# HARPP 3.3.1 Release Notes

| | |
|---|---|
| Document Classification | Public |
| Date | April 28, 2017 |
| Version | 3.3.1 |



## New Features

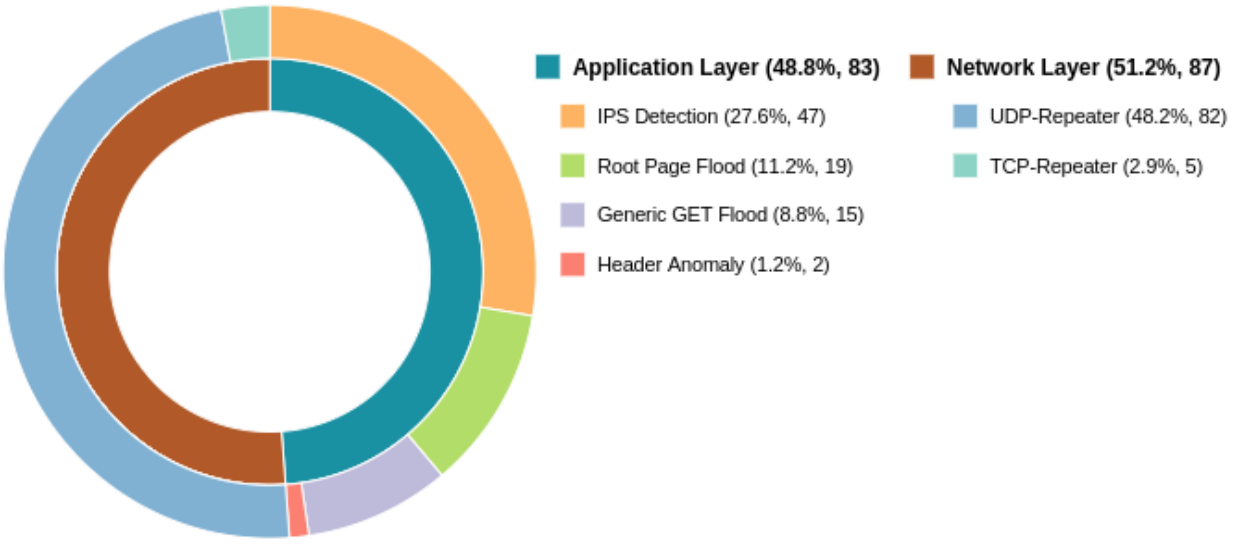
### Fresh New Reporting Engine and Report Templates

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.

