Radware DefensePro DDoS Mitigation Release Notes

Software Version 8.13.01

Last Updated: December, 2017

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

TABLE OF CONTENTS

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

Content

Radware announces the release of Radware DefensePro DDoS Mitigation version 8.13.01.

These release notes document describes new capabilities and maintenance fixes since the previous released version of DefensePro for Cisco Firepower 9300 version 8.10.01.

Release Summary

This release introduces Next Generation DNS Flood Protection, which greatly enhances the DNS protection capabilities of DefensePro DDoS Mitigation, as well as a number of other enhancements, as described in this release notes document.

Release date: October 2017

Build number: 9

Supported Platforms and Modules

This 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 is supported by APSolute Vision version 3.90.00 and later. If you are using a previous version of APSolute Vision, it is recommended to upgrade to version 3.90.00.

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/c6c88ad3-8a68-4a2b-9f35-4f9109f1c3dd/Help-Upgrade-File-for-APSolute-Vision-Version-3-90 to the APSolute Vision server.

Installation instructions are in the appendix “Managing the Online-Help Package on the Server” of the APSolute Vision User Guide, located at https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision.

What’s New

This section describes what’s new in version 8.13.01.

Next Generation DNS Protection

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

Version 8.13 introduces the Next Generation DNS (NG DNS) Flood Protection, designed for the next generation of sophisticated DNS attacks. The NG DNS Flood Protection is based on an innovative behavioral mechanism designed to protect your environment from all types of query floods, including zero-day floods, such as the Mirai botnet DNS Water Torture.

NG DNS Flood Protection is able to automatically and accurately detect and mitigate all types of DNS query floods, from a basic flood to a sophisticated random-subdomains flood. In the random-subdomains flood scenario, both legitimate (“good”) queries and attack (“bad”) queries appear legitimate to the DNS server. NG DNS Flood Protection is able to distinguish, automatically and accurately, between “good” and the “bad” queries, allowing only the “good” queries to pass to the DNS server.

NG DNS is purely stateless. To achieve accurate detection of DNS query floods, Radware DefensePro DDoS Mitigation does not store any state of the DNS session.

NG DNS Flood Protection is designed for use in ingress-only environments, relying solely on incoming DNS queries for detection and mitigation. This is a key advantage that ensures early protection, especially in case of recursive random-subdomains flood, which is often revealed only after NXDomain responses are received. Radware DefensePro DDoS Mitigation can accurately and automatically detect and mitigate a recursive random-subdomains flood based solely on the incoming queries, without the need to wait for the NXDomain responses.

NG DNS Flood Protection maintains the query-type granularity, and is able to accurately detect and mitigate a query flood on a specific query type, such as A, AAAA, and so on.

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

Positive Protection Model

Version 8.13.01 introduces a novel behavioral mechanism, based on a positive protection model for DNS queries. NG DNS Flood Protection collects rate and rate-invariant statistics on query type, query rate, and Fully Qualified Domain Names (FQDNs) during peacetime. The NG DNS Flood Protection engine analyzes and correlates all the statistics, for accurate attack detection and mitigation.

Enhanced Real-Time Signature

To complement the positive protection model, NG DNS Flood Protection adds enhancements to the Real-Time Signature algorithm. In version 8.13.01, the Real-Time Signature algorithm is able to accurately isolate the target domain name within the FQDN. This enhancement provides high granularity in attack characterization, and therefore, accurate and surgical mitigation of random-subdomains floods.

DNS Configuration

The new positive protection model and Real-Time Signature enhancements operate automatically after attaching a DNS profile to an active Network Protection policy. As such, there are no new settings required, apart from the existing DNS profile settings.

The main changes in DNS configuration screens are as follows:

- **Learning Suppression Threshold** is now available through APSolute Vision. (APSolute Vision Configuration perspective, **Setup > Security Settings > DNS Flood Protection > Learning Suppression Threshold**.) Learning suppression is essential to ensure accurate DNS detection. Learning suppression helps maintain a normal baseline that is sufficiently high for flood detection when the DNS query rate drops significantly below the baseline.
- In the configuration of a DNS Protection profile (APSolute Vision Configuration perspective, **Network Protection > DNS Protection Profiles > DNS Profile**):
  - New Rate Settings tab–consolidates all rate-related settings for the behavioral engine configuration, which contains the following parameters:
    - **Expected DNS Query Rate**—moved from Query Protections and Quotas tab
    - **Max Allowed QPS** and **Signature Rate-Limit Target**—moved from Action tab.
  - New Subdomains Whitelist tab—The Subdomains Whitelist is an aggregated list of the top-n FQDNs (by occurrences) seen in the traffic. A single Radware DefensePro DDoS Mitigation device is able to process and analyze tens of millions of FQDNs, which are aggregated for visibility and management purposes into the Subdomains Whitelist. You can import and export the Subdomains Whitelist and add manual entries.

