Pulse Secure®

VPN Tunneling Configuration Guide

Published November 2020

Document Version 1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

VPN Tunneling Configuration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

VPN Tunneling

About VPN Tunneling

The VPN tunneling access option (formerly called Network Connect) provides a VPN user experience, serving as an additional remote access mechanism to corporate resources using Connect Secure. This feature supports all Internet-access modes, including dial-up, broadband, and LAN scenarios, from the client machine and works through client-side proxies and firewalls that allow SSL traffic.

When a user launches VPN tunneling, the system transmits all traffic to and from the client over the secure VPN tunnel. The only exception is for traffic initiated by other system-enabled features, such as Web browsing, file browsing, and telnet/SSH. If you do not want to enable other system features for certain users, create a user role for which only the VPN tunneling option is enabled and make sure that users mapped to this role are not also mapped to other roles that enable other system features.

With VPN tunneling, the client's machine effectively becomes a node on the remote (corporate) LAN and becomes invisible on the user's local LAN; the system serves as the Domain Name Service (DNS) gateway for the client and knows nothing about the user's local LAN. Users may define static routes on their PCs, however, to continue to access the local LAN while simultaneously connecting to the remote LAN. Since PC traffic goes through the VPN tunnel to your internal corporate resources, make sure that other hosts within a user's local network cannot connect to the PC through the VPN tunnel.

In the event of broken network connectivity, only the Windows and Macintosh versions of VPN tunneling try (indefinitely) to reconnect.

You can ensure that other hosts in a remote user's LAN cannot reach internal corporate resources by denying the user access to the local subnet (configured on the Users > User Roles > Select Role > VPN Tunneling tab). If you do not allow access to a local subnet, then the system terminates VPN tunneling sessions initiated by clients on which static routes are defined. You may also require clients to run endpoint security solutions, such as a personal firewall, before launching a network-level remote access session. Host Checker, which performs endpoint security checks on hosts that connect to a device, can verify that clients use endpoint security software.

Note: A Hosts file entry is added by VPN tunneling to support the following case:

- If, when VPN Tunneling connects, split tunneling is disabled and the original externally resolved hostname (the hostname the user initially connected to prior to the VPN tunnel launch) resolves to another IP address against the internal DNS, the browser will redirect to a "Server not found" page, because no route is defined within the client system.
- At a graceful termination (sign-out or timeout) of the VPN tunnel client connection, the Hosts file is restored. If the Hosts file was not restored in a prior case due to an ungraceful termination, the Hosts file will be restored the next time the user launches VPN tunneling.

For VPN tunneling to communicate, the following ports must be open:

- UDP port 4242 on loopback address
- TCP port 443
- If using ESP mode, the UDP port configured on the device (default is UDP 4500).

The VPN tunneling option provides secure, SSL-based network-level remote access to all enterprise application resources using the device over port 443. Port 4242 is used for IPC communication between the VPN tunneling service and the VPN tunnel executable on the client PC. Typically, endpoint products do not block this type of IPC communication. However, if you have an endpoint product that does block this communication, you must allow it for VPN tunneling to work properly.

Note: If you enable the multiple sessions per user feature, VPN tunnel clients may not be assigned the same IP address. For example, VPN tunnel client may be assigned a different VIP address each time they connect to a device when the system is obtaining the DHCP addresses from a DHCP server.

VPN Tunneling on 64-Bit Linux Platforms

A native 64-bit VPN Tunneling client is not yet available. Instead, changes in the existing 32-bit client were made so that it can be run on 64-bit platforms. Because of this, VPN Tunneling has dependencies with 32-bit Java and 32-bit standard libraries even when running on a 64-bit platform.

See the *Pulse Connect Secure Supported Platforms Guide* for a list of supported browsers, platforms and plug-ins for VPN Tunneling.

To run VPN Tunneling on a 64-bit Linux platform, you must perform the following tasks on your Linux system:

- Install a 64-bit web browser and configure the Java plug-in.
- Download and install the 32-bit Java for Linux.
- Update the Java alternatives links. If you install the 32-bit Java using package managers like "apt-get" and "yum" and so forth, the Java alternatives links are updated automatically, and you can skip this step.
  - **sudo update-alternatives --install /usr/bin/java java 32-bit-Java-path priority.**
  - Check that 64-bit Java is the default. To see which is the default Java, use the update-alternatives --display java command.
  - If necessary, use the **sudo update-alternatives --config java** command to change the default Java.
- Install the standard 32-bit libraries and components. For example, see Table 1

Table 1 Installing Standard 32-Bit Libraries and Components

Linux Distribution Method	Command
Ubuntu	
Note: This command installs Java 7 64-bit, the plugin for your browser, and the 32-bit Java with all related 32-bit libraries.	apt-get install icedtea-7-plugin openjdk-7-jre:i386
Fedora	yum -y install xterm yum -y ld-linux.so.2 yum -y libstdc++.so.6 yum -y libz.so.1 yum -y libXext.so.6 yum -y libXrender.so.1 yum -y libXtst.so.6
OpenSUSE	zypper install libXi.so.6
The syntax for launching VPN Tunneling from the command line is:	
32-bit_Java_path -cp NC.jar NC -h ivehostname-u username-p password[-r realm] -f sa_certificate_in_der_format[-l gui_log_level [-L ncsvc_log_level] [-y proxy-z proxy_port[-s proxy_username-a proxy_password[-d proxy_domain]]]	
There are no changes in the Connect Secure admin GUI or in the VPN Tunneling client user interface to run on a 64-bit Linux platform, however you should note the following: • The 32-bit Java path must be used when launching VPN Tunneling from the command line. • If the VPN Tunneling launcher cannot find the 32-bit Java path in the alternative's links, the "Setup Failed. Please install 32-bit Java and update alternatives links using update-alternatives command. For more details, please refer KB article KB25230." error appears. • Agentless host checker is supported when VPN Tunneling is launched from a browser but is not supported when VPN Tunneling is launched from command line.	

Configuring VPN Tunneling

The following steps do not account for preliminary configuration steps such as specifying the system's network identity or adding user IDs.

