

HARPP 3.3.1 Release Notes



Document Classification	Public
Date	April 28, 2017
Version	3.3.1

- New Features
 - Fresh New Reporting Engine and Report Templates
 - Cascade HA Topology with Active/Active Topologies
 - Hardware Bypass Status and Configuration
 - Advanced SYN Flood Prevention Options
 - Automated Failure Recovery
 - TFTP Reply Flood Signature
- Improvements/Enhancements
 - Performance Improvements on Inspection Mechanism
 - Performance Improvements on UDP Traffic
 - Duration Field Added to Repeater Blocking Custom Rule
- Bug Fixes
- Known Issues

New Features

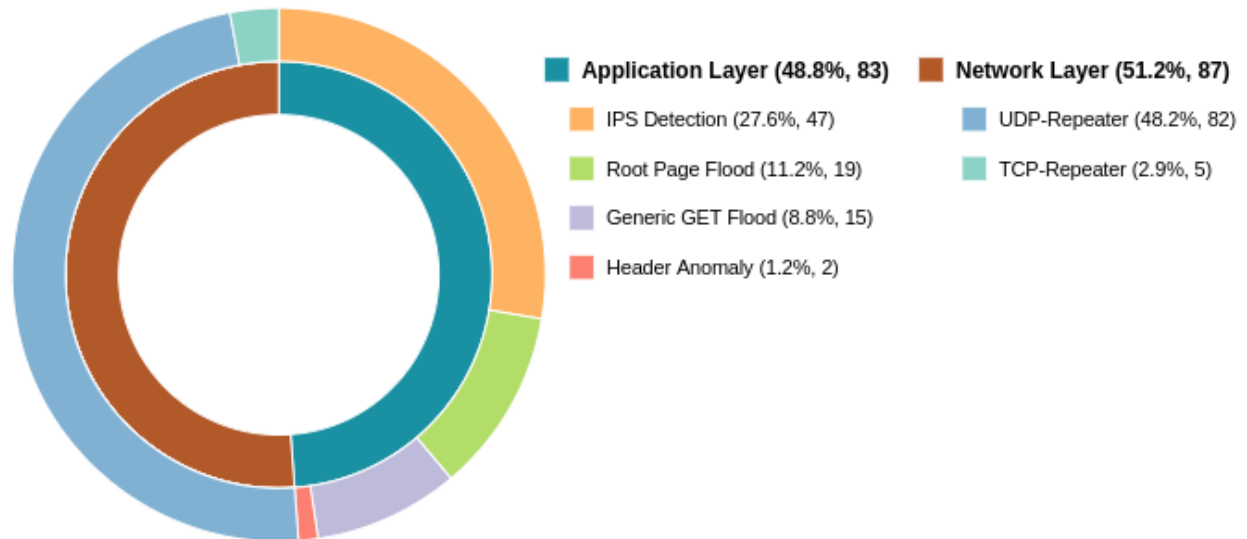
Fresh New Reporting Engine and Report Templates

Reporting engine is able to prepare modern looking reports with the release. This template clearly separate different report types and also provide Network-Application Layer attack breakdown of attacks. Please see some screenshots below.

