



Secure Domain Logon: Preparing Your Network

Authored By: Ron Naken
Date: May 22, 2000
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: Assaf Parag
Version: 4.1.202

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.

Note: Throughout this document, the term “Win98” is used to describe both Windows 95 and Windows 98. The term SecureClient will be used to describe both SecuRemote and SecureClient.

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 one of a three document collection. For further reference, please consult the following documents:

- 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

With the release of CP2000, it is possible to provide a Secure Domain Logon (SDL) to remote VPN clients. Using this configuration, remote users can log onto their remote workstations using domain accounts, the logon will be authenticated by a domain controller through the VPN, and the user’s profile and logon scripts will be executed as it does when the user is local to the domain.

It should be noted that in the CP2000 release of VPN-1, there is a new facility that allows clients to pull LMHOSTS entries during topology download. With this new feature, we can secure access to WINS without allowing public access for “nbname” as in previous implementations. Using dnsinfo.C, we can allow remote clients to locate one or more domain controllers before the VPN is established. This is necessary since we will secure the WINS, allowing access only through the VPN. With WinNT as a client, this is all that is necessary to allow complete remote access to the domain. An additional LMHOSTS entry will be required for Win98 clients to enable the population of network neighborhood, and this will be discussed in the *SDL: Win98 as a Client* white-paper.

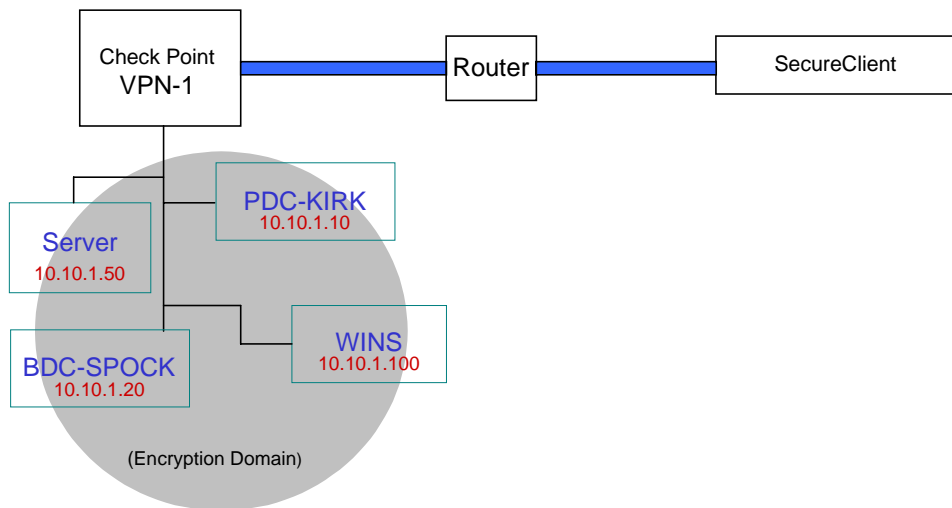
If you will be using Network Address Translation (NAT) with NetBIOS services, you will need to add the following property to the objects.C file on your management server:

:netbios_nat (true)

This property should be added to the :props section of the file. Restart your management server and push a policy to activate this change. Please note that if NAT is only occurring on encapsulated VPN traffic, this option will not be necessary.

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.

Configuration

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 SecureClient to internal hosts on the remote network has been confirmed using a tool such as PING.

1. Create a dnsinfo.C file in the \$FWDIR/conf folder of your management server as described in the VPN-1 User Guides. We will create an :LMdata section as shown below:

```
:LMdata (
  : (
    :ipaddr (10.10.1.10)
    :name (PDC-KIRK)
    :domain (DOM-NCC1701)
  )
  : (
    :ipaddr (10.10.1.20)
    :name (BDC-SPOCK)
    :domain (DOM-NCC1701)
  )
)
```

This section allows us to centrally manage LMHOSTS entries on the remote clients. These entries are necessary if we will secure access to the WINS. In the sample above, we have included an entry for the PDC (PDC-KIRK) and a BDC (BDC-SPOCK) for the domain (DOM-NCC1701). These entries will be integrated into the SecureClient LMHOSTS files during topology download and will appear as follows:

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

Push a policy to your firewall after creating or making changes to dnsinfo.C to ensure the firewall receives a copy.

Note: If your clients are only using Dial-Up Networking to connect, or you are not going to secure access to WINS, LMHOSTS entries may not be necessary.

Note: There is a complete working copy of dnsinfo.C included at the end of this document. If you are concerned about the syntax, you may cut & paste that dnsinfo.C and modify it to suit your needs.

2. Update the site on SecureClient to download the dnsinfo.C information.
3. Ensure the LMHOSTS file was updated during topology download. This file is located in the following locations:

```
Win98:          \windows\lmhosts
WinNT:          \winnt\system32\drivers\etc\lmhosts
```

If the LMHOSTS file is not modified when a site is created or updated, it is likely the format of your dnsinfo.C is not valid. A sample dnsinfo.C file is included in a later section of this document.

4. Make sure your Client Encrypt rule allows the “NBT” group of services or “Any” for access to the remote servers and domain controllers, as shown below:

Note: The NBT service group includes all NetBIOS over TCP/IP services we need to access, browse, and authenticate on domain resources. These are nname, nbssession, and nbdatagram.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Sales@Any	Encrypt_Domain	NBT	Client Encrypt		Gateways	business_jrc

5. Configure a WINS server as shown below under the section *Installing WINS on NT Server*. You may place the WINS in the encryption domain of the firewall if you wish to secure remote access to VPN clients only. The WINS allows our remote clients to resolve NetBIOS names to locate servers that have registered with WINS.

Note: The WINS server is not necessary if you intend to manage LMHOSTS files for name resolution. A combination of WINS and LMHOSTS is used in this configuration for scalability and ease.

6. Configure your remotely-accessible servers and domain controllers to be clients to the WINS server. See "Configuring a WINS client on NT" below.

Note: Our remote clients will locate their domain controllers with the LMHOSTS entries we manage in dnsinfo.C. If there are domain controllers you will not list in dnsinfo.C, be sure to include them as WINS clients so remote users can locate them.

7. Configure your remote VPN clients as discussed in the white-papers on SDL client configurations.

Installing WINS on NT Server

Installing a WINS server on NT 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.

Configuring a WINS Client on Win98

- 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. See below.



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

Sample dnsinfo.C

```
(
  :dns_servers (
    : (spock
      :obj (
        : (10.10.1.100)
      )
      :topology (
        : (
          :ipaddr (10.10.1.0)
          :ipmask (255.255.255.0)
        )
      )
      :domain (
        : (
          :dns_label_count (10)
          :domain (.trek.com)
        )
      )
    )
  )
  :encrypt_dns (true)
  :LMdata (
    : (
      :ipaddr (10.10.1.10)
      :name (PDC-KIRK)
      :domain (DOM-NCC1701)
    )
  )
  : (
```

```
:ipaddr (10.10.1.20)
:name (BDC-SPOCK)
:domain (DOM-NCC1701)
```

```
)
)
)
```