



NetWyl Informatik
IT-Security Experts

Checkpoint VPN IPsec Site-to-Site

Version 1.0

Dokument Name: Checkpoint_VPN IPsec Site-to-Site

Dokumentenkontrolle

Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
A.1	18.08.2004				

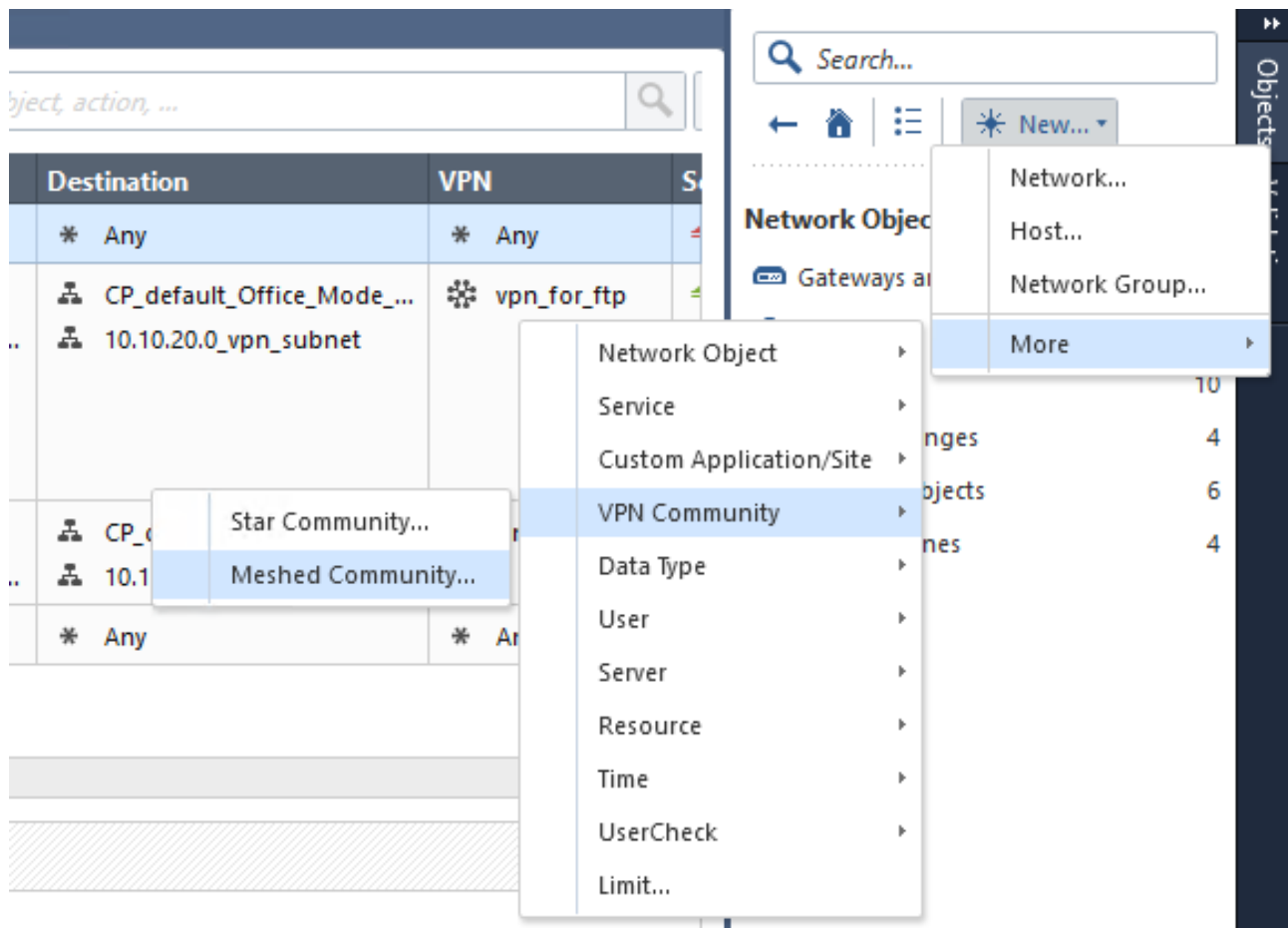
Copyright 2024 NetWyl Informatik

NetWyl Informatik GmbH
Täschmattstrasse 19
6015 Luzern
info@netwyl-informatik.ch
Phone: +41 41 520 73 90

