# Check Point Device

## Prerequisites

- Console Cable
- Physical access to device (arrange any local site Engineer)


figure 1.0

## Configuration

### Step 1

- Connect the Power cable to the Check point Device.
- Connect the ethernet cable to check point Device and system.
- Open run dialog box with shortcut key - ***Win+R***
- Type the following command - ***ncpa.cpl*** & hit enter

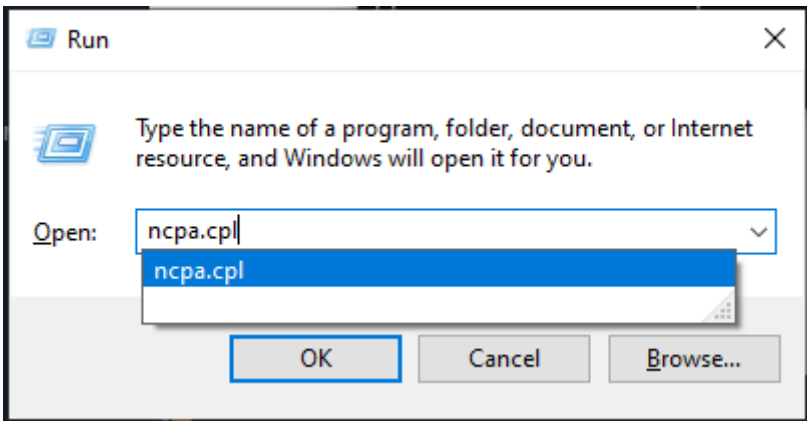



figure 1.1

## Step 2

- Control panel will open by the above command
- Select the **ethernet** which we connected for check point
- Right click on the ethernet connection and select **Properties**
- Ethernet Properties dialog box will open
- Select Internet Protocol Version 4 and assign IP address as shown in figure 1.2

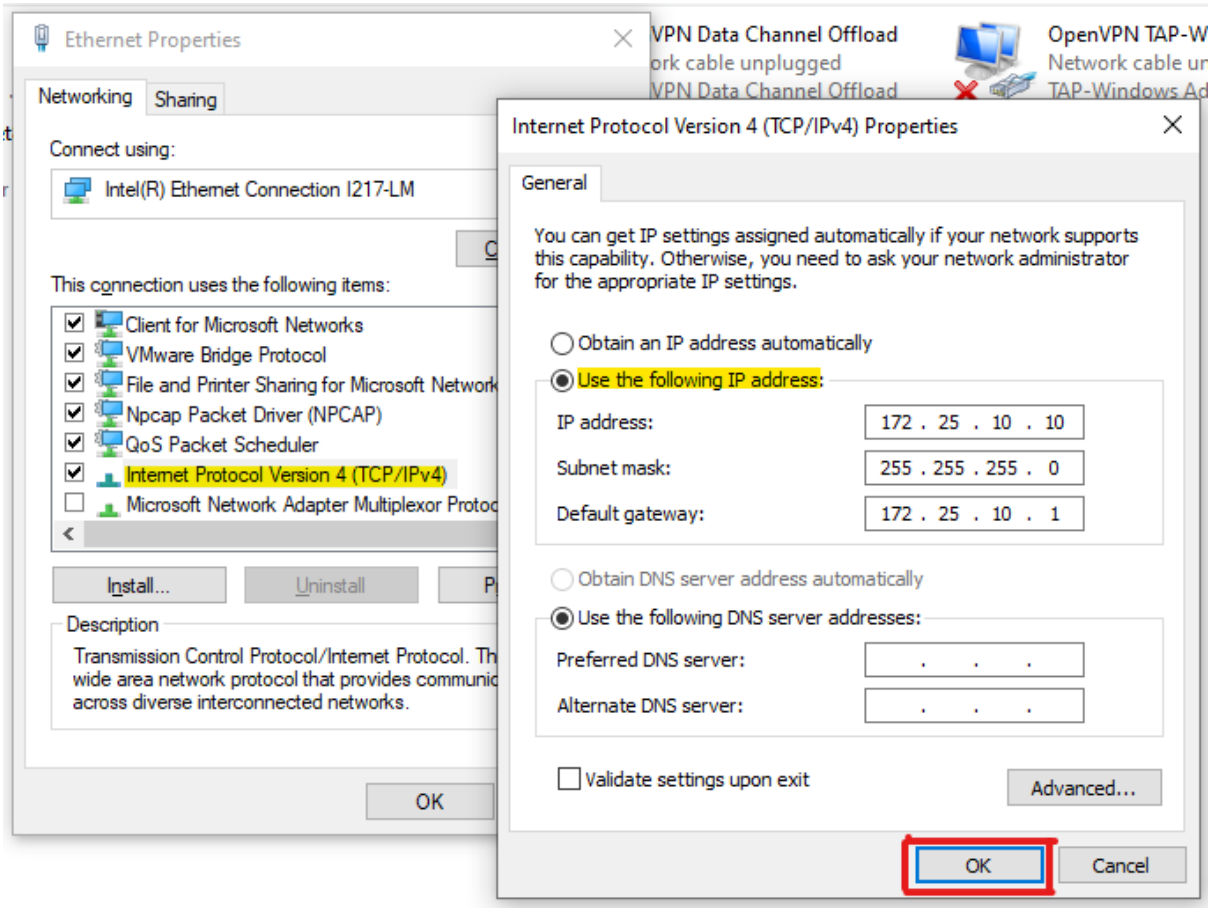



figure 1.2

## Step 3

- After the configuration check the IP of the system.
- Using command `#ipconfig` Configured IP can be viewed.
- Now try to Ping the check point device to check the connectivity
- Gateway IP is the IP of a check point device. `#Ping <Gateway-IP>`
- Show in figure 1.3

```
C:\Users\Tevel>ping 172.25.10.1

Pinging 172.25.10.1 with 32 bytes of data:
Reply from 172.25.10.1: bytes=32 time<1ms TTL=64
Reply from 172.25.10.1: bytes=32 time<1ms TTL=64
Reply from 172.25.10.1: bytes=32 time<1ms TTL=64
Reply from 172.25.10.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.25.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

figure 1.3

## Step 4

- Now access check point from any Browser using ip address
- Enter the Gateway IP address on the browser

  `# http://<ip-add>`
- It will open the Login page.

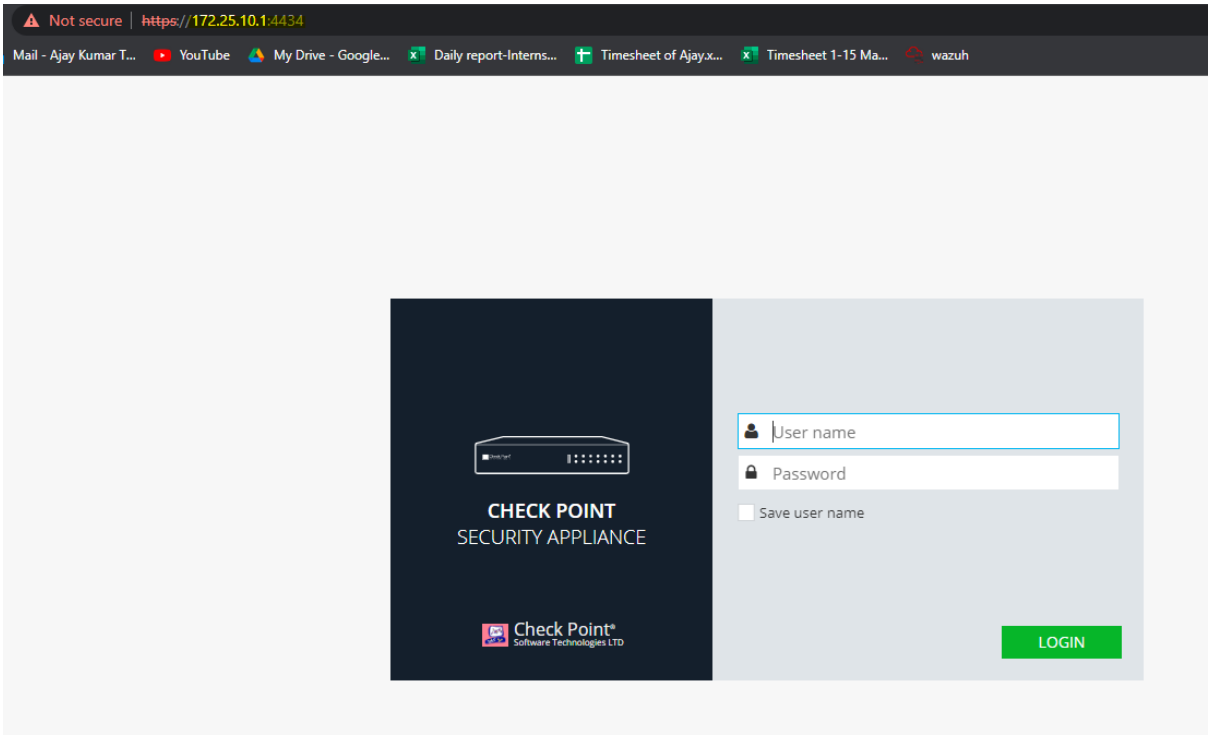



figure 1.3

## Step 5

- Enter the login credential
- Get logged in
- Check point dashboard will look like this.
- You will get the all  the General information in the visual representation format
- Information like system info, network, notification, mobile app, network activity all shown here. Refer figure 1.4

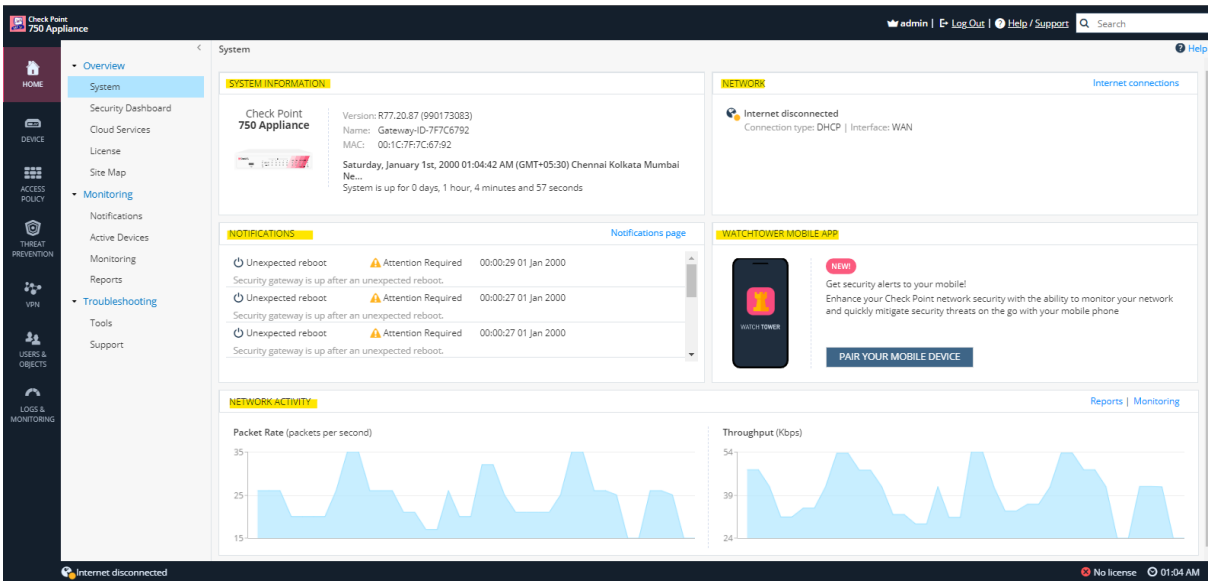



figure 1.4

# Features & Options

## Home

### Security dashboard

- View **Home -> Security Dashboard.**
- In this option we can Control, monitor software blades configuration and check status
- All the blades show here we can turn on or off as well. Show in figure 1.5.1

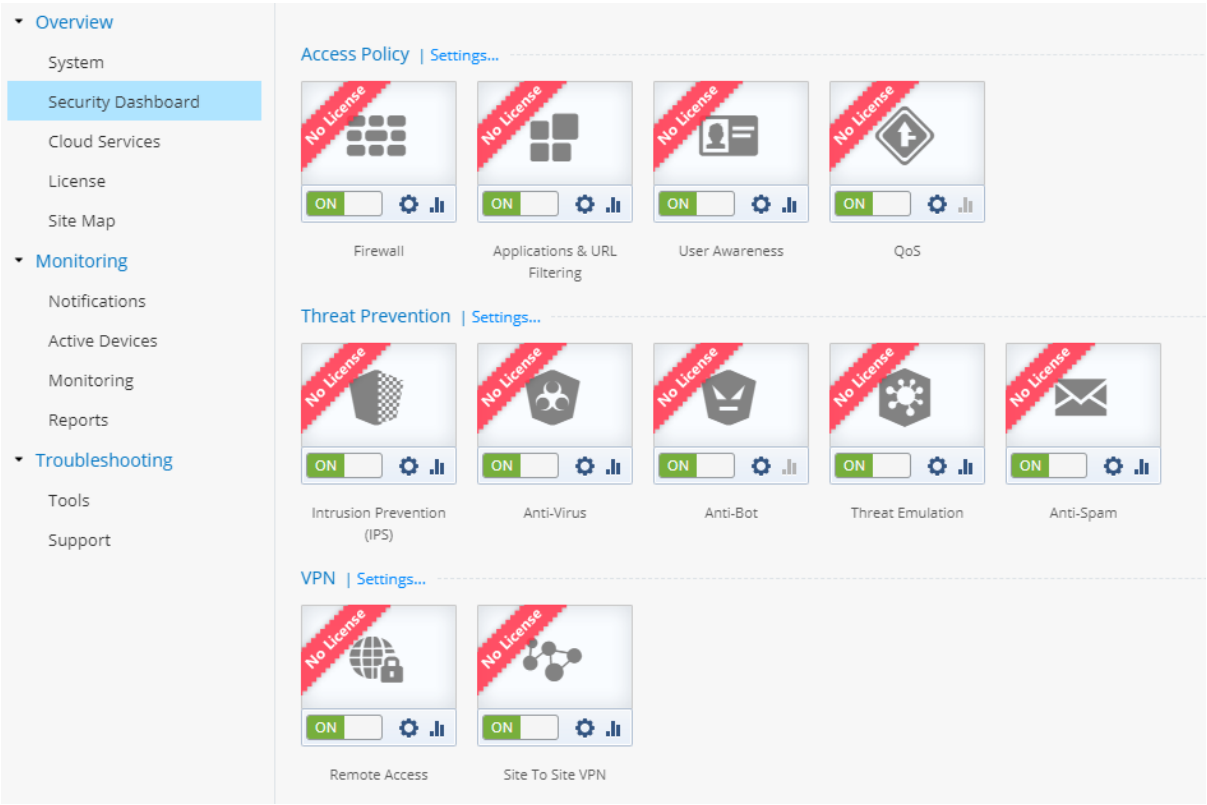



figure 1.5.1

### Cloud services

- View **Home -> Cloud services.**
- This option gives you the permission of setting up a cloud provider.
- Which can handle your security policy and supply a variety of services.
- Cloud network security unifies threat visibility and enforcement across your cloud and on-premises infrastructures. Refer figure 1.5.2

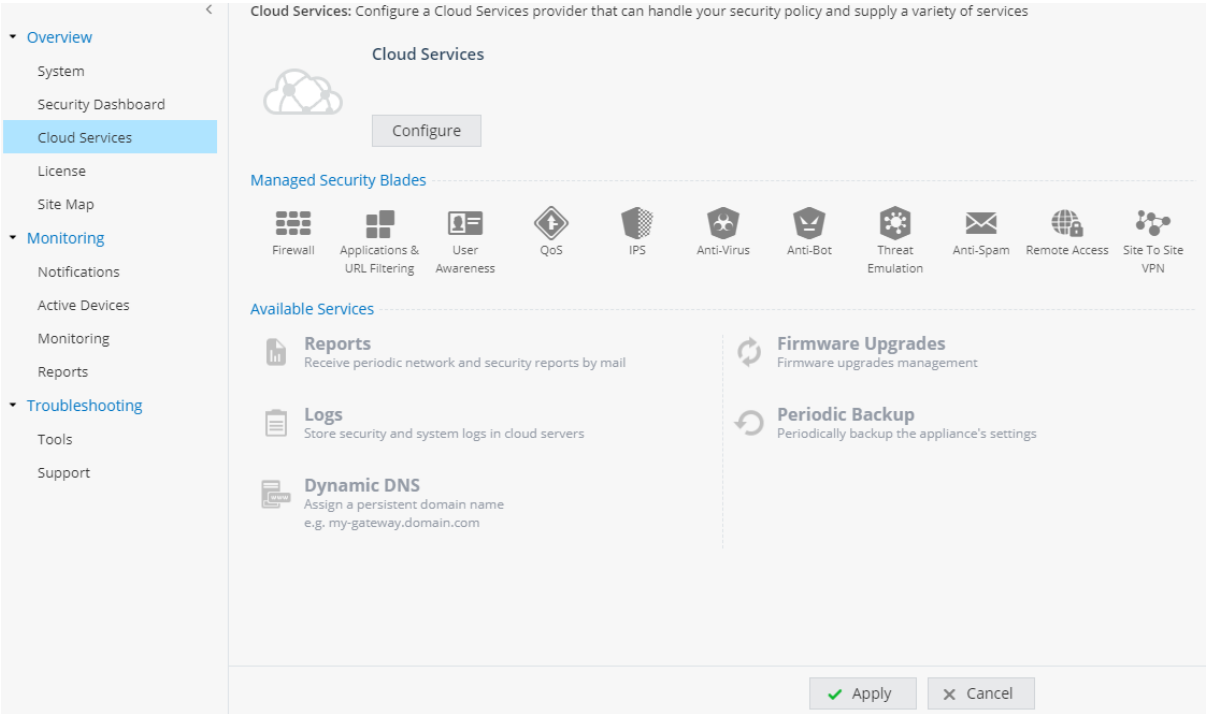



figure 1.5.2

## Licence

- View **Home -> licence**
- In this option we can view and configure licences.
