

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

Table of Contents

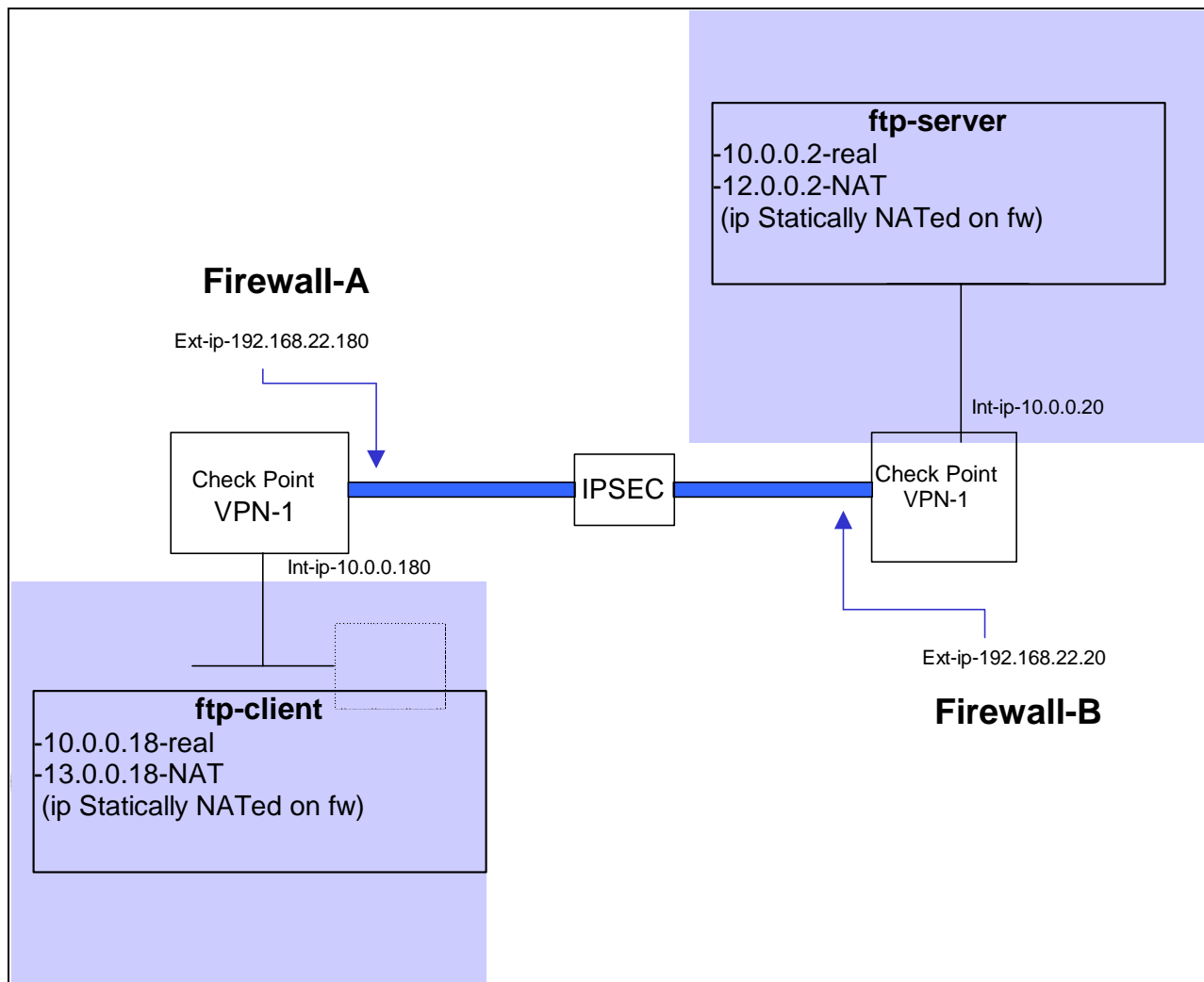
1	Introduction	3
2	Test Bed Layout.....	3
3	Firewall-A Setup.....	4
3.1	Rules setup.....	4
3.2	NAT Setup.....	4
3.3	Encryption Domains	7
3.4	ARP and Routing.....	9
4	Firewall-B Setup.....	10
4.1	Rules setup.....	10
4.2	NAT Setup.....	10
4.3	Encryption Domain.....	13
4.4	ARP and Routing.....	15
5	Test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

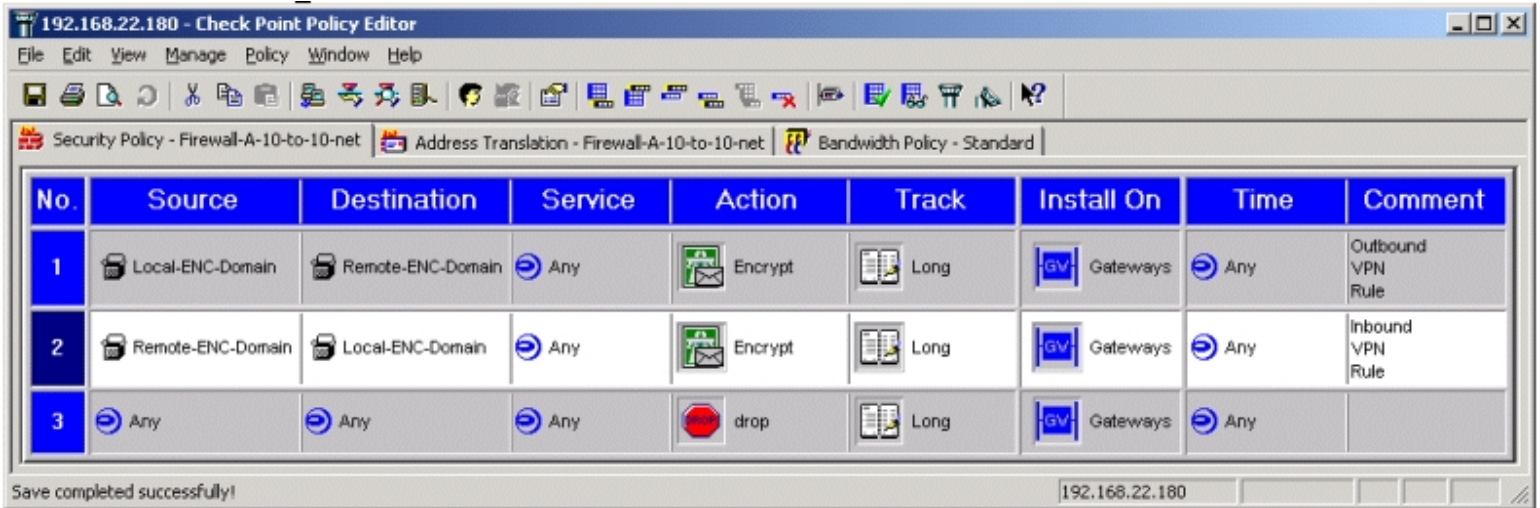
Most of the screens shown below are for CP 4.1, however, when using Check Point Next Generation, the setup of rules is the same however NAT rules must be automatic so that client side NAT can be enabled. If this is done correctly, no static routes are needed. The default settings in global properties 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

