:

CompTIA Security+® Lab Series

Lab 7: Configuring the pfSense Firewall

CompTIA Security+® Domain 1

Objective 1.1: Explain the security function and purpose of network devices and technologies
Objective 1.2: Apply and implement secure network administration principles

Document Version: 2013-08-02

Organization: Moraine Valley Community College
Author: Jesse Varsalone

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).

Contents

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to configure a pfSense software firewall.

This lab includes the following tasks:

1 – Configuring ICMP on the Firewall
2 – Redirecting Traffic to Internal Hosts on the Network
3 – Setting up a Virtual Private Network

Objectives: Explain the security function and purpose of network devices and technologies

Companies need to protect their internal resources. This is often done by using a hardware or software firewall. Certain types of traffic can be blocked or allowed through the firewall. Understanding how a firewall operates and its relationship to the internal and external networks is critical to having an understanding of network security.

ICMP – The Internet Control Message Protocol, or ICMP, is used by ping, tracert, and traceroute. Network utilities like ping and tracert can be used to test for connectivity. If ICMP is blocked by the firewall, testing for connectivity becomes more difficult.

Firewall – In Networking, a firewall is a software or hardware device that regulates traffic. Certain types of traffic can be blocked or allowed through the firewall.

Redirection – Most firewalls can be configured to allow incoming traffic on their external interfaces to be redirected to internal hosts.

NAT – Network Address Translation will allow internal hosts to reach the external network through a single IP address. Most firewalls can be configured to perform NAT.

Port Scanning – A Port Scan can be used to determine which ports are open and closed on the firewall. Tools like Nmap can be used to perform port scanning.

Pod Topology

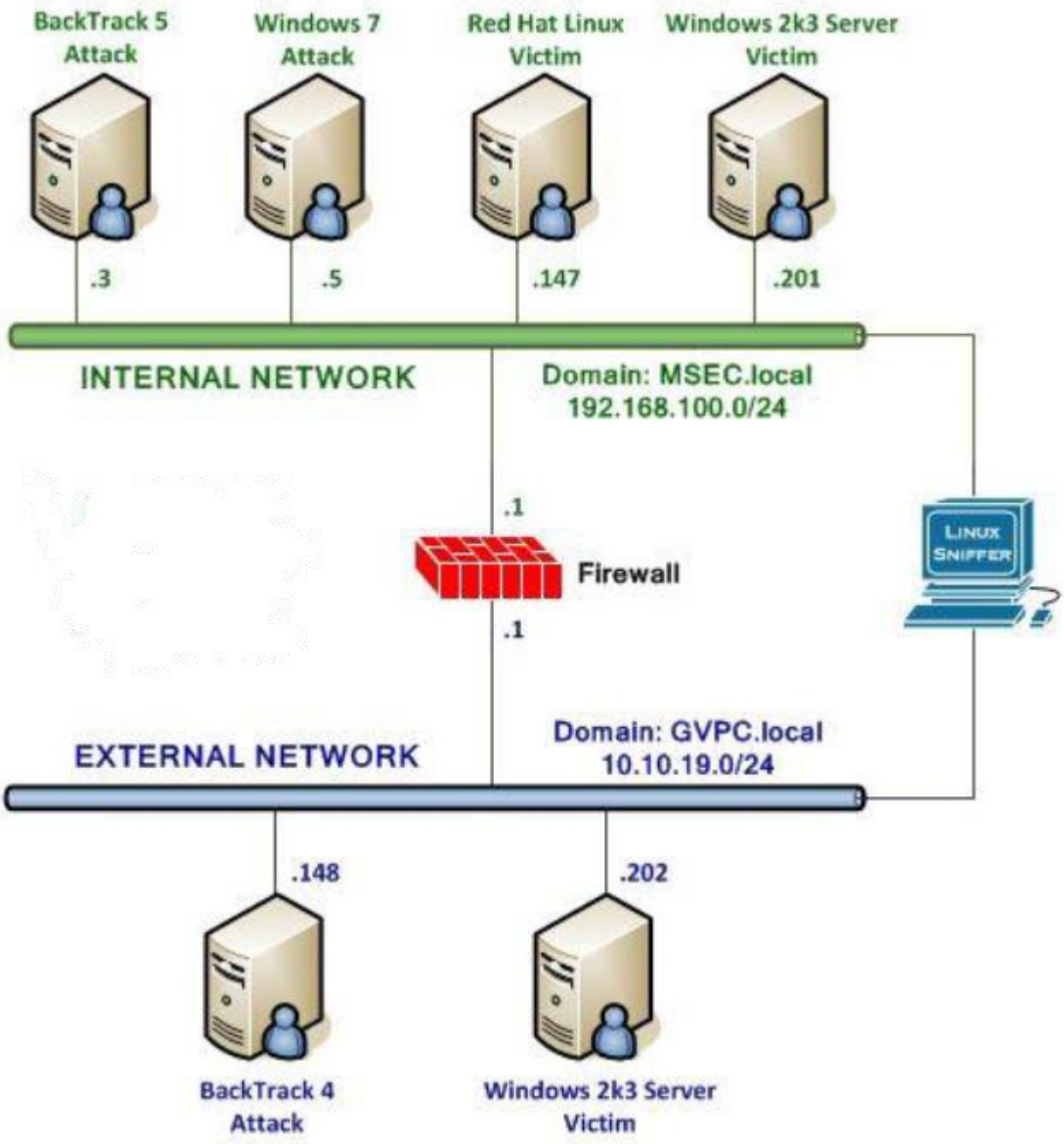


Figure 1: Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password
Red Hat Enterprise Linux Internal Victim Machine	192.168.100.147
Red Hat Enterprise Linux root password	password
pfSense Firewall	10.10.19.1 192.168.100.1
pfSense password	admin/pfsense
BackTrack 4 External Attack Machine	10.10.19.148
BackTrack 4 External root password	password
Windows 2k3 Server External Victim Machine	10.10.19.202
Windows 2k3 Server administrator password	password

BackTrack 5 Internal Attack Login:

1. Click on the **BackTrack 5 Internal Attack** icon on the topology.
2. Type **root** at the **bt login**: username prompt and press enter.
3. At the password prompt, type **password** and press **enter**.

Figure 2: BackTrack 5 login

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the **root@bt:~#** prompt and press **enter**.

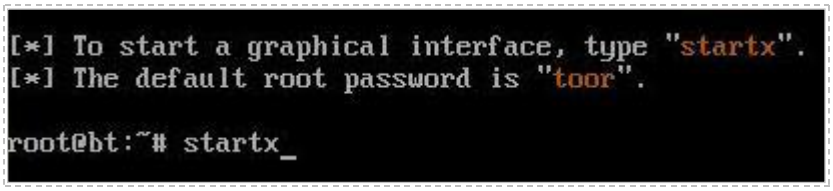


Figure 3: BackTrack 5 GUI start up

Windows 2003 Server Login: (internal and external victim machines):

1. Click on the **Windows2k3 Server Internal Victim** icon on the topology
2. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).
3. Enter the User name, **Administrator** (verify the username with your instructor).
4. Type in the password, **password**, and click the **OK** button (verify the password with your instructor).
5. **Repeat** these steps to log into the **Windows 2k3 Server External Victim**.

Figure 4: Windows 2k3 login

Red Hat Enterprise Linux Login:

1. Click on the **Red Hat Linux Internal Victim** icon on the topology.
2. Type **root** at the **rhel login:** prompt and press **Enter**.
3. Type **password** at the **Password:** prompt and press **Enter**.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the **[root@rhe ~]#** prompt and press **Enter**.

Figure 5: RHEL login

BackTrack 4 External Attack Login:

1. Click on the **BackTrack 4 External Attack** icon on the topology.
2. Type **root** at the **bt login:** username prompt and press enter.
3. At the password prompt, type **toor** and press **enter**.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the **stroot@bt:~#** prompt and press **enter**.

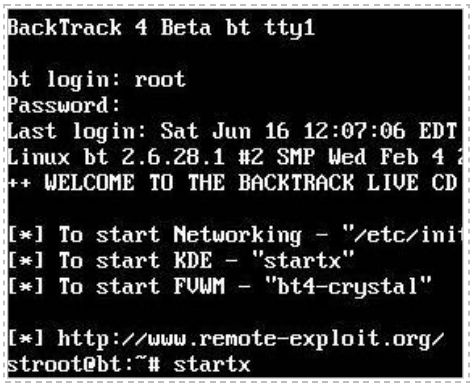


Figure 6: BackTrack 4 login

1 Configuring ICMP on the Firewall

There are many firewall solutions that companies can use. PfSense is an open source, FreeBSD based operating system, which requires minimal disk space. You can download the pfSense Live CD or Virtual Machine. It can be downloaded from the following link: http://www.pfsense.org/index.php?option=com_content&task=view&id=58&Itemid=4/

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Configuring ICMP on pfSense

1. Open a terminal on the BackTrack 4 External Attack Machine by clicking on the image to the left of Firefox in the task bar, in the bottom of the screen.

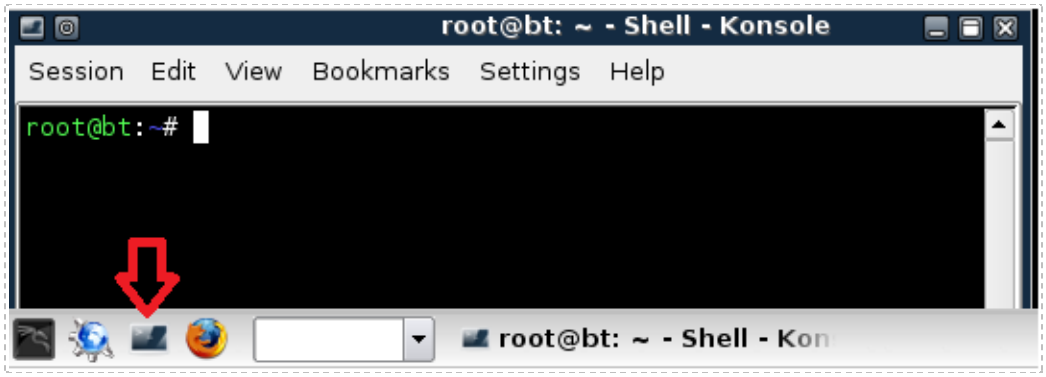


Figure 7: The BackTrack Terminal

2. Type the following to display the IP address for the Backtrack 4 External Attack Machine:
root@bt:~#**ifconfig**

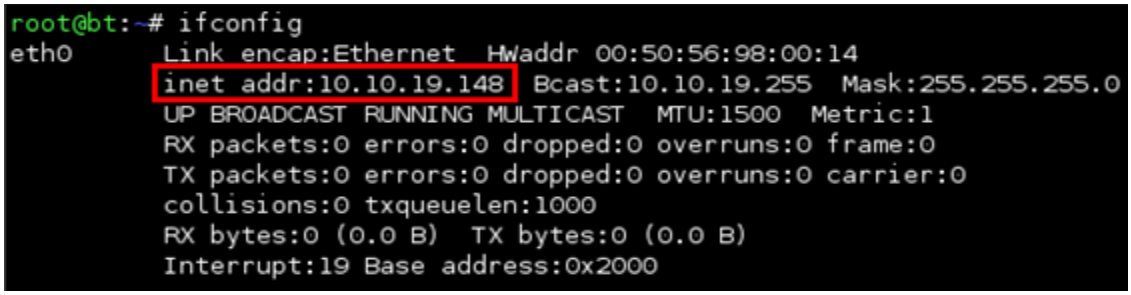


Figure 8: IP address of External BackTrack

3. Log on to the **Windows 2k3 Server Internal Victim Machine**. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log on with the username of **Administrator** and the password of **password**.

If you have already logged into the machine, as described in the Lab Settings section, you may skip this step.

