Configuring Route-Based VPNs

This document describes how to configure a route-based VPN between the following:

- Two Check Point Embedded NGX gateways
- An Embedded NGX gateway and a Check Point VPN-1 Pro NGX gateway, using Check Point SmartCenter R60 and above, with or without the Check Point SmartLSM extension

**Note:** Embedded NGX gateways include VPN-1 Edge gateways. Route-based VPN between VPN-1 Edge gateways and Nokia IP40 gateways is not supported.

**Note:** This document assumes the reader is familiar with the basic concepts of working with Check Point SmartCenter.

**Introduction**

You can improve network and VPN management efficiency for large networks by configuring route-based VPNs. Route-based VPNs allow routing connections over VPN tunnels, so that remote VPN sites can participate in dynamic or static routing schemes.

A static routing scheme requires configuring static routes for packets originating in a certain subnet and/or destined for a certain subnet. Since such schemes require reconfiguring the static routes each time the network topology changes, they are mainly suitable for small or relatively unchanging networks.

The advantage of using a route-based VPN with static routes over a “traditional” VPN is that the VPN tunnel operates as a regular operating system (OS) interface; this means that the VPN tunnel is taken into consideration in routing decisions, as interfaces go up and down. You can influence routing decisions by assigning a "cost" for each route. The Embedded NGX appliance always routes packets through the lowest cost next hop.

For example, if a company has a frame relay line running over one Internet connection (WAN2) and a route-based VPN (VTI1) running over another Internet connection (WAN), then the company can configure two static routes to their headquarters (HQ): one through the frame relay line (WAN2), and one through the VPN (VTI1). If the cost of the route through WAN2 is 10, and the cost of the route through VTI1 is 20, then normally traffic to the HQ will go through WAN2. If WAN2 fails, then traffic will go through VTI1, and when WAN2 recovers, traffic will go through WAN2 once again.
For constantly changing networks, it is recommended to use a route-based VPN combined with an OSPF (Open Shortest Path First) dynamic routing scheme. OSPF distributes routing information between routers in a single autonomous system (AS). Each router in the AS distributes its local state (that is, the router’s usable interfaces and reachable neighbors) to the other routers in the AS, and uses the link-state advertisements of the other routers to build and maintain a database describing the entire AS topology. Therefore, whenever you make a change to the network topology, such as by adding an internal network, the routers are automatically updated with all changes to the network topology.

Using route-based VPN with OSPF dynamic routing schemes has the same advantages as route-based VPN with static routing schemes. However, while the failure detection capabilities in static routing schemes are limited to detecting the availability of the next hop gateway, these capabilities are greater in dynamic routing schemes: whenever a router anywhere in the network fails, even a router several hops away, the failure is quickly detected, and the routing tables are updated to route around the failure through the next best (shortest) open path, if one exists. OSPF is a standard protocol, so your dynamic routing scheme can include both Check Point and non-Check Point routers in your organization.

**Note:** Embedded NGX appliances and SmartCenter support OSPF version 2.

This document includes information on configuring route-based VPNs for both static routing schemes and OSPF dynamic routing schemes.

**Configuring Route-Based VPNs between Embedded NGX Gateways**

**Overview**

To configure a route-based VPN:

1. On each gateway, add the other gateway as a VPN site. For example, on gateway A, add gateway B as a VPN site; on gateway B, add gateway A as a VPN site. See “Adding a VPN Site,” page 2.

2. Do one of the following:

   - To work with a static routing scheme, on each gateway, add a static route to the network behind the other gateway. See “Adding Static Routes,” page 5.
   - To work with an OSPF dynamic routing scheme, on each gateway, configure OSPF. See “Configuring OSPF on Gateways,” page 7.

**Adding a VPN Site**

To add a VPN site:

1. Click **VPN** in the main menu, and click the **VPN Sites** tab. The **VPN Sites** page appears with a list of VPN sites.
2. Click New Site. The VPN-1 Edge VPN Site Wizard opens, with the Welcome to the VPN Site Wizard dialog box displayed.