To configure Connect Secure for VPN tunneling:

1. Enable access to VPN tunneling at the role-level using settings in the **Users > User Roles > Role > General > Overview page of the admin console.**

2. Create VPN tunneling resource policies using the settings in the **Users > Resource Policies > VPN Tunneling tabs**:

    a. Specify general access settings and detailed access rules for VPN tunneling in the **Access Control** tab of the admin console.

    b. Specify Connection Profiles to assign to remote users in the **Connection Profiles** tab of the admin console.

   c. (Optional) Specify split tunneling behavior for VPN tunneling in the **Split Tunneling** tab of the admin console.

3. Specify whether or not to enable GINA/Credential Provider installation, employ split tunneling, and/or auto-launch behavior in the **Users > User Roles > Role > VPN Tunneling page** of the admin console.

Note: If you choose to activate split tunneling behavior in this page, you must first create at least one split-tunneling resource profile, as described above.

You must enable VPN tunneling for a given role if you want a user mapped to that role to be able to use GINA/ Credential Provider during Windows logon.

4. Specify an IP address for the VPN tunneling server-side process to use for all VPN tunneling user sessions on the System > Network > VPN Tunneling page in the admin console.
5. Ensure that an appropriate version of VPN tunneling is available to remote clients.
6. If you want to enable or disable client-side logging for VPN tunneling, configure the appropriate options in the System > Log/Monitoring > Client Logs > Settings page of the admin console.

To install VPN tunneling, users must have appropriate privileges, as described in the *Connect Secure Client-Side Changes Guide*. If the user does not have these privileges, use the Pulse Installer Service available from the Maintenance > System > Installers page of the admin console to bypass this requirement.

VPN tunneling requires signed ActiveX or signed Java applets to be enabled within the browser to download, install, and launch the client applications.

By default, Vista Advanced firewall blocks all inbound traffic and allows all outbound traffic. For VPN tunneling to work in conjunction with Vista Advanced firewall, configure the following settings:

- Change the Vista Advance firewall default settings to block all inbound and outbound traffic
- Create the following outbound rules in the appropriate firewall profile:
  - Create a port rule to allow any to any IP and TCP any port to 443
  - Create a custom rule to allow 127.0.0.1 to 127.0.0.1 TCP any to any
- Allow iExplorer.exe

In prior releases you could specify whether the system compiles packet logs for specific VPN tunneling users. This option is no longer available as it impacts performance.

VPN Tunneling Execution

The VPN tunneling agent executes as follows:

1. If Graphical Identification and Authorization (GINA) is installed and registered on the remote client, the client automatically initiates a VPN tunnel to the device when the user signs into Windows; otherwise, the user needs to sign into the device and click on the VPN Tunneling link on the end-user home page (if you have not configured VPN tunneling to launch automatically).

   Note: SSO is supported only when VPN tunneling GINA is the only GINA installed on the client's system.

2. If the user does not have the latest version of the VPN tunneling installer, the system attempts to download an ActiveX control (Windows) or a Java applet (Macintosh and Linux) to the client machine that then downloads the VPN tunneling software and performs installation functions. If the system fails to download or upgrade the ActiveX control to a Windows client due to restricted access privileges or browser restrictions, the system uses a Java applet to deliver the VPN tunneling software to the client.

   Note: If Microsoft Vista is running on the user's system, the user must click the setup link that appears during the installation process to continue installing the setup client and VPN tunneling. On all other Microsoft operating systems, the setup client and VPN tunneling install automatically.

Whether the system downloads an ActiveX control or a Java applet, both components attempt to identify the presence and version of existing VPN tunneling software on the client before determining which of the following installation functions to perform:

- If the client machine has no VPN tunneling software, install the latest version.
- If the client machine has an earlier version of VPN tunneling software, upgrade the shared VPN tunneling components to the newer version and install the most current UI version.

  Note: For information about valid Java applets, installation files and logs, and the operating system directories in which delivery mechanisms run, see the Pulse Connect Secure Client-Side Changes Guide.

3. Once installed, the VPN tunneling agent sends a request to the system to initialize the connection with an IP address from the pre-provisioned IP pool (as defined by the VPN Tunneling Connection Profiles resource policies applicable to the user's role).
4. The VPN tunneling system tray icon starts running in the taskbar on a Windows client or in the Dock on a Mac client.
5. The system allocates an IP address (from a VPN Tunneling Connection Profiles resource policy) and assigns a unique IP to the VPN tunneling service running on the client.
6. The client-side VPN tunneling service uses the assigned IP address to communicate with the VPN tunneling process running on the system.
7. After the system allocates an IP address to the client, it opens a direct channel of communication between the client and all enterprise resources to which the user's resource policy allows access. The internal application server sees the source IP as the client's IP address.

The client-side VPN tunneling agent communicates with the device, which, in turn, forwards client requests to enterprise resources.

Note: If you use Host Checker to validate the presence of client-side security components based on policies you define on the system and the client cannot conform to the security policies at any point during a VPN tunneling session, Host Checker terminates the session.

Credential Provider for Windows Vista and Later

In releases prior to Windows Vista, the customization of interactive user logon was done by creating a custom GINA. Users entered their authentication credentials in the logon UI and GINA passed this information to Winlogon for authentication. However, because GINAs do more than pass authentication information, they are typically difficult to implement.

Windows Vista introduced a new authentication model where the logon UI and Winlogon talk directly with each other. A credential provider is a module that plugs into the logon UI and describes the credential information required for the login UI to render and to communicate with an external authentication provider. After the credential provider gathers the credential information, it passes the final credentials to Winlogon.

There are two basic types of credential providers: standard authentication and Pre-Logon Access Providers (PLAP). Standard authentication includes password-based or certificate-based credentials. A PLAP is a special type of credential provider that allows users to make a network connection before logging in to their system. Another difference between these two types of providers is timeout. PLAP credentials have no timeout where standard credentials typically have a 120 second timeout.

The VPN tunneling credential provider is a PLAP provider. This provider is visible only if the system is configured as part of a domain. The VPN tunneling provider creates a network connection. If the user's credentials are the same as the domain credential (SSO) then the credential information is entered only once. If the user's credentials are not the same as the domain credentials, the users select another credential provider for domain authentication.