Figure 9: Send Ctrl-Alt-Del to the Windows 2003 Server

4. Double-click the shortcut to the command prompt icon on the Windows 2003 desktop.

Figure 10: Windows 2003 Command Prompt

5. Type the following command to view your IP address:
   C:\>**ipconfig**

```
Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.100.201
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
```

Figure 11: The IP address information

6. From the **Windows 2k3 Server Internal Victim Machine**, ping the internal pfSense IP address by typing:
   C:\>**ping 192.168.100.1**

```
C:\>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 12: Pinging the Internal Address of the Firewall

7. From the **Windows 2k3 Server Internal Victim Machine**, ping the external BackTrack IP address by typing:
   C:\>**ping 10.10.19.148**

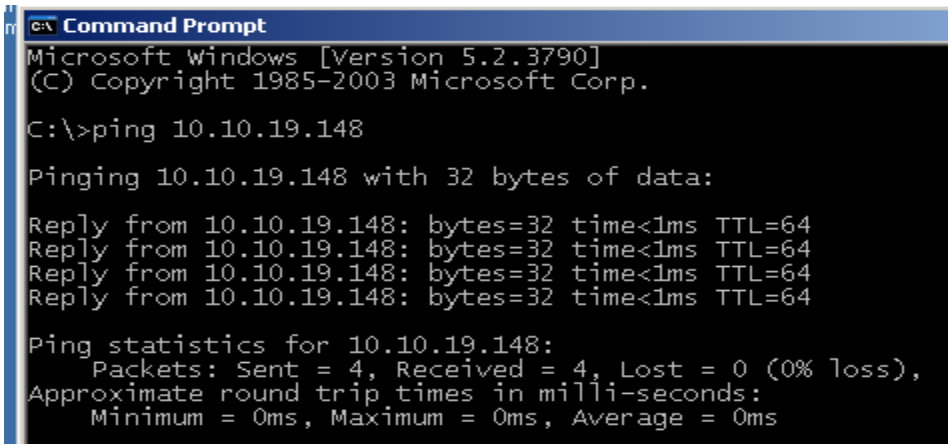


Figure 13: Pinging the External IP address

Internet Control Message Protocol, or ICMP, is allowed from any of the four Internal clients to the two machines on the External Network. While ICMP is commonly allowed out within most organizations, I have worked in several places where you cannot ping out.

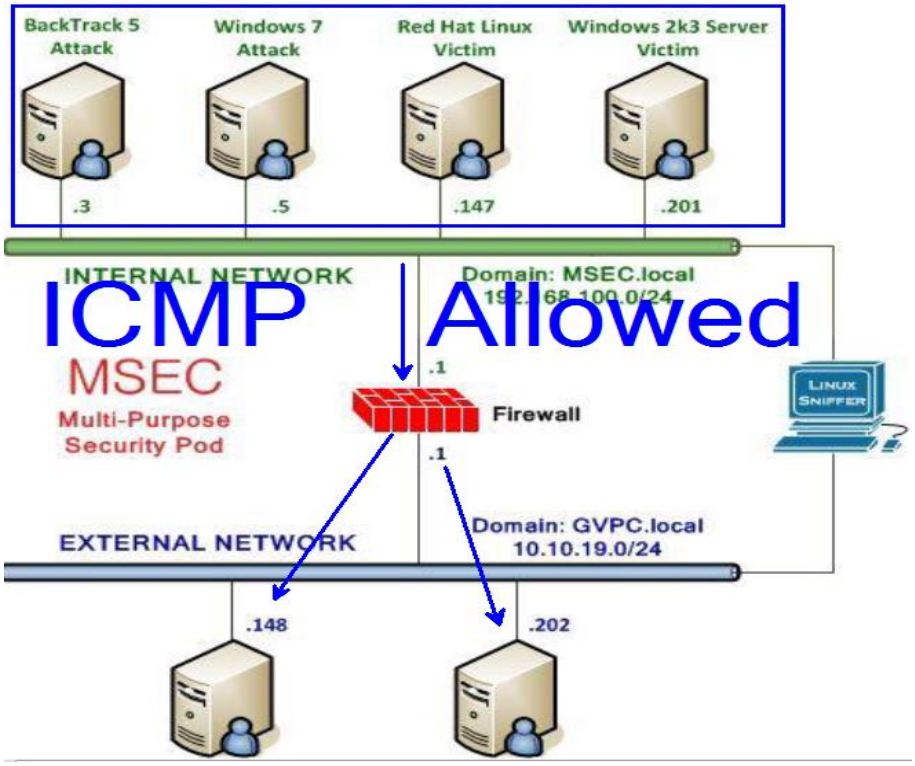


Figure 14: ICMP is Allowed OUT

Now that we have determined ICMP is allowed out, it is also a good idea to determine which TCP ports on the pfSense firewall are accessible to clients on the internal network. Although the pfSense firewall is fairly locked down, some ports are accessible internally.

8. To determine what ports are accessible on the internal network, login to the **BackTrack 5 Internal Attack Machine** with the username **root** and the password of **password**.

Skip to the next step if you have already logged into the machine.

9. Open a terminal window and type:
   root@bt:~#**nmap 192.168.100.1**

```
root@bt:~# nmap 192.168.100.1

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2013-05-21 11:25 EDT
Nmap scan report for pfSense.localdomain (192.168.100.1)
Host is up (0.00030s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:21:4A:E0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.67 seconds
```

Figure 15: Two TCP ports are Accessible Internally

An internal scan reveals that only 2 TCP ports are accessible from the Internal Network

Protocol	Port Number
Domain Name System	53
Hyper Text Transfer Protocol	80

The default settings of pfSense keep the external settings fairly locked down. By default, external machines will not be able to ping the external IP of the firewall.

10. From the **Windows 2k3 Server External Victim Machine**, attempt to ping pfSense by typing:
    C:\>**ping 10.10.19.1**

```
C:\>ping 10.10.19.1

Pinging 10.10.19.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.19.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 16: The Pings Fail

11. On the **BackTrack 4 External Attack Machine,** Determine if the pfSense firewall is allowing any incoming ports by typing:
    root@bt:~**#nmap 192.168.100.1**

```
root@bt:~# nmap 10.10.19.1

Starting Nmap 4.68 ( http://nmap.org ) at 2013-05-27 18:40 EDT
All 1717 scanned ports on 10.10.19.1 are filtered
MAC Address: 00:0C:29:21:4A:EA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 49.80 seconds
```

Figure 17: No Ports are Open

We will now configure the pfSense Firewall to allow ICMP from external hosts.

12. On the **Red Hat Enterprise Linux Internal Victim Machine**, open Firefox by clicking **Applications** in the top left menu, selecting **Internet**, then selecting **Firefox Web Browser**.

Figure 18: Opening Firefox

13. Type the following URL in the browser: http://192.168.100.1

Figure 19: Opening pfSense

14. For the username, type **admin**. For the password, type **pfsense**. Click **Login**.

Figure 20: Logging in to pfSense

15. From the **Interfaces** Tab of pfSense, select **Wide Area Network (WAN).**

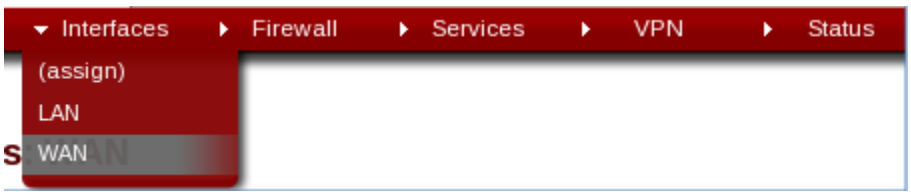


Figure 21: The WAN Interface

16. Scroll down to **Private Networks**. Uncheck the option to **Block Private Networks** and click **Save.**

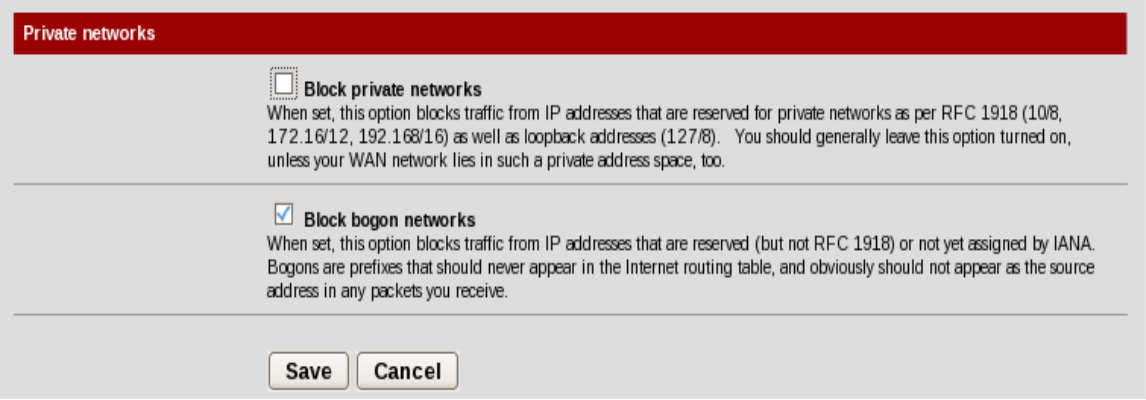


Figure 22: Unchecking Block Private Networks

17. In order for the new configuration to take effect, click the **Apply changes** button.

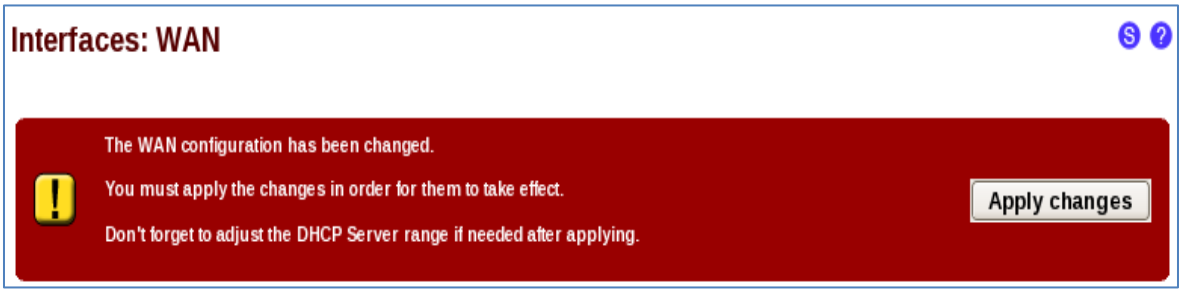


Figure 23: Applying the New Configuration

18. Create a rule to allow incoming ICMP traffic by selecting **Firewall**, then **Rules**.

Figure 24: Configuring Firewall Rules

19. Click the **+** button to create a new Firewall rule for the WAN interface.

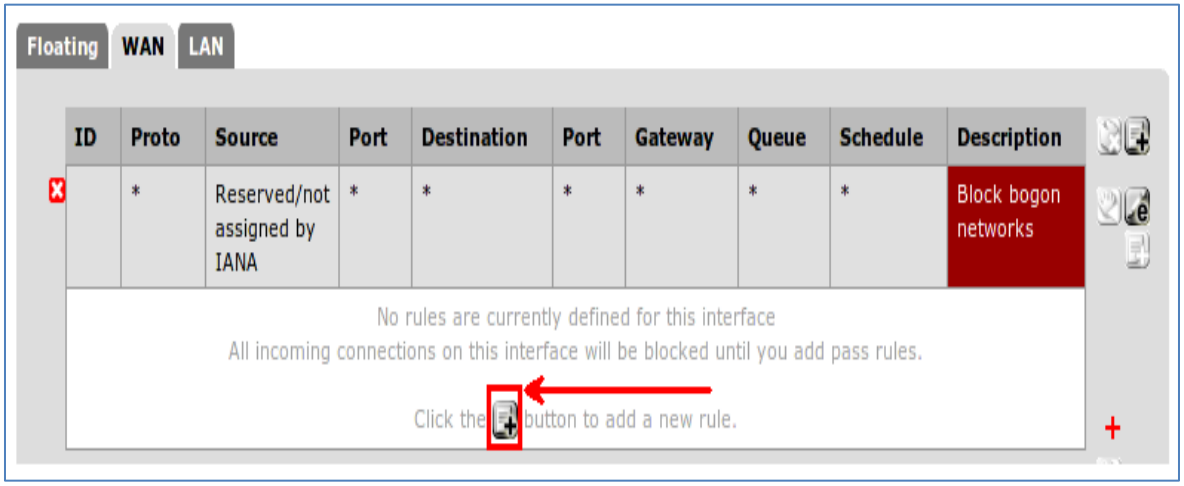


Figure 25: Adding a New Rule

20. In the **Protocol** menu, select **ICMP** from the dropdown box. In order to save the changes, click the **save** button directly above the **Advanced features** section.

