Unified Threat Manager

User Manual

allo.com

Copy Right

Proprietary Rights

The information in this document is Confidential to Allo and is legally privileged. The information and this document are intended solely for the addressee. Use of this document by anyone else for any other purpose is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution of this information is prohibited and unlawful.

Disclaimer

Information in this document is subject to change without notice and should not be construed as a commitment on the part of **allo.com.** And does not assume any responsibility or make any warranty against errors. It may appear in this document and disclaims any implied warranty of merchantability or fitness for a particular purpose.

About this manual

This manual describes the allo product application and explains how to work and use it major features. It serves as a means to describe the user interface and how to use it to accomplish common tasks. This manual also describes the underlying assumptions and users make the underlying data model.

Document Conventions

In this manual, certain words are represented in different fonts, typefaces, sizes, and weights. This highlighting is systematic; different words are represented in the same style to indicate their inclusion in a specific category. Additionally, this document has different strategies to draw User attention to certain pieces of information. In order of how critical the information is to your system, these items are marked as a note, tip, important, caution, or warning.

Icon	Purpose
	Note
	Tip/Best Practice
	Important
	Caution
	Warning

- **Bold** indicates the name of the menu items, options, dialog boxes, windows and functions.
- The color blue with underline is used to indicate cross-references and hyperlinks.
- Numbered Paragraphs - Numbered paragraphs are used to indicate tasks that need to be carried out. Text in paragraphs without numbering represents ordinary information.
- The Courier font indicates a command sequence, file type, URL, Folder/File name e.g. www.allo.com

Support Information

Every effort has been made to ensure the accuracy of the document. If you have comments, questions, or ideas regarding the document contact online support: http://support.allo.com

Table of Contents

1. Introduction

1.1 Overview

Shield UTM Appliances is the Unified Threat Management solution that target the security needs for Home/SOHO users. The appliance provides the integrated Firewall, Intrusion Prevention, SSLVPN functionalities.

Unified threat management (UTM) is an emerging trend in the network security market. UTM appliances have evolved from traditional firewall/VPN products into a solution with many additional capabilities. UTM solutions also provide integrated management, monitoring, and logging capabilities to streamline deployment and maintenance. UTM appliances combine firewall, gateway anti-virus, and intrusion detection and prevention capabilities into a single Platform. UTM is designed protect users from blended threats while reducing complexity.

The Unified Threat Management (UTM) Appliance connects your local area network (LAN) to the Internet through one or two external broadband access devices such as cable mode ms or DSL modems. Dual wide area network (WAN) ports allow you to increase the effective data rate to the Internet by utilizing both WAN ports to carry session traffic, or to maintain a backup connection in case of failure of your primary Internet connection. As a complete security solution, the UTM combines a powerful, flexible firewall with a content scan engine that protect your network from denial of service (DoS) attacks, unwanted traffic, traffic with objectionable content, spam, phishing, and Web-borne threats such as spyware, viruses, and other malware threats. The UTM provides advanced IPSec and SSL VPN technologies for secure and simple remote connections. The use of Gigabit Ethernet LAN and WAN ports ensures extremely high data transfer speeds. The UTM is a plug-and-play device that can be installed and configured within minutes

1.2 Technical Specifications

No of Interfaces	Two 1Gbps WAN port & four 1Gbps LAN ports, 1 console interface, 1 USB port
Status Firewall Inspection	Yes
Deep Packet Inspection	Yes
Signatures Support	~4000 active signatures from snort VRT/emerging threats
Application Protocols Detection	70+
Maximum No of Connections	20000
Maximum No of New Connections Per Second	1800
Maximum No of SSLVPN Clients	100
Authentication	X509 certificates, internal user DB
Logging	Local log viewer, Syslog
Device Management	HTTPS GUI, SNMP
Hardware	Cavium Octeon II 63xx, 2cores 800MHz
RAM	1 GB

Notification LEDs (On the front panel of the UTM)

1.3 Equipment Structure

1.3.1 UTM Rear View

Figure 1: UTM Rear View

1.3.2 UTM Front View

Figure 2: UTM Front View

1.4 Initial Setup & Configuration

1.4.1 Connecting the Hardware

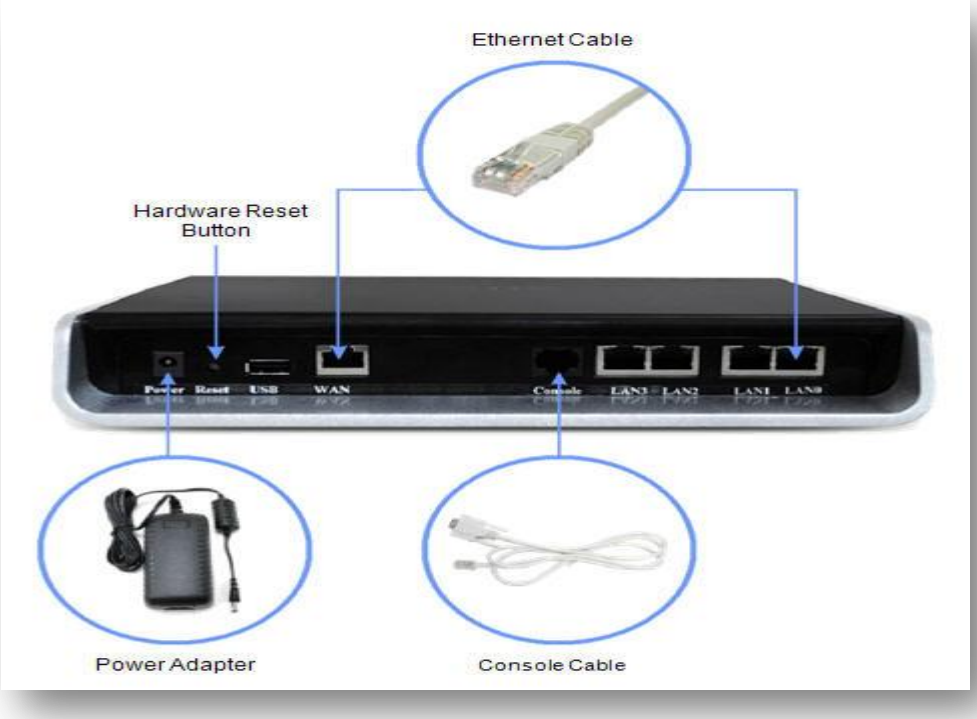


Figure 3: Connecting the Hardware

1.4.2 Network Deployment

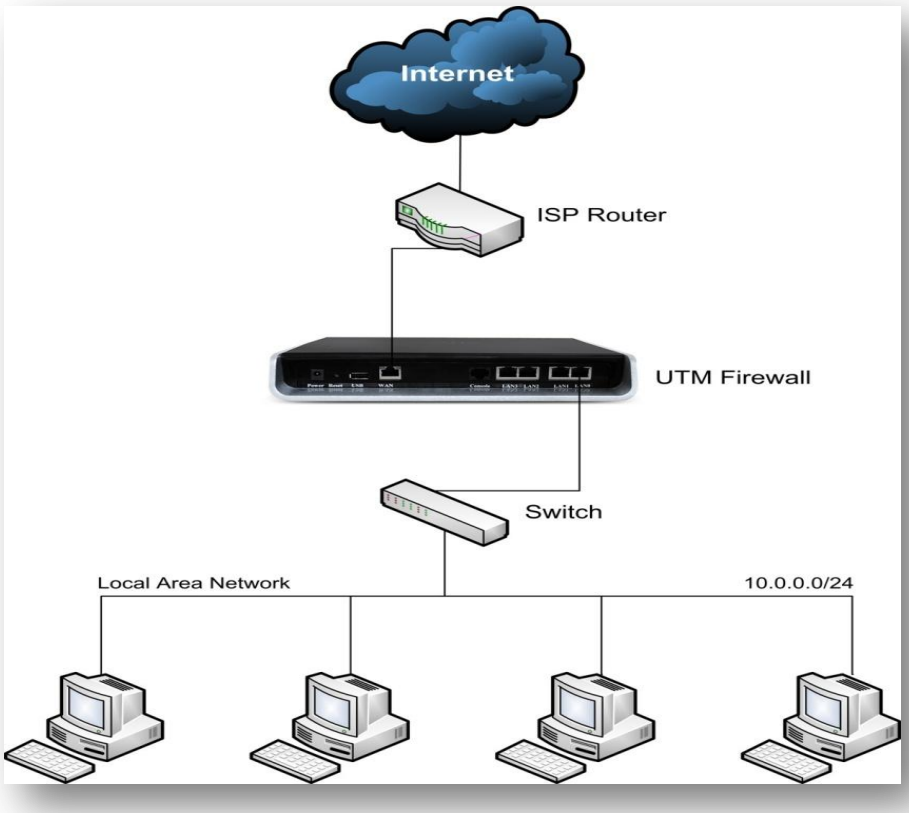


Figure 4: Network Deployment

Default Configuration

Ethernet Port	IP Address
LAN 0-3 > eth1	10.0.0.1/255.255.255.0
WAN > eth0	10.1.0.1/255.255.255.0
Management VLAN (Accessible via LAN Ports)	192.168.1.1/255.255.255.0
Default Firewall Mode	Router

Management Service	Default Credentials
Web UI	admin/admin
SSHCLI	admin/admin123

1.4.3 Connect UTM Firewall

- Connect the appliance to the power socket using the power cable.
- Connect the PC to one of the LAN ports of the Appliance.
- Your PC will get an IP address from 10.0.0.0/24 subnet.
- You can access the Configuration management WebUI from the browser on the PC with the URL http://10.0.0.1/ or http://192.168.1.1
- The recommended browsers for accessing UTM 1.0 WebUI is Mozilla Firefox / Internet Explorer 8 and above.
- Accept the Self signed SSL Certificate and Login to the UTM appliance using default Web UI credentials.

Figure 5: UTM Login page

- WebUI is running on the secure http server. Accessing http://10.0.0.1 or http://192.168.1.1 will redirect to https://10.0.0.1/ or https://192.168.1.1/

2. Dashboard

On logging into the UTM WebUI, the dashboard will be shown. The user can visit the dashboard page from the any configuration page in the UTM WebUI, by clicking the UTM Product Icon that appears in the left corner of the Top panel.

The Dashboard shows memory usage, CPU usage, uptime of the device, a list of all interfaces with their IP address and status, etc..,

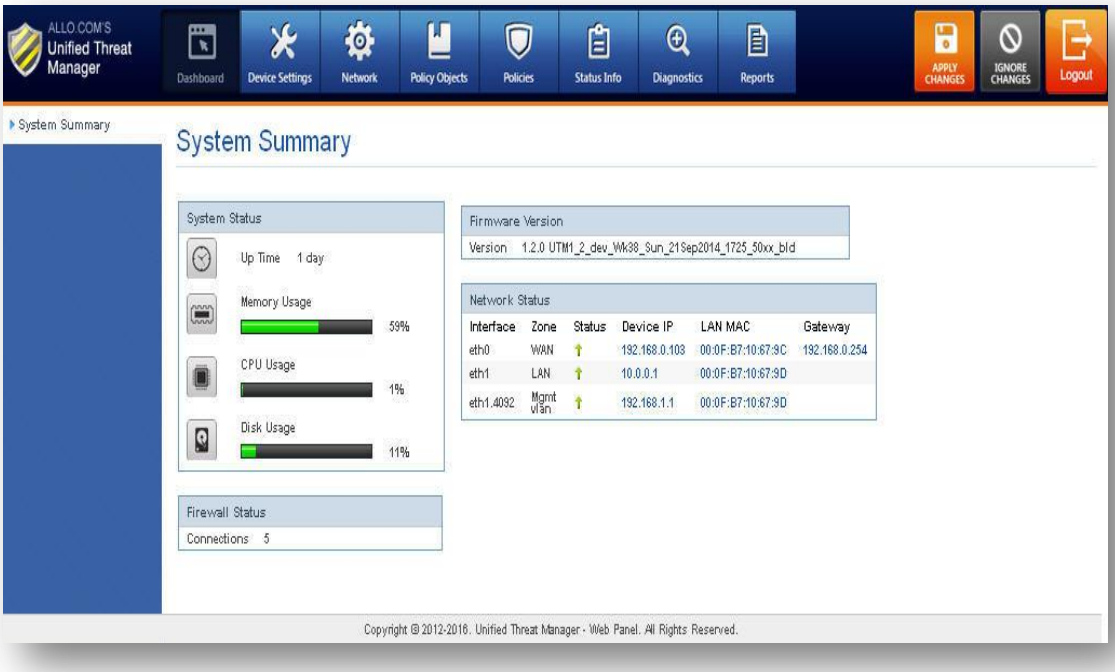


Figure 6: Dashboard

3. Device Settings

3.1 Host Config

Navigate through **Device Settings** > **Host Config**

Configuring hostname and domain name of the device.

Figure 7: Host Config

3.2 Admin User

Navigate through **Device Settings** > **Admin User**

The user allows for configuring web UI administrator username and password. User can change the web UI username and password.

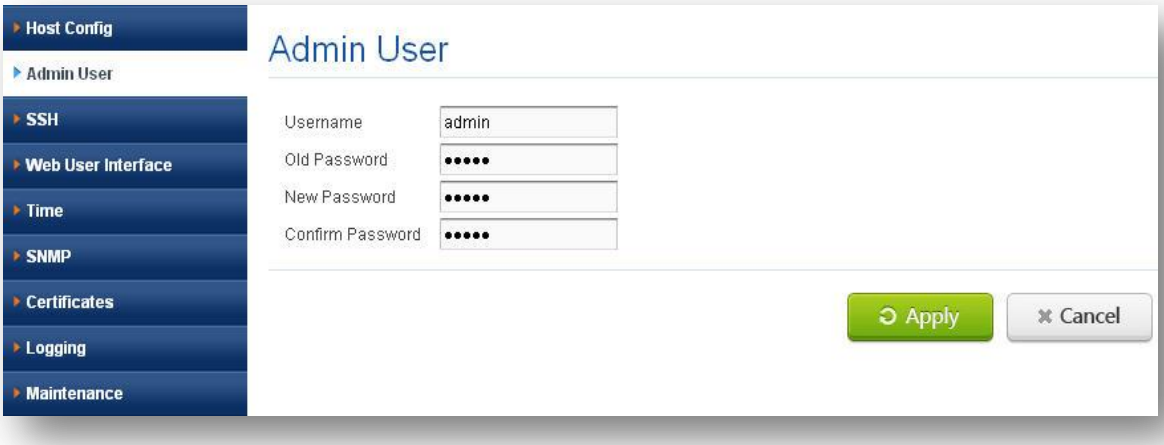


Figure 8: Admin user

3.3 SSH

Navigate through **Device Settings** > **SSH**

Secure SHell (**SSH**) is a network protocol for secure data communication, remote command line login, remote command execution, and other secure network services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH Client programs, respectively.

SSH works on top of TCP protocol and its default port number is 22.

It is used to login into the device securely using public and private host keys. This section includes port and session timeout. Session timeout specifies how long the user session show is valid.

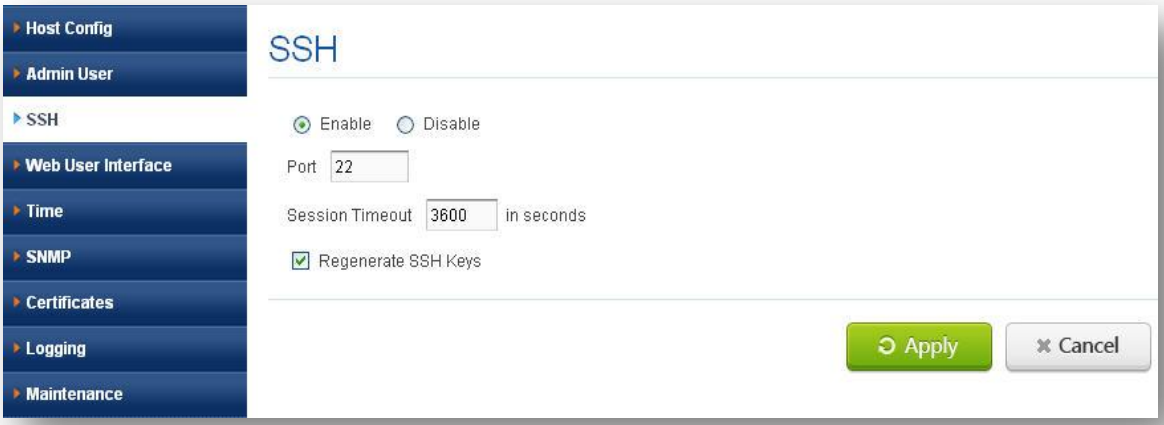


Figure 9: SSH

3.4 Web User Interface

Navigate through **Device Settings**> **Web User Interface**

It helps configuring web UI port and session time out. Session timeout specifies how long the web UI session should be valid.

Figure 10: Web User Interface

3.5 Time

Navigate through **Device Settings** > **Time**

The user allows for configuring time settings to the device using NTP server or using manual settings. Using sync with NTP, the user has to provide the NTP servers to sync with the time along with the zone specified in the zone list. In manual settings, user has to set the hour/minute and select hour format (AM/PM), date/month/year. The Time zone list provides a list of all time zones. NTP synchronizes for every specified update interval.

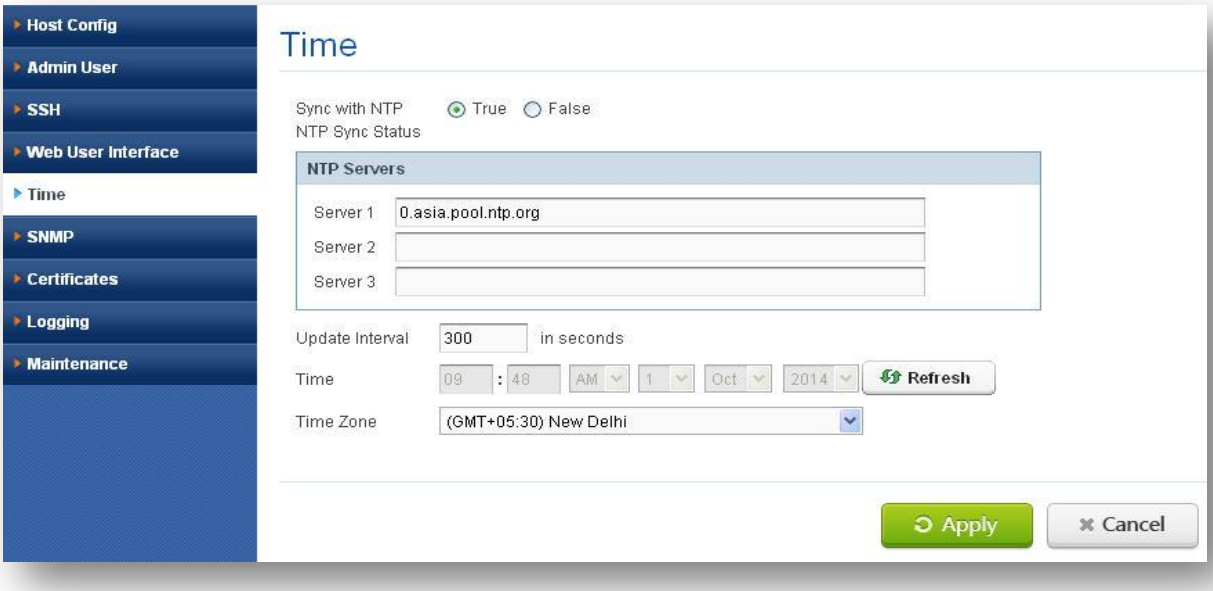


Figure 11: Time

3.6SNMP

Navigate through **Device Settings > SNMP**

Simple Network Management Protocol (SNMP) is an application layer protocol for managing devices on IP networks. It runs on port 161 and 162(trap) and mostly used in network management systems to monitor network-attached devices.

In UTM's SNMP can be Enabled/Disable by clicking on the respective buttons. User can configure any appropriate System Name, System Contact, and System Location into those fields.

Access Control List: SNMP Access controls Lists (ACL) are configured in order to allow the SNMP traffic through the UTM Device.

Figure 12: Add Access Control List

Trap Servers List: A trap is an SNMP agent's way of notifying the manager that "something is wrong". UTM SNMP traps will capable of sending SNMP traps on their own to alert an SNMP manager when they experience a problem.

Figure 13: Create Trap Servers List

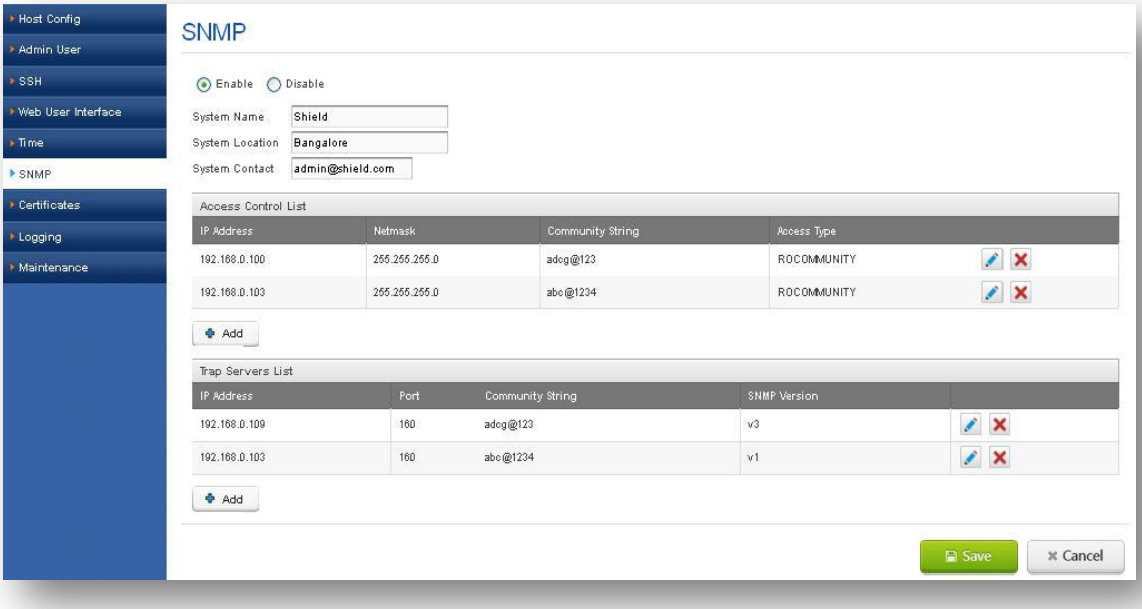


Figure 14: SNMP

3.7 Certificates

Navigate through **Device Settings** > **Certificates**

In this section includes two sections:

3.7.1Built-in certificates

#Built-In which includes default root certificates about 200+.

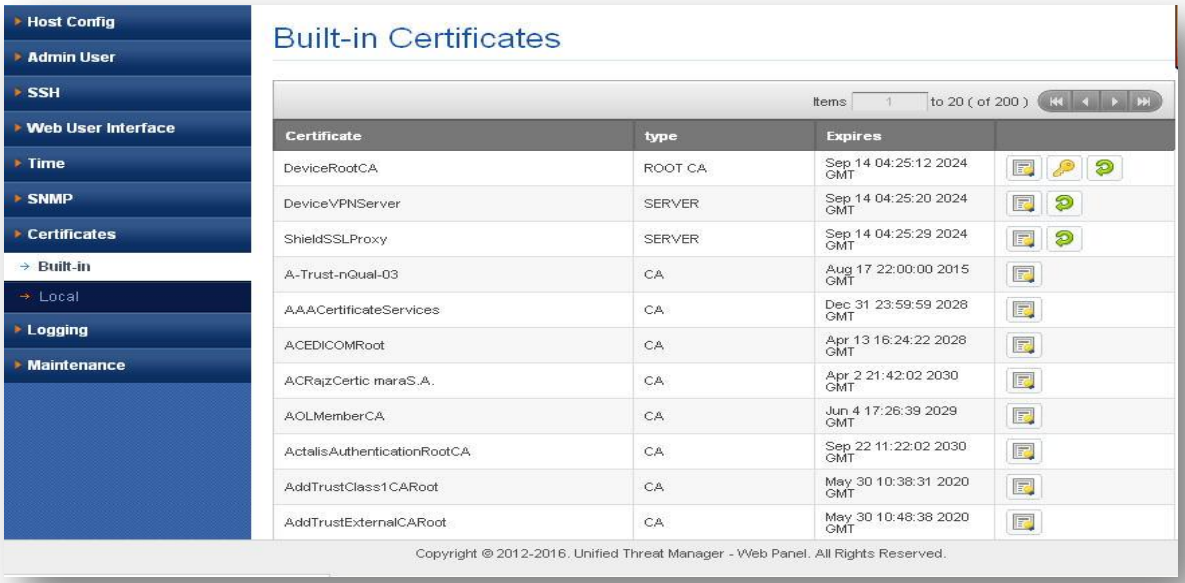


Figure 15: Built-in Certificates

3.7.2 Local Certificates

Local which user uploaded certificates in PKCS12 format contains root certificate, server certificate and server key. Challenge password is the password for extracting uploaded PKCS12 file and New Certificate Name is the name for uploaded certificate.