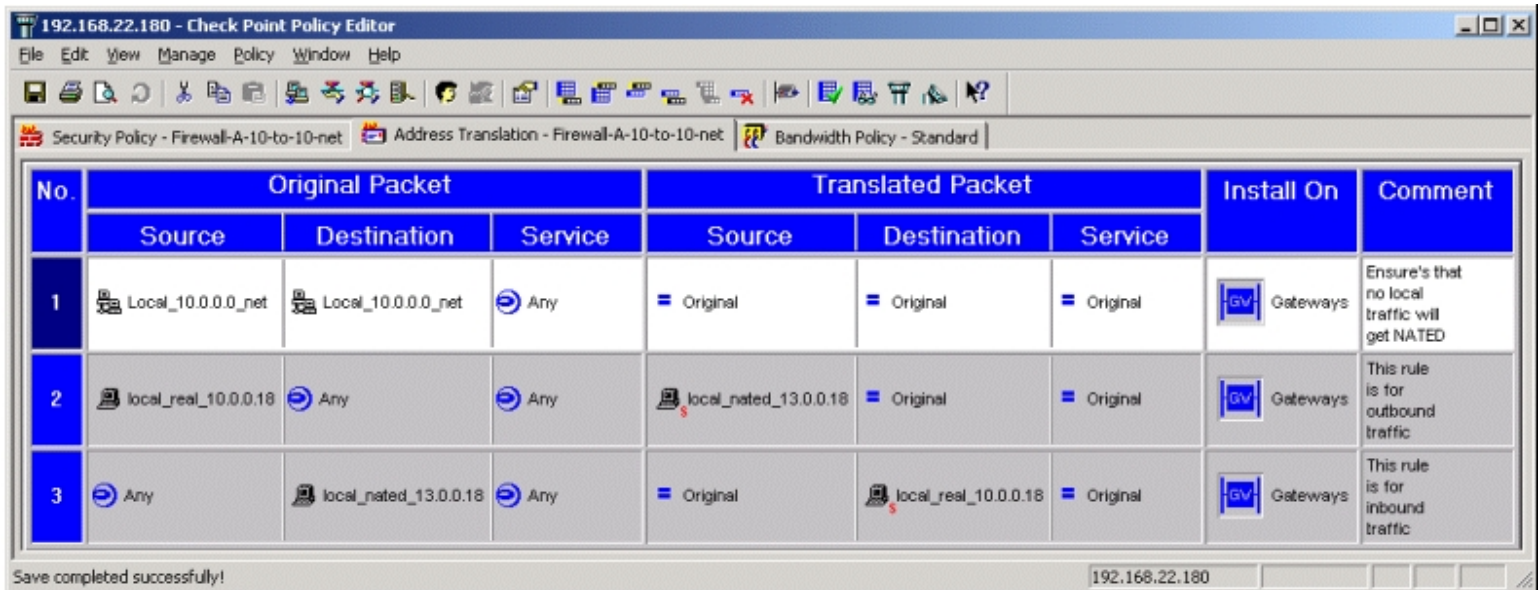
3.1 Rules setup



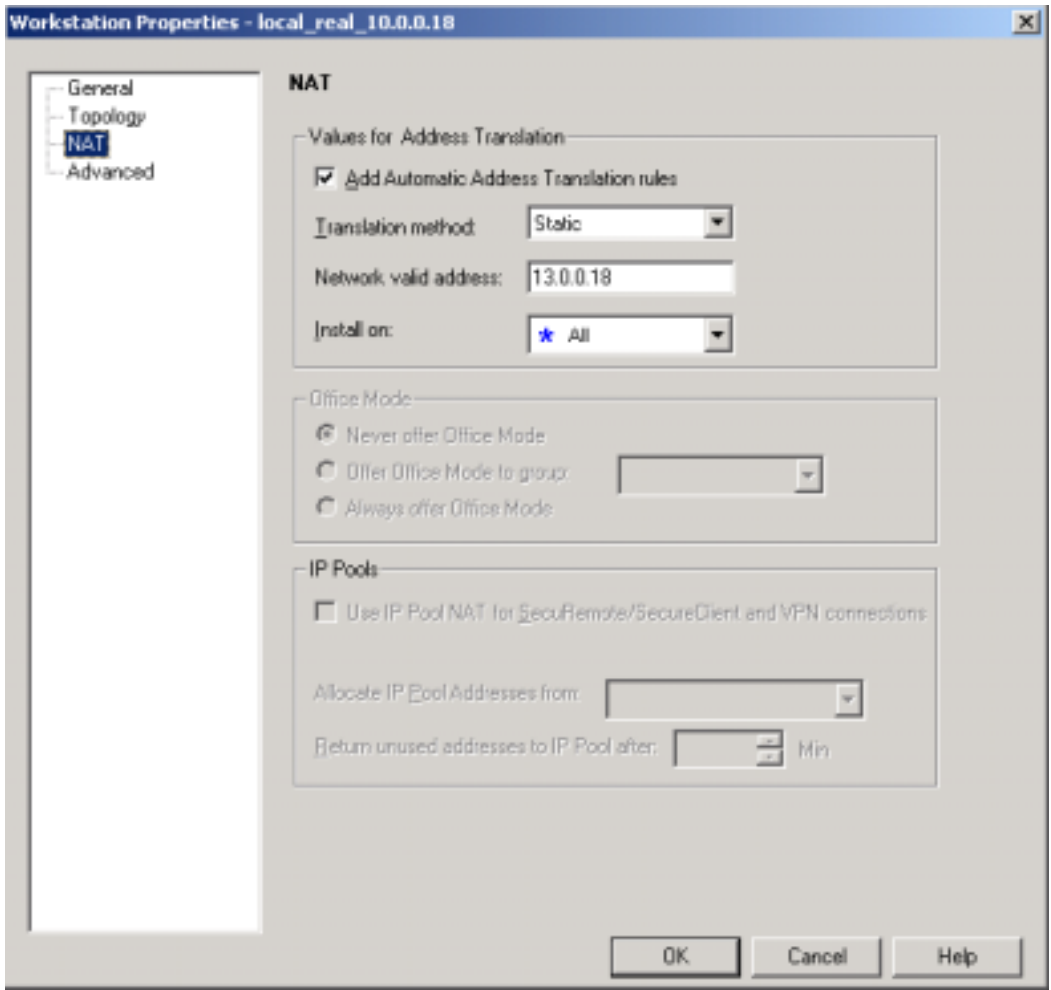
For Check Point Next Generation (NG), the rules are the same.

