

Configuring Check Point Security Gateway with VPN

Version 1.0

Dokument Name: Configuring Check Point Security Gateway with VPN



Dokumentenkontrolle

| Version | Datum | Änderungsnotiz | Betroffene Seiten | Status | Author |
|---------|------------|----------------|----------------------|--------|--------|
| 1.0 | 10.07.2024 | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Copyright 2024 NetWyl Informatik

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



Note: If you have a fresh installed Check Point Gateway that is also defined as Security Management server and should be used as a VPN Gateway, start from step 6. In most cases this Gateway has the icon and is named "gw-". To create Check Point Security Gateway:

1. Click * New, go to More ->Network Object -> Gateways and Servers -> Gateway:



2. Click Wizard Mode



| Check Point Security Gateway Creation 📀 🛛 🗙 | | | | | | |
|---|-------------------|--|--|--|--|--|
| Create the Check Point Securi | ty Gateway using: | | | | | |
| Wizard Mode | Classic Mode | | | | | |
| Don't show this again | | | | | | |

- 3. Enter
- 4. Gateway name
- 5. Gateway platform
- 6. IP address



| Check Point Ga | ateway Instal | llation Wizard | |
|----------------|---------------|----------------|--|
|----------------|---------------|----------------|--|

| General Properties Specify the Gateway name, platform and IP address. • General Properties • Trusted Communication • Blade Activation • End Gateway IP address: | |
|---|--|
| ▶ General Properties Gateway name: my-vpn-gw ■ Trusted Communication Blade Activation Gateway platform: Øpen server ■ End Gateway IP address: Gateway IP address: | |
| Static IP address: IPv4: 172.23.34.190 <u>R</u> esolve from Name IPv6: Dynamic IP address (e.g. assigned by DHCP server) | |
| | |

7. Click Next and enter the one-time password as defined on Check Point Security Gateway during installation.

| Check Point Gateway Installat | ion Wizard | | ? | \times |
|--|--|---|-----|----------|
| Secure Internal | Communication Initializat Internal Communication. | ion | | |
| General Properties Trusted Communication End | Initiate trusted communication Enter an one-time password the Internal Communication betwee Management Server. This one-time password must be in the 'Secure Internal Commu- configured the Check Point secure Gateway's Name: One-time password: Trust State: Skip and initiate trusted commu- | now. hat will be used to initialize the Secure en the gateway my-vpn-gw and the Security be the same one-time password you entered nication' tab when you installed and iftware on the gateway my-vpn-gw. my-vpn-gw Uninitialized unication later | | |
| Check Point" | | < Back Next > | Can | cel |

- 8. Click Next after trusted communication established, then click Finish.
- 9. In the General Properties window of your Security Gateway, make sure the 'IPSec VPN' checkbox is selected.



| Check Point Gateway - my-vp | on-gw 📀 🛛 🗙 |
|---|---|
| General Properties NAT HTTPS Inspection HTTP/HTTPS Proxy HTTP/HTTPS Proxy Comparison HITP/HTTPS Proxy Platform Portal Mail Transfer Agent Platform Portal Mail Transfer Agent Platform Portal Mail Transfer Agent Comparison Platform Portal Mail Transfer Agent Comparison HIT Count Conter Other | Machine Name: my-vpn-gw Color: Black IPv4 Address: IPv6 Address: Dynamic Address IPv6 Address: Comment: Communication: Trust established Communication Platform Communication: Trust established Communication Platform Markive: Open server Version: R80.40 OS: Gaia Get Network Security (2) Threat Prevention (0) Management (0) Get Get Network Security (2) Threat Prevention (0) Management (0) Get Access Control: Opnamic Routing Dynamic Routing SecureXL Ops Policy Server Opsic Server Optication Control Other: Optications IVEL Filtering Optications Other: Optications Anti-Spam & Email Security Identity Awareness Ontent Awareness Optications for organizations' email Motiversemail Mathicspam & Email Security Comprehensive and multidimensional protection for organizations' email Get |
| | infrastructure. Opdates are included. |
| | OK Cancel |

10. Define VPN encryption domain for your Gateway. Make sure that you have at least one internal and one external interfaces.

| Check Point Gateway - my-vpn-gw | ? | × |
|--|---|---|
| General Properties Network Management System Backup VPN Domain Proxy NAT Advanced HTTP Inspection HTTP/HTTPS Proxy CA Search Get Interfaces With Topology Comments Get Interfaces Without Topology Comments Get Interfaces Without Topology Comments C | | |

