
# Administration Guide for HARPP DDoS Mitigator

Distributed Denial of Service Mitigation
Version 3.3.2-1

http://www.harppddos.com/contactus/
Tel: +90 850 455 4555

## Copyright



## Disclaimer

## Table of Contents

## About Labris Networks Inc.

Since 2002, Labris Networks Inc. has been an R&D focused and rapidly-growing provider of network security solutions through its globally-proven products. Labris ensures ultimate network security through its extensive product line including Firewall/VPN, Web Security, E-Mail Security, Lawful Interception and Availability Protection solutions on Labris UTM, Labris LOG and Harpp DDoS Mitigator appliances. Next-generation solutions are developed to detect, identify all kinds of real-time threats, applications providing a smart shield against intrusions, viruses, spam, malware and availability attacks.

Labris products protect networks of all sizes with a variety of topologies and deployment scenarios. Through Labris FLEX firmware options, the customers have privileges to get the security software they need as well as extra modules such as Wireless Guest Authentication, Detailed Internet Reporting, Lawful Interception and Logging. Having a customer-focused, future-oriented and flexible approach, Labris also offers its state-of-the-art security software as a Cloud Service.

Having operations in a rapidly growing global network of more than 20 countries, Labris products protect enterprises, brands, government entities, service providers and mission-critical infrastructures.

Labris with its worldwide partners is committed to the highest levels of customer satisfaction and loyalty, providing the best after-sales support by the multilingual Global Support Center. Being one of the Common Criteria EAL4+ certified security gateway brands in the world and rapidly growing global player, Labris provides its customers the top-level security with optimum cost. Labris, headquartered in Ankara, Turkey, has offices serving Europe, Middle East, North Africa, Caucasus and Southeast Asia.

## About HARPP DDOS Mitigator

Most business today depend on internet for Revenues, Customer access, Employee engagement and Every day business operations including voice over IP, email system. Without internet business quickly grains to halt. Today DDOS protection is a critical requirement in most of the organizations.

Harpp DDOS mitigator appliance is the first level of protection for your entire network against cyber attacks ensuring online business continuity. Harpp DDOS mitigator appliance provides best functionality in detecting and defeating the attacks completely. Harpp DDOS mitigator is purpose build for wide range of organizations including online money making operations, Critical public infrastructure, Enterprise networks, E-government operations and agencies.

Harpp DDOS mitigator is available for Small Enterprises, Medium Enterprises as well as Large Enterprises.

## How to Purchase DDoS Mitigator?

To purchase DDoS Mitigator, Visit - http://www.harppddos.com/contactus/

## Connecting Appliance

## Accessing the Web Admin Console

**Labris Default Management Port** = enp11s0f0/enp0s3/Port1/Net0/Mgt (first port to device)

**Labris Default IP Address**: 169.254.1.1

**Labris Default Username:** labris

**Labris Default Password**: labris

**Step-1:** Connect your computer to the first port on the Labris and then open computer's network settings section and assign IP address **169.254.1.2** and subnet **255.255.0.0**.

**Step-2:** Open your browser and browse https://169.254.1.1:8888(Here IP address is the IP address of your device) to access **Harpp DDoS** Web Console (GUI).

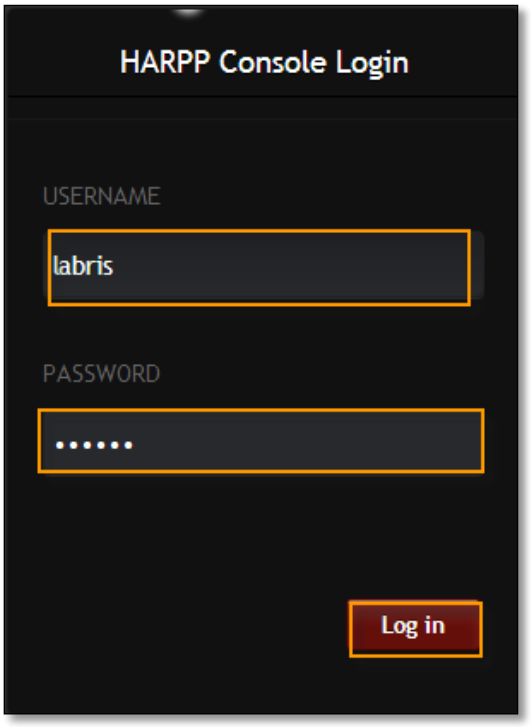
**Step-3:** Login page is displayed and you are prompted to enter login credentials. Use default **username** and **password** to log on.

## Login in to DDOS Mitigator

**DDOS – Distributed Denial of service**

Once you set DDOS Mitigator properly this is how you will login in to the Appliance.

It has a login screen.




These are the inputs for DDOS Login screen

| | | |
|---|---|---|
| 1 | **Username** | Type in your valid Default **username. This username is the one which you have given during the installation** |
| 2 | **Password** | Type in your valid Default **password. This password is the one which you have given during the installation. A good password is a mix of alphabets, numerical, special characters with a minimum length of 8** |
| 3 | **Log-in** | Click on **"Log-in"** button to enter into the appliance |

# 1. User Interface Settings

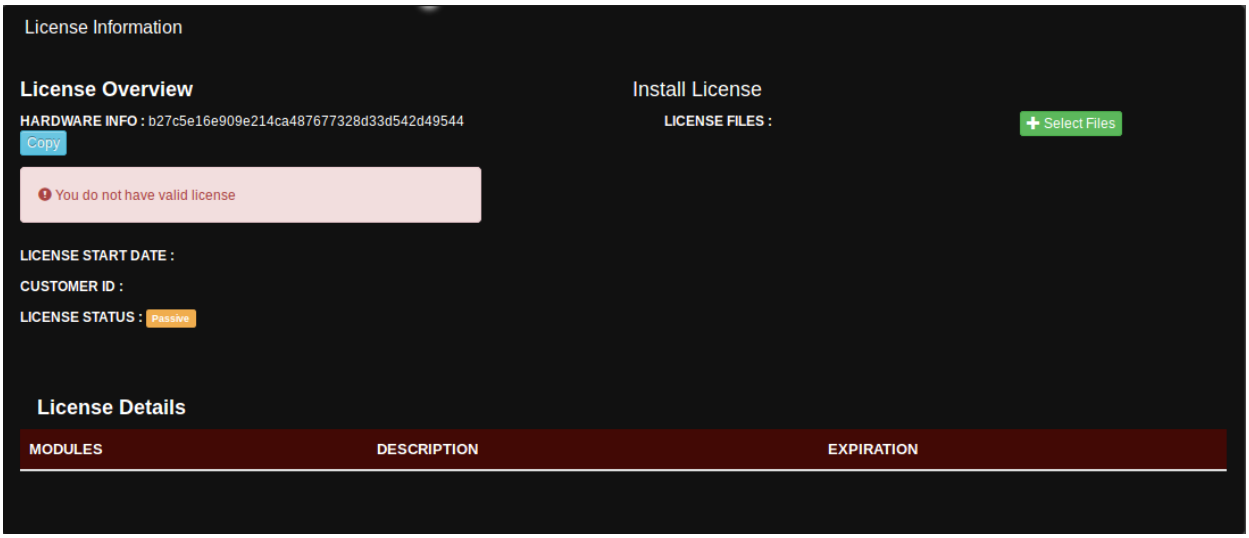
## 1.1 Accessing DDoS Mitigator

Once the default user name and password are provided for the first time, we will be automatically redirected to the licensing interface.

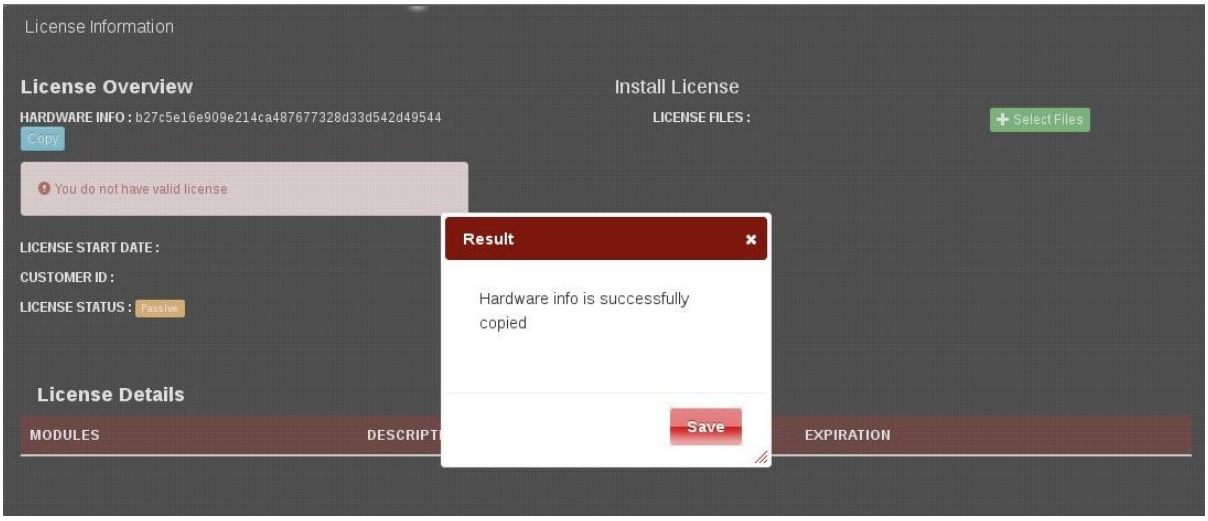
### 1.1.1 Harpp Licensing Interface

License interface is used to install license files which are provided by Labris Networks as specific for your device. As other usages of license interface; monitoring current license status, updating installed license can be aimed.

The first usage screen is as follows:

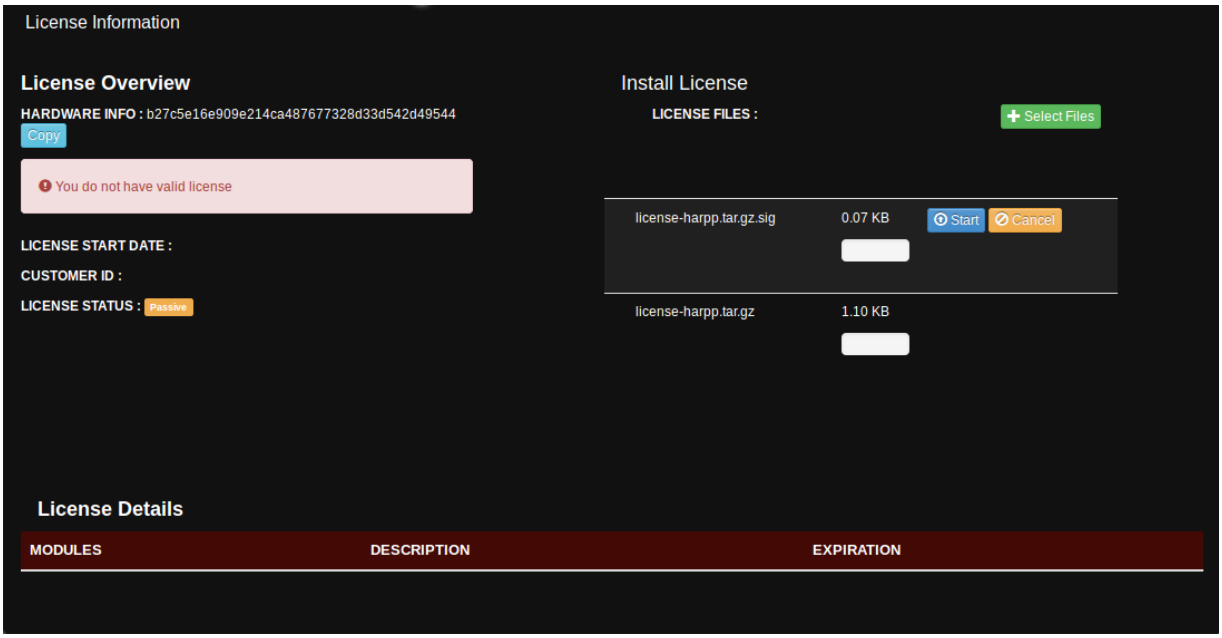



| | |
|---|---|
| **HARDWARE INFO** | Unique id number of the device |
| **LICENSE START DATE** | Start date of the license |
| **CUSTOMER ID** | Unique customer id |
| **LICENSE STATUS** | Current status of the license. The status can be "*Active*" or "*Passive*". |



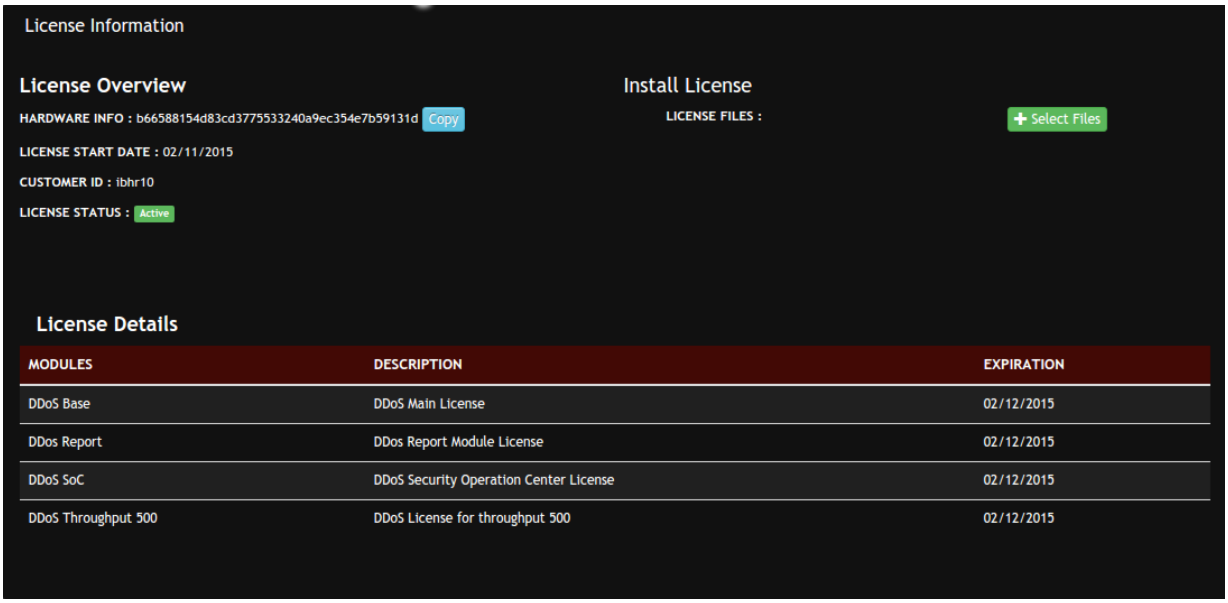

**Copy:** Copy hardware info to clipboard

**Select Files:** To select license files on opening file selector dialog box




**Start:** Apply the selected license files

**Cancel:** Cancel installing the selected license files

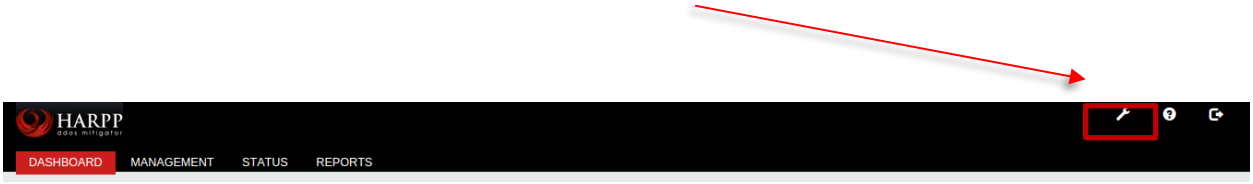



After license activation you should make settings by setup wizard. In setup wizard you can configure your HARPP device in six steps.

### 1.1.2 Harpp Setup Wizard

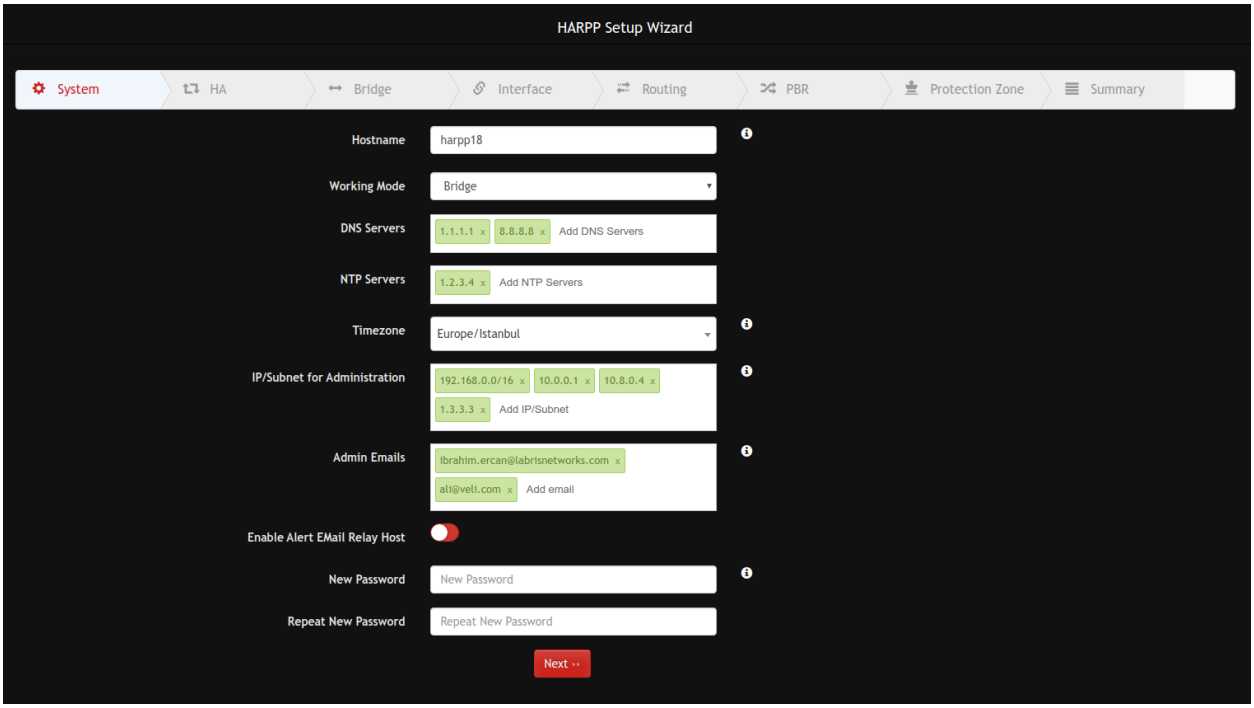
Installation wizard enables simple configuration of Harpp DDoS Mitigator products by users in just a few steps.

Installation wizard can be accessed via product's web interface. The wizard is fixed at the top right corner of the web interface.



### 1.1.2.1 Step 1: System

In this step we can configure basic system settings.




**Hostname:** Hostname of the device should be a fully qualified domain name.

**Working Mode:** You should choose whether device will be work as gateway (router) or bridge.

**DNS Servers**: DNS servers that will be used to resolve domains.

**NTP Servers**: NTP servers that will be used for time synchronization.

**Timezone:** Timezone of the device. Reports will also be shown according to this time zone.

**IP/Subnets for Administration**: Only these networks can reach HARPP after wizard configured. That's why please be sure you added your own IP address.

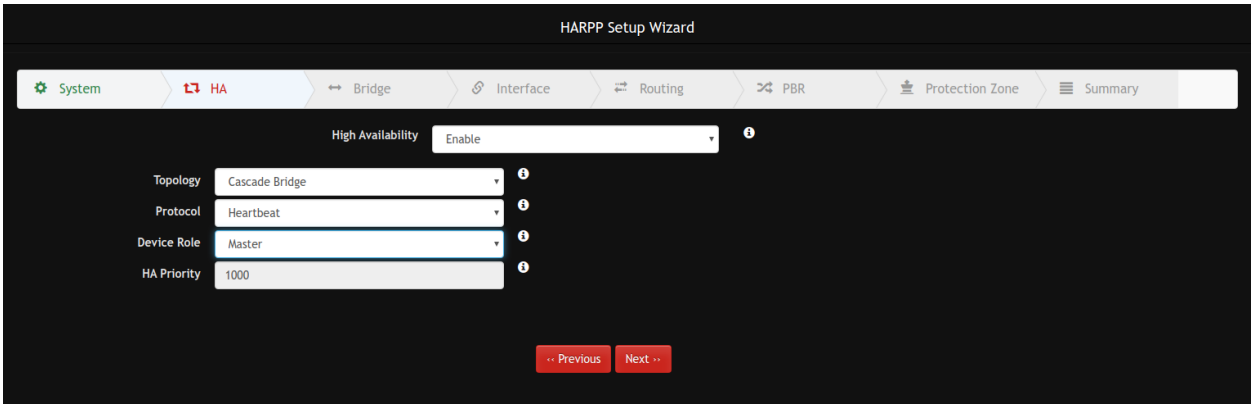
**Relay Host:** Alert and report emails will be send by using this host. Note that mail server should be configured accordingly.

**Relay Port:** This is the port that will be used to connect relay mail host.

**Password:** Password must contain 8 to 32 characters and at least one letter and one number.

### 1.1.2.2 Step 2: HA

If working mode set as Bridge, HA step will be activated.




**Topology:** This is the topology for HA configuration. Right now only cascade topology is supported.

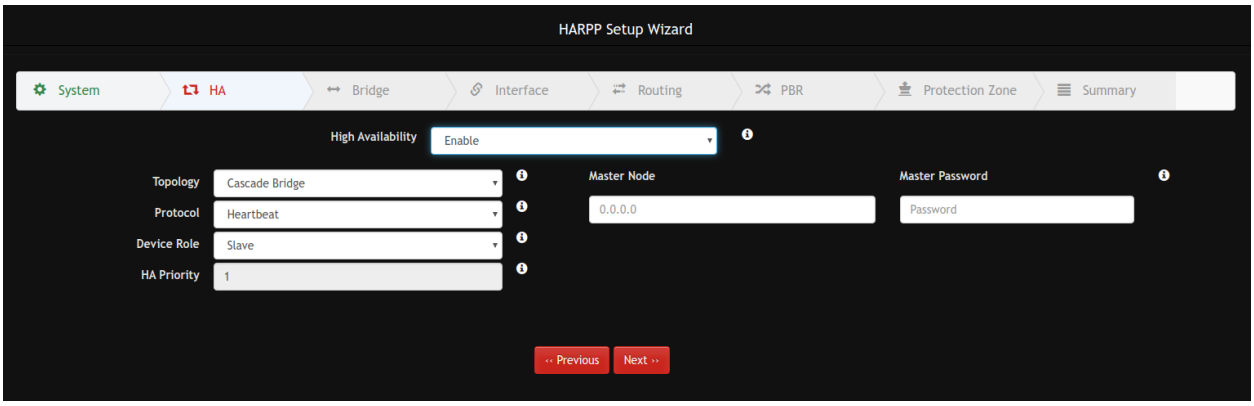
**Protocol:** Protocol that HARPP machines will communicate. Heartbeat is only supported protocol.

**Device Role:** Device role can be master or slave. Choose device role according to given network topology.

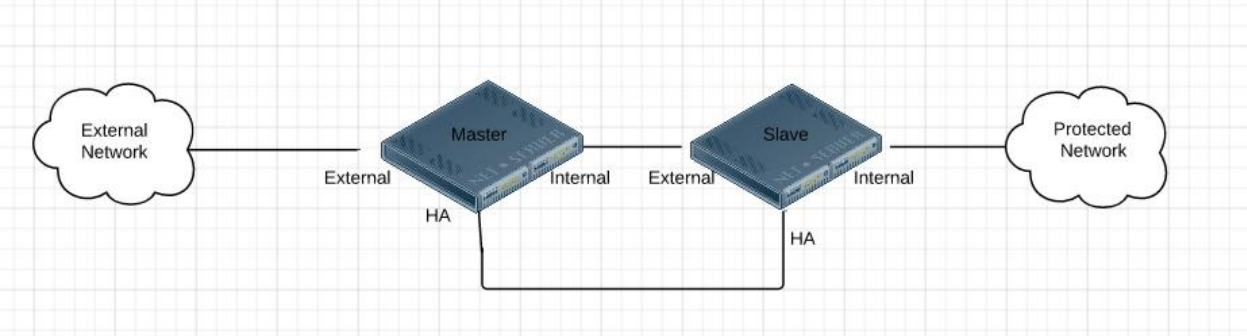
**HA Priority:** This is the priority of that node. For master it cannot be changed and it is 1000. For a slave node, it is in range 1-1000.

If a node is configured as a slave, we also need to provide IP address of HA interface of master node and root password and set priority a value between 1 and 1000.

After configuration done, complete wizard on master firstly. Master node will wait for slave to complete. Go to slave and complete wizard on slave also.

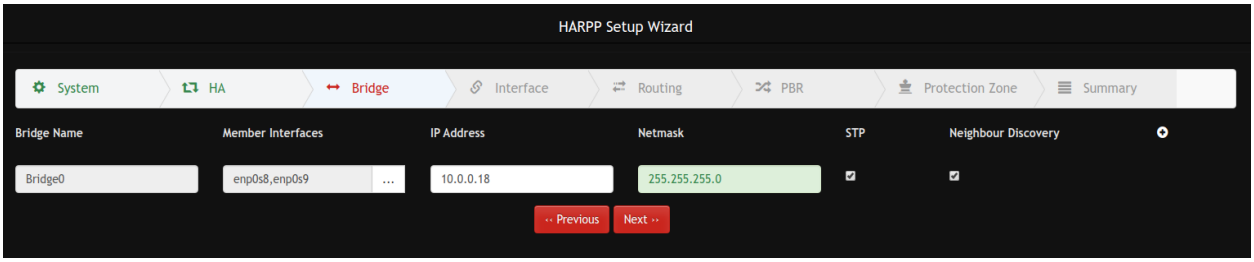


Below screen illustrates simple HA topology. If you enable HA you should also configure HA interface on Interface step.



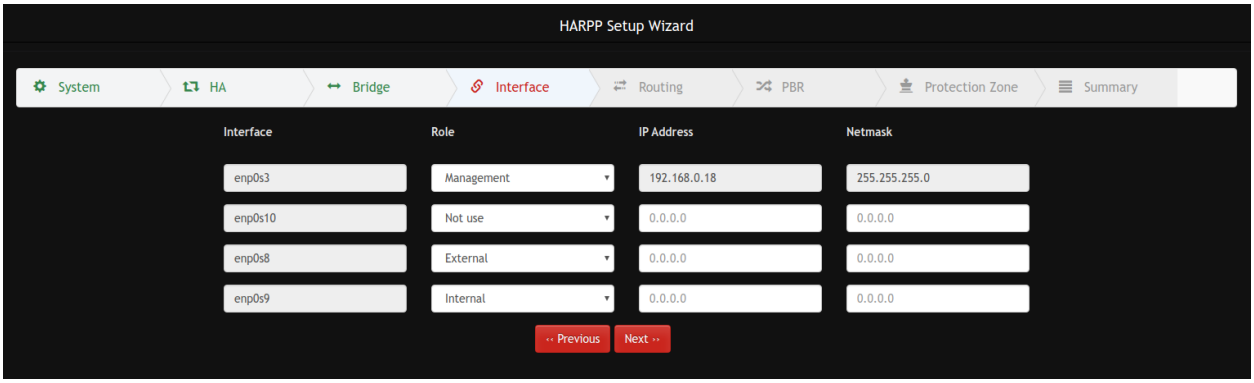

### 1.1.2.3 Step 3: Bridge

If working mode is set as Bridge, you should set bridge members and can assign IP address to bridges.



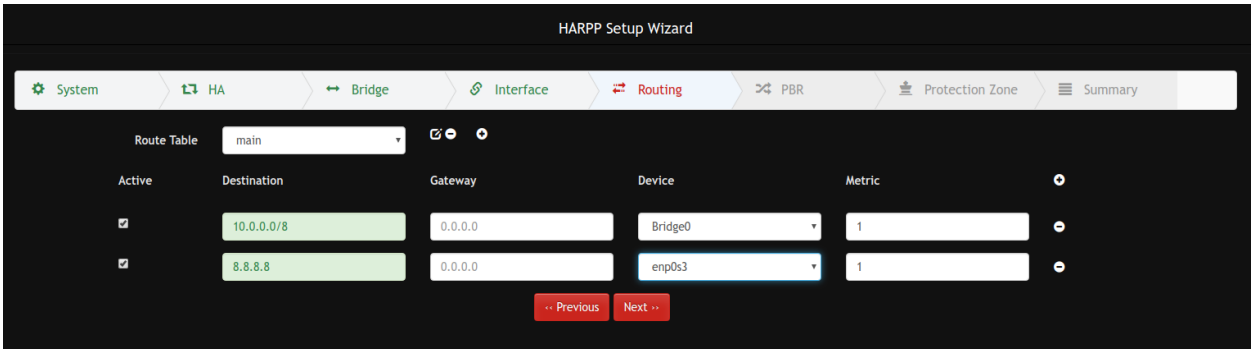

### 1.1.2.4 Step 4: Interface

In this step, we need to configure interface roles. IP addresses also should be configured if working mode is gateway.



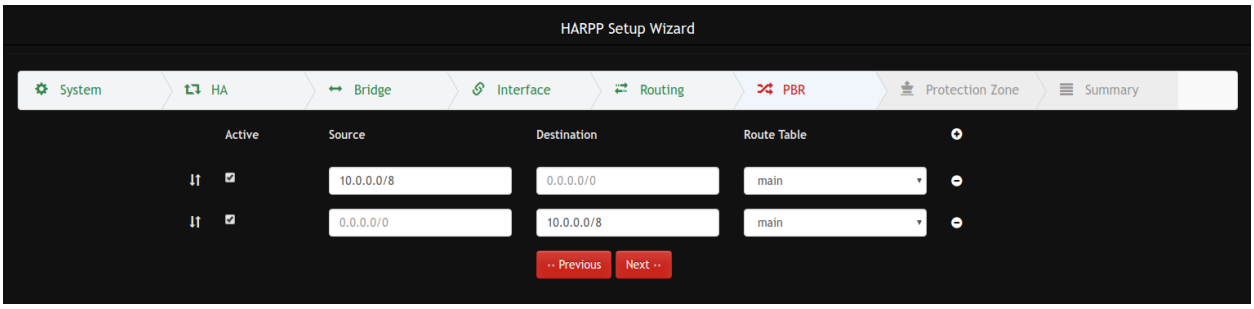
### 1.1.2.5 Step 5: Routing

In this step, we can configure routes and route tables. Most cases only main table should be enough.



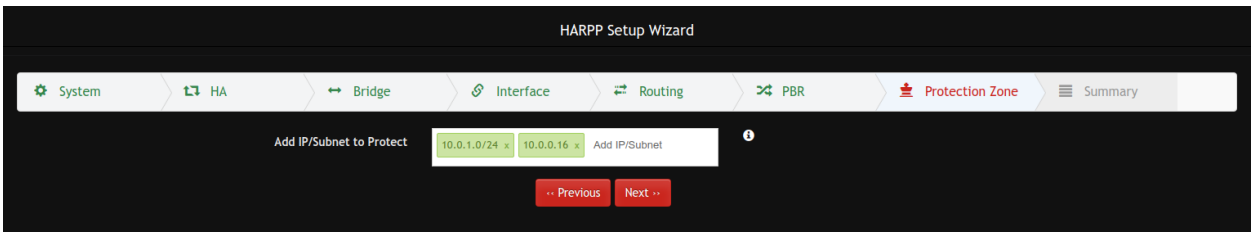

### 1.1.2.6 Step 6: PBR

In this step, we can configure policy based routing in case more than one route table configured.



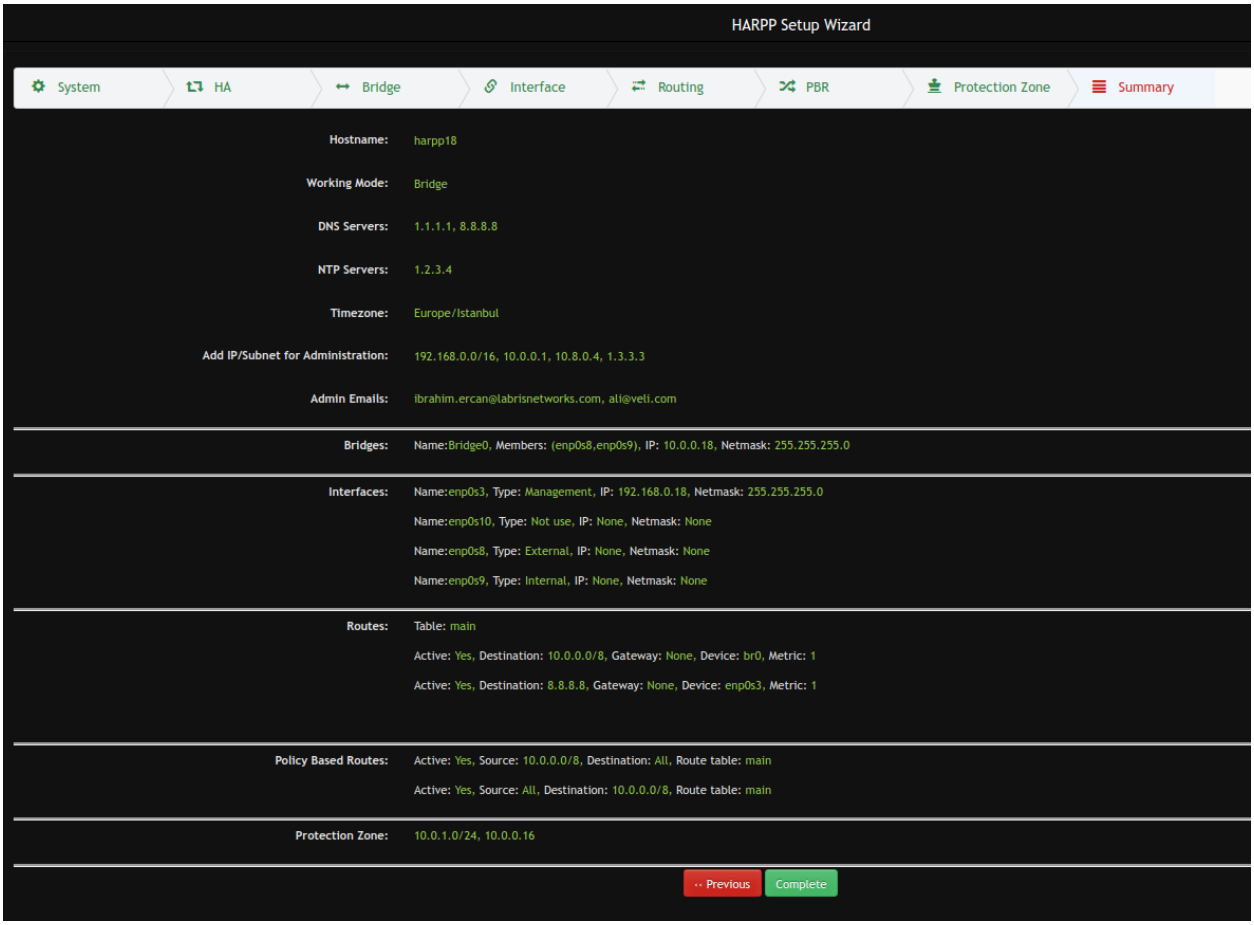

### 1.1.2.7 Step 7: Protection Zone

In this step we need to define network zones to be protected.



#### 1.1.2.8 Step 8: Summary and Completion

In this step, we can view changes and complete wizard.




### 1.1.3 Multiple Bridge

HARPP DDoS Mitigator supports multiple bridge and asymmetric traffics. With multiple bridge configuration, traffic will be divided into bridges so that performance of HARPP will increase.

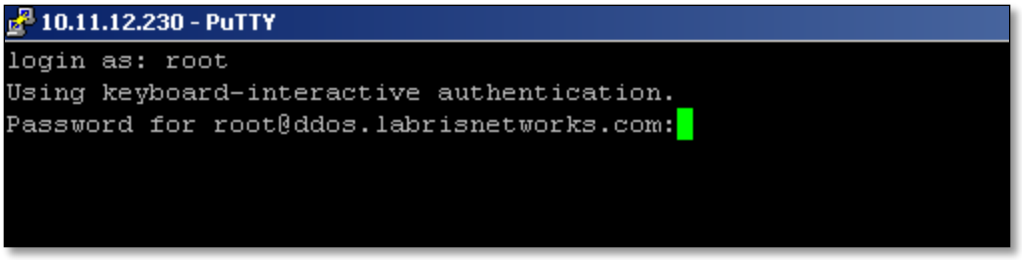
### 1.1.4 Command line Login Details using PuTTY

**Default Username**: root

**Default Password**: labris

**Port**: 22

Open Putty and give the default **username, password, Portnum** and click on **connect**.




**Edit/Add/Delete Interface, Default Route and Static Route**

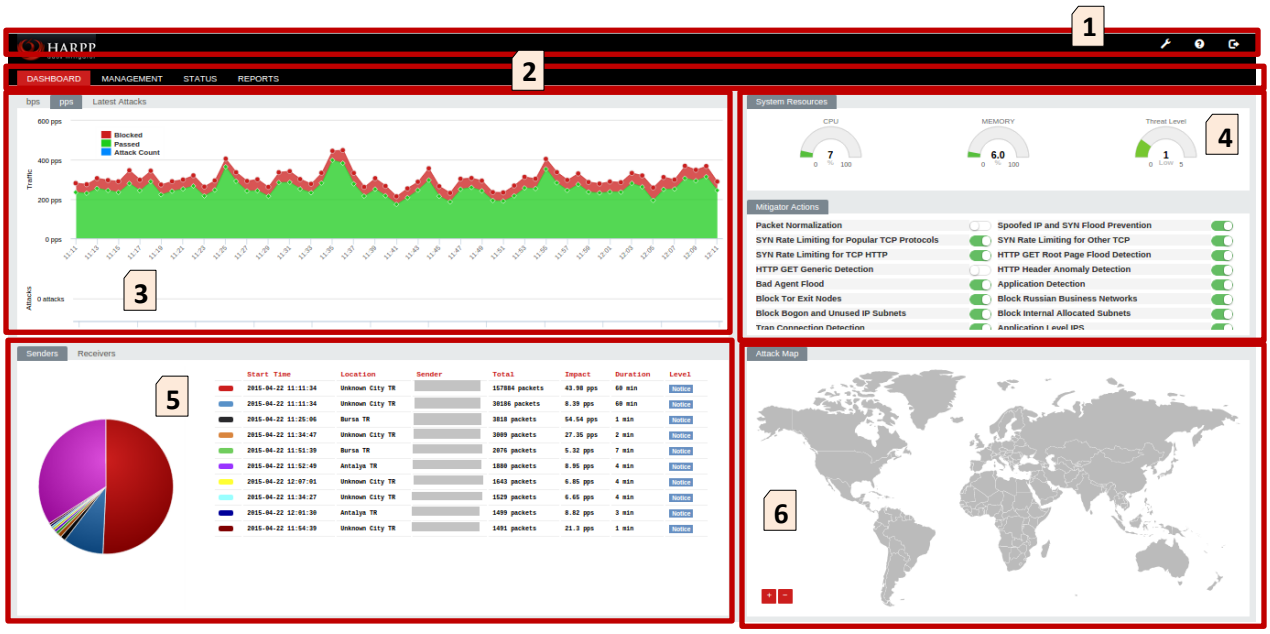
Interfaces to the ip is carried out via the CLI definitions. SSH login with root user and password by making a connection.

Interface and route information is kept in the **/etc/sysconfig/network-scripts/*** files.

## 1.2 General View of DDoS Mitigator Dashboard

### Understanding your landing page or home screen

In this section you will understand various sections of **Harpp DDoS Mitigator** home screen after the initial login.



| | | |
|---|---|---|
| 1 | **Page Header Section** | In this section, you will find links to **Wizard, Help** and **Logout**. Notice the right hand top corner for **Wizard, Help** and **Logout**. |
| 2 | **Tab Section** | You can navigate to various sections such as **Dashboard**, **Management**, **Status** and **Reports**. In addition to these you will also find option to Auto refresh. |
| 3 | **DDOS Cumulative attack, bps and pps graph** | DDOS cumulative field in the dashboard displays information on Attack, pps and bps ,drop and passed count in pictorial format for **every 10 mins, 1hour, last day** which makes us to understand easily. |
| 4 | **System Information and Mitigation Action** | System Information field in the dashboard displays information on the **CPU Usage, RAM Usage and Threat Level.** |
| 5 | **Packet Flow Information** | List of senders and receivers for the last 60 minutes. |
| 6 | **Attacks Map** | Attack map that displays the city and country information of the attackers. |

## 1.3 Management

Management tab in DDOS mitigator helps us to manage different things which are associated with it.

Management tab consists of seven sub fields as mentioned below.

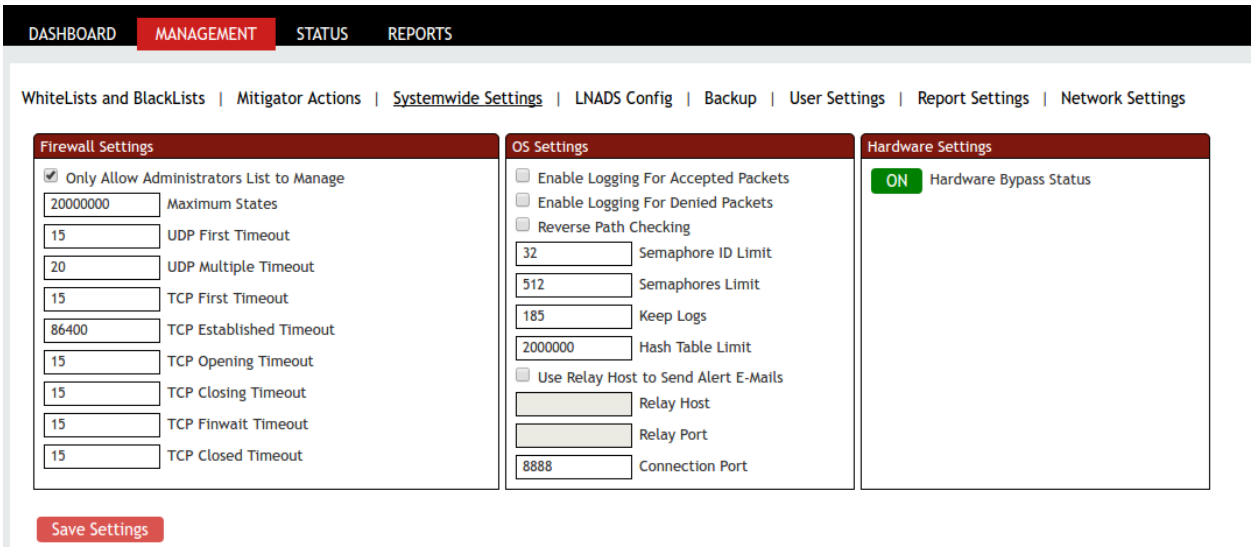
i) System Wide Settings
ii) White lists and Black lists
iii) Mitigator Actions
iv) Backup
v) LNADS Config
vi) User Settings
vii) Report Settings

### 1.3.1. System Settings (System wide Settings)

All the system related settings like operating system settings, ports numbers etc can be edited or changed with the help of system wide settings tab.

In the management section, select **Systemwide Settings** tab.

In Systemwide Settings we can find three types of settings **Firewall Settings**, **OS settings** and **Hardware Settings**

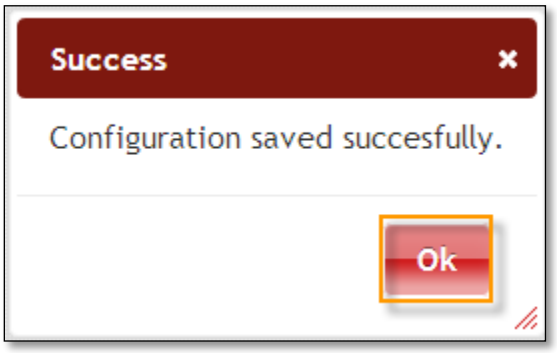



### 1.3.1.1 Firewall Settings

We can change the required fields with appropriate values and click on **Save Settings** tab to save the changes made to the Firewall Settings.

If Only Allow Admisnistrators List to Manage is checked, device will not accept any other connection but only connections from Administrator IP addresses defined in Whitelist and Blacklist section.

Success tab appears stating **Configuration saved successfully**, click **OK**




### 1.3.1.2 OS settings

On Os settings tab, we can change OS related settings.

After selecting the desired configuration, click on **Save Settings** tab to save the changes.

Table 1: System Settings

| Interface Name | Parameter | Information |
|---|---|---|
| **Maximum States** | set limit states | The system determines the maximum number of open connections. |
| **UDP First Timeout** | set timeout udp.first | When using the UDP protocol determines the timeout the request packet. |
| **UDP Multiple Timeout** | set timeout udp.multiple | When using the UDP protocol source determines the length of time to wait before the connection with the original author 's. |
| **TCP First Timeout** | set timeout tcp.first | TCP protocol when using the triple handshake that specifies the timeout for the second package during the process. |
| **TCP Established Timeout** | set timeout tcp.established | When using the TCP protocol specifies how much time will be with a link table. |
| **TCP Opening Timeout** | set timeout tcp.opening | When using the TCP protocol that specifies the timeout for future target computer package. |
| **TCP Closing Timeout** | set timeout tcp.closing | When using the TCP protocol that specifies the timeout of the connection close FIN packet. |
| **TCP Finwait Timeout** | set timeout tcp.finwait | When using the TCP protocol FIN/fin-ACK and the connection closed after a series of delayed that specifies the timeout for packets. |

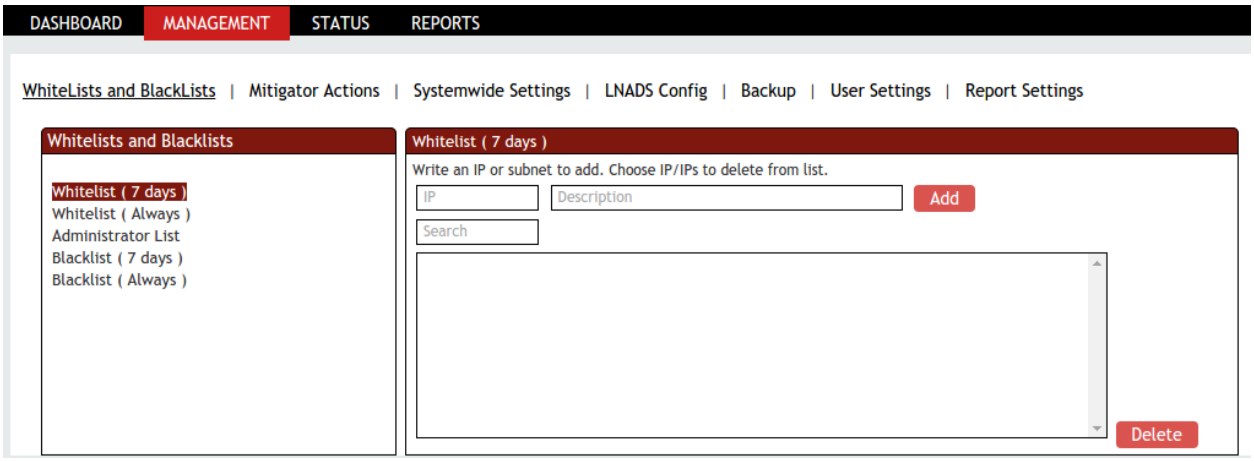
| | | |
|---|---|---|
| **TCP Closed Timeout** | set timeout tcp.closed | When using the RST packet is sent, the TCP protocol then specifies the timeout for future package. |
| **Only Allow Administrator List to Manage** | F2 number rule | F2 numbered rule active. This rule with the main interface or provided access to the ip addresses specified only as admin console. This list is created in the White and black lists.<br><br>**Warning!:** If you use ip address admin if you do not have access to the machine is not in the list will be cut off this option while the registration. To do this, first you need to add at your own address in the admin list. |
| **Enable Logging For Accepted Packets** | | When this control is checked, the accepted packets are logged. |
| **Enable Logging For Denied Packets** | | When this control is checked, the denied packets are logged. |
| **Reverse Path Checking** | rp_filter | When this control is checked, if the reply to a packet wouldn't go out the interface this packet came in, then this is a bogus packet and should be ignored. |
| **Semaphore ID Limit** | kern.ipc.semmni | Semafor id limit |
| **Semaphore Limit** | kern.ipc.semmni | Semafor limit |
| **Hash Table Limit** | | Rate limit working by hash algorithms. This is the limit of hash table that will be used for these mitigations. |
| **Connection Port** | | Webgui listening port on HARPP device. |

#### 1.3.1.3 Hardware settings

In this section we can enable/disable hardware bypass service. If the machine corrupts somehow such as power down, hardware bypass will be activated so that there will be no connection lost.

### 1.3.2. Whitelists and Blacklists

In the management section, select WhiteLists and BlackLists tab.

