Radware DefensePro DDoS MitigationRelease Notes

Software Version 8.22.2

Last Updated: August 2020

TABLE OF CONTENTS

CONTENT

Radware announces the release of Radware DefensePro DDoS Mitigation version 8.22.2.0 for Cisco Firepower.

This Release Notes document describes new capabilities and maintenance fixes since the last releasedversion of Radware DefensePro DDoS Mitigation, version 8.13.01.

RELEASE SUMMARY

Version 8.22.2.0 introduces many new features and enhancements, such as Anti-Scanning Protection,Burst-Attacks Protection, Connection PPS Protection, Traffic Filters, and more.

Release Date: August 2020
Build Number: 27

SUPPORTED PLATFORMS AND MODULES

This software version is supported by the following platforms

Product	Platform	SME	DME
Radware DefensePro DDoS Mitigation	Virtual	Software-based	No

DEVICE MANAGEMENT

This Radware DefensePro DDoS Mitigation version was tested using APSolute Vision version

4.60.00. If you are using a previous version of APSolute Vision, you are advised to upgrade to version 4.60.00 or later.

UPGRADING THE SOFTWARE

Direct upgrade to version 8.22.2.0 is supported from Radware DefensePro DDoS Mitigation version8.13.01.

Upgrade the Radware DefensePro DDoS Mitigation version using Firepower Chassis Manager, as follows:

1. Click on **Logical Devices**. The *Logical Device List* is displayed.
2. Select the Security module and the Radware DefensePro DDoS Mitigation application you wish to upgrade.
3. Select the **Set version**. The *Update image version* window is displayed.
4. Select New Version 8.22.2.0, the *Resource Profile* you wish to use, and then, click **OK**.

WHAT'S NEW

This section describes what is new in version 8.22.2.0

Anti-Scanning Protection

The Anti-Scanning feature protects against malicious scanning activity, which includes zero-day self-propagating network worms, port scans, and IP-addresses scans.

When Anti-Scanning Protection is enabled, upon detecting an attack, the protection implements the blocking footprint rule for a predefined, initial blocking duration. When the protection identifies repeated scanning activities from the same source, the protection extends the blocking duration.

Burst-Attack Protection

Burst attacks, also known as *hit-and-run DDoS*, use repeated short bursts of high-volume attacks at random intervals. Each short burst may last just a few seconds and may reach hundreds of gigabits of throughput per second.

This version combines the following capabilities to protect against burst attacks.

- Mitigates large volume per second of burst attacks, which sometimes last only seconds, at random intervals.
- Automatically creates a signature to block attack traffic and allows legitimate traffic to pass through
- Dynamically adjusts to changing and multiple attack vectors across bursts.
- Minimizes false positives.

BDoS Protection Additions and Enhancements

Change of Syntax of the BDoS Real-Time Signature

The syntax of the real-time signature for **Medium** strictness is changed, enabling improved detection granularity of attack traffic versus legitimate traffic. The new syntax, when the **Footprint Strictness** is **Medium**, is such that at least one Boolean AND condition must exist, and no Boolean OR condition is allowed in the top-level Boolean expression representing the BDoS real-time signature.

For example:

- AAND B
- (A OR B OR C) AND D AND E
  [where "(A OR B OR C)" is a nested expression]

Overblocking Prevention

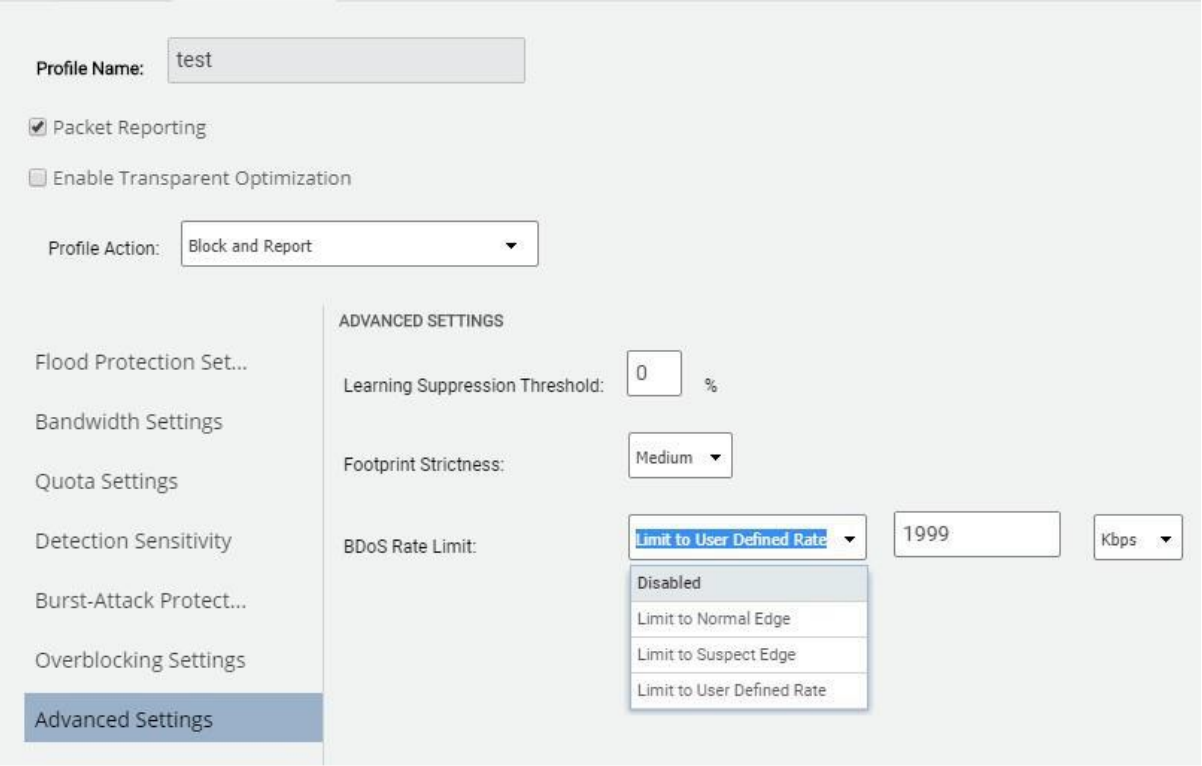
When enabled, *Overblocking Prevention* addresses a situation in which the BDoS profile creates a signaturethat meets all required criteria-matching the specified strictness level and

