Cisco VPN Support for HP Thin Clients and Blade PCs

Introduction

This white paper provides a reference implementation of layered security policy enforcement created by integrating HP thin clients and Consolidated Client Infrastructure (CCI) blade PCs with SSL and IPSEC VPN solutions from Cisco. The combination of HP thin clients and Consolidated Client Infrastructure (CCI) blade PCs provides a very robust, secure, and cost-effective computing solution that can be applied to any network. Like any other networked component, it is important to examine security issues associated with their operation. This paper addresses key requirements to properly configure HP thin clients and blade PCs for use in a with CISCO VPN concentrators. Overviews of SSL and IPSEC VPN properties as well as usage models and known working implementations, are provided.

The Components

HP PC Client Computing Solutions

HP PC client computing solutions consist of two major components: thin clients and blade PCs. A thin client is a computing device without a hard drive that provides display and input/output for applications running on remotely located servers or blade PCs. A basic thin client consists of a processor, flash memory for storing the embedded operating system, local RAM, a network adapter, and standard input/output for the display and other select peripherals. HP thin clients have no moving parts, offering higher reliability than a PC, lower ownership costs, enhanced security, and extended product life. These small, robust devices consume significantly less energy than a desktop PC, put out less heat into your office spaces, are made with much less material than a desktop, and are practically silent.

HP offers thin clients based on three operating systems: Windows XPe, Debian Linux, and Windows CE. Each operating system provides protection for the OS image housed within the flash device while creating a partition on that flash device to act as a virtual hard drive. Only an account with administrator privileges can make changes to the base image to add applications or operating system patches. With the Windows XPe operating system, HP also includes a Sygate firewall on the base image that locks down all ports except those necessary for typical Microsoft Remote Desktop Protocol (RDP) and Citrix-level connections and general Web browsing. The Sygate settings must be edited to unlock any additional ports on the thin client.

Consolidated Client Infrastructure (CCI) is the enterprise/data center computing architecture through which blade PCs can be allocated to end-users connecting on thin clients. The blade PCs are stored and managed in a centralized location, and are accessed through HP Remote Graphics Software (RGS) or RDP. A remote user can present credentials to the HP Session Allocation Management (SAM) service and be connected to a computing session on a blade PC with access to network resources such as applications and data. Unlike Terminal Services-, Citrix-, or VDI-hosted computing sessions, CCI computing sessions typically match up a connected user onto a blade PC that is not shared, which provides a stable computing experience that does not change as additional users are added to the array of PC blades.

Although CCI blade PCs are housed in the data center for security, they are full-blooded PC systems running the latest operating systems. As such, it is assumed in this paper that images for blades are configured with a firewall and virus scanning software as a security baseline. For the usage models presented here, the blades were configured to use the native Windows XP firewall, as well as anti-malware software.

Virtual Private Networks

Advancements in computer networking have significantly changed the way people and organizations communicate and access information. Networks have become critical resources in many organizations, providing real-time communications and access, through both the Internet and enterprise intranets. As organizations take advantage of the benefits of making information available, they increasingly turn to virtual private networks (VPNs) to protect valuable proprietary information. They also might be responsible for complying with government regulations related to data privacy.

VPN refers to an array of technologies that provide encryption and encapsulation of data through an otherwise unsecured network (such as the internet). However, both encryption and encapsulation are generic functions that can be performed by multiple technologies and can be combined in different implementation topologies. Thus, VPNs can vary widely from vendor to vendor.

Cisco VPN Capabilities

In this paper, we show how to use a CISCO VPN 3000 Concentrator to provide data tunneling (also known as data encapsulation) across a public TCP/IP network, such as the Internet, to create secure connections (tunnels) between remote users and a private corporate network.

The VPN 3000 Concentrator functions as a bidirectional tunnel endpoint:

- It can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination.

  Or

- It can receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

The VPN 3000 concentrator supports the most popular VPN tunneling protocols:

- PPTP: Point-to-Point Tunneling Protocol
- L2TP: Layer 2 Tunneling Protocol
- IPSec: IP Security Protocol
- WebVPN: VPN via an HTTPS-enabled Web browser, does not require a client

The concentrator also supports L2TP over IPSec, which provides interoperability with the VPN Client provided by Microsoft. The VPN 3000 Concentrator is interoperable with other clients that conform to L2TP/IPSec standards, but it does not formally support those clients.

Implementation Prerequisites

For the purpose of this white paper, we assume a basic network infrastructure is already in place. The reference implementation consists of HP BladeSystem bc2000 Blade PCs and HP BladeSystem bc2500 Blade PCs running Windows XP SP2. **HP Compaq t5720 Thin Clients** (t5720) running Windows XPe are used as access devices.

The network topology for this reference implementation consists of a Cisco VPN 3000 concentrator sitting between two Class-C networks: 10.1.1.xxx/24 on the public interface and 10.2.2.x on the private interface. Details of the reference network can be found in Appendix A – CISCO 3560 Switch Configuration.

The Implementation

VPN Installation

This section covers use of a CISCO VPN 3000 appliances in conjunction with a CISCO layer 3 switch to ensure that thin clients and blade PCs meet configuration policy prior to connection with the trusted network segment. The network topology used in this reference implementation is found in Figure 1 below.

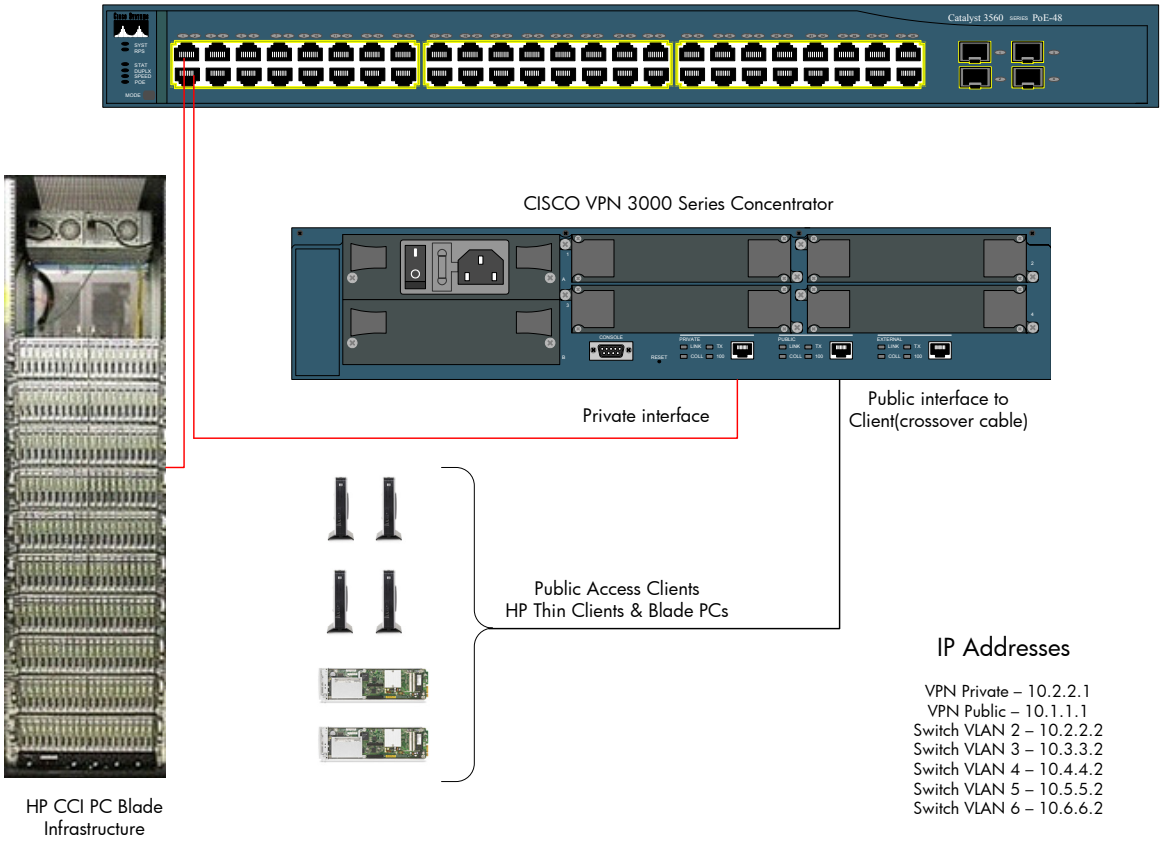


Figure 1 - Reference VPN topology

The Cisco 3560 switch is configured with VLANs assigned to ports 1 to 5, as shown in Figure 1 above. Full switch configuration settings can be found in Appendix A – CISCO 3560 Switch Configuration.