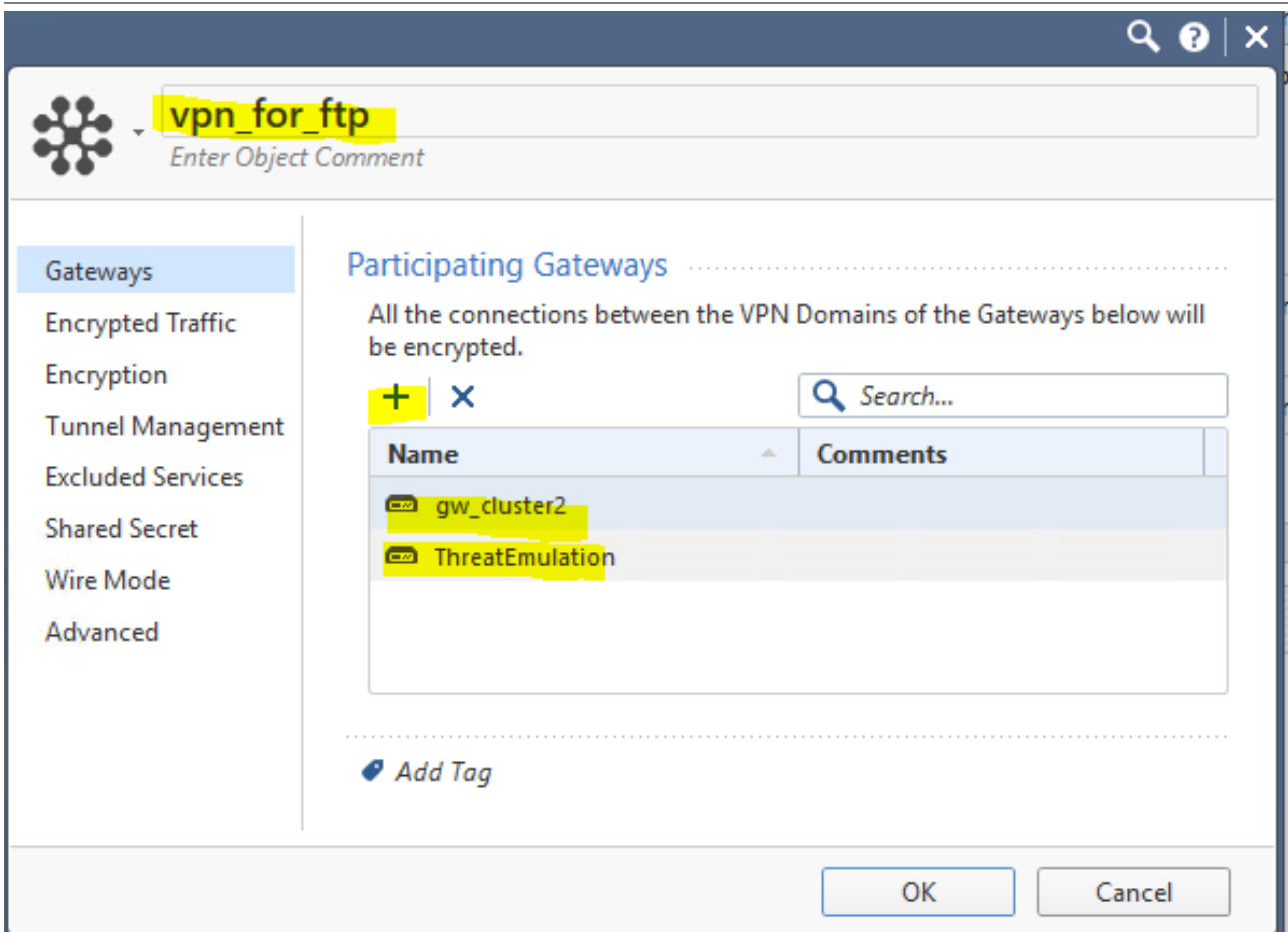
VPN IPsec Site-to-Site

1. Create a VPN community object

New -> More -> VPN community -> Meshed Community

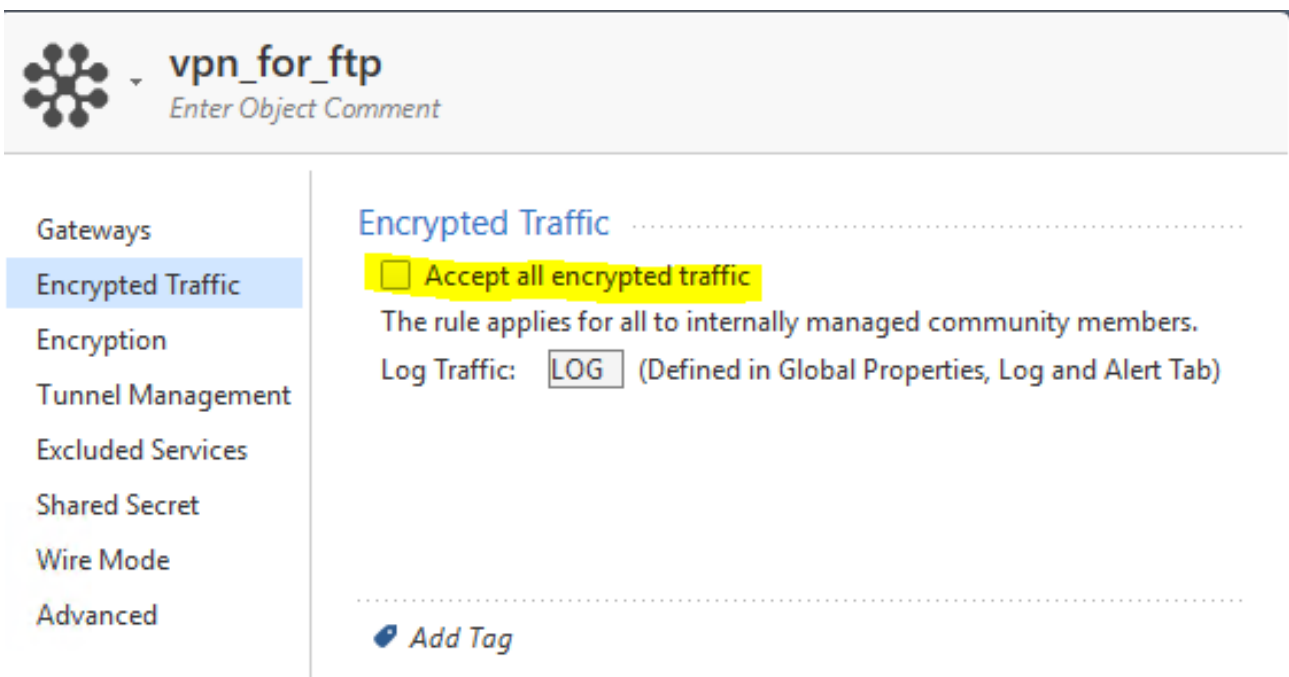


2. Give a name to your VPN community and add Gateway you want to participate in building a tunnel



The screenshot shows a configuration window titled "vpn_for_ftp" with a search icon and a close button in the top right. Below the title bar is a search field containing "vpn_for_ftp" and a placeholder "Enter Object Comment". A sidebar on the left lists navigation options: Gateways, Encrypted Traffic, Encryption, Tunnel Management, Excluded Services, Shared Secret, Wire Mode, and Advanced. The main area is titled "Participating Gateways" and contains the text: "All the connections between the VPN Domains of the Gateways below will be encrypted." Below this text are a plus sign (+) and a minus sign (x) button, and a search field labeled "Search...". A table with two columns, "Name" and "Comments", lists two gateway entries: "gw_cluster2" and "ThreatEmulation". At the bottom of the main area is an "Add Tag" button. The window concludes with "OK" and "Cancel" buttons.

3. Check if you want your Firewall accept all traffic that's going inside that community (Creates implied rules)



This screenshot shows the "Encrypted Traffic" configuration window for "vpn_for_ftp". The sidebar on the left is the same as in the previous screenshot, but "Encrypted Traffic" is now selected. The main area is titled "Encrypted Traffic" and features a checkbox labeled "Accept all encrypted traffic" which is currently unchecked. Below the checkbox is the text: "The rule applies for all to internally managed community members." and "Log Traffic: LOG (Defined in Global Properties, Log and Alert Tab)". At the bottom of the main area is an "Add Tag" button.