blocking the attack, but the mitigation also blocks some legitimate traffic.

BDoS Enhancement for Randomized Floods

BDoS uses advanced machine-learning techniques to detect, analyze, and mitigate network- layer volumetric attacks. Randomized attacks, by nature, are designed to mimic legitimate traffic to avoid detection. The BDoS Protection fallback to rate-limiting allows DefensePro to apply an additional protection layer against such sophisticated attacks by automatically rate-limiting traffic based on the BDoS baselines and only under specific circumstances.

Figure 1: BDoS Enhancement for Randomized Floods



DNS Traffic Excluded from BDoS Real-Time Signature Generation Process

Starting with this version, if DNS Flood Protection is enabled, BDoS Protection does not consider DNStraffic while evaluating traffic for generating the BDoS real-time signatur

Black List and White List

Radware DefensePro DDoS Mitigation now offers **Black List** and **White List** rules for data traffic. The **Black List** comprises the traffic that the device always blocks without inspection. You use the **Black List** as policy exceptions for network policies. The **White List** determines the traffic that is exempt from security inspection.

Carpet-Bombing Protection Toolset

This release adds a set of tools aimed at assisting organizations to protect themselves from an

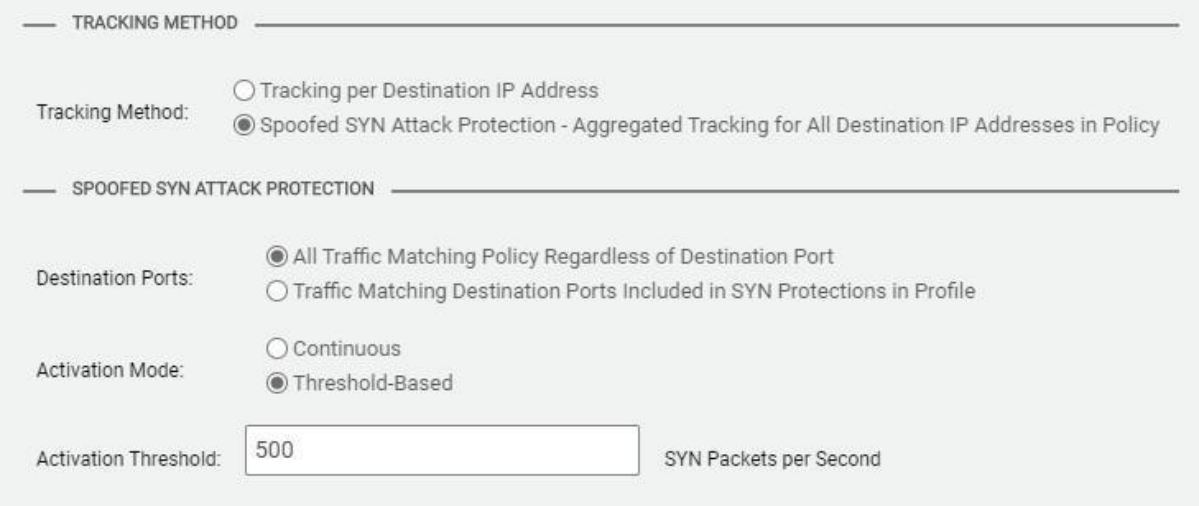
attack technique becoming increasingly popular among attackers, known as carpet bombing. Carpet-bombing attacks combine known attack tactics such as spoofing, reflection, and amplification, to generate attacks that require less firepower to launch, and, at the same time, are more difficult to detect, characterize, and mitigate.

