

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

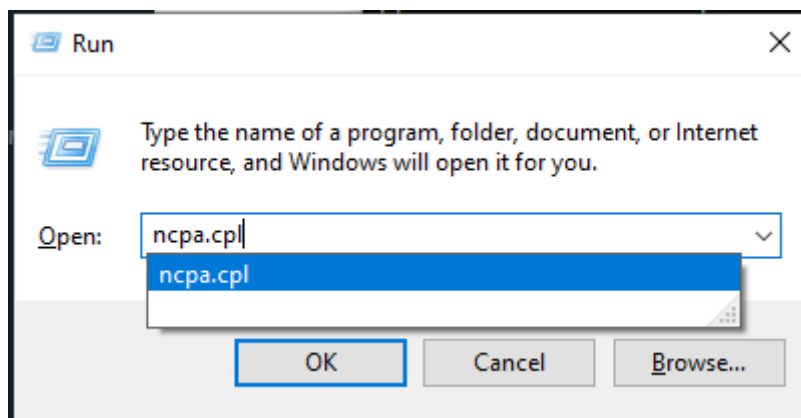


figure 1.1

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

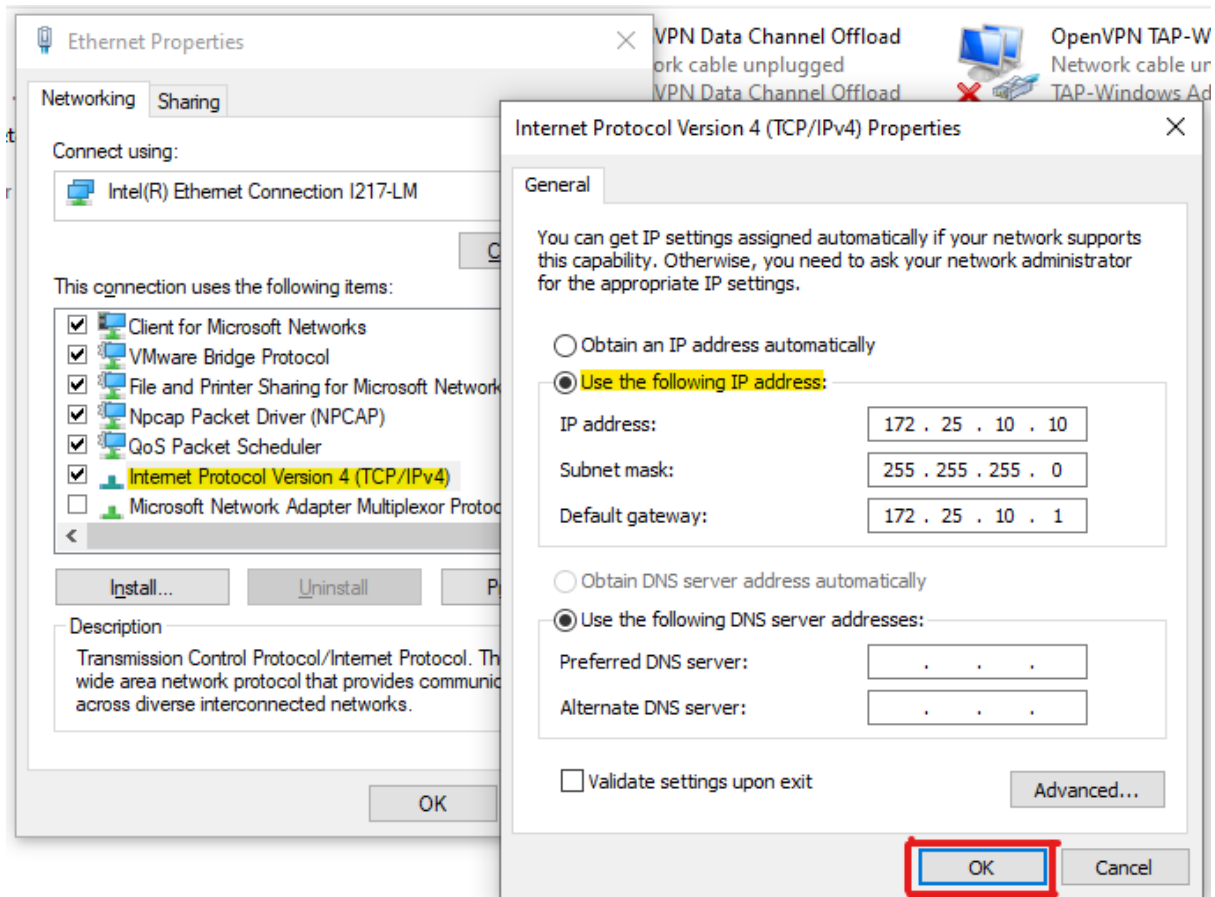


figure 1.2

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.