Basic VPN Configuration

This paper focuses on the integration of VPN services to HP thin clients and blade PCs. As such, we are exploring only configuration settings that are pertinent to these clients. This does not exhaust all possible VPN configurations, and in a production environment, you may wish to validate many more OS configuration components than are discussed in this reference white paper. For full documentation on the possible setup options for the Cisco VPN3000 appliance, please see *VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7* at

http://www.cisco.com/en/US/docs/security/vpn3000/vpn3000_47/configuration/config.html.

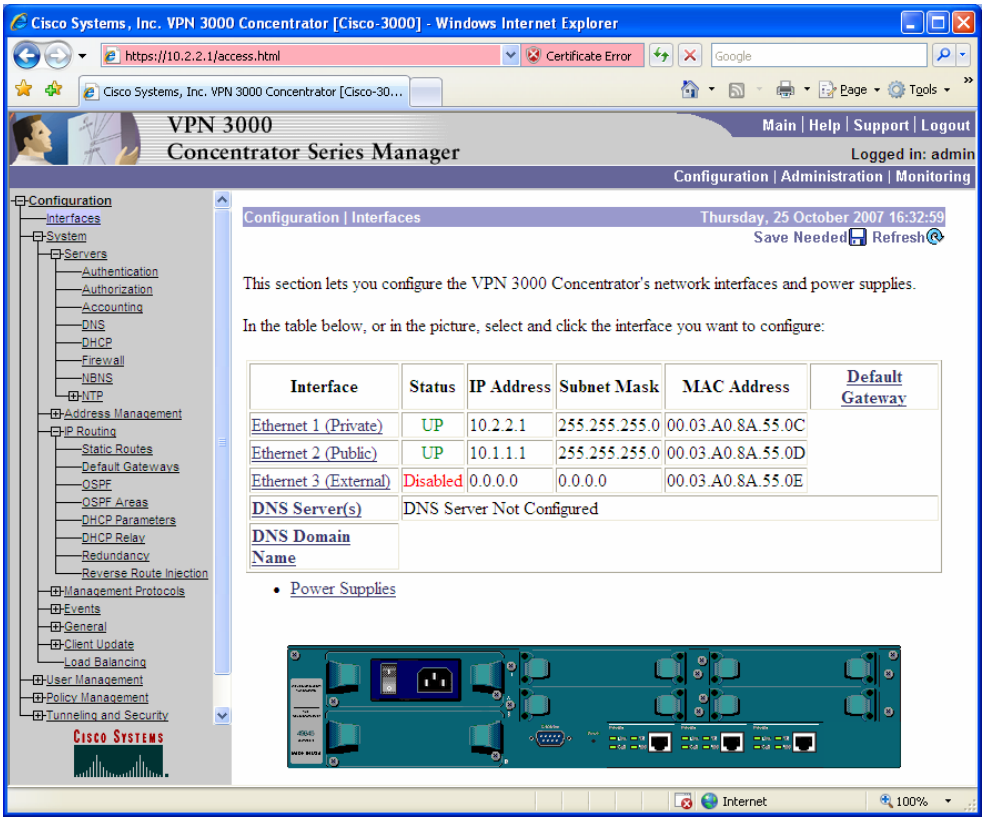
Instructions below step through a basic Virtual-IP VPN configuration from a public network to private LAN. As previously mentioned, the public network is Class-C with scope 10.1.1.x/255. The Cisco VPN3000 Concentrator, like other servers/services on the public interface, has a fixed IP address at 10.1.1.2 and bridges to the private Class C network with scope 10.2.2.x/255.

Access to the VPN3000 configuration screens is possible via serial port or via a WEB interface via the private Ethernet address. Screen captures for VPN3000 setup are shown below via the WEB console, although the terminal interface (serial port) was initially used to set 10.2.2.2 as the private interface address. The terminal server is running on the private interface to a terminal or PC running terminal emulator at 9600bps, 8 bits, no parity, 1 stop bit (9600,8,N,1).

VPN 3000 Appliance Settings

1. Log on to VPN 3000 concentrator (https://10.2.2.2) using an account with administrator privileges.

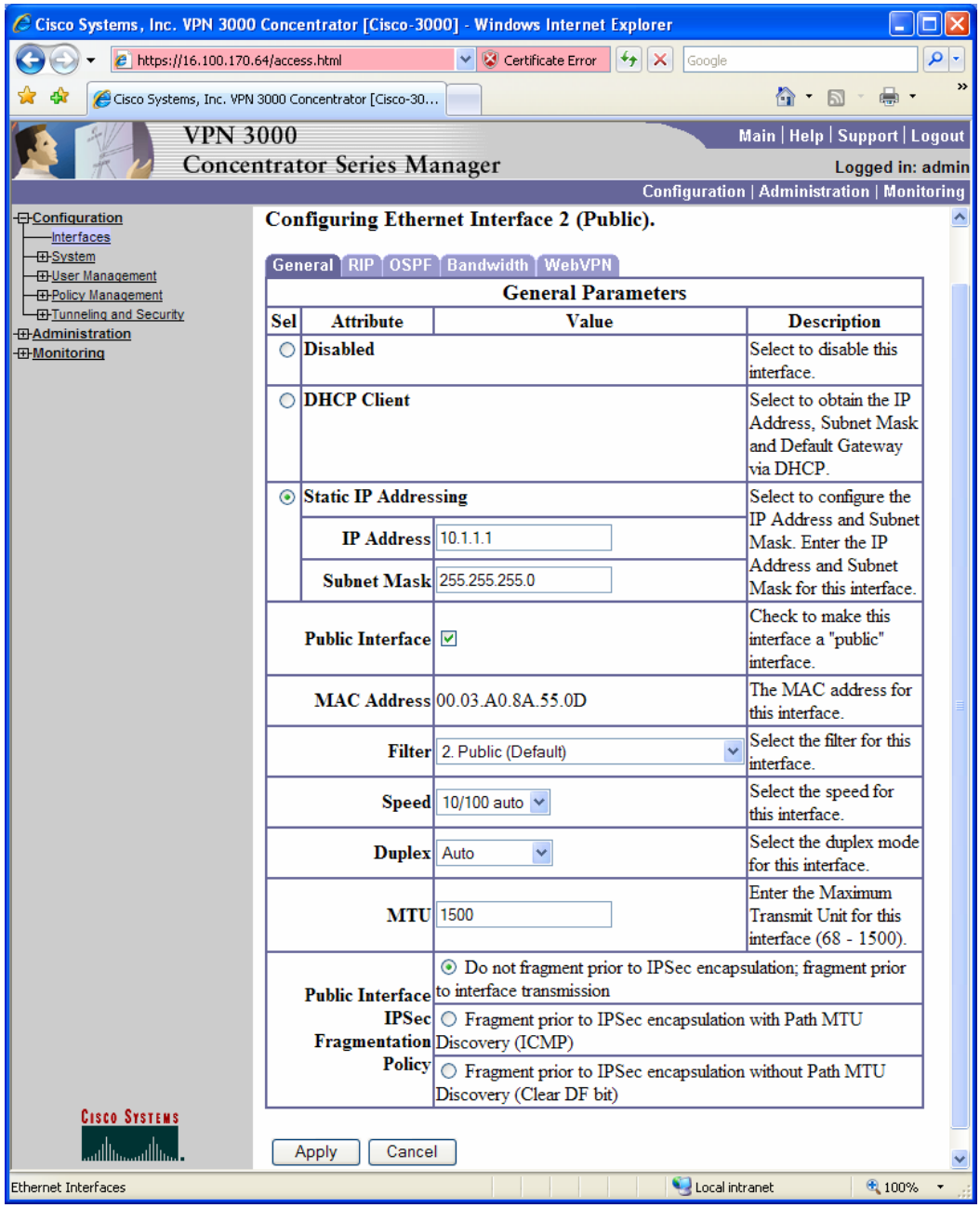
2. From the initial VPN 3000 setup screen, click **Configuration\Interfaces** in the left panel. This brings up a graphical configuration window with hyperlinks to facilitate easy setup options.



3. Access private and public interface configuration options by clicking the appropriate links in the **Interface** column.

4. The public interface window is shown in the following illustration. Select **DHCP Client** or **Static IP Addressing**, as appropriate for the public network.

   NOTE: For this reference implementation, the VPN 3000 concentrator has been assigned a static address of 10.1.1.1 and is connected via port #1 of a CISCO 3560, layer 3 switch. The physical switch has an internal address of 10.1.1.2 for routing within the switch. This routing address is entered as the Default Gateway address (also accessible via the Configuration\Interfaces window above).



