



Radware DefensePro DDoS Mitigation Release Notes
Software Version 8.10.01
Last Updated: August, 2016

Table of Contents

CONTENT	3
RELEASE SUMMARY	3
SUPPORTED PLATFORMS AND MODULES	3
MANAGEMENT SUPPORT	3
UPGRADING THE APSOLUTE VISION VERSION 3.40 DEVICE DRIVER FOR RADWARE DEFENSEPRO DDOS MITIGATION	3
SCHEDULED TASK FOR DEFENSEPRO CONFIGURATION TEMPLATES IS REMOVED	5
UPDATING THE ONLINE HELP ON THE APSOLUTE VISION SERVER	5
WHAT'S NEW	6
PERFORMANCE ENHANCEMENTS	6
POLICY EXPORT AND IMPORT	6
OUT-OF-STATE PROTECTION	6
SESSION TABLE	6
GRACE PERIOD FOR OUT-OF-STATE PROTECTION ENFORCEMENT	6
UDP FRAGMENTATION FLOOD IN BEHAVIORAL DOS PROTECTION	7
BYPASS SUPPORT FOR JUMBO FRAMES	7
DIAGNOSTICS PACKET CAPTURE	7
SUPPORT FOR TLS V1.2 ON THE MANAGEMENT INTERFACE	7
REMOVED DEFAULT DEVICE PASSWORD	7
KNOWN LIMITATIONS	7
LIMITATIONS IN VERSION 8.10.01	8

Content

Radware announces the release of Radware DefensePro DDoS Mitigation version 8.10.01.

These release notes document describes new capabilities and maintenance fixes since the previous released version of DefensePro for Cisco Firepower 9300 version 1.01.02.

Release Summary

This release continues enhancements of the new DefensePro architecture, which is able to demonstrate high detection and mitigation capacity.

Release date: July 2016

Build number: 14

Supported Platforms and Modules

This version is supported by the following platforms:

Product	Platform	SME	DME
Radware DefensePro DDoS Mitigation	Virtual	No	No

Management Support

This Radware DefensePro DDoS Mitigation version is supported by APSolute Vision version 3.60.00 and later. If you are using a previous version of APSolute Vision, it is recommended to upgrade to version 3.60.00.

Alternatively, Radware DefensePro DDoS Mitigation version 8.10.01 can be supported by APSolute Vision version 3.40.00. In order for APSolute Vision version 3.40.00 to support the full range of new capabilities introduced by Radware DefensePro DDoS Mitigation version 8.10.01, the Radware DefensePro DDoS Mitigation driver for APSolute Vision must be updated. For more information, see the following section “Upgrading the APSolute Vision Version 3.40 Device Driver for Radware DefensePro DDoS Mitigation .”

Upgrading the APSolute Vision Version 3.40 Device Driver for Radware DefensePro DDoS Mitigation

This section contains the procedure for upgrading the APSolute Vision version 3.40 device driver for Radware DefensePro DDoS Mitigation.

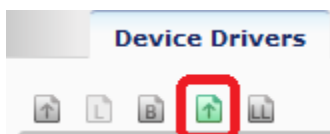
The procedure is not necessary if you are using APSolute Vision version 3.60.00 or later.

The procedure must be performed only after upgrading the Radware DefensePro DDoS Mitigation device to version 8.10.01.


To upgrade the APSolute Vision version 3.40 device driver for Radware DefensePro DDoS Mitigation

1. On the Radware.com Customer Portal, download the file DefensePro Software Version 8.10.00 Driver for APSolute Vision v3.40 from <https://portals.radware.com/getattachment/2cd15289-40ee-468c-95e8-2dbd983de59a/DefensePro-Software-Version-8-10-00-Driver-for-APS>.
2. On your APSolute Vision version 3.40 server, in the APSolute Vision *Settings* view *System* perspective, select **General Settings > Device Drivers**.
3. From the list of device drivers, select the row showing DefensePro product version 8.10.00.
4. Make sure that the *Driver in Use* column shows *Hud_DefensePro-8.10.00-DD-1.00_36*.

5. Click the  (Upload Device Driver) button.



Note: Make sure that you do *not* click the *Update Device Driver* button.

6. In the *Upload Device Driver* dialog box, browse to the file you downloaded in step 1, and click **Upload**.
7. Make sure that the *Latest Driver* column shows *Hud_DefensePro-8.10.00-DD-1.00_502*. If it does not, refresh the browser page.
8. From the list of device drivers, select the row showing DefensePro product version 8.10.00.
9. Click the  (Update to Latest Driver) button.



Note: Make sure that you do *not* click the *Update All Drivers to Latest* button.

10. Make sure that the *Driver in Use* column shows *Hud_DefensePro-8.10.00-DD-1.00_502*.

Scheduled Task for DefensePro Configuration Templates Is Removed

The APSolute Vision scheduled task *DefensePro Configuration Templates* has been temporarily removed from APSolute Vision due to a critical device issue: in some cases, this task may cause Radware DefensePro DDoS Mitigation devices to crash. Upon upgrade to version 3.60.00, existing *DefensePro Configuration Templates* tasks are deleted and new tasks of this type cannot be created. The task is planned to be reinstated in a future version, once the issue is resolved.

Updating the Online Help on the APSolute Vision Server

To upgrade the online help on the APSolute Vision server and include the content of this version, upload the online-help–upgrade package from the following location <https://portals.radware.com/getattachment/fa1064e5-8951-435d-b4da-a2bad5182486/OLH-DP-v8-10-00-APSVision-v3-60-00> to the APSolute Vision server. Installation instructions are in the appendix “Managing the Online-Help Package on the Server” of the *APolute Vision User Guide*, located at <https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APolute-Vision>.