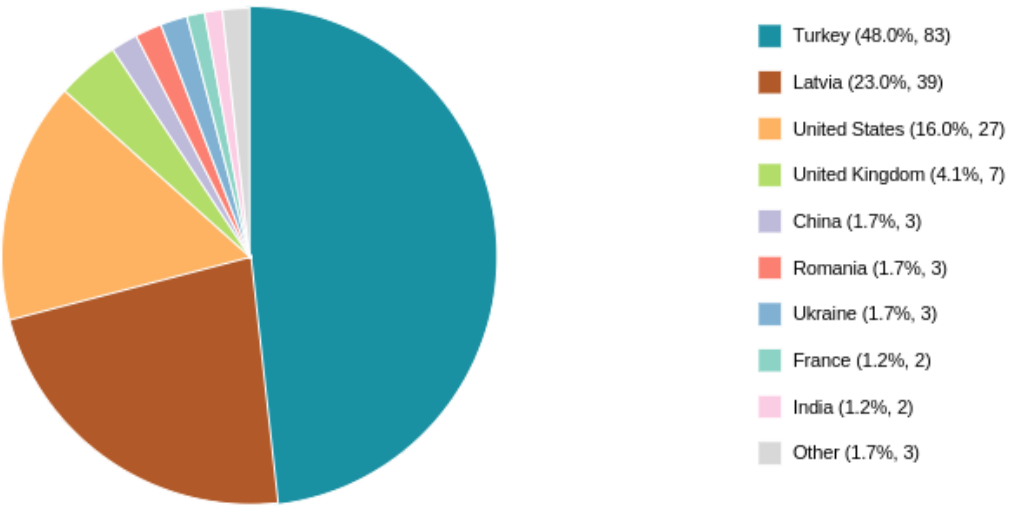
Summary

Description	Value
Total Attacks	170
Top Attack Type	UDP-Repeater (82)
Top Attack From	Turkey (83)
Top Attacker	46.183.221.146 (39)
Top Incoming PPS (Packets/s)	947,282
Average Dirty PPS (Packets/s)	1,667
Top Incoming BPS (Mbits/s)	9,455
Average Client Count (Clients/s)	42
Average Cpu Usage (%)	14
Average HTTP Traffic (Requests/s)	1
Top Session Count	21,217

