Site to Site VPN’s between two networks with the same IP Address scheme.

Authored By: Elie Bitton
Creation Date: June 21, 2001
Revision Date: December 3rd, 2001
Purpose: Describe a configuration allowing an IPSEC tunnel to be established between two networks with the same IP scheme.
Product Class: Firewall-1, VPN-1
Product Version: CP 2000 4.1 (SP5) and Next Generation (NG) FP-1

Using NAT and IPSEC to tunnel between two networks with the same IP scheme.
© 2000 Check Point Software Technologies LTD.
Table of Contents

1 Introduction ............................................................................................................................ 3
2 Test Bed Layout ..................................................................................................................... 3
3 Firewall-A Setup .................................................................................................................. 4
3.1 Rules setup ....................................................................................................................... 4
3.2 NAT Setup ......................................................................................................................... 4
3.3 Encryption Domains ......................................................................................................... 7
3.4 ARP and Routing ............................................................................................................. 9
4 Firewall-B Setup .................................................................................................................. 10
4.1 Rules setup ....................................................................................................................... 10
4.2 NAT Setup ......................................................................................................................... 10
4.3 Encryption Domain ......................................................................................................... 13
4.4 ARP and Routing ............................................................................................................. 15
5 Test results .......................................................................................................................... 16
6 Conclusion ............................................................................................................................ 20
1 Introduction

The goal of this document is to show how to establish an IPSEC VPN between two sites with the same IP address scheme. For simplicity, a hub connects the external interfaces of the gateways. It assumes the reader has knowledge of VPN-1.

Most of the screens shown below are for CP 4.1, however, when using Check Point Next Generation, the setup of rules is the same however NAT rules must be automatic so that client side NAT can be enabled. If this is done correctly, no static routes are needed. The default settings in global properties were used for these tests for both 4.1 and NG. They were new installations (not upgrades) on a fresh OS install.

2 Test Bed Layout
3 Firewall-A Setup

3.1 Rules setup

For Check Point Next Generation (NG), the rules are the same.

3.2 NAT Setup

3.2.1 Using one to one
For Check Point NG, create an automatic NAT rule by going on the NAT tab of the 10.0.0.18 object and fill in the fields as follows:

![NAT Settings Screen](image)

The above action will yield the following Nat rules (rules 2 and 3):

<table>
<thead>
<tr>
<th>ID</th>
<th>Original Packet</th>
<th>Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image" alt="Net_10.0.0.0" /></td>
<td><img src="image" alt="Net_10.0.0.0" /></td>
</tr>
<tr>
<td>2</td>
<td><img src="image" alt="Local_real_10.0.0.18" /></td>
<td><img src="image" alt="Local_real_10.0.0.18" /></td>
</tr>
<tr>
<td>3</td>
<td><img src="image" alt="Any" /></td>
<td><img src="image" alt="Any" /></td>
</tr>
</tbody>
</table>
3.2.2 Using IP Pools

These pools can be as large as needed. For this example a range of twenty addresses are used.

For Check Point NG, you should create automatic NAT rules from the NAT tab of the address range objects. This will automatically generate NAT rules. Automatic NAT rules are need so that you don’t have to use static routes.
3.3 Encryption Domains

3.3.1 Firewall-A Local Encryption Domain

For this test, the Local Encryption Domain was only made to include the two addresses below. However you will have to include all the hosts that you want to VPN enable. You must also include the addresses used in your NAT rules that represent the local NATed addresses.
3.3.2 Creation of Remote Enc Domain for Firewall-B in Firewall-A’s object database

For this test, the remote encryption domain was only made to include the one addresses below. However you will have to include all the hosts that you want to VPN enable. You do not have to include the real addresses that represent the remote hosts in the Remote Encryption Domain.

NOTE: The fact that the Remote Encryption Domain definition does not require you to have the real addresses allows you to create a VPN between two hosts with identical IP addresses. For example, you can create a tunnel between 10.0.0.18 on one side of the network and a 10.0.0.18 host on the other side of the remote VPN.
3.4 ARP and Routing

ARP Setup

No special ARP setup is needed since we are not “connecting” to the made up addresses, they are just used in the translation rules.