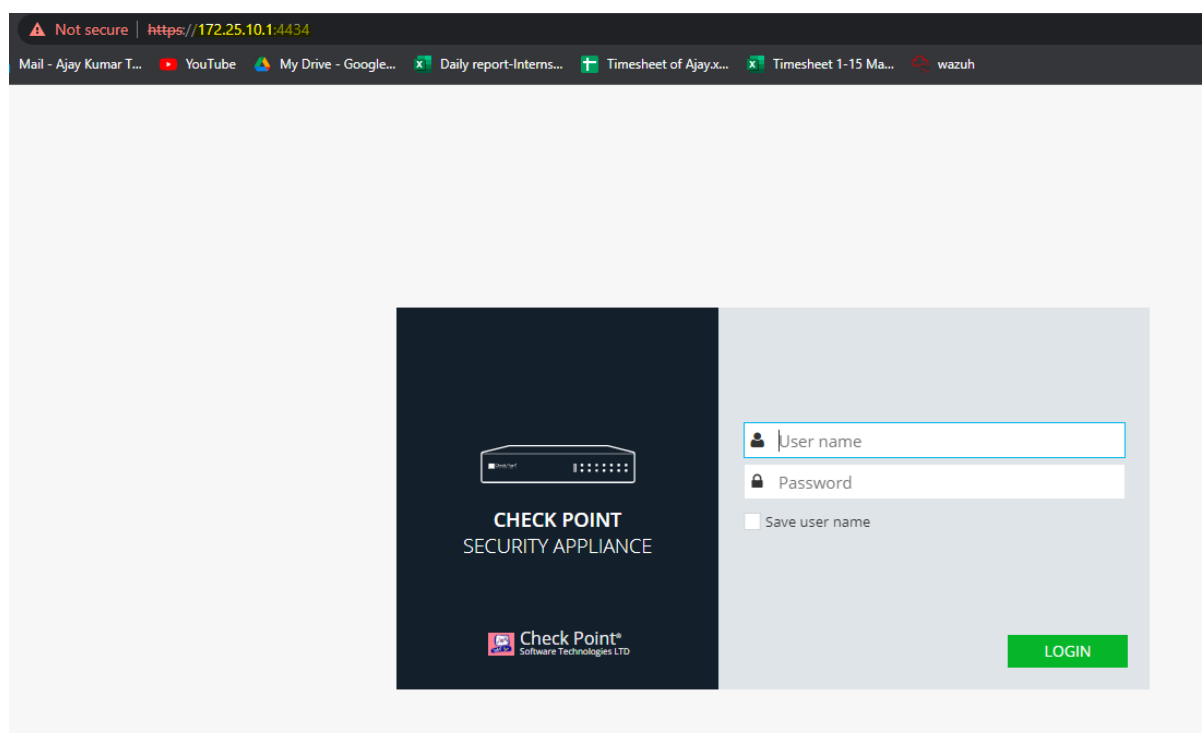


figure 1.3

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

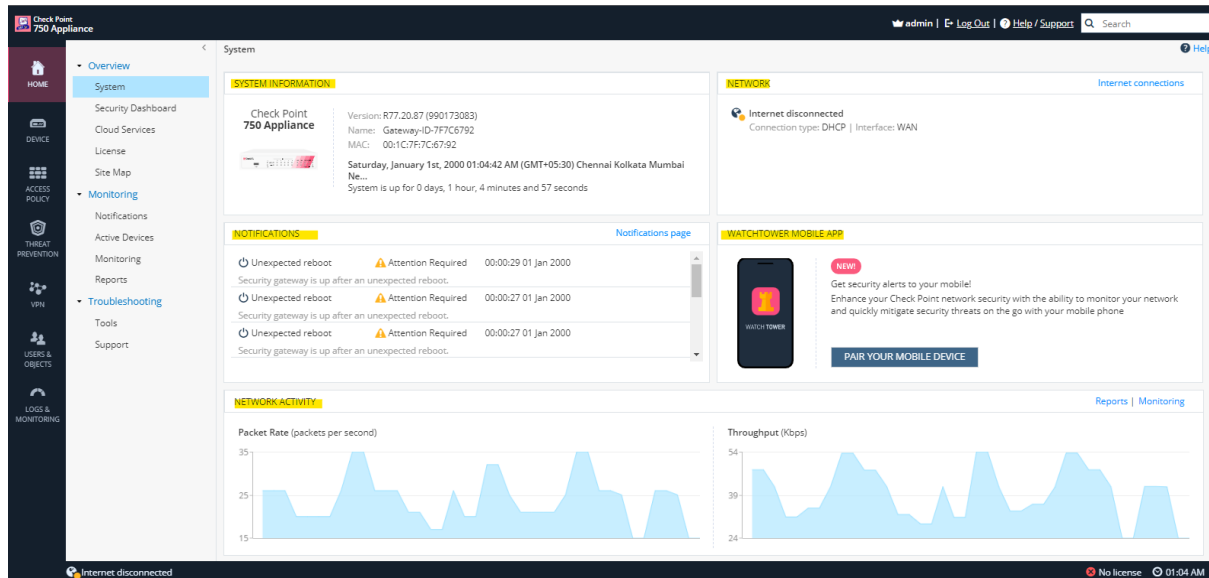


figure 1.4

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**

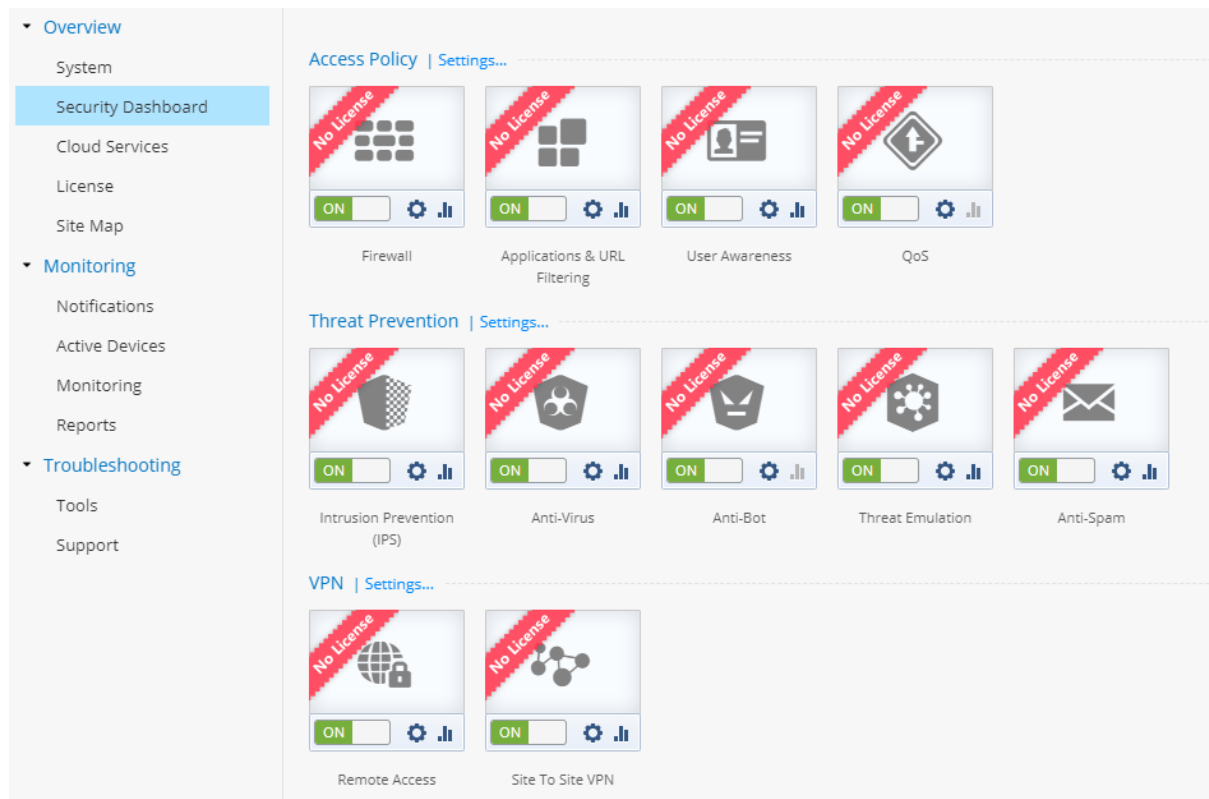


figure 1.5.1

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**

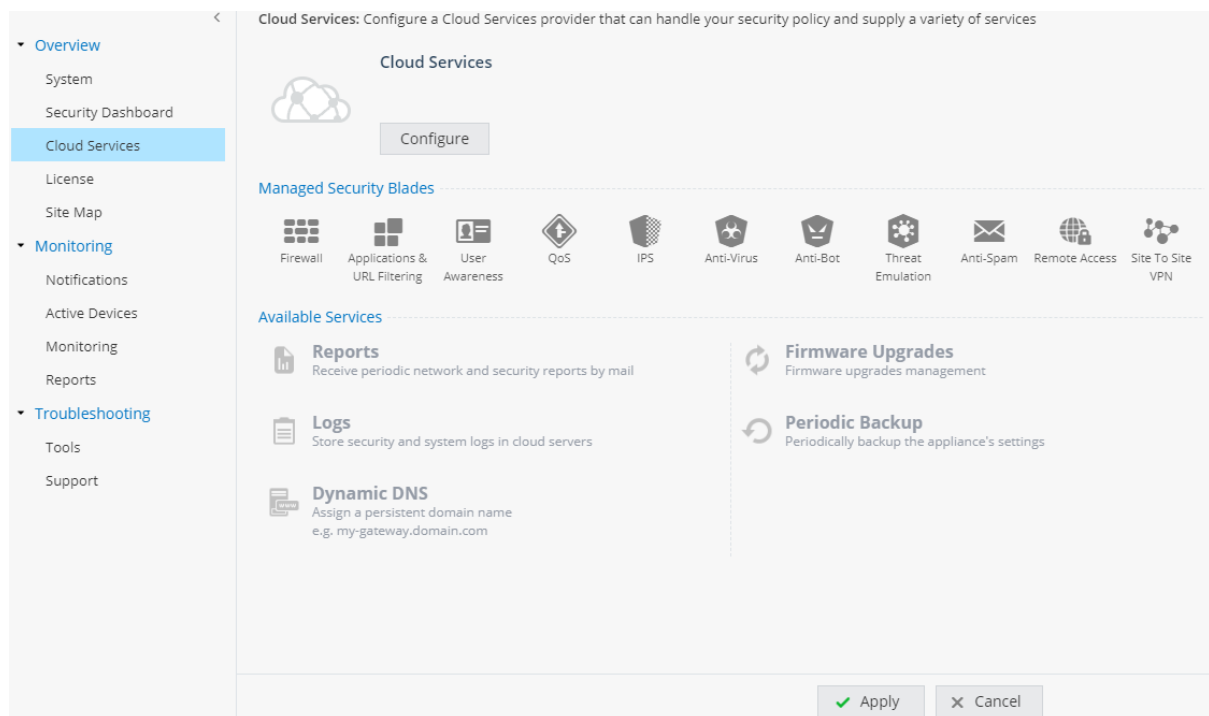


figure 1.5.2

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

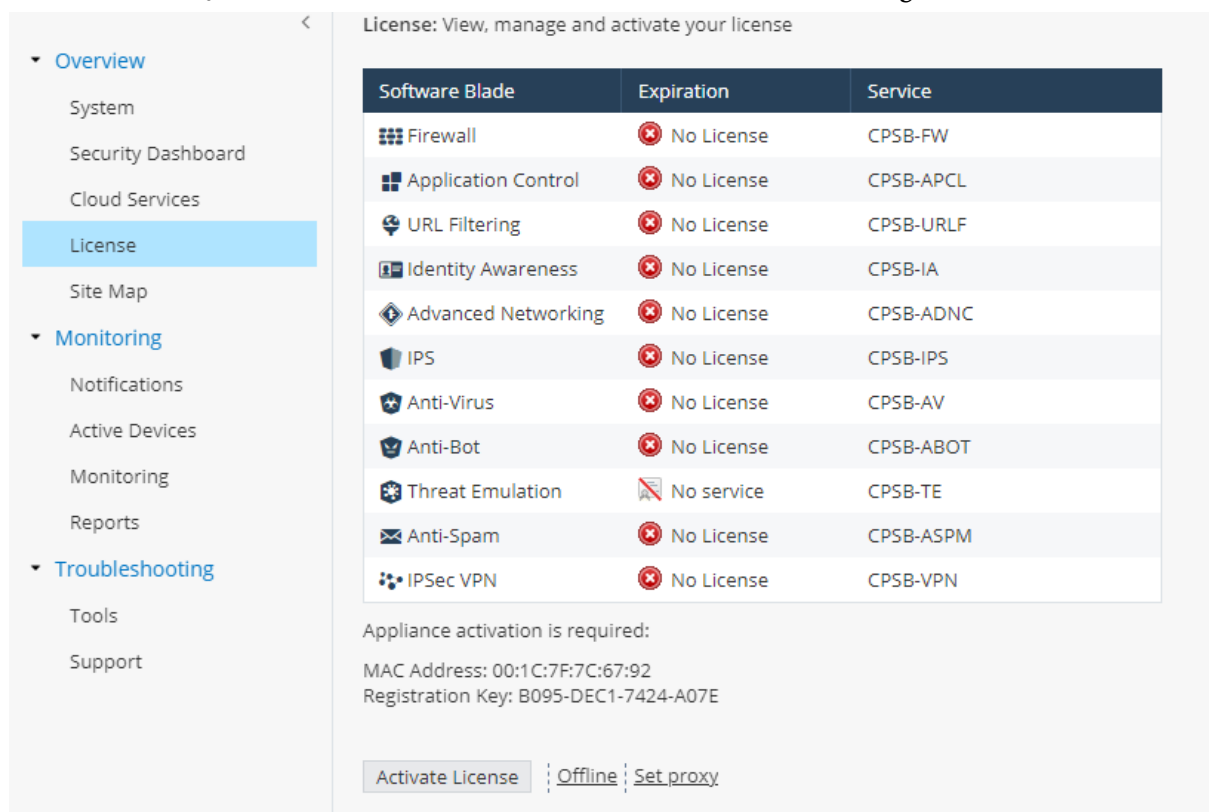


figure 1.6

Site map

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

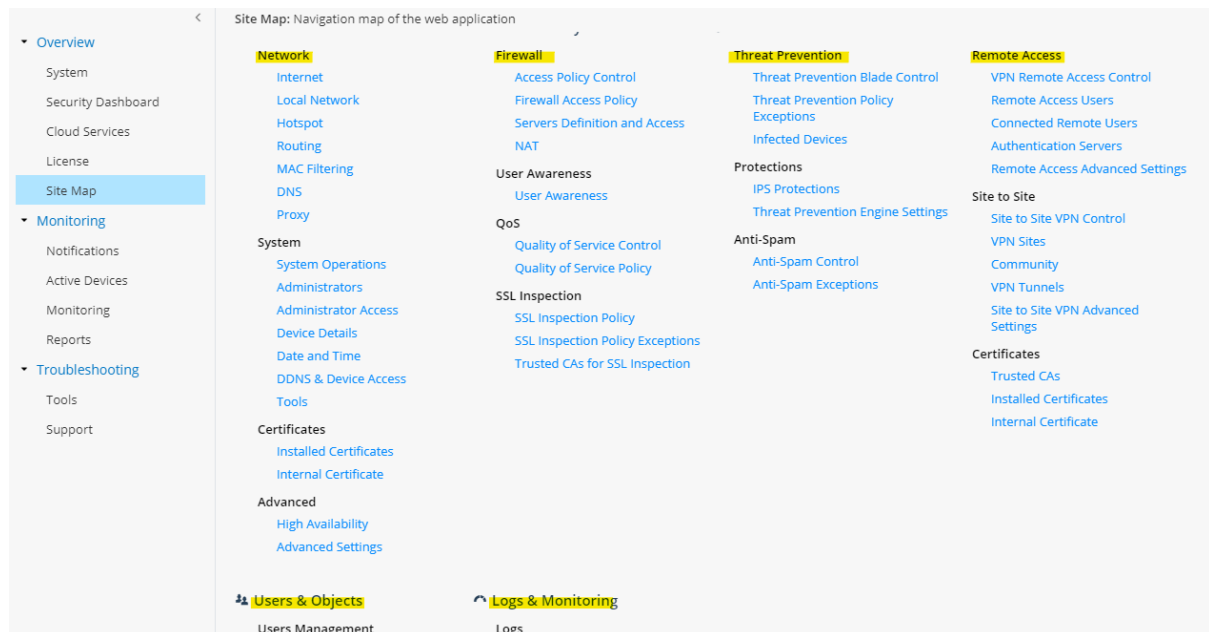


figure 1.7

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**

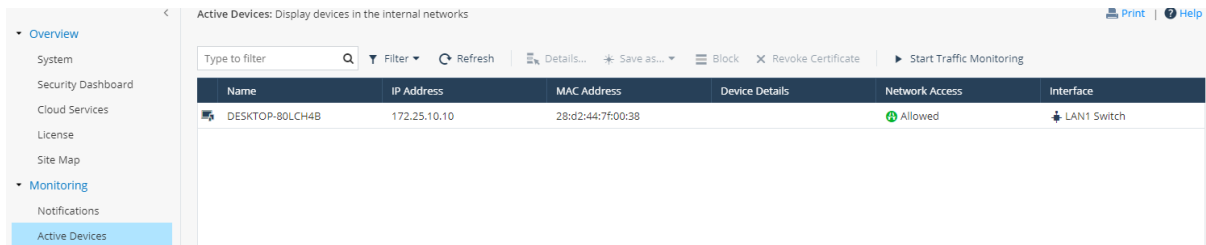
The screenshot shows the 'Notifications: System and security events' page. It features a table with columns for Time, Severity, Subject, and Message. The table lists several notifications, including 'Unexpected reboot' events and a 'New device detected' event.

Time	Severity	Subject	Message
00:00:29 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:27 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:27 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:27 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:26 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:26 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:25 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:51:18 01 Jan 2011	Informative Event	New device detected	kowshik (172.25.10.2) connects to your network (LAN1) for the first time.

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**

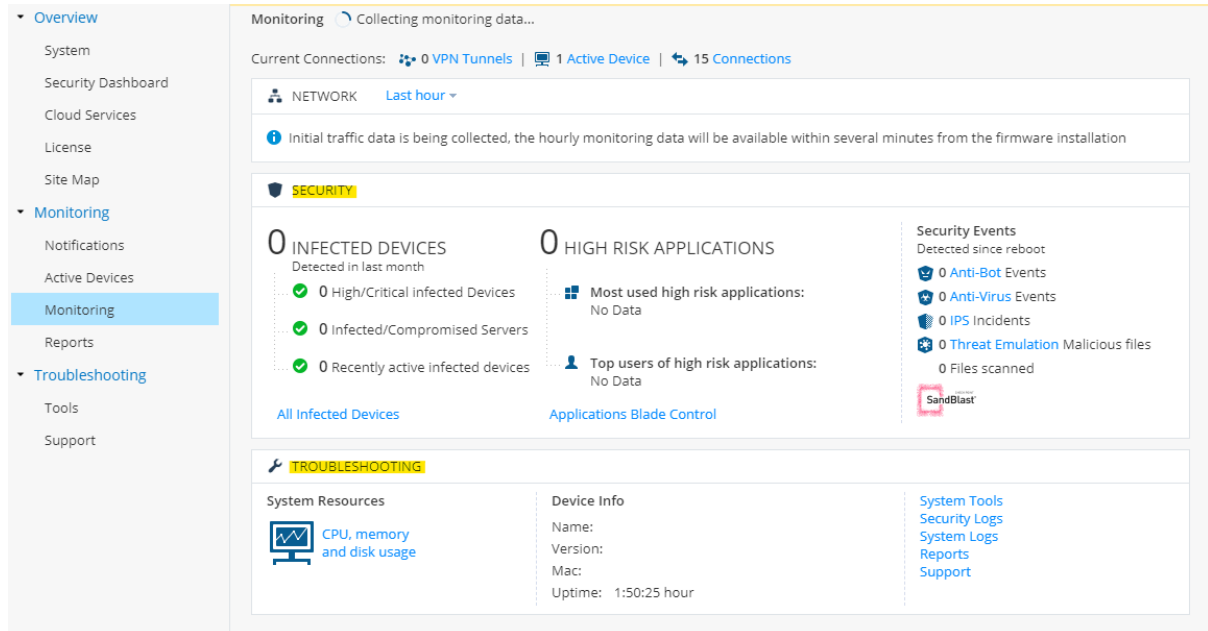


Name	IP Address	MAC Address	Device Details	Network Access	Interface
DESKTOP-80LCH4B	172.25.10.10	28:d2:44:7f:00:38		Allowed	LAN1 Switch

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**



Monitoring Collecting monitoring data...

Current Connections: 0 VPN Tunnels | 1 Active Device | 15 Connections

NETWORK Last hour

Initial traffic data is being collected, the hourly monitoring data will be available within several minutes from the firmware installation

SECURITY

0 INFECTED DEVICES
Detected in last month

- 0 High/Critical infected Devices
- 0 Infected/Compromised Servers
- 0 Recently active infected devices

All Infected Devices

0 HIGH RISK APPLICATIONS

Most used high risk applications: No Data

Top users of high risk applications: No Data

Applications Blade Control

Security Events
Detected since reboot

- 0 Anti-Bot Events
- 0 Anti-Virus Events
- 0 IPS Incidents
- 0 Threat Emulation Malicious files

0 Files scanned

SandBlast

TROUBLESHOOTING

System Resources

CPU, memory and disk usage

Device Info

Name:
Version:
Mac:
Uptime: 1:50:25 hour

System Tools
Security Logs
System Logs
Reports
Support

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.

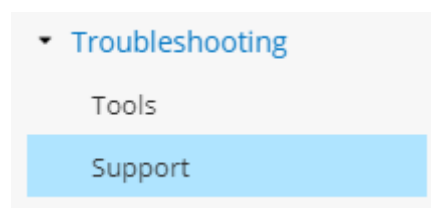


figure 2.1

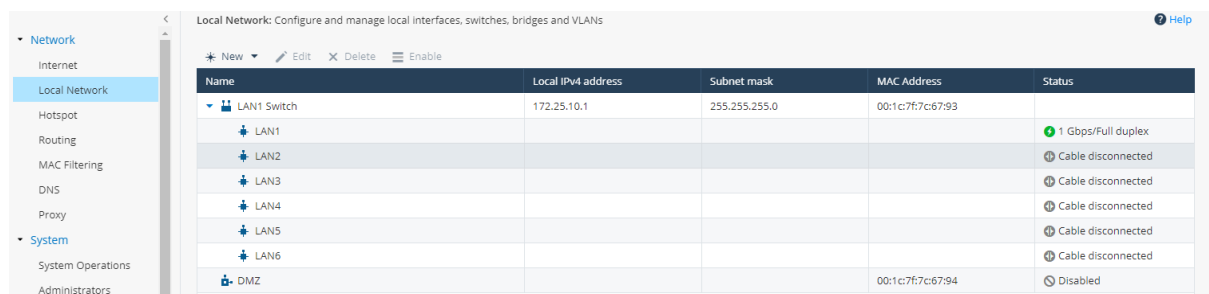
Device

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

A screenshot of a web interface for 'Local Network' configuration. The page title is 'Local Network: Configure and manage local interfaces, switches, bridges and VLANs'. On the left is a sidebar with a tree view containing 'Network' (expanded), 'Internet', 'Local Network' (selected), 'Hotspot', 'Routing', 'MAC Filtering', 'DNS', 'Proxy', 'System' (expanded), 'System Operations', and 'Administrators'. The main content area has a table with columns: Name, Local IPv4 address, Subnet mask, MAC Address, and Status. The table lists a 'LAN1 Switch' with IP 172.25.10.1 and subnet 255.255.255.0, and six LAN ports (LAN1-LAN6) with MAC addresses and status 'Cable disconnected'. A 'DMZ' entry is also listed with status 'Disabled'.

Name	Local IPv4 address	Subnet mask	MAC Address	Status
LAN1 Switch	172.25.10.1	255.255.255.0	00:1c:7f:7c:67:93	
LAN1				1 Gbps/Full duplex
LAN2				Cable disconnected
LAN3				Cable disconnected
LAN4				Cable disconnected
LAN5				Cable disconnected
LAN6				Cable disconnected
DMZ			00:1c:7f:7c:67:94	Disabled

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

DNS: Configure DNS and Domain settings for the device

IPv4 DNS

IPv4 DNS Servers

⚠ DNS is not configured. Anti-Virus, URL Filtering and Anti-Spam features will not function properly.