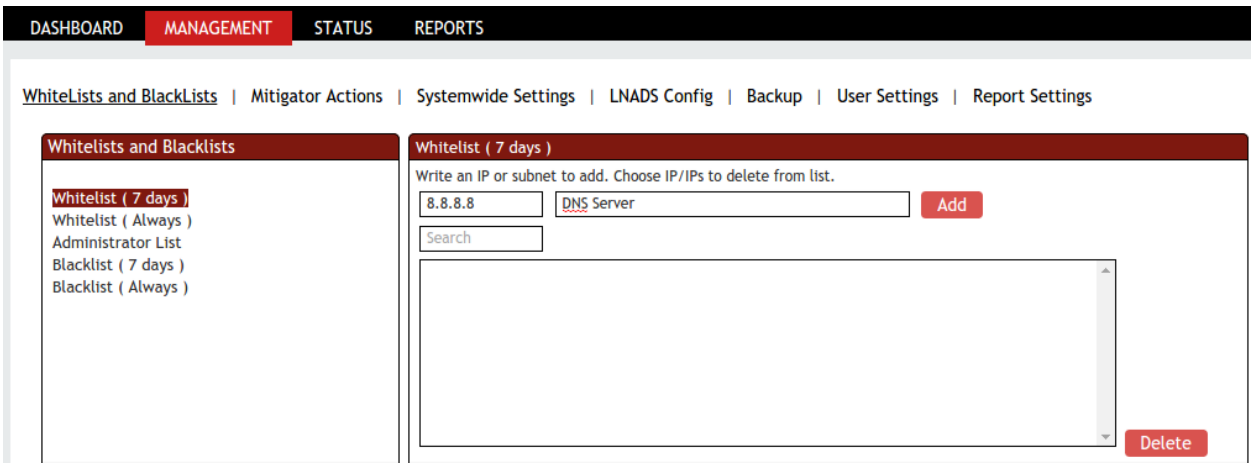



#### 1.3.2.1 Whitelist (7 days)

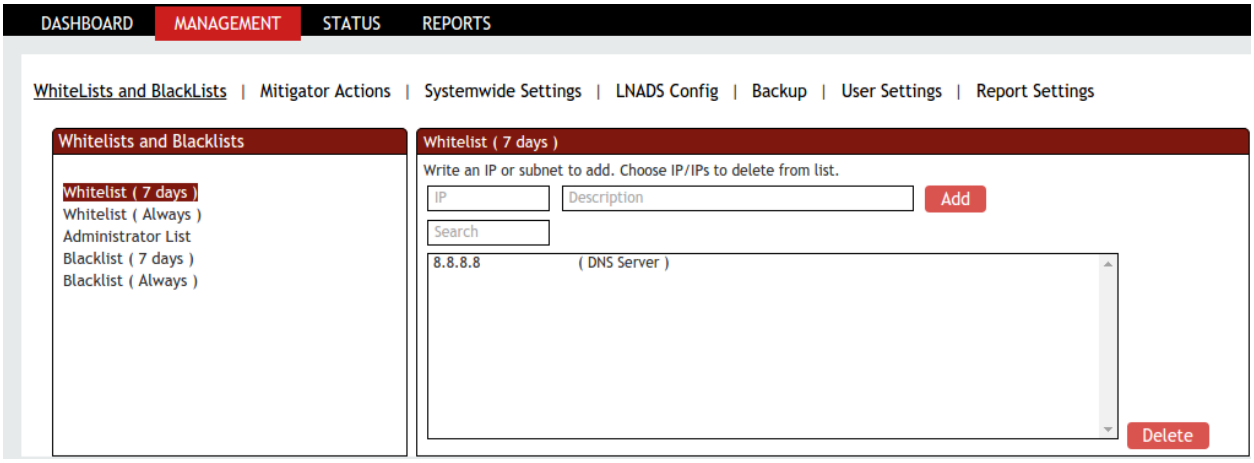
**Temporary white list**

All the IP Addresses added to the "Whitelist (7 days)" are allowed to have a limited access to resources. The IP addresses which are added to this list are not blocked completely. All the required / known IP addresses can be added to the "Whitelist (7 days)".

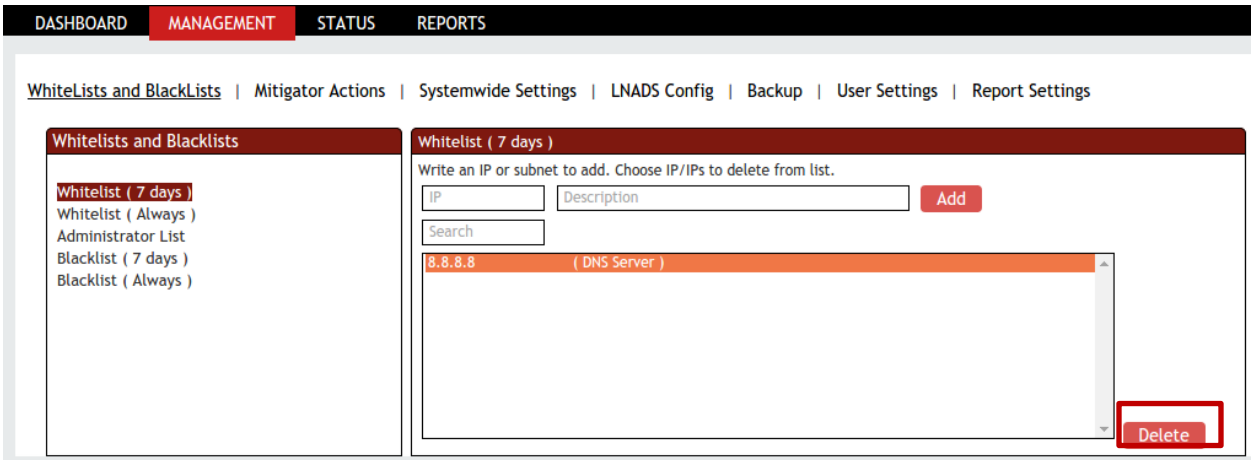
In "Whitelist (7 days)" section give the **IP Address** and **description** which we wanted to add to this list and click on **ADD** tab.



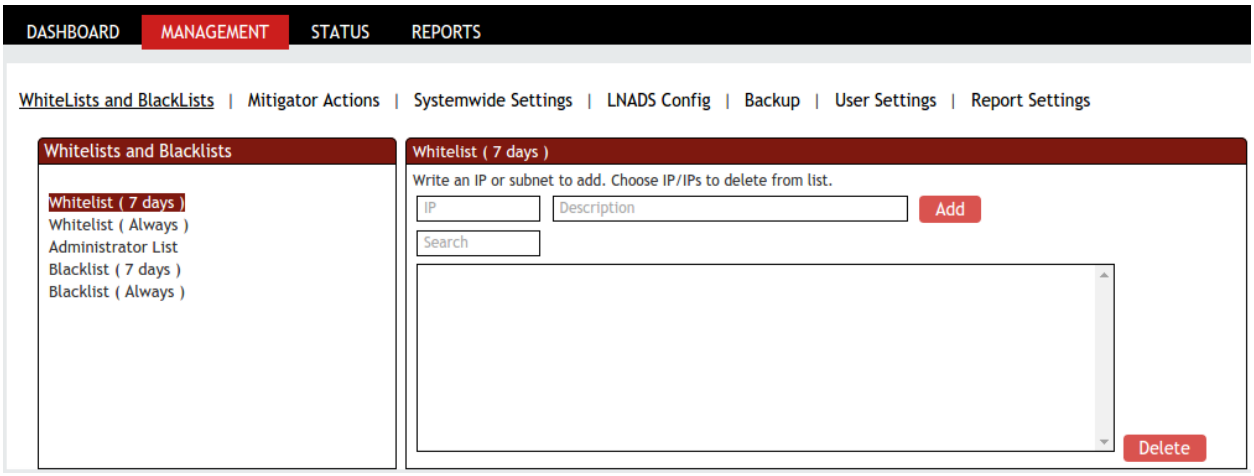
In the below screen, we can notice that IP Address is added to Systemwide Whitelist. **Search** box can be used to filter added IP addresses.




Select the IP Address and click on **Delete** tab to delete it from this list.




In the below screen, we can notice selected IP Address is **deleted** from the Systemwide Whitelist.

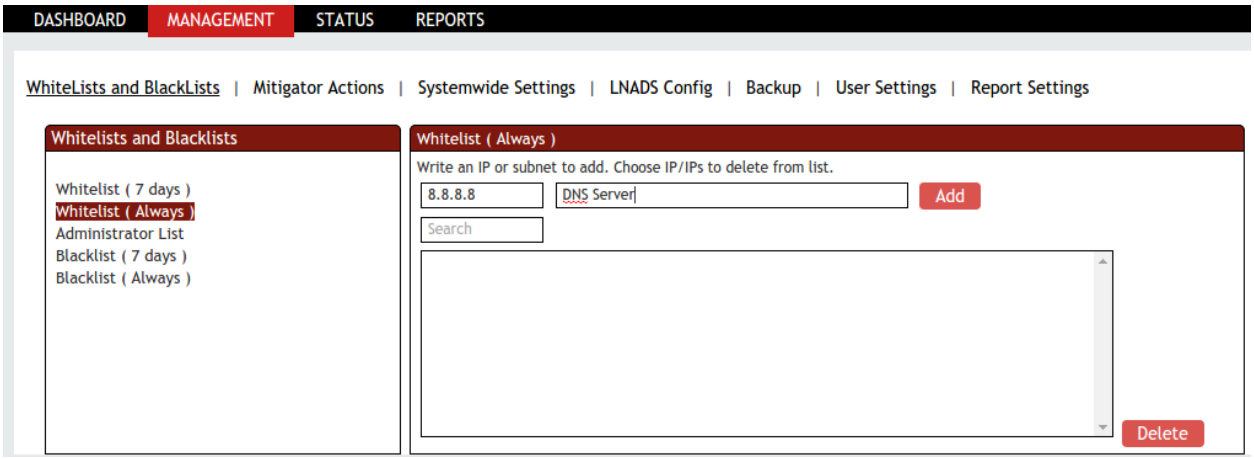



### 1.3.2.2 Whitelist (Always)

**Permanent White list**

All the IP Addresses added to the "Whitelist (Always)" list will have limited access to resources. The IP's added to this list are not blocked completely. "Whitelist (Always)" is like long term Whitelist.

In "Whitelist (Always)" section give the **IP Address** and **description** which we want to add to this list and click on **Add** tab.

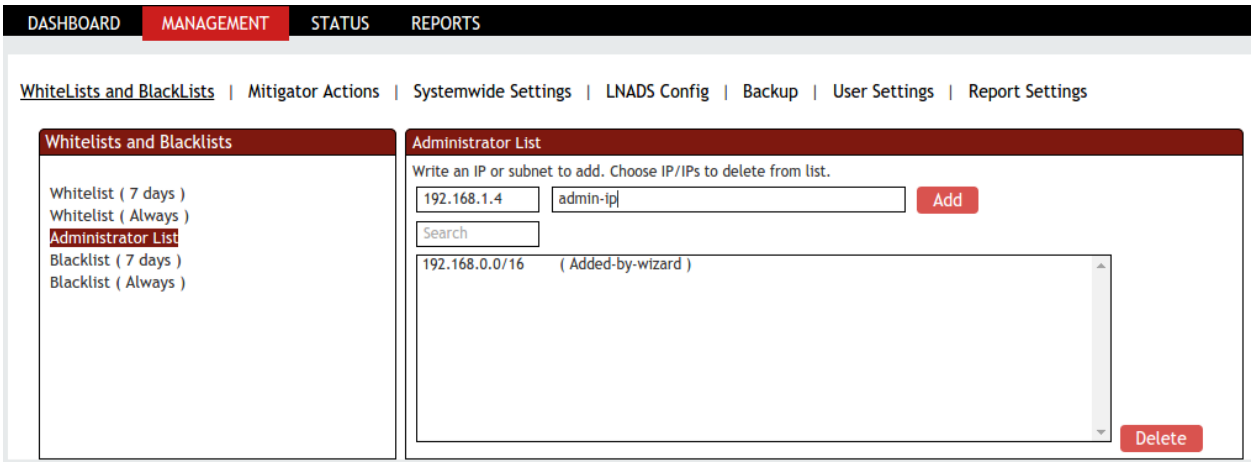



### 1.3.2.3 Administrator List

IP Addresses added to this list will have access to the resources. The entire administrator's IP Addresses can be added to the administrator's list.

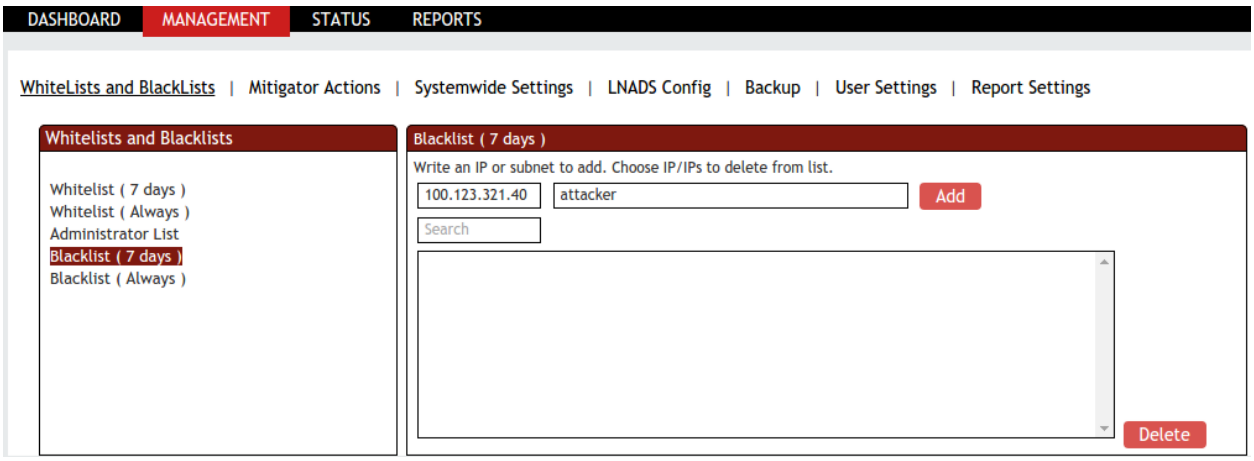
In Administrator list section give the **IP Address** and **description** which we wanted to add to this list and click on **Add** tab.

On this tab, the following illustration shows the IP addresses contained in the website.




### 1.3.2.4 Blacklist (7 days)

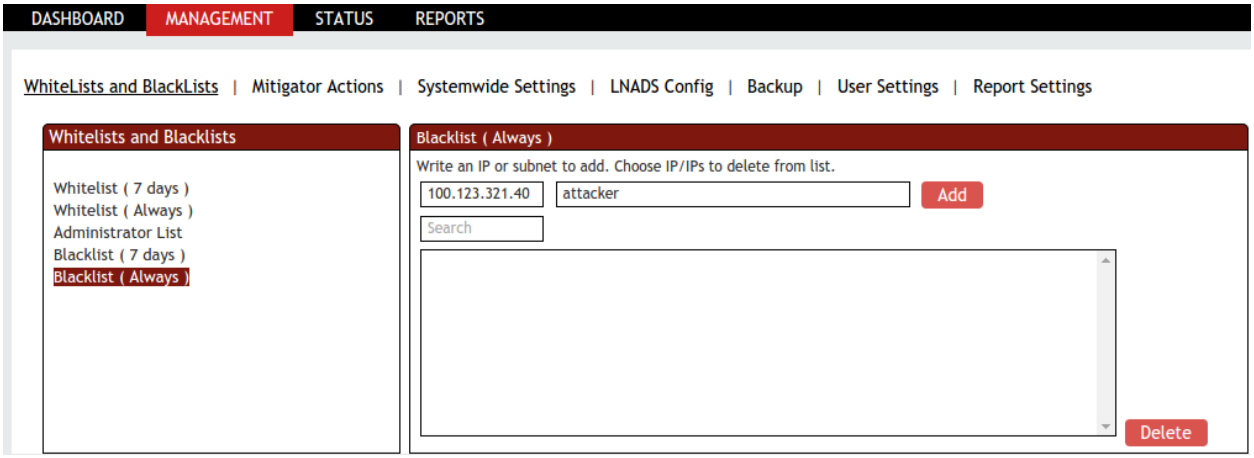
IP Addresses added to the "Blacklist (7 days)" are restricted to access the resources. All these IP Addresses specified in this list are blocked. All the attackers or intruder's IP Addresses can be added to the "Blacklist (7 days)".




### 1.3.2.5 Blacklist (Always)

IP Addresses added to the "Blacklist (Always)" are restricted to access the resources for lifetime. All these IP Addresses specified in this list are blocked. All the attackers or intruder's IP Addresses can be added to the "Blacklist (Always)".

In "Blacklist (Always)" section give the **IP Address** and **description** which we wanted to add to this list and click on **Add** tab.




### 1.3.3. Prevention Methods (Mitigator Actions)

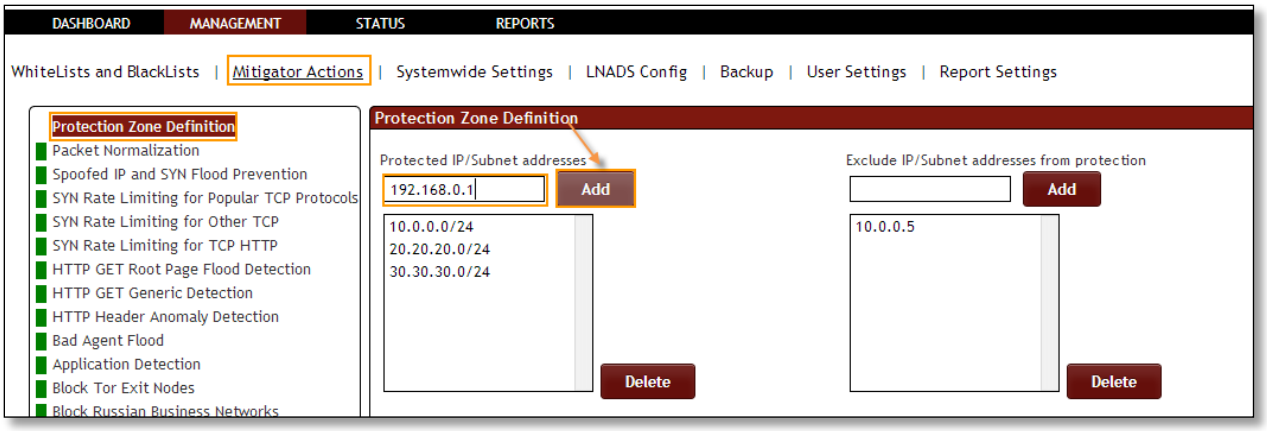
In the mitigator actions tab we can change all the firewall rules which are defined into active / passive mode.

Red color indicates – **OFF**
Green color indicates –**ON**

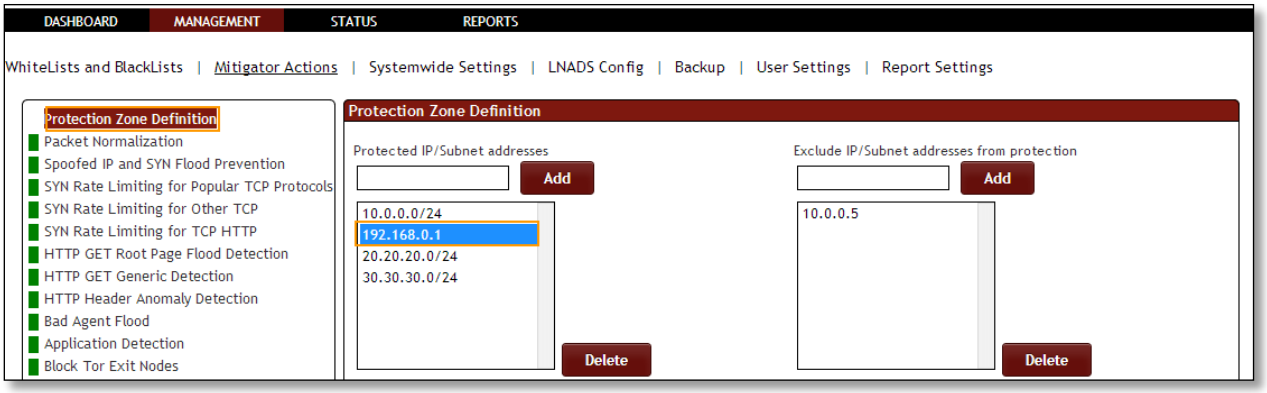
#### 1.3.3.1 Protection Zone Definition

List of IP/ subnet provided under protection zone definition is used to protect IP /subnets within the network. All IP addresses that you want to protect in your network should be defined under this tab.

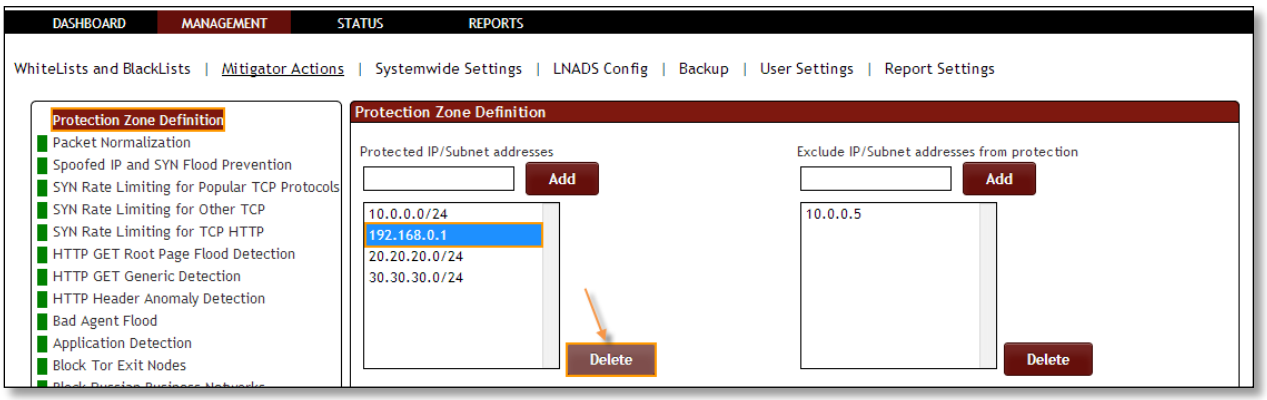
Protection Zone Definition helps to protect all the IP Addresses which are in our network. The IP Addresses which are important / critical for your business environment can be added to this list.
Give the IP subnet to the IPs of Zone field and click on **Add** tab.



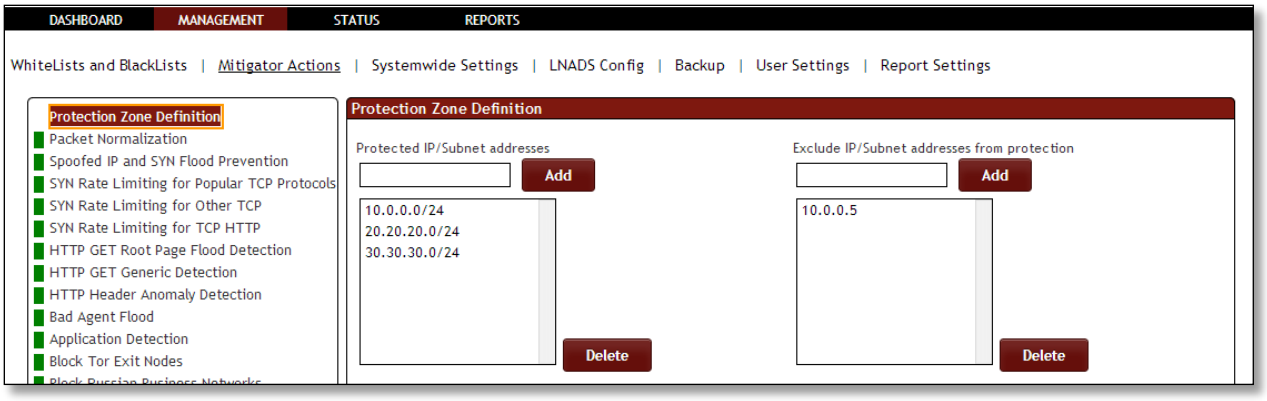

We can notice IP Sub net added in the list of Protection Zone.



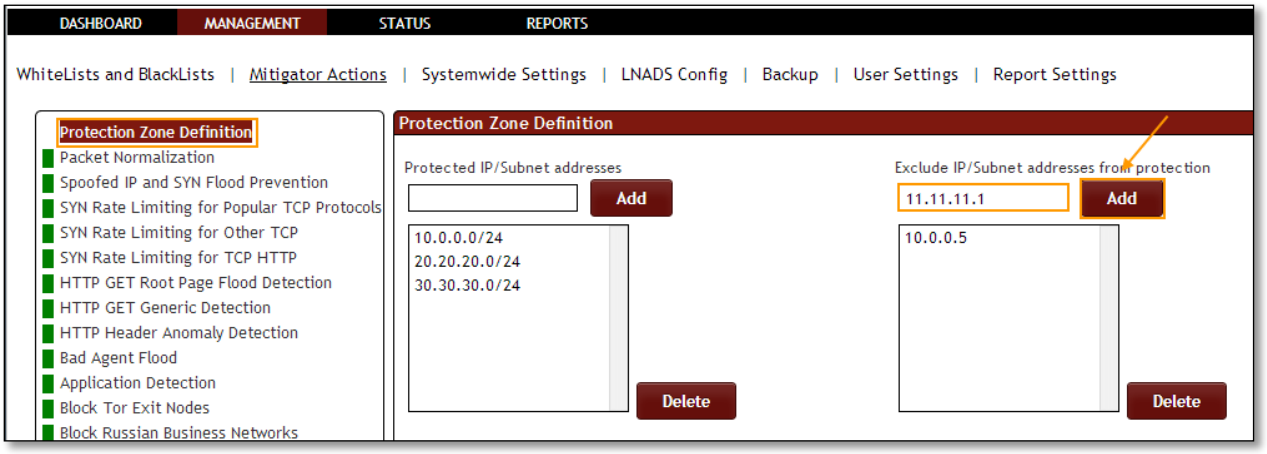

Select the IP Subnet and click on **Delete** tab.



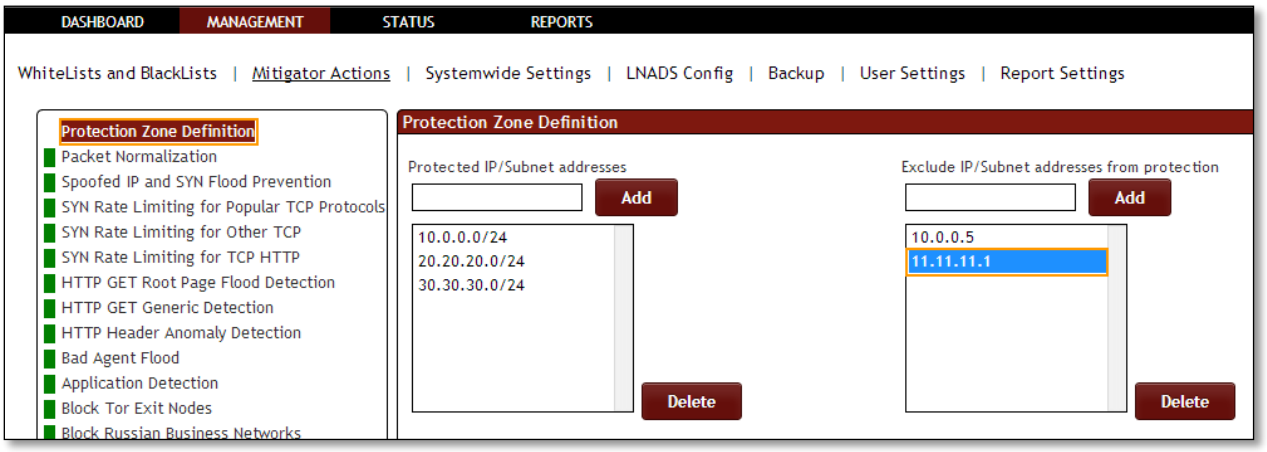

In the below screen, we can notice of IP Subnet is deleted from the list Protected Zone.



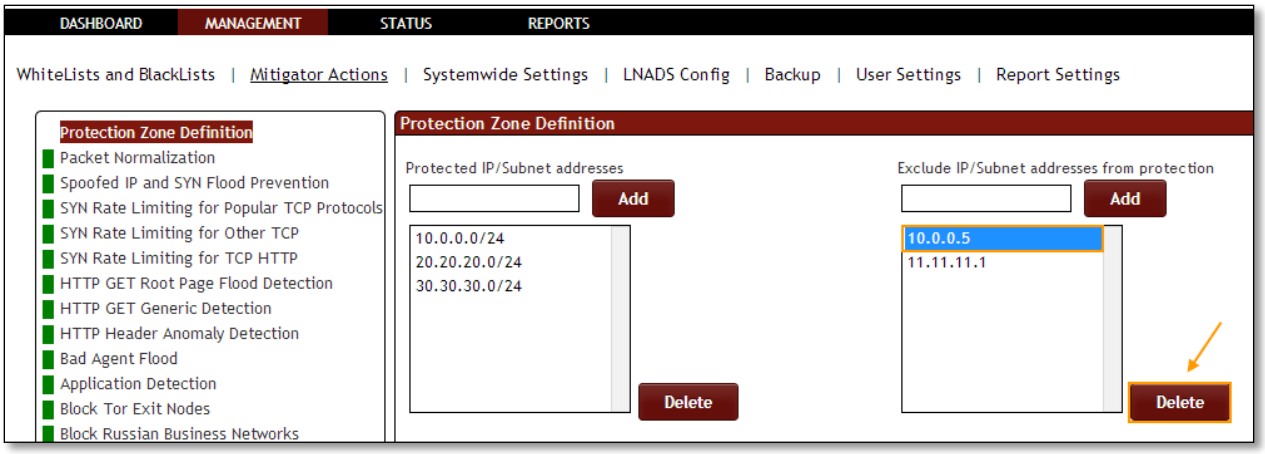

To Exclude IP / Subnet addresses from protection Zone, give the IP/Subnet in specific tab as click on **Add** tab.



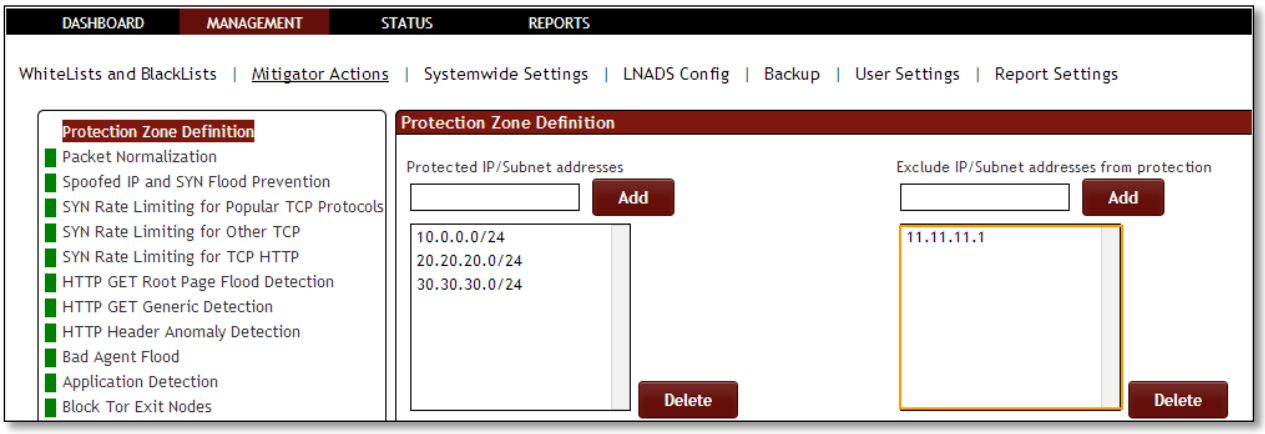

In the below screen we can notice IP/Subnet added to the List of Excluding IP/Subnet addresses from protection.




To delete IP/Subnet from the list, select the **IP/Subnet** and click on **Delete** tab.




In the below screen, we can notice IP/Subnet deleted from the list.

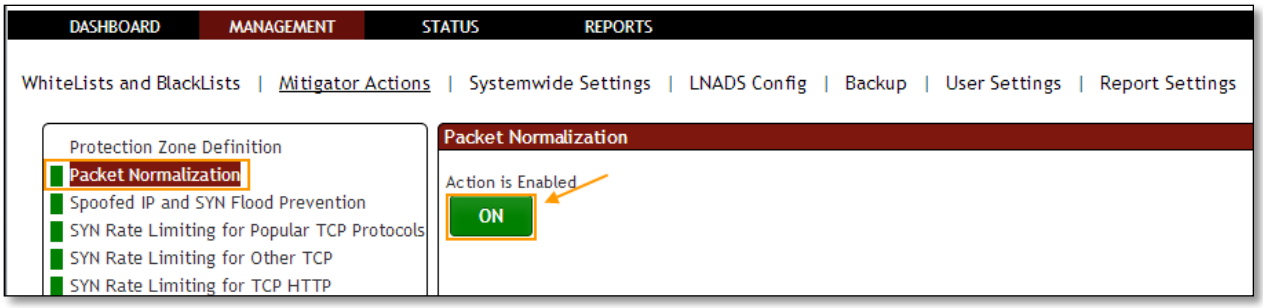



### 1.3.3.2 Packet Normalization

**Rule F3:** Packet Normalization active/passive.

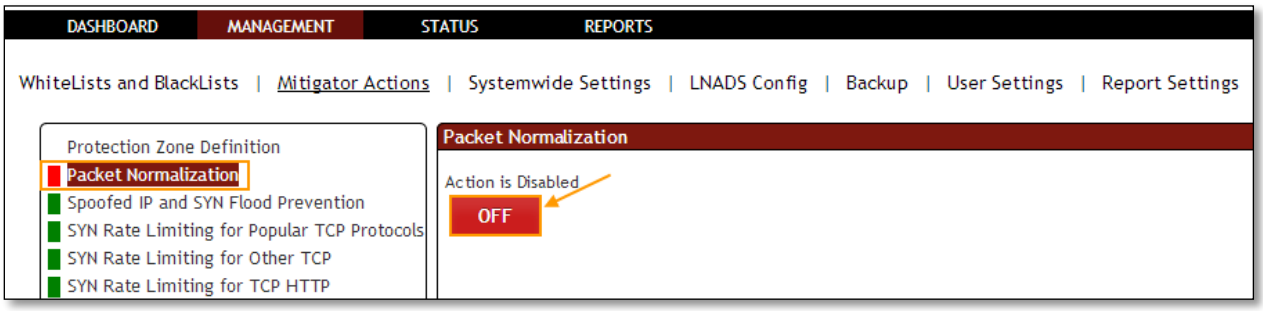
In Packet Normalization tab we have an option to **Enable / Disable the option**.

We can notice Packet Normalization Action is enabled, it is in **ON** state.




Click on the same action tab to **disable the option**.

Packet Normalization Action is Disabled, it is in **OFF** state.

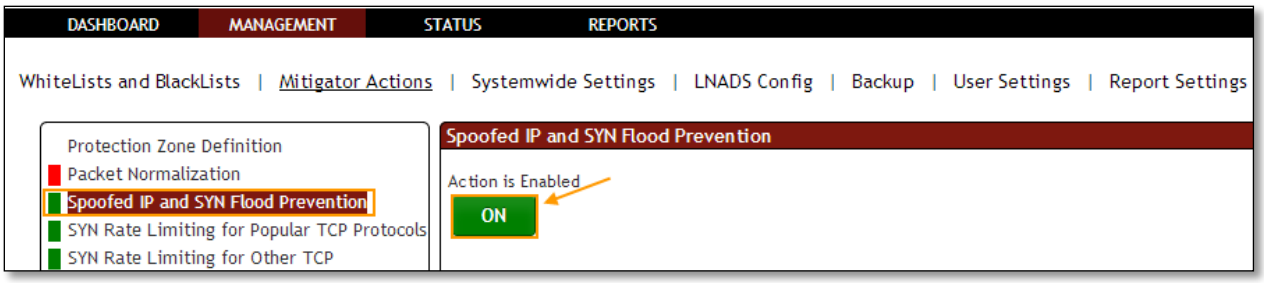



### 1.3.3.3 Spoofed IP and SYN Flood Prevention

**Rule F25:** SYN proxy Active/Passive

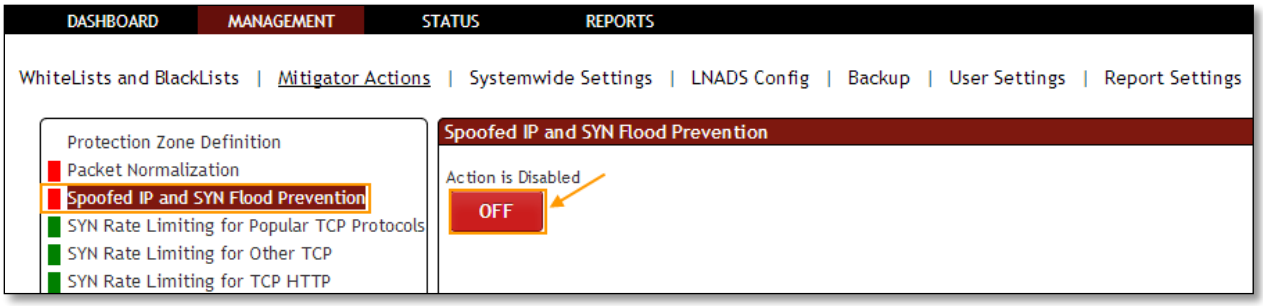
In **Spoofed IP and SYN Flood Prevention** tab we have an option to **Enable / Disable the option**.

Spoofed IP and SYN Flood Prevention Action is **Enabled**, it is in **ON** state.




Click on the same action tab to **disable the option**.

Spoofed IP and SYN Flood Prevention Action is **Disabled**, it is in **OFF** state.




### 1.3.3.4 SYN Rate Limiting for popular TCP protocols

**Rule F35:** SYN package speed limitation is active/passive. This is a list of the port you want the block period to apply, you can change the maximum number of connections the speed ratio, and through the interface.

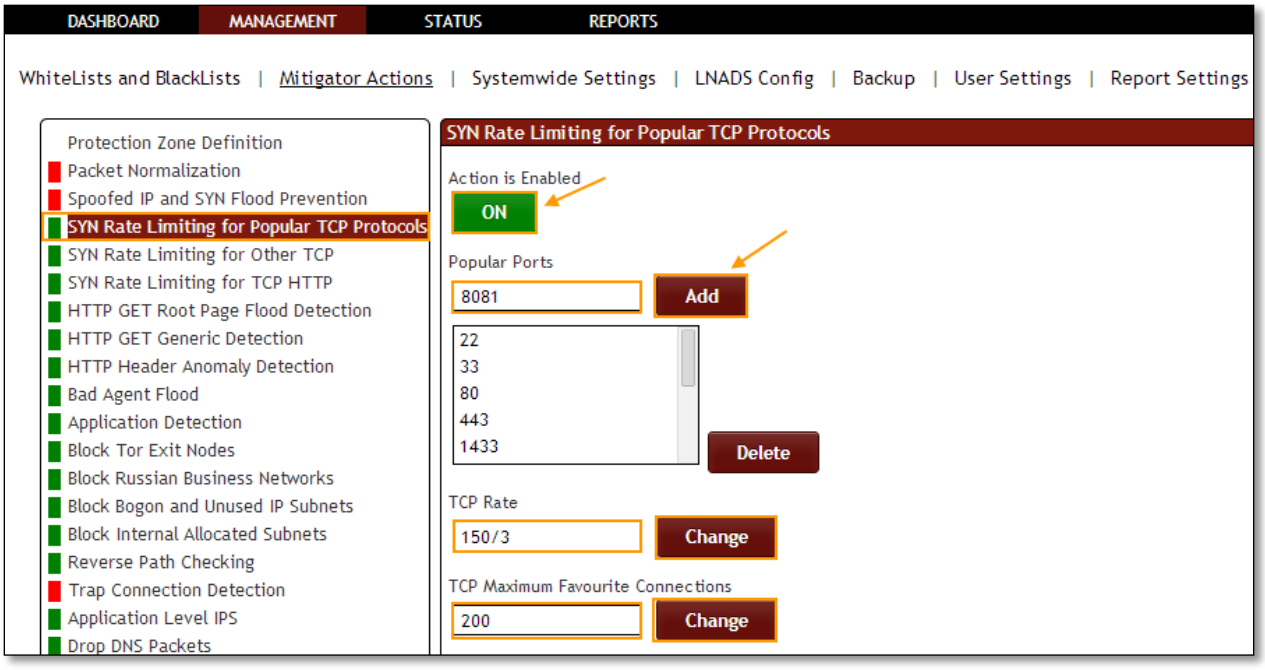
In **SYN Rate Limiting for popular TCP protocols** tab we have an option to **Enable / Disable the option**.

Other options in **SYN Rate Limiting for popular TCP protocols**, we can add the popular port number so that restrictions are applied to the port list.

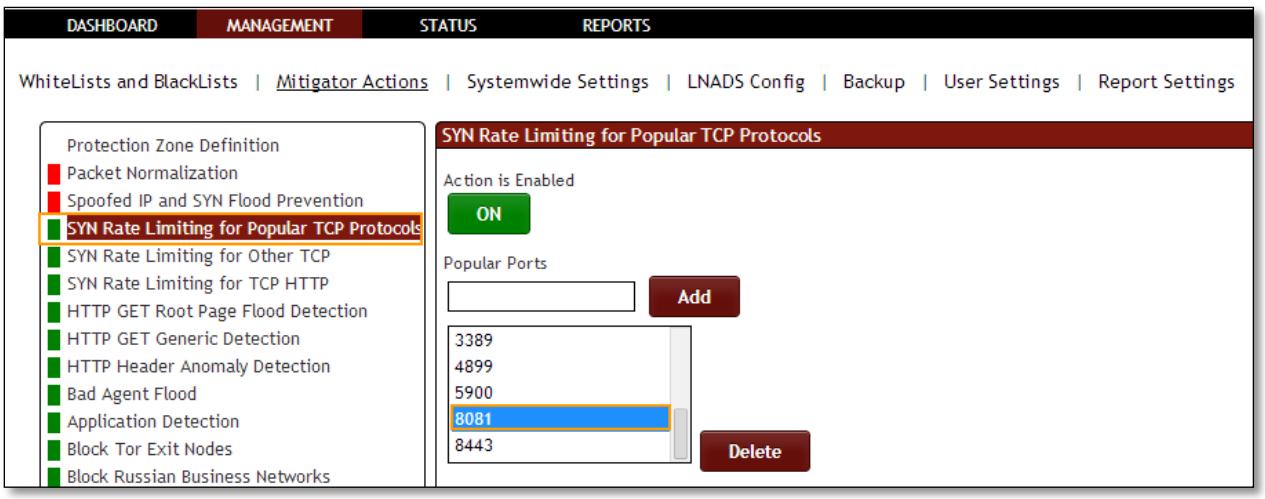
Using TCP rate tab we can change the speed ratio and also the number of connections can be changed using TCP Maximum Favorite Connections.

SYN Rate Limiting for Popular TCP Protocols Action is enabled, it is in ON state.

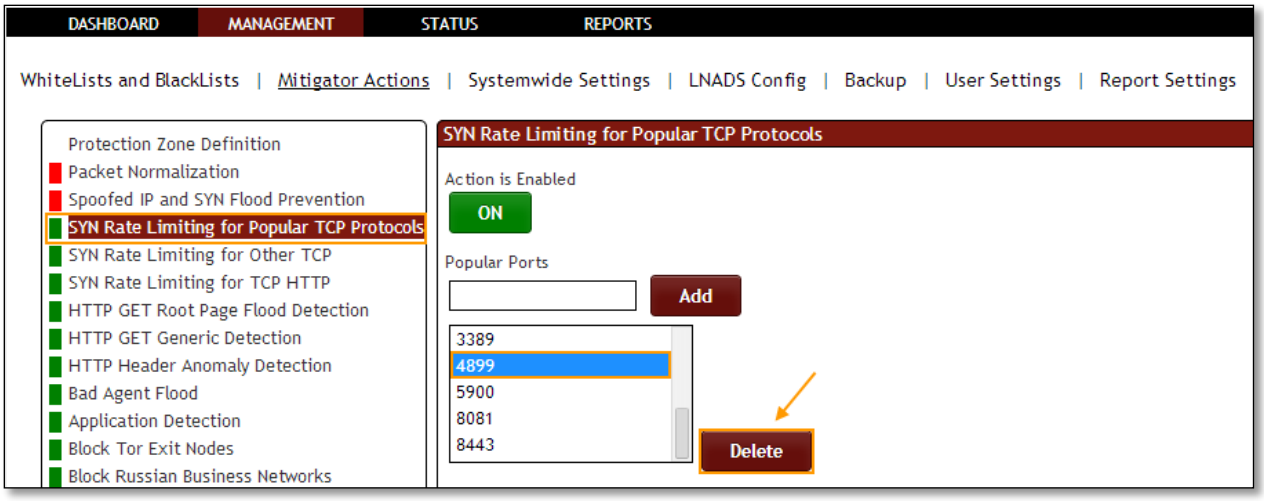
Mention popular port number and click on **Add** tab. There are other options like **TCP Rate** and **TCP Maximum Favorite Connections** options. Click on **Change** to apply the changes.




In the below screen we can notice popular port number added.



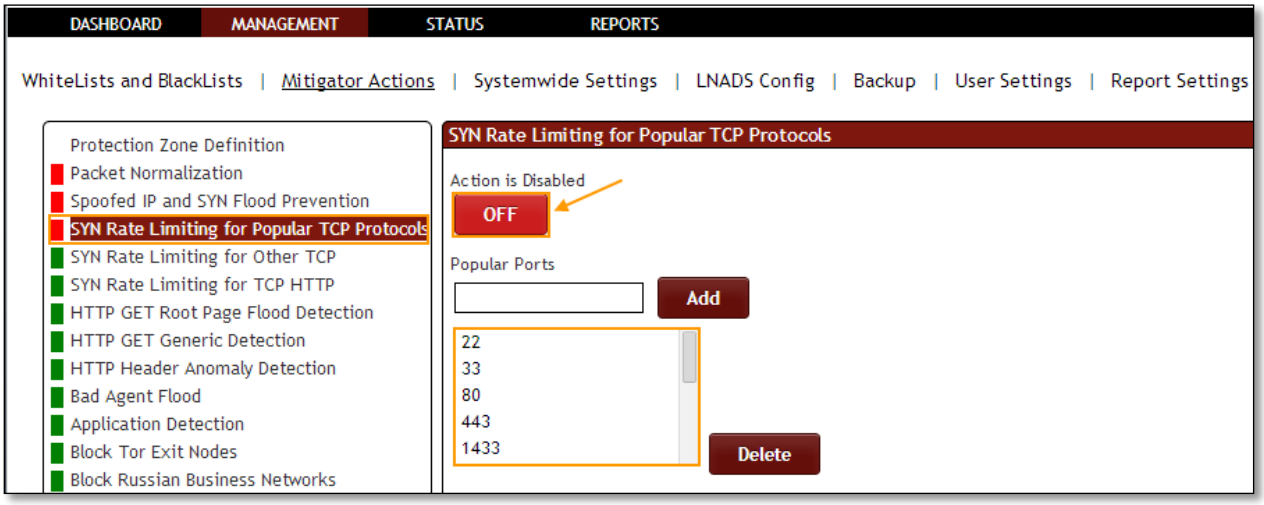

Select the Port and click on **Delete** tab to delete popular port.




Click on the same action tab to **disable the option**.

SYN Rate Limiting for Popular TCP Protocols Action is disabled, it is in OFF state.

We can notice selected port number got deleted in the list of popular ports.

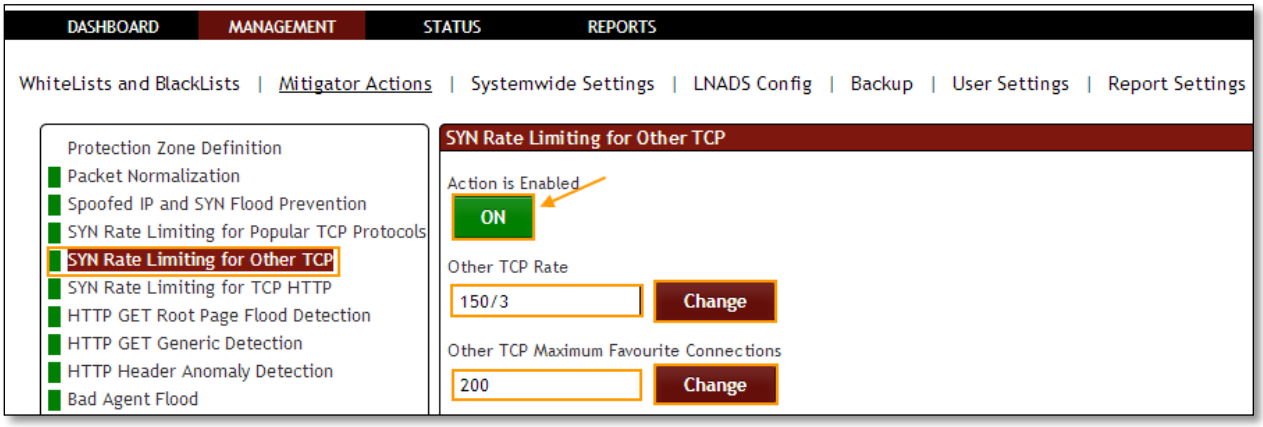



### 1.3.3.5 SYN Rate limiting for other TCP Action

**Rule F36:** The SYN packet to speed limit outside the popular ports can be active/passive. This İs the maximum number of connections the speed ratio of the block period to apply and you can modify through the interface.