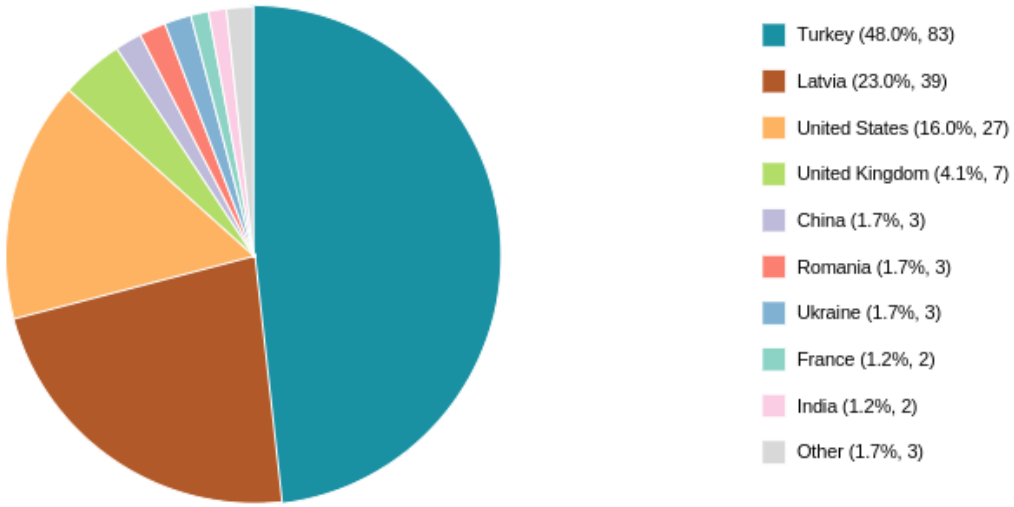
## Summary

| 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 |

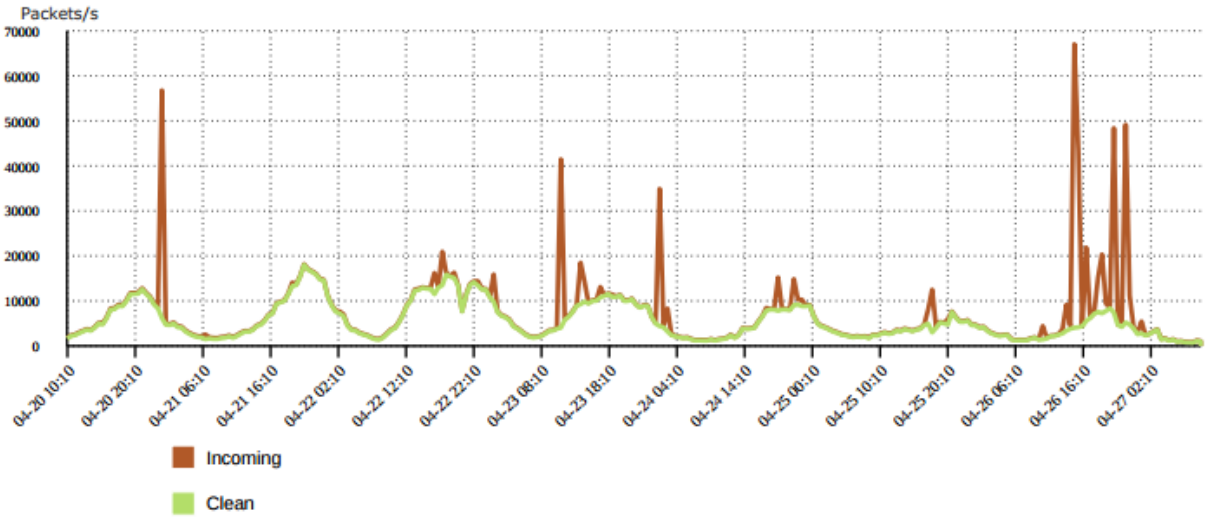
## Attacks Based on Types



## Blocked IP Sources

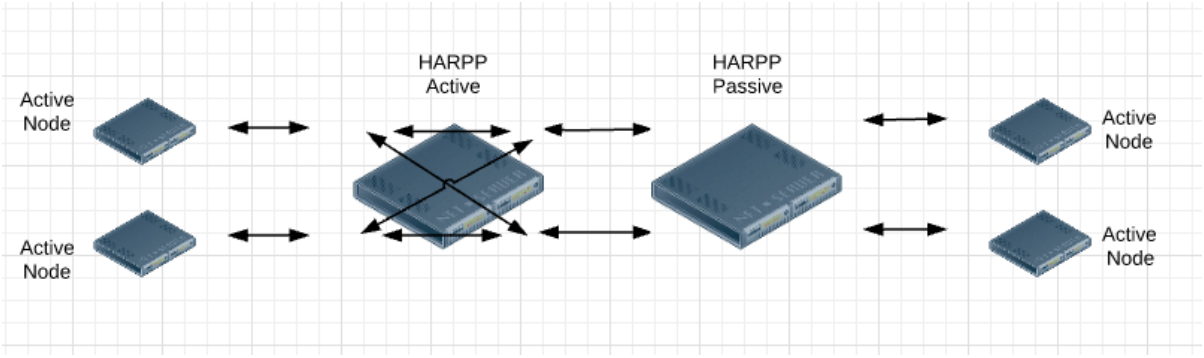



## Incoming vs Clean PPS



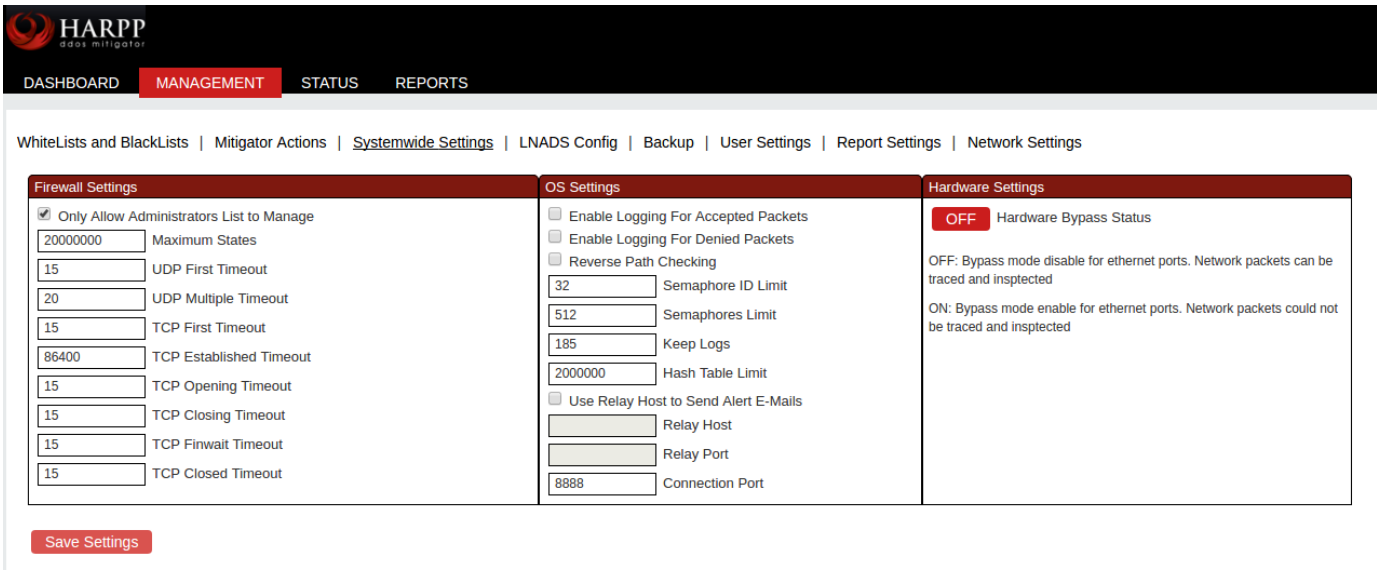