☐ Configure DNS servers
These settings will be applied on all Internet connections

First DNS server:

Second DNS server:

Third DNS server:

☒ Use DNS servers configured for the active Internet connection(s)

Connection Name	First DNS Server	Second DNS Server	Third DNS Server
No items were found			

IPv4 DNS Proxy

☒ Enable DNS proxy
Relay DNS requests from internal network clients to the DNS servers defined above

☒ Resolve [Network Objects](#)
Use network objects as a hosts list to translate names to their IP addresses

Domain Name

Domain name:

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

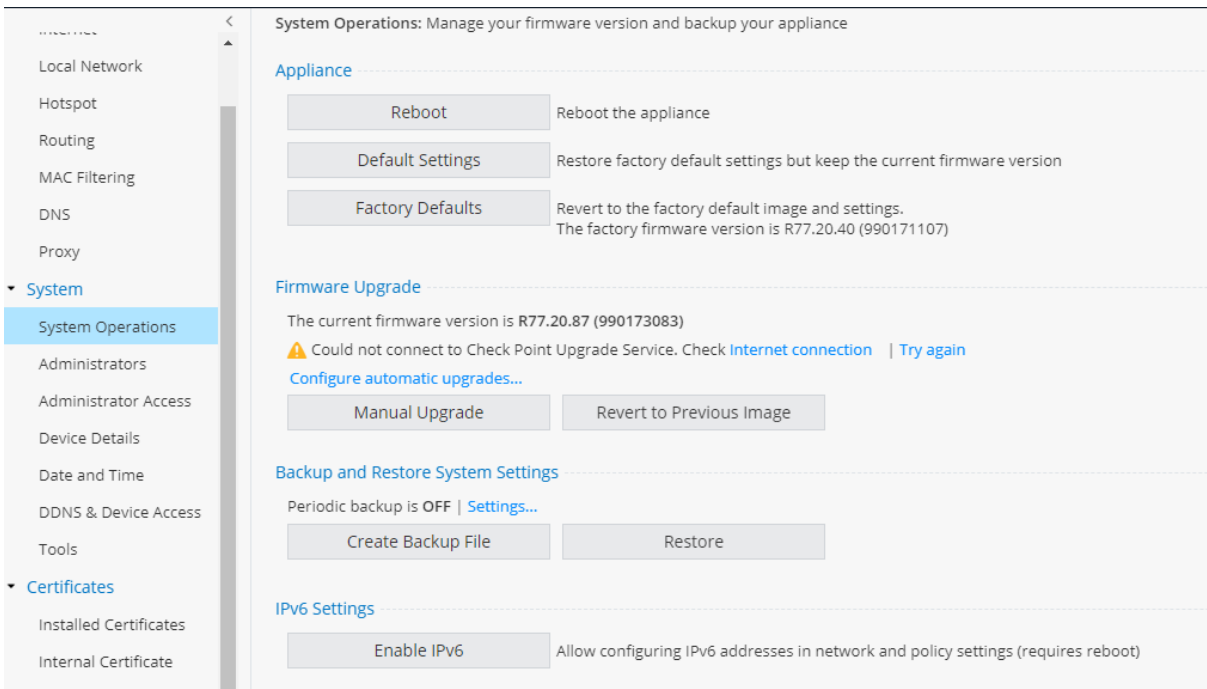


figure 2.3

Administrator

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

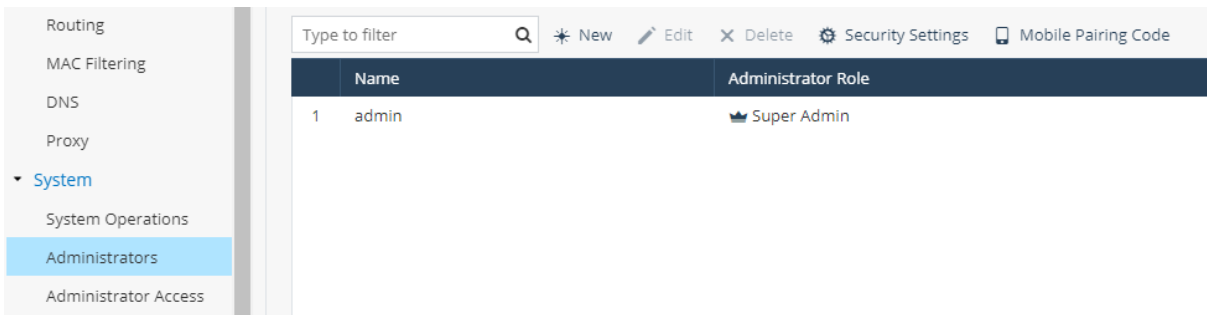
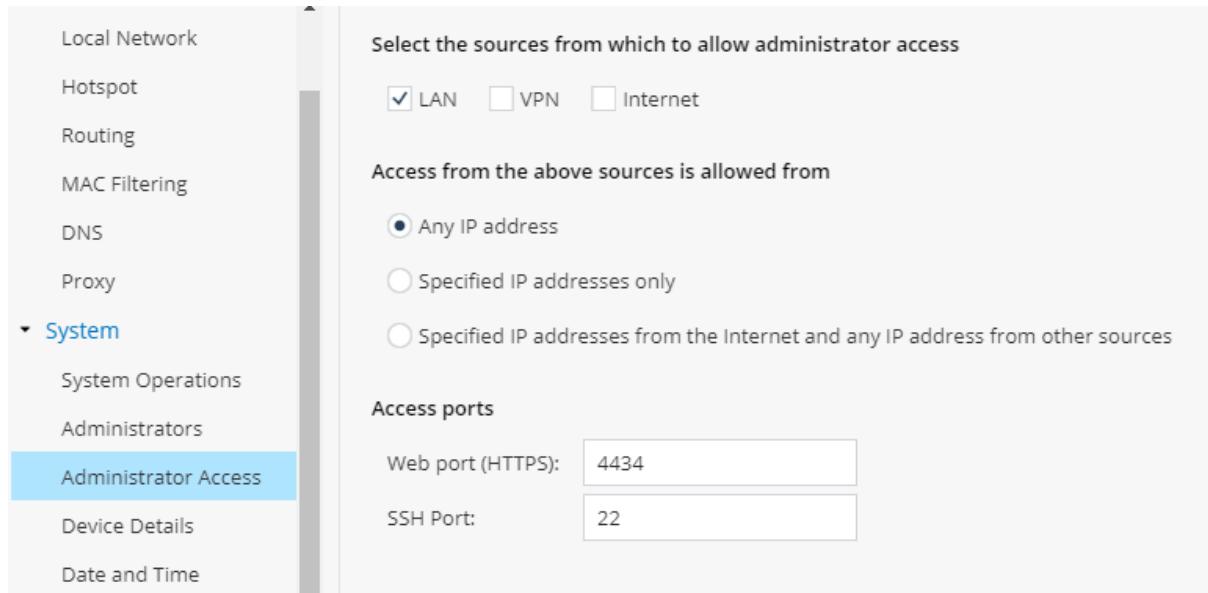


figure 2.3

Administrator access

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



The screenshot shows a web interface for configuring administrator access. On the left is a sidebar menu with the following items: Local Network, Hotspot, Routing, MAC Filtering, DNS, Proxy, System (expanded), System Operations, Administrators, Administrator Access (highlighted), Device Details, and Date and Time. The main content area is titled 'Select the sources from which to allow administrator access'. It contains three checkboxes: LAN (checked), VPN (unchecked), and Internet (unchecked). Below this, a section titled 'Access from the above sources is allowed from' has three radio button options: 'Any IP address' (selected), 'Specified IP addresses only', and 'Specified IP addresses from the Internet and any IP address from other sources'. At the bottom, the 'Access ports' section has two input fields: 'Web port (HTTPS):' with the value '4434' and 'SSH Port:' with the value '22'.

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

The screenshot shows a 'Tools' section with the following elements:

- Monitor System Resources**: Display CPU usage, memory usage and processes
- Show Routing Table**: Display the routing table of the gateway
- Test Cloud Services Ports**: Verify that the appliance could connect to Cloud Services
- Generate CPInfo File**
- Ping or Trace an IP Address**: Includes a text input for 'Host name or IP address:' and buttons for 'Ping' and 'Traceroute'.
- Perform a DNS Lookup**: Includes a text input for 'Host name or IP address:' and a 'Lookup' button.
- Packet Capture**: Includes a dropdown for 'Select network:' (currently showing 'All Interfaces'), a 'Start' button, and a 'Download File' button.
- [Download](#) Windows driver for Mini-USB console socket

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

[Reinitialize Certificates](#) [Replace Internal CA](#) [Export Internal CA Certificate](#) [Sign a Request](#)

Internal CA Certificate

i The internal CA certificate is the certification which authenticates the internal CA to sign on the internal certificates

Certificate: O=00:1C:7F:7C:67:92..mq4t99

Not valid before: Friday, December 31st, 2010 06:12:18 AM

Not valid after: Thursday, December 26th, 2030 06:12:18 AM

Fingerprint: FLOG OAK EASY NERO VICE CERN TUCK ROSS LEON ITCH GOES DAME

Internal VPN Certificate

i The internal VPN certificate is the certificate used for this appliance to authenticate itself on VPN based certificate configurations

Certificate: CN=00:1C:7F:7C:67:92 VPN Certificate,O=00:1C:7F:7C:67:92..mq4t99

Not valid before: Friday, December 31st, 2010 06:12:29 AM

Not valid after: Thursday, December 31st, 2015 06:12:29 AM

Fingerprint: WOVE VAN HILL TACT YET COY MOLT CUTS GLEE NO JAW TIER

CRL Distribution: http://my.firewall:18264/ICA_CRL1.crl

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

⚠ Changing these advanced settings can be harmful to the stability, security and performance of the appliance

Type to filter [Edit](#) [Restore Defaults](#)

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

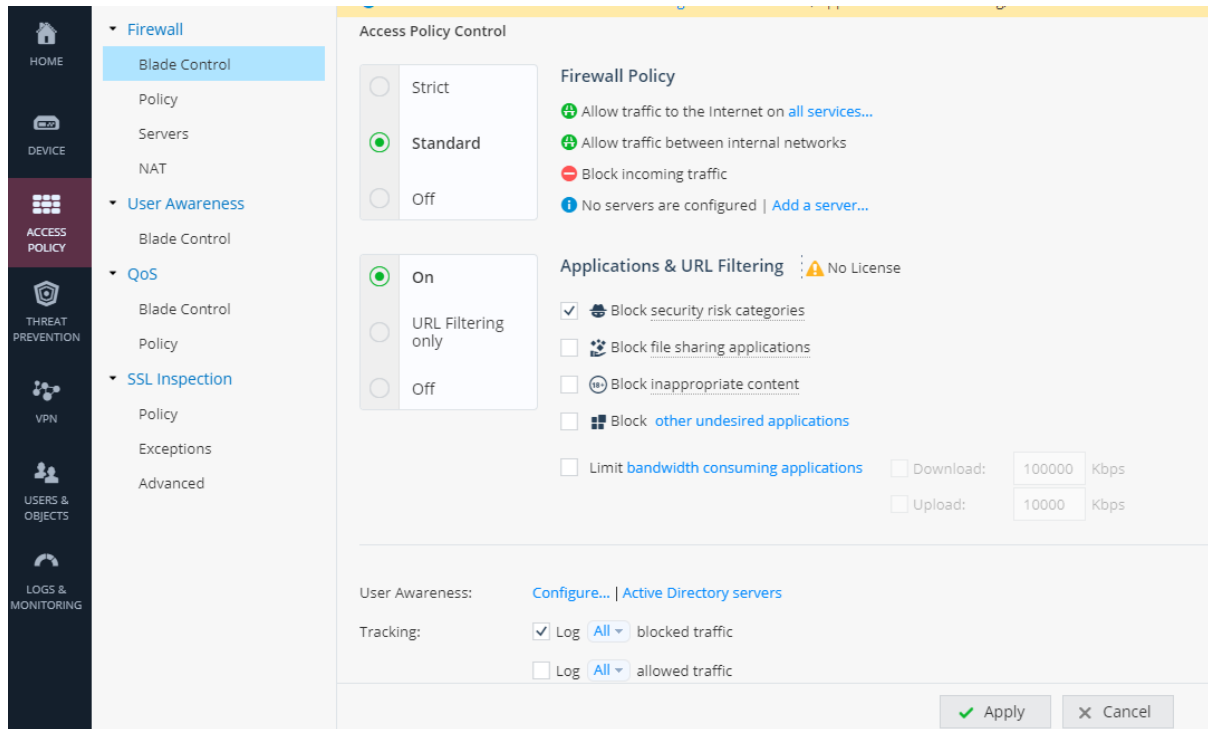


figure 2.7

Policy

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

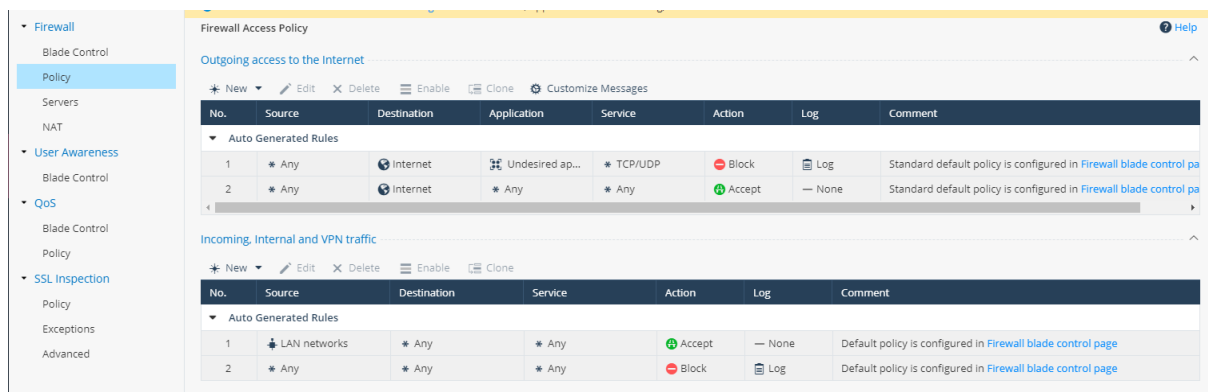
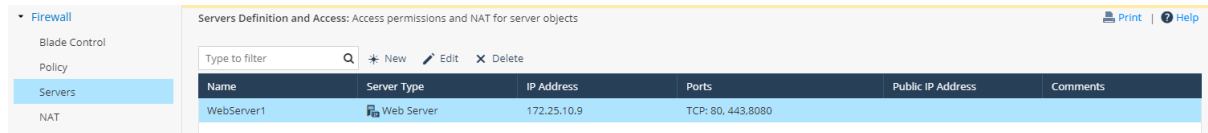


figure 2.8

Servers

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

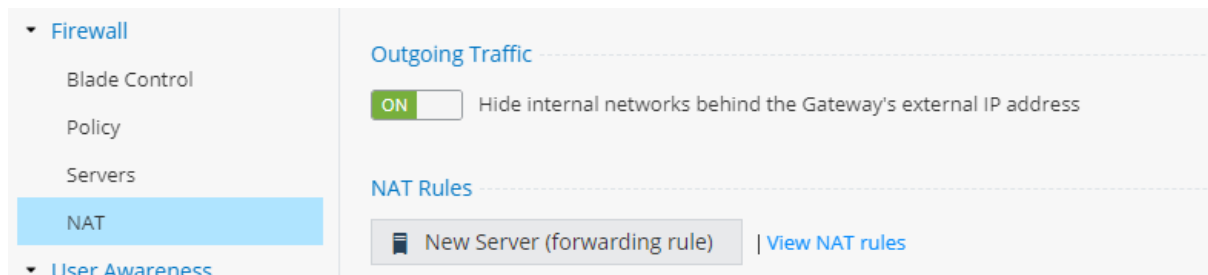


Name	Server Type	IP Address	Ports	Public IP Address	Comments
WebServer1	Web Server	172.25.10.9	TCP: 80, 443, 8080		

