

Browsing an NT Domain Through a VPN: The Windows NT Client Using a NIC

Version 1.0

Author: Ron Naken
Date: September 24, 1999
Purpose: To describe a configuration that will allow VPN clients to browse and authenticate on a remote domain, using SecuRemote over a Network Interface Card. An example scenario covered by this configuration would be a Windows NT client behind a Cable Modem.

© 1999 Check Point Software Technologies LTD.

This document is written under the assumption that the firewall and SecuRemote client have already been installed and configured. This document also assumes that connectivity from the SecuRemote client to internal hosts on the remote network has been confirmed using a tool such as PING.

Note: Throughout this document, the term “Windows 98” is used to describe both Windows 95 & Windows 98. The version of Windows NT covered in this document is 4.0.

There are quite a few ways in which we can configure a remote Windows NT client to browse our NT domain through a VPN. The configuration discussed in this document was chosen for its ease of configuration and support.

For further reference, please see the following documents:

Browsing an NT Domain Through a VPN: Preparing Your Network

Browsing an NT Domain Through a VPN: The Windows 98 Client Using Dial-Up

Browsing an NT Domain Through a VPN: The Windows 98 Client Using a NIC

Browsing an NT Domain Through a VPN: The Windows NT Client Using Dial-Up

FAQ: NT Domain Authentication and Browsing Across “Hidden” Sites

FAQ: Troubleshooting Hints for Browsing an NT Domain

Discussion: Windows NT on the WAN

Quite a few issues exist in attempting to make a Windows NT client browse a remote domain. Regardless of the configuration chosen for the remote client, there will be small issues we will have to contend with as administrators. The objective of this document is to create a configuration that will be easy on the end-user.

Scenario 1: Machine & Users In Domain

Though it is possible to use domain accounts over a VPN for logon at a remote Windows NT SecuRemote client, this configuration is really for Check Point's SecureServer. User-authenticated VPN products (i.e. SecuRemote) will not establish a VPN until after the user has completed the logon process. This could cause problems if we require VPN access to the domain controllers. To allow VPN access to the domain controllers BEFORE a user logs on, we need to use a host-authenticated VPN solution, such as SecureServer, which can establish a VPN irrespective of the user.

Scenario 2: Machine in Domain, User Local

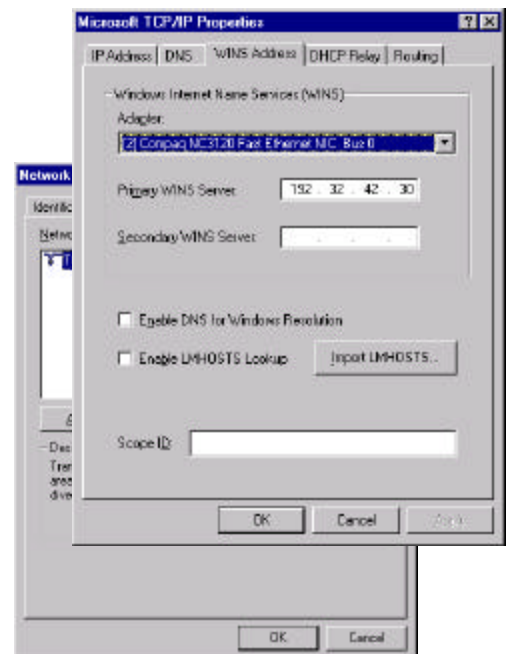
Since we are looking for SecuRemote solutions that are easy to manage, we will configure the workstations to this scenario. This will allow us to provide transparent domain authentication and browsing to the end-user. By having the user's workstation join the domain, the user will be able to avoid potential delays in populating Network Neighborhood. It is also possible to use a configuration where the user's workstation remains in a workgroup with the same name as the domain, instead of joining the domain. That configuration seems to be subject to delays in populating the Network Neighborhood.

Note: Something to consider when using SecuRemote on Windows NT is the SSO (Single Sign On) option that is available on the "Passwords" menu in SecuRemote. With SSO enabled, the user will be pre-authenticated to SecuRemote at login and would not have to enter their username and password. This will further help to avoid potential delays in populating Network Neighborhood and is an ideal solution for the remote user. Documentation on configuring SecuRemote with SSO can be found at <http://www.checkpoint.com/~joe>.