- Currently this check point Device licence has expired. Refer figure 1.6

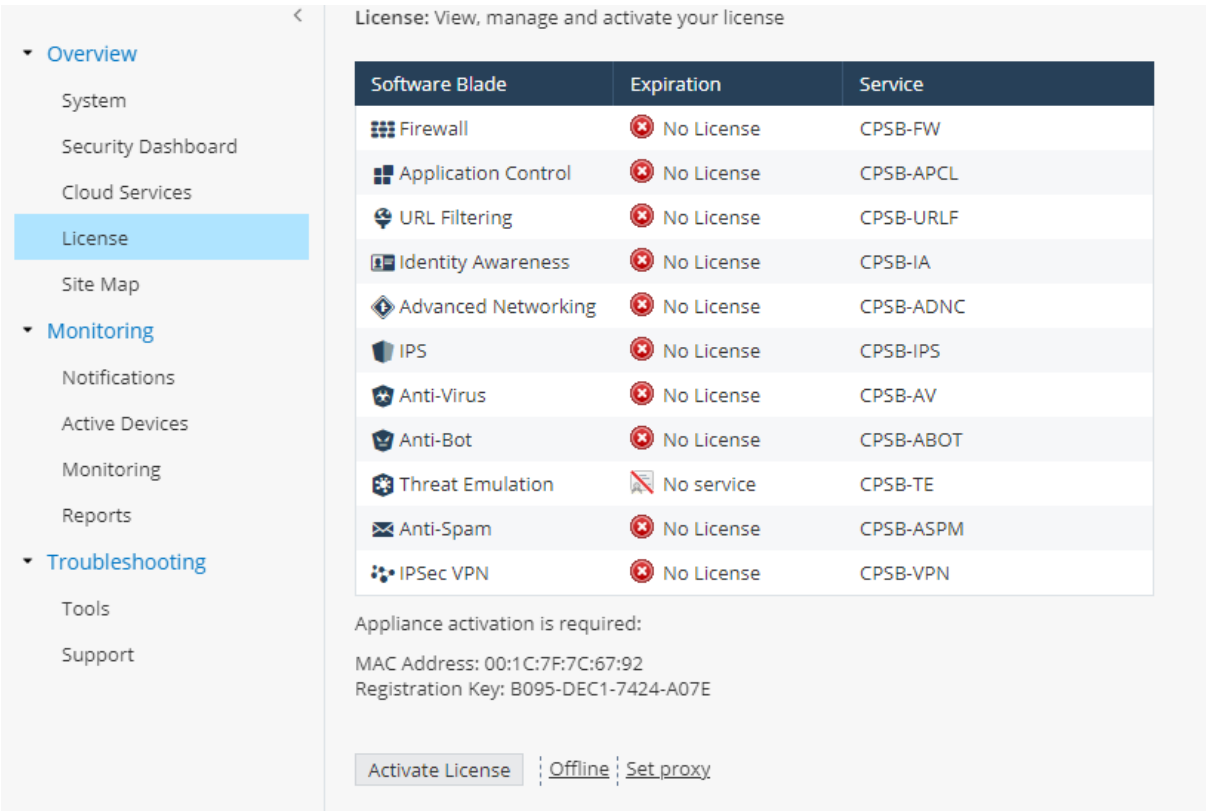



figure 1.6

## Site map

- View **Home -> Site map.**
- Navigation map of the different options can be found here. Refer figure 1.7

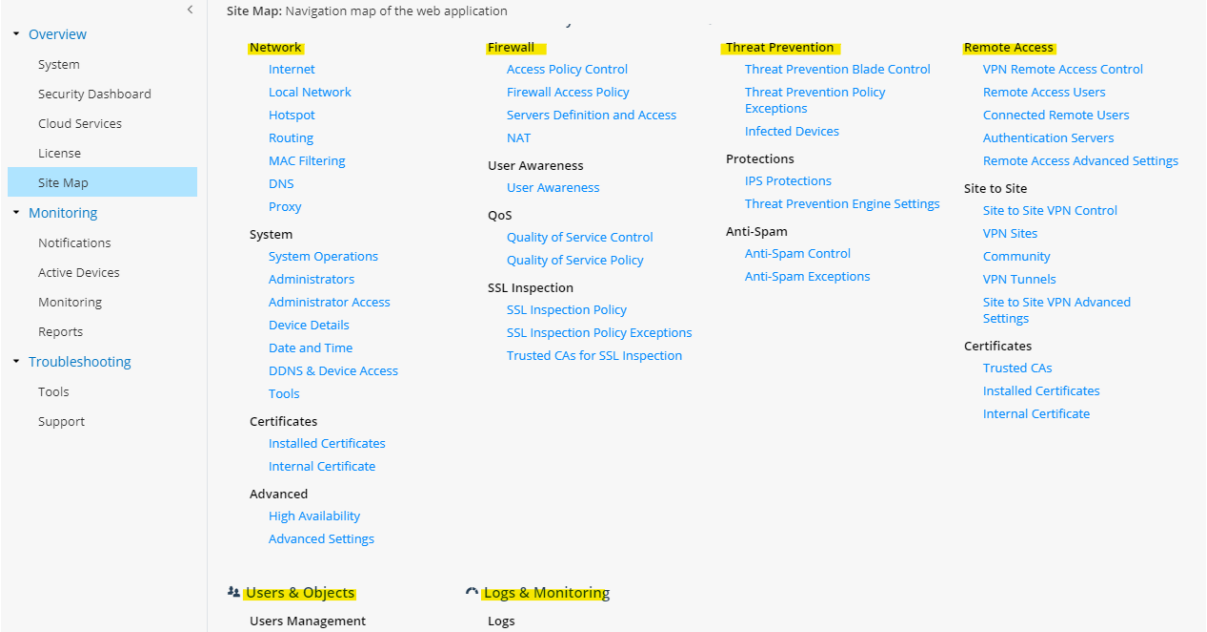



figure 1.7

## Notification

This option can be found in under **monitoring** section

- View **Home -> Monitoring -> notification**
- Notification of system events and security events can be viewed from here figure 1.8

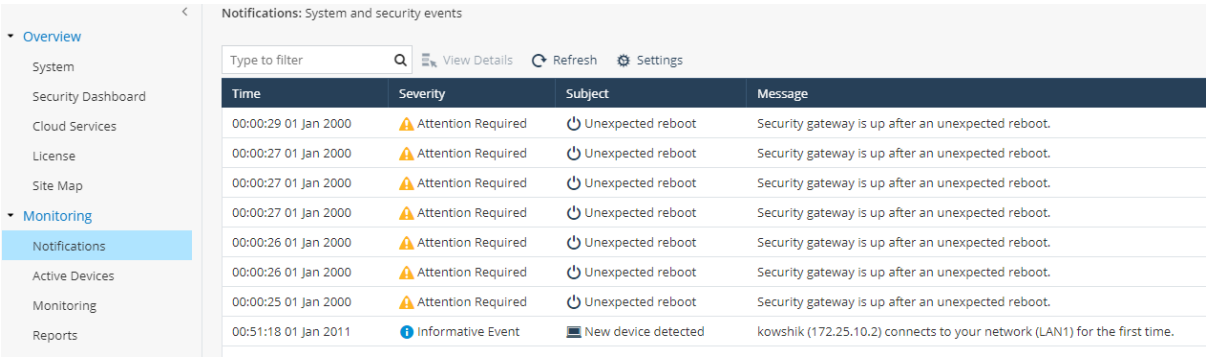



figure 1.8

## Active devices

- View **Home -> Monitoring -> active devices**
- It will display devices in internal network
- Currently we have a single device connected.
- Which we used to configure the check point. Refer figure 1.9

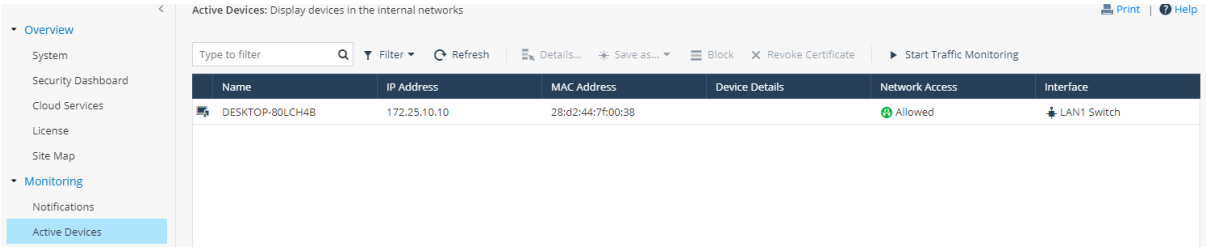



figure 1.9

## Monitoring

- View **Home -> Monitoring -> monitoring**
- It shows the Security Dashboard
- Infected devices, high risk application, security events & troubleshooting system resources etc., can be Viewed here.
- We can also view different logs here. Refer figure 2.0

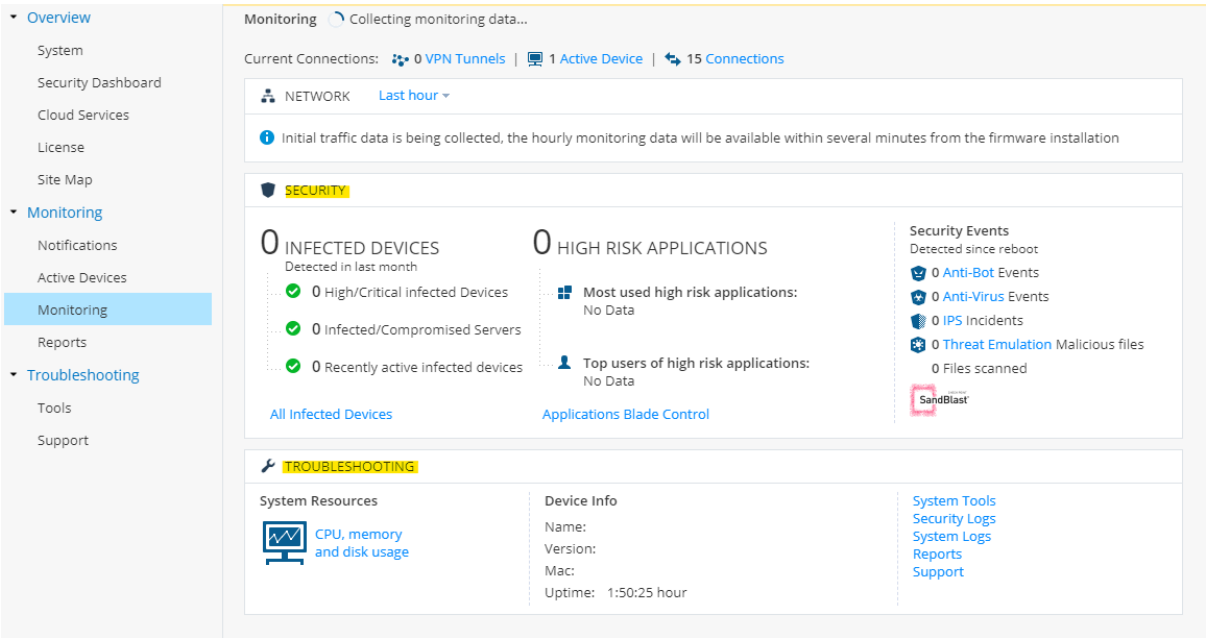



figure 2.0

### Reports

- View **Home -> Monitoring -> monitoring**
- We can get reports here
- Report can be monthly, weekly, daily
- Currently we Don't have any data to generate reports.

### Troubleshoot

- View **Home -> Troubleshoot**
- Tools to diagnose problems with the appliance & support option found here in the tools section.
- Also services of technical support found here in the support section.

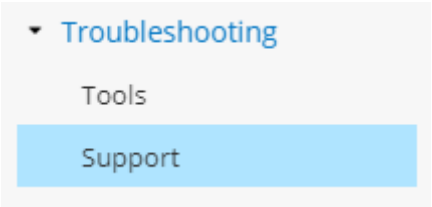



figure 2.1

## Device

### Network

- View **Device -> Network**
- In this we can view internet connections and manage all the connections

### Local network

- View **Device -> Local network**
- Configuration & management of  local interface switches, Bridge and VLAN's can be done from here. Refer figure 2.2

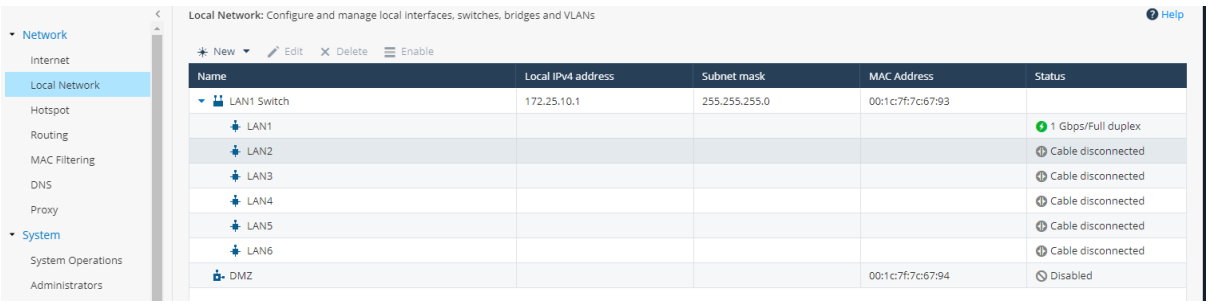



figure 2.2

## Hotspot

- View **Device -> Hotspot**
- Configure guest access and hotspot browser based authentication.

## Routing

- View **Device -> Hotspot**
- View routing tables and configure manual routing rules from here.

## Mac Filtering

- View **Device -> Mac Filtering**
- Allow clients with specific MAC addresses to access the internet.