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



Outgoing Traffic

☒ ON Hide internal networks behind the Gateway's external IP address

NAT Rules

[New Server \(forwarding rule\)](#) | [View NAT rules](#)

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

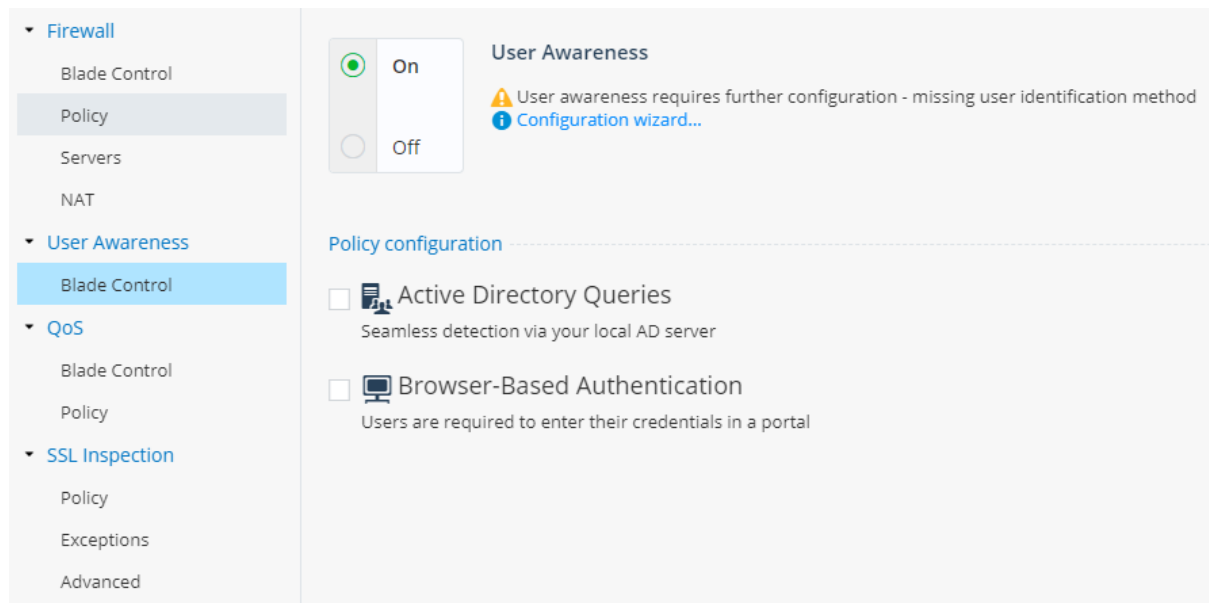


figure 3.1

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

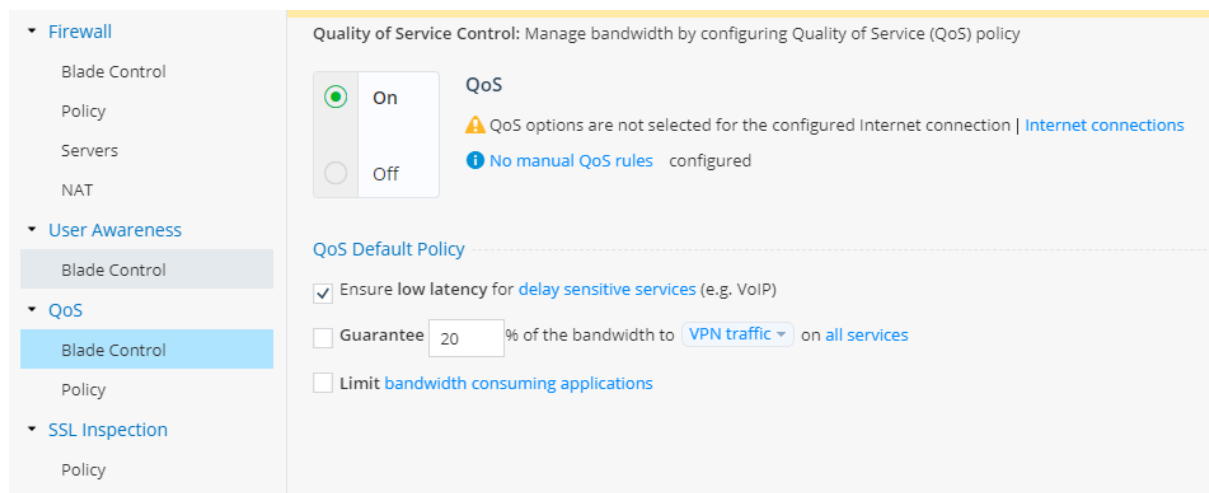


figure 3.2

Policy

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

No.	Source	Destination	Service	Guarantee/Limit	Weight	Track	Comment
1	* Any	* Any	Delay sensitiv...	Latency: low	10	— None	Note: Ensure low latency for Delay Sensitive Services (e.g. VoIP)
2	* Any	* Any	* Any (encrypted)	20% / -	10	— None	Note: Guarantee bandwidth for all services
3	* Any	* Any	* Any	- / -	10	— None	Note: Default QoS policy

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

☐ SSL traffic inspection

☒ **HTTPS Categorization**

☐ Off

SSL Inspection

Allow URL filtering for HTTPS sites and applications based on server's certificate, without activating SSL traffic inspection

Protocols to inspect

☒ HTTPS

☐ IMAPS

Bypass SSL inspection for the following categories:

Categories to bypass:

☒ Health ☐ Media Streams

☒ Government/Military ☒ Well known update services | More info

☒ Financial Services ☒ Bypass other categories and sites...

Tracking

☐ Enable inspect logs

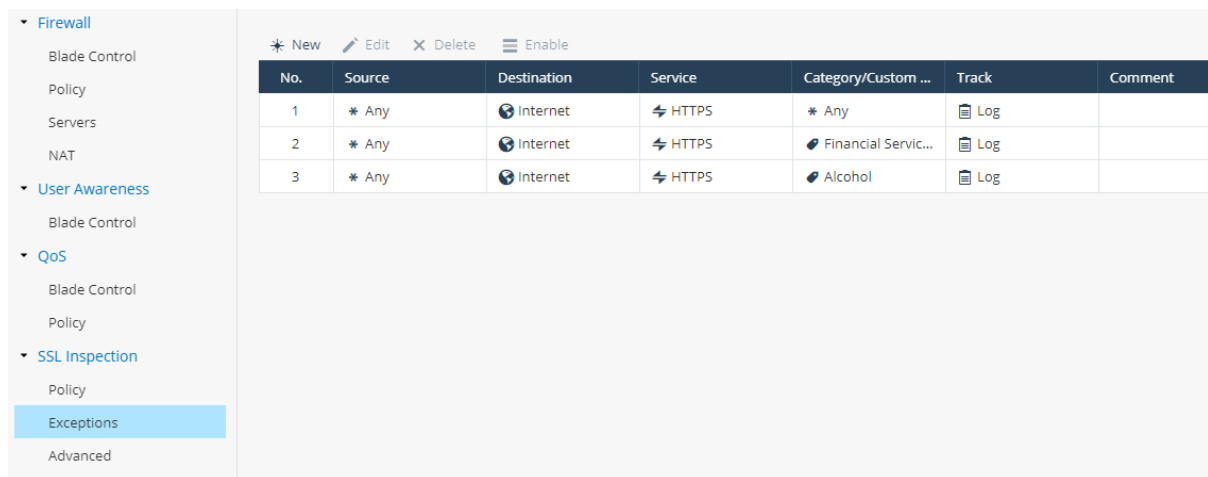
☐ Enable bypass logs

Apply Cancel

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

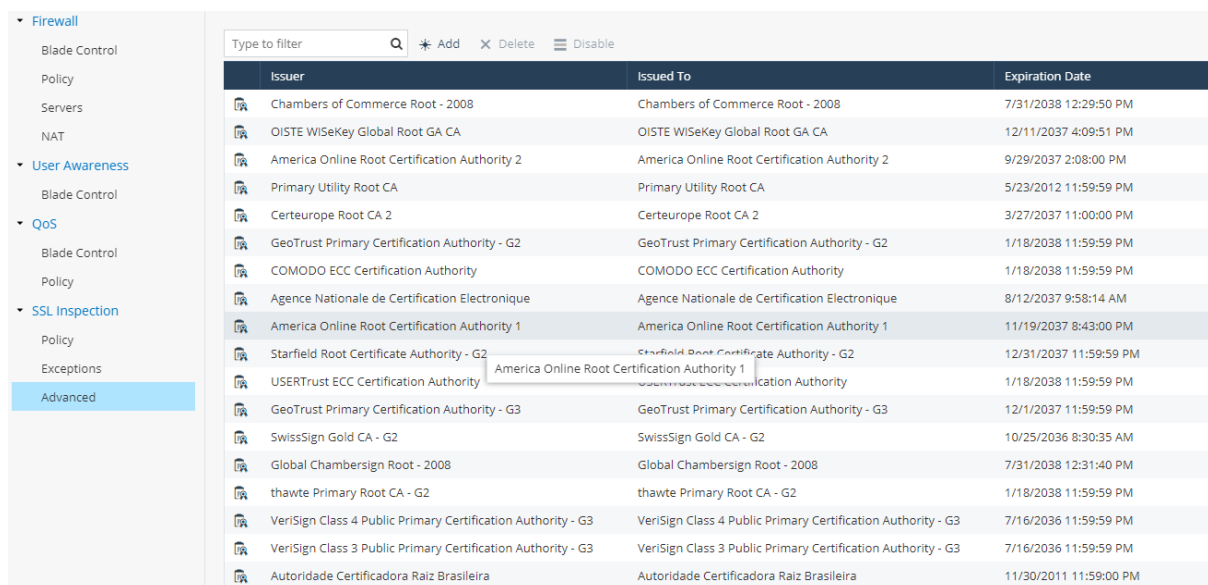


No.	Source	Destination	Service	Category/Custom ...	Track	Comment
1	* Any	Internet	HTTPS	* Any	Log	
2	* Any	Internet	HTTPS	Financial Servic...	Log	
3	* Any	Internet	HTTPS	Alcohol	Log	

figure 3.4

Advanced

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



Issuer	Issued To	Expiration Date
Chambers of Commerce Root - 2008	Chambers of Commerce Root - 2008	7/31/2038 12:29:50 PM
OISTE WiSeKey Global Root GA CA	OISTE WiSeKey Global Root GA CA	12/11/2037 4:09:51 PM
America Online Root Certification Authority 2	America Online Root Certification Authority 2	9/29/2037 2:08:00 PM
Primary Utility Root CA	Primary Utility Root CA	5/23/2012 11:59:59 PM
Certeurope Root CA 2	Certeurope Root CA 2	3/27/2037 11:00:00 PM
GeoTrust Primary Certification Authority - G2	GeoTrust Primary Certification Authority - G2	1/18/2038 11:59:59 PM
COMODO ECC Certification Authority	COMODO ECC Certification Authority	1/18/2038 11:59:59 PM
Agence Nationale de Certification Electronique	Agence Nationale de Certification Electronique	8/12/2037 9:58:14 AM
America Online Root Certification Authority 1	America Online Root Certification Authority 1	11/19/2037 8:43:00 PM
Starfield Root Certificate Authority - G2	Starfield Root Certificate Authority - G2	12/31/2037 11:59:59 PM
USERTrust ECC Certification Authority	USERTrust ECC Certification Authority	1/18/2038 11:59:59 PM
GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Authority - G3	12/1/2037 11:59:59 PM
SwissSign Gold CA - G2	SwissSign Gold CA - G2	10/25/2036 8:30:35 AM
Global Chambersign Root - 2008	Global Chambersign Root - 2008	7/31/2038 12:31:40 PM
thawte Primary Root CA - G2	thawte Primary Root CA - G2	1/18/2038 11:59:59 PM
VeriSign Class 4 Public Primary Certification Authority - G3	VeriSign Class 4 Public Primary Certification Authority - G3	7/16/2036 11:59:59 PM
VeriSign Class 3 Public Primary Certification Authority - G3	VeriSign Class 3 Public Primary Certification Authority - G3	7/16/2036 11:59:59 PM
Autoridade Certificadora Raiz Brasileira	Autoridade Certificadora Raiz Brasileira	11/30/2011 11:59:00 PM