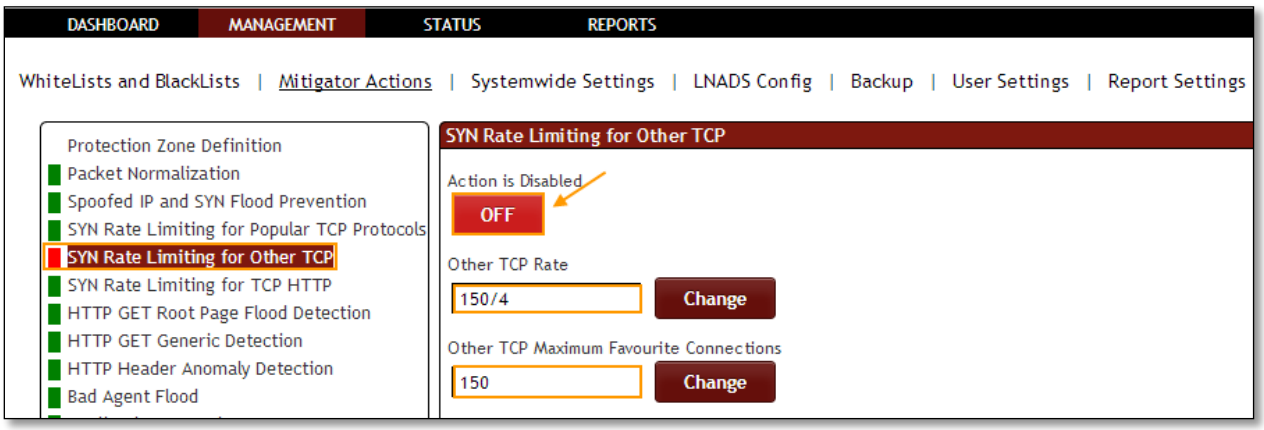
In **SYN Rate Limiting for other TCP Action** tab we have an option to **Enable / Disable the option**.

SYN Rate limiting for other TCP Action is enabled, it is in **ON** state. There are other options like **Other TCP Rate** and **Other TCP maximum Favorite Connections .**Enter the values and click on **change** to apply the changes.




Click on the same action tab to **disable the option**.

SYN Rate limiting for other TCP Action is **disabled**, it is in **OFF** state. We can also notice the Changes in **Other TCP Rate** and **Other TCP maximum Favorite Connections.**




### 1.3.3.6 SYN Rate Limiting for TCP HTTP Action

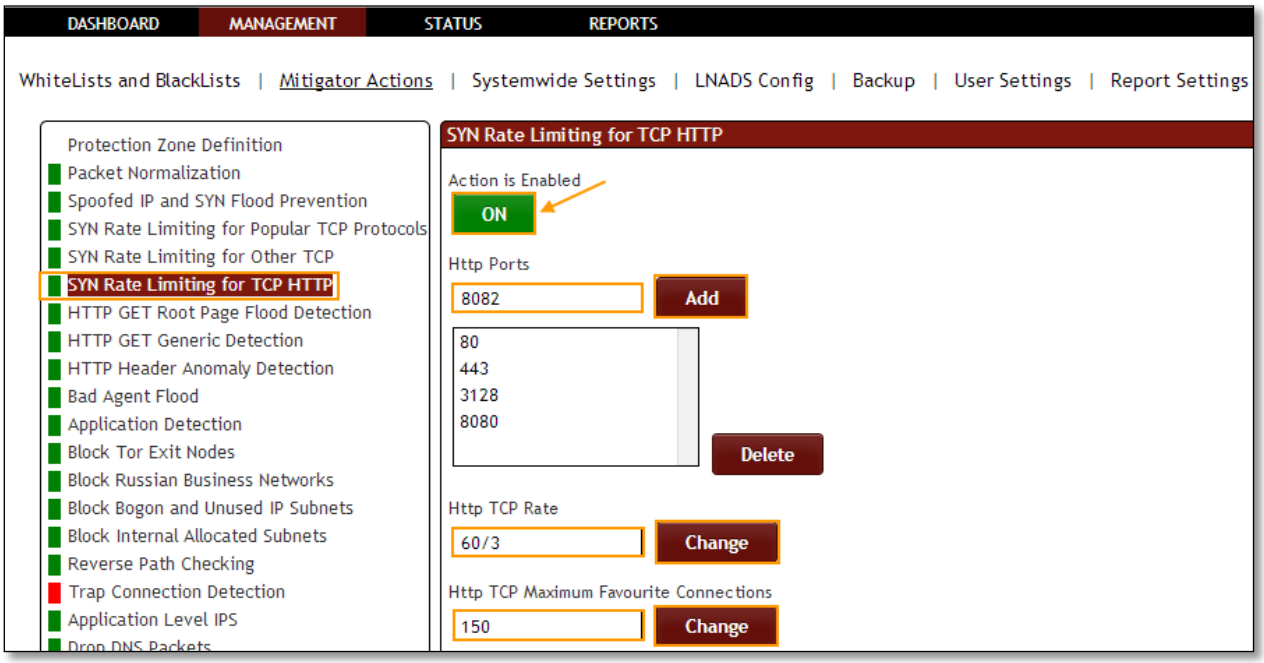
**Rule F26:** The SYN packet to the HTTP ports speed limitation is active/passive. This is a list of the port you want the block period to apply, you can change the maximum number of connections the speed ratio, and through the interface.

In **SYN Rate Limiting for TCP HTTP Action** tab we have an option to **Enable / Disable the option**.

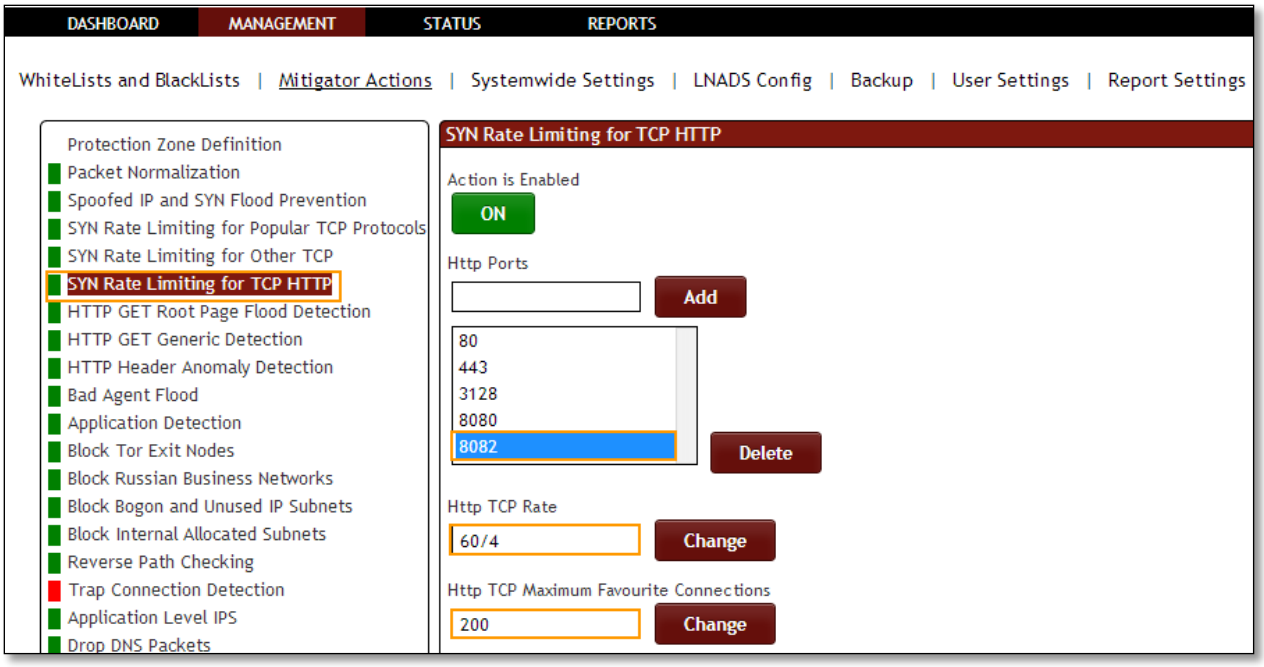
SYN Rate Limiting for TCP HTTP Action is **Enabled**, it is in **ON** state.

Mention HTTP Port number and click on **Add** tab.

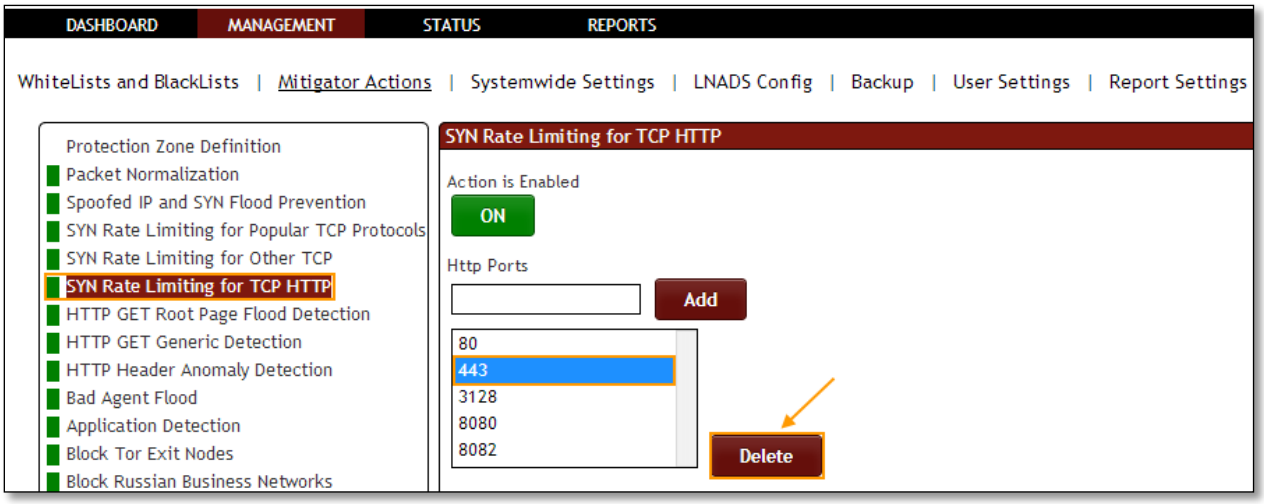
We can change **Http TCP rate** which defines SYN per second and **Http TCP Maximum Favorite Connections** which defines Connections count. Enter the values and click on **change** to apply the changes.




We can notice Http Port added in the list of Http Ports. And also **Http TCP Rate** and **Http TCP Maximum Favorite Connections** is also changed in the below tab.



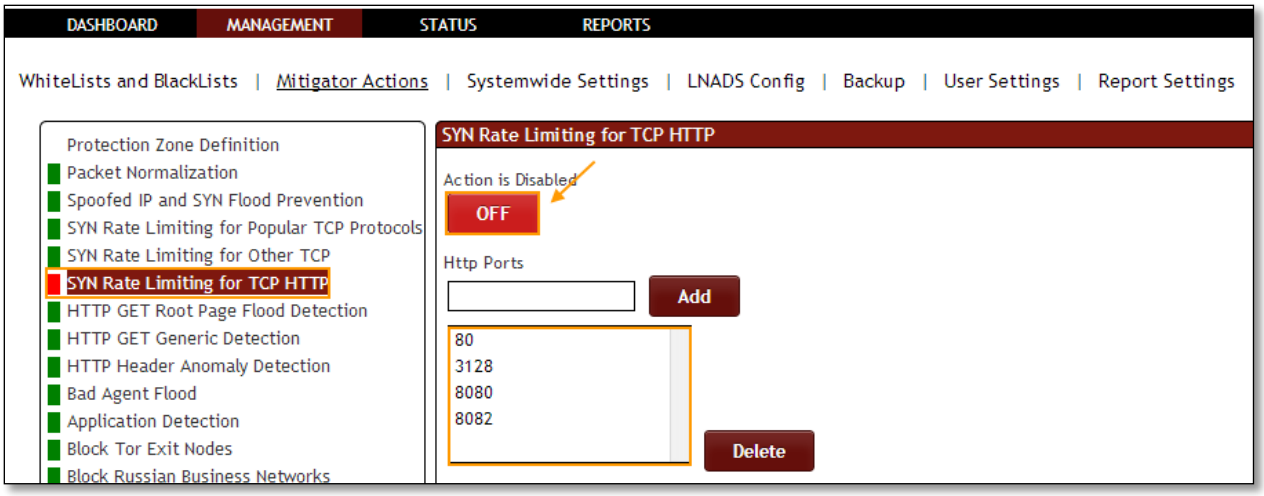

Select Http port and click on **Delete** tab.




Click on the same action tab to **Disable the option**.

SYN Rate Limiting for TCP HTTP Action is **disabled**, it is in **OFF** state.

We can notice selected Http Port deleted in the list of Http Ports.

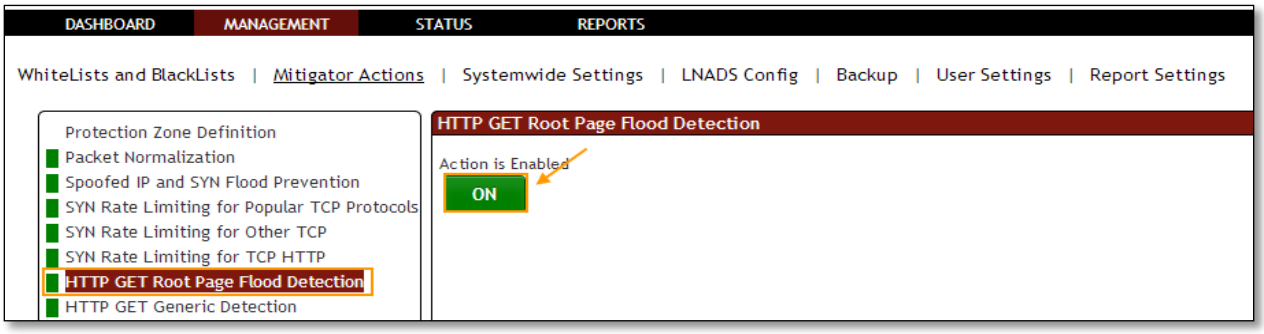



### 1.3.3.7 Http GET Root Page Flood Detection

**Rule 32:** HTTP GET/Flood prevention can be active/passive.

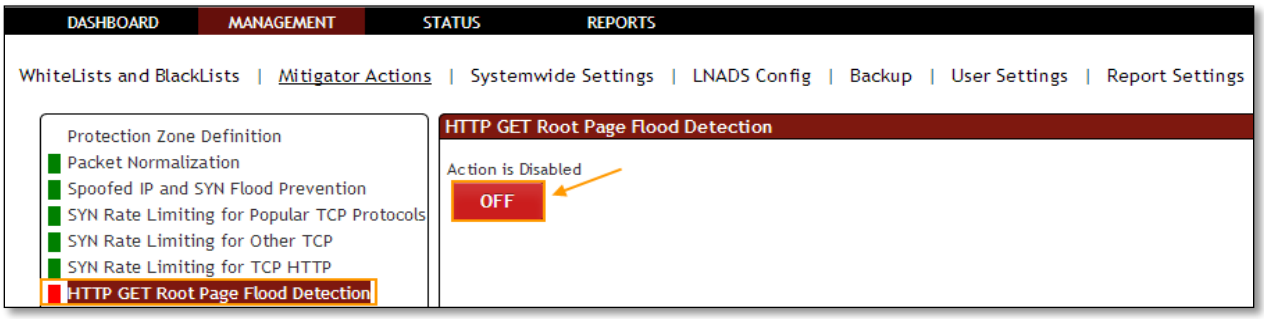
In **Http GET Root Page Flood Detection** tab we have an option to **Enable / Disable the option**.

Http GET Root Page Flood Detection and blocking Action is **Enabled**, it is in **ON** state.




Click on the same action tab to disable the option.

In the below screen, we can notice Http GET Root Page Flood Detection and blocking Action is **Disabled**, it is in **OFF** state.

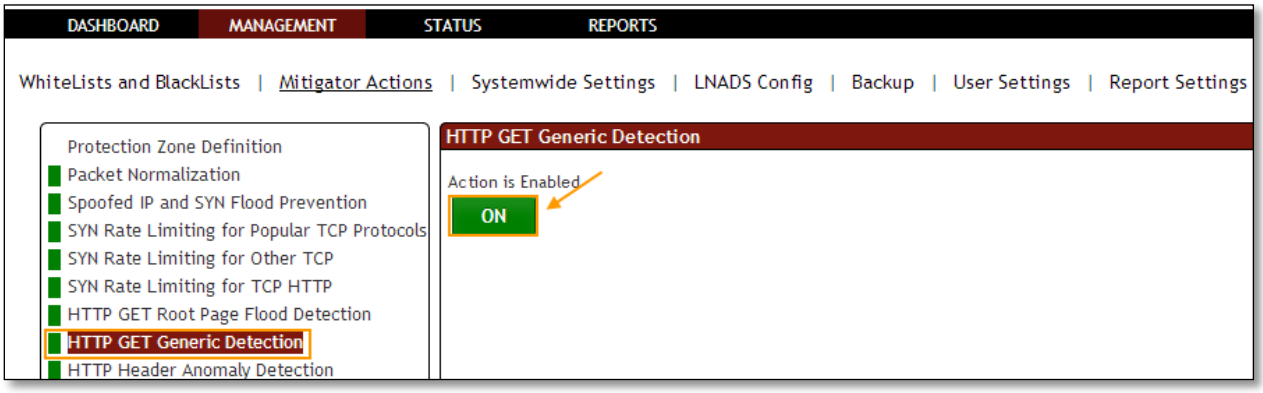


### 1.3.3.8 HTTP GET Generic Detection Action

**Rule F31:** HTTP GET Generic can be active/passive.

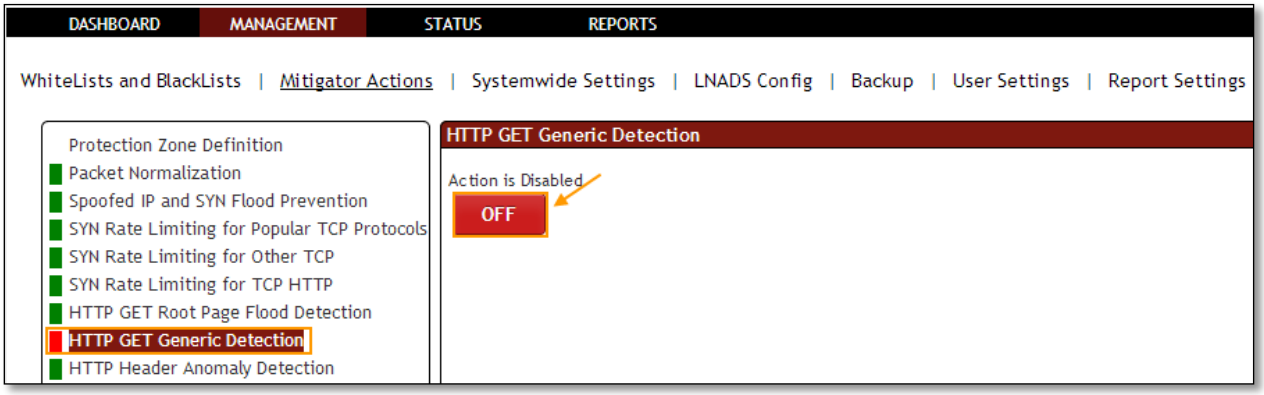
In **HTTP GET Generic Detection Action** tab we have an option to **Enable / Disable the option**.

HTTP GET Generic Detection and Blocking Action is **Enabled**, it is in **ON** state.




Click on the same action tab to disable the option.

HTTP GET Generic Detection and Blocking Action is **Disabled**, it is in **OFF** state.

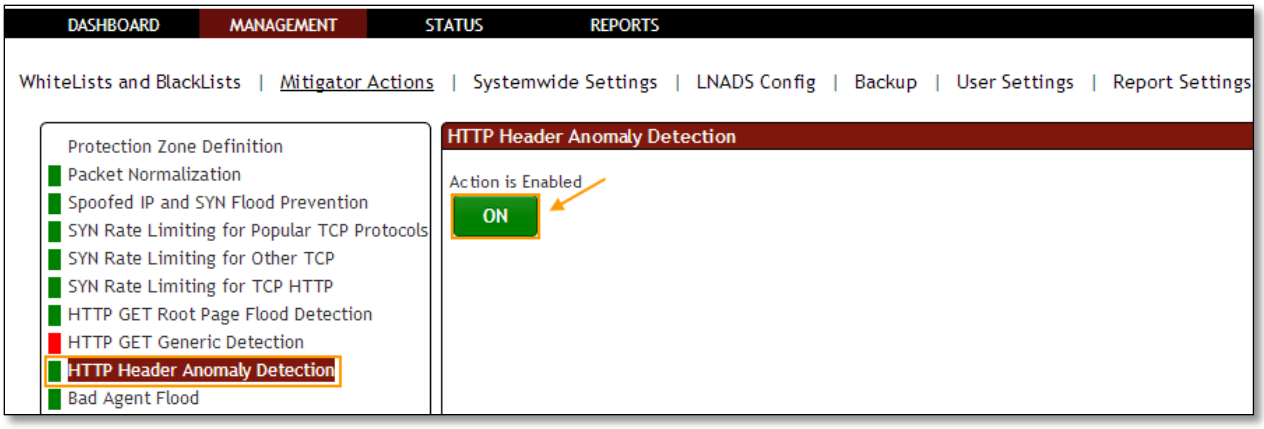



### 1.3.3.9 HTTP Header Anomaly Detection

**Rule F33:** This system is activated; the system prevents the abnormal sees http requests.

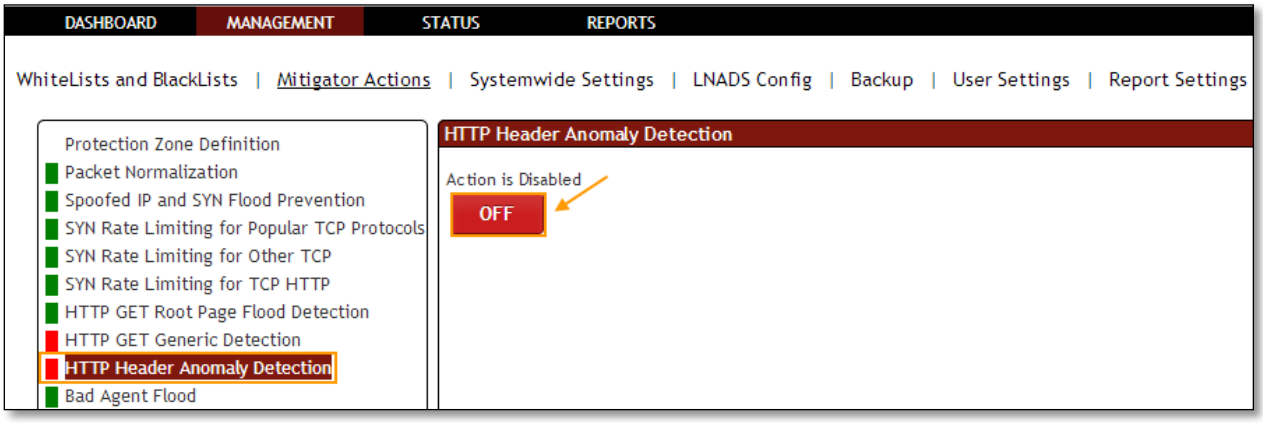
In **HTTP Header Anomaly Detection** tab we have an option to **Enable / Disable the option**.

HTTP Header Anomaly Detection and Blocking Action is **Enabled,** it is in **ON** state.




Click on the same action tab to disable the option.

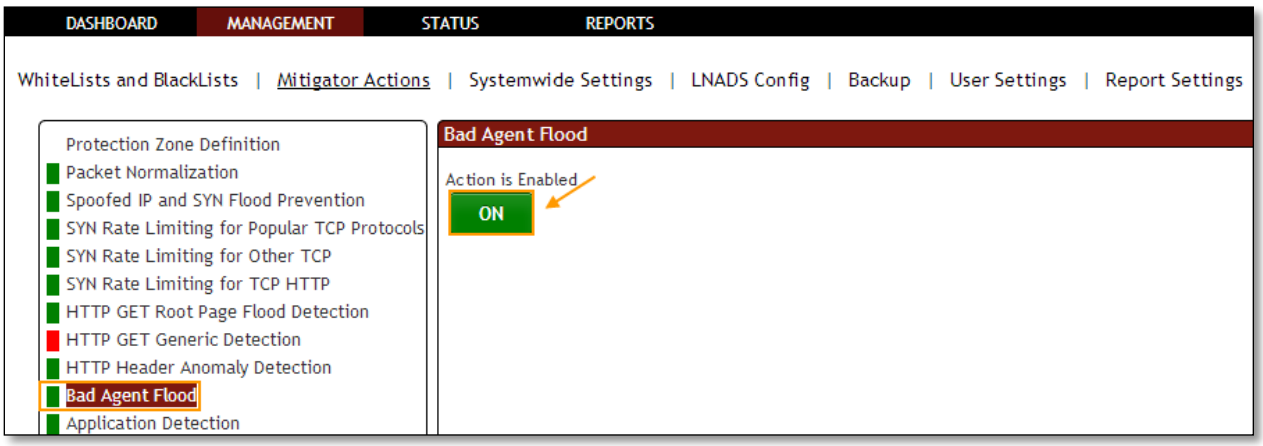
HTTP Header Anomaly Detection and Blocking Action is **Disabled**, it is in **OFF** state.




### 1.3.3.10 Bad Agent Flood

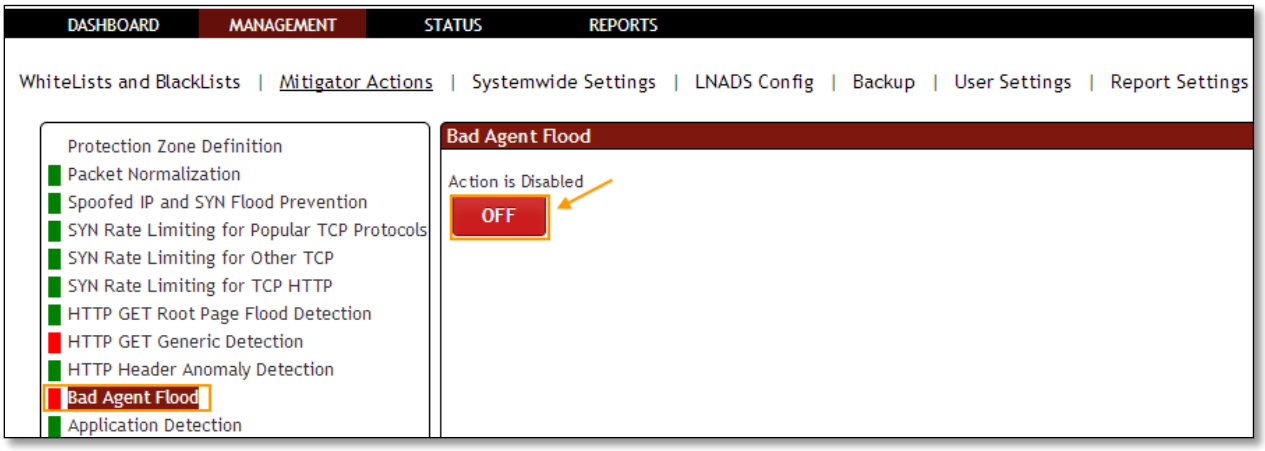
In **Bad Agent Flood** tab we have an option to **Enable / Disable the option**.

Flood black list agent blocking Action is **Enabled**, it is in **ON** state.



Click on the same action tab to disable the option.

Flood black list agent blocking Action is **Disabled,** it is in **OFF** state.

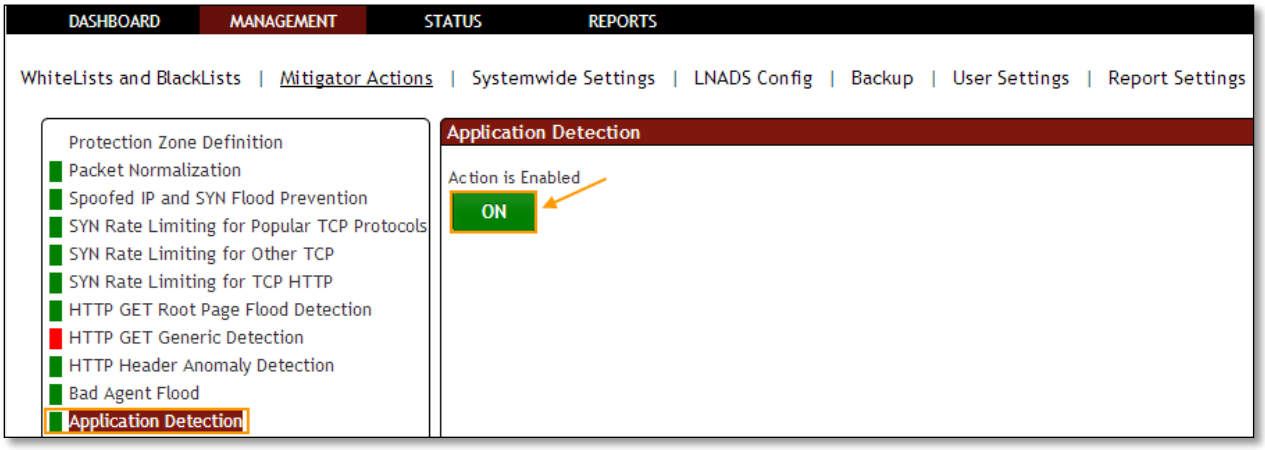



### 1.3.3.11 Application Detection

**Rule F16:** Application Detection is used to prevent attacks from application like juno.

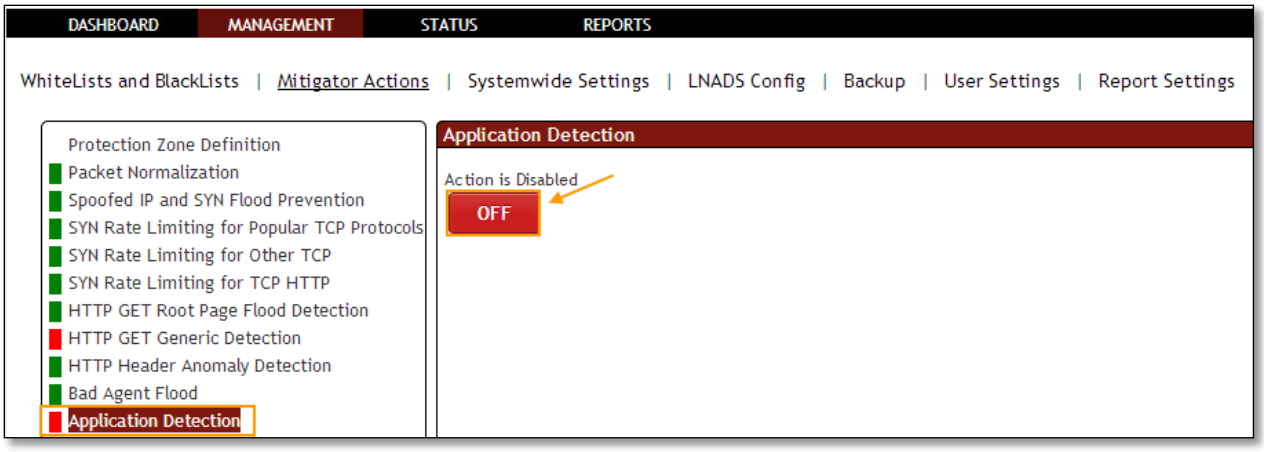
In **Application Detection** tab we have an option to **Enable / Disable the option**.

Application Detection Action Enabled for blocking according to DoS/DDoS tool characteristics, it is in **ON** state.




Click on the same action tab to disable the option.

Application Detection Action is **Disabled**, it is in **OFF** state.

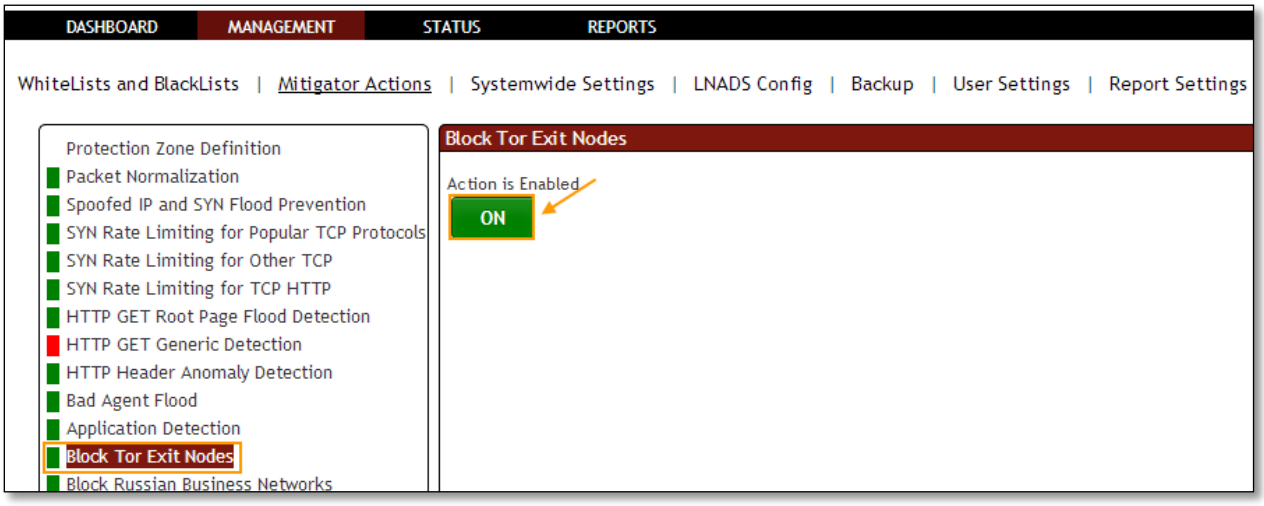



### 1.3.3.12 Block Tor Exit Nodes

**Rule F8:** Tor Exit Nodes * servers. This list is kept in/etc/pf/tables/db/tor_exit_nodes.

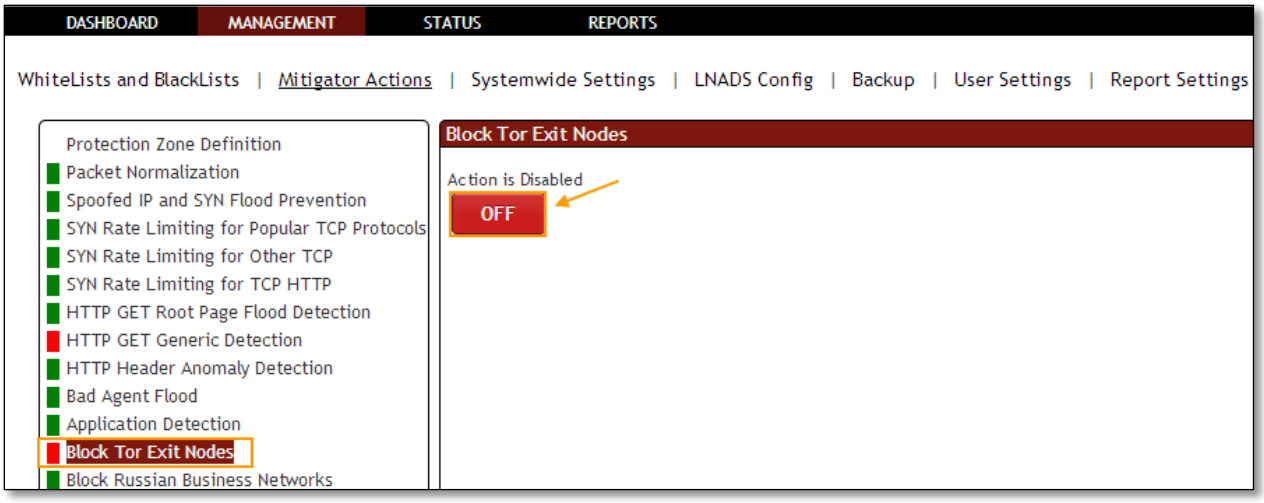
In **Block Tor Exit Nodes** tab we have an option to **Enable / Disable the option**.

Block Tor Exit Nodes Action is **Enabled** for blocking of Tor Exit nodes IPs, it is in **ON** state.




Click on the same action tab to disable the option.

Block Tor Exit Nodes Action is **Disabled**, it is in **OFF** state.

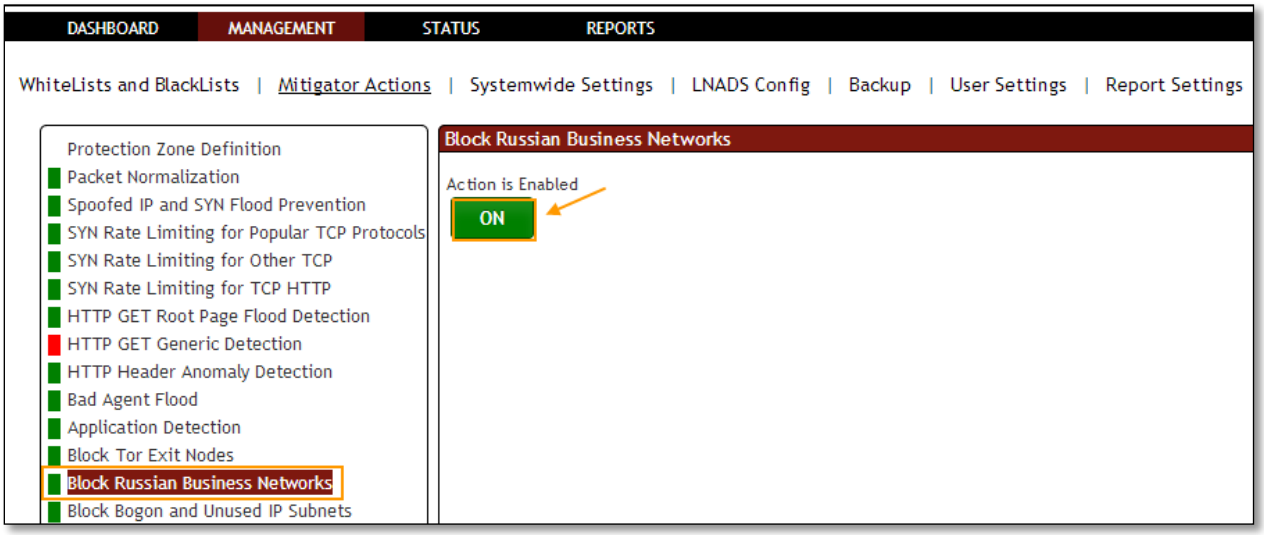



### 1.3.3.13 Block Russian Business Networks

**Rule F9:** RBN servers. This list is kept in/etc/pf/tables/db/rbn_servers.

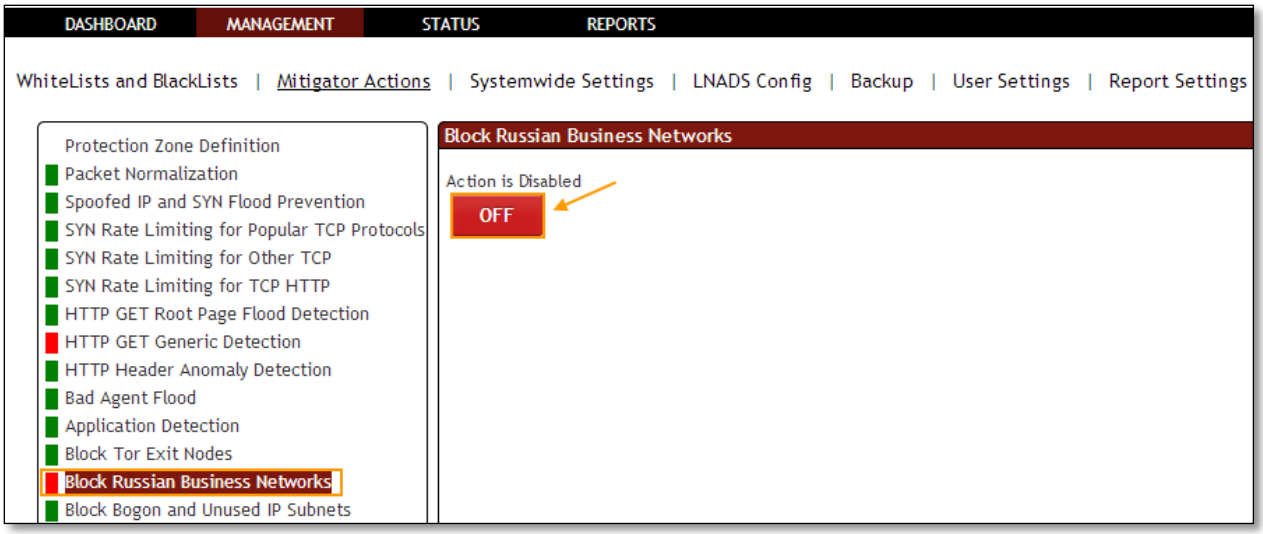
In **Block Russian Business Networks** tab we have an option to **Enable / Disable the option**.

Block Russian Business Networks (RBN) Action is **Enabled** for blocking of RBN Server, it is in **ON** state.




Click on the same action tab to disable the option.

Block Russian Business Networks (RBN) Action is **Disabled**, it is in **OFF** state.

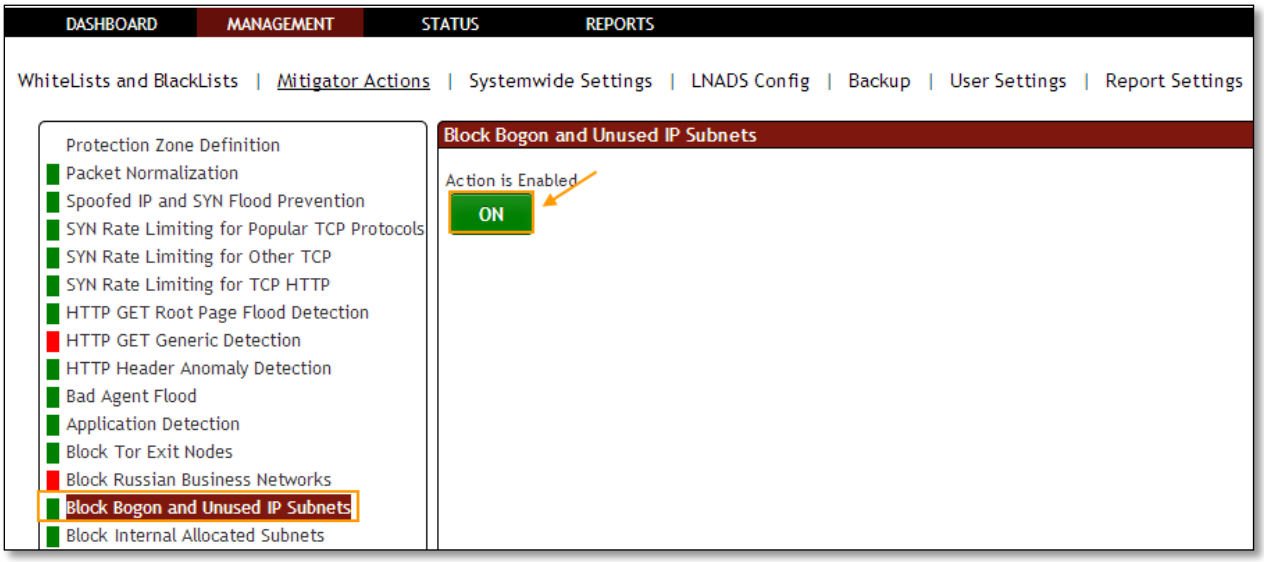



### 1.3.3.14 Block Bogon and Unused IP Subnets

**Rule F10: P**rovides the IP addresses be blocked unused and bogon. This list is kept in/etc/pf/tables/db/bogon_nets.

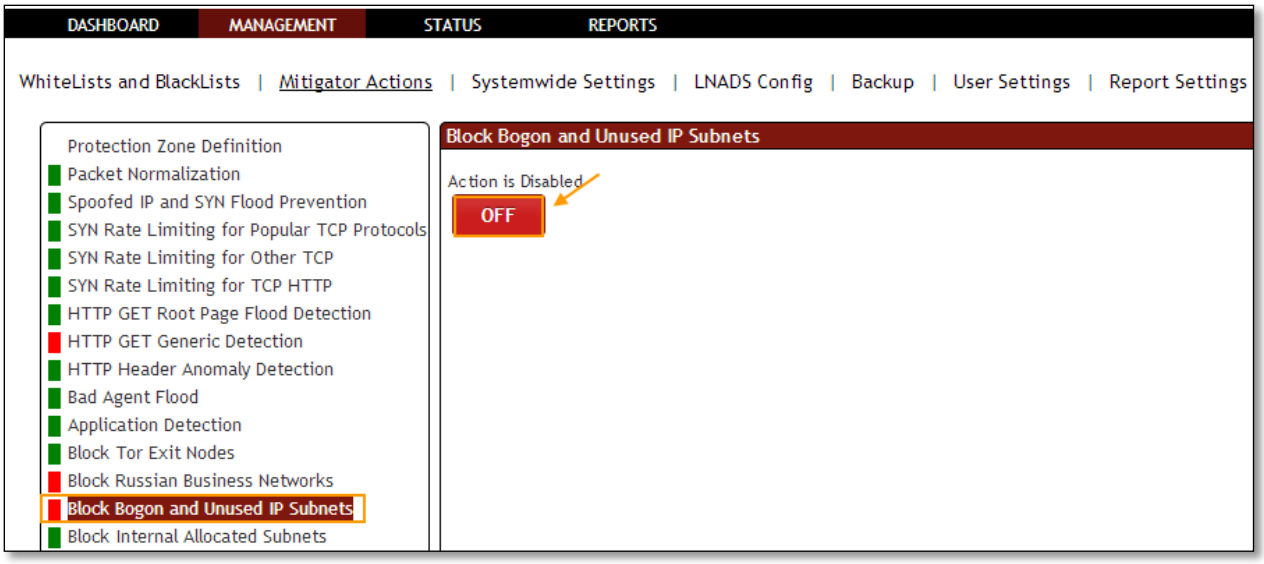
In **Block Bogon and Unused IP Subnets** tab we have an option to **Enable / Disable the option**.

Block Bogon and Unused IP Subnets Action is **Enabled** for blocking of Bogon Unused Subnet IPs, it is in **ON** state.




Click on the same action tab to disable the option.

Block Bogon and Unused IP Subnets Action is **Disabled**, it is in **OFF** state.

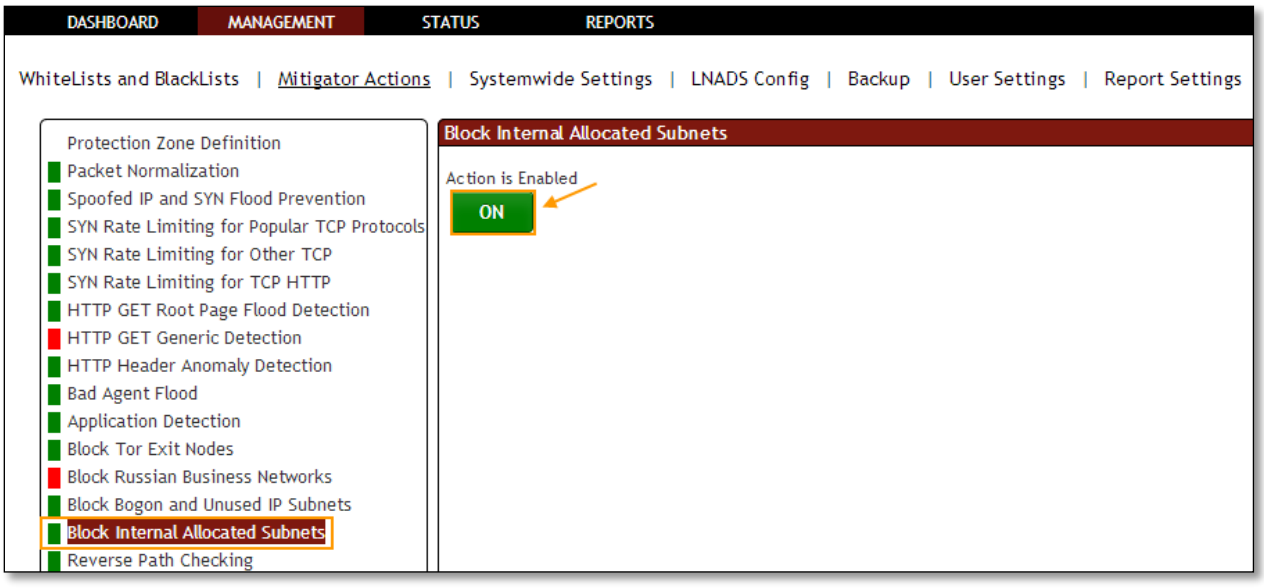



### 1.3.3.15 Block Internet Allocated Subnets

**Rule F11:** On the internal network with the IP address used in the attack. This list is kept in/etc/pf/tables/db/internal_nets.

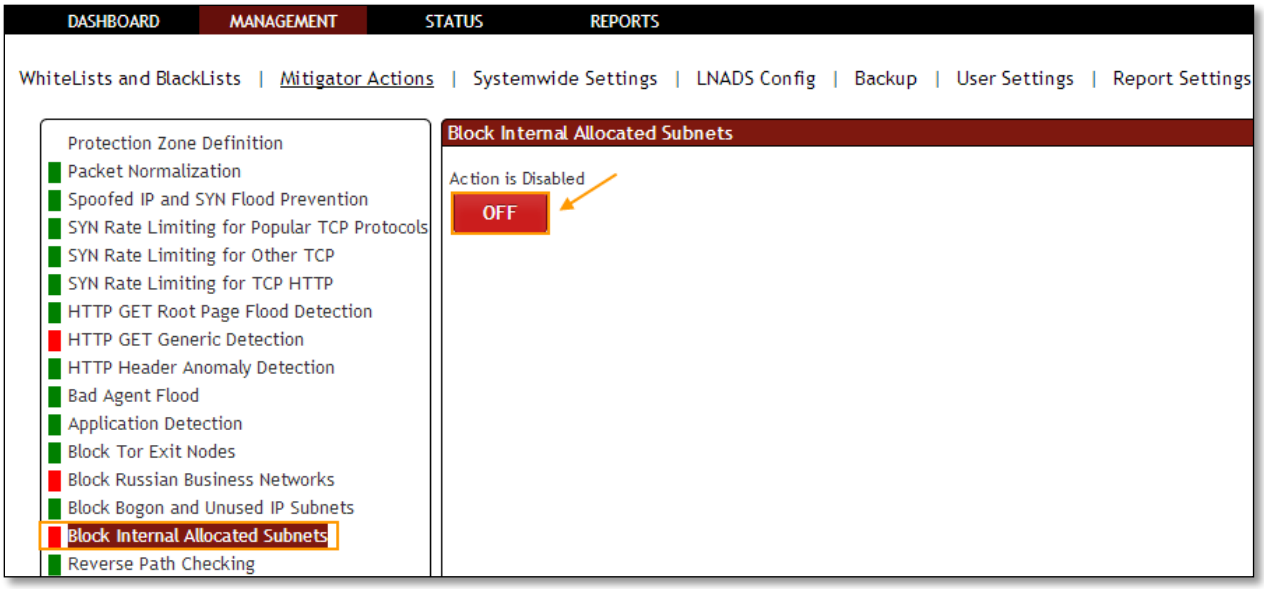
In **Block Internet Allocated Subnets** tab we have an option to **Enable / Disable the option**.