VPN encryption domain will be defined to all networks behind internal interface.



| Check Point Gateway - my | ? × | |
|---|--|------|
| General Properties | VPN Domain All IP Addresses behind Gateway based on Topology information | |
| ··· Proxy | O User defined | View |
| - Advanced - HTTPS Inspection - HTTP/HTTPS Proxy - ICAP Server | Set Specific VPN Domain for Gateway Communities: Set | |
| Platform Portal Mail Transfer Agent IPSec VPN | | |

11. Click Accept

| t Topology Re | sults | | |
|--|--|---|-----------------------------|
| The following tab Networks (or a gr | le shows every interface fo oup of them) that reside be | ound for the given mac ehind each interface an | hine. e also shown here. |
| Name | IPv4 Address | IPV4 Netmask | IPv6 Address |
| <u>⊡</u> ∽ eth0 | 172.23.34.190 | 255.255.255.0 | 2620:0:2a03:82: |
| <u>⊡</u> ∽ eth1 | 10.15.15.1 | 255.255.255.0 | fc00::2:1/120 |
| 4 | | | |
| egend | | | · |
| New object v | vas created. | | |
| Existing object | t was used. | | |

- 12. Click OK and close the Gateway dialog Configuring the Interoperable Device and VPN community Create an object to represent the peer gateway.
- 13. In New, go to Network Objects -> More -> Interoperable Device



| Check Point Smart Console Search Console Search Console Search Console Search Console Search Network Host | | | | | | |
|---|--|---|---|-------------|---|--|
| Network Group | | | | | | |
| Networks Hosts Hosts Groups 1 Address Ranges 4 Dynamic Objects 6 Security Zones 5< ♥ Domains 1 | Network Object Service Custom Application/Site IoT Discovery Service VPN Community Data Type User Server Resource Time UserCheck LSM Profile Limit | b | Gateways and Servers Network Host Group Address Range Dynamic Objects Wildcard Object Security Zone LSV Profile | F F F | Interoperable Device Domain VoIP Domain ▶ Logical Server OSE Device Access Point Name | |

14. Give the gateway a name, IP address, and (optional) description in the properties dialog window that is displayed and click OK.

| Interoperable Device - remo | te-vpn-peer | 🕑 🛛 🗙 |
|--|--|-------|
| General Properties Topology ⊕- IPSec VPN | Machine Name: remote-vpn-peer Color: Black IPv4 Address: 172.23.34.200 Resolve from Name Dynamic Address IPv6 Address: | < > |
| | Products: | |

15. In Access Tools, go to VPN Communities. Click * on the top panel and select Meshed Community.



| ⊡ : • | 🗊 Objects 🕶 😍 Install Policy | | 🌐 Discard Session 👻 🧐 🐊 Publish |
|-----------------------|--------------------------------|---|-------------------------------------|
| | Corporate_Policy + | | |
| | ** • Access Control | VPN Communities | * • • × Q Search |
| GATEWAYS & SERVERS | Policy | Name | ▲ Topol |
| | NAT | 🗱 MyIntranet | Meshe |
| | - Threat Prevention | Partner Access to Corporate's Data Cent | er LAN Meshed Custom |
| SECURITY POLICIES | Policy | RemoteAccess | Remote Access Custom |
| | Exceptions | Site2Site | Mesnea Custom |
| \sim | - HTTPS Inspection | | |
| LOGS & MONITOR | Policy | | |
| MANAGE & SETTINGS | Shared Policies | | |
| | | 🗱 MyIntranet | |
| | Access Tools | Participating Gateways | ncryption |
| | - Werd Communities | Pł | nase 1: |

16. A Meshed Community Properties dialog pops up. In the General menu, enter your VPN community name

In the Participating Gateways menu click: Add, select your both gateways objects, and click OK.

| Meshed Community | | ୍ |
|--|---|--|
| Site25 Enter Oby | SiteVPN ject Comment | |
| 44 Gateways Encrypted Traffic Encryption | Participating Gateways All the connections between the VPN Dor + \ X | mains of the gateways below will be encrypted. Q <i>Search</i> |
| Tunnel Management Excluded Services Shared Secret Wire Mode | Gateway A Gateway Image: Second seco | ay Comments VPN Domain All IP addresses behind gateway based on topo All IP addresses behind gateway based on topo |
| Advanced | | OK Cancel |

