the DefensePipe User Guide.
- **vDirect button**—Opens the vDirect interface in the APSolute Vision server.
- **DefenseFlow button**—Opens the DefenseFlow interface (when the DefenseFlow IP address is configured in the APSolute Vision CLI).
- **Toolbox button**—Opens the Toolbox pane, which includes the Toolbox tab and the Advanced tab. By default, the Toolbox tab displays predefined Toolbox scripts. From the Advanced tab, you can manage Toolbox scripts, use AppShape templates, and manage DefensePro configuration templates.
- **Security Control Center button**—Opens the Security Control Center.
- **Scheduler button**—Opens the Scheduler to schedule various operations for the APSolute Vision server and managed devices.
- **APSolute Vision Settings button**—Opens the APSolute Vision Settings view.
- **Refresh button and last refresh time.**
- **User ribbon**—Clicking the arrow in the **User** ribbon, , opens the User drop-down dialog box. Use the User 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 21: User Dialog Box



APolute Vision Settings View

Click the  (APolute Vision Settings) button at the top of the main screen to open the APolute Vision Settings view.

The APolute Vision Settings view includes the following perspectives:

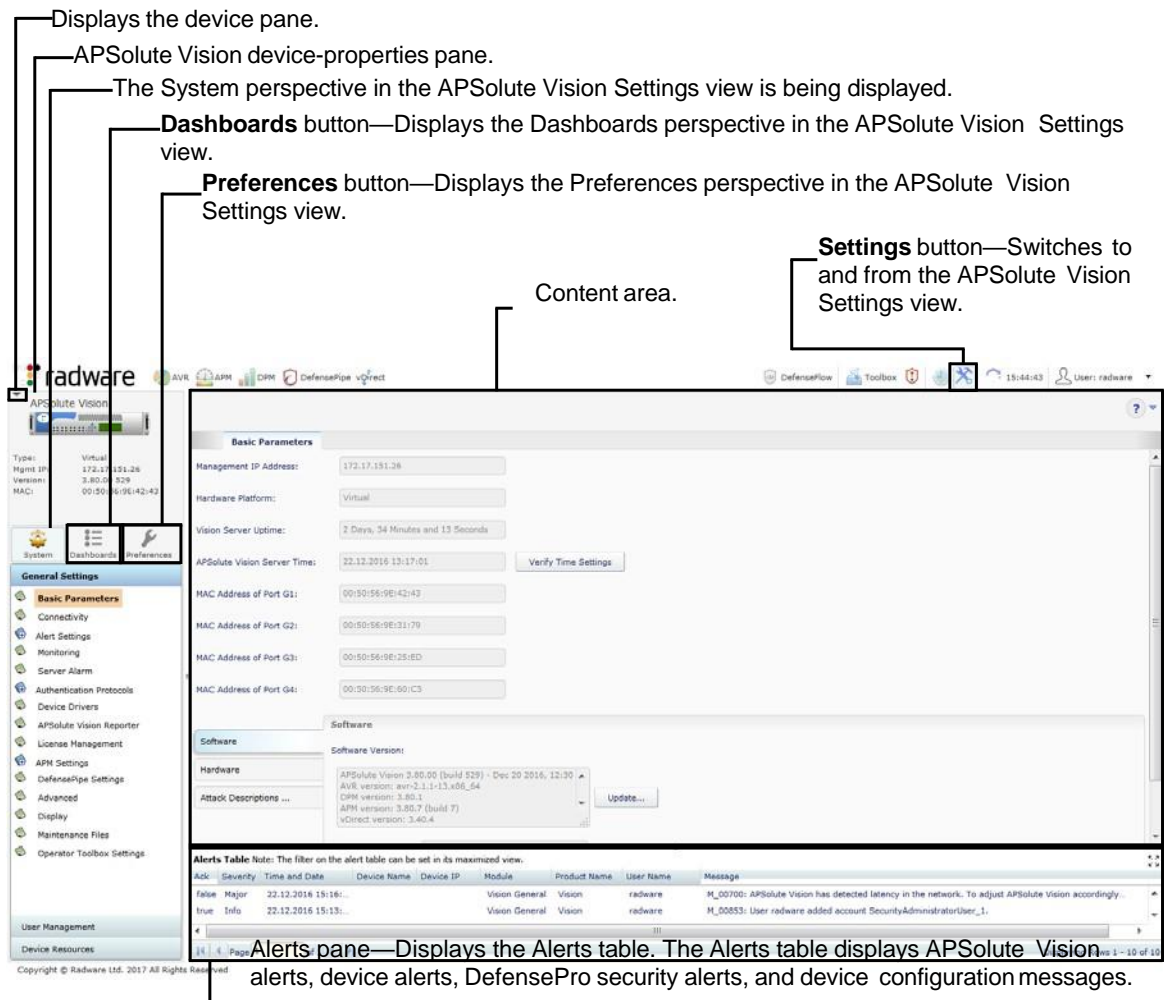
- **System**—For more information, see [Settings View—System Perspective, page 46](#). Access to the APolute Vision Settings view System perspective is restricted to administrators.
- **Dashboards**—For more information, see [Settings View—Dashboards Perspective, page 47](#).
- **Preferences**—For more information, see [Settings View—Preferences Perspective, page 47](#).

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

At the upper-left of the APolute Vision Settings view, APolute Vision displays the APolute Vision device-properties pane. For more information, see [Device-Properties Pane, page 49](#).

When you hover over a device node in the device pane, a popup displays. For more information, see [Device-Properties Hover Popup, page 49](#).

Figure 22: Settings View (Showing the System Perspective)



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 DefensePro
 - Licenses
 - Application Performance Monitoring (APM)

- DefensePipe URL
- 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

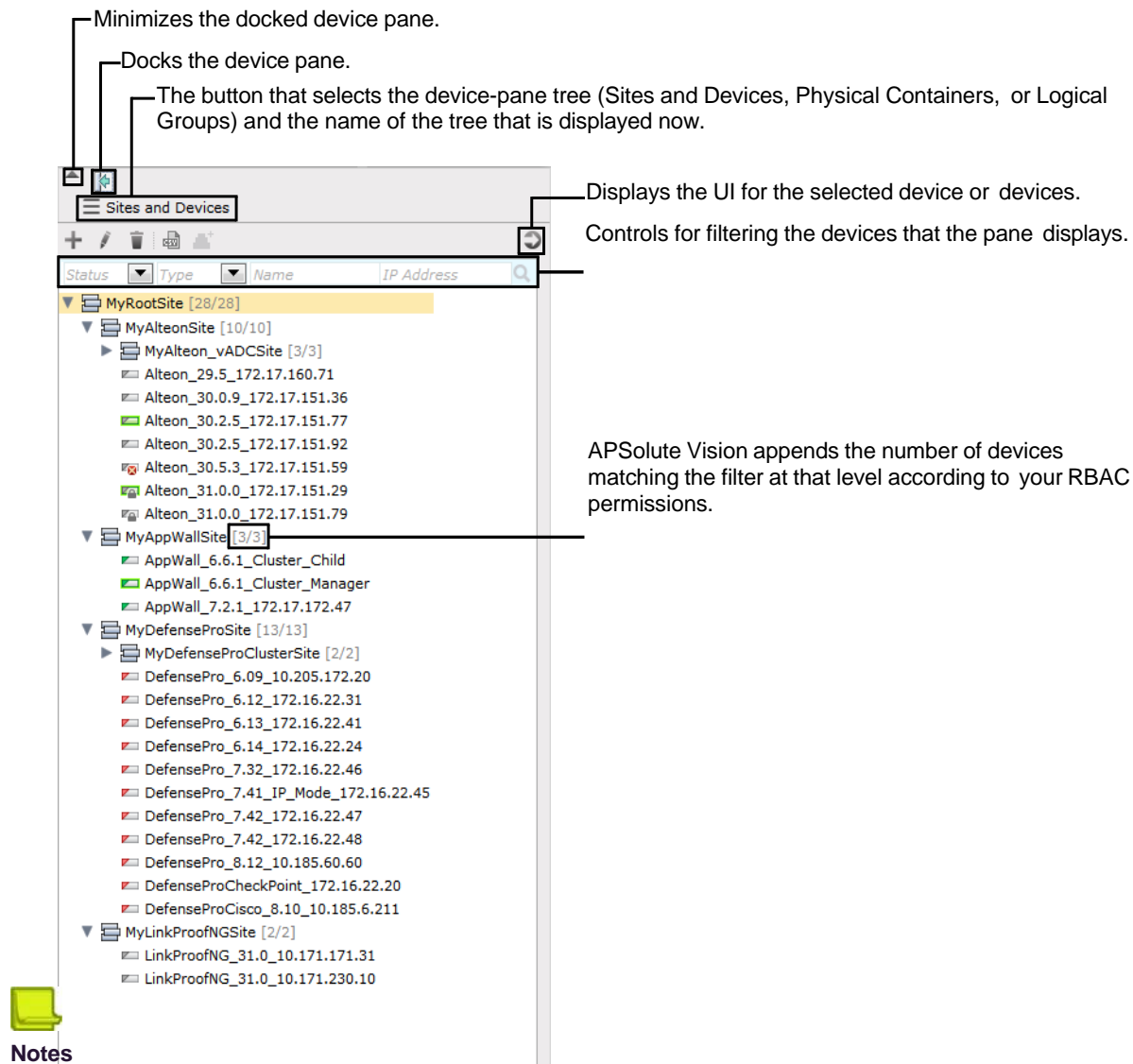
Users with a proper role can use the device pane to add or delete the Radware devices that the APSolute Vision server manages.

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 DefensePro.
- **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 23: Device Pane (Not Docked)— Showing the Sites and Devices Tree




- For information on how to add or delete the Radware devices that the APSSolute Vision server manages, see [Managing Radware DefensePro DDoS Mitigation Devices and APSSolute Vision Sites and Logical Groups, page 55](#).
- For more information on the device pane, see [Using the Device Pane, page 56](#).
- When you double-click a device in the Sites and Devices tree, APSSolute Vision displays the device-properties pane and the last perspective that you viewed on the device along with the 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 APSSolute Vision User Guide.
- For more information on Logical Groups, see, see [Using Logical Groups of Devices, page 69](#).

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, **DefensePro**.
- **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 driver name.
- **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 DefensePro.

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 70](#).

Device-Properties Pane

When you select a single device in the device pane, all APSolute Vision perspectives display the device-properties pane (see [Figure 22 - Settings View \(Showing the System Perspective\), page 46](#), [Figure 26 - Monitoring Perspective—DefensePro, page 51](#), [Figure 27 - Security Monitoring Perspective—Showing the Security Dashboard, page 52](#)).

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, DefensePro, 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.
- **Mngt IP**—The host or IP address of the devices.
- **Version**—The device version.
- **MAC**—The MAC address.
- **HA Status**—The high-availability status of the device: **Standalone**, **Primary**, or **Secondary**.

- **Device Driver**—The device 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 Radware devices. Choose the device to configure in the device pane.

You can view and modify device configurations in the content area.

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 APSolute Vision 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 the APSolute 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 orange background.

Figure 24: Update Policies Button

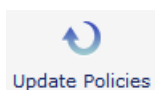





Figure 25: Update Policies Required Button





Example Device selection in the Configuration perspective

The following example shows the selections you would make to view or change configuration parameters for a Radware 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 26: Monitoring Perspective—DefensePro

Device pane (docked) with the Sites and Devices tree displayed—Displays, according to your filter, the configured Sites and DefensePro devices. The Physical Containers tree (not shown) is not relevant for DefensePro.

The Monitoring perspective is being displayed.

Device-properties pane.

DefensePro configuration-management buttons.

ACK	Severity	Time and Date	Device Name	Device IP	Module	Product Name	User Name	Message
true	Info	03.01.2017 16:01:			Vision General	Vision	radware	M_00853: User radware added account avil
true	Info	03.01.2017 16:00:			Vision General	Vision	radware	M_00863: Account radware successfully log

Alerts Table—Displays APSolute Vision alerts, device alerts, and DefensePro configuration messages.

Content pane.

Security Monitoring Perspective

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.

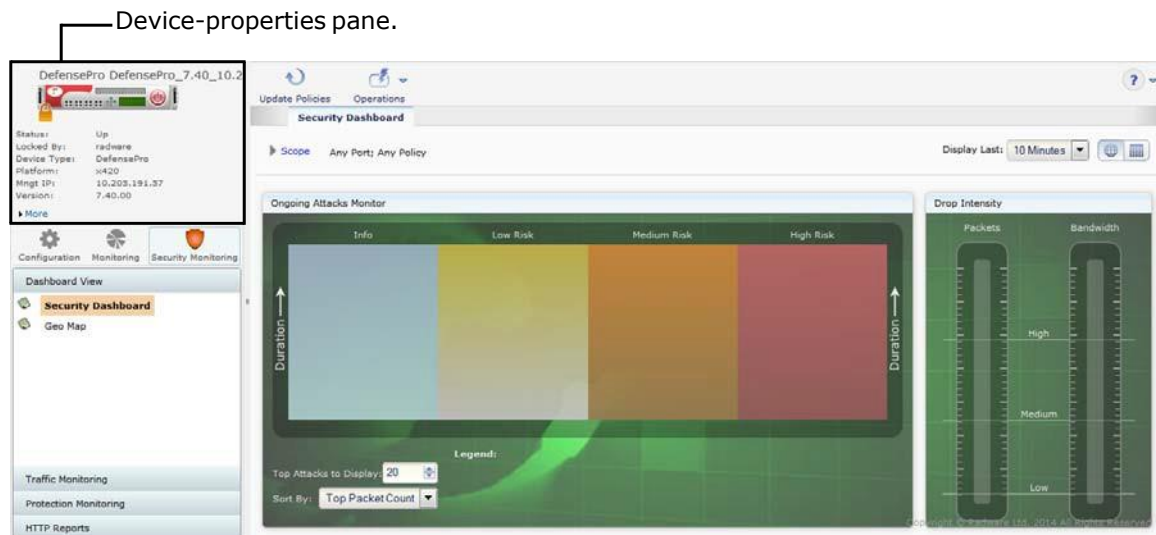
You can filter the Sites and devices that APSolute Vision displays. The filter does not change the contents of the tree, only how APSolute Vision displays the tree to you.

In the Security Monitoring perspective, you can access a collection of real-time security-monitoring tools that provide visibility regarding current attacks that the Radware DefensePro DDoS Mitigation device has detected. The Properties pane displays information about the currently selected device.

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 27: Security Monitoring Perspective—Showing the Security Dashboard



Note: For more information on the Security Monitoring perspective, see [Using Real-Time Security Monitoring, page 1](#).

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	<p>The page that APSolute Vision displays when you open APSolute Vision WBM.</p> <p>Values:</p> <ul style="list-style-type: none">• 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. <p>Default: None</p> <p>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.</p>

Using Common GUI Elements in APSolute Vision

This section contains the following:

- [Icons/Buttons and Commands for Managing Table Entries, page 54](#)
- [Filtering Table Rows, page 55](#)

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 mouse 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 22](#)).
- 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 according to 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 you enter **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 and 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.

The following topics describe how to set up your network of APSolute Vision Sites, Logical Groups and DefensePro devices:

- [Using the Device Pane, page 56](#)
- [Configuring Sites, page 56](#)
- [Managing Individual DefensePro Devices in APSolute Vision, page 58](#)
- [Locking and Unlocking Devices, page 64](#)
- [Using the Multi-Device View and the Multiple Devices Summary, page 66](#)
- [Using Logical Groups of Devices, page 69](#)
- [After You Set Up Your Managed Devices, page 73](#)



Note: To add DefensePro 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 56](#)
- [Icons for High Availability, page 56](#)
- [Configuring Sites, page 56](#)
- [Tree Nodes, page 58](#)
- [Exporting a CSV File with the Devices in the Sites and Devices Tree, page 58](#)
- [Filtering Entities in the Device Pane, page 58](#)




Note: For a picture of the device pane, see [Figure 23 - Device Pane \(Not Docked\)—Showing the Sites and Devices Tree, page 48](#).

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 DefensePro devices.
- **Physical Containers**—The Physical Containers tree is not relevant for DefensePro.
- **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 [Using Logical Groups of Devices, page 69](#).

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

Icons for High Availability

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 and devices.





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 parent Sites 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 node in 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 users locally, 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. For example, a Site called Alteon_Site appears before a Site at the same level called DefensePro_Site.

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 63](#).

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**, **DefensePro**, 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 DefensePro Devices in APSolute Vision

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

The number of Radware 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—DefensePro, page 64](#).

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 63](#).
- 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 DefensePro, APSolute Vision uses Transport Layer Security (TLS) protocol version 1.1 or later.



Caution: If a DefensePro 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 59](#). 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 59](#)
- [To delete a device, page 63](#)



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	<p>The name of the device.</p> <p>Notes:</p> <ul style="list-style-type: none"> • 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	<p>The management IP address as it is defined on the managed device.</p> <p>Note: Once you add the device to the APSolute Vision configuration, you cannot change its IP address.</p>
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 .)	<p>The username for the SNMP connection.</p> <p>Maximum characters: 18</p>
Use Authentication (This parameter is displayed only when SNMP Version is SNMPv3 .)	<p>Specifies whether the device authenticates the user for a successful connection.</p> <p>Default: Disabled</p>

Table 5: Device Properties: SNMP Parameters (cont.)

Parameter	Description
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 DefensePro supports only the DES privacy protocol. Value: DES Default: DES Caution: Do not choose AES128 . If you select AES128 , APSolute Vision will fail to connect to the device.
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: 18
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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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—DefensePro, page 64. <hr style="border: 0.5px solid blue; margin-top: 10px;"/>
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.

Table 8: Device Properties: Event Notification Parameters (cont.)

Parameter	Description
<p>Remove All Other Targets of Device Events</p> <p>(This parameter is available only when the Register This APSolute Vision Server for Device Events checkbox is selected.)</p>	<p>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.</p> <p>Default: Disabled</p> <p>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.</p>





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— DefensePro

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 device events 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.

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

When multiple APSolute Vision servers manage the same DefensePro 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 Radware device. While the device is locked:

- The device icon in the device pane includes a small lock symbol— for DefensePro.
- Configuration panes are displayed in read-only mode to other users with configuration 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 (using standard 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 (using standard 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 69](#).
- 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 DefensePro devices.
- **Use a Logical Group to configure the devices in it**—For information about configuring multiple devices simultaneously, see [Configuring Multiple Devices, page 191](#).
- **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 191](#).
- **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 231](#).

Figure 28: 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.

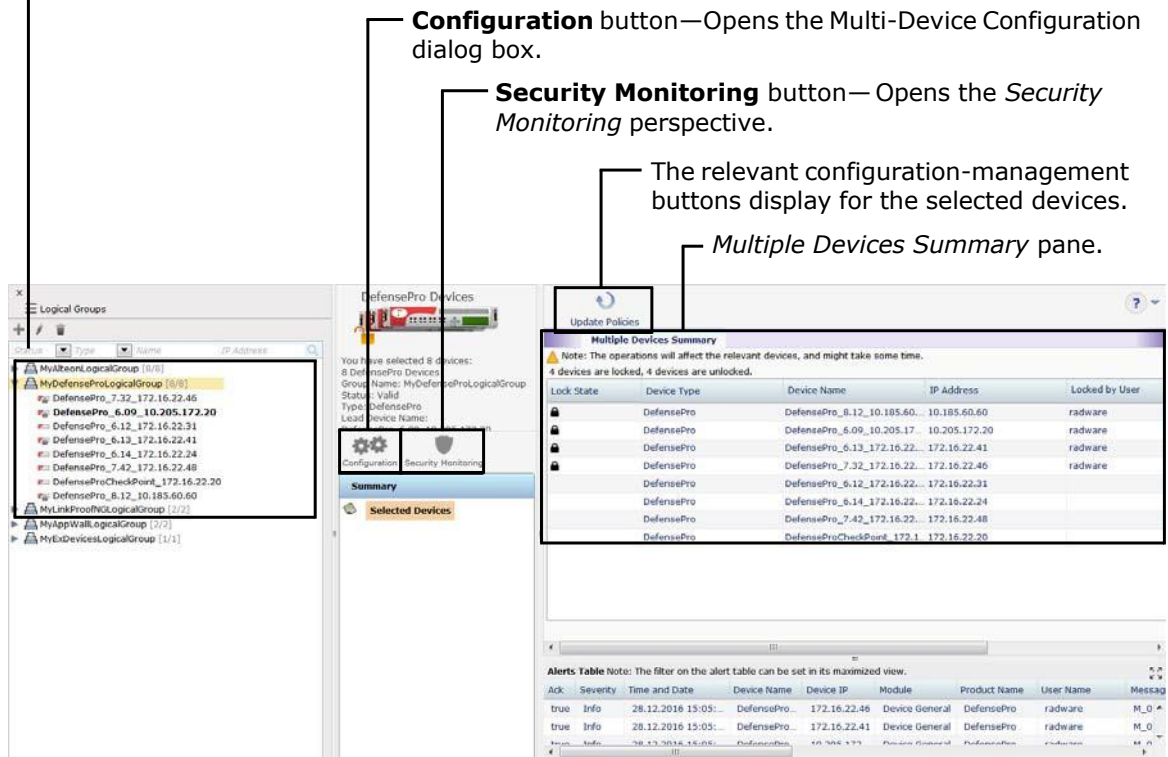
The relevant configuration-management buttons display for the selected devices.

Multiple Devices Summary pane.



Lock State	Device Type	Device Name	IP Address	Locked by User	Status
	AppWall	AppWall_6.6.1_Cluster_Child	172.17.165.137		Down
	AppWall	AppWall_6.6.1_Cluster_Manager	172.17.165.139		Maintenance
	AppWall	AppWall_7.2.1_172.17.172.47	172.17.172.47	radware	Up
	DefensePro	DefensePro_6.14_172.16.22.24	172.16.22.24		Up
	DefensePro	DefensePro_6.09_10.205.172.20	10.205.172.20		Up
	DefensePro	DefensePro_7.42_172.16.22.48	172.16.22.48		Up
	DefensePro	DefensePro_92_172.16.22.92	172.16.22.92		Up
	DefensePro	DefensePro_93_172.16.22.93	172.16.22.93		Up
	DefensePro	DefensePro_6.12_172.16.22.31	172.16.22.31		Up
	DefensePro	DefensePro_6.13_172.16.22.41	172.16.22.41		Up
	DefensePro	DefensePro_7.32_172.16.22.46	172.16.22.46	radware	Up
	DefensePro	DefensePro_7.41_IP_Mode_172.16.22.45	172.16.22.45		Up

Figure 29: Multi-Device View from the Logical Groups Tree

A Logical Group is selected, which automatically opens the multi-device view. APSSolute Vision displays the name of the *lead device* with **bold lettering**. APSSolute 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.




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 69](#)
- [Logical Group User Interface, page 70](#)
- [Managing Logical Groups, page 71](#)

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 devices in 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 66](#)) 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, IP Address, 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 191](#).
 - **Run configuration-management actions for the relevant devices**—You can run the Update Policies action on multiple DefensePro 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 231](#).
- **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, see the [Scheduling APSolute Vision and Device Tasks, page 199](#).
- **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 DefensePro, 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 DefensePro configuration templates**—In addition to selecting individual devices, you can specify one or more Logical Groups of DefensePro devices. For more information on DefensePro configuration templates, see [Using Configuration Templates for Security Policies, page 184](#).