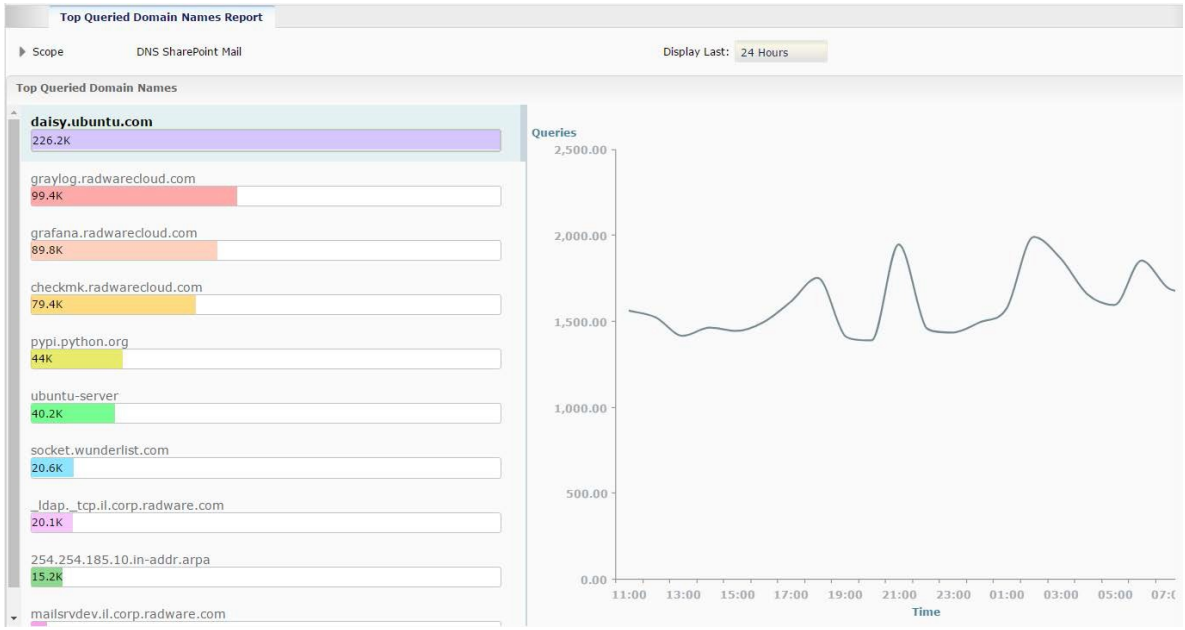
New DNS Reports

Version 8.13.01 introduces a brand-new report that displays the top 10 FQDNs in the environment. The report shows the top 10 FQDNs, by number of occurrences, within the selected period. The available periods are 10 minutes, 1 hour, 12 hours, and 24 hours. You can examine the trend of occurrences for each FQDN by double-clicking on a specific FQDN in the list.

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

The new report, named **Top Queried Domain Names Report**, is in the Security Monitoring perspective, under Traffic Monitoring.

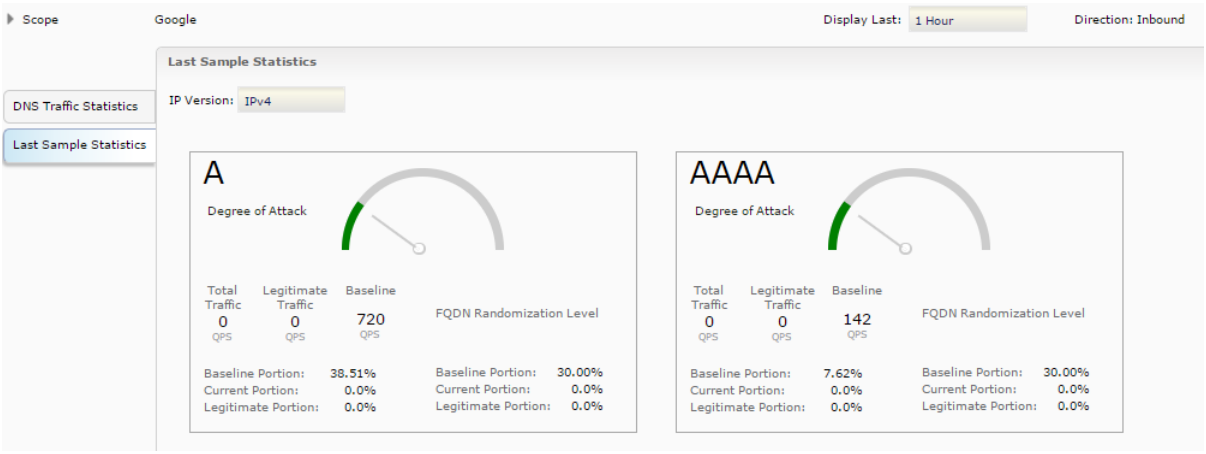
Figure 1: Top Queried Domain Names Report