Block Internet Allocated Subnets Action is **Enabled** for IPs defined in non public internal IP subnets, it is in **ON** state.




Click on the same action tab to disable the option.

Block Internet Allocated Subnets Action is **disabled,** it is in **OFF** state.

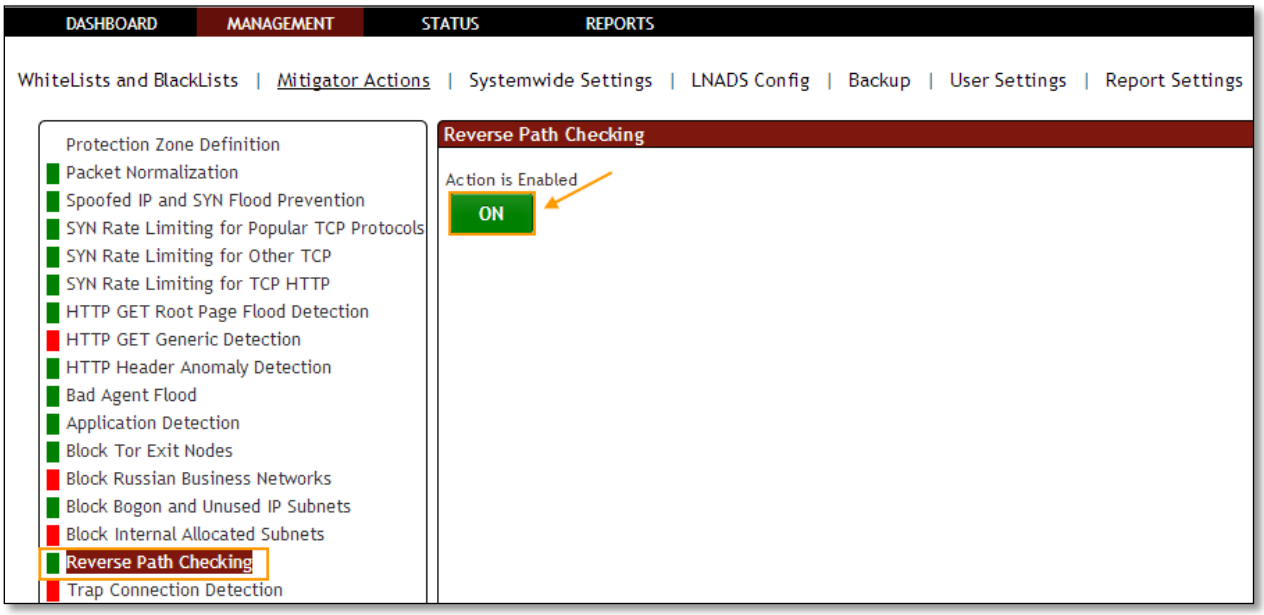



### 1.3.3.16 Reverse Path Checking

**Rule F29:** Followed by the path to the package that came with the package, followed by the same way whether the monitoring.

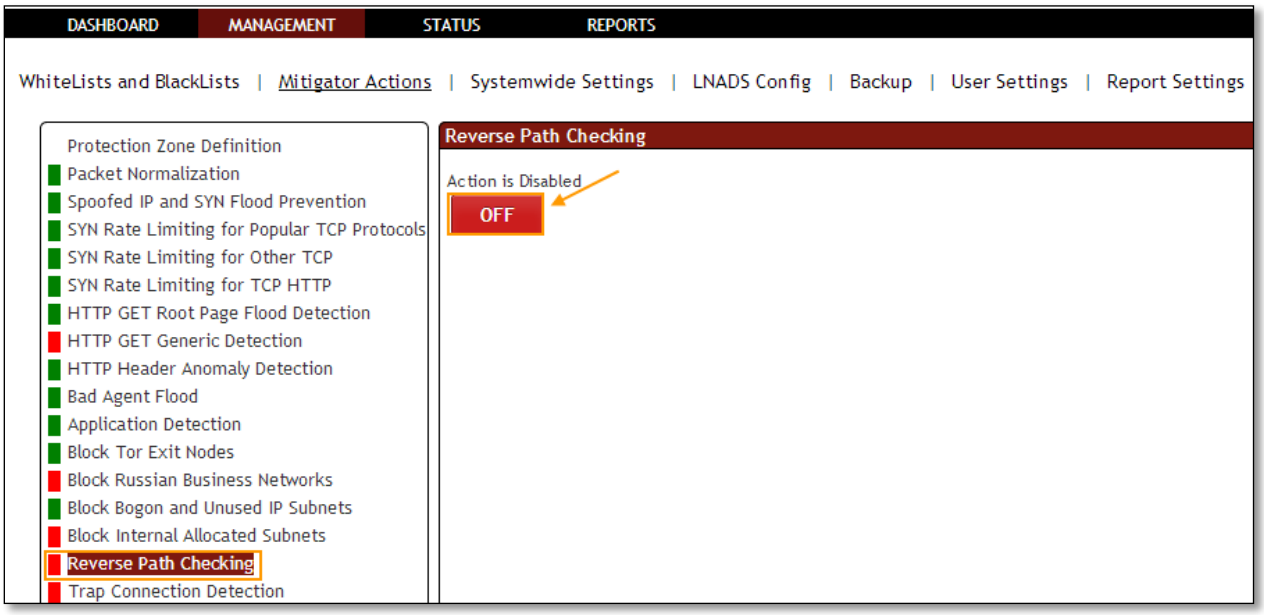
In **Reverse Path Checking** tab we have an option to **Enable / Disable the option**.

Reverse Path Checking Action is **Enabled** to enforce the ingress path of packets, it is in **ON** state.




Click on the same action tab to disable the option.

Reverse Path Checking Action is **Disabled**, it is in **OFF** state.




### 1.3.3.17 Trap Connection Detection

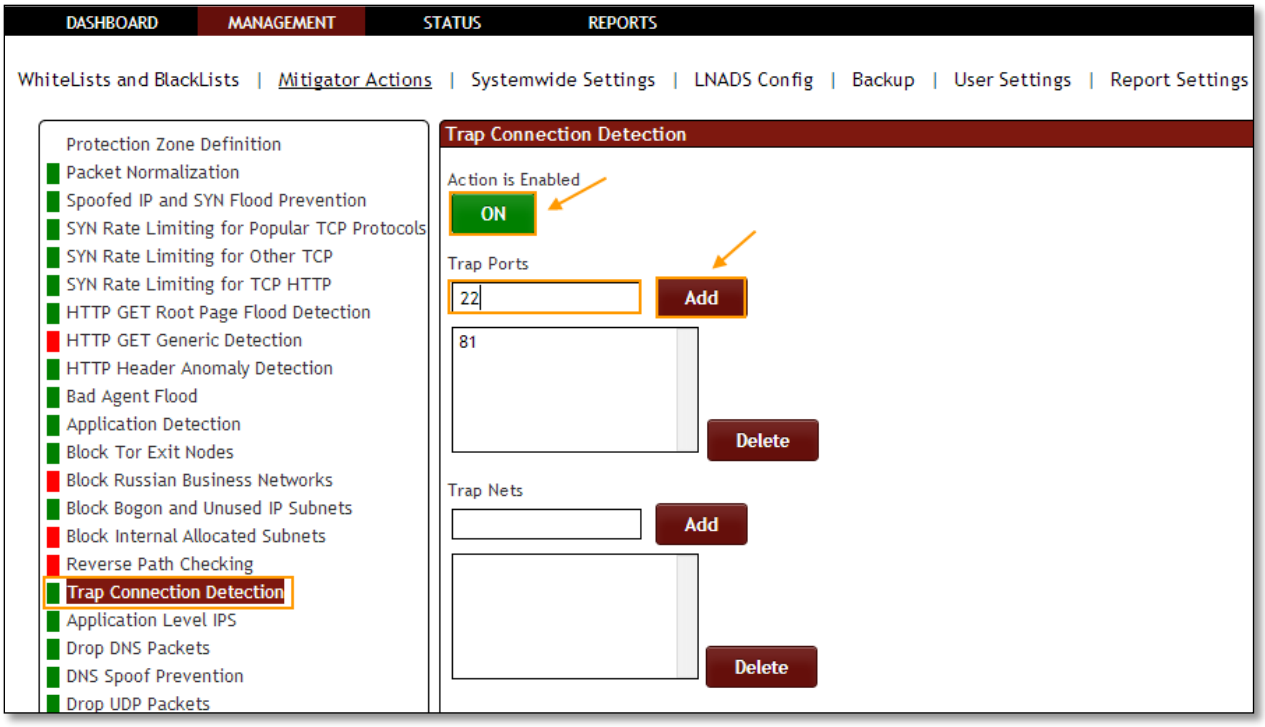
**Rule F6:** Trap port to capture the active/passive. This is a list of port and IP interface can change through the block period to apply.

In **Trap Connection Detection** tab we have an option to **Enable / Disable the option**.

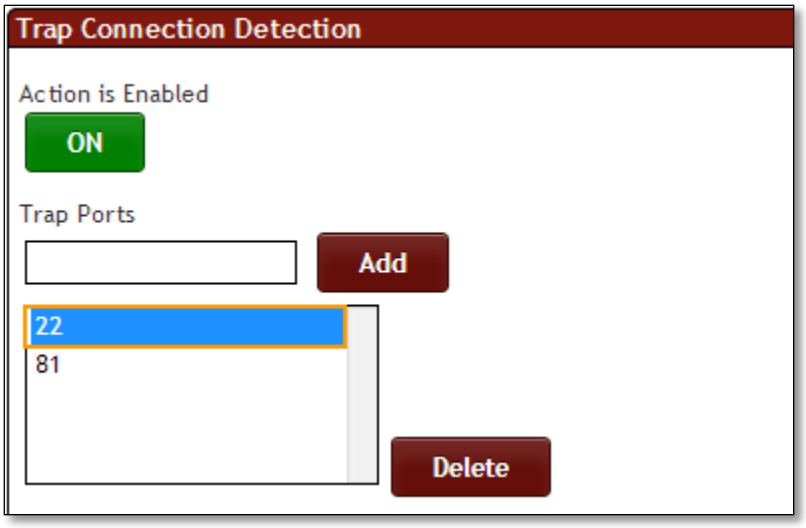
Trap Connection Detection Action is enabled for making DDOS Mitigator monitoring for a trap network Zone on a trap destination port which is unused in normal conditions, it is in ON state.

Mention Trap port number and click on **Add** tab**.**

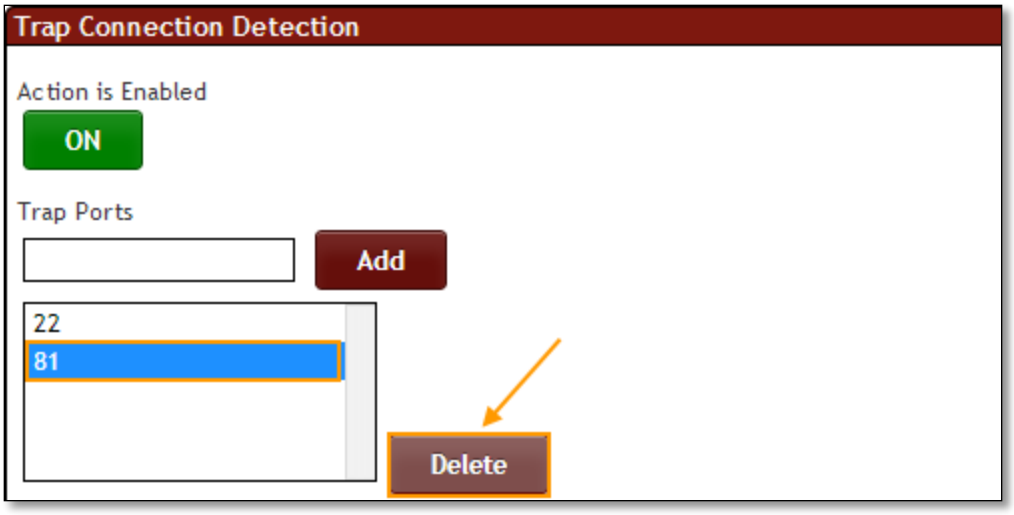
TCP port numbers between numbers (1-65535) are only valid.



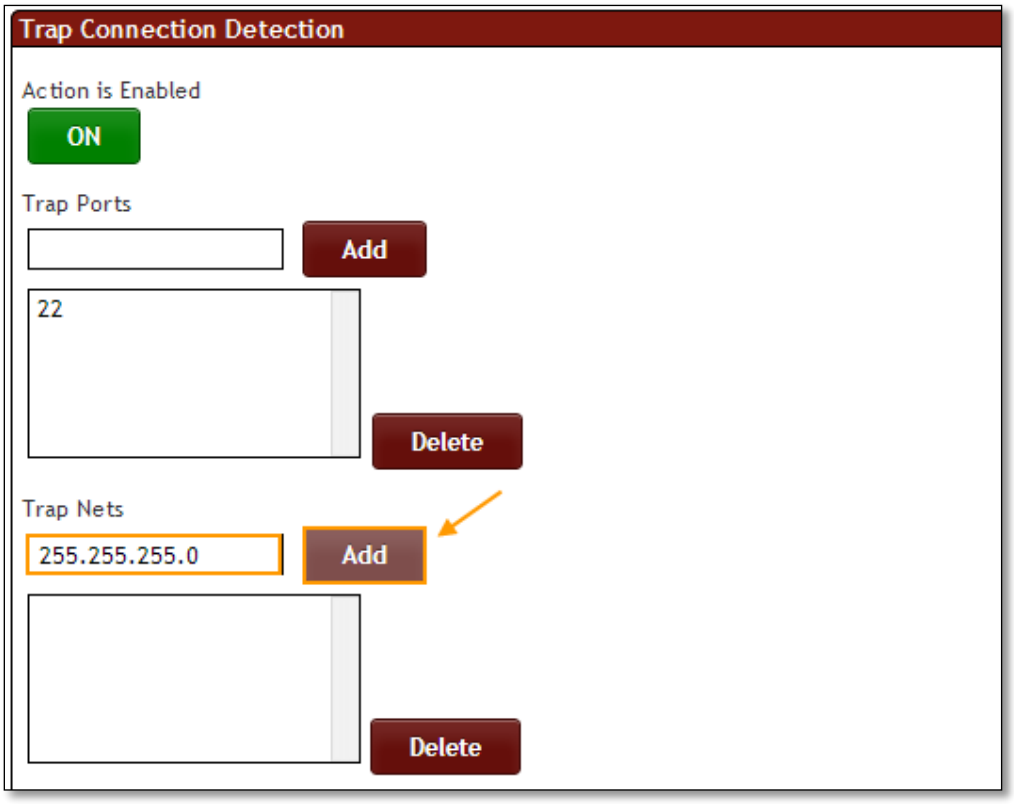

In the below screen, we can notice Trap port number added in the list of Trap Ports.



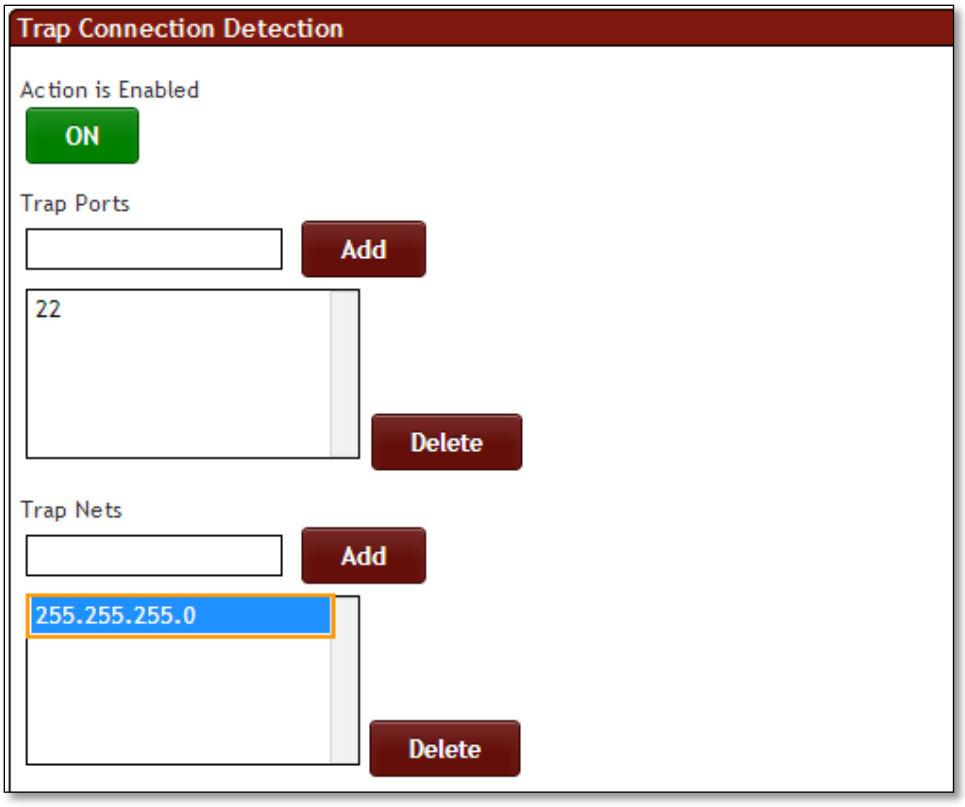

Select the Port number and click on **Delete** tab**.**



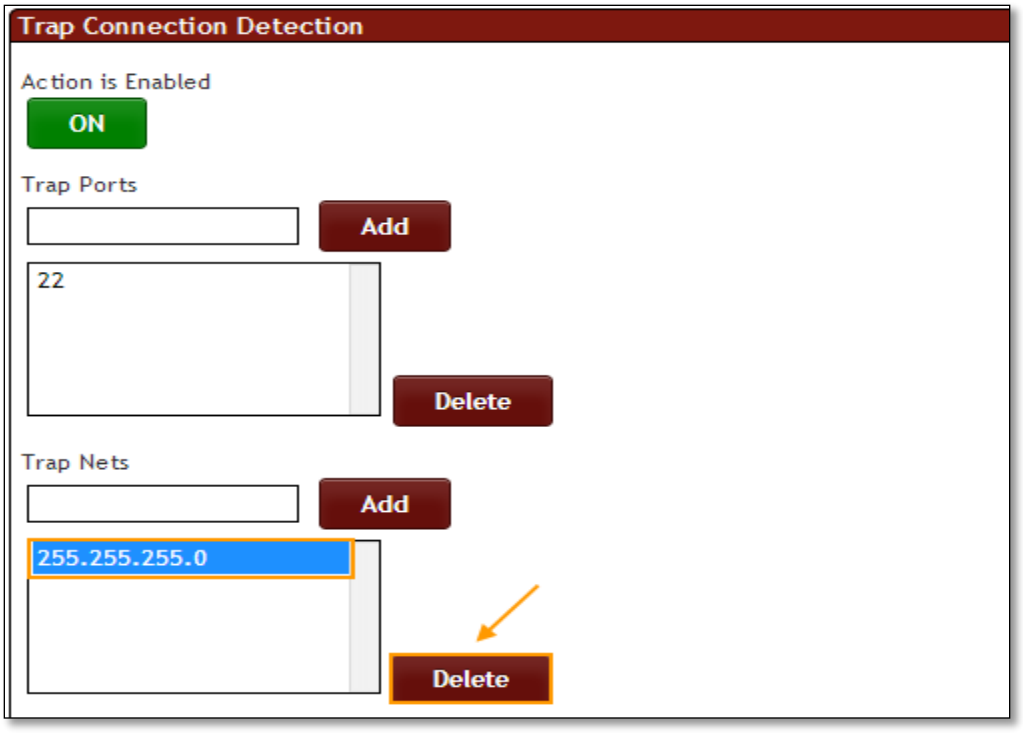

Mention Subnet/Network IP and click on **Add** tab.



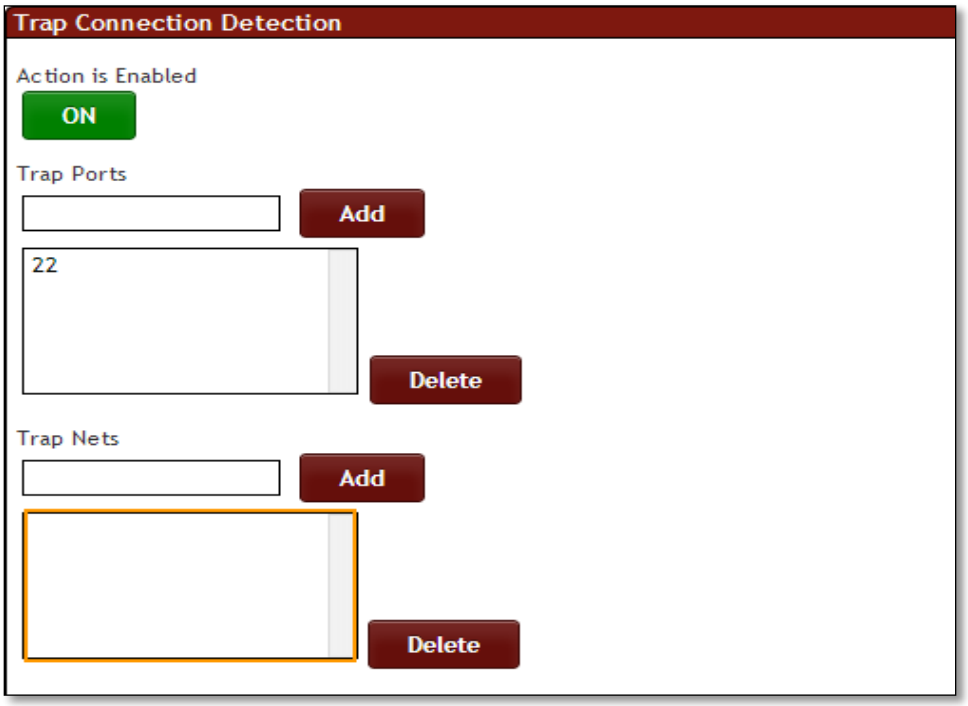

In the below screen, we can notice Subnet IP in the list of Trap Nets.




Select the Subnet IP and click on **Delete** tab.

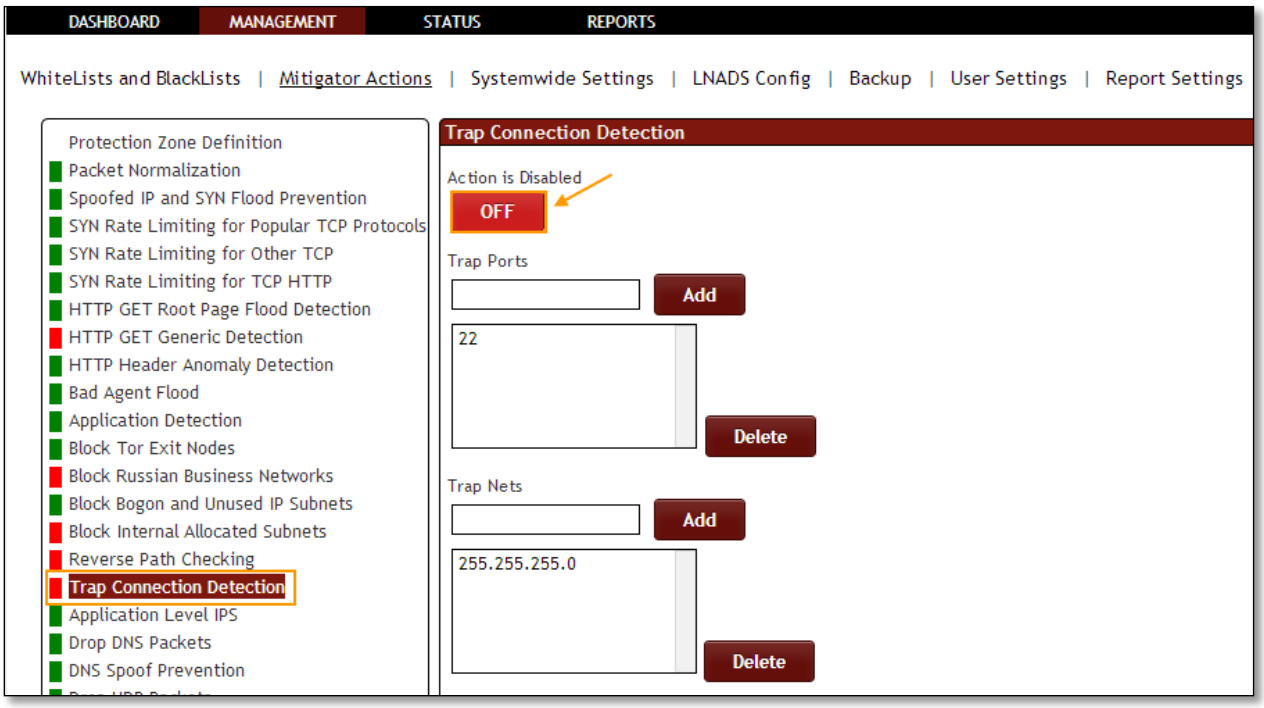


In the below screen, we can notice Subnet IP deleted.




Click on the same action tab to disable the option.

Trap Connection Detection Action is **Disabled**, it is in **OFF** state.

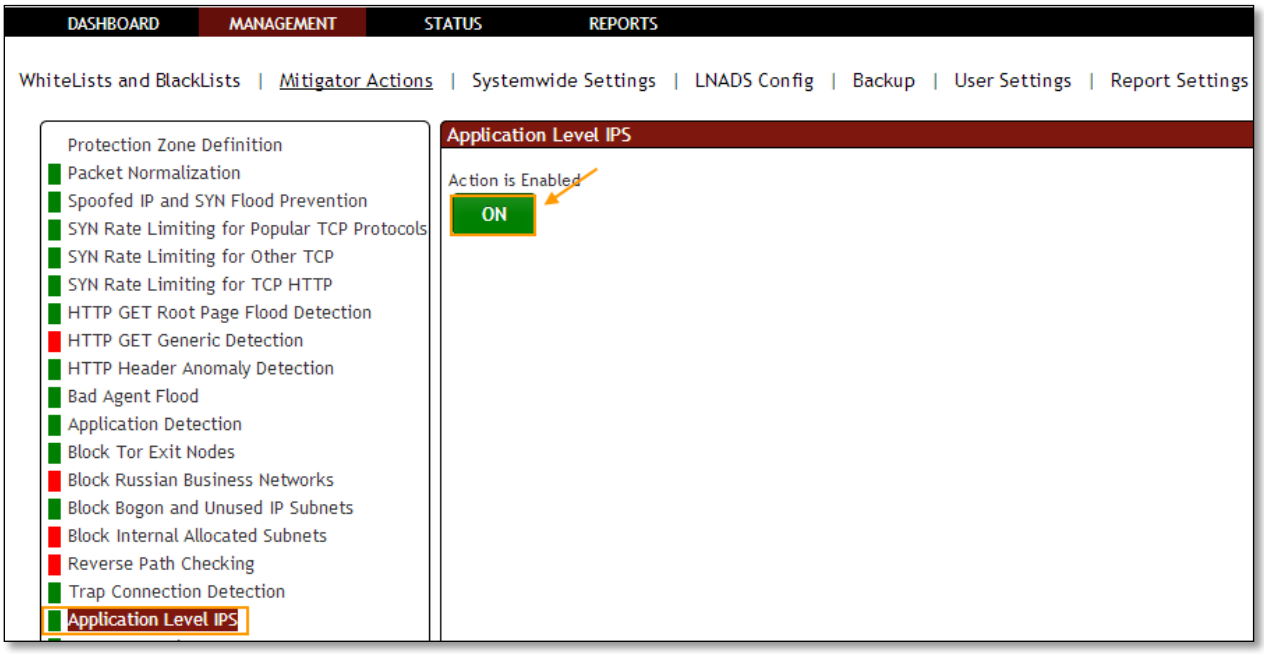


### 1.3.3.18 Application Level IPS

**Rule F15:** The Ramada provides specific application's IP be blocked.

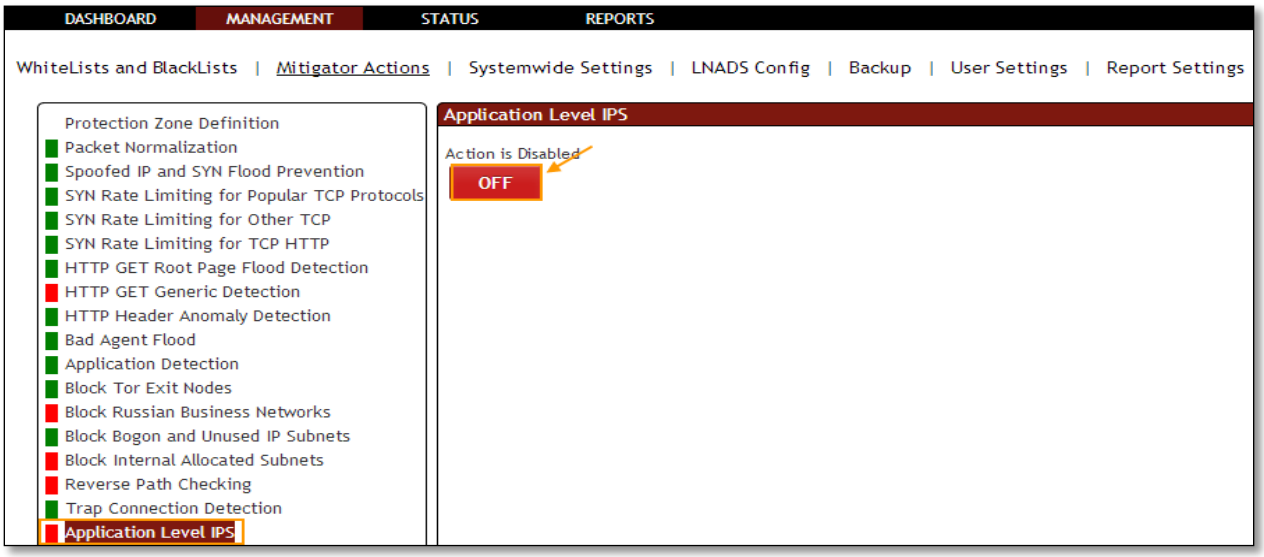
In **Application Level IPS** tab we have an option to **Enable / Disable the option**.

Application Level IPS Action is **Enabled** for blocking of IPs detected by embedded DDoS specific IPS, it is in **ON** state.




Click on the same action tab to disable the option.

Application Level IPS Action is **Disabled**, it is in **OFF** state.

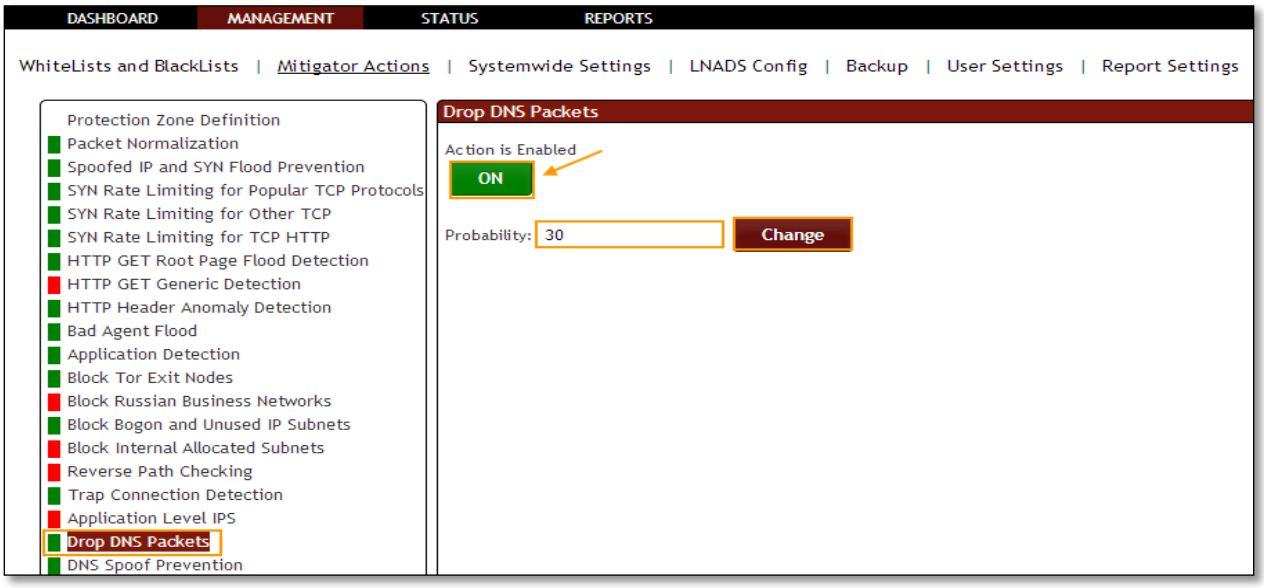


### 1.3.3.19 Drop DNS Packets

**Rule F17:** Provides DNS packets falling rate entered.

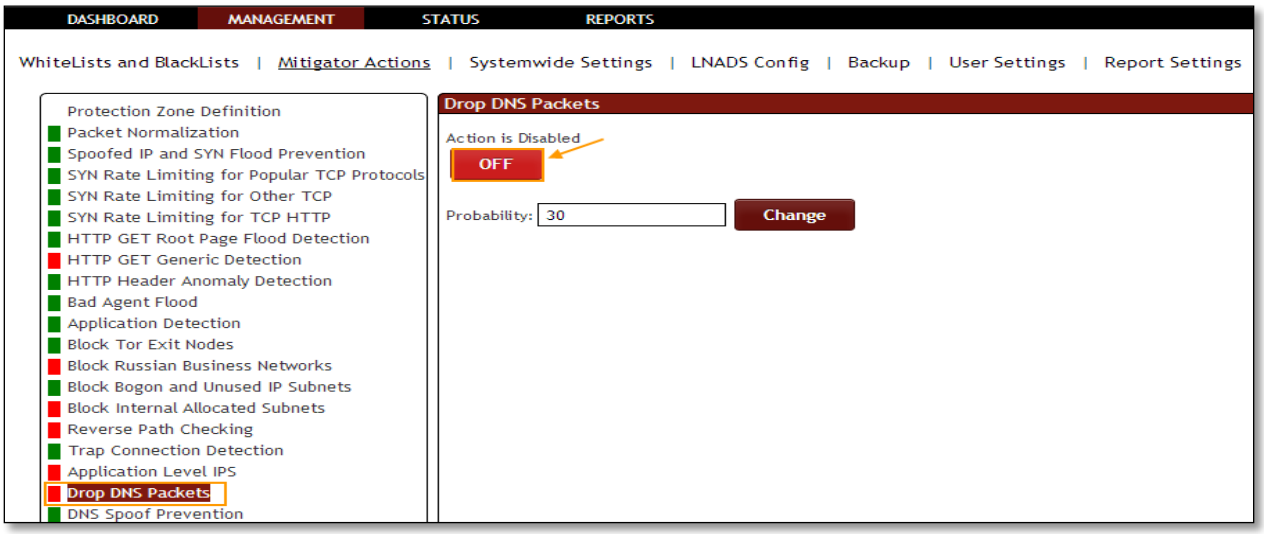
In **Drop DNS Packets** tab we have an option to **Enable / Disable the option**.

Drop DNS Packets Action is **Enabled** for mitigation of DNS, it is in **ON** state. There is another option **Probability**. Enter the value and click on **change** to apply the changes.




Click on the same action tab to disable the option.

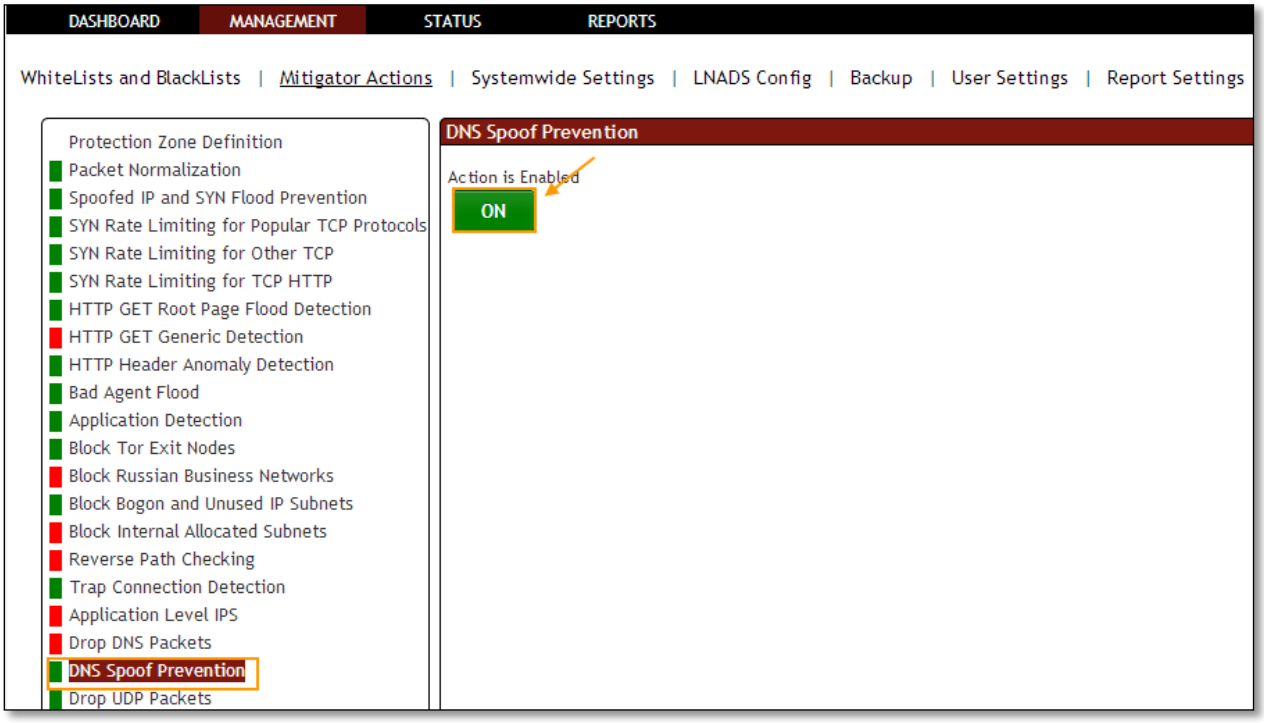
Drop DNS Packets Action is **Disabled**, it is in **OFF** state.



### 1.3.3.20 DNS Spoof Prevention

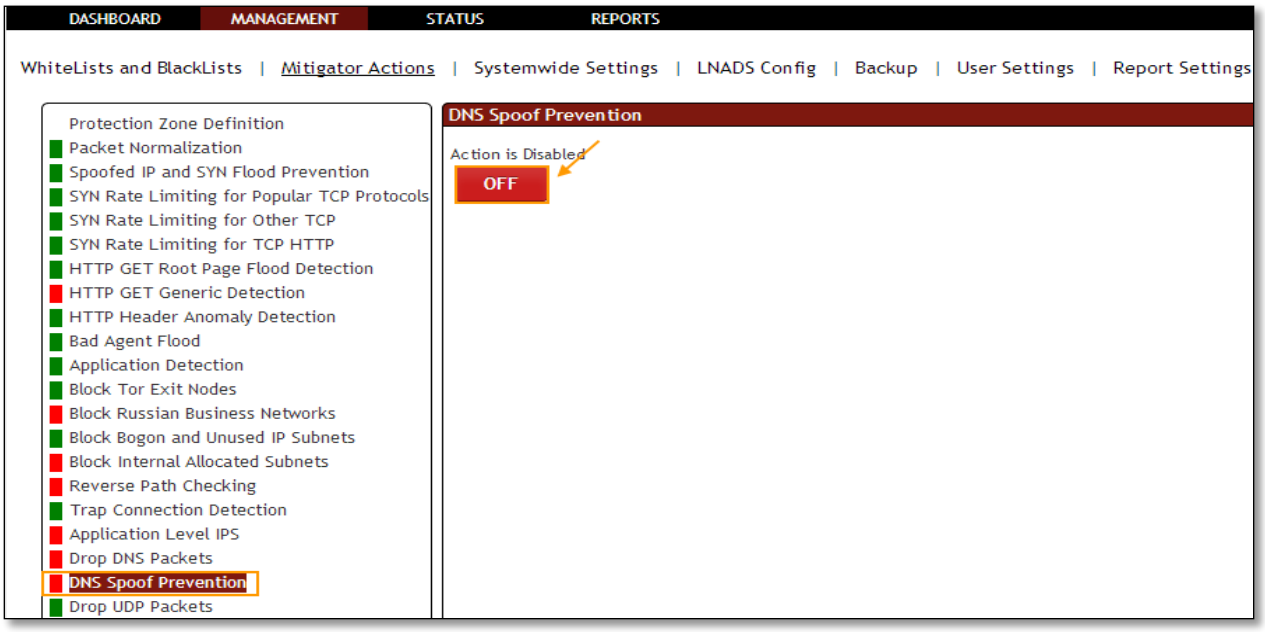
In **DNS Spoof Prevention** tab we have an option to **Enable / Disable the option**.

DNS Spoof Prevention Action is **Enabled** to use TCP packets for DNS, it is in **ON** state.

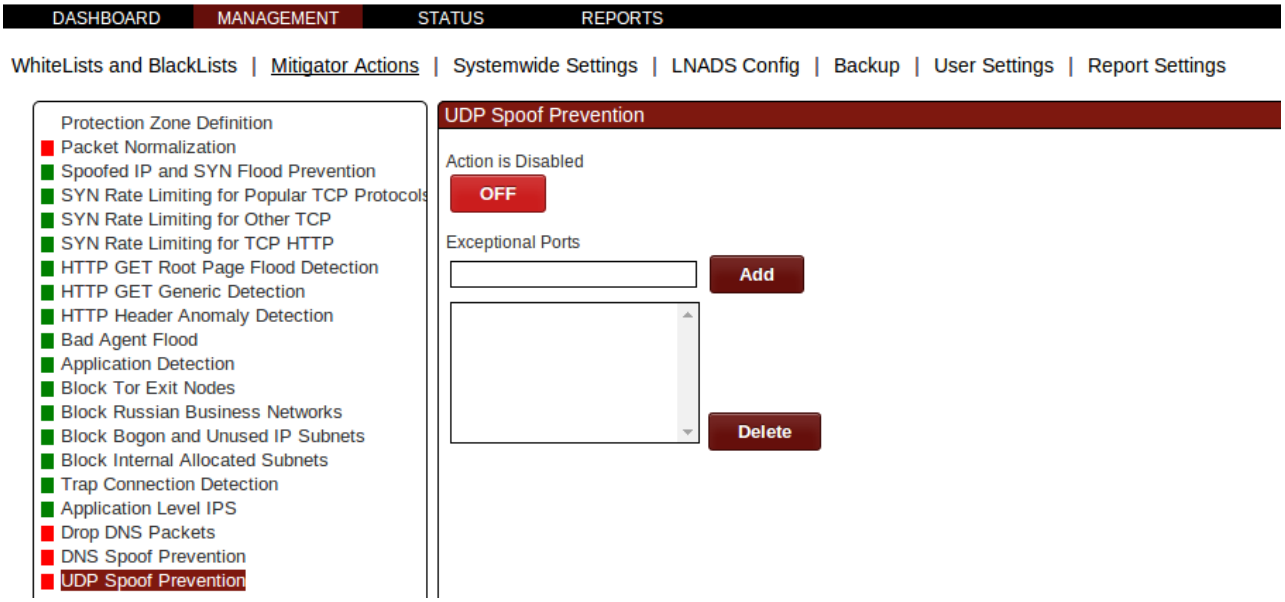



Click on the same action tab to disable the option.

DNS Spoof Prevention Action is **Disabled**, it is in **OFF** state.




### 1.3.3.21 UDP Spoof Prevention




UDP Spoof Prevention feature provides "drop first accept second" functionality for udp packets. If any exception ports are specified, then UDP Spoof Prevention is not performed on udp packets that are destined for the specified exceptional ports.

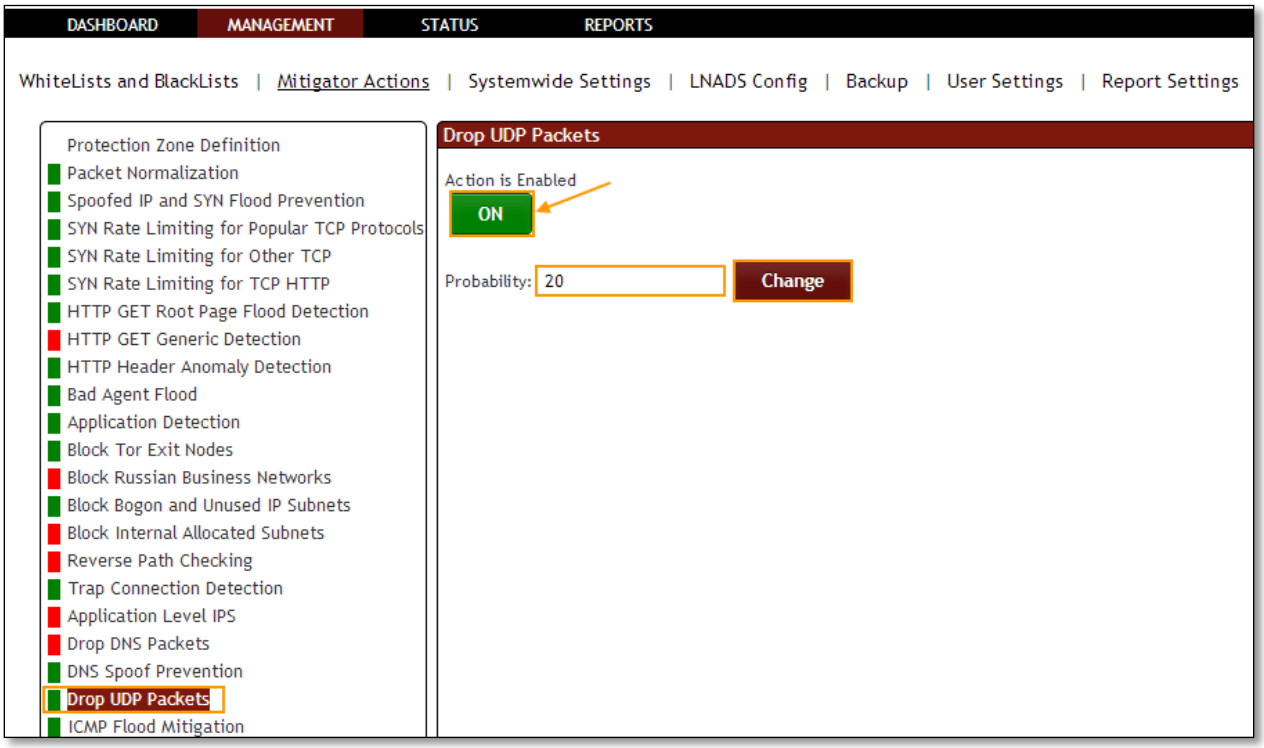
### 1.3.3.22 Drop UDP Packets

**Rule F23:** Provides UDP packets from falling significantly Entered.

In **Drop UDP Packets** tab we have an option to **Enable / Disable the option**.