Uncheck to make your Firewall more granular for specific hosts, ports etc.
-> Like that

No.	re	Source	Destination	VPN	Services & Applicat...	Action	Track	Install On
1		* Any	* Any	* Any	FW1_topo	Drop	Log	* Policy...
2		10.10.20.0_vpn_subnet CP_default_Office_Mode_a...	CP_default_Office_Mode_... 10.10.20.0_vpn_subnet	vpn_for_ftp	ftp-pasv ftp-bidir ftp ftp-port tcp-high-ports	Accept	Log	Threa... gw_cl...
3	nup rule	10.10.20.0_vpn_subnet CP_default_Office_Mode_a...	CP_default_Office_Mode_... 10.10.20.0_vpn_subnet	* Any	* Any	Drop	Log	* Policy...

4. Choose your Encryption settings for Phase 1 and Phase 2

Enter Object Comment

- Gateways
- Encrypted Traffic
- Encryption
- Tunnel Management
- Excluded Services
- Shared Secret
- Wire Mode
- Advanced

Encryption Method

Encryption Method:

Encryption Suite

Use this encryption suite:

Custom encryption suite:

IKE Security Association (Phase 1)

Encryption Algorithm:

Data Integrity:

Diffie-Hellman group:

IKE Security Association (Phase 2)

Encryption Algorithm:

Data Integrity:

More

IKE Security Association (Phase 1)

Use aggressive mode

IKE Security Association (Phase 2)

Use Perfect Forward Secrecy

Diffie-Hellman group:

Support IP Compression

5. Choose how you will build tunnel



vpn_for_ftp

Enter Object Comment

- Gateways
- Encrypted Traffic
- Encryption
- Tunnel Management**
- Excluded Services
- Shared Secret
- Wire Mode
- Advanced

Permanent Tunnels

Set Permanent Tunnels:

- On all tunnels in the community
- On all tunnels of specific gateways Select Gateways...
- On specific tunnels in the community Select Permanent Tunnels...
- Enable Route Injection Mechanism (RIM) Settings...

Tunnel down track: Log

Tunnel up track: Log

VPN Tunnel Sharing

- One VPN tunnel per each pair of hosts
- One VPN tunnel per subnet pair
- One VPN tunnel per Gateway pair

6. If there are any services, you want to exclude from your VPN. You can do it either here, or inside the Firewall policy



vpn_for_ftp

Enter Object Comment

- Gateways
- Encrypted Traffic
- Encryption
- Tunnel Management
- Excluded Services**
- Shared Secret
- Wire Mode
- Advanced

