



VPN: NT Domains Across Remote Sites

Authored By: Ron Naken
Date: May 26, 2000
Purpose: Describe a configuration that will allow full domain access between remote corporate sites through a VPN tunnel.
Version: 4.1.100

The following products were tested during the creation of this document:

Check Point VPN-1 4.1 (SP1) on Sun Solaris
Microsoft Windows NT Server 4.0 (SP5)

This document describes domain access through a site-to-site VPN. For information on domain access for remote VPN users, please consult the following documents:

Secure Domain Logon: Preparing Your Network
Secure Domain Logon: Win98 as a Client
Secure Domain Logon: WinNT as a Client

All documents discussed in this white-paper can be found in Check Point's Knowledge Base at the following URL:

<http://support.checkpoint.com/kb>

Discussion

The configuration discussed in this document includes Network Address Translation (NAT), and describes sites that are hidden behind the external interface of the firewall. Since this scenario will NAT the traffic between sites only after it is encapsulated, we have no special considerations with respect to NAT on NetBIOS traffic.

Note: This document assumes the encapsulating firewalls will be performing the NAT

NAT and encapsulation are not normally necessary -- they provide us the ability to access non-routable addresses through the VPN. If all hosts are assigned routable IP addresses, NAT and encapsulation are not necessary. Please see *Secure Domain Logon: Preparing Your Network* for considerations when using NAT on NetBIOS traffic without encapsulation.

In providing domain access over the VPN tunnel, we have to contend with the standard domain WAN browsing issues. In a domain environment, hosts cannot normally locate domain controllers on other subnets. To solve this, we will setup a WINS server in one of our sites. Though we will discuss the use of only one WINS server, the ideal solution might be to use a separate WINS server on each site and configure replication between them.

For this configuration, IKE / IPsec is used to provide the encapsulated VPN tunnel.

Configuration:

1. Confirm connectivity to the remote site through the VPN. This can be done by using PING from a host behind one FW to a host behind the remote firewall.

Use the Firewall-1 Log Viewer to make sure encryption is working. After a successful PING, you should see an encrypt of the ICMP echo request that is sent to the remote host, as well as a decrypt of the ICMP echo reply that is sent back:

```

0  19Sep97 10:24:21 [icon] dae... 192.32.42.32 [icon] control  ctl
1  19Sep97 10:24:25 [icon] dae... 192.32.42.32 [icon] log      [icon] decrypt 192.32.52.30 192.32.32.32  icmp
2  19Sep97 10:24:25 [icon] dae... 192.32.42.32 [icon] log      [icon] encrypt 192.32.32.32 192.32.52.30  icmp

```

2. Modify your site-to-site VPN rule to allow the “NBT” service to pass between sites through the VPN.

Id.	Source	Destination	Service	Action	Track
1	internal-domain external-domain	external-domain internal-domain	NBT Audio_Video_Voice	Encrypt	Long

3. Create a WINS server at one of the sites. See below, *Installing WINS on NT Server*.
4. Configure all servers and domain controllers as clients to the WINS server. See below, *Configuring a WINS Client on NT* and *Configuring a WINS Client on Windows 98*.

Note: You might also consider configuring the WINS as a client to itself. WINS does not inherently know answers about the machine it is installed on.

5. Configure all workstations as clients to the WINS server. See below, *Configuring a WINS Client on NT* and *Configuring a WINS Client on Windows 98*.
6. Verify domain access and browsing still functions within each individual site. This can be done through “Network Neighborhood”. You should see the remote site once all machines reconfigured as WINS clients are restarted.

Note: The absence of machines in Network Neighborhood is not necessarily indicative of failed connectivity or configuration. It often takes 15 minutes or so to populate a browse list in Network Neighborhood. A better test might be to map a file share using Universal Naming Convention (UNC) in the form \\<host>\<share>. This can be done by selecting Start->Run-> and typing \\<IP address>\<share to map>.

7. Verify domain access and browsing is working between sites. See step 6.

Installing WINS on NT Server

Installing a WINS server on NT server is deceptively simple. Keep in mind that the WINS service on NT will not know of itself, so you might consider setting the WINS server up as a WINS client to itself after you get it installed (see below). This document will not discuss replication between WINS servers.

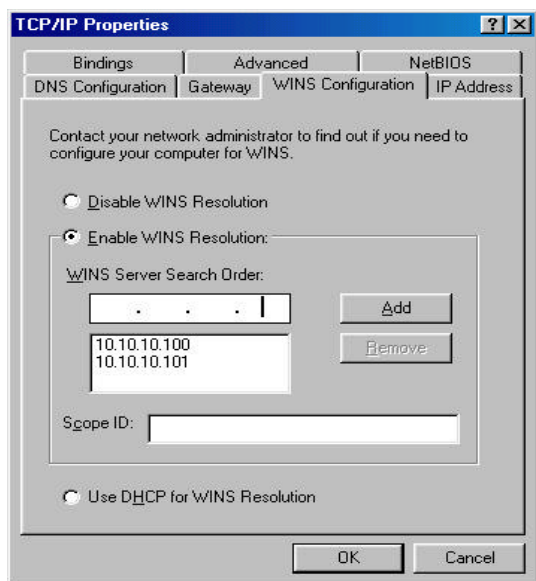
1. Go to Control Panel->Network. Select the “services” tab and add a service. Select WINS and click OK.
2. Once the WINS service is installed, you will need to reboot the machine.

Configuring a WINS Client on NT

1. Go to Control Panel->Network. Select the “Protocols” tab and edit properties of “TCP/IP Protocol”.
2. Select the “WINS Address” tab and enter the IP address of the WINS server in the “Primary WINS Server” field.
3. Click OK.
4. Remember to restart the machine after configuring it as a WINS client.

Configuring a WINS Client on Windows 98

- 1) Go to Control Panel->Network. Select properties of the “TCP/IP” that is bound to the network adapter card you will be using. Dial-up Networking is covered in another document.
- 2) Select the “WINS Configuration” tab and enter the IP address of the WINS server in the “WINS Server Search Order” field.



- 3) Click OK.
- 4) Remember to restart the machine after configuring it as a WINS client.