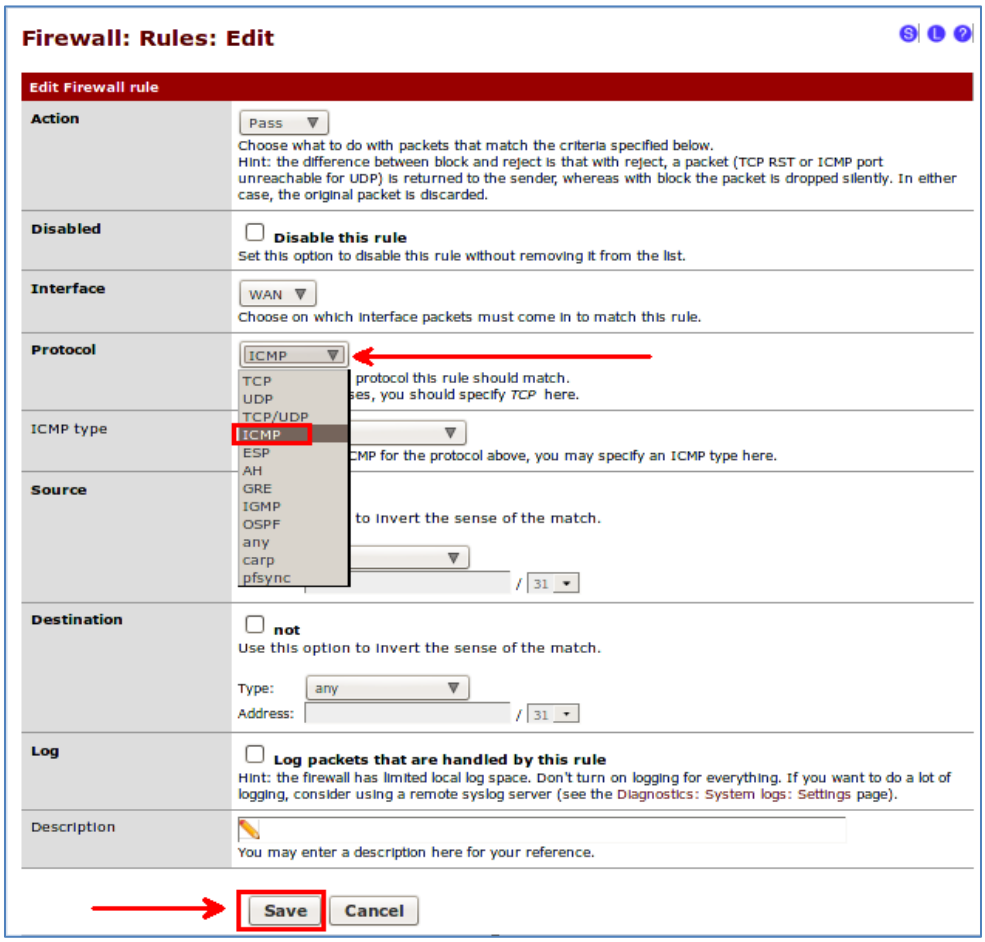


Figure 26: Saving the New Rule

21. In order for the new configuration to take effect, click the **Apply changes** button.

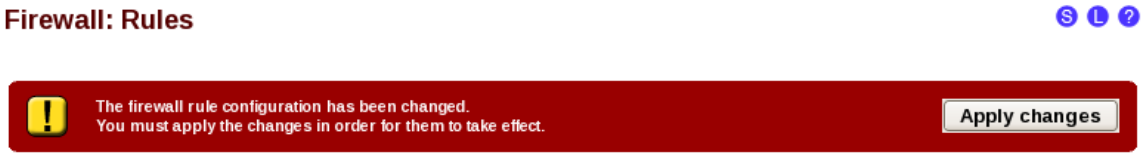
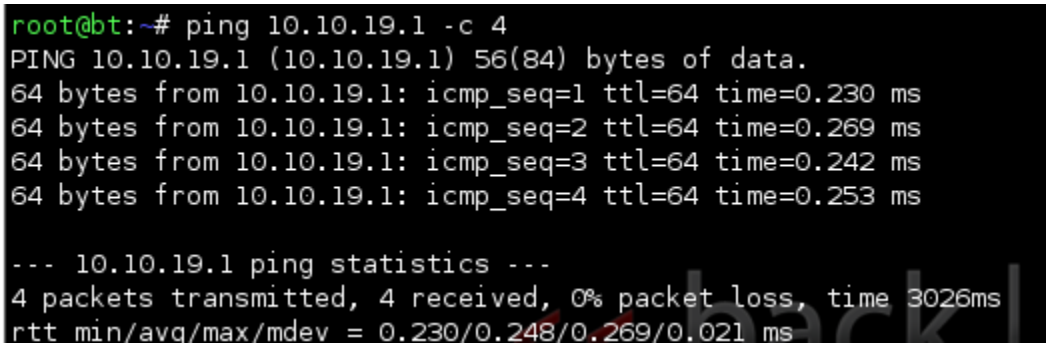


Figure 27: Applying the Changes

22. From the **BackTrack 4 External Attack Machine**, attempt to ping 10.10.19.1



```
root@bt:~# ping 10.10.19.1 -c 4
PING 10.10.19.1 (10.10.19.1) 56(84) bytes of data.
64 bytes from 10.10.19.1: icmp_seq=1 ttl=64 time=0.230 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.269 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=0.242 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=0.253 ms

--- 10.10.19.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3026ms
rtt min/avg/max/mdev = 0.230/0.248/0.269/0.021 ms
```

Figure 28: Successfully Pining the Firewall's External IP address

After configuring the firewall, the pings to the eternal interface should be successful.

1.2 Conclusion

With a firewall, both incoming and outgoing traffic can be limited. In most cases, the incoming traffic will be much more restricted than the outgoing. In the example covered in Task 1, outgoing ICMP traffic was allowed while incoming ICMP traffic was blocked. By configuring the firewall, we allowed incoming ICMP traffic.

1.3 Discussion Questions

1. What does ICMP stand for?
2. By default, how many TCP ports are open on a pfSense internal interface?
3. By default, how many TCP ports are open on a pfSense external interface?
4. What needs to be done in order for rule changes to take effect on pfSense?

2 Redirecting Traffic to Internal Hosts on the Network

In many cases when a firewall is implemented, systems will re-direct traffic to machines on the internal network hosting various internal services. This is done by configuring a firewall to allow a port and by re-directing requests to clients on the internal network.

2.1 Configuring a Firewall to Allow a Port and Re-directing Requests

1. Red Hat Enterprise Linux Internal Victim Machine. From the **pfSense** menu, choose **Firewall**, then choose **NAT** from the menu.

Figure 29: Network Address Translation

2. From the **Firewall: NAT: Port Forward** menu, click the **+** button on the right.

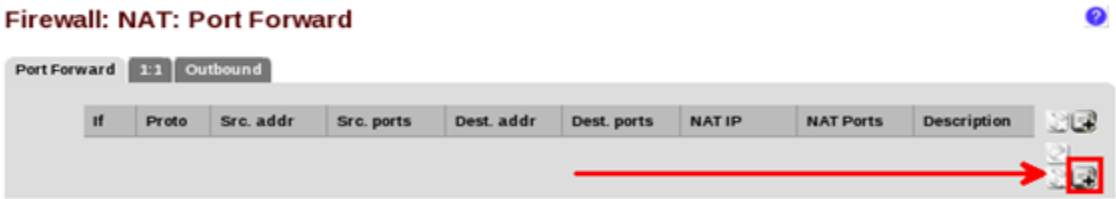


Figure 30: NAT Port Forward Menu

3. In the **Firewall: NAT: Port Edit** menu, Change only these three options:

   - Change Destination port range to **SSH** in the dropdown box menu
   - Change Redirect Target IP to **192.168.100.147** (Internal Red Hat Machine)
   - Change Redirect Target Port to **SSH** in the dropdown box menu

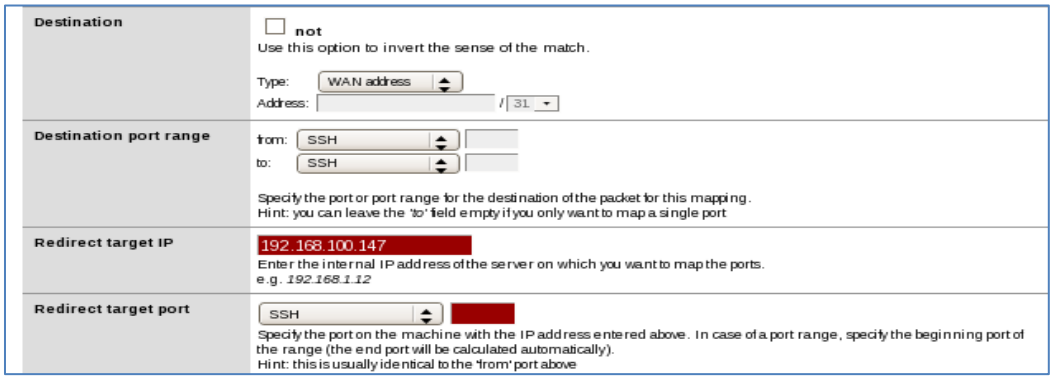


Figure 31: Setting the Redirected IP and Port

4. Click **Save**. In order for the new configuration to take effect, click the **Apply changes** button.

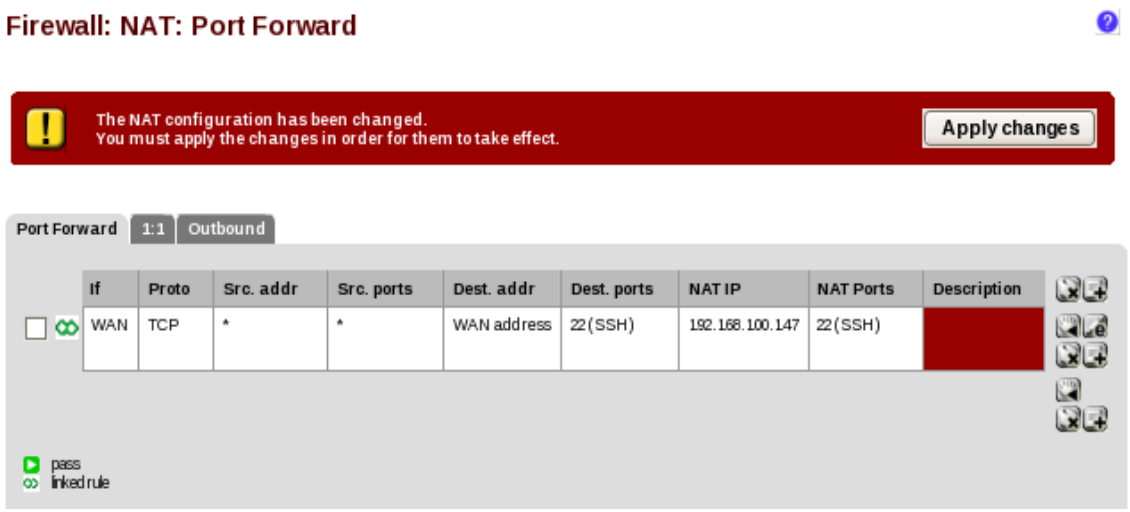


Figure 32: Applying the Changes

5. On the **BackTrack 4 External Attack Machine,** Determine if the pfSense firewall is allowing any incoming ports by typing:
root@bt:~**#nmap 10.10.19.1**

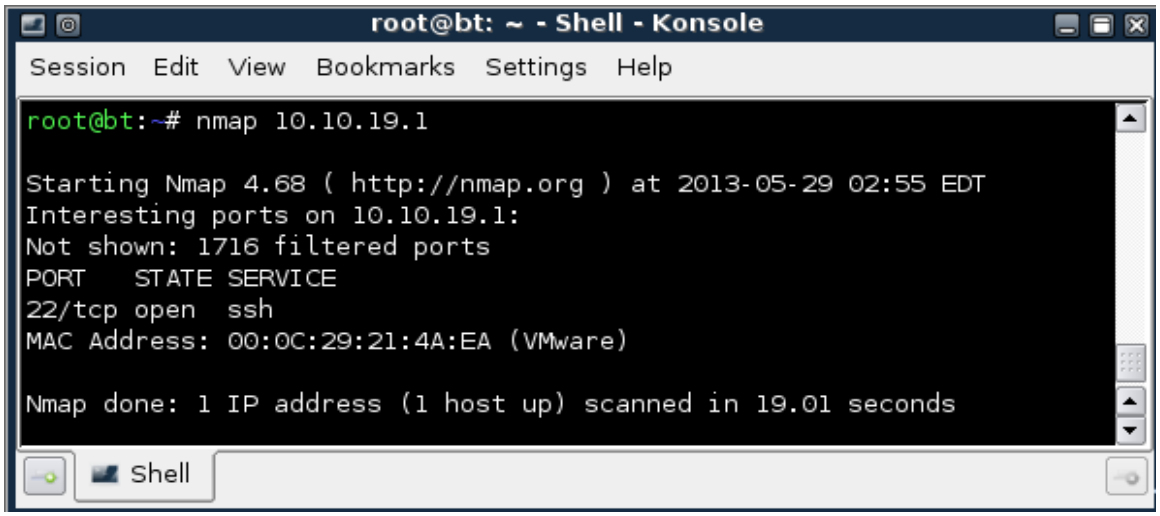


Figure 33: Port 22 is Now Open

During the scan prior to configuring the Firewall: NAT: Port Forward no ports were accessible from the external network. Port 22 (SSH) is now accessible to external clients.