## DNS

- View **Device -> DNS**
- Configure DNS and Domain Settings can be done from here. Refer figure 2.3

## Proxy

- View **Device -> Proxy**
- Configuration of proxy Session for connecting with check point update and licensees servers can be done from here

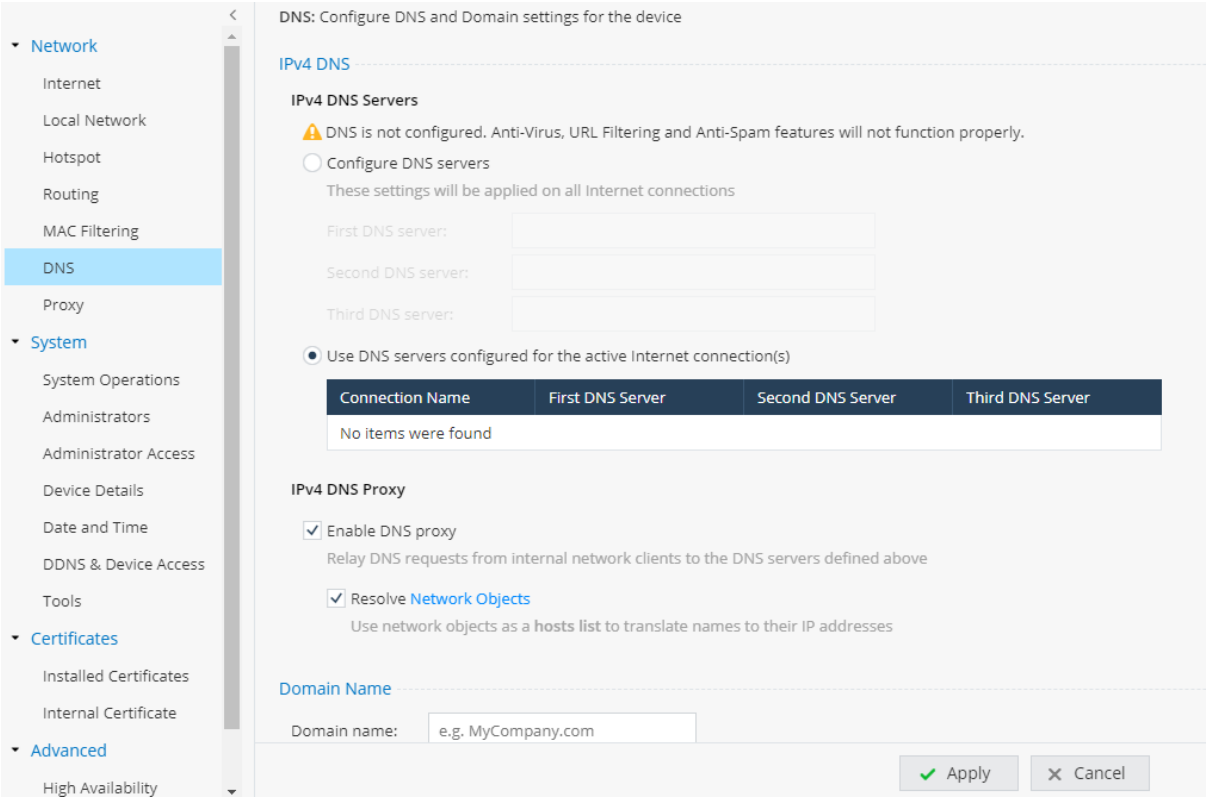



figure 2.2

## System Operations

- View **Device -> System -> System Operations**
- System operations manages your firmware version & backup your appliances
- This can be managed from here. Refer figure 2.3

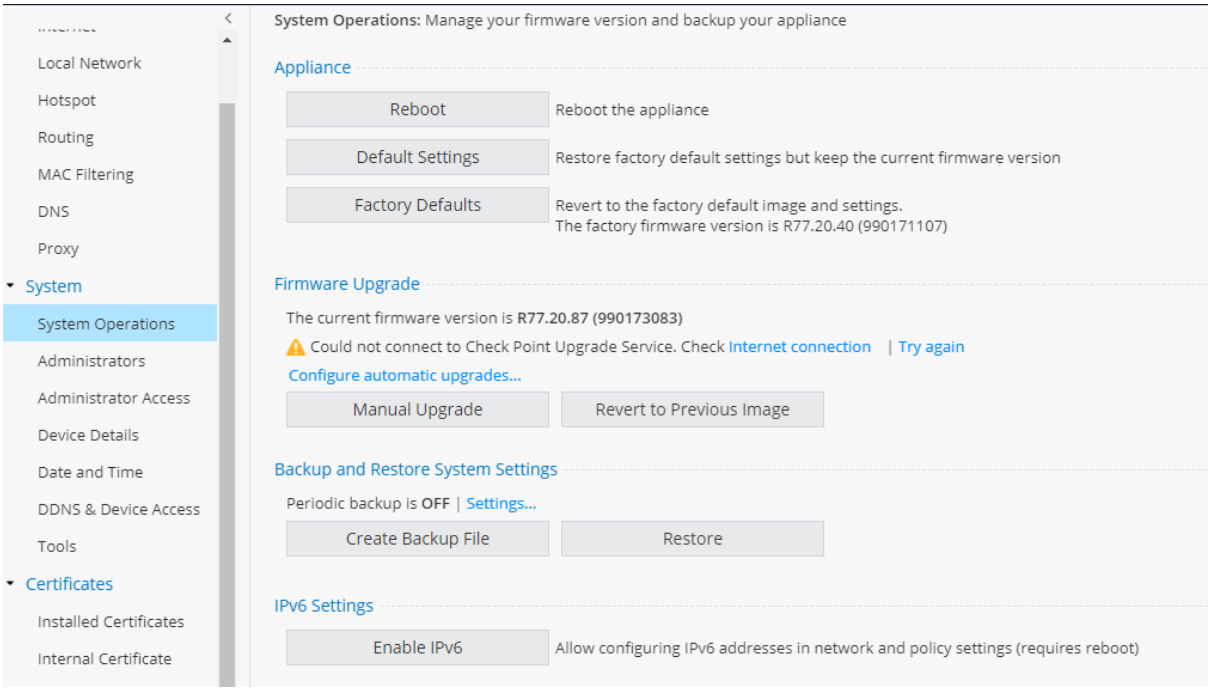



figure 2.3

## Administrator

- View **Device -> System -> Administrator**
- Assign Admin and connect mobile devices to the gateway from here. Refer figure 2.4

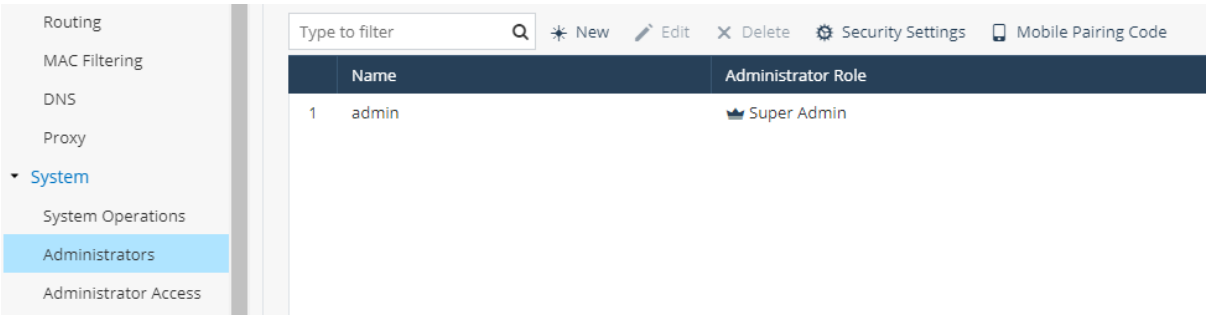



figure 2.3

## Administrator access

- View **Device -> System -> Administrator access**
- Web HTTP and SSH access for Administrator can be set up form here
- Refer figure 2.4

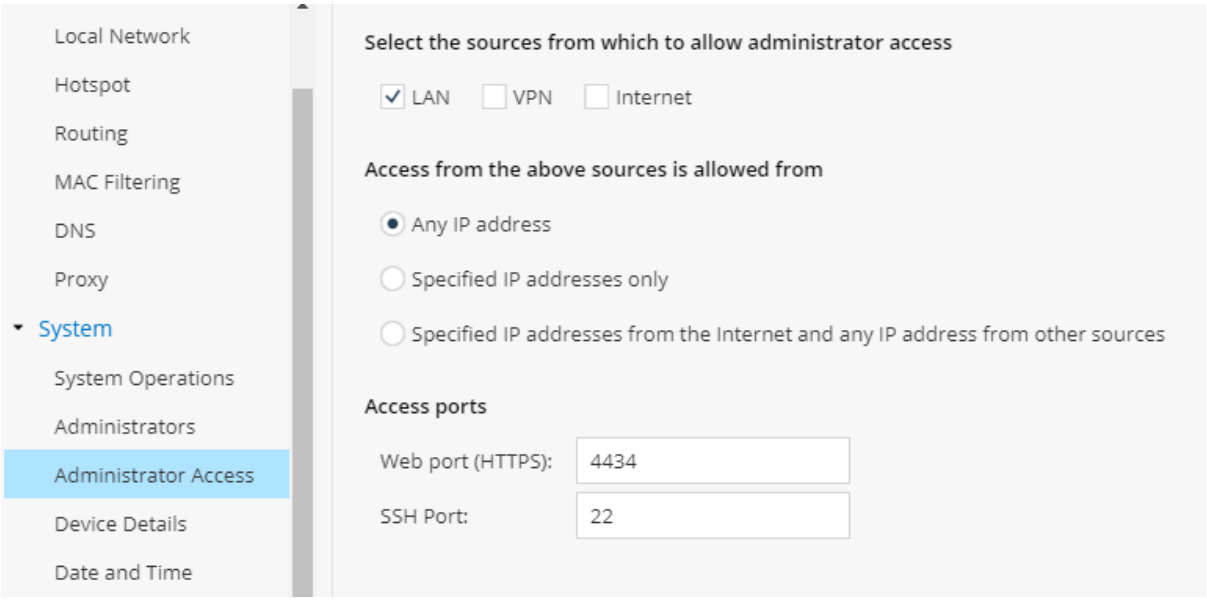



figure 2.4

## Device Details

- View **Device -> System -> Device Details**
- Configuration of Device NAME & Details can be Done from here. Refer figure 2.5

## Date & Time

- View **Device -> System -> Date and Time**
- Date & Time can be configured from here

## DDNS & Device access

- View **Device -> System -> DDNS & Device access**
- This option used to configure a persistent domain name for the Devices

## Tools

- View **Device -> System -> Tools**
- In this various tools are used to diagnose problems with the appliances. Refer figure 2.5

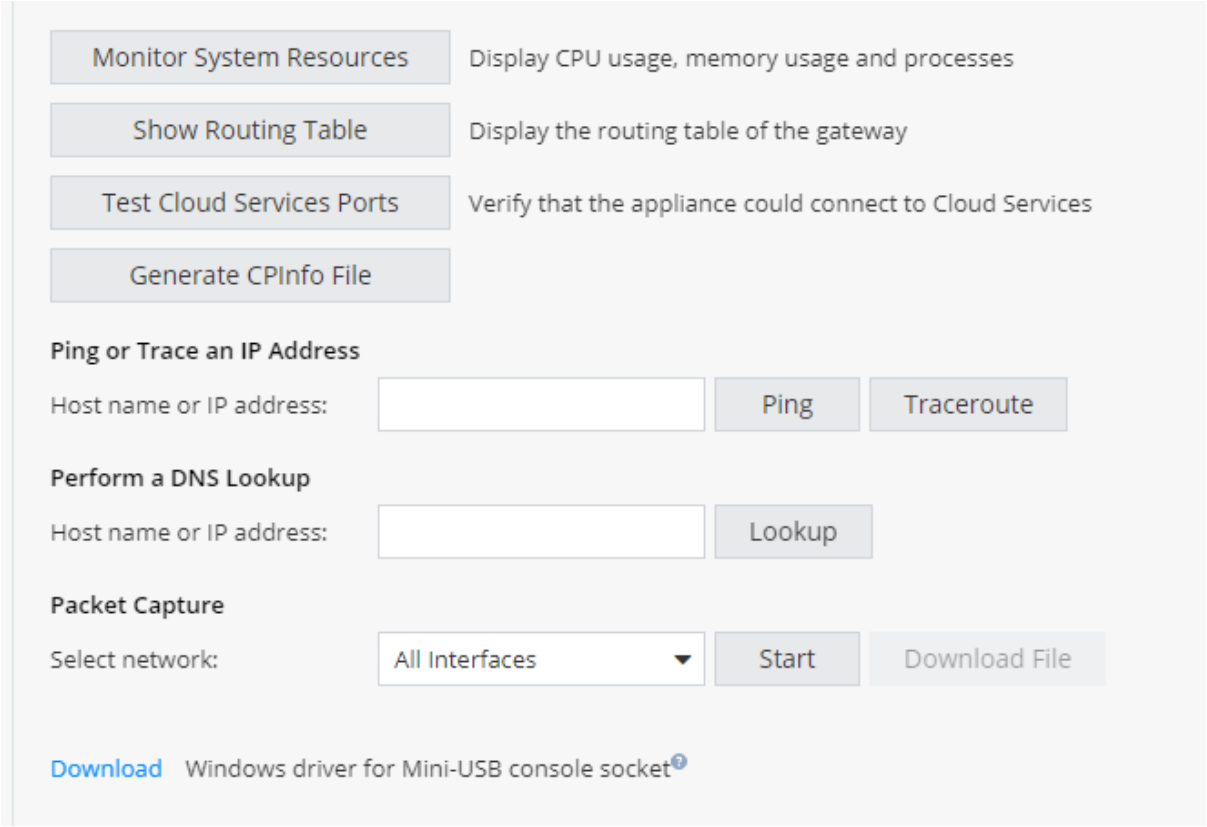



figure 2.5

## Certificates

- View **Device -> Certificates**
- Installed Certificate option allows you to create & manage appliances certificates
- Internal Certificate option Displays the appliances internal CA Certificate & internal VPN certificates . Refer figure 2.6

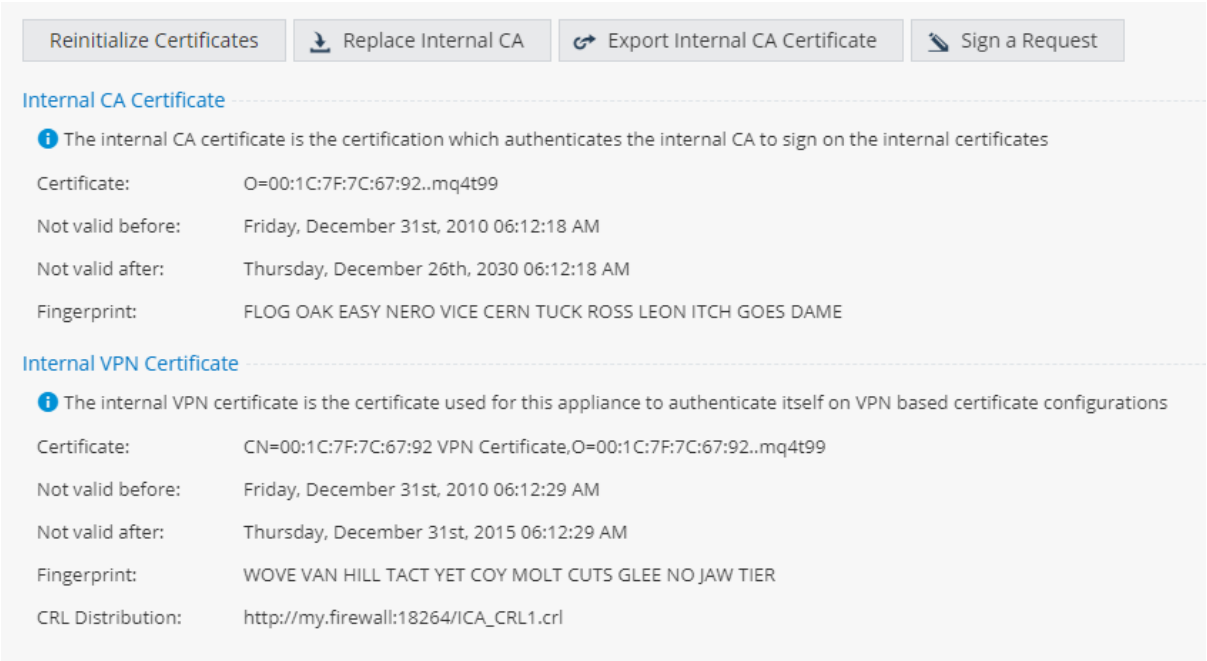



figure 2.6

## Advanced

- View **Device -> Advanced**
- High availability clusters between two appliances can be configured.
- In Advance setting we can manage very advanced settings of the Devices
- Refer figure 2.7


| Attribute Name | Type | Value | Description |
|---|---|---|---|
| Admin Lockout - Mobile application session timeout | int | 90 | Allowed mobile application session before automatic logout is executed (in days) |
| Administrators RADIUS authentication - Local authentication (RADIUS ina... | bool | false | Perform local administrator authentication only if RADIUS server is not configured or is inacc... |
| Aggressive aging - Aggress ive aging enforcement method | options | Both | Choose when aggressive aging timeouts are enforced |
| Aggressive aging - Connection table percentage limit | int | 80 | |
| Aggressive aging - Enable aggressive aging of connections | bool | true | |
| Aggressive aging - Enable reduced timeout for ICMP connections | bool | true | |
| Aggressive aging - Enable reduced timeout for TCP handshake | bool | true | |
| Aggressive aging - Enable reduced timeout for TCP session | bool | true | |
| Aggressive aging - Enable reduced timeout for TCP termination | bool | true | |
| Aggressive aging - Enable reduced timeout for UDP connections | bool | true | |
| Aggressive aging - Enable reduced timeout for non TCP/UDP/ICMP conne... | bool | false | |
| Aggressive aging - Enable reduced timeout for non TCP/UDP/ICMP conne... | bool | false | |
| Aggressive aging - ICMP connections reduced timeout | int | 3 | |