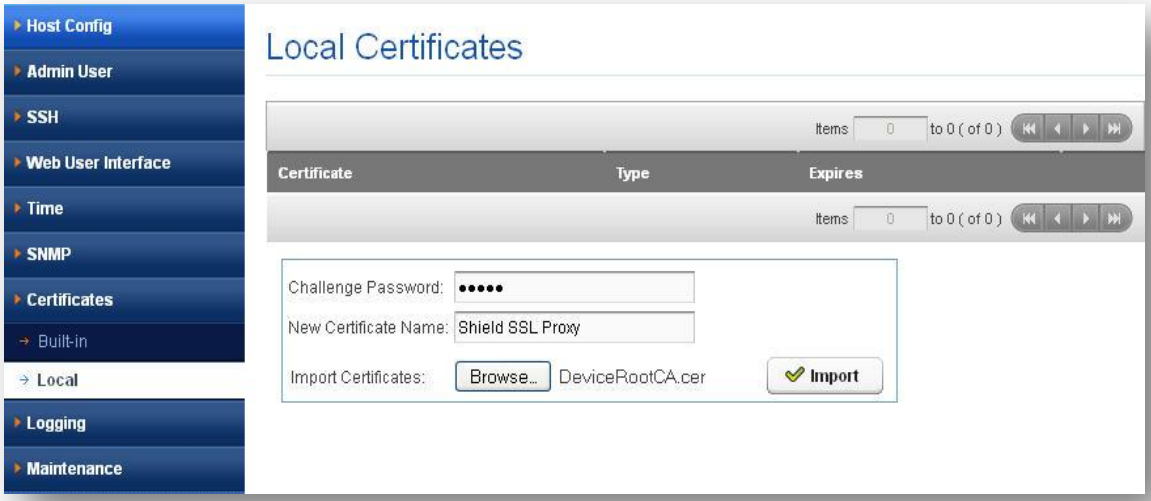


Figure 16: Local Certificates

3.8 Logging

Navigate through **Device Settings** > **Logging**

Configuring logging server address to where the log information has to be sent like Firewall alerts, IPS alerts, VPN alerts etc.

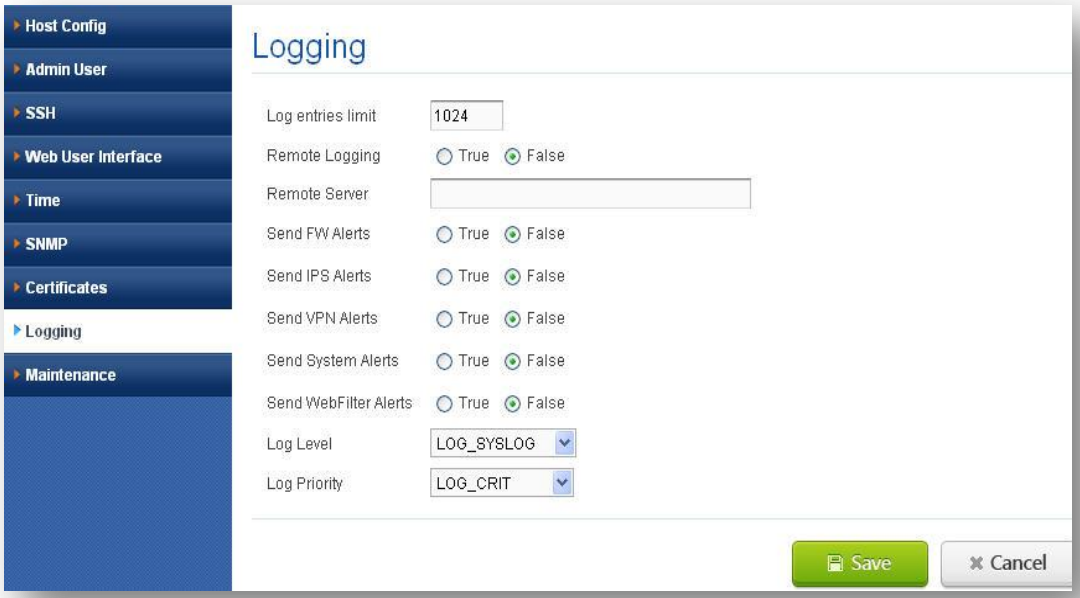


Figure 17: Logging

3.9 Maintenance

Navigate through **Device Settings** > **Maintenance**

This section consists of two parts: Administration and Firmware.

3.9.1 Administration

Navigate through **Device Settings** > **Maintenance** > **Administration**

It includes

#restart services which restart all the services in device like IPS, VPN, etc..

#restart appliance which reboots the device.

To shut down appliance which turns off the device.

#configuration backup includes

•Backup configuration which provides facility to take back up of current configuration settings.

•Restore configuration which provides facility to restore the configuration which is provided.

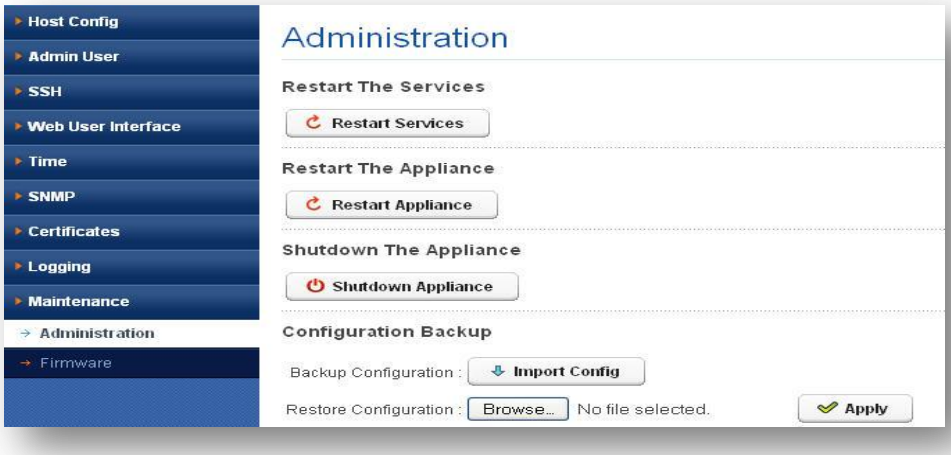


Figure 18: Administration

3.9.2 Firmware

Navigate through **Device Settings** > **Maintenance** > **Firmware**

It includes

#factory reset- it resets the device to default configuration settings.

#uploads firmware which provides the facility to upload the latest firmware build and install it on the device.

the firmware last update shows the last firmware update information.

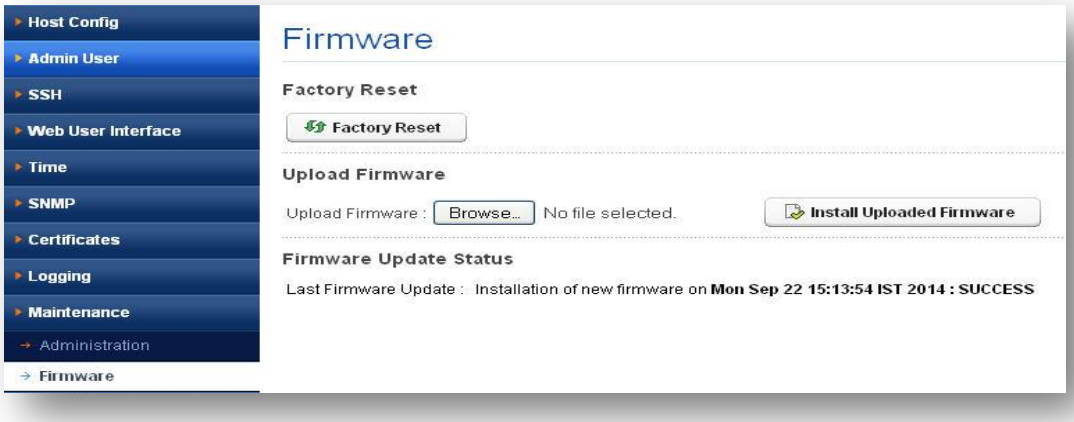


Figure 19: Firmware

4. Network Settings

4.1 Interfaces

Navigate through **Network** > **Interfaces**

In this section, we can configure interfaces like WAN (eth0), LAN (eth1), and whether the interface can be in DHCP mode or Static mode. By default WAN interface has IP address 10.1.0.1/255.255.255.0 which is in Static mode and LAN interface has IP address 10.0.0.1/255.255.255.0 which has DHCP running on this interface.

We can configure gateway to the interfaces only in Static mode. And also Maximum Transmission Unit (MTU) (68 - 1500) (communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards) for each interface.

Select which interface will be used for this connection either on external or internal interfaces. PRIMARY means the connection will be on the external interface.

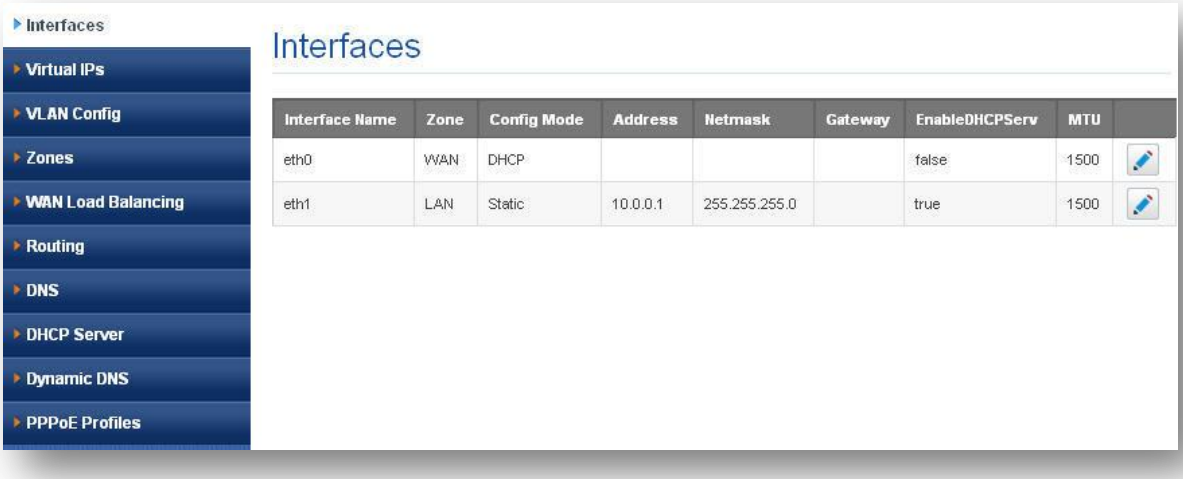


Figure 20: Interfaces

4.2 Virtual IPS

Navigate through **Network** > **Virtual IPS**

UTM's VIPs addressing enables hosting for several different applications and virtual appliances on a server with only one logical IP address

Figure 21: Create Virtual IPS

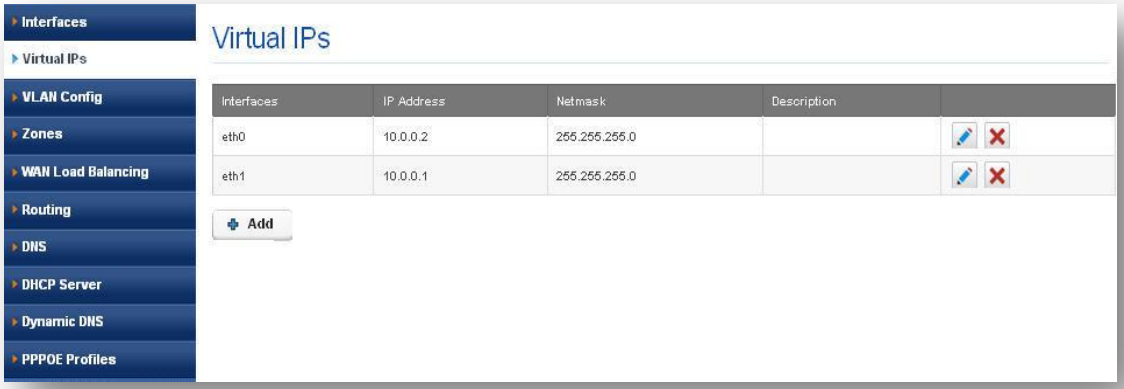


Figure 22: Virtual IPS

4.3 VLAN Config

Navigate through **Network** > **VLAN Config**

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

The user can configure Virtual Local Area Network (VLAN) by providing information like Tag ID which specifies unique tag id for each VLAN, interface name to be selected. VLAN routing, IP address and net mask for VLAN whether to enable DHCP for VLAN. By default management VLAN is added to the device.

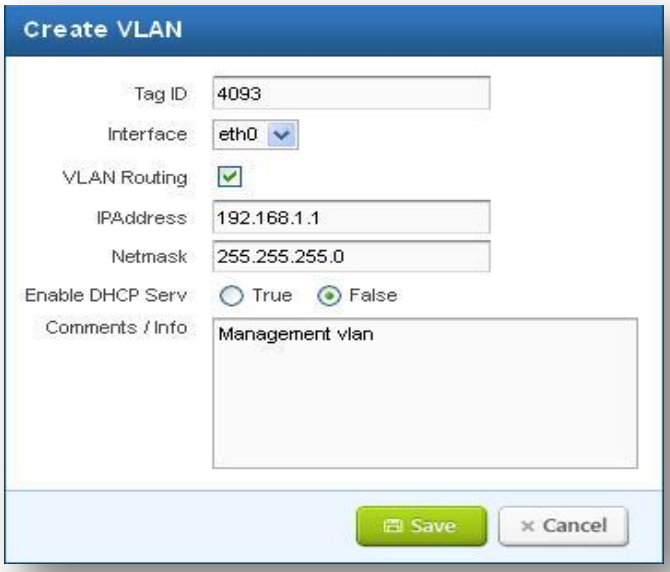


Figure 23: Create VLAN

Figure 24: VLAN Config

4.4 Zones

Navigate through **Network** > **Zones**

UTM zones are used to create any area that is separated from another. It allows user to create their individual LAN and WAN Zone according to their network environment naturally.

Figure 25: Create Zone

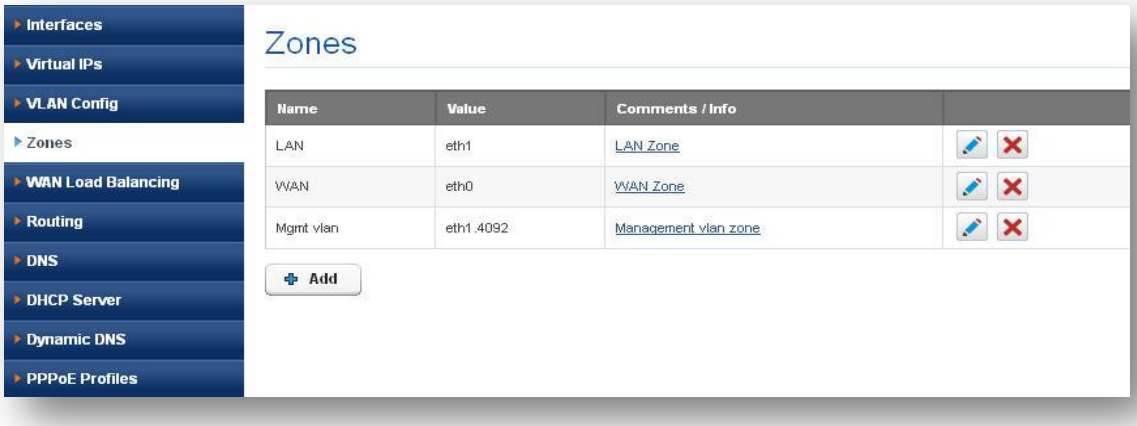


Figure 26: Zones

4.5 WAN Load Balancing

Navigate through **Network** > **WAN Load Balancing**

UTM has the ability to balance traffic across two WAN links without using complex routing protocols. It uses following 4 techniques to balance load across two WAN:

- Active Failover
- Round Robin
- Spill over
- Weight based

User can make use of any above Load balancing technique for managing their network traffic.

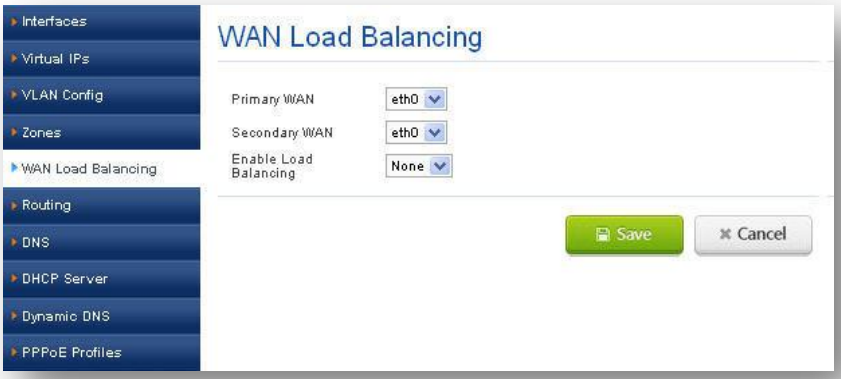


Figure 27: Web Load Balancing

4.6 Routing

4.6.1 Static Routes

Navigate through **Network** > **Routing> Static Routes**

We configure routes to the destination network by specifying destination address, net mask and metric value (0 - 31). Gateway is optional.

Figure 28: Routing

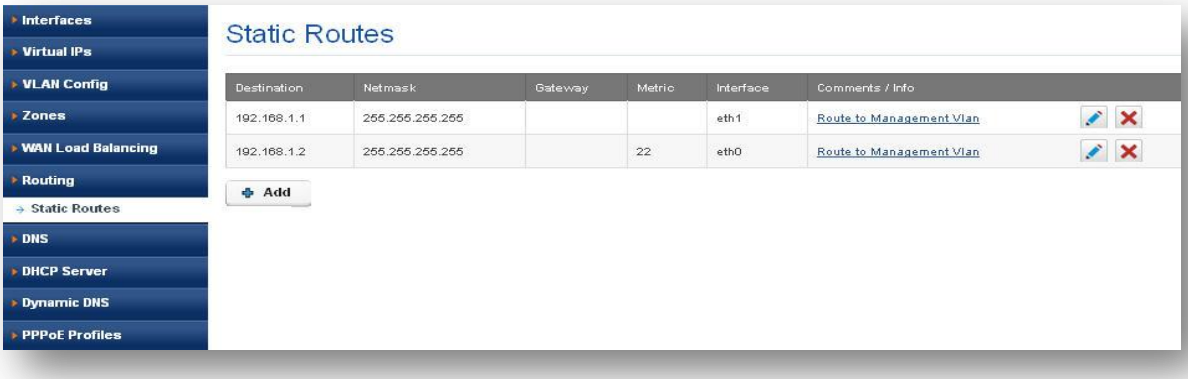


Figure 29: Static Routes

4.7 DNS

Navigate through **Network** > **DNS**

Domain Name System (DNS) is a service translates domain names into IP addresses. In UTM user can configure Primary DNS, Secondary DNS, and Tertiary DNS by giving either DNS server IP or name.

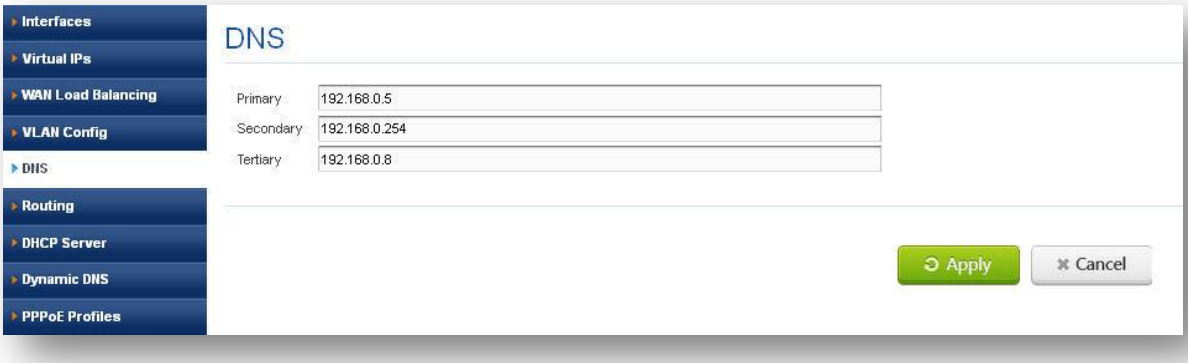


Figure 30: DNS

4.8 DHCP Server

Navigate through **Network** > **DHCP Server**

It is used to configure automatic dynamic and static IP leasing to DHCP requests received from network hosts.

We can configure Dynamic Host Configuration Protocol (DHCP) for each LAN and VLAN interfaces. We need to specify interface name, start address, end address, network mask and gateway. And also specify primary DNS (mandatory), secondary DNS, WINS and Domain.

Figure 31: Add DHCP Server Settings

Conflict time (60 – 3600)

Decline time (60 – 3600)

Offer time (60 – 3600) and

Max lease (1 – 125).

We can configure static mapping by adding the MAC address of a client , the IP address assign to clients, hostname to the client and whether to enable this rule or not.

Figure 32: DHCP Server

4.9 Dynamic DNS

Navigate through **Network** > **Dynamic DNS**

It is used to configure access to third-party dynamic DNS service providers

Figure 33: Add DDNS

If another Dynamic DNS Profile has been enabled on the WAN interface already; you can enable only one Dynamic DNS profile on the WAN interface at a time.

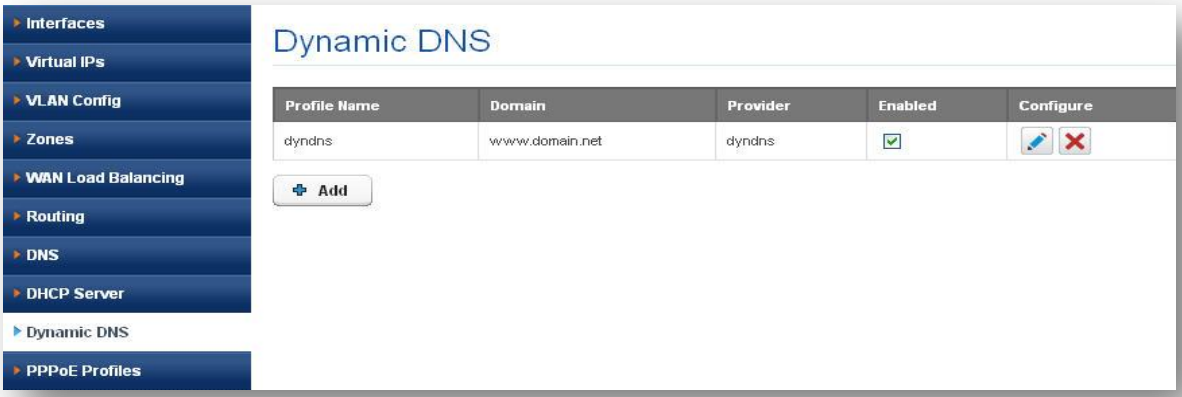


Figure 34: Dynamic DNS

4.10 PPPoE Profiles

Navigate through **Network** > **PPPoE Profiles**

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames and allows data communication between two network entities or points. UTM allows user to configure PPPOE profiles in PAP /CHAP authentication modes.

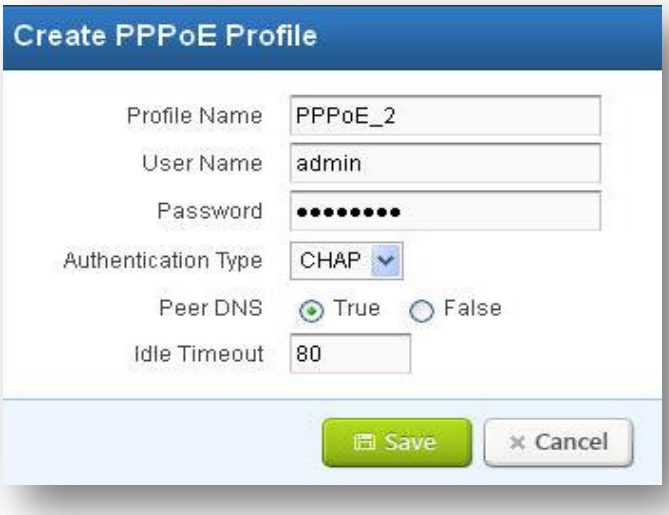


Figure 35: Create PPPoE Profile

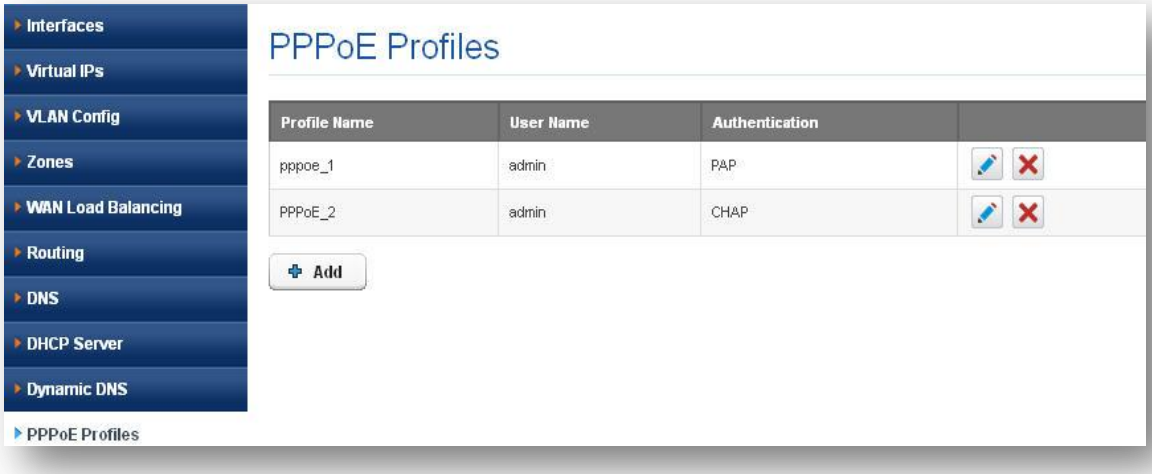


Figure 36: PPPoE Profiles

5. Policy Objects

Policy objects are building blocks for configuring Firewall, VPN, Web Filter, User Policies etc in UTM. They are something that can be configured once and then used over and over again to build what you need. They can assist in making the administration of the UTM unit easier and more intuitive as well as easier to change.