Excluded Services

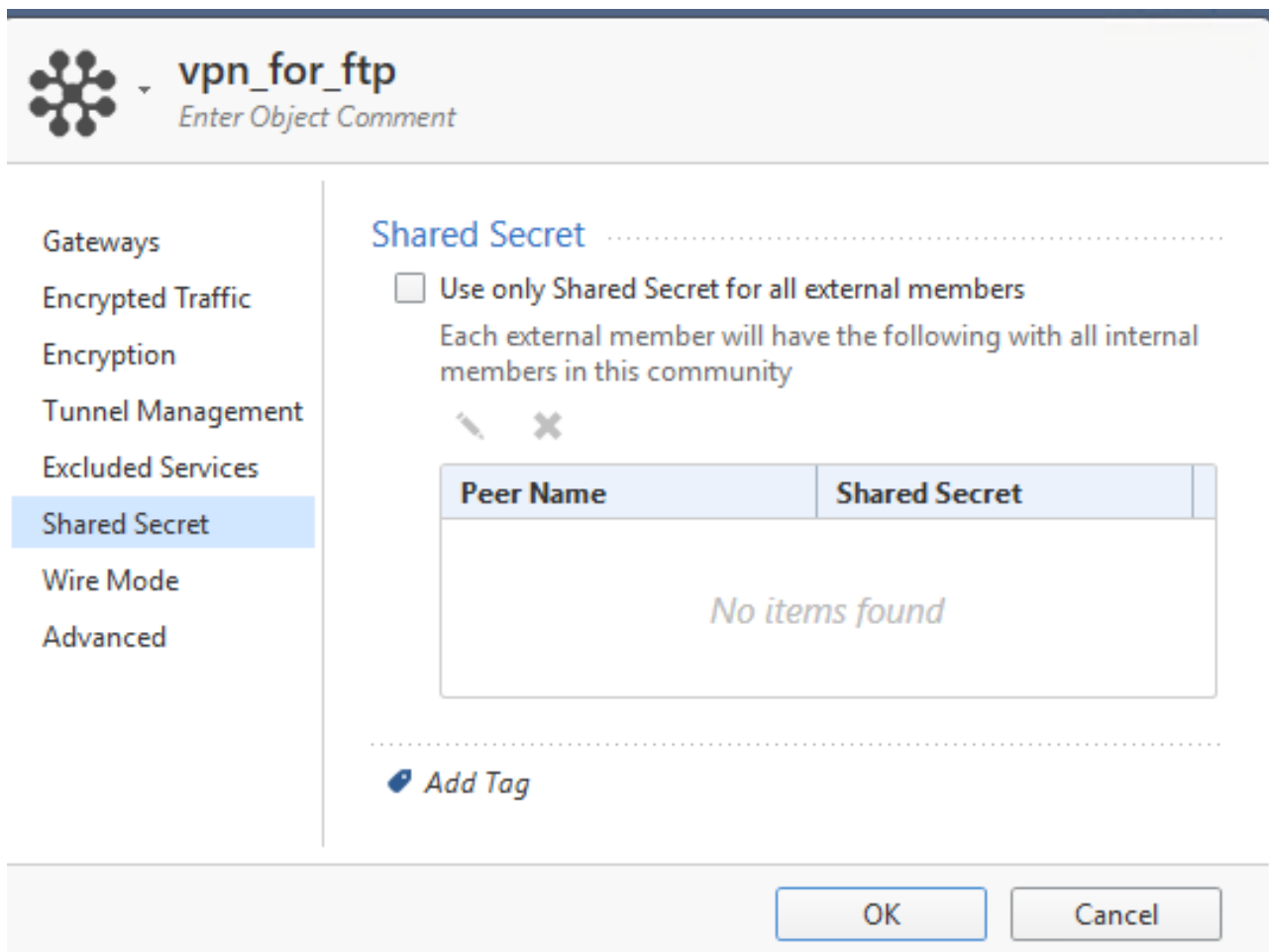
The following services are excluded from the community. Connections with these services will not be encrypted and will not match rules specifying the community in the VPN community.

+ | ×

🔍 Search...

Name	Comments
No items found	

7. Pre-shared key can be used instead of a Certificate with Third Party vendors or Check Point gateways that are managed by a different Management Server





The screenshot shows a configuration window for a VPN object named 'vpn_for_ftp'. The left sidebar contains a menu with the following items: Gateways, Encrypted Traffic, Encryption, Tunnel Management, Excluded Services, **Shared Secret** (highlighted), Wire Mode, and Advanced. The main content area is titled 'Shared Secret' and contains a checkbox labeled 'Use only Shared Secret for all external members'. Below the checkbox is the text: 'Each external member will have the following with all internal members in this community'. There are two small icons (a pencil and an 'X') above a table. The table has two columns: 'Peer Name' and 'Shared Secret'. The table is currently empty, displaying the text 'No items found'. Below the table is a dotted line and an 'Add Tag' button. At the bottom right of the window are 'OK' and 'Cancel' buttons.

vpn_for_ftp
Enter Object Comment

Gateways
Encrypted Traffic
Encryption
Tunnel Management
Excluded Services
Shared Secret
Wire Mode
Advanced


Shared Secret

Use only Shared Secret for all external members
Each external member will have the following with all internal members in this community


Peer Name	Shared Secret
<i>No items found</i>	

.....

 *Add Tag*

OK Cancel

8. If you want to bypass your firewall stateful inspection

 **vpn_for_ftp**
Enter Object Comment


Gateways
Encrypted Traffic
Encryption
Tunnel Management
Excluded Services
Shared Secret
Wire Mode
Advanced