After a user logs in through VPN tunneling credential providers, the user has 5 minutes to log in to Vista either through single sign-on or through another credential provider. After the user logs into Vista, VPN tunneling attaches to the tunnel. If the user does not log in to Vista within 5 minutes, the VPN tunneling tunnel is disconnected.

To install the VPN tunneling credential provider,

1. Make sure your client user is part of a Windows domain.
2. In the Admin console, go to **User Roles > VPN tunneling** and select the **Require VPN tunneling to start when logging into Windows** option.
3. When installing VPN tunneling on the client system (running Windows Vista), you are prompted by the GINA/Credential Provider window to configure the GINA/Credential Provider authentication. Click **OK**.
4. Once the VPN tunnel is established on the client system, open the VPN tunneling window. Go to the Advanced View and select the **Information** tab. In the Results section, ensure that the GINA/Credential Provider plug-in is configured. You should see something similar to GINA Plug-In: Configured.

To use credential provider:

1. Log out of Windows and press **Ctrl+Alt+Delete**.

   You should see the **Network logon** icon. If you see only the Windows user standard tiles, click the **Switch user** option under the standard Windows credential tiles to see the Network logon icon.
2. Click the **Network logon** icon and then click the **Connect Secure logon** icon.
3. Enter your Windows domain credential and click the right arrow button. For your username, use the format domain\username or user@domain.

VPN tunneling signs the user in to the default URL and proxy server in config.ini.

> **Note:** If your Connect Secure credential is not the same as your Windows domain credential, an alert box appears. Click **OK** and enter your Connect Secure credentials in the login window that appears. The window also contains an option button to launch another window to enter a URL, proxy server, and so forth.

VPN tunneling credential provider supports the following authentication provider: Active Directory, local authentication, RADIUS (UN/PWD only), NIS and Dial-up connection. In additional, smart card credential provider supports certificate login.

Smart Card Credential Provider

Windows Vista also supports smart card credential provider-passing user credentials upon a smart card being inserted. If there is smart card present, a VPN tunneling Smart Card Credential Provider DLL tile shows on the PLAP layer. Click the tile and enter your smart card PIN to log in.

To install the smart card VPN tunneling credential provider,

1. Make sure your client user is part of a Windows domain.
2. In the Admin console, select **User Roles >** ***Role*** **> VPN Tunneling** and select the **Require client to start when logging into Windows** option.
3. When installing VPN tunneling on the client system (running Windows Vista), you are prompted by the GINA window to configure the GINA authentication. Click **OK**.

   Use the smart card to log in to the device from a browser so the config.ini file will contain the smart card login URL which can then be used by the smart card DLL.
4. Once the VPN tunnel is established on the client system, open the VPN tunneling window. Go to the Advanced View and select the **Information** tab. In the Results section, ensure that the GINA plug-in is configured. You should see something similar to GINA Plug-In: Configured.

To use the smart card credential provider:

1. Log out of Windows and press **Ctrl+Alt+Delete**.

   You should see the **Network logon** icon located in the lower right corner of your screen. If you see only the Windows user standard tiles, click the **Switch user** option under the standard Windows credential tiles to see the Network logon icon.
2. Click the **Network logon** icon and then click the **smart card** icon.
3. Enter your PIN number or password and click the right arrow button.

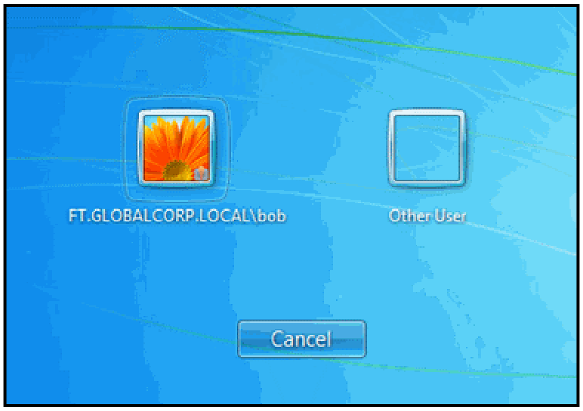
VPN tunneling uses the PIN to retrieve the stored certificate and to log in to Connect Secure. After a successful login, the PIN is passed to Winlogon to log in to Vista.

> **Note:** If your Connect Secure credential is not the same as your Windows domain credential, an alert box appears. Click **OK**. If a connection icon appears in the lower right corner of your screen, switch to the standard credential login tiles and log in to Vista. Otherwise, enter your Windows credential in the login box.
>
> VPN tunneling retrieves the user principal name (UPN) from the smart card and compares them with the login user and domain names. If they do not match, the tunnel is disabled. The UPN typically has the format user@domain.

Credential Provider Authentication for Connect Secure

The Pulse credential provider integration enables connectivity to a network that is required for the user to log on to the Windows domain. For example, the domain controller might reside behind a firewall and the endpoint uses credential provider login to connect to Connect Secure prior to domain login. Pulse integrates with Microsoft credential providers to enable password-based login and smart card login. A credential provider interface appears as a tile on a Windows (Vista or later) login screen. See Figure 1.

Figure 1 Pulse Logon Tile



You enable Pulse credential provider support on a Pulse connection. After the connection has been downloaded to the endpoint through the normal Pulse distribution methods, a Pulse logon tile appears on the endpoint's desktop. When the user initiates the logon process, Pulse establishes the connection.

Pulse supports the following credential provider types:

- **user-at-credprov** - The connection is established before the user login using credentials collected at the selected credential tile, which provides single-sign-on functionality. The connection is maintained as an active connection on the user's desktop.
- **machine-then-user-at-credprov** - The connection is established using machine credentials when no user is logged in. When a user clicks a logon tile and provides user credentials, the machine connection is disconnected, and a new connection is established. When the user logs off, the user connection is disconnected, and the machine connection is reestablished. In one typical machine-then-user-at-cred prov implementation, the machine connection and the user connection are mapped to different VLANs.