When clients from the 10.10.19.0/24 network connect to the IP address of the pfSense firewall of 10.10.19.1, they will be redirected to the Internal Red Hat Linux machine.

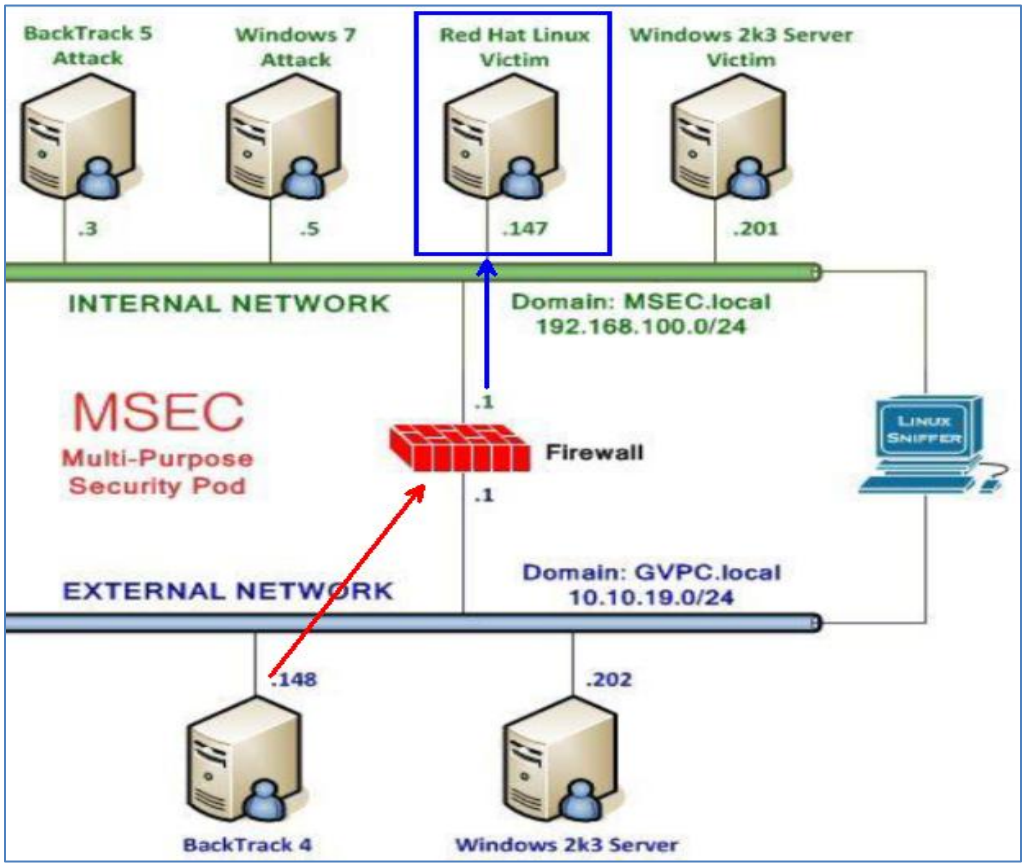


Figure 34: Redirection Explained

6. On the **BackTrack 4 External Attack Machine**, Verfiy the configuration on the pfSense firewall by typing the following:
   root@bt:~**#ssh 10.10.19.1**

7. Type **yes** when you are asked if you are sure you want to continue connecting.
8. When you are prompted for the root@10.10.19.1's password, type **password.**

```
root@bt:~# ssh 10.10.19.1
The authenticity of host '10.10.19.1 (10.10.19.1)' can't be established.
RSA key fingerprint is 21:88:ba:44:07:d8:69:62:12:5f:49:f3:cc:ac:a3:24.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.19.1' (RSA) to the list of known hosts.
root@10.10.19.1's password:
Last login: Thu Apr  4 21:53:15 2013
```

Figure 35: SSH Connection to the Remote Host

9. Verify you are on the correct internal machine by typing the following command: root@bt:~#**ifconfig**

```
[root@rhel ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:B0:4B:38
          inet addr:192.168.100.147  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:67266 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10258 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14627271 (13.9 MiB)  TX bytes:1189354 (1.1 MiB)
          Interrupt:67 Base address:0x2024
```

Figure 36: IP address

Although the external configuration has been changed, performing an Nmap scan on the *Internal* network will indicate that the ports that are accessible remains the same.

10. To determine what ports are accessible on the internal network, on the **BackTrack 5 Internal Attack Machine** type: root@bt:~#**nmap 192.168.100.1**

```
root@bt:~# nmap 192.168.100.1

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2013-05-21 11:25 EDT
Nmap scan report for pfSense.localdomain (192.168.100.1)
Host is up (0.00030s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:21:4A:E0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.67 seconds
```

Figure 37: Two TCP Ports are Accessible Internally

2.2 Conclusion

Firewalls are often configured to redirect traffic to hosts on the internal network. Even though external clients are connecting to the IP address of the pfSense firewall, they will be redirected to a machine hosting the given service on the internal network.

2.3 Discussion Questions

1. In what section of the pfSense firewall is internal redirection configured?
2. What tool can be utilized to verify ports have been open on the firewall?
3. Does changing the external configuration change the accessible internal ports?
4. What utility can be utilized to determine which internal machine you are on?

3 Setting up a Virtual Private Network

A Virtual Private Network (VPN) allows clients from an external network to connect to and utilize the resources of an internal network. Virtual Private Networks, which are encrypted, allow individuals to work from remote locations. The encryption of a Virtual Private Network allows external users to access internal resources in a secure manner.

A VPN can be configured on the pfSense Firewall to allow external users to access internal resources on the network. After connecting to the firewall, the external user will be assigned an internal IP address on the 192.168.100.0/24 network.

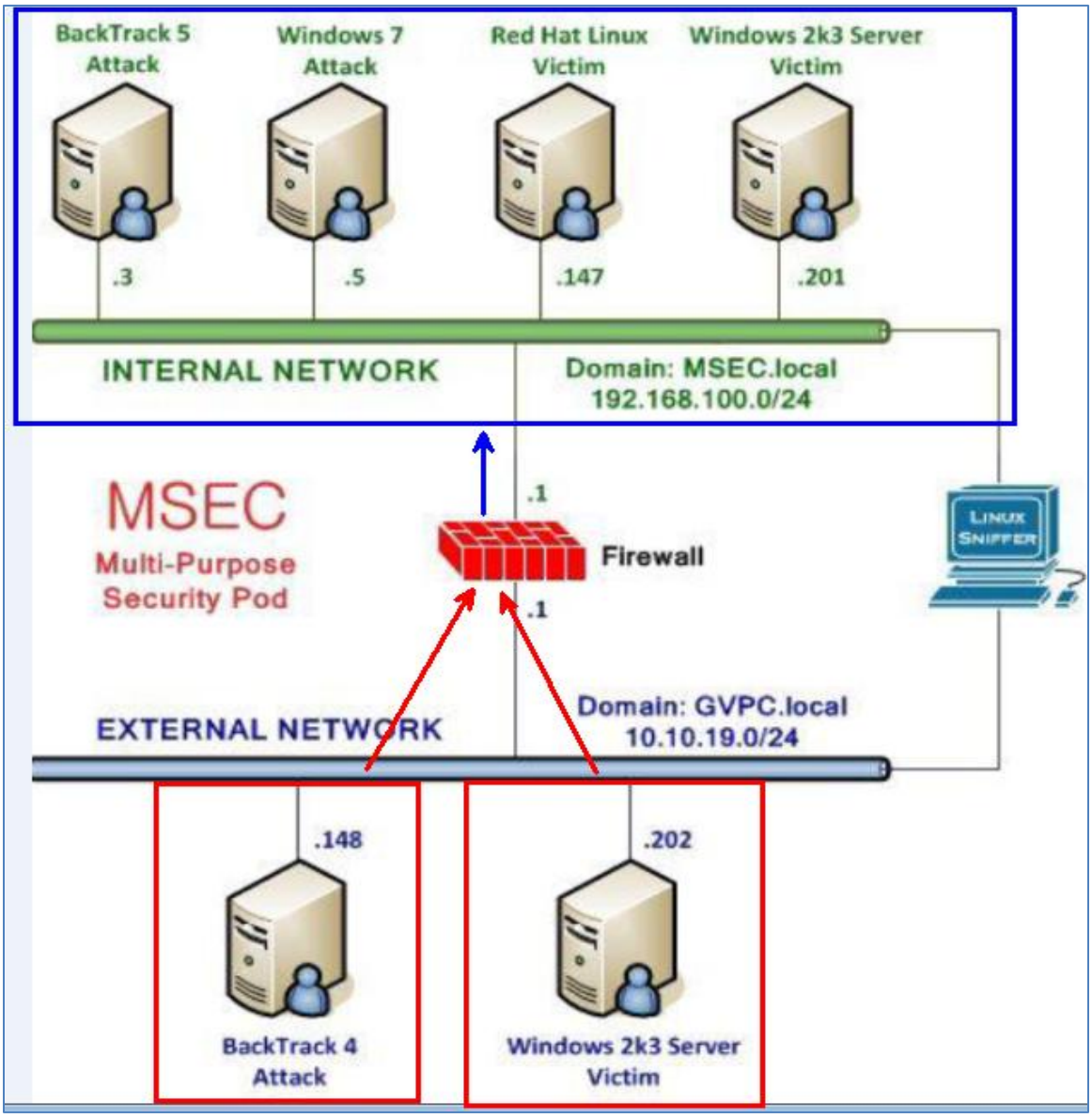


Figure 38: Virtual Private Network Explanation

3.1 Configure the pfSense Firewall to allow Virtual Private Network Traffic

1. On the Internal BackTrack machine open Firefox by clicking **Applications** in the top left menu, selecting **Internet**, then selecting **Firefox Web Browser**.

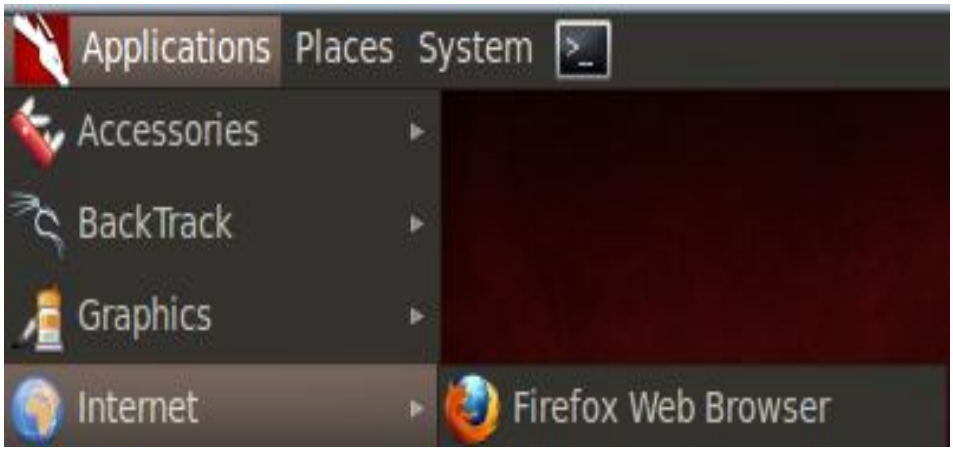


Figure 39: Opening Firefox

2. Type the following URL in the browser: http://192.168.100.1

Figure 40: Opening pfSense

3. For the username, type **admin**. For the password, type **pfsense**. Click Login.

Figure 41: Logging in to pfSense

Two of the most common tunneling protocols for Virtual Private Networks are:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)