| Aggressive aging - Memory consumption percentage limit | int | 80 | |
| Aggressive aging - Other IP protocols reduced timeout | int | 15 | |

figure 2.7

# Access Policies

## Blade Control

- View **Access Policies -> Blade Control**
- We can control blade from here figure 2.8

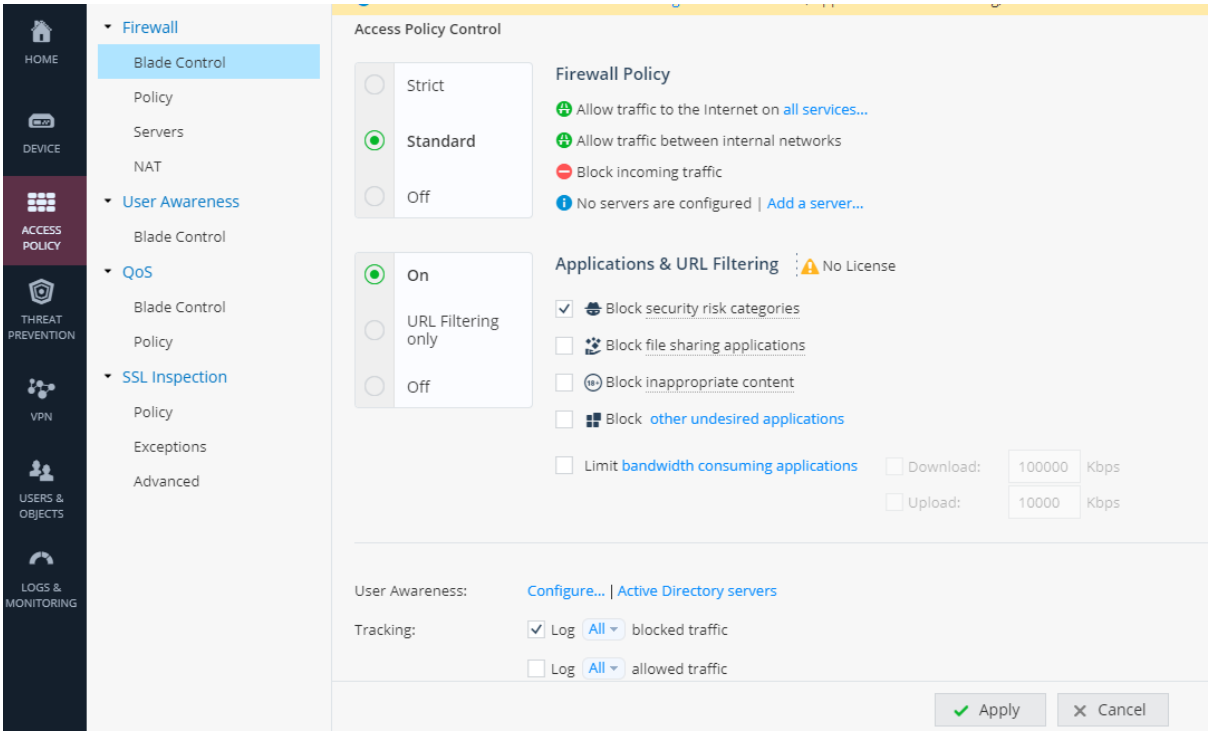



figure 2.7

## Policy

- View **Access Policies -> Policy**
- We can set the policy of incoming and outgoing traffic using firewall blades. Refer figure 2.8

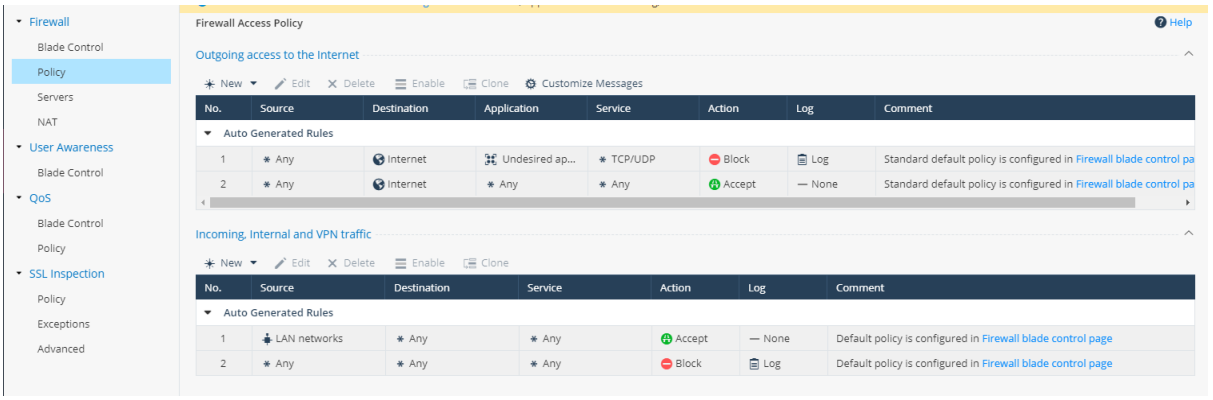



figure 2.8

## Servers

- View **Access Policies -> Servers**
- It allows server Definiton & Access permissions configuration. Refer figure 2.9

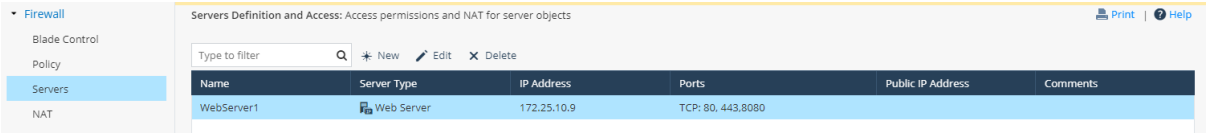



figure 2.9

## NAT

- View **Access Policies -> NAT**
- From this option we can turn on/off outgoing traffic & can configure NAT. Refer figure 3.0

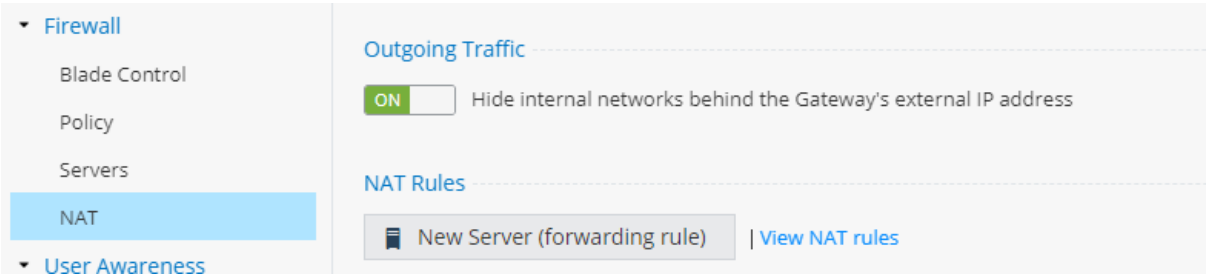



figure 3.0

## Blade control

- View **Access Policies -> User awareness -> Blade control**
- In this we can incorporate users into access policy and Display users in Security Logs. Refer figure 3.1

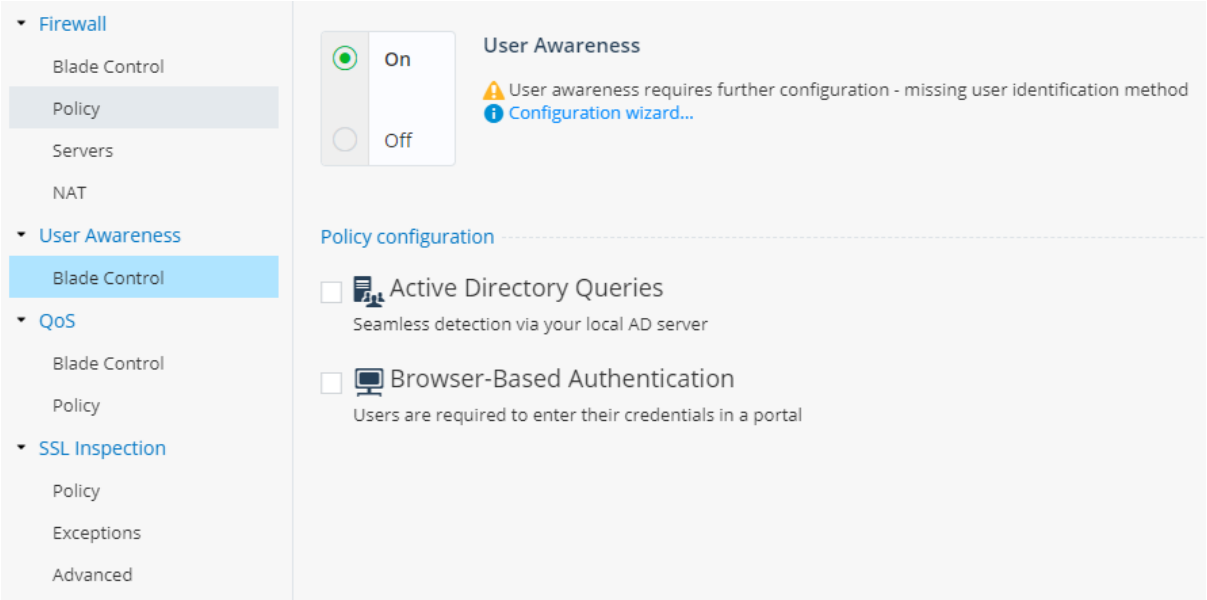



figure 3.1

## QoS

### Blade control

- View **Access Policies -> QoS -> Blade control**
- In this option we can turn on/off Qos blade & manage bandwidth by configuring quality of services Qos policy. Refer figure 3.2

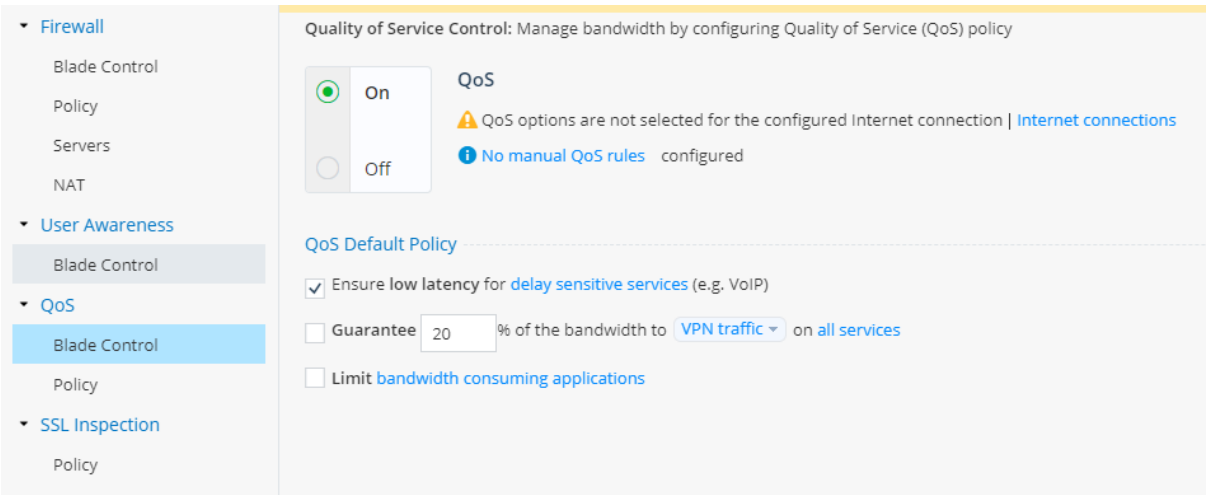



figure 3.2

## Policy

- View **Access Policies -> QoS -> Policy**
- In this option we can manage bandwidth by configuring quality of services Qos policy. Refer figure 3.3

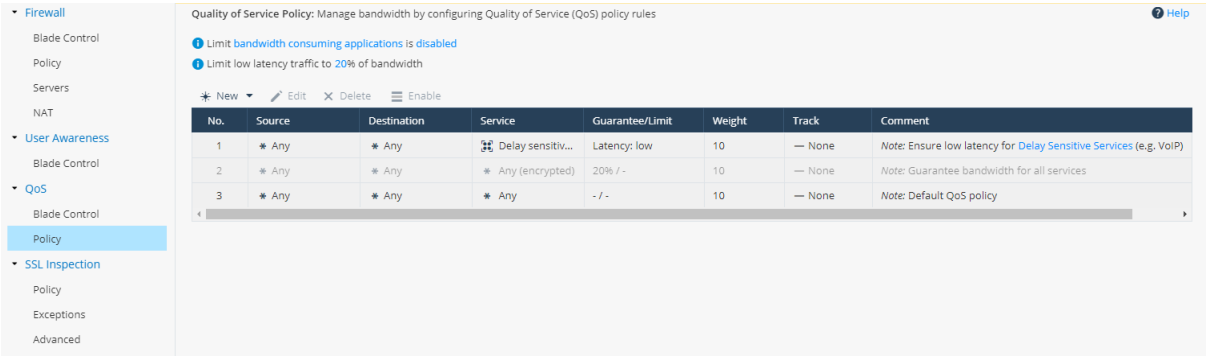



figure 3.3

## SSL Inspection

## Policy

- View **Access Policies -> SSL Inspection -> Policy**
- In this option we can configure ssl traffic inspection & http categorization. Refer figure 3.4

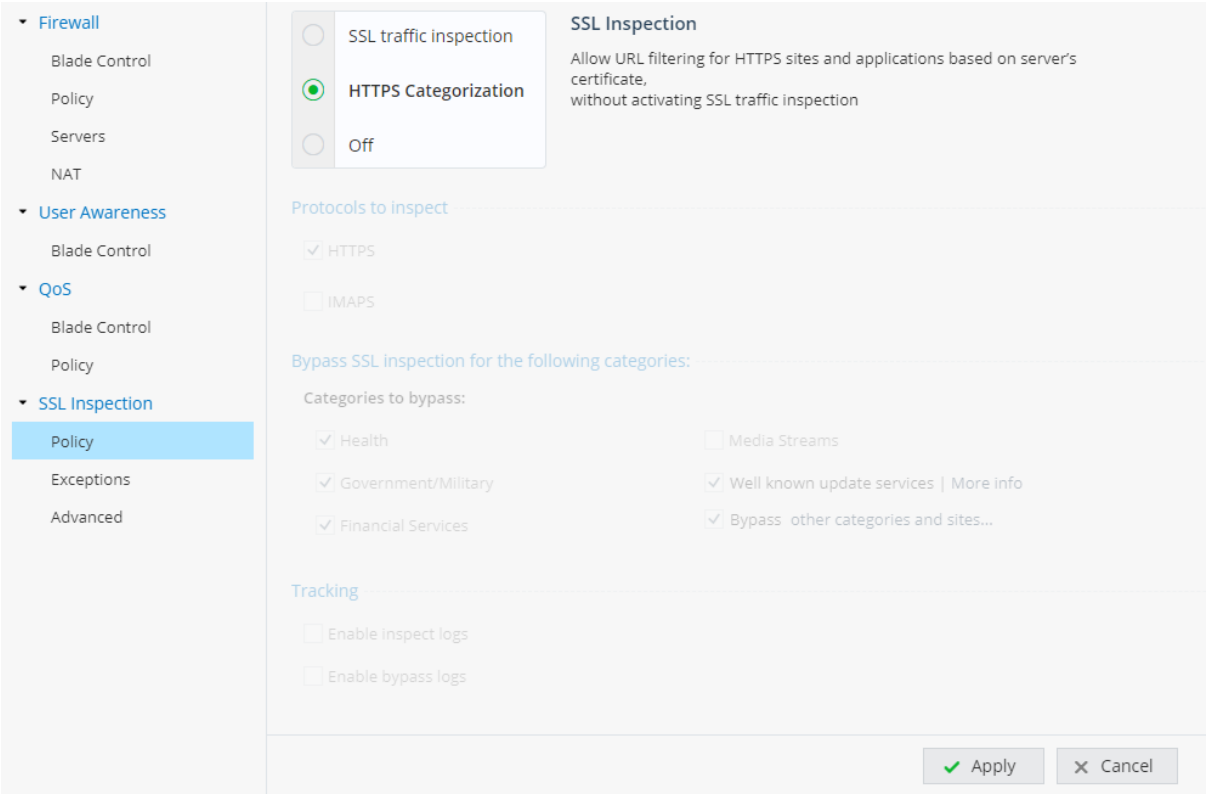



figure 3.3

## Exception

- View **Access Policies -> SSL Inspection -> Exception**
- In this we can configure the exception using which policy we created. Refer figure 3.4

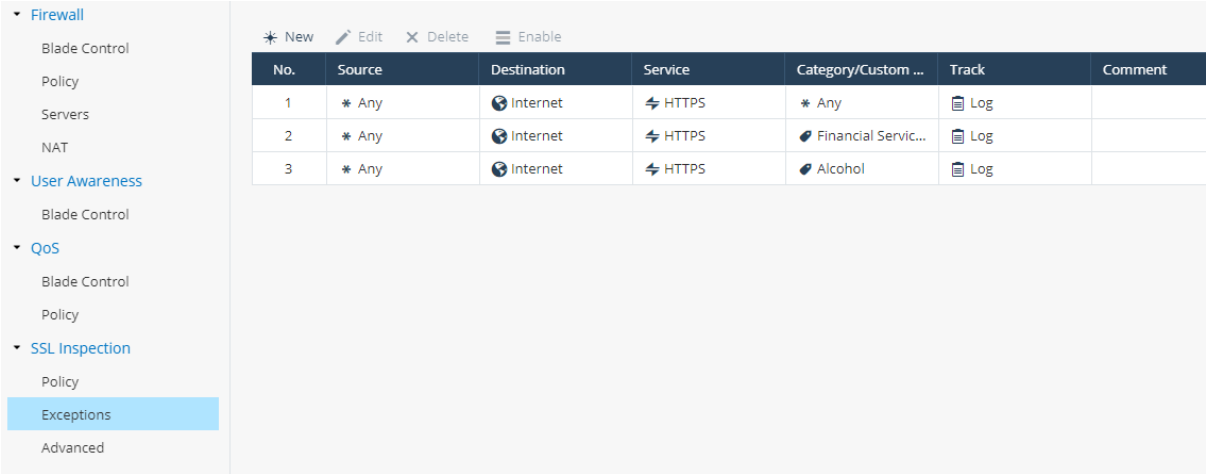



figure 3.4

## Advanced

- View **Access Policies -> SSL Inspection -> Advanced**
- In this we can view advanced ssl inspection. Refer figure 3.5

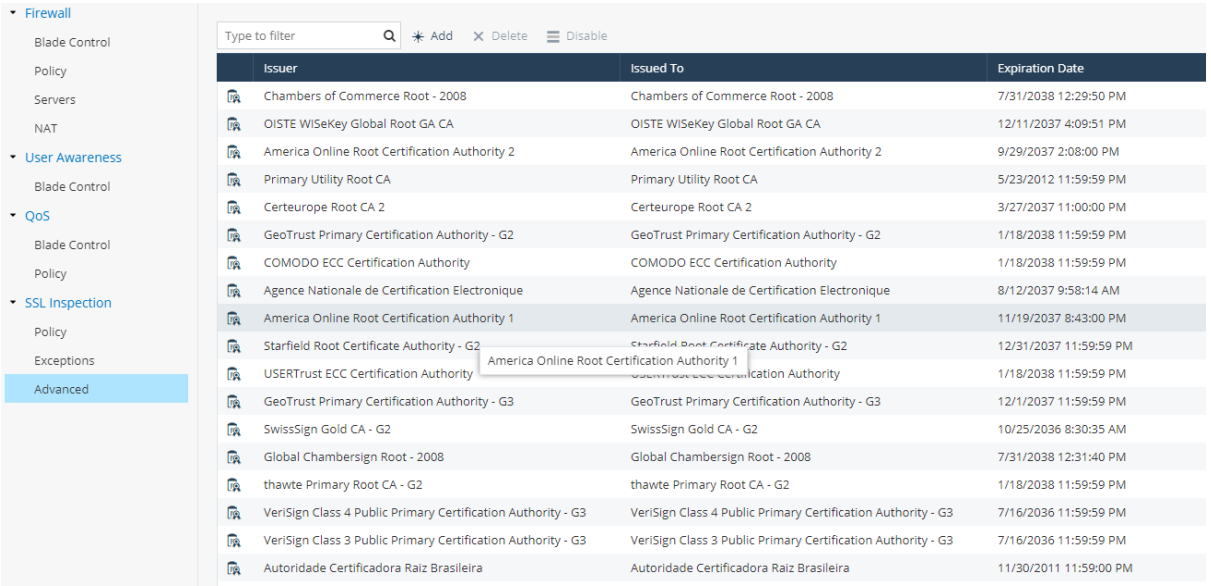



figure 3.5

# Threat Prevention

## Blade control

- View **Threat Prevention -> threat prevention -> Blade control**
- We can control blades from here options like IPS, anti-virus, anti-bot, Threat emulation. Refer figure 3.6

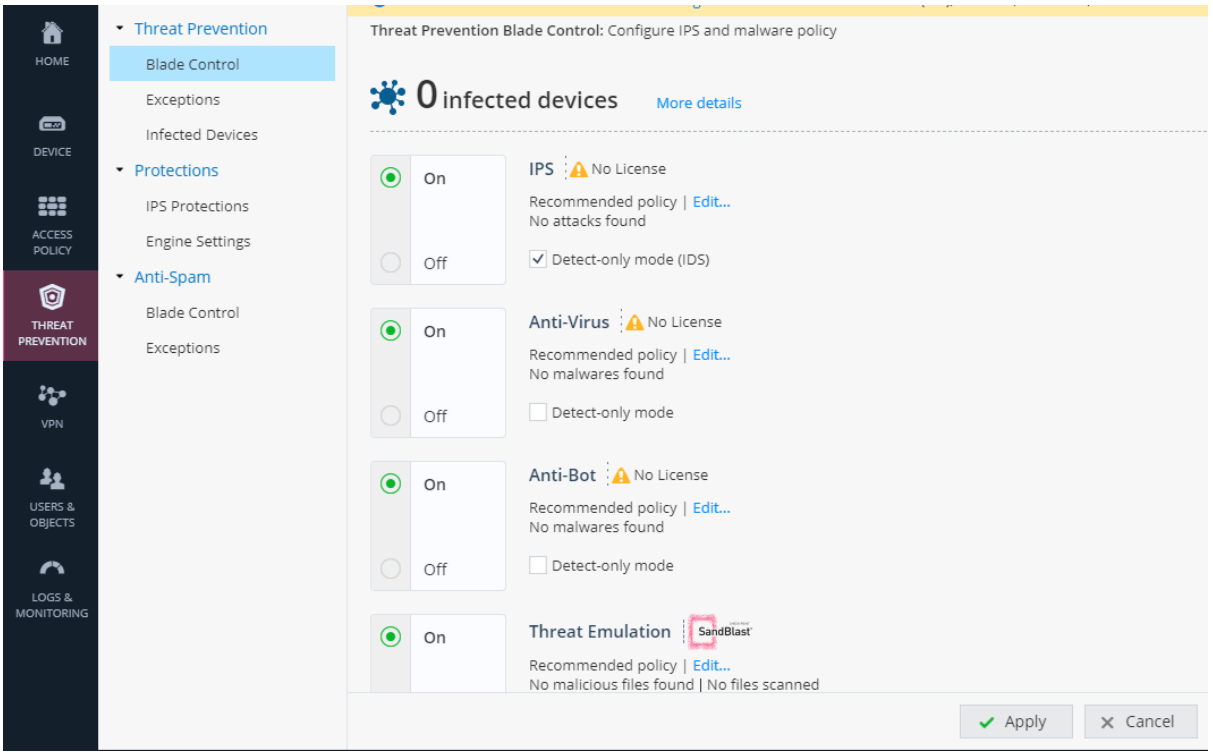



figure 3.6

## Exception

- View **Threat Prevention -> threat prevention -> Exception**
- We can configure threat prevention policy exceptions for specific traffic. Refer figure 3.7

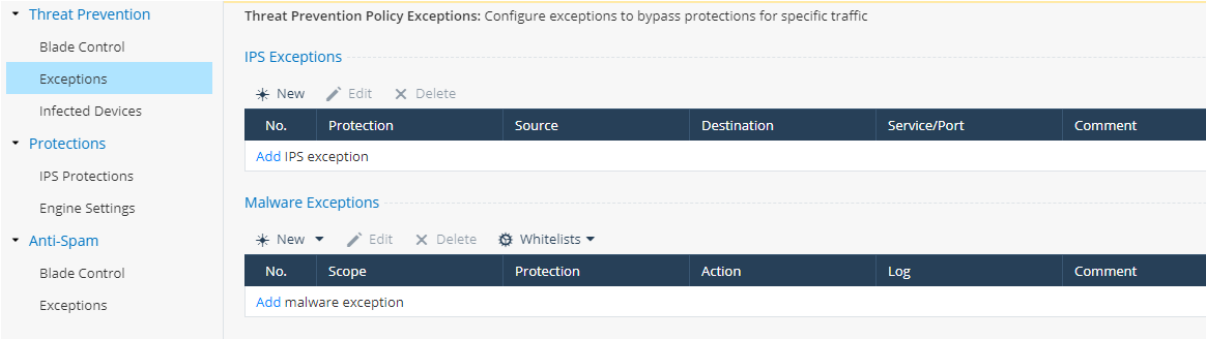



figure 3.7

## Infected Device

- View **Threat Prevention -> threat prevention -> Infected Device**
- This option shows infected devices in a network. Refer figure 3.8

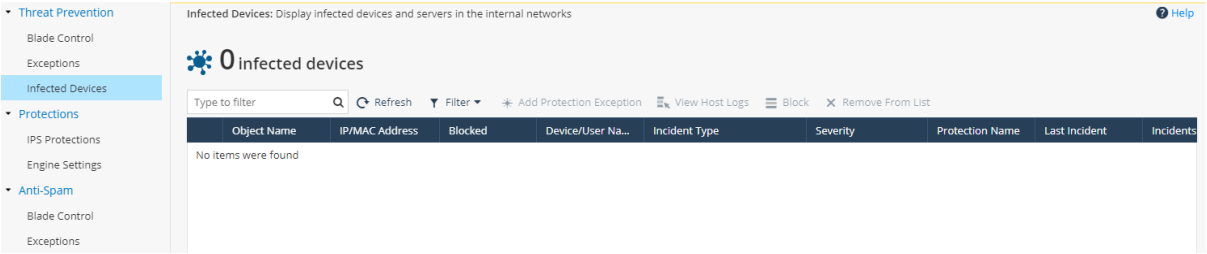



figure 3.8

## Protections

## IPS Protection

- View **Threat Prevention -> Protection -> IPS Protection**
- In this you will see a monitor protection list and manually configure protection to override general protection. Refer figure 3.9

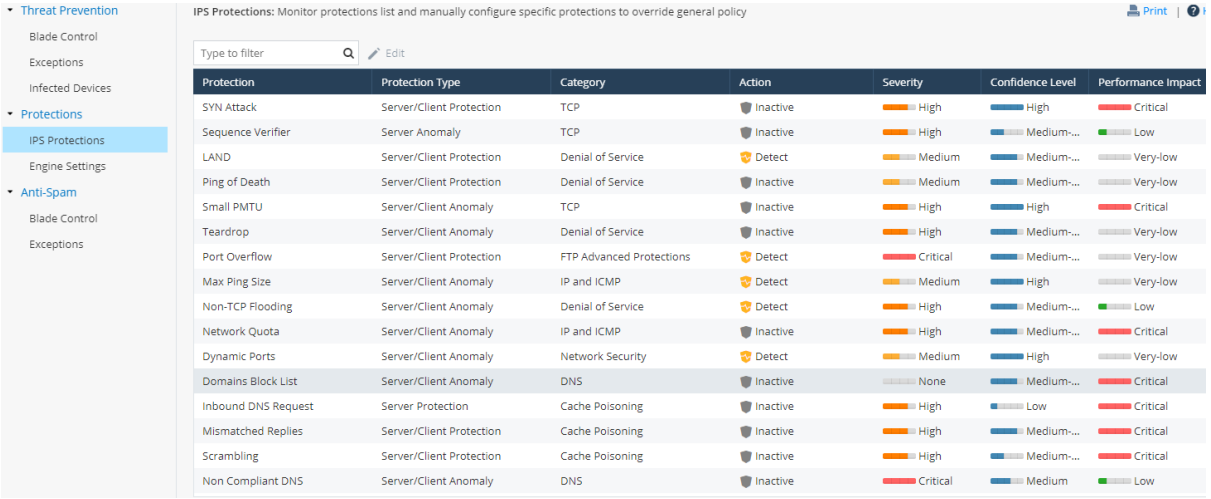



figure 3.9

## Engine settings

- View **Threat Prevention -> Protection -> Engine settings**

- Here you will find Advance engine & policy settings.