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:

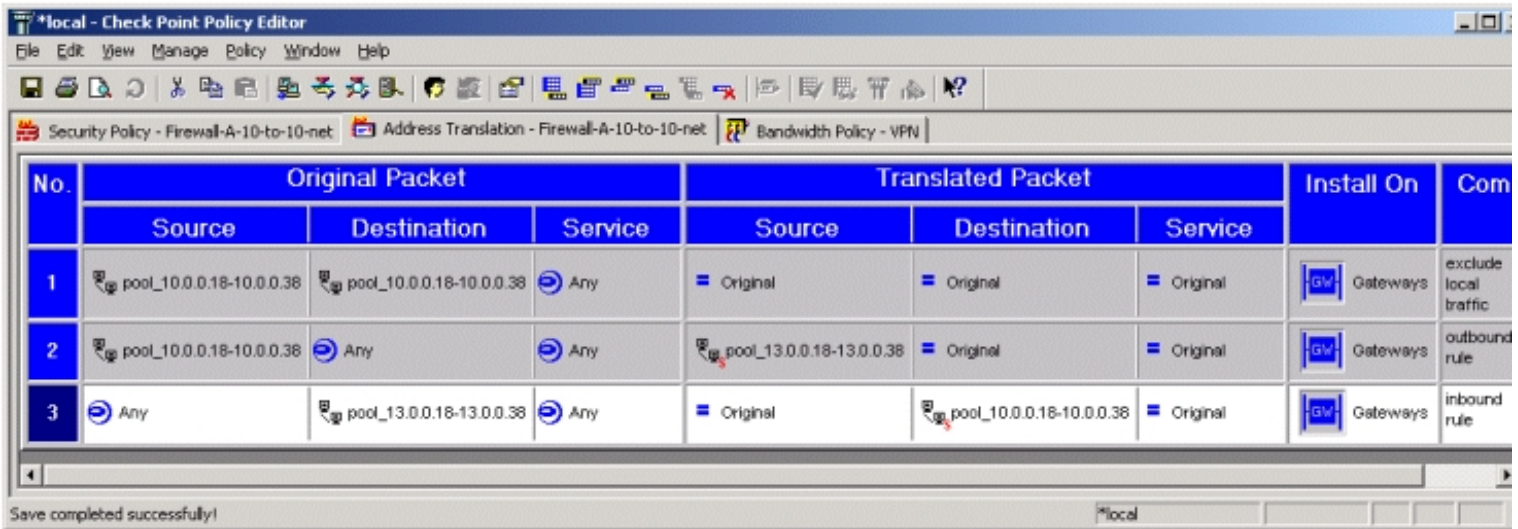


The above action will yield the following Nat rules (rules 2 and 3):

#0.	ORIGINAL PACKET			TRANSLATED PACKET		
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
1	net_10.0.0.0	net_10.0.0.0	Any	Original	Original	Original
2	local_real_10.0.0.18	Any	Any	local_real_10.0.0.18 (Valid Address)	Original	Original
3	Any	local_real_10.0.0.18	Any	Original	local_real_10.0.0.18	Original

3.2.2 Using IP Pools

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



The screenshot shows the Check Point Policy Editor interface. The main window displays a table of NAT rules. The table has columns for 'No.', 'Original Packet' (Source, Destination, Service), 'Translated Packet' (Source, Destination, Service), 'Install On', and 'Comments'. Three rules are visible:

No.	Original Packet			Translated Packet			Install On	Comments
	Source	Destination	Service	Source	Destination	Service		
1	pool_10.0.0.18-10.0.0.38	pool_10.0.0.18-10.0.0.38	Any	Original	Original	Original	Gateways	exclude local traffic
2	pool_10.0.0.18-10.0.0.38	Any	Any	pool_13.0.0.18-13.0.0.38	Original	Original	Gateways	outbound rule
3	Any	pool_13.0.0.18-13.0.0.38	Any	Original	pool_10.0.0.18-10.0.0.38	Original	Gateways	inbound rule