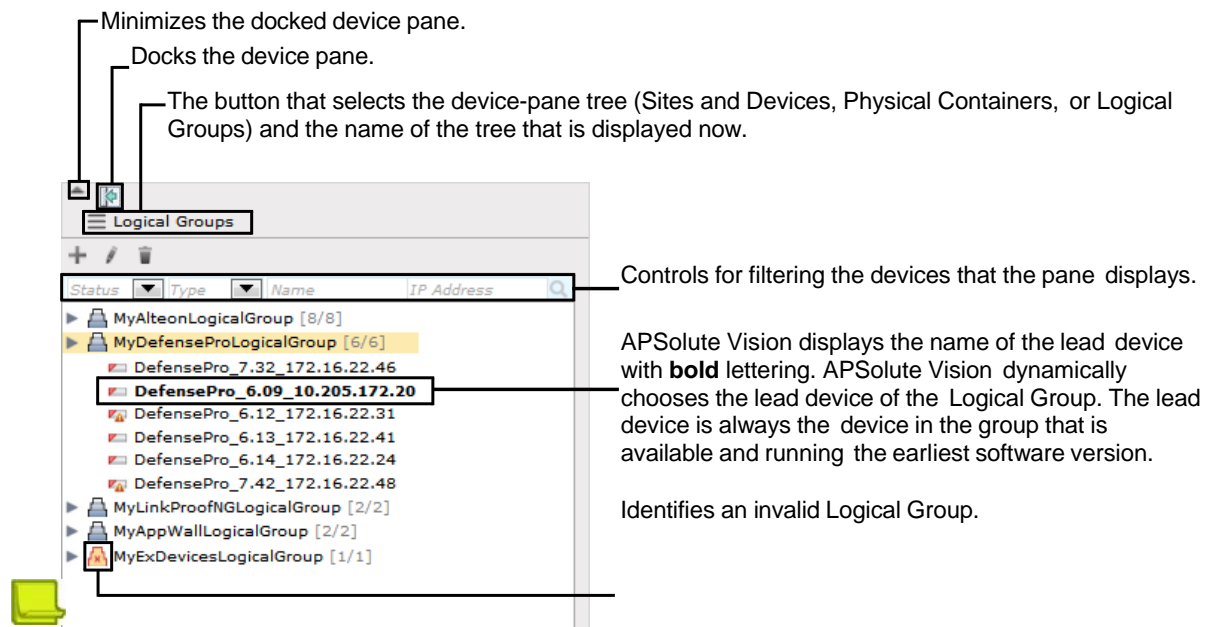
- **Specify devices for Alert Profile**—In addition to selecting individual devices, you can specify one or more relevant Logical Groups. For more information on Alert Profiles, see the APSolute Vision User Guide or online help.
- **Specify devices for the Alerts Table Filter**—In addition to selecting 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 each Logical 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 66](#). For more information, see [Using the Multi-Device View and the Multiple Devices Summary, page 31](#).

Figure 30: Device Pane (Not Docked)—Showing the Logical Groups Tree with a Logical Group of DefensePro Devices



Note: For information on filtering the display of the tree, see [Filtering Entities in the Device Pane, page 58](#).

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**, **DefensePro**, 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 31: Popup for Logical Group Node in the Device Pane

```
Group Name: MyDefenseProLogicalGroup
Status: Valid
Type: DefensePro
Lead Device Name: DefensePro_6.09_10.205.172.20
Description: This is a group of some DefensePro devices.
```

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: <ul style="list-style-type: none"> ● Alteon ● AppWall ● DefensePro ● 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 of the 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 scheduling tasks, making backups, and so on.
- Monitor managed devices through APSolute Vision.



Chapter 3 – Managing the DefensePro Setup

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

- [Configuring the DefensePro Global Parameters, page 75](#)
- [Configuring the DefensePro Networking Setup, page 84](#)
- [Configuring the DefensePro Device-Security Setup, page 89](#)
- [Configuring the DefensePro Security-Settings Setup, page 104](#)
- [Configuring the DefensePro Advanced-Parameters Setup, page 123](#)
- [Configuring the DefensePro Reporting-Settings Setup, page 126](#)
- [Configuring the Radware DefensePro DDoS Mitigation Clustering Setup, page 130](#)

Configuring the DefensePro Global Parameters

This section contains the following topics:

- [Viewing and Configuring Basic Global Parameters, page 75](#)
- [Managing Certificates, page 76](#)
- [Upgrading Licenses for DefensePro Devices, page 81](#)
- [Configuring Date and Time Settings in DefensePro, page 83](#)

Viewing and Configuring Basic Global Parameters

You can view and configure the following:

- Basic device-setup parameters
- The time and date 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 11: 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 Up Time	(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 12: 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 13: Global Parameters: Version Information Parameters

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

Managing Certificates

This section describes certificates for DefensePro, and how to manage the certificates using APSolute Vision.

This section contains the following topics:

- [Certificates, page 76](#)
- [Keys, page 77](#)
- [Self-Signed Certificates, page 77](#)
- [Modifying Certificate Information for a Selected Device, page 77](#)
- [Configuring Certificates, page 77](#)
- [Configuring Default Certificate Attributes, page 79](#)
- [Importing Certificates, page 79](#)
- [Exporting Certificates, page 80](#)
- [Showing Certificate Content, page 81](#)

Certificates

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.

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 the digital certificate was issued by a valid agency

Keys

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 personnel 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 the following key size lengths: 512, 1024, or 2048 bytes.

Self-Signed Certificates

Self-signed certificates do not include third-party verification. When you open an HTTPS session, the Radware DefensePro DDoS Mitigation device uses a certificate for identification. By default, the device has self-signed Radware SSL certificates. You can also specify your own self-signed SSL certificates.

Modifying Certificate Information for a Selected Device

You can view and modify certificate information for a selected device.



To view and modify certificate information for a selected device

- > In the Configuration perspective, select **Setup > Global Parameters > Certificates**.

The Certificates table displays information for each certificate stored on the device. From here, you can add, edit, and delete certificates. You can also import and export certificates, and show certificate text.

Configuring Certificates

You can create or modify a self-signed certificate for HTTPS access to through APSolute Vision. You can also create certificate signing requests and keys for new certificates.



To create or modify a certificate or key

1. In the Configuration perspective, select **Setup > Global Parameters > Certificates**.
2. Do one of the following:
 - To add a certificate, click  (Add).
 - To edit a certificate, double-click the certificate name.
3. Configure certificate parameters and click **Submit**.

Table 14: Certificate Parameters

Parameter	Description
Name	The name of the key or certificate. Caution: Do not define a certificate name longer than 49 characters. This can corrupt the Certificate Table.
Type	The type of certification. Values: <ul style="list-style-type: none"> • Certificate • Certificate of Client CA¹ • Certificate Signing Request • Intermediate CA Certificate¹ • Key—When you select Key, only the Key Size and Passphrase fields are available. Default: Key
Key Size	The key size, in bytes. Larger key sizes offer an increased level of security. Radware recommends that certificates have a key size of 1024 or more. Using a certificate of this size makes it extremely difficult to forge a digital signature or decode an encrypted message. Values: 512 Bytes, 1024 Bytes, 2048 Bytes Default: 1024 Bytes
Common Name	The domain name of the organization (for example, www.radware.com) or IP address.
Organization	The name of the organization.
Email Address	Any e-mail address that you want to include within the certificate.
Key Passphrase	The Key Passphrase encrypts the key in storage and is required to export the key. Since Private Keys are the most sensitive parts of PKI data, they must be protected by a passphrase. The passphrase should be at least four characters and Radware recommends using stronger passphrases than that based on letters, numbers and signs.
Verify Key Passphrase	After you define the key passphrase, re-enter it for verification.
Locality	The name of the city.
State / Province	The state or province.
Organization Unit	The department or unit within the organization.
Country Name	The organization country.
Certificate Expiration	The duration, in days, that the certificate remains valid. Values: 1–4,294,967,295 (4 GB) Default: 365

1 – If you select this option when it is not allowed (according to the type of certificate you are using), the device alerts you with an error message.

Configuring Default Certificate Attributes

Use certificate defaults to define your organization's default parameters to be used when creating signing requests or self-signed certificates.

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 > Global Parameters > Certificates > Default Attributes**.
2. Configure the parameters, and then, click **Submit**.

Table 15: Default Certificate Parameters

Parameter	Description
Common Name	The domain name of the organization. For example, www.radware.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.

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 Key and for certificate, you must import them consecutively with the same entry name.



Caution: A certificate that you import must not include a header or footer. (Header and footer example: -----BEGIN PUBLIC KEY-----, -----END PUBLIC KEY-----) If the certificate that you want to import includes a header or footer, you must remove it before importing it. Common external applications such as openssl or ssh-keygen may include a header and footer when they generate a certificate. A certificate that Radware DefensePro DDoS Mitigation generates does not include a header or footer.



To import a certificate or key

1. In the Configuration perspective, select **Setup > Global Parameters > Certificates**.
2. Click the **Import** button below the table.
3. Configure the parameters, and then, click **Submit**.

Table 16: Importing Certificates Parameters

Parameter	Description
Entry Name	A new entry name to create by import, or an existing entry name to overwrite or complete a Key or CSR.
Entry Type	<p>Values:</p> <ul style="list-style-type: none"> • Key—Imports a key from backup or exported from another system. To complete the configuration, you will need to import a certificate into this key. • Certificate—Imports a certificate from backup or exported from another machine. The certificate must be imported onto a matching key or signing request. • Certificate of Client CA—Imports a Client CA certificate. <p>Default: Key</p> <p>Note: In Web Based Management, Radware DefensePro DDoS Mitigation supports the following three additional options: Intermediate CA Certificate, Certificate and Key, SSH Public Key.</p>
Passphrase (This parameter is available only when the Entry Type is Key .)	Since Private Keys are the most sensitive parts of PKI data they must be protected by a passphrase. The passphrase should be at least four characters, and Radware recommends using stronger passwords than that based on letters, numbers, and signs.
Verify Passphrase (This parameter is available only when the Entry Type is Key .)	Since Private Keys are the most sensitive parts of PKI data they must be protected by a passphrase. The passphrase should be at least four characters, and Radware recommends using stronger passwords than that based on letters, numbers, and signs.
File Name	The certificate file to import.

Exporting Certificates

Key, certificate and signing request export is used for backup purposes, moving existing configurations to another system or for completion of Signing Request processes. You can export certificates from a device by copying and pasting a key or by downloading a file. Keys and certificates are exported to PEM format.



Note: The Radware key is created without a Radware password at system startup, thus it can be exported without a Radware password.



To export a certificate or key

1. In the Configuration perspective, select **Setup > Global Parameters > Certificates**.
2. Click the **Export** button below the table.
3. Configure the parameters, and then, click **Submit**.

Table 17: Export Certificate Parameters

Parameter	Description
Entry Name	Select the name of the entry to export. By default, the name of the selected certificate in the Certificates table is displayed.
Entry Type	According to the selected entry name, you can export Certificate, Certificate Chain, Client CA Certificate, Key, or Certificate Signing Request.
Passphrase	Required when exporting Keys. Use the passphrase entered when the key was created or imported. You must enter the key passphrase to validate that you are authorized to export the key.

Showing Certificate Content

You can display the content of keys, certificates, or signing requests listed in the Certificates table. The content is displayed in encrypted text format for copy-paste purposes, for example sending signing requests to a certificate signing authority.



To display certificate content

1. In the Configuration perspective, select **Setup > Global Parameters > Certificates**.
2. Click **Show** below the table.
3. Select the entry name to show. By default, the name of the selected certificate in the Certificates table is displayed.
4. Select the entry type, and password for the key, if required.
5. Click **Show** to display the content in the Certificate field.

Upgrading Licenses for DefensePro Devices

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

The license provided to you, is a one-time license. To change licenses, you must use a new license key, after which, the old license key cannot be reused.

Each license is based on the device's MAC address and on a license ID, which is changed every time a new license is used. To obtain a license upgrade or downgrade, you must include the MAC address and the current license ID of the device when you order the required license part number. This information is displayed in the License Upgrade pane.

After you enter the new license information in the License Upgrade pane, the old license cannot be reused.



To upgrade a license after receiving new license keys

1. In the Configuration perspective, select **Setup > Global Parameters > License Upgrade**.
2. Configure license upgrade parameters for the new license keys, and then, click **Submit**.

Upgrading a License on Radware DefensePro DDoS Mitigation

Radware DefensePro DDoS Mitigation requires a valid throughput license. The throughput license determines the maximum throughput of legitimate traffic that DefensePro 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 DDoS Mitigation for Cisco Firepower, please contact your Cisco representative or refer to the Cisco documentation.



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



To upgrade a license after receiving new license keys

1. In the Configuration perspective, select **Setup > Global Parameters > License Upgrade**.
2. Configure license upgrade parameters for the new license keys, and then, click **Submit**.
3. If you have upgraded the vCPU license, do the following to fully utilize the vCPU license:
 - a. Shut down the Radware DefensePro DDoS Mitigation instance.
 - b. Change the number of vCPUs in the Radware DefensePro DDoS Mitigation instance to correspond with the vCPU license.
 - c. Start the Radware DefensePro DDoS Mitigation instance.

Table 18: 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: <ul style="list-style-type: none">● 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: <ul style="list-style-type: none">● 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.
vCPU License ID	(Read-only) The device vCPU license ID that was provided when requesting the new vCPU license.
vCPU License Key	The key for the device vCPU license.

Table 18: License Upgrade Parameters for Radware DefensePro DDoS Mitigation (cont.)

Parameter	Description
vCPU License Method	(Read-only) The method used to generate the license. Values: <ul style="list-style-type: none"> 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.
vCPU License IP Address	(Read-only) Values: <ul style="list-style-type: none"> The IP address that was used to generate the vCPU license. None—The license generator used the MAC address of the device to generate the vCPU license.

Configuring Date and Time Settings in DefensePro

This section describes configuring basic DefensePro date and time settings, and also [Configuring DefensePro Daylight Saving, page 83](#).

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 DefensePro Daylight Saving

DefensePro supports daylight savings time. You can configure the daylight savings time start and end dates and times. During daylight savings time, the device automatically adds one hour to the system clock. The device also indicates whether it is on standard time or daylight saving time.



Note: When the system clock is manually configured, the system time is changed only when daylight saving time starts or ends. When daylight saving time is enabled during the daylight saving time period, the device does not change the system time.



To configure DefensePro daylight saving

- In the Configuration perspective, select **Setup > Global Parameters > Time Settings > Daylight Saving**.
- Configure the parameters, and then, click **Submit**.

Table 19: Daylight Saving Parameters

Parameter	Description
Enabled	Enables or disables daylight saving time. Default: Disabled
Begins at	The start date and time for daylight saving time.

Table 19: Daylight Saving Parameters (cont.)

Parameter	Description
Ends at	The end date and time for daylight saving time.
Current Mode	Specifies whether the device is on standard time or daylight saving time.

Configuring the DefensePro Networking Setup

This section contains the following topics:

- [Configuring the Basic Parameters of the DefensePro Networking Setup, page 84](#)
- [Configuring IP Interface Management in the Networking Setup, page 85](#)
- [Configuring DNS for the DefensePro Networking Setup, page 88](#)

Configuring the Basic Parameters of the DefensePro Networking Setup

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

IPv4 and IPv6 Support

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

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

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

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. The device identifies all the fragments belong to same datagram, then classifies and forwards them accordingly. The device 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 DefensePro 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 network policy configured on the device.

Configuring the Basic Networking Parameters

This section describes how to configure the basic networking parameters.



To configure the basic networking parameters

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

Table 20: Basic: 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

Radware DefensePro DDoS Mitigation performs routing between all IP interfaces defined on its Layer 2 interfaces (ports, trunks, and VLANs). Radware DefensePro DDoS Mitigation also performs routing based on other network layers, such as Layer 4 and Layer 7.



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**.


Configuring IP Routing in DefensePro

This section describes IP routing in DefensePro.

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 DefensePro

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 21: 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.
Type	(Read-only) This field is displayed in the Static Routes table. Values: <ul style="list-style-type: none">• 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 22: IP Routing: Advanced Parameters

Parameter	Description
Enable Sending Trap on ICMP Error	<p>Specifies whether Radware DefensePro DDoS Mitigation sends a trap if there is an ICMP error message.</p> <p>Default: Enabled</p> <p>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.</p>

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 23: 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.
Type	<p>The entry type.</p> <p>Values:</p> <ul style="list-style-type: none"> ● 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 24: 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 DefensePro Networking Setup

You can configure DefensePro 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 DefensePro 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 25: DNS Client Parameters

Parameter	Description
Enable DNS Client	Specifies whether the DefensePro 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 DefensePro uses for domain-name resolution.
Alternative DNS Server	The IP address of the alternative DNS server that DefensePro 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: <ul style="list-style-type: none"> • Host Name—The domain name for the specified IP address • IP Address—The IP address for the specified domain name

Configuring the DefensePro Device-Security Setup

This section contains the following topics:

- [Configuring Access Protocols for the DefensePro Device-Security Setup, page 89](#)
- [Configuring Authentication Protocols for Device Management, page 91](#)
- [Configuring SNMP in the DefensePro Device-Security Setup, page 93](#)
- [Configuring Device Users in the DefensePro Device-Security Setup, page 103](#)
- [Configuring Advanced Parameters in the DefensePro Device-Security Setup, page 91](#)

Configuring Access Protocols for the DefensePro Device-Security Setup

Radware DefensePro DDoS Mitigation supports the following access protocols:

- **HTTPS**—For APSolute Vision communication with DefensePro.
- **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 26: Access Protocols: Secured Web Access Parameters

Parameter	Description
Enable Secured Web Access	Specifies whether to enable HTTPS access to DefensePro. 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 27: Access Protocols: Telnet Parameters

Parameter	Description
Enable Telnet	Specifies whether to enable Telnet access to DefensePro. Default: Disabled

L4 Port

The TCP port used by the Telnet. Default: 23

Table 27: Access Protocols: Telnet Parameters (cont.)

Parameter	Description
Session Timeout	The time, in minutes, that DefensePro 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 28: Access Protocols: SSH Parameters

Parameter	Description
Enable SSH	Specifies whether to enable SSH access to DefensePro. Default: Disabled
L4 Port	The source port for the SSH server connection. Default: 22
Session Timeout	The time, in minutes, that DefensePro 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 29: Access Protocols: Web Services Parameter

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

Configuring Advanced Parameters in the DefensePro 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 30: 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.
Web Access	When selected, allows access to the port using WBM.
SSL Access	When selected, allows access to the port using SSL.

Configuring Port Pingging

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 allow pings.



To define the ports to be pinged

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

Configuring Authentication Protocols for Device Management

This section comprises the following:

- [Configuring RADIUS Authentication for Device Management, page 91](#)

Configuring RADIUS Authentication for Device Management

DefensePro 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 the CLI, Telnet, or SSH.



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 and must allow device access.
- Radware DefensePro DDoS Mitigation uses Password Authentication Protocol (PAP) when connecting to the RADIUS server.

With RADIUS authentication for device management, DefensePro 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.



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 device, and then, click **Submit**.

Table 31: RADIUS Authentication: General Parameters

Parameter	Description
Timeout	The length of time the device waits for a reply from the RADIUS server before a retry, or, if the Retries value is exceeded, before the device 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, DefensePro will not re-authenticate the client with the RADIUS server. If the client logs in again after the lifetime expires, DefensePro re-authenticates the client. Default: 30

Table 32: 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 DefensePro 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	When defining the password, reenter it for verification.
Server IP Address Type	Values: IPv4, IPv6
Server IP Address	The IP address of the primary RADIUS server.

Table 33: 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 DefensePro 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	When defining the password, reenter it for verification.
Server IP Address Type	Values: IPv4, IPv6
Server IP Address	The IP address of the backup RADIUS server.

Configuring SNMP in the DefensePro 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 devices can work with all versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3. The default Radware 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 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 94](#)
- [Configuring DefensePro SNMP Users, page 94](#)
- [Configuring SNMP Community Settings, page 96](#)
- [Configuring the SNMP Group Table, page 97](#)
- [Configuring SNMP Access Settings, page 91](#)
- [Configuring SNMP Notify Settings, page 99](#)
- [Configuring SNMP View Settings, page 100](#)
- [Configuring the SNMP Target Parameters Table, page 100](#)
- [Configuring SNMP Target Addresses, page 102](#)

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 34: 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 DefensePro 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 DefensePro user, the DefensePro device must be configured to support SNMPv3 (Configuration perspective, select **Setup > Device Security > SNMP > SNMP Versions > V3**).

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



1. Using the default DefensePro user and connected to APSolute Vision 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 DefensePro user

1. In the APSolute Vision device pane Sites and Devices tree, select the DefensePro 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 > SNMP User 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 35 - SNMP User Parameters, page 96](#)), and then, click **Submit**.
6. In the Configuration perspective, select **Setup > Device Security > SNMP > Group Table**.
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 97](#).

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 98](#).

Table 35: SNMP User Parameters

Parameter	Description
User Name	The username, also known as a security name. Maximum characters: 18
Authentication Protocol	The protocol used during authentication process. The option that you select must match the configuration in the Device Properties dialog box (see Table 68 - Device Properties: SNMP Parameters, page 9). 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: <ul style="list-style-type: none"> • MD5 • SHA Default: None Caution: None is not a valid value.
Authentication Password	The authentication password.
Privacy Protocol	The algorithm used for encryption. Values: <ul style="list-style-type: none"> • DES—The device uses Data Encryption Standard. Default: None Caution: None is not a valid value.
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 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 SNMP community parameters and click **Submit**.

Table 36: 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
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 Addresses table. At least one entry in the SNMP Target Addresses 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.

Access rights are defined for groups of users in the SNMP Access table.



To configure SNMP group settings

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

Table 37: SNMP Group Parameters

Parameter	Description
Group Name	The name of the SNMP group.

Table 37: SNMP Group Parameters (cont.)

Parameter	Description
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: <ul style="list-style-type: none"> • 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.



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 SNMP access parameters and click **Submit**.

Table 38: 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: <ul style="list-style-type: none"> • SNMPv1 • SNMPv2c • User Based—That is, SNMPv3 Default: SNMPv1

Table 38: SNMP Access Parameters (cont.)

Parameter	Description
Security Level	The security level required for access. Values: <ul style="list-style-type: none"> • 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.
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.

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 SNMP notify parameters and click **Submit**.

Table 39: 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 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 SNMP view parameters and click **Submit**.

Table 40: 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 target parameter settings and click **Submit**.

Table 41: 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: <ul style="list-style-type: none"> • 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 the notification is generated. For other security models, the security name identifies the SNMP community used when the notification is generated.
Security Level	Specifies whether the trap is authenticated and encrypted before it is sent. Values: <ul style="list-style-type: none"> • 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 Addresses 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 target address parameters and click **Submit**.

Table 42: 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.

Configuring Device Users in the DefensePro 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, HTTP(S)). 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 43: Device User Parameters

Parameter	Description
User Name	The name of the user.
Password	The password of the user. Then, repeat to verify.
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: <ul style="list-style-type: none">• 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
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. The device 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: <ul style="list-style-type: none">• 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 44: Advanced Parameters for the Device Users

Parameter	Description
Authentication Mode	<p>The method for of authenticating a user's access to the device. Values:</p> <ul style="list-style-type: none">• Local User Table—The device uses the User Table to authenticate access.• RADIUS and Local User Table—The device uses the RADIUS servers to authenticate access. If the request to the RADIUS server times out, the device uses the User Table to authenticate access. <p>Default: Local User Table</p>

Configuring the DefensePro Security-Settings Setup

Before you configure a Network 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 Signature Protection, page 104](#)
- [Configuring Global DoS Shield Protection, page 105](#)
- [Configuring Global Behavioral DoS Protection, page 107](#)
- [Configuring Global SYN Flood Protection, page 111](#)
- [Configuring Global Out-of-State Protection, page 112](#)
- [Configuring Global Packet Anomaly Protection, page 115](#)
- [Configuring Global DNS Flood Protection, page 118](#)



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 enabling features within the same navigation branch.
- When you enable or disable Signature Protection, the device requires an Update Policies action to take effect.

Configuring Global Signature Protection

Signature Protection is enabled by default.

When DefensePro detects a signature in a TCP session, DefensePro drops all packets of the session.