## Anti spam

### Blade control

- View **Threat Prevention -> Anti spam -> Blade control**
- You can configure & turn on/off anti spam control. Refer figure 4.0

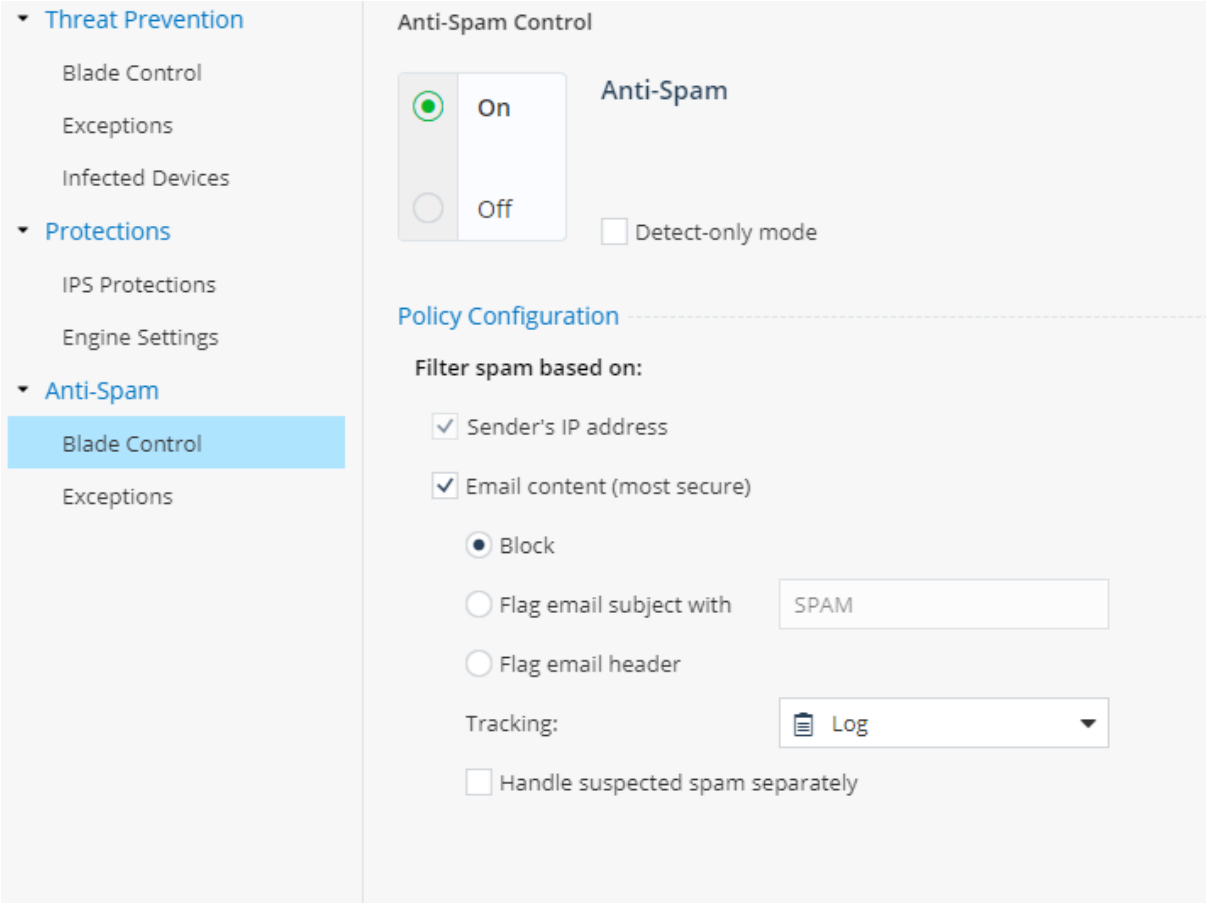



figure 4.0

### Exception

- View **Threat Prevention -> Anti spam -> Exception**

- Anti-spam exception - manually configure IP Address and Email Address to be exempt from the inspection or blocked. Refer figure 4.1

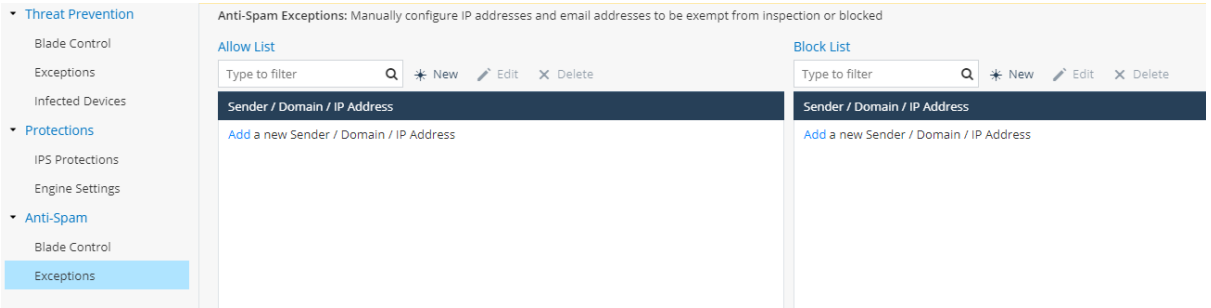



figure 4.1

# VPN

## Remote Access

### Blade control

- View **VPN -> Remote Access -> Blade Control**
- From here we can turn on/off Remote Access and other controls related to VPN. Refer figure 4.2

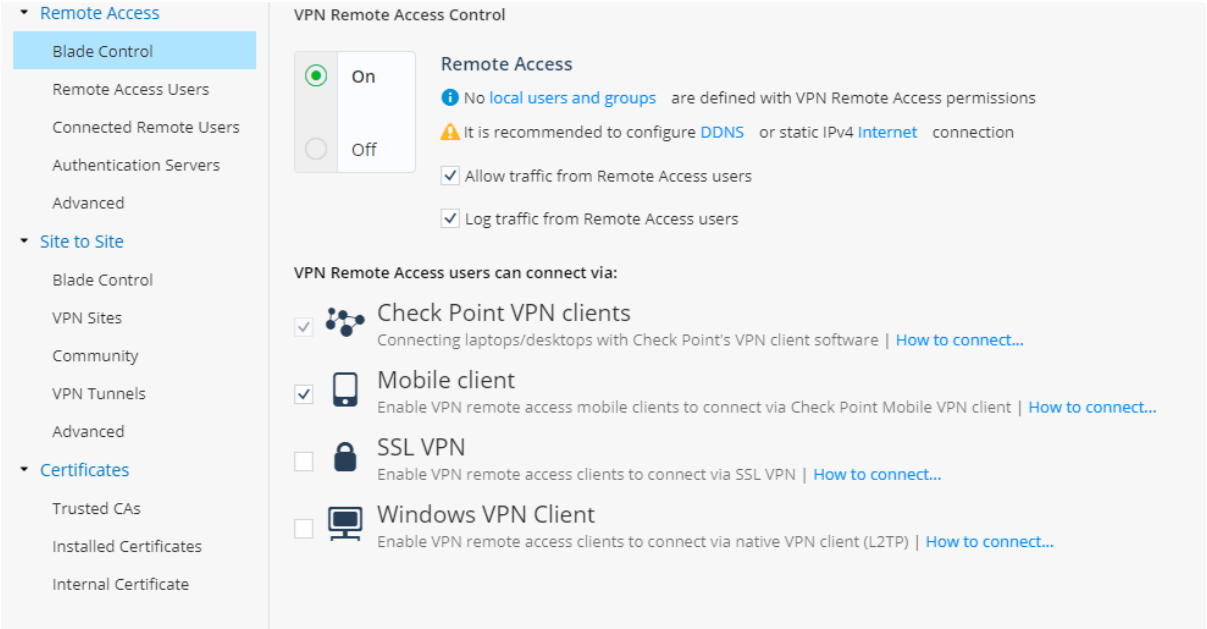



figure 4.2

## Remote Access Users

- View **VPN -> Remote Access -> Remote Access Users**
- From here we can configure access permission for users and Group. Refer figure 4.3

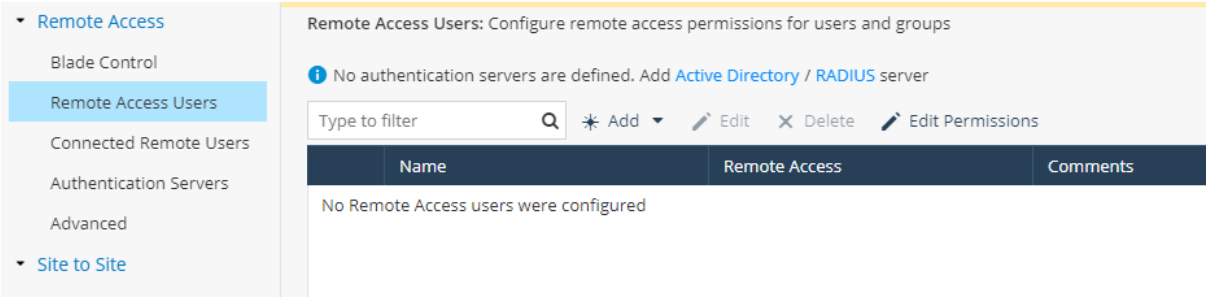



figure 4.3

## Connected  Remote users

- View **VPN -> Remote Access -> Connected Remote Users**
- We can configure and connect different users Remotely.

## Authentication Servers

- View **VPN -> Remote Access -> Authentication Servers**
- Configure remote access permission of users and groups. Refer figure 4.4

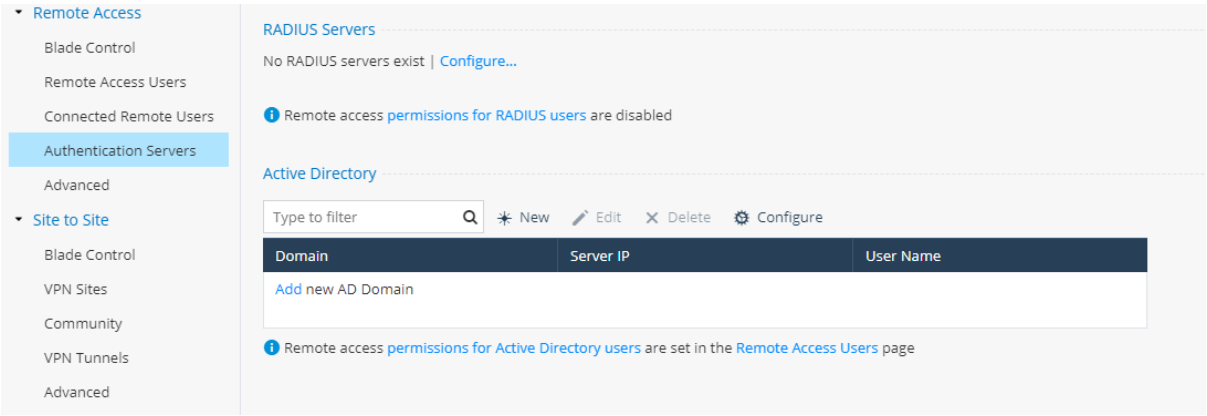



figure 4.4

## Advanced

- View **VPN -> Remote Access -> Advanced**
- Configure additional Advance options for VPN remote access users. Refer figure 4.5

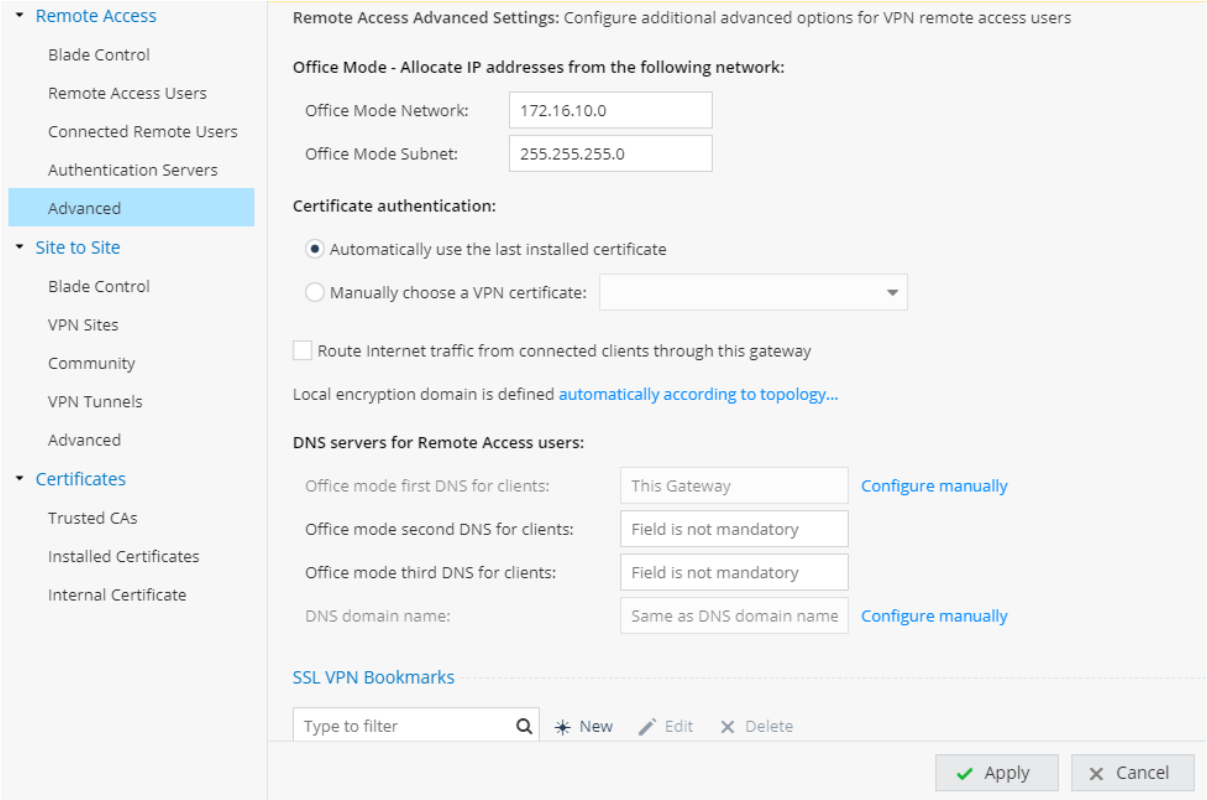



figure 4.5

## Site To Site

### Blade Control

- View **VPN -> Site To Site -> Blade Control**
- Turn on/off Site to Site VPN blade. Refer figure 4.6

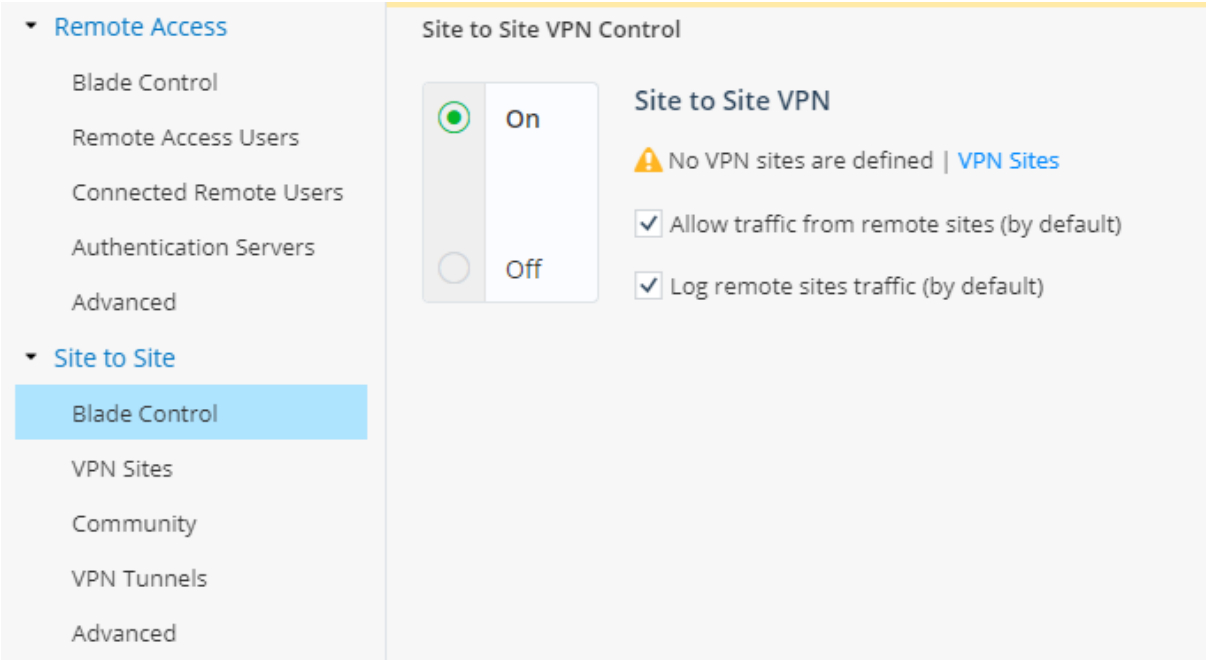



figure 4.6

## VPN Sites

- View **VPN -> Site To Site -> VPN Sites**
- Configure Remote VPN from this option

## Community

- View **VPN -> Site To Site -> Community**
- Get the community help from this Option.