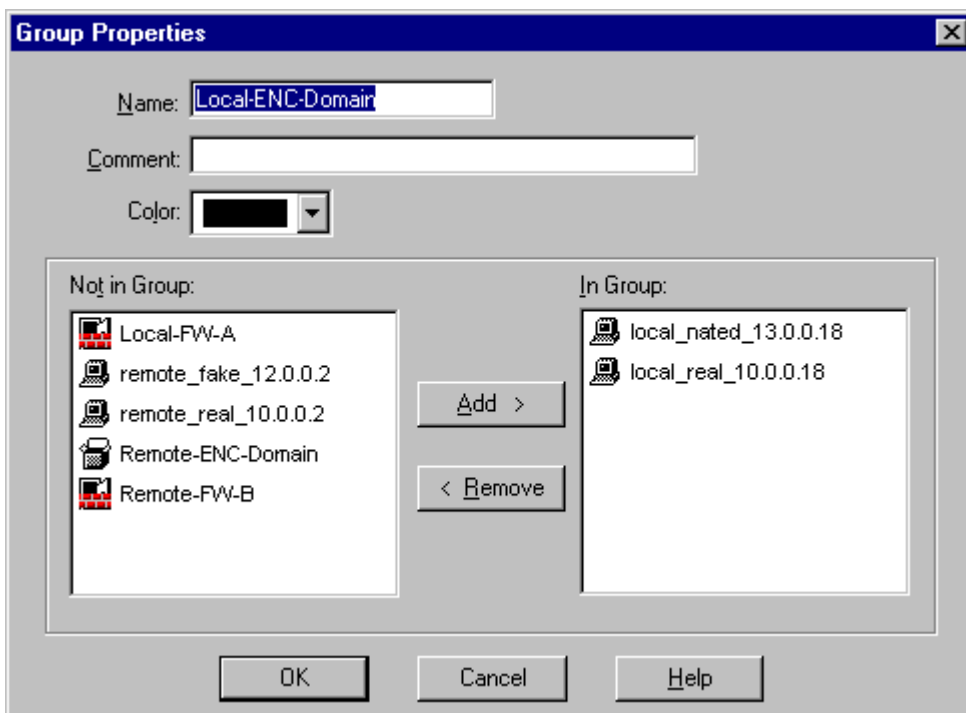
At the bottom of the window, a status bar indicates 'Save completed successfully!'.

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

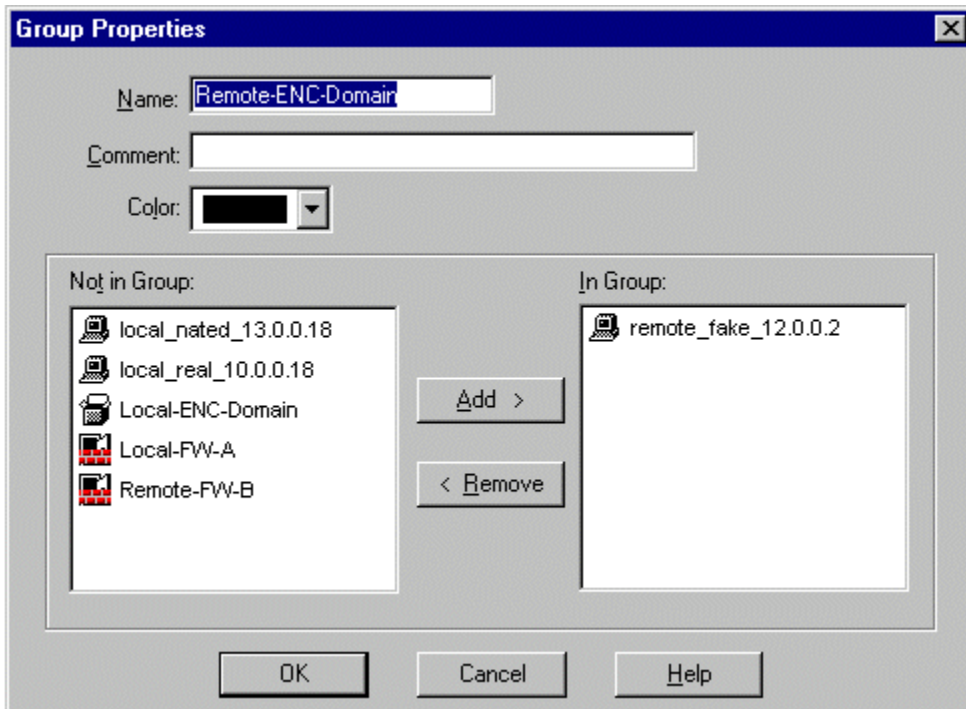
For this test, the Local Encryption Domain was only made to include the two addresses below. However you will have to include all the hosts that you want to VPN enable. You must also include the addresses used in your NAT rules that represent the local NATed addresses.



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:

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	192.168.22.20	CU	0	0	eth-s3p1c0	
13.0.0/24	10.0.0.18	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.

4 Firewall-B Setup

4.1 Rules setup

192.168.22.20 - Check Point Policy Editor

File Edit View Manage Policy Window Help

Security Policy - Firewall-B-10-to-10-net | Address Translation - Firewall-B-10-to-10-net | Bandwidth Policy - Standard

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Local-ENC-Domain	Remote-ENC-Domain	Any	Encrypt	Long	Gateways	Any	Outbound VPN Rule
2	Remote-ENC-Domain	Local-ENC-Domain	Any	Encrypt	Long	Gateways	Any	Inbound VPN Rule
3	Any	Any	Any	drop	Long	Gateways	Any	