Pulse credential provider support usage notes:

- If the endpoint includes more than one Pulse Layer 2 connection, Windows determines which connection to use:

1. If a network cable is attached to the endpoint, Layer 2 wired connections are attempted, and then wireless connections. If there are more than one wireless network available, the order is determined by the scan list specified as a Pulse connection option.
2. After all Layer 2 options are attempted, Pulse runs location awareness rules to find one or more eligible Layer 3 connections that are configured for credential provider login. If more than one Layer 3 connection is found, Pulse prompts the user to select a connection. A user can cancel the network connection attempt by clicking the cancel button.

3. After Pulse evaluates all configured connection options, Pulse returns control to Windows, which enables the user login operation.

- For connections that use user credentials, the Pulse connection may be configured so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt. For connections that use machine credentials, Pulse prompts cause the connection to fail because there is no interface to allow a response to the prompts. You can suppress any potential realm and role choice by specifying a preferred realm and role for the connection.
- Pulse upgrade notifications and actions are disabled during credential provider login and postponed until the user connection is established. Host Checker remediation notifications are displayed.
- To allow users to log in using either a smart card or a password, you can create different authentication realms for each use case and then specify a preferred smart card logon realm and a preferred password logon realm as part of the connection properties.

To enable user-at-credprov credential provider support for a Pulse connection:

1. Create a Pulse connection set for the role (**Users > Pulse > Connections),** and then create a **new Pulse connection.** You can select **Connect Secure or Policy Secure (L3), Policy Secure (802.1X), or SRX for the** connection type.
2. In the Connection is established section, select one of the following options:

- **Automatically at user login** - The user credentials are used to establish the authenticated Pulse connection to the network, log in to the endpoint, and log in to the domain server. The Pulse connection may be configured so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt.
- **Automatically when the machine starts. Connection is authenticated again at user login** - Machine credentials are used to establish the authenticated Pulse connection to the network when the endpoint is started. When a user clicks the login tile and provides user credentials, the connection is authenticated again, and the original connection is dropped. When the user logs off, the user connection is ended and the machine connection is established again. In one typical use case, the machine credentials provide access to one VLAN and the user credentials provide access to a different VLAN. Be sure that the Pulse connection does not result in Pulse prompts, for example, prompts for realm or role selection or a server certificate trust prompt, because the machine credential login does not present an interface to respond to the prompts.

3. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type Any as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.
4. Specify **Realm and Role Preferences** to suppress realm or role selection dialogs during the logon process:

- **Preferred User Realm** - Specify the realm that for this connection. The connection ignores any other realm available for the specific logon credentials

  The following options enable you to allow the user to log in using a smart card or a password:

  - **Preferred Smartcard Logon Realm** - Preferred realm to be used when user logs in with a smart card.

  - **Preferred Password Logon Realm** - Preferred realm to be used when user logs in with a password.

Note: Be sure that the authentication realms you specify exist, and that they support the appropriate login credential option.

- **Preferred User Role Set** - Specify the preferred role or the name of rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.

To enable machine-then-user-at-credprov credential provider support for a Pulse connection:

1. Create a **Pulse** connection set for the role **(Users > Pulse > Connections),** and then create a new Pulse connection. You can select C**onnect Secure or Policy Secure (L3), Policy Secure (802.1X), or SRX for the connection type.**
2. In the Connection is established section, select one of the following options:
   - **Automatically at user login -** The user credentials are used to establish the authenticated Pulse connection to the network, log in to the endpoint, and log in to the domain server. The Pulse connection may be configured so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt.
   - **Automatically when the machine starts. Connection is authenticated again at user login -** Machine credentials are used to establish the authenticated Pulse connection to the network when the endpoint is started. When a user clicks the login tile and provides user credentials, the connection is authenticated again, and the original connection is dropped. When the user logs off, the user connection is ended, and the machine connection is established again. In one typical use case, the machine credentials provide access to one VLAN and the user credentials provide access to a different VLAN. Be sure that the Pulse connection does not result in Pulse prompts, for example, prompts for realm or role selection or a server certificate trust prompt, because the machine credential login does not present an interface to respond to the prompts.
3. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type Any as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.
4. Specify Realm and Role Preferences to suppress realm or role selection dialogs during the logon process for both machine logon and user logon:
   - **Preferred Machine Realm** - Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm available for the specific logon credentials
   - **Preferred Machine Role Set** - Specify the role or the name of rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.
   - **Preferred User Realm** - Specify the realm that for this connection that is used when a user logs onto the endpoint. The connection ignores any other realm available for the user's logon credentials.
   - **Preferred User Role Set** - Specify the preferred role or the name of rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.

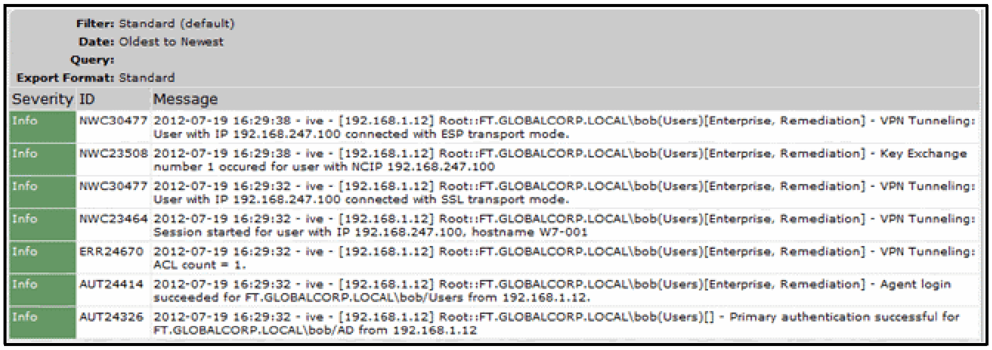
5. Optionally specify pre-login preferences:
   - **Pre-login maximum delay** - The time period (seconds) that a Windows client waits for an 802.1x connection to succeed during the login attempt. The range 1 to 120 seconds.
   - **Pre-login user based virtual LAN** - If you are using VLANs for the machine login and the user login, you can enable this check box to allow the system to make the VLAN change.
6. Click **Save Changes** and then distribute the Pulse connection to Pulse client endpoints.

The Pulse tile appears on the login page the next time the end users log in.