4. From the **VPN** Tab of pfSense, select **PPTP**.

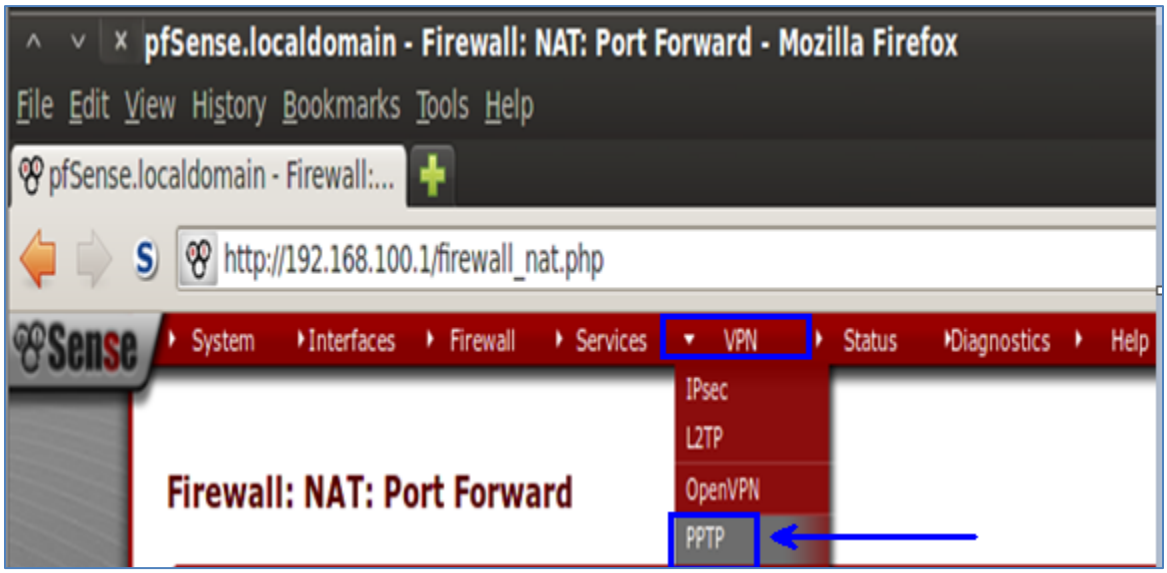


Figure 42: Selecting PPTP

5. Click the radio button next to **Redirect incoming PPTP connection to:** which will allow incoming PPTP connections, In the **PPTP redirection** box, type **192.168.1.201**, which is the IP address of the Internal Windows 2k3 Server Victim machine. Scroll down to the bottom of the web page and click the **save** button.

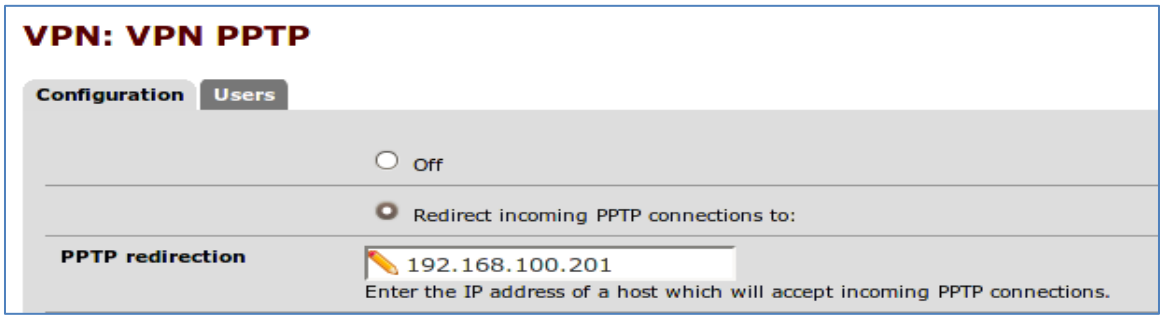


Figure 43: Allowing Redirection to the Client

6. Create a rule to allow incoming PPTP traffic by selecting **Firewall**, then **Rules**.

Figure 44: Configuring the Firewall Rules

7. Click the **+** button to add a new firewall rule to allow incoming PPTP Traffic.

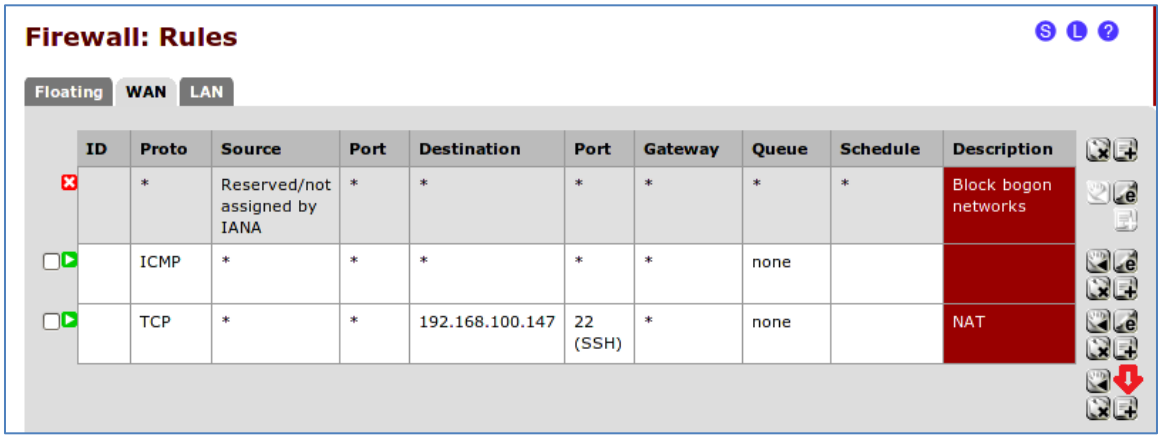


Figure 45: Adding a Firewall Rule

7. In the **Firewall: Rules: Edit** menu, make the following configuration changes:

   - In the Destination area, select **Single host or alias** from the drop down box.
   - In the Address box, type **192.168.100.201**
   - In the Destination port range, select **PPTP** from the drop down box.

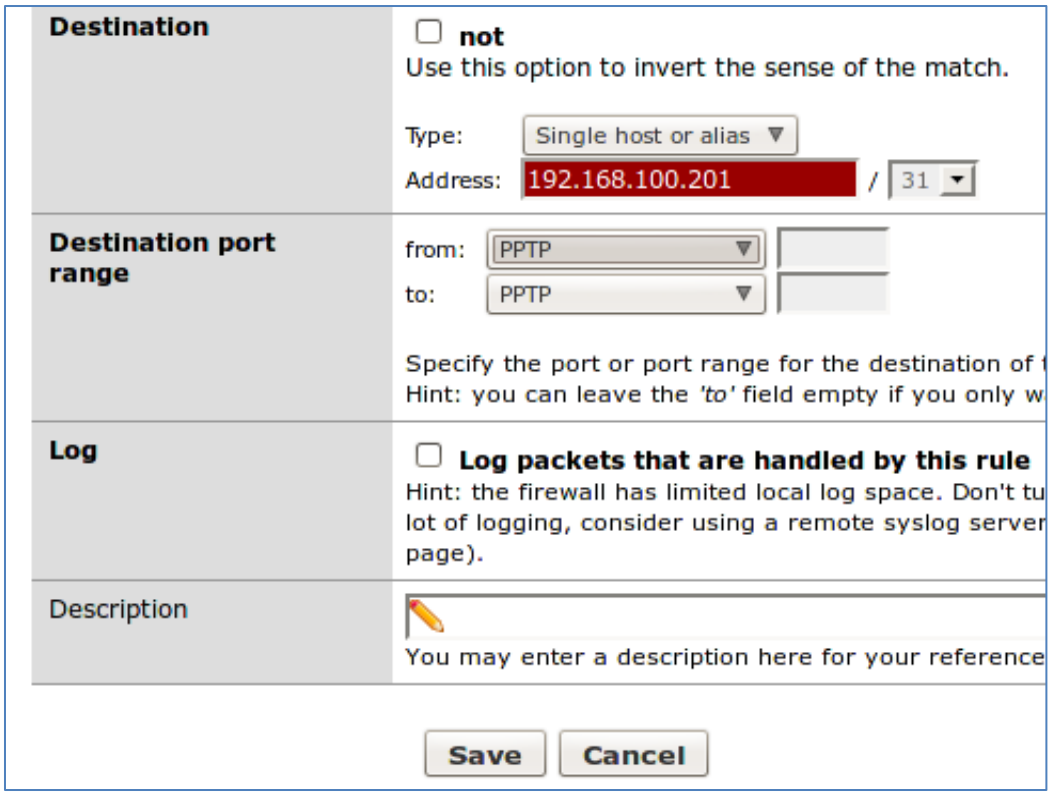


Figure 46: Configuring the Firewall to allow PPTP Traffic

8. Click **Save.** In order for the changes to take effect, click the **Apply Changes** button.

Figure 47: Applying the Changes

11. On the BackTrack 4 External Attack Machine, determine if the pfSense firewall is allowing any incoming ports by typing:
    root@bt:~#**nmap 10.10.19.1**

```
root@bt:~# nmap 10.10.19.1

Starting Nmap 4.68 ( http://nmap.org ) at 2013-06-07 23:15 EDT
Interesting ports on 10.10.19.1:
Not shown: 1715 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
1723/tcp closed pptp
MAC Address: 00:0C:29:21:4A:EA (VMware)
```

Figure 48: Scanning the External IP of the Firewall using Nmap

Now, ports 22 (Secure Shell), and PPTP (Point-to-Point Tunneling Protocol) are shown After we configure PPTP on the 192.168.100.201, thee port state will change to open. Next we will configure a PPTP Server on the Windows 2k3 Server Internal Victim Machine. Options such as NAT and PPTP can be configured in Routing and Remote Access in Windows.

10. On the **Windows 2k3 Server Internal Victim Machine**, click on **Start**, select **Administrative Tools** and select **Routing and Remote Access.**