By configuring these objects with their future use in mind as well as building in accurate descriptions the firewall will become almost self documenting. That way, months later when a situation changes, you can take a look at a policy that needs to change and use a different firewall object to adapt to the new situation rather than build everything new from the ground up to accommodate the change.

5.1 Address Groups

Navigate through **Policy Objects** > **Address Groups**

Address Objects are grouped together to create some policies called as Address Groups. Policies can apply to created group itself.

If you have a number of addresses or address ranges that will commonly be treated the same or require the same security policies, you can put them into address groups, rather than entering multiple individual addresses in each policy refers to them. It saves user time.

It specifies the group of address objects which includes network address, host address; address range of hosts etc..,

Group Name: It specifies the unique address group name which can be used in Policies like Firewall Policies, User Policies, etc..; it ranges from 5 – 32 characters. Eg. LAN_GROUP

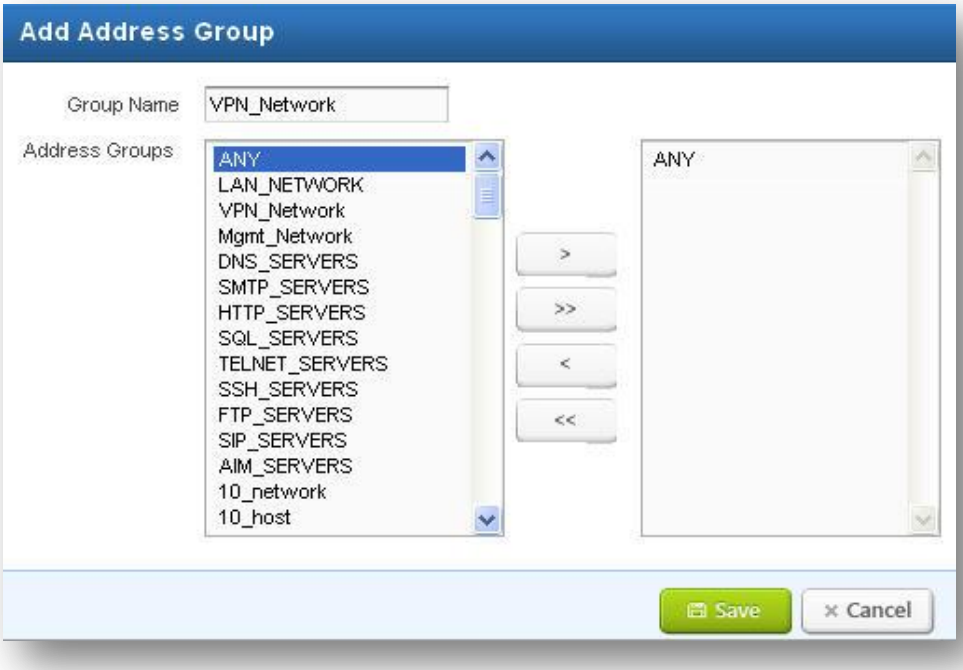


Figure 37: Add Address Group

Figure 38: Address Groups

5.2 Address objects

Navigate through **Policy Objects** > **Address Objects**

Address Objects defines sources and destinations of network traffic and are used when creating policies. When properly set up these Address objects can be used with great flexibility to make the configuration of firewall/Web filtering policies simpler and more intuitive. The UTM policies verify and check the IP addresses contained in packet headers with a security policy's source and destination addresses to determine if the security policy matches the traffic.

It determines the network address, host address, range of addresses and Mac address of the server. Address object name specifies the unique name for address object which used in Policies, etc.., it ranges from 3 – 32 characters. Eg. LAN_NETWORK.

In network address, user has to define the IP address and net mask (Eg. IP address: 10.0.0.0, Net mask: 255.255.255.0). In host address, user has to specify a valid host address (Eg. 10.0.0.5). In range of addresses, user has to specify start and end address (Eg. Start IP: 10.0.0.5, End IP: 10.0.0.8). In Mac address, user has to specify a valid Mac address in ':' format (Eg. 11:22:33:44:55:66).

Figure 39: Create Address Object

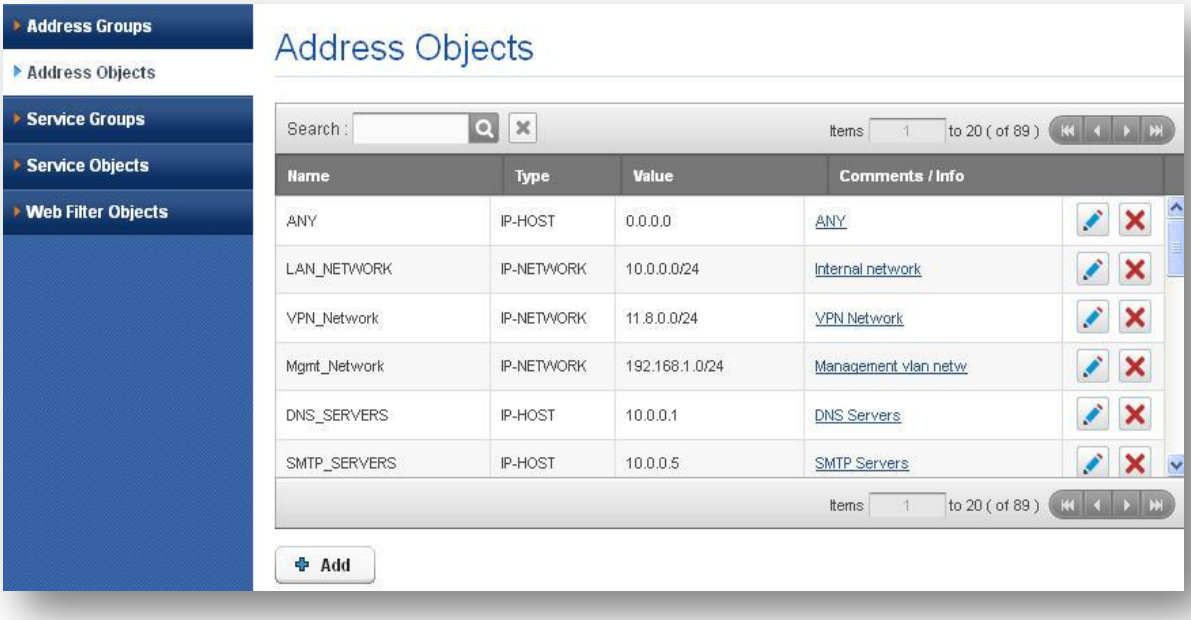


Figure 40: Address Objects

5.3 Service Groups

Navigate through **Policy Objects** > **Service Groups**

Like Address Objects, services can also be bundled into Service groups for ease of administration.

Ex: TCP_Services (HTTP, FTP, SMTP)

UDP_SERVICES (DNS, TFTP)

It designates the group of service targets which includes services like ssh, http, SMTP, etc..,

Group Name: It specifies the unique group name which can be used in Policies like Firewall Policies, User Policies, etc... It ranges from 3 – 32 characters. Eg. WEB_SERVICES

Figure 41: Create Service Group

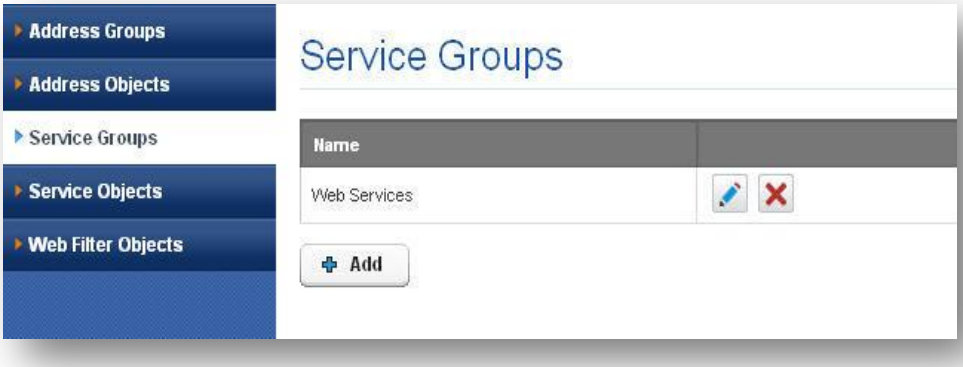


Figure 42: Service Groups

5.4 Service objects

Navigate through **Policy Objects** > **Service Objects**

TCP/IP suite is having a number of different services and Protocols. These protocols & Services using port number from 1-65535 port numbers. Each port number is having its own service.

For example HTTP having port number 80 (TCP)

SMTP having port number 25(TCP)

DNS having port number 53 (UDP) etc.

Using port number we can create services and configure Firewall, NAT, Web Filtering policies etc.

It specifies the services like SSH, http, SMTP, SIP, etc.., Object name specifies the unique name for service object which used in Policies, etc.., and it ranges from 3 – 32 characters. Eg. Http.

Figure 43: Create Service Object

Protocol: It specifies which protocol to be used for the service object. Protocols like TCP, UDP, TCP_UDP and ICMP.

Port: It specifies the port for protocols like TCP and UDP. Eg. 22

ICMP type: It specifies the type of icmp to be used for the service object. Eg. Type 0: Echo Reply

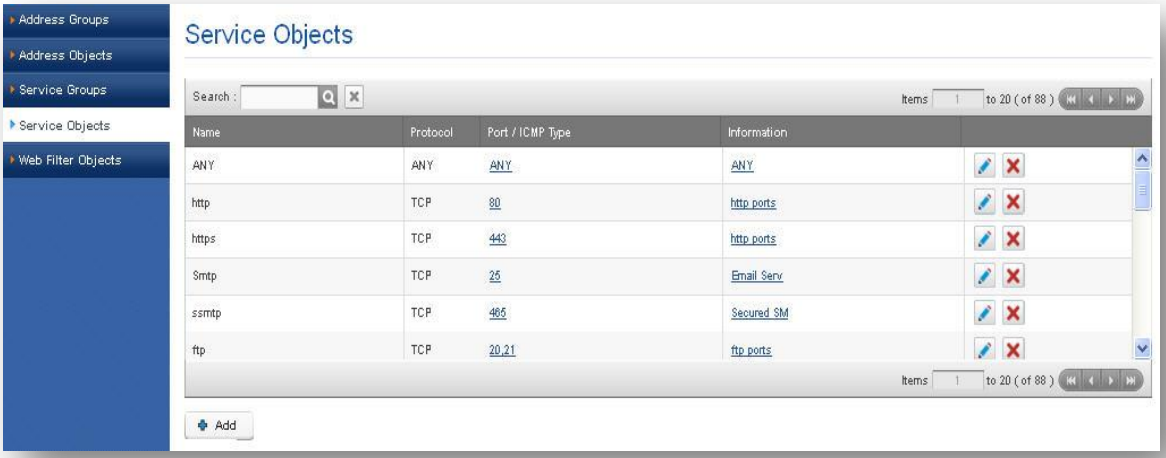


Figure 44: Service Objects

5.5 Web Filter objects

Navigate through **Policy Objects** > **Web Filter Objects**

It narrows down the list of objects which are used in Web Filtering for blocking specific sites using the URL, IP Address, Keyword and Categories.

Figure 45: Create Web Filter Objects

Name: unique name for web filter objects. It ranges from 3 -32 characters. Eg. Videos

URL: It specifies the URL list, which is used in web filtering for blocking the sites mentioned. Eg. www.allo.com

IP address: It specifies the IP addresses of sites to be blocked using web filtering. Eg. IP address of www.google.com is 173.194.117.114.

Keyword: It specifies a list of keywords which are used to block sites based on the keywords listed. Eg. Face to block Facebook site.

Categories: It specifies a list of categories like ads, blog, etc.., Eg. Ads

Figure 46: Web Filter objects

6. Policies

6.1 Firewall

Navigate through **Policies**> **Firewall**

It filters the inbound and outbound traffic on a network, allowing safe & secure traffic to pass while blocking insecure traffic.

A firewall is used to maintain a network secure. The primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a configured rule set.

A network's firewall builds a bridge between an internal network that is assumed to be securing, trusted, and another network, usually an external (Untrusted) network, such as the Internet, that is not assumed to be secure and trusted.

6.1.1 Firewall Settings

Navigate through **Policies**> **Firewall > Firewall Settings**

Firewall Settings allows user to configure TCP connection timeout, TCP Session timeout, TCP/UDP connection Flood Detect Rate in Global firewall Settings.

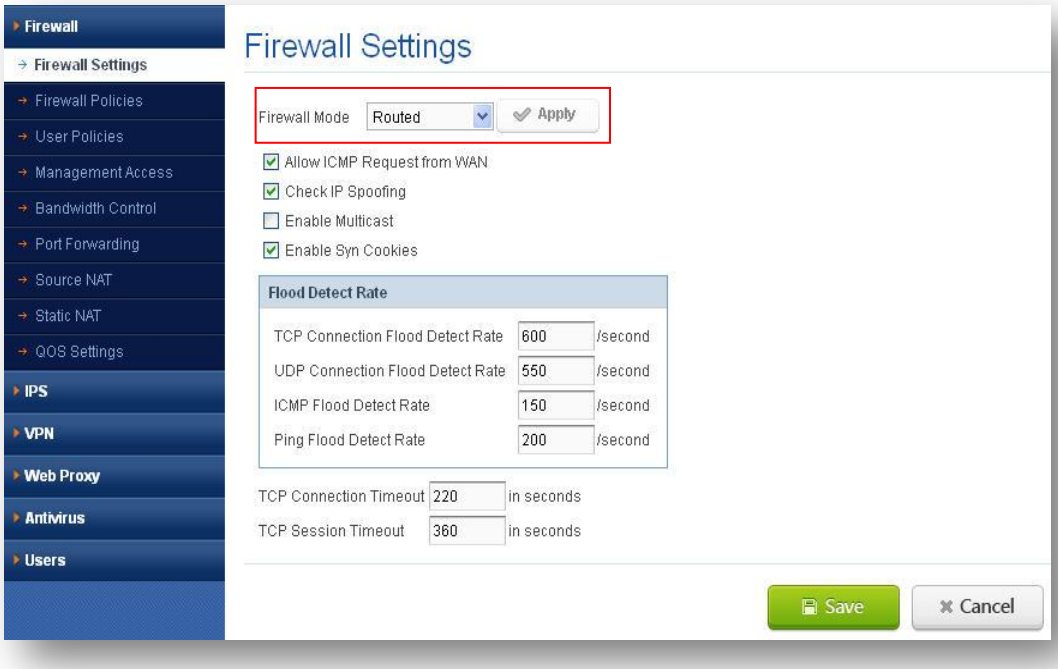


Figure 47: Firewall Settings

UTM Firewall works in two modes:

I. Routed
II. Transparent

Routed Mode

UTM firewall having LAN (Private/trusted) &WAN (Public/Untrusted) networks. Routed mode allows traffic coming from private network (LAN) to Public network (WAN) without much inspection. It will filter and do the deep inspection on whatever the traffic coming from WAN to LAN. If any malicious traffic coming from WAN/Public network to LAN then UTM Firewall and IPS (Intrusion Prevention System) will simply drop the particular packet.

Transparent Mode

There are no LAN & WAN networks it works in bridge mode. Transparent mode is typically used to apply the features such as Security Profiles etc. on a private network where the UTM unit will be behind an existing firewall or router.

The characteristics of transparent mode are:

• The UTM device is invisible to the network.

• All of its interfaces are on the same subnet and having the IP addresses which are in same network.

6.1.2 Firewall Policies

Navigate through **Policies**> **Firewall > Firewall Policies**

- The default policy configuration of the UTM Firewall allows all connections from LAN to WAN.
- To check /Modify Navigate to: Policies > Firewall Policies > LAN > Edit > Policy Setting > (You can see here Destination Zone 'WAN' Action 'Allow' Direction 'OUTBOUND')

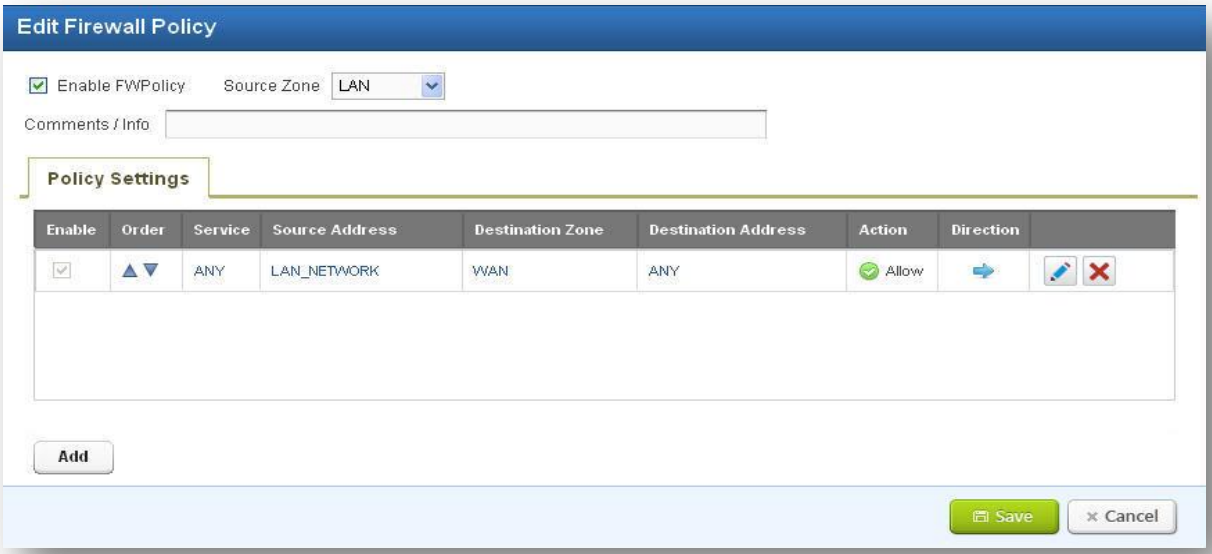


Figure 48: Edit Firewall Policy

Click Edit button, user can edit the preconfigured firewall rules according to user network structure.

Policy Rules

User can configure policy rules by making use of created address objects and Service objects. For example, if user wants to block SSH from host 192.168.0.25 then user has to create address object for 192.168.0.25 and service object SSH.

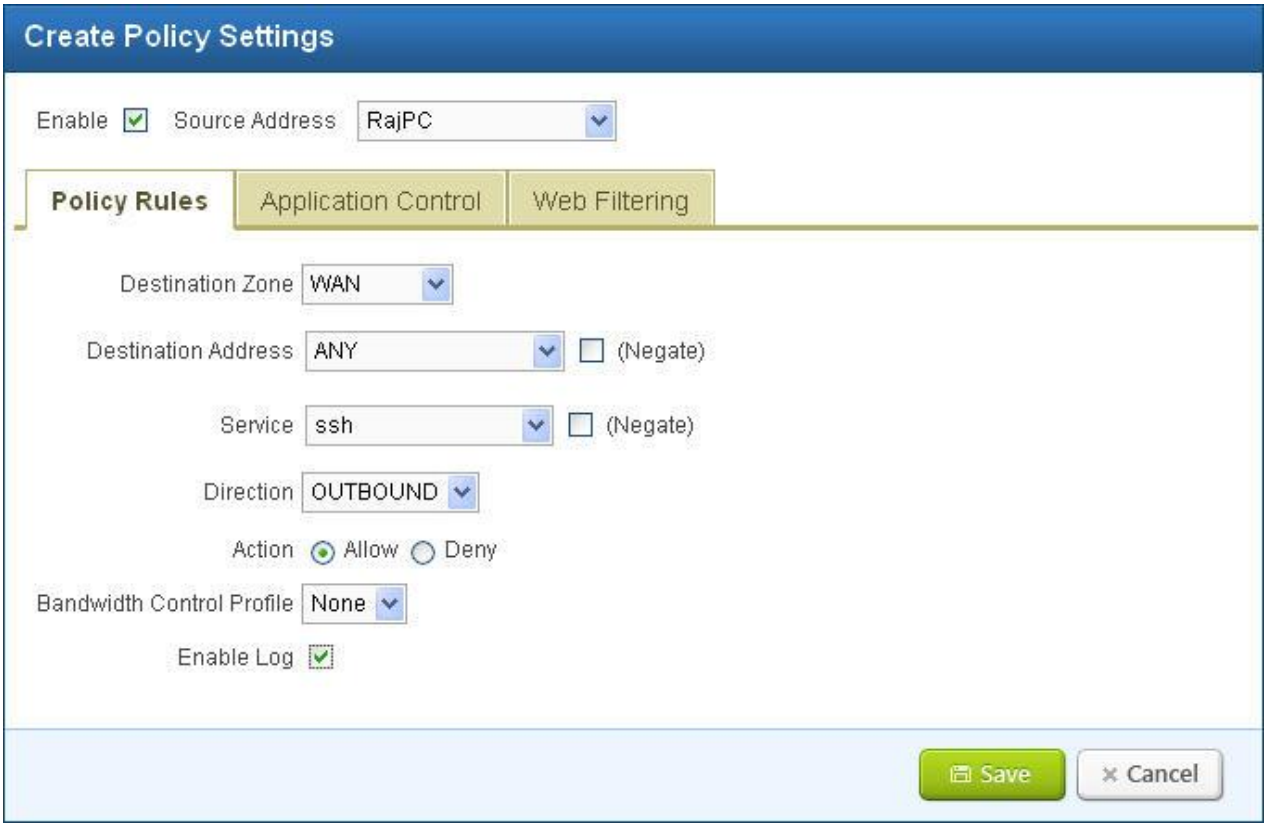


Figure 49: Create Policy Rules

Application Control

The online threat to productivity and security in your organization has evolved beyond simple web traffic. Problematic applications such as Bit Torrent, Skype, and TOR can compromise available bandwidth and expose you to inappropriate and illegal activity. Using protocols are not identified by conventional web filters, these types of applications are difficult to stop.

Shield UTM allows you to stop this traffic at the gateway itself.

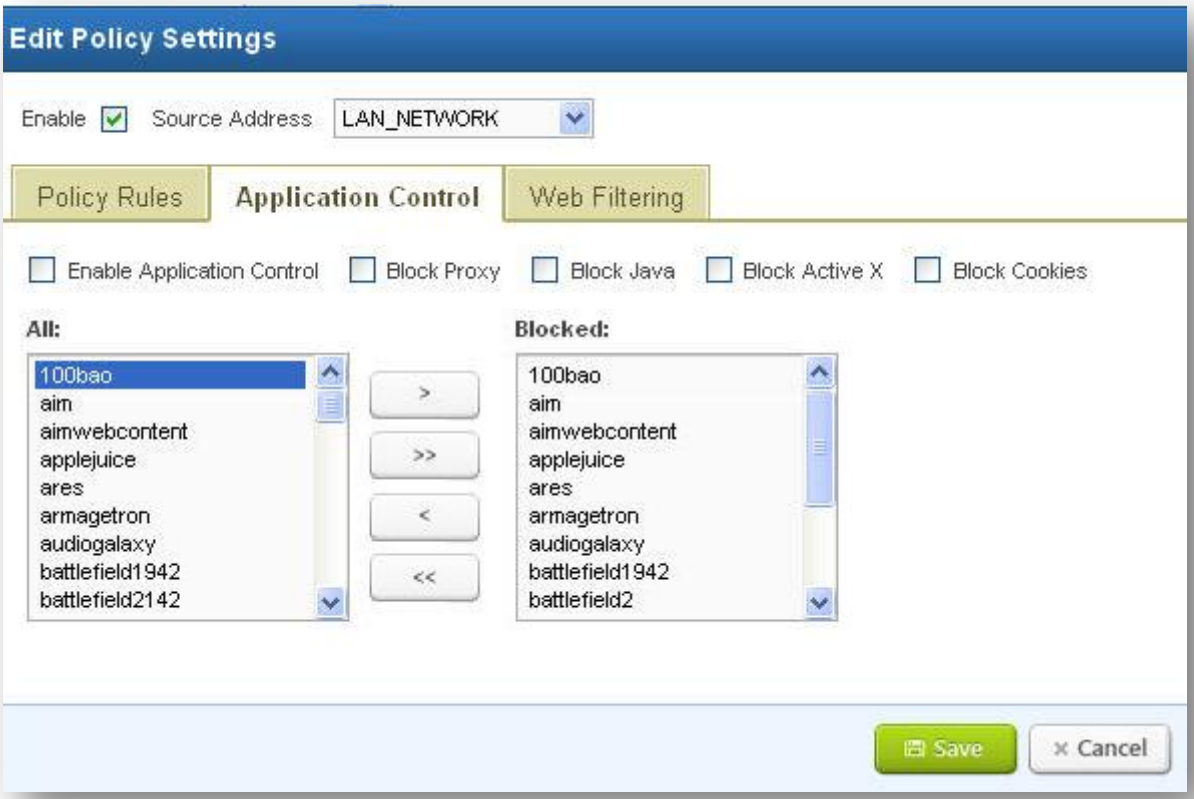


Figure 50: Application Control

Web Filtering

A Web filter is a program that can screen an incoming Web page to determine whether some or all of it should not be displayed to the user. The filter checks the origin or content of a Web page against a set of rules provided by company or person who has installed the Web filter.