## Cascade HA Topology with Active/Active Topologies

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.

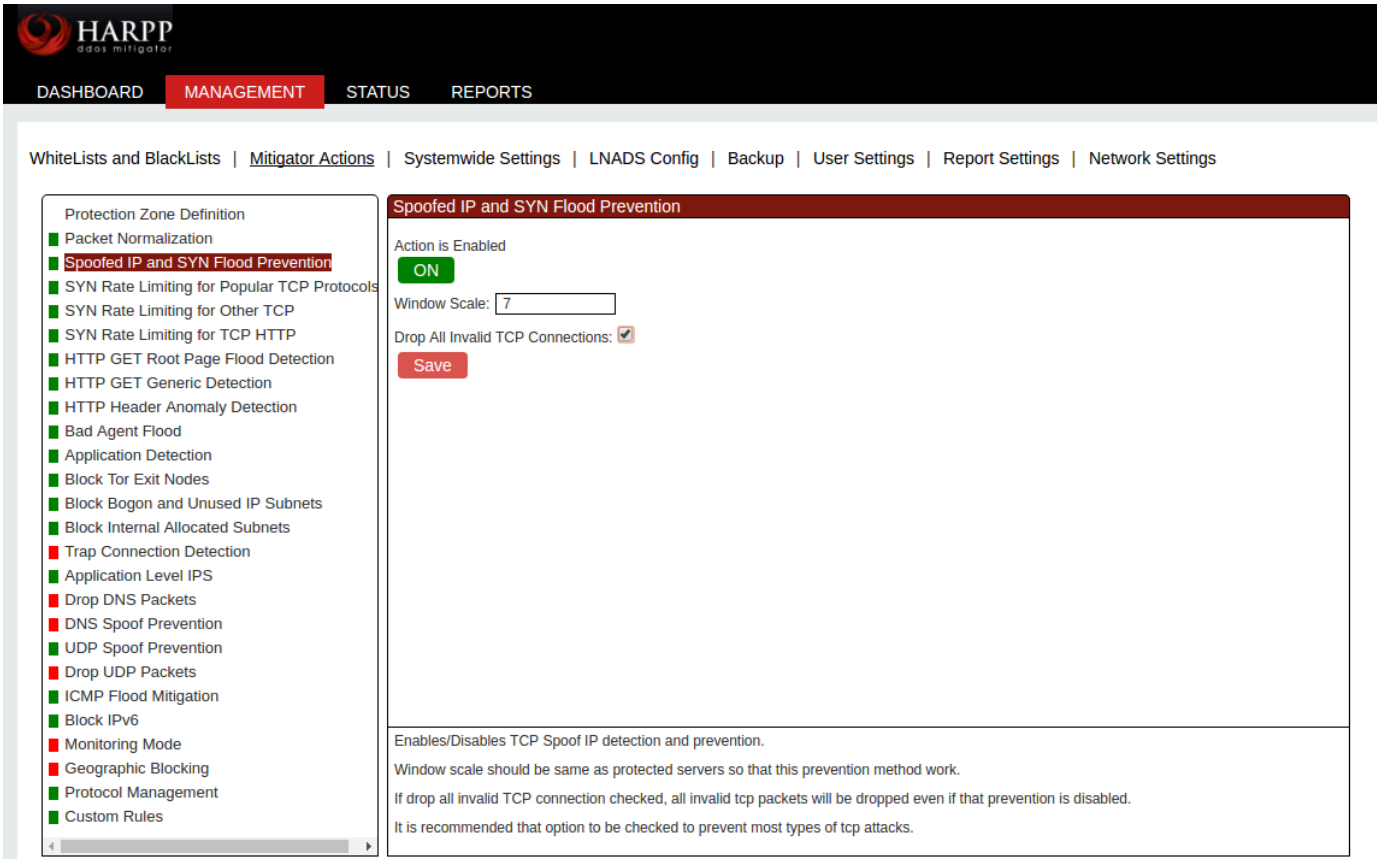



## Advanced SYN Flood Prevention Options

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.