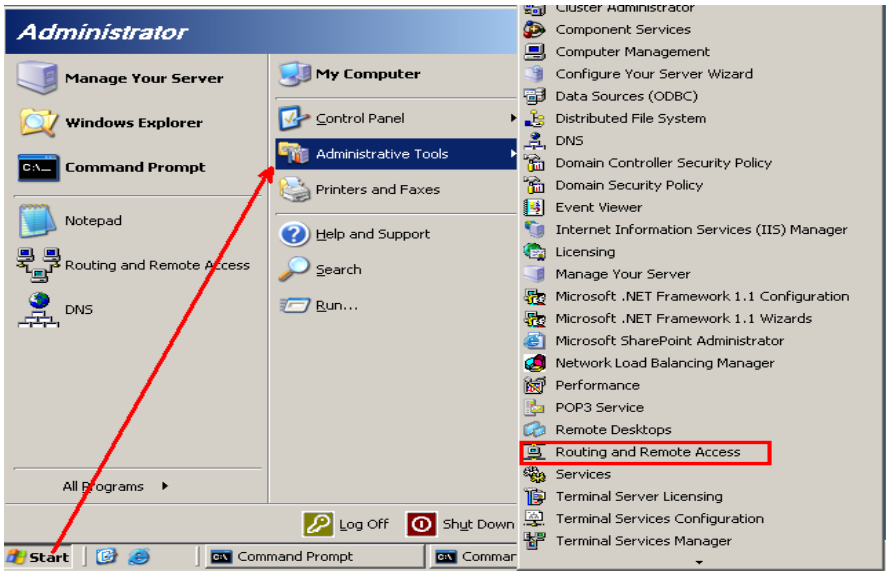


Figure 49: Opening Routing and Remote Access

11. Right-click on **WIN2k3DC** and select **Configure and Enable Routing and Remote Access**

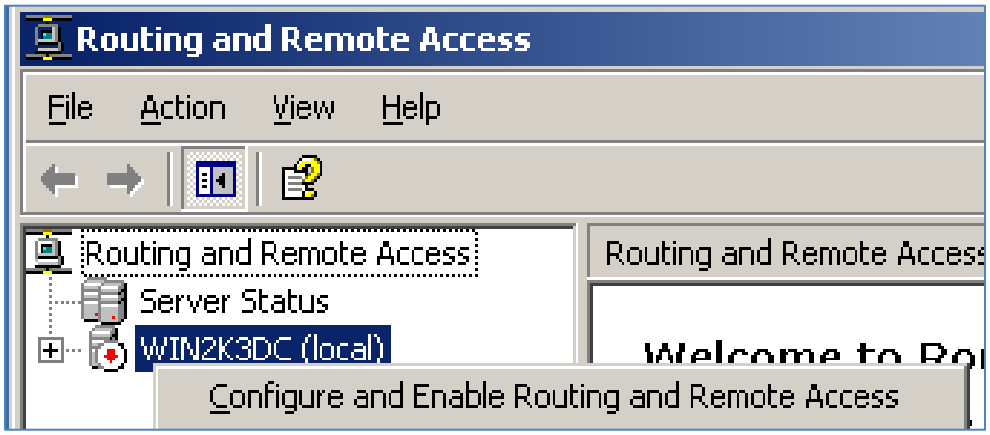


Figure 50: Configuring Routing and Remote Access

12. At the Routing and Remote Access Server Setup Wizard, click **Next**.

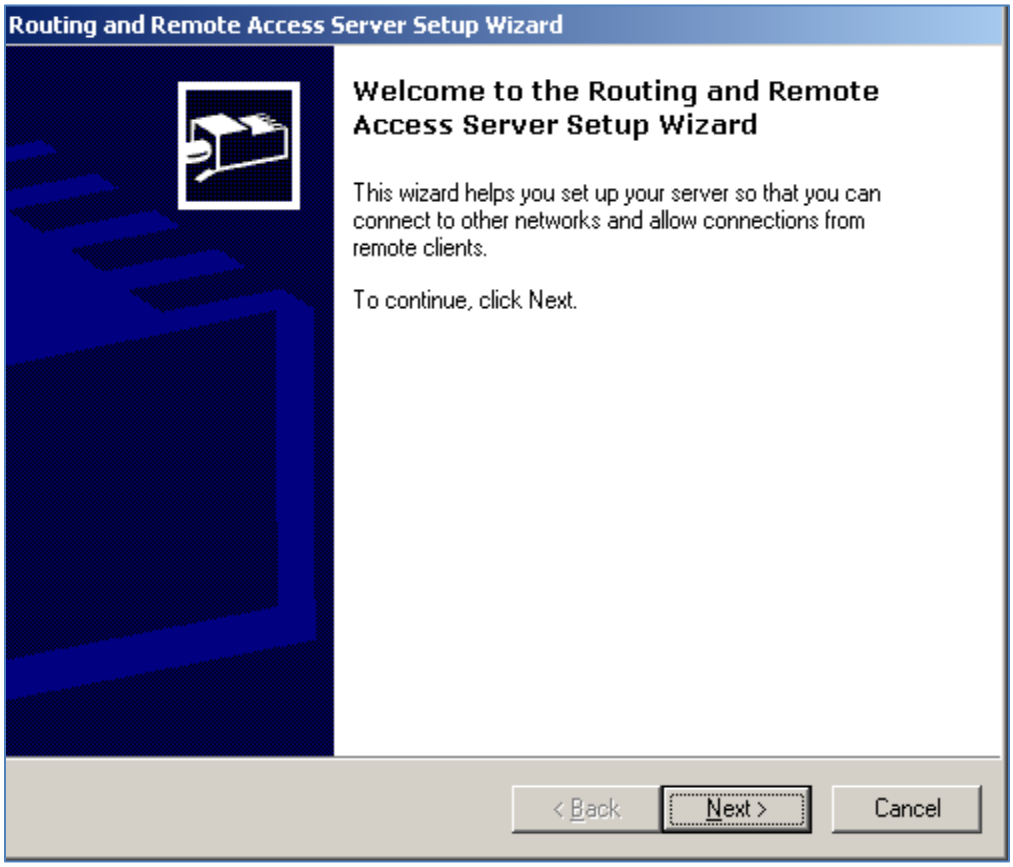


Figure 51: Remote Access Server Setup Wizard

13. At the configuration screen, select **Custom configuration** and click **Next**.

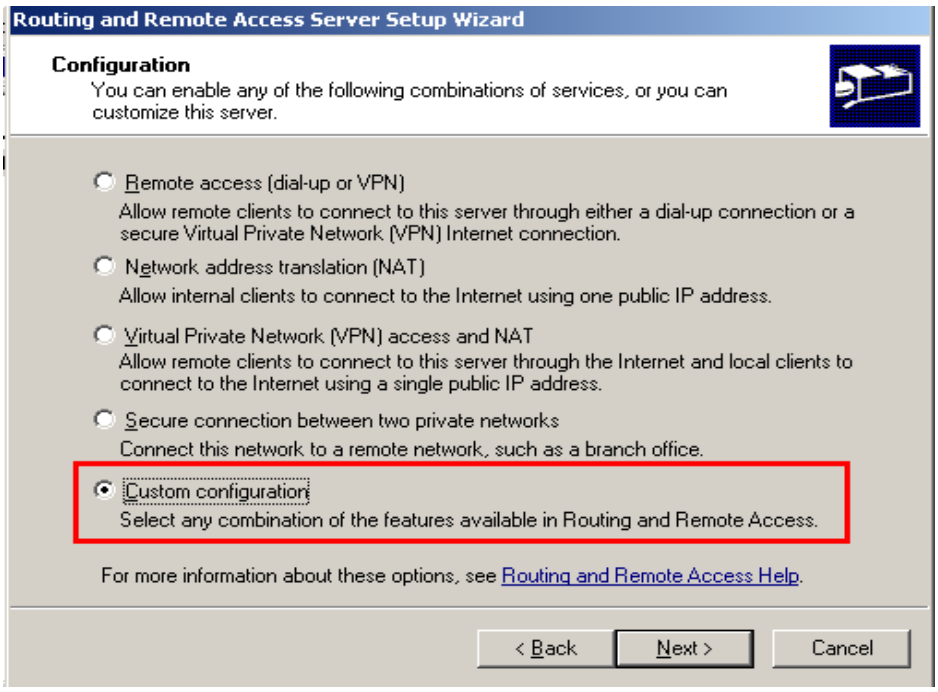


Figure 52: Custom Configuration

14. At the Custom Configuration, check the **VPN access** checkbox and click **Next**.

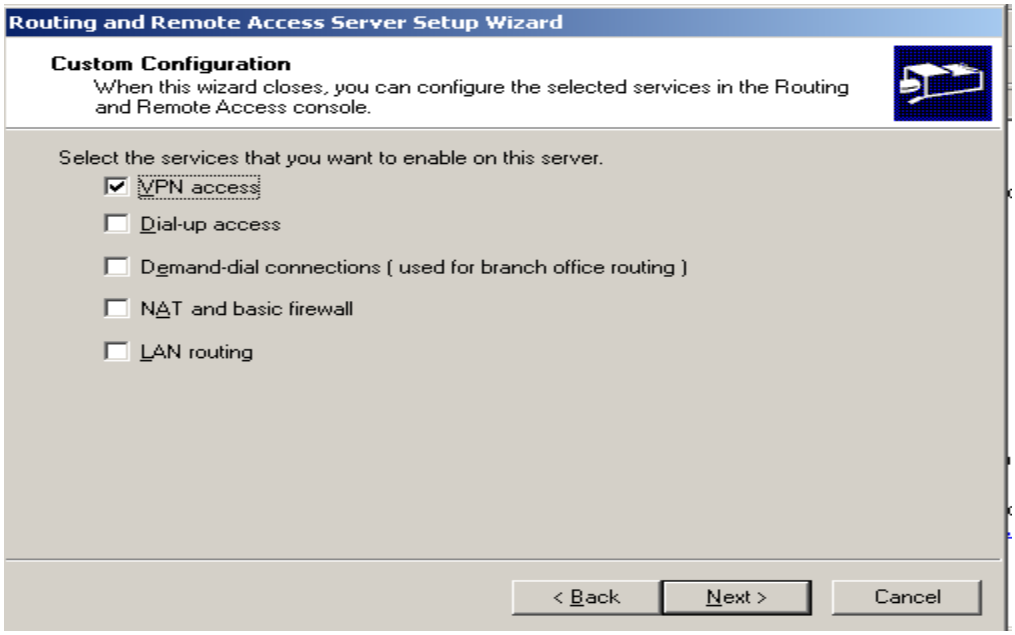


Figure 53: VPN Access

15. Click **Finish** on VPN Access, to close the routing and remote access wizard.

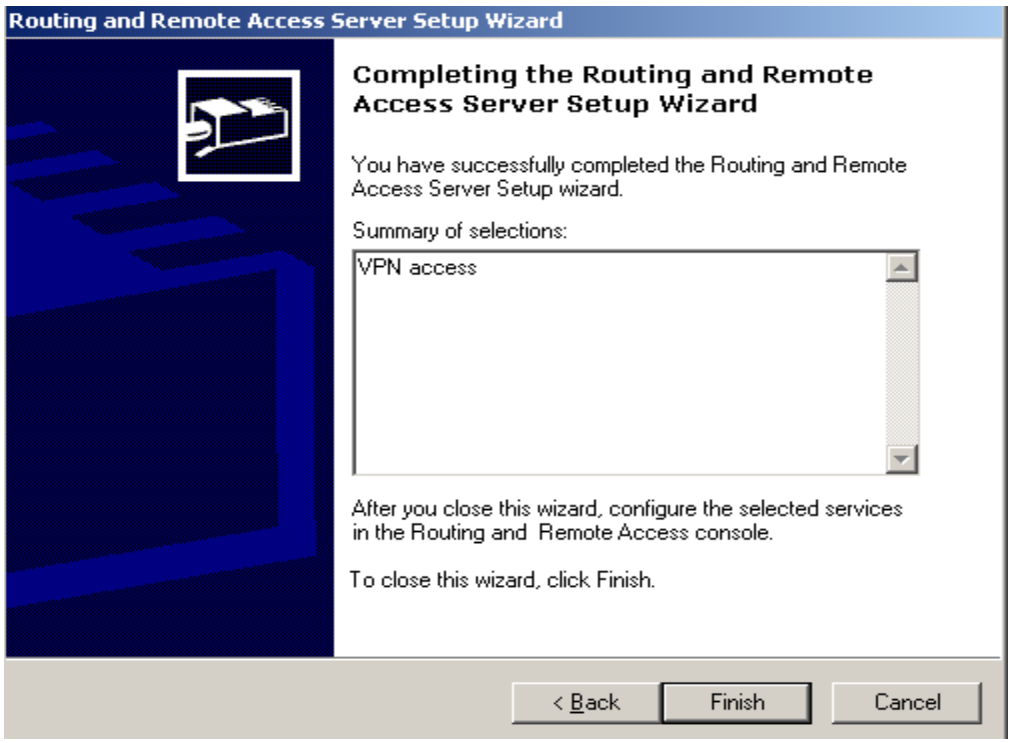


Figure 54: Completing the Routing and Remote Access Server Setup

16. Click **Yes** to start the Routing and Remote Access service.

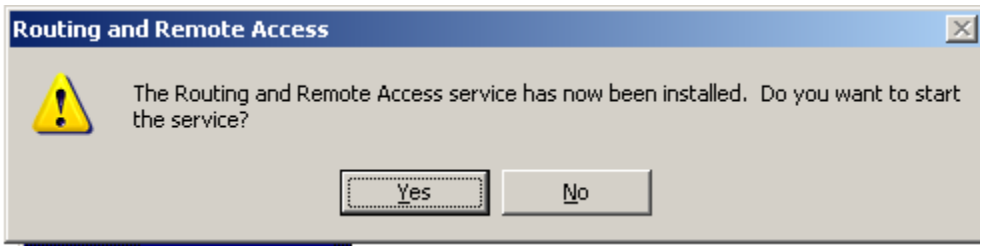


Figure 55: Stating the Routing and Remote Access Service

The VPN server needs to be configured to assign IP addresses to clients that connect so they can access internal resources. The internal clients currently have IP addresses of:

- 192.168.100.1
- 192.168.100.3
- 192.168.100.147
- 192.168.100.201

We will configure other external clients who VPN to receive a 192.168.100.0/24 address.