## VPN Tunnels

- View **VPN -> Site To Site -> VPN Tunnels**
- From here we can configure VPN Tunnels

## Advanced

- View **VPN -> Site To Site -> Advanced**
- Configure additional advanced options for site to site VPN. Refer figure 4.7

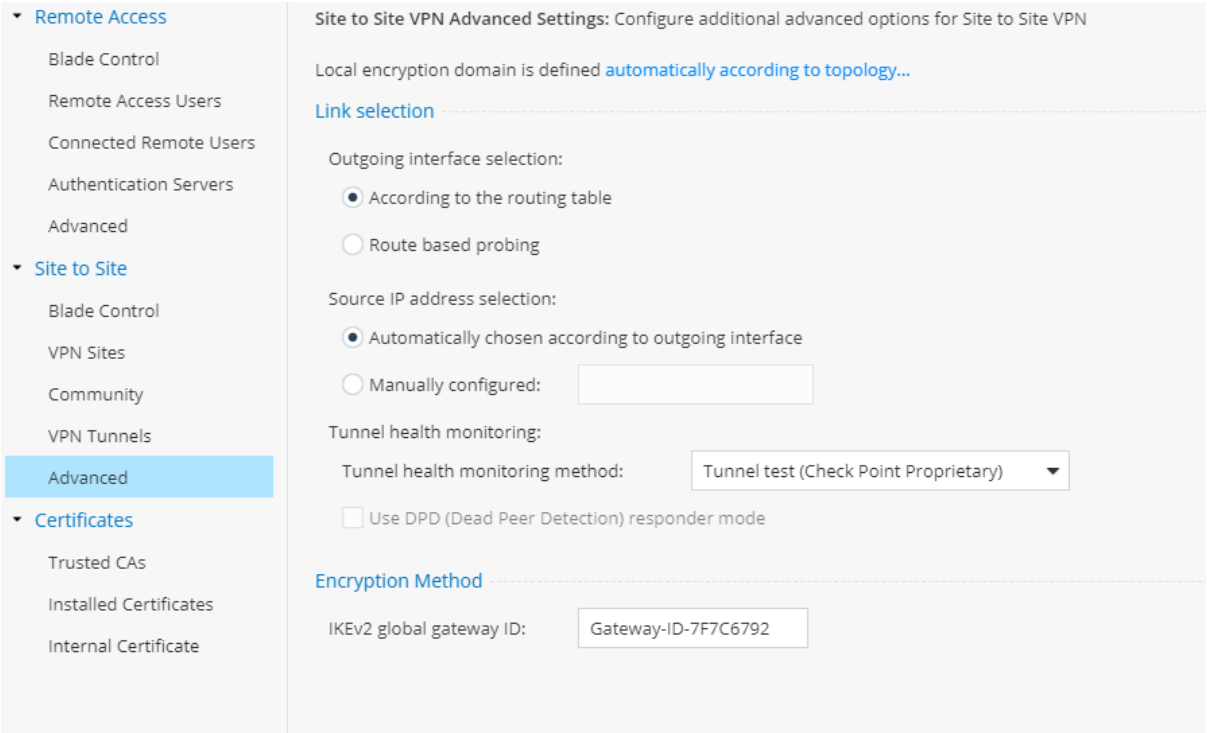



figure 4.7

## Certificates

### Trusted CAs

- View **VPN -> Certificates -> Trusted CAs**
- From these options manage trusted Certificates authorities. Refer figure 4.8

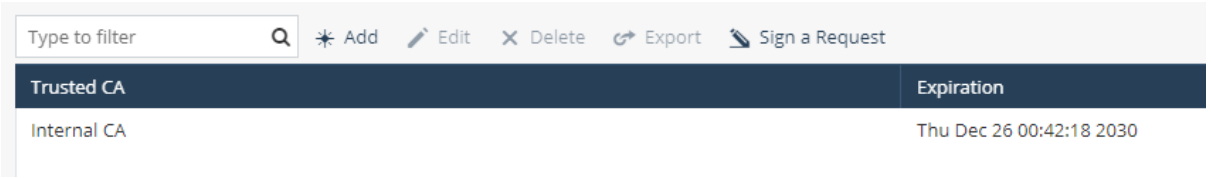



figure 4.8

### Installed Certificates

- View **VPN -> Certificates -> Installed Certificates**
- From this option Create & manage appliances. Refer figure 4.9

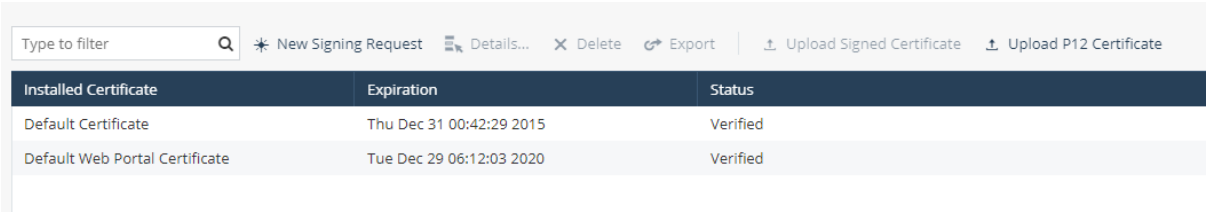



figure 4.9

### Internal Certificates

- View **VPN -> Certificates -> Internal Certificates**
- It Displays the appliances internal CA certificates and Internal Certificates And Internal VPN Certificates. Refer figure 5.0

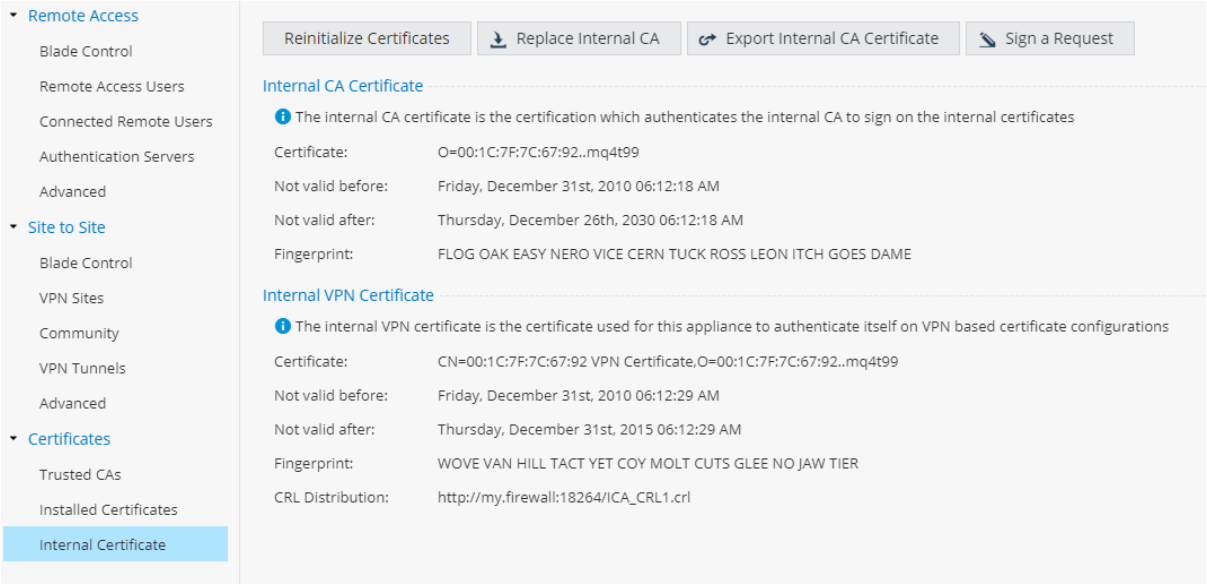



figure 5.0

# Users & Objects

## User Management

### User awareness

- View **Users & Objects -> User Management -> User Awareness**
- From here we can Turn on/off User awareness Blade and also we can configure active directory queries & Browser-Based authentication. Refer figure 5.1

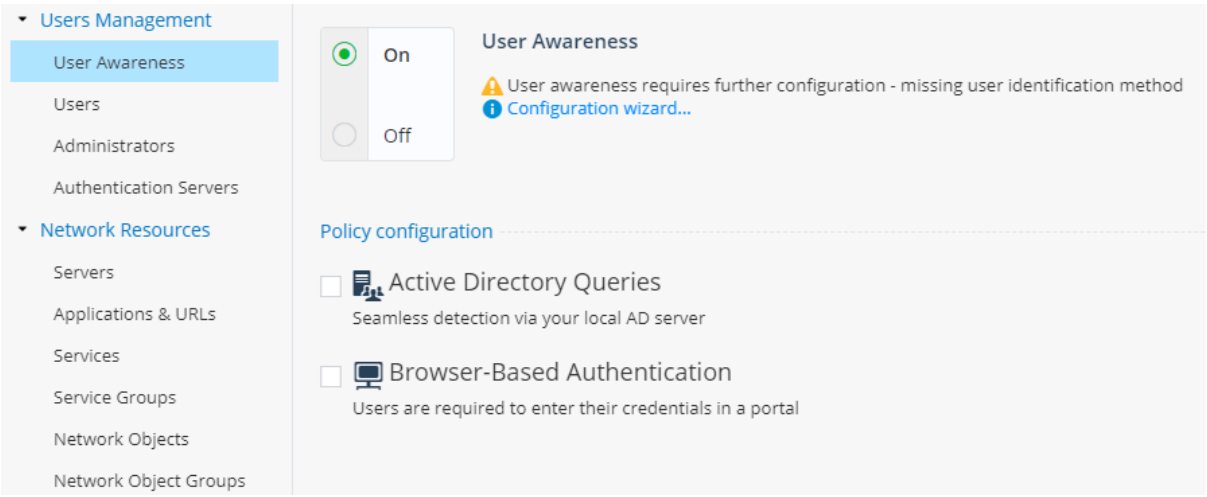



figure 5.1

## Users

- View **Users & Objects -> User Management -> Users**
- From this option we can add new users. Refer figure 5.2

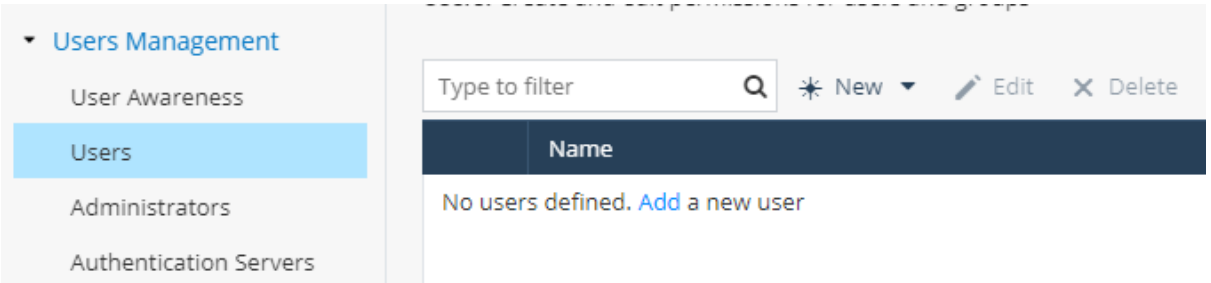



figure 5.2

## Administrator

- View **Users & Objects -> User Management -> Administrator**
- From this option we can configure or add administrator roles. Refer figure 5.3

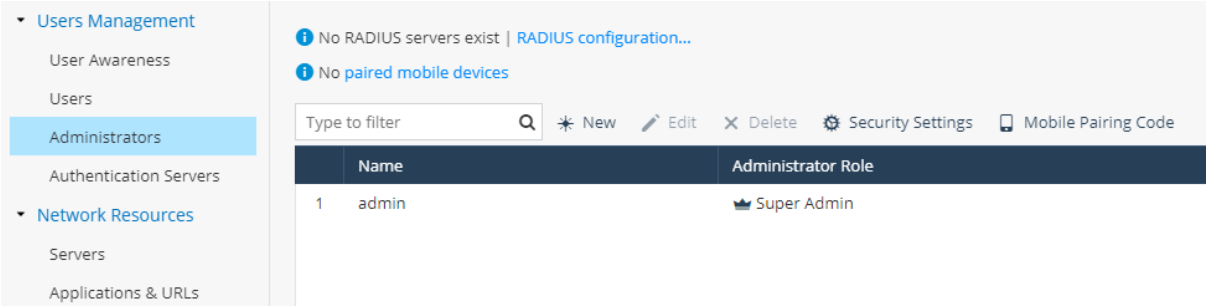



figure 5.3

## Authentication Servers

- View **Users & Objects -> User Management -> Authentication Servers**
- From this option we can configure RADIUS Servers & set users for RADIUS. Refer figure 5.4

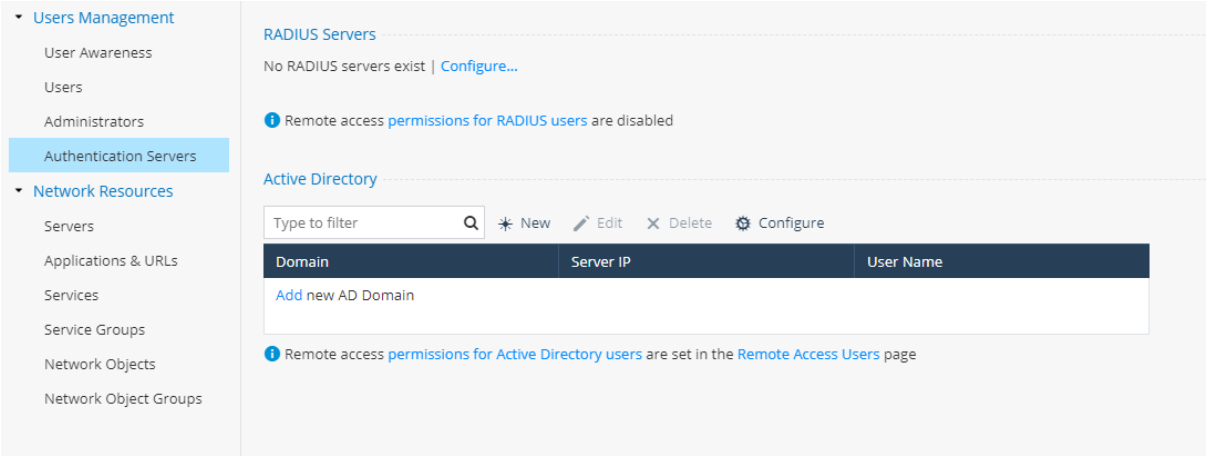



figure 5.4

## Network Resources

## Servers

- View **Users & Objects -> Network Resources -> Servers**
- From this option Servers Definition and Access permission and NAR for Server objects can be configured. Refer figure 5.5

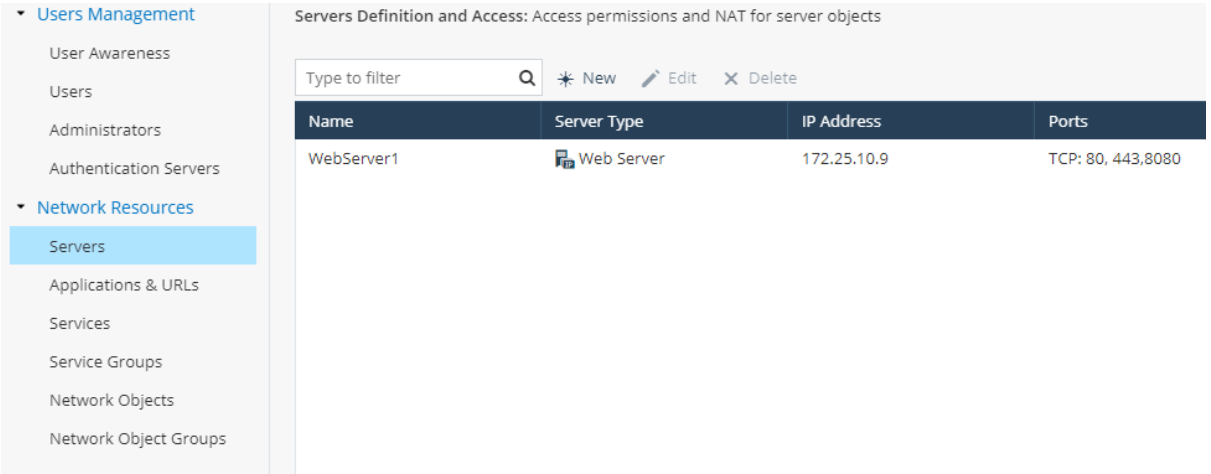



figure 5.5

## Applications & URLs

- View **Users & Objects -> Network Resources -> Application & URLs**
- It Defines custom application and application group. Refer figure 5.6