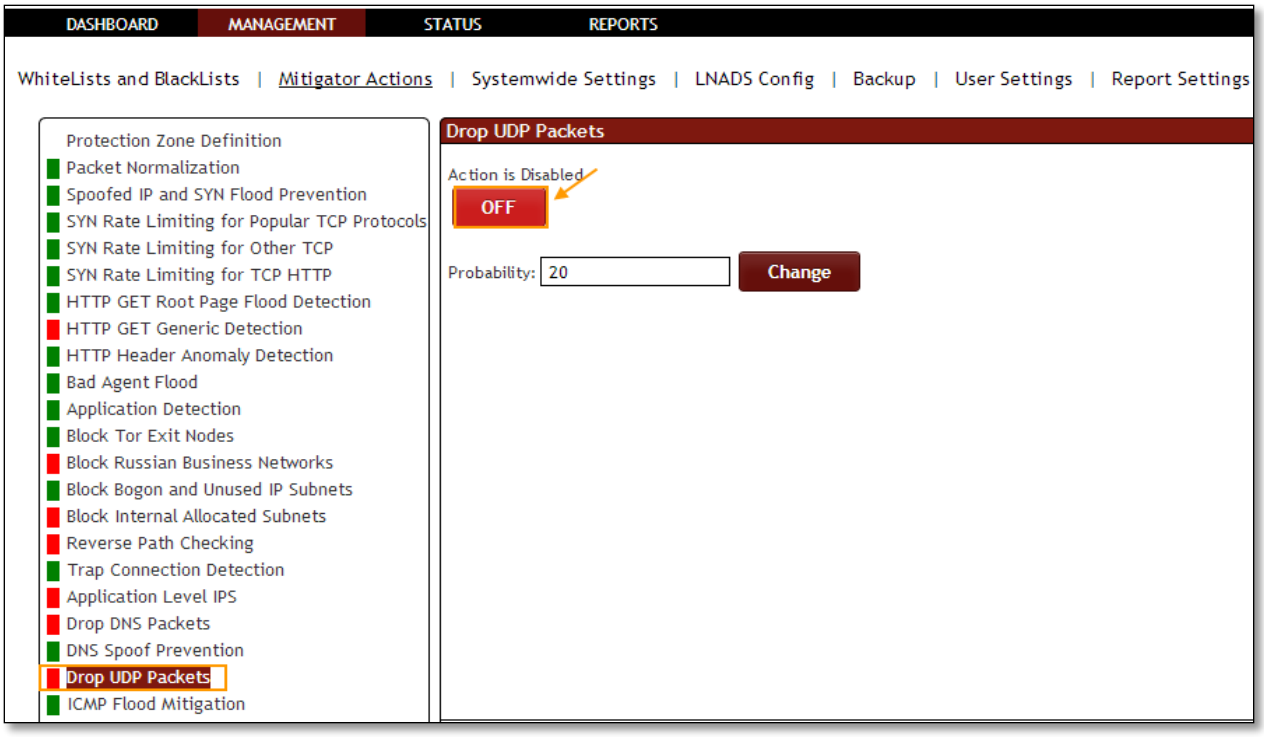
Drop UDP Packets Action is **Enabled** for Mitigation of some highly used UDP Packets protocols, it is in **ON** state.

We can change probability number of packets. Enter the value and click on **change** to apply the changes.




Click on the same action tab to disable the option.

Drop UDP packets Action is **Disabled**, it is in **OFF** state

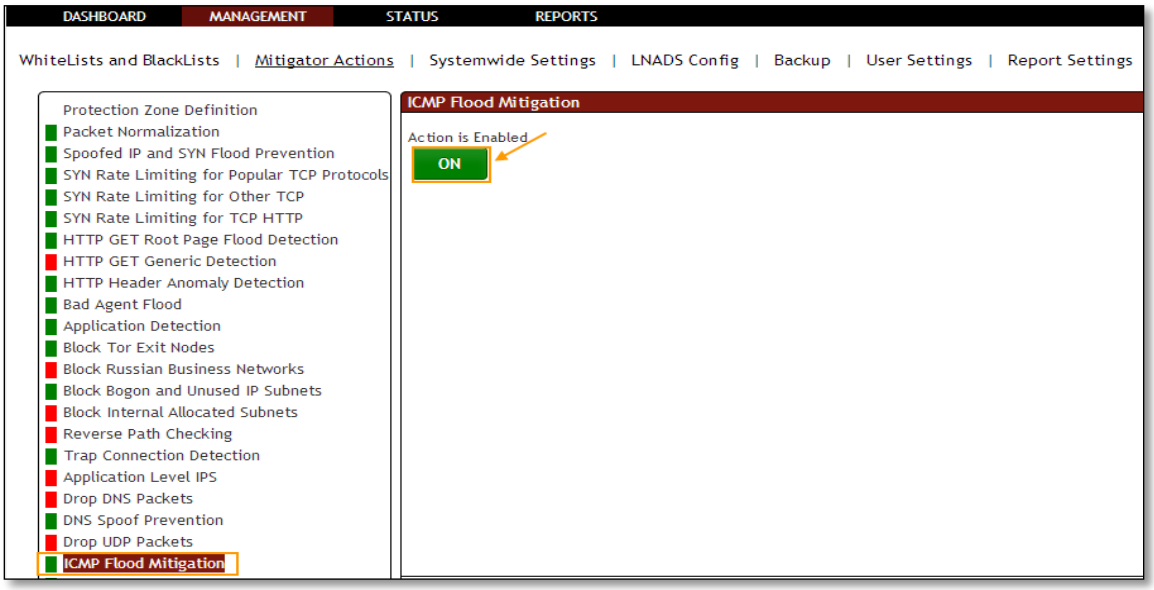



### 1.3.3.23 ICMP Flood Mitigation

**Rule F24:** ICMP Flood attacks.

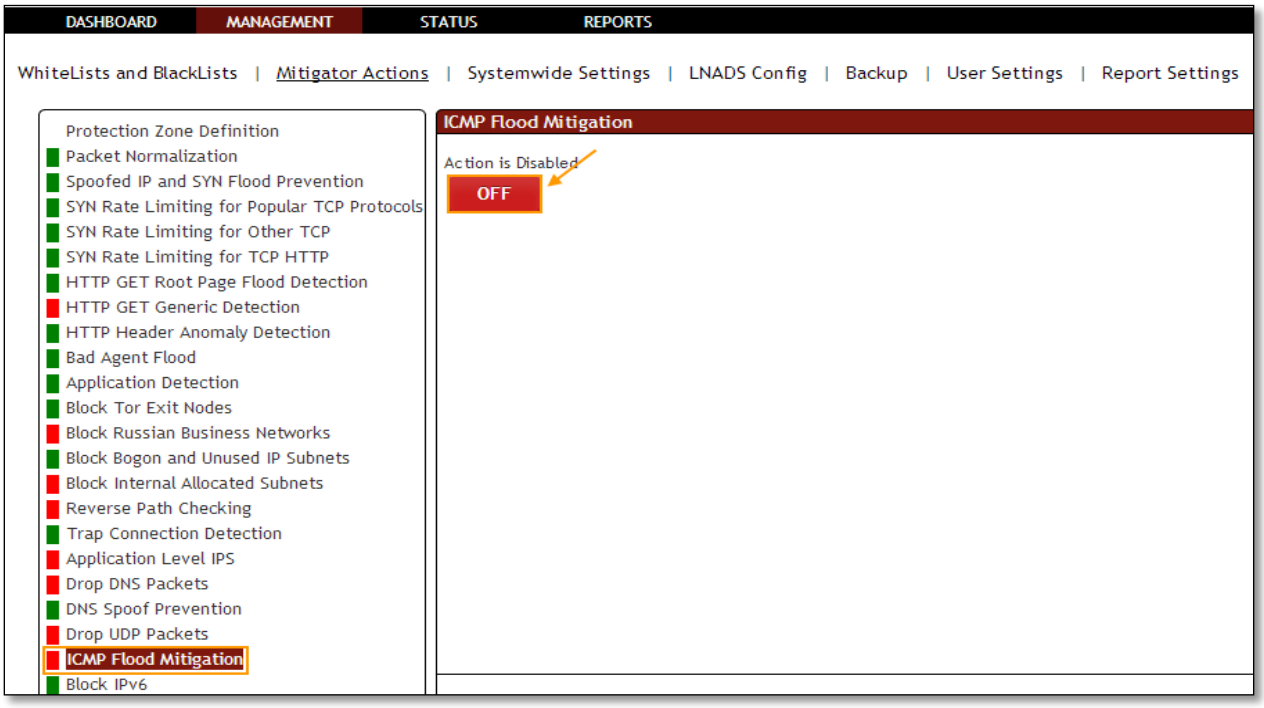
In **ICMP Flood Mitigation** tab we have an option to **Enable / Disable the option**.

ICMP Flood Mitigation Action is **Enabled** for mitigation of ICMP floods, it is in **ON** state.



Click on the same action tab to disable the option.

ICMP Flood Mitigation Action is **Disabled**, it is in **OFF** state.

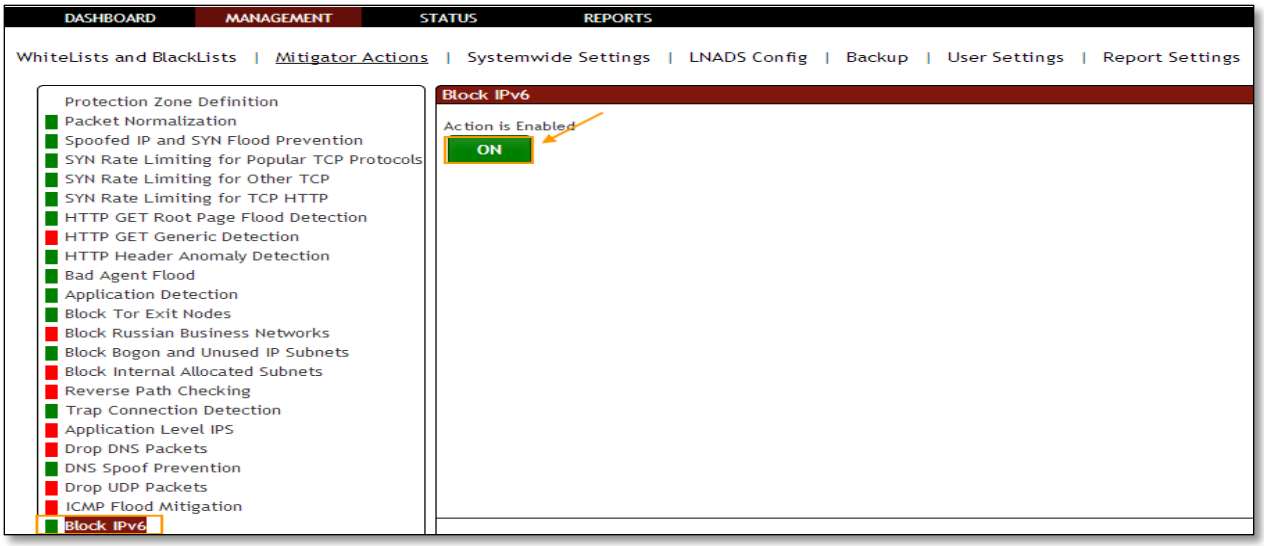



### 1.3.3.24 Block IPv6

**Rule F28:** Prevents the IPv6 addresses.

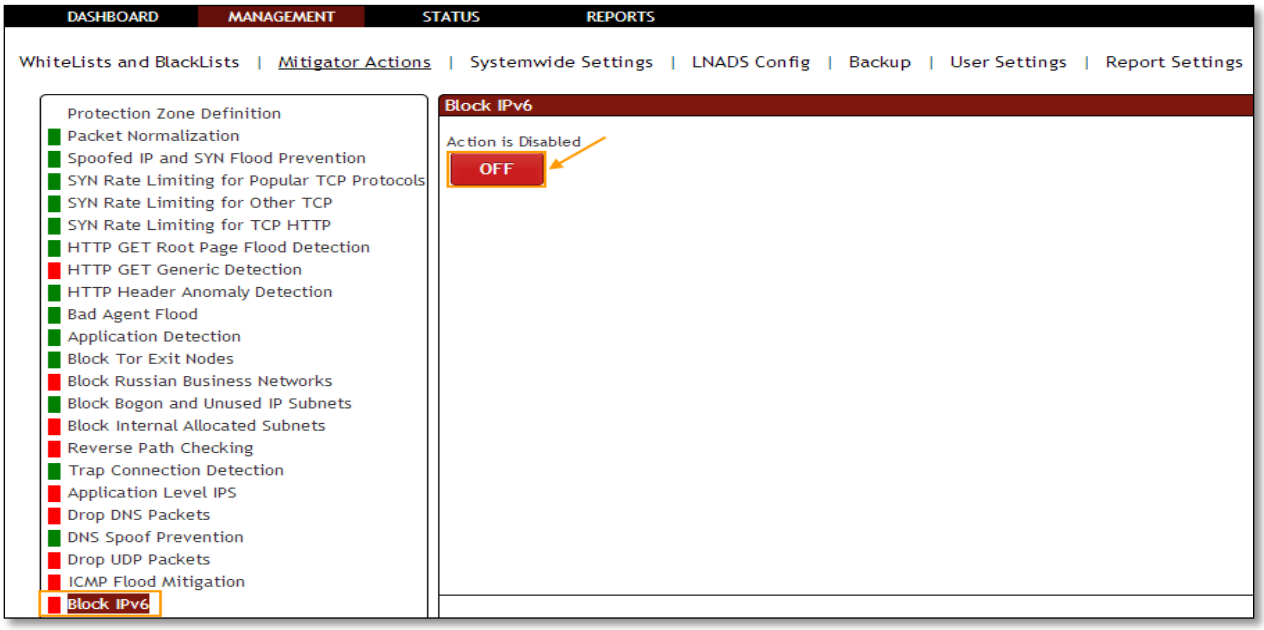
In **Block IPv6** tab we have an option to **Enable / Disable the option**.

Block IPv6 Action is **Enabled** for Blocking IPv6 completely, it is in **ON** state.



Click on the same action tab to disable the option.

Block IPv6 Action is **Disabled**, it is in **OFF** state.

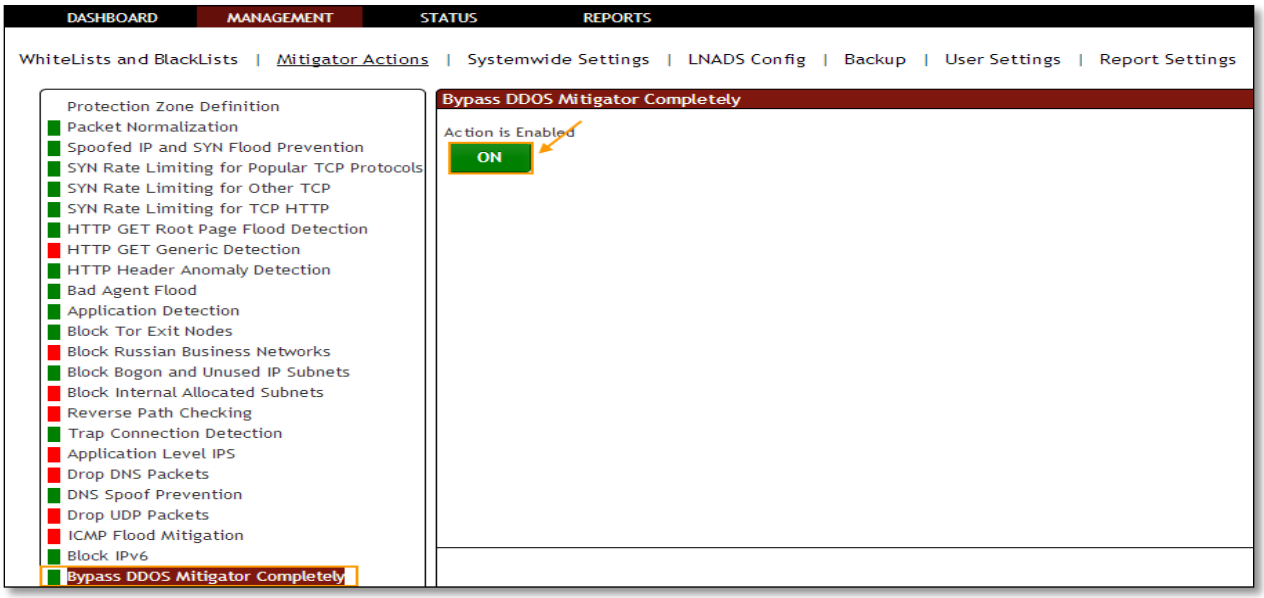



### 1.3.3.25 Bypass DDOS Mitigator Completely

**Rule F30:** DDoS prevention system disables.

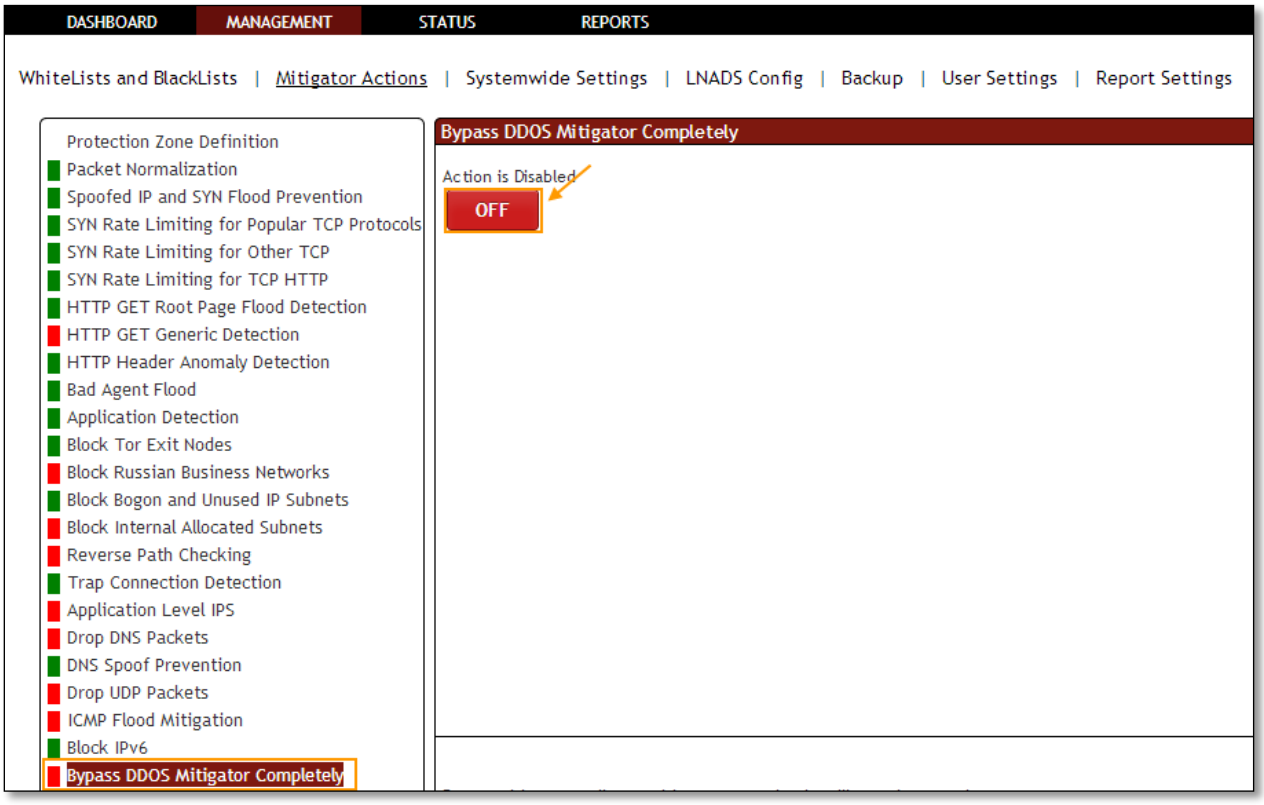
In **Bypass DDOS Mitigator Completely** tab we have an option to **Enable / Disable the option**.

Bypass DDOS Mitigator Completely Action is **Enabled**, it is in **ON** state.



Click on the same action tab to disable the option.

Bypass DDOS Mitigator Completely is **Disabled**, it is in **OFF** state.

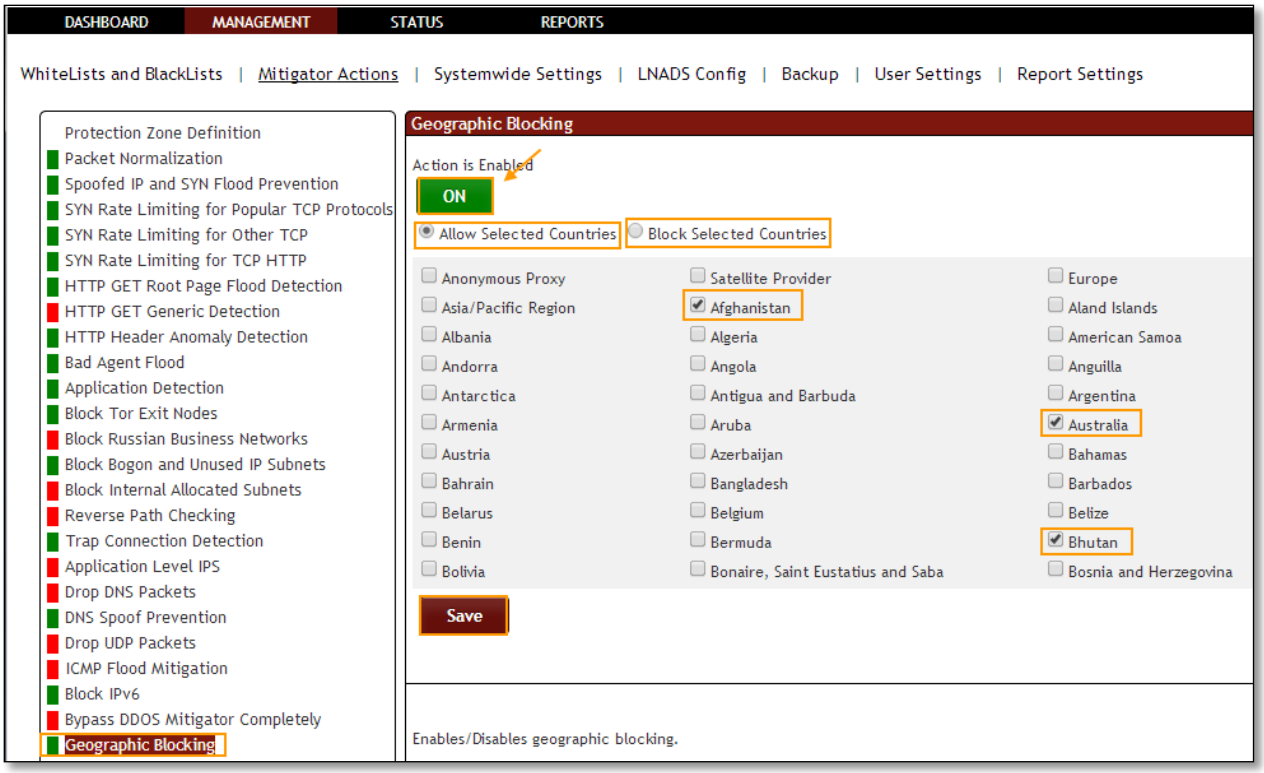



### 1.3.3.26 Geographic Blocking

In **Geographic Blocking** tab we have an option to **Enable / Disable the option**.

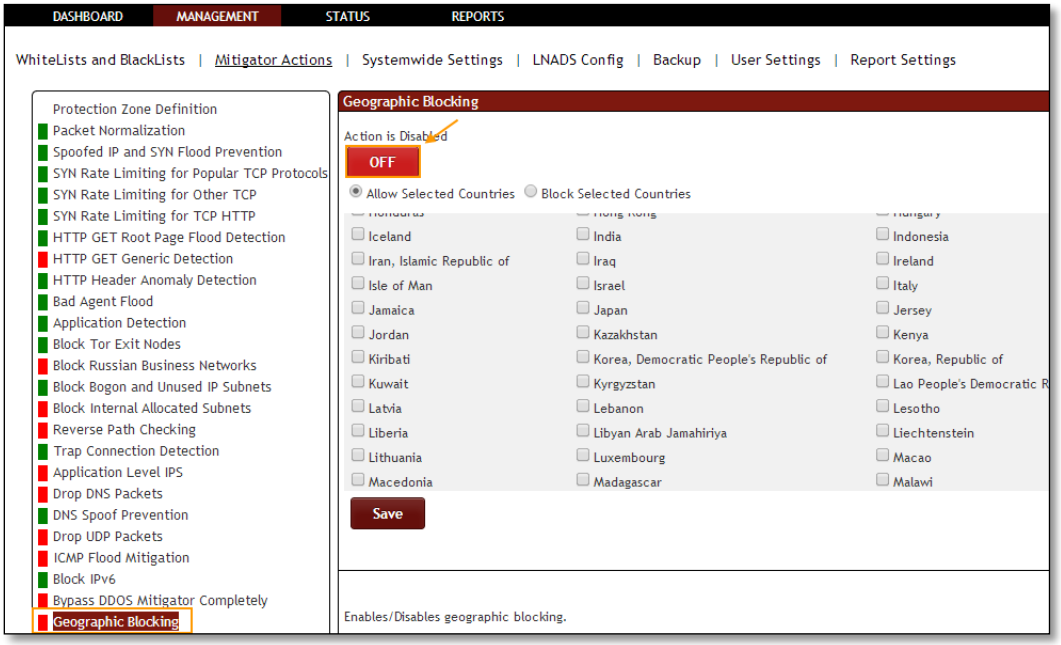
Geographic Blocking Action is **Enabled** for Allowing or Blocking selected list of Countries, it is in **ON** state.

Choose one of the preferred radio buttons for the selected countries and click on **Save** tab.



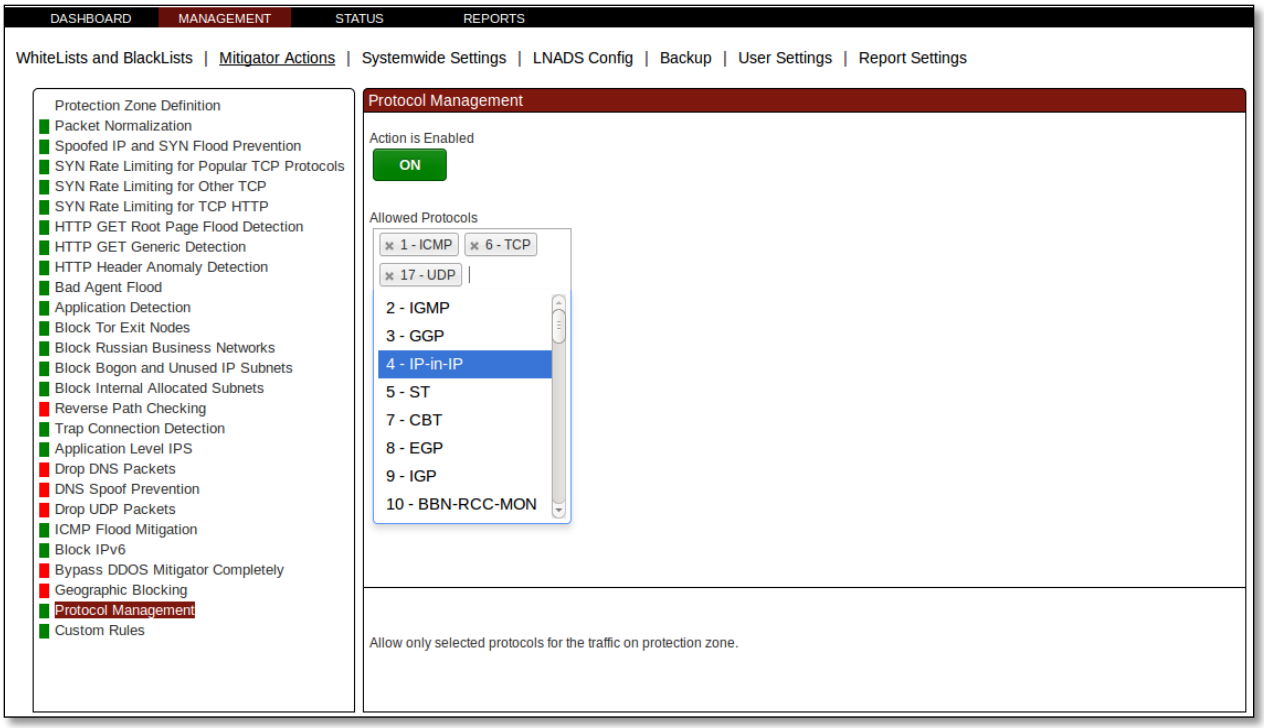

Click on the same action tab to disable the option.

Geographic Blocking Action is **Disabled**, it is in **OFF** state.



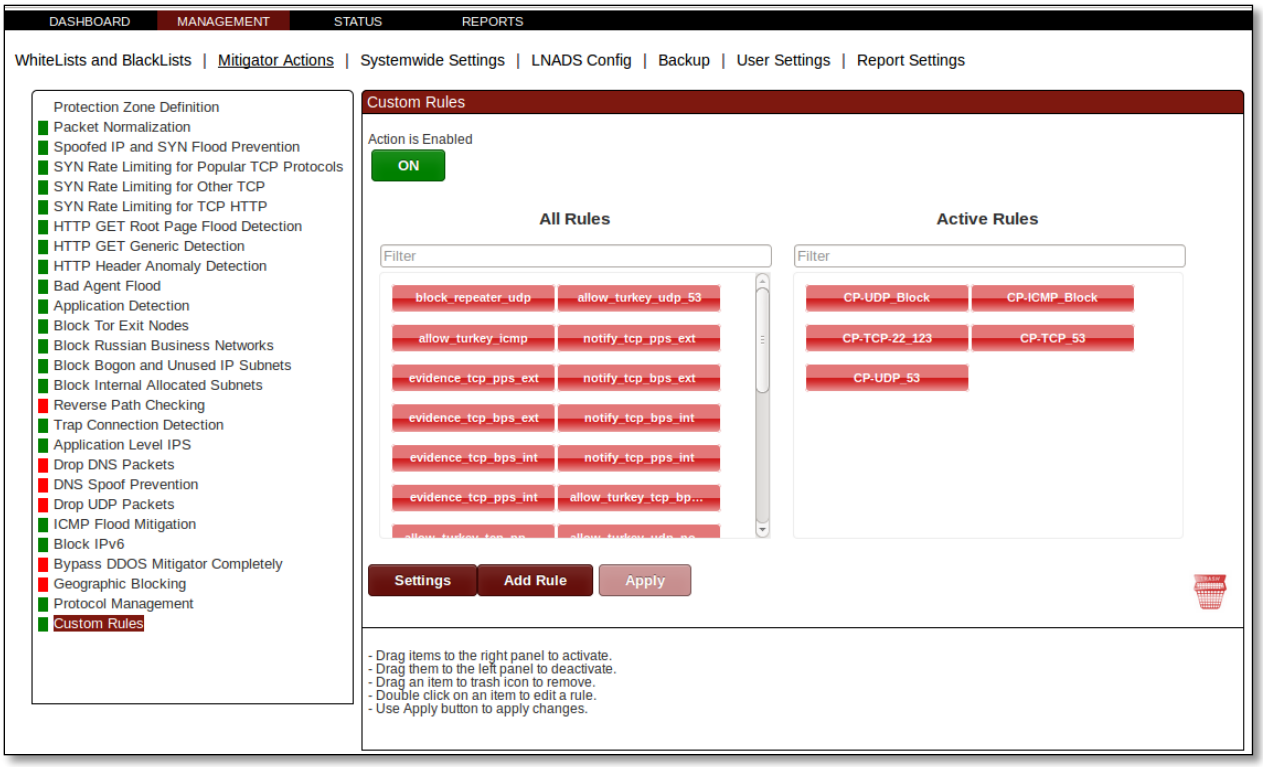
### 1.3.3.27 Protocol Management

In **Protocol Management** tab we have an option to **block** specified protocols. To activate, choose protocols to be allowed and click **Enable/Disable** button. If action is already enabled, clicking to **Save** button will be enough.




### 1.3.3.28 Custom Rules

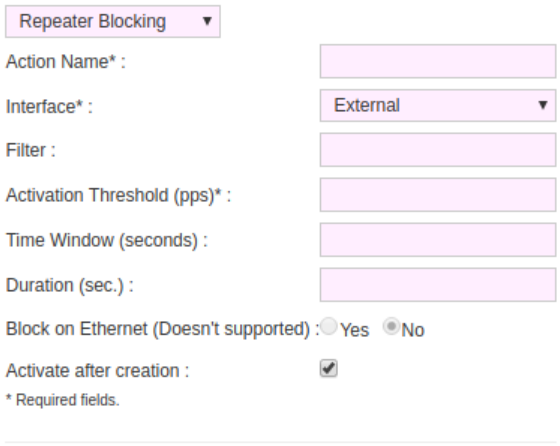
Custom rules tab can be used to create advanced rules that monitor the environment and perform actions when the specified conditions are met. ON/OFF button is used to start or stop all the custom rules that have been created. Filter control can be used to search custom rules. Settings window can be used to specify the log level of the running custom rules. A new custom rule can be added to the system by clicking the Add Rule button. Currently, there are 9 custom rule types:




#### 1.3.3.27.1 Repeater Blocking

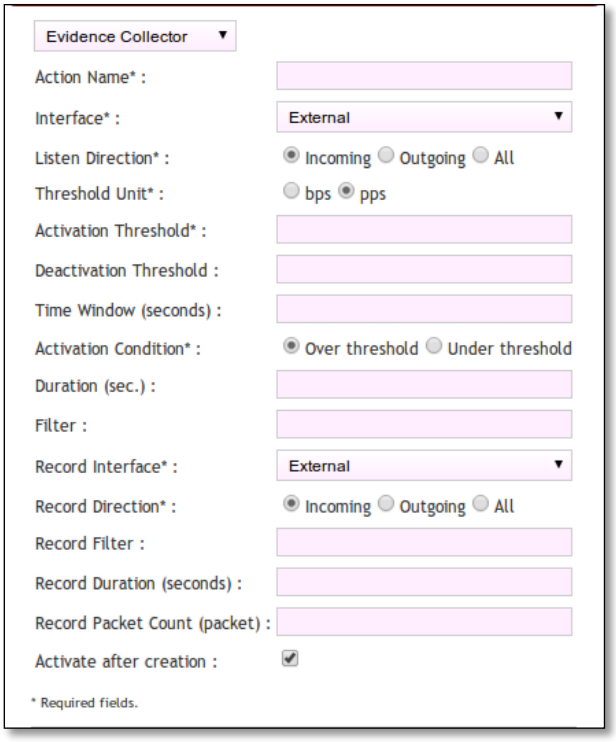
Repeater Blocking rule monitors the network traffic on the specified interface and direction. If it detects any IP's which are sending packets to a specific IP, port pair at a rate which is above the specified Activation Threshold, the sender IP is blocked.

If Block on Ethernet option is available and selected as yes, the attacker will be blocked on Ethernet device.




### 1.3.3.27.2 Evidence Collector

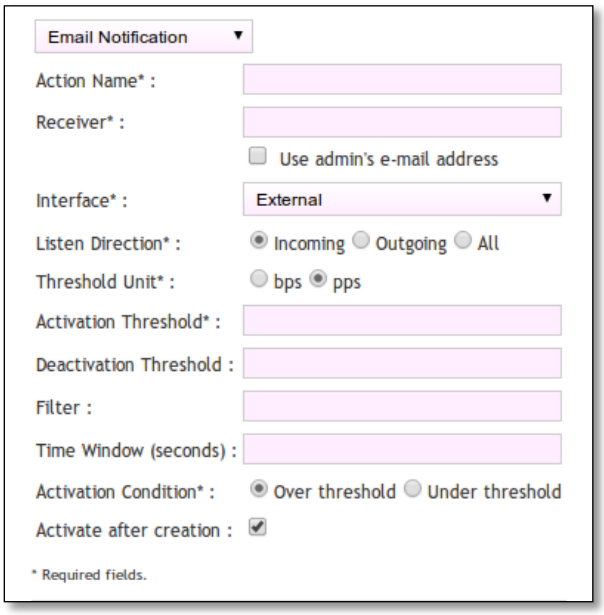
Evidence Collector rule monitors the network traffic rate on the specified interface and direction. If the network traffic rate exceeds the specified Activation Threshold, the traffic is recorded into the pcap files based on the specified filter. It's also possible to trigger this rule in case the network traffic rate is below the specified Activation Threshold.




### 1.3.3.27.3 Email Notification

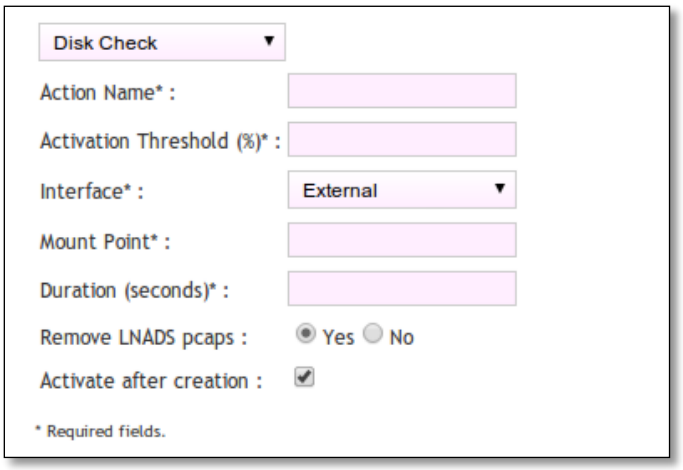
Email Notification rule monitors the network traffic rate on the specified interface and direction. If the network traffic rate exceeds the specified Activation Threshold, an email will be

sent to the Receiver email address. It's also possible to trigger this rule in case the network traffic rate is below the specified Activation Threshold.



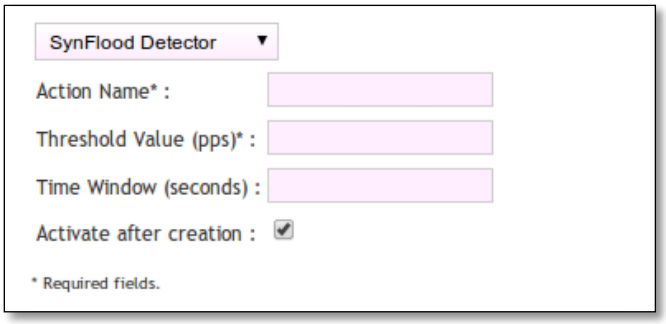

### 1.3.3.27.4 Disk Check

Disk Check rule monitors the used disk space percentage on the specified Mount Point. If the used disk space percentage exceeds the specified Activation Threshold, pcap recording will be stopped on the specified network interface. In addition, optionally, the pcaps already created by LNADS will be removed from the system.



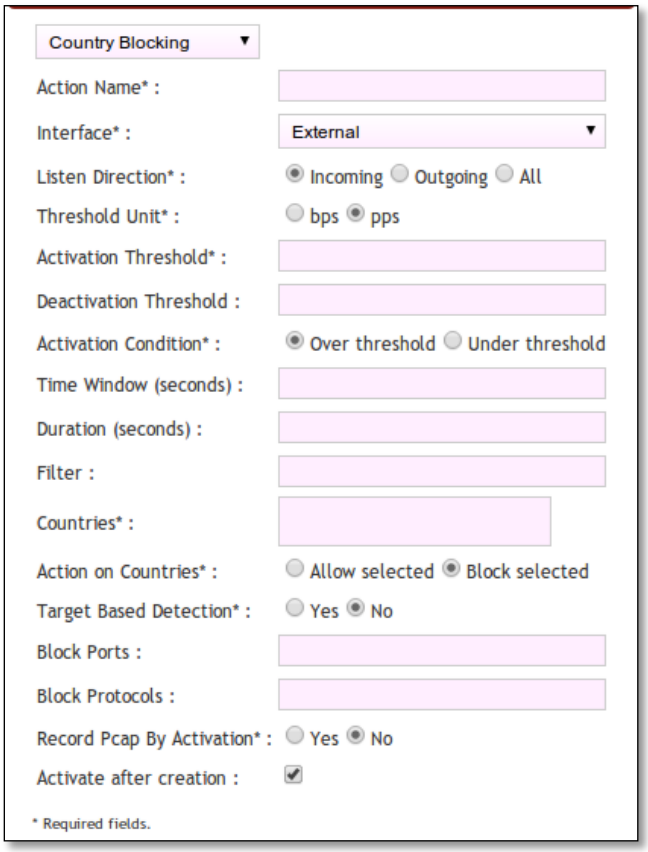
#### 1.3.3.27.5 SynFlood Detector

Syn Flood Detector rule monitors the Syn flood rate. If Syn attack with a rate bigger than the specified threshold is detected, this attack is reported on the Reports page.



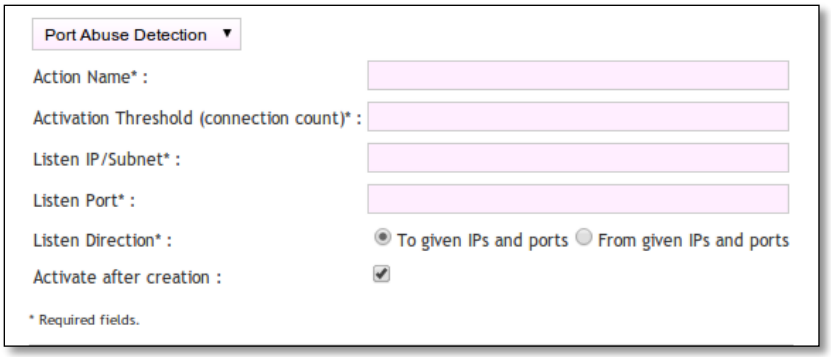

#### 1.3.3.27.6 Country Blocking

Country Blocking rule monitors the network traffic rate on the specified interface and direction. If the traffic rate exceeds the specified Activation Threshold, either the selected countries are blocked or only the selected countries are allowed based on user's selection. If the Target Based Detection is enabled, country blocking/allowing action will only be performed on the specific source IP that attacks a target IP instead of all the source IP's.



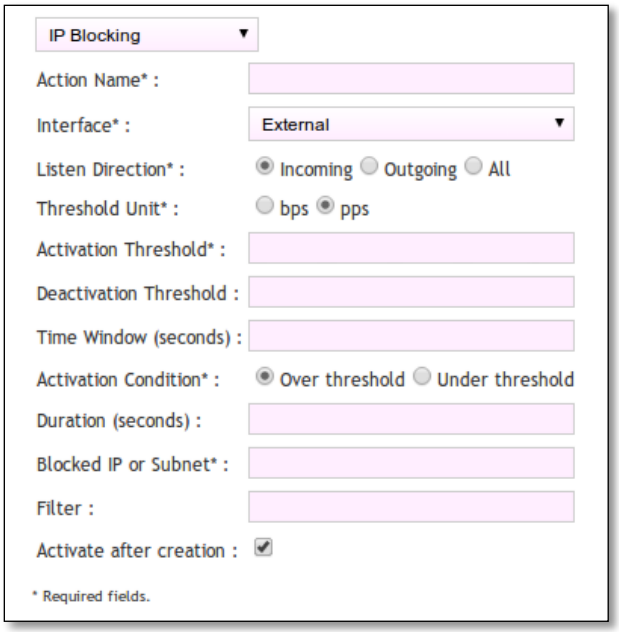
#### 1.3.3.27.7 Port Abuse Detection

Port Abuse Detection rule monitors the number of connections between the external IPs and the specified internal IP/subnet and port. If the number of connections exceeds the specified Activation Threshold, the external IP's are blocked.



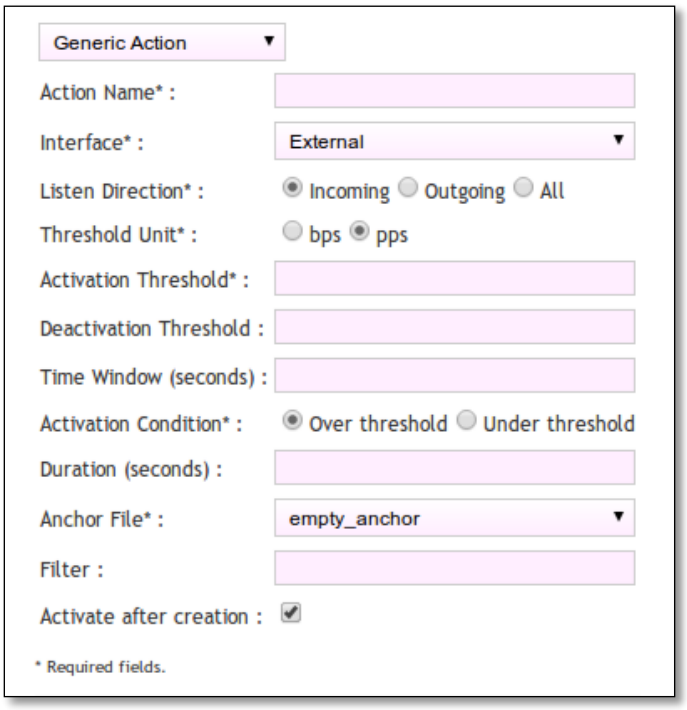

#### 1.3.3.27.8 IP Blocking

IP Blocking rule monitors the network traffic rate on the specified interface and direction. If the network traffic rate exceeds the specified Activation Threshold, the specified IP/subnet is blocked for the given time interval. If Record Pcap By Activation is enabled, a pcap file is created from the network traffic.



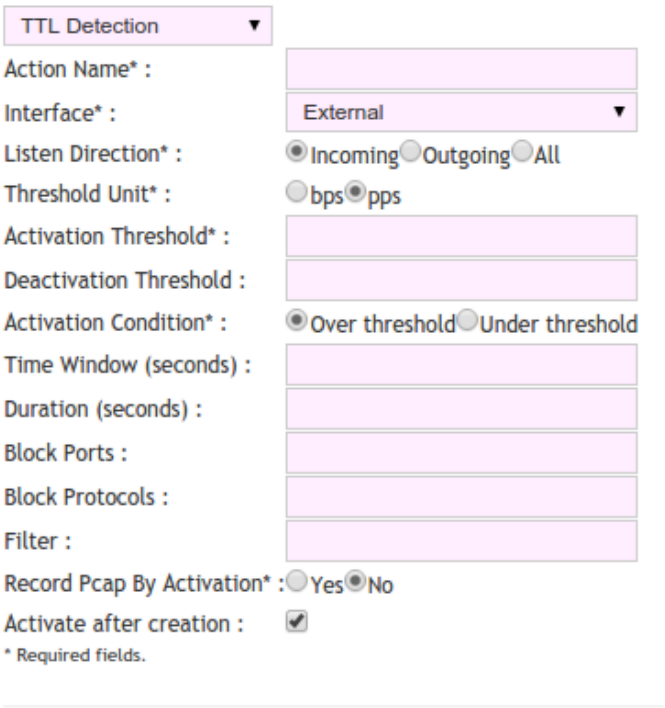
#### 1.3.3.27.9 Generic Action

Generic Action rule monitors the network traffic rate on the specified interface and direction. If the amount of traffic exceeds the specified Activation Threshold, the selected anchor file is activated during the given time duration. If Record Pcap By Activation is enabled, a pcap file is created from the network traffic.




#### 1.3.3.27.10 TTL Detection Action

TTL Detection rule monitors the network traffic rate on the specified interface and direction. If the amount of traffic based on TTL values exceeds the specified Activation Threshold, the packets which have the same TTL value is blocked during the given time duration. If Record Pcap By Activation is enabled, a pcap file is created from the network traffic.

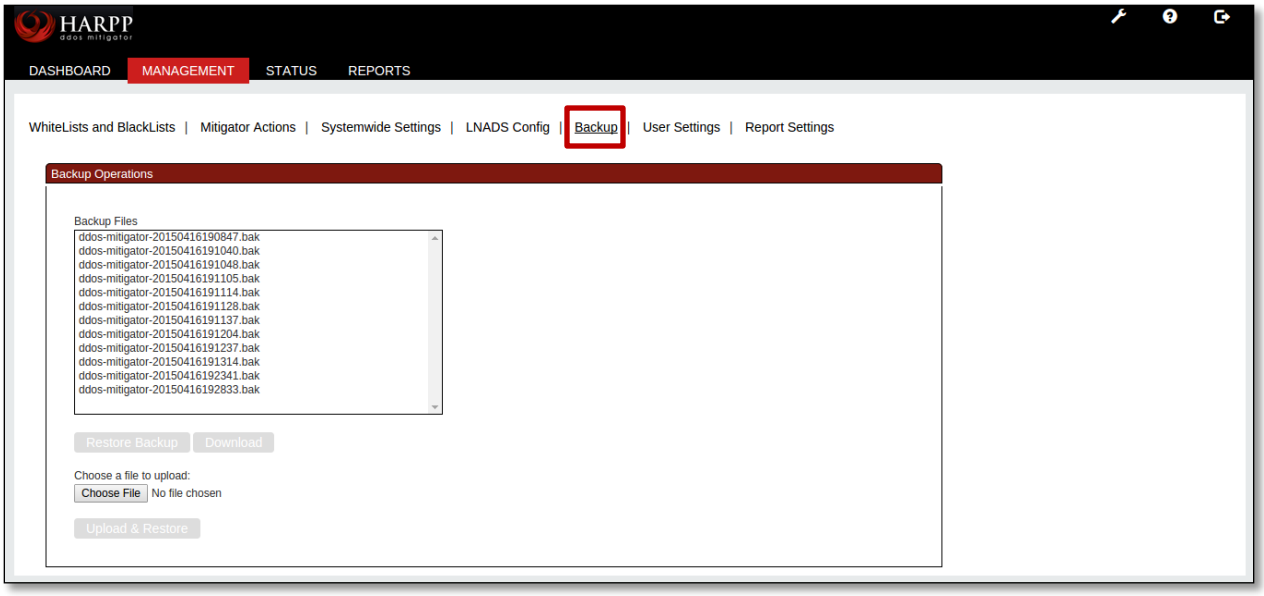



### 1.3.4. Backups

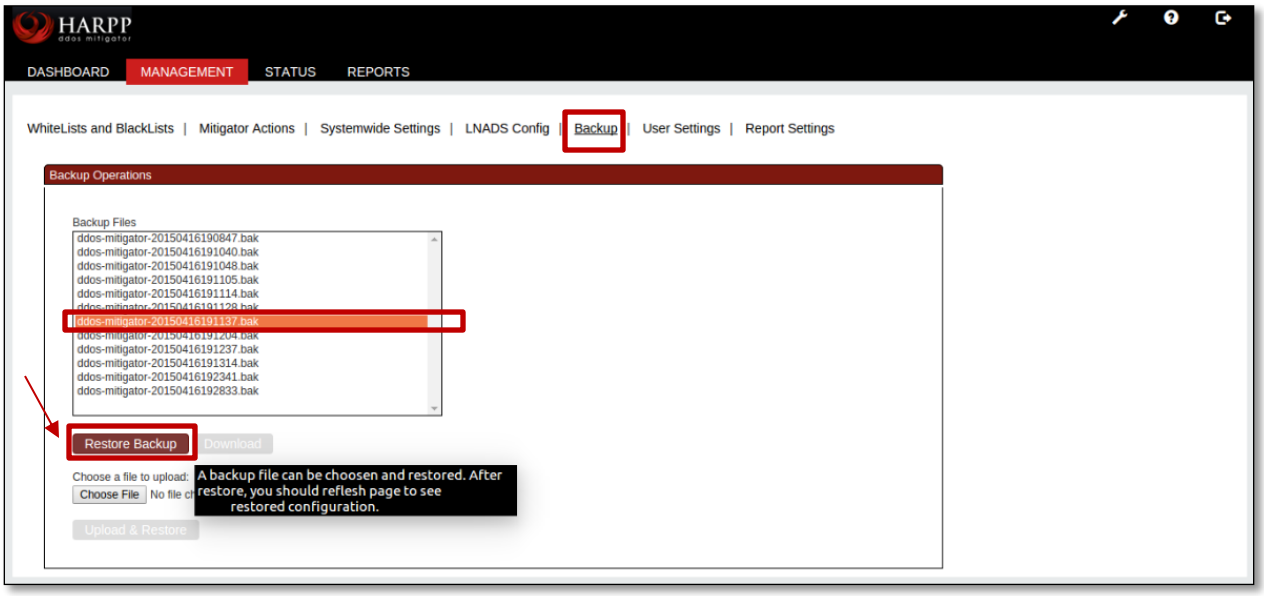
Back up tab in DDOS mitigator provides us with options like **Restore, Download, Upload & Restore** the files from / to the DDOS mitigator.