### 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

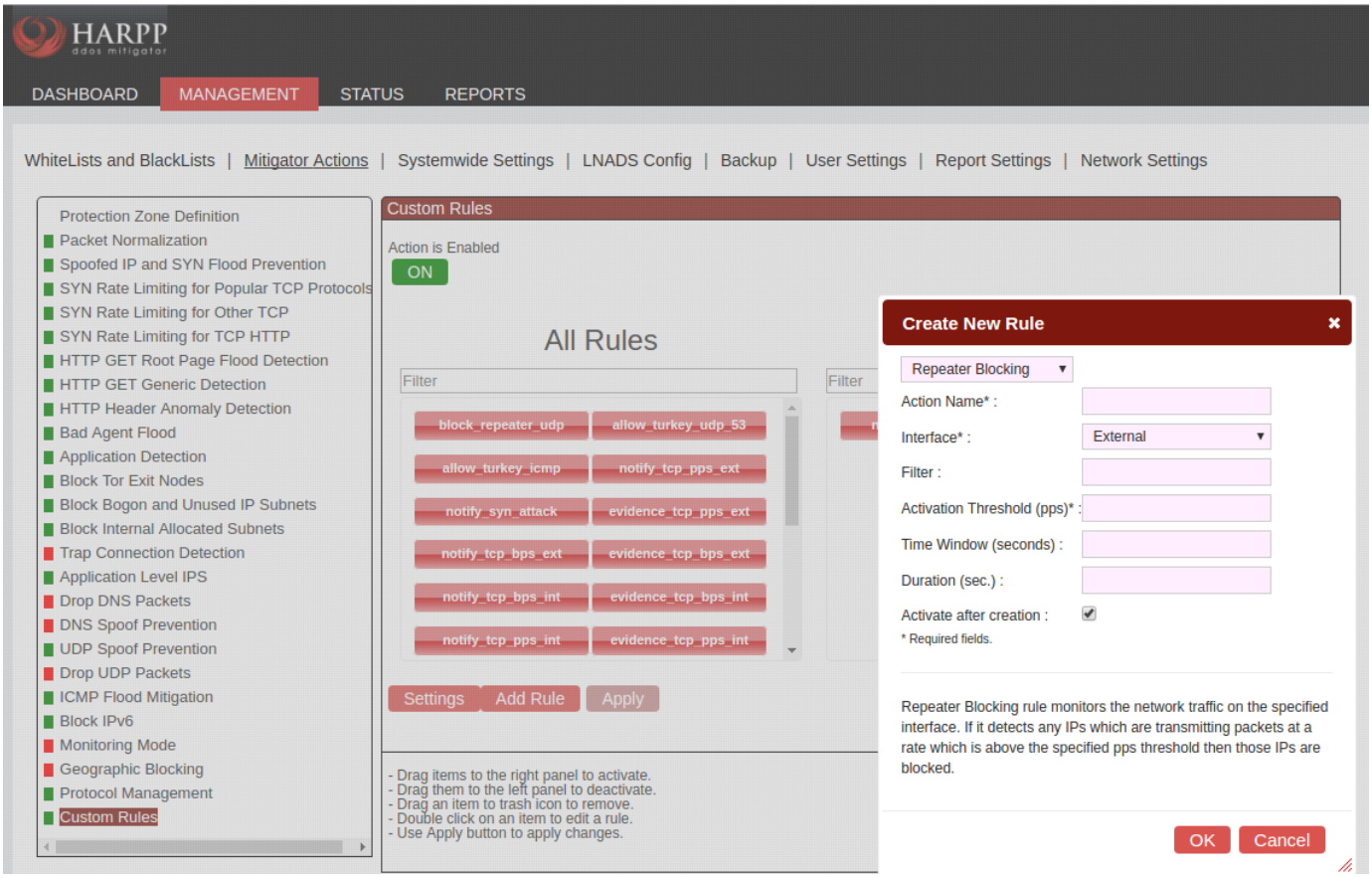
In these release, we have improved performance by enhancing inspection and evidence collection methods of all applications.

### 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.




---

## 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 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.