Caution: When DefensePro 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 > Signature Protection**.
2. Select or clear the **Enable Application Security Protection** checkbox to specify whether 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 management interfaces. 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. Samples of the traffic are compared with the list of protections in Dormant state. When a specified number of packets is reached, the status 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 > DoS Shield**.
2. Configure the parameters, and then, click **Submit**.

Table 45: 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 Network Protection policy

- > In the Configuration perspective, select **Network Protection > Network Protection Policies > + (Add) > Action > Signature Protection Profile > All-DoS-Shield**. For more information, see [Managing DefensePro Network Protection Policies, page 139](#).

Configuring Global Behavioral DoS Protection

Behavioral Denial-of-Service (BDoS) Protection, which you can use in a Network 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 Network 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 > BDoS Protection**.
2. Configure the parameters, and then, click **Submit**.

Table 46: 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 the learning response to one month. Use a one-day period for testing purposes only. Values: Day, Week, Month Default: Week

Table 46: BDoS Protection (Global): General Parameters (cont.)

Parameter	Description
Enable Traffic Statistics Sampling	<p>Specifies whether the BDoS module uses traffic-statistics sampling during the creation phase of the BDoS footprint. When the parameter is enabled, and the BDoS module is trying to generate a real-time signature and there is a high rate of traffic, the device evaluates only a portion of the traffic. The BDoS module tunes the sampling factor automatically, according to the traffic rate. The BDoS module screens all traffic at low traffic rates (below 100K PPS) and only a portion of the traffic at higher rates (above 100K PPS).</p> <p>Default: Enabled</p> <p>Note: For best performance, Radware recommends that the parameter be Enabled.</p>
Footprint Strictness	<p>When the Behavioral DoS module detects a new attack, the module generates an attack footprint to block the attack traffic. If the Behavioral DoS module is unable to generate a footprint that meets the footprint-strictness condition, the module 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 device cannot generate a footprint.</p> <p>Values:</p> <ul style="list-style-type: none"> ● High—Requires at least two Boolean AND operators and no other Boolean OR value in the footprint. This level lowers the probability for false positives but increases the probability for false negatives. ● Medium—Requires at least one Boolean AND operator and no more than two additional Boolean OR values in the footprint. ● Low—Allows any footprint suggested by the Behavioral DoS module. This level achieves the best attack blocking, but increases the probability of false positives. <p>Default: Low</p> <p>Notes:</p> <ul style="list-style-type: none"> ● Radware DefensePro DDoS Mitigation 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 48 - Footprint Strictness Examples, page 110, shows examples of footprint strictness requirements.

Table 47: BDoS Protection (Global): Advanced Parameters

Parameter	Description
	<p>These settings affect periodic attack behavior. The settings are used to effectively detect and block these attack types.</p>
<p>Duration of Non-attack Traffic in Blocking State</p>	<p>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.</p> <p>Values: 45–300</p> <p>Default: 45</p>
<p>Duration of Non-attack Traffic in Anomaly or Non-Strictness State</p>	<p>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.</p> <p>Values: 45–300</p> <p>Default: 45</p>
<p>Learning Suppression Threshold</p>	<p>The percentage of the specified bandwidth, below which, DefensePro suppresses BDoS-baseline learning.</p> <p>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.</p> <p>There are two typical scenarios where, at times, Radware DefensePro DDoS Mitigation handles very little traffic:</p> <ul style="list-style-type: none"> • Out-of-path deployments—In an out-of-path deployment, when traffic is diverted through DefensePro for mitigation. During an attack, the traffic is diverted and routed through DefensePro. During peacetime, no traffic passes through DefensePro (except for maintenance messages). When no traffic is diverted to DefensePro, the BDoS 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 dramatically throughout the day. <p>The specified bandwidth refers to the Outbound Traffic and Inbound Traffic parameters under the Network Protection tab, BDoS Profiles > Outbound Traffic Inbound Traffic.</p> <p>The Learning Suppression Threshold applies to all BDoS profiles and controllers, but Radware DefensePro DDoS Mitigation calculates the threshold per Network 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).</p> <p>Values:</p> <ul style="list-style-type: none"> • 0—Specifies that BDoS profiles use no Learning Suppression Threshold. • 1–50 <p>Default: 0</p>

Table 47: BDoS Protection (Global): Advanced Parameters (cont.)

Parameter	Description
Reset BDoS Baseline	<p>Click to reset the BDoS baseline. Then, select whether to reset the baseline for all Network Protection policies that contain a BDoS profile, or for a specific Network Protection policy that contains a BDoS profile; and then, click Submit.</p> <p>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.</p>

Table 48: Footprint Strictness Examples

Footprint Example	Low Strictness	Medium Strictne	High Strictness
TTL	Yes	No	No
TTL AND Packet Size	Yes	Yes	No
TTL AND Packet Size AND Destination Port	Yes	Yes	Yes

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 footprint bypass


1. In the Configuration perspective, select **Setup > Security Settings > BDoS Protection > BDoS Footprint Bypass**.
2. From the **Footprint Bypass Controller** drop-down list, select the attack protection for which you want to configure footprint bypass, and click the  (Search) button. The table displays the bypass types and values for the selected attack protection.
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 49: BDoS Footprint Bypass Parameters

Parameter	Description
Footprint Bypass Controller	(Read-only) The selected attack protection for which you are configuring footprint bypass.
Bypass Field	(Read-only) The selected bypass type to configure.

Table 49: BDoS Footprint Bypass Parameters (cont.)

Parameter	Description
Bypass Status	The bypass option. Values: <ul style="list-style-type: none"> • Bypass—The Behavioral DoS module bypasses all possible values of the selected Bypass Field when generating a footprint. • Accept—The Behavioral DoS module bypasses only the specified values (if such a value exists) of the selected Bypass Field when generating a footprint.
Bypass Values	If the value of the Bypass Status parameter is Accept , when generating the footprint, the Behavioral DoS mechanism does not use the specified Bypass Values of the corresponding selected Bypass Field. The valid Bypass Values vary according to the selected Bypass Field. Multiple values in the Bypass Values field must be comma-delimited.

Selecting Packet Header Fields for Early Blocking of DoS Traffic

This feature is non-operational in Radware DefensePro DDoS Mitigation.

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 Protection as a Network Protection to allow easier protection of multiple network elements.

Before you configure SYN profiles for the Network 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 tab.



To configure global SYN Flood Protection

1. In the Configuration perspective, select **Setup > Security Settings > SYN Flood Protection**.
2. Select or clear the **Enable SYN Flood Protection** checkbox to specify whether SYN Flood Protection is enabled on the device. Default: Enabled



Caution: Changing the setting of this parameter requires a reboot to take effect.

3. Click **Submit**.
4. In the Configuration perspective, select **Setup > Security Settings > SYN Flood Protection > SYN Protection Parameters**.
5. Configure the parameters, and then, click **Submit**.

Table 50: SYN Protection Parameters: Advanced Parameters

Parameter	Description
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
Minimum Allowed SYN Retransmission Time	The minimum time, in seconds, for the SYN-packet retransmission in the Safe-Reset authentication mechanism to consider the retransmission to be valid. Values: 2–15 Default: 2 Note: For more information, see Managing SYN Protection Profile Parameters, page 173 .
Maximum Allowed SYN Retransmission Time	The maximum time, in seconds, for the SYN-packet retransmission in the Safe-Reset authentication mechanism to consider the retransmission to be valid. Values: 3–15 Default: 4 Note: For more information, see Managing SYN Protection Profile Parameters, page 173 .

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 for Network Protection, page 181](#).

Radware DefensePro DDoS Mitigation implements several different graceful-startup periods for Out-of-State Protection actions for different scenarios. During one of these graceful-startup 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 viewing the status of graceful-startup 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 graceful-startup period for Out-of-State Protection actions for the following scenarios:

- **After startup or reboot when the selected Startup Mode is Graceful**—This timer is the **Startup Timer** parameter in the Out-of-State Protection global parameters (in the procedure below). Default: 1800 seconds (30 minutes).
- **When an Update Policies action finishes**—This graceful-startup period is configurable only in the CLI. Default: 30 seconds.
- **When the Session table is no longer full**—This graceful-startup period is configurable only in the CLI. Each core manages its own Session table. Default: 1800 seconds (30 minutes).



To configure global Out of State Protection

1. In the Configuration perspective, select **Setup > Security Settings > Out of State**.
2. Configure the parameters, and then, click **Submit**.

Table 51: Out-of-State Protection Global Parameters

Parameter	Description
Enable Out-of-State Protection	Specifies whether the Radware DefensePro DDoS Mitigation enables Out-of-State Protection configuration and learning. Default: Enabled
Activate (Without Reboot) (This parameter is available only after selecting the Enable Out-of-State Protection checkbox.)	<p>Values:</p> <ul style="list-style-type: none"> ● Enabled—Activate Out-of-State Protection actions immediately. ● Disabled—Deactivate Out-of-State Protection actions immediately. <p>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 (Without Reboot) checkbox.</p> <p>When the Activate (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.</p> <p>When the Activate (Without Reboot) checkbox is selected and the selected Startup Mode is Graceful, after startup, the Activate (Without Reboot) checkbox is cleared for the duration of the Startup Timer. After the Startup Timer has elapsed, the Activate (Without Reboot) checkbox is automatically selected (that is, enabled again).</p> <p>When the Activate (Without Reboot) checkbox is selected and the selected Startup Mode is Off, after startup, the Activate (Without Reboot) checkbox is cleared.</p>

Table 51: Out-of-State Protection Global Parameters (cont.)

Parameter	Description
<p>Startup Mode (This parameter is available only after selecting the Enable Out-of-State Protection checkbox.)</p>	<p>The behavior of the device after startup.</p> <p>Values:</p> <ul style="list-style-type: none"> ● 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. <p>Default: Graceful</p> <p>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 (Without Reboot) checkbox.</p>
<p>Startup Timer (This parameter is available only after selecting the Enable Out-of-State Protection checkbox.)</p>	<p>When the selected Startup Mode is Graceful, this parameter specifies the time, in seconds, after startup or reboot, that the 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. After this time, the Out-of-State Protection module inspects packets and decides whether a packet is out of state. DefensePro then takes action according to the configuration of the matching Network Protection policy and Out-of-State Protection profile.</p> <p>Values: 0–65,535</p> <p>Default: 1800 (30 minutes)</p>
<p>Sampling Frequency</p>	<p>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.</p> <p>Values: 4–10</p> <p>Default: 10</p> <p>Note: For more information on the Termination Threshold parameter (Configuration perspective, Network Protection > Out Of State Protection Profiles > Termination Threshold), see Configuring Out of State Protection Profiles for Network Protection, page 181.</p>

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 52 - Packet-Anomaly Protection Parameters, page 115](#).

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 > Packet Anomaly**.
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 52 - Packet-Anomaly Protection Parameters, page 115](#).

Table 52: Packet-Anomaly Protection Parameters

Parameter	Description
ID	(Read-only) The ID number for the packet-anomaly protection. The ID is a Radware ID that appears in the trap sent to APSolute Vision Security logs.
Protection Name	(Read-only) The name of the packet-anomaly protection.
Action	<p>The action that the device takes when the packet anomaly is detected. The action is only for the specified packet-anomaly protection.</p> <p>Values:</p> <ul style="list-style-type: none">• 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. <p>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.</p>

Table 52: Packet-Anomaly Protection Parameters (cont.)

Parameter	Description
Risk	The risk associated with the trap for the specific anomaly. Values: Info, Low, Medium, High Default: Low
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 100—Unrecognized L2 Format • 104—Invalid IP Header or Total Length • 107—Inconsistent IPv6 Headers • 131—Invalid L4 Header Length

Table 53: Default Configuration of Packet-Anomaly Protections

Anomaly	Description
Invalid IPv4 Header or Total Length	The IP packet header length does not match the actual header length, or 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	The TTL field value is equal to 0. ID: 105 Default Action: Report Default Risk: Low Default Report Action: Process
Inconsistent IPv6 Headers	Inconsistent IPv6 headers. ID: 107 Default Action: Drop Default Risk: Low Report Action: Bypass ¹

Table 53: Default Configuration of Packet-Anomaly Protections (cont.)

Anomaly	Description
IPv6 Hop Limit Reached	IPv6 hop limit is not be greater than 1. ID: 108 Default Action: Report Default Risk: Low Default Report Action: Process
Unsupported L4 Protocol	Traffic other than UDP, TCP, ICMP, or IGMP. ID: 110 Default Action: No Report Default Risk: Low Default Report Action: Process
Invalid TCP Flags	The 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	The 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)	The 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
L4 Source or Dest. Port Zero	The Layer 4 source port or destination port equals zero. ID: 125 Default Action: Drop Default Risk: Low Default Report Action: Bypass
Invalid L4 Header Length	The length of the Layer 4, TCP/UDP/SCTP header is invalid. ID: 131 Default Action: Drop Default Risk: Low Report Action: Bypass ¹

1 – You cannot select **Process** for this packet-anomaly protection.

Configuring Global DNS Flood Protection

DNS Protection, which you can use in your Network 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 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 DefensePro 8.x versions 8.13 and later, the DNS 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 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 Network Protection policies with DNS 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 Flood Protection**.
2. Configure the parameters, and then, click **Submit**.

Table 54: DNS Flood Protection: General Parameters

Parameter	Description
Enable DNS Flood Protection	<p>Specifies whether DNS Flood Protection is enabled.</p> <p>Caution: Changing the setting of this parameter requires a reboot to take effect.</p>
Learning Response Period	<p>The initial period from which baselines are primarily weighted.</p> <p>The default and recommended learning response period is one week.</p> <p>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.</p> <p>Values: Day, Week, Month</p> <p>Default: Week</p>
Enable Traffic Statistics Sampling	<p>Specifies whether the DNS Flood Protection module uses traffic- statistics sampling during the creation phase of the DNS-flood footprint. When Enable Traffic Statistics Sampling is enabled, Radware DefensePro DDoS Mitigation evaluates only a portion of the traffic, when the DNS Flood Protection module is trying to generate a real-time signature and there is a high rate of traffic. The DNS Flood Protection module tunes the sampling factor automatically, according to the traffic rate. The DNS Flood Protection module screens all traffic at low traffic rates (below 100K PPS) and only a portion of the traffic at higher rates (above 100K PPS).</p> <p>Default: Enabled</p> <p>Note: For best performance, Radware recommends that the parameter be Enabled.</p>
Footprint Strictness	<p>When the DNS Flood Protection module detects a new attack, the module generates an attack footprint to block the attack traffic. If the module is unable to generate a footprint that meets the footprint- strictness condition, the module 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 module cannot generate a footprint.</p> <p>Values:</p> <ul style="list-style-type: none"> ● High—Requires at least two Boolean AND operators and no other Boolean OR value in the footprint. This level lowers the probability for false positives but increases the probability for false negatives. ● Medium—Requires at least one Boolean AND operator and no more than two additional Boolean OR values in the footprint. ● Low—Allows any footprint suggested by the DNS Flood Protection module. This level achieves the best attack blocking, but increases the probability of false positives. <p>Default: Low</p> <p>Note: The DNS Flood Protection module 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 57 - DNS Footprint Strictness Examples, page 121 shows examples of footprint strictness requirements.</p>

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
Learning Suppression Threshold	The percentage of the specified Expected DNS Query Rate (in the DNS Flood Protection profiles), below which, Radware DefensePro DDoS Mitigation suppresses DNS-baseline learning. Values: <ul style="list-style-type: none"> 0—Specifies that DNS Flood Protection profiles use no DNS Learning Suppression threshold (that is, DNS-baseline learning is always active) 1–100 Default: 0 Note: For more information, see DNS Learning Suppression, page 121 .
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

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 Network Protection policies that contain a DNS profile, or for a specific Network 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 Strictne	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

DNS Learning Suppression

You can use the DNS Learning Suppression feature to help preserve a good DNS-baseline value in scenarios where, at certain times, Radware DefensePro DDoS Mitigation handles very little traffic. The **DNS Learning Suppression Threshold** specifies the percentage of the specified **Expected DNS Query Rate** (configured in the DNS Flood Protection profiles), below which, Radware DefensePro DDoS Mitigation suppresses DNS-baseline learning.

There are two typical scenarios where, at certain 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 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 dramatically throughout the day.**

The **DNS Learning Suppression Threshold** applies to all DNS profiles, but Radware DefensePro DDoS Mitigation calculates the threshold per Network Protection policy and per IP version (IPv4 or IPv6).



Example

Consider two policies, Policy1 and Policy2. Policy1 has a DNS profile with the **Expected DNS Query Rate** value **1000**. Policy2 has a DNS profile with **Expected DNS Query Rate** value **500**. 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 baseline for Policy2 will not change (that is, learning is suppressed) if the traffic rate drops below 25 QPS.



To view the Network Protection policies with a DNS Flood Protection profile and the runtime status of the DNS Learning Suppression feature per Network Protection policy