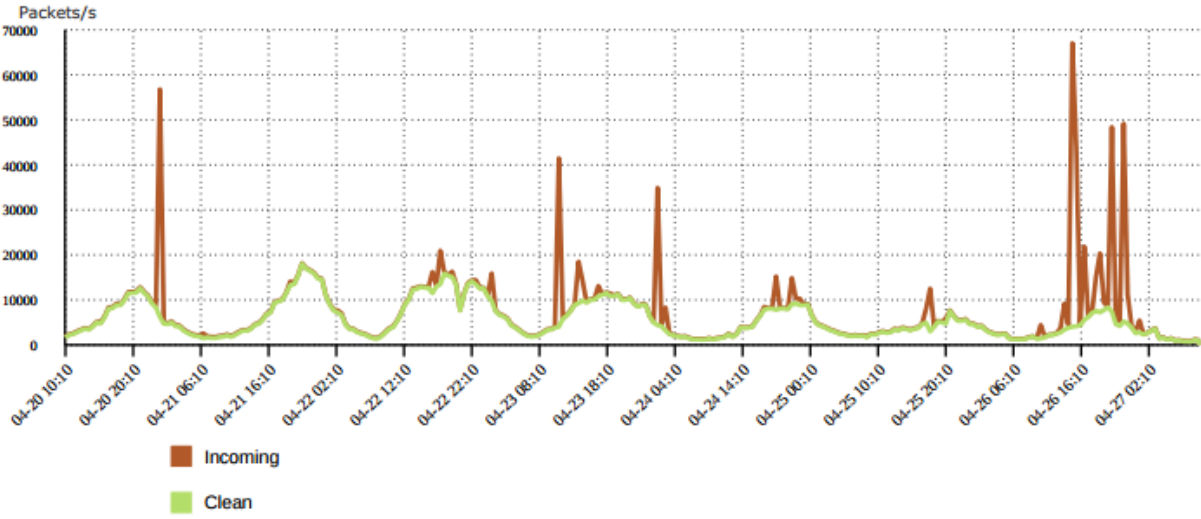
Attacks Based on Types



Blocked IP Sources

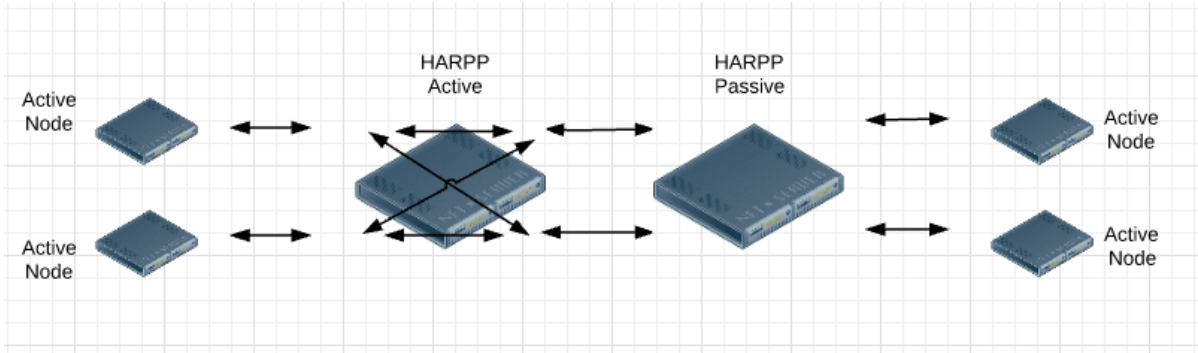


Incoming vs Clean PPS



Cascade HA Topology with Active/Active Topologies

HARPP is added Cascade HA topology for installation in Active/Active network topologies. Configuration is easy and requires just adding all connected interfaces into a single bridge interface. Also, Installation Wizard is capable of the new configuration.



Hardware Bypass Status and Configuration

Hardware bypass status can be seen on graphical interface. It can be also enabled/disabled by there.

The screenshot shows the HARPP Management interface. The top navigation bar includes 'DASHBOARD', 'MANAGEMENT', 'STATUS', and 'REPORTS'. Below this, there are links for 'WhiteLists and BlackLists', 'Mitigator Actions', 'Systemwide Settings', 'LNADS Config', 'Backup', 'User Settings', 'Report Settings', and 'Network Settings'. The main content area is divided into three columns: 'Firewall Settings', 'OS Settings', and 'Hardware Settings'. A 'Save Settings' button is located at the bottom left.

Firewall Settings	OS Settings	Hardware Settings
<input checked="" type="checkbox"/> Only Allow Administrators List to Manage <input type="text" value="20000000"/> Maximum States <input type="text" value="15"/> UDP First Timeout <input type="text" value="20"/> UDP Multiple Timeout <input type="text" value="15"/> TCP First Timeout <input type="text" value="86400"/> TCP Established Timeout <input type="text" value="15"/> TCP Opening Timeout <input type="text" value="15"/> TCP Closing Timeout <input type="text" value="15"/> TCP Finwait Timeout <input type="text" value="15"/> TCP Closed Timeout	<input type="checkbox"/> Enable Logging For Accepted Packets <input type="checkbox"/> Enable Logging For Denied Packets <input type="checkbox"/> Reverse Path Checking <input type="text" value="32"/> Semaphore ID Limit <input type="text" value="512"/> Semaphores Limit <input type="text" value="185"/> Keep Logs <input type="text" value="2000000"/> Hash Table Limit <input type="checkbox"/> Use Relay Host to Send Alert E-Mails <input type="text" value=""/> Relay Host <input type="text" value=""/> Relay Port <input type="text" value="8888"/> Connection Port	<input type="checkbox"/> Hardware Bypass Status <p>OFF: Bypass mode disable for ethernet ports. Network packets can be traced and inspected</p> <p>ON: Bypass mode enable for ethernet ports. Network packets could not be traced and inspected</p>

Advanced SYN Flood Prevention Options

Advanced SYN Flood Prevention options can be configured via graphical interface, now. There 2 configuration options.

- 1- "Window scale" should be same as protected servers' window scale value to SYN authentication functions work properly.
- 2- If 'Drop All Invalid TCP Connections' checked, all invalid TCP connections will be dropped even if this prevention method disabled. It is recommended that option to be checked to prevent most types of TCP DDoS attacks.