Spoofed SYN Attack Protection

A spoofed-SYN-flood carpet-bombing attack is not the usual, *run-of-the-mill* SYN-flood attack, which is typically focused on one or specific critical servers in the victim network. A spoofed-SYN-flood carpet- bombing attack takes advantage of TCP reflection and amplification by sending massive amounts of junk traffic, masquerading as sourcing from multiple subnets, to many random destination IP addresses included inthe protected network. Such attacks have the potential to *fly under the radar* of anti-DDoS solutions, which typically track the amount of traffic sent towards each individual destination server in the protected server. Anti-DDoS solutions such as these may not distinguish a well-distributed attack that uses various protocols, such as DNS, HTTP, HTTPS, C-LDAP, and so on, and which targets many or even all of the IP addresses of a protected network.

This version of Radware DefensePro DDoS Mitigation introduces an addition to SYN Flood Protection: *Spoofed SYN Attack Protection.* Spoofed SYN Attack Protection handles attacks that use multiple, spoofedsource IP addresses, and which target entire destination subnets and/or CIDRs.

Figure 2: Spoofed SYN Attack Protection

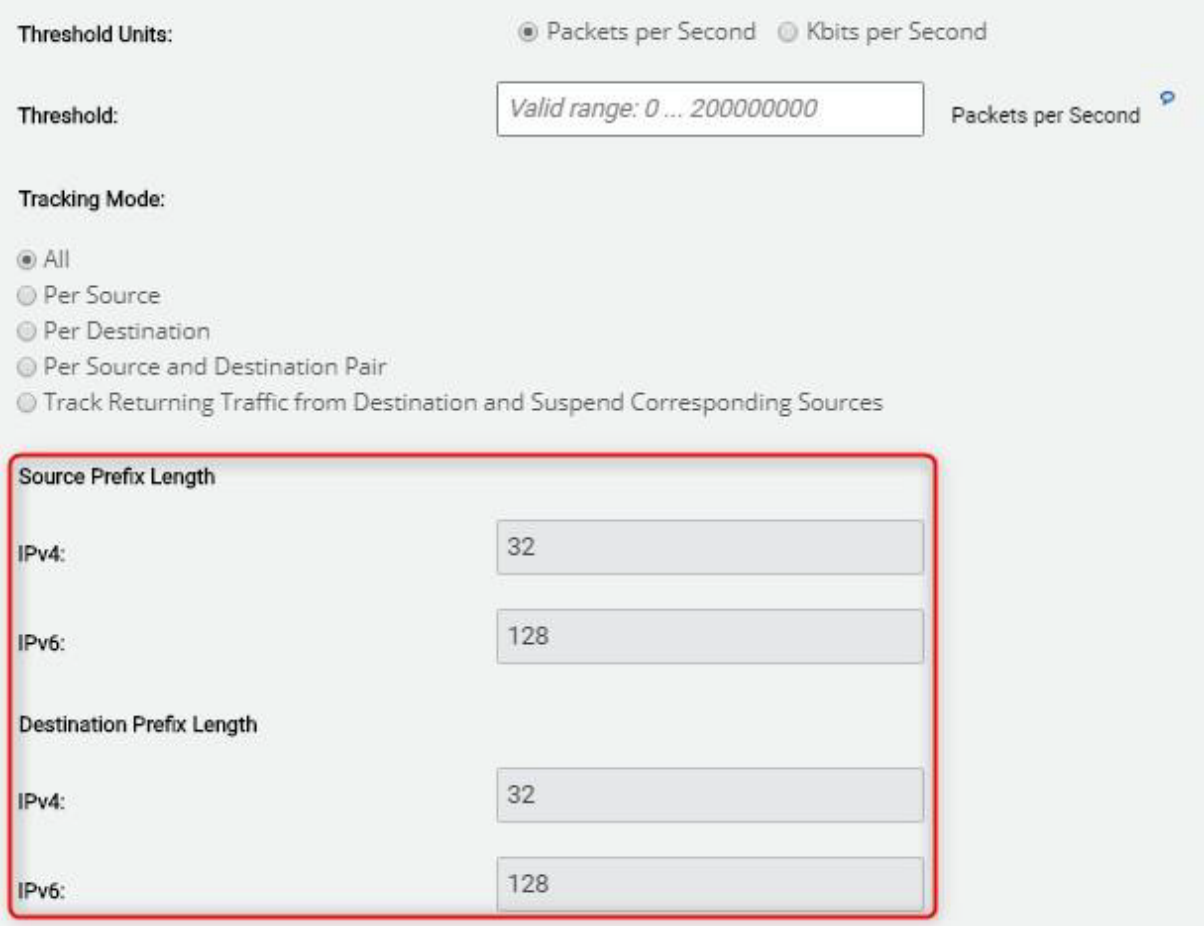


Traffic Filters Enhancement

One of the tactics bad actors utilize in carpet-bombing attacks is the use of full subnets for reflection and amplification effect, in which each individual source sends a relatively small amount of traffic. In this scenario, an ineffective protection measure is to use *per-source* rate- limiting, because using high thresholds would not detect the low rate of traffic per source, and using low thresholds might cause false-positive detection, thus negatively impacting legitimate users.