Configuring the Windows NT Client

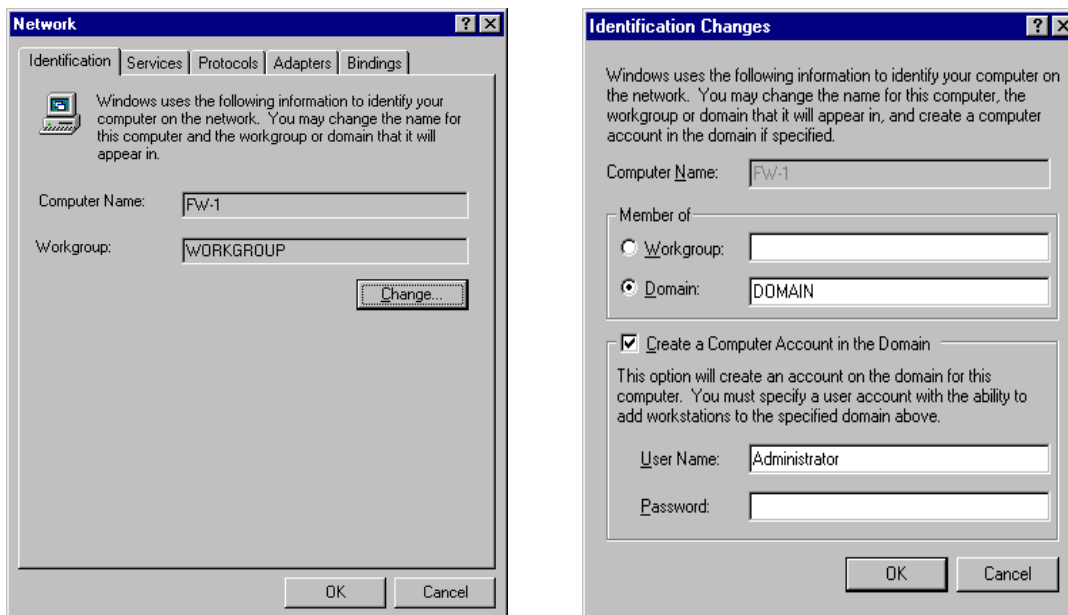
After we have verified connectivity from SecuRemote to our remote domain, the next steps to enable browsing are to join the domain and configure our Windows NT client to use our corporate WINS server. This will allow our client to get answers from WINS as to who our domain controllers are, who are master browsers are, and what the servers' IP addresses are.

1. Go into Control Panel->Network. Select the "Protocols" page and double-click TCP/IP. Select the "WINS Address" page and enter the IP address of your WINS in the "Primary WINS Server" field. Select "OK" when done. Select "OK" again and select "Yes" to reboot.



Note: Make sure you use a publicly accessible IP address for the WINS servers to avoid delays in populating Network Neighborhood. With Windows NT over a NIC, it is possible to require VPN authentication for access to the WINS servers; however, the client will need to either wait or tickle a server to populate their browse list. If this VPN client will be accessing an illegally addressed remote network through a VPN tunnel, you should configure NAT on the firewall to provide static translation of the WINS server's illegal address into a publicly accessible address. This is to allow the VPN client access to the WINS servers before the VPN tunnel is created. For information on configuring the WINS server and firewall, consult *"Browsing an NT Domain Through a VPN: Preparing Your Network"*.

2. Go to Control Panel->Network. On the "Identification" page, click "Change". Select to join the domain and enter the remote domain name. If your administrator has not already pre-created an entry in the domain for your machine to join, you must check the box that reads "Create a machine account" and specify an account to use when adding the machine. This account requires the advanced user right "Create machines in domain". An account that is a member of the "Domain Admins" group will have this user right. Select "OK". Select "OK" again and select "Yes" to reboot.



Note: You should have been prompted by SecuRemote for your username and password after selecting to join the domain. If you did not authenticate with SecuRemote quick enough, adding a machine to the domain will fail. Just try again. Keep in mind, the client will attempt to access the PDC when joining the domain -- a BDC will not suffice.

Note: An administrator can pre-create machine accounts in the domain by using Server Manager. This will allow the workstations to join without having to give users any advanced user rights.

Discussion: Accessing Domain Resources – Fixing a Feature

Once the machine reboots, we will be able to browse the remote domain. Keep in mind you should use a local account on the workstation with the same username and password as that used in the domain. In this way, as we attempt to access resources shared from domain controllers, authentication will be transparent to the user; however,

as we attempt to access resources on member servers, authentication will not be so transparent unless we intervene. Upon inspection, we see that member servers in the domain try to authenticate our user account as a “local” account to them. This is because when we logged onto our workstation as a “local account”, that told our workstation not to send domain qualifiers with the username. From our perspective, a domain account should be named “DOMAIN\USERNAME”. Since our username will be sent as “USERNAME”, we will have to “trick” the member servers to allow transparent authentication for the user. We have a couple options:

- Enable the “Guest” account and ensure nobody has an account with the same name as one present on the member server. This is a poor solution.
- Install all servers as domain controllers. This has potential, but is not a good solution.
- Pre-authenticate connections to the servers for the user.

We will select to pre-authenticate connections for the user. Attached to the right is **Pre-auth.vbs** which is a Windows Scripting Host script that can be placed in the Startup folder or used as a Logon Script to pre-authenticate users to their servers at login. Another solution would be to create a batch file, like Logon.bat below, and place it in the user’s Startup folder or allow the user to launch it, manually.