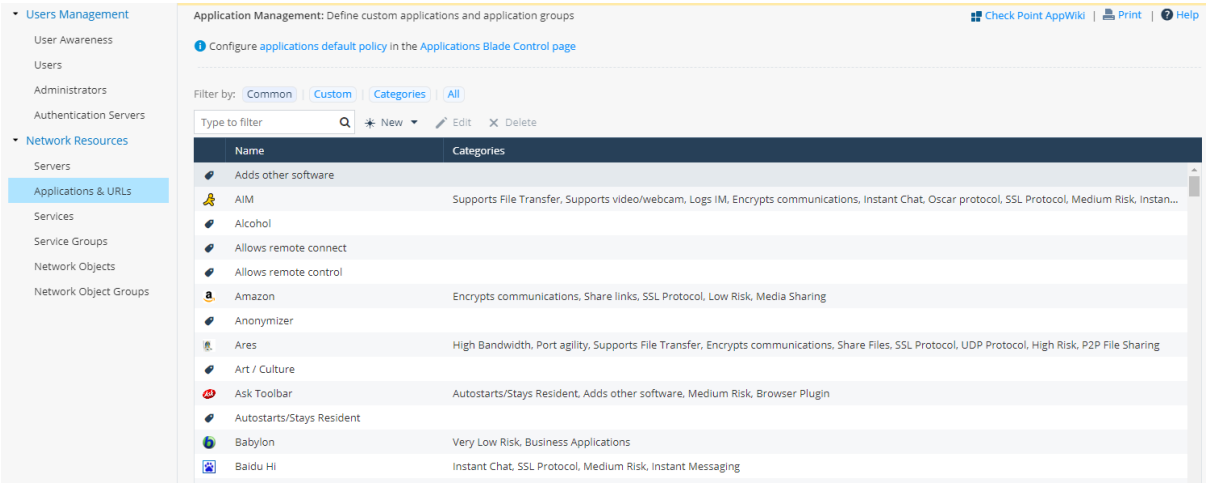



figure 5.6

## Services

- View **Users & Objects -> Network Resources -> Services**
- Change system service configuration & create/edit new service objects. Refer figure 5.7

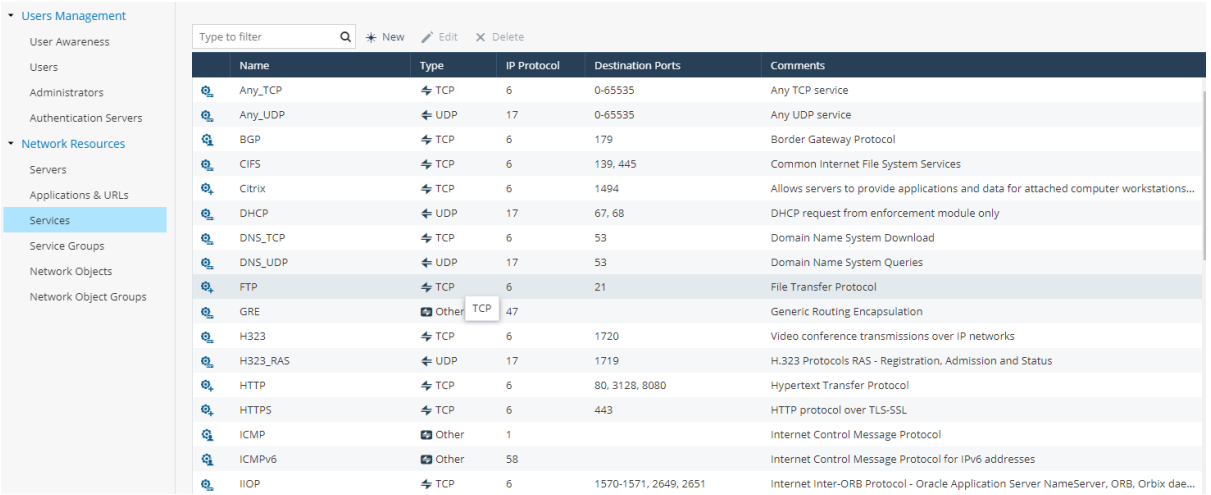



figure 5.7

## Service group

- View **Users & Objects -> Network Resources -> Service Group**
- Change system  service group configuration create/edit new services groups. Refer figure 5.8

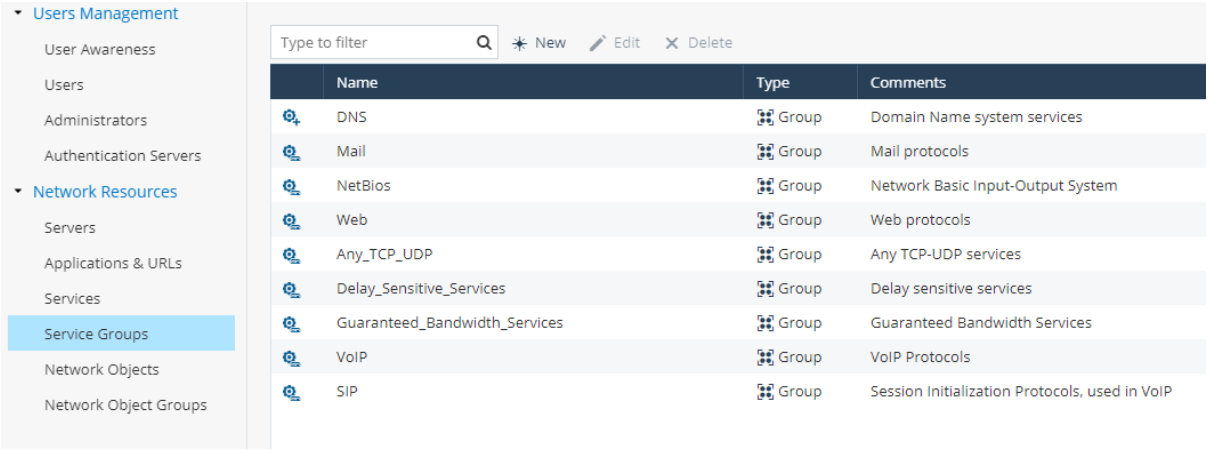



figure 5.8

## Network object

- View **Users & Objects -> Network Resources -> Network Object**
- From this option you can create/edit a new services group. Refer figure 5.9

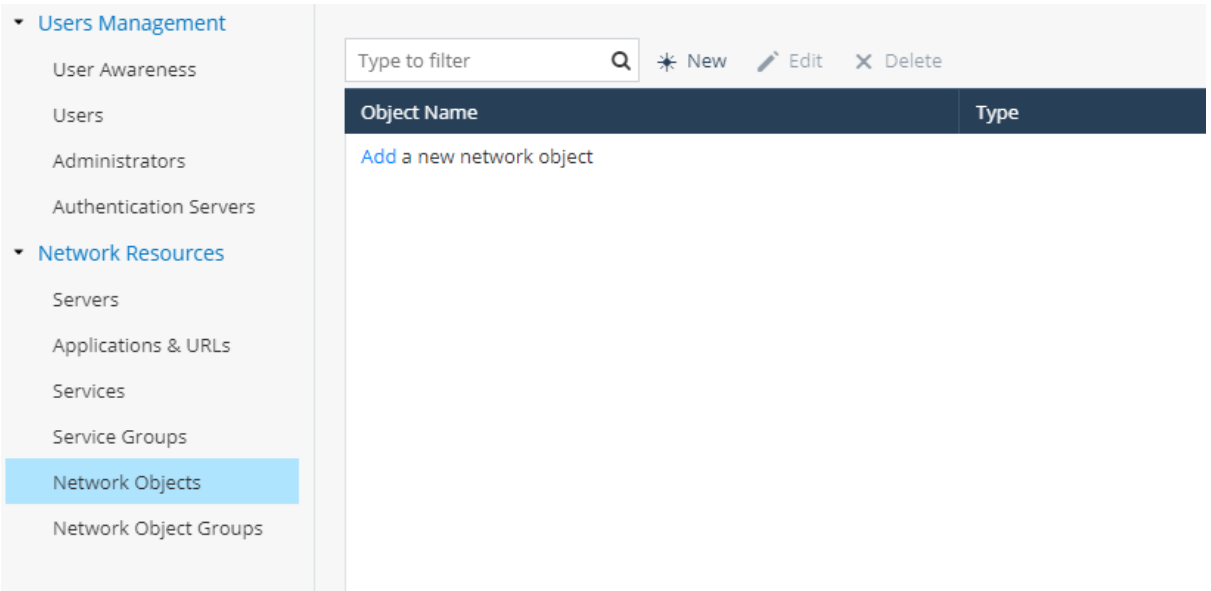



figure 5.9

### Network object groups

- View **Users & Objects -> Network Resources -> Network Object Groups**
- Create and edit network object groups that will be used in device & feature configuration. Refer figure 6.0

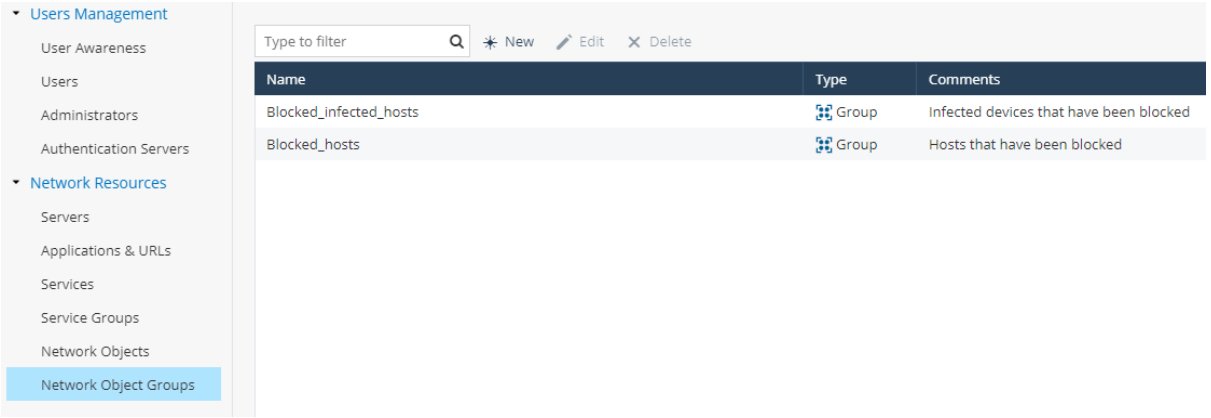



figure 6.0

## Logs & Monitoring

### Logs

### Security logs

- View **Logs & Monitoring -> Logs -> Security Logs**
- From this option you can Monitor Check point security logs created by appliances. Refer figure 6.1

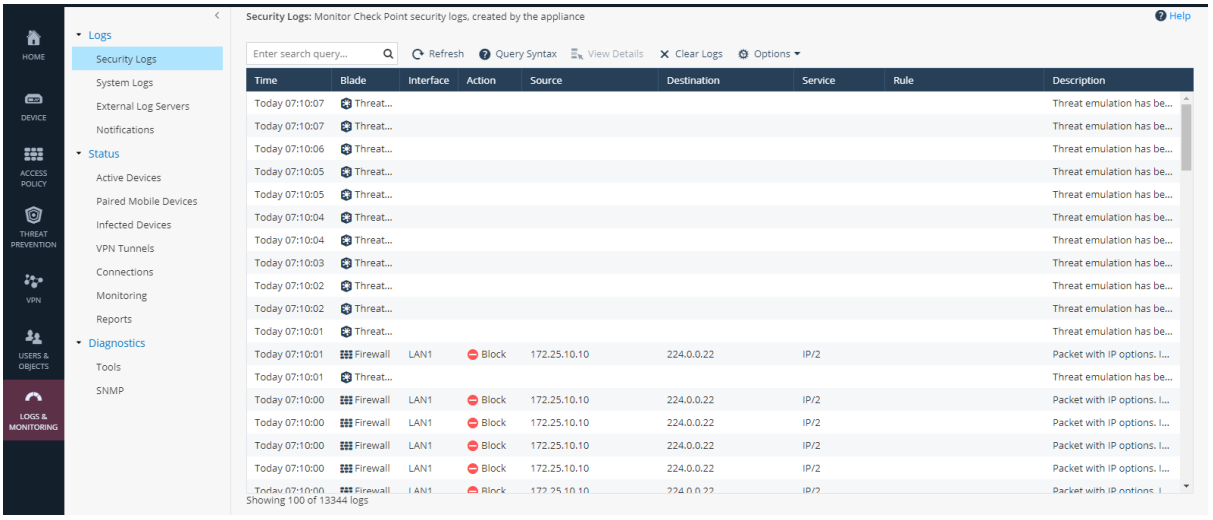



figure 6.1

## System logs

- View **Logs & Monitoring -> Logs -> System logs**
- From this option you can monitor check point system Logs created by appliances. Refer figure 6.2

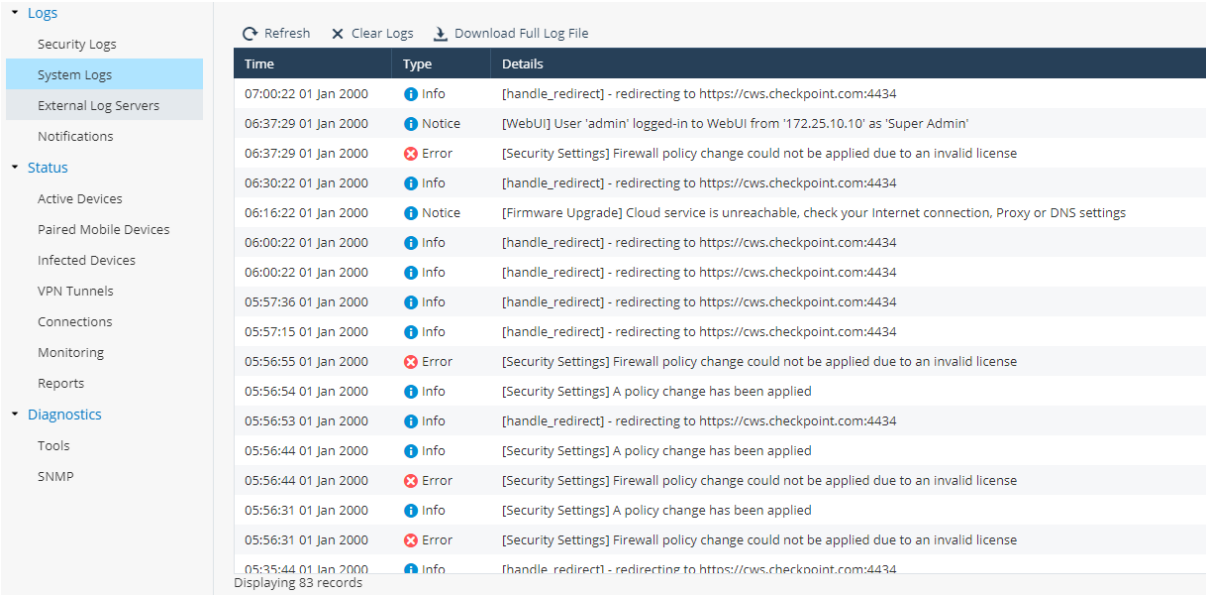



figure 6.2

## External Log Servers

- View **Logs & Monitoring -> Logs -> External Log Servers**
- From this option other logs can be monitored like check point log server, syslog server. Refer figure 6.3

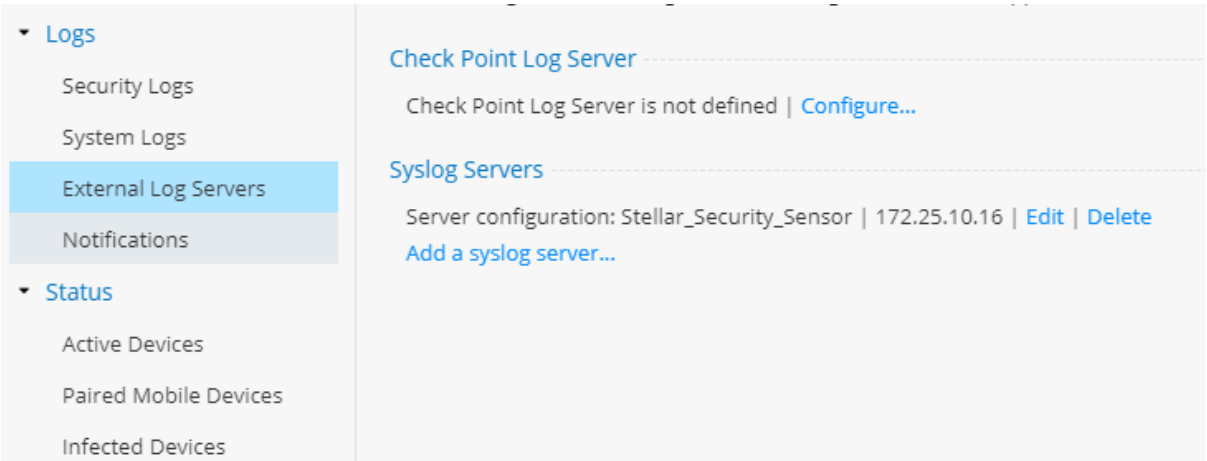



figure 6.3

## Notification

- View **Logs & Monitoring -> Logs -> Notification**
- From here all the logs notification can be monitored. Refer figure 6.4

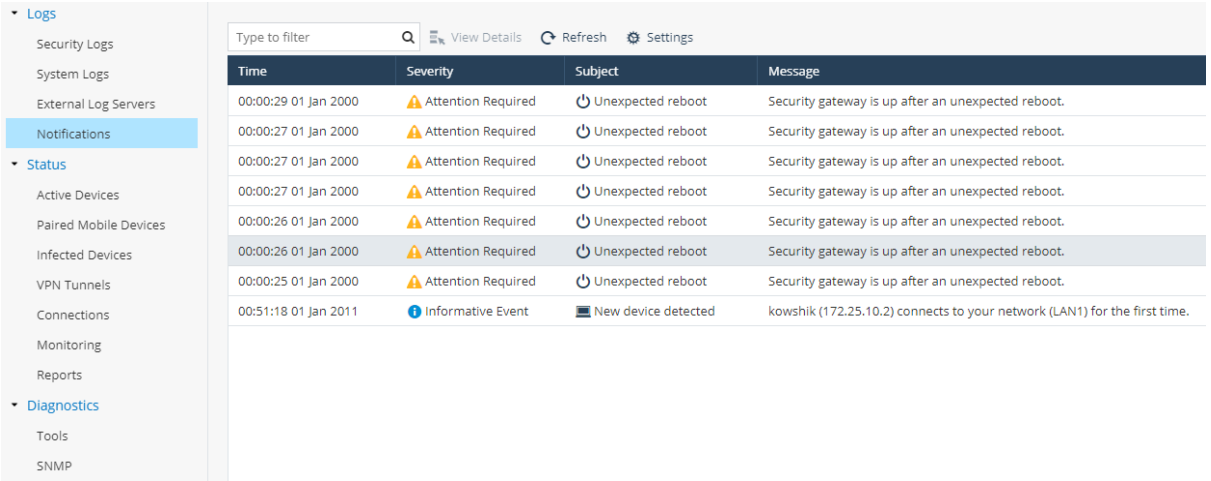



figure 6.4

## Status

### Active Devices

- View **Logs & Monitoring -> Status -> Active Device**
- From this option an active device can be displayed. Refer figure 6.5

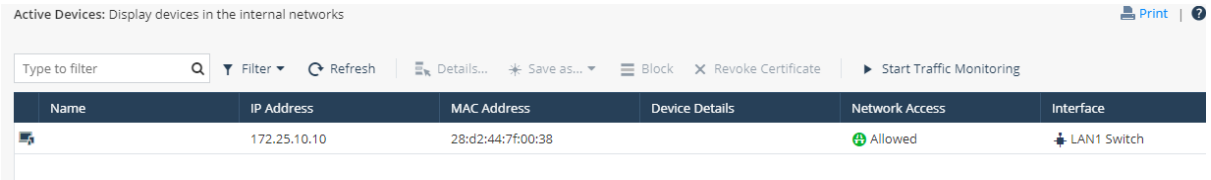



figure 6.5

## Paired Mobile Device

- View **Logs & Monitoring -> Status -> Paired Mobile Device**
- From this option we can see Paired mobile Device information. Refer figure 6.6

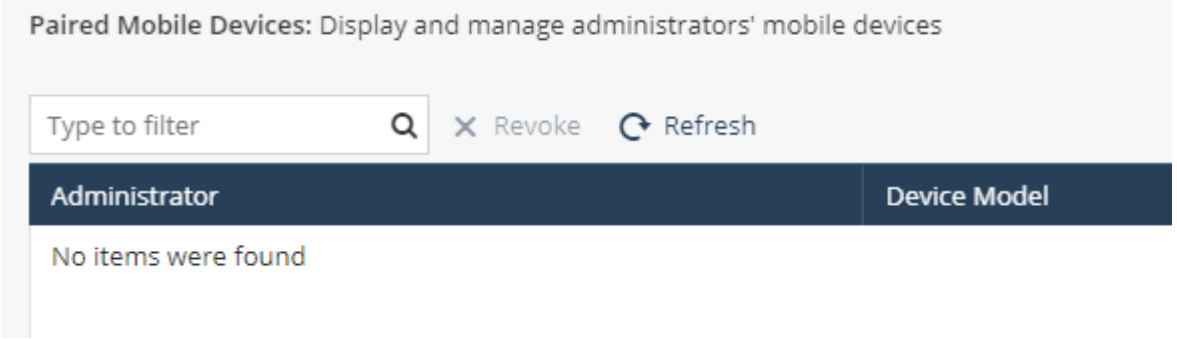



figure 6.6

## Infected Devices

- View **Logs & Monitoring -> Status -> Infected Devices**