What's New

This section describes what's new in version 8.10.01.

Performance Enhancements

The performance of Radware DefensePro DDoS Mitigation has improved significantly in version 8.10.01. The expected performance of a single Virtual DefensePro for Cisco Firepower 9300 instance, using five (5) virtual cores for traffic and one (1) virtual core for management, is as follows:

Parameter	Measured	Payload
Throughput	Up to 14 Gbps	10 HTTP transactions per connection, 1 MB response
Packets per second (PPS)	Up to 1,800,000	Packet size: 78 bytes

Note: The Cisco Firepower 9300 chassis supports up to three (3) Radware DefensePro DDoS Mitigation instances.

Policy Export and Import

Radware DefensePro DDoS Mitigation version 8.10.01 adds the capability to export and import Network Protection policies. These can be then used as configuration templates. Configuration templates can include the configuration (that is, the definitions and security settings) and the policy baselines of a Network Protection policy, such as the baselines from the associated DNS or BDoS profiles.

Out-of-State Protection

Out-of-State Protection detects out-of-state packets, which provides additional protection for TCP session-based attacks.

Session Table

This release adds support for the Session table, which tracks sessions that DefensePro bridges and forwards.

Grace Period for Out-of-State Protection Enforcement

The Out-of-State Protection feature in Radware DefensePro DDoS Mitigation version 8.10.01 includes the ability of this protection to enter a grace period upon several triggers:

- After device startup or reboot.
- After *Update Polices* has occurred.
- After the Session table exits the *full* state, for a configurable time length, during which the enforcement of state is not performed.

UDP Fragmentation Flood in Behavioral DoS Protection

This release enables the configuration and use of a new type of BDoS Protection profile: *UDP Fragmentation Flood*.

Bypass Support for Jumbo Frames

This version introduces a configuration option allowing users to select whether jumbo frames received by the device are dropped or forwarded.

Diagnostics Packet Capture

Radware DefensePro DDoS Mitigation version 8.10.01 adds the capability to perform packet capture of data traffic, for diagnostic purposes. The capture files are stored on the device, can be downloaded using APSolute Vision, and can be inspected using a third-party network-protocol analyzer, such as Wireshark.

Support for TLS v1.2 on the Management Interface

TLS v1.2 is now supported when using HTTPS on the management interface.

Removed Default Device Password

This release introduces a change of behavior regarding the default username and password used for the Radware DefensePro DDoS Mitigation device. Previous versions allow the use of the default local-user credentials *radware/radware*. Starting with version 8.10.01, new deployments do not accept the default password *radware*. The user is required to configure a password during the initial *Startup Configuration* process.

Known Limitations

This section lists known limitations for this release.

Limitations in Version 8.10.01	
Item	Description
1.	A one-time <i>throughput license exceeded</i> warning might be displayed when changing licenses.
2.	Traffic statistics values displayed by Real Time Monitoring (in the APSolute Vision <i>Security Monitoring</i> perspective) do not account for the packet CRC size.
3.	Inspection of tunneled traffic is not supported on SYN Flood Protection, Packet Anomalies.
4.	No warning is displayed for 90% utilization of the licensed throughput.
5.	Packet leak may occur when sending traffic matched to PA 103.
6.	For PA 107, some packets are processed, instead of being passed through.
7.	When handling IPv6 traffic, PA 104 may also trigger PA 107.
8.	When handling IPv4 traffic, PA 104 also triggers PA 103.
9.	PA 108 traffic is dropped without reporting.
10.	The PA 110 Report Action <i>Process</i> behaves as <i>Bypass</i> .
11.	Under certain circumstances, a packet anomaly may not send traps to CLI, when the <i>Report Action</i> is set to <i>Report</i> .
12.	SYN Flood Protection in APSolute Vision Reporter reports <i>No traffic statistics</i> .
13.	Web authentication over SYN Flood Protection does not support fragmented GET or POST requests.
14.	In some scenarios, when using SYN Flood Protection with Safe-Reset, some of the RESET packets sent back by clients challenged might be forwarded to the server.
15.	When in manual mode, DNS Flood Protection may report “forward” while actually dropping traffic.
16.	In Security Monitoring per policy, Dropped Packets / Dropped Bytes are not displayed.
17.	A management port cannot be configured to use VLAN.

Limitations in Version 8.10.01

Item	Description
18.	Fragmented traffic is not shown in traffic statistics monitoring in APSolute Vision Security Monitoring.
19.	The console banner for login via SSH/Telnet must not contain a backslash (\).
20.	Network Protection policy names in APSolute Vision Reporter (AVR) must not include a comma (,) a slash (/), or a backslash (\).
21.	Excessive broadcast messages on the management network may impact the communication between Radware DefensePro DDoS Mitigation and APSolute Vision, resulting in slower operations in APSolute Vision.
22.	When resetting BDoS Protection or DNS Flood Protection baselines (which could also occur when tuning settings), the normal edge is immediately updated in APSolute Vision Security Monitoring, however the attack and suspect edges are updated within a few minutes.

North America
Radware Inc.
Ltd.
575 Corporate Drive
St. Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware
22 Raoul Wallenberg
Tel Aviv 69710, Israel
Tel: 972 3 766 8666

© 2016 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in 2 the U.S. and other countries. All other trademarks and names are the property of their respective owners. Printed in the U.S.A.



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)