Wire Mode

Bypass Firewall

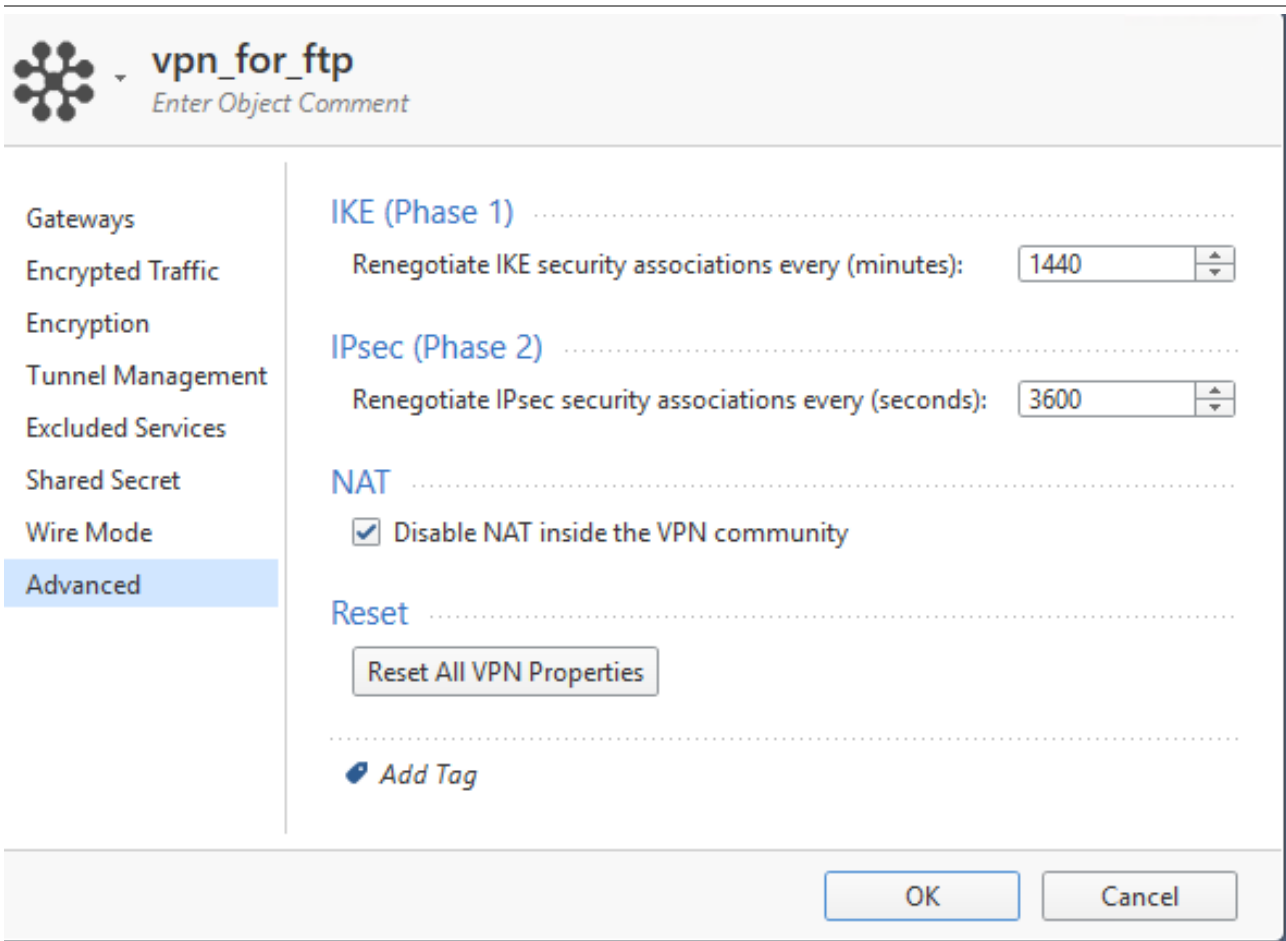
- Allow uninspected encrypted traffic between Wire mode interfaces of this Community members
- Wire mode routing - Allow members to route uninspected encrypted traffic in VPN routing configurations

.....