- > Open the Radware DefensePro DDoS Mitigation CLI, and enter the following command: `system internal security dns learning suppression threshold get` The CLI displays a table like this:

```

+-----+
| Policy Name          | IP Version | 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 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 > DNS Flood Protection > DNS Footprint Bypass**.
2. From the Footprint Bypass Controller list, 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 Bypass 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: <ul style="list-style-type: none"> • Bypass—The DNS Flood Protection module bypasses all possible values of the selected Bypass Field when generating a footprint. • Accept—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	Used if the value of the Bypass Status parameter is Accept . DNS Flood Protection bypasses only the values of a selected Bypass Type, while it may use all other values. These values vary according to the selected Bypass Field . The values in the field must be comma-delimited.

Configuring the DefensePro Advanced-Parameters Setup

This section contains the following topics:

- [Configuring Authentication Tables Settings, page 123](#)
- [Configuring DefensePro Session Table Settings, page 124](#)

Configuring Authentication Tables Settings

Use the following procedure to configure the settings for Authentication Tables.



To configure Authentication Table settings

1. In the Configuration perspective, select **Setup > Advanced Parameters > Authentication Tables**.
2. To change a current value, enter the new value in the New Value column, and then, click **Submit**. You can reboot immediately or at a later time. Changes do not take effect until after reboot.

Table 59: Authentication Tables Settings: Aging Parameters

Parameter	Description
TCP Authentication Table Aging	The time, in seconds, that the device keeps idle sources in the TCP Authentication table. Values: 60–3600 Default: 1200
HTTP Authentication Table Aging	The time, in seconds, that the device keeps idle sources in the HTTP Authentication table. Values: 60–3600 Default: 1200

Configuring DefensePro Session Table Settings

DefensePro includes a Session table, which tracks sessions that Radware DefensePro DDoS Mitigation bridges and forwards.



Note: In Radware DefensePro DDoS Mitigation 8.x versions, there is one Session table for each core.



To configure Session table settings

1. In the Configuration perspective, select **Setup > Advanced Parameters > Session Table Settings**.
2. Configure the parameters, and then, click **Submit**.

Table 60: 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 60: 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
Incomplete TCP Handshake Timeout	How long, in seconds, the device waits for the three-way handshake to complete. When the timeout elapses, the device deletes the session. Values: <ul style="list-style-type: none"> 0—The device uses the specified Session Aging Time. 1–10—The TCP handshake timeout in seconds. Default: 10

Table 61: Session Table Advanced Parameters

Parameter	Description
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 option 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 Action	The action that the device takes when the Session table is at full capacity. Values: <ul style="list-style-type: none"> Allow new traffic—The device bypasses new sessions 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 the DefensePro Reporting-Settings Setup

This section contains the following topics:

- [Configuring DefensePro Syslog Settings, page 126](#)
- [Enabling Configuration Auditing on the DefensePro Device, page 127](#)
- [Configuring Security Reporting Settings, page 127](#)

Configuring DefensePro 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, Radware recommends configuring the APSolute Vision server to convey the syslog messages from all devices.



Note: For information about configuring syslog reporting on the APSolute Vision server, see the APSolute Vision User Guide or 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 62: 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 DefensePro Syslog Monitor (Monitoring perspective > Resource Utilization tab > Syslog Monitor).
Syslog Server	The IP address or hostname of the device running the syslog service (syslogd).
Source Port	The syslog source port. Default: 514 Note: Port 0 specifies a random port.

Table 62: Syslog Parameters (cont.)

Parameter	Description
Destination Port	The syslog destination port. 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: <ul style="list-style-type: none"> • 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

Enabling Configuration Auditing on the DefensePro 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, DefensePro 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 DefensePro 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.



Notes

- DefensePro does not provide sampled captured packets from suspicious sources that DefensePro challenged. (DefensePro supports an option to challenge sources in HTTP Flood Protection, SYN Flood Protection, DNS Flood Protection, and SSL Protection.)
- DefensePro does not provide sampled GRE-encapsulated captured packets.

You can also configure DefensePro 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.



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 63: Advanced Reporting Settings: Security Reporting Parameters

Parameter	Description
Report Interval	The frequency, in seconds, Radware DefensePro DDoS Mitigation sends reports through 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

Table 63: Advanced Reporting Settings: Security Reporting Parameters (cont.)

Parameter	Description
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
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 64: 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 65: 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

Table 65: Advanced Reporting Settings: netForensics Parameters (cont.)

Parameter	Description
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 66: 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 DefensePro 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 Radware DefensePro DDoS Mitigation Clustering Setup

Use the Clustering tab to configure clustering multiple DefensePro instances.

Clustering enables multiple Radware DefensePro DDoS Mitigation instances to support SYN Flood Protection among the cluster members.

Running several separate DefensePro 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 DefensePro 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 67: 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
Device-Management-Channel Netmask	(Read-only) The network mask of the device management channel. ¹
Cluster-Master IP Address	<p>The IP address of the cluster master. That is, the IP address to which cluster members connect.</p> <p>For this Radware DefensePro DDoS Mitigation instance to be the cluster master, specify the value in the Device-Management- Channel IP Address field.</p> <p>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.</p> <p>Caution: You can change the value only when the Cluster State is Disabled, after you have clicked Submit.</p>
Cluster State	<p>The state of the cluster or cluster membership.</p> <p>Values:</p> <ul style="list-style-type: none"> ● Enabled—One of the following: <ul style="list-style-type: none"> — 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: <ul style="list-style-type: none"> — 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. <p>Default: Disabled</p>

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 DefensePro. This chapter contains the following sections:

- [Managing Network Classes, page 133](#)
- [Managing Context Group Classes, page 134](#)
- [Managing Application Classes, page 135](#)
- [Managing MAC Address Classes, page 136](#)
- [Managing SGT Classes, page 137](#)

You can configure classes based on the following:

- **Networks**—To classify traffic in a Network Protection policy.
- **Context Groups**—To classify traffic in a Network Protection policy.
- **Application ports**—To define or modify applications based on Layer 4 destination ports.
- **MAC addresses**—To classify traffic whose source or destination is a transparent network device.
- **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 Network 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.



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 68: 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: 64
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: <ul style="list-style-type: none">• A subnet mask in dotted decimal notation—for example, 255.0.0.0 or 255.255.0.0.• An IP prefix, that is, the number of mask bits—for example, 8 or 16.

Managing Context Group Classes

You can define network segments using Context Group classes. Use them to classify traffic in security policies.

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 DefensePro device supports up to 64² definitions.



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 69: Context Groups Class Parameters

Parameter	Description
Context Group Name	The name of the group. Maximum characters: 19
Group Mode	Values: <ul style="list-style-type: none"> 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



- In the Configuration perspective, select **Classes > Applications**.
- 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.
- Configure the application class parameters, and then, click **Submit**.
- To activate your configuration changes on the device, click **Update Policies** ().

Table 70: 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.
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 MAC Address Classes

MAC groups identify traffic whose source or destination is a transparent network device.



To configure a MAC address class

1. In the Configuration perspective, select **Classes > Addresses**.
2. To add or modify a MAC address 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. Enter a name for the MAC group and the MAC address associated with the group, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** ().

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 71: SGT Class Parameters

Parameter	Description
Name	The name of the SGT. Maximum characters: 20
Value	The numerical SGT value. Values: 0–65535 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 DefensePro Network Protection Policies

Network Protection policies protect your configured networks using protection profiles. Each Network Protection policy uses one or more protection profiles that are applied on a predefined network segment. Each policy includes the action to take when an attack is detected.

Before you configure Network Protection policies and profiles, ensure that you have enabled all the required protections and configured the corresponding global protection parameters under **Setup > Security Settings**.



Note: The terms Network Protection Policy, and network policy may be used interchangeably in APSolute Vision and in the documentation.

There are two main types of network protections, intrusion preventions (see [Table 72 - Intrusion Prevention Protections, page 139](#)) and denial-of-service protection (see [Table 73 - Denial of Service Protections, page 139](#)). The set of supported protections depends on the Radware DefensePro DDoS Mitigation version.

Table 72: Intrusion Prevention Protections

Protection	Description
Signatures	Prevents known application vulnerabilities and exploitation attempts, and protects against known DoS/DDoS flood attacks.
DoS Shield	Protects against known flood attacks and flood-attack tools that can also cause a denial-of-service effect.

Table 73: Denial of Service Protections

Protection	Description
Behavioral DoS (BDoS)	Protects against zero-day DoS/DDoS-flood attacks.
Connection Limit	Protects against connection flood attacks.
DNS Protection	Protects against zero-day DNS-flood attacks.
Out-of-State Protection	Detects out-of-state packets to provide additional protection for TCP- session-based attacks.
SYN Protection	Protects against SYN-flood attacks using SYN cookies.

Configuring Network Protection Policies

Each Network Protection policy consists of 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, DefensePro considers the packet to be inbound. If the packet data matches the destination-to-source configuration, DefensePro 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.



Note: The terms Network Protection policy and network policy may be used interchangeably in APSolute Vision and in the documentation.

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Network 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 184](#).

Before you configure a policy, ensure that you have configured the following:

- The Classes that will be required to define the protected network segment. For more information, see [Managing Classes, page 133](#).
- The Network Protection profiles—for more information see:
 - [Configuring BDoS Profiles for Network Protection, page 164](#)
 - [Configuring Connection Limit Profiles for Network Protection, page 167](#)
 - [Configuring DNS Protection Profiles for Network Protection, page 177](#)
 - [Configuring Out of State Protection Profiles for Network Protection, page 181](#)
 - [Configuring Signature Protection for Network Protection, page 144](#)
 - [Configuring SYN Protection Profiles for Network Protection, page 170](#)



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 Network Protection policy, you must enter the value **none** for the profile.



To configure a Network Protection policy

1. In the Configuration perspective, select **Network Protection > Network 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 Network Protection policy parameters, and then, click **Submit**.
4. To activate your configuration changes on the device, click **Update Policies** (↻).

Table 74: Network Protection Policy: General Parameters

Parameter	Description
Enabled	Specifies whether the policy is enabled.
Policy Name	The name of the Network Protection policy. Maximum characters: 19 Caution: The name must not include a comma (,).

Table 75: Network Protection Policy: Classification Parameters

Parameter	Description
Priority	The unique priority of the Network Protection policy. The highest value is the highest priority. DefensePro processes each packet using one Network Protection policy. When there are multiple policies whose classification specification overlap, only the policy with the highest Priority processes the packet. Values: <ul style="list-style-type: none">• 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 Network 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.

Table 75: Network Protection Policy: Classification Parameters (cont.)

Parameter	Description
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.
Direction	The direction of the traffic to which the policy relates. Values: <ul style="list-style-type: none"> 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
Context	The Context Group class that the policy uses. Values: <ul style="list-style-type: none"> A Context Group class displayed in the Classes tab None

Table 76: Network Protection Policy: Profiles and Action Parameters

Parameter	Description
Protection Profiles	(Displayed in the table, not the configuration) The profiles applied to the network segment defined in this policy.
BDoS Profile	The BDoS profile applied to the network segment defined in this policy. Note: You can click the adjacent button to open the dialog box in which you can add and modify profiles.
DNS Profile	The DNS Protection profile applied to the network segment defined in this policy. Note: You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Signature Protection Profile	The Signature Protection profile applied to the network segment defined in this policy. Note: You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Out of State Profile	The Out of State profile to apply to the network segment defined in this policy. Note: You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Connection Limit Profile	The Connection Limit profile applied to the network segment defined in this policy. Note: You can click the adjacent button to open the dialog box in which you can add and modify profiles.

Table 76: Network Protection Policy: Profiles and Action Parameters (cont.)

Parameter	Description
SYN Flood Profile	The SYN Flood profile applied to the network segment defined in this policy. Note: You can click the adjacent button to open the dialog box in which you can add and modify profiles.
Action	The default action for all attacks under this policy. Values: <ul style="list-style-type: none"> Block and Report—The malicious traffic is terminated and a security event is generated and logged. Report Only—The malicious traffic is forwarded to its destination and a security event is generated and logged. Default: Block and Report Note: Signature-specific actions override the default action for the policy.


Table 77: Network 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 feature 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).
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 Network Protection policies, you have two options: **Delete Policy Only**, and **Delete Policy and Related Elements**.



To delete one or more Network Protection policies

- In the Configuration perspective, select **Network Protection > Network Protection Policies**.
- Select the row or rows.
- 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**, DefensePro 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 Signature Protection for Network Protection

Signature Protection detects and prevents network-oriented attacks, Operation System (OS) oriented attacks and application-oriented attacks by comparing each packet to the set of signatures stored in the Signatures database.

This section contains the following:

- [Signature Protection in DefensePro, page 144](#)
- [Configuration Considerations with Signature Protection, page 145](#)
- [Configuring Signature Protection Profiles, page 146](#)
- [Managing Signature Protection Signatures, page 148](#)
- [Managing Signature Protection Filters, page 158](#)
- [Configuring Signature Protection Attributes, page 161](#)

Signature Protection in DefensePro

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. These Radware profiles are updated along with the weekly signature database, which is maintained by the Radware Vulnerability Research Team (VRT).

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 signatures, you can create a new profile with those signatures and a new **Threat Type** attribute (see [Table 97 - Attribute Types, page 162](#)).



Notes

- The Radware Vulnerability Research Team (VRT) is responsible for researching, handling, and mitigating vulnerabilities, DDoS tools, and DDoS malware.
- If you require assistance creating a new signature, you can contact the relevant Radware department—according to your service agreement.
- 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 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

Radware 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 78 - Implications of Policy Directions, page 145](#).

Policies containing Signature Protection profiles can be configured with Direction set to either One Way or Two Way.

Protections can be configured 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 78: 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. The user-defined profile is 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 104](#) and [Configuring Global DoS Shield Protection, page 105](#).

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. 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.





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 (by VRT) 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 **Network Protection > 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 mouse cursor 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.

Rule Name	Attribute Type	Attribute Value
Search	Search	Search
+ Rule 1	+ Complexity + Confidence + Risk + Threat Type	Low High High DoS - Floods Worms

- 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**.
- To edit the attribute value of a rule:
- a. In the Attribute Type column of the table, move your mouse cursor 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.

Rule Name	Attribute Type	Attribute Value
Search	Search	Search
+ Rule 1	+ Complexity + Confidence + Risk + Threat Type	Low High High DoS - Floods Worms

- b. In the **Attribute Value** drop-down list, select or type the required value.
- c. Click **Submit**.



Note: Alternatively, to edit the attribute type and/or attribute value of an existing profile, you can do the following (as supported in APSolute Vision version 3.20 and earlier):

- 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 attributes.
 5. To save the signature profile configuration, click **Submit**.

Table 79: 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 163). 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.
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 80: 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 type, and each attribute type can contain one or more attribute values.
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 DefensePro tracks and treats malicious packets once DefensePro recognizes the signature in the traffic. Each attack is bound to a tracking function, which defines how DefensePro 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.

DefensePro divides signatures into the following types:

- **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 148](#).
- **Application Security signatures**—Use the Application Security mechanism. Application Security signatures support high complexity and string matching.

DefensePro provides predefined signatures, referred to as Radware-defined signatures or static signatures. You can also define your own signatures as necessary. You can edit and remove only these user-defined signatures. For Radware-defined signatures, you can edit only the general parameters.



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, Radware recommends that you specify as many additional attributes as possible, and prevent Radware DefensePro DDoS Mitigation using your user-defined signature improperly.

The tables that display the signatures provide filters that enable viewing Radware 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.



To locate all the policies and profiles that use a specific signature


1. In the Configuration perspective, select **Network Protection > 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 **Network Protection > 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 **Network Protection > 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 **Network Protection > 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.

5. Click the  (Filter) button.

Managing DoS Shield Signatures

The table in the DoS Shield tab 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 **Network Protection > 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 81: Signature: 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.

Table 81: Signature: General Parameters (cont.)

Parameter	Description
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 , DefensePro 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
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: <ul style="list-style-type: none"> Drop—Radware DefensePro DDoS Mitigation discards the packet. Report Only—Radware DefensePro DDoS Mitigation forwards the packet to the defined destination. Default: Drop
Packet Reporting	Enables the sending of sampled attack packets to APSolute Vision for offline analysis. Default: Disabled


Table 82: Signature: Attack Description

Parameter	Description
	(Read-only) A description of the static signature. You cannot configure a description for a user-defined signature.

Table 83: Signature: 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. For more information, see Configuring Filters for a DoS Shield Signature, page 152 .

Table 84: 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 Configuring Signature Protection Attributes, page 161).
	To add an attribute, in the table, click the  (Add) button.



To locate all the policies and profiles that use a specific signature

1. In the Configuration perspective, select **Network Protection > 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 **Network Protection > 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 85: Filter Parameters for 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: <ul style="list-style-type: none"> ● ICMP ● ICMPv6 ● IP ● TCP ● UDP Default: IP

Table 85: Filter Parameters for 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 135 .
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 135 .

Table 86: Filter Parameters for Signatures: 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: <ul style="list-style-type: none"> • 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, DefensePro uses the L3 content size as the packet size.

Table 87: Filter Parameters for Signatures: OMPC Parameters

Parameter	Description
Offset Mask Pattern Condition (OMPC) parameters are a set of attack parameters that define rules 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: <ul style="list-style-type: none"> • Equal • Greater Than • Not Applicable • Less Than • Not Equal Default: Not Applicable

Table 87: Filter Parameters for Signatures: OMPC Parameters (cont.)

Parameter	Description
OMPC Length	<p>The length of the OMPC data.</p> <p>Values:</p> <ul style="list-style-type: none"> • Not Applicable • 1 Byte • 2 Bytes • 3 Bytes • 4 Bytes <p>Default: 1 Byte</p>
OMPC Offset	<p>The location in the packet from where data checking starts looking for specific bits in the IP/TCP header.</p> <p>Values: 0–65,535</p> <p>Default: 0</p>
OMPC Offset Relative to	<p>Specifies to which OMPC offset the selected offset is relative. Values:</p> <ul style="list-style-type: none"> • None • IP Header • IP Data • L4 Data • L4 Header • Ethernet <p>Default: None</p>
OMPC Pattern	<p>The fixed size pattern within the packet that OMPC rules attempt to find.</p> <p>Values: A combination of hexadecimal numbers (0–9, a–f). The value is defined by the OMPC Length parameter.</p> <p>The OMPC Pattern definition contain eight symbols. When the OMPC Length is less than four bytes, complete it with zeros.</p> <p>For example, when the OMPC Length is two bytes, the OMPC Pattern can be abcd0000.</p> <p>Default: 00000000</p>
OMPC Mask	<p>The mask for the OMPC data.</p> <p>Values: A combination of hexadecimal numbers (0–9, a–f). The value is defined by the OMPC Length parameter.</p> <p>The OMPC Mask definition contains eight symbols. When the OMPC Length value is less than four bytes, complete it with zeros.</p> <p>For example, When the OMPC Length is two bytes, the OMPC Mask can be abcd0000.</p> <p>Default: 00000000</p>

Table 88: Filter Parameters for Signatures Content Parameters

Parameter	Description
	This feature is non-functional for DoS Shield signature filters.

Managing Application Security Signatures

The table in the Application Security tab displays all the Application Security (AppSec) signatures stored on the device. You can modify the signatures and create new ones as necessary.



To configure an Application Security signature

1. In the Configuration perspective, select **Network Protection > 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 89: Signature: 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	Specifies how Radware DefensePro DDoS Mitigation determines which traffic to block or drop when under attack. Values: <ul style="list-style-type: none"> ● 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.

Table 89: Signature: General Parameters (cont.)

Parameter	Description
<p>Tracking Period (This parameter is active only when the Tracking Type is not Track All.)</p>	<p>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, DefensePro 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.</p>
<p>Activation Threshold (This parameter is active only when the Tracking Type is not Track All.)</p>	<p>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.</p>
<p>Drop Threshold (This parameter is active only when the Tracking Type is not Track All.)</p>	<p>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.</p>
<p>Termination Threshold (This parameter is active only when the Tracking Type is not Track All.)</p>	<p>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.</p>

Table 89: Signature: General Parameters (cont.)

Parameter	Description
Action	<p>The action that Radware DefensePro DDoS Mitigation takes when an attack is detected.</p> <p>Values:</p> <ul style="list-style-type: none"> 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 as the Protocol (see Managing Basic Filters for Signatures, page 158). Report Only—Radware DefensePro DDoS Mitigation forwards the packet to the defined destination. <p>Default: Drop</p>
Packet Reporting	<p>Enables the sending of sampled attack packets to APSolute Vision for offline analysis.</p> <p>Default: Disabled</p>


Table 90: Signature: Attack Description

Parameter	Description
(Read-only)	<p>A description of the static signature.</p> <p>You cannot configure a description for a user-defined signature.</p>

Table 91: Signature: Filter Table

Parameter	Description
	<p>An Application Security signature can include one Basic filter to scan and classify traffic. Filters match scanned packets with attack signatures in the Signatures database.</p> <p>To specify the filter for the signature, from the Filter Name drop-down list, select the required filter.</p> <p>The Filter Name drop-down list contains the filters that are defined in the Basic Filters tab (see Managing Signature Protection Filters, page 158).</p>

Table 92: Signature: Attributes Table

Parameter	Description
	<p>The attributes for the signature determine the attack characteristics used in the rule creation process.</p> <p>The attributes in the Attributes Table tab are defined in the Attributes tab (see Configuring Signature Protection Attributes, page 161).</p> <p>To add an attribute, in the table, click the  (Add) button.</p>



To locate all the policies and profiles that use a specific signature

1. In the Configuration perspective, select **Network Protection > Signature Protection > Signatures > Application Security**.
2. Select the signature.
3. Click Find Usages.

Managing Signature Protection Filters

Use the Filters tab to manage the filters for Application Security signatures.

This version of Radware DefensePro DDoS Mitigation supports only Basic filters for Application Security signatures.

Managing Basic Filters for Signatures

Use the Basic Filter tab to manage the set of Basic filters for Application Security signatures.



To configure a filter for an Application Security signature


1. In the Configuration perspective, select **Network Protection > Signature Protection > Signatures > Filters > Basic Filters**.
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 93: 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: <ul style="list-style-type: none"> ● ICMP ● ICMPv6 ● IP ● TCP ● UDP Default: IP

Table 93: Filter: 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 135 .
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 135 .

Table 94: 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: <ul style="list-style-type: none"> • 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 95: Filter Parameters for Signatures: OMPC Parameters

Parameter	Description
Offset Mask Pattern Condition (OMPC) parameters are a set of attack parameters that define rules 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: <ul style="list-style-type: none"> • Equal • Greater Than • Not Applicable • Less Than • Not Equal Default: Not Applicable

Table 95: Filter Parameters for Signatures: OMPC Parameters (cont.)

Parameter	Description
OMPC Length	<p>The length of the OMPC (Offset Mask Pattern Condition) data. Values:</p> <ul style="list-style-type: none"> ● Not Applicable ● 1 Byte ● 2 Bytes ● 3 Bytes ● 4 Bytes <p>Default: 1 Byte</p>
OMPC Offset	<p>The location in the packet from where data checking starts looking for specific bits in the IP/TCP header.</p> <p>Values: 0–65,535</p> <p>Default: 0</p>
OMPC Offset Relative to	<p>Specifies to which OMPC offset the selected offset is relative. Values:</p> <ul style="list-style-type: none"> ● None ● IP Header ● IP Data ● L4 Data ● L4 Header ● Ethernet <p>Default: None</p>
OMPC Pattern	<p>The fixed size pattern within the packet that OMPC rules attempt to find.</p> <p>Values: A combination of hexadecimal numbers (0–9, a–f). The value is defined by the OMPC Length parameter.</p> <p>The OMPC Pattern definition contain eight symbols. When the OMPC Length is less than four bytes, complete it with zeros.</p> <p>For example, when the OMPC Length is two bytes, the OMPC Pattern can be abcd0000.</p> <p>Default: 00000000</p>
OMPC Mask	<p>The mask for the OMPC data.</p> <p>Values: A combination of hexadecimal numbers (0–9, a–f). The value is defined by the OMPC Length parameter.</p> <p>The OMPC Mask definition contains eight symbols. When the OMPC Length value is less than four bytes, complete it with zeros.</p> <p>For example, When the OMPC Length is two bytes, the OMPC Mask can be abcd0000.</p> <p>Default: 00000000</p>

Table 96: Filter Parameters for Signatures Content Parameters

Parameter	Description
	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. The Content parameters are available only for TCP, UDP, and ICMP.
Content Type	Specifies whether the filter tries to match specific text. Values: <ul style="list-style-type: none"> ● Not Applicable—The filter does not try to match the L4 data of the packet. ● Text—The filter tries to match text anywhere in the packet. Default: Not Applicable
Content Encoding (This parameter is available only when the Content Type is not Not Applicable .)	Application Security can search for content in languages other than English, for case-sensitive or case-insensitive text, and hexadecimal strings. Values: <ul style="list-style-type: none"> ● Not Applicable ● Case Insensitive ● Case Sensitive ● Hex Default: Case Insensitive
Content (This parameter is available only when the Content Type is not Not Applicable .)	The value of the content search, except for HTTP headers, cookies, and FTP commands. 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 { } ~
Regular Expression Content	Specifies whether the Content 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.

Configuring 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. The Radware Vulnerability Research Team (VRT) assigns the attributes when creating the signature as a way to describe the signature.

You can use the existing attributes, add new attributes, or remove attributes from the list.



Note: You can view properties of attribute types, and for the attribute types Complexity, Confidence, and Risk, you can also specify the **Match Method (Minimum or Exact)**. For more information, see [Viewing and Modifying Attribute Type Properties, page 163](#).

Attributes are derived from the Signatures database and are added dynamically with any update.



To configure Signature Protection attributes




1. In the Configuration perspective, select **Network Protection > Signature Protection > Attributes**.
2. To view attributes:
 - To view all attributes, select All and click the  (Search) button.
 - To view attributes for a single attribute type, select the attribute type and click the  (Search) button.
3. To add a new attribute:
 - a. Click the  (Add) button.
 - b. Select the attribute type, and enter the attribute name.
 - c. Click **Submit**.

Table 97: Attribute Types

Attribute Type	Description
Applications	The applications that are vulnerable to this exploit. Examples: Web servers, mail servers, browsers The parameter is optional; that is, the attribute may or may not contain a value. There can be multiple values.
Complexity	The level of analysis performed as part of the attack lookup mechanism. There can be only a single value for the parameter. Values: <ul style="list-style-type: none">● Low—This signature has negligible impact on device performance.● High—This signature has stronger impact on the device performance.
Confidence	The level of certainty to which an attack can be trusted. The confidence level is the opposite of the false-positive level associated with an attack. For example, if the attack confidence level is set to high, its false-positive level is low. The parameter is mandatory. There can be only a single value for the parameter. Values: Low, High, Medium
Groups	Enables you to create customized attack groups.
Platforms	The operating systems that are vulnerable to this exploit. Examples: Windows, Linux, Unix The parameter is optional; that is, the attribute may or may not contain a value. There can be multiple values.

Table 97: Attribute Types (cont.)

Attribute Type	Description
Risk	The risk associated with the attack. For example, attacks that impact on the network are very severe and are defined as high-risk attacks. The parameter is mandatory. There can be only a single value for the parameter. Values: Info, Low, Medium, High
Services	The protocol that is vulnerable to this exploit. Examples: FTP, HTTP, DNS The parameter is optional; that is, the parameter may or may not contain a value. There can be only a single value for the parameter.
Target	The target of the threat—client side or server side.
Threat Type	The threats that best describe the signature. Examples: floods, worms There can be multiple values.

Viewing and Modifying Attribute Type Properties

You can view the following properties of the attribute types that the device supports:

- **Multiple Values in Attack**—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.
- **Multiple Values 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, 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**.
 - **Exact**—Specifies that the **Attribute Value** uses only its own results. For example, when the **Attribute Type** is **Risk** with **Match Method Exact**, the **Attribute Value High** uses only for High-risk results.

You can change the **Match Method** for the attribute types **Complexity**, **Confidence**, and **Risk**.



To view the attribute types that the device supports

- > In the Configuration perspective, select **Network Protection > Signature Protection > Attributes > Attribute Type Properties**.



To change the Match Method for Complexity, Confidence, and Risk attribute types

1. In the Configuration perspective, select **Network Protection > 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 BDoS Profiles for Network 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.

To configure BDoS profiles, BDoS Protection must be enabled (Configuration perspective, **Setup > Security Settings > BDoS Protection**).

Radware DefensePro DDoS Mitigation for Cisco Firepower version 8.13 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, DNS servers segment, Web server segments, Mail servers segments, and so on). This assures optimized learning of normal traffic 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 110](#).



To configure a BDoS profile


1. In the Configuration perspective, select **Network Protection > 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, and click **Submit**.

Table 98: BDoS Profile: General Parameters

Parameter	Description
Profile Name	The name of the BDoS profile.
Enable Transparent Optimization	<p>Specifies whether transparent optimization is enabled.</p> <p>Some network environments are more sensitive to dropping packets (for example, VoIP). Therefore, it is necessary to minimize the probability that legitimate traffic is dropped by the IPS device. This transparent optimization can occur during BDoS closed-feedback iterations until a final footprint is generated.</p> <p>Note: When transparent optimization is enabled, the profile does not mitigate the attack until the final footprint is generated, which takes several seconds.</p>

Table 99: BDoS Profile: Flood Protection Settings Parameters

Parameter	Description
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 100: BDoS Profile: Bandwidth Parameters

Parameter	Description
Inbound Traffic	<p>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.</p> <p>Values: 1–33,554,430</p> <p>Caution: You must configure this setting to start Behavioral DoS protection.</p> <p>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.</p> <p>Note: For the definition of inbound traffic and outbound traffic, see Configuring Network Protection Policies, page 140.</p>
Outbound Traffic	<p>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.</p> <p>Values: 1–32,000,000</p> <p>Caution: You must configure this setting to start Behavioral DoS protection.</p> <p>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.</p> <p>Note: For the definition of inbound traffic and outbound traffic, see Configuring Network Protection Policies, page 140.</p>

Table 101: BDoS Profile: Quota Settings Parameters

Parameter	Description
Default Quota (button)	Restores the hard-coded default values to all the quotas.
TCP	<p>For each traffic type, specify the quota—the maximum expected percentage of incoming and outgoing traffic out of the total traffic.</p> <p>Radware 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.</p> <p>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.</p> <p>Note: The total quota values may exceed 100%, because each value represents the maximum volume per protocol.</p>
UDP	
Fragmented UDP	
ICMP	
IGMP	

Table 102: BDoS Profile: Advanced Parameters

Parameter	Description
UDP Packet Rate Detection Sensitivity	<p>The packet-rate detection sensitivity—that is, to what extent the BDoS engine considers the UDP PPS-rate values (baseline and current).</p> <p>This parameter is relevant only for only for BDoS UDP protection. Values:</p> <ul style="list-style-type: none"> • Disable • Low • Medium • High <p>Default: Low</p> <p>Note: In certain legacy versions, this parameter is labeled Level Of Regularization.</p>

Table 103: BDoS Profile: Packet Reporting and Trace Setting Parameters

Parameter	Description
Packet Report	<p>Specifies whether the profile sends sampled attack packets to APSolute Vision for offline analysis.</p> <p>Note: When this feature is enabled, for the feature to take effect, the global setting must be enabled (Configuration perspective, Setup > Reporting Settings > Advanced Reporting Settings > Packet Reporting and > Enable Packet Reporting).</p>
Packet Trace	This version does not support the Packet Trace feature.

Configuring Connection Limit Profiles for Network Protection

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.

Recommended settings for policies that include Connection Limit profiles:

- Configure policies containing Connection Limit profiles using Networks only with source = Any, the public network, and destination = 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.
- Policies containing Connection Limit profiles can be configured 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 **Network Protection > 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 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 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 169](#).



Note: A Connection Limit profile should include all the Connection Limit attacks that you want to apply in a Network Protection policy.

Table 104: 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 <ol style="list-style-type: none"> 1. In the table, click the + (Add) button. 2. From the Protection Name drop-down list, select the protection, and then, click Submit. <p>Note: In each Network 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.</p>
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 for network protection.



To configure a Connection Limit protection

1. In the Configuration perspective, select **Network Protection > 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 105: 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 Name	The Layer 4 port or class object that defines the application you want to protect. To specify any port, the field may contain the value any or be empty. Note: You can click the adjacent button to open the dialog box in which you can add a class.
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 or source-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: <ul style="list-style-type: none">• 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. Default: Source Count

Table 105: Connection Limit Protection Parameters (cont.)

Parameter	Description
Action	The action when an attack is detected. Values: <ul style="list-style-type: none"> Drop—The packet is discarded. Report-only—The packet is forwarded to the destination IP address. Default: Drop
Risk	The risk assigned to this attack for reporting purposes. Values: High, Info, Low, Medium Default: Medium
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 and Packet Trace > Enable Packet Reporting).

Configuring SYN Protection Profiles for Network Protection

SYN Protection profiles defend against SYN-flood attacks.

You can configure up to 50 SYN Protection profiles on a DefensePro 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 Protection profile, ensure the following:

- 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 global settings apply to all the profiles on the device. For more information, see [Configuring Global SYN Flood Protection, page 150](#).



To configure a SYN Protection profile


1. In the Configuration perspective, select **Network Protection > SYN Protection Profiles**.
2. Do one of the following:
 - To add a profile, click the **+** (Add) button. Enter the profile name and 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 Protections Table**.



Note: A SYN profile should contain all the SYN flood protections that you want to apply in a Network Protection policy.

Table 106: SYN Protection Profile Parameters

Parameter	Description
Profile Name	(Read-only) The name of the profile.
SYN Protection Table	<p>Contains the protections applied for the selected profile.</p> <p>To add a protection, in the table, click the  (Add) button, select the protection name, and click Submit.</p> <p>Note: In each Network 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.</p>
Go to Protection SYN Table (button)	Opens the SYN Protections tab in which you can add and modify SYN protections.
Go to Profile Parameters (button)	Opens the Profile Parameters tab in which you can view and modify the configuration of the SYN Protection profiles.

Defining SYN Flood Protections

After you define SYN flood protections, you can add them to SYN profiles.



To define a SYN protection


1. In the Configuration perspective, select **Network Protection > SYN Protection Profiles > SYN 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 107: SYN Flood Protection Parameters

Parameter	Description
Protection Name	A name for easy identification of the attack for configuration and reporting. Note: Predefined SYN 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 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. Note: You can click the adjacent button to open the dialog box in which you can add a class.
Activation Threshold	A number of SYN packets received per second at a certain destination above which Radware DefensePro DDoS Mitigation starts the mitigation actions. Values: 1–150,000 Default: 2500
Termination Threshold	A number of SYN packets received per second at a certain destination for specified Tracking Time ¹ below which Radware DefensePro DDoS Mitigation stops the mitigation actions. Values: 0–150,000 Default: 1500
Risk	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 Radware recommends.

Table 108: Verification Type Values Parameters

Protocol	Destination Port	Verification Type
FTP_CNTL	21	ack
HTTP	80	request
HTTPS	443	request
IMAP	143	ack
POP3	110	ack
RPC	135	ack
RTSP	554	request

Table 108: Verification Type Values Parameters (cont.)

Protocol	Destination Port	Verification Type
SMTP	25	ack
TELNET	23	ack

Managing SYN Protection Profile Parameters

After you define a SYN Protection profile, you can configure the authentication parameters for it.



To configure SYN Protection profile parameters

1. In the Configuration perspective, select **Network Protection > SYN Protection Profiles > Profiles Parameters**.
2. Double-click the relevant profile.
3. Configure the parameters, and then, click **Submit**.

Table 109: SYN Flood Protection Profile Parameters

Parameter	Description
Profile Name	(Read-only) The name of the profile.
Network Level Authentication	
Use TCP Reset for Supported Protocols	<p>Specifies whether DefensePro uses the TCP-Reset method for HTTP, HTTPS, SMTP, and custom-protocol traffic rather than the default Authentication Method: Safe-Reset.</p> <p>Radware recommends enabling the Use TCP Reset for Supported Protocols option in symmetric and ingress-only environments that include HTTP, HTTPS, and SMTP traffic.</p> <p>Default: Disabled</p> <p>Notes:</p> <ul style="list-style-type: none"> • For more information on the TCP-Reset method, see TCP Reset, page 175. • Using the Safe-Reset method, when DefensePro receives a SYN packet, DefensePro responds with an ACK packet with an invalid Sequence Number field as a cookie. If the client responds with RST and the cookie, DefensePro 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 DefensePro, and the session is approved for the server. DefensePro saves the source IP address for a specified time.

Table 109: SYN Flood Protection Profile Parameters (cont.)

Parameter	Description
Application Level Authentication	
Use HTTP Authentication	<p>Specifies whether DefensePro authenticates the transport layer of HTTP traffic using SYN cookies and then authenticates the HTTP application layer using the specified HTTP Authentication Method.</p> <p>Values:</p> <ul style="list-style-type: none"> Enabled—DefensePro authenticates the transport layer of HTTP traffic using SYN cookies, and then, authenticates the HTTP application layer using the specified HTTP Authentication Method. Disabled—DefensePro handles HTTP traffic using the specified TCP Authentication Method. <p>Default: Disabled</p>
HTTP Authentication Method	<p>The method that the profile uses to authenticate HTTP traffic at the application layer.</p> <p>Values:</p> <ul style="list-style-type: none"> 302-Redirect—Radware DefensePro DDoS Mitigation authenticates HTTP traffic using a 302-redirect response code. JavaScript—Radware DefensePro DDoS Mitigation authenticates HTTP traffic using a JavaScript object, which DefensePro generates. <p>Default: 302-Redirect</p> <p>Notes:</p> <ul style="list-style-type: none"> Some attack tools are capable of handling 302-redirect responses. 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 Authentication Method: <ul style="list-style-type: none"> 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

¹ – For example, if the protected server supplies content that is requested using a JavaScript tag, the DefensePro JavaScript is enclosed within the original JavaScript block. This violates JavaScript rules, which results in a challenge failure. In the following example, the request accesses a secure server. The returned challenge page contains the <script> tag again, which is illegal, and therefore, it is dropped by the browser without making the redirect.