17. In Routing and Remote Access, right-click on **WIN2K3DC** and go to **properties**.

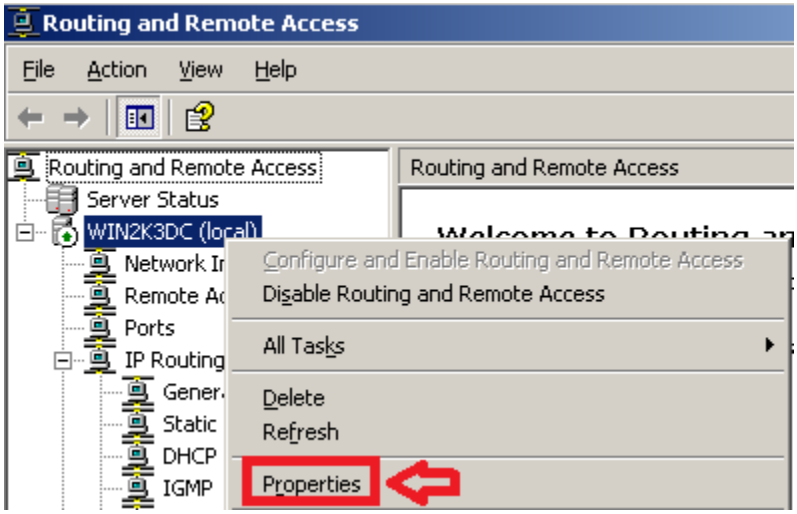


Figure 56: Selecting the Properties in Routing and Remote Access

18. Within the local properties of WIN2K3DC, click on the **IP** tab.

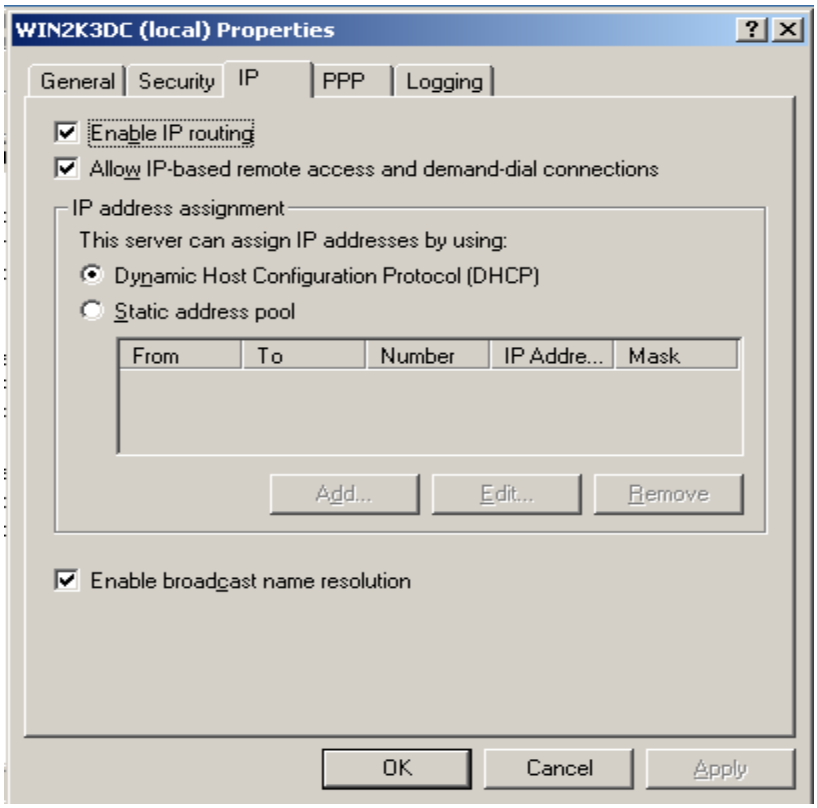


Figure 57: Selecting the IP Tab

19. Click the **Static Address Pool** Radio button. Click the **Add** Button.

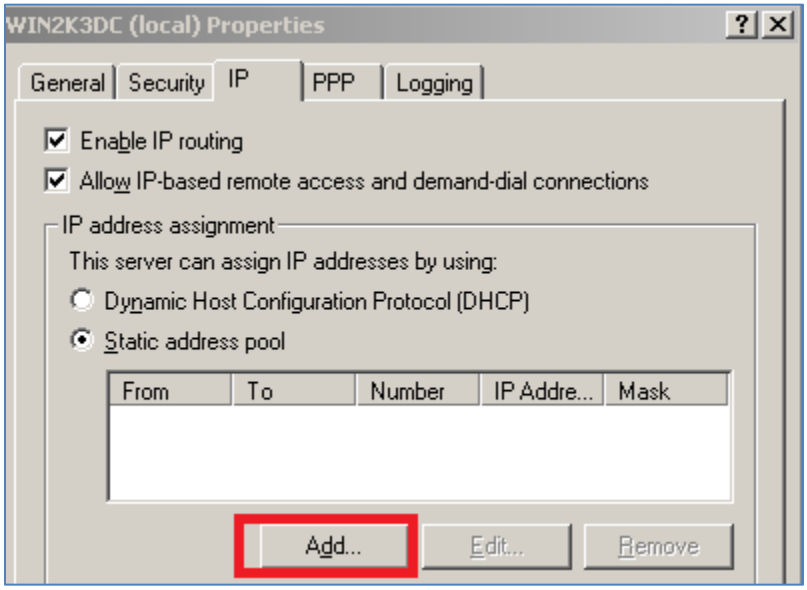


Figure 58: Adding a Static Address Pool

20. Type the following in the New Address Range box:

- For the Start IP address, type **192.168.100.240**
- For the End IP address, type **192.168.100.249**
- For the number of addresses, type **10**

Click the **OK** button so the New Address Range will be accepted.

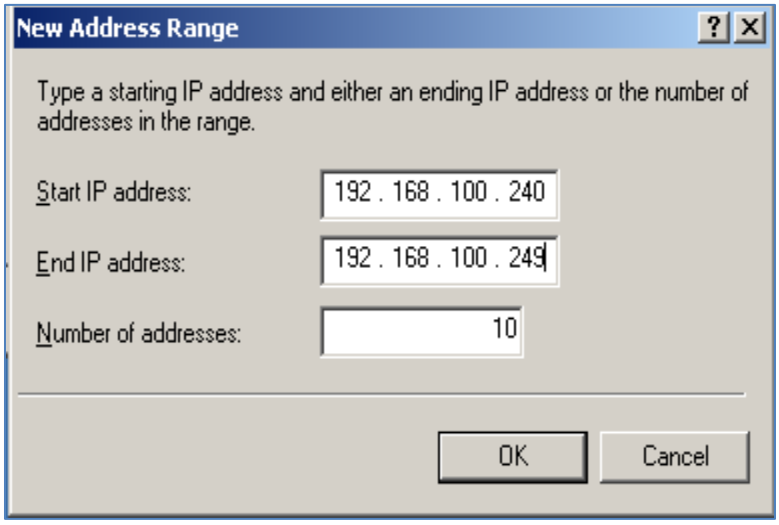


Figure 59: The Static Address Range

Now, we will need to give the administrator account dial-in permissions to VPN in.

21. Click on **Start**, then **run** and type **dsa.msc** to open Active Directory.

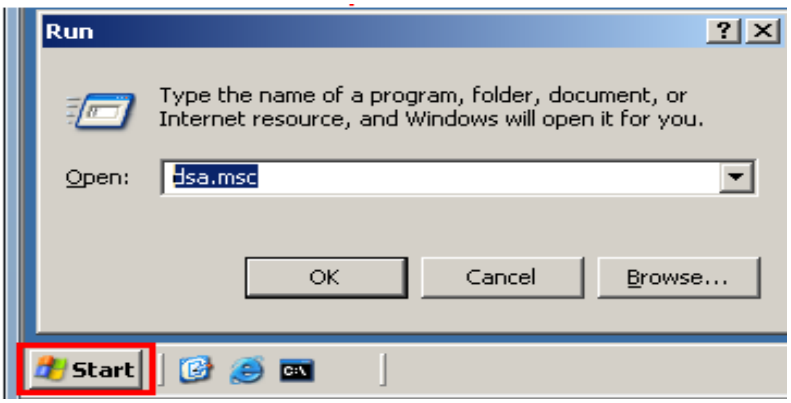


Figure 60: Opening Active Directory

22. The Active Directory Users and Computers snap-in will load. Expand the **msec.local** domain if necessary. Click on the **Users** folder in the left-hand pane. Double-click the **administrator** account in the pane on the right.

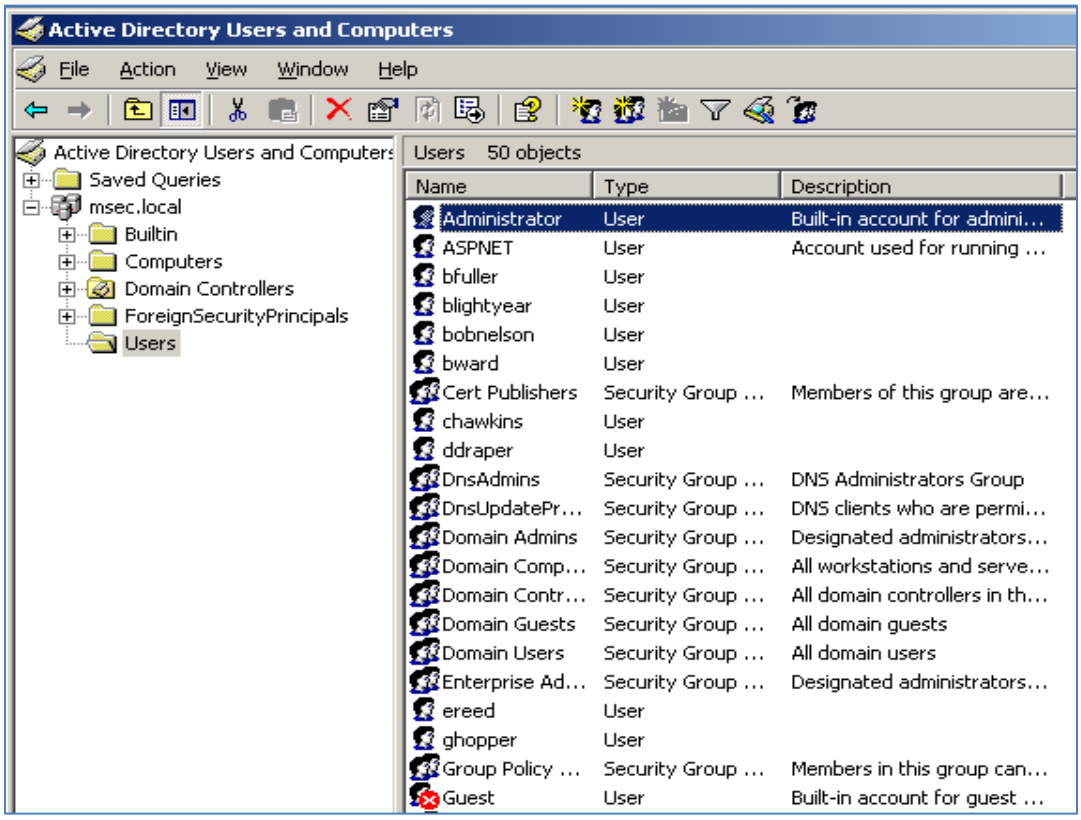


Figure 61: The Administrator Account

23. Click the **Dial-in** Tab. Change the **Remote Access Permissions** from Deny to **Allow**. Click **OK.**

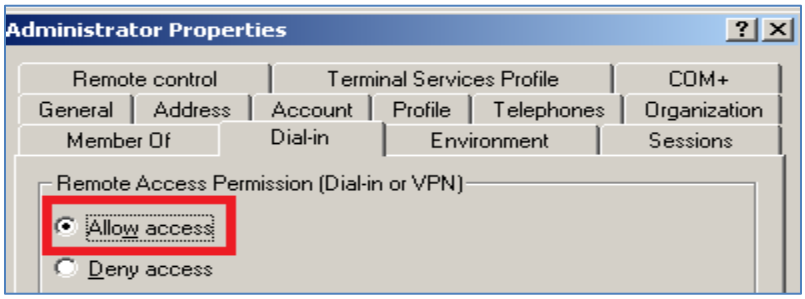


Figure 62: Allowing Remote Access

24. BackTrack 4 External Attack Machine Determine if the pfSense firewall is allowing any incoming ports by typing:
root@bt:~#**nmap 10.10.19.1**

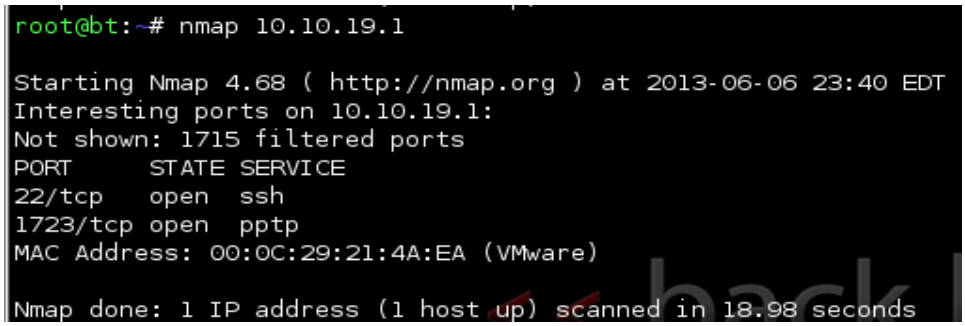


Figure 63: Scanning the Firewall

Notice that the PPTP port is now in the open state.