5. Next, enter the DNS Server, DNS Domain Name, and Default Gateway information by clicking the appropriate links on the **Configuration\Interfaces** window.

   NOTE: These settings can also be set via System\Servers\DNS and System\IP routing\Default Gateways, etc.

   For full configurations options for VPN 3000 concentrator information, refer to CISCO documentation.

End-Point Configuration

Thin Client Firewall Exceptions

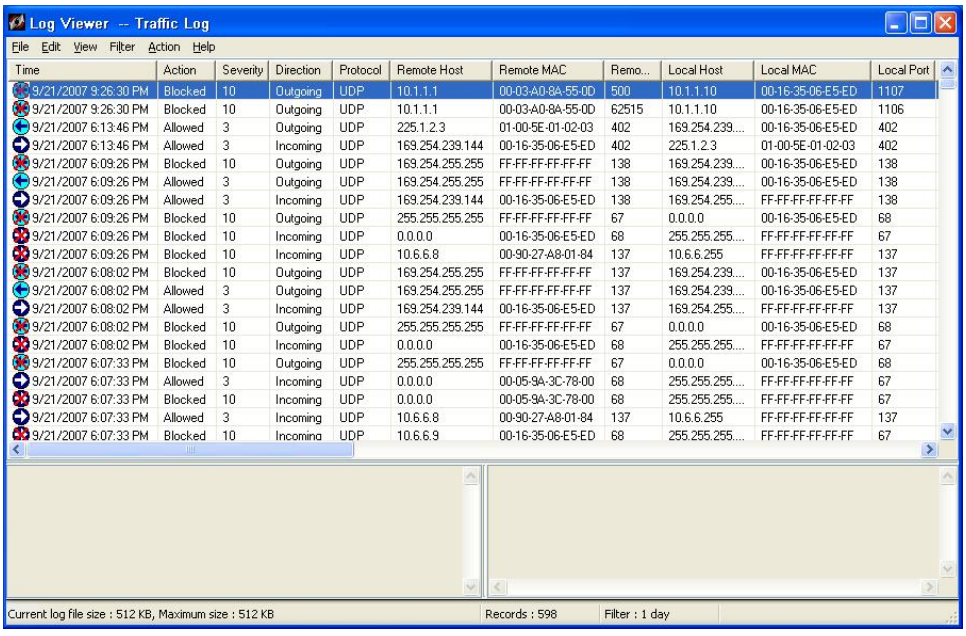
The HP t5720 XPe-based Thin Client is configured by default with the Sygate firewall actively blocking all ports except those required for basic Web browsing and RDP connections. The HP Compaq t5720 Thin Clients used in this reference white paper also had firewall port exceptions added for RGS, which accelerates graphics in a manner superior to RDP.

In order to properly configure VPN client software to communicate outside of basic Windows well-known ports, the Sygate firewall must be modified as follows:

Description	IP Address	Remote Ports	Local Ports	Incoming/Outgoing
Allow Virtual NIC operation (Deterministic Networks)	10.1.1.2 10.2.2.2	8905,8906		Both
Allow VPN UDP traffic		500,1562,8905, 8906,62515		Both

Identifying Required Firewall Modifications (Ports to Open)

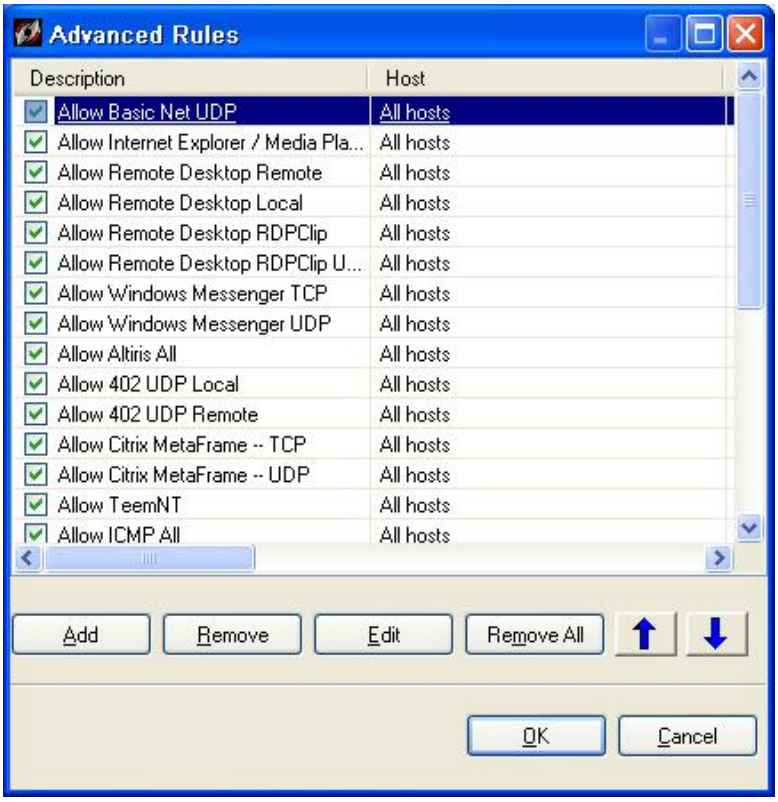
This document does not provide a full tutorial on debugging Sygate port requirements for generalized application use. However, the general methodology is to consult the Sygate traffic log carefully as applications encounter failures/errors and check for blocked traffic. In the following example, the Cisco 3560 switch internal port (10.1.1.1) in the reference configuration can clearly be seen to have blocked traffic on remote ports ports 500 and 62515 (first two entries).



Firewall Configuration

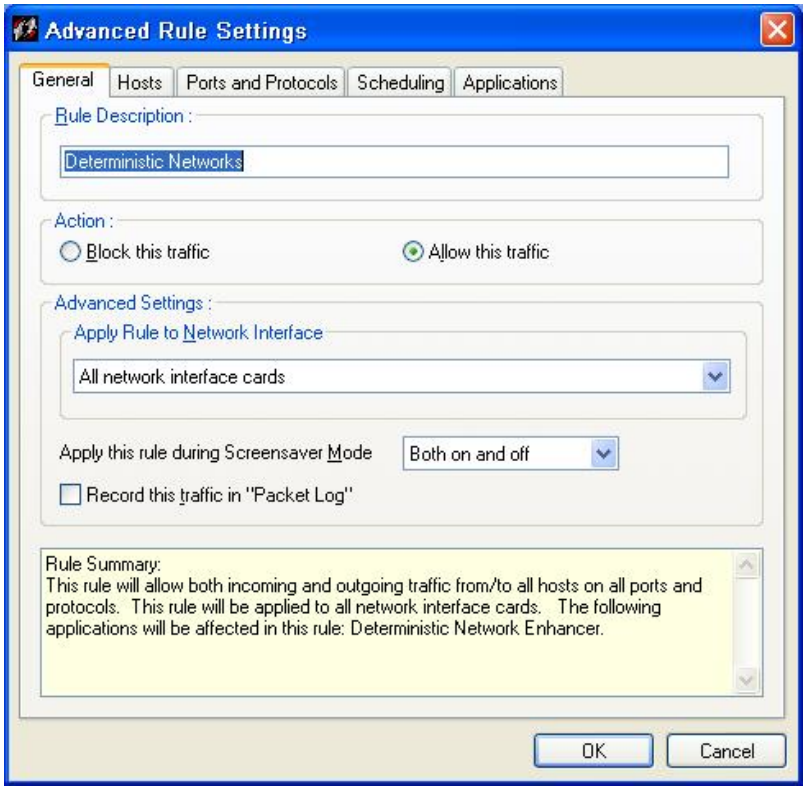
1. Reboot the t5720 and log on using an account with administrator privileges. This ensures that the thin client is in a known, clean OS state.
2. In the **System Tray**, right-click the **Sygate** icon.
3. Select **Advanced Rules**.
4. Read the warning notification and click **OK**.