Save completed successfully! 192.168.22.20

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

4.2 NAT Setup

4.2.1 Using one to one

192.168.22.20 - Check Point Policy Editor

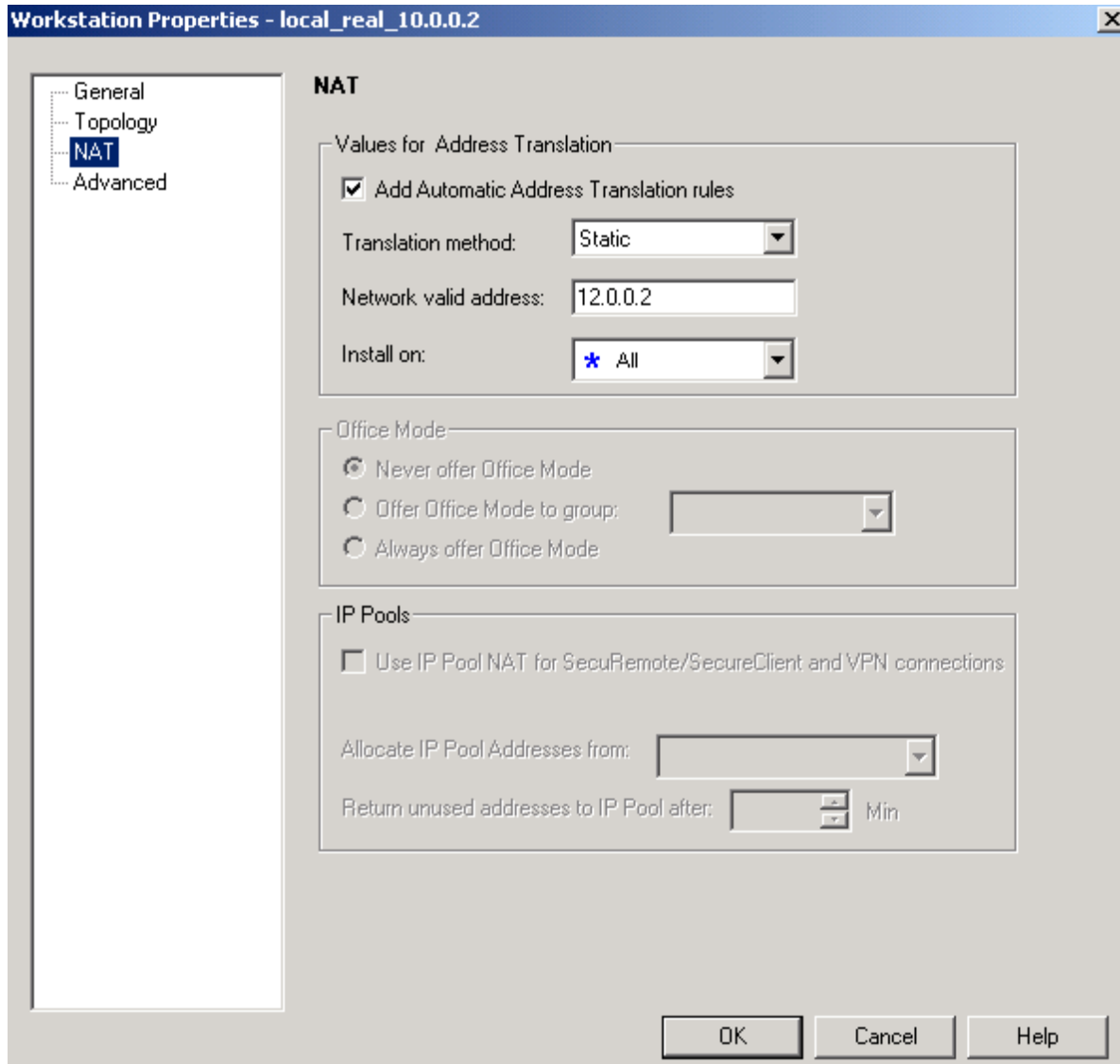
File Edit View Manage Policy Window Help

Security Policy - Firewall-B-10-to-10-net | Address Translation - Firewall-B-10-to-10-net | Bandwidth Policy - Standard

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	Local_10.0.0.0_net	Local_10.0.0.0_net	Any	= Original	= Original	= Original	Gateways	Ensure's that no local traffic will get NATED
2	local_real_10.0.0.2	Any	Any	local_nated_12.0.0.2	= Original	= Original	Gateways	This rule is for outbound traffic
3	Any	local_nated_12.0.0.2	Any	= Original	local_real_10.0.0.2	= Original	Gateways	This rule is for inbound traffic

For Help, press F1 192.168.22.20

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):

NO.	ORIGINAL PACKET			TRANSLATED PACKET		
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
1	net_10.0.0.0	net_10.0.0.0	* Any	Original	Original	Original
2	local_real_10.0.0.2	* Any	* Any	local_real_10.0.0.2 (Valid Address)	Original	Original
3	* Any	local_real_10.0.0.2 (Valid Address)	* Any	Original	local_real_10.0.0.2	Original

4.2.2 Using IP Pools

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

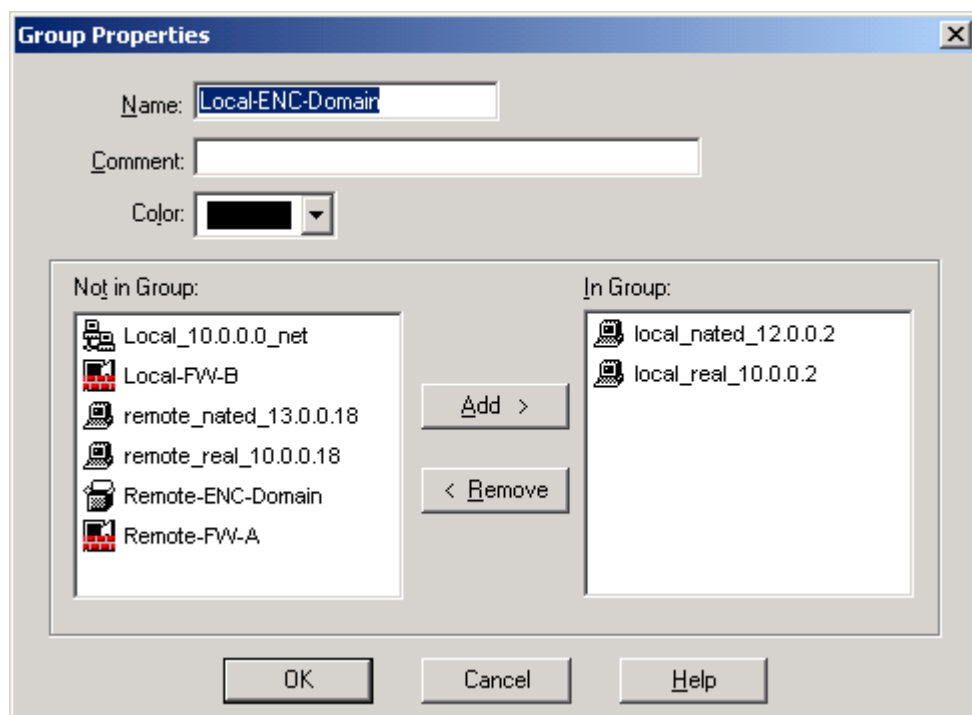
No.	Original Packet			Translated Packet			Install On	Comm
	Source	Destination	Service	Source	Destination	Service		
1	pool_10.0.0.2-10.0.0.22	pool_10.0.0.2-10.0.0.22	Any	Original	Original	Original	Gateways	exclude local traffic
2	pool_10.0.0.2-10.0.0.22	Any	Any	pool_12.0.0.2-12.0.0.22	Original	Original	Gateways	outbound rule
3	Any	pool_12.0.0.2-12.0.0.22	Any	Original	pool_10.0.0.2-10.0.0.22	Original	Gateways	Inbound rule