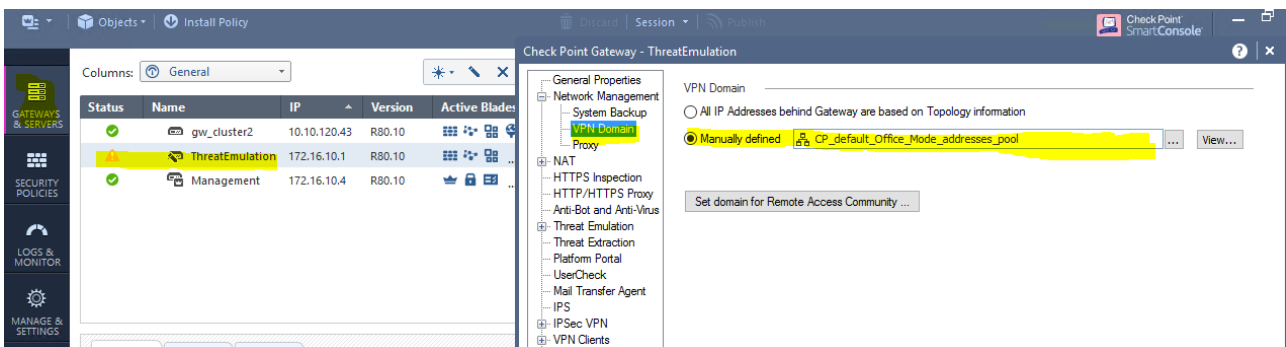
 *Add Tag*

OK Cancel

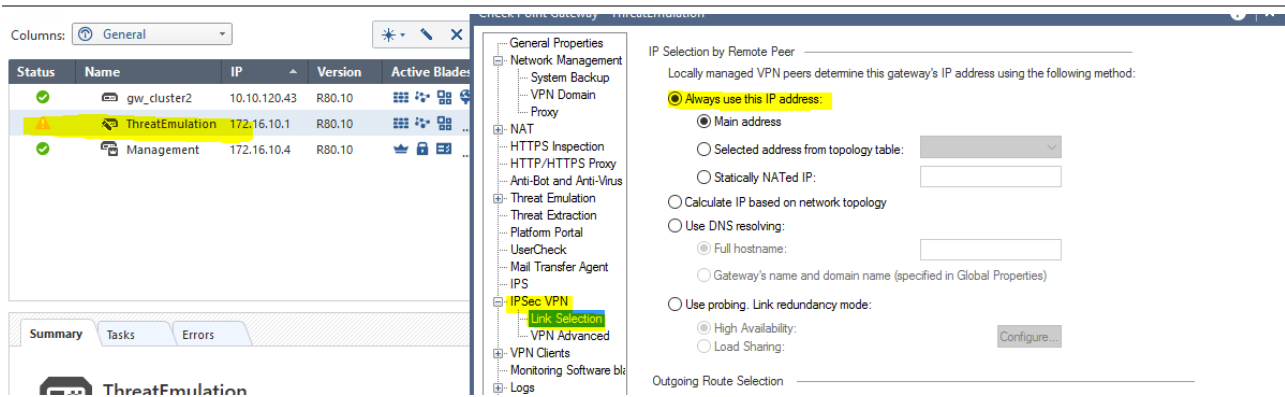
9.



10. Define your Encryption domain Inside the Gateways properties.



11. Do the same thing for Other Gateways
12. Define your Peer IP in the following tab



The screenshot shows a network management interface. On the left, a table lists components: gw_cluster2 (10.10.120.43), ThreatEmulation (172.16.10.1), and Management (172.16.10.4). The ThreatEmulation component is highlighted. Below the table are tabs for Summary, Tasks, and Errors. The main area shows a tree view of services, with 'IPSec VPN' and 'Link Selection' highlighted. The right pane displays 'IP Selection by Remote Peer' settings, where 'Always use this IP address' is selected, and 'Main address' is chosen under 'Locally managed VPN peers determine this gateway's IP address using the following method:'.

13 . If you have not enabled “Accept Encrypted Traffic” in the step number 3. You need to create firewall rules.

No.	ie	Source	Destination	VPN	Services & Applicat...	Action	Track	Install On
1		* Any	* Any	* Any	FW1_topo	Drop	Log	* Policy...
2		10.10.20.0_vpn_subnet CP_default_Office_Mode_a...	CP_default_Office_Mode_... 10.10.20.0_vpn_subnet	vpn_for_ftp	ftp-pasv ftp-bidir ftp ftp-port tcp-high-ports	Accept	Log	Threa... gw_cl...
3	nup rule	10.10.20.0_vpn_subnet CP_default_Office_Mode_a...	CP_default_Office_Mode_... 10.10.20.0_vpn_subnet	* Any	* Any	Drop	Log	* Policy...