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

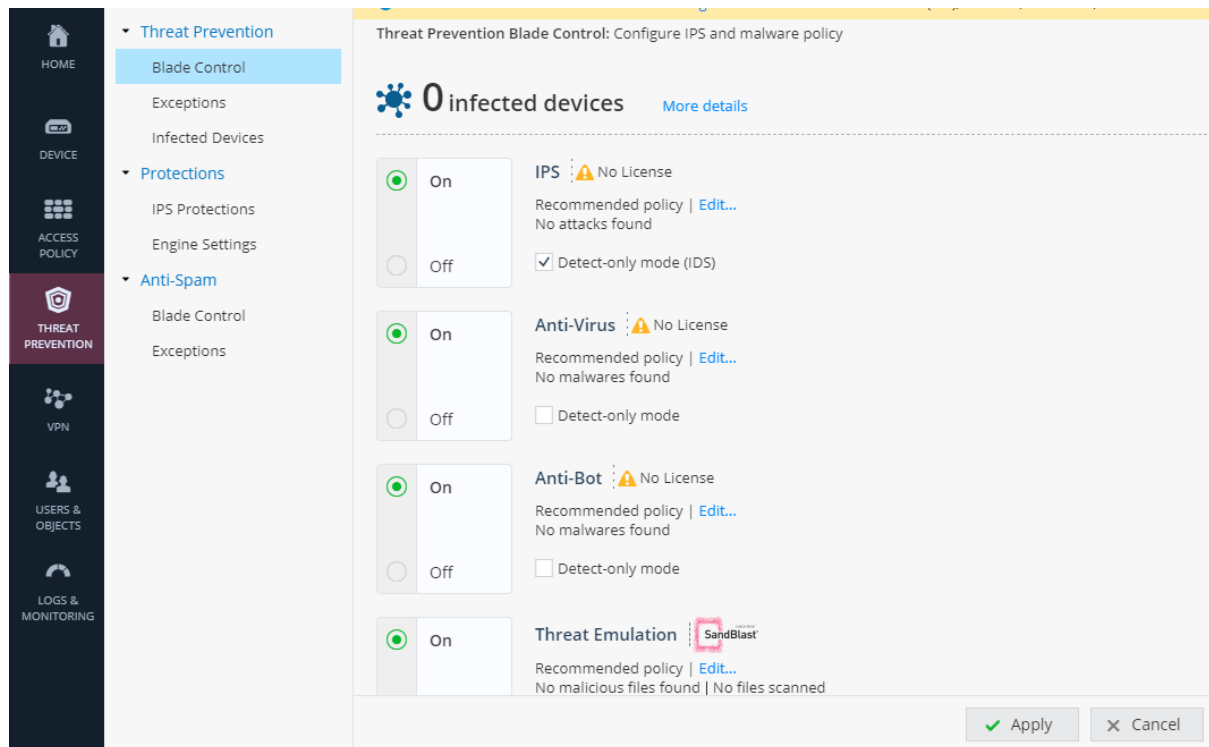


figure 3.6

Exception

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

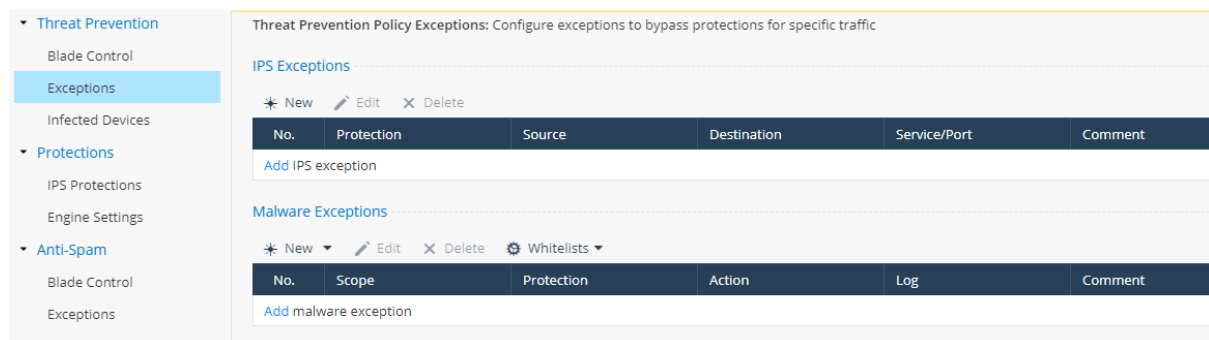


figure 3.7

Infected Device

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

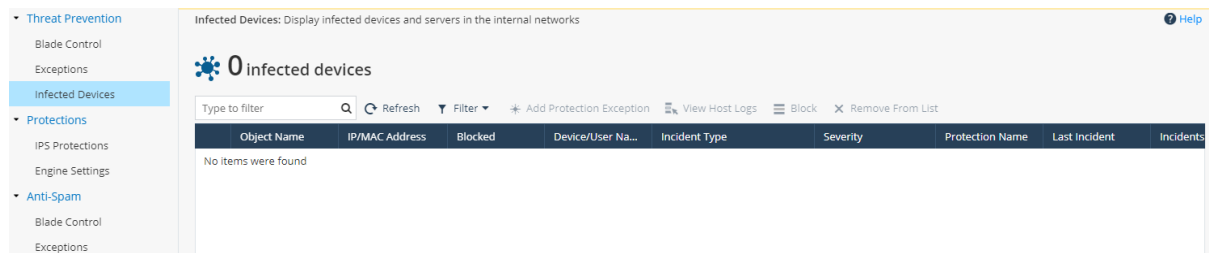


figure 3.8

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

The screenshot shows the 'IPS Protections' page under the 'Threat Prevention' menu. The page title is 'IPS Protections: Monitor protections list and manually configure specific protections to override general policy'. It features a search bar and an 'Edit' button. Below these is a table with columns: Protection, Protection Type, Category, Action, Severity, Confidence Level, and Performance Impact.

Protection	Protection Type	Category	Action	Severity	Confidence Level	Performance Impact
SYN Attack	Server/Client Protection	TCP	Inactive	High	High	Critical
Sequence Verifier	Server Anomaly	TCP	Inactive	High	Medium...	Low
LAND	Server/Client Protection	Denial of Service	Detect	Medium	Medium...	Very-low
Ping of Death	Server/Client Protection	Denial of Service	Inactive	Medium	Medium...	Very-low
Small PMTU	Server/Client Anomaly	TCP	Inactive	High	High	Critical
Teardrop	Server/Client Anomaly	Denial of Service	Inactive	High	Medium...	Very-low
Port Overflow	Server/Client Protection	FTP Advanced Protections	Detect	Critical	Medium...	Very-low
Max Ping Size	Server/Client Anomaly	IP and ICMP	Detect	Medium	High	Very-low
Non-TCP Flooding	Server/Client Anomaly	Denial of Service	Detect	High	Medium...	Low
Network Quota	Server/Client Anomaly	IP and ICMP	Inactive	High	Medium...	Critical
Dynamic Ports	Server/Client Anomaly	Network Security	Detect	Medium	High	Very-low
Domains Block List	Server/Client Anomaly	DNS	Inactive	None	Medium...	Critical
Inbound DNS Request	Server Protection	Cache Poisoning	Inactive	High	Low	Critical
Mismatched Replies	Server/Client Protection	Cache Poisoning	Inactive	High	Medium...	Critical
Scrambling	Server/Client Protection	Cache Poisoning	Inactive	High	Medium...	Critical
Non Compliant DNS	Server/Client Anomaly	DNS	Inactive	Critical	Medium	Low

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

Anti-Spam Control

☒ On ☐ Off ☐ Detect-only mode

Anti-Spam

Policy Configuration

Filter spam based on:

☒ Sender's IP address

☒ Email content (most secure)

☒ Block

☐ Flag email subject with

☐ Flag email header

Tracking:

☐ Handle suspected spam separately

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

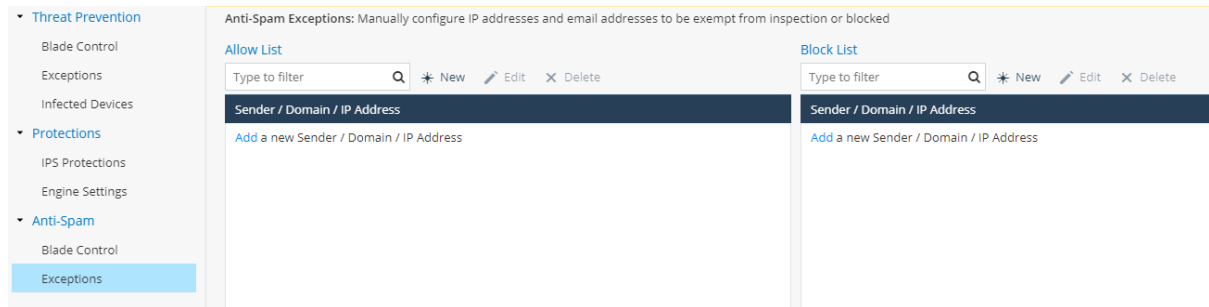


figure 4.1

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

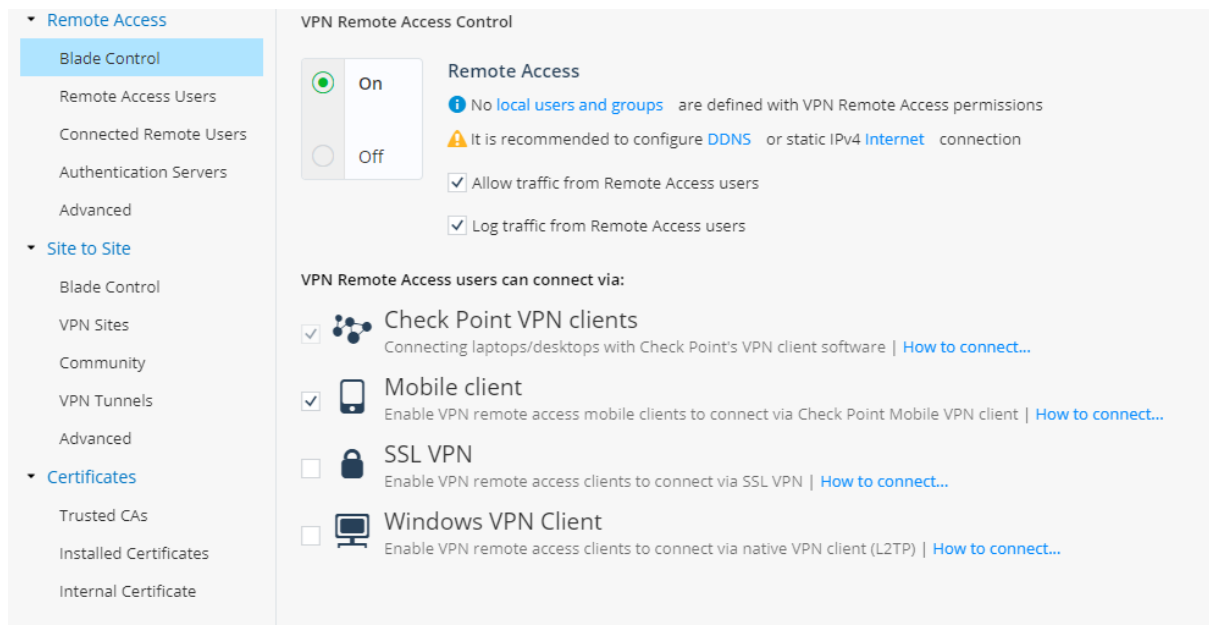


figure 4.2

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

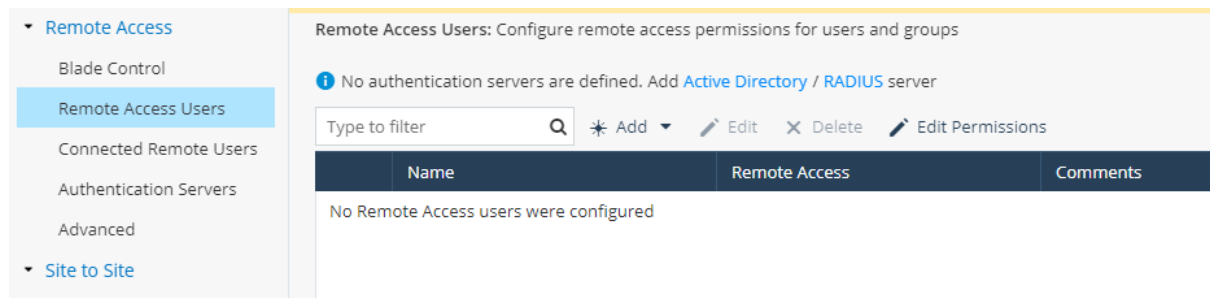


figure 4.3

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

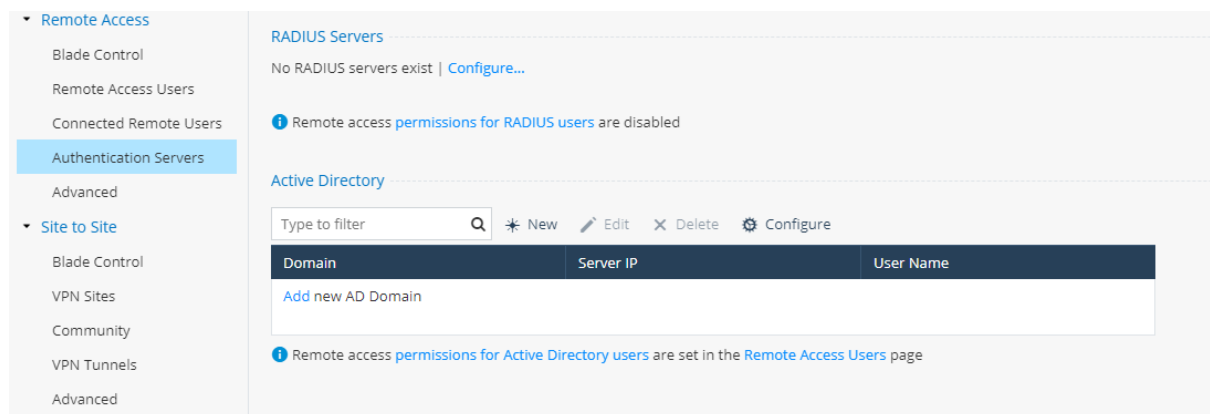


figure 4.4

Advanced

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

Remote Access

Blade Control

Remote Access Users

Connected Remote Users

Authentication Servers

Advanced

Site to Site

Blade Control

VPN Sites

Community

VPN Tunnels

Advanced

Certificates

Trusted CAs

Installed Certificates

Internal Certificate

Remote Access Advanced Settings: Configure additional advanced options for VPN remote access users

Office Mode - Allocate IP addresses from the following network:

Office Mode Network: 172.16.10.0

Office Mode Subnet: 255.255.255.0

Certificate authentication:

☒ Automatically use the last installed certificate
 ☐ Manually choose a VPN certificate:

☐ Route Internet traffic from connected clients through this gateway

Local encryption domain is defined automatically according to topology...