```
<script> setTimeout(function(){
    varjs=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

Radware recommends enabling the TCP-Reset option in symmetric and ingress-only environments that include HTTP, HTTPS, and SMTP traffic.



Caution: When DefensePro 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, DefensePro 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 8.13, is Safe-Reset).

Custom-protocol refers to traffic that you define for the TCP-Reset method to handle. To enable you to do this, DefensePro 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 176.](#))

When DefensePro implements the TCP-Reset method, DefensePro 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

DefensePro 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, DefensePro does the following:

1. When it receives a SYN packet, DefensePro 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, DefensePro waits for the first data packet from the client. (If DefensePro receives an ACK with no data before the first data packet, DefensePro drops the packet.) When the DefensePro 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, DefensePro 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. DefensePro checks each SYN packet against the entries in the TCP Authentication table. If there is a match, DefensePro forwards the packet to the other DefensePro inspection modules and later forwards the SYN packet to the destination as-is, so the protected server will open a connection with the source.
4. Once DefensePro has authenticated a source, DefensePro 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 DefensePro receives multiple SYNs from the same source, DefensePro implements the TCP-Reset authentication process per SYN packet, until one of the connections is authenticated.
- DefensePro always uses the TCPReset-Data behavior ([step 2](#) above) for traffic through ports included in **HTTP** Application Port Group and **HTTPS** Application Port Group.
- DefensePro 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 For Supported Protocols** checkboxes, DefensePro 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 150](#)), DefensePro always uses the TCP-Reset method, regardless of other SYN Protection profile configuration.



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 a single 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 Protection profile (see [To configure a SYN Protection profile, page 170](#)).
3. Configure a SYN Protection (see [To define a SYN protection, page 171](#)) for the SYN 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 DNS Protection Profiles for Network Protection

To configure DNS Protection profiles, DNS Flood Protection must be enabled (Configuration perspective, **Setup > Security Settings > DNS Flood Protection**).

When you configure a DNS 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 8.13 supports a maximum of 50 DNS Protection profiles.

Radware recommends configuring Network Protection policies that include DNS Protection profiles using networks with **SRC Network** set to **any** (that is, the public network) and **DST Network** set to the protected network.

DNS Protection profiles operate only on ingress traffic. However, you can use a DNS 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 122](#).



To configure a DNS Protection profile

1. In the Configuration perspective, select **Network Protection > DNS 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, and click **Submit**.

Table 110: DNS Protection Profile: General Parameter

Parameter	Description
Name	The name of the profile.

Table 111: DNS Protection Profile: Query Protections and Quotas Parameters

Parameter	Description
Default Quotas (button)	Configures all the quotas with the hard-coded default values after you have specified the Expected DNS Query Rate (in the Rate Settings tab).
Select All Query Types	Specifies whether the profile protects all the listed DNS query types. Default: Disabled

Table 111: DNS Protection Profile: Query Protections and Quotas Parameters (cont.)

Parameter	Description
A Query	<p>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.</p> <p>Radware 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.</p> <p>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.</p> <p>Note: The total quota values may exceed 100%, because each value represents the maximum volume per query type.</p>
MX Query	
PTR Query	
AAAA Query	
Text Query	
SOA Query	
NAPTR Query	
SRV Query	
Other Queries	

Table 112: DNS Protection Profile: Rate Settings Parameters

Parameter	Description
<p>Note: The device implements the parameters in this tab only when the Use Manual Triggers option is disabled.</p>	
Expected DNS Query Rate	<p>The expected rate, in queries per second, of DNS queries.</p> <p>Caution: When you change the Expected DNS Query Rate and click Submit, the quota settings (see Table 111 - DNS Protection Profile: Query Protections and Quotas Parameters, page 177) 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.</p>
Max Allowed QPS	<p>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).</p> <p>Values: 0–4,000,000 Default: 0</p> <p>Caution: If the Max Allowed QPS is lower than the DNS baseline, the profile drops every packet that matches the real-time signature.</p>
Signature Rate-Limit Target	<p>The maximum level of DNS traffic, in percent, relative to the DNS baseline, that the profile allows under a DNS-flood attack. This is relevant to the traffic that matches the real-time signature.</p> <p>Values: 0–100 Default: 0</p> <p>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.</p>

Table 113: DNS 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 , DefensePro 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 DefensePro 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 DefensePro 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 DefensePro 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
Escalation Period	The time, in seconds, that DefensePro waits before escalating to the next enabled Mitigation Action. Values: 0–30 Default: 3 Note: For more information on Mitigation Actions, see Table 55 - DNS Flood Protection: Mitigation Actions Parameters, page 120 .

Table 114: DNS Protection Profile: Subdomains Whitelist Parameters

Parameter	Description
	<p>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.</p> <p>There is one Subdomains Whitelist per DNS Protection profile per Network Protection policy. You can export and import the Subdomains Whitelist as a text file.</p> <p>The Subdomains Whitelist file can include the following types of FQDNs:</p> <ul style="list-style-type: none"> 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. <p>Note: You can manually add this entry type, and it will age as part of the aging mechanism.</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>You can import a Subdomains Whitelist file into the current profile that is configured in the specified Network Protection policy.</p>
Network Protection Policy	The Network Protection policy for which you want to apply actions on the Subdomains Whitelist. A DNS Protection profile can be used in multiple Network 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 Network 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.
Clear Subdomains Whitelist Before Importing	Values: <ul style="list-style-type: none"> 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 Network 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 Network Protection Policy . ¹
Clear All Entries (button)	Clears all entries from the current Subdomains Whitelist of the profile that is configured in the selected Network Protection Policy . ¹

¹ – The profile must be configured in the selected **Network Protection Policy**.

Table 115: DNS Protection Profile: Packet Reporting Settings Parameters

Parameter	Description
Packet Reporting	Specifies whether DefensePro sends sampled attack packets to APSolute Vision for offline analysis. Default: Disabled Note: When this feature is enabled, for the feature 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).

Table 116: DNS Protection Profile: Action

Parameter	Description
Note: The device implements the parameters in this tab only when the Manual Triggers option is not enabled.	
Profile Action	The action that the profile takes on DNS traffic during an attack. Values: Block & Report, Report Only Default: Block & Report

Configuring Out of State Protection Profiles for Network Protection

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**).

In this version of Radware DefensePro DDoS Mitigation, you can configure up to 50 Out of State Protection profiles.



Caution: In cases of overlapping Network 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 **Network Protection > Out Of State 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, and click **Submit**.

Table 117: 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 DefensePro 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 DefensePro 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 DefensePro resumes normal operation. Values: 0–249,999 Default: 4000
Profile Risk	The risk—for reporting purposes—assigned to the attack that the profile detects. Values: Info, Low, Medium, High Default: Low
Allow SYN-ACK	Values: <ul style="list-style-type: none"> • Enabled—The DefensePro device opens a session and processes a SYN-ACK packet even when the DefensePro has identified no SYN packet for the session. This option supports asymmetric environments, when the first packet that DefensePro receives is the SYN-ACK. • Disabled—When the DefensePro device receives a SYN-ACK packet and has identified no SYN packet for the session, DefensePro passes through the SYN-ACK packet (unprocessed) if the packet is below the specified activation threshold, and DefensePro drops the packet if it is above the specified activation threshold. Default: Enabled
Enable Packet Reporting	Specifies whether the profile reports out-of-state packets. 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 and Packet Trace > Enable Packet Reporting). In addition, a change to this parameter takes effect only after you update policies.
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

Chapter 6 – Managing DefensePro Operations and Maintenance

This chapter describes the following operation and maintenance tasks:

- [Updating Policy Configurations on a DefensePro Device, page 183](#)
- [Rebooting or Shutting Down a DefensePro Device, page 184](#)
- [Using Configuration Templates for Security Policies, page 184](#)
- [Configuring Multiple Devices, page 191](#)
- [Downloading a Device's Log File to APSolute Vision, page 193](#)
- [Updating a Radware Signature File, page 193](#)
- [Downloading Technical-Support and Configuration Files, page 195](#)
- [Managing DefensePro Device Configurations, page 196](#)
- [Resetting the Baseline for DefensePro, page 198](#)
- [Scheduling APSolute Vision and Device Tasks, page 199](#)
- [Updating the Attack Description File, page 212](#)



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 64](#).
- 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 DefensePro, which automate and streamline common configuration and management actions. For more information, see the APSolute Vision User Guide or online help.


Updating Policy Configurations on a DefensePro Device

You can apply the following configuration changes to a Radware DefensePro DDoS Mitigation device in a single operation:

- Network Protection policy
- Classes



To update policy configurations on a DefensePro device

- > In the device pane, select the device, and then, click **Update Policies** (.


Rebooting or Shutting Down a DefensePro 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 Network Protection policy and/or Server Protection policy.

A template from a Network 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 DefensePro device (that is, the target DefensePro device into which you are importing the policy template). For example, if you export a Network Protection policy that includes a BDoS Protection profile, the DefensePro device into which you are importing the policy template must have BDoS Protection enabled globally (Configuration perspective, **Setup > Security Settings > BDoS Protection > Enable BDoS Protection**).
- **User-defined signatures.**
- **SYN Protection profiles with a user-defined SYN Protection.**



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, DefensePro recalculates the baseline or baselines according to the configuration of the profile. (For information on the configuration of profiles, see [Configuring BDoS Profiles for Network Protection, page 164](#) and [Configuring DNS Protection Profiles for Network Protection, page 177](#).)



Notes

- The terms Network Protection policy, and network policy may be used interchangeably in APSolute Vision and in the documentation.
- You can import Network Protection policies from DefensePro platforms running supported 6.x versions into platforms running supported 6.x or 7.x versions.
- You can import Network Protection policies from DefensePro platforms running supported 7.x versions into platforms running supported 7.x versions.
- You can import Network Protection policies from DefensePro platforms running supported 8.x versions into platforms running supported 8.x versions.
- APSolute Vision provides a predefined Toolbox script for exporting and importing DefensePro configurations, DefensePro Export/Import Policies. For more information, see the APSolute Vision User Guide or online help.

Exporting a Network Protection Policy as a Template

Use the following procedure to export a Network Protection policy as a template.



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 118: Export Network Protection Parameters

Parameter	Description
Download To	Values: <ul style="list-style-type: none"> • Client—DefensePro exports the template to the location specified in the filepath or by browsing to the location with the Browse button. • Server—DefensePro exports the template to the APSolute Vision database. Default: Server
Configuration	Specifies whether DefensePro exports the template with the configuration of the policy. Default: Enabled
DNS Baseline	Specifies whether DefensePro exports the template with the current DNS baseline of the policy. Default: Enabled

Table 118: Export Network Protection Parameters (cont.)

Parameter	Description
BDoS Baseline	Specifies whether DefensePro exports the template with the current BDoS baseline of the policy. Default: Enabled
User-Defined Signature Protection Profile	Specifies whether Radware DefensePro DDoS Mitigation exports the template with the current user-defined Signature Protection 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: MyDefensePro_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 DefensePro Configuration Templates

Use the DefensePro Configuration Templates pane to manage security-protection templates.

The DefensePro Configuration Templates pane contains the table of templates, which comprises the following columns:

- **Source Device Name**—Displays one of the following:
 - 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 Network 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 DefensePro devices.**
- **Delete the templates from one or more DefensePro devices**—The delete command does the following:
 - Removes the selected templates from the table.
 - Removes, from the DefensePro 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 template table.**
- **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. Click the **Toolbox** () button.
2. Click the **Advanced** () button to open the DefensePro Configuration Templates pane.
3. Configure the parameters, and then, click the  (Search) button.

Table 119: Template-List Filter Parameters

Parameter	Description
Source Device Name	Values: <ul style="list-style-type: none">● 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: <ul style="list-style-type: none">● Server Protection—Shows the templates from Server Protection policies.● Network Protection—Shows the templates from Network Protection policies.
File Name	The filename that the filter uses. The value supports one or two wildcards (*). Examples: <ul style="list-style-type: none">● *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. Click the **Toolbox** () button.
2. Click the **Advanced** () button to open the DefensePro Configuration Templates pane.
3. Click **Clear**.



To send templates to DefensePro devices



1. Click the **Toolbox** () button.
2. Click the **Advanced** () button to open the DefensePro Configuration Templates pane.
3. Configure the filter as necessary (see the procedure [To filter the display of the template list, page 187](#)).
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 120: Send to Devices: Select Devices to Update Parameters

Parameter	Description
	<p>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.</p> <p>Select entries from the lists and use the arrows to move the entries to the other lists as required.</p> <p>Notes:</p> <ul style="list-style-type: none"> • 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 34.
Update Method	<p>Values:</p> <ul style="list-style-type: none"> • Append to 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 name exists in a target device, the update fails. • 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. <p>Default: Overwrite Existing Configuration</p>

Table 120: Send to Devices: Select Devices to Update Parameters (cont.)

Parameter	Description
Install on Instance (This parameter is relevant only for DefensePro x420 platforms.)	The identifier of the Radware DefensePro DDoS Mitigation hardware instance onto which to add the template. Values: 0, 1 Default: 0
Update Policies After Sending Configuration	Values: <ul style="list-style-type: none"> • 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



To delete templates and associated configuration objects from DefensePro devices



1. Click the **Toolbox** () button.
2. Click the **Advanced** () button to open the DefensePro Configuration Templates pane.
3. Configure the filter as necessary (see the procedure [To filter the display of the template list, page 187](#)).
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 121: Delete from Devices: Select Devices to Update Parameters

Parameter	Description
	<p>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.</p> <p>Select entries from the lists and use the arrows to move the entries to the other lists as required.</p> <p>Notes:</p> <ul style="list-style-type: none"> • The Available device list can contain only the devices that support the templates features. • The Selected device list can contain only DefensePro 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 34.
Update Policies After Sending Configuration	<p>Values:</p> <ul style="list-style-type: none"> • 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. <p>Default: Disabled</p>



To add (upload) templates from another location to the template list






1. Click the **Toolbox** () button.
2. Click the **Advanced** () button to open the DefensePro Configuration Templates pane.
3. Click the **+** (Add) button.
4. Configure the parameters, and then click **Submit**.

Table 122: Upload File to Server Parameters

Parameter	Description
File Type	<p>Values:</p> <ul style="list-style-type: none"> • Server Protection—The template defines a Server Protection policy. • Network Protection—The template defines a Network 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. Click the **Toolbox** () button.
2. Click the **Advanced** () button to open the DefensePro Configuration Templates pane.
3. Configure the filter as necessary (see the procedure [To filter the display of the template list, page 187](#)).
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. Click the **Toolbox** () button.
2. Click the **Advanced** () button to open the DefensePro Configuration Templates pane.
3. Configure the filter as necessary (see the procedure [To filter the display of the template list, page 187](#)).
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 69](#).
- 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 56](#).




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 66](#).

2. Click . 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 69](#).
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 or the Physical Containers tree, and 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.

2. Click the  (View) button.

3. Click . 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 try to change.
6. Click **Go**. The GUI of the lead device opens. The device pane shows the lead device and the 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

You can upload an updated Radware signature file to a DefensePro device.

You can upload an updated Radware signature file to a DefensePro 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 DefensePro physical platforms.
 - <Device-IP-address>.sig—For DefensePro virtual platforms.



Caution: Updating the signature file consumes large amounts of resources, which may cause the device to go temporarily into an overload state. Radware recommends updating the signature file during hours of low activity.



Note: You can schedule signature-file updates in the APSolute Vision scheduler. For more information, see [Configuring Tasks in the Scheduler, page 200](#).



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 123: Update Device Signature File Parameters

Parameter	Description
Signature Type	The type of the signature file to upload to the device. Values: <ul style="list-style-type: none"> • Radware Signatures • RSA Signatures
Update From	The location of the signature file to upload. Values: <ul style="list-style-type: none"> • 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 available for Radware signatures.
File Name (This parameter is displayed only when Update From Client is selected)	Name of the signature file on the client system.



Note: A signature file on a Radware DefensePro DDoS Mitigation device may also be referred to as the attack database.

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 Radware 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 124: 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 using CLI

- > In the CLI, run the following command:
`manage support save-file`

Managing DefensePro Device Configurations

This section describes how to manage configurations of the DefensePro devices that are configured on APSolute Vision.

DefensePro Configuration File Content

The configuration file content is divided into two sections:

- **Commands that require rebooting the device**—These include Application Security status, Operation Mode, tuning parameters, 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 are not 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.

