



Secure Domain Logon: Windows 2000 as a Client

Authored By: Steve Tierney
Date: March 22, 2002
Purpose: Describe a configuration allowing remote users to authenticate and browse NT domains through a VPN tunnel while allowing logon scripts and profiles to be executed.
Credits: Ron Naken
Version: 4.1.1

There are quite a few ways in which we can configure remote clients to logon with a domain account and browse our NT domain through a VPN. The configuration discussed in this document was chosen for its scalability and ease of configuration, and allows for the use of logon scripts, profiles, and a secured WINS.

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

Check Point VPN-1 4.1 (SP1) on Sun Solaris
Check Point SecureClient (Build 4153)
Microsoft Windows NT Server 4.0 (SP5)

The configuration described in this document is part two of a three-document collection. For further reference, please consult the following documents:

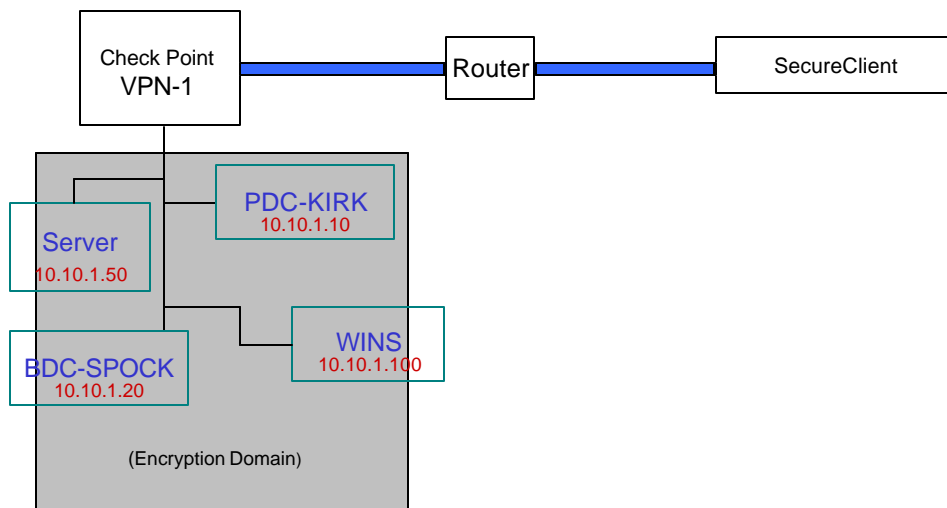
Secure Domain Logon: Preparing Your Network
Secure Domain Logon: Win98 as a Client

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

<http://support.checkpoint.com/login.html>

Configuration: Sample Diagram

The following diagram depicts the configuration used during the creation of this document:



Note: If you will be using overlapping encryption domains as in a Multiple Entry Point (MEP) configuration, you will need to place the firewalls in the encryption domain.

Preface for Authentication Timeout

SDL on Windows 2000 provides a facility to configure Single Sign-On (SSO) for the user. By enabling SSO, a user's VPN credentials are effectively attached to their domain login. This allows the user to authenticate on both the domain and the VPN by entering only their domain username and password. It is important to note that if any users will not be using SSO, they will have a limited time to enter their VPN credentials before login will fail. The default timeout period is 45 seconds, and this can be adjusted by adding the following property to the :props section of objects.C on the management server:

```
:sdl_netlogon_timeout (45)
```

This value can be in the range of 0 to 300 seconds. If it is too short, users will not be able to enter their credentials fast enough to authenticate the VPN before the host attempts to contact a domain controller. When a domain controller cannot be contacted, Windows 2000 will attempt to log the user on using a cached profile if one exists. This behavior can be disabled in the registry as follows:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current
Version\Winlogon\CachedLogonCount