5. In the **Advanced Rules** window, click **Add**.

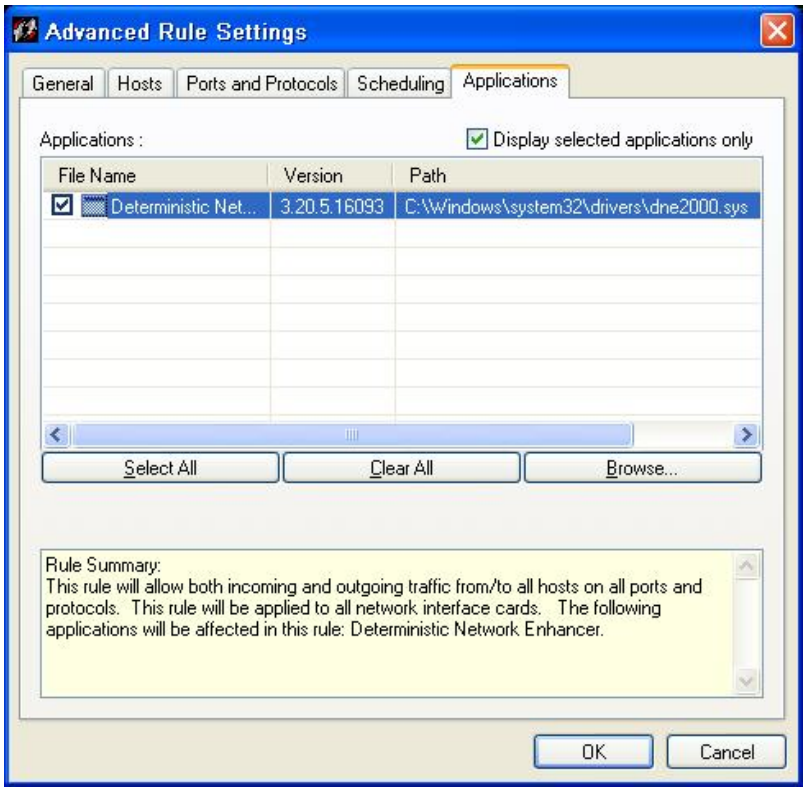


6. On the **General** tab, type `Deterministic Networks` in the **Rule Description** field.
7. Select **Allow this traffic**.

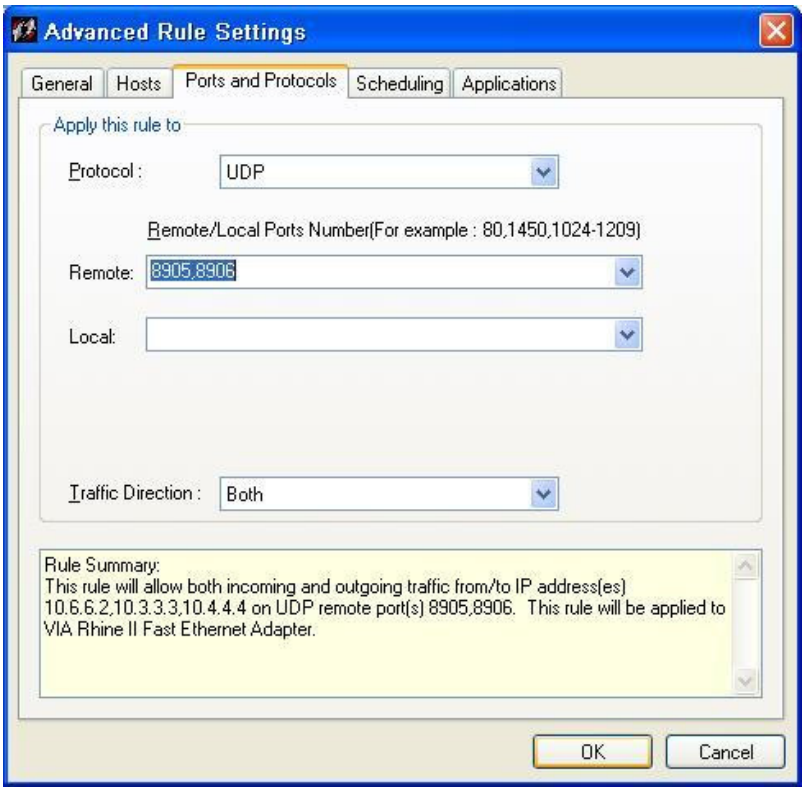
8. Select a specific network interface card or the default, **All network interface cards**.



9. On the **Applications** tab, click **Clear All** to ensure no prior application is selected.
10. Scroll down and select **Deterministic Network**s. You could also click **Browse** and browse to **c:\windows\system32\drivers\dne2000.sys** to select the t5720 network driver.
11. Select **Display selected applications only** to see the applications for this rule.

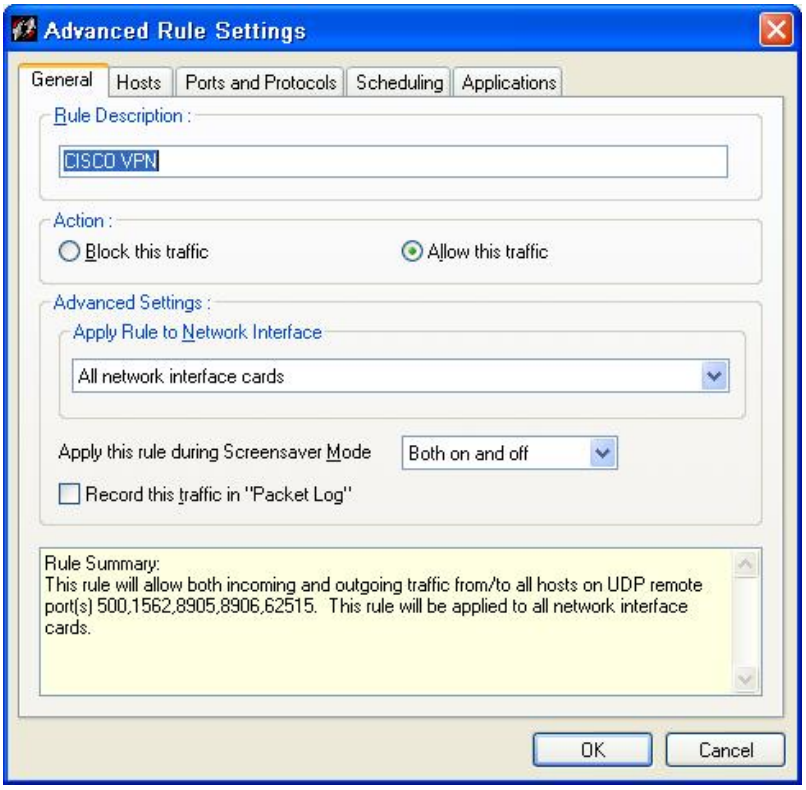


12. On the **Ports and Protocols** tab in the **Protocol** list, select **UDP**.
13. Type `8905,8906` in the **Local** field.

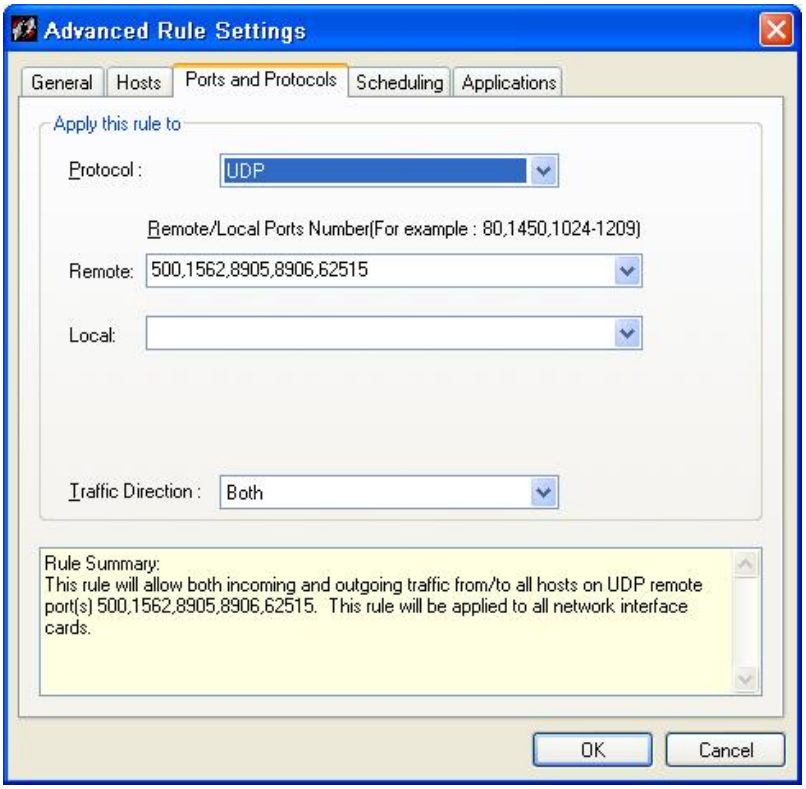


14. In the **Traffic Direction** list, select **Both**.
15. Click **OK**.
16. Next, let's add a rule for VPN UDP traffic. First, in the **Advanced Rules** window, click **Add**.
17. In the **Advanced Rule Settings** window on the **General** tab, type `CISCO VPN` in the **Rule Description** field.
18. Select **Allow this traffic**.