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

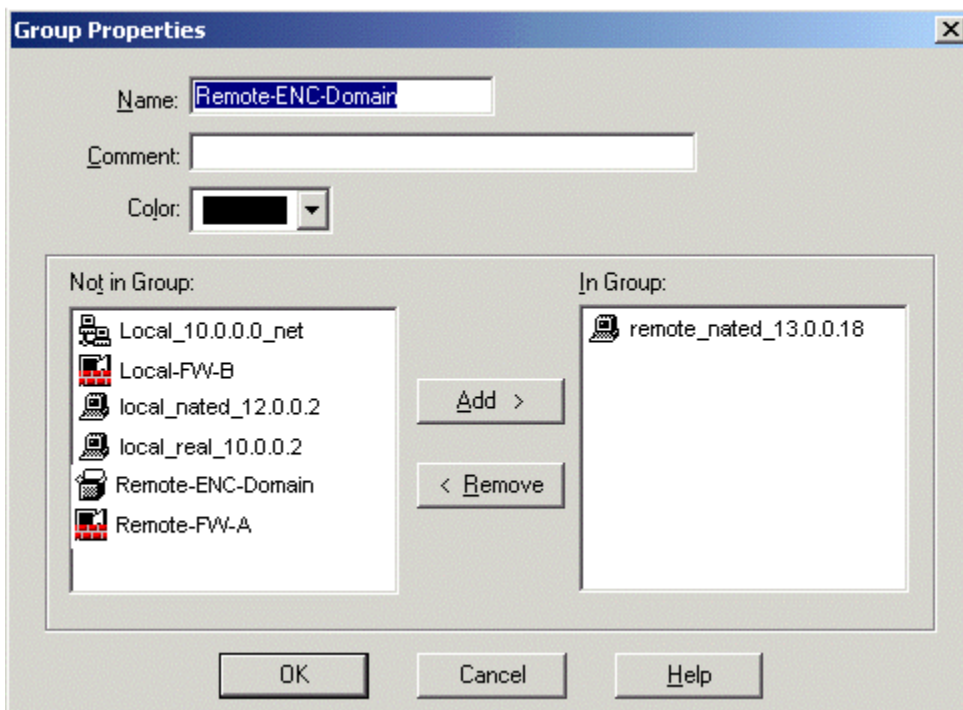
For this test, the local encryption domain was only made to include the two addresses below. However you will have to include all the hosts that you want to VPN enable. You must also include the addresses used in your NAT rules that represent the local NATed addresses.



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	

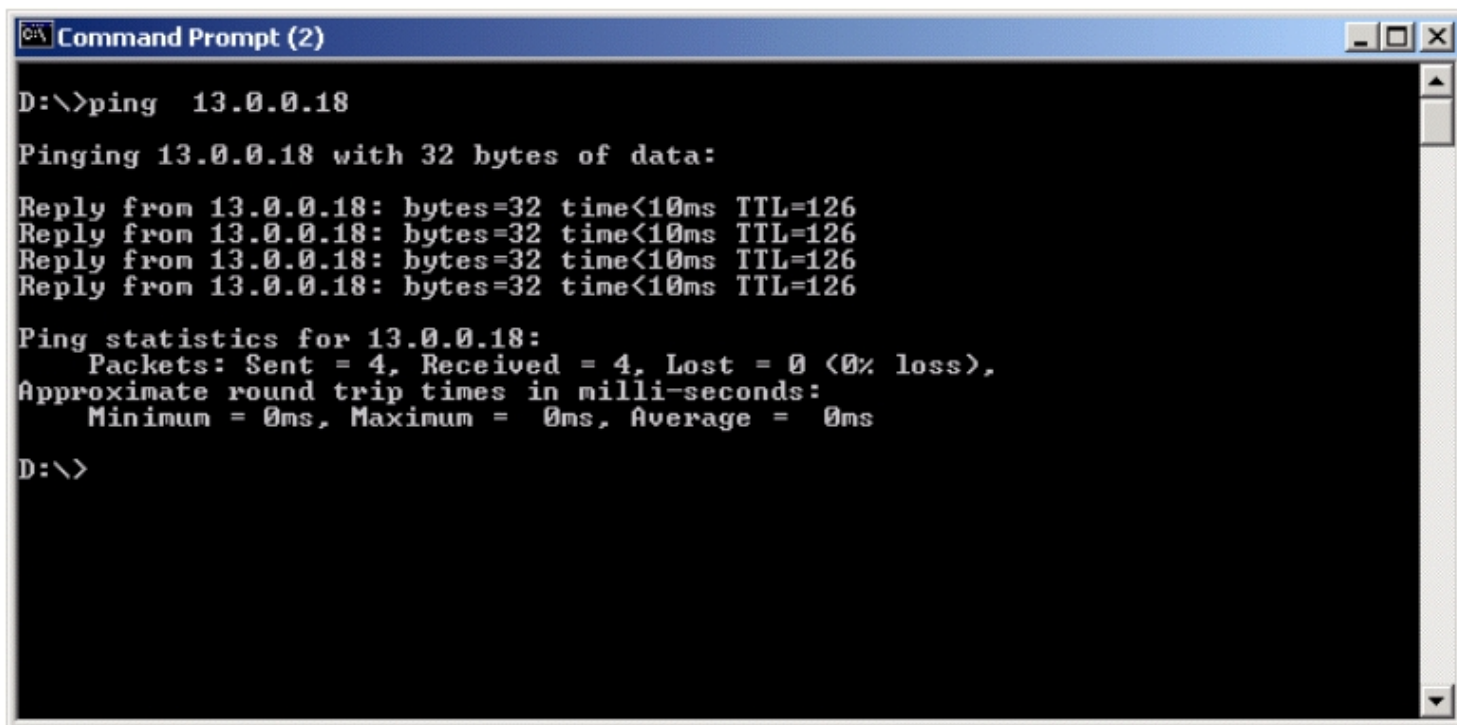
*Entries have been deleted for clarity

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.



```
Command Prompt (2)
D:\>ping 13.0.0.18

Pinging 13.0.0.18 with 32 bytes of data:

Reply from 13.0.0.18: bytes=32 time<10ms TTL=126
Reply from 13.0.0.18: bytes=32 time<10ms TTL=126
Reply from 13.0.0.18: bytes=32 time<10ms TTL=126
Reply from 13.0.0.18: bytes=32 time<10ms TTL=126

Ping statistics for 13.0.0.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\>
```

Log showing the above ping. Take note of the translation from 10.0.0.2 to 12.0.0.2.