For Radware DefensePro DDoS Mitigation version 8.13.01, the Last Sample Statistics tab under Protection Monitoring has been redesigned. Now, the Last Sample Statistics tab graphically displays, per query type, the degree of attack along with the DNS rate-based and rate-variant statistics.

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

Figure 2: Last Sample Statistics Tab



Signature Protection – Application Security

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 Signature Protection module includes DoS Shield protection (which was already available in previous Radware DefensePro DDoS Mitigation 8.x versions) and the newly added Application Security module. Both the DoS Shield and the Application Security protections use signatures from the Radware Signatures database. This database is continuously updated by Radware's Vulnerability Research Team (VRT), and protects against all known threats. Additionally, you can create user-defined signatures.

Application Security protection uses a powerful software-based string-matching engine (SME).

In this release, Application Security supports the following:

- Low complexity filters
- The Track All tracking type
- The Drop and Report Only actions
- The Text and Regular Expression content types
- The Destination Reset signature action
- Packet tracking options:
    - By Source Count
    - By Destination Count
    - By Source and Destination Count

More Signature Protection capabilities are planned for future Radware DefensePro DDoS Mitigation releases.

Connection Limit Protection

Connection Limit protection protects against session-based attacks, such as half-open SYN attacks, request attacks, and connection attacks, by limiting the number of new TCP or UDP connections per second allowed for specific source, or destination, or source and destination pair.

Passive Challenge for DNS Flood Protection

When using the DNS Flood Protection Passive Challenge, Radware DefensePro DDoS Mitigation mitigates DNS Flood attacks by dropping A and AAAA DNS queries originating from a client that has not yet been authenticated. When the same client retransmits a query within the specified period, Radware DefensePro DDoS Mitigation considers the client legitimate.

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

Diagnostics Packet Capture Enhancements

Radware DefensePro DDoS Mitigation version 8.13.01 enhances the capability to perform packet capture of data traffic, for diagnostic purposes, by adding the following capabilities:

- Configurable option to select whether traffic capture is performed on data ports only, on management ports only, or on both management and data ports.
- Configurable option to decide the packet capture rate, which applies per Radware DefensePro DDoS Mitigation core (DPE).
- Capture files stored on the device are now compressed before download through APSolute Vision.

DNS Baseline Learning Suppression

The DNS Baseline Learning Suppression feature enables preserving a good DNS-baseline value in scenarios where, at certain times, Radware DefensePro DDoS Mitigation handles very little DNS traffic. A CLI-only option was added in this release, which allows the configuration of a threshold, specified as a percentage of the Expected DNS Query Rate, below which Radware DefensePro DDoS Mitigation suppresses DNS-baseline learning.

TLS version 1.1 or Later Required for Management Interface

In this release, HTTPS connectivity to the management interface of Radware DefensePro DDoS Mitigation requires TLS version 1.1 or later, no longer accepting TLS version 1.0.

Compression of the Technical Support File

In this release, the Radware DefensePro DDoS Mitigation technical-support file is compressed before download through APSolute Vision. The compression greatly reduces the size of the technical-support file, thus enabling shorter download time.

Fix for the NTP Vulnerability Exposed by CVE-2015-5300

This release includes a fix to address the NTP panic threshold bypass vulnerability, as exposed by CVE-2015-5300.

© 2017 Cisco | Radware. All rights reserved. This document is Cisco Public.

North America	International
Radware Inc.	Radware Ltd.
575 Corporate Drive	22 Raoul Wallenberg St.
Mahwah, NJ 07430	Tel Aviv 69710, Israel
Tel: +1-888-234-5763	Tel: 972 3 766 8666

© 2017 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in 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)