19. In the **Apply Rule to Network Interface** field, ensure that the proper network interface card is selected.

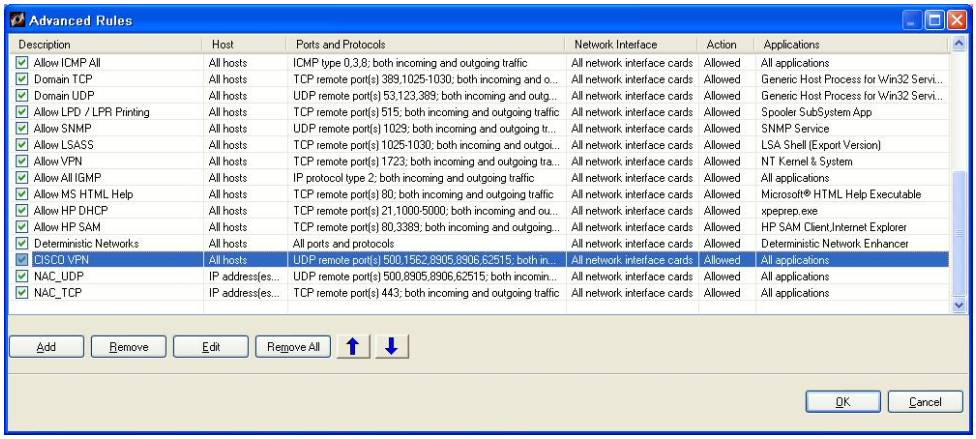


20. On the **Ports and Protocols** tab in the **Protocol** list, select **TCP**.
21. Type `500,1562,8905,8906,62515` in the **Remote** field.



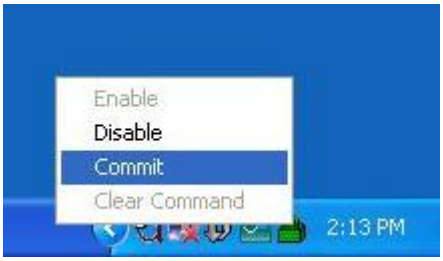
22. In the **Traffic Direction** list, select **Both**.
23. Click **OK**.

24. At this point, scroll down in Sygate **Advanced Rules** window to ensure that the two new VPM policies are defined and active.



Change Commitment to Enhances Write Filter (EWF)

At this point the Clean Access Agent is installed on the HP t5720 Thin Client. Note, however, that these image changes are not permanent. If you wish to permanently enable the agent on the thin client, please select **Commit** on the **EWF** taskbar icon or in the Control Panel EWF applet.



After restarting the thin client, the changes are permanent. The Clean Access Agent can now authenticate the user for network access and scan the user's device for software configuration compliance.

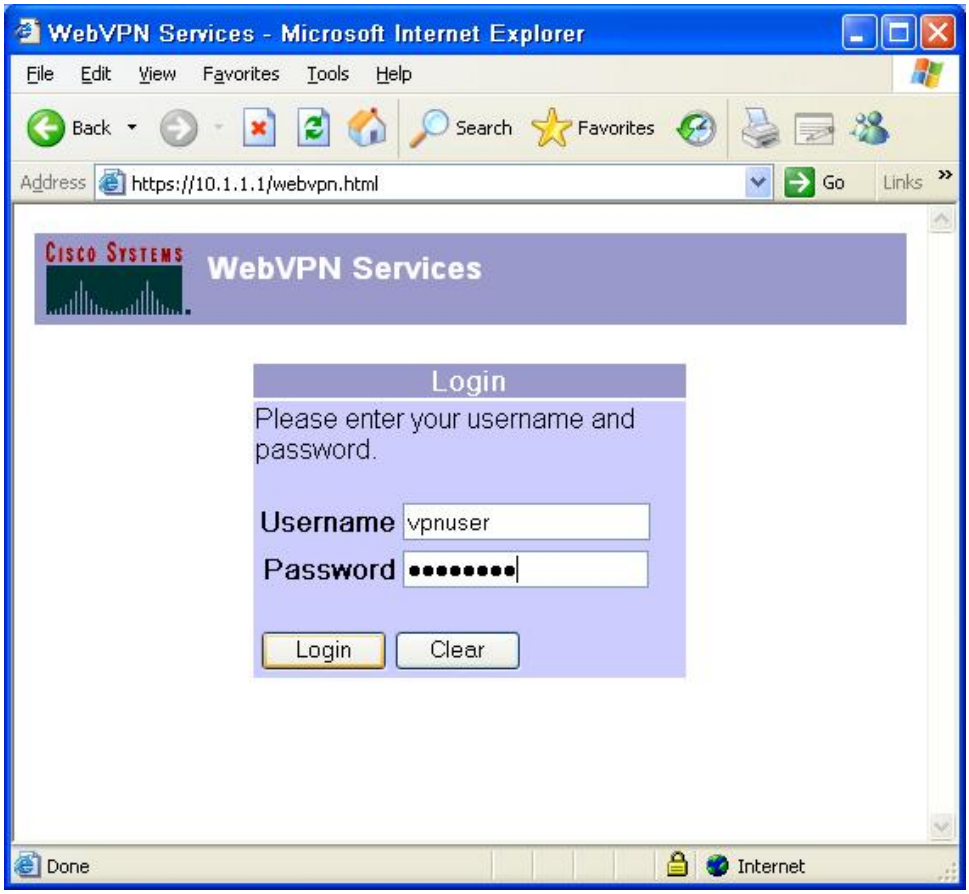
SSL VPN Access

No agent software installation is required for SSL VPN access, provided that access is allowed to Web sites on the private network only. Access to Web-enabled applications requires installation of the Java Runtime Environment (JRE) to the client device. In the case of the t5720 thin client, additional firewall settings are also required, as covered in Thin Client Firewall Exceptions.

Thin Client SSL Access

1. Turn on the thin client connected through the public interface of the VPN 3000 concentrator.
2. Go to https://10.1.1.1 in your Web browser; this launches the home page for WebVPN access to the private network.

3. Log into WebVPN Services with valid VPN credentials. Valid credentials can be stored on an internal database on the VPN 300 concentrator or on an internal user database or they can be an external RADIUS authentication. For this reference implementation, we are using credentials stored on an internal user database on the VPN 3000 concentrator.

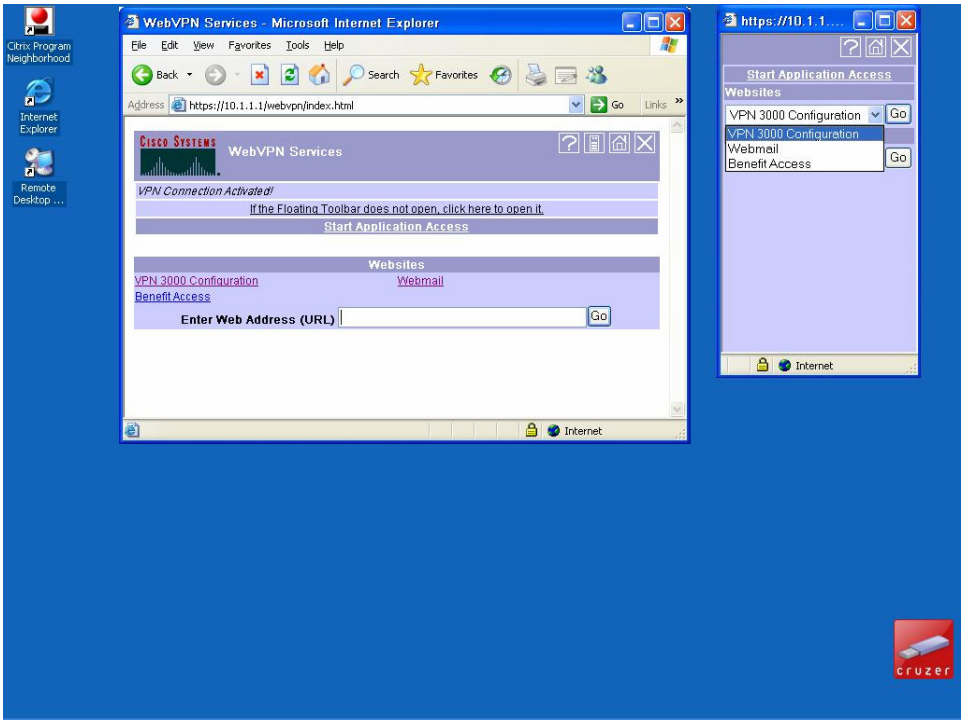


Upon successful validation of login credentials, a welcome message is displayed.