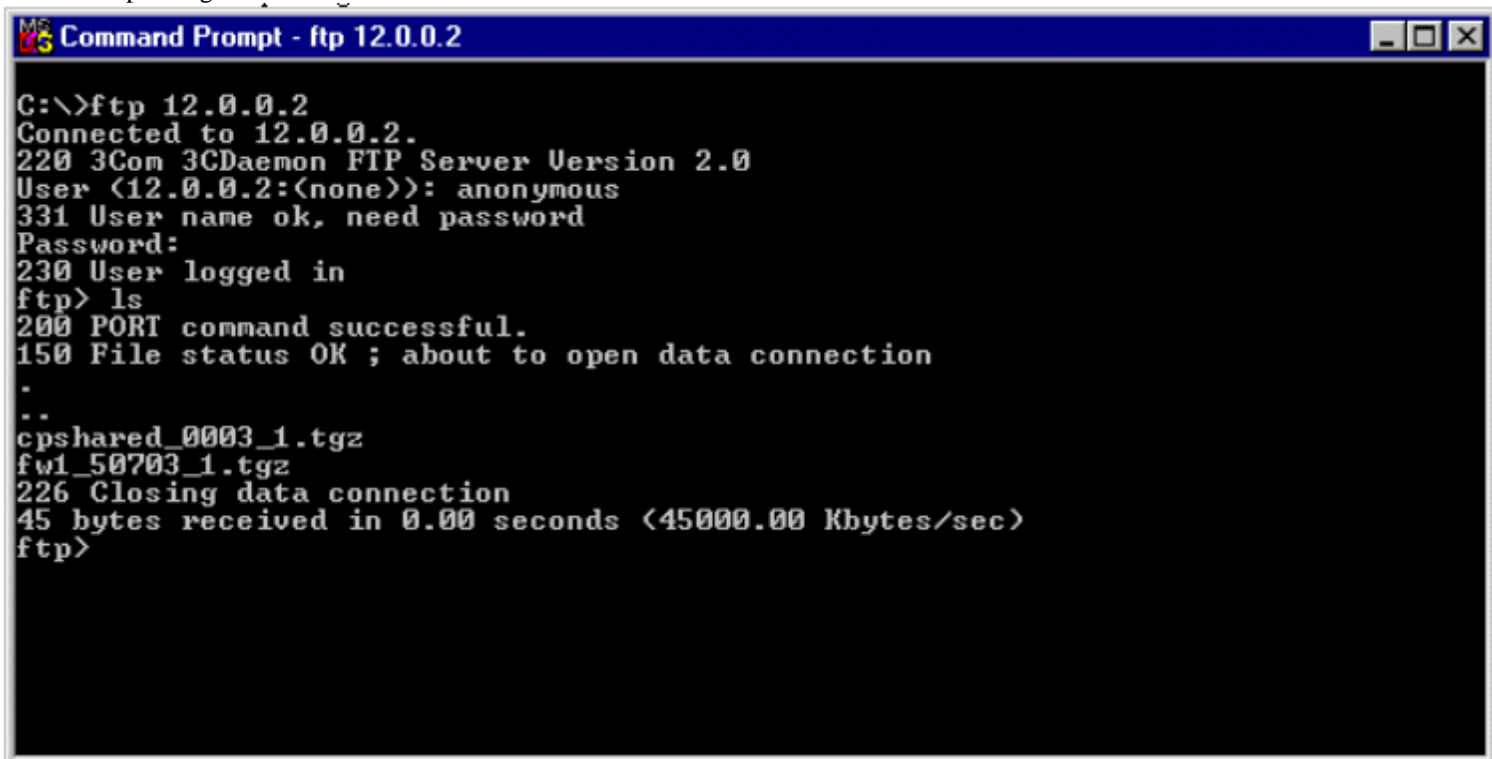
N..	Date	Origin	Action	Service	Source	Destination	Proto.	Rule	XlateSrc	XlateDst	Info.
0	10Nov2001	192.168.22.20	ctl								started sending log to localhost
1	10Nov2001	192.168.22.20	key install		192.168.22.20	192.168.22.180					IKE Log: Phase 1 (aggressive) completion. 3D
2	10Nov2001	192.168.22.20	key install		192.168.22.20	192.168.22.180	ip	0			scheme: IKE methods: Combined ESP: 3DES
3	10Nov2001	192.168.22.20	encrypt		10.0.0.2	13.0.0.18	icmp	1	12.0.0.2		icmp-type 8 icmp-code 0 scheme: IKE method
4	10Nov2001	192.168.22.20	key install		192.168.22.180	192.168.22.20	ip	0			scheme: IKE methods: Combined ESP: 3DES
5	10Nov2001	192.168.22.20	key install		192.168.22.20	192.168.22.180	ip	0			scheme: IKE methods: Combined ESP: 3DES
6	10Nov2001	192.168.22.20	decrypt		13.0.0.18	10.0.0.2	icmp	2		12.0.0.2	icmp-type 0 icmp-code 0 scheme: IKE method

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.