> Note: The user account must exist on both the Windows PC and on Connect Secure with the same login name.

Check the user logs for credential provider log-in information. See Figure 2.

Figure 2 Credential Provider Log Information



Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Info	NWC30477	2012-07-19 16:29:38 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: User with IP 192.168.247.100 connected with ESP transport mode.
Info	NWC23508	2012-07-19 16:29:38 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - Key Exchange number 1 occured for user with NCIP 192.168.247.100
Info	NWC30477	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: User with IP 192.168.247.100 connected with SSL transport mode.
Info	NWC23464	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: Session started for user with IP 192.168.247.100, hostname W7-001
Info	ERR24670	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: ACL count = 1.
Info	AUT24414	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - Agent login succeeded for FT.GLOBALCORP.LOCAL\bob/Users from 192.168.1.12.
Info	AUT24326	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[] - Primary authentication successful for FT.GLOBALCORP.LOCAL\bob/AD from 192.168.1.12

Launching VPN Tunneling During a Pulse Secure Application Manager Session

Users can launch VPN tunneling while signed in to Connect Secure via Pulse Secure Application Manager (PSAM). When a user launches VPN tunneling in this scenario, however, the VPN tunneling installer automatically terminates the PSAM session prior to launching VPN Tunneling.

During the process, the user is prompted with a warning message informing them that they are about to terminate their PSAM session in favor of launching VPN tunneling. We recommend that you configure users' VPN tunneling resource policies to feature as much access to network resources as they would have in their PSAM sessions. This way, when users choose to launch VPN tunneling (simultaneously terminating PSAM) they will still be able to access the same network resources.

> Note: If users choose not to launch VPN tunneling, the VPN tunneling installer still automatically installs the client application on their computer, but does not launch VPN tunneling. After the client application has been installed, users can choose to uninstall it manually via their secure gateway home page or the folder options available in the Windows Start menu.

Logging in to Windows Through a Secure Tunnel

Use the Logoff on Connect feature for users to log in to their Windows environment through an existing VPN tunnel. This feature lets them authenticate against a Windows Domain server in real time, as opposed to authenticating with the locally cached credentials. When this feature is enabled, they are automatically logged off Windows after the VPN tunneling session starts. The standard Windows login screen re-appears, and they log in using their Windows credentials. Their Windows environment is now established through the VPN tunnel.

> **Note:** Users must log in to Windows within 5 minutes of the login screen re-appearing or before the Host Checker policy evaluate period ends, whichever is shorter. If they do not, their VPN tunnel connection may time out and they will not be logged in to Windows through a secure tunnel. An error appears if the VPN tunnel connection times out.

The Logoff on Connect feature is not supported within SVW.

1. To use the **Logoff** on Connect feature:
2. Users log on to their local machine using their domain cached credentials. Their machine must be part of a Windows domain.
3. Users launch VPN tunneling and click **Tools** from the login page.
4. Select the **Logoff on Connect** option and click **OK**.
5. Users enter their username and password credentials in the login page.

   A tunnel is established and logs them off of their local machine. The Windows login page appears.
6. Users enter their username and password credentials to sign in to their Windows Domain using the VPN tunnel.

VPN Tunneling Connection Profiles with Support for Multiple DNS Settings

To ensure remote users are able to perform DNS searches as efficiently or as securely as possible, you can configure the system to allow multiple DNS settings during VPN tunneling sessions, based on a user's role membership.

When the system launches a user's VPN tunneling session, it uses a matching profile based on the user's role membership containing IP address, DNS, and WINS settings.

If you enable split-tunneling, the DNS search order setting allows you to define which DNS setting takes precedence-for example, search for a DNS server on the client's LAN before the system's DNS server, or vice-versa. VPN tunneling makes a backup of the client's DNS settings/search order preference before establishing a connection. After the session terminates, VPN tunneling restores the client to the original DNS settings. If you disable split-tunneling, all DNS requests go to the system's DNS server and your setting for the DNS search order preference does not apply.

Note: After stopping and restarting a DNS client, the client may not pick up the search order of multiple DNS addresses in a timely manner, resulting in an incorrect lookup order when launching VPN tunneling. The rules governing DNS name resolution and failover are complex and often specific to the particular client operating system. You or the end user can attempt to run the ipconfig /registerdns commands from a command window on the client machine. This may reset the search order to the correct order. To understand the search resolution order for DNS servers, refer to the appropriate Microsoft DNS documentation for your operating system platform.

When employing a multi-site cluster of Connect Secure devices, the IP pool and DNS settings may be unique to each device residing at a different site. For this reason, the system allows the VPN Tunneling Connection Profile policy to be node-specific. That is, the resource policy enables the client to connect to the same device in the cluster each time a new session is established.

VPN Tunneling Incompatibility with Other VPN Client Applications

Third-party vendor VPN client applications may be incompatible with VPN tunneling. Table 2 lists known VPN client vendors and VPN tunneling's relative compatibility with those vendors' VPN client applications.

Table 2 VPN tunneling Compatibility with Third-Party VPN Clients

Vendor	Compatible?
Cisco	Yes
Nortel	Yes
NS Remote	Yes
Intel	Yes
Checkpoint	Yes

If you want to install VPN tunneling on a client featuring an incompatible VPN client application, you must uninstall the incompatible application before you install or launch VPN tunneling on the client.

Linux Client Requirements

Linux clients signing in to VPN tunneling via Mozilla Firefox must ensure that the OpenSSL libraries are installed on the client. Most Linux versions come pre-packaged with OpenSSL. If you encounter a Linux user that does not have the required OpenSSL libraries, you can direct them to the following resource where they can be obtained and installed for free:

See http://www.openssl.org/related/binaries.html for details. (You can also advise users to compile their own version by directing them to the source at http://www.openssl.org/source/ .) The required version is libssl.so.0.9.6b.

Note: Install the full version of OpenSSL. The "light" version of OpenSSL will not work.

Client-Side Logging

VPN tunneling client-side logs are files that reside on the remote client containing sign-in, debug, and other statistical information you can use to troubleshoot potential issues with VPN tunneling. When you enable client-side logging for VPN tunneling users, the client records VPN tunneling events in a series of log files, continually appending entries each time a feature is invoked during subsequent user sessions. The resulting log files are useful when working with the support team to debug problems with VPN tunneling.