It allows an enterprise or individual user to block out pages from Web sites that are likely to include objectionable advertising, pornographic content, Spyware, Viruses and other objectionable content. Vendors of Web filters claim that their products will reduce recreational Internet surfing among employees and secure networks from Web-based threats.

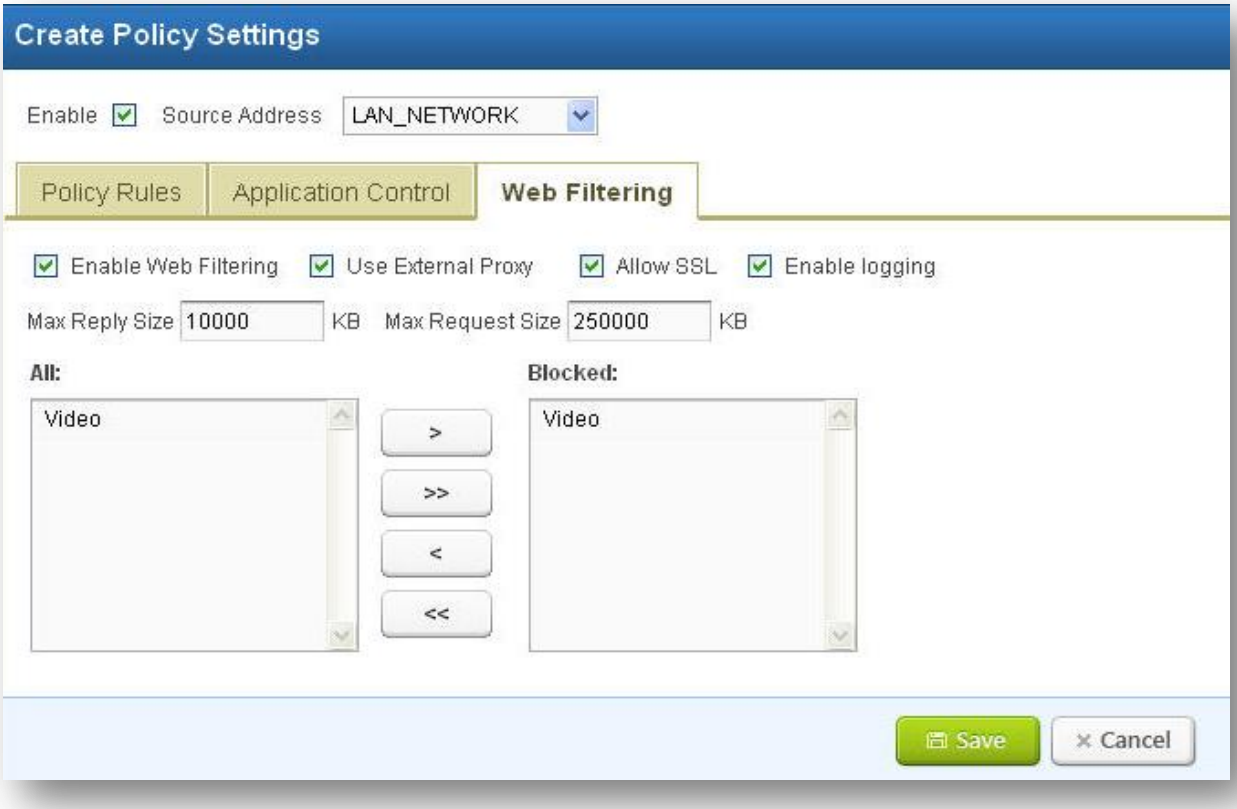


Figure 51: Web Filtering

The Web filter works primarily by looking at the destination location request for a HTTP(S) request made by the sending computer. If the URL is on a list that you have configured to list unwanted sites, the connection will be disallowed. If the site is part of a category, then user can configured to deny connections to the session. User can also configure the content filter to check for specific key strings of data on the actual web site and if any of those strings of data appear the connection will not be allowed.

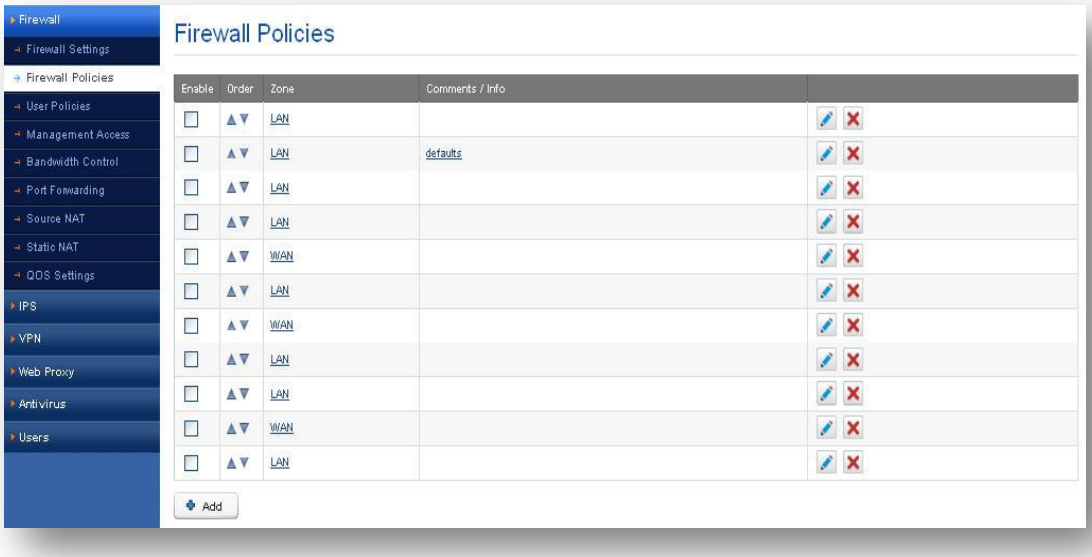


Figure 52: Firewall Policies

6.1.3 User Policies

Navigate through **Policies**> **Firewall > User Policies**

UTM allows user to configure their own User Policies according to their need in firewall.

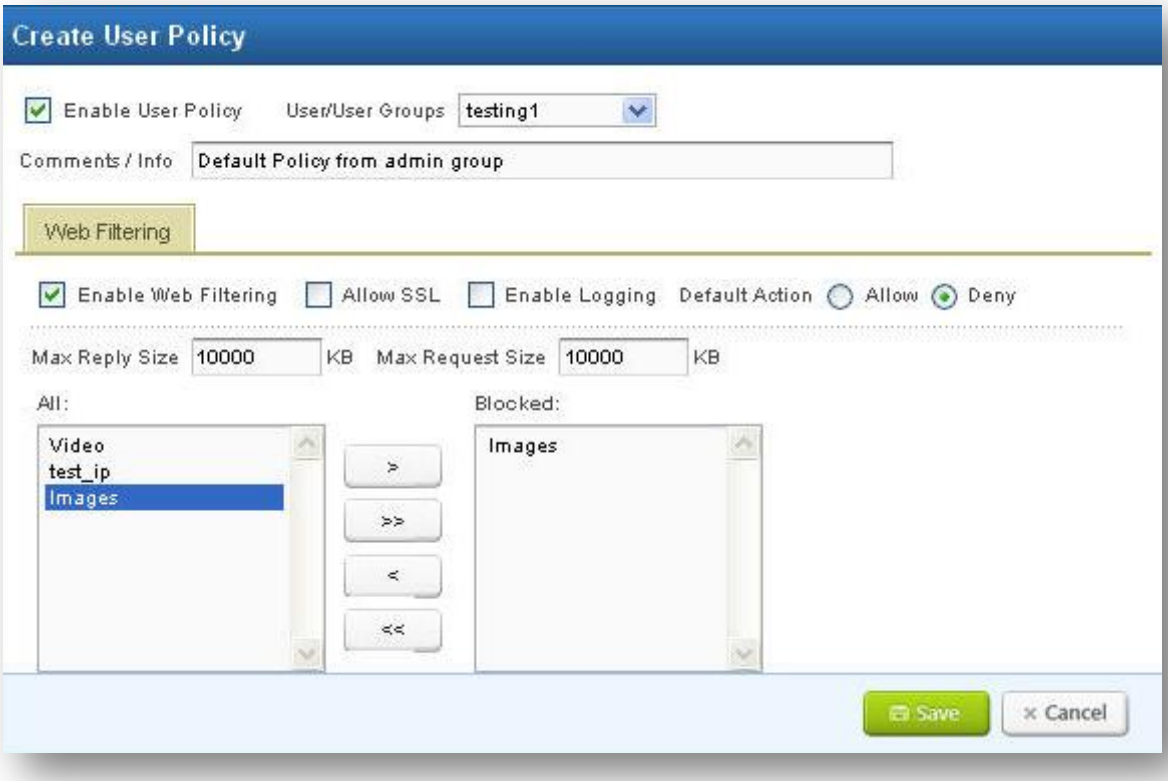


Figure 53: Create User Policy

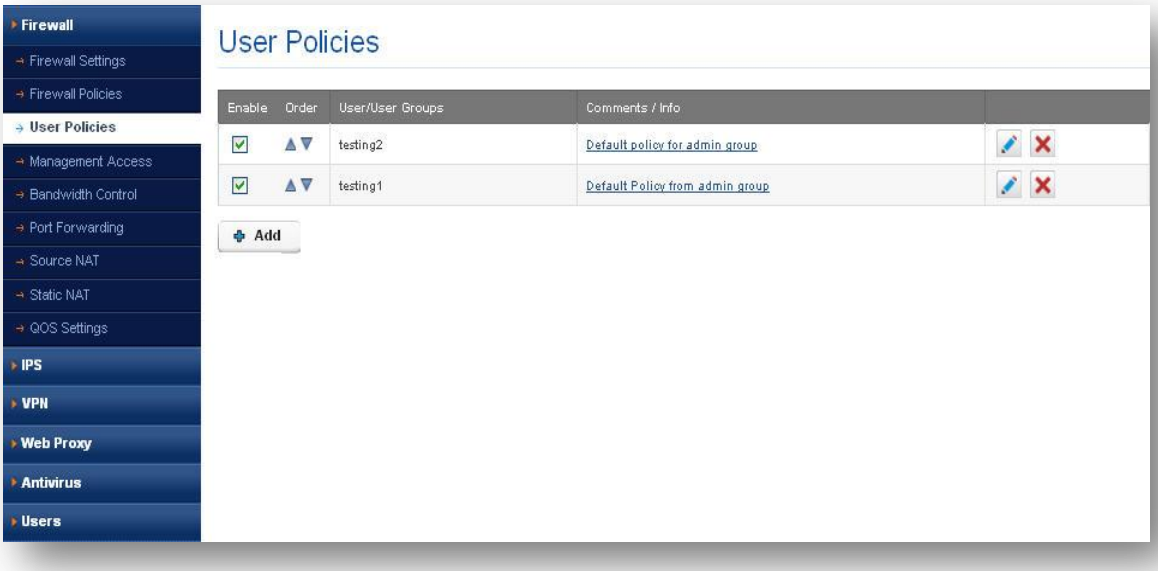


Figure 54: User Policies

6.1.4 Management Access

Navigate through **Policies**> **Firewall > Management access**

Management Access rules define the rules that traffic must meet to happen through an interface.

When you define rules for outgoing traffic, i.e. LAN Management Access profile, they are utilized to the traffic before any other policies are enforced.

When you define rules for incoming traffic i.e. WAN Management Access profile, they are applied to the traffic before any other policies are applied.

Figure 55: Add Management Access

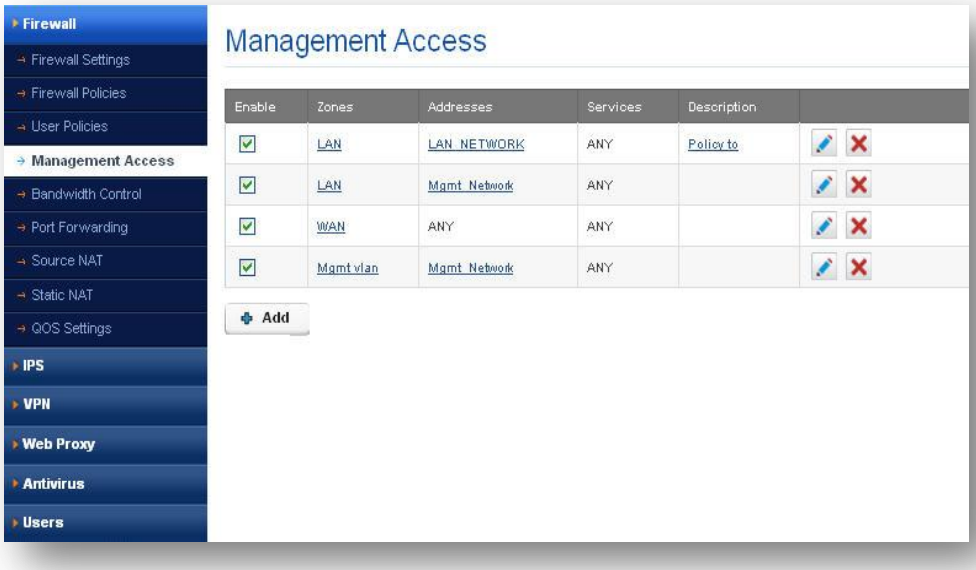


Figure 56: Management Access

6.1.5 Bandwidth control

Navigate through **Policies**> **Firewall > Bandwidth Control**

UTM Bandwidth control is designed to minimize the impact caused when the connection is under heavy load. Using Bandwidth Control, we can assign a specific minimum or maximum bandwidth for each computer, which means they have less impact on each other.

In UTM user can create BW profile in 2 ways:

i. Priority

ii. Rate

i. Priority

In Priority type user can select any one of following priority value to configure their BW profile. They are:

- 0 Realtime
- 1 Highest
- 2 High
- 3 Medium High
- 4 Medium
- 5 Medium Low
- 6 Low
- 7 Lowest

Figure 57: Add Bandwidth Control Profile

ii. Rate

In Rate, user can configure BW (Bandwidth) control profile by ID, Min & Max Download Rate, and Min & Max Upload Rate. Rates are in kbps only.

Figure 58: Add Bandwidth Control profile-Rate

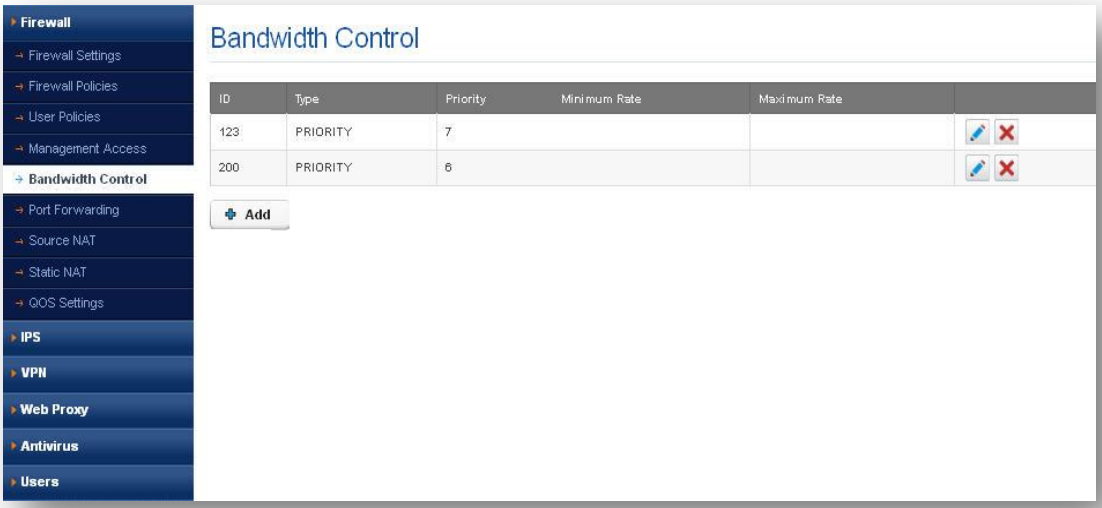


Figure 59: Bandwidth Control

NAT

NAT (Network Address Translation) translates the source IP address of a device on one network interface, usually the Internal, to a different IP address as it leaves another interface, usually the interface connected to the ISP and the Internet. This enables a single public address to represent a significantly larger number of private addresses.

UTM NAT Supports following types:

i. Static NAT

ii. Source NAT

iii. Dynamic NAT/Port Forwarding

6.1.6 Port Forwarding/Destination NAT

Navigate through **Policies**> **Firewall > Port Forwarding**

It changes the **destination** address in IP header of a packet and also changes the **destination** port in the TCP/UDP headers. The typical usage is to redirect incoming packets with a destination of a public address/port to a private IP address/port inside your network.

It is used to forward incoming connection requests to internal network hosts.

Figure 60: Add Destination NAT Rule

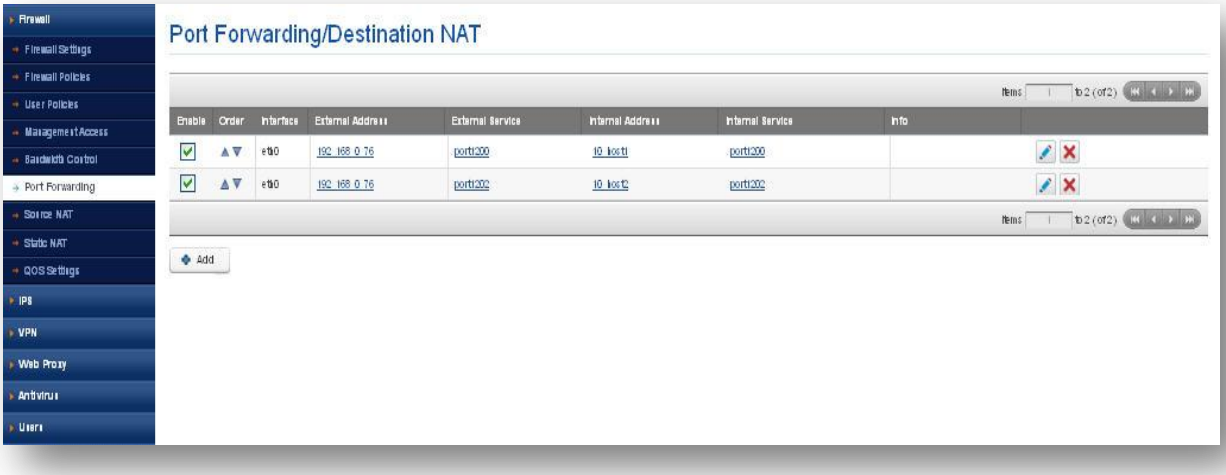


Figure 61: Port Forwarding Destination NAT

6.1.7 Source NAT

Navigate through **Policies**> **Firewall > Source NAT**

It changes the **source** address in IP header of a packet and also changes the **source** port in the TCP/UDP headers. The typical usage is to change the private address/port into a public address/port for packets leaving your network.

Masquerading is a special form of Source NAT where the source address is unknown at the time the rule is added to the tables in the kernel. If you want to allow hosts with private address behind your firewall to access the Internet then external address is variable (DHCP). Masquerading will modify the source IP address and port of the packet to be the primary IP address assigned to the outgoing interface

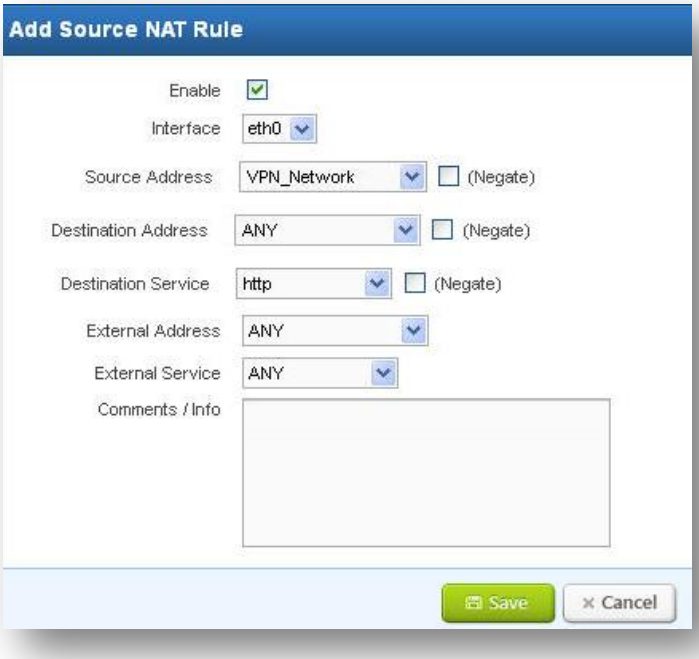


Figure 62: Add Source NAT Rule

UTM Source NAT changes the **source** address in the IP header of a packet. It may also change the **source** port in the TCP/UDP headers. The typical usage is to change the private address/port into a public address/port for packets leaving your network.

User can configure SNAT by making use of interface, Source & Destination address, Source & Destination port and External Address & port.

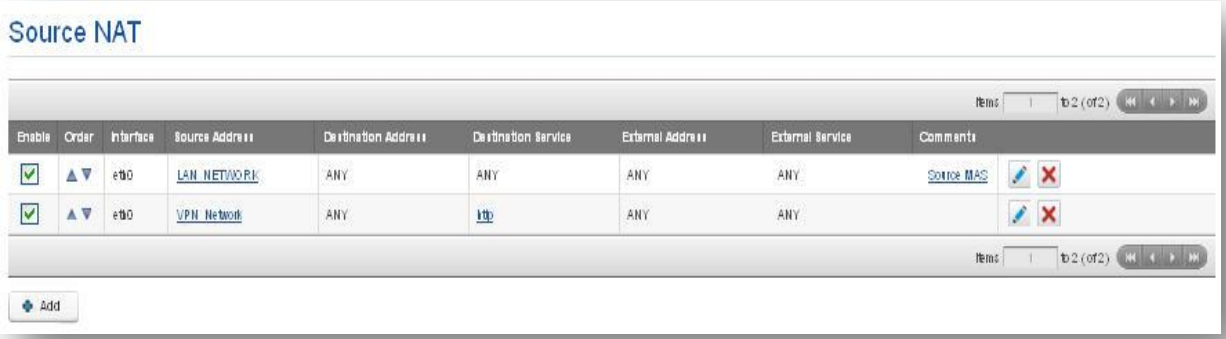


Figure 63: Source NAT

6.1.8 Static NAT

Navigate through **Policies**> **Firewall > Static NAT**

UTM Static NAT changes the source address in the IP header of a packet. It also changes the destination address in the IP header of a packet which is coming from the public network. User can configure Static NAT by making use of the interface, internal address &port, External Address & port/service. In Static NAT one internal IP address is always mapped to the same public IP address.

Figure 64: Add Static NAT Rule

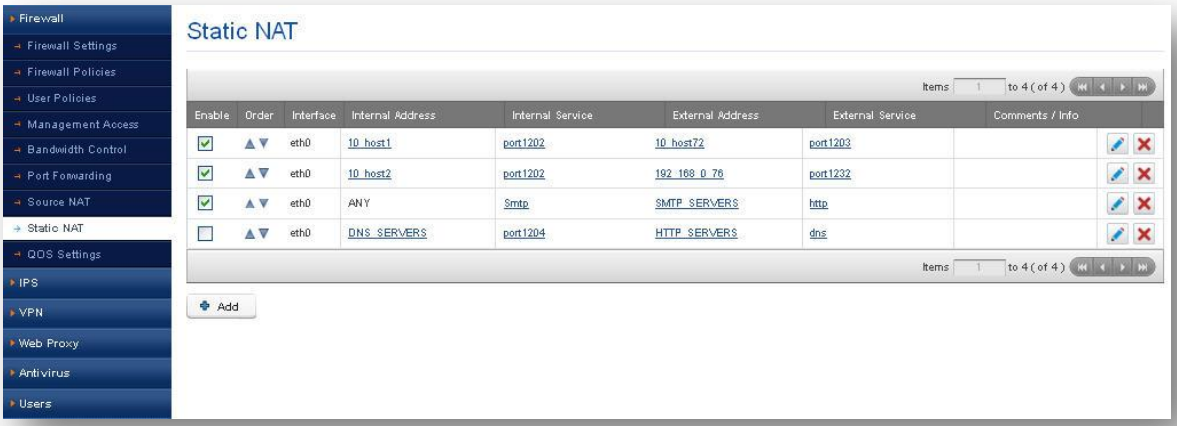


Figure 65: Static NAT

6.1.9 QOS Settings

Navigate through **Policies**> **Firewall > QOS Settings**

(Quality of Service) In relation to leased lines, QOS is a contractual guarantee of uptime and bandwidth.