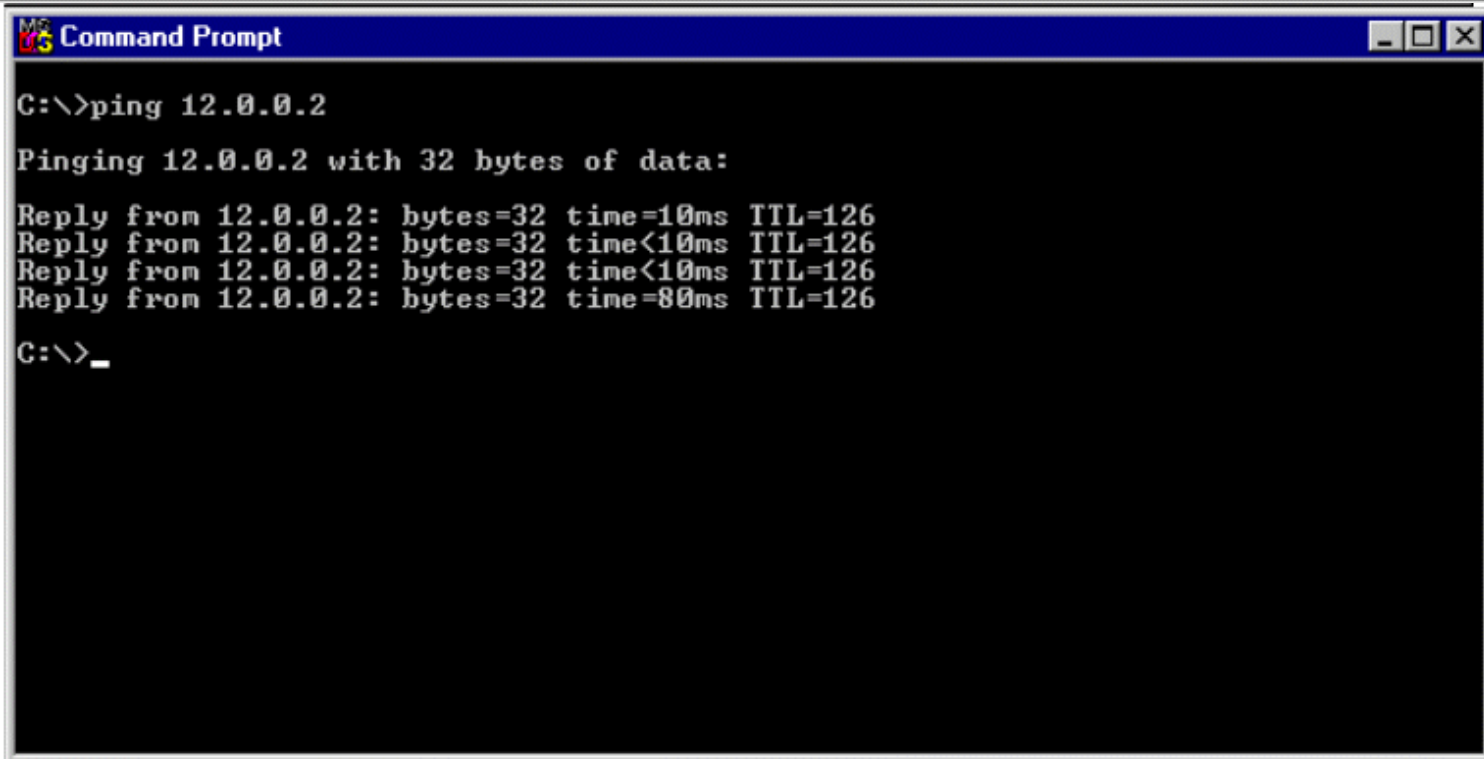
N..	Date	Origin	Action	Service	Source	Destination	Proto.	Rule	XlateSrc	XlateDst	Info.
0	10Nov2001	192.168.22.180	ctl								started sending log to localhost
1	10Nov2001	192.168.22.180	key install		192.168.22.20	192.168.22.180					IKE Log: Phase 1 (aggressive) comple
2	10Nov2001	192.168.22.180	key install		192.168.22.20	192.168.22.180	ip	0			scheme: IKE methods: Combined ESP:
3	10Nov2001	192.168.22.180	decrypt		12.0.0.2	13.0.0.18	icmp	2		10.0.0.18	icmp-type 8 icmp-code 0 scheme: IKE
4	10Nov2001	192.168.22.180	key install		192.168.22.180	192.168.22.20	ip	0			scheme: IKE methods: Combined ESP:
5	10Nov2001	192.168.22.180	encrypt		13.0.0.18	12.0.0.2	icmp	1	10.0.0.18		icmp-type 0 icmp-code 0 scheme: IKE
6	10Nov2001	192.168.22.180	key install		192.168.22.20	192.168.22.180	ip	0			scheme: IKE methods: Combined ESP:

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.

N..	Date	Origin	Action	Service	Source	Destination	Proto.	Rule	XlateSrc	XlateDst	Info.
0	10Nov2001	192.168.22.180	ctl								started sending log to localhost
1	10Nov2001	192.168.22.180	encrypt	ftp	10.0.0.18	12.0.0.2	tcp	1	13.0.0.18	12.0.0.2	scheme: IKE methods: Combined ESP:
2	10Nov2001	192.168.22.180	encrypt		10.0.0.18	12.0.0.2	icmp	1	13.0.0.18		icmp-type 8 icmp-code 0 scheme: IKE
3	10Nov2001	192.168.22.180	decrypt		12.0.0.2	10.0.0.18	icmp	2		13.0.0.18	icmp-type 0 icmp-code 0 scheme: IKE

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.

N..	Date	Origin	Action	Service	Source	Destination	Proto.	Rule	XlateSrc	XlateDst	Info.
1	10Nov2001	192.168.22.20	decrypt	ftp	13.0.0.18	12.0.0.2	tcp	2	13.0.0.18	10.0.0.2	scheme: IKE methods: Combined ESP: 3DES
5	10Nov2001	192.168.22.20	decrypt		13.0.0.18	12.0.0.2	icmp	2		10.0.0.2	icmp-type 8 icmp-code 0 scheme: IKE methoc
6	10Nov2001	192.168.22.20	encrypt		12.0.0.2	13.0.0.18	icmp	1	10.0.0.2		icmp-type 0 icmp-code 0 scheme: IKE methoc

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.