To overcome this limitation when dealing with carpet-bombing attacks, Traffic Filters now allow you to select the tracking method to suit your protection needs. In addition to the existing discrete source or destination IP- address tracking methods, you can now also select tracking *per source subnet* or *per destination subnet*. The purpose of this enhancement is to allow detection of volumetric traffic originating from subnets, where each individual source IP address sends a small amount of traffic in order to avoid per-source detection

Figure 3: Traffic Filters Enhancement



Anti-Scanning Enhancement

Anti-Scanning is a robust behavioral protection against scanning and reconnaissance attacks. Scanningtechniques are used by attackers as pre-attack probing on their potential victims. To achieve their goal, attackers use a real IP address in order to receive responses on the probing attempts.

As mentioned previously, one of the tactics used in carpet-bombing attacks is utilizing large subnets such that each bad actor, generates, on average, a small number of packets. In this sense, a SYN-based carpet- bombing attack can be perceived as a *distributed scanning attack* on the reflector side or on the victim network side. In this version, Anti-Scanning is enhanced to enable mitigation of distributed scanning attacks originating from multiple sources.

Connection PPS Protection

This release of Radware DefensePro DDoS Mitigation introduces *Connection PPS Protection,* which is focused on mitigating in-connection-based flood attacks. This protection enables you to track and to limit the packet-per-second rate per connection, thus helping to eliminate malicious activity originating from established connections.

Connection PPS profiles offer granular protection within a single Protection policy, allowing

you to configure multiple, individual PPS Protections, where each PPS Protection is configured to apply to a specific transportprotocol-TCP and/or UDP, the destination IP address, and the destination port or ports.

DNS Flood Protection Enhancements

Change of Syntax of the DNS Real-Time Signature

The syntax of the real-time signature for **Medium** strictness is changed, enabling improved detection granularity of attack traffic versus legitimate traffic. The new syntax, when the **Footprint Strictness** is **Medium,** is such that at least one Boolean AND condition must exist, and no Boolean OR condition isallowed in the top-level Boolean expression representing the DNS real-time time signature.

For example:

- AAND B
- (A OR B OR C) AND D AND E
  [where "(A OR B OR C)" is a nested expression]

Geolocation Protection Solution

Radware's Geolocation protection solution visualizes top DDoS attacking countries using a live map and feed.You can block traffic from specific countries immediately, with a click of a button in APSolute Vision Analytics, using a new dedicated attack map, which presents top attacking countries.

The mitigation solution allows the following two modes of blocking activation, depending on the need and the current threat landscape or business requirement:

- **Always-active-Persistent** configuration of allowed-country list or blocked-country list. This is done using a Geolocation profile.
- **On-demand-**Temporary country-blocking for a configurable duration. This is done using the new
  Geolocation Map in APSolute Vision Analytics.

Geolocation protection supports per-policy block/allow list configuration, providing carriers and service providers with the ability to quickly configure their tenants' country block and allow lists, making it a great solution for multi-tenant networks.

Geolocation protection requires an active subscription to the *ERT Silver Protection Package* or the *ERT GoldProtection Package.* The ERT Silver Protection Package includes the Security Update Subscription, ERT Active Attackers Subscription, and Geolocation Subscription. The ERT Gold Protection Package includes the ERT Silver Protection Package and ERT Under Attack Service.

On-Device TLS/SSL Mitigation

This version of Radware DefensePro DDoS Mitigation introduces support for software-based on-device TLS/SSL mitigation-also known as *DefenseSSL. DefenseSSL* is Radware's patented SSL-attack-mitigationsolution.

DefenseSSL offers the most efficient SSL-attack protection, with the widest coverage against SSL-based DDoS attacks, with the lowest latency.

The on-device SSL/TLS mitigation capability offers you the option to choose a simplified, one-box deployment model, to protect against clear-text, as well as against TLS/SSL encrypted volumetric attacks.

HTTPS Flood Protection

This version introduces *HTTPS Flood Protection,* to protect against flood attacks carried over the HTTPS protocol. This protection uses an innovative algorithm, which enables attack detection, attack-source characterization, and attack mitigation in the most efficient way, with minimal decryption of traffic.

HTTPS Flood Protection comprises the following stages:

1. **Attack detection-HTTPS** flood attacks are detected using an innovative proprietary algorithm that does not require traffic decryption. Radware DefensePro DDoS Mitigation establishes HTTPS traffic baselinesduring peacetime, and detects attacks based on deviations from the baselines learned, while allowing for legitimate temporary increases in traffic volume, such as in the case of *flash crowds.*

2. **Attack-sources characterization-In** the characterization stage, Radware DefensePro DDoS Mitigation uses again its innovative algorithm to distinguish between legitimate sources and sources suspected as attackers. Like the *attack detection* stage mentioned above, the *attack-sources characterization* stage does not require traffic decryption. In this stage, Radware DefensePro DDoS Mitigation creates a list of suspect sources, which is then used to mitigate the attack.