Figure 66: DSCP Mapping

6.2 IPS

Navigate through **Policies**> **IPS**

Intrusion Prevention System (IPS) can detect and block attacks before damage has been done. It performs in-line inspection of network traffic in real-time manner. The inspection identifies attacks using known vulnerabilities of commonly used software products and protocols. The attack patterns with unusual activity are based on connection sequences or traffic length.

UTM IPS supports:

i. Predefined IPS signatures.

UTM is having predefined signatures for all known attacks.

ii. Custom IPS signatures.

Custom Signatures allows user to configure own signatures to block any kind of attacks that are targeting to your network.

6.2.1 IPS Settings

Navigate through **Policies**> **IPS > IPS Settings**

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS) are network security appliances that monitor network and/or system activities for malicious activity.

In IPS Settings, users can enable/disable the IPS by radio button present at GUIs.

User can Enable Signature Update by making use of given URL and even he can schedule the update the signatures based on a time basis like Monthly, Daily and Weekly. Or he can download and update the signatures.

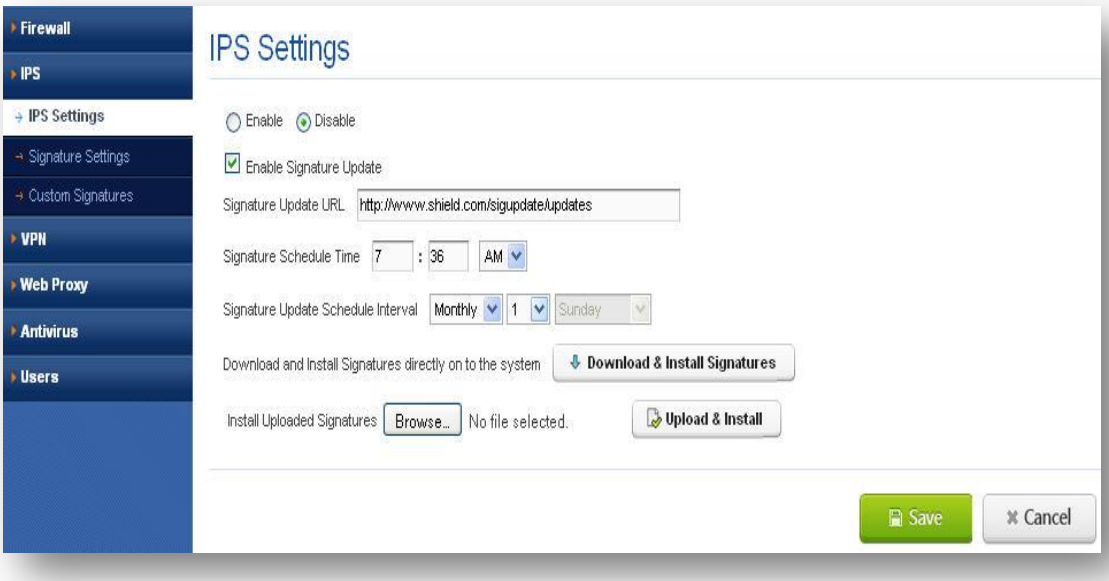


Figure 67: IPS Settings

6.2.2 Signature Settings

Navigate through **Policies**> **IPS > Signature Settings**

UTM user can change signature policy actions by selecting edit Buttons. He can change policy action to Prevent/Inspect/Disable in GUI. UTM user can have flexibility to change policy actions by following ways:

- By ID
- By Category
- By Severity

By ID

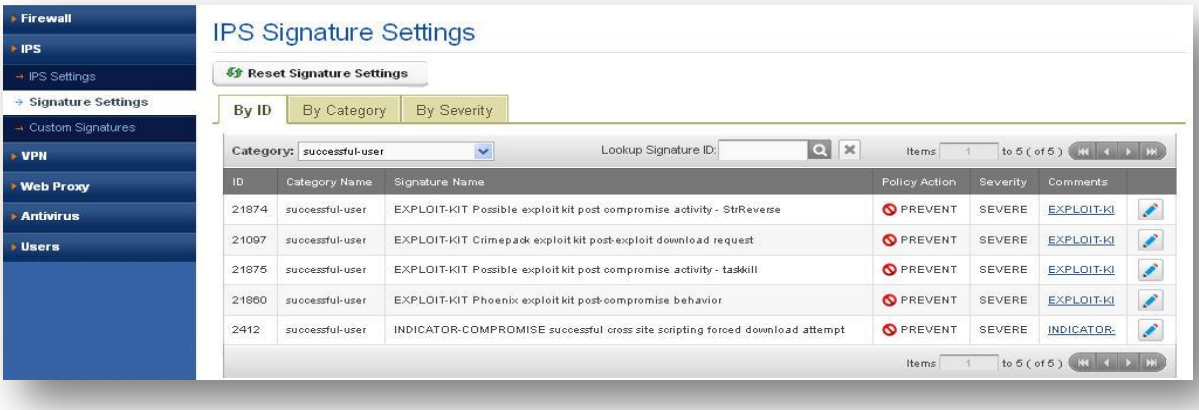


Figure 68: Signature Setting by ID

By Category

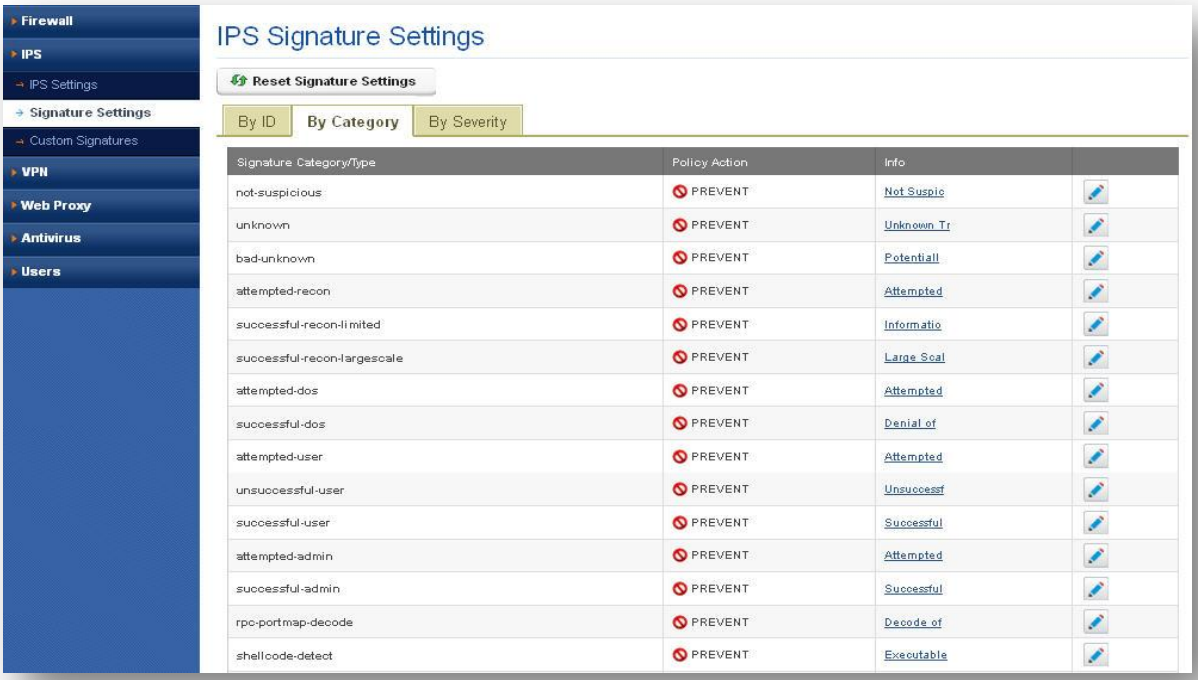


Figure 69: Signature Settings by Category

By Severity

Figure 70: Signature Settings by Severity

6.2.3 Custom Signatures

Navigate through **Policies**> **IPS > Custom Signatures**

UTM user can customize or write their signatures for any newer attacks. The UTM IPS GUI allows user to add signatures, Export Signatures and preview signatures.

When adding any new signatures, user just makes use of available options to customize their signatures.

Figure 71: Add Custom Signature

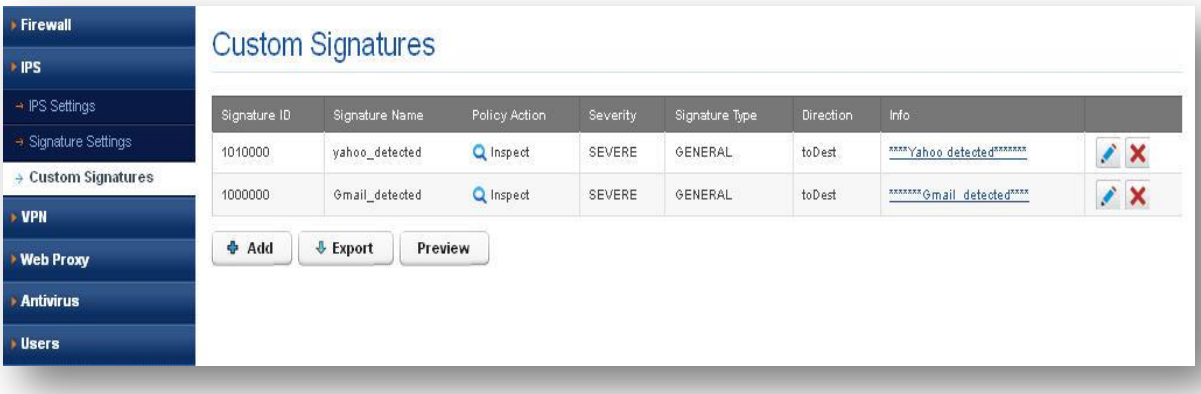


Figure 72: Custom Signatures

6.3 VPN

Navigate through **Policies**> **VPN**

A virtual private network (VPN) tunnel provides a secure communication channel either between two gateway VPN firewalls or between a remote VPN client and gateway VPN firewall. As a

result, the IP address of at least one of the tunnel endpoints needs to be known in advance in order for the other tunnel endpoint to establish (or reestablish) the VPN tunnel.

This private network used as a public network to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site or employee.

6.3.1 SSLVPN Server Settings

Navigate through **Policies**> **VPN > SSLVPN Server Settings**

It allows users to remotely access restricted network resources via a secure and authenticated pathway. By encrypting all network traffic and giving the appearance that the user is on the local network, regardless of geographic location. This protocol achieves a higher level of compatibility with client platforms and configurations for remote networks and firewalls, providing a more reliable connection.

It allows access to administrative systems, critical infrastructure, and sensitive information maintained by system administrators. SSL VPN access can be granted to system administrators as well as vendors and other external collaborators.

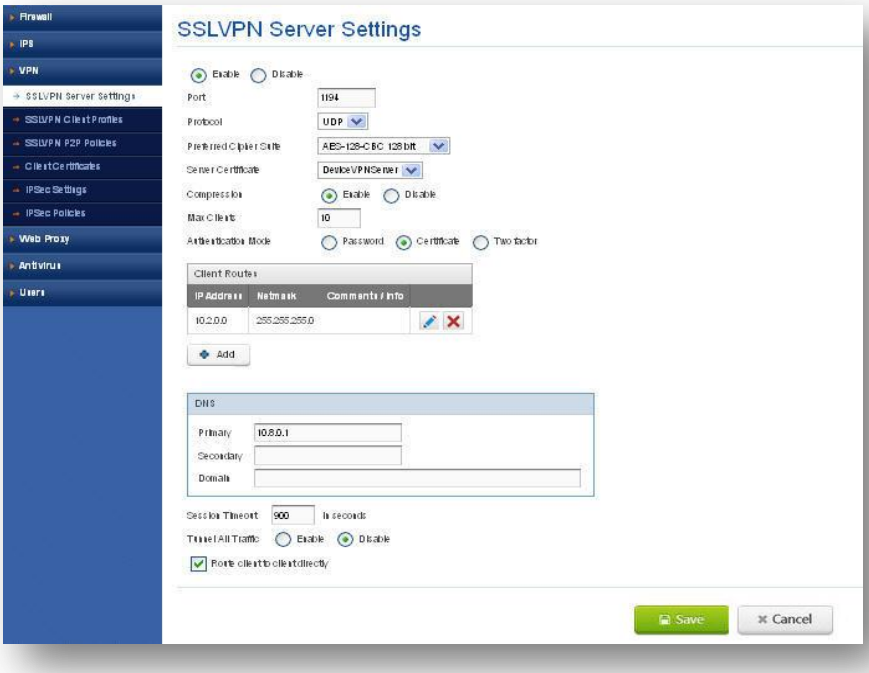


Figure 73: SSLVPN Server Settings

Enable: To enable SSLVPN

Port: Client can use this port to connect

Protocol: Sever and client to use protocol (UDP/TCP)

Preferred Cipher Suite: Cipher used for encrypting of data b/w client and server

Server Certificate: Certificates used server for the connection.

Compression: Enable/disable of compressed data

Authentication Mode: Server and client can communicate in 3 modes

Password: where Client and Server authentication is done using user name and password. User credentials are configured in Users pages.

Certificate: Authentication is performed by using credentials.

Two factors: Authentication is done in both password and certificate mode

Max Clients: Maximum number of clients that SSLVPN server can connect

Client Routes: Network on the server side which is accessible for all clients connected

Figure 74: Add Client Route

Session Timeout: If no traffic b/w SSLVPN server and customer. Then the client gets disconnected after the Session

Tunnel All Traffic: Enable/Disable all the traffic from client side need to be passed via SSLVPN server.

Route client to client directly: If checked, then client connected with SSLVPN server can communicate with each other.

6.3.2 SSLVPN Client Profiles

Navigate through **Policies**> **VPN > SSLVPN Client Profiles**

The Customer demands to be plugged in and configured here.

Figure 75: Configure SSLVPN Client Profile

User Name: Select the username to be configured. (The user is added in Users tab)

Remote Nets: Clients side network to be accessed via server side

Push Nets: Server side network to be accessed from configured user.

Static IP: Assigning IP to the user

Allo/Deny: if checked the this user is authenticated

Enable access via Secondary WAN: If the dual WAN is enabled, then the customer can relate with any of the one side (applied in multiple WANs)

Enable Tunnel all traffic: if checked, all the traffic for this user is sent via SSLVPN server

Figure 76: SSLVPN Client Profiles

6.3.3 SSLVPN P2P Policies

Navigate through **Policies**> **VPN > SSLVPN P2P Policies**

SSLVPN P2P tunnel provides a good communication channel between two gateway VPN firewalls.

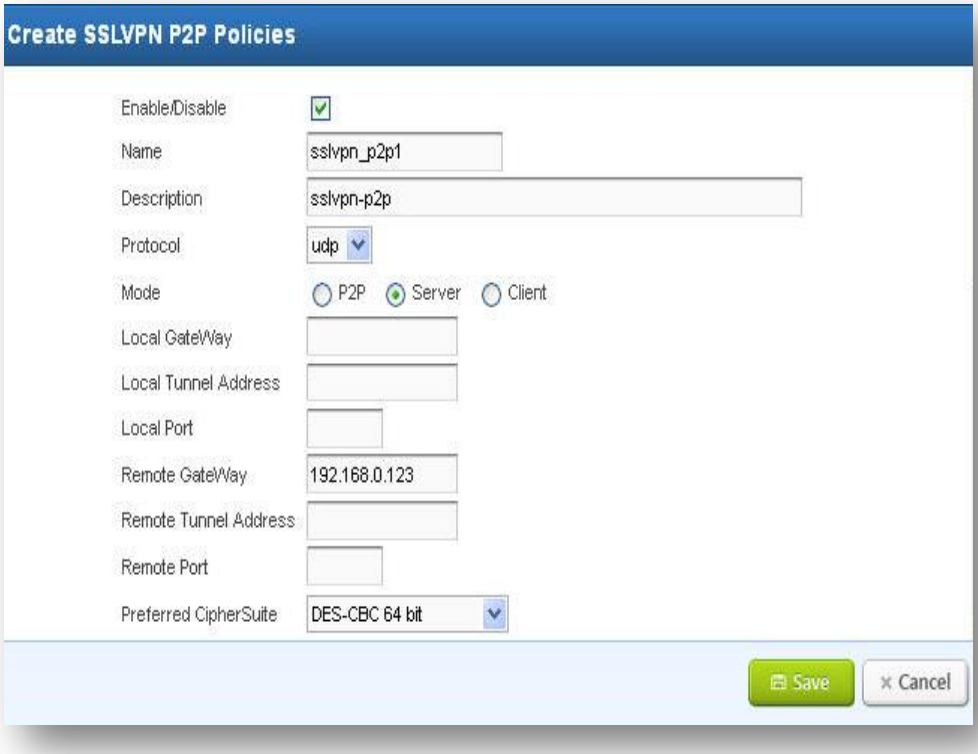


Figure 77: Create SSLVPN P2P Policies

Protocol and Mode: Protocol used to communicate between 2 VPN gateways

Protocol UDP:

- Tunnel can be created in all the 3 modes
- Mode p2p is selected on 1st gateway then p2p gateway has to select on the remote gateway
- Mode Server is selected on 1st gateway then the Client has to be configured on the remote gateway.

Protocol TCP:

- Tunnel can be created in all the 2 modes
- Mode Server is selected on first gateway then the Client has to be configured on the remote gateway
- **Local Gateway:** gateway IP of first gateway
- **Local Tunnel Address:** Virtual tunnel IP
- **Local Port:** Port used to connect
- **Remote Gateway:** Gateway IP of the 2nd gateway to which it has to relate.
- **Remote Tunnel Address:** virtual tunnel IP to be connects of the remote gateway.
- **Remote Port:** Port used to connect to the remote gateway
- **Preferred Cipher Suite:** Cipher to be used in encryption b/w gateways

Authentication:

- **Pre shared key:** Pre Shared Key dialog is enabled .Press generate button to generate the key. Use the generate key on the remote gateway
- **Certificate:** Certificate Use the same certificate on both gateways
- **Compression:** enable/disable of compression of data
- **Remote Nets:** remote gateway network to be accessed from 1 gateway side
- **Inactive Timeout:** If no traffic b/w two gateways at this time. Communication is terminated b/w gateway
- **Notify On Exit:** If one side of the gateway terminates, then it notifies the remote side. This is applicable for the UDP protocol.

Figure 78: SSLVPN P2P Policies

6.3.4 Client Certificates

Navigate through **Policies**> **VPN > Client Certificates**

The user can generate certificates signed by Device RootCa .Common name should match with SSLPVN client profile user name.

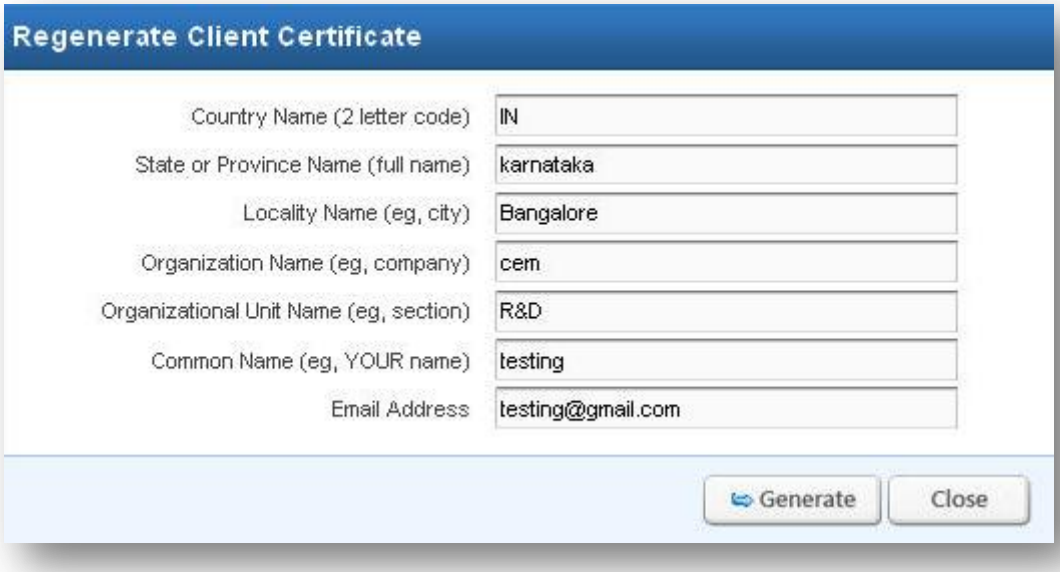


Figure 79: Regenerate Client Certificate

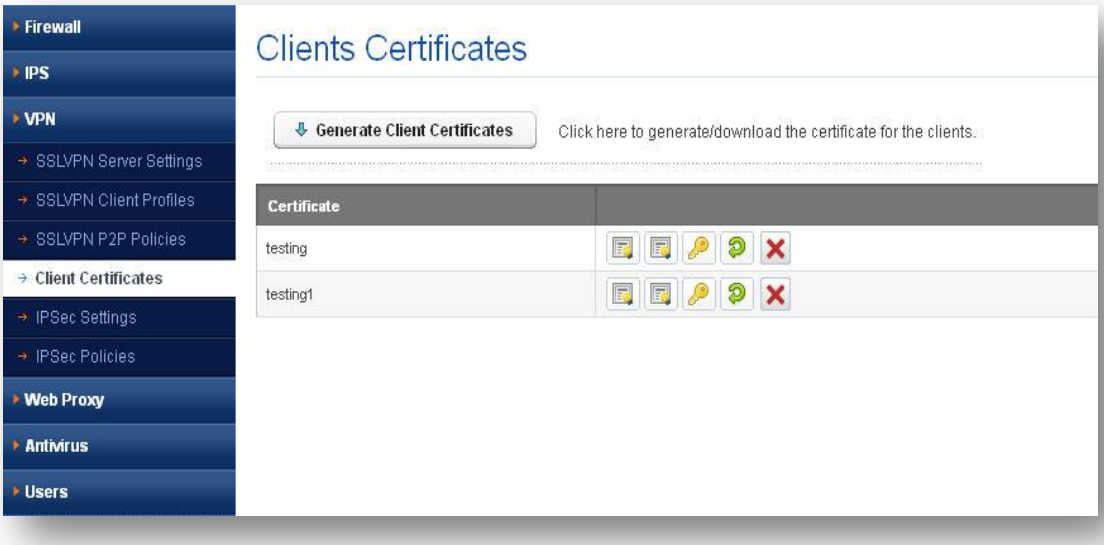


Figure 80: Clients Certificates

6.3.5 IPSec Settings

Navigate through **Policies**> **VPN > IPSec Settings**

The IPSec provides a method to manage authentication and data protection between multiple crypto peers engaging in secure data transfer. It includes the Internet Security Association and Key Management Protocol (ISAKMP)/Oakley and two IPSec

IPSec protocols: Encapsulating Security Protocol (ESP) and Authentication Header (AH). IPSec uses symmetrical encryption algorithms for data protection. Symmetrical encryption algorithms are more efficient and easier to implement in hardware. These algorithms need a secure method of key exchange to ensure data protection. Internet Key Exchange (IKE) ISAKMP/Oakley protocols provide this capability. If this is enabled, then IPSec policies are applied.

Figure 81: IPSec Settings

Click on the save button, the message will prompt your IPSec Settings are saved successfully.

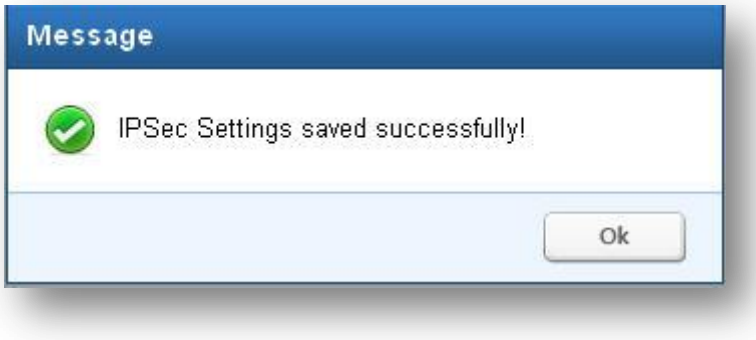


Figure 82: Save the IPSec Settings

6.3.6 IPSec Policies

Navigate through **Policies**> **VPN > IPSec Policies**

Policy settings tab:

IPSec Modes

IPSec has the following two modes of forwarding data across a network:

- Tunnel mode
- Transport mode

Each differs in its application as well as the amount of overhead added to the passenger packet. These modes are described in more detail in the next two sections.

Tunnel Mode

It works by encapsulating and protecting an entire IP packet. Because tunnel mode encapsulates or hides the IP header of the pre-encrypted packet, a new IP header is added so that the packet can be successfully forwarded. The encrypting devices themselves own the IP addresses used in this new header.