24. On the **Windows 2k3 Server External Victim Machine**, Click on **Start**, then **run** and type **ncpa.cpl** to open Network Connections.

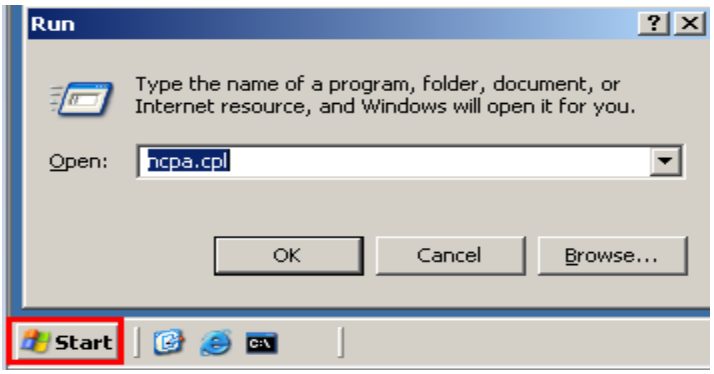


Figure 64: Opening Network Connections

25. Click the **New Connection Wizard** to order to create a VPN connection.

Figure 65: New Connection Wizard

26. Click the **next** button at the Welcome to the New Connection Wizard Screen.

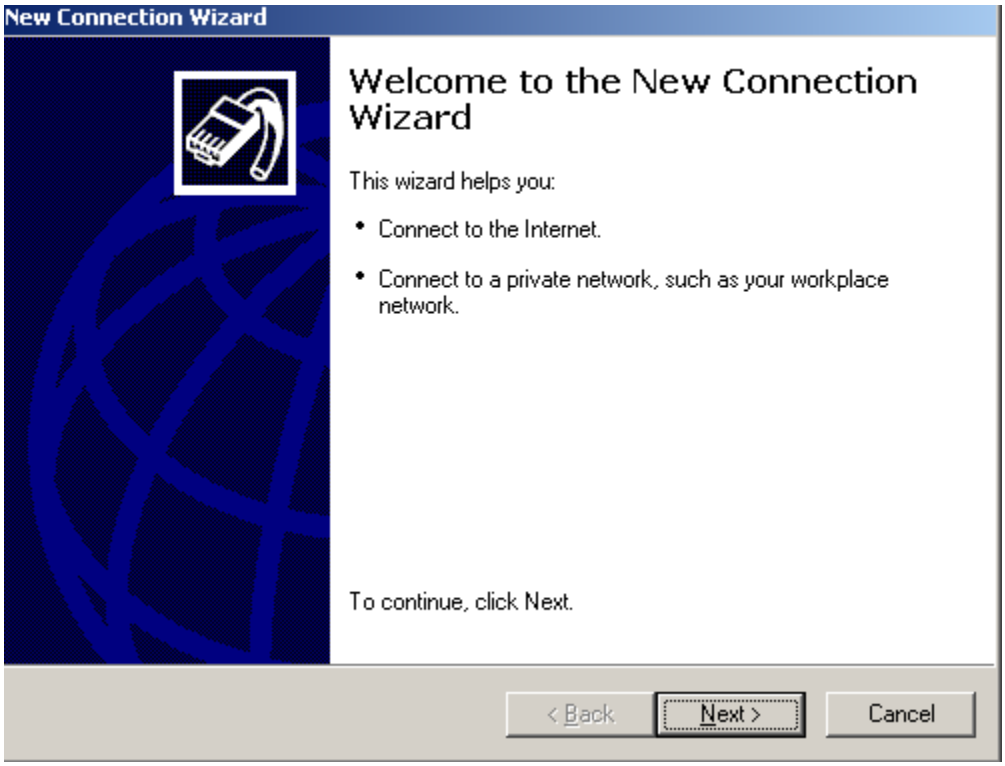


Figure 66: The New Connection Wizard

27. Select the middle choice to **Connect to the network at my workplace**.

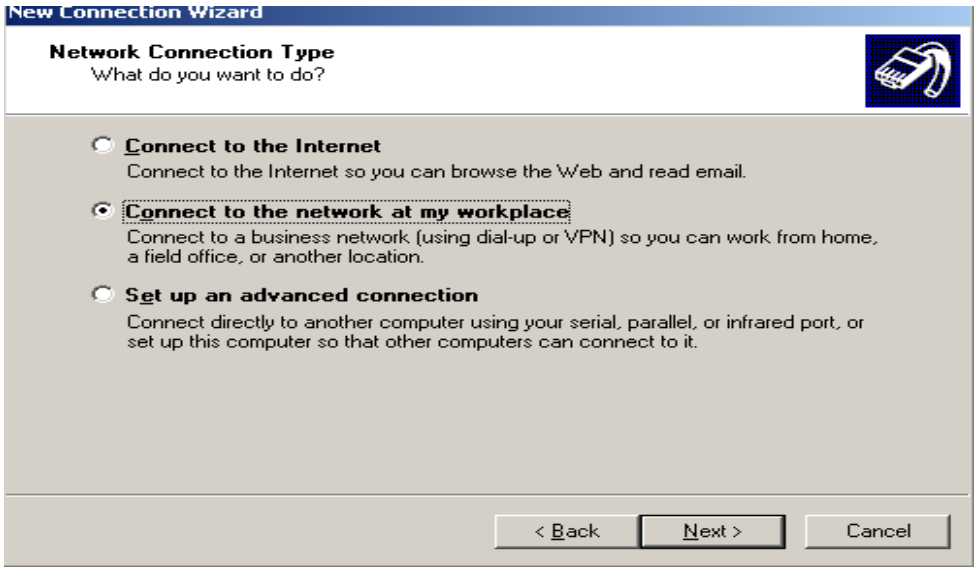


Figure 67: Selecting VPN as Connection Type

28. Select the bottom choice of **Virtual Private Network Connection.**

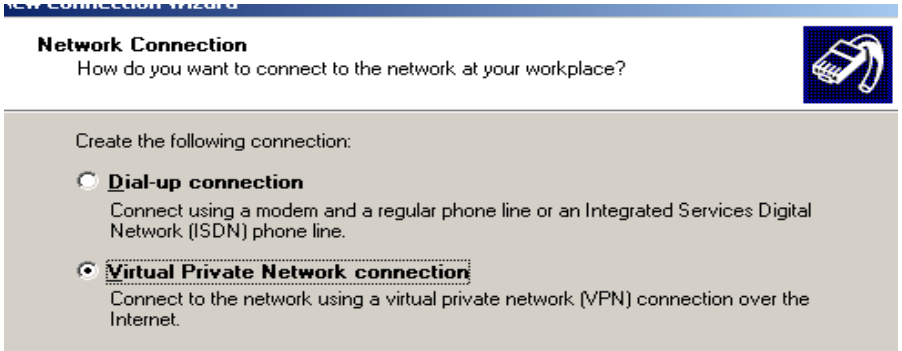


Figure 68: VPN Connection

29. For the name of the company you are establishing a connection to, type **XYZ**. Click **Next.**

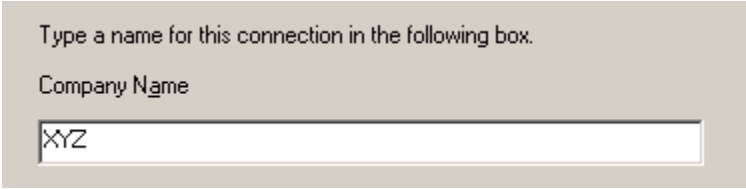


Figure 69: Identifying the company name

30. Type **10.10.19.1** for the IP address. Click **Next. On the next screen, select My use only** and Click **Next.** On the final page, click **Finish**.

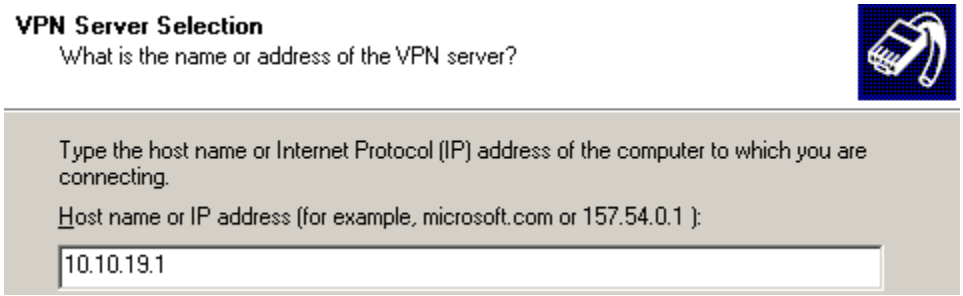


Figure 70: Entering the Remote IP address

31. In the Connect XYZ box, type **password** for the password and click **connect**.

Figure 71: Connecting to the Server

In the right corner of your screen, you will see that XYZ is now connected.

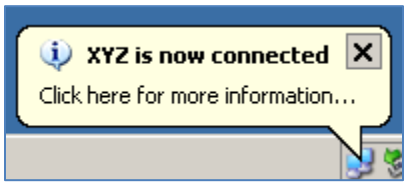


Figure 72: Connection Established

32. Open a command prompt on the Windows 2k3 Server External Victim Machine External Windows server and type **ipconfig**.

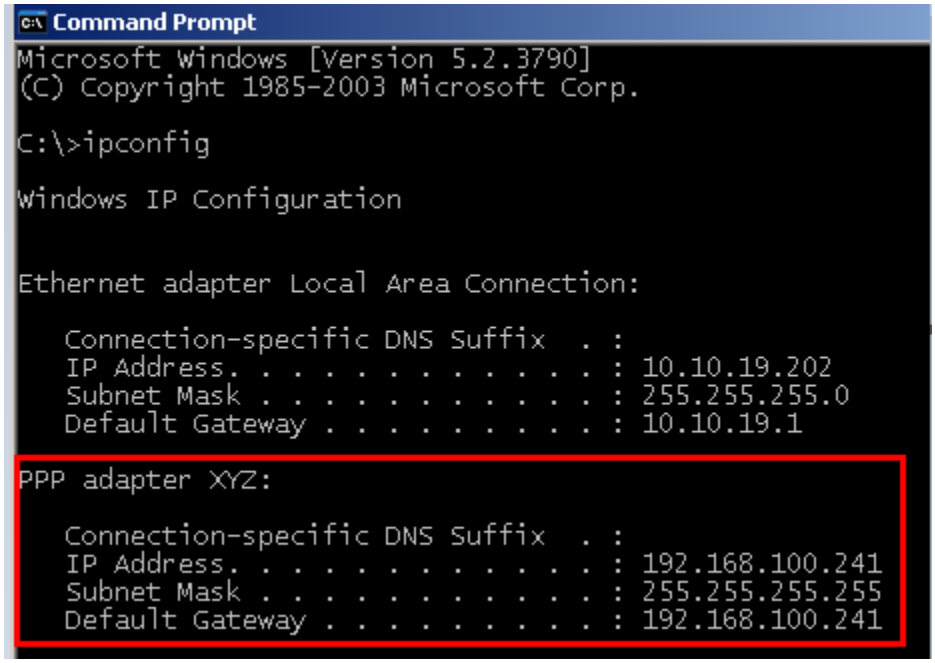


Figure 73: The VPN IP address is Displayed

3.2 Conclusion

When you use a Virtual Private Network, or VPN, users can connect to internal systems and access resources. Users must have accounts with proper credentials in order to successfully authenticate to the server. After establishing a VPN connection with a remote server, the client will be issued a new IP address allowing internal access.

3.3 Discussion Questions

1. What port does Point-to-Point Tunneling Protocol use?
2. Does Point-to-Point Tunneling Protocol use TCP or UDP?
3. What tool can be used to determine if the port for PPTP is open?
4. What still must be configured if PPTP shows up as closed during a scan?

References

1. Nmap:
   http://www.nmap.org

2. ICMP:
   https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

3. VPN:
   http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs

4. pfSense:
   http://www.pfsense.org/

5. Secure Shell (SSH):
   http://www.openssh.org/