If VPN tunneling users turn client-side logging off, (even if logging is enabled on the system) the client does not record any new client-side log information. If the user turns on the logging function and the system is then configured to disable client-side logging, the client does not record any new client-side log information.

VPN Tunneling Proxy Support

VPN tunneling provides support for remote clients using a proxy server to access the Internet (and Connect Secure via the Internet), as well as clients who do not need a proxy to access the Internet, but who access resources on an internal network through a proxy. VPN tunneling also provides support for clients accessing a Proxy Automatic Configuration (PAC) file that specifies client and system proxy settings enabling access to Web applications.

> **Note:** The VPN tunneling client does not support the use of the MS Winsock proxy client. Please disable the MS Winsock proxy client before running the VPN tunneling client. For more information, see http://www.microsoft.com/windowsxp/using/mobility/expert/vpns.mspx.

To address these varying methods of proxy implementation, VPN tunneling temporarily changes the proxy settings of the browser so that only traffic intended for the VPN tunneling session uses the temporary proxy settings. All traffic not intended for the VPN tunneling session uses the existing proxy settings.

> **Note:** The VPN tunneling client does not support the option to automatically detect proxy settings. You must choose to use either an automatic configuration script (PAC) or specify a proxy server. You cannot use both a proxy server and an automatic configuration script, together. You can define one or the other under the Proxy section in Users > Resource Policies > VPN Tunneling > Connection Profiles > Profile.

Whether split-tunneling is enabled or disabled, the system supports the following proxy scenarios:

- Using an explicit proxy to access Connect Secure
- Using an explicit proxy to access internal Web applications
- Using a PAC file to access Connect Secure
- Using a PAC file to access internal Web applications

Please note the following exceptions:

- The system does not support redirect downloads and therefore does not support the redirecting of the internal PAC file download.
- The system's dsinet client does not support SSL; you cannot obtain the internal PAC file from the SSL server.
- The system does not support "auto detect proxy". If both static proxy and "auto proxy script (pac)" are defined, it uses the static proxy configuration.

- The VPN tunneling profile does not have a static proxy exception field for internal proxy. If you require proxy exceptions, you can use a PAC file with proxy exception logic.
- The VPN tunneling client supports "auto proxy script (pac)" only when the configuration is the PAC file URL. If the URL is a redirect URL or IE proxy configuration script it is not supported.

  When split-tunneling is enabled, VPN tunneling manages proxy settings in one of the following ways, depending on the method with which the proxy is implemented:
- For remote clients using a proxy server to access the Internet, all HTTP requests generated by the browser and intended for the system go through either an explicit proxy or a PAC file accessed by the remote client. Because the presence of an explicit proxy or access to a PAC file is already provisioned on the client-side, the client sets up the local, temporary proxy before attempting to establish a VPN tunnel.
- For remote clients using a proxy server to access the Internet, all HTTP requests generated by the browser and intended for the system go through either an explicit proxy or a PAC file accessed by the remote client. Because the presence of an explicit proxy or access to a PAC file is already provisioned on the client-side, the client sets up the local, temporary proxy before attempting to establish a VPN tunnel.
- When a remote client accesses a preconfigured HTTP-based PAC file, the client cannot access the PAC file until after a VPN tunnel is established. After a connection is established, the client accesses the PAC file, includes the PAC file contents in the local temporary proxy, and then refreshes the browser proxy setting.

VPN Tunneling Quality of Service

To support quality of service (QoS) on your internal network via VPN tunneling, the system translates the "inner" IP packet header (for Application-layer packet encapsulation, for example) to the "outer" packet header, thus enabling Network layer-level packet prioritization. Routers in the network are then able to identify, prioritize, and appropriately forward VPN tunneling IPsec packets across the network. This feature helps ensure that you are able to support time-sensitive IP packet transmission and reception like IP video streams, for example.

Note: VPN tunneling QoS applies to UDP (IPsec) packets only. SSL packet encapsulation and forwarding behavior remains unchanged when you employ the QoS feature.

VPN Tunneling Multicast Support

To enable streaming IP video broadcasts over the internal network, VPN tunneling features Internet Group Management Protocol (IGMP) gateway multicast proxy support.

Note: VPN tunneling does not support IGMP v2. If you are using VPN tunneling multicast support, and you are using L2 switches, make sure the switches support IGMP v3.

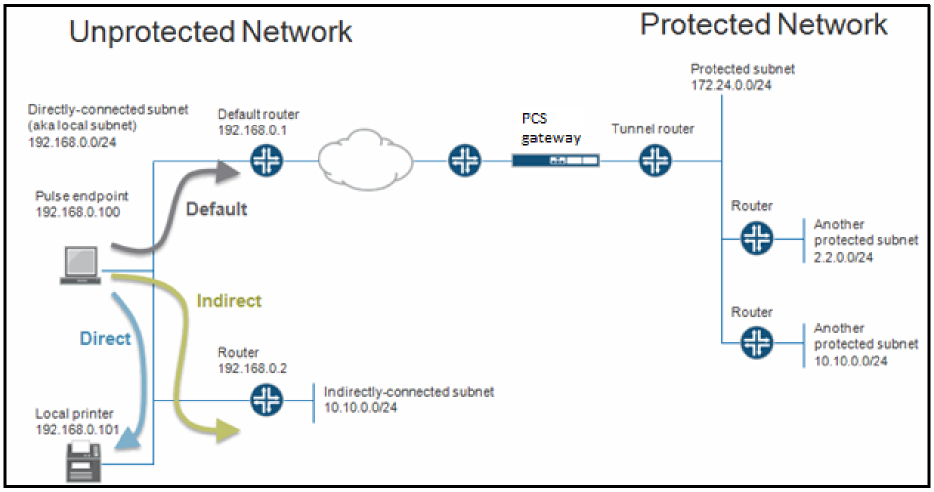
When users initiate a request to join a multicast group, the system initiates an IGMP join message to the local multicast router or switch on the client's behalf. In addition, the system stores the IGMP group request queries in its cache so that whenever a multicast router in the network polls the system for IGMP group information, it responds with its current collection of multicast user and group requests. If a router or switch does not receive a response from the system, the system's multicast group information is removed from the router or switch's forwarding table.