After each change, device will backup automatically.

In management section, select **backup** tab.

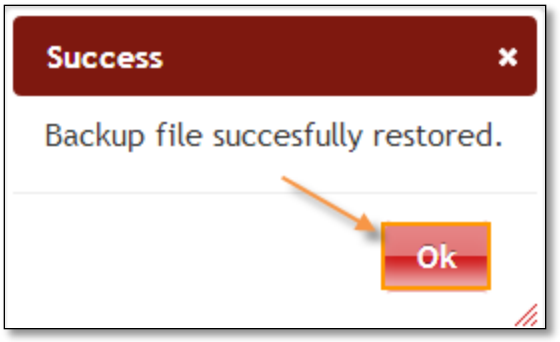



If we want to restore any back up file select the file from the list and click on **Restore Backup** option.



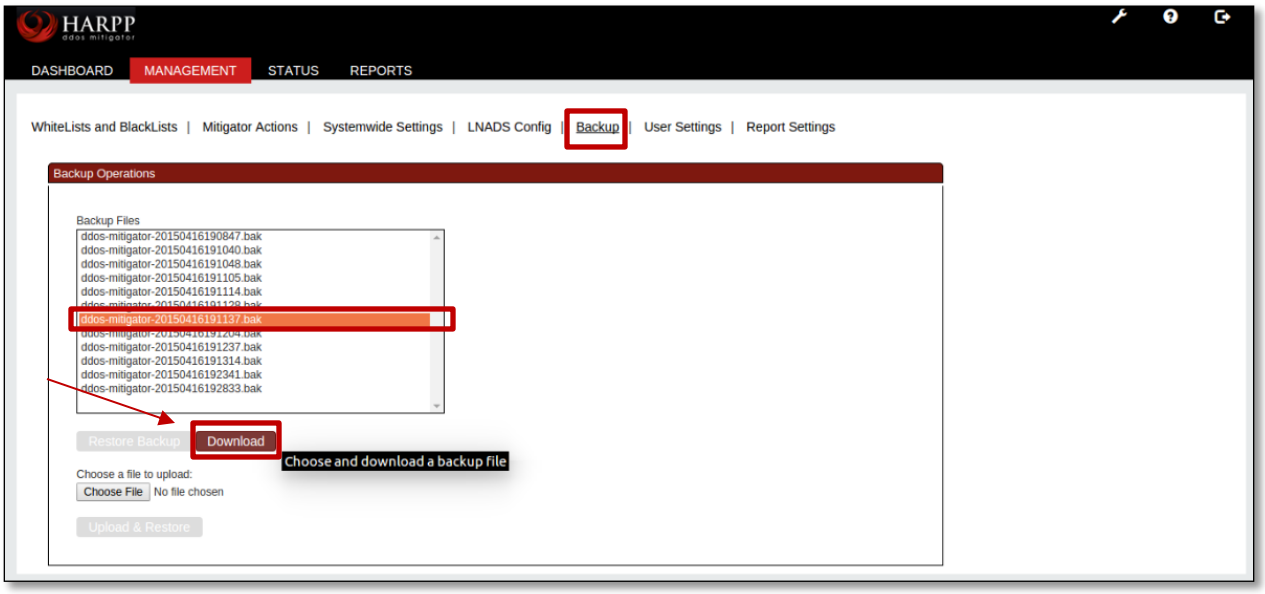

After few seconds Success screen is displayed stating that **Backup file successfully Restored**. Click **Ok**

Refresh the screen to find the restored file.



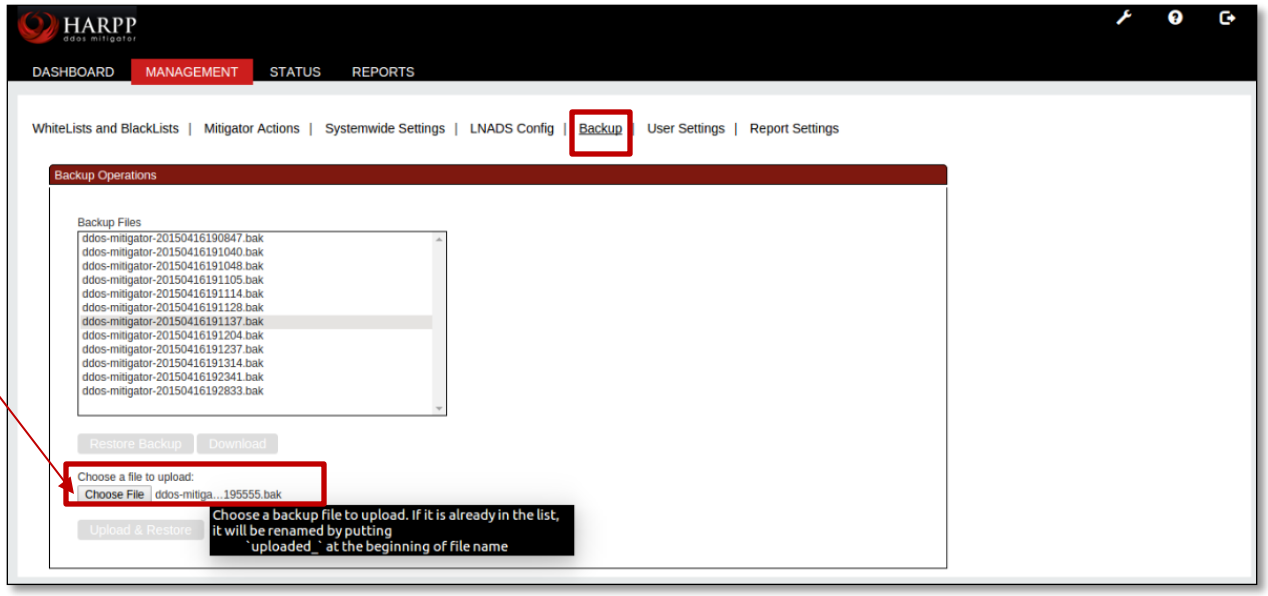

Select a backup file from the list and click on **Download** option to download the file in to our local machine.

In the below screen you can find the downloaded file.




If we want to upload or restore any files in to this list we can choose the file and upload it using the upload & restore option.

Click on **Choose File** option to select the file.



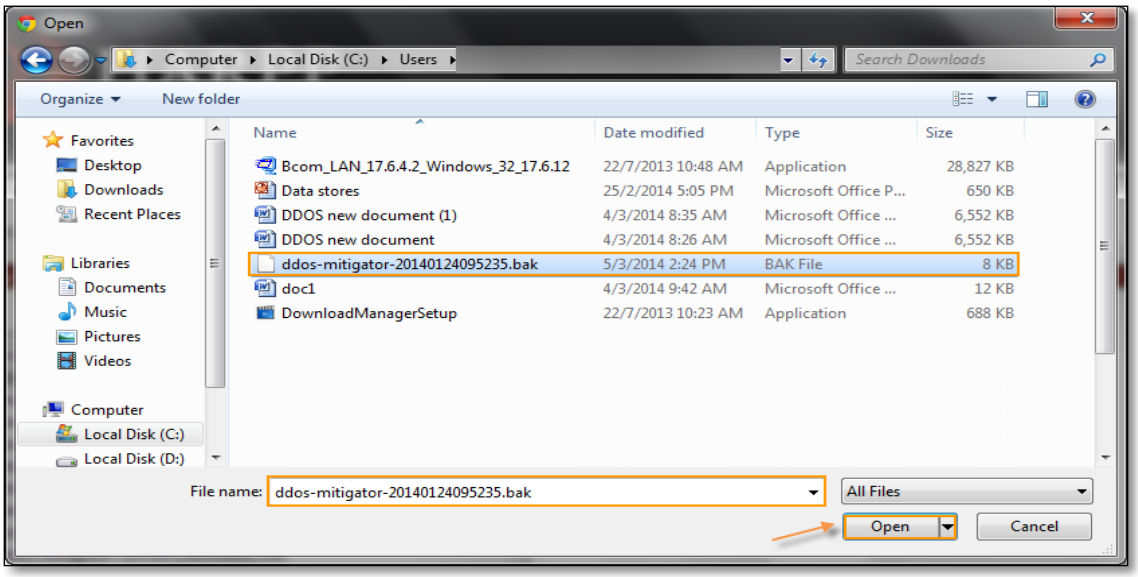

Now browse to the location where your file is located.

In the below screen, we have navigated to downloads folder and selected the **.bak** file.

Click on **Open**

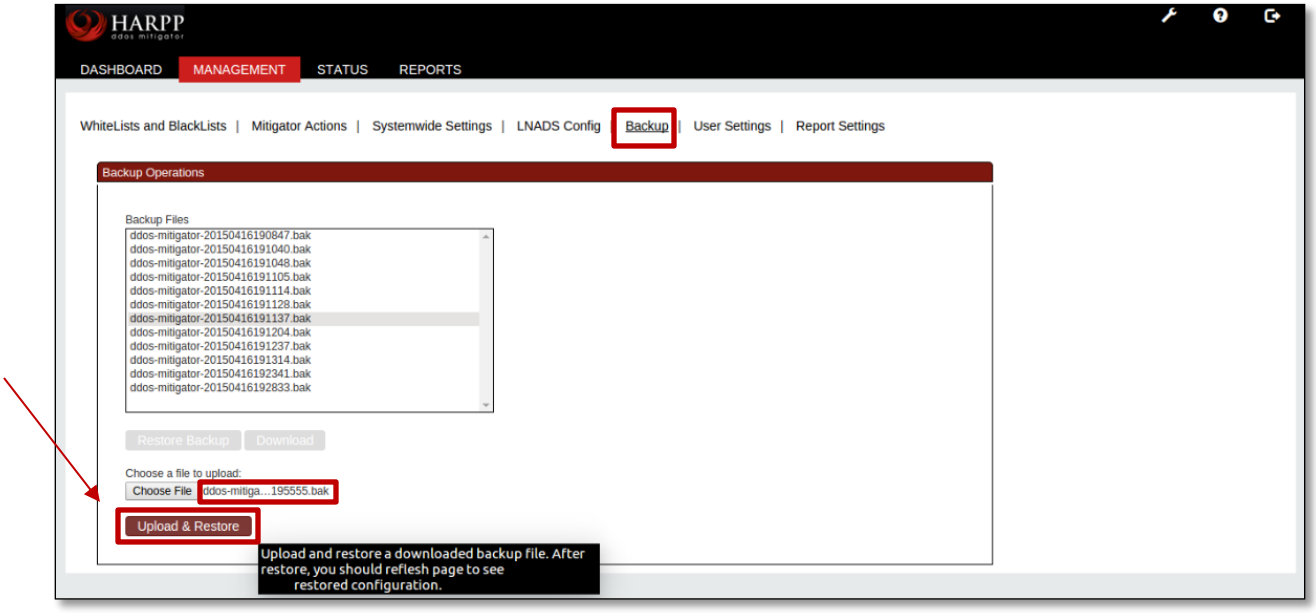
Note

- *The files with the extension of **.bak** only can be uploaded.*

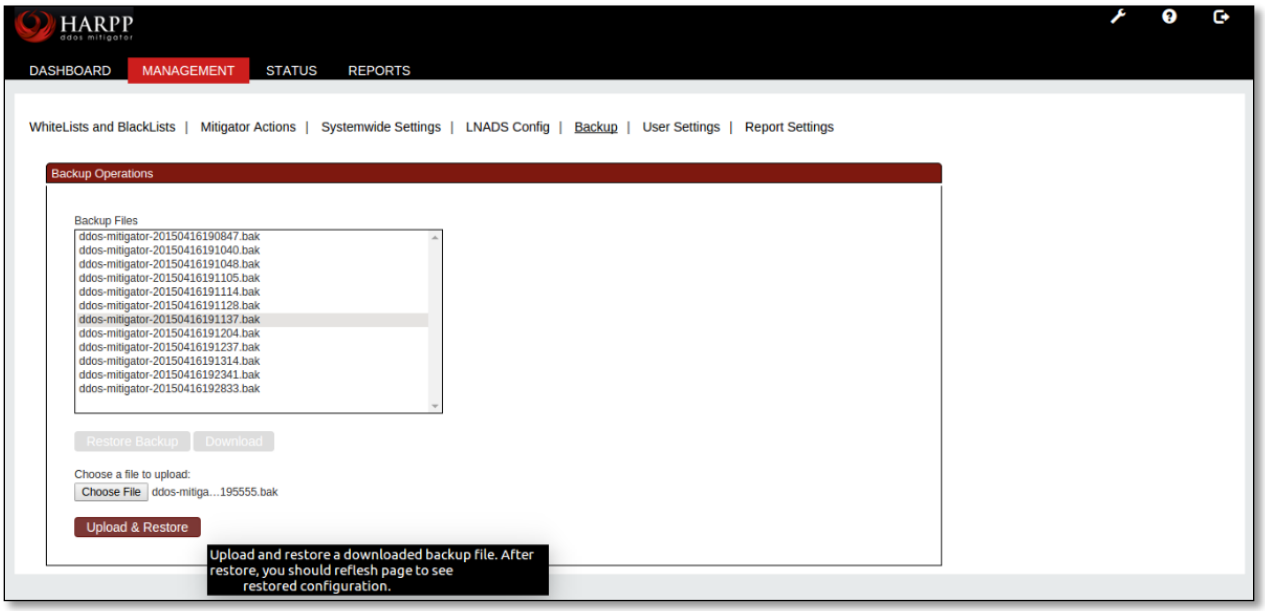


In the below screen you can find the file is selected.

Click on **Upload & Restore** option to Upload the file in this list.




You can find the selected file is successfully uploaded.



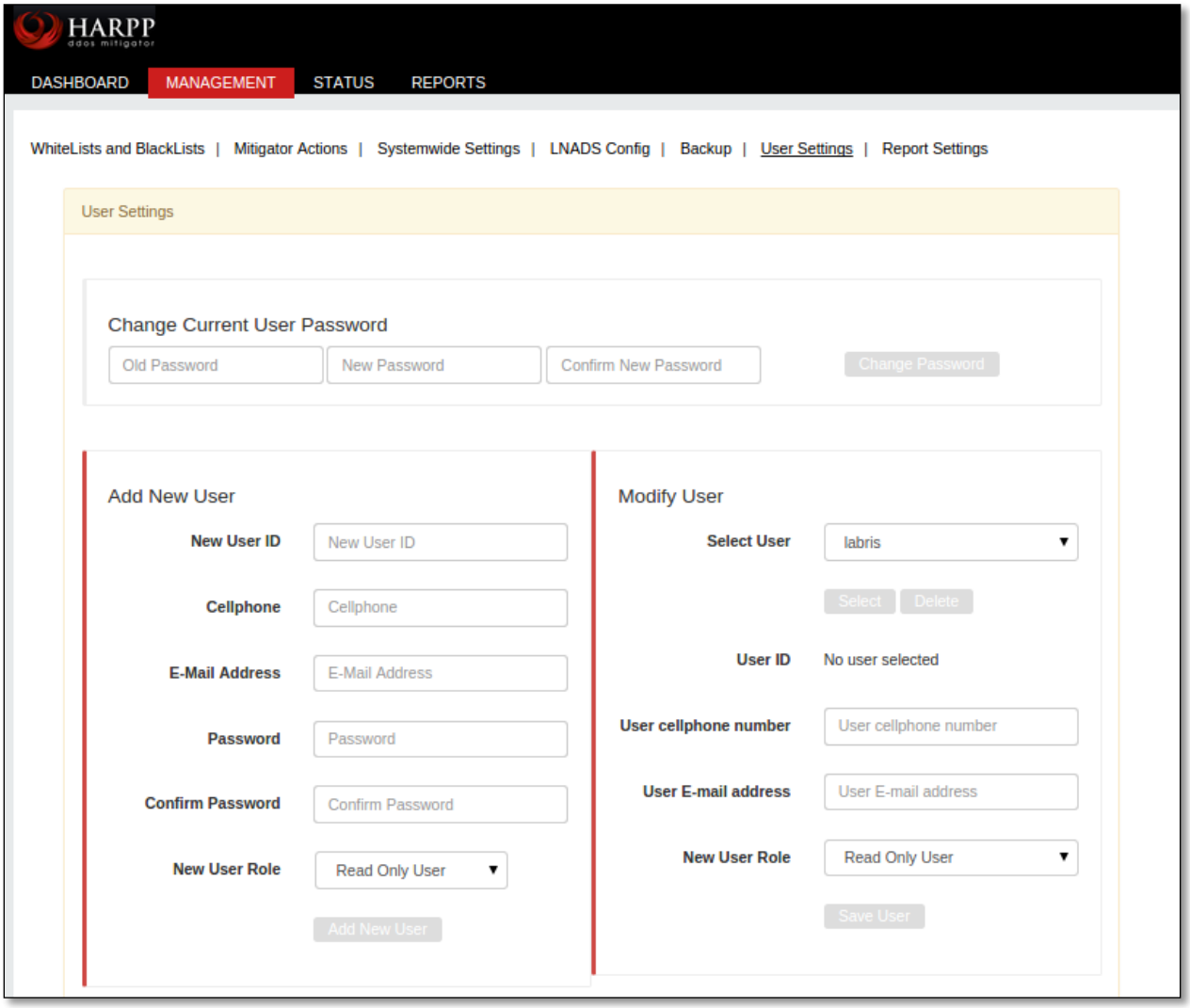

### 1.3.5. LNADS Settings

For LNADS settings please refer section 2 (Labris Network Anomaly Detection System)

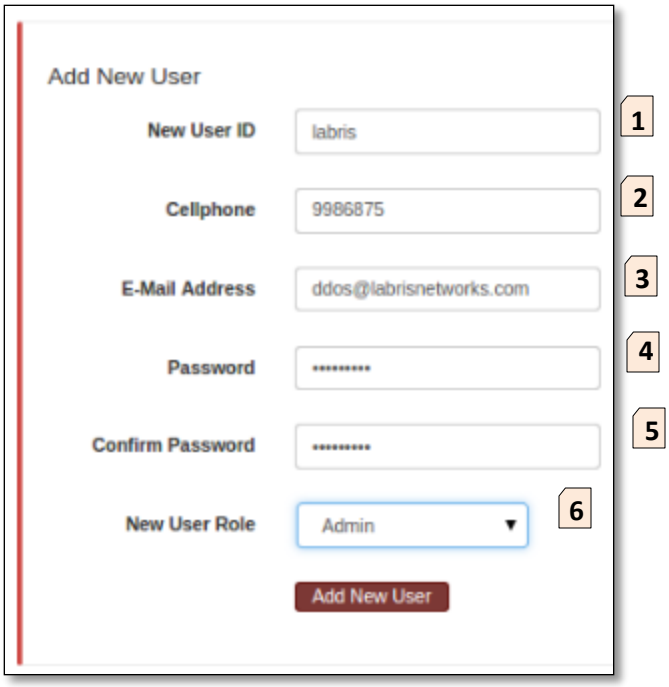
### 1.3.6. User Settings

User Settings tab consists of four fields, which are Add New User, Change Current User Password, Modify User, Modify User Information.

It enables us to add new user, changing Current User password, Modifying Users which are existing and also Modifying User Information.



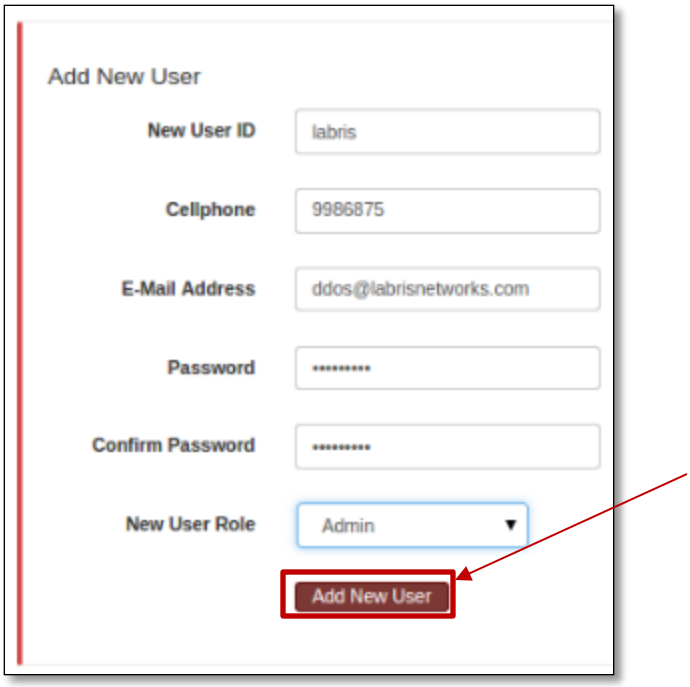

**Adding New User**



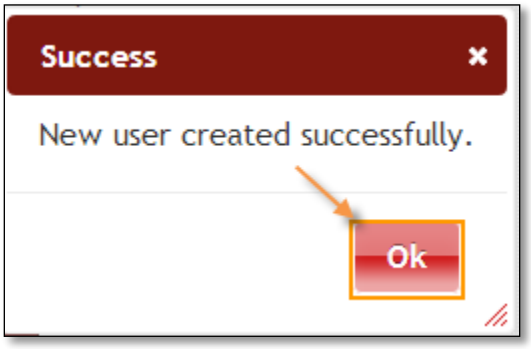

These are the inputs to add New User.

| | | |
|---|---|---|
| 1 | **New User ID** | Type the New User ID |
| 2 | **Cell phone** | Give the mobile number of the User |
| 3 | **E-mail Address** | Give the E-mail Address of the User |
| 4 | **New User Password** | Type the Password of the User |
| 5 | **Confirm New User Password** | Retype the Password of the user |
| 6 | **New User Role** | Select one of role of the New User from the drop down menu. |

Admin role is selected for the new User. Click on **Add New User** tab.

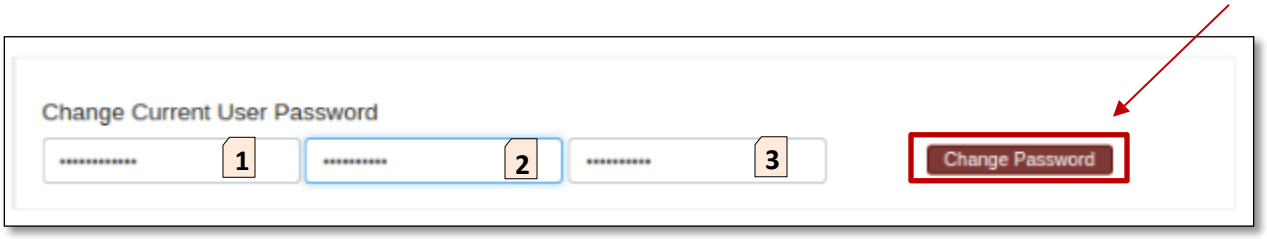



Success tab appears **Stating New User created successfully,** click on OK.




## Change Current User Password

For changing Password of the User we find three fields.

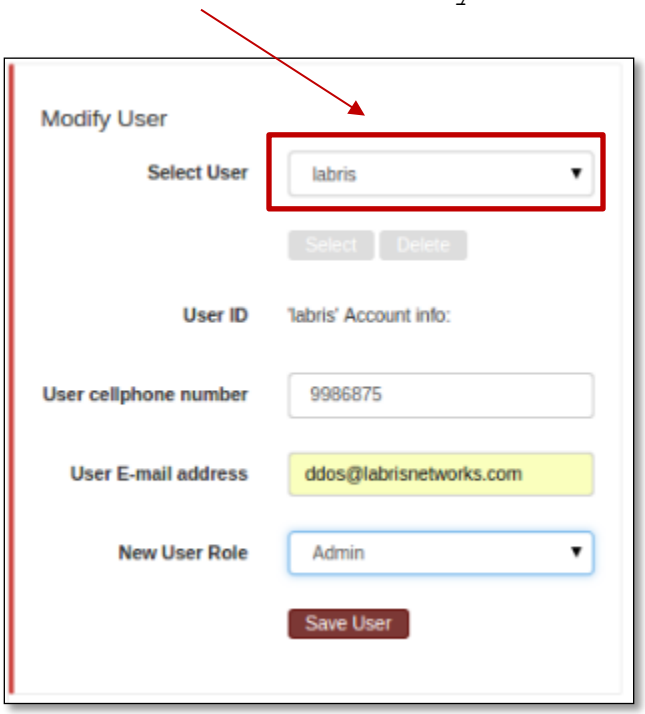


These are the inputs to change current User Password.

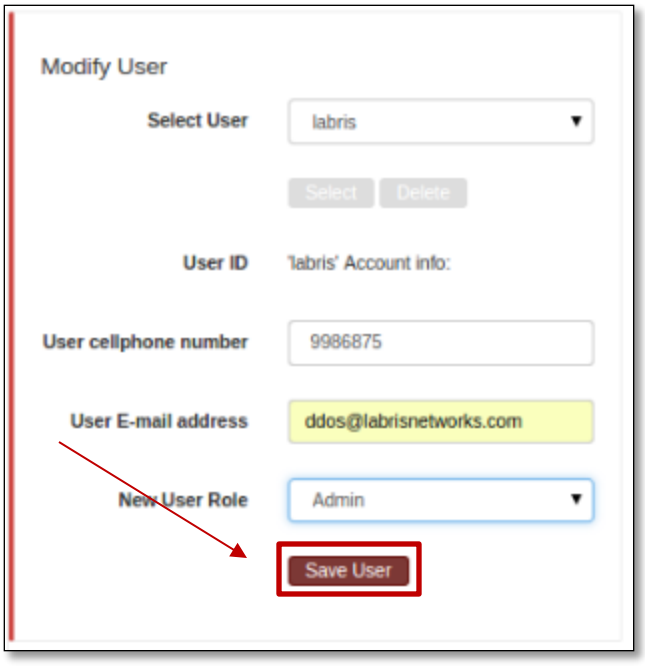
| | | |
|---|---|---|
| 1 | **Old Password** | Type the Old password of the User |
| 2 | **New Password** | Type the New Password |
| 3 | **Confirm New Password** | Confirm New Password |

### Modify User

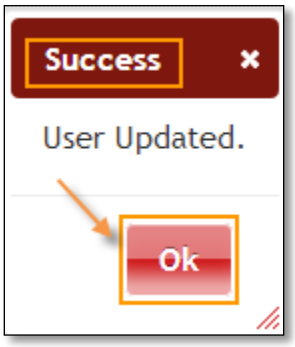
We can notice Users list under Modify User tab.
Select the User to Modify User Information.



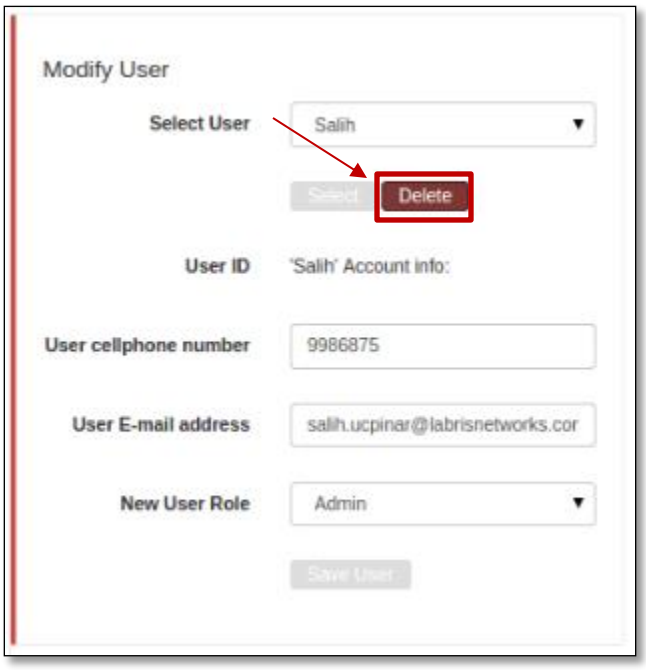

After click on Select tab we can notice User details appearing in the Modify User Information tab.
If necessary make changes to the User and click on **Save**tab to apply changes made to the User.



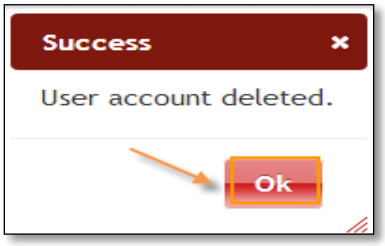

Success tab appears stating User Updated, click Ok.




Select the User and click on Delete tab.

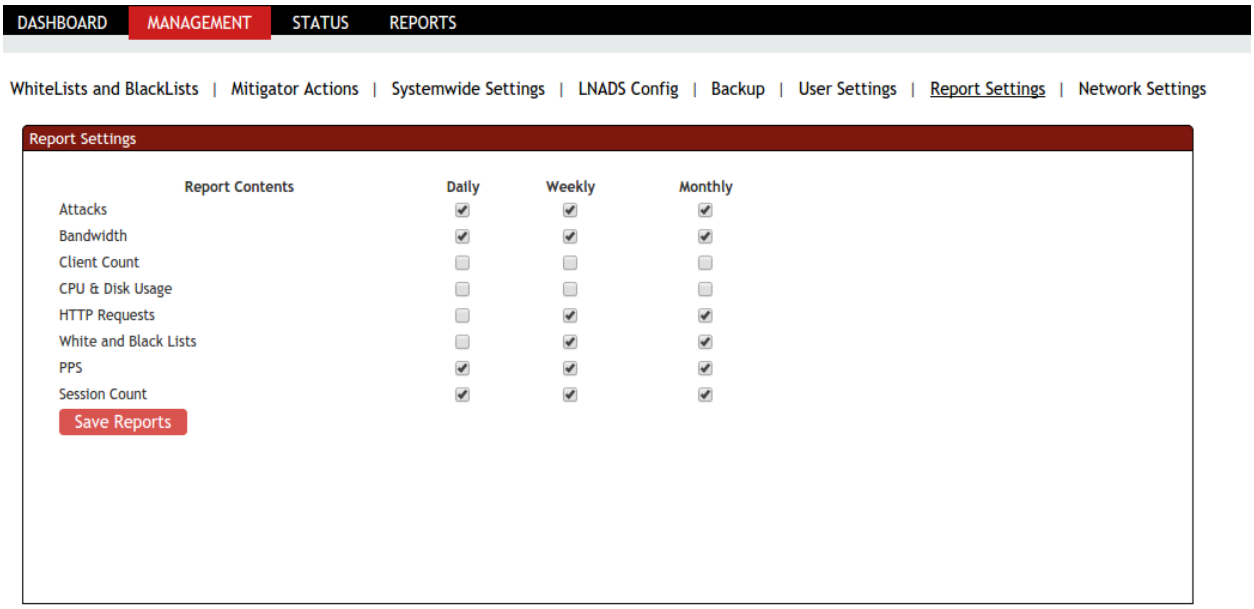



Success tab appears stating User account deleted, click on OK.




### 1.3.7. Report Settings

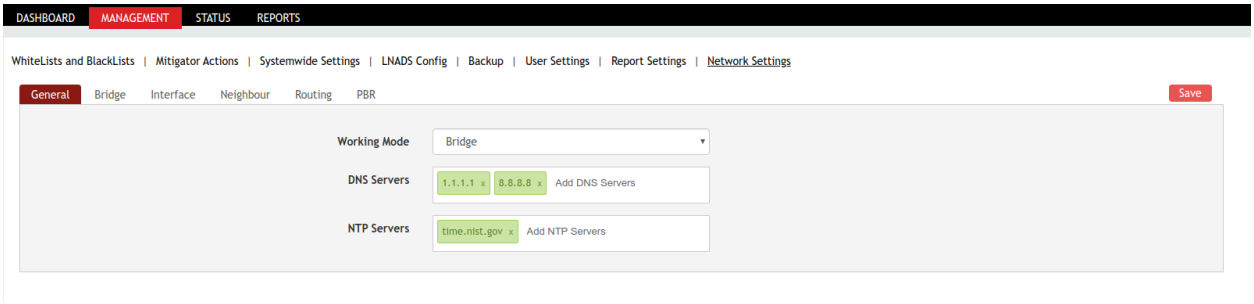
In Report Setting pane, we can configure contents of daily weekly and monthly reports separately.



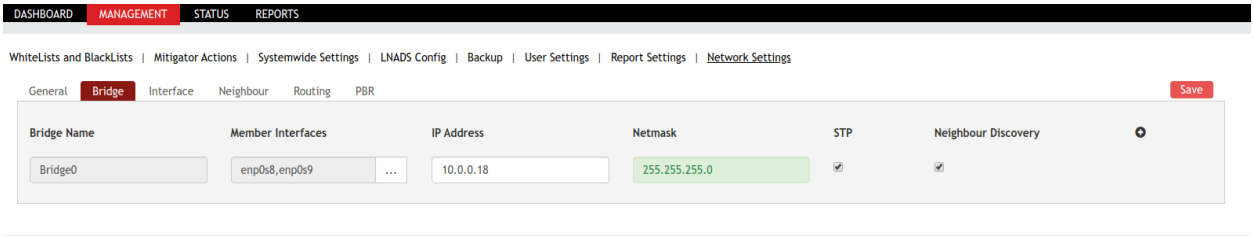

### 1.3.8. Network Settings

In Network Setting pane, we can modify network details.

On General tab working mode, DNS servers and NTP servers can be set. If Bridge is chosen as working mode, Bridge tab will be activated for configuration.

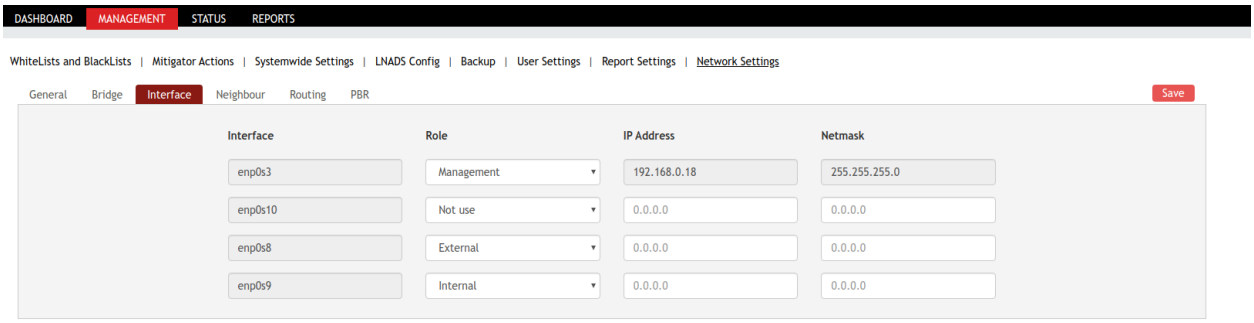



If working mode is selected as Bridge on Bridge tab, you can configure bridge members, IP and netmask, STP (Spanning Tree Protocol) and Neighbor discovery.

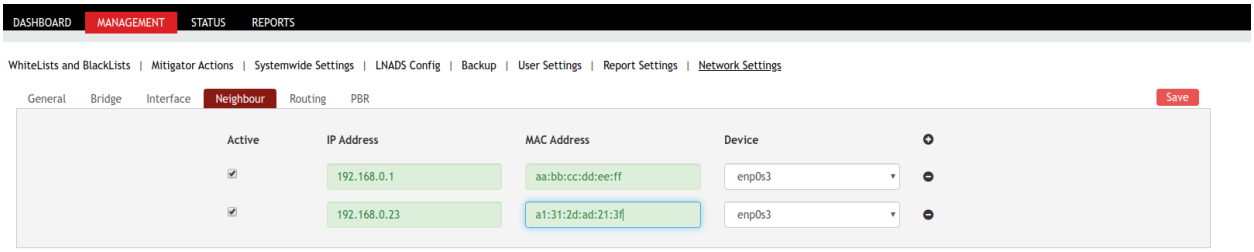



If you assign an IP address we recommend to deactivate neighbor discovery.

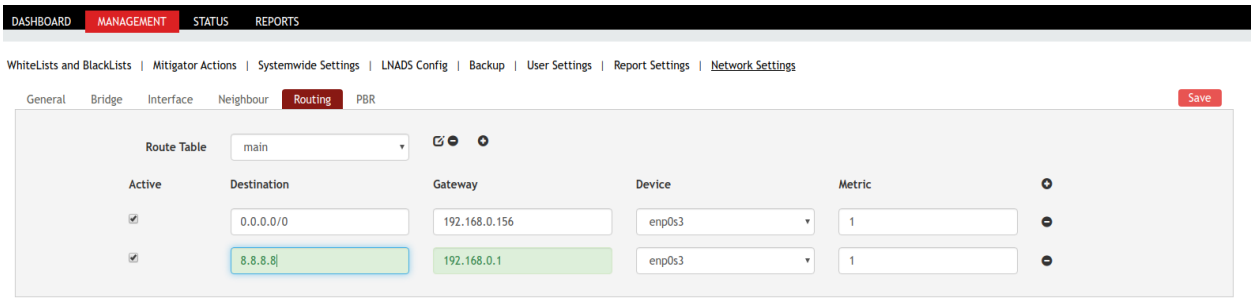
On Interface tab, you can configure interface roles, IP and netmask addresses. Note that every device should have set at least one of each management, external and internal interface.



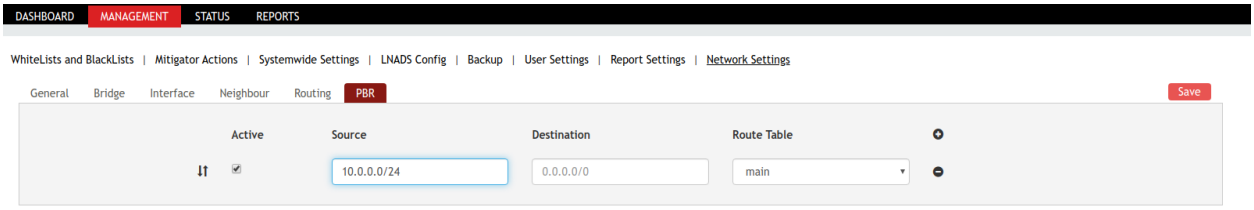

On Neighbor tab, you can define assign static mac addresses to neighbor devices.




On Routing tab, you can configure different routes and route tables. In most case just main table would be enough.



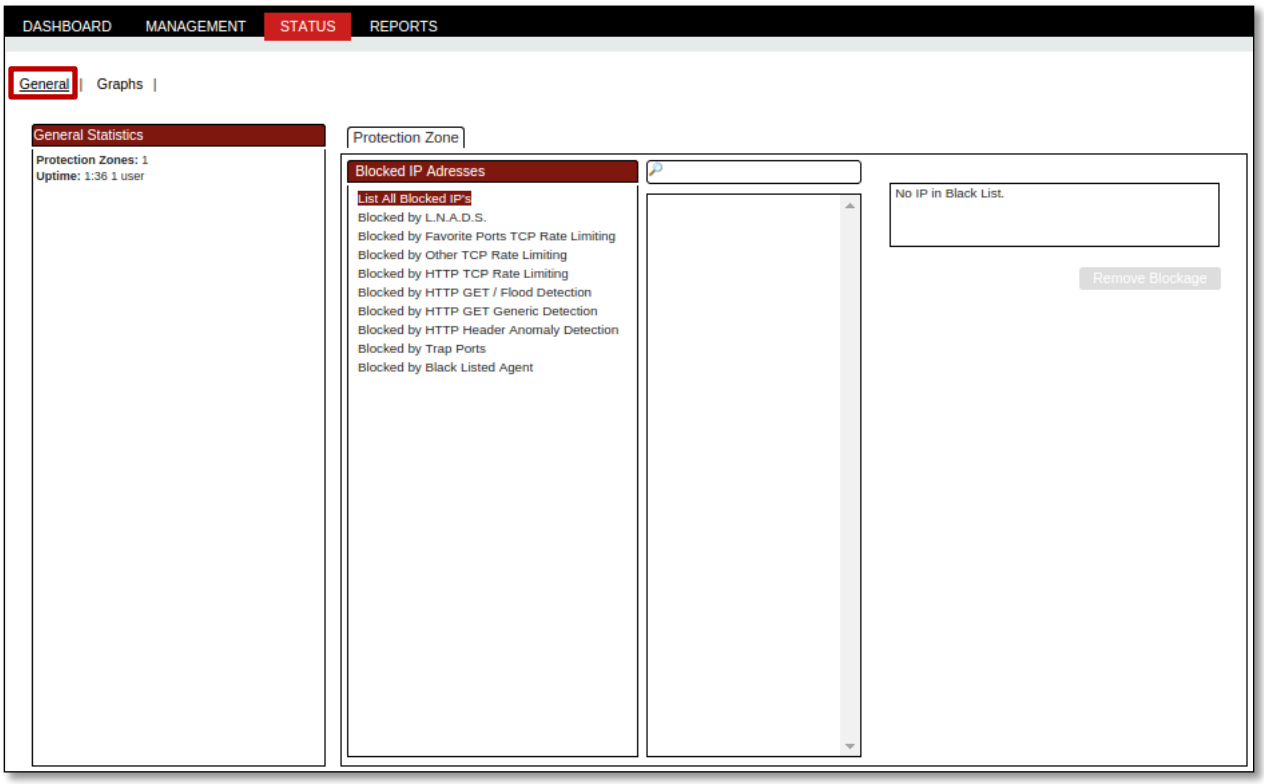
If needed, policy based routing can be defined on PBR tab. If source or destination field is empty it will match all traffic.




## 1.4 Status

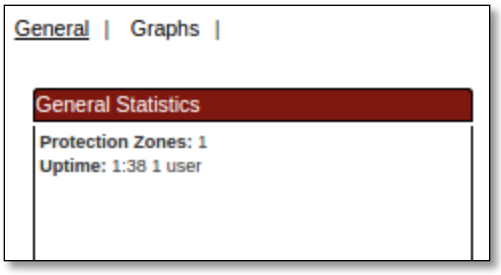
In Status section we can notice General and Graphs Information.

Under Protection Zone, List of All Blocked IP's are displayed.



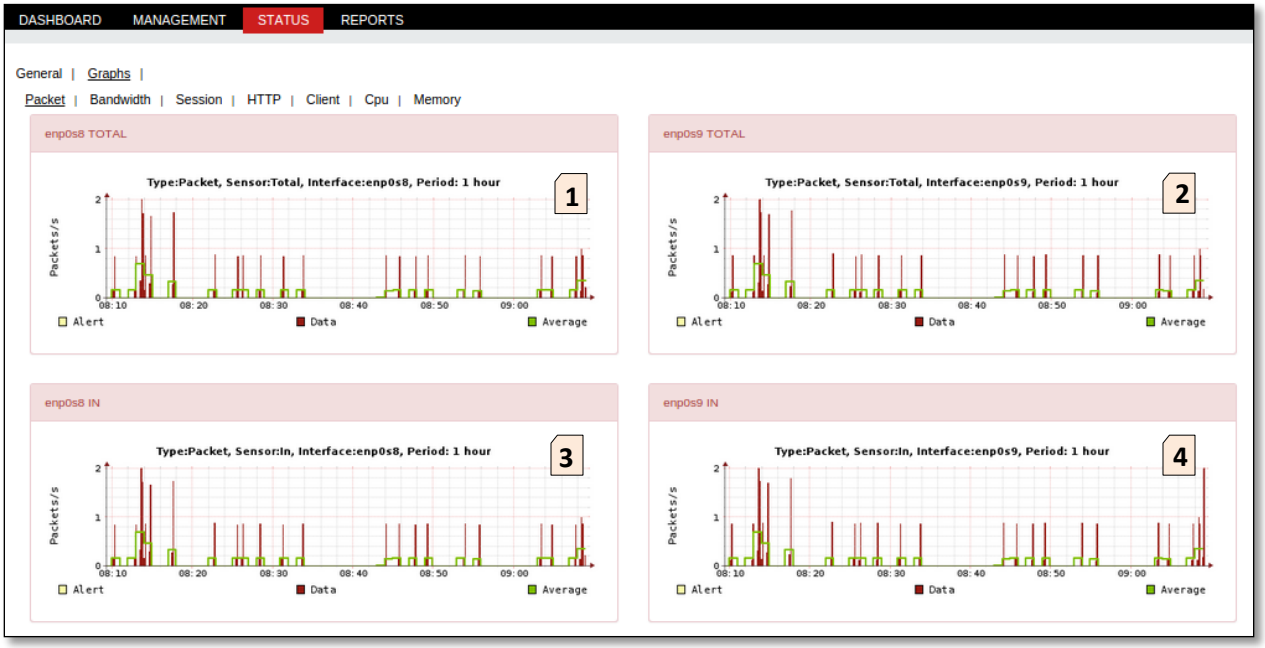

### 1.4.1 General Statistics

In the below screen we can notice General statistics. Information regarding Protection zone and Uptime is being displayed in the below screen.




### 1.4.2 Graphics

In Graphs section click on packets to view and analyze Graphical representation regarding Packets information with different types of Interfaces.

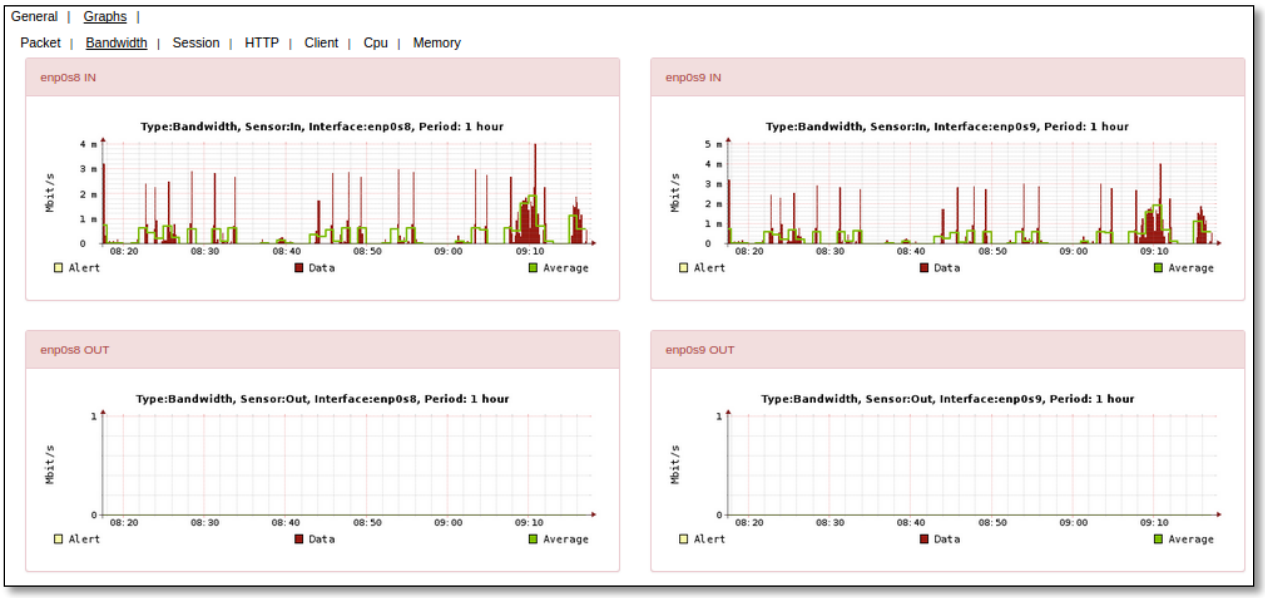



From the above Graphs we can notice below Points

| | | |
|---|---|---|
| 1 | **enp0s8 Total** | We can monitor the data transfer rate from enp0s8 interface. |
| 2 | **enp0s9 Total** | We can monitor the data transfer rate from enp0s9 interface. |
| 3 | **enp0s8 IN** | We can monitor the INPUT data transfer rate from enp0s8 IN interface. |
| 4 | **enp0s9 IN** | We can monitor the INPUT data transfer rate from igb4 IN interface. |

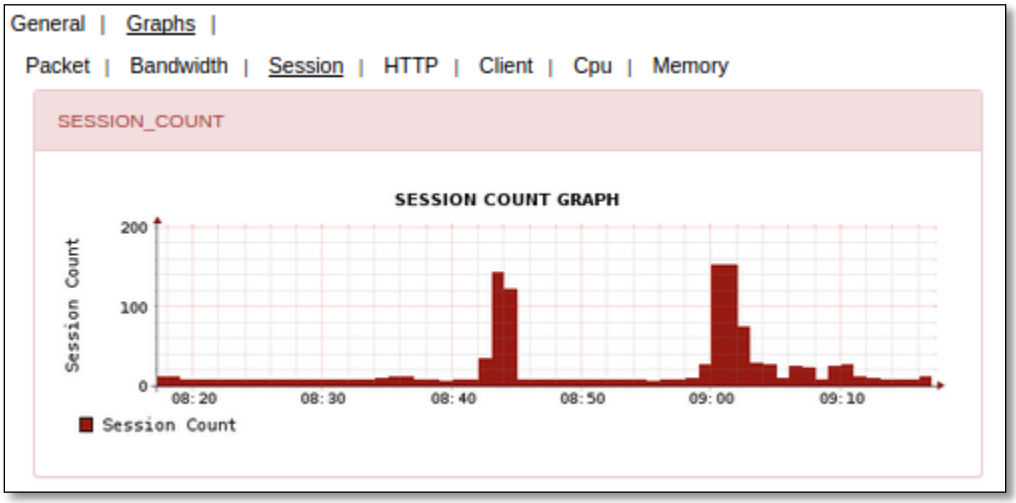
**Bandwidth**

In Graphs section click on Bandwidth to view and analyze Graphical representation regarding Bandwidth information with different types of Interfaces.