17. In the Encryption menu, you can change the Phase 1 and Phase 2 properties. You can also define which IKE version should be used. For IKEv1 leave the default, for IKEv2 select IKEv2 only.



| Meshed Community | ୍ 🔞 | × |
|---|--|---|
| Site2S Enter Oby | iteVPN ect Comment | |
| " Gateways Encrypted Traffic Encryption Turned Management | Encryption Method Encryption Method: IKEv1 for IPv4 and IKEv2 for IPv6 only • Encryption Suite | |
| Excluded Services | Use this encryption suite: Suite-B-GCM-256 (AES-GCM-256, SHA-384, EC Di Custom encryption suite: IKE Security Association (Phase 1) | |
| Wire Mode Advanced | Encryption Algorithm: AES-256 Data Integrity: SHA1 Diffie-Hellman group: Group 2 (1024 bit) IKE Security Association (Phase 2) | |
| | Encryption Algorithm:AES-128Data Integrity:SHA1 | |
| | More IKE Security Association (Phase 1) Use aggressive mode IKE Security Association (Phase 2) Use Perfect Forward Secrecy Diffie-Hellman group: Group 2 (1024 bit) Support IP Compression Add Tag | |
| | OK Cancel | |



Meshed Community

| Site2S Enter Obj | SiteVPN ject Comment |
|---|--|
| 44 Gateways Encrypted Traffic Encryption | Encryption Method Encryption Method: IKEv1 for IPv4 and IKEv2 for IPv6 only |
| Tunnel Management Excluded Services | Encryption Suite Use this encryption suite: Suite-B-GCM-256 (AES-GCM-256, SHA-384, EC Di * Custom encryption suite: |
| Shared Secret Wire Mode Advanced | IKE Security Association (Phase 1) Encryption Algorithm: AES-256 Data Integrity: SHA1 Diffie-Hellman group: Group 2 (1024 bit) |
| | IKE Security Association (Phase 2) Encryption Algorithm: AES-128 Data Integrity: SHA1 |
| | More IKE Security Association (Phase 1) Use aggressive mode |
| | IKE Security Association (Phase 2) Use Perfect Forward Secrecy Diffie-Hellman group: Group 2 (1024 bit) |
| | Support IP Compression Add Tag |
| | OK Cancel |

Note: Make a note of the values you select in order to set the peer to match them

- 18. In the Tunnel Management menu you can define how to setup the tunnel.Note: The recommended tunnel sharing method is one VPN tunnel per subnet pair (default). This shares your network on either side of the VPN and makes the Phase 2 negotiation smooth. It also requires fewer tunnels to be built for the VPN. If you need to restrict access over the VPN, you can do that later through your security Rule Base.
- For preshered authentication, expand the Advanced Settings menu and select: Shared Secret.

Select the 'Use only Shared Secret for all External members' checkbox.

Select your peer gateway from the entries in the list below and click Edit to edit the shared secret.Note: remember this secret, as your peer will need it to set up the VPN on the other end.



| Meshed Community | ୍ ହ ା × |
|--|--|
| Site2S Enter Obj | iteVPN iect Comment |
| Gateways Encrypted Traffic Encryption Tunnel Management Excluded Services Shared Secret | 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 remote-vpn-peer |
| Wire Mode Advanced | Add Tag OK Cancel |

20. Expand the Advanced Settings menu and select: Advanced VPN Properties. Here, you can modify the more advanced settings regarding Phase 1 and 2.Note: Keep note of the values used. It is also a good idea to select:

Disable NAT inside the VPN community so you can access resources behind your peer gateway using their real IP addresses, and vice versa.

21. Click OK on the VPN community properties dialog to exit back to the SmartDashboard. You may see the following message:

| SmartConsol | e | × |
|-------------|---|---|
| | Not all externally managed gateways have shared secret defined. Do you wish to save the changes anyway? | |
| | Yes No | |

22. We are about to address the VPN domain setup in the next section, so click Yes to continue.

Now you can see your VPN community defined:



| VPN Communities | ★ - ▲ Q Search | | | | |
|---|--|------------------|----------|--|--|
| Name 🔺 | Topology | Encryption Suite | Comments | | |
| **** MyIntranet | Meshed | Custom | | | |
| Partner Access to Corporate's Data Center LAN | Meshed | Custom | | | |
| ‡ ²² Ω RemoteAccess | Remote Access | Custom | | | |
| 👯 Site2Site | Meshed | Custom | | | |
| Site2SiteVPN | Meshed | Custom | | | |

Defining VPN encryption domain for Interoperable Device

You now need to define your VPN encryption domains.