DNS servers for Remote Access users:

Office mode first DNS for clients: This Gateway [Configure manually](#)

Office mode second DNS for clients: Field is not mandatory

Office mode third DNS for clients: Field is not mandatory

DNS domain name: Same as DNS domain name [Configure manually](#)

SSL VPN Bookmarks

Type to filter

New Edit Delete

Apply

Cancel

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

Remote Access

Blade Control

Remote Access Users

Connected Remote Users

Authentication Servers

Advanced

Site to Site

Blade Control

VPN Sites

Community

VPN Tunnels

Advanced

Site to Site VPN Control

☒ On
 ☐ Off

Site to Site VPN

No VPN sites are defined | [VPN Sites](#)

☒ Allow traffic from remote sites (by default)
 ☒ Log remote sites traffic (by default)

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

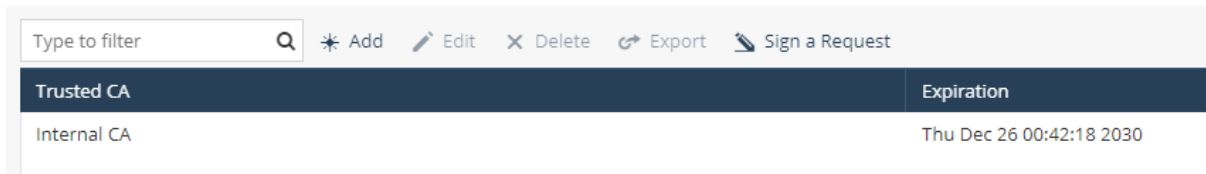
The screenshot displays the 'Site to Site VPN Advanced Settings' configuration page. On the left is a navigation sidebar with categories: 'Remote Access' (containing Blade Control, Remote Access Users, Connected Remote Users, Authentication Servers, and Advanced), 'Site to Site' (containing Blade Control, VPN Sites, Community, VPN Tunnels, and Advanced), and 'Certificates' (containing Trusted CAs, Installed Certificates, and Internal Certificate). The 'Advanced' option under 'Site to Site' is selected and highlighted in blue. The main content area is titled 'Site to Site VPN Advanced Settings: Configure additional advanced options for Site to Site VPN'. It includes a note that the 'Local encryption domain is defined automatically according to topology...'. A section titled 'Link selection' contains 'Outgoing interface selection' with radio buttons for 'According to the routing table' (selected) and 'Route based probing'. Below this is 'Source IP address selection' with radio buttons for 'Automatically chosen according to outgoing interface' (selected) and 'Manually configured:' followed by an empty text box. The 'Tunnel health monitoring' section shows 'Tunnel health monitoring method' set to 'Tunnel test (Check Point Proprietary)' in a dropdown menu, and an unchecked checkbox for 'Use DPD (Dead Peer Detection) responder mode'. A final section titled 'Encryption Method' shows the 'IKEv2 global gateway ID' set to 'Gateway-ID-7F7C6792' in a text box.

figure 4.7

Certificates

Trusted CAs

- View **VPN -> Certificates -> Trusted CAs**
- From these options manage trusted Certificates authorities. Refer [figure 4.8](#)



Type to filter	Q	* Add	✎ Edit	✕ Delete	↗ Export	✉ Sign a Request
Trusted CA		Expiration				
Internal CA		Thu Dec 26 00:42:18 2030				

figure 4.8

Installed Certificates

- View **VPN -> Certificates -> Installed Certificates**
- From this option Create & manage appliances. Refer [figure 4.9](#)

Type to filter

Q

New Signing Request

Details...

Delete

Export

Upload Signed Certificate

Upload P12 Certificate

Installed Certificate	Expiration	Status
Default Certificate	Thu Dec 31 00:42:29 2015	Verified
Default Web Portal Certificate	Tue Dec 29 06:12:03 2020	Verified

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](#)