## Session

In Graphs section click on Session to view and analyze Graphical representation regarding Session count.

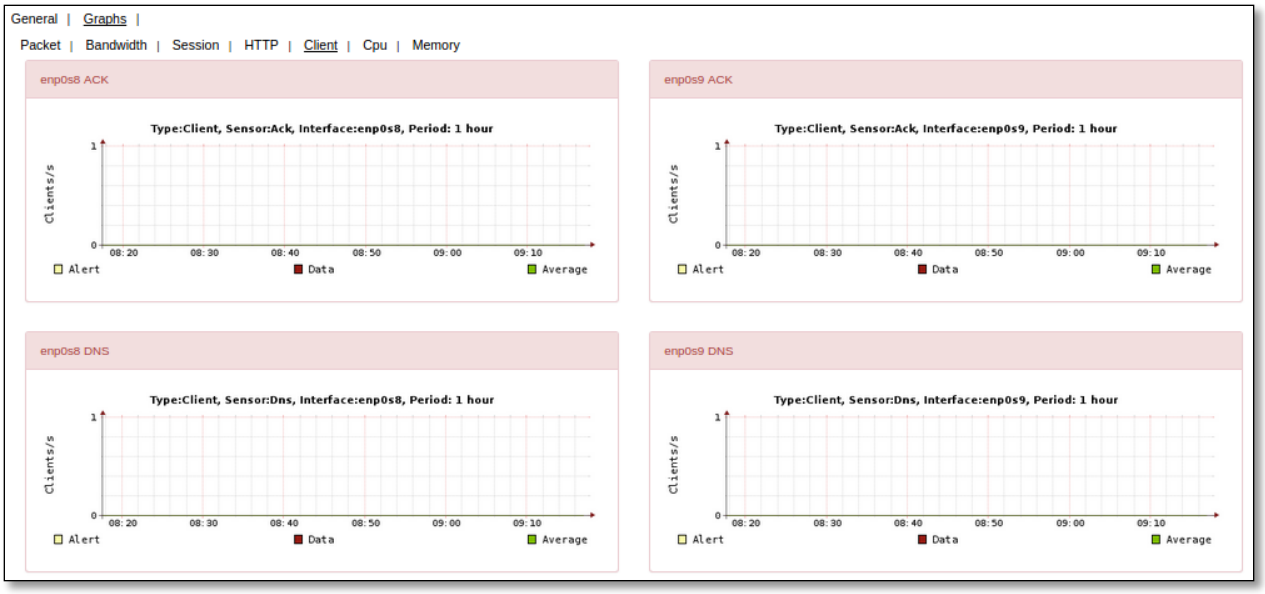



## HTTP

In Graphs section click on HTTP to view and analyze Graphical representation regarding HTTP information with different types of interfaces.

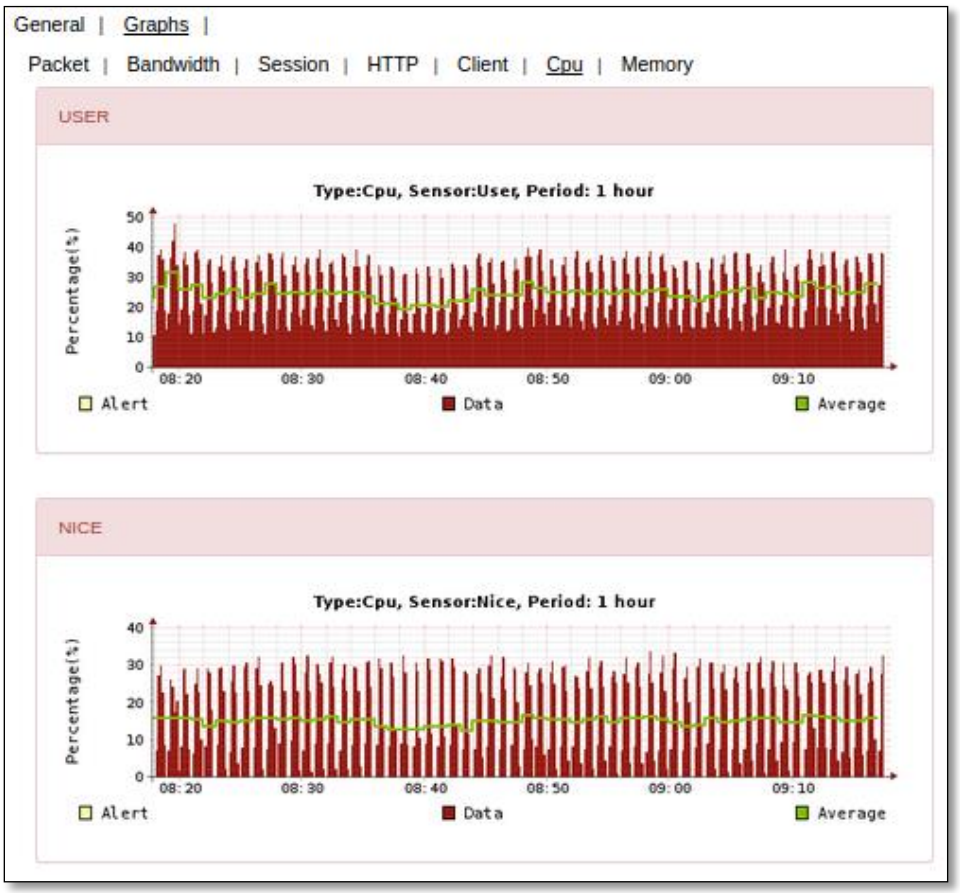

### Client

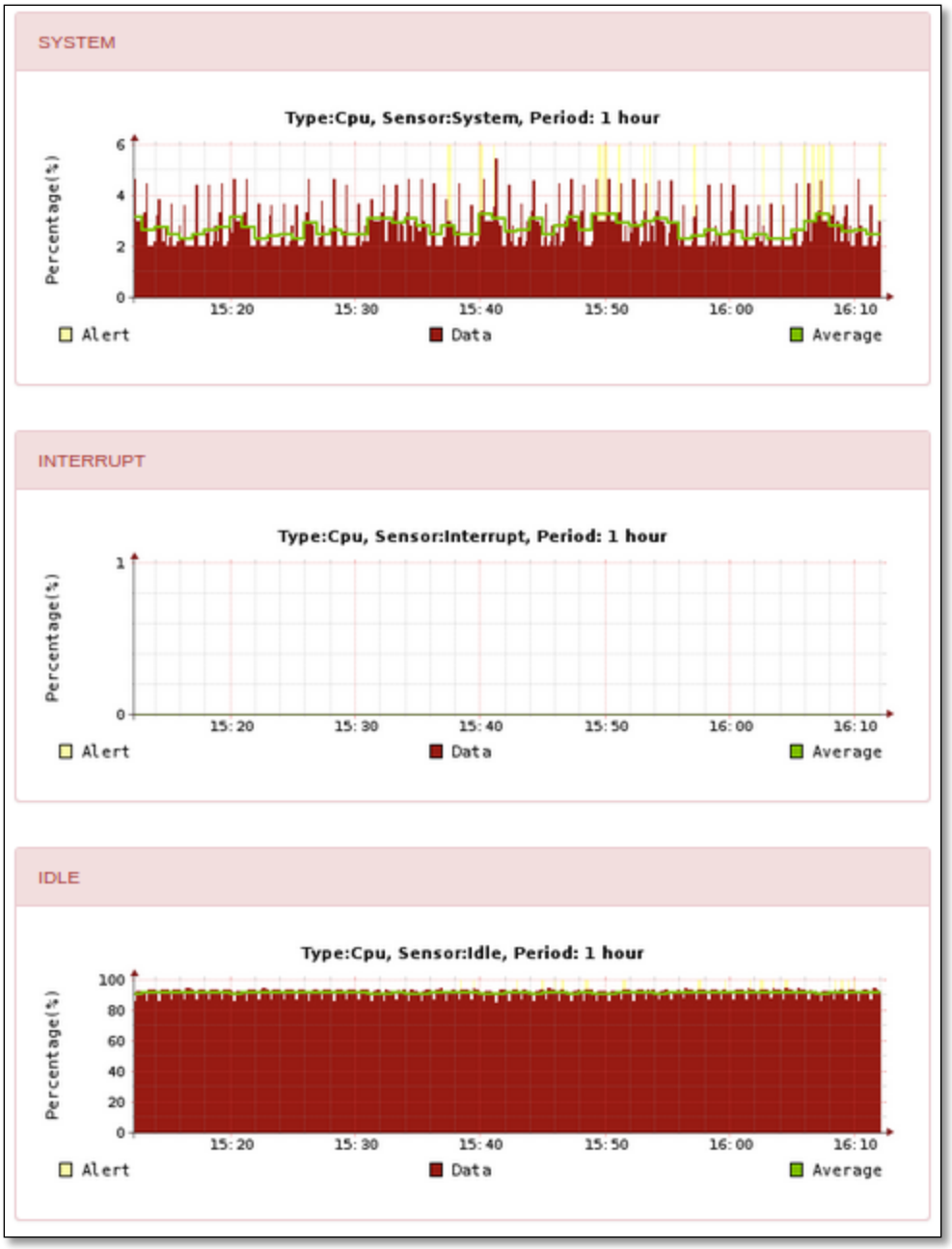
In Graphs section click onClient to view and analyze Graphical representation regarding Client (ACK, DNS) information with different types of interfaces.




### CPU

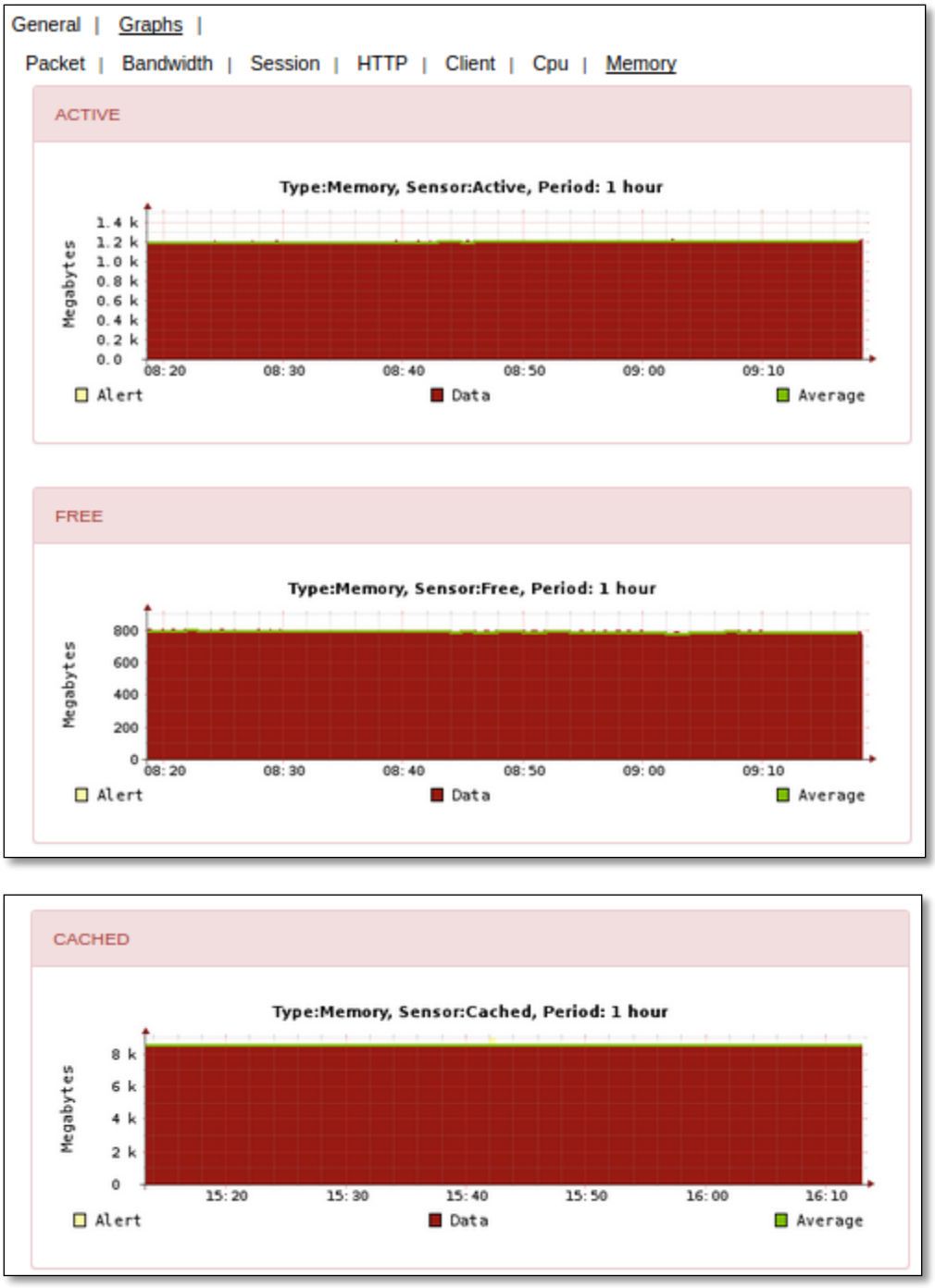
In Graphssection click on CPU to view and analyze Graphical representation regarding USER and NICE, System, Interrupt, Idle CPU information.






### Memory

In Graphs Section click on Memory to view and analyze Graphical representation regarding ACTIVE, FREE and Cached Memory information.

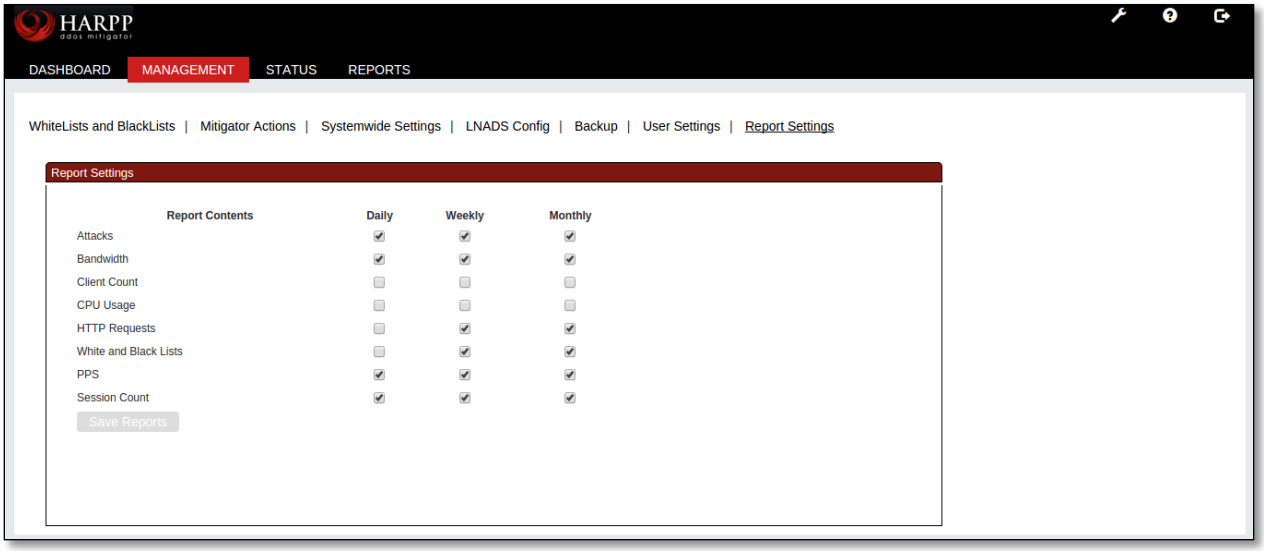



## 1.5 Report Settings

Report Settings contains fields such as **Report Contents.**

In which we can choose a specific time period as Daily or Weekly or Monthly for certain contents to generate reports accordingly.

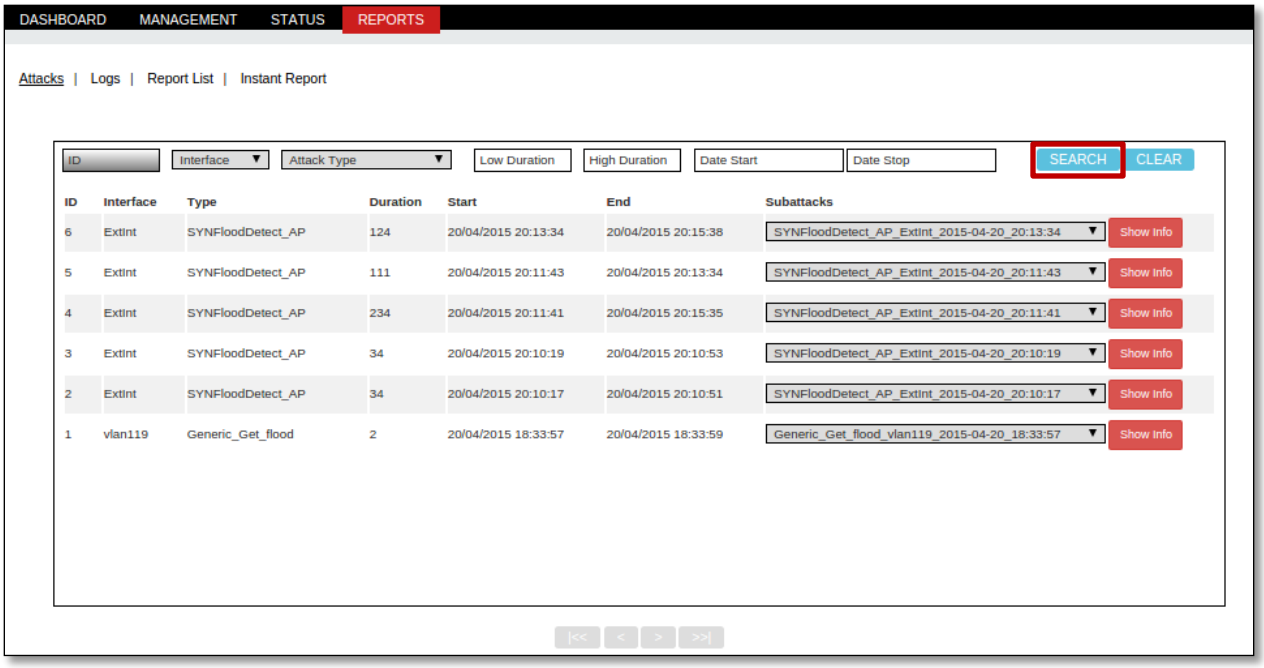
After selecting appropriate options click on **Save**tab.



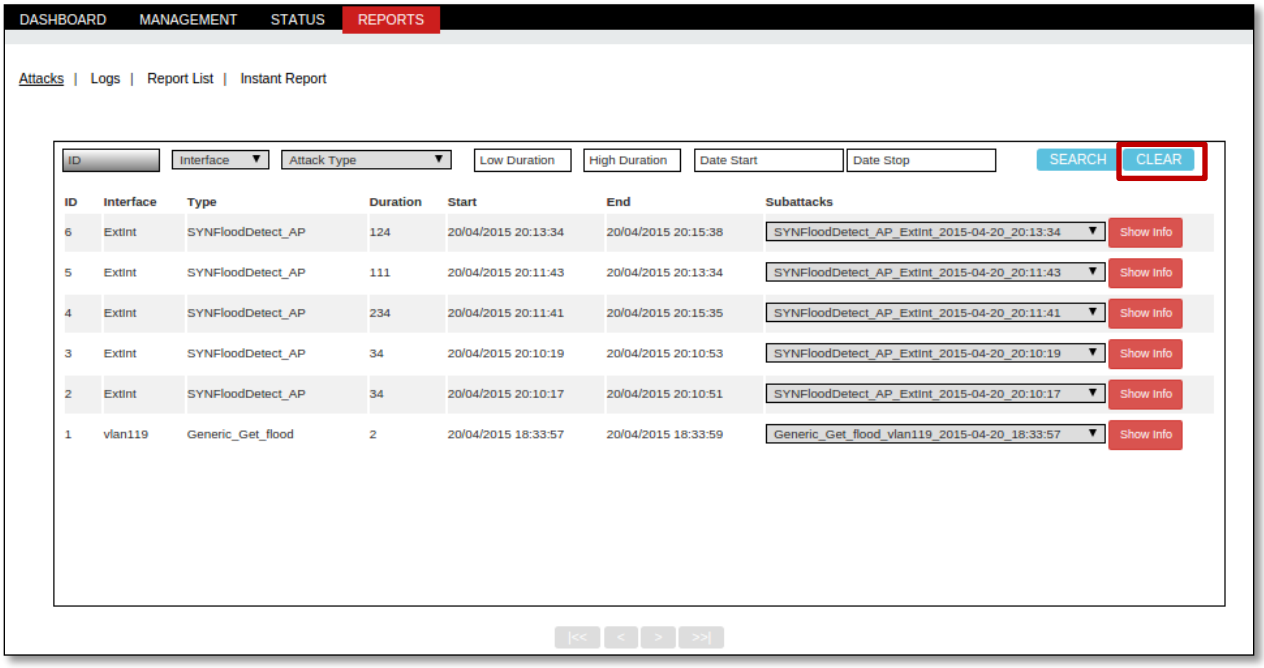

### 1.5.1 Attacks

Under Reports Tab we can notice Attacks with the fields ID, Interface, Attack Type, Duration, Start Date and Stop Date.

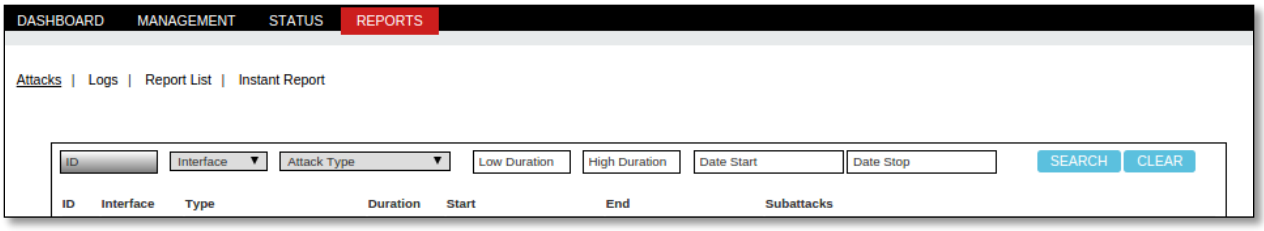
To search any specific Attack give the details of that particular Attack in the specific fields and click on **Search** tab.



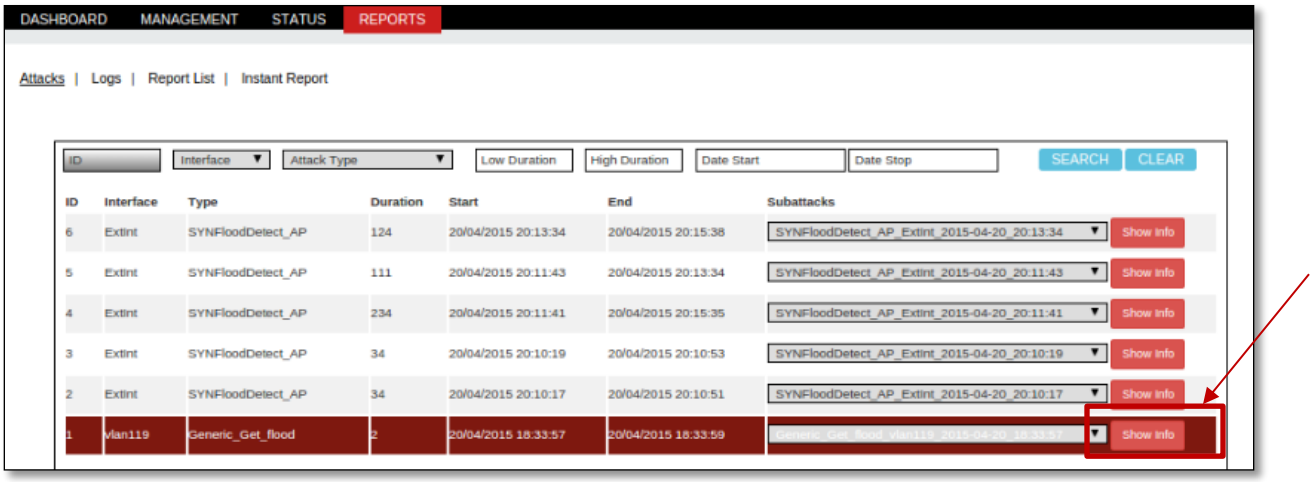

Click on **Clear** tab to clear all the fields in the Attacks section.



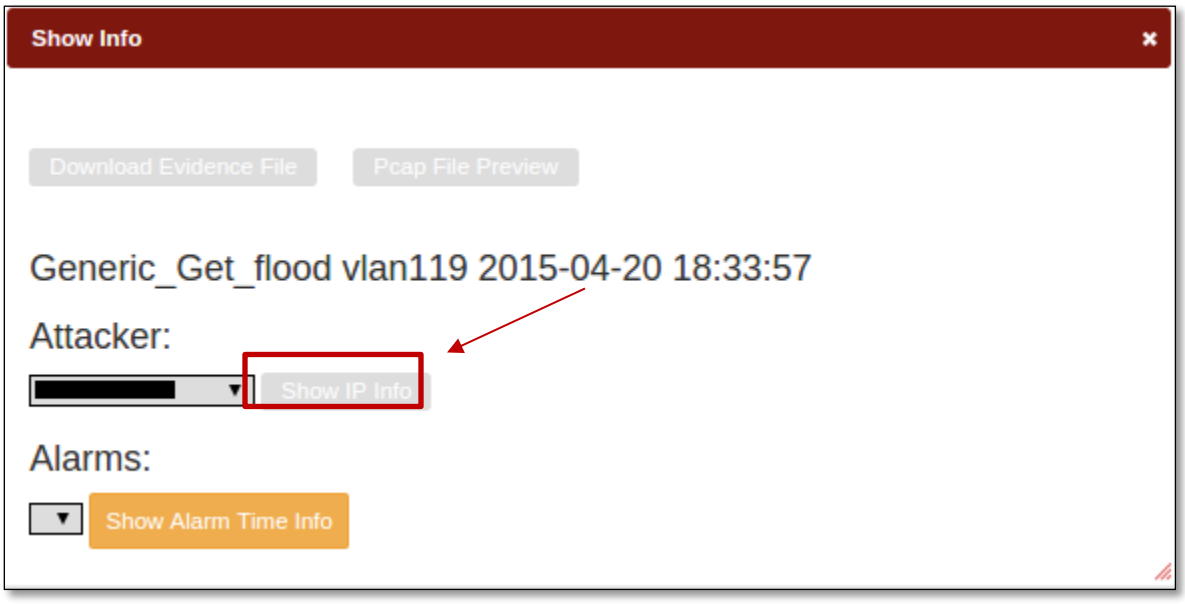

In the below screen, we can notice all the before entries in the fields are clear.



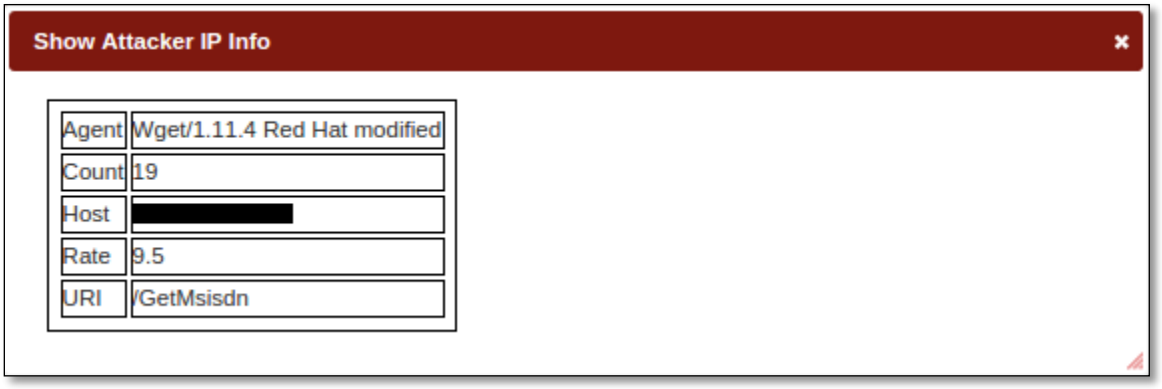

Select the particular field and click on **Show Info** tab.



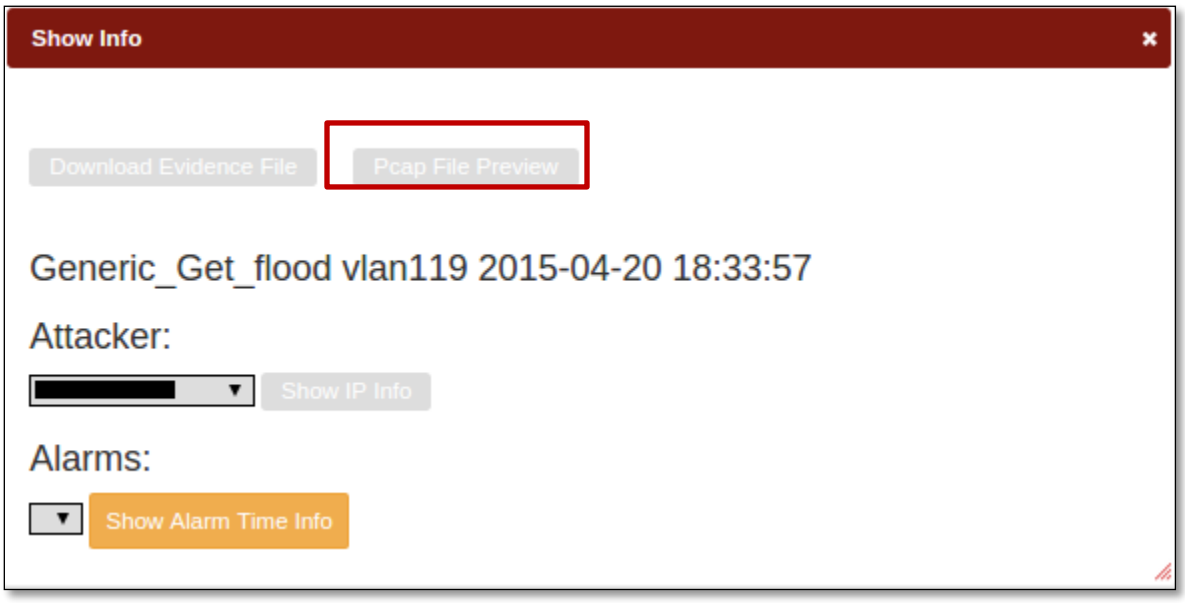

Show Info tab appears displaying Attackers information such as Attack type, IP and Alarm timing.



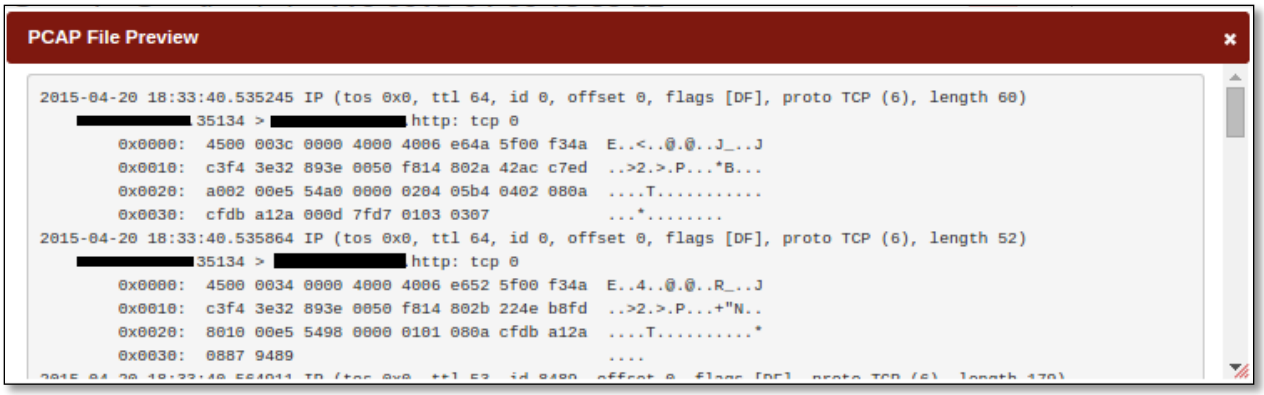
Click on **Show IP Info** tab.




It helps us to Download Evidence File and Pcap File Preview.
Click on **Pcap File Preview** tab.

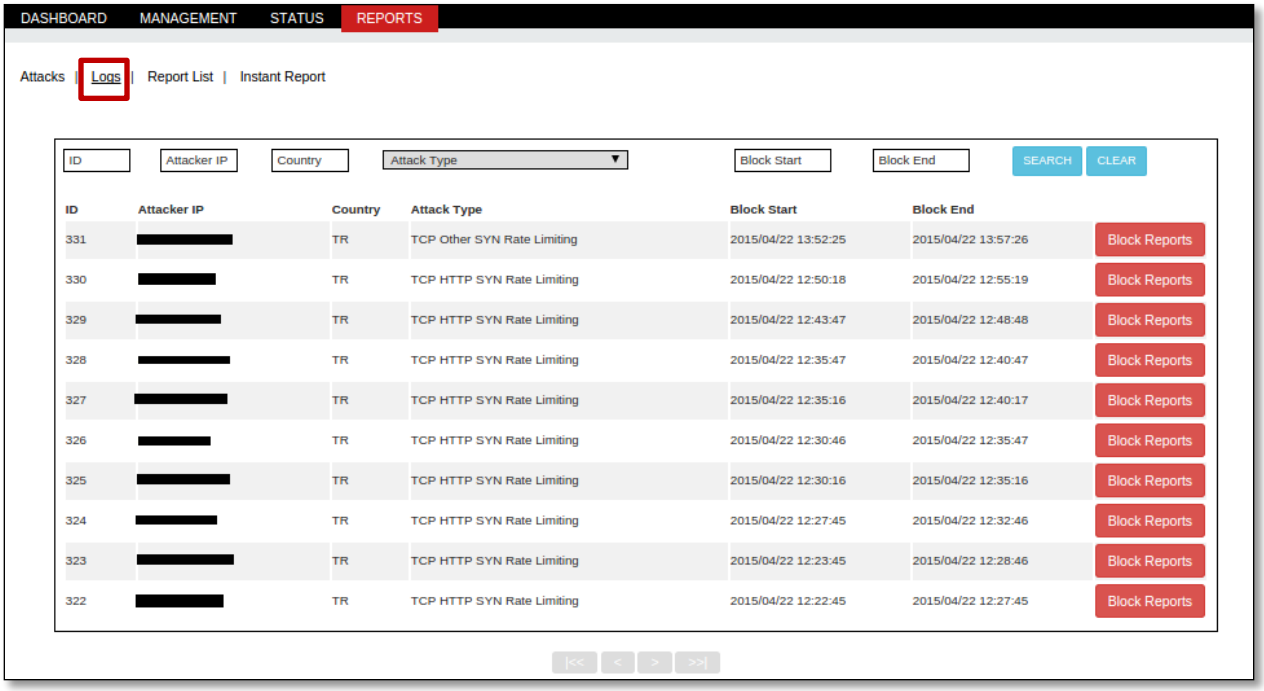



Pcap File Preview tab appears displaying information regarding the Attack.

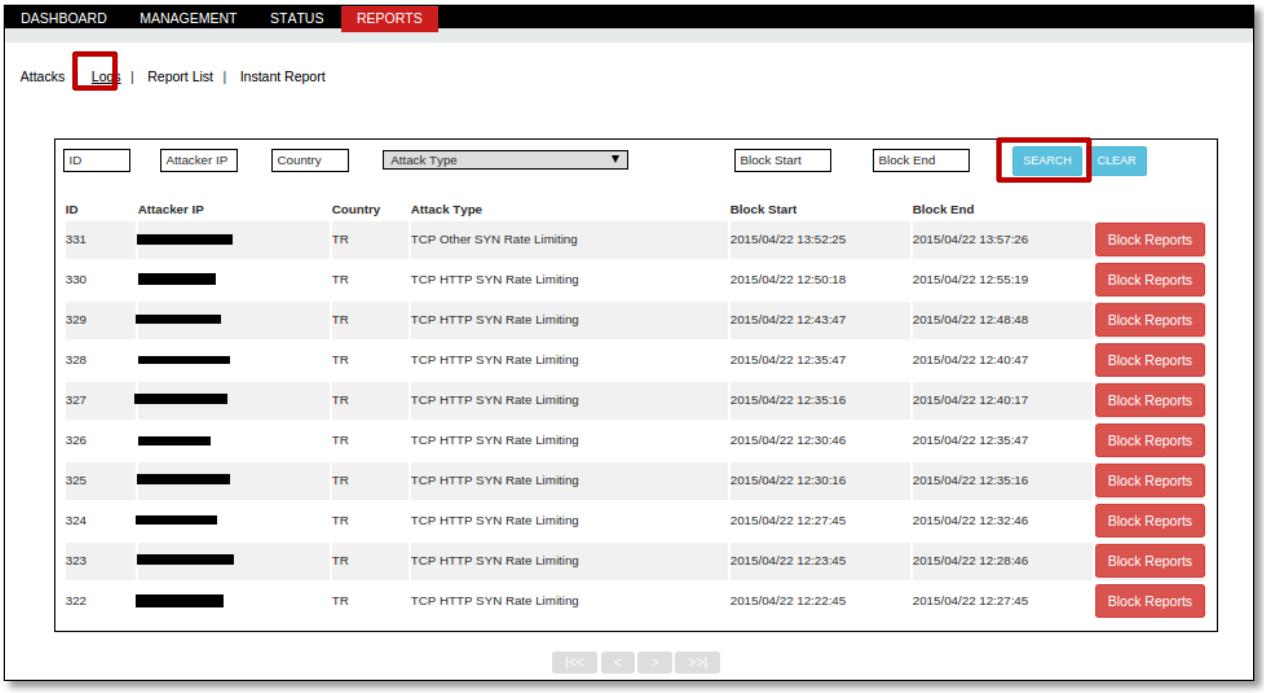



### 1.5.2 Logs

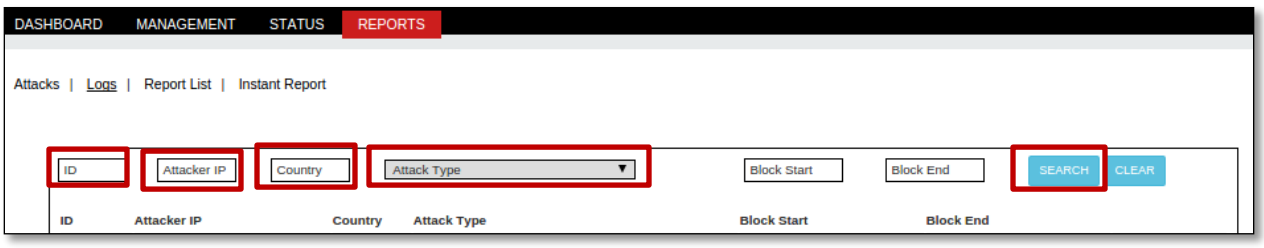
Under Reports tab, we can notice Logs with the fields ID, Attack IP, Country, Attack Type, Block start date and Block end date.




To search any specific Log give the details of that particular log in the specific fields and click on **Search** tab.



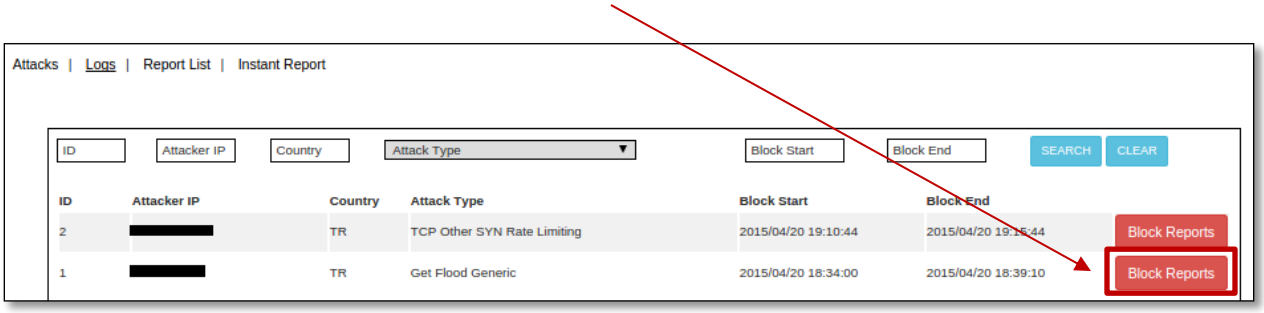

We can notice no logs available relate to our search criteria.



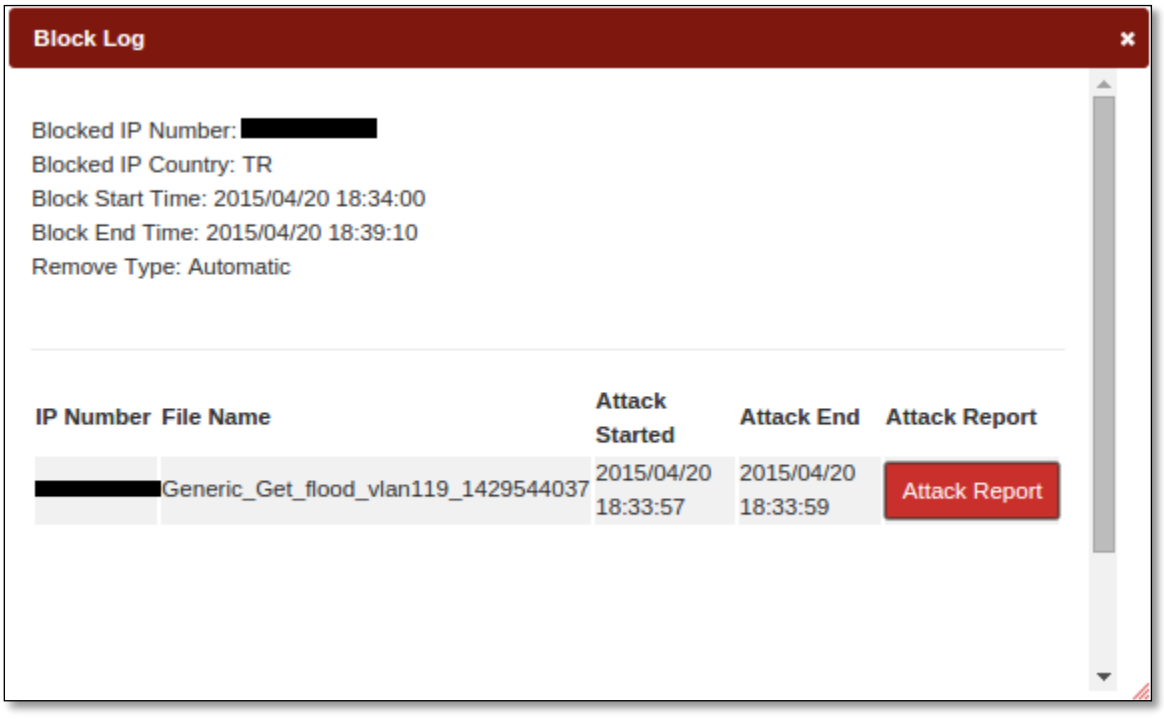

Click on **Clear** tab to clear all the fields in the Log section.


In the below screen, we can notice all the before entries in the fields are clear.


Select the particular log and click on **Block Reports** tab.

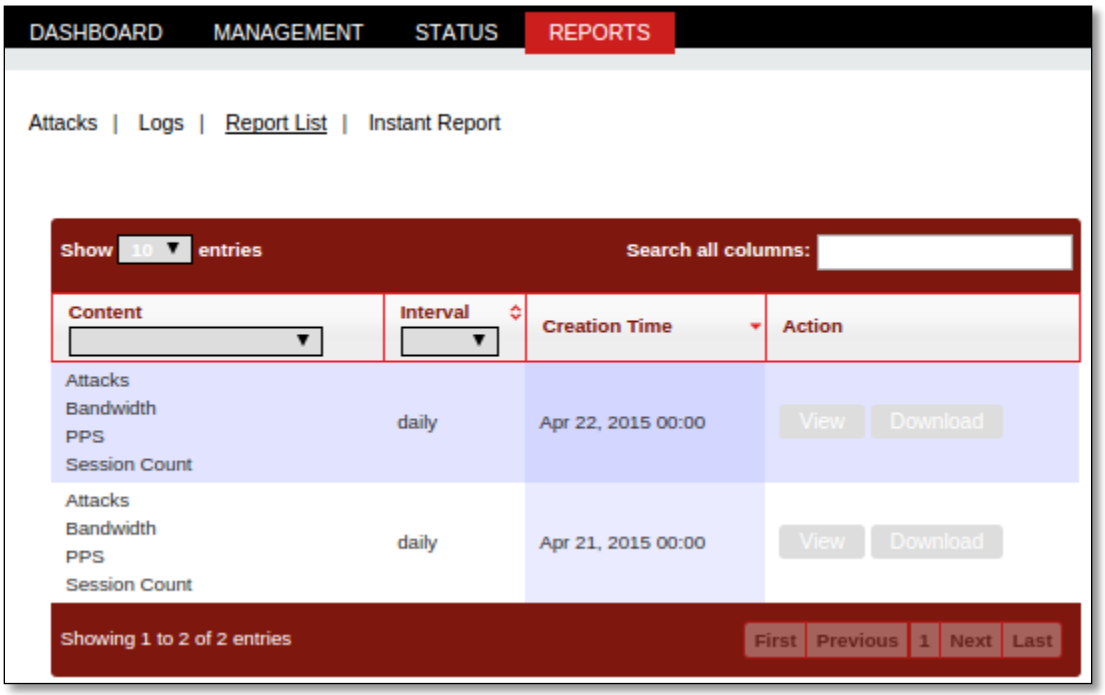



Block Log tab is appeared with the Log details such as Blocked IP Number, Blocked IP Country, Blocked Start Time, Blocked End Time and Remove Type.

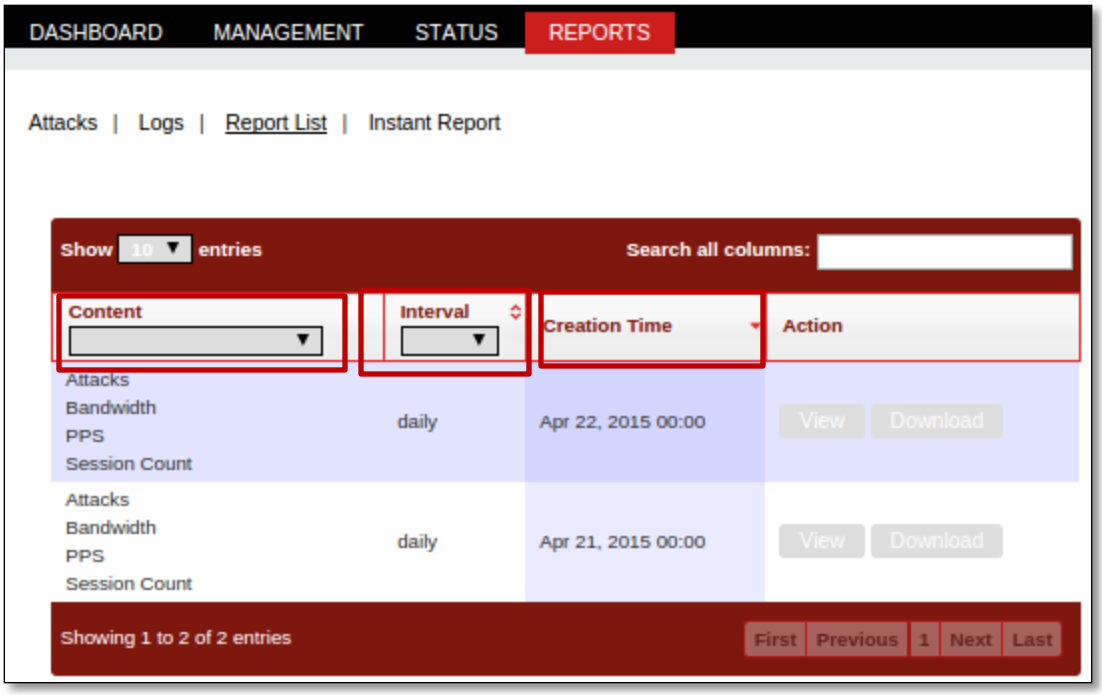



### 1.5.3 Report List

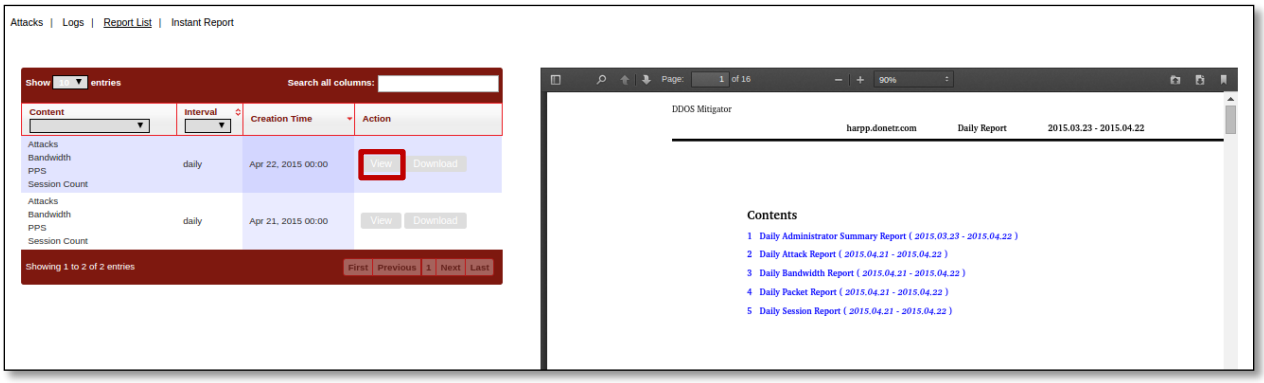
We can select the number of entries from drop down in the **Show tab.**
We come across four fields in Reports section such as **Content, Interval, Creation Time and Action.**
We have chosen 5 entries to show.
Contents tab unable us to choose the specific subject type from the drop down list and
Choose interval time from the drop down list.
It also enables us to view creation time and perform Actions like View and Download.