Note: VPN tunneling supports streaming media at up to 2 mbps on a single tunnel (megabits per second).

About Split Tunneling Role Options

shows an unprotected network that contains the endpoint client and other unprotected resources, and a protected network that contains networks that can only be accessed through a VPN tunnel through Connect Secure.

Figure 3 Example Network Scenario



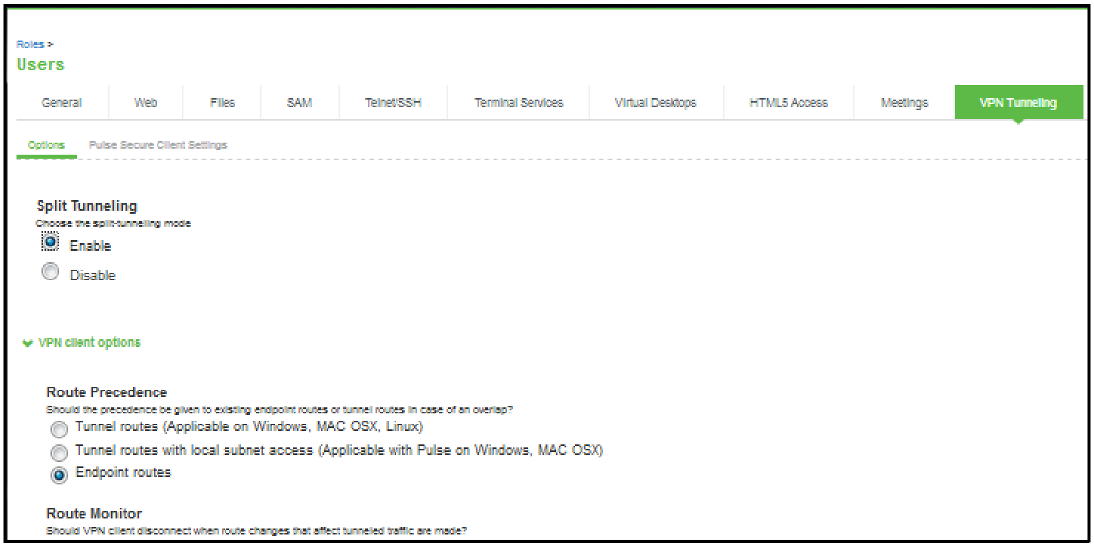
Before a VPN tunnel is created, there are three types of endpoint routes.

- Directly-connected subnet routes-Hosts on the directly-connected subnet can be reached without forwarding through a router. The ability to access these hosts is defined as local subnet access. 192.168.0.0/24 is an example of a directly-connected subnet route.
- Indirectly-connected subnet routes-These routes that have an explicit non-direct entry in the route table. Traffic must go through a router. 10.10.0.0/24 is an example of an indirectly-connected subnet route.
- Default route-this route if the destination is neither a direct-connected or indirect-connected subnet route. 0.0.0.0 is an example of a default route.

Enabling Split Tunneling

Options on the Users > User Roles > Role Name >VPN Tunneling page determine how the endpoint routes are modified when the VPN tunneling is established. See Figure 4

Figure 4 Split Tunnel User Role Options



Split Tunneling

Choose the split-tunneling mode

● Enable

○ Disable

Route Precedence

Should the precedence be given to existing endpoint routes or tunnel routes in case of an overlap?

○ Tunnel routes (Applicable on Windows, MAC OSX, Linux)

○ Tunnel routes with local subnet access (Applicable with Pulse on Windows, MAC OSX)

● Endpoint routes

Route Monitor

Should VPN client disconnect when route changes that affect tunneled traffic are made?

Split Tunneling options are:

- **Enable** - Adds or modifies routes for specific subnets to go to the tunnel, allowing access to the protected subnets. Subnets are defined in the Users > User Roles > Role-Name > VPN Tunneling > Options window. In the case of subnet overlap (the specified split-tunnel subnet conflicts with an existing endpoint route), the Route Precedence option is used. For example, 2.2.2.0/24 goes through the tunnel. 10.10.0.0/24 is both a split-tunnel subnet and an indirectly-connected subnet. The Routing Table, defined below, defines how 10.10.0.0/24 is handled.
- **Disable -** Modifies the default route to go through the tunnel, allowing access to the protected network. For example, 0.0.0.0 now goes through the tunnel.

Note:

- These settings apply only to systems with Split Tunneling enabled.
- These settings do not apply to third-party clients.
- Windows 8 (and later) will send a DNS request to only one interface. So, for Windows 8+ clients, selecting the first radio button sends DNS requests to the client's DNS only, whereas clicking either the second or third radio button sends DNS requests only to the Pulse Secure gateway's DNS.
- For IP based Split Tunneling on Windows 8.1 machine, the DNS requests are sent to both the IVE and the Client DNS servers at the same time due to the limitation in platform API.
- For IP based Split Tunneling on Windows 10 machine, the DNS requests are sent to the IVE DNS server first and then sent to the Client DNS servers, irrespective of the DNS search order configured (1st or 2nd radio button).
- For FQDN based Split Tunneling, the DNS requests are sent to the IVE DNS servers only (3rd radio button), irrespective of the option selected.
- OSX does not support sending DNS requests to only the Pulse Secure gateway's DNS. So, for OSX clients, clicking the third radio button will have the same effect as the second button.

- For Windows Phone and Windows machines running the In-Box VPN client, checking the third radio button sends all DNS requests to only the Pulse Secure gateway's DNS. Having either other button checked causes only DNS requests matching the DNS domains (listed above) to go to the gateway's DNS, and all other requests go to the client's DNS.