NOTE: while a simple **VPN Connection Activated** message is used for this reference implementation, the message is fully customizable from the private network via the VPN 3000 Appliance Settings Web console. This console is at https://10.2.2.1 for this reference implementation.

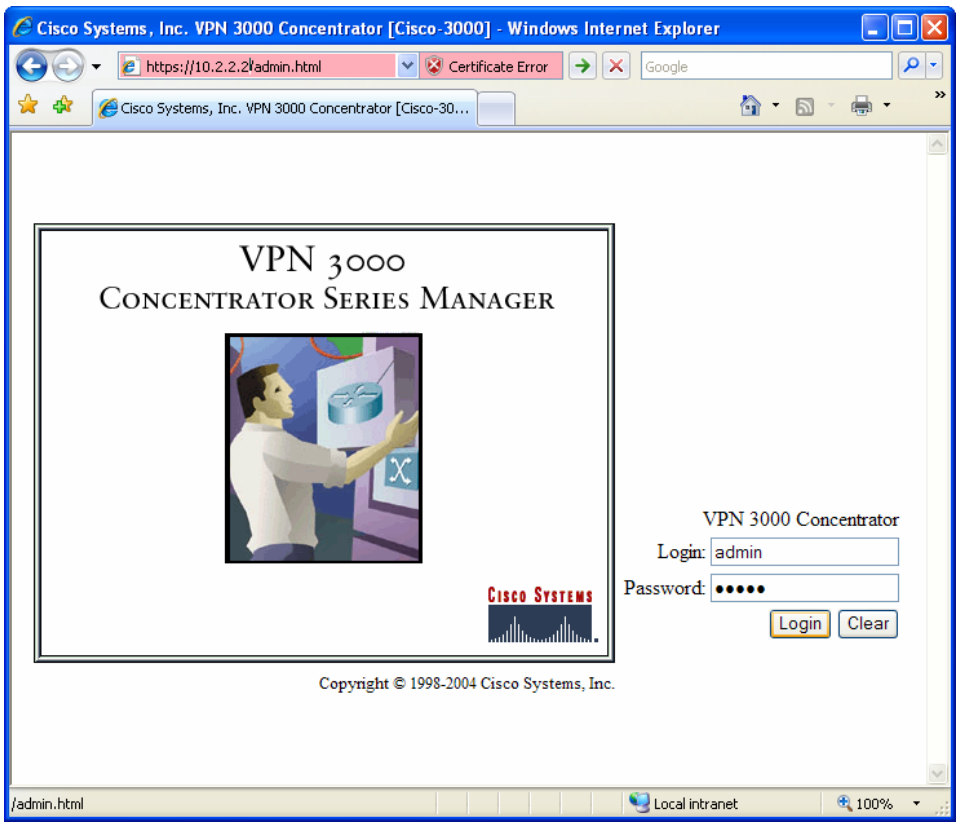
4. Click **OK** to continue.

5. Two windows are launched that allow access to Web sites and Web-enabled applications on the private interface. In this reference implementation, a few Web server URLs are pre-configured for one click access: VPN 3000 Configuration, Webmail and Benefit Access. This configuration.



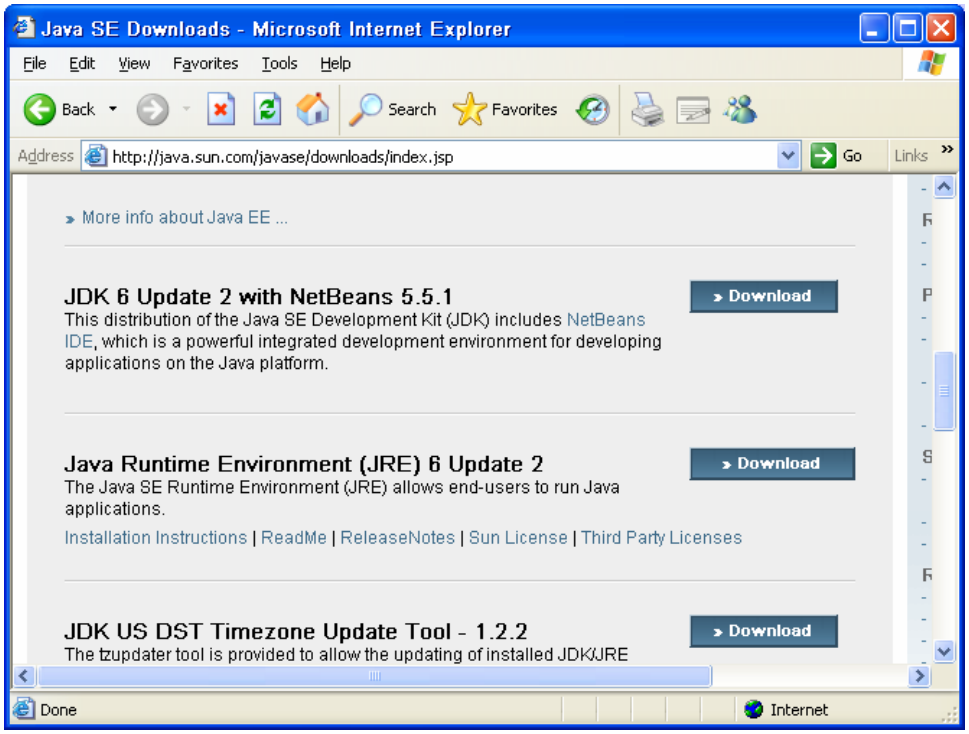
For information on configuring URLs, refer to Figures 15-28, 15-29 and accompanying text from CISCO VPN 3000 Series Concentrator Reference documentation:
http://www.cisco.com/en/US/docs/security/vpn3000/vpn3000_47/configuration/config.html

6. At this point, entering any allowed URL (http and/or https as configured on the VPN console via private interface) is allowed. To verify that the private network is accessible, type https://10.2.2.2 into the WebVPN Services window. This should launch the VPN 3000 manager Web page.



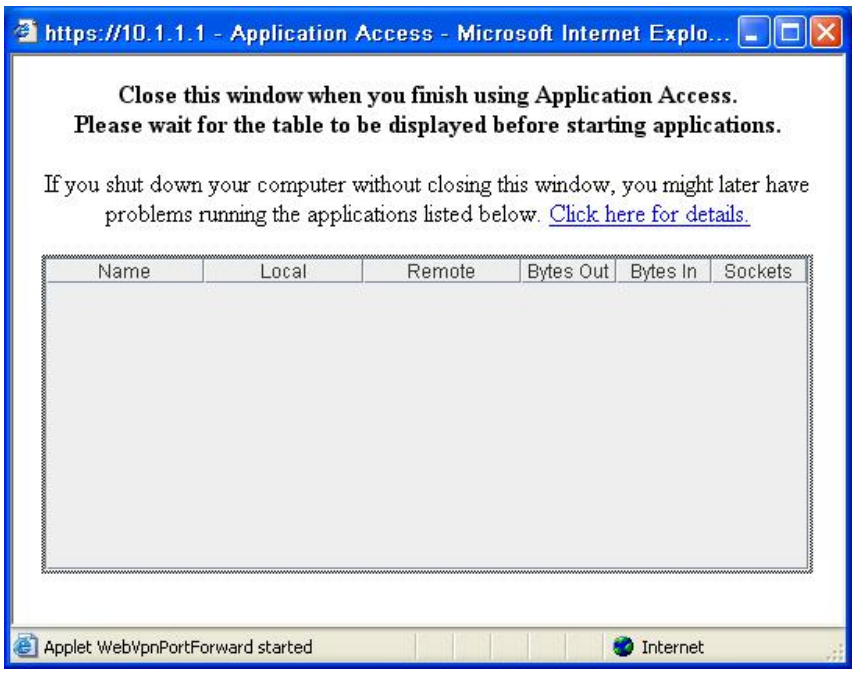
7. Now, let's return to the WebVPN console. While this white paper does not focus on Application Access via WebVPN, the following steps ensure that your t5720 is properly configured. Select **Start Application Access** to launch a Java applet window listing configured applications.

8. JRE must be installed on the client. If it is not already configured, go to the Sun Microsystems Web site at http://www.sun.com/download/index.jsp to download the latest JRE. As of the writing of this white paper, the latest t5720-compatible JRE is the 6.2 release, as shown below. Download JRE and proceed with the installation instructions.