Protection Zone Definition

- Packet Normalization
- **Spoofed IP and SYN Flood Prevention**
- SYN Rate Limiting for Popular TCP Protocols
- SYN Rate Limiting for Other TCP
- SYN Rate Limiting for TCP HTTP
- HTTP GET Root Page Flood Detection
- HTTP GET Generic Detection
- HTTP Header Anomaly Detection
- Bad Agent Flood
- Application Detection
- Block Tor Exit Nodes
- Block Bogon and Unused IP Subnets
- Block Internal Allocated Subnets
- Trap Connection Detection
- Application Level IPS
- Drop DNS Packets
- DNS Spoof Prevention
- UDP Spoof Prevention
- Drop UDP Packets
- ICMP Flood Mitigation
- Block IPv6
- Monitoring Mode
- Geographic Blocking
- Protocol Management
- Custom Rules

Spoofed IP and SYN Flood Prevention

Action is Enabled **ON**

Window Scale:

Drop All Invalid TCP Connections:

Save

Enables/Disables TCP Spoof IP detection and prevention.
Window scale should be same as protected servers so that this prevention method work.
If drop all invalid TCP connection checked, all invalid tcp packets will be dropped even if that prevention is disabled.
It is recommended that option to be checked to prevent most types of tcp attacks.

Automated Failure Recovery

In case of operating system failures, HARPP will reboot itself and collect dump file for inspection. This feature prevents connection problems of HARPP appliances configured as bridges without bypass interfaces.

TFTP Reply Flood Signature

TFTP Reply Flood attack signature has been added to DDoS IPS database so that these type of attacks will be detected.

Improvements/Enhancements

Performance Improvements on Inspection Mechanism

In these release, we have improved performance by enhancing inspection and evidence collection methods of all applications.

Performance Improvements on UDP Traffic

We have adjusted UDP hash mechanism for received traffic to improve routing performance.

Duration Field Added to Repeater Blocking Custom Rule

Duration field determine the minimum duration for that attacker will be released. Now, it can be configured during rules creation.

The screenshot displays the HARPP (ddos mitigator) web interface. The top navigation bar includes 'DASHBOARD', 'MANAGEMENT' (selected), 'STATUS', and 'REPORTS'. Below this, a secondary navigation bar lists various settings: 'WhiteLists and BlackLists', 'Mitigator Actions', 'Systemwide Settings', 'LNADS Config', 'Backup', 'User Settings', 'Report Settings', and 'Network Settings'. The main content area is divided into a left sidebar with a list of protection zones (e.g., 'Packet Normalization', 'Spoofed IP and SYN Flood Prevention') and a central 'Custom Rules' section. The 'Custom Rules' section shows 'Action is Enabled' with a green 'ON' button and a list of rules under the heading 'All Rules'. A 'Create New Rule' dialog box is open, allowing configuration of a new rule. The dialog includes fields for 'Action Name*' (set to 'Repeater Blocking'), 'Interface*' (set to 'External'), 'Filter', 'Activation Threshold (pps)*', 'Time Window (seconds)', and 'Duration (sec.)'. It also features an 'Activate after creation' checkbox which is checked. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. A help text at the bottom of the dialog explains the Repeater Blocking rule: 'Repeater Blocking rule monitors the network traffic on the specified interface. If it detects any IPs which are transmitting packets at a rate which is above the specified pps threshold then those IPs are blocked.'

Bug Fixes

- STP (Spanning Tree Protocol) is enabled on bridged interfaces to prevent bridge loops and the broadcast radiation.
- Showing attacker IP as destination IP on rate limit typed attack's report bug has been fixed.
- "Show Evidences" link button removed for attacks which are not collecting pcap evidence such as rate limiting or custom rules.
- Contradiction between link attack duration and attack start/end time of reports is fixed.

Known Issues

- Syn proxy may block traffic for a VMware Vcenter server. Vcenter server should be added to whitelist.
- Routes may not be synced properly if HA devices have different interface names for external and internal.
- HA configuration will fail after factory reset.