Routing Tables

For Check Point NG routes are NOT needed is you are using Automatic NAT rules (and client side NAT is selected in Global Properties)

The following routes are needed for 4.1

Nokia-7[admin]# netstat -rn
Routing tables *

IPv4:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Flags</th>
<th>Refs</th>
<th>Use</th>
<th>Netif</th>
<th>Expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>192.168.22.20</td>
<td>CU</td>
<td>0</td>
<td>0</td>
<td>eth-s3p1c0</td>
<td></td>
</tr>
<tr>
<td>13.0.0/24</td>
<td>10.0.0.18</td>
<td>CU</td>
<td>0</td>
<td>0</td>
<td>eth-s4p1c0</td>
<td></td>
</tr>
</tbody>
</table>

*Entries have been deleted for clarity

Highlighted in bold is the static route needed in order for the Static NAT to work (In NG you no longer need this). Normally the gateway for this static route would be the IP address of the interface closest to the firewall on your internal router. For this test, the gateway is actually the pc behind the firewall.
### 4 Firewall-B Setup

#### 4.1 Rules setup

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Time</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Local ENC Domain</td>
<td>Remote ENC Domain</td>
<td>Any</td>
<td>Encrypt</td>
<td>Long</td>
<td>Av Gateways</td>
<td>Any</td>
<td>Outbound VPN Rule</td>
</tr>
<tr>
<td>2</td>
<td>Remote ENC Domain</td>
<td>Local ENC Domain</td>
<td>Any</td>
<td>Encrypt</td>
<td>Long</td>
<td>Av Gateways</td>
<td>Any</td>
<td>Inbound VPN Rule</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>drop</td>
<td>Long</td>
<td>Av Gateways</td>
<td>Any</td>
<td></td>
</tr>
</tbody>
</table>

For Check Point Next Generation (NG), the rules are the same.

#### 4.2 NAT Setup

##### 4.2.1 Using one to one

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Packet Source</th>
<th>Original Packet Destination</th>
<th>Original Packet Service</th>
<th>Translated Packet Source</th>
<th>Translated Packet Destination</th>
<th>Translated Packet Service</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Local 10.0.0.0 net</td>
<td>Local 10.0.0.0 net</td>
<td>Any</td>
<td>Original</td>
<td>Original</td>
<td>Original</td>
<td>Av Gateways</td>
<td>Ensure's that no local traffic will get NATED</td>
</tr>
<tr>
<td>2</td>
<td>local_real 10.0.0.2</td>
<td>Any</td>
<td>Any</td>
<td>local_nated 12.0.0.2</td>
<td>Original</td>
<td>Original</td>
<td>Av Gateways</td>
<td>This rule is for outbound traffic</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>local_nated 12.0.0.2</td>
<td>Any</td>
<td>local_real 10.0.0.2</td>
<td>Original</td>
<td>Original</td>
<td>Av Gateways</td>
<td>This rule is for inbound traffic</td>
</tr>
</tbody>
</table>
For Check Point NG, create an automatic NAT rule by going on the NAT tab of the 10.0.0.2 object and fill in the fields as follows:

The above action will yield the following Nat rules (rules 2 and 3):

<table>
<thead>
<tr>
<th>NO</th>
<th>ORIGINAL PACKET</th>
<th>TRANSLATED PACKET</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SOURCE</td>
<td>DESTINATION</td>
</tr>
<tr>
<td>1</td>
<td>net_10.0.0.0</td>
<td>net_10.0.0.0</td>
</tr>
<tr>
<td>2</td>
<td>local_real_10.0.0.2</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>local_real_10.0.0.2 (Valid Address)</td>
</tr>
</tbody>
</table>
4.2.2 Using IP Pools

These pools can be as large as needed. For this example a range of twenty addresses are used.

For Check Point NG, you should create automatic NAT rules from the NAT tab of the address range objects. This will automatically generate NAT rules. Automatic NAT rules are need so that you don’t have to use static routes.
4.3 Encryption Domain

4.3.1 Firewall-B Local Encryption Domain

For this test, the local encryption domain was only made to include the two addresses below. However you will have to include all the hosts that you want to VPN enable. You must also include the addresses used in your NAT rules that represent the local NATed addresses.