3. **Attack mitigation-For** this stage, you have the option to select from several mitigation methods. You can decide to configure Radware DefensePro DDoS Mitigation to perform traffic decryption of the first HTTPS request to send a challenge to the suspect sources. Alternatively, for cases where the SSL certificate is not available, you can opt for attack mitigation by rate-limiting the amount of HTTPS traffic from suspect sources. You can select several mitigation methods, which will be applied in an escalating manner, until the attack is fully mitigated

Radware ERT Active Attackers Feed

Radware ERT Active Attackers Feed enhances the protection of Radware-customer applications and data centers by introducing a preemptive protection layer on top of Radware DefensePro DDoS

Mitigation, available as a yearly subscription.

The feed supplies Radware DefensePro DDoS Mitigation with the non-spoofed IP addresses of a high- precision list of attackers that were recently actively involved in a DDoS attack, thus enabling the platform to preemptively block currently active, known DDoS attackers before they come anywhere near your assets andinitiate an attack.

Radware's ERT Threat Research Center provides the list of known and currently active perpetrators. The ERTActive Attackers Feed focuses on unique, real-time intelligence, which can provide preemptive protection against emerging DDoS-specific threats, including evolving loT botnets and new attack vectors.

ERT Active Attackers Feed profiles take advantage of the ERT Active Attackers Feed subscriptionallowing you to:

- Select Tor and Web Attacker blocking specifically.
- Select *Report Only* mode per category and risk level {High, Medium, Low).
- Activate and configure ERT Active Attackers Feed protection per policy.

Traffic Filters

Traffic Filters is a new protection that enables control over processing traffic through Radware DefensePro DDoS Mitigation at the policy level. Traffic Filters complement the Radware DefensePro DDoS Mitigation protections with additional manual control. With Traffic Filters, you can block or rate-limit traffic that matches specified values-or traffic *not* matching specified values. Additionally, Traffic Filters allow you to define specific network addresses or port values within the policy as the Filter Criteria.

Use cases for Traffic Filters include the following:

- **Predefined maximum rate-You** can configure a Traffic Filter for all the traffic towards a specific policy with the maximum rate {in packets per second) of the protected network and servers. This predefined Traffic Filter can help cap the maximum rate from Radware DefensePro DDoS Mitigation towards the protected network at any given time. You can configure such a filter during the initial configuration of the
- Radware DefensePro DDoS Mitigation instance.
- **Whitelisting under attack-You** can configure a Traffic Filter for the traffic that Radware DefensePro DDoS Mitigation inspects towards the protected network and block all other traffic that might match thepolicy. This way you can inspect only the expected legitimate traffic and block the rest of the traffic that reaches this policy. You can achieve this by specifying the **Non-Matching** option in Traffic Filters
- **Blocking traffic under attack**-**You** can configure a Traffic Filter for blocking or rate- limiting specific traffic or all traffic towards the policy.

Packet Anomaly Protection Additions

New Packet-Anomaly Protection: Incorrect GRE Version (ID 126)

This new packet-anomaly protection matches packets whose GRE version is not 0 or 1.

New Packet-Anomaly Protection: Invalid GRE Header (ID 128)

This new packet-anomaly protection matches packets that fulfill the following criteria: partial or sliced packets, or one or more flags are not RFC compliant.

Signature Protection Application Security Enhancements

Support for ERT Security Update Service (SUS)

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

ERT SUS consists of the following key service elements:

- **Weekly updates-Scheduled** periodic updates to the signatures file, typically weekly, with automatic distribution through APSolute Vision. ERT SUS provides protection for most known attack tools and recent vulnerabilities sourced directly from Radware's ERT group. SUS updates include DoS flooding tools, slow-Dos attacks and tools, DoS single packet vulnerabilities, and critical data-center applications vulnerabilities. Periodic updates are typically available on a weekly basis and include all new filters, including those previously released as an *Emergency* update.
- **Emergency updates-For** cases where an immediate response is necessary, Radware issues an emergency signature-file update. Emergency updates are released outside of the weekly release when there are critical vulnerabilities that put customers at risk, based on ERT analysis. These updates are accompanied by an ERT threat alert, which also provides guidance for preventive actions in addition to the signature update. Registered customers are notified via email once the emergency update is availablefor download from the Radware domain.

Complex Filters

In this version of Radware DefensePro DDoS Mitigation, you can configure complex filters for Application Security signatures. Complex filters are groups of filters assigned to the same signature, where a BooleanAND condition exists between the filters. This capability gives you

improved granularity to search for and match malicious traffic.

Additional Content Types for Filters

This release of Radware DefensePro DDoS Mitigation adds numerous **Content Type** options for Application Security signature filters. The options include: **HTTP Request Header, HTTP Request Data, *HTTP URL*, Normalized HTTP URL,** and **HTTP Cookie Header**.