It can be configured with either or both IPSec protocols (ESP and AH). Tunnel mode results in additional packet expansion of approximately 20 bytes because of the new IP header.

Tunnel mode is widely considered more secure and flexible than transport mode. IPSec tunnel mode encrypts the source and destination IP addresses of the original packet, and hides that information from the unprotected network.

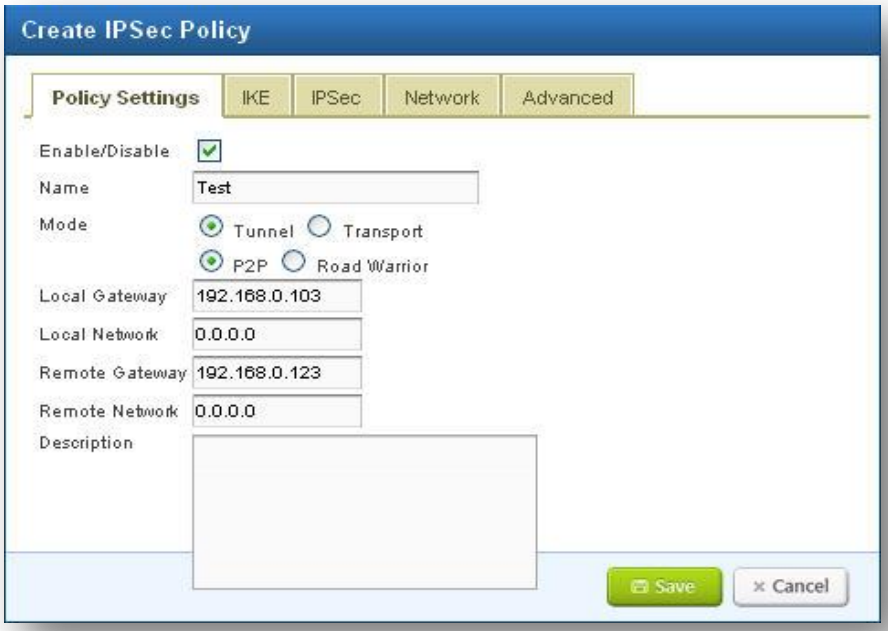


Figure 83: Policy Settings

Enable/Disable: If checked, then this policy is deployed

Name: Enter the Policy name to create IPSec Policy

Mode: User can select different modes p2p / Road warrior depending on these 2, tunnels and transport can be selected

Local gateway: Gateway IP of the device

Local network: Network behind the gateway need to be accessed. Eg: 192.168.0.0/24

Remote gateway: user can configure the Remote gateway IP.

Remote network: Remote gateway to be accessed. Eg: 192.168.1.0/24

IKE (Internet Key Exchange)

To implement a VPN solution with encryption, periodic changing of session encryption keys is necessary. Failure to change these keys makes the VPN susceptible to brute force decryption attacks. IPSec solves the problem with the IKE protocol, which makes use of two other protocols to authenticate a crypto peer and to generate keys. IKE uses a mathematical algorithm called a Diffie-Hellman exchange to generate symmetrical session keys to be used by two crypto peers. IKE also manages the negotiation of other security parameters such as the data to be protected, the strength of the keys, the hash methods used, and whether the packets are protected from anti-replay. ISAKMP normally uses UDP port 500 as both the source and destination port.

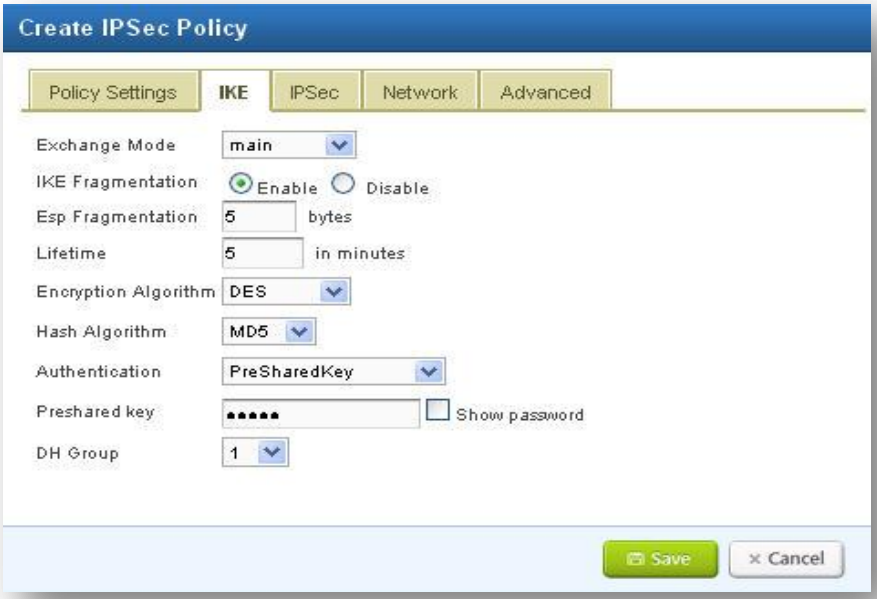


Figure 84: Create IPSec Policy-IKE

Exchange Mode: Main and aggressive mode is sustained.

IKE Fragmentation: User can either enable or disable the Fragmentation.

ESP fragmentation: User can configure the ESP fragmentation.

Lifetime: Time after the renegotiation of phase 2 happens

Encryption Algorithm: Encryption algorithm used during phase 1 negotiation

Hash Algorithm: User can select either MD5 or SHA1 algorithm from the dropdown menu.

Authentication: Supports 4 types of authentication and depending of authentication selected need to configure the field

IPSec

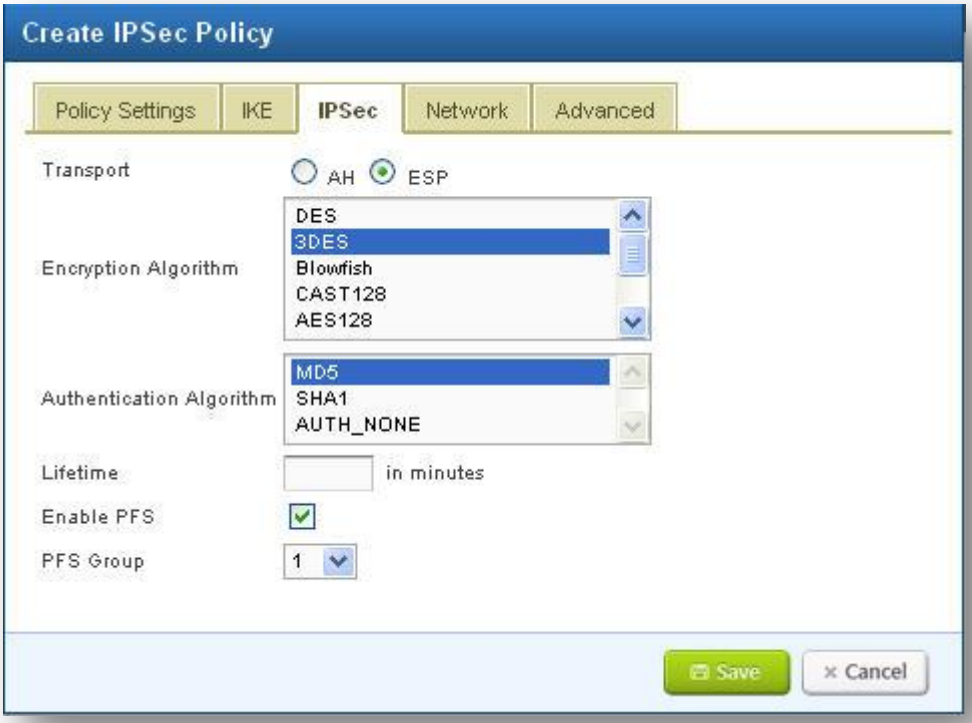


Figure 85: Create IPSec Policy-IPSec

Transport: can use AH/ESP mode.

AH (Authentication Header)

The AH protocol (IP protocol 51) forms the other part of IPSec. It does not encrypt data in the usual sense, by hiding the data but it adds a tamper-evident seal to the data. It also protects the non-mutable fields in the IP header carrying the data, which includes the address fields of the IP header.

The AH protocol should not be used alone when there is a requirement for data confidentiality.

ESP (Encapsulating Security Protocol)

The ESP header (IP protocol 50) forms the core of the IPSec protocol. This protocol, in conjunction with an agreed-upon set of security Parameters or transform set, protects data by rendering it indecipherable. This protocol encrypts the data portion of the packet only and uses other protections (HMAC) for other protections (data integrity, anti-replay, and man-in-the-middle). Optionally, it can also provide for authentication of the protected data.

Encryption Algorithm: User can select the available encryption methods.

Authentication Algorithm: User can select the available authentication algorithm.

Lifetime: User can configure the lifetime for the configured IPSec tunnel. If the lifetime configure expires the tunnel become inactive.

Network:

This should be configured if in Policy Settings->Road warrior mode is selected

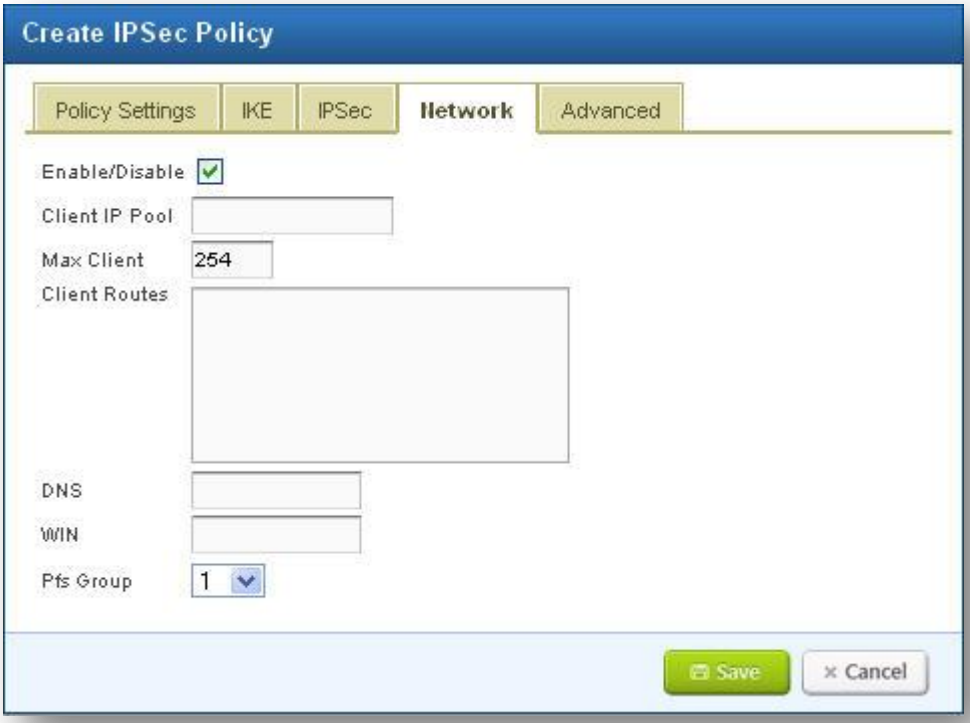


Figure 86: Create IPSec Policy-Network

Client IP Pool: User can assign IP Pool for clients. E.g.: 10.0.0.3-10.0.0.35

Client Routes: User can specify the client routes. E.g.:10.0.0.0/255.255.255.0

DNS: User can configure the DNS server for IPSec Policy. E.g.: 10.0.0.1

WIN: User can configure the WIN server for IPSec Policy.E.g.:10.0.0.254

Pfs Group: User can select the Pfs group value from the dropdown menu.

Advanced

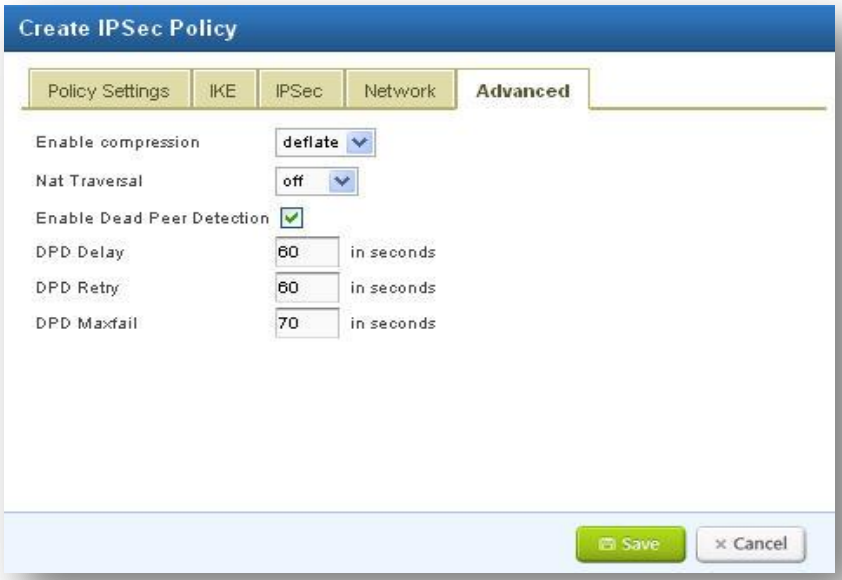


Figure 87: Create IPSec Policy-Advanced

Enable compression: deflate is a compression algorithm used to compress traffic

Nat Traversal: This feature can be enabling or disable by selecting viable options.

6.4 Web Proxy

Navigate through **Policies**> **Web Proxy**

Web proxy is a caching proxy for the Web supporting HTTP, HTTPS. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages. Web proxy has extensive access controls and makes a great server accelerator.

6.4.1 Proxy Configuration

Navigate through **Policies**> **Web Proxy> Proxy Configuration**

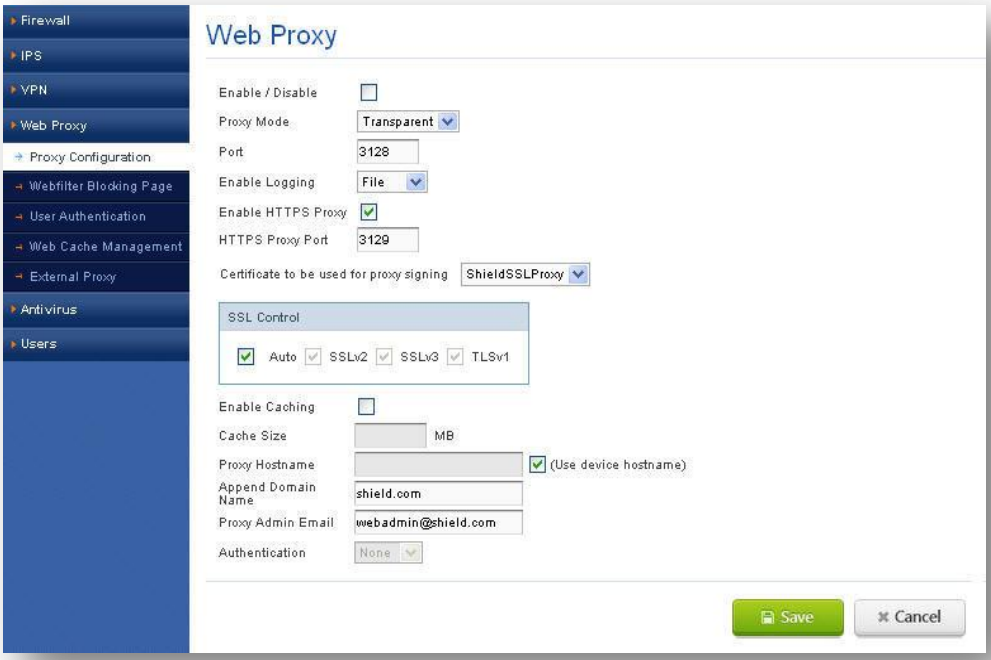


Figure 88: Web Proxy

Proxy Mode: We have two modes: Transparent and Explicit.

•**Transparent proxy:** A transparent proxy server is also a caching, server but the server is configured in such a way that it eliminates the client side (browser side) configuration. Typically the proxy server resides at the gateway and intercepts the WWW requests (port 80, 443 etc.) from the clients and fetches the content for the first time and subsequently replies from its local cache. The name Transparent is due to the fact that the client doesn't know that there is a proxy server which mediates their requests.

•**Explicit proxy:** A regular caching proxy server is a server which listens on a separate port (e.g. 3128) and the clients (browsers) are configured to send requests for connecting to that port. So the proxy server receives the request, fetches the content and stores a copy for future use. So next time when another client requests for the same webpage the proxy server just replies to the request with the content in its cache thus improving the overall request-reply speed.

Port: It specifies the HTTP port for web proxy.

Enable logging: This specifies where to log the web proxy logs. We have three types:

- **None:** any logging.
- **File:** Log to files in the device, which in turn can he seen in web filter reports page.
- **Syslog:** Log to another remote system by enabling logging in device settings option.

Enable HTTPS proxy: It specifies whether to enable HTTPS proxying.

HTTPS proxy port: It specifies the HTTPS port for web proxy.

Certificate to be used for proxy signing: It provides a list of self signed SSL certificates for HTTPS proxy.

SSL Control: It specifies the versions of SSL supported in web proxy. By default all versions are enabled, i.e.., Auto. Other SSL versions are SSLv2 (Secure Socket Layer version 2), SSLv3 and TLSv1 (Transport Layer Security version 1).

Enable Caching: It specifies where to enable caching when secondary device is employed.

Cache Size: It specifies how much size of caching can be done on secondary device.

Proxy Hostname: It specifies the hostname for web proxy. By default, device hostname is used for proxy.

Append Domain Name: It specifies the domain name for proxy. Eg. allo.com

Proxy Admin Email: It specifies the email id of admin, who will receive mail in case cache dies.

Authentication: It specifies the authentication scheme used when the proxy is in explicit mode.

Authentication schemes:

•**Digest authentication scheme:** In this scheme, the user is authenticated based username and password added in Users(Policies->Users) and the admin has to configure User policies(Policies->Firewall->User Policies) to block/allow users based on web filter objects and web filter options.

6.4.2 Web filter blocking page

Navigate through **Policies**> **Web Proxy> Web filter blocking page**

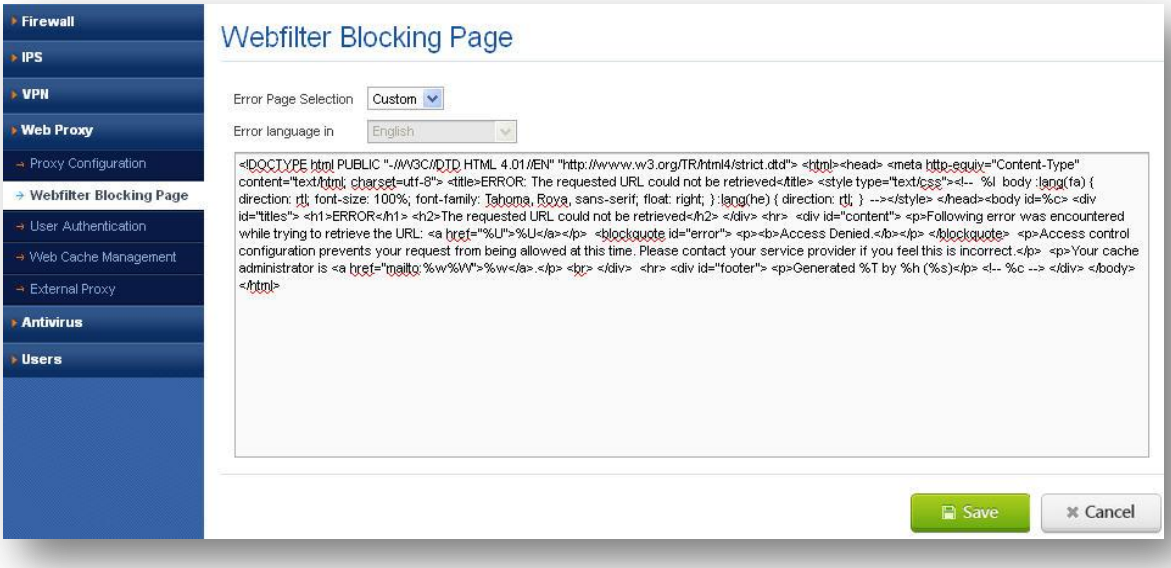


Figure 89: Web filter blocking page

Error page selection: It specifies the error page to be displayed when user accesses are denied sites. It has Default and Custom. By default, an error page will be displayed from web proxy standard error page depending on the language selected in 'Error language in' where as in custom; error page will be displayed upon the user entered text in the text area.

Error language in: It specifies in which language the error page should be exhibited. It will be enabled only in Default error page selection.

6.4.3 User Authentication

Navigate through **Policies**> **Web Proxy> User Authentication**

Authentication interval: It specifies how long the authentication scheme should be valid for the users. After the specific interval of time, the user is again prompted for authentication. Interval range is 10 – 1440(mins).

Figure 90: User Authentication

6.4.4 Web Cache Management

Navigate through **Policies**> **Web Proxy> Web Cache Management**

Clear web cache: It specifies to clear the web cache contents present on secondary device.

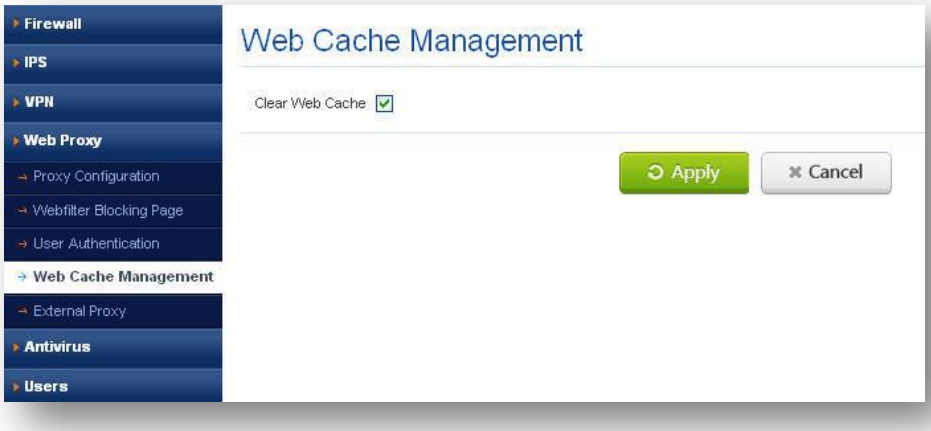


Figure 91: Web Cache Management

6.4.5 External Proxy

Navigate through **Policies**> **Web Proxy> External Proxy**

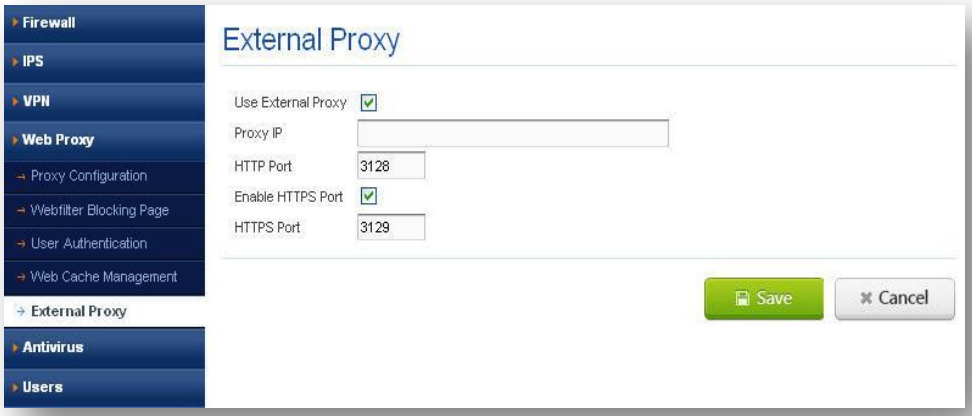


Figure 92: External Proxy

Use External Proxy: It specifies to use the external proxy which is running on a remote system.

Proxy IP: It specifies the remote system IP address where the proxy is running. Eg. 10.0.0.5

HTTP Port: It specifies the HTTP port of external proxy on the remote system.

Enable HTTPS Port: It specifies whether to enable HTTPS proxy form external proxy.

HTTPS Port: This will be used when we enable HTTPS Port option. It specifies the HTTPS port of external proxy.

6.5 Anti Virus

Navigate through **Policies**> **Antivirus**

Anti virus is computer software/Program used to prevent, detect and remove malicious software.

Internet can be a dangerous place filled with malware of various flavors. Currently, the malware that is most common in the Internet, in descending order, is Trojan horses, viruses, worms, adware, back door exploits, spyware and other variations. UTM antivirus filter works by inspecting the traffic that is transmitted through it.

Enable: It specifies whether to enable Antivirus on the device or not. It will be applied to all the firewall policies when this option in enabled.

6.5.1 Anti Virus Settings

Navigate through **Policies**> **Antivirus > Antivirus Settings**

Figure 93: Anti Virus Settings

6.6 Users

Navigate through **Policies**> **Users**

In this section, we can create users to system by configuring username and password.

Figure 94: Create User Information

Username: It specifies the username (5 – 32 characters)

Password: It specifies the password for the current user. (Password must be about 8-32 characters with at least one numeric and one special character)

Enable/Disable: it specifies whether to allow or deny the user.