If you have not already done so, create network objects to represent your local networks and the peer networks they will be sharing with you.

To define VPN encryption domains:

23. From the Network Objects menu, right click on Networks and select Network to define a new network. In the following image, we are creating a network to represent our peer's internal network that they will be sharing with Check Point VPN gateway:



| Network Properties - r | emote-peer-internal-network | | ? X |
|--------------------------|------------------------------|--------------|--------|
| General NAT | | | |
| <u>N</u> ame: | remote-peer-internal-network | Color: Black | - |
| <u>C</u> omment: | | | |
| IPv4 | | | - |
| Network <u>A</u> ddress: | 192.168.1.0 | | |
| Net <u>M</u> ask: | 255.255.255.0 | | |
| Broadcast address | | | |
| Included | | | |
| Not included | 1 | | |
| IPv6 | | | _ |
| Network <u>A</u> ddress: | | / | |
| | | | |
| | | | |
| | | ОК | Cancel |

24. If you or your peer is sharing more than one network over the tunnel, create groups to represent each side's VPN domain. From the Network Objects menu, right click on Groups, select Groups and then Simple Group...In this example, only one network is shared, so the group will have only one object included, but you can put as many networks in this group as you want to share.

Note: it is important not to add groups within a group as this can impact performance. Make sure the group is "flat".

Give your group a meaningful name such as: Local_VPN_Domain.

Click OK once you have added all of your local networks and then repeat the procedure to create a group to represent your peer's shared networks.

25. Open the properties for the peer gateway and select the group/network that represents its VPN domain:



| | Interoperable Device - remo | ote-vpn-peer |
|--|---|---|
| | General Properties Topology ⊕ IPSec VPN | Topology Type to Search Q Image: Colspan="2">New Image: Colspan="2">Search Actions Name Network IPv4 Address IPv4 Netmask IPv6 Address Topology |
| | | |
| | | VPN Domain |
| <mark>+</mark> € € 8 8 | | Manually defined |
| Network Objects Check Point Codes Check Point Codes Check Point Ch | | |
| | | OK Cancel |

26. Click OK to complete the peer gateway configuration.

Creating a rule for the traffic

Now, you have both objects set up for VPN and you have defined your community. All that is left is to create a rule for the traffic.

Here is where you should restrict access if it is required.

To create a rule for the traffic:

27. To allow VPN traffic, you should add the relevant rules to your Firewall Rule Base. Navigate Rule Base, Firewall -> Policy

| | 28. | | | | | | | |
|---|----------|-----------------------------|------|--|------------|----------------------|-------------------------------------|---|
| E | • • • | C 🗄 🗶 🛃 🕒 🛚 | ista | ll Policy 💦 💭 Smar | tConsole - | | | |
| I | Firewall | Application & URL Filtering | Č | Data Loss Prevention | U IPS | Threat Prevention | Anti-Spam & Mail | 5 |
| | Overview | | ¢ | Policy | | | | |
| Ч | | | | No. Hits | Name | Source | Destination | V |
| | | | _ | 1 💷 17K | | 🚼 Any | 🚼 Any | * |
| | Policy | | | No. Hits 1 17K | Name | Source Any | Destination Any | V |



- **28.** Decide where in your rule base you need to add your VPN access rule and right click the number on the rule just above where you want it and select: Add Rule -> Below.
- **29.** You should explicitly set the VPN community in the VPN column on your rule, you have created before.

In the VPN column, right-click the Any Traffic icon and select: Edit Cell....



Select the: Only connections encrypted in specific VPN Communities option button and click Add. Select the VPN community created in the above steps and click OK and then OK again.

| VPN Match Conditions | | | | | | |
|--|--|--|--|--|--|--|
| Match conditions | | | | | | |
| Any connections, whether Clear or Encrypted | | | | | | |
| Only connections encrypted in any Site-to-Site VPN Community | | | | | | |
| Only connections encrypted in specific VPN Communities | | | | | | |
| Site2SiteVPN | | | | | | |
| Add Remove | | | | | | |
| For a typical example of usage of the VPN column, please see Help. | | | | | | |
| OK Cancel Help | | | | | | |