3. Click Site-to-Site VPN.

4. Click Next. The VPN Gateway Address dialog box appears.
5. Complete the fields as desired. Refer to the User Guide for information.
6. Click Next.
   The VPN Network Configuration dialog box appears.

7. Click Route Based VPN.
8. Click Next. The Route Based VPN dialog box appears.
9. In the **Tunnel Local IP** field, type a local IP address for this end of the VPN tunnel. This must be unique for each VPN site.

   The tunnel local IP address that you configure on gateway A will be the tunnel **remote** IP address on gateway B. For example, if you configure the local IP address on gateway A as 192.168.10.10, then you must configure the **remote** IP address on gateway B as 192.168.10.10.

10. In the **Tunnel Remote IP** field, type the IP address of the remote end of the VPN tunnel. This is the VPN site's VTI (Virtual Tunnel Interface). This must be unique for each VPN site.

   The tunnel remote IP address that you configure on gateway A will be the tunnel **local** IP address on gateway B. For example, if you configure the remote IP address on gateway A as 192.168.10.20, then you must configure the **local** IP address on gateway B as 192.168.10.20.

11. To use OSPF dynamic routing, in the **OSPF Cost** field, type the cost of this link for dynamic routing purposes. OSPF always prefers to send traffic through routes with the lowest cost. The default value is 10.

12. Click **Next**.

13. Complete the wizard as desired. Refer to the User Guide for information. The **VPN Sites** page reappears displaying the new site.

### Adding Static Routes

If you want to use a static routing scheme, you must create static routes to specify which traffic should be sent through the VTI that you configured in “Adding a VPN Site,” page 2.

Alternatively, you can configure OSPF using the procedure “Configuring OSPF on Gateways,” page 7.

**To add a static route:**

1. Click **Network** in the main menu, and click the **Routes** tab. The **Static Routes** page appears, with a list of existing static routes.
2. Click New Route.
   The Static Route Wizard opens displaying the Step 1: Source and Destination dialog box.

3. In the Source drop-down list, select **ANY**.
5. In the **Network** field, type the IP address of the remote network.
6. In the **Netmask** drop-down list, select the subnet mask.
7. Click **Next**. The **Step 2: Next Hop and Metric** dialog box appears.

8. In the **Next Hop IP** field, type the IP address to which to route the packets destined for the remote network. This is the remote network's VTI (Virtual Tunnel Interface) that you configured in “Adding a VPN Site,” page 2.
9. In the **Metric** field, type the static route's metric. The gateway sends a packet to the route that matches the packet's destination and has the lowest metric. The default value is 10.
10. Click **Next**. The **Routes** page reappears displaying the new static route.

**Configuring OSPF on Gateways**

If you want to use an OSPF dynamic routing scheme, you must configure OSPF on the gateways. Configuring OSPF is done via CLI commands. You can run the necessary commands by using the Embedded NGX Portal's command line interface or by using the SSH (Secure Shell) management protocol. For information, refer to the *Embedded NGX CLI Reference Guide*.

Alternatively, you can configure a static routing scheme using the procedure “Adding Static Routes,” page 5.
To configure OSPF

1. Enable OSPF by entering the following command:
   
   ```
   set ospf mode internal
   ```

2. Publish the local network IP address, subnet mask, and OSPF area by entering the following command:

   ```
   add ospf network address address mask mask area area
   ```

   where:
   
   - **address**: The local network's IP address.
   - **mask**: The local network's subnet mask.
   - **area**: The OSPF area's IP address.

   For example:

   ```
   add ospf network address 192.168.20.0 mask 255.255.255.0 area 0.0.0.0
   ```

3. Publish the local VTI by entering the following command:

   ```
   add ospf network address address mask mask area area
   ```

   where:
   
   - **address**: The local VTI's IP address.
   - **mask**: The local VTI's subnet mask.
   - **area**: The OSPF area's IP address.

   For example:

   ```
   add ospf network address 1.1.1.1 mask 0.0.0.0 area 0.0.0.0
   ```

4. To verify that OSPF is configured correctly, enter the following commands:

   - `info ospf neighbor`
   - `info ospf routes`

   Information about the OSPF neighbors and routers appears.