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 parameter 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 200](#).



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 125: 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. You must include the private key information to restore the private keys; otherwise, the device reverts to default keys. Default: Disabled
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, DefensePro can print the configuration file to screen or download the configuration as a file.

DefensePro 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 126: 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 client system, 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 server, select the configuration to upload.

Resetting the Baseline for DefensePro

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 Network Protection policies that contain a BDoS or DNS Protection profile, or for a selected Network Protection policy that contains a BDoS or DNS Protection profile.

For information about managing Network Protection policies, see [Managing DefensePro Network Protection Policies, page 139](#).



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 Network Protection policies that contain a BDoS profile, or for a specific Network 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 Network Protection policies that contain a DNS profile, or for a specific Network Protection policy that contains a DNS profile.
3. Click **Submit**.



Note: APSolute Vision provides a predefined Toolbox script for exporting and importing DefensePro 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 199](#)
- [Configuring Tasks in the Scheduler, page 200](#)
- [Task Parameters, page 202](#)



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.

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 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:

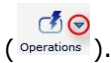
- Back up a device configuration
- Back up the APSolute Vision Reporter data
- Reboot a device

- Update the Radware security signature file onto a DefensePro device from Radware.com or the proxy server
- Run an Operator Toolbox script



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 DefensePro Device, page 184](#)
- [Updating a Radware Signature File, page 193](#)
- [Downloading a Device-Configuration File, page 196](#)

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 32: 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 **Sort Ascending** or **Sort Descending**.

Name	Descrip	Current St	Ena
Search			
MyAAADeviceConfigBUTas			
MyAPVisionConfigBackup	Backs	Waiting	En
MyDeviceRebootTask		Waiting	En



Note: For more information on filtering table rows, see [Filtering Table Rows, page 15](#).

Table 127: Tasks Table Parameters




Parameter	Description
Task Type	The type of task to be performed.
Name	The name of the configured task.
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.

Table 127: Tasks Table Parameters (cont.)

Parameter	Description
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Daily • Minutes • Once • Weekly





To configure a scheduled task

1. In the APSolute Vision toolbar, click the  (Scheduler) button. The Tasks 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 5](#)



To run an existing task

1. In the APSolute Vision toolbar, click the  (Scheduler) button. The Tasks 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 Radware DefensePro DDoS Mitigation-related Scheduler tasks:

- [APSolute Vision Reporter Backup—Parameters, page 202](#)
- [Update Security Signature Files—Parameters, page 204](#)
- [Device Configuration Backup—Parameters, page 206](#)
- [Device Reboot Task—Parameters, page 208](#)
- [Operator Toolbox Task—Parameters, page 210](#)



Note: Some tasks that APSolute Vision exposes are non-operational/irrelevant for certain Radware DefensePro DDoS Mitigation versions.

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 data 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 description Scheduler-generated.

Table 128: 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 129: APSolute Vision Reporter Backup: Schedule Parameters

Parameter	Description
Run	<p>The frequency at which the task runs.</p> <p>Select a frequency, then configure the related time and day/date parameters.</p> <p>Values:</p> <ul style="list-style-type: none"> 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. <p>Note: Tasks run according to the time as configured on the APSolute Vision client.</p>
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	<p>Specifies whether the task always runs or only during the defined period. Values:</p> <ul style="list-style-type: none"> 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. <p>Default: Enabled</p>
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 130: APSolute Vision Reporter Backup: Destination Parameters

Parameter	Description
Backup Configuration To	The destination of the backup configuration files. Values: <ul style="list-style-type: none"> • APSolute Vision Server • APSolute Vision and External Location Default: APSolute Vision Server
Protocol ¹	The protocol that APSolute Vision uses for this task. Values: <ul style="list-style-type: none"> • FTP • SCP • SFTP • SSH
IP Address ¹	The IP address of the external location.
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 15 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 DefensePro devices.

Table 131: Update Security Signature Files: 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 132: Update Security Signature Files: Schedule Parameters

Parameter	Description
Run	<p>The frequency at which the task runs.</p> <p>Select a frequency, then configure the related time and day/date parameters.</p> <p>Values:</p> <ul style="list-style-type: none"> 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. <p>Note: Tasks run according to the time as configured on the APSolute Vision client.</p>
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	<p>Specifies whether the task always runs or only during the defined period. Values:</p> <ul style="list-style-type: none"> 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. <p>Default: Enabled</p>
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 133: Update Security Signature Files: Target Device List

Parameter	Description
	<p>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.</p> <p>Select entries from the lists and use the arrows to move the entries to the other lists as required.</p> <p>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 34.</p>

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 134: 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 135: Device Configuration Backup: Schedule Parameters

Parameter	Description
Run	<p>The frequency at which the task runs.</p> <p>Select a frequency, then configure the related time and day/date parameters.</p> <p>Values:</p> <ul style="list-style-type: none"> 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. <p>Note: Tasks run according to the time as configured on the APSolute Vision client.</p>
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 135: Device Configuration Backup: Schedule Parameters (cont.)

Parameter	Description
Run Always ⁴	<p>Specifies whether the task always runs or only during the defined period. Values:</p> <ul style="list-style-type: none"> • 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. <p>Default: Enabled</p>
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 136: Device Configuration Backup: Parameters Parameters

Parameter	Description
Include Private Keys	<p>Specifies whether to include the certificate private key information in the configuration file in devices that support private keys.</p> <p>Default: Disabled</p>

Table 137: Device Configuration Backup: Destination Parameters

Parameter	Description
Backup Configuration To	<p>The destination of the backup configuration files.</p> <p>Values:</p> <ul style="list-style-type: none"> • APSolute Vision Server • External Location <p>Default: APSolute Vision Server</p>
Protocol ¹	<p>The protocol that APSolute Vision uses for this task.</p> <p>Values:</p> <ul style="list-style-type: none"> • FTP • SCP • SFTP • SSH
IP Address ¹	The IP address of the external location.

Table 137: Device Configuration Backup: Destination Parameters

Parameter	Description
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 15 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 138: Device Configuration Backup: Target Device List

Parameter	Description
	<p>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.</p> <p>Select entries from the lists and use the arrows to move the entries to the other lists as required.</p> <p>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 34.</p>

Device Reboot Task—Parameters

The Device Reboot task reboots the specified devices.

Table 139: 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 140: Device Reboot: Schedule Parameters

Parameter	Description
Run	<p>The frequency at which the task runs.</p> <p>Select a frequency, then configure the related time and day/date parameters.</p> <p>Values:</p> <ul style="list-style-type: none"> 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. <p>Note: Tasks run according to the time as configured on the APSolute Vision client.</p>
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	<p>Specifies whether the task always runs or only during the defined period. Values:</p> <ul style="list-style-type: none"> 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. <p>Default: Enabled</p>
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 141: Device Reboot: Target Device List

Parameter	Description
	<p>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.</p> <p>Select entries from the lists and use the arrows to move the entries to the other lists as required.</p> <p>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 34.</p>

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 in the **Target Device List** are deleted from APSolute Vision, APSolute Vision disables the task.

Table 142: 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 143: Operator Toolbox: Schedule Parameters

Parameter	Description
Run	<p>The frequency at which the task runs.</p> <p>Select a frequency, then configure the related time and day/date parameters.</p> <p>Values:</p> <ul style="list-style-type: none"> 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. <p>Note: Tasks run according to the time as configured on the APSolute Vision client.</p>
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	<p>Specifies whether the task always runs or only during the defined period. Values:</p> <ul style="list-style-type: none"> 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. <p>Default: Enabled</p>
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 144: Operator Toolbox: Configuration Template

Parameter	Description
Selected Script	(Read-only) The script that is selected in the table—with the file name.
<p>To select the script, click the script from the Action Title column.</p> <p>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.</p> <p>Note: When you change a selection, the parameters in the Parameters tab change accordingly.</p>	

Table 145: Operator Toolbox: Parameters Parameters

Parameter	Description
<p>Note: This tab is available only when the script that is selected in the Configuration Template tab includes configuration parameters.</p>	
<p>The parameters for the selected script.</p>	

Table 146: Operator Toolbox: Target Device List

Parameter	Description
<p>Note: This tab is available only when the script that is selected in the Configuration Template tab includes configuration parameters.</p>	
<p>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.</p> <p>Select entries from the lists and use the arrows to move the entries to the other lists as required.</p> <p>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 34.</p>	

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 DefensePro 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 DefensePro devices.

The file versions on APSolute Vision and on the DefensePro devices should be identical. Radware recommends synchronizing regular updates of the file at regular intervals on APSolute Vision and on the individual devices.



Note: Radware also recommends updating the Attack Description file each time you update the Signature files on DefensePro 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 **General Settings > 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 **General Settings > Basic Parameters**.
2. Do one of the following:
 - To update the Attack Description file from Radware, 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 7 – Monitoring and Controlling the DefensePro Operational Status

APolute Vision's online monitoring for DefensePro 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 DefensePro Device Information, page 215](#)
- [Monitoring and Controlling DefensePro Ports and Trunks, page 216](#)
- [Monitoring DefensePro Resource Utilization, page 218](#)
- [Monitoring Security Group Tags \(SGTs\), page 220](#)

Monitoring the General DefensePro Device Information

The Overview tab 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 147: 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	Virtual devices do not have a serial number. For virtual devices, the field displays 000000000 .

Table 148: Overview: Signature Update Parameters

Parameter	Description
Radware Signature File Version	The version of the Radware Signature File installed on the device.

Table 149: Overview: Software Parameters

Parameter	Description
Software Version	The version of the product software installed on the device.
APolute OS Version	The version of the APolute OS installed on the device—for example, 10.31-03.01:2.06.08.
Build	The build number of the current software version.



Table 149: Overview: Software Parameters (cont.)

Parameter	Description
Version Status	The state of this software version. Values: <ul style="list-style-type: none">● Open—Not yet released● Final—Released version
Throughput License	Values: <ul style="list-style-type: none">● The maximum throughput, in Gbps, that the license allows.● Unlimited

Table 150: 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 DefensePro Ports and Trunks

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 151: 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 152: 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 higher sub-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.

Table 152: L2 Interface Statistics Parameters (cont.)

Parameter	Description
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.
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 DefensePro Resource Utilization

This section contains the following topics:

- [Monitoring DefensePro CPU Utilization, page 218](#)
- [Monitoring and Clearing DefensePro Authentication Tables, page 219](#)
- [Monitoring DME Utilization According to Configured Policies, page 220](#)
- [Monitoring DefensePro Syslog Information, page 220](#)

Monitoring DefensePro CPU Utilization

You can view statistics for the device's average resource utilization and the utilization for each accelerator.



To monitor device utilization for a selected DefensePro device

- > In the Monitoring perspective, select **Operational Status > Resource Utilization > CPU Utilization**.

Table 153: CPU Utilization: General Parameters

Parameter	Description
Resource Utilization	The percentage of the device's CPU currently utilized.
Last 5 sec. Average Utilization	The average utilization of resources in the last 5 seconds.
Last 60 sec. Average Utilization	The average utilization of resources in the last 60 seconds.

Table 154: CPU Utilization: Engine 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 and Clearing DefensePro 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 DefensePro device

- > In the Monitoring perspective, select **Operational Status > Resource Utilization > Authentication Tables**.

Table 155: 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 156: DefensePro 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 DefensePro 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 DME Utilization According to Configured Policies

The contents of this tab are irrelevant for Radware DefensePro DDoS Mitigation.

Monitoring DefensePro Syslog Information

You can view information relating to the syslog mechanism.



To monitor DefensePro syslog information

> In the Monitoring perspective, select **Operational Status > Resource Utilization > Syslog Monitor**.

Table 157: DefensePro Syslog Monitoring Parameters

Parameter	Description
Syslog Server	The name of the syslog server.
Status	The status of the syslog server. Values: <ul style="list-style-type: none">• 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 137](#).



To monitor SGTs

> In the Monitoring perspective, select **Operational Status > SGT**.

Table 158: SGT Monitoring Parameters

Parameter	Description
Name	The name of the SGT.
Value	The value of the SGT.

Chapter 8 – Monitoring DefensePro Clustering

Use the Clustering Status tab to monitor cluster nodes in Radware DefensePro DDoS Mitigation for Cisco Firepower.



To monitor clustering

- > In the Monitoring perspective, select **Clustering > Cluster Status**.

Table 159: Clustering Monitoring Parameters

Parameter	Description
IP Address	The IP address of the cluster node.
Status	The state of the cluster node.



Chapter 9 – Monitoring DefensePro Statistics

Monitoring DefensePro statistics comprises the following topics:

- [Monitoring DefensePro SNMP Statistics, page 223](#)
- [Monitoring DefensePro IP Statistics, page 224](#)

Monitoring DefensePro SNMP Statistics

You can view statistics for the SNMP layer of the device.



To monitor DefensePro SNMP statistics

- > In the Monitoring perspective, select **Statistics > SNMP Statistics**.

Table 160: DefensePro 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'.
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'.



Table 160: DefensePro SNMP Statistics (cont.)

Parameter	Description
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 DefensePro 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 DefensePro device

- > In the Monitoring perspective, select **Statistics > IP Statistics**.

Table 161: 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.
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 162: 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 10 – Monitoring and Controlling DefensePro Networking

Monitoring and controlling DefensePro networking comprises the following topics:

- [Monitoring and Controlling the DefensePro Session Table, page 227](#)
- [Monitoring Routing Table Information, page 228](#)
- [Monitoring DefensePro ARP Table Information, page 228](#)

Monitoring and Controlling the DefensePro Session Table

Monitoring and controlling DefensePro Session table comprises the following topic: [Monitoring Session Table Information, page 227](#).

Monitoring Session Table Information

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. DefensePro 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 > Session Table**.

Table 163: 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 DefensePro 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 164: 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: <ul style="list-style-type: none">• 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 DefensePro 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 DefensePro device

> In the Monitoring perspective, select **Networking > ARP**.

Table 165: DefensePro 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: <ul style="list-style-type: none">● 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**.



Chapter 11 – Using Real-Time Security Monitoring

When an attack is detected, DefensePro 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 231](#)
- [Using the Dashboard Views for Real-Time Security Monitoring, page 232](#)
- [Viewing Real-Time Traffic Reports, page 249](#)
- [Protection Monitoring, page 257](#)
- [HTTP Reports, page 264](#)



Notes

- Your user permissions (your RBAC user definition) determine the DefensePro devices and policies that the Security Monitoring perspective displays to you. You can view and monitor only the attacks blocked by the DefensePro 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.
- When calculating the real-time network traffic and statistical parameters, Radware DefensePro DDoS Mitigation does not include traffic that exceeded the throughput license.

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 166: 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.

Table 166: Risk Levels (cont.)

Risk Level	Description
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 233](#)
- [Using the Current Attacks Table, page 234](#)
- [Using the Ongoing Attacks Monitor, page 239](#)
- [Attack Details, page 240](#)
- [Sampled Data Tab, page 248](#)
- [Viewing Real-Time Traffic Reports, page 249](#)
- [Viewing the Traffic Utilization Report, page 249](#)

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 33 - Current Attacks Table, page 235](#)).
- **Ongoing Attacks Monitor**—which includes a graphical, chart display (see [Figure 34 - Ongoing Attacks Monitor, page 239](#)).

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 233](#).

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 167: Security Monitor Dashboard View—Display Parameters

Parameter	Description
Scope	<p>The physical ports and the Network Protection policies that the dashboard displays.</p> <p>By default, the Scope is Any Port; Any Policy. That is, by default, the dashboard displays all the information.</p> <p>To control the scope of the information that the dashboard displays in DefensePro, see the procedure To control the scope of the information that the Dashboard View displays, page 234.</p>
Display Last	<p>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.</p> <p>Values:</p> <ul style="list-style-type: none"> ● 10 Minutes ● 20 Minutes ● 30 Minutes ● 1 Hour ● 2 Hours ● 6 Hours ● 12 Hours ● 24 Hours Default: <p>10 Minutes</p>
Top Attacks to Display (This parameter is available only in the Ongoing Attacks Monitor.)	<p>The number of attacks that the Ongoing Attacks Monitor displays. Values:</p> <p>1–50</p> <p>Default: 20</p>
Sort By (This parameter is available only in the Ongoing Attacks Monitor.)	<p>Values:</p> <ul style="list-style-type: none"> ● 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. <p>Default: Top Packet Count</p>



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 Network Protection policies that the dashboard displays, select the corresponding checkboxes.
 - To display the information for all the currently relevant Network 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 Network 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 233](#)).




Note: Once Radware DefensePro DDoS Mitigation reports a Packet Anomaly attack of a certain **Radware ID**, the **Status** value **Occurred** and the **Start Time** value remain indefinitely. 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 DefensePro 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 115](#).)



To display the Current Attacks Table

1. In the Security Monitoring perspective, select the DefensePro device, Site, or Logical Group for which to display data.
2. Select **Dashboard View > Current Attacks Table**. 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 55](#).
 - **Sort the rows**—You can change the row order from ascending to descending or vice versa. To do this, hover the mouse over the column to display the arrow and change the order.
 - **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 240](#).
 - **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.



(Pause). When the table display is

Figure 33: Current Attacks Table

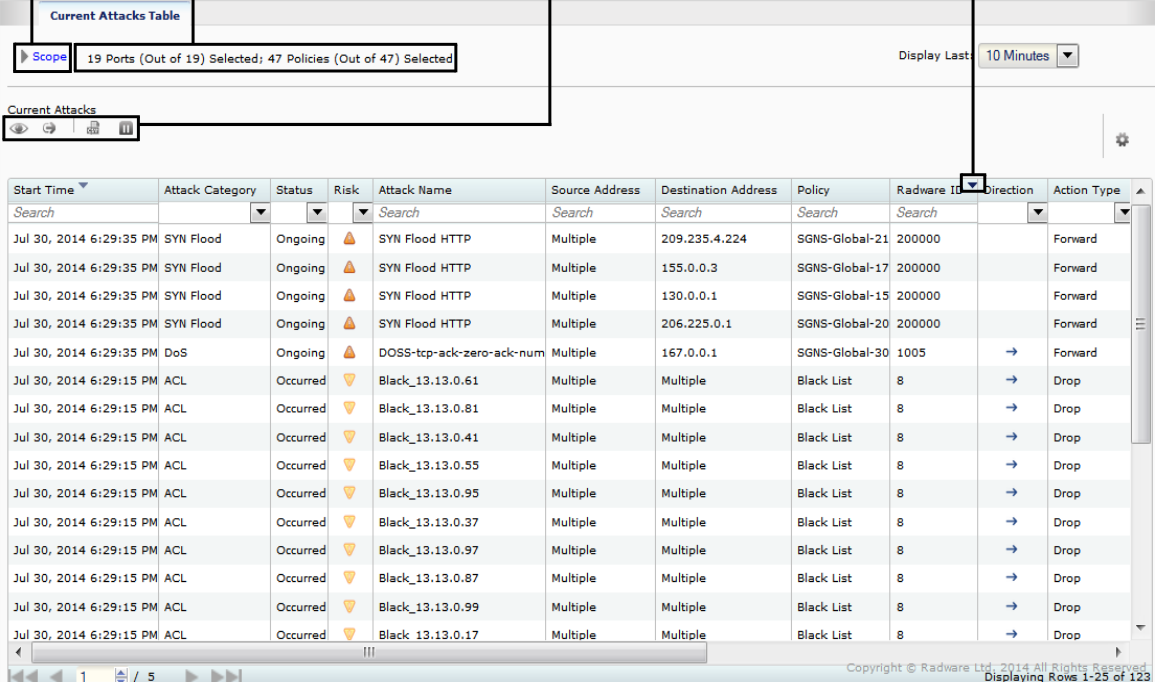
Scope—Displays the tables to select the physical ports and Network Protection policies that the Dashboard View displays.

The **Scope** summary.

Function buttons:

- View Attack Details
- Go to Policy
- Export Table to CSV
- Pause

Arrow for sorting ascending or descending.



Start Time	Attack Category	Status	Risk	Attack Name	Source Address	Destination Address	Policy	Radware ID	Direction	Action Type
Jul 30, 2014 6:29:35 PM	SYN Flood	Ongoing	▲	SYN Flood HTTP	Multiple	209.235.4.224	SGNS-Global-21	200000		Forward
Jul 30, 2014 6:29:35 PM	SYN Flood	Ongoing	▲	SYN Flood HTTP	Multiple	155.0.0.3	SGNS-Global-17	200000		Forward
Jul 30, 2014 6:29:35 PM	SYN Flood	Ongoing	▲	SYN Flood HTTP	Multiple	130.0.0.1	SGNS-Global-15	200000		Forward
Jul 30, 2014 6:29:35 PM	SYN Flood	Ongoing	▲	SYN Flood HTTP	Multiple	206.225.0.1	SGNS-Global-20	200000		Forward
Jul 30, 2014 6:29:35 PM	DoS	Ongoing	▲	DOSS-tcp-ack-zero-ack-num	Multiple	167.0.0.1	SGNS-Global-30	1005	→	Forward
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.61	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.81	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.41	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.55	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.95	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.37	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.97	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.87	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.99	Multiple	Multiple	Black List	8	→	Drop
Jul 30, 2014 6:29:15 PM	ACL	Occurred	▼	Black_13.13.0.17	Multiple	Multiple	Black List	8	→	Drop

Table 168: 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: <ul style="list-style-type: none"> • ACL • Anomalies¹ (in DefenseFlow, detection was performed by an external detector) • Anti-Scanning • Bandwidth Management • Behavioral DoS • DNS Flood • DoS • HTTP Flood • Intrusions • Server Cracking • Stateful ACL • SYN Flood
Status	The last-reported status of the attack. Values: <ul style="list-style-type: none"> • 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.¹ • 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 231). Values: <ul style="list-style-type: none"> •  —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 DefensePro cannot report a specific value. The Search string can be any legal IPv4 or IPv6 address, and can include a wildcard (*).

Table 168: Current Attacks Table Parameters (cont.)



Parameter	Description
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 DefensePro cannot report a specific value.
Policy	The name of the configured Network Protection policy or Server 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 unique attack 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: <ul style="list-style-type: none"> ● 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. ● Drop & Quarantine—Radware DefensePro DDoS Mitigation discards the traffic and adds the destination to the Web quarantine. ● Forward—Radware DefensePro DDoS Mitigation continues to process the traffic and eventually forwards the packet to its destination. ● Proxy ● Quarantine—Radware DefensePro DDoS Mitigation adds the destination to the Web quarantine. ● 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.

Table 168: Current Attacks Table Parameters (cont.)

Parameter	Description
Volume ¹	For most protections, this value is the volume of the attack, in kilobits, from when the attack started. For SYN 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.
Application Protocol ²¹	The transmission protocol used to send the attack: Values: <ul style="list-style-type: none"> ● TCP ● UDP ● ICMP ● IP
MPLS RD	The Multi-protocol Label Switching Route Distinguisher in the policy that handled the attack. The value N/A or 0 (zero) in this field indicates that the MPLS RD is not available.
VLAN Tag / Context	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. 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.
Source Port ²	The Layer 4 source port of the attack.
Destination Port	The Layer 4 destination port of the attack. If there are multiple destination L4 ports, this field displays Multiple . In cases when DefensePro cannot report a specific value, the field displays 0 (zero).
Physical Port ²	The port on the device to which the attack packets arrived. In cases when DefensePro cannot report a specific value, the field displays 0 (zero).
Source MSISDN	The MSISDN Resolution feature is not supported in APSolute Vision version 3.0 and later.
Destination MSISDN	The MSISDN Resolution feature is not supported in APSolute Vision version 3.0 and later.

1 – Once Radware DefensePro DDoS Mitigation reports a Packet Anomaly attack of a certain **Radware ID**, the **Status** value **Occurred** and the **Start Time** value remain indefinitely. 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 DefensePro 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 115.](#))

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 the relevant 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 233](#)).