Logon.bat

```
@echo off
set DOMAIN=MYDOMAIN
net use /p:n
net use * \\www-1\Public /user:%DOMAIN%\%USERNAME%
net use * \\www-2\Public /user:%DOMAIN%\%USERNAME%
```

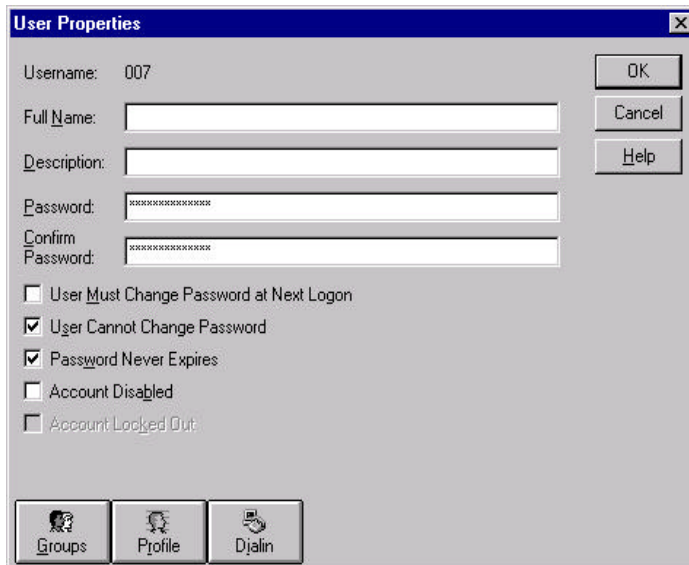
The batch file works by connecting the user to shares on member servers and specifying to use the domain\user account for the session. The “net use /p:n” line ensures the system will not attempt to reconnect to these shares automatically once the user logs off. The other “net use *” commands map a share (in this case “Public”) on each of our member servers for which the user should receive transparent authentication. When we connect to the shares, we use “/user:%DOMAIN%\%USERNAME%” as the user’s account. This allows us to specify the domain in our variable set on the second line of the logon script – in this case, it is MYDOMAIN. The %USERNAME% value is equivalent to the username the user entered at logon.

Note: Remember, we only need to pre-connect to shares in this manner on servers which should TRANSPARENTLY authenticate the user. If a member server is not pre-authenticated, the user will be prompted for a username and password. It would be a good idea to start with a batch file during initial testing and implement the WSH script after you are familiar with the configuration.

Pre-Authenticating Member-Server Connections

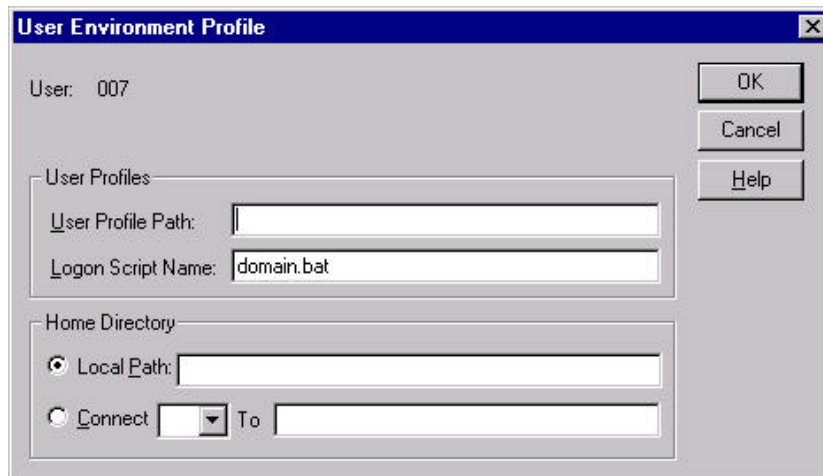
If you choose to run a logon script to pre-authenticate the user on critical member servers, follow these guidelines:

3. Select Start->Programs->Administrative Tools->User Manager on the remote workstation. Double-click the user's account.



The "User Properties" dialog box is shown. It has a title bar with a close button. The fields include: Username: 007, Full Name: (empty), Description: (empty), Password: (masked with asterisks), and Confirm Password: (masked with asterisks). On the right are buttons for OK, Cancel, and Help. At the bottom are three buttons: Groups, Profile, and Dialin. Below the password fields are several checkboxes: "User Must Change Password at Next Logon" (unchecked), "User Cannot Change Password" (checked), "Password Never Expires" (checked), "Account Disabled" (unchecked), and "Account Locked Out" (unchecked).

4. Press the "Profile" button and enter the name of your logon script in "Logon Script Name". Select OK. Select OK again and close User Manager.



The "User Environment Profile" dialog box is shown. It has a title bar with a close button. The fields include: User: 007, User Profile Path: (empty), Logon Script Name: domain.bat, and Home Directory: Local Path: (empty). On the right are buttons for OK, Cancel, and Help. At the bottom are two radio buttons: "Local Path" (selected) and "Connect" (unselected). The "Connect" option has a dropdown menu and a "To" field.

Note: At this point, when the user logs on, the logon script will pre-authenticate the user to all critical servers that are not domain controllers. Remember, domain controllers always assume the account is from the domain, so authentication on domain controllers will always be transparent, using our above configurations.