   **Note**: Embedded NGX gateways support several additional commands for configuring OSPF. For information, refer to the *Embedded NGX CLI Reference Guide*.

### Configuring Route-Based VPNs between an Embedded NGX Gateway and a VPN-1 Pro NGX Gateway

#### Overview

The method used to configure a route-based VPN depends on whether the Embedded NGX gateway is managed by SmartCenter or externally managed.
Configuring Route-Based VPNs between an Externally Managed Gateway and a VPN-1 Pro NGX Gateway

To configure a route-based VPN:

1. Prepare SmartCenter for route-based VPN, by doing the following:
   a. Create a gateway object for the Embedded NGX gateway. For information, refer to SmartCenter documentation.
   
   ![Note: In the General Properties tab, you must select the Externally Managed Gateway check box.](image)
   
   b. Configure the gateway's VPN settings. See “Configuring Embedded NGX Gateways' VPN Settings,” page 11.
   c. Create a Meshed or Star community. For information, refer to SmartCenter documentation.
   d. Add the gateway object to the community you created. For information, refer to SmartCenter documentation.
   e. To work with an OSPF dynamic routing scheme, configure OSPF on the VPN-1 Pro NGX gateway. See “Configuring OSPF on the VPN-1 Pro NGX Gateway,” page 11.

2. Prepare the Embedded NGX gateway for route-based VPN, by doing the following:
   a. Add SmartCenter as a VPN site. See “Adding a VPN Site,” page 2.
   b. Do one of the following:
      - To work with a static routing scheme, add a static route to the network behind the VPN-1 Pro NGX gateway. See “Adding Static Routes,” page 5.
      - To work with an OSPF dynamic routing scheme, configure OSPF. See “Configuring OSPF on Gateways,” page 7.

Configuring Route-Based VPNs between a SmartCenter-Managed Gateway and a VPN-1 Pro NGX Gateway

![Note: This procedure is relevant for Embedded NGX gateways with firmware version 6.0.53 and above.](image)
To configure a route-based VPN:

1. Prepare SmartCenter for route-based VPN, by doing the following:
   a. Create a gateway object for the Embedded NGX gateway.
      For information, refer to SmartCenter documentation.
   b. Configure the gateway's VPN settings.
      See “Configuring Embedded NGX Gateways' VPN Settings,” page 11.
   c. Create a Meshed or Star community.
      For information, refer to SmartCenter documentation.
   d. Add the gateway object to the community you created.
      For information, refer to SmartCenter documentation.
   e. To work with an OSPF dynamic routing scheme, configure OSPF on the VPN-1 Pro
      NGX gateway.
      See “Configuring OSPF on the VPN-1 Pro NGX Gateway,” page 11.

2. Connect the Embedded NGX gateway to SmartCenter. For information, refer to "Connecting
   to a Service Center" in the User Guide.

3. Configure route-based VPN on the Embedded NGX gateway object in SmartCenter, by doing
   the following:
   a. Create a CLI script that adds the VPN-1 Pro NGX gateway as a VPN site and
      includes the relevant OSPF or static route settings.
      The script must also include the following command that disables the Enterprise
      VPN site:

      ```
      set vpn enterprise-site disabled true
      ```

      **Note:** This command is available from Embedded NGX version 6.5. If
you are using version 6.0, you must disable the Enterprise VPN site
locally. For information, refer to "Enabling/Disabling a VPN Site" in
the User Guide.

For example, the following script configures route-based VPN with an OSPF
dynamic routing scheme. The first command adds SmartCenter as a VPN site, the
second command sets the OSPF mode, the third command sets the internal
network behind the Embedded NGX gateway, the fourth command sets the
Embedded NGX local VTI, and the final command disables the Enterprise VPN
site.

```sql
set vpn enterprise-site disabled true
clear vpn sites
add vpn sites disabled false name OSPF_vpn gateway 212.150.8.72
gateway2undefined loginmode automatic configmode routebased authmethod sharedsecret typesitesite keepalive disabled bypassnat enabled bypassfw enabled user """"password {S}nS43OjEmNyA= toopass """" net1 undefined netmask1 undefined net2undefined netmask2 undefined net3 undefined netmask3 undefined usepfs falsephaseslikealgs automatic phase1exptime 1440 phase1dhgroup automatic phase2ikealgsautomatic phase2exptime 3600 phase2dhgroup automatic dnsname
```
212.150.8.72vtilocalip 1.1.1.1 vtiremoteip 2.2.2.2
set ospf mode internal
set ospf router-id 10
clear ospf network
add ospf network address 192.168.20.0 mask 255.255.255.0 area 0.0.0.0
add ospf network address 1.1.1.1 mask 255.255.255.255 area 0.0.0.0