30. In this example, we are allowing any service/any host across the tunnel in both directions. Your rule should now show the VPN community in the VPN column:

| No. | Hits | Name | Source | Destination | VPN | Service | Action | Track | Install On | Time |
|-----|-----------------|--------------------|--------|-------------|---------------|---------|----------|--------|------------------|-------|
| 1 | ─ ── 17K | Site2Site VPN rule | 法 Any | 🗶 Any | Site2SiteVPN | 法 Any | 🕜 accept | 🖹 Log | 🖈 Policy Targets | 🖈 Any |
| 2 | 0 | | 法 Any | 法 Any | 密 Any Traffic | 法 Any | 🔘 drop | - None | 🖈 Policy Targets | 法 Any |

Completing the procedure

- **31.** Install the policy to your local Check Point gateway.
- **32.** Once the remote side has setup their VPN to match, verify that you have secure communication with their site.

Troubleshooting

1. Problem: Traffic is dropped by 3rd party gateway and main IP configuration was defined to internal IP address for Check Point Gateway.

Generally, it is recommended to define main gateway IP address with external IP (in Check Point Gateway – General Properties). In some cases, for example: StandAlone gateway, administrator wants to define main IP address as internal IP in order to allow managing from internal network.

In this case, VPN link selection should be changed.

Open Check Point gateway properties dialog, select IPSec VPN -> Link Selection and click Source IP address settings...

In opened dialog, select Selected address from topology table and select relevant external IP address, used by remote peer



| Check Point Gateway - my-v | pn-gw | 2 X |
|---|--|---|
| General Properties General Properties Topology AT HTTPS Inspection HTTP/HTTPS Proxy Platform Portal FISEc VPN Fisc VPN Clients Fisch Policy Optimizations Ht Count Other | Link Selection IP Selection by Remote Peer — Locally managed VPN peers of Always use this IP address Always use this IP address settings. Always use this IP address settings Always use this IP address settings Always use this IP address settings Always use this IP address A | determine this gateway's IP address using the following method: m topology table: Link Selection - Source IP Address Settings When initiating a tunnel use the following IP address as the source IP of outgoing packets: Automatic (derived from method of IP selection by remote peer) Main IP address Selected address from topology table: Main IP address Selected address of chosen interface K Cancel Help Mone None |
| | | OK Cancel |

2. Problem: IKE keys were created successfully, but there is no IPsec traffic (relevant for IKEv2 only).

In some cases, remote peer chooses NAT-T encapsulation but Check Point gateway sends traffic without this encapsulation. As a result, a remote peer drops the IPsec traffic since it expecting NAT-T.

There are two workarounds available to resolve this problem:

33. If IKEv2 is required by remote peer, NAT-T should be disabled.

To do so, open Check Point gateway properties dialog, select IPSec VPN -> VPN Advanced and clear 'Support NAT traversal (applies to Remote Access and Site to Site connections)' checkbox:

Configuring Check Point Security Gateway with VPN



| Check Point Gateway - my-v | /pn-gw | | | - 844 | R. Anna Search | ? X |
|--|--|------------|---------|-------|----------------|--------|
| ···· General Properties | VPN Advanced | | | | | |
| Topology NAT HTTPS Inspection HTTP/HTTPS Proxy Platform Portal IPSec VPN Link Selection VPN Advanced VPN Clients Logs Each Palier; | VPN Tunnel Sharing | | | | | |
| | Control the number of VPN tunnels opened between peer Gateways | | | | | |
| | Use the <u>c</u> ommunity settings | | | | | |
| | Custo <u>m</u> settings | | | | | |
| | One VPN tunnel per each pair of <u>h</u> osts | | | | | |
| | One VPN tunnel per <u>s</u> ubnet pair | | | | | |
| ···· Optimizations | One VPN tunnel per Gateway pair | | | | | |
| i⊷ Hit Count ⊛- Other | Restart Options | | | | | |
| | Perform an organized shutdown of tunnels upon gateway restart | | | | | |
| | Wire mode | | | | | |
| | Support Wire mode (and Wire mode routing - route uninspected encrypted traffic in VPN routing configurations) | | | | | |
| | Select the interfaces where traffic destined to Wire mode communities will | | | | | |
| | bypass the Filewall | | | | | |
| | Name | IP Address | Netmask | | | |
| | | | | | | |
| | | | | | | |
| | | Perrena | | | | |
| | | | | | | |
| | | | | | | |
| | NAT traversal (industry standard) | | | | | |
| | Support NAT traversal (applies to Remote Access and Site to Site connections) | | | | | |
| | | | | | | |
| | | | | | | Cancel |
| | | | | | | Cancer |