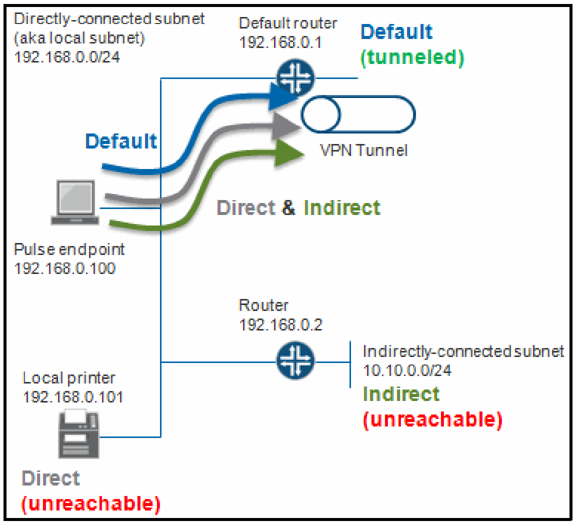
Defining the Route Precedence Options

The Route Precedence option determines how the directly-connected subnet routes and the indirectly-connected subnet routes are modified. This depends on whether split-tunneling is enabled.

If split tunneling is disabled:

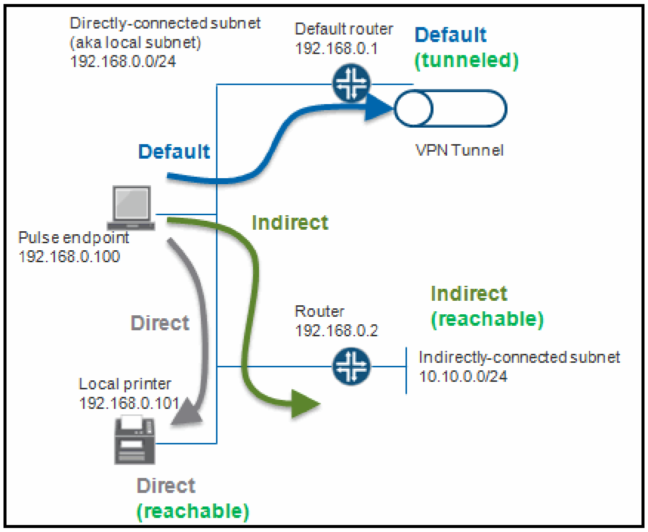
- Tunnel routes have precedence-Both directly-connected subnet routes and indirectly-connected subnet routes go through the tunnel. Endpoints lose access to the unprotected subnets. See Figure 6.

Figure 5 Tunnel Route Precedence Example



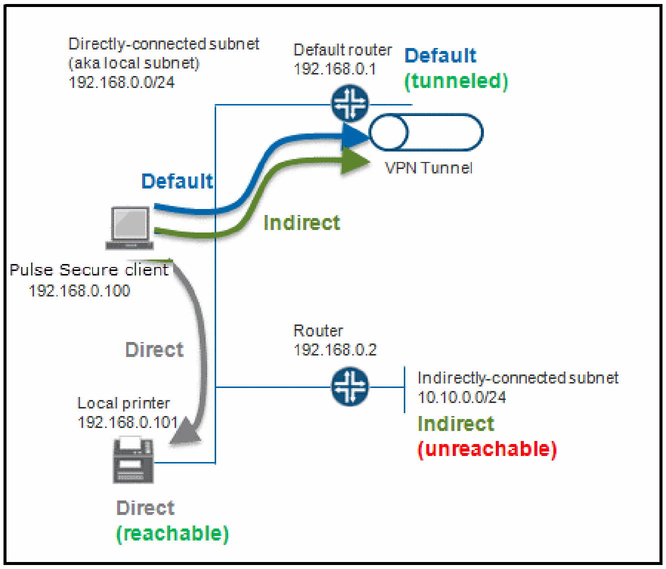
- Endpoint routes have precedence-Neither directly-connected subnet routes nor indirectly-connected subnet routes go through the tunnel. See Figure 6.

Figure 6 Endpoint Route Precedence Example



- Tunnel routes with local subnet access-Similar to the tunnel routes have precedence option except that directly-connected subnet routes do not go through the tunnel. Stated another way, tunnel all traffic except for traffic that is destined for the local subnet. This allows endpoints to access the local subnet. See Figure 7.

Figure 7 Tunnel Routes with Local Subnet Access Example



If split tunneling is enabled:

- Non-overlapped subnets are added to the route table. For example, 2.2.0.0/24 goes through the tunnel. See Figure 3.
- Overlapped subnets have 2 options:
  - **Tunnel routes have precedence** - These routes are modified to go through the tunnel and endpoints lose access to the unprotected overlapped subnet. For example, 10.10.0.0/24 goes through the tunnel. See Figure 145.

- **Endpoint routes have precedence** - These routes do not go through the tunnel. For example, 10.10.0.0/24 does not go through the tunnel. See Figure 3.

Table 3 summarizes how split tunneling and route precedence works with directly-connected subnet routes, indirectly-connected subnet routes, and default routes.

Table 3 Split Tunnel and Route Precedence

Split Tunnel	Route Precedence	Direct Endpoint Route	Indirect Endpoint Route	Default Endpoint Route	Split Tunnel Policy Routes
Disabled	Tunnel	Goes through tunnel.	Goes through tunnel.	Goes through tunnel.	NA
Disabled	Tunnel with local subnet access	Does not go through tunnel.	Goes through tunnel.	Goes through tunnel.	NA
Disabled	Endpoint	Does not go through tunnel.	Does not go through tunnel.	Goes through tunnel.	NA
Enabled	Tunnel	Routes are modified to go through the tunnel only if they overlap with the split-tunneling subnets. Otherwise the routes do not go through the tunnel.	Routes are modified to go through the tunnel only if they overlap with the split-tunneling subnets. Otherwise the routes do not go through the tunnel.	Does not go through tunnel	New routes are added to go through the tunnel.
Enabled	Tunnel with local subnet access	Does not go through tunnel.	Routes are modified to go through the tunnel only if they overlap with the split-tunneling subnets. Otherwise the routes do not go through the tunnel.	Does not go through tunnel.	New routes are added to go through the tunnel.
Enabled	Endpoint	Does not go through tunnel.	Does not go through tunnel.	Does not go through tunnel.	New routes are added to go through the tunnel.

Defining VPN Tