



3/1/2003 2:13 PM

Configuring site-to-site VPN between two VPN-1/FireWall-1 Gateways using mesh topology

Version 1.0

By Tasawar Jalali



3/1/2003 2:13 PM

Table of Contents

Introduction	3
Network Layout.....	3
Configuring VPN on NewYork VPN-1/Firewall-1 Server	4
Creating a Node	4
Adding New Checkpoint VPN Gateways.....	6
Testing the VPN Tunnel	15
Comments and Feedback:	15

Introduction

Thanks to Checkpoint NG FP3, configuring VPN is as easy as installing MS Office on Windows. I am not sure how easy it can get, however, FP3 might confuse FireWall-1 admin's since UI has changed quite a bit, especially when you are trying to configure VPN. New terms like VPN Community and VPN's Site have been introduced. Now you are not required to define encryption rules since these will be automatically created when you define a VPN domain.

This paper assumes basic knowledge of Firewalls, especially some familiarity with Checkpoint VPN-1/Firewall-1. This is a very basic tutorial for System Admins who are new to Check Point Firewall.

Network Layout

Firewall Configuration use for this setup:

- **NewYork**
 - External Interface - 172.16.1.2
 - Internal Interface – 10.10.1.1
 - Host behind this Firewall (Trusted Network) – Client1: 10.10.1.2
 - Network Behind this Firewall – 10.10.1.0
 - Net Mask: 255.255.255.0 for both internal and external networks

- **Kashmir**
 - External Interface - 172.16.3.2
 - Internal Interface – 10.10.3.1
 - Host behind this Firewall (Trusted Network) – Client2: 10.10.3.2
 - Network Behind this Firewall – 10.10.3.0
 - Net Mask: 255.255.255.0 for both internal and external networks

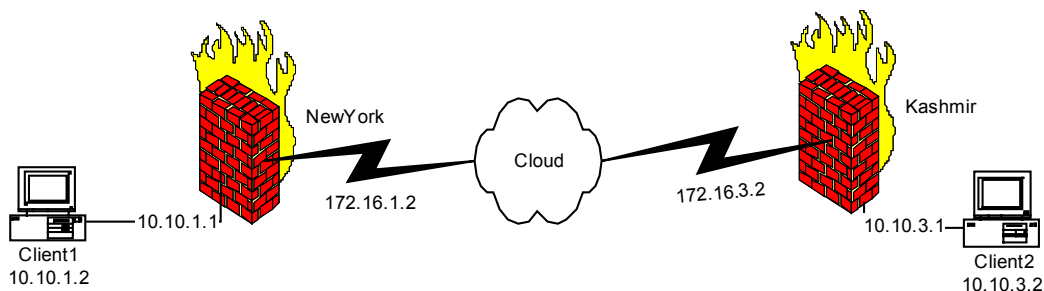


Figure-1: Schematics of the Networks

Configuring VPN on NewYork VPN-1/Firewall-1 Server

Creating a Node

First ensure that you have defined at least one Check Point host that is behind NewYork. This can be simply done by going to the “**Manage**” menu and select “**Network Objects**” → “**New**” → “**Node**” → **Host**

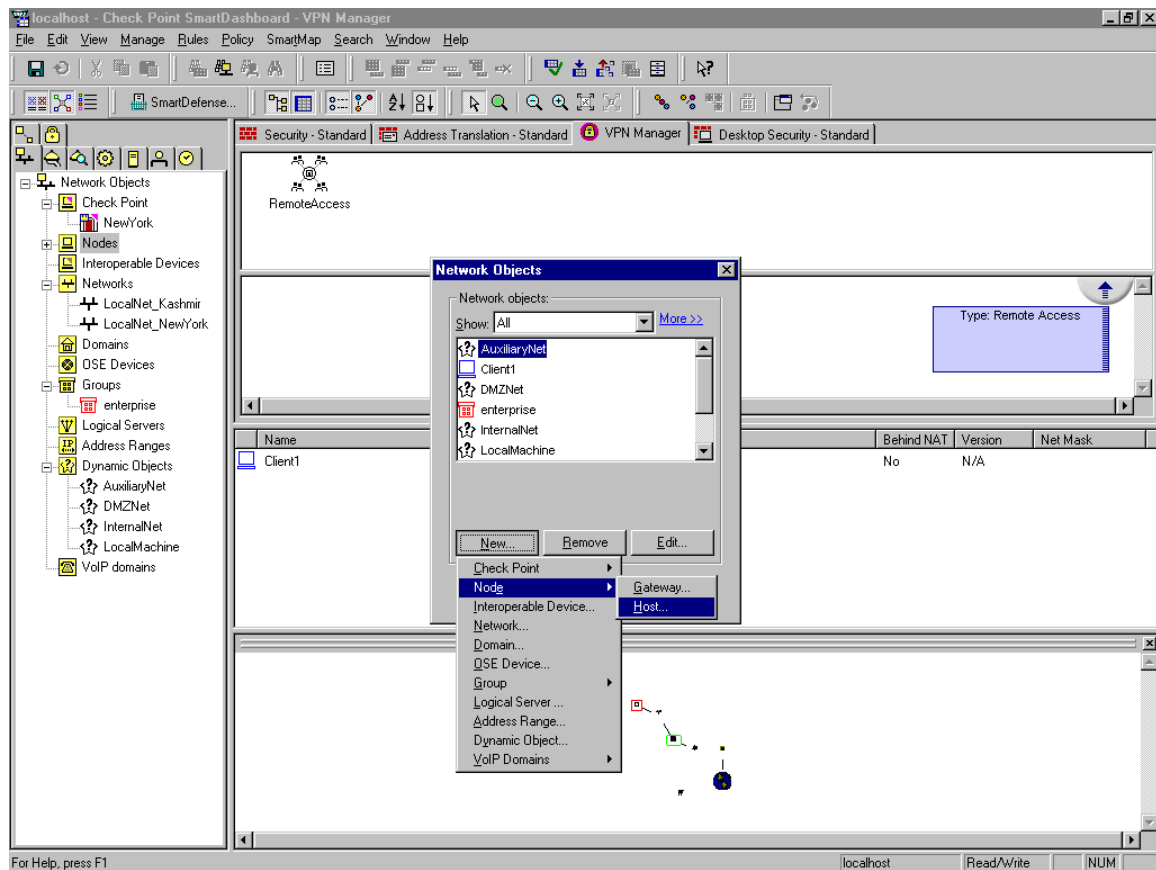


Figure 2:

Next, you will be presented with “**Host Node**” window. Enter name of the host and the IP address. Make sure you define the IP addresses under topology.

- Do not add NAT to this object.

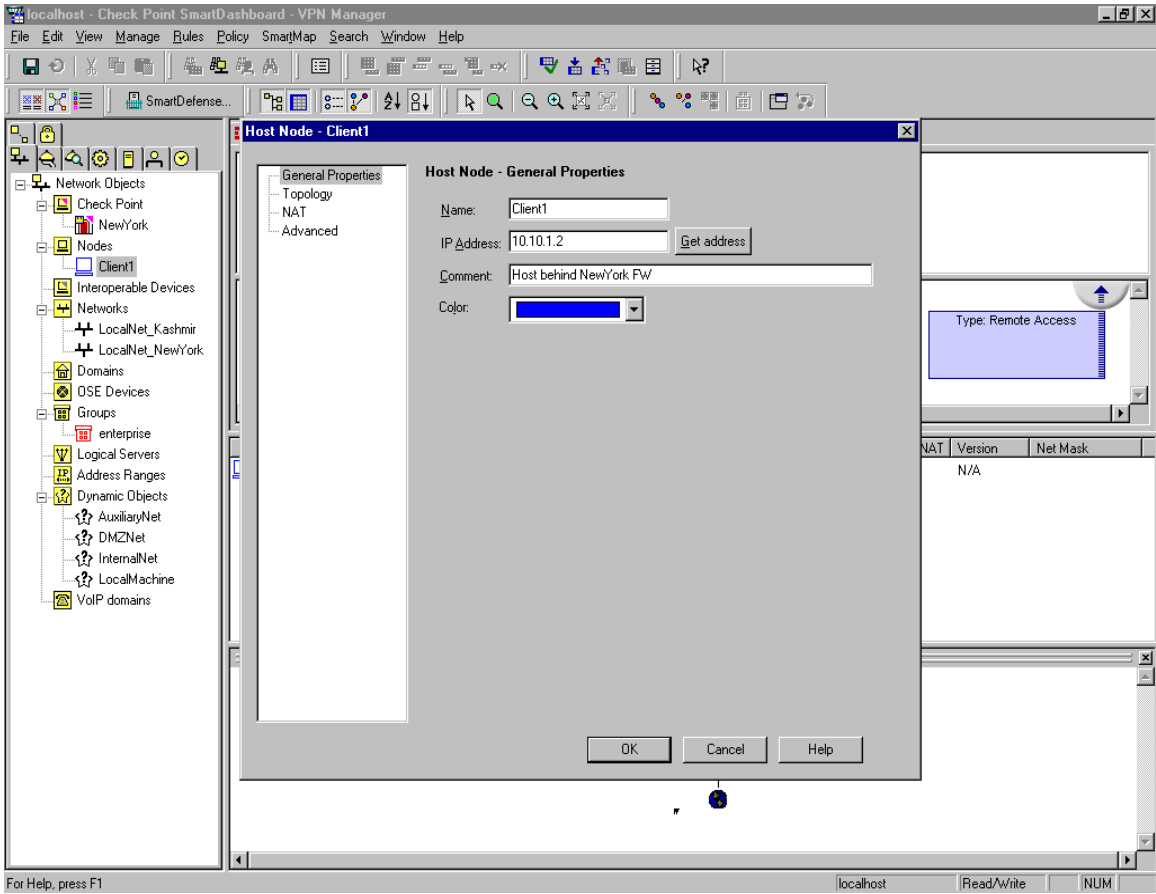


Figure 3:

Adding New Checkpoint VPN Gateways

First let's ensure that VPN is enabled for our local Firewall (NewYork). This can be done by going to **Manage** menu → **Network Objects** and edit local firewall object (NewYork in our case) and check VPN-1 Pro under “**Check Point Products**” section. Figure-4

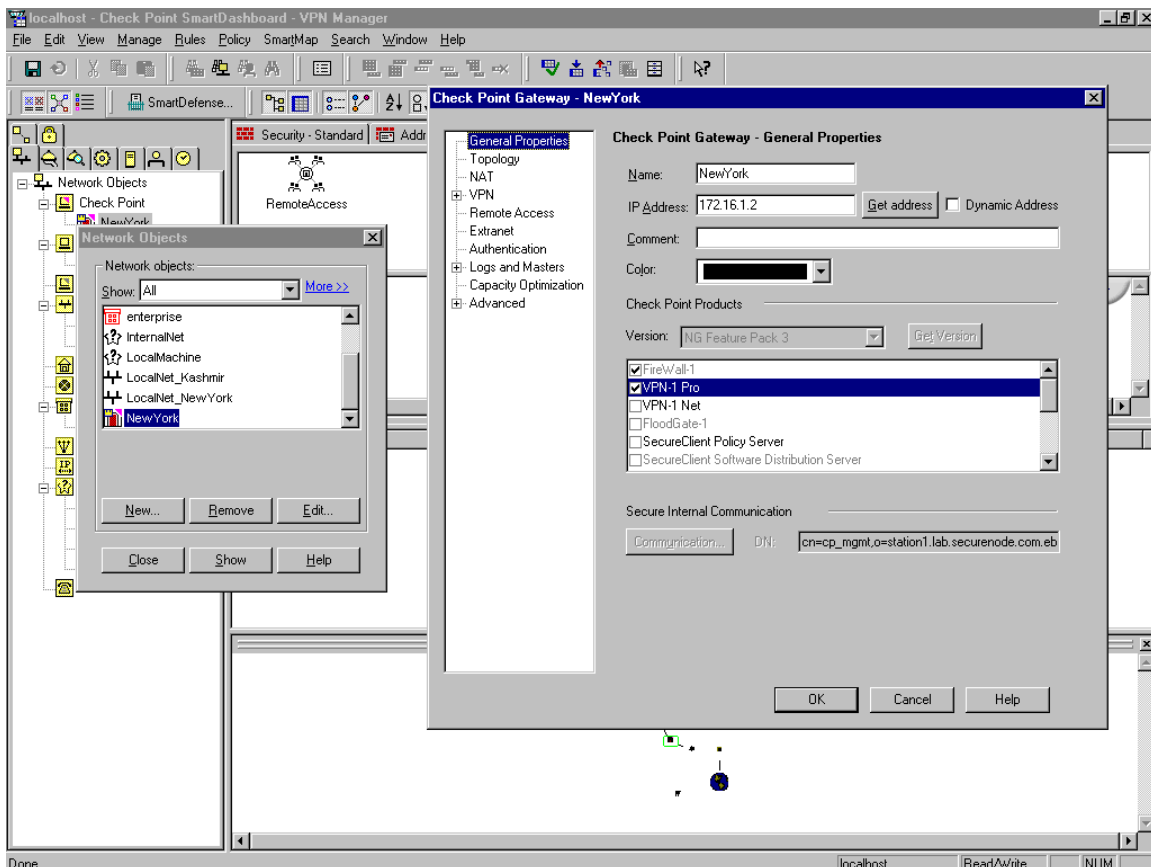


Figure 4

Since we will be using the “**Pre-Shared Secret**” keys to build a VPN tunnel between two gateways, we need to define the secret key. Figure 5

Double click on Check Point Gateway from the left column in SmartDashBoard (in our case NewYork). Click on **VPN** → **Traditional Mode Configuration** → Check “**Pre-shared Secret**” → Click on “**Edit Secrets**” → select your peer GW (in our case Kashmir) → Click on **Edit** → Type in your password and click on “**Set**” the password. You will need to use the same password when

configuring this section on the peer GW. Also, ensure that you use the same Encryption and hashing algorithms in the peer GW.

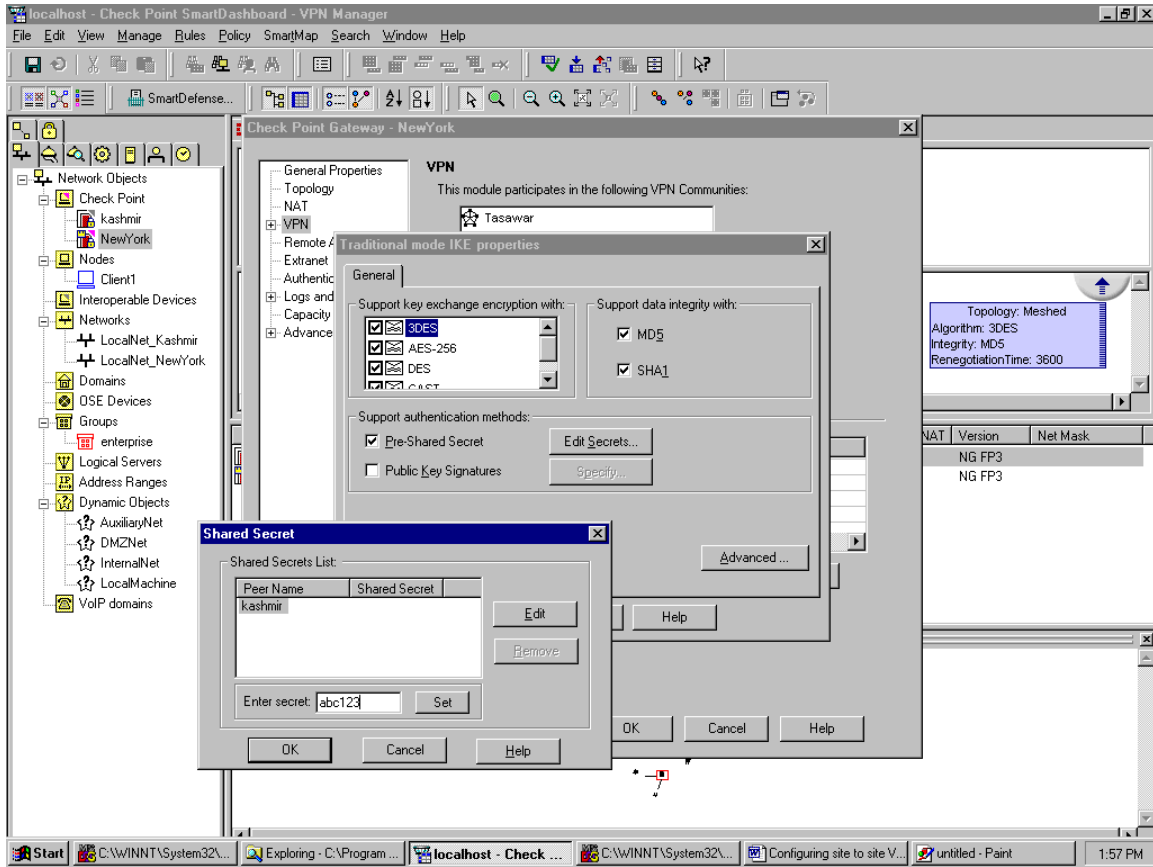


Figure 5

Now let's add the peer gateway (VPN-1/FireWall-1). This can be done by going to Manage menu → Network Objects → New → Check Point → Externally Managed Gateway... Figure-6

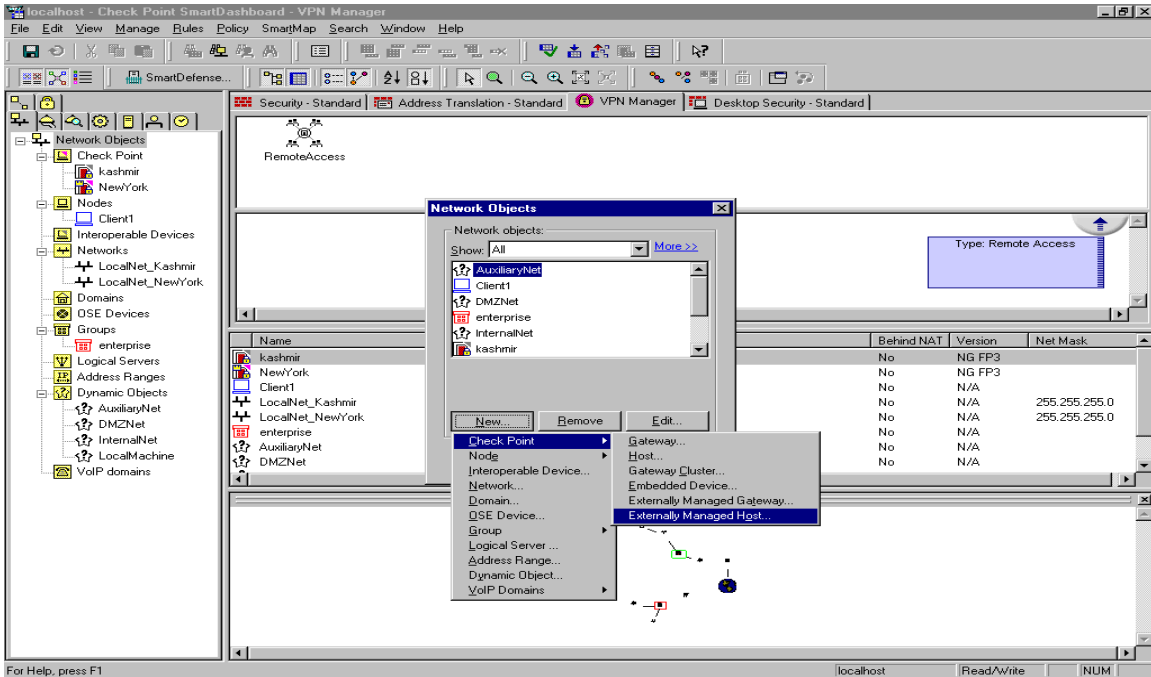


Figure 6

In the “**Externally Managed Check Point Gateway**” property window, enter the name and the IP address of external interface of the peer gateway by selecting “**General Properties**” in the left column. Ensure you check the **VPN-1 Pro** under “**Check Point Products**” section.

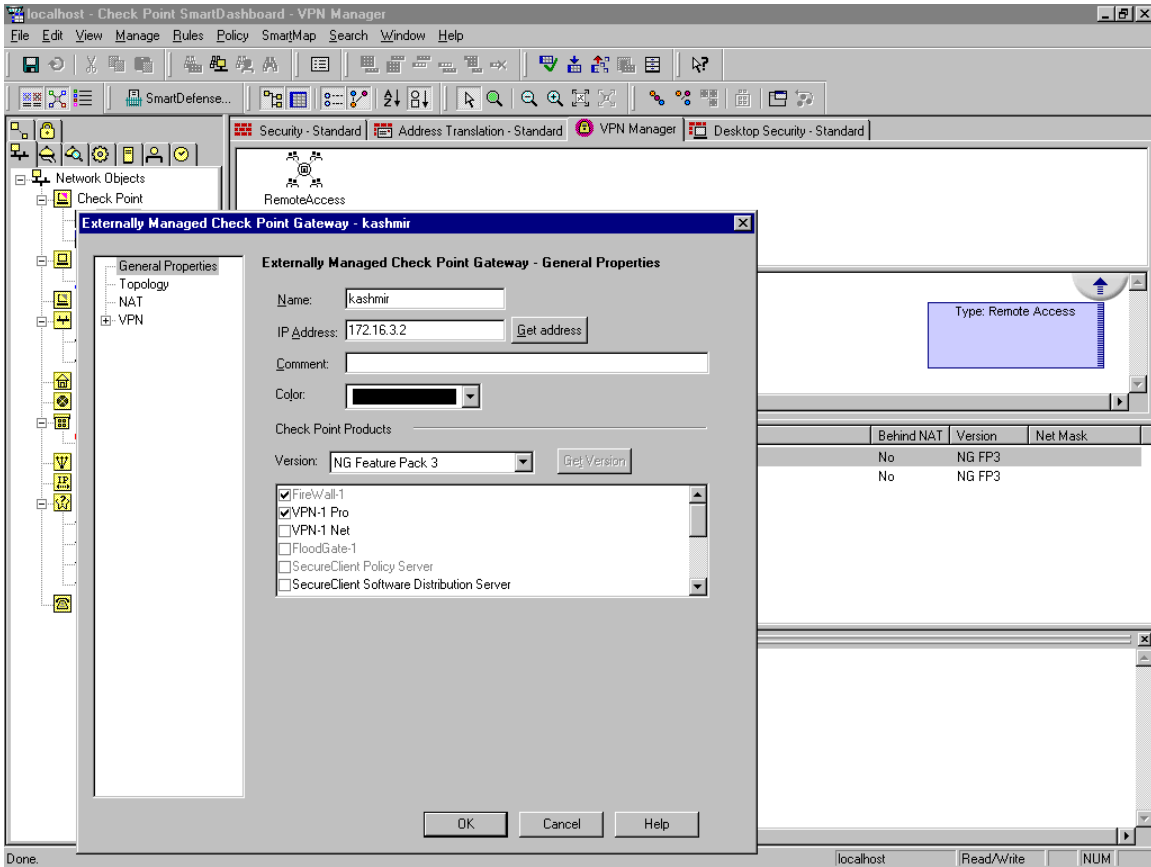


Figure 7

Define the topologies of your peer gateway properly (in our case Kashmir). Under VPN Domain, check the “All IP addresses behind Gateway based.....” box Figure 8.

Click OK once you are done.

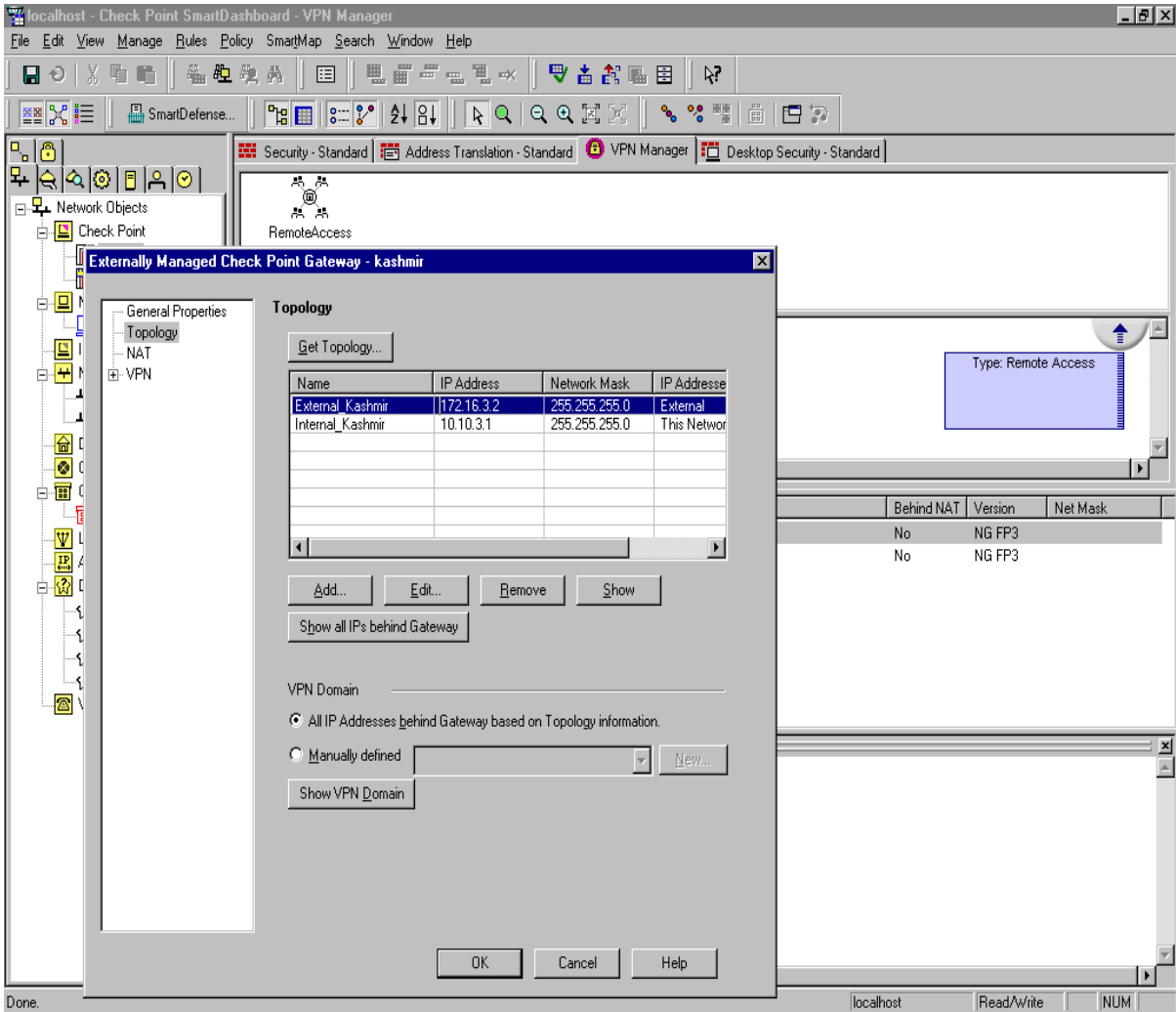


Figure 8

Defining VPN Communities

In the SmartDashBoard window click on VPN Manager tab and right click anywhere to define new VPN Community. You may also choose VPN Communities by clicking on Manage Menu.

If you right click in VPN manager window you will be presented with following window. Select New Communities→ Meshed. Figure 9

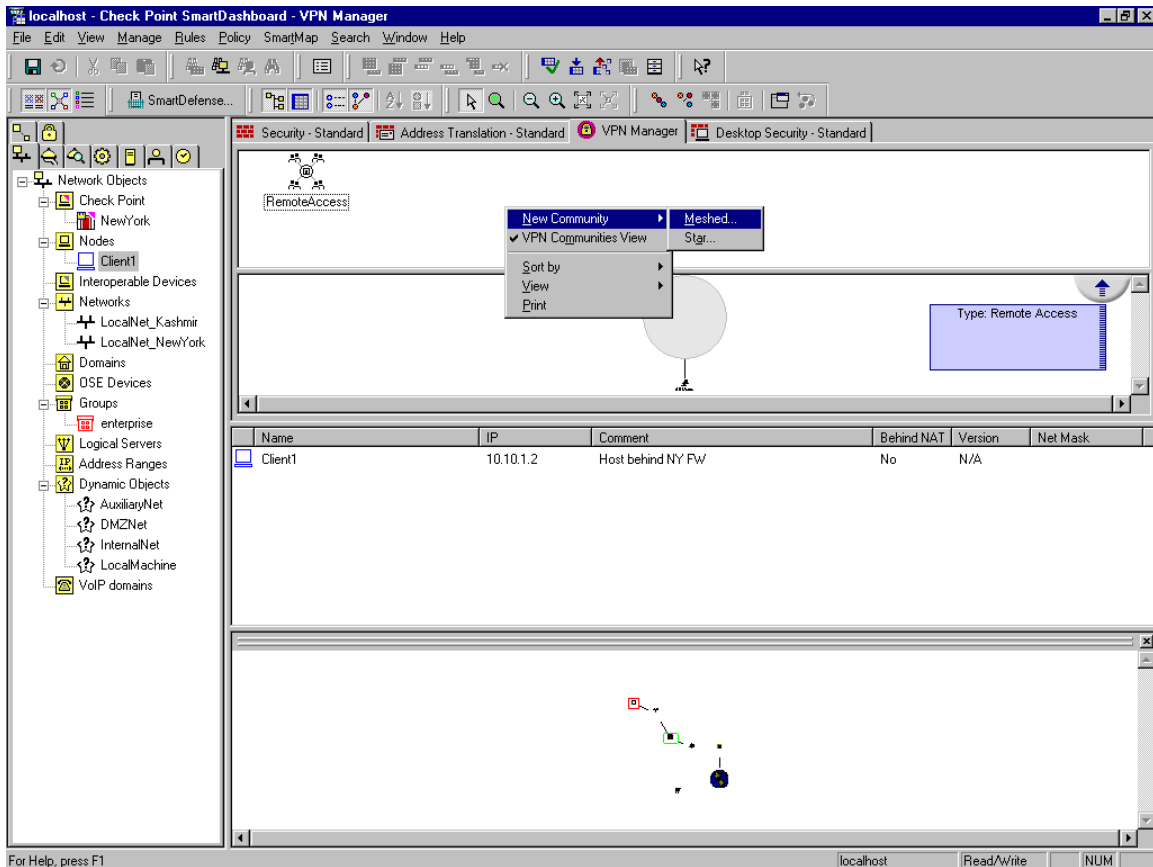


Figure 9:

As soon you click on Meshed, you will be presented with “Meshed Community Properties” window. Figure-10

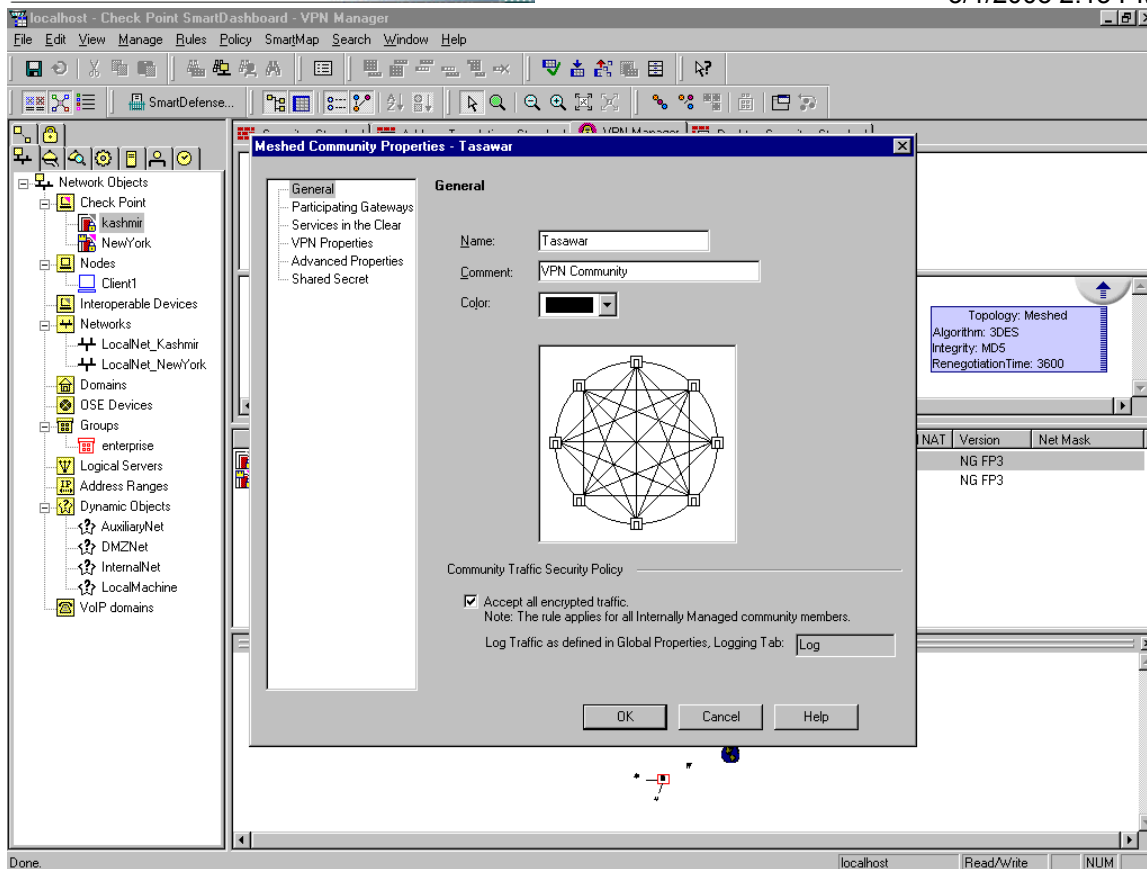


Figure-10

- Enter any name you want to call your VPN Community and add relevant comments.
Check **“Accept all encrypted traffic”** checkbox.
- Click on **“Participating Gateways”**, click on **Add**, select each Firewall and click OK once you have added both (NewYork and Kashmir). See Figure-11
- For this tutorial, you don’t need to modify **“Services in the Clear”** section.
- In the **“VPN Properties”** section you MUST make sure that all encryption and hashing algorithms you choose are the same when defining the peer VPN Community on Kashmir. Figure 12

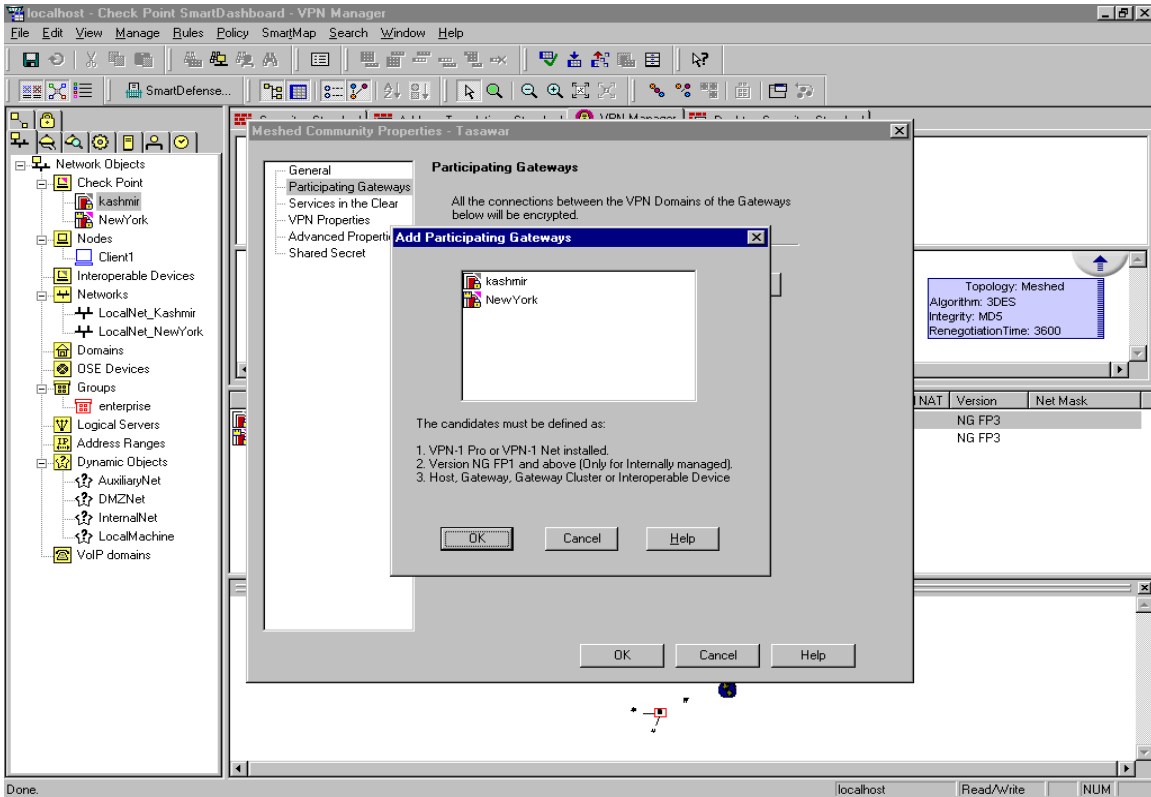


Figure 11

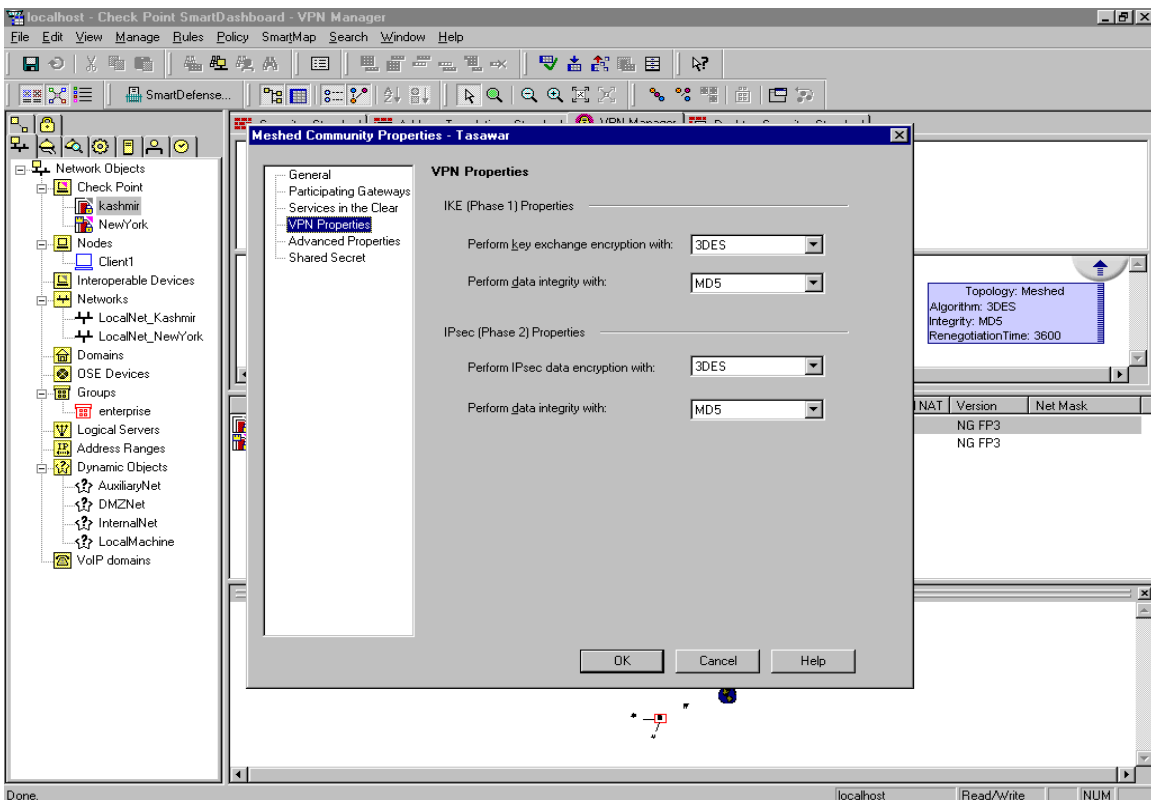


Figure 12

Click on “Shared Secret” and check “**Use only shared key for all external members**” box See Figure 13. Select peer GW and click edit, make sure the password is the one you intend to use, since there is no verification of passwords, if mistyped, once entered.

Click OK.

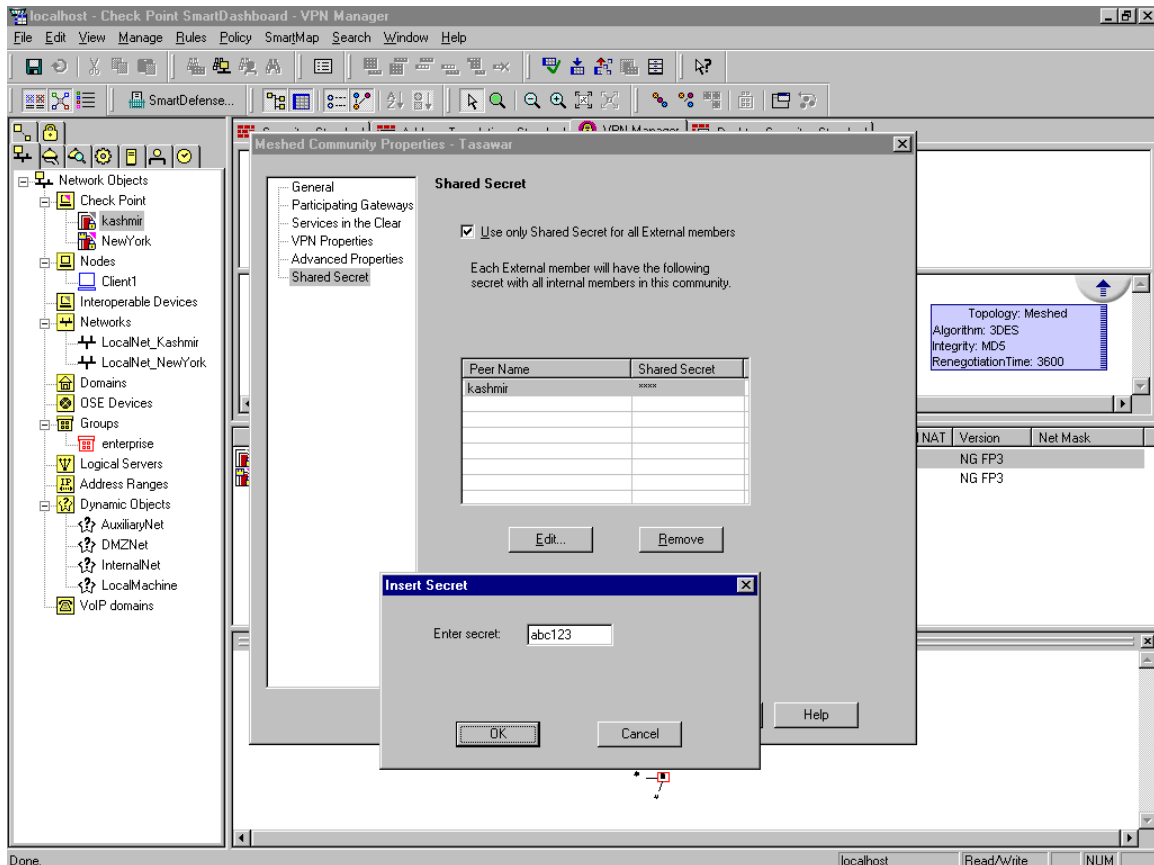


Figure 13

From the main menu, click on verify and install policy and if you don't receive any error's you are done.

You will repeat the same steps on the peer Gateway.

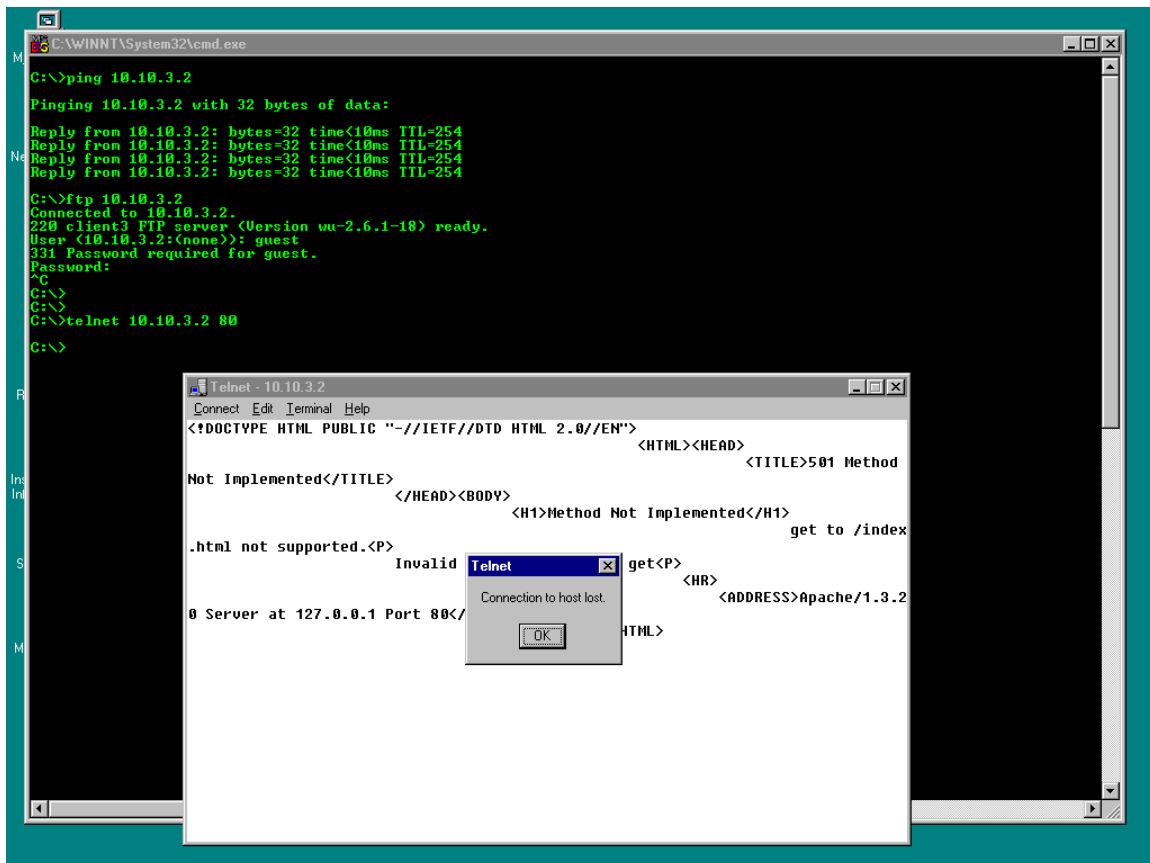
Testing the VPN Tunnel

Open the command line prompt from any host behind the firewall (NewYork). In our case it was client1 (10.10.1.2) and try:

- 1) Ping IP 10.10.3.2, which is a host behind Kashmir. See Figure 1
- 2) Telnet 10.10.3.2 @ port 80
- 3) [FTP 10.10.3.2](#)

You should be able to access all services transparently

PS: I have installed web server and FTP server on the host 10.10.3.2



```
C:\WINNT\System32\cmd.exe
C:\>ping 10.10.3.2
Pinging 10.10.3.2 with 32 bytes of data:
Reply from 10.10.3.2: bytes=32 time<10ms TTL=254
Reply from 10.10.3.2: bytes=32 time<10ms TTL=254
Reply from 10.10.3.2: bytes=32 time<10ms TTL=254
Reply from 10.10.3.2: bytes=32 time<10ms TTL=254
C:\>ftp 10.10.3.2
Connected to 10.10.3.2.
220 eliant3 FTP server (Version wu-2.6.1-18) ready.
User (10.10.3.2:(none)): guest
331 Password required for guest.
Password:
^C
C:\>
C:\>telnet 10.10.3.2 80
C:\>

Telnet - 10.10.3.2
Connect Edit Terminal Help
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
    <HTML><HEAD>
        <TITLE>501 Method
        Not Implemented</TITLE>
    </HEAD><BODY>
        <H1>Method Not Implemented</H1>
        .html not supported.<P>
        Invalid get<P>
        0 Server at 127.0.0.1 Port 80</
        <HR>
        <ADDRESS>Apache/1.3.2
        HTML>
```

Comments and Feedback:

I am sure this document has some errors. Please email all your questions or feedback to tasawar@securenode.com