NOTE: as in the previous configuration changes to the thin client, you must **Commit** the JRE software update to the saved thin client software image or it will be lost upon the next reset/restart. Refer to Change Commitment to Enhances Write Filter (EWF).

The application access window is shown below once system is properly configured with JRE.



Blade PC SSL Access

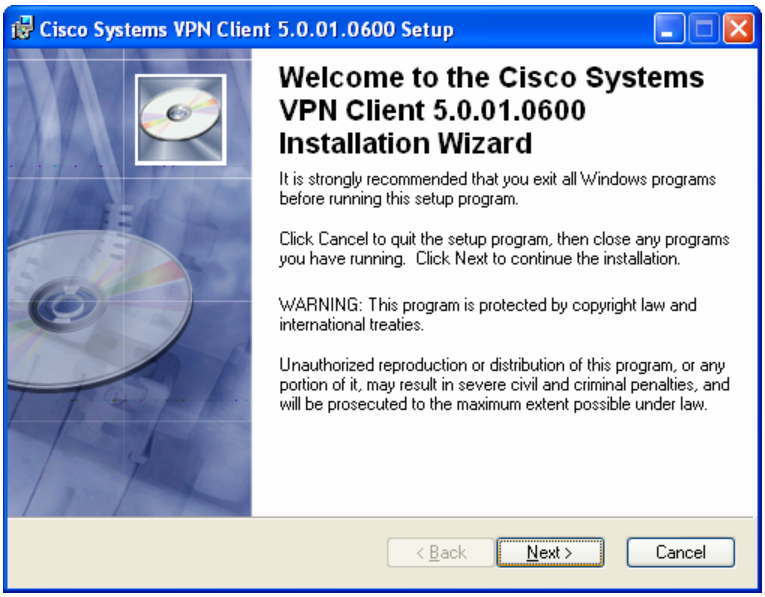
Blade PC access from public interface to the Private network follows the same steps for thin clients. The exception is that there is no requirement to **Commit** write filter to ensure that JRE software is permanently added to the blade PC software image. Provided that JRE is installed with administrative privileges, the software is added to the image on the blade.

IPSEC VPN Access

IPSEC VPN Access requires the installation of Cisco Clean Access agent (CCA) for both thin client and blade PC. IPSEC access to the private network actually allows full IP level access to the private network, with no architectural restrictions on applications and network services on the private network that can be accessed from the public interface.

Software Installation

1. Ensure that the system is loaded with the latest CISCO VPN Client. In this case, we're using Cisco Systems VPN Client V5.0.01.0600, as shown below.



2. Click **Next**, then proceed though the VPN Client installation wizard. Accept the license agreement and the default configuration settings.

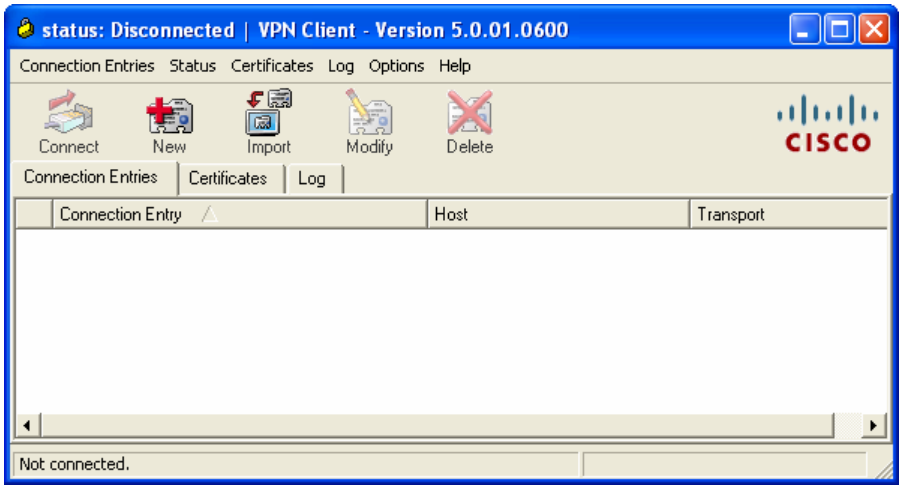
   A reboot is required to install the VPN software.

   NOTE: thin client consideration: Please **Commit** the new CCA agent to the permanent image via the EWF prior to reboot or the agent will be lost. Refer to Change Commitment to Enhances Write Filter (EWF).

Thin Client and Blade PC IPSEC Access

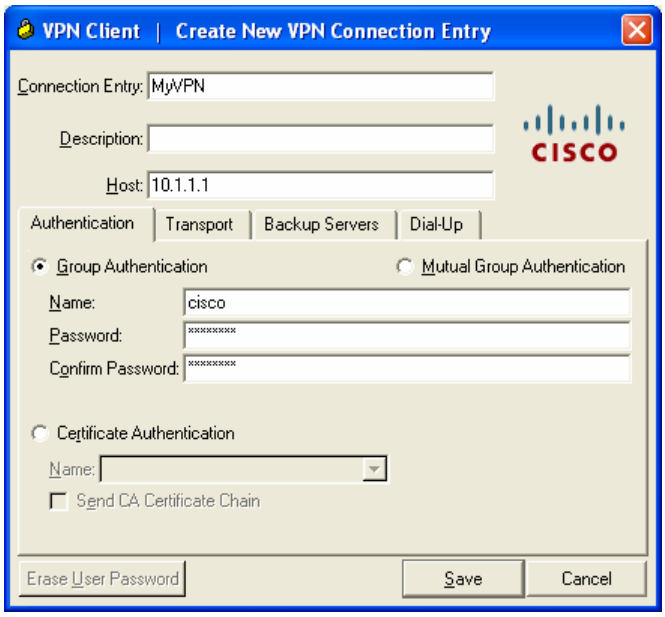
1. Launch the CCA VPN client previously installed by clicking **Start** → **All Programs** → **Cisco System VPN Client** → **VPN Client**, as shown below.

2. Click on **New** icon within the **VPN Client** status window.



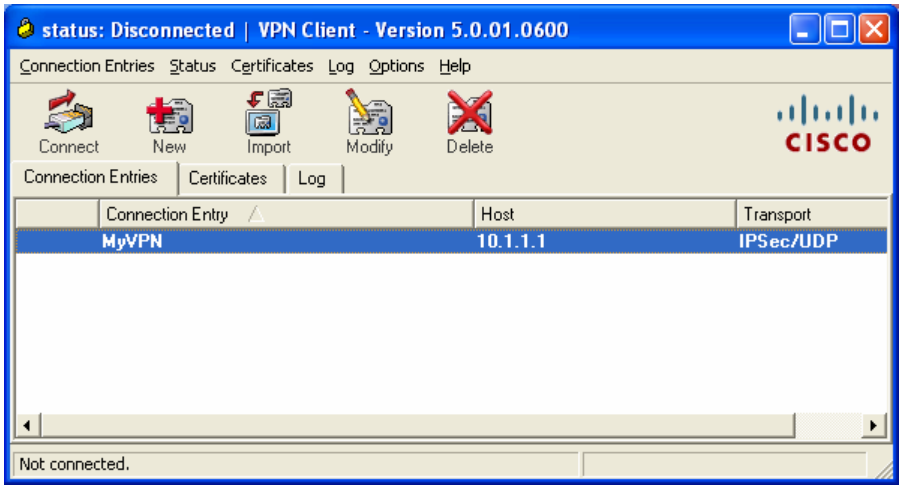
3. Type a name and host IP address for this connection (`MyVPN` and `10.1.1.1` for this reference implementation). Select **Group Authentication** as configured above and type the group name/password.

   NOTE: while group information is entered, authentication is still required from the user. If the group information is not provided here, the user is required to enter both group name/password and user name/password.

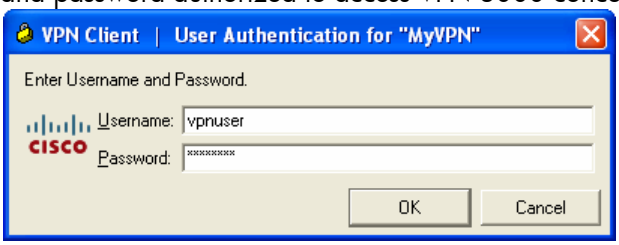


   NOTE: thin client consideration: Please **Commit** the Connection entry with Group Authentication onto the thin client permanent software image via the EWF prior. Refer to Change Commitment to Enhances Write Filter (EWF). Following the reboot, once again start the CCA VPN Client from the Windows **Start** menu as shown in step 1, and then skip to step 4.