![Group Properties Window]

- Local_10.0.0.0_net
- Local-FW-B
- remote_nated_13.0.0.18
- remote_real_10.0.0.18
- Remote-ENC-Domain
- Remote-FW-A

- local_nated_12.0.0.2
- local_real_10.0.0.2

OK Cancel Help
4.3.2 Creation of Remote Enc Domain for Firewall-A in Firewall-B’s object database

For this test, the remote encryption domain was only made to include the one address below. However you will have to include all the hosts that you want to VPN enable. You do not have to include the real addresses that represent the remote hosts in the Remote Encryption Domain.

NOTE: The fact that the Remote Encryption Domain definition does not require you to have the real addresses allows you to create a VPN between two hosts with identical IP addresses. For example, you can create a tunnel between 10.0.0.18 on one side of the network and a 10.0.0.18 host on the other side of the remote VPN.
4.4 ARP and Routing

ARP Setup

No special ARP setup is needed since we are not “connecting” to the made up addresses, they are just used in the translation rules.

Routing Tables

For Check Point NG routes are NOT needed is you are using Automatic NAT rules (and client side NAT is selected in Global Properties)

The following routes are needed for 4.1

Nokia-8[admin]# netstat -rn
Routing tables *

IPv4:
Destination Gateway Flags Refs Use Netif Expire
default 192.168.22.180 CU 0 0 eth-s3p1c0
12.0.0/24 10.0.0.2 CU 0 0 eth-s4p1c0

*Entries have been deleted for clarity

Highlighted in bold is the static route needed in order for the Static NAT to work (In NG you no longer need this). Normally the gateway for this static route would be the ip address of the interface closest to the firewall on your internal router. For this test, the gateway is actually the pc behind the firewall.
5 Test results

5.1.1 Ping from PC behind FW-A (Real-10.0.0.2/NAT-12.0.0.2) to PC behind FW-B (Real-10.0.0.18/NAT-13.0.0.18)

This test is a ping from the pc behind Firewall A to a PC behind Firewall B. The log entry for the corresponding connection is also shown. Notice the source IP address of 10.0.0.2 has been translated to 12.0.0.2 before sending the encrypted packets to FW-B.
Log showing the above ping. Take note of the translation from 10.0.0.2 to 12.0.0.2.

Below are the logs from Firewall-A. Notice the translation of 13.0.0.18 to 10.0.0.18 thus completing the double NAT sequence which effectively made it possible to send a packet from 10.0.0.2 to 10.0.0.18 (on another network) through the VPN tunnel.
5.1.2 FTP and ping from PC behind FW-B (Real-10.0.0.18/NAT-13.0.0.18) to the PC behind FW-A (Real-10.0.0.2/NAT-12.0.0.2)

This test is a ping and ftp from the pc behind Firewall B to a PC behind Firewall A. The log entry for the corresponding connection is also shown.

C:\>ftp 12.0.0.2
Connected to 12.0.0.2.
220 3Com 3CDaemon FTP Server Version 2.0
User <12.0.0.2>:<none>>: anonymous
331 User name ok, need password
Password:
230 User logged in
ftp> ls
200 PORT command successful.
150 File status OK; about to open data connection

   cpshared_0003_1.tgz
   fw1_50703_1.tgz
226 Closing data connection
45 bytes received in 0.00 seconds (45000.00 Kbytes/sec)
ftp>

C:\>ping 12.0.0.2
Pinging 12.0.0.2 with 32 bytes of data:
Reply from 12.0.0.2: bytes=32 time=10ms TTL=126
Reply from 12.0.0.2: bytes=32 time<10ms TTL=126
Reply from 12.0.0.2: bytes=32 time=10ms TTL=126
Reply from 12.0.0.2: bytes=32 time=80ms TTL=126

C:\>
Notice the source IP address of 10.0.0.18 has been translated to 13.0.0.18 before sending the encrypted packets to FW-A.

Below are the logs from Firewall-A. Notice the translation of 12.0.0.2 to 10.0.0.2 thus completing the double NAT sequence, which effectively made it possible to send a packet from 10.0.0.18 to 10.0.0.2 (on another network) through the VPN tunnel.
6 Conclusion

Hopefully this document has shown how easy it is to setup a VPN tunnel from a 10.x.x.x (or any other private address) network behind a VPN/FW to another 10.x.x.x network behind a different VPN/FW device. A static NAT and a static route were required to accomplish this. As you have seen, with Check Point Next Generation, it is even easier to do this due to the new “client side NAT” feature.

This Check Point configuration may be useful when connecting to business partners that may have the same internal IP address scheme that your company has.