These users are used in SSLVPN Authentication and in User Policies for proxy authentication.

6.6.1 User Groups

Navigate through **Policies**> **Users > User Groups**

We can create user groups as set of users. It provides a list of users in the system, in which we can configure which user can be selected from the group.

Figure 95: Create User Groups

User Group Name: Is specifies the user group name which is used in system scheme. (max. 16 characters)

These user groups are used in SSLVPN Authentication and in User Policies for proxy authentication.

7. Status Information

7.1 Interfaces

Navigate through **Status Info** > **Interfaces**

UTM Interfaces demonstrate interface's name, IP address and their Link status. User can Set, Update and refresh the interface Page.

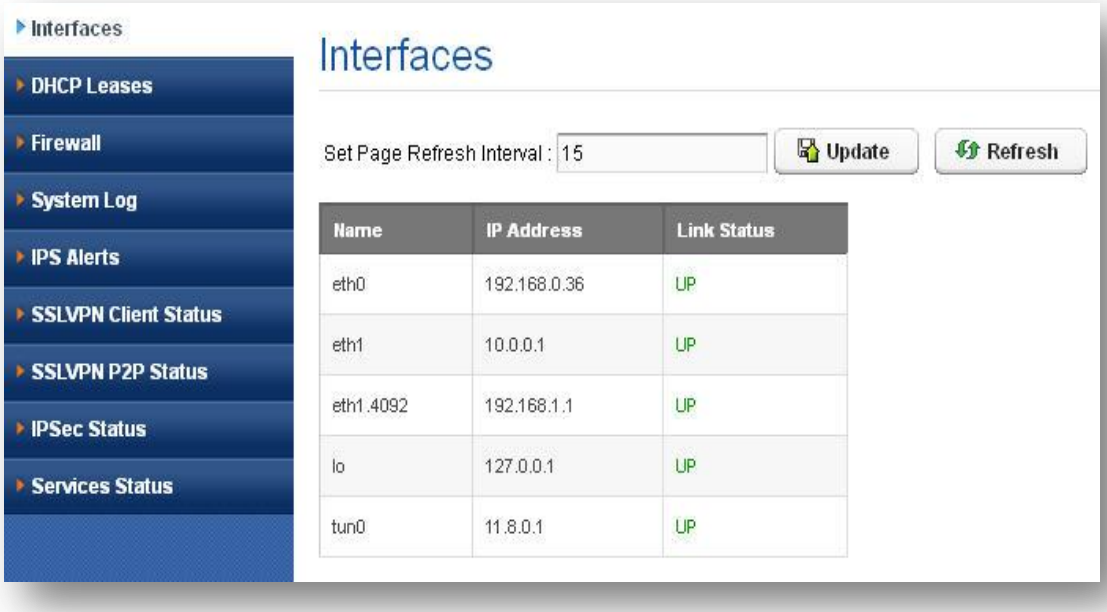


Figure 96: Interfaces

7.2 DHCP leases

Navigate through **Status Info** > **DHCP Leases**

It is used to view all current DHCP leases, including IP address, MAC address, hostname, lease start and end time, and the expires in.

MAC & IP Address: It shows MAC address of connected host (IP) to DHCP Server and IP address obtained from DHCP server.

Expires In: It demonstrates the length of time over, which IP address will lose from DHCP host

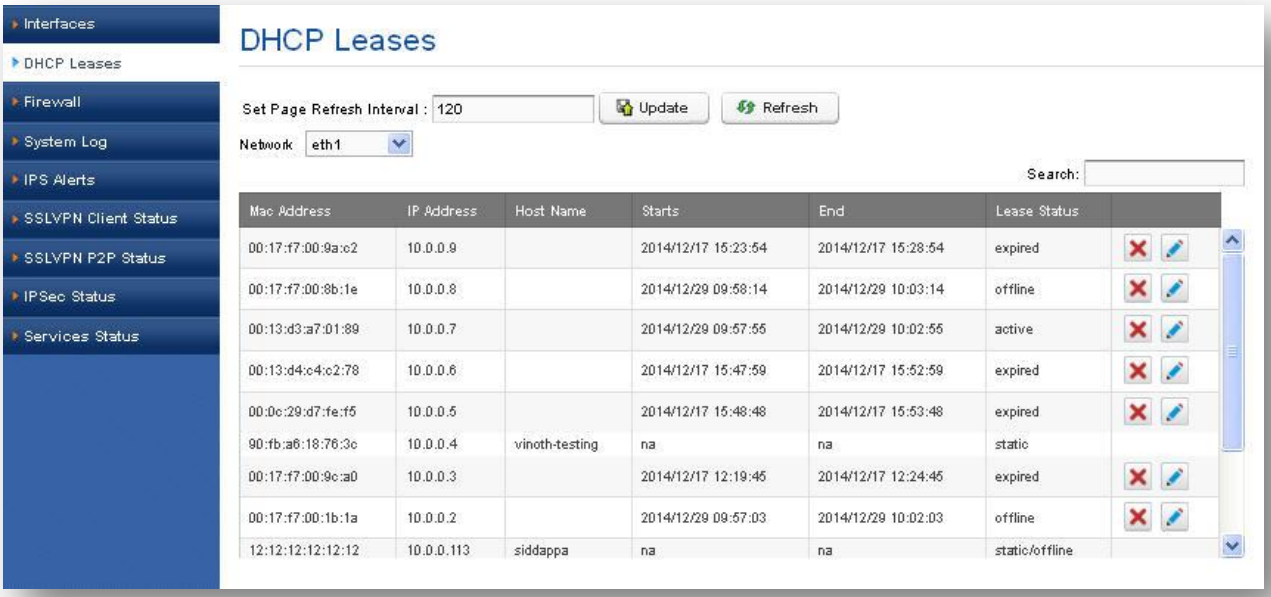


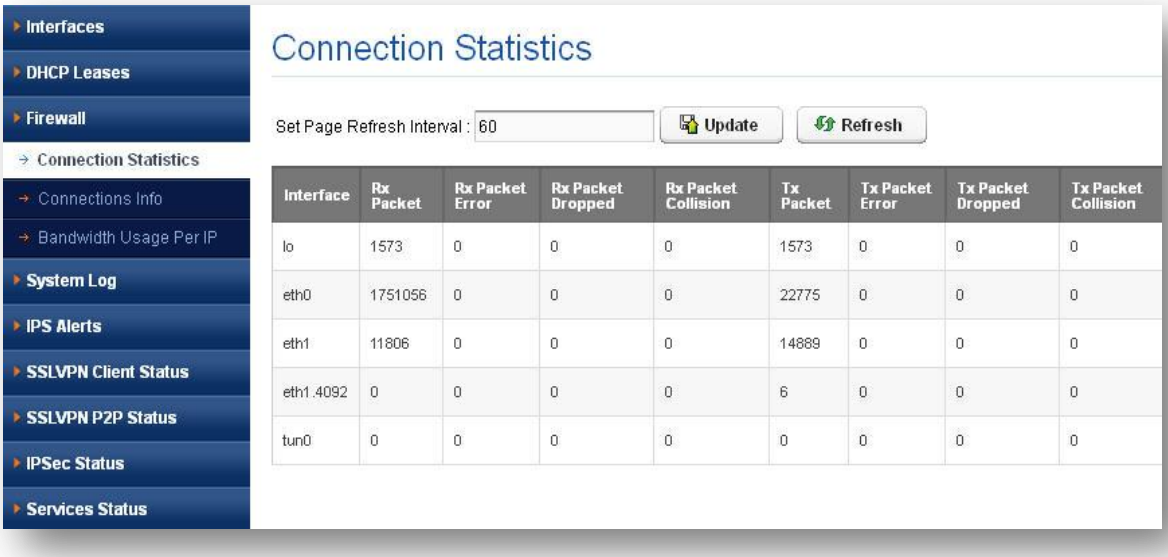
Figure 97: DHCP Leases

7.3 Firewall

7.3.1 Connection Statistics

Navigate through **Status Info** > **Firewall** > **Connection Statistics**

It shows UTM Firewall's Rx/Tx packets & their packet errors, packets dropped values and packet collisions. User can Set, Update and refresh Page. It shows list of interface names of UTM.e.g. eth0, eth1



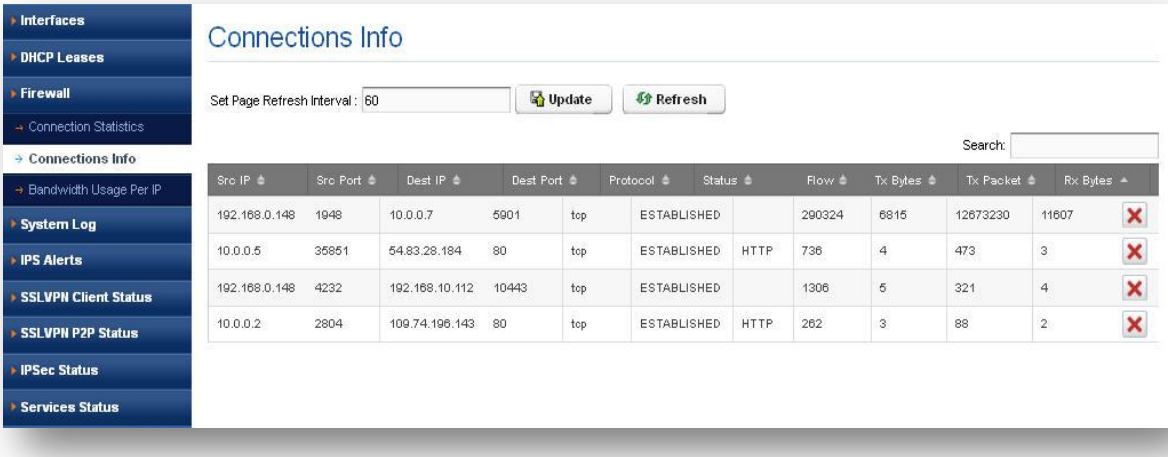
Interface	Rx Packet	Rx Packet Error	Rx Packet Dropped	Rx Packet Collision	Tx Packet	Tx Packet Error	Tx Packet Dropped	Tx Packet Collision
lo	1573	0	0	0	1573	0	0	0
eth0	1751056	0	0	0	22775	0	0	0
eth1	11806	0	0	0	14889	0	0	0
eth1.4092	0	0	0	0	6	0	0	0
tun0	0	0	0	0	0	0	0	0

Figure 98: Connection Statistics

7.3.2 Connection info

Navigate through **Status Info** > **Firewall** > **Connection Info**

The Connection information page shows source IP, Source port, destination IP and port, Connection status, Flow, Tx/Rx packets with size in bytes. It also shows connection Status, Flow. The user can search particular log and even delete the unwanted connection log.



Src IP	Src Port	Dest IP	Dest Port	Protocol	Status		Flow	Tx Bytes	Tx Packet	Rx Bytes
192.168.0.148	1948	10.0.0.7	5901	tcp	ESTABLISHED		290324	6815	12673230	11607
10.0.0.5	35851	54.83.28.184	80	tcp	ESTABLISHED	HTTP	736	4	473	3
192.168.0.148	4232	192.168.10.112	10443	tcp	ESTABLISHED		1306	5	321	4
10.0.0.2	2804	109.74.196.143	80	tcp	ESTABLISHED	HTTP	262	3	88	2

Figure 99: Connections Information

7.3.3 Bandwidth Usage per IP

Navigate through **Status Info** > **Firewall** > **Bandwidth Usage per IP**

It shows bandwidth usage per IP with Upstream& Downstream of both TCP&UDP statuses.

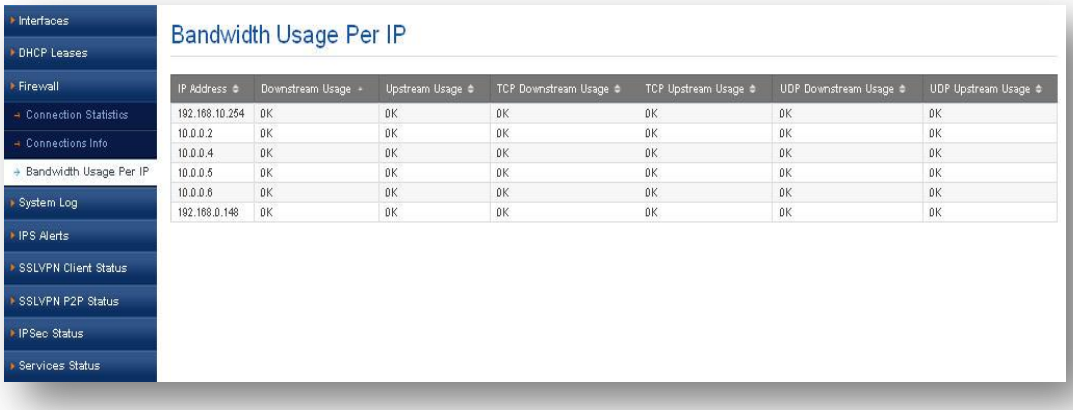


Figure 100: Bandwidth Usage per IP

7.4 System Log

Navigate through **Status Info** > **System Log**

System logs shows logs with messages of particular module and logs time stamps. User can download the System Logs. User also Update & Refresh the page refresh interval. Particular log can search by making use of Search field.

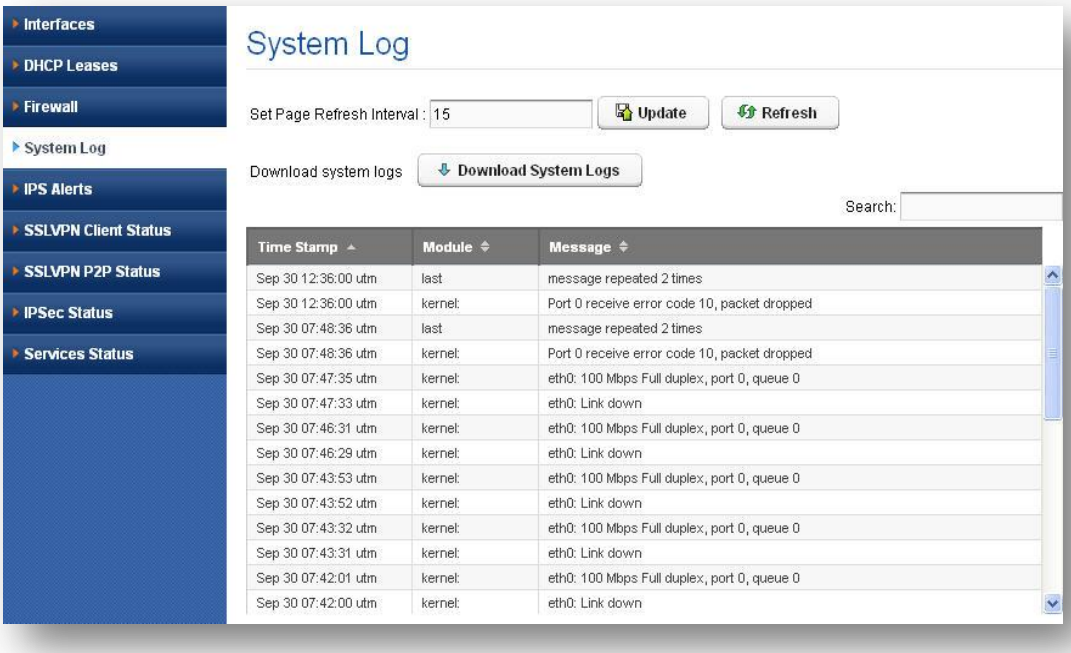


Figure 101: System Log

The System log page shows the time stamp logs, module name from which alert triggered and log generated from any module.

7.5 IPS Alerts

Navigate through **Status Info** > **IPS Alerts**

It shows alerts generated by the IPS engine with signature ID, Signature category and alert message. IPS alert shows its Time Stamp information at which alert got triggered, Source IP & Port, Destination IP& Port and Type of protocol whether it is TCP or UDP.

The user can search particular alert using Search field. User can set & Update refreshes interval and Download IPS alert for further analysis.

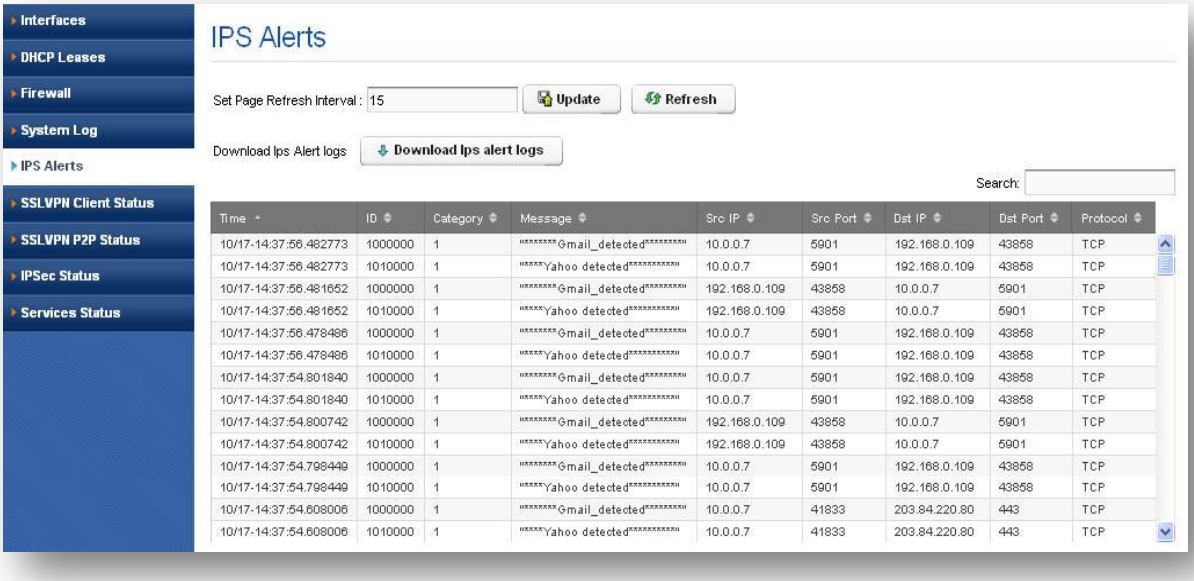


Figure 102: IPS Alerts

7.6 SSLVPN Client Status

Navigate through **Status Info** > **SSLVPN Client Status**

It read the client connection details which is connected to the SSLVPN Server Gateway. It shows connected VPN clients to the VPN server with the client username, Client real address, and Client virtual address, Connected Since, Byte it has received and sent.

SSLVPN client status gives you an idea about the user who connected to the VPN server, the IP address for both real customers and Virtual customers. Also the duration of the connection received and transferred bytes.

Figure 103: SSLVPN Client Status

7.7 SSLVPN P2P Status

Navigate through **Status Info** > **SSLVPN P2P Status**

It shows the list of SSLVPN P2P gateways connecting.

Figure 104: SSLVPN P2P Status

7.8 IPSec Status

Navigate through **Status Info** > **IPSec Status**

IPSec Status shows the list of clients connected to IPSec with IP destination of the Local gateway, the IP address of remote gateway, transport type, mode of connection and connection state. In UTM, an algorithm is a mathematical procedure that manipulates data to encrypt and decrypt it. Created On designates the time at which connection established and byte transacted counts in bytes.

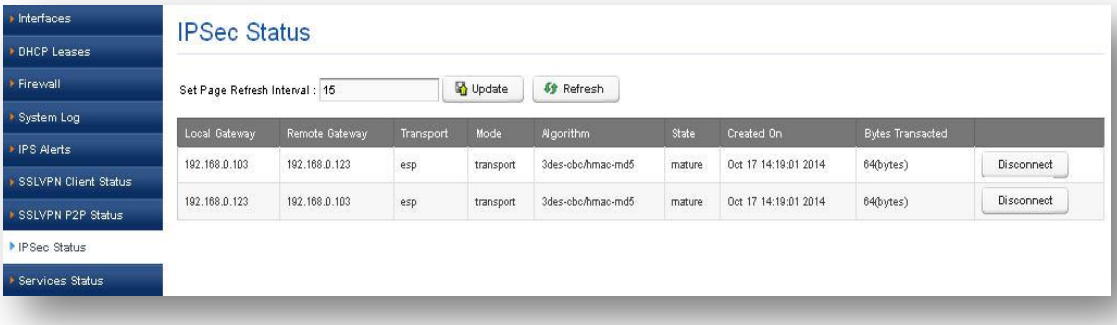


Figure 105: IPSec Settings

7.9 Service Status

Navigate through **Status Info** > **Service Status**

It shows UTM important services running/Stopped status with description. The user can restart the stopped/running status and user can set and update refresh interval. The service status page indicates service name, description name of services and connection status.

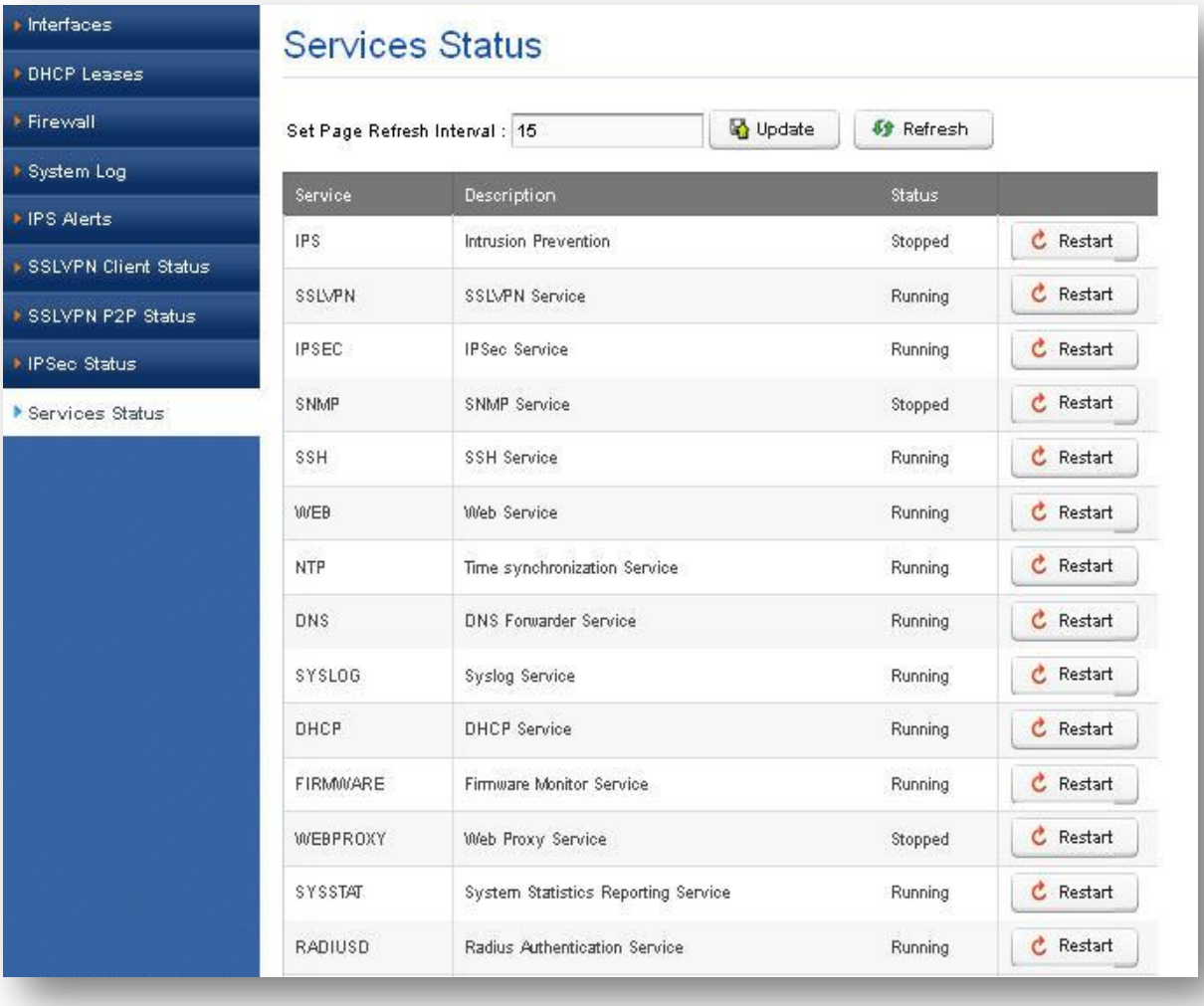


Figure 106: Service Status

8. Diagnostics

8.1 Diagnostics Report

The diagnostics page will allow the administrator to gather the troubleshooting logs which will help allo Support team in debugging any issues faced with UTM deployment setup.