4. Double click the **MyVPN** entry to start a connection.



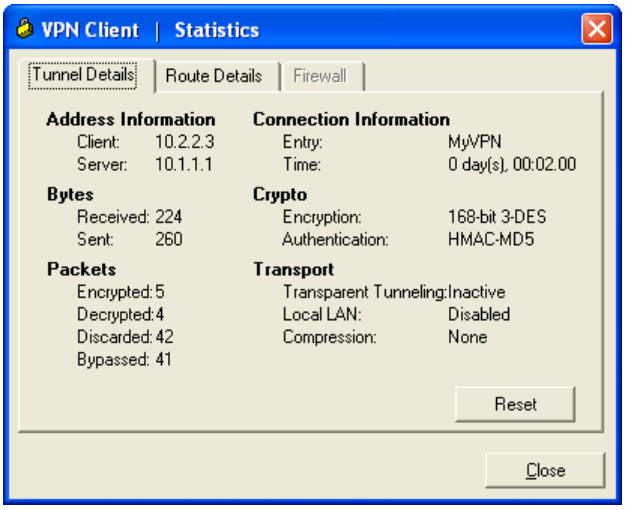
5. Enter a username and password authorized to access VPN 3000 concentrator.



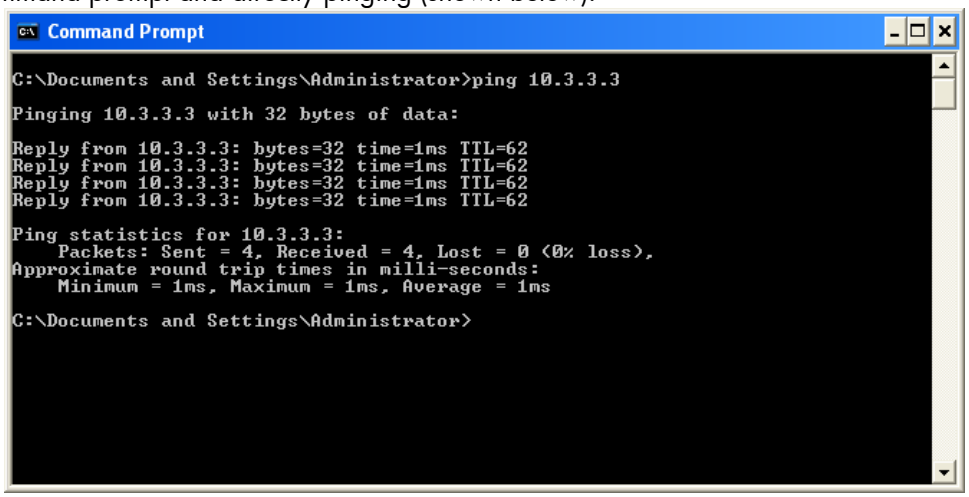
As in the case of WebVPN above, the user is greeted with a configurable banner screen upon successful connection. For this reference, a simple **VPN Connection Ac** message is used.

NOTE: this message provides an excellent opportunity to list policy restrictions governing the use of VPN and to allow the user to accept or deny those policies!

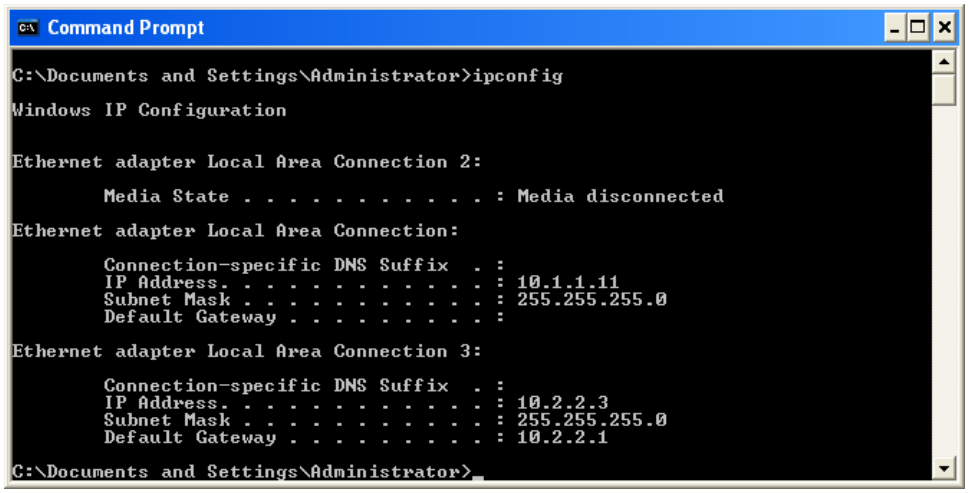
6. VPN tunnel statistics and routing information are available by right-clicking the VPN icon in taskbar. Select **Statistics** to open the following window:



7. At this point, the internal network is fully accessible via IP tunnel. We can validate this initially by pinging an address from the private network. For this reference implementation, there is a Cisco NAC appliance at 10.3.3.3., so let's make sure there is connectivity by opening a command prompt and directly pinging (shown below).



8. Run the **ipconfig** command to verify that the new IP address of the tunnel is in the 10.2.2.x subnet, as specified in the previous CAS configuration steps.



The VPN connection can be terminated via the taskbar icon. Right-click and select to disconnect the VPN tunnel.

NOTE: depending on the setting chosen within the VPN configuration process, the local network may not be accessible while the VPN tunnel is active. This is actually a preferred feature to prevent inadvertently bridging public and private networks by any client.

Appendix A – CISCO 3560 Switch Configuration

```
Switch#show configuration
Using 4021 out of 524288 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
no aaa new-model
vtp mode transparent
ip subnet-zero
ip routing
ip dhcp excluded-address 10.5.5.1 10.5.5.5
ip dhcp excluded-address 10.6.6.1 10.6.6.5
!
ip dhcp pool DHCP
 network 10.5.5.0 255.255.255.0
 default-router 10.5.5.2
!
ip dhcp pool DHCP6
 network 10.6.6.0 255.255.255.0
 default-router 10.6.6.2
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2
 name Vlan2
!
vlan 3
 name Vlan3
!
vlan 4
 name Vlan4
!
vlan 5
 name Vlan5
!
vlan 6,100,200
!
interface FastEthernet0/1
 description **TRUSTED INTERFACE ON CAS**
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 4,6,100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 2
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport access vlan 3
 spanning-tree portfast
!
interface FastEthernet0/4
 description **UNTRUSTED INTERFACE ON CAS**
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 200
 switchport trunk allowed vlan 5,200
 switchport mode trunk
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport access vlan 5
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 6
```

```
 spanning-tree portfast
!
interface FastEthernet0/10
 description **CAS CLIENT INTERFACE**
 switchport access vlan 5
 snmp trap mac-notification added
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport access vlan 6
 switchport mode access
 snmp trap mac-notification added
 spanning-tree portfast
!
interface Vlan1
 no ip address
!
interface Vlan2
 ip address 10.2.2.2 255.255.255.0
!
interface Vlan3
 ip address 10.3.3.2 255.255.255.0
!
interface Vlan4
 ip address 10.4.4.2 255.255.255.0
!
interface Vlan6
 ip address 10.6.6.2 255.255.255.0
!
interface Vlan100
 no ip address
!
interface Vlan200
 no ip address
!
ip classless
ip http server
!
access-list 101 permit udp any any
access-list 101 permit ip any host 10.4.4.4
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Vlan4
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification
snmp-server enable traps stpx root-inconsistency loop-inconsistency
snmp-server host 10.3.3.3 public mac-notification snmp
!
end
```

For more information

For more information about the HP thin clients or any other HP product, contact your HP Authorized Reseller or visit these online locations to learn more about HP products, services, and support:

HP Links:

- HP home page: www.hp.com/sbso/busproducts.html
- HP desktop, blade PC or thin client information: www.hp.com/desktops
- HP workstations information: www.hp.com/workstations
- HP security: www.hp.com/go/security
- HP notebook information: www.hp.com/notebooks
- HP notebooks options information: www.hp.com/notebooks/options
- HP desktop options information: www.hp.com/desktops/options
- HP Services: www.hp.com/go/services
- HP support: www.hp.com/go/support
- HP Care Pack: www.hp.com/hps/carepack
- "How to buy": www.hp.com/buy/howtobuy

CISCO VPN Links:

- *VPN* 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7. *http://www.cisco.com/en/US/docs/security/vpn3000/vpn3000_47/configuration/config.html*

Sun Microsystems Links:

- http://www.sun.com/download/index.jsp

466207-001, January 2008