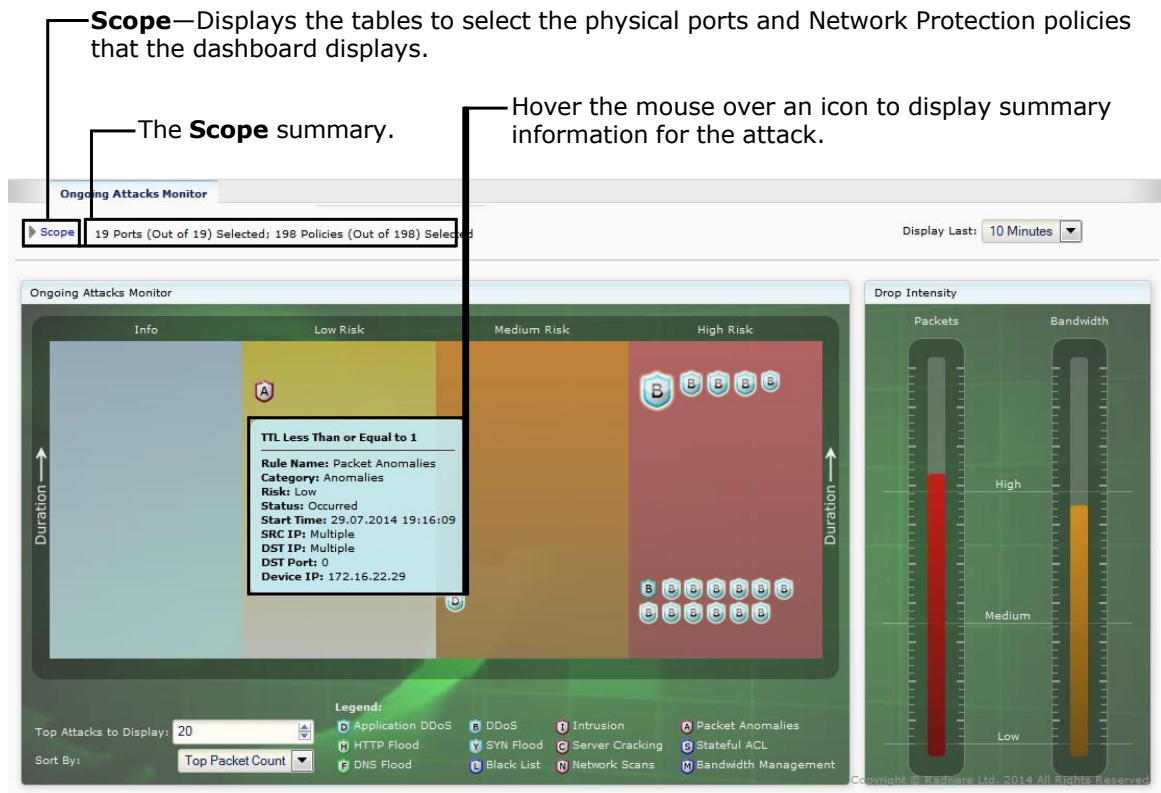
To display the Ongoing Attacks Monitor

1. In the Security Monitoring perspective, select the DefensePro device, 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 231](#)). 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 mouse 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 240](#).

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 34: 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:

- [BDoS Attack Details, page 241](#)
- [DNS Flood Attack Details, page 243](#)
- [DoS Attack Details, page 245](#)
- [Intrusions Attack Details, page 245](#)
- [Packet Anomalies Attack Details, page 246](#)
- [SYN Flood Attack Details, page 246](#)






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 212](#).

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 248](#).
- **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 capture 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, DefensePro 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 for the 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.

BDoS Attack Details

Table 169: BDoS Attack Details: Characteristics Parameters

Parameter	Description
<p>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.</p>	
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	<p>The VLAN tag value or Context Group in the policy that handled the attack.</p> <p>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.</p>
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.
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 ports that the attack uses or used.
DNS ID	The DNS ID that the attack uses or used.

Table 169: BDoS Attack Details: Characteristics Parameters (cont.)

Parameter	Description
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 170: BDoS Attack Details: Info Parameters

Parameter	Description
Packet Size Anomaly Region	<p>The statistical region of the attack packets.</p> <p>The formula for the packet-size baseline for a policy is as follows: $\{(AnomalyBandwidth/AnomalyPPS)/(NormalBandwidth/NormalPPS)\}$ </p> <p>Values:</p> <ul style="list-style-type: none"> • 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.
State	<p>The state of the protection process.</p> <p>Values:</p> <ul style="list-style-type: none"> • Footprints Analysis—Behavioral DoS Protection has detected an attack and is currently determining an attack footprint. • Blocking—Behavioral DoS Protection is blocking the attack based on the attack footprint created. Through a closed feedback loop operation, the Behavioral DoS Protection optimizes the footprint rule, achieving the narrowest effective mitigation rule. • Non-attack—Nothing was blocked because the traffic was not an attack—no footprint was detected or the blocking strictness level was not met.

Table 171: 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 172: BDoS Attack Details: Attack 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 173: BDoS Attack Details: Attack 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 174: 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 Protection Profiles for Network Protection, page 177](#) and [DNS Protection Profile: Subdomains Whitelist Parameters, page 180](#).

Table 175: 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.
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.

Table 175: DNS Flood Attack Details: Characteristics Parameters (cont.)

Parameter	Description
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 176: DNS Flood Attack Details: Info Parameters

Parameter	Description
State	The state of the protection process.
Mitigation Action	The mitigation action. Values: <ul style="list-style-type: none"> ● Signature Challenge ● Signature Rate Limit ● Collective Challenge ● Collective Rate Limit

Table 177: 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 178: DNS Flood Attack Details: Attack 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 179: DNS Flood Attack Details: Attack 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 180: 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

Table 181: DoS 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.
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 182: DoS Attack Details: Info Parameters

Parameter	Description
Action	The protection Action taken.
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 183: 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 184: Intrusions 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.
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 always displayed.

Table 185: 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 186: 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 187: 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 188: 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.
Packet Count	The packet count of the attack.
Volume (Kbits)	The volume, in Kbits, that the attack uses or used.

Table 188: SYN 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.

Table 189: SYN Flood Attack Details: Info Parameters

Parameter	Description
	The information is displayed when the protection action is blocking mode. Caution: If SYN 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 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 190: 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 Table Authentication table.

Table 191: 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.

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 DefensePro device, 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 DefensePro device, 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 on selected port pairs. The information includes data on overall IP traffic, protocol mix, and packet discards. You can display the data in graph or table format.

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 249](#)
- [Viewing the Connection Rate Report, page 252](#)
- [Viewing the Concurrent Connections Report, page 254](#)
- [Viewing the Top Queried Domain Names Report, page 255](#)

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 of time.

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 118](#).
- **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).



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 DefensePro device:

dp rtm-stats get [port number]



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 Traffic Utilization Report

1. In the Security Monitoring perspective, select the Radware DefensePro 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 displayed traffic data, as required. The displayed information refreshes automatically.

Table 192: Traffic Utilization Report: Display Parameters for Graph and Table

Parameter	Description
Scope (link, which displays the table)	<p>The Network Protection policies that the Traffic Utilization Report displays.</p> <p>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.</p> <p>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 251.</p>
Display Last	<p>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.</p> <p>Values:</p> <ul style="list-style-type: none"> ● 10 Minutes ● 20 Minutes ● 30 Minutes ● 1 Hour Default: 10 Minutes
Scope (drop-down list)	<p>The scope of the graph view.</p> <p>Values:</p> <ul style="list-style-type: none"> ● Devices/Physical Ports—The graph shows traffic according to physical ports on the specified device. ● Devices/Policies—The graph shows traffic according to Network Protection policies on the specified device. <p>Default: Devices/Physical Ports</p>
Units	<p>The units for the traffic rate.</p> <p>Values:</p> <ul style="list-style-type: none"> ● 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 Network Protection policies that the report displays, select the corresponding checkboxes.
 - To display the information for all the currently relevant physical ports or Network 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 Network Protection policy, click in the top-left table cell, and then, select **Select None**.

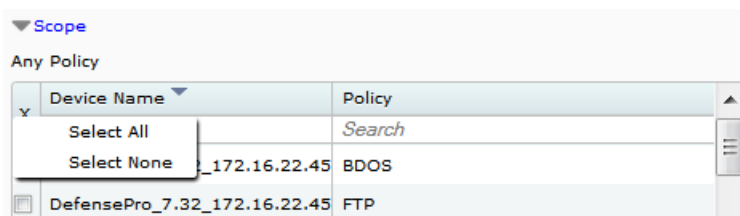


Table 193: Traffic Utilization Report: Filter Parameters for the Traffic Statistics Graph

Parameter	Description
Direction	<p>The traffic that the graph shows.</p> <p>Values:</p> <ul style="list-style-type: none"> • 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. <p>Note: The direction of traffic between a pair of ports is defined by the In Port setting in the port pair configuration.</p>
Protocol	<p>The traffic protocol to display.</p> <p>Values:</p> <ul style="list-style-type: none"> • 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. <p>Caution: When the Scope is Devices/Policies, the Other traffic does not include IPsec traffic.</p>

Table 194: Traffic Utilization Report: Traffic Authentication Statistics (Challenge/Response) Parameters

Parameter	Description
Protocol	The protocol for 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 195: Traffic Utilization Report: Last Sample Statistics Parameters

Parameter	Description
Protocol	The traffic protocol. Values: <ul style="list-style-type: none"> ● TCP ● UDP ● ICMP ● IGMP ● SCTP ● Other—The statistics of the traffic that is not TCP, UDP, ICMP, IGMP, or SCTP. ● All—Total traffic statistics. <p>Caution: When the Scope is Devices/Policies, the Other traffic does not include IPsec traffic.</p>
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 DefensePro device, 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 196: Connection Rate Report: Display Parameters

Parameter	Description
Scope (link, which displays the table)	<p>The physical ports and the Network Protection policies that the Connection Rate Report shows.</p> <p>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.</p> <p>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 254.</p>
Display Last	<p>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.</p> <p>Values:</p> <ul style="list-style-type: none"> ● 10 Minutes ● 20 Minutes ● 30 Minutes ● 1 Hour Default: <p>10 Minutes</p>
Scope (link, which displays the table)	<p>The scope of the graph view.</p> <p>Values:</p> <ul style="list-style-type: none"> ● Devices/Physical Ports—The graph shows traffic according to physical ports on the specified device. ● Devices/Network Policies—The graph shows traffic according to Network Protection policies on the specified device. <p>Default: Devices/Physical Ports</p> <p>Caution: In this version of DefensePro, the Connection Rate Report works only when the Scope is Devices/Network Policies.</p>
Direction	<p>Values:</p> <ul style="list-style-type: none"> ● Both—Show both inbound traffic and outbound traffic. Data for inbound and outbound are displayed as separate lines, not as totals. ● Inbound—Show only inbound traffic. ● Outbound—Show only outbound traffic. <p>Note: The direction of traffic between a pair of ports is defined by the In Port setting in the port pair configuration.</p>
Protocol	<p>The traffic protocol to display.</p> <p>When you select All, total traffic statistics are displayed.</p>

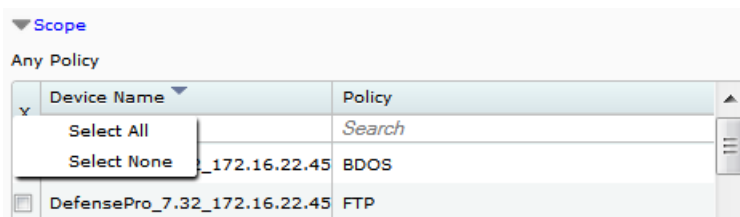
Table 196: Connection Rate Report: Display Parameters (cont.)

Parameter	Description
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, Radware 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.
Select Policies (This button is displayed only when the Scope is Devices/Policies .)	Opens the Select Policies dialog box. Select the Network 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 Network Protection policies that the report displays, select the corresponding checkboxes.
 - To display the information for all the currently relevant physical ports or Network 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 Network 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 197: 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: <ul style="list-style-type: none">● 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.



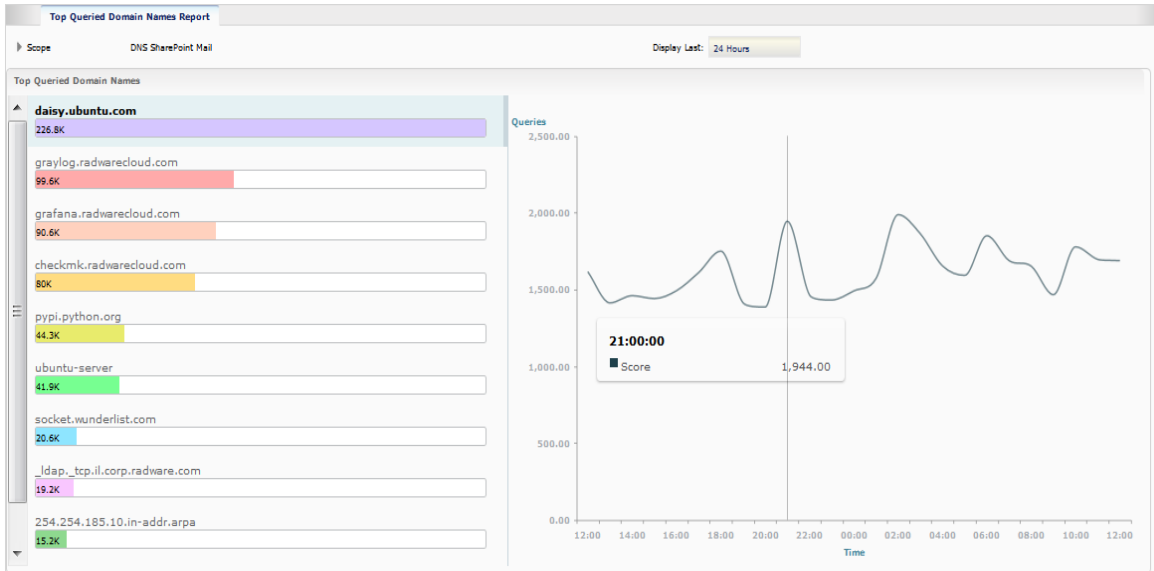
Note: For more information, see [Configuring DNS Protection Profiles for Network Protection, page 177](#).

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 Network 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 mouse 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 35: 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 198: Top Queried Domain Names Report: Display Parameters

Parameter	Description
Scope (drop-down list)	The Network Protection policy whose 10 most-queried DNS domain names the tab displays.
Display Last	Determines the following: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 257](#)
- [Monitoring the Traffic Under BDoS Protection, page 257](#)
- [Monitoring the Traffic Under DNS Flood Protection, page 260](#)

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 Network 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 DefensePro device to monitor.
2. Select **Protection Monitoring > Attack Status Report**. 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 Network Protection policy that includes BDoS protection. Traffic information is displayed in the following tabs:

- [BDoS Traffic Statistics, page 259](#)
- [Last Sample Statistics, page 260](#)



Caution: When traffic matches multiple Network 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 Network Protection policies. This is because when traffic matches multiple Network Protection policies with Out-of-State protection, all those Network Protection policies count the same dropped traffic.



To display traffic information for a Network Policy that includes BDoS protection

1. In the Security Monitoring perspective, select the device to monitor.
2. Select **Protection Monitoring > BDoS Traffic Monitoring Reports**.
3. Configure the general parameters for the display of the BDoS Traffic Statistics graph and Last Sample Statistics table.

Table 199: BDoS Traffic Monitoring Reports: General Parameters

Parameter	Description
Scope	The Network 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: <ul style="list-style-type: none">● 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: <ul style="list-style-type: none">● Kbps—Kilobits per second● Packets/Sec—Packets per second

BDoS Traffic Statistics

The graph displays the traffic rates for the selected Network Protection policy according to the specified parameters.

Table 200: 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: <ul style="list-style-type: none">● 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 201: 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 DefensePro 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.

Table 201: Statistics Graph Legend (cont.)

Line	Description
Suspected Edge (- - - - - dashed orange)	The traffic rate that indicates a change in traffic that might be an attack. Caution: DefensePro reports the Suspected Edge in Kbps only. The graph displays the Suspected Edge only when the Scope parameter Units is Kbps (see Table 203 - DNS Traffic Monitoring Reports: General Parameters, page 261). When the Scope parameter Units is Packets/Sec , the graph does not display the Suspected Edge.
Attack Edge (- - - - - dashed red)	The traffic rate that indicates an attack. Caution: DefensePro reports the Attack Edge in Kbps only. The graph displays the Attack Edge only when the Scope parameter Units is Kbps (see Table 203 - DNS Traffic Monitoring Reports: General Parameters, page 261). 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 202: 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 DefensePro 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 Network Protection policy that includes DNS Flood protection. APSolute Vision displays traffic information in the following tabs:

- [DNS Traffic Statistics, page 261](#)
- [Last Sample Statistics, page 262](#)



To display traffic information for a Network Protection policy that includes DNS 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 Last Sample Statistics table.

Table 203: DNS Traffic Monitoring Reports: General Parameters

Parameter	Description
Scope	The Network 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. Values: 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


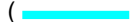



DNS Traffic Statistics

The graph displays the traffic rates for the selected Network Protection policy according to the specified parameters.

Table 204: 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: <ul style="list-style-type: none">● 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 205: 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 DefensePro 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 Protection Profiles for Network Protection, page 177](#).

Figure 36: DNS Last Sample Statistics—Example Showing the “A” Panel

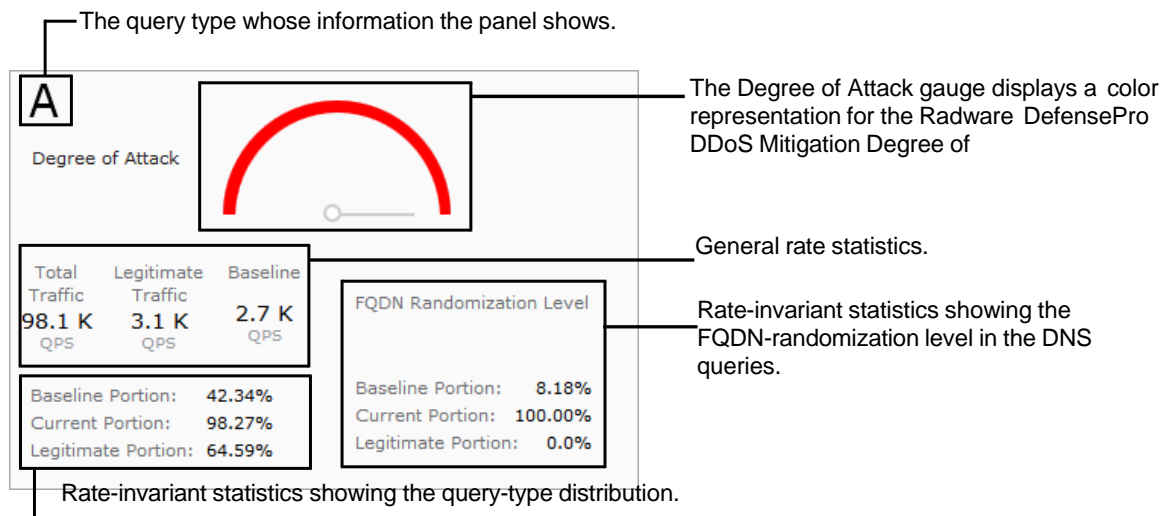


Table 206: Last Sample Statistics Parameters

Parameter	Description
Query Type	The DNS query type. Values: <ul style="list-style-type: none"> ● 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 in 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.

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

APbsolute 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 DefensePro 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 207: 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.	<quantity 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: <Network Protection policy>;	Detected by rule: <Network 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 – Attack categories (for all possible Radware DefensePro DDoS Mitigation versions and configurations):
 - ACL
 - Anti-Scanning
 - Behavioral DoS
 - DoS
 - HTTP Flood
 - Intrusions
 - Server Cracking
 - SYN Flood
 - Anomalies
 - Stateful ACL
 - DNS
 - BWM
- 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 are comma- 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 DefensePro 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 12 – Administering Radware DefensePro DDoS Mitigation

This chapter describes administering Radware DefensePro DDoS Mitigation and contains the following sections:

- [Command Line Interface, page 267](#)
- [Web Services, page 270](#)
- [API Structure, page 270](#)
- [APSSolute API Software Development Kit \(SDK\), page 271](#)

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 APSSolute 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 APSSolute Vision and send it to Radware Technical Support (see [Downloading a Device-Configuration File, page 196](#)).

Table 208: 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.
security	Device security.
services	General networking services.

Table 208: Radware DefensePro DDoS Mitigation CLI Commands and Menus (cont.)