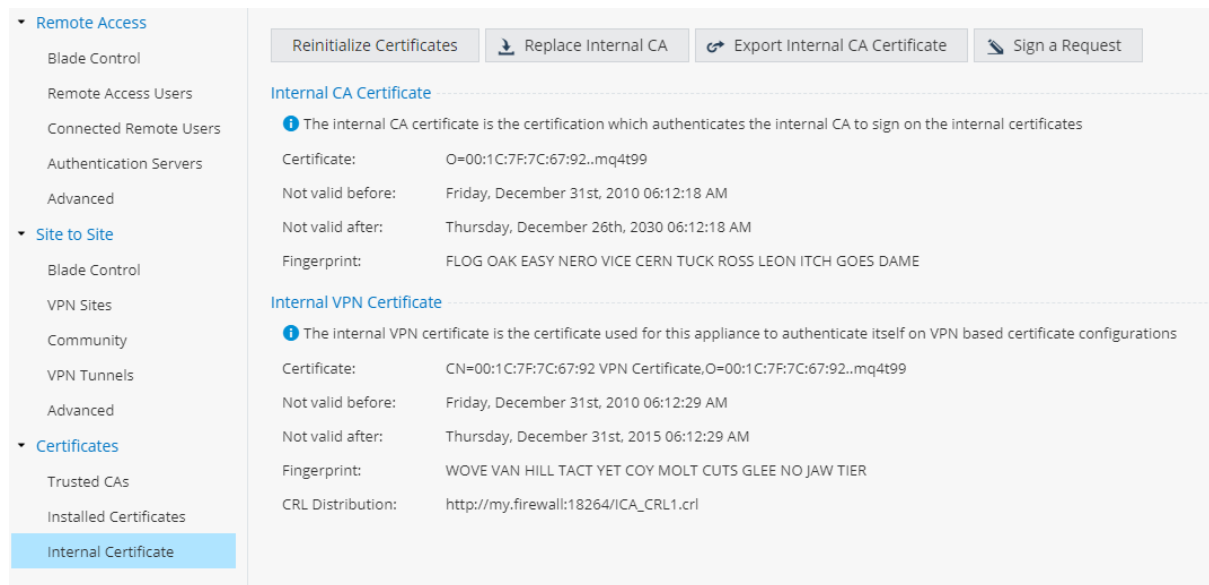


figure 5.0

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

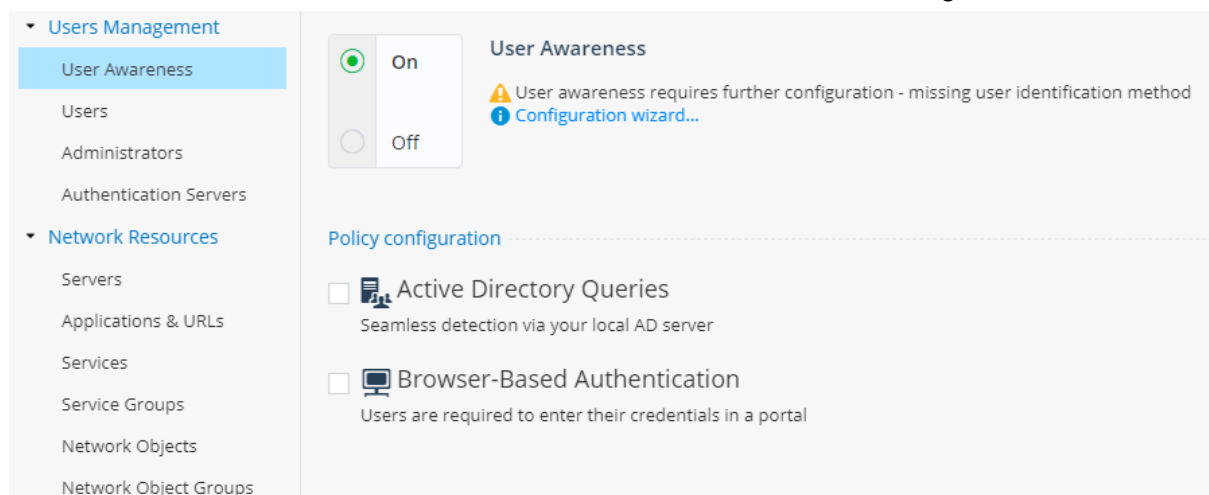


figure 5.1

Users

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

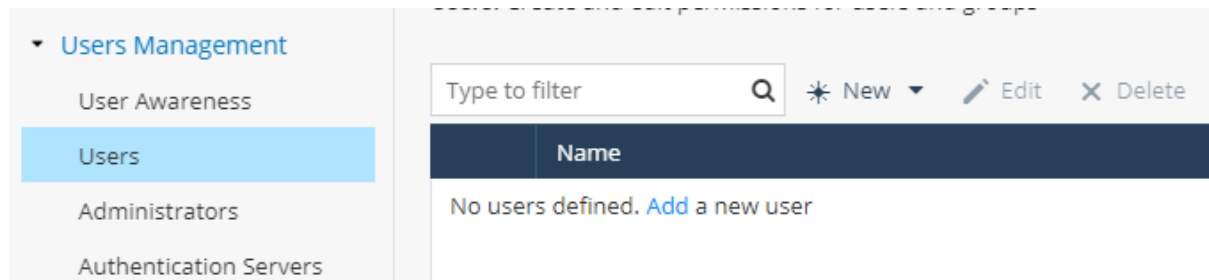


figure 5.2

Administrator

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

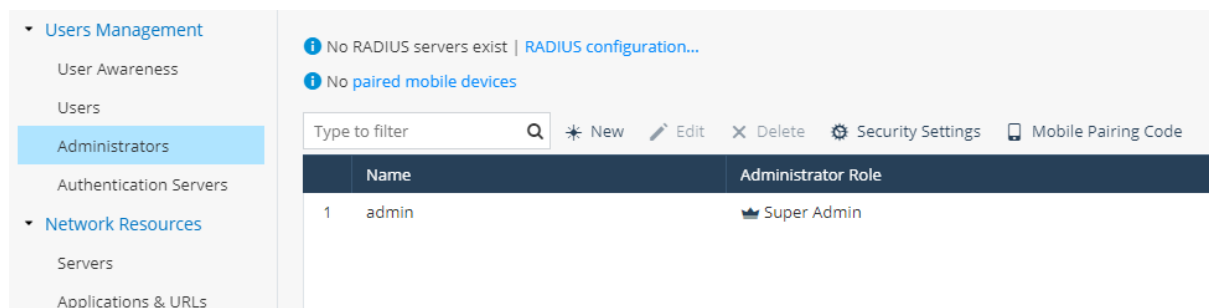


figure 5.3

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**

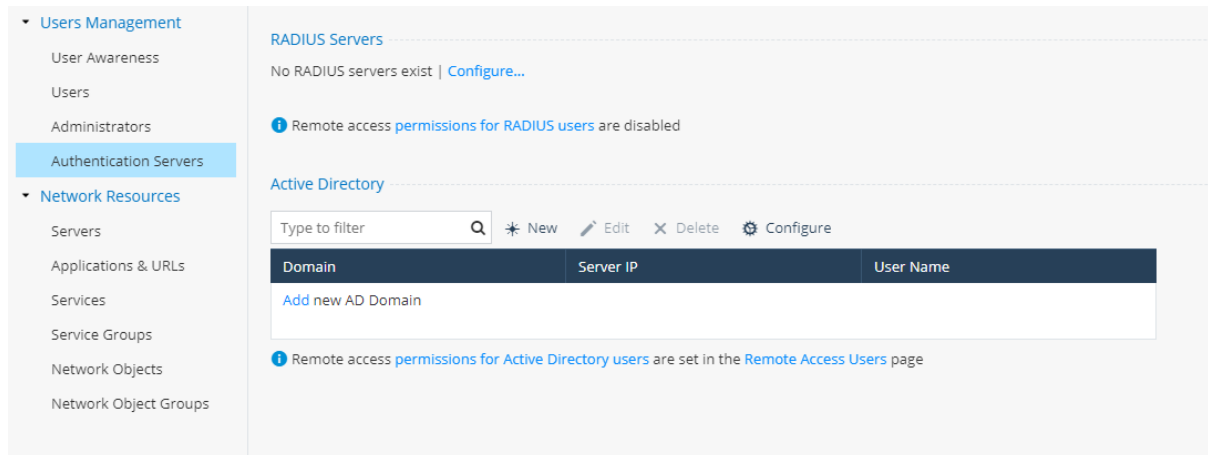


figure 5.4

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**

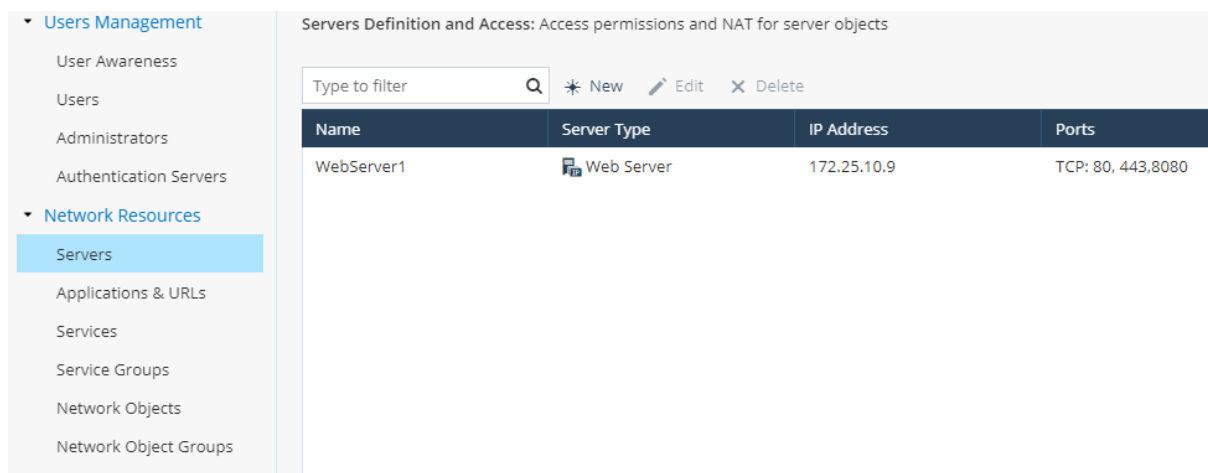


figure 5.5

Applications & URLs

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

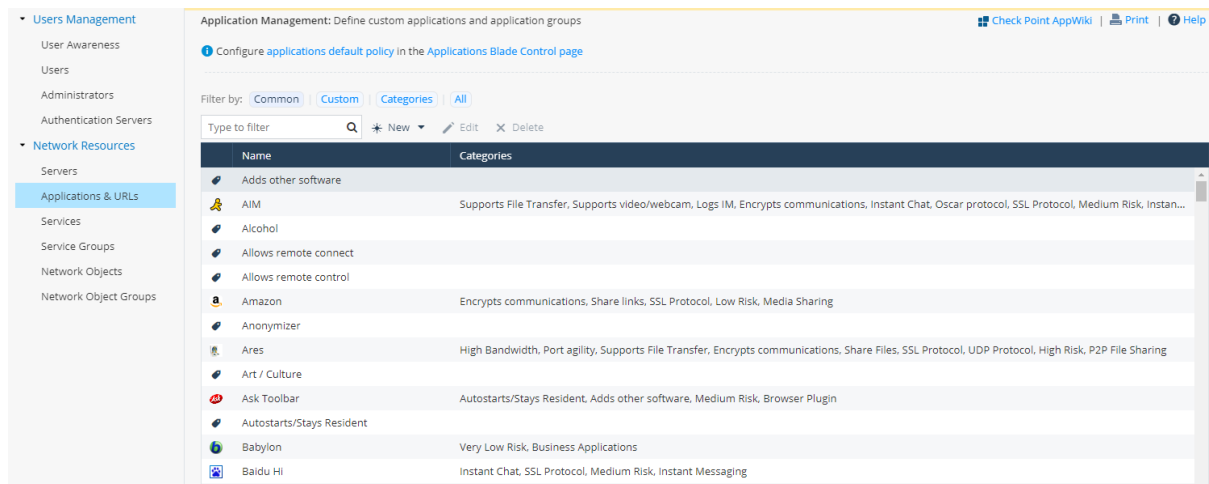


figure 5.6

Services

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

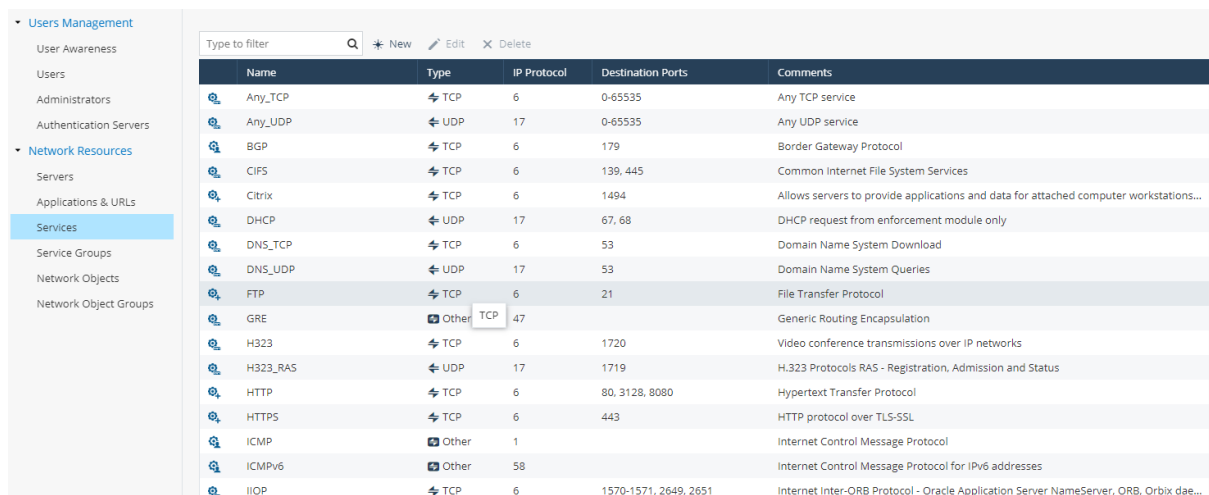
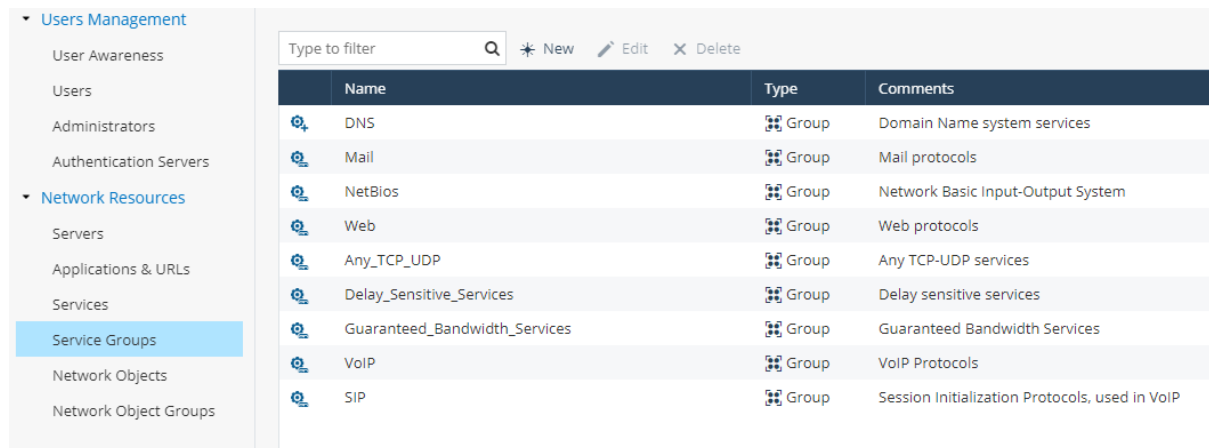


figure 5.7

Service group

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



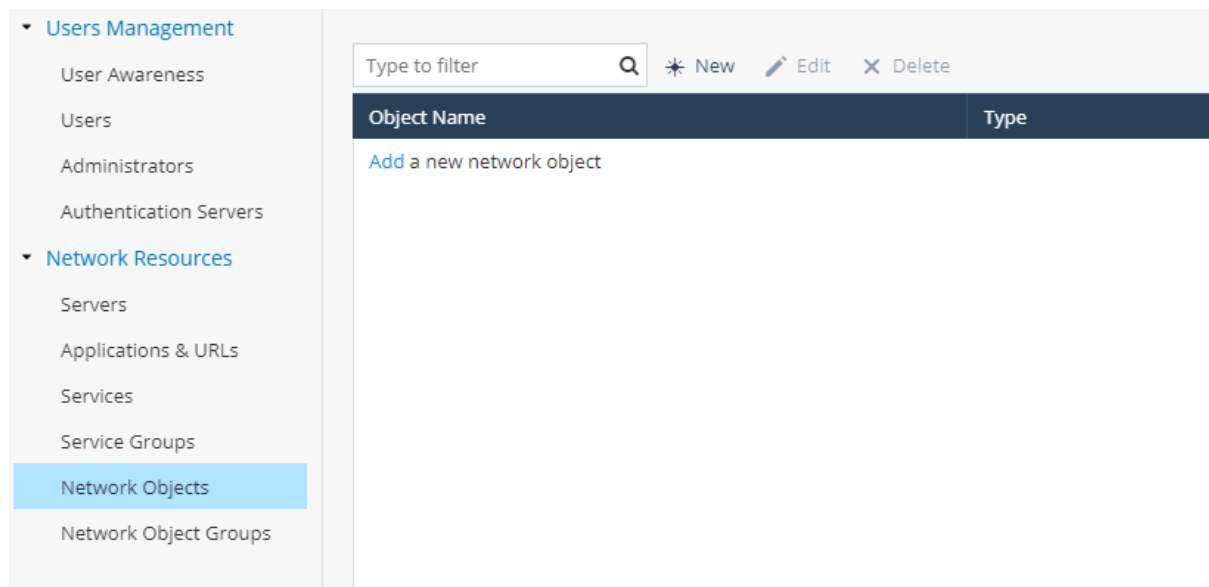
The screenshot shows a management console interface. On the left is a sidebar with a tree view containing 'Users Management' and 'Network Resources'. 'Network Resources' is expanded, and 'Service Groups' is selected. The main area displays a table of service groups. Above the table is a search bar and three action buttons: 'New', 'Edit', and 'Delete'. The table has four columns: 'Name', 'Type', and 'Comments'. It lists nine service groups, all of which are of type 'Group'.

Name	Type	Comments
DNS	Group	Domain Name system services
Mail	Group	Mail protocols
NetBios	Group	Network Basic Input-Output System
Web	Group	Web protocols
Any_TCP_UDP	Group	Any TCP-UDP services
Delay_Sensitive_Services	Group	Delay sensitive services
Guaranteed_Bandwidth_Services	Group	Guaranteed Bandwidth Services
VoIP	Group	VoIP Protocols
SIP	Group	Session Initialization Protocols, used in VoIP

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**



The screenshot shows the 'Network Objects' configuration page. The sidebar is similar to the previous figure, but 'Network Objects' is selected under 'Network Resources'. The main area features a search bar and 'New', 'Edit', and 'Delete' buttons. Below these is a table with two columns: 'Object Name' and 'Type'. The table is currently empty, with a link 'Add a new network object' provided for creating a new entry.

Object Name	Type
Add a new network object	

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

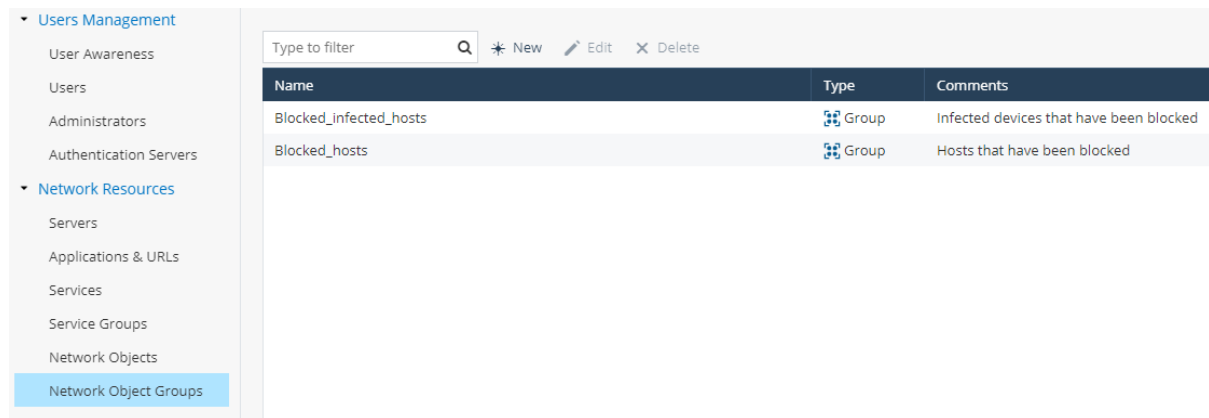


figure 6.0

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

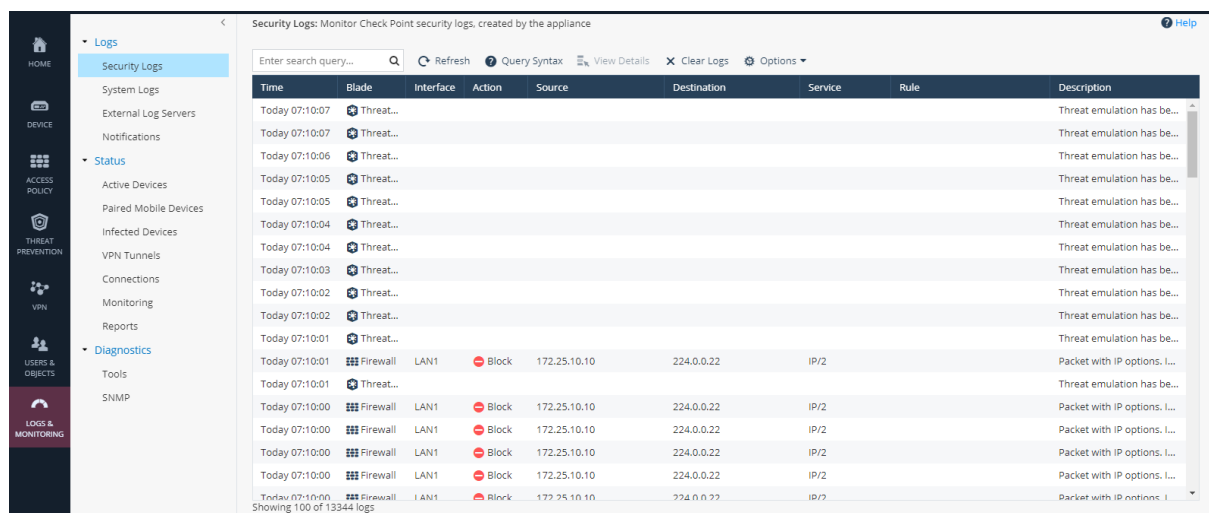
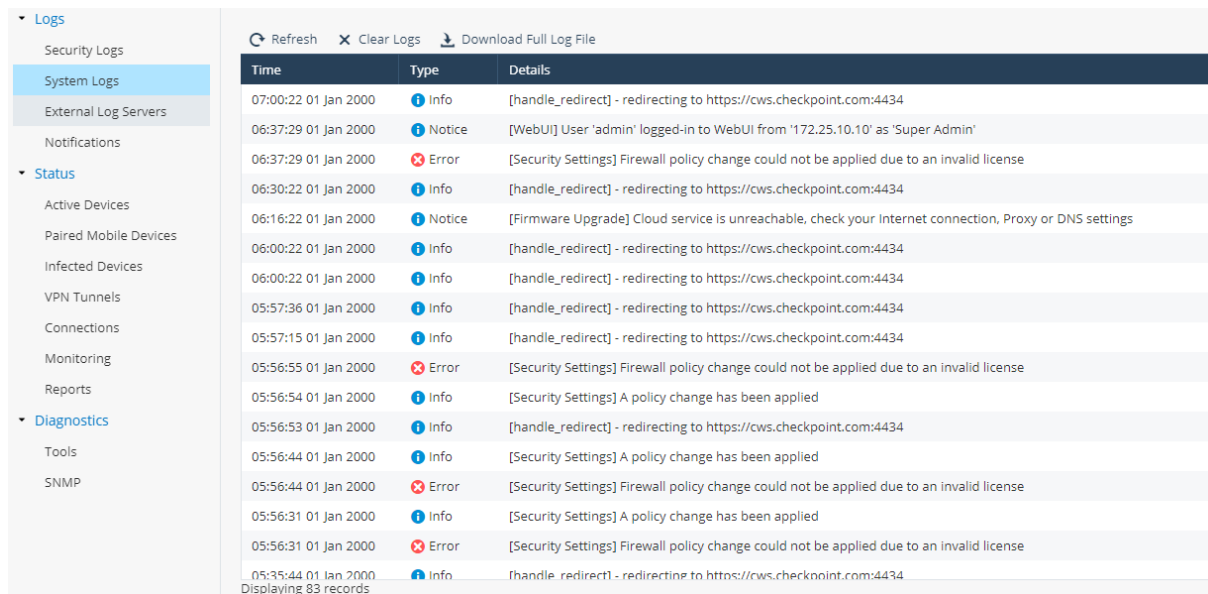


figure 6.1

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



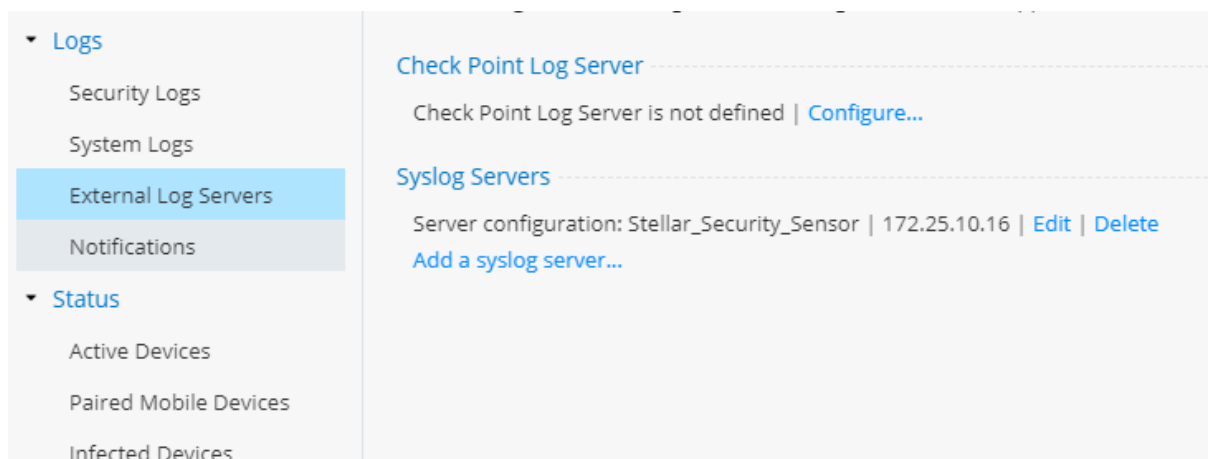
Time	Type	Details
07:00:22 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434
06:37:29 01 Jan 2000	Notice	[WebUI] User 'admin' logged-in to WebUI from '172.25.10.10' as 'Super Admin'
06:37:29 01 Jan 2000	Error	[Security Settings] Firewall policy change could not be applied due to an invalid license
06:30:22 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434
06:16:22 01 Jan 2000	Notice	[Firmware Upgrade] Cloud service is unreachable, check your Internet connection, Proxy or DNS settings
06:00:22 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434
06:00:22 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434
05:57:36 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434
05:57:15 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434
05:56:55 01 Jan 2000	Error	[Security Settings] Firewall policy change could not be applied due to an invalid license
05:56:54 01 Jan 2000	Info	[Security Settings] A policy change has been applied
05:56:53 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434
05:56:44 01 Jan 2000	Info	[Security Settings] A policy change has been applied
05:56:44 01 Jan 2000	Error	[Security Settings] Firewall policy change could not be applied due to an invalid license
05:56:31 01 Jan 2000	Info	[Security Settings] A policy change has been applied
05:56:31 01 Jan 2000	Error	[Security Settings] Firewall policy change could not be applied due to an invalid license
05:35:44 01 Jan 2000	Info	[handle_redirect] - redirecting to https://cws.checkpoint.com:4434

Displaying 83 records

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



Check Point Log Server
Check Point Log Server is not defined Configure...