To run the utility on the device, the administrator needs to click the 'Run diagnostics' button. The device will run the diagnostics task in the backend and display the results once the task is complete. The administrator can download the reports by clicking the 'Get Report' button and send the report to allo Support team (Note: You can submit through support ticket: http://support.allo.com

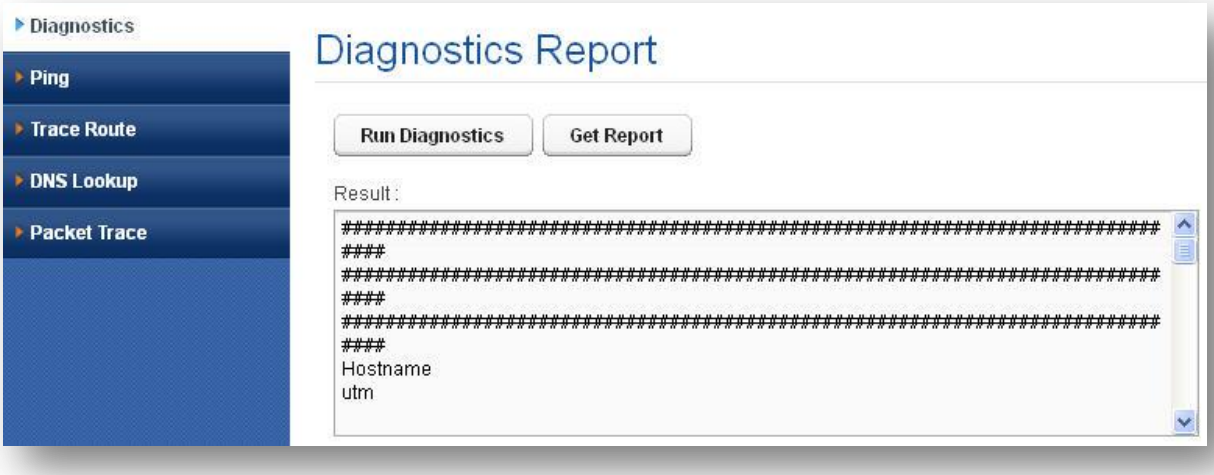


Figure 107: Diagnostics Report

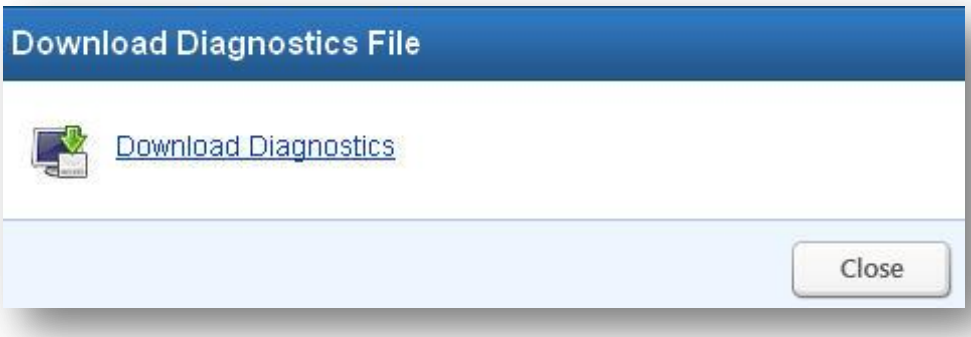


Figure 108: Download Diagnostics File

8.2 Ping

Navigate through **Diagnostics** > **Ping**

The administrator can troubleshoot the network connectivity issues with running ping from the UTM device. The administrator needs to enter the IP address that needs to be pinged from the UTM appliance/ping count and click the 'Ping' button to run the task. The ping results will be displayed in the text area once the ping task is complete.

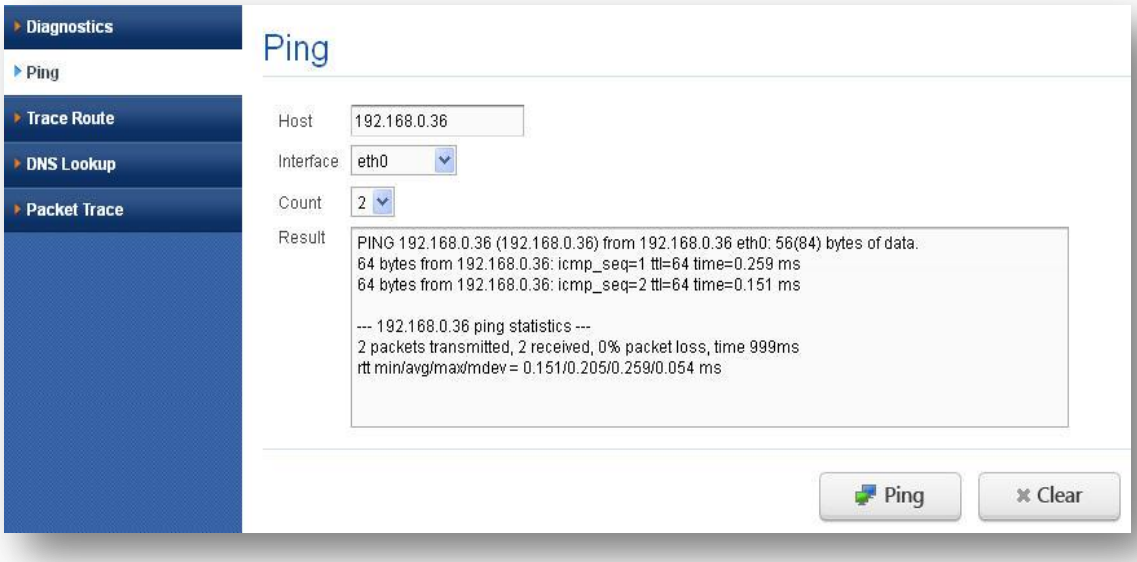


Figure 109: Ping

8.3 Trace Route

Navigate through **Diagnostics** > **Traceroute**

The administrator can troubleshoot the network connectivity issues with running a trace route from the UTM device.

The administrator needs to enter the IP address, which the route needs to be traced from the UTM appliance/hop count and click the 'Trace route' button to run the task.

The trace route results will be displayed in the text area once the trace route task is complete.

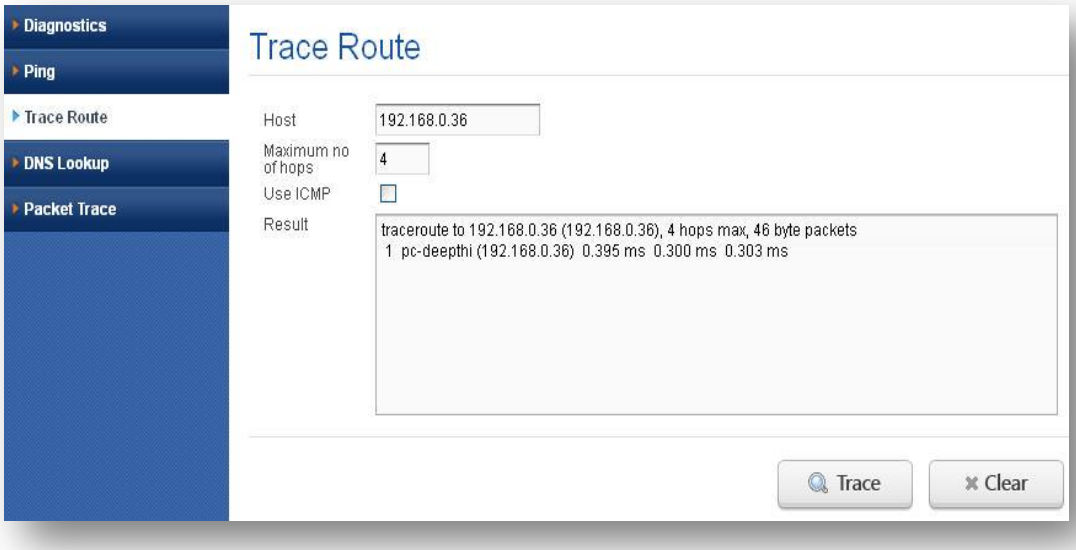


Figure 110: Trace Route

8.4 DNS Lookup

Navigate through **Diagnostics** > **DNS Lookup**

To look up a DNS address:

1. Locate the Perform a DNS Lookup section on the Diagnostics screen. In the DNS Server Name field, enter a server name.

Click the Lookup button. The results of the lookup action are displayed in a new screen. To return to the Diagnostics screen, click back on the browser menu bar.

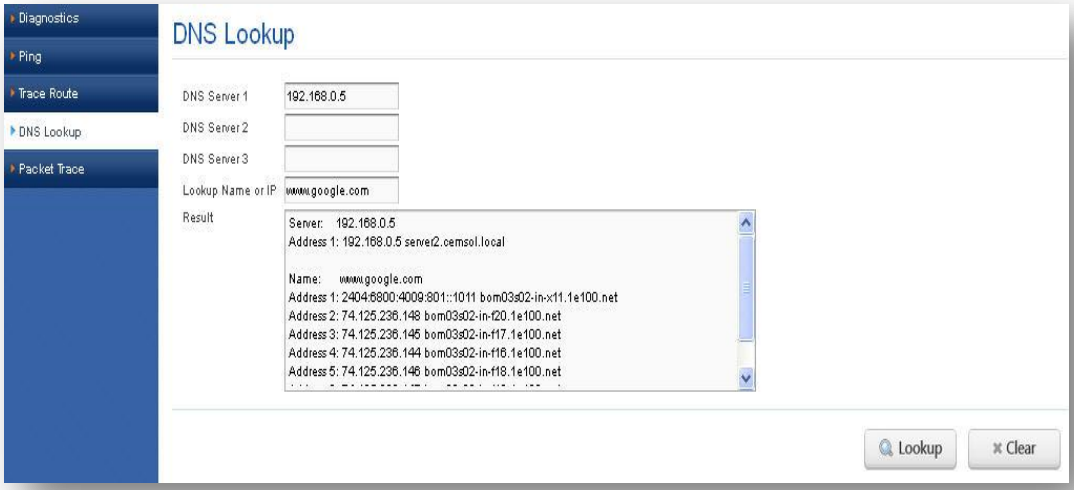


Figure 111: DNS Lookup

8.5 Packet Trace

Navigate through **Diagnostics** > **Packet Trace**

It gives detailed information about the trace of packets in UTM with description message and time stamp. User can download the packet trace for further analysis.

Figure 112: Packet Trace

9. Reports

9.1 System

It provides Simple logging information for the internal system services.

9.1.1System usage

Navigate through **Reports** > **System > System usage**

It shows the CPU usage of device during last 1 minute and records it in the graph of CPU usage vs. time in seconds.

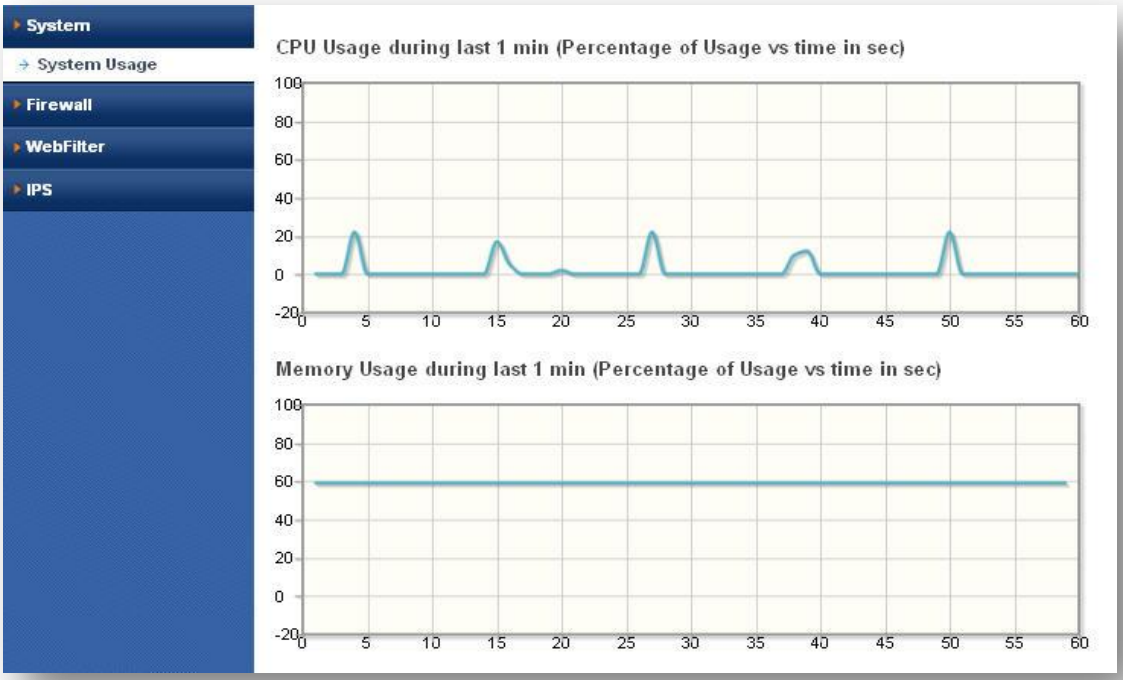


Figure 113: System Usage

9.2 Firewall

A real-time view of the firewall logs with some filtering options.

9.2.1 Internet Usage

Navigate through **Reports** > **Firewall > Internet usage**

It shows the internet usage of IP in graph format. And also shows top 25 IP connections and their usage of Upstream & Downstream in KB.

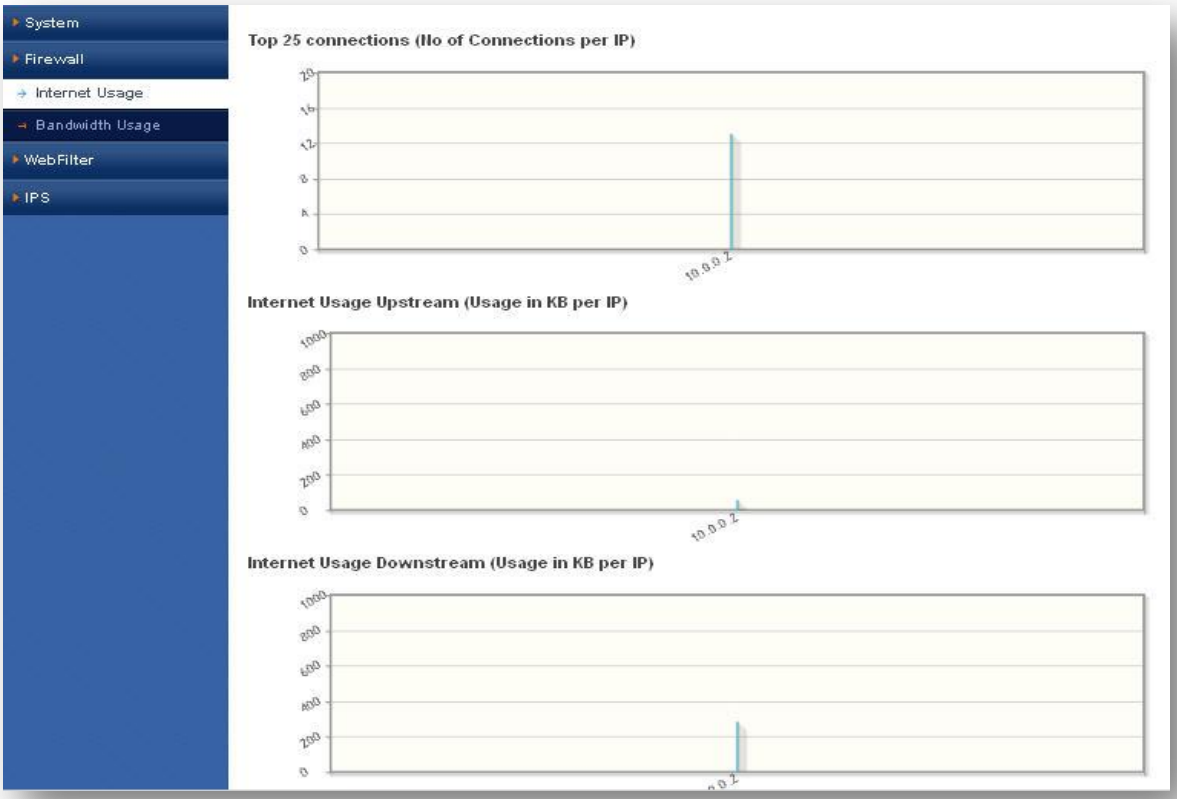


Figure 114: Internet Usage

9.2.2 Bandwidth Usage

Navigate through **Reports** > **Firewall > Bandwidth usage**

It shows WAN bandwidth usage in graphs.

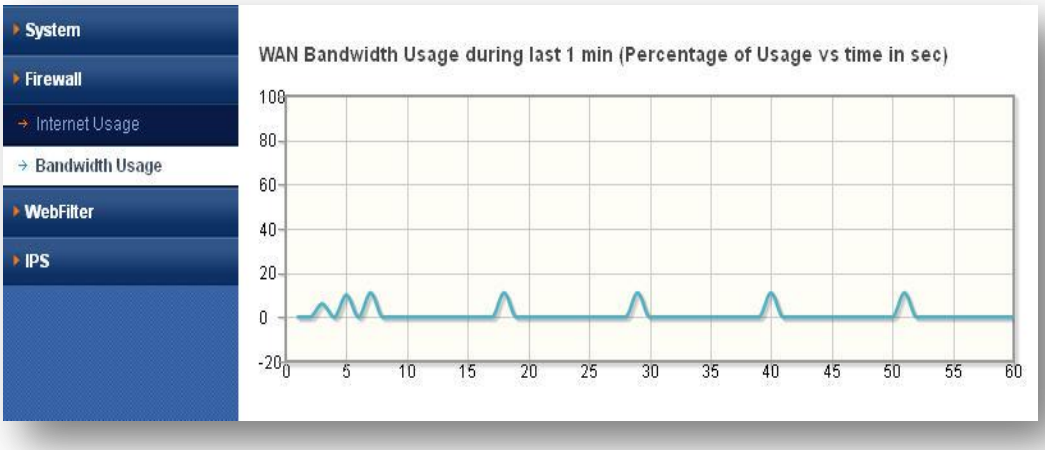


Figure 115: Bandwidth Usage

9.3 Web filter

Navigate through **Reports** > **Web filter**

It displays the web filter log viewer running in real-time mode. User can refresh reports and go to web filters main page.

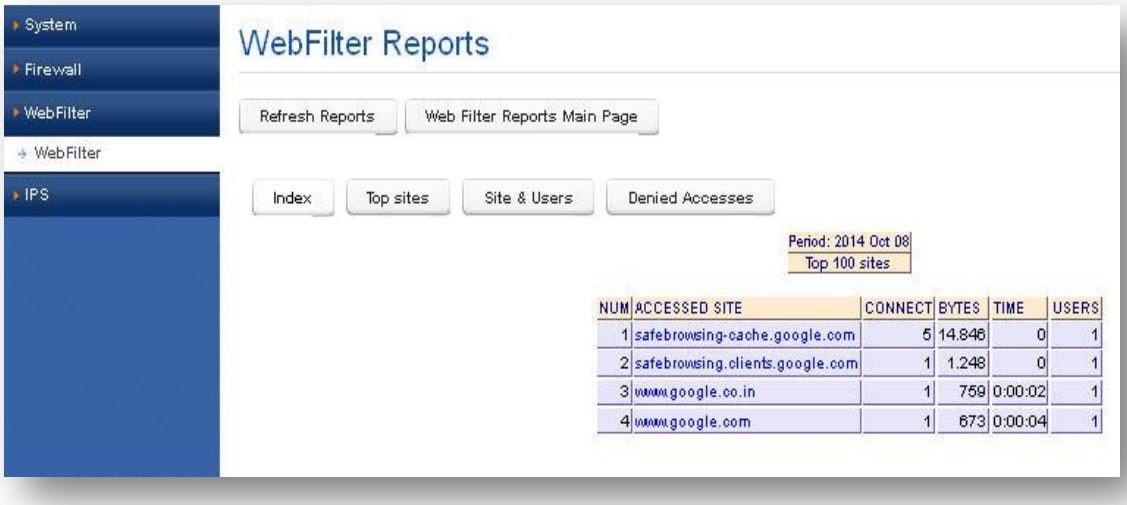


Figure 116: Web filter

9.4 IPS Alert Reports

Navigate through **Reports** > **IPS Alert Reports**

It shows top 25 signatures hit per IP in the graph. It also shows top 25 signature categories per IP & Top IP source alerts

Frequently Asked Questions (FAQs)

What are unified threat management (UTM) devices?

It's an approach for security management that allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console.

UTM devices combine an Intrusion Prevention System (IPS), Web filtering, Firewall and antivirus into a single hardware platform.

What is Network Security? How UTM gives security to Network?

Network Security consists of the providers and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

UTM gives security to internal network by making use of Firewall, IPS (Intrusion Prevention System), VPN Connectivity, Layer 7 filtering, Web filtering, NAT etc.

What is Proxy? What application proxies are included?

A proxy server is a hardware or software system that acts as an intermediary between an endpoint device and another server from that device is requesting a service. UTM supports HTTP, SSH Proxies.

What are the advantages of Unified Threat Management?

Unified Threat Management is a cost-effective solution to integrate multiple features into a single appliance.

i. Easy to Configure
ii. Less time used for maintenance
iii. Better Performance
iv. Effective Cost

What does Unified Threat Management include?

Unified Threat Management is a cost-effective solution to integrate multiple features into a single appliance. It includes following features:

i. Firewall
ii. IPS (Intrusion Prevention System)
iii. NAT (Network Address Translation)
iv. Web Filtering
v. VPN (SSLVPN and IPSec VPN)
vi. Layer-7 Filtering
vii. Anti-Virus

What is Layer 7 Application Control?

The online threat to productivity and security in your organization has evolved beyond simple Web traffic. Problematic applications such as Bit Torrent, Skype, and TOP can compromise available bandwidth and expose you to inappropriate and illegal activity.

Protocols are not identified by conventional web filters, these types of applications are difficult to stop.

Shield UTM allows you to stop this traffic at the gateway itself.

What user authentication methods are supported by shield UTM?

I. PAP (Password Authentication Protocol)
II. CHAP (Challenge Authentication Protocol) &
III. RADIUS Authentication etc.

Glossary

Term	Definition
BPS *Bit per Second*	The bit/sec is a common measure of data speed for computer modems and transmission carriers.
SSH*- Secure SHell*	It works on TCP protocol & Port number is 22, sometimes known as Secure Socket Shell. It is a UNIX-based command interface and protocol for securely getting access to a remote computer.
HTTP *-Hyper Text Transport Protocol*	It works on TCP protocol & Port number is 80. The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text.
HTTPS *-Hyper Text Transport Protocol over Secure Socket Layer*	It stands for Hypertext Transfer Protocol Secure, makes it more difficult for hackers, the NSA, and others to track users. The protocol makes sure the data isn't being transmitted in plain-text format, which is much easier to eavesdrop on.
VPN *-Virtual Private Networks*	VPN is a network that is constructed by using public wires usually the Internet to connect to a private network, such as a company's internal network. There are a number of systems that enable you to create networks using the Internet as the medium for transporting data.
IPSec *-Internet Protocol Security*	It is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
SSLVPN *-Secure Socket Layer Virtual Private Network*	This is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPSec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer.
NTP *- Network Timing Protocol*	It is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
SNMP*- Simple*	It is an "Internet-standard protocol for managing devices on IP networks".

Term	Definition
Network Management Protocol	Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.
DNS Domain Name Server	DNS is the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.
PPPoE Point-to-Point Protocol over Ethernet	It is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices.
***PAP** Password Authentication Protocol*	It's an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources. Almost all network operating system remote servers support PAP.
***CHAP**- Challenge Handshake Authentication Protocol*	In computing, it authenticates a user or network host to an authenticating entity.
***SIP**-Session Initiation Protocol*	This is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks.
***DHCP**- Dynamic Host Control Protocol*	It is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
***FTP**- File Transfer Protocol*	This is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

Term	Definition
TFTP- *Trivial File Transfer Protocol*	It's a simple, lock-step, file transfer protocol which allows a client to get from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a Local Area Network.
SMTP - *Simple Mail Transfer Protocol*	A protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.
SSL - *Secure Socket Layer*	It is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
IP - *Internet Protocol*	It is a set of rules governing the format of data sent over the Internet or other network. The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
MAC - *Media Access Control*	Media Access Control layer is one of two sub layers of the Data Link Control layer and is concerned with sharing the physical connection to the network among several computers.
ICMP - *Internet Control Message Protocol*	This is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
IMAP- *Internet Message Access Protocol*	It is a protocol for e-mail retrieval and storage.
POP3- *Post office Protocol version 3*	This standard protocol for retrieving e-mail. The POP3 protocol controls the connection between a POP3 e-mail client and a server where e-mail is stored. The POP3 service uses the POP3 protocol for retrieving e-mail from a

Term	Definition
	mail server to a POP3 e-mail client.
TCP *- Transmission Control Protocol*	It is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet.
UDP *- User datagram protocol*	UDP is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP).
TCP/IP*-Transmission Control Protocol/ Internet Protocol*	TCP/IP is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.
VLAN *- Virtual Local Area Network*	A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.
LAN *- Local Area Network*	It is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area.
WAN *- Wide Area Network*	It's a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN).
VIP *- Virtual Internet Protocol*	A virtual IP address (VIP or VIPA) is an IP address that doesn't correspond to an actual physical network interface (port). Uses for VIPs include Network Address Translation (especially, One-to-many NAT), fault-tolerance, and mobility.

Thank you for choosing

allo.com

Adarsh Eco Place, #176, Ground Floor, EPIP Industrial Area, Kundalahalli
KR Puram Hobali, Whitefield, Bangalore - 560066.

Email: globalsales@allo.com
indiasales@allo.com

Phone: +91 80 67080808