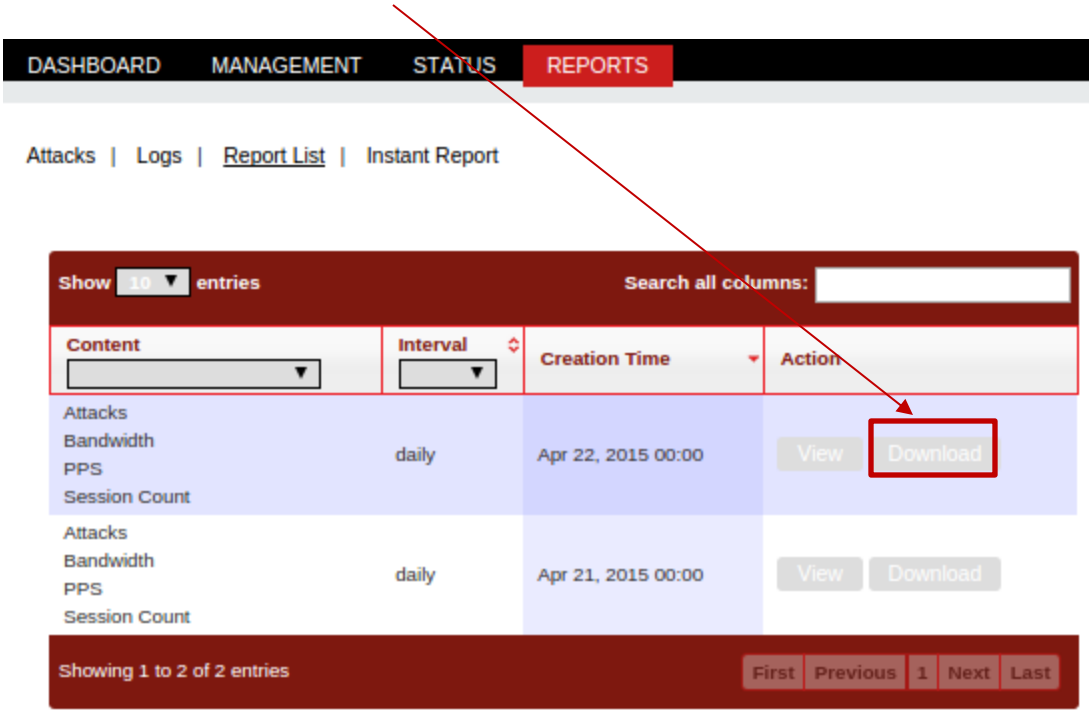

We have selected content type as Attacks and Interval as daily.



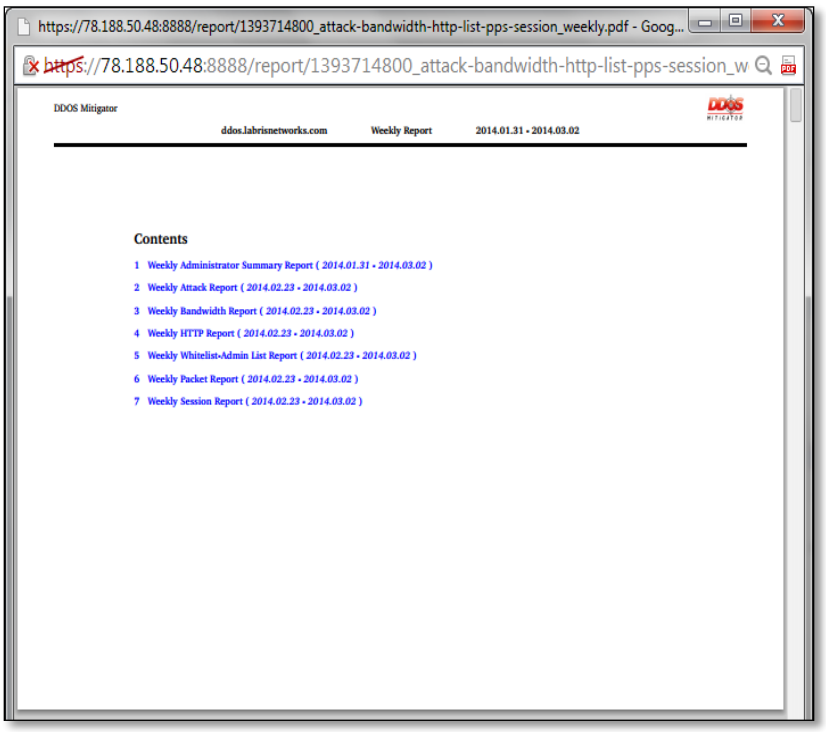

Choose **view** in the Actions field to view the Reports for the selected type of content.
When we click on View tab, in the right pane we can notice daily report on the particular selected section.




Click on **Download** tab to download the selected Section of report.



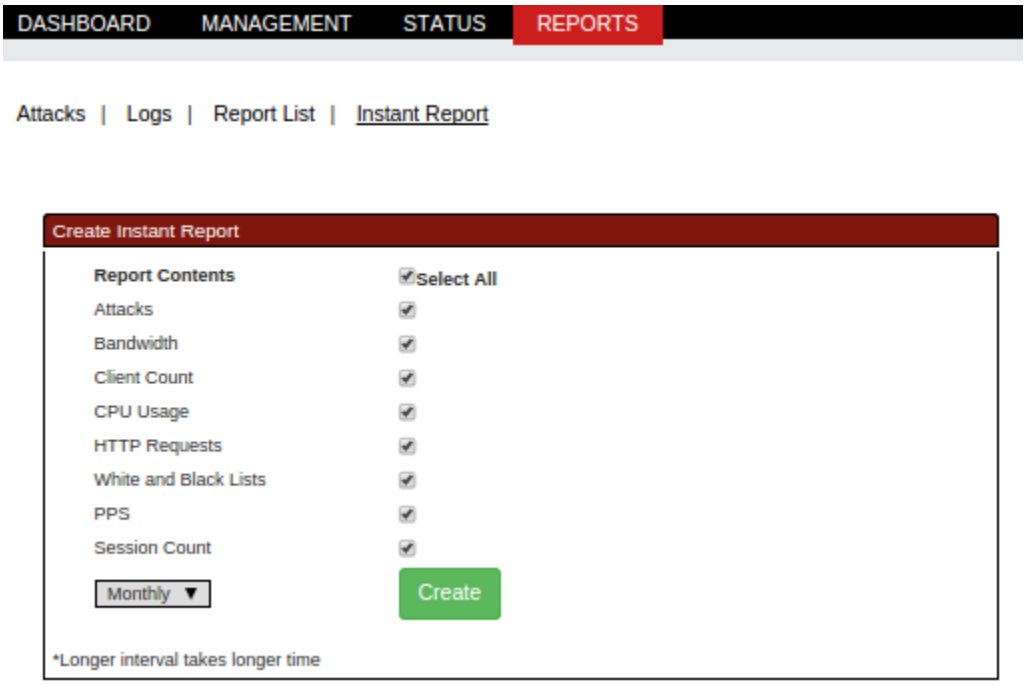

We can notice the selected section is opened in the new window as shown in the below screen.



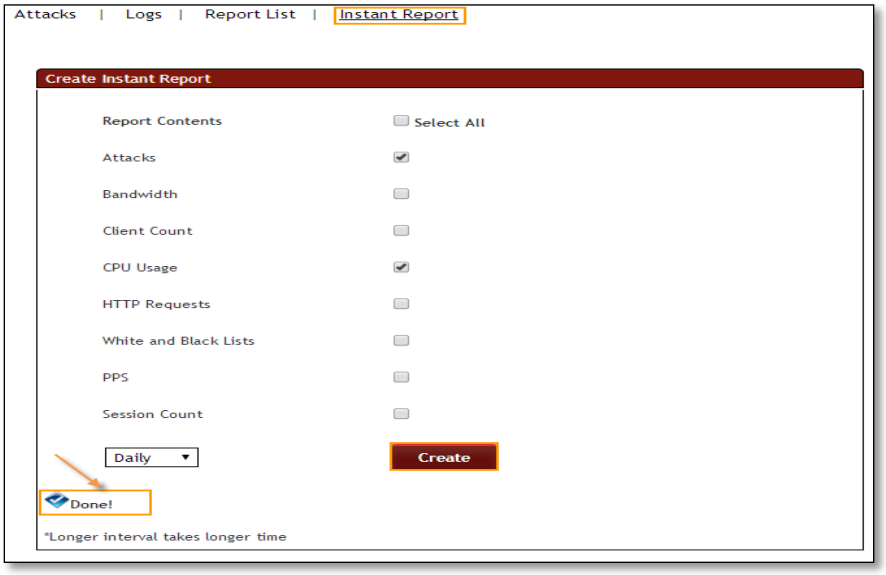

### 1.5.3 Instant Report

It enables us to create an instant report.

Select the content type for which we need to generate an instant report.
Click on **Create** tab.
We can notice creation of instant report is in process.




In the below screen we can notice the creation of instant report is done.




## 2. LNADS (Labris Network Anomaly Detection System)

LNADS is a system that detects network anomalies (DDoS).

Functions performed by LNADS are:

1. Identifies the attacker ip address and prevents access by typing the PF tables.
2. Creates by using the graphics shown in the rrdtool.
3. The attack and keeps the package logs shaped.

## 2.1 Console commands

LNADS/etc/init.d/labris_ddos command scriptis handled with the following steps.

/etc/init.d/labris_ddos <Komut> (Type the command for performing actions like start, restart and relode )

The command may **start, stop, restart** and **reload** value.

start: LNADS.
stop: stops the LNADS yi.
restart: restarts the LNADS yi completely.
reload: reloads the LNADS settings without stopping the program located in the folder/etc/labris.

## 2.2 DDoS Config Parameters

LNADS setting parameters are in the**/etc/labris/ddos.conf** file.

These parameters areinterfaces that  can be changed manually by selecting the file, or ddos.

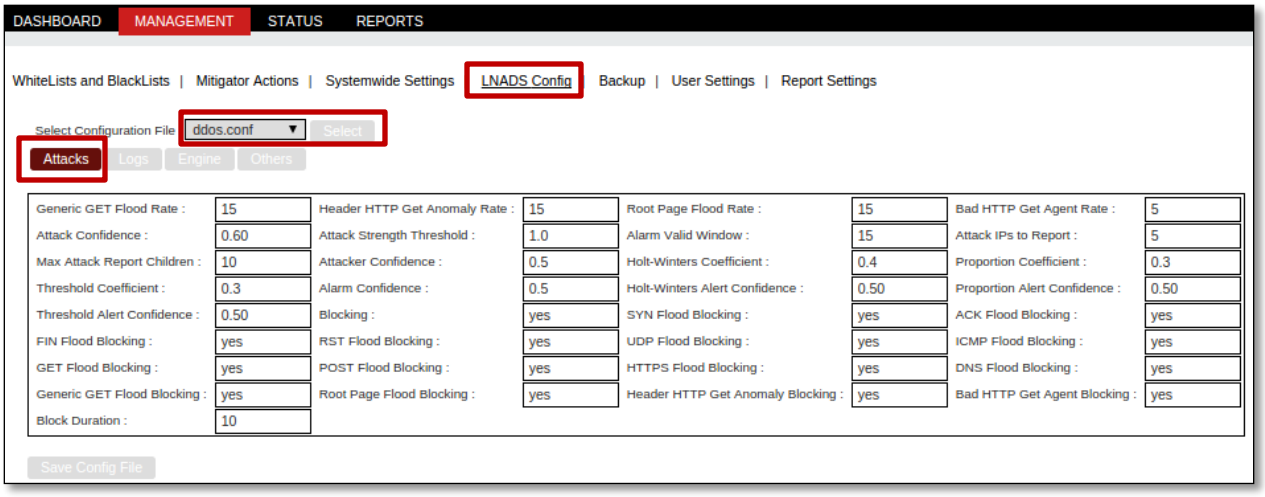
Parameters <parameter> is written in the form of < space > Details table shows < value >.

LNADS config tab consists of fields like **Attacks**, **Logs**, **Engine**, **Others.**

Select configuration file from the drop down menu.

Click on **Attacks**tab.

We can be able to view and make any necessary changes to the different fields present under Attacks and click on **Save Config File** to apply changes `if any are made to it.`


DASHBOARD
MANAGEMENT
STATUS
REPORTS
WhiteLists and BlackLists | Mitigator Actions | Systemwide Settings | LNADS Config | Backup | User Settings | Report Settings
Select Configuration File
ddos.conf
Select
Attacks
Logs
Engine
Others
Generic GET Flood Rate : 15
Header HTTP Get Anomaly Rate : 15
Root Page Flood Rate : 15
Bad HTTP Get Agent Rate : 5
Attack Confidence : 0.60
Attack Strength Threshold : 1.0
Alarm Valid Window : 15
Attack IPs to Report : 5
Max Attack Report Children : 10
Attacker Confidence : 0.5
Holt-Winters Coefficient : 0.4
Proportion Coefficient : 0.3
Threshold Coefficient : 0.3
Alarm Confidence : 0.5
Holt-Winters Alert Confidence : 0.50
Proportion Alert Confidence : 0.50
Threshold Alert Confidence : 0.50
Blocking : yes
SYN Flood Blocking : yes
ACK Flood Blocking : yes
FIN Flood Blocking : yes
RST Flood Blocking : yes
UDP Flood Blocking : yes
ICMP Flood Blocking : yes
GET Flood Blocking : yes
POST Flood Blocking : yes
HTTPS Flood Blocking : yes
DNS Flood Blocking : yes
Generic GET Flood Blocking : yes
Root Page Flood Blocking : yes
Header HTTP Get Anomaly Blocking : yes
Bad HTTP Get Agent Blocking : yes
Block Duration : 10
Save Config File

| Parameter | Interface Name | Information | Example |
|---|---|---|---|
| <progress>_log_level | <Progress> Log Level | Entered in progress (ddos, attacks, alerts, alarms, engine, blocks) to determine the log levels. The Log levels are DEBUG, INFO, warning, ERROR, CRITICAL, and can be one of the values. | ddos_log_level DEBUG |
| period | Data Period | The value of the data-flow period. | Period 10 |
| attack_confidence | Attack Confidence | A request is the minimum required to be perceived as attacking confidence. | attack_confidence 0.3 |
| attack_strength_threshold | Attack Strength Threshold | Attack detection during an attack force threshold. | attack_strength_threshold 1.0 |
| alarm_valid_window | Alarm Valid Window | An alarm can be valid. | alarm_valid_window 15 |
| attack_ips_toreport | Attack Ips Teleport | It is required to validate an alarm. | attack_ips_toreport 5 |
| max_attack_report_children | Max Attack Report Children | Specifies the number of maximum child progress reporting during that attack. | max_attack_report_children 10 |
| attacker_confidence | Attacker Confidence | An ip address is the minimum required to be perceived as aggressive confidence. | attacker_confidence 0.3 |

| | | | |
|---|---|---|---|
| hw_coefficient | Hw Coefficient | Hold Winters storeys | hw_coefficient 0.4 |
| prop_coefficient | Proportion Coefficient | Proportion number of floors | prop_coefficient 0.3 |
| thresh_coefficient | Thresh Coefficient | Thresh storeys | thresh_coefficient 0.3 |
| alarm_confidence | Alarm Confidence | The value of the minimum required for a request to create an alarm confidence. | alarm_confidence 0.3 |
| hw_alert_confidence | Hw Alert Confidence | Hold the value for the Winters alert confidence. | hw_alert_confidence 0.3 |
| prop_alert_confidence | Proportion Alert Confidence | Proportion of the alert for the confidence value. | prop_alert_confidence 0.3 |
| thresh_alert_confidence | Thresh Alert Confidence | Thresh alert for confidence. | thresh_alert_confidence 0.3 |
| block_enabled | Blocking | yes/no values with the "active/passive" block. | block_enabled yes |
| block_enabled_<attack> | <attack> Blocking | attack value for blocking Active post attack variants. attack of the SYN_flood, ACK_flood, FIN_flood, RST_Flood, UDP_Flood, ICMP_flood, GET_Flood, POST_Flood, HTTPs_Flood, can be entered as DNS_Flood. | block_enabled_ACK_flood yes |
| block_duration | Block Duration | Perceived as aggressive ip's frustration. | block_duration 60 |

| | | | |
|---|---|---|---|
| Whitelist | - | Indicates that the file contains its ip white list. This is more than one file interface serves all of whitelist. It is not recommended to change this value, that's why. | Whitelist whitelist.conf |
| tcpstat_period | TCP Stat Check Period | Specifies the range of TCP Stat Control. | tcpstat_period 1 |
| capture_snaplen | Capture Snaplen | Specifies the size of each of the data being read during listening to the network. | capture_snaplen 9182 |
| <sensor>_prop | <Sensor> Proportion | Determines the value of the specified sensor for proportion. Sensor values to see the sensor. (Table 12) | cpu_system_prop 2 |
| <sensor>_thresh | <Sensor> Threshold | Specifies the threshold value for the specified sensor. Sensor values to see the sensor. (Table 12) | cpu_system_thresh 90 |
| http_exclude_exts | Http Exclude File Extensions | Excludes the specified file extensions for Http requests. Can be entered into more than one extension by using a comma. | http_exclude_exts jpg,jpeg,gif,png |
| http_exclude_uri_regexps | Http Exclude Uri Words | The url containing the words entered is excluded. Can be entered multiple words by using a comma. This value is used; it is recommended that | http_exclude_uri_regexps nh\.php,fp\.php |

| | | | |
|---|---|---|---|
| | | you change only the interface as a regex. | |
| http_exclude_regexps | - | Entered the regex matches the requests are excluded. Do not change this value is manually managed by the interface. | http_exclude_regexps Range:.byte,Accept:.*image.* |
| engine_period | Engine Period | Engine working period. | engine_period 10 |
| engine_packet_chunk_size | Engine Packet Chunk Size | Engine packages to chunk specify the number of times. | engine_packet_chunk_size 1 |
| engine_adaptive_chunk_size | Engine Adaptive Chunk Size | The number of active engine compatible with chunk. | engine_adaptive_chunk_size yes |
| engine_adaptive_chunk_divisor | Engine Adaptive Chunk Divisor | Compatible engine chunk divisor. | engine_adaptive_chunk_divisor 100 |
| engine_child_count | Engine Child Count | The total number of children in the process Engine. | engine_child_count 2 |
| engine_int_child_count | Engine Internal Child Count | The number of internal network for child process. | engine_int_child_count 1 |
| engine_ext_child_count | Engine External Child Count | The number of external network for child process. | engine_ext_child_count 1 |
| graph_period | Graph Period | The period of the chart is created. | graph_period 60 |
| email_reports_to | Email Reports To | The reports will be sent to mail address. Can be entered | email_reports_to example@labristeknoloji.com |

| | | | |
|---|---|---|---|
| | | separated by commas, and more. | |
| sequence_control_value | Sequence Control Value | -TODO | sequence_control_value 20 |
| Interface | - | Interface specifies the Web.config file. The interface is managed by the manual do not change. | interface enp0s8.conf |

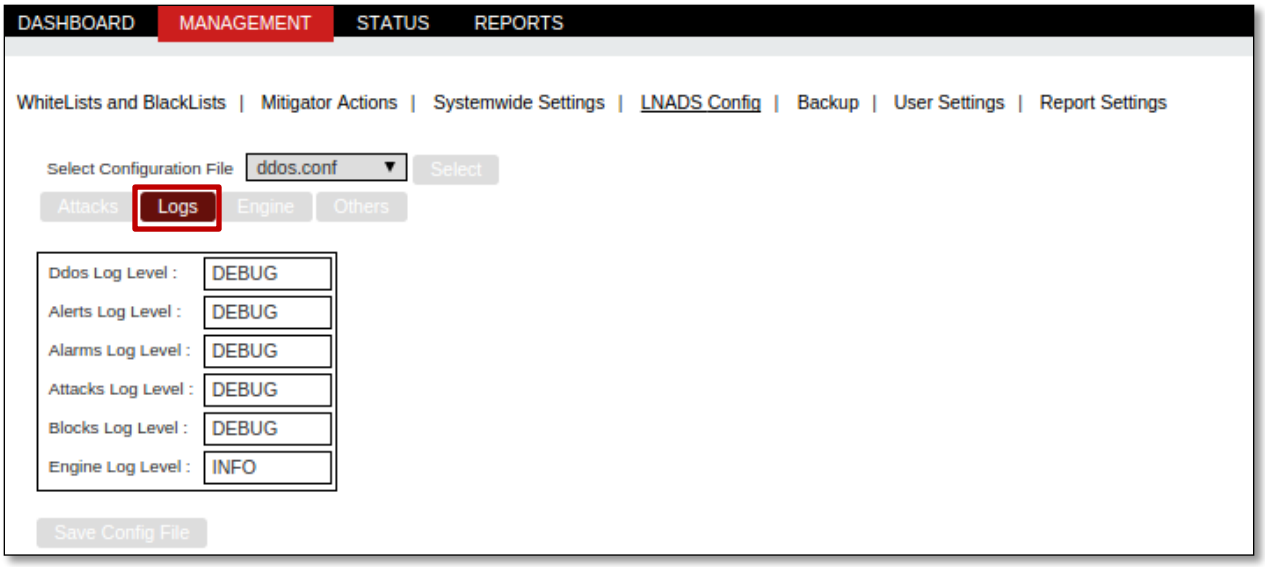
### DDOS config Senser List

The below table represents DDoS Config file Senser List.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Cpu User | Cpu Nice | Cpu System | Cpu Interrupt | Cpu Idle | Memory Active | Memory Cached | Memory Free |
| Bandwidth In | Bandwidth Out | Bandwidth Drop | Bandwidth Inerr | Bandwidth Coll | Packet Total | Packet In | Packet Out |
| Packet TCP | Packet SYN | Packet ACK | Packet FIN | Packet RST | Packet UDP | Packet DNS | Packet ICMP |
| Packet HTTPs | Packet Other | Packet IP4 | Packet IP6 | HTTP Get | HTTP Post | Client TCP | Client SYN |
| Client ACK | Client FIN | Client RST | Client UDP | Client DNS | Client ICMP | Client HTTPs | Client Other |
| Client Get | Client Post | Client IP6 | | | | | |

### Logs

Click on**Logs** tab.
We can view and change the different Log levels if required and click on **Save Config File** to apply changes if any are made to it.

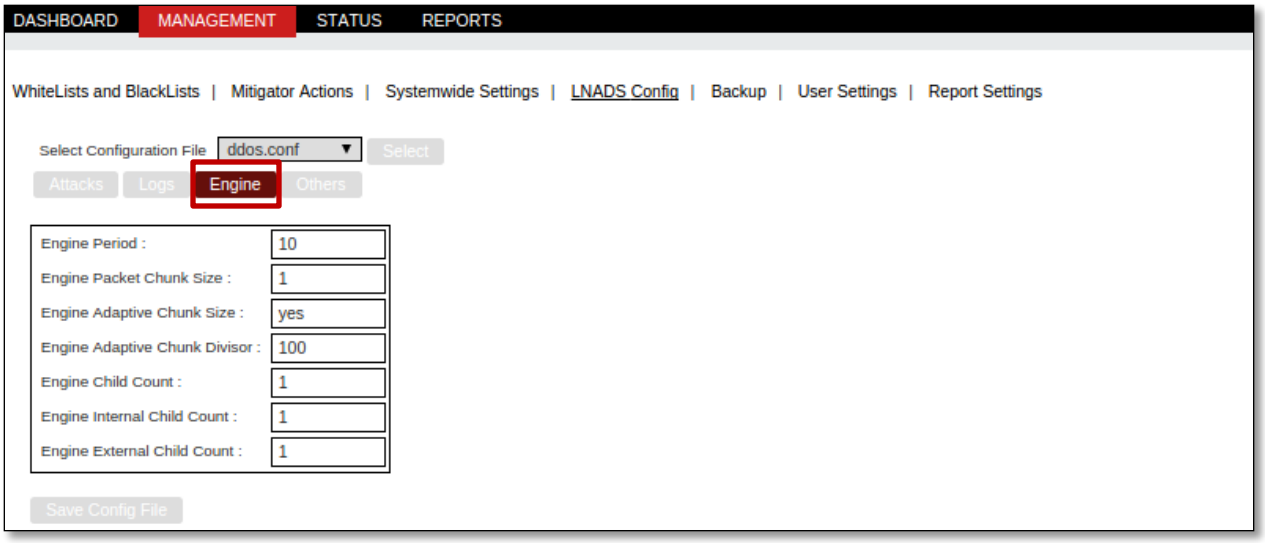



### Log Level

- DEBUG
- INFO
- WARNING
- ERROR
- CRITICAL

### Engine

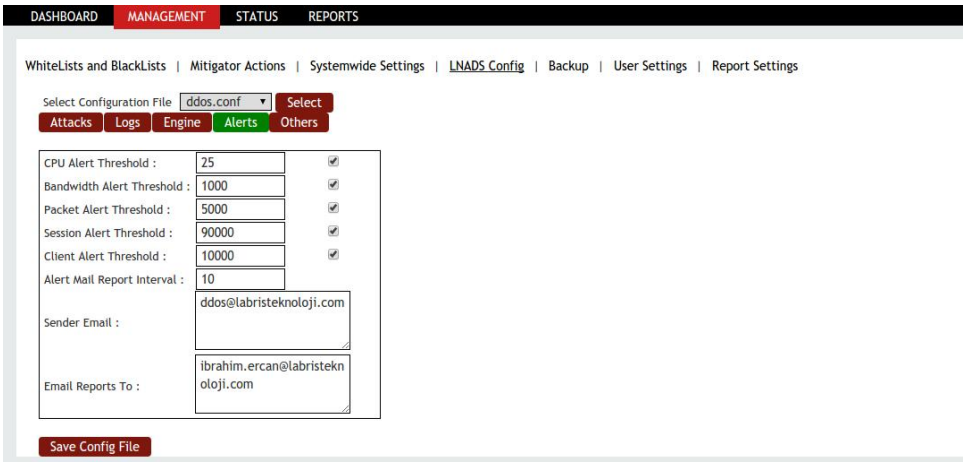
Click on **Engine** tab.
We can view and change the different Engine fields if required and click on **Save Config File** to apply changes if any are made to it.




## Alerts

Click on Alerts tab.

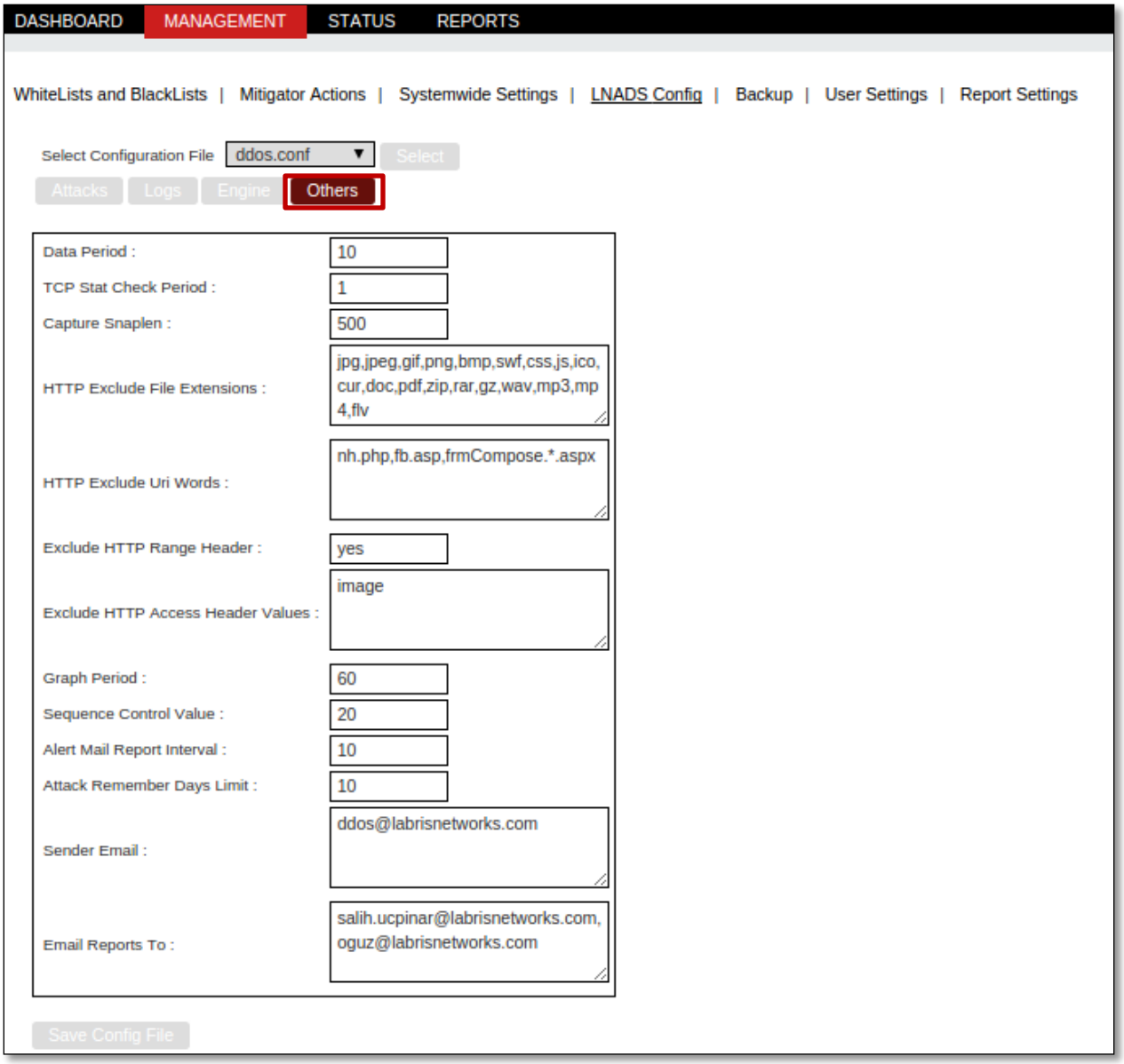
We can view and change the e-mail alerts fields if required and click on **Save Config File** to apply changes if any are made to it.




## Others

Click on **Others** tab.

We can view and change the other fields if required and click on **Save Config File** to apply changes if any are made to it.




## 2.4 Interface Config Parameters

Interface files are given the value of the ddos file interfaces. In the file LNADS if the values of the interface parametrers are not registered then they are not readable.

The values in the interface are as follows.

External Interface = enp0s8

Internal Interface = enp0s9

### External Interface Config Parameter

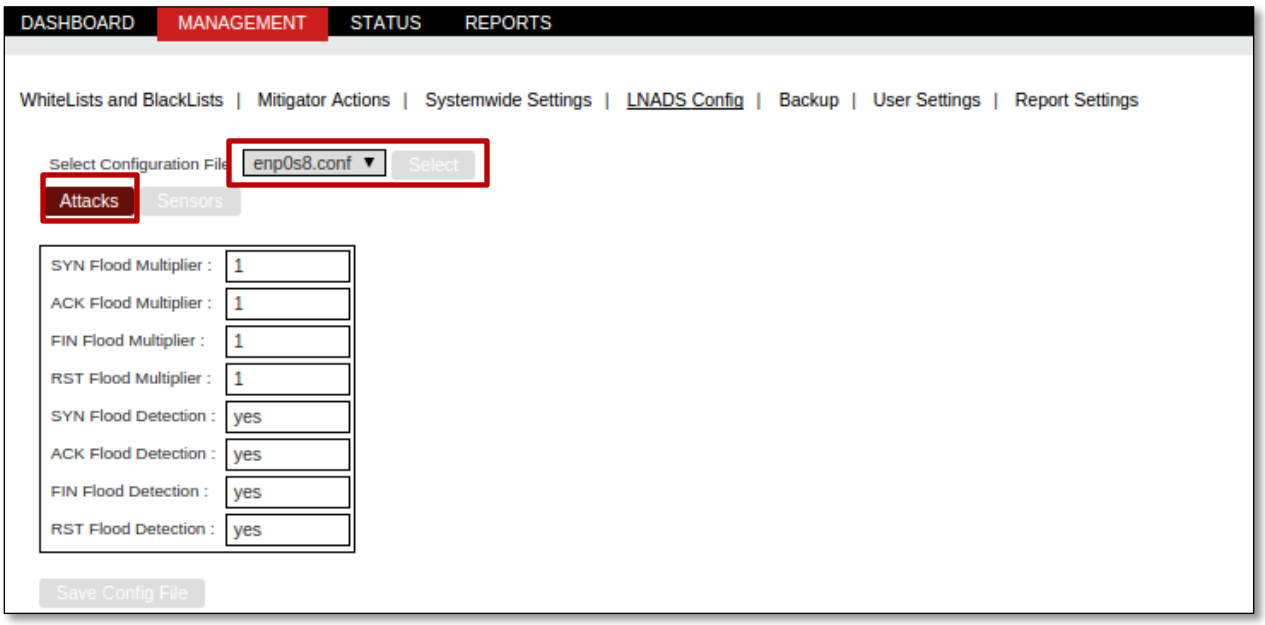
Select Configuration file interface as enp0s8.conf.

In Attacks section various Flood Multipliers and Flood Detections such as **SYN, ACK, FIN, RST** are avaliable.

Interface various Flood Multipliers value is one.

Interface Flood detection may be Active or Passive.

Click on **Save Config File** to save changes if any are made to it.

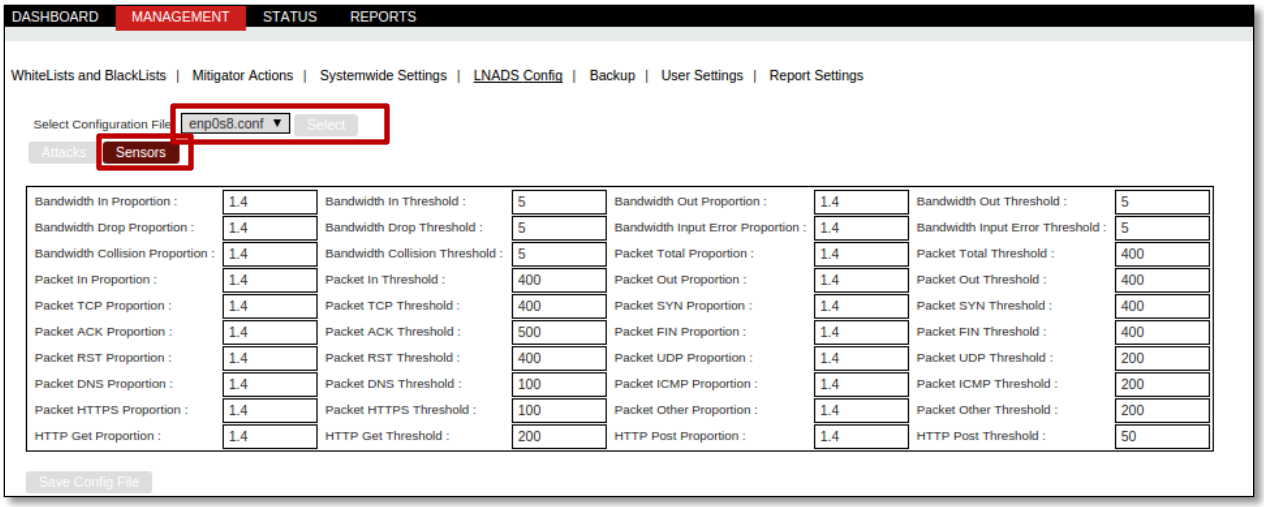



### External Interface Sensor Config

Select Configuration file interface as enp0s8.conf.

In Sensor section we find information regarding Bandwidth, Packets of the Interface with appropriate values.

Click on **Save Config File** tab to save changes if any are made to it.




## Internal Interface Config Parameter

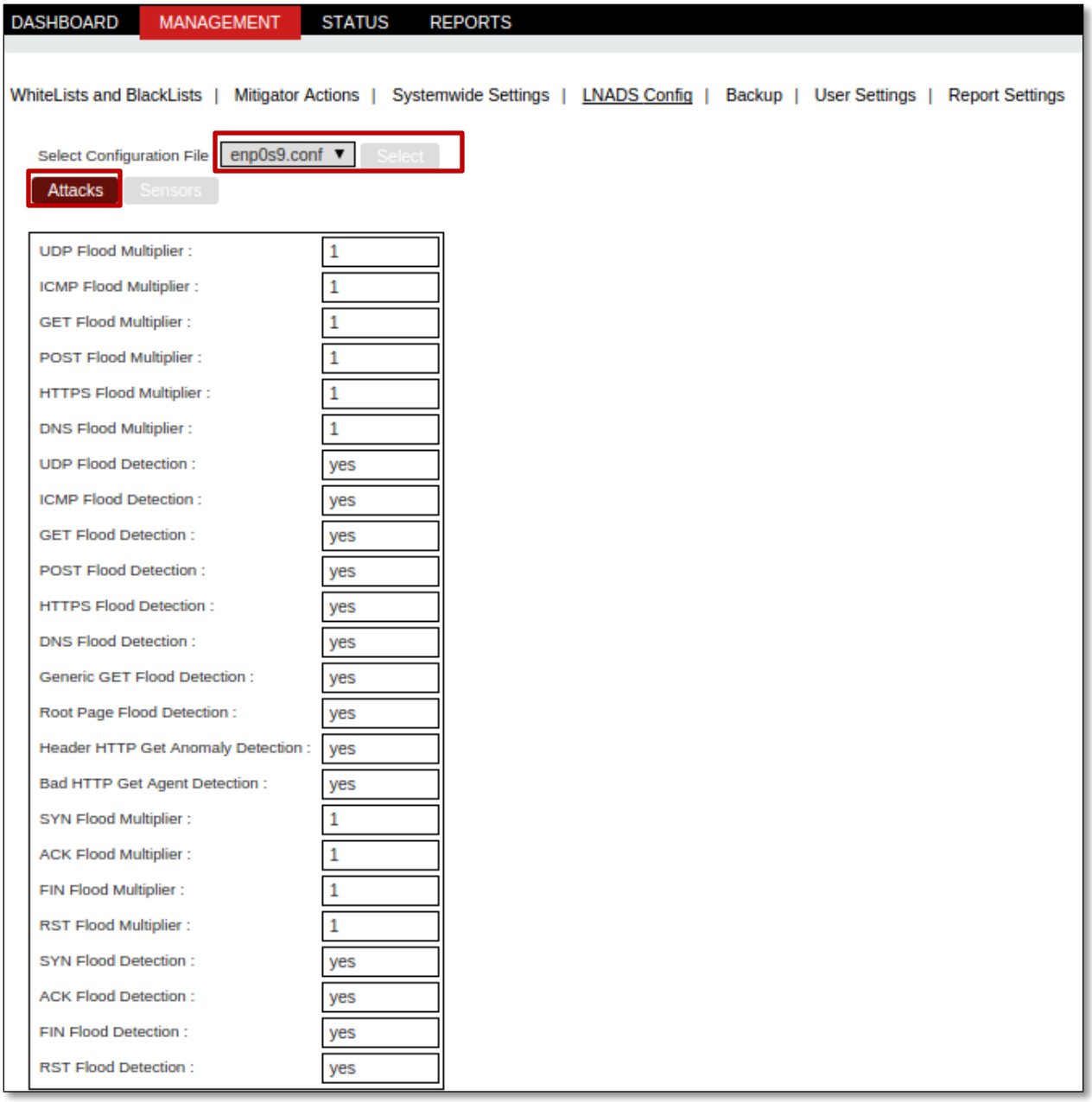
Select Configuration file interface as enp0s9.conf.

In Attacks section various Flood Multipliers  such as SYN, ACK, FIN, RST are avaliable along with UDP and ICMP Flood Detection.

Interface various Flood Multipliers value is one.

Interface Flood Detection may be Active or Passive.

Click on **Save Config File**tab  to save changes if any are made to it.

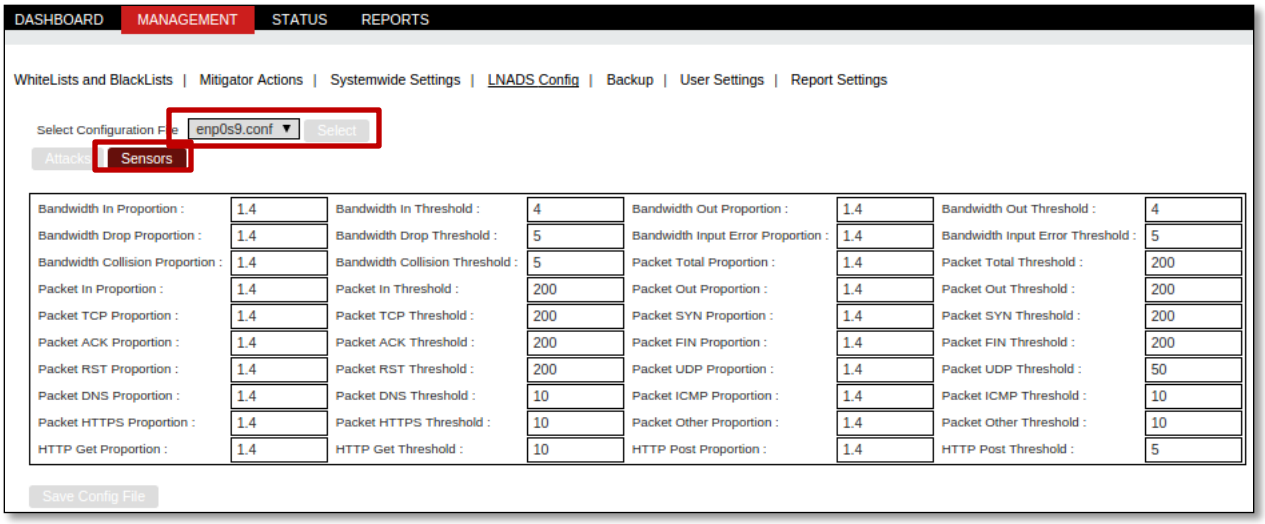



### Internal Interface Sensor Config

Select Configuration file interface as enp0s9.conf.

In Sensor section we find information regarding Bandwidth, Packets of the Interface with appropriate values.

Click on **Save Config File**tab to save changes if any are made to it.




| Parameters | Interface | Information | Example |
|---|---|---|---|
| Interface | - | Gives the name of the interface and shows the internal or external leg is used. Are managed by the interface to manually do not change. | interface enp0s8,ext |
| <sensor>_prop | <Sensor> Proportion | Determines the value of the specified sensor for proportion. Sensor values to see the sensor. | bandwidth_in_prop 1.4 |
| <sensor>_thresh | <Sensor> Threshold | Specifies the threshold value for the specified sensor. Sensor values to see the sensor. | bandwidth_in_thresh 1000 |
| <attack>_packet_syn | <attack> Multiplier | Albright used the multiplier while detecting. For the external interface used in the SYN Flood attack, ACK, fin, RST Flood, inner leg used for UDP Flood, ICMP | SYN_flood_packet_syn 1 |

| | | | |
|---|---|---|---|
| | | Flood, Flood, Flood, Flood, HTTPs DNS can Flood the POST. | |
| <attack>_packet_syn_enable | <attack> Detection | The detection of the attack. Types of inner and outer leg is used to attack is like a multiplier. | GET_flood_http_get_enable yes |

### Interface Sensor List

Table represents the Sensor List of the Interfaces.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Bandwidth In | Bandwidth Out | Bandwidth Drop | Bandwidth Inerr | Bandwidth Coll | Packet Total | Packet In | Packet Out |
| Packet TCP | Packet SYN | Packet ACK | Packet FIN | Packet RST | Packet UDP | Packet DNS | Packet ICMP |
| Packet HTTPs | Packet Other | Packet IP4 | Packet IP6 | HTTP Get | HTTP Post | | |

## 3. Auxiliary Scripts (Script)

Auxiliary section consists of briefly described scripts used by the system. These programs are kept in the folder**/opt/labris/libexec**. And the necessary conf files are kept in the folder **/opt/labris/etc/sysconfig**.

Note

- In order to run the commands in the following way is possible by running the **/opt/labris/libexec** command, then cd must enter into libexec folder

Functions of Scripts are mentioned below respectively.

• **labris-ddos-interfaces**

This program is using the machine interfaces to be used in the web interface of this information by specifying in the**/opt/labris/etc/sysconfig**/interfaces file. It takes a half an hour to run cron-adjustment and thus it has been made. In the case if a new machine is added to the interface to a maximum of half an hour or**/labris-ddos**-interfaces must be run manually with the command in this program. Otherwise, the new interfacein the web interfacesdoesn't appear.

• **lnads-conf-backup**

This script provides the system httpd.conf files and these files are being backed up. These backup files can bemanaged, backup interface described in Chapter 1.3.4. Backup files or folders will be**/opt/labris/etc/sysconfig/lnads-confbackup-**files should be written to file.

This is the same directory as the files to exclude list lnads-confbackup-exludes file should be written.Backup files lnads with openssl-confbackup-pass is encrypted password in reading. Do not change this file or do not remove!.
By running the backup_dosya with the command**/lnads-conf-backup**< backup_dosya > with the given name backup.

• **threshold_suggestions. Py**

This script is taken from the appropriate threshold values for the usingsystem.
threshold_suggestion is run with the command. Receipt information system suitable for data history for using after a certain period of time the installation is required.

• **lnads-conf-files**

This script lnads-lnads-confbackup-confbackup-files and files in the given backup requested exludes/unwanted outputs a list of files.
**/lnads-conf**-files command is not to be desired whether backup file ... the list can be checked for accuracy.

• **lnads-auto-backup**

This script lnads-conf-makes a backup of the backup script by using the four times a day. To change the time of the backup, as described in the**/etc/crontab** file before
**0 */6 *** root/opt/labris/libexec/lnads-auto-**backupline required changes can be made.

Backing up front as defined in the**/usr/local/www/apache22/ddos-webgui/backups** folder. It is recommended that you not change this folder.

• **lnads-conf-restore**

This script using any backup file is reinstalled. After reinstalling the current conf files or you must be careful. Apart from that, the programs that uses the confs being introduced not need to be considered again in the program files are installed. This is why it is recommended that you do the restore process from the web interface.

By running the**/lnads-conf-restore < backup_dosya >** shaped shoulders again, the requested file is installed in the system.

• **lnads-log-cleaner**

The interface is specified in the Keep argument the old meta (/data/labris/attack extension) files and backup files are cleaned up. If the disks load over 90% occupancy rate of the meta files then this value will be removed until the bottom. Once a day to run cron setting, **/etc/crontab file0 0 *** root/opt/labris/libexec/lnads-logcleaner**work as desired can be achieved by changing the line.

Conf file as**/opt/labris/etc/sysconfig/lnads-log-cleaner.conf** uses. This file contains the metadata and backup files to extract the value of the extension and the extension of the xml file should be set to keep log.

• **ntuple-manager**

This script allow you control ethernet based rules. Here is simple usage

Add new rule

ntuple-manager -A -i interface [-s src_ip | -d dst_ip | -p src_port | -o dst_port | -P <tcp|udp> ]

Delete a rule by its rule index

ntuple-manager -D rule_index -i interface

List rules of an interface

ntuple-manager -L -i interface

• **labris-remote-manager**

With this script, remote synchronization can be configured between two or more HARPP appliance.

```
# labris_remote_manager.py --help

Usage: labris_remote_manager.py [--add|--delete|--exec|--list] [options]

 Use --help to see all options

This script manages remote labris servers with ansible

Options:

 -h, --help          show this help message and exit

 Modes:

  You can use below modes give commands

  --add             Add host with given host parameters

  --delete          Delete given host

  --exec=<playbook,[playbook]>

                    Run given playbooks on given hosts

  --list            List added hosts.

 Options:

  You can use below options to give mode parameters

  --host=<host,[host]>

                    Host IP. Should be given on add, delete. On exec mode

                    you can give more than host or leave it if you want to

                    run on all hosts.

  --password=<password>

                    Password for host. Should be given on adding.
```

**Tasks**

Tasks are located at /opt/labris/etc/labris-remote-manager/playbooks

| | |
|---|---|
| lnads.yml | Syncs lnads configuration. |
| logs.yml | Syncs attacks evidence and logs. |
| mitigatiton.yml | Syncs mitigation options. |
| reports.yml | Syncs reports. |
| rrd.yml | Syncs rrd database. |
| users.yml | Syncs users. |
| whitelist.yml | Syncs whitelist, blacklist and admin list. |

Labris
NETWORKS