Syslog Servers
Server configuration: Stellar_Security_Sensor 172.25.10.16 Edit Delete
Add a syslog server...

figure 6.3

Notification

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

Logs

Security Logs

System Logs

External Log Servers

Notifications

Status

Active Devices

Paired Mobile Devices

Infected Devices

VPN Tunnels

Connections

Monitoring

Reports

Diagnostics

Tools

SNMP

Type to filter

View Details

Refresh

Settings

Time	Severity	Subject	Message
00:00:29 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:27 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:27 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:27 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:26 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:26 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:00:25 01 Jan 2000	Attention Required	Unexpected reboot	Security gateway is up after an unexpected reboot.
00:51:18 01 Jan 2011	Informative Event	New device detected	kowshik (172.25.10.2) connects to your network (LAN1) for the first time.

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

Active Devices: Display devices in the internal networks

Print

Type to filter

Filter

Refresh

Details...

Save as...

Block

Revoke Certificate

Start Traffic Monitoring

Name	IP Address	MAC Address	Device Details	Network Access	Interface
	172.25.10.10	28:d2:44:7f:00:38		Allowed	LAN1 Switch

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

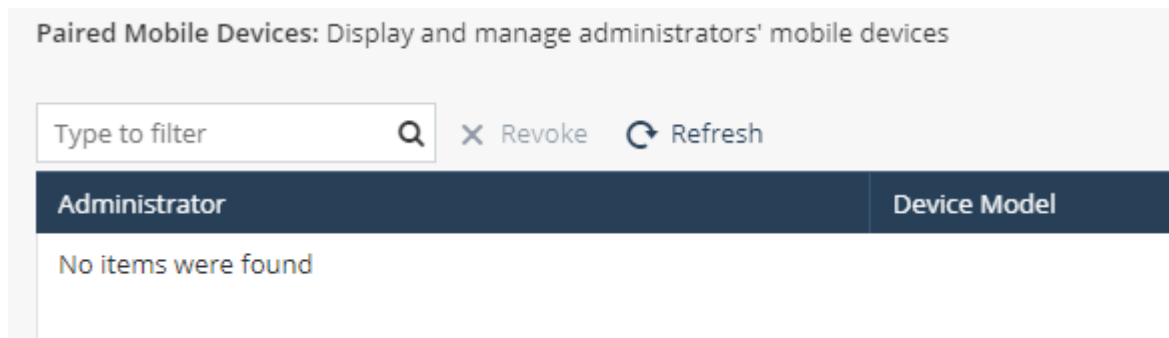


figure 6.6

Infected Devices

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

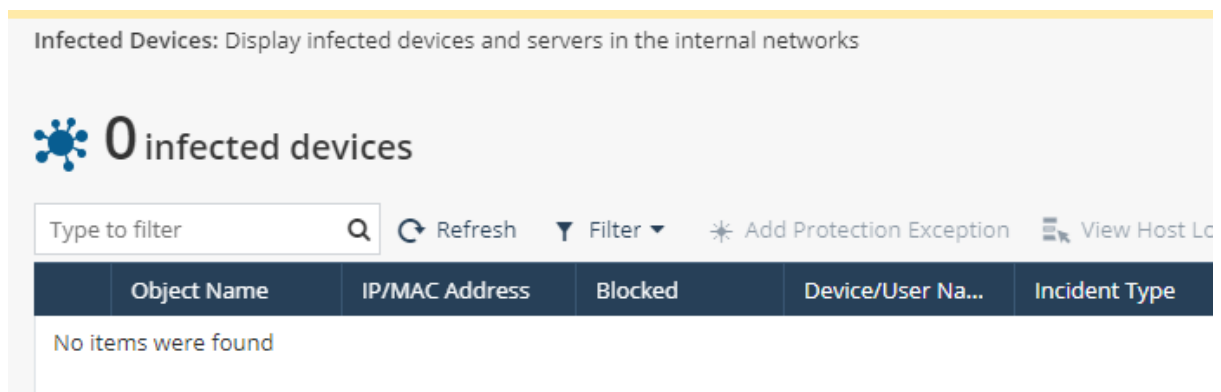


figure 6.7

VPN Tunnels

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

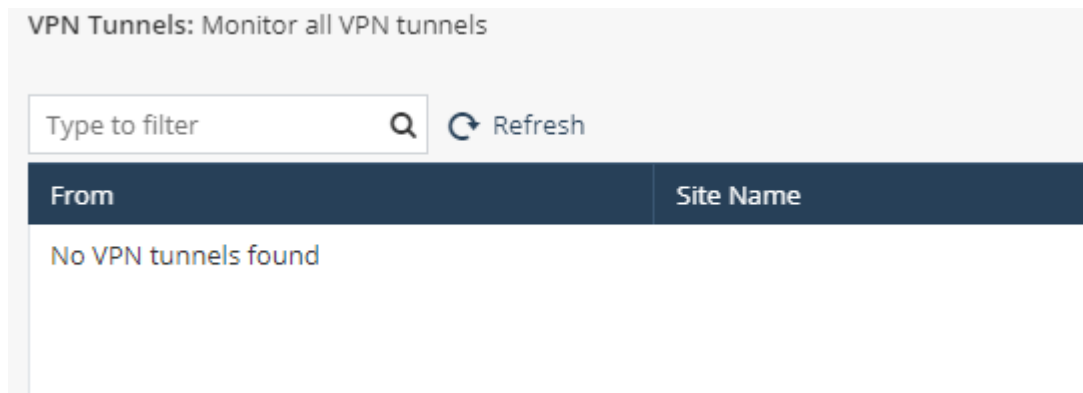



figure 6.8

Connections

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

Connections: View all active connections  [Print](#)

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

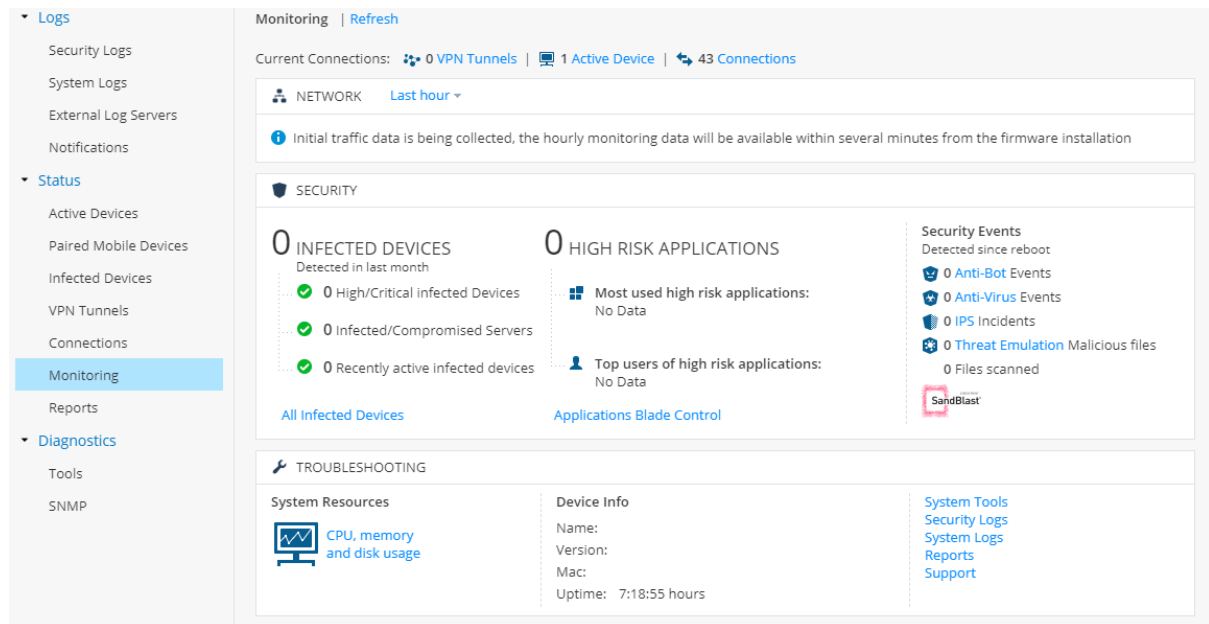


figure 7.0

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

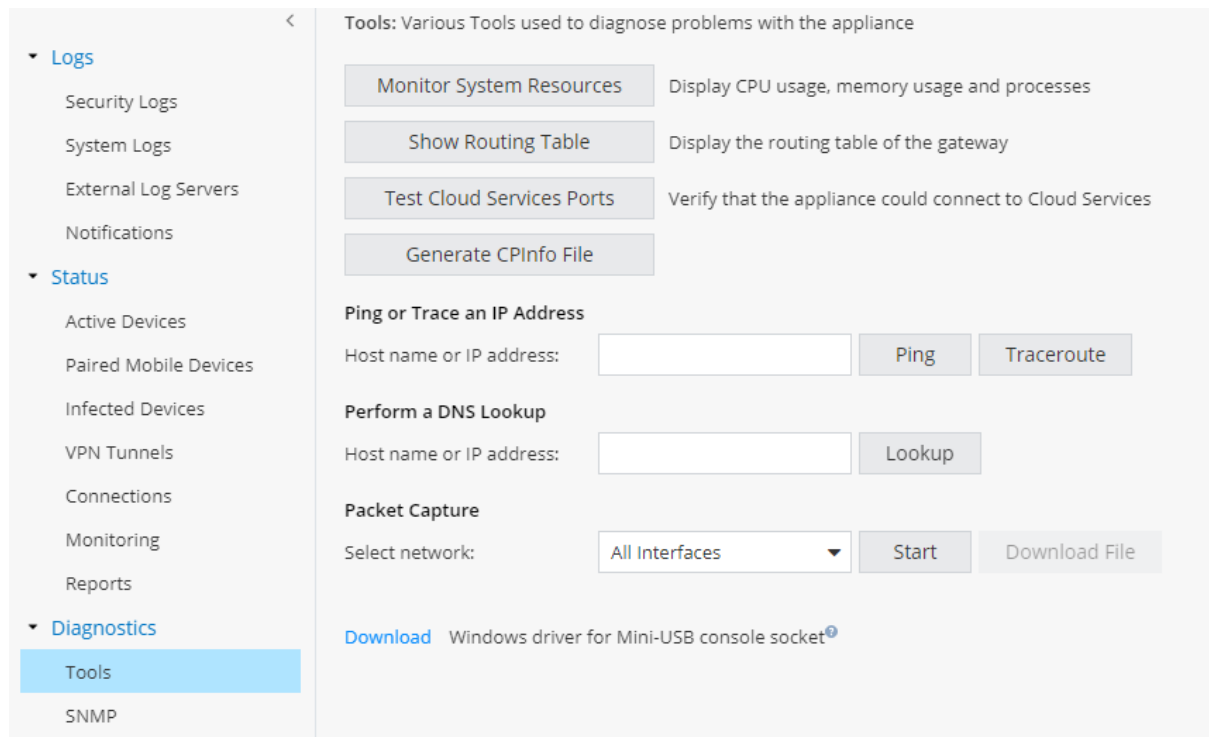


figure 7.1

SNMP

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

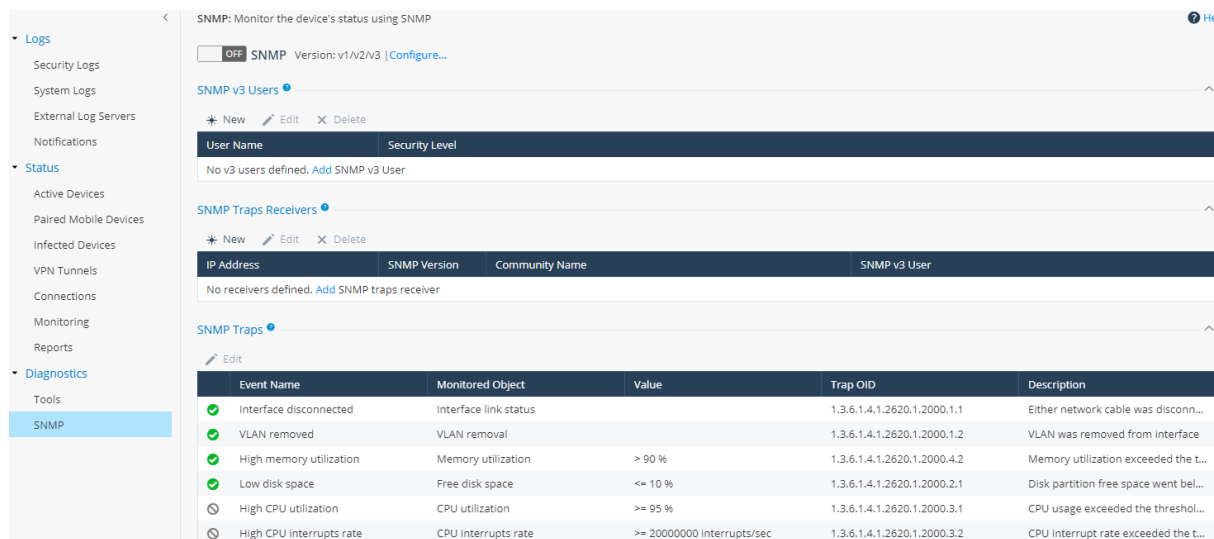


figure 7.2

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

-----EOD-----