The following script configures route-based VPN with a static routing scheme. The first command adds SmartCenter as a VPN site, the second command adds a static route to the VPN-1 Pro NGX gateway, and the final command disables the Enterprise VPN site.

| set vpn enterprise-site disabled true |
| clear vpn sites |
| add vpn sites disabled false name OSPF_vpn gateway 212.150.8.72 gateway2undefined loginmode automatic configmode routebased authmethod sharedsecret typesitetosite keepalive disabled bypassnat enabled bypassfw enabled user ""password {S}nS43OjEmNyA= topopass "" net1 undefined netmask1 undefined net2undefined netmask2 undefined net3 undefined netmask3 undefined usepfs falsephaseslikealgs automatic phase1exptime 1440 phase1dhgroup automatic phase2ikealgsautomatic phase2exptime 3600 phase2dhgroup automatic dnsname 212.150.8.72vtilocalip 1.1.1.1 vtiremoteip 2.2.2.2 |
| clear routes |
| add route network 192.168.10.0 mask 255.255.255.0 gateway 2.2.2.2 |

For information on the relevant CLI commands, refer to the *Embedded NGX CLI Reference Guide.*

b. Add the script to the gateway object. See “Adding CLI Scripts to Embedded NGX Gateways,” page 13.

**Configuring Embedded NGX Gateways' VPN Settings**

**To configure Embedded NGX gateway VPN settings:**

1. In SmartDashboard, double-click the desired gateway object. The VPN-1 Edge/Embedded Gateway dialog box appears displaying the **General Properties** tab.
2. Select the **VPN Enabled** check box.
3. Click **Connects as Site To Site Gateway**.
4. Complete the rest of the fields as desired. For information, refer to SmartCenter documentation.
5. Click **OK**.

**Configuring OSPF on the VPN-1 Pro NGX Gateway**

To configure OSPF:

1. In the VPN-1 Pro NGX gateway, create the VTI on the VPN-1 Pro NGX gateway, by entering the following commands:

```bash
vpn shell
interface
add
numbered
numbered localIP remoteIP peerName
```

Where:

- `localIP` The VPN-1 Pro NGX gateway IP address.
- `remoteIP` The gateway's IP address.
peerName The gateway object's name.

For example, the last command might be:

```
numbered 2.2.2.2 1.1.1.1 edge_ospf
```

2. Enable OSPF by entering the following commands:

```
router
enable
configure terminal
router ospf routerName
```

where:

```
routerName The name of the OSPF router.
```

For example:

```
router ospf 100
```

3. Publish the local network IP address, subnet mask, and OSPF area by entering the following command:

```
network address mask area
```

Where:

```
address The local network's IP address.
mask The local network's subnet mask.
area The OSPF area's IP address.
```

For example:

```
network 192.168.200.0 0.0.0.255 area 0.0.0.0
```

4. Publish the VTI by entering the following command: `network address mask area`

where:

```
address The Peer VTI's IP address
mask Should be set to 0.0.0.0
area The OSPF area's IP address.
```

For example:

```
network 1.1.1.1 0.0.0.0 area 0.0.0.0
```

**Adding CLI Scripts to Embedded NGX Gateways**

To add a CLI script to a Embedded NGX gateway:

1. In SmartDashboard, double-click the desired gateway object. The VPN-1 Edge/Embedded Gateway dialog box appears displaying the General Properties tab.
2. Click the **Advanced** tab. The **Advanced** tab appears.
3. Copy the prepared CLI script and paste it into the **Configuration Script** text box.
4. Click **OK**.