Additional Content Parameters for Filters

This version of Radware DefensePro DDoS Mitigation introduces additional **Content Parameters** in the configuration of Application Security signature filters. Some of the additional **Content Parameters** are: **StartSearch at Offset, Stop Search at Offset,** and **Content Value to Match.**

HTTP Actions for Signature Protection-Application Security Signatures

The Signature Protection module protects against server-based vulnerabilities, such as Web, mail, FTP, worms and viruses, trojans and backdoors, bots, spyware, and so on. The Application Security (AppSec)module uses signatures from the Radware Signatures database, as well as user-defined signatures, andemploys a powerful string-matching engine (SME).

This release of Radware DefensePro DDoS Mitigation adds the capability to configure the followingadditional actions for Application Security signatures:

- HTTP 200 OK
- HTTP 200 OK and Reset Destination
- HTTP 403 Forbidden
- HTTP 403 Forbidden and Reset Destination

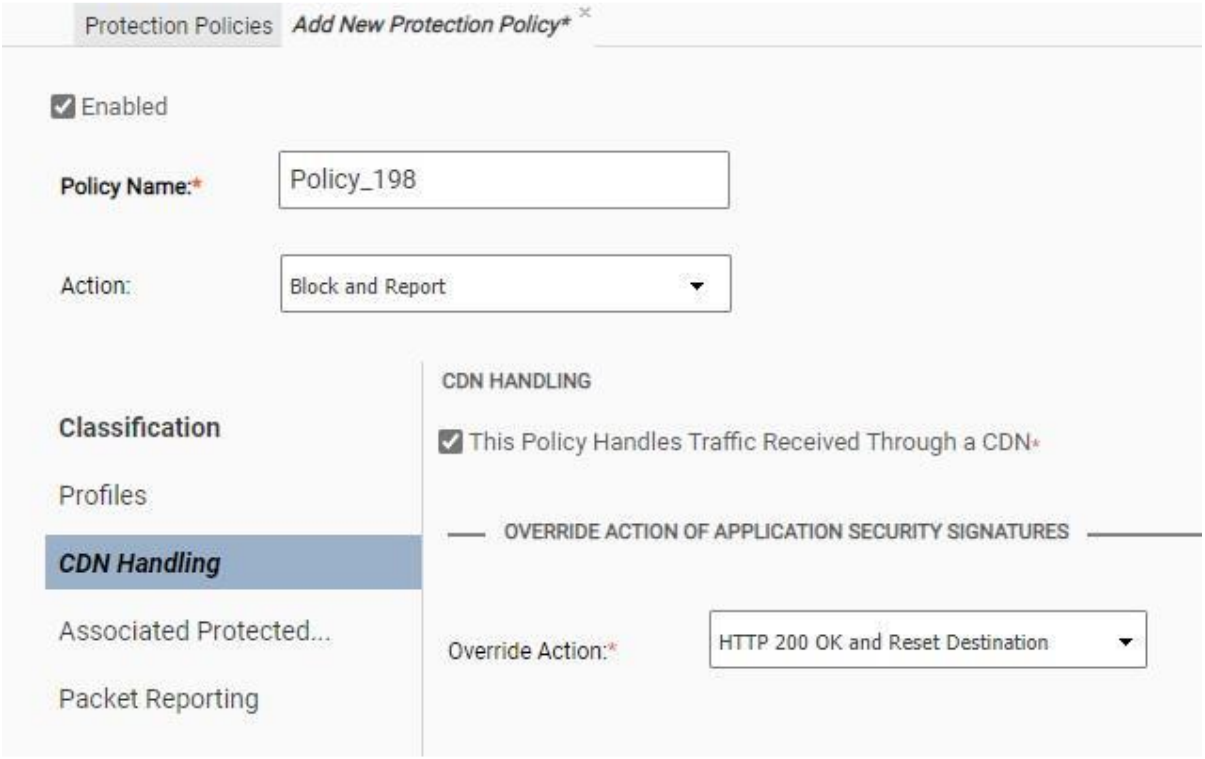
Transparent Proxy Authentication for SYN Flood Protection

Transparent Proxy is an additional authentication method available for you to use in the configuration of SYN Flood Protection profiles. This is in addition to the existing authentication methods: **Safe Reset** and **TCP Reset.** Using **Transparent Proxy,** when Radware DefensePro DDoS Mitigation receives a SYN packet, it first authenticates the TCP session by completing a three-way handshake that includes a SYN cookie with the client. Then, once the session is determined to be legitimate, Radware DefensePro DDoS Mitigation opens a connection with the destination and acts as transparent proxy between the source and the destination, for the remainder of the session.

Per-Policy CDN Support by Signature Protection-Application Security

In this release, you have the option to configure, at the policy level, whether the traffic handled by the policy is received from a CON-and if so, whether the Signature-Protection Application- Security signatures use one of the available HTTP actions for traffic that matches the signature.