Command	Description
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 8.13 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 config` command 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, using the `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 other hosts.
- Traceroute—Use the following command: `trace-route`

<destination IP address> Output format:

```
DP#trace-route www.radware.com
```

```
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 Radware devices can be managed through SNMP, a serial port, Telnet, SSH, 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 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 the 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:**

This interface does not provide support for:

- Commands that are not configuration commands or monitoring, such as ping, telnet and 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 SOAP commands that mirror Radware's SNMP MIB:**

The following type 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 comes with all the necessary components and documentation to enable rapid development of control and monitoring capabilities in custom-developed applications. This includes the following:

- Web Service Description Language (WSDL) files for all interfaces and modules
- API Reference
- Product overview
- Sample code for some basic device configuration/monitoring functions

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 protection and contains the following main sections:

- [BDoS Footprint Bypass Fields and Values, page 274](#)
- [DNS Footprint Bypass Fields and Values, page 281](#)

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 274](#)
- [BDoS Footprint Bypass Fields and Values for All TCP Controllers, page 277](#)

For more information, see [Configuring BDoS Footprint Bypass, page 110](#).

Table 209: 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 209: 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 ICMP IGMP	tos	Accept	N/A	The type of Service value from the IP packet header.

Table 209: 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 209: 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 210: 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 210: BDoS Footprint Bypass Fields and Values for All TCP Controllers (cont.)

Controllers	Field	Default Status	Default Value or	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 210: BDoS Footprint Bypass Fields and Values for All TCP Controllers (cont.)

Controllers	Field	Default Status	Default Value or	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 the IPv6 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 210: BDoS Footprint Bypass Fields and Values for All TCP Controllers (cont.)

Controllers	Field	Default Status	Default Value or Range 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 122](#).

Table 211: DNS Footprint Bypass Fields and Values

Field	Default Status	Default Value or	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 211: DNS Footprint Bypass Fields and Values (cont.)

Field	Default Status	Default Value or Range 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 list may vary depending on the product version.

Table 212: 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	ffffff
ares_ft_udp_1	Ares_FT_udp	UDP	40	f0000000
bearshare_download_tcp_0	BearShare_Download_tcp	TCP	0	ffffff
bearshare_download_tcp_1	BearShare_Download_tcp	TCP	4	ffffff
bearshare_request_file_udp_0	BearShare_Request_File_udp	UDP	0	ffffff
bearshare_request_file_udp_1	BearShare_Request_File_udp	UDP	4	00ffffff
bittorrent_command_1_0	BitTorrent	TCP	0	ffffff
bittorrent_command_1_1	BitTorrent	TCP	4	ffffff
bittorrent_command_1_2	BitTorrent	TCP	8	ffffff
bittorrent_command_1_3	BitTorrent	TCP	12	ffffff
bittorrent_command_1_4	BitTorrent	TCP	16	ffffff
bittorrent_command_2_0	BitTorrent	TCP	0	ffffff
bittorrent_command_2_1	BitTorrent	TCP	4	ffffff
bittorrent_command_2_2	BitTorrent	TCP	8	ffffff
bittorrent_command_2_3	BitTorrent	TCP	12	ffffff

Table 212: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
bittorrent_command_2_4	BitTorrent	TCP	16	ffffff
bittorrent_command_2_5	BitTorrent	TCP	20	ffffff
bittorrent_command_3_0	BitTorrent	TCP	0	ffffff
bittorrent_command_3_1	BitTorrent	TCP	4	ffffff
bittorrent_command_3_2	BitTorrent	TCP	8	ffffff
bittorrent_command_3_3	BitTorrent	TCP	12	ffffff
bittorrent_command_3_4	BitTorrent	TCP	16	ffffff
bittorrent_command_3_5	BitTorrent	TCP	20	fff0000
bittorrent_command_4_0	BitTorrent	TCP	8	fffff00
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	fffff00
bittorrent_udp_1_1	BitTorrent_UDP_1	UDP	12	fff0000
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	ffffff
directconnect_file_transfer_2	DirectConnect_File_transfer	TCP	25	ffffff
dns	Session for DNS	UDP	0	0
emule_tcp_file_request_0	eMule	TCP	0	ff000000
emule_tcp_file_request_1	eMule	TCP	4	fff0000
emule_tcp_hello_message_0	eMule	TCP	0	ff000000

Table 212: 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	fffffff
gnutella_tcp_2_1	Gnutella_TCP_2	TCP	4	fffffff
gnutella_tcp_3_0	Gnutella_TCP_3	TCP	0	ffffff00
googletalk_ft_1_0	GoogleTalk_FT_1	UDP	24	fffffff
googletalk_ft_1_1	GoogleTalk_FT_1	UDP	28	fffffff
googletalk_ft_1_2	GoogleTalk_FT_1	UDP	32	fffffff
googletalk_ft_1_3	GoogleTalk_FT_1	UDP	36	ffff0000
googletalk_ft_2_0	GoogleTalk_FT_2	UDP	24	fffffff
googletalk_ft_2_1	GoogleTalk_FT_2	UDP	28	fffffff
googletalk_ft_4_0	GoogleTalk_FT_4	UDP	67	fffffff
googletalk_ft_4_1	GoogleTalk_FT_4	UDP	71	fffffff
groove_command_1_0	Groove	TCP	6	fffffff
groove_command_1_1	Groove	TCP	10	fffffff
groove_command_1_2	Groove	TCP	14	fffffff
groove_command_2_0	Groove	TCP	6	fffffff
groove_command_2_1	Groove	TCP	10	ffff0000
groove_command_3_0	Groove	TCP	7	fffffff
groove_command_3_1	Groove	TCP	11	fffffff
groove_command_3_2	Groove	TCP	15	fffffff
groove_command_3_3	Groove	TCP	19	fffffff
h.225-session	Session Of H225	TCP	0	0

Table 212: 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	ffffff
icecast_2	IceCast_Stream	TCP	4	ffffff
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	ffffff
icq_aol_ft_1	ICQ_AOL_FT	TCP	0	ffffff
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	ffffff
imesh_download_tcp_1	iMesh_Download_tcp	TCP	4	ffffff
imesh_request_file_udp_0	iMesh_Request_File_udp	UDP	0	ffffff
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	ffffff
itunesdaap_ft_1	iTunesDaap_FT	TCP	4	ffffff
itunesdaap_ft_2	iTunesDaap_FT	TCP	8	fffff00
itunesdaap_ft_3	iTunesDaap_FT	TCP	2	ffff0000
kazaa_request_file_0	Kazaa_Request_File	TCP	0	ffffff

Table 212: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
kazaa_request_file_1	Kazaa_Request_File	TCP	4	ffffff
kazaa_request_file_2	Kazaa_Request_File	TCP	8	ffff0000
kazaa_udp_packet_0	Kazaa_UDP_Packet	UDP	6	ffffff
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	ffffff
manolito_file_transfer_0_1	Manolito	TCP	0	ffffff
manolito_file_transfer_0_2	Manolito	TCP	0	ffffff
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	ffffff
meebo_get_1	MEEBO_GET	TCP	4	ffffff
meebo_get_2	MEEBO_GET	TCP	8	ffffff
meebo_get_3	MEEBO_GET	TCP	12	ffffff

Table 212: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
meebo_get_4	MEEBO_GET	TCP	16	ffffff
meebo_get_5	MEEBO_GET	TCP	20	ffffff
meebo_get_6	MEEBO_GET	TCP	24	ffffff
meebo_get_7	MEEBO_GET	TCP	28	ffffff
meebo_get_8	MEEBO_GET	TCP	32	ff000000
meebo_post_0	MEEBO_POST	TCP	0	ffffff
meebo_post_1	MEEBO_POST	TCP	4	ffffff
meebo_post_2	MEEBO_POST	TCP	8	ffffff
meebo_post_3	MEEBO_POST	TCP	12	ffffff
meebo_post_4	MEEBO_POST	TCP	16	ffffff
meebo_post_5	MEEBO_POST	TCP	20	ffffff
meebo_post_6	MEEBO_POST	TCP	24	ffffff
meebo_post_7	MEEBO_POST	TCP	28	fffff00
msn-any	MSN Messenger Chat	TCP	0	ffffff
msn-msg	MSN Messenger Chat	TCP	0	0
msn_msgr_ft_0	MSN_MSGR_FT	TCP	0	ffffff
msn_msgr_ft_1	MSN_MSGR_FT	TCP	48	ffffff
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 212: 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	fffffff
skype-80-l-56	Skype signature for port 80	TCP	2	ffff0000
skype-80-proxy	Skype signature for port 80	TCP	0	fffffff
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	fffffff
soulseek_pierce_fw_1	SoulSeek_Pierce_FW	TCP	4	ff000000
soulseek_pierce_fw_2	SoulSeek_Pierce_FW	TCP	2	ffff0000

Table 212: 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	ffffff
yahoo_ft_1	YAHOO_FT	TCP	10	fff0000
yahoo_get_0	YAHOO_GET	TCP	0	ffffff
yahoo_get_1	YAHOO_GET	TCP	4	ffffff
yahoo_get_2	YAHOO_GET	TCP	8	ffffff
yahoo_get_3	YAHOO_GET	TCP	12	ffffff
yahoo_get_4	YAHOO_GET	TCP	16	ff000000
yahoo_post_0	YAHOO_POST	TCP	0	ffffff

Table 212: Predefined Basic Filters (cont.)

Name	Description	Protocol	OMPC Offset	OMPC Mask
yahoo_post_1	YAHOO_POST	TCP	4	ffffff
yahoo_post_2	YAHOO_POST	TCP	8	ffffff
yahoo_post_3	YAHOO_POST	TCP	12	ffffff
yahoo_post_4	YAHOO_POST	TCP	16	ffff0000

Appendix C – DefensePro Attack-Protection IDs

This appendix describes the DefensePro Attack-Protection IDs.

This release does not support all the protections listed in the following table.

Table 213: DefensePro Attack-Protection IDs

ID Number or Range	Attack-Protection Name	Category (for Prevention)	Default Risk	Default Action	Report Action	Description
8	White List	N/A				White-list encounters are not reported as security events.
9	Black List	Access				Black-list access violation.
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.
75	Network flood IPv4 TCP-ACK	Behavioral-DoS				Network flood IPv4 TCP with ACK 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.
82	Network flood IPv6 IGMP	Behavioral-DoS				Network flood IPv6 IGMP.
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.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Protection	Default Action	Report Action	Description
85	Network flood IPv6 TCP-ACK	Behavioral-DoS				Network flood IPv6 TCP with ACK 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.
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.
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.
112	Invalid TCP Header Length	Anomalies				(This anomaly protection is available only in DefensePro 5.11 and 5.12.) Invalid TCP header length.
113	Invalid TCP Flags	Anomalies	Low	Block	Bypass	Invalid TCP flags.
116	Invalid UDP Header Length	Anomalies				Invalid UDP header length.
119	Source or Dest Address same as Local Host	Anomalies	Low	Block	Bypass	Source or destination IP address same as local host.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report	Description
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.
131	Invalid L4 Header Length		Low	Block	Bypass	Invalid L4 header length
150	HTTP Page Flood Attack	HttpFlood				HTTP page flood attack.
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.
400	Brute Force Web					A Brute Force Web attack is an attempt to break into a restricted area on a site that is protected by native HTTP authentication.
401	Web Scan					A Web-vulnerability scan is an information-gathering attack that is usually launched as a prequel to an intrusion attack on the scanned Web server. The attacker is trying to gather the information on the Web server by sending different types of HTTP requests and analyzing the server responses. Automatic tools are often used in this case.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report	Description
402	Brute Force SMTP					A Brute Force SMTP attack is an attempt to break into restricted accounts on the SMTP mail server that is protected by username and password authentication.
403	Brute Force FTP					A Brute Force FTP attack is an attempt to break into a restricted account on the FTP server that is protected by username and password authentication.
404	Brute Force POP3					A Brute Force POP3 attack is an attempt to break into restricted accounts on the POP3 mail server that is protected by username and password authentication.
405	Brute Force SIP (UDP)					A Brute Force SIP (UDP) attack is an attempt to break into restricted accounts on the SIP server, over UDP, which is protected by username and password authentication. This type of attack can also cause a Register flood on the SIP server.
406	Brute Force SIP (TCP)					A Brute Force SIP (TCP) attack is an attempt to break into restricted accounts on the SIP server, over TCP, which is protected by username and password authentication. This type of attack can also cause a Register flood on the SIP server.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report	Description
407	Brute Force MySQL					A Brute Force MySQL attack is an attempt to break into restricted Database accounts on the MySQL database server that is protected by username and password authentication.
408	Brute Force MSSQL					A Brute Force MSSQL attack is an attempt to break into a restricted database accounts on the MSSQL database server that is protected by username and password authentication.
409	SIP Scan (UDP)					SIP scan attacks intend to identify the SIP server in order to find vulnerabilities or to harvest the server for existing subscriber phone numbers (also known as SIP users or SIP URI). The phone numbers can be used later to launch a SPIT (SPAM over IP Telephony) attack.
410	SIP Scan (TCP)					SIP scan attacks intend to identify the SIP server in order to find vulnerabilities or to harvest the server for existing subscriber phone numbers (also known as SIP users or SIP URI). The phone numbers can be used later to launch a SPIT (SPAM over IP Telephony) attack.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report	Description
414	SIP Scan DST (TCP)					SIP scan attacks intend to identify the SIP server in order to find vulnerabilities or to harvest the server for existing subscriber phone numbers (also known as SIP users or SIP URI). The phone numbers can be used later to launch a SPIT (SPAM over IP Telephony) attack.
416	Brute Force SIP DST (TCP)					A Brute Force SIP DST (TCP) attack is an attempt to break into restricted accounts on the SIP server, over TCP, which is protected by username and password authentication. The specific attack was detected from error responses that were found on sessions that originated from the server. This type of attack can also cause a Register flood on the SIP server.
417	Brute Force SMB					A Brute Force SMB attack is an attempt to break into restricted accounts on the SMB (file share) server that is protected by username and password authentication.
418	Brute Force SIP DST (UDP)					A Brute Force SIP DST (UDP) attack is an attempt to break into restricted accounts on the SIP server, over UDP, which is protected by username and password authentication. The specific attack was detected from error responses that were found on sessions that originated from the server. This type of attack can also cause a Register flood on the SIP server.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Protection)	Default Risk	Default Action	Report	Description
419	SIP Scan DST (UDP)					SIP scan attacks intend to identify the SIP server in order to find vulnerabilities or to harvest the server for existing subscriber phone numbers (also known as SIP users or SIP URI). The phone numbers can be used later to launch a SPIT (SPAM over IP Telephony) attack.
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.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Protection)	Default Risk	Default Action	Report	Description
469	DNS flood IPv6 DNS-ALL	DNS-Protection				DNS query flood over IPv6.
720	SYN Flood protection		High	According to policy Action		Start, ongoing, and termination of attacks per protection policy.
721	SYN Flood enabled protection		High	According to policy Action		Ongoing message when the SYN rate relative to the first ACK/Data packet rate is above 1000 packets per second.
722	SYN Flood protect full table		Medium	According to policy Action		(This event is not generated in version 5.10 and later.) Used for DefensePro's session table protection.
723	SYN ACK Reflection protection		High	According to policy Action		(This event is not generated in version 5.10 and later.) Used for SARP (SYN ACK Reflection Protection).
724	SYN Protect delete frag		Info	According to policy Action		Used when a fragmented packet arrives during the authentication process. The packet will be discarded.
725	SYN Protect delete reset		Info	According to policy Action		Used when a RESET packet that does not match an existing session arrives during the authentication process. The packet will be discarded.
726	SYN Protect out of context		Info	According to policy Action		(This event is not generated in version 5.10 and later.) Used when a packet that does not match an existing session arrives during the authentication process. The packet will be deleted and a RESET will be sent to the source.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Reporting)	Default Risk	Default Action	Report	Description
727	SYN Protect full table		Medium	According to policy Action		Used when the SYN 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.
729	SYN Protect out of context		Info	According to policy Action		Used when a packet that does not match an existing session arrives during the authentication process. The packet will be deleted and a RESET will be sent to the source.
730	SYN Protect unverified cookie		Info	Drop		Used when a ACK packet arrives with a SYN cookie that does not match the one sent by the DefensePro device. This error is generated only when the policy is configured with Block and Report.
731	SYN Protect incompleteness		Info	Drop		(This event is not relevant before version 5.1x.) Used when a new session is aged during the authentication process before the first data packet has arrived.
732	SYN Protect delete wrong tcp		Info	Drop		Used when an unexpected packet or one with illegal TCP flags arrives during the authentication process. The packet will be discarded.
740	TCP session dropped	Stateful-ACL	High	Drop		Reports on traffic that matched an ACL policy.
741	TCP session allowed	Stateful-ACL	Info	Forward		Reports on traffic that matched an ACL policy.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Protection)	Default Risk	Default Action	Report	Description
742	UDP session dropped	Stateful-ACL	High	Drop		Reports on traffic that matched an ACL policy.
743	UDP session allowed	Stateful-ACL	Info	Forward		policy on traffic that matched an ACL rule.
744	ICMP session dropped	Stateful-ACL	High	Drop		Reports on traffic that matched an ACL policy.
745	ICMP session allowed	Stateful-ACL	Info	Forward		Reports on traffic that matched an ACL policy.
746	IP session dropped	Stateful-ACL	High	Drop		Reports on IP traffic that matched an ACL policy that is not supported explicitly in the ACL (that is, traffic that is not, for example, TCP, UDP, ICMP, IGMP, SCTP, or supported tunneling protocols).
747	IP session allowed	Stateful-ACL	Info	Forward		Reports on IP traffic that matched an ACL policy that is not supported explicitly in the ACL (that is, traffic that is not, for example, TCP, UDP, ICMP, IGMP, SCTP, or supported tunneling protocols).
748	TCP Mid Flow packet	Stateful-ACL	Medium	Drop		Reports on traffic that matched an ACL policy.
749	TCP Invalid reset	Stateful-ACL	Medium	Drop		Reports on traffic that matched an ACL policy.
750	TCP handshake violation	Stateful-ACL	Medium	Drop		Reports on traffic that matched an ACL policy.
751	ICMP Smurf packet	Stateful-ACL	Medium	Drop		Reports on traffic that matched an ACL policy.
752	ICMP packet anomaly	Stateful-ACL	Medium	Drop		Reports on traffic that matched an ACL policy.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Protection)	Default Risk	Default Action	Report	Description
753	GRE session dropped	Stateful-ACL	High	Drop		Reports on traffic that matched an ACL policy.
754	GRE session allowed	Stateful-ACL	Info	Forward		Reports on traffic that matched an ACL policy.
755	SCTP session dropped	Stateful-ACL	High	Drop		Reports on traffic that matched an ACL policy.
756	SCTP session allowed	Stateful-ACL	Info	Forward		Reports on traffic that matched an ACL policy.
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 signature.
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.

Table 213: DefensePro Attack-Protection IDs (cont.)

ID Number or Range	Attack-Protection Name	Category (for Protection)	Default Risk	Default Action	Report	Description
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.
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. The device generates the ID number sequentially when the user creates the protection.
600,000–675,000	User-defined Connection PPS Limit protections	DoS				Range for user-defined Connection PPS Limit protections. The device generates the ID number sequentially when the user creates the protection.



Appendix D – Protocols Supported by DefensePro

This appendix lists the protocols and operating systems that DefensePro signatures can protect. DefensePro 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 Timbuku
- 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
- XDMCP

DefensePro 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 Radware Technical Support with relevant information.

For troubleshooting hardware-related issues, please consult Cisco Technical Support. This appendix contains the following section: [Technical Support File, page 309](#).

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:

-v displays 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 214: 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

This glossary is a list of terms and definitions used in the Radware technical environment, with special emphasis on Radware DefensePro. Some of the words belong to the public domain, and some are Radware-specific, but all are used in the Radware documentation.

Table 215: Glossary Terms

Term	Definition
AMS	<p>Attack Mitigation Service.</p> <p>AMS is a solution offering from Radware, which comprises the following products:</p> <ul style="list-style-type: none"> ● DefensePro ● Cloud DDoS Protection (previously DefensePipe) ● DefenseFlow ● AppWall ● Cloud WAF ● APSolute Vision ● ERT—Emergency Response Team
Anomaly	<p>An anomaly is unusual or unexpected behavior of traffic patterns or a protocol.</p>
Attack	<p>An attack is a realization of a threat, a malicious action taken against a network, host, or service.</p>
Attack Signatures Database / Signatures Database	<p>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.</p>
Behavioral DoS (BDoS)	<p>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.</p> <p>BDoS profiles do this by identifying the footprint of the anomalous traffic. Network-flood protection types include:</p> <ul style="list-style-type: none"> ● 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	<p>You can define DefensePro Black List rules to block certain traffic. Black List rules are used as exceptions for DefensePro security policies (see Security policy). You can define Black List rules for a single IP address or using a Network class.</p>

Table 215: Glossary Terms (cont.)

Term	Definition
Certificate	<p>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.</p>
Class	<p>In DefensePro, classes define groups of elements of the same type of entity.</p>
DDoS	<p>Distributed Denial of Server 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.</p> <p>When the DNS server is configured to provide recursion, the DNS server, if the requested domain name isn’t available locally, 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.</p> <p>Radware’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.</p>
Deep Packet Inspection	<p>Inspection of the packet’s payload as opposed to only its header. This enables the security device to perform inspection at the application level.</p>
DME	<p>DoS/DDoS mitigation engine.</p>
DoS	<p>Denial of Service is an attack intended to consume system resources and create a temporary loss of service.</p>
ERT	<p>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.</p>
Exploit	<p>An exploit is a program or technique that takes advantage of a software vulnerability.</p> <p>The program can be used for breaking security, or otherwise attacking a host over the network.</p>
Filter	<p>In the context of the DefensePro Signature Protection module, filters are components of a signature. Each filter contains the exact pattern of the attack. DefensePro scans, classifies and matches packets to the filters in the Signatures database. Upon a match, the Signature Protection module takes the configured action.</p>

Table 215: Glossary Terms (cont.)

Term	Definition
Heuristic analysis	<p>Heuristic analysis is behavior-based analysis, targeted to provide a filter blocking the abnormal phenomena.</p> <p>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.</p>
Historical security reporting	<p>The Attack Mitigation Service (AMS), using APSolute Vision, offers a built-in security information and event management (SIEM) for historical security reporting of DefensePro security events.</p>
Inspection port	<p>An inspection port is a port on a Radware DefensePro DDoS Mitigation device that you can configure to receive, inspect, and transmit traffic.</p>
Intrusion	<p>An intrusion is an attempted or successful access to system resources in any unauthorized manner.</p>
Intrusion Detection System (IDS)	<p>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.</p> <p>There are two system-monitoring approaches:</p> <ul style="list-style-type: none"> ● 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. <p>Organizations generally choose a combination of these approaches, based on known vulnerabilities.</p>
IPS	<p>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.</p> <p>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.</p>

Table 215: Glossary Terms (cont.)

Term	Definition
IP interface	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Network class	<p>A Network class is a type of class in the DefensePro 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).</p>
NHR	<p>A Next-Hop Router (NHR) is a network element with an IP address through which traffic is routed.</p>
Protection policy	<p>Another term for a DefensePro security policy (see Security policy).</p>
Security event reporting	<p>DefensePro security events include all events related to attack detection and mitigation. When an attack is detected, DefensePro creates and reports a security event, which includes the information relevant to the specific attack.</p>
Security policy	<p>A security policy in an organization is a set of rules that defines what constitutes a secure network and how DefensePro reacts to security violations.</p> <p>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.</p>

Table 215: Glossary Terms (cont.)

Term	Definition
Server Cracking Protection	<p>Radware's Server Cracking Protection is a behavioral server-based technology that detects and prevents both known and unknown application scans and brute-force attacks.</p> <p>This behavioral protection is part of Radware's Radware DefensePro DDoS Mitigation Full Spectrum Protection Technology. The technology includes:</p> <ul style="list-style-type: none"> ● An adaptive behavioral network-based protection that mitigates network DoS and DDoS attacks ● Adaptive behavioral user-based protections that mitigate network pre-attack probes and zero-day worm propagation activities ● Stateful signature-based protections against exploitation attempts of known application vulnerabilities. <p>See also Server Cracking Protection Profiles.</p>
Server Cracking Protection Profile	<p>A Server Cracking Protection profile provides application level protection that identifies excessive frequencies of error responses from various applications. The profile initiates blocking of hacking sources, while allowing legitimate traffic to pass through.</p> <p>Application scanning and authentication brute force attempts are usually precursors to more serious exploitation attempts. An attacker tries to gain access to a restricted section, or to find a known vulnerability by sending a list of legitimate-looking requests and analyzing the responses. Both cracks and scanning attempts are characterized by a higher than usual error responses from the application to a few specific users.</p>
Server Protection Profile	<p>Server Protection profiles are designed to defend from network and application attacks targeting network servers or services, such as:</p> <ul style="list-style-type: none"> ● Connection limit ● Server cracking ● HTTP Page floods
Server, Reporting	<p>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.</p>
Service	<p>A feature that provides protection against a set of attacks.</p>
Signature	<p>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.</p>
Signature Protection module	<p>The DefensePro Signature Protection module protects against known network vulnerabilities, application vulnerabilities, exploitation attempts, and DoS/DDoS flood attacks.</p>
SME	<p>String-matching engine.</p>
Spoof	<p>A spoof is when one system entity poses as or assumes the identity of another entity.</p>

Table 215: Glossary Terms (cont.)

Term	Definition
SYN cookie	<p>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:</p> <ul style="list-style-type: none"> ● Top 5 bits: $t \text{ mod } 32$, 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. <p>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.</p> <p>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.</p> <p>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.</p>
SYN flood	<p>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.</p> <p>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.</p> <p>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.</p>

Table 215: Glossary Terms (cont.)

Term	Definition
SYN-ACK Reflection Attack Prevention	<p>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.</p> <p>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.</p>
Threat	<p>A threat, in Internet security terms, is a person, thing, event, or idea, that poses a danger to an asset.</p> <p>A fundamental threat can be any of the following: information leakage, Denial of Service, integrity violation, and illegitimate use.</p>
Trojan Horse	<p>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.</p> <p>It is usually designed to provide unrestricted access into internal systems, bypassing security monitoring and auditing policies.</p>
Virus	<p>A virus is a malicious program code written with the intention to damage computer systems and to replicate itself to extend the possible damage.</p>
Web application attack	<p>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.</p>
White List	<p>DefensePro White List rules allow certain traffic without inspection. White List rules are used as exceptions for DefensePro security policies (see Security policy). You can define White List rules for a single IP address or using a Network class.</p>
Worm	<p>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.</p>
Zero-day attack / zero-minute attack	<p>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.</p>



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 HEREIN ABOVE 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.

- 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 (or the 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. 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 first obtaining 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 accordance with 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.

COPYRIGHT © 2017, Radware Ltd. All Rights Reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)