- From here we can monitor Infected Devices & Take measures of remediation. Refer figure 6.7

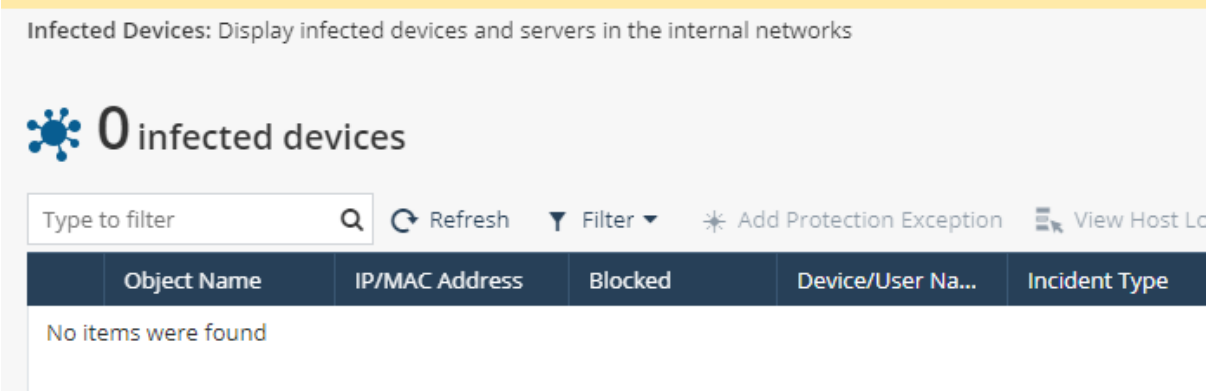



figure 6.7

## VPN Tunnels

- View **Logs & Monitoring -> Status -> VPN Tunnels**
- From this option we can Monitor all VPN Tunnels. Refer

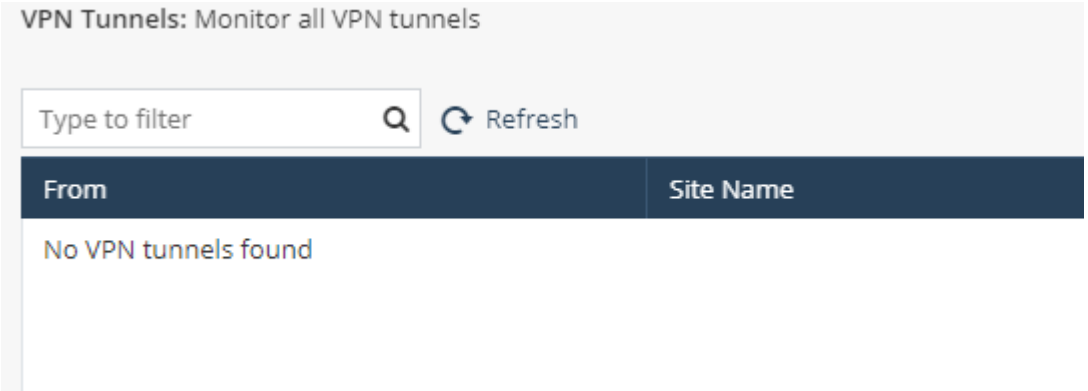
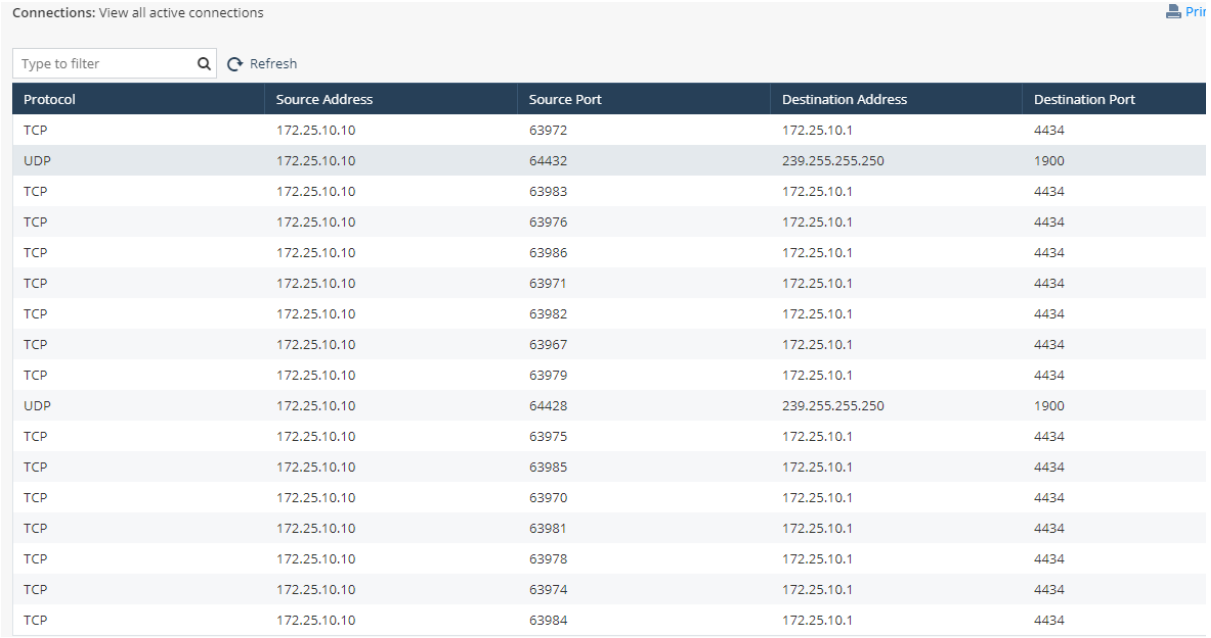



figure 6.8

## Connections

- View **Logs & Monitoring -> Status -> Connections**
- We can view all active connections from here. Refer figure 6.9




| Protocol | Source Address | Source Port | Destination Address | Destination Port |
|---|---|---|---|---|
| TCP | 172.25.10.10 | 63972 | 172.25.10.1 | 4434 |
| UDP | 172.25.10.10 | 64432 | 239.255.255.250 | 1900 |
| TCP | 172.25.10.10 | 63983 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63976 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63986 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63971 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63982 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63967 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63979 | 172.25.10.1 | 4434 |
| UDP | 172.25.10.10 | 64428 | 239.255.255.250 | 1900 |
| TCP | 172.25.10.10 | 63975 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63985 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63970 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63981 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63978 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63974 | 172.25.10.1 | 4434 |
| TCP | 172.25.10.10 | 63984 | 172.25.10.1 | 4434 |

figure 6.9

## Monitoring

- View **Logs & Monitoring -> Status -> Monitoring**
- We can monitor all the main things from here. Refer figure 7.0

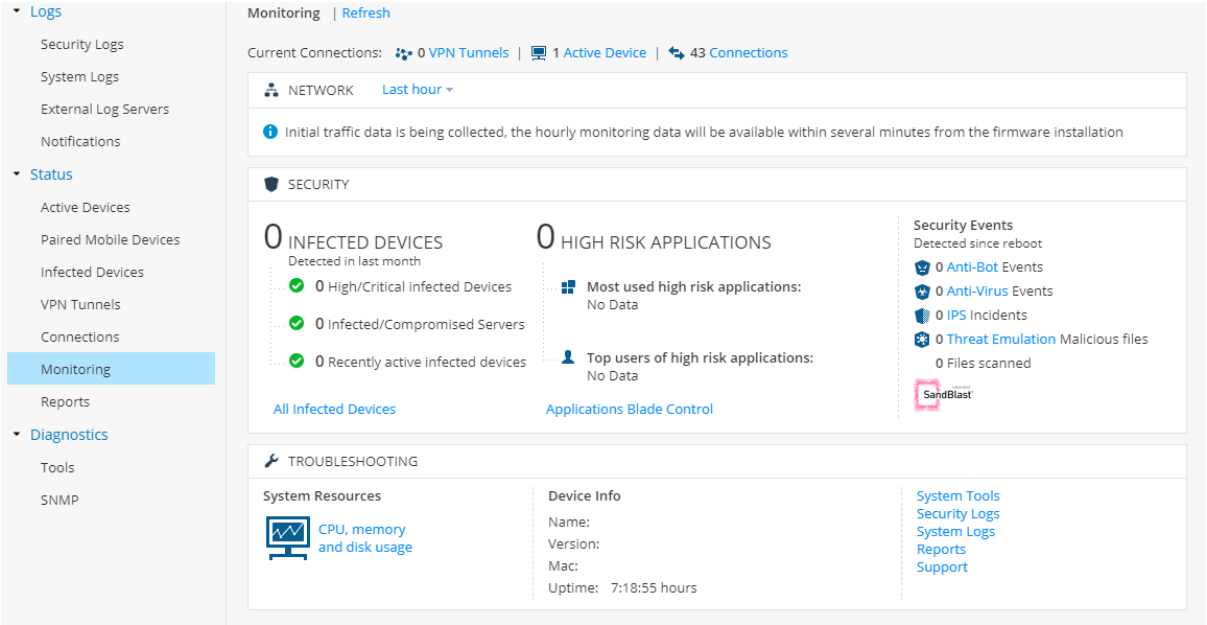



figure 7.0

## Reports

- View **Logs & Monitoring -> Status -> Reports**
- We can generate all the reports of monitoring devices.

## Diagnostic

## Tools

- View **Logs & Monitoring -> Diagnostic -> Tools**
- From here various tools used to diagnose problems with the appliances can be configured. Refer figure 7.1

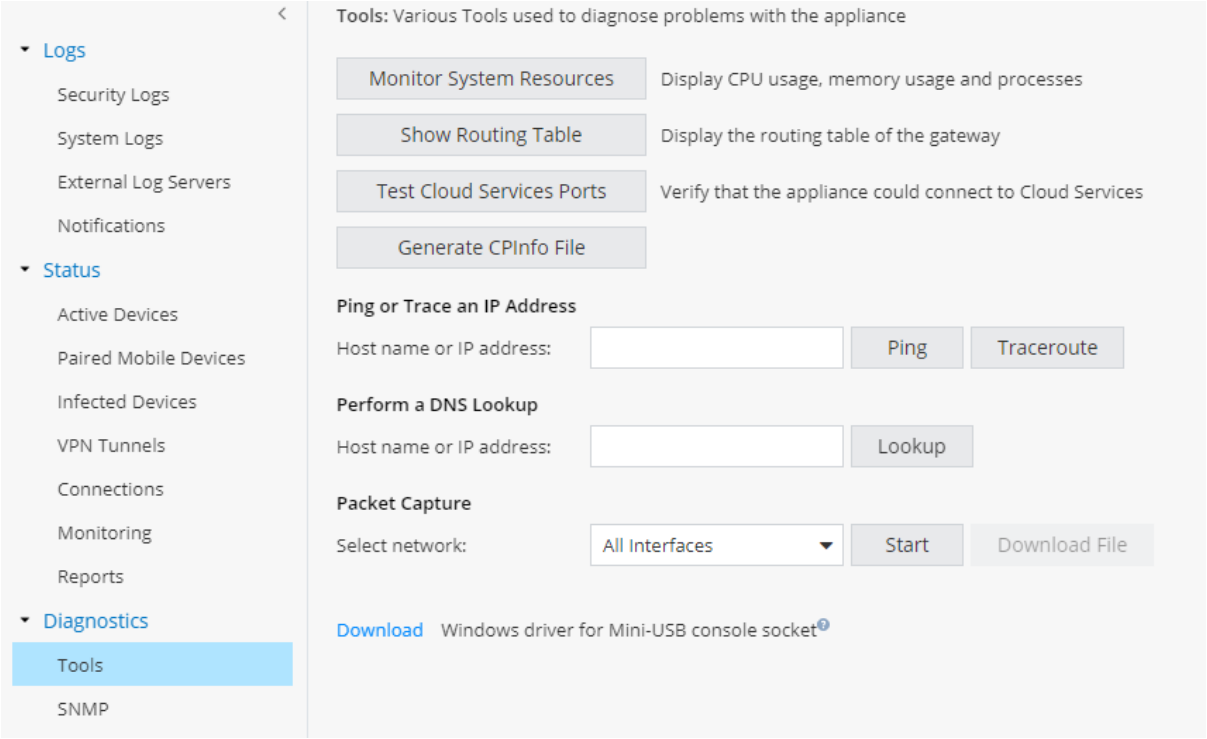



figure 7.1

## SNMP

- View **Logs & Monitoring -> Diagnostic -> SNMP**
- SNMP helps to monitor the device Status. Refer figure 7.2

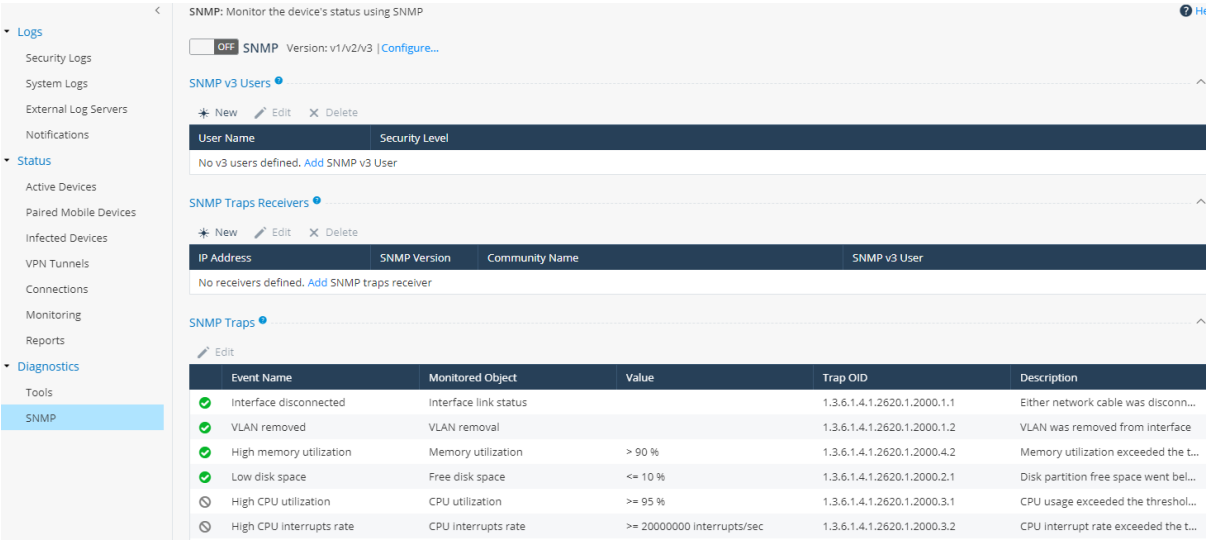



figure 7.2

These are the features and options of CHECK-POINT FIREWALL.

—----------EOD—----------