Figure 4: CDN Handling Policy Settings



Suspend Action for Connection Limit Protection

This release of Radware DefensePro DDoS Mitigation adds support for *Suspend* actions on Connection Limit protection. Depending on your configuration, Radware DefensePro DDoS Mitigation can suspend traffic-for adefined period of time, from one or more IP addresses that are the source of a Connection Limit attack.

Furthermore, recurring offending source IP addresses can be suspended additional times, with increasedsuspension times.

Reset Destination of Aged Unestablished Sessions

This configuration setting enables Radware DefensePro DDoS Mitigation to send a TCP Reset packet to the destination of aged, unestablished sessions. DefensePro considers a session as unestablished or not fully established, when the session establishment does not complete within the **Non-Established-Session Aging**

Time, and according to the configuration of **Consider Session Established Only If Data Sent after TCP Handshake** parameter.

Allow Large EONS Packets

Extension Mechanisms Protocol for DNS (EDNS) is a set of extension mechanisms to expand the size of the DNS message. While the first EDNS standards date back to 1999, on February 1, 2019, major DNS software and service providers removed DNS workarounds that allowed users to bypass EDNS.

You can now decide, when checking for DNS protocol compliance, whether to allow large EDNS packets, meaning packets larger than 512 bytes.

Enable Syslog Granular Reporting by Message Type

You can now configure the type of syslog event messages that Radware OefensePro OOoS Mitigation will send to each syslog server configured. For each target syslog server you configure, you can select whether Radware OefensePro OOoS Mitigation will send security events, and/or device-health events, and/or configuration-auditing events.

Enable Sending of SNMP Traps by Event Type

You can now configure the type of SNMP trap messages that Radware OefensePro OOoS Mitigation sendsto each SNMP target configured. For each SNMP target server that you configure, you can select whether OefensePro will send security-event traps, and/or device-health-event traps, and/or audit-event traps.

Support for TLS 1.3 and for Elliptic Curve Cryptography Certificates

This release of Radware OefensePro OOoS Mitigation adds support for the configuration and use of TLS 1.3cryptographic protocol for data traffic, as part of the configuration of *Protected SSL Objects.* TLS 1.3 includes major improvements in the areas of privacy and security, and only includes support for algorithms with no known vulnerabilities at the time of its standartization (August 2018).

Additionally, this release introduces support for using *Elliptic Curve Cryptography* (ECC) certificates. ECC useskeys that are substantially shorter than RSA, resulting in less data being verified during TLS handshakes, and hence, less computational overhead.

CLI-based Option to Control the TLS Versions Used by the HTTPSManagement Interface

This release introduces a CLI-based option, manage ssl version, which allows you to control the TLSversions used by the Radware OefensePro OOoS Mitigation HTTPS management interface.

TACACS+ for Device Authentication

You can now use a TACACS+ authentication server to authenticate users logging in to Radware OefensePro OOoS Mitigation.

Monitoring CPU Utilization per Policy

Aimed at shared-device use cases, monitoring of the CPU utilization per Protection policy enables better understanding of resource consumption by each Radware OefensePro OOoS Mitigation Protection policy.

The additional visibility can assist you in the following:

- Tuning the Protection policy for optimized device-resource usage
- Detecting "heavy consumers"
- Maintaining an acceptable device-CPU utilization level by tuning, removing, or diverting "noisy" Protection policies

Monitoring CPU Utilization per Protection policy provides the following:

- Peacetime and under-attack CPU utilization per-policy graph using APSolute Vision Analytics(AVA) AMS
- Configurable thresholds for policy CPU-utilization alert activation and termination
- AVA AMS, SNMP, and syslog alerting options

Per-Profile Granular Reporting Settings for BDoS and SYN Flood Protection

BDoS and SYN Flood Protection profiles now allow you the option to decide whether traffic that matches the profile should be blocked and reported, or only reported.

SNMP 01D for Monitoring of Concurrent Sessions

The following two SNMP object identifiers (OID) have been added:

- OID .1.3.6.1.4.1.89.35.1.104.53retrieves the aggregated number of sessions monitored by the Radware DefensePro DDoS Mitigation device.
- OID .1.3.6.1.4.1.89.35.1.104.54.1.2retrieves the number of sessions monitored per Radware DefensePro DDoS Mitigation flow-engine {OPE).

WHAT IS CHANGED

This section describes what is changed in version 8.22.2.0.

BDoS Real-Time Signature Optimization for Fragmented Traffic

The priority of the frag-bit attribute during the creation of the BDoS Real-Time Signature (RTS) has been increased. The goal of this optimization is to enable improved mitigation of fragmented attacks by the Radware DefensePro DDoS Mitigation BDoS module.

BDoS and DNS Protection Global Settings Moved to Profile Settings

Several BDoS and DNS Flood Protection settings, which were configurable globally, per Radware DefensePro DDoS Mitigation instance, are now configurable per profile.

