How To Set up a Site-to-Site VPN with Overlapping Networks Using Check Point 600 Series Appliances
Objective

This document explains how to allow VPN communication between hosts on networks that have overlapping IP ranges.

Details

Supported Versions

R75.20.50 and later

Supported OS

Gaia embedded

Supported Appliances

600 and 1100 (locally managed)

Before You Start

Related Documentation and Assumed Knowledge

- 600 Appliance Administration Guide
- 1100 Appliance (locally managed) Administration Guide
- R7x VPN Administration Guide
- R7x Release Notes

Impact on the Environment and Warnings

- This configuration will require static NAT addresses for each host that will require access.
- This will not enable full communication between entire subnets.
- The examples in this guide use two 600 series appliances, running R75.20.67.

Example Setup

In this guide, we use two 600 appliances, already configured to be Check Point firewalls. We call them: “600A” and “600B.”

Static NAT is required. This will hide the overlapping IP networks in the encryption domains.

For this example, we will translate HostA on 192.168.54.15 to 10.99.99.15, and HostB on 192.168.2.71 to 10.99.100.71.
Configuring Necessary Network Objects

This setup requires a network object for the external NAT addresses. Create one network object to reflect two networks that do not really exist, external to the firewall.

Example:
- 10.99.2.71 will belong to the 10.99.2.0/24 network
- 0.99.100.71 will belong to the 10.99.100.0/24 network

Create these network objects in both firewalls:
- The host in the A network (HostA)
- The host in the B Network (HostB)
- The external NAT IP for the host in the A network (A_NAT)
- The external NAT IP for the host in the B network (B_NAT)
- The IP range of A's internal network (A_Net)
- The IP range of B's internal network (B_Net)
- The external NAT network for the A network (A_NAT_net)
- The external NAT network for the B network (B_NAT_net)

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Type</th>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHost</td>
<td>Single IP</td>
<td>192.168.54.15</td>
</tr>
<tr>
<td>BHost</td>
<td>Single IP</td>
<td>192.168.2.71</td>
</tr>
<tr>
<td>A_NAT</td>
<td>Single IP</td>
<td>10.99.90.15</td>
</tr>
<tr>
<td>B_NAT</td>
<td>Single IP</td>
<td>10.99.106.71</td>
</tr>
<tr>
<td>A_Net</td>
<td>Network</td>
<td>192.168.8.0/255.255.0.0</td>
</tr>
<tr>
<td>B_NAT_net</td>
<td>Network</td>
<td>10.99.108.0/255.255.255.0</td>
</tr>
<tr>
<td>A_NAT_net</td>
<td>Network</td>
<td>10.99.99.0/255.255.255.0</td>
</tr>
<tr>
<td>B_Net</td>
<td>Network</td>
<td>192.168.2.0/255.255.255.0</td>
</tr>
</tbody>
</table>

Manually Defining Encryption Domains

Define the local encryption domain for each firewall. This must include the actual internal network and the network used for external NAT.

Site to Site Local Encryption Domain

- Automatically determine local network topology
- Define local network topology manually

<table>
<thead>
<tr>
<th>Object Name</th>
<th>IP Addresses</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A_Net</td>
<td>192.168.0.0</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>A_NAT_net</td>
<td>10.99.99.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Configuring Static NAT

There must be a one-to-one static NAT for each pair of hosts. This setup requires two Static NAT rules for each pair of hosts (incoming and outgoing).

Example on 600A:

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Source</th>
<th>Original Destination</th>
<th>Original Service</th>
<th>Translated Source</th>
<th>Translated Destination</th>
<th>Translated Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>B_NAT</td>
<td>A_NAT</td>
<td>Any</td>
<td>Original</td>
<td>AHost</td>
<td>Original</td>
</tr>
<tr>
<td>2</td>
<td>AHost</td>
<td>B_NAT</td>
<td>Any</td>
<td>A_NAT</td>
<td>Original</td>
<td>Original</td>
</tr>
</tbody>
</table>

Example on 600B:

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Source</th>
<th>Original Destination</th>
<th>Original Service</th>
<th>Translated Source</th>
<th>Translated Destination</th>
<th>Translated Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BHost</td>
<td>A_NAT</td>
<td>Any</td>
<td>B_NAT</td>
<td>Original</td>
<td>Original</td>
</tr>
<tr>
<td>2</td>
<td>A_NAT</td>
<td>B_NAT</td>
<td>Any</td>
<td>Original</td>
<td>BHost</td>
<td>Original</td>
</tr>
</tbody>
</table>
Configuring Site to Site VPN

1. Make sure **Disable NAT** is not selected.
2. Make sure the remote encryption domain includes the external NAT IP range of the opposite firewall.
Configuring Access Policy

- If your firewall is configured in “strict” mode, create inbound and outbound access policies to allow the traffic to/from the VPN.
- If your firewall is configured in “standard” mode, by default, the traffic will be allowed based on the auto generated VPN site rule.

Depending on your environment and existing policies, the access policy may need fine-tuning to allow this VPN traffic.

Completing the Procedure

You can add additional hosts to this VPN network. Create more NAT rules.
Example: In network A, you can now add a host at 192.168.54.189, with STATIC NAT rules for translation from/to 10.99.99.189.

Verifying

To see that the new VPN and NAT are working properly, ping a host on the other end of the tunnel.
For example: ping 192.168.54.15 from the host at 192.168.2.71