Data Type:    REG_SZ
Value:        0
```

If a cached profile does not exist or has been disabled as shown above, the user will not be able to logon when a domain controller cannot be reached. It is a good idea to allow a minute or so before making another attempt.

Configuration Checklist

This document assumes you have experience defining virtual private networks with Check Point products. A checklist is provided to ensure the few steps to creating this VPN are completed, and a more detailed discussion of the configuration is covered in later sections. Please note that this document does not cover the Check Point side of this configuration in great detail, since this information can be found in the *Virtual Private Networking User Guide for VPN-1*.

- Configure your network as described in *SDL: Preparing Your Network*.
- Confirm LMHOSTS entries are properly downloaded with topology.
- Configure the client to use WINS.
- Configure the client to join the domain.
- Enable SDL and SSO in SecureClient.
- Configure SSO in SecureClient.
- Reboot and you should be able to logon to the workstation using domain accounts. If you require DUN to access the domain, check Logon Using Dial-Up Networking before logging on.

Configuring Windows 2000

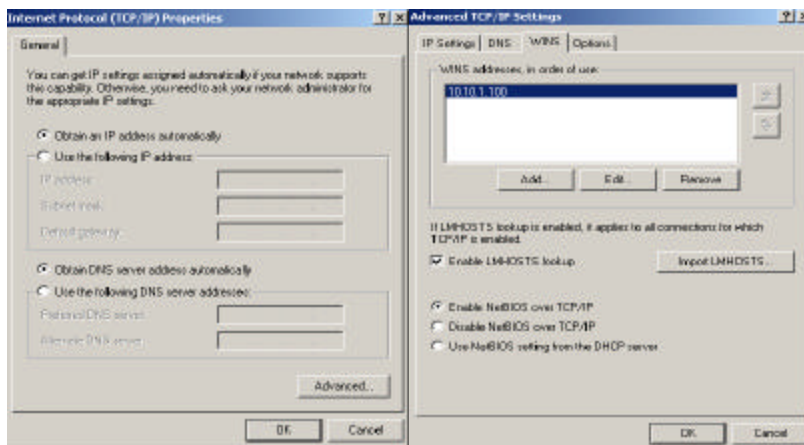
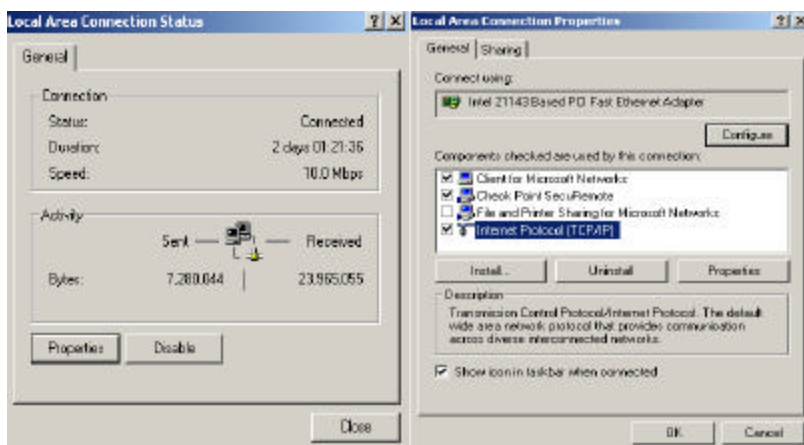
This document is written under the assumption that the firewall and SecureClient have already been installed and configured. This document also assumes that connectivity from the SecuRemote client to internal hosts on the remote network has been confirmed using a tool such as PING. Both Dial-Up and NIC based configurations will be discussed. For Dial-Up configuration, it is assumed you have already configured and tested Dial-Up Networking.

1. Configure your network as described in *SDL: Preparing Your Network*.
2. Ensure your LMHOSTS file is updated with the information from dnsinfo.C after creating or updating your site. These should look as follows:

```
10.10.1.10      pdc-kirk      #PRE #DOM:dom-ncc1701 #SecuRemote
10.10.1.20      bdc-spock     #PRE #DOM:dom-ncc1701 #SecuRemote
```

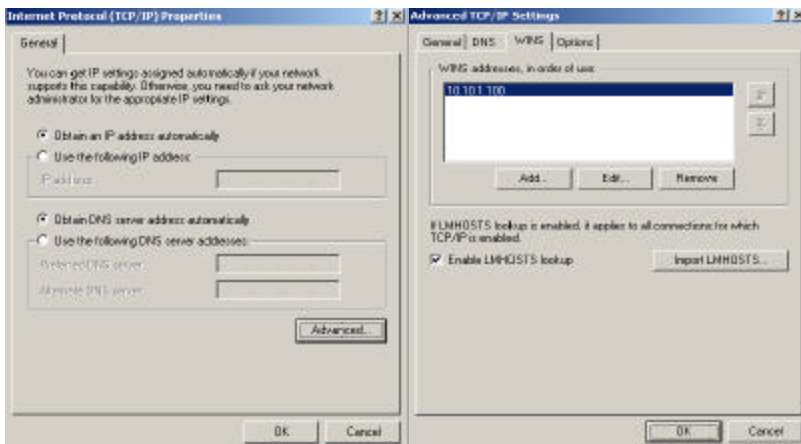
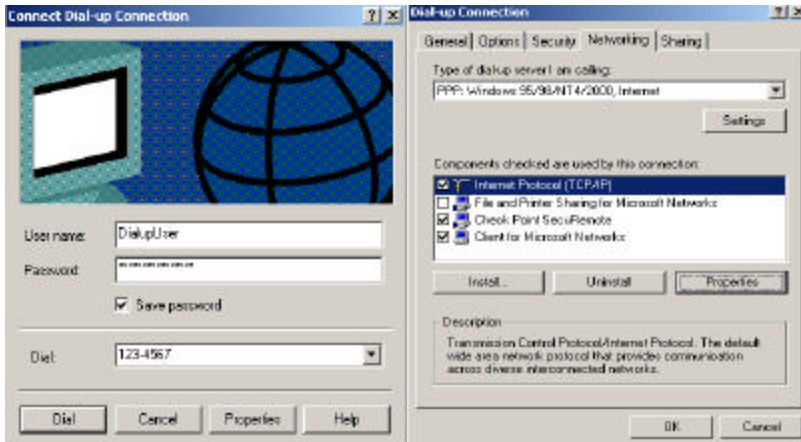
3. Configure your host as a client to WINS.

Go into Control Panel->Network and Dial-up Connections. Select the Local Area connection you are using. Click on the Properties button. Select Internet Protocol (TCP/IP) and click on properties. Click on the Advanced button. Click on the WINS tab. Click on Add and enter the IP address of your WINS in the Primary WINS Server field. Select OK.



If you are using Dial-Up Networking (DUN):

You may wish to configure WINS properties in DUN instead of in the general network properties as described above. This is useful if you will only be using WINS while connected through DUN, or if you will be using a separate WINS for DUN and general networking. To do this, open the properties dialog for the Dial-Up connection you will be using. Click on the Properties button. Select Internet Protocol (TCP/IP) and click on properties. Click on the Advanced button. Click on the WINS tab. Click on Add and enter the IP address of your WINS in the Primary WINS Server field. Select OK when finished.

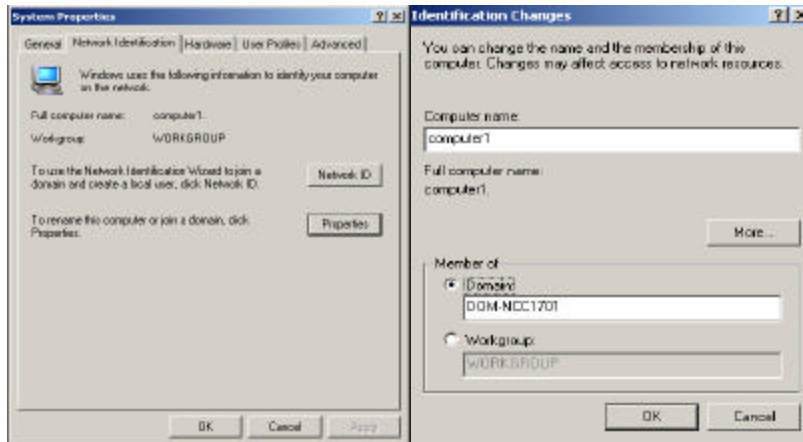


Note: If your WINS address is configured in DUN instead of general network settings, LMHOSTS entries may not be required when securing access to WINS.

4. Configure the client to join the domain.

If you are using Dial-Up Networking, you must dial your ISP before so you can join the domain.

Right click on My Computer and click on Properties. Click on the network Identification Tab. Click on the Properties Button. Select to join the domain and enter the remote domain name. Press OK. Press OK again and press Yes to reboot.



Note: SecureClient should have prompted you for your username and password after selecting to join the domain. If you did not authenticate with SecureClient quickly 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.

5. Enable SDL and SSO in SecureClient.

Launch SecureClient by double-clicking the icon in your system tray. Select the Passwords menu and select Enable SSO. Select the Password menu again and select Enable SDL.

Note: Once SDL is enabled on a Windows 2000 client, do not remove the client from the domain or join another domain. Warning messages will be received each time the machine is rebooted if SDL is not disabled before changing the client's domain membership.

6. Configure SSO in SecureClient.

Select the Passwords menu and select Configure SSO. Enter your NT Domain username and password, as well as your SecureClient username and password.



The image shows a Windows dialog box titled "Single SignOn". It contains the following fields and controls:

- NT User Name:
- NT Password:
- Confirm:
- SecureClient Username:
- SecureClient Password:
- Confirm:

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

7. Reboot the machine. Once the machine restarts, you can logon using your domain account. If you require Dial-Up Networking to logon to the remote domain, be sure to check "Logon Using Dial-Up Networking" at the Windows 2000 logon under the options tab on the authentication dialog box.