The settings are:

- BDoS *Footprint Strictness*
- BDoS *Learning Suppression Threshold*
- BDoS *Overblocking Prevention*
- DNS *Footprint Strictness*
- DNS *Learning Suppression Threshold*

DNS Flood Protection Global Settings

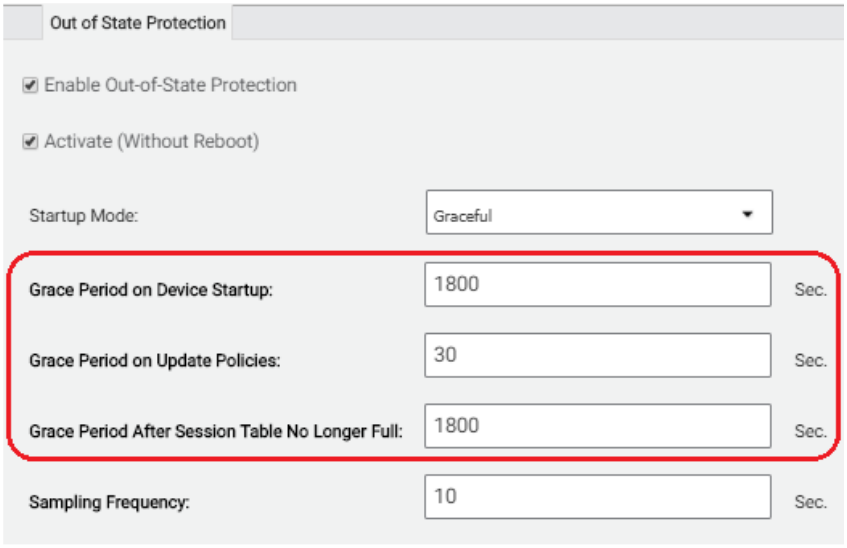
DNS Flood Protection is now enabled by default.

Configuration Options for Out-of-State Protection Grace Periods

Radware DefensePro DDoS Mitigation implements several different grace periods for Out-of-State Protection actions for different scenarios. During these grace periods, Radware DefensePro DDoS Mitigation delays Out-of-State Protection mitigation actions.

This release introduces configuration options for the different Out-of-State Protection grace periods, using APSolute Vision, CLI, and SOAP.

Figure 5: Out of state Protection Grace Periods



Enhancements to Packet-Anomaly Protection *Unrecognized L2 Format* (ID 100)

The packet-anomaly protection *Unrecognized L2 Format* (ID 100) is enhanced with the following:

- Added additional criteria
- Changed the default **Action** to **Report**

Multiple Packet Reporting Destinations

You can now configure up to five IP addresses as destinations for Packet Reporting.

NTP Settings

The user-configured **Polling Interval** is applicable when the NTP server is available as well as when the NTP server is not reachable/unavailable.

A new CLI command, services ntp server-last-poll, has been added. This command enables the device to display the time of the last successful poll of the NTP server and the NTP-server/device deviation, expressed in seconds.

128-bit Encryption for SNMPv3 Security

Starting with this version, Radware DefensePro DDoS Mitigation supports the use of AES with 128-bit keysize the SNMPv3. AES-128 enhances encryption capabilities of SNMPv3 beyond the SNMPv3 standard.

Stronger Encryption Ciphers for SSH

This release of Radware DefensePro DDoS Mitigation enables, by default, encryption ciphers for SSH that areconsidered stronger, such as aes128-cbc, aes192-cbc, and aes256-cbc-and disables, by default, encryption ciphers for SSH that are considered weak, such as arcfour and

blowfish-cbc.

The new CLI command, manage ssh algorithms set, enables you to set the encryption ciphers used forSSH.

Support File Generation Without Hashed Passwords

By default, when you generate the DefensePro technical support file, the file includes some passwords,which are always encrypted or hashed.

A new CLI command is now available, enabling you to request that DefensePro generates its technicalsupport files without any user credentials (that is, files without even encrypted or hashed passwords).

The syntax of the command is:

system internal config-file remove credentials-info {011}

where:

- **0** specifies that the feature is disabled. That is, generated technical support files includeencrypted or hashed user credentials.
- **1** specifies that the feature is enabled. That is, generated technical support files contain nouser credentials.

Default: 0

Additional Enhancements

This version of Radware DefensePro DDoS Mitigation includes the following additional enhancements:

- The Radware DefensePro DDoS Mitigation device password now supports using ASCII non- alphabetical symbol characters.
- The maximum allowed length for a policy name is increased to 64 characters.
- Radware DefensePro DDoS Mitigation always processes IPsec traffic, meaning traffic using IP protocol numbers 50 and 51.
- SNMP credentials are now masked in messages sent to syslog servers.
- The default value for the **Capture Port Group** parameter of the *Diagnostic Tool Parameters* is now **On Data Ports.**

KNOWN LIMITATIONS

The list of known limitations, available to customers only, is available at the following link: https://support.radware.com/app/answers/answerview/aid/1025271 .

RELATED DOCUMENTATION

The following documentation is related to this version:

- *Radware DefensePro DDoS Mitigation 8.22.2.0 User Guide*

For the latest Radware product documentation, visit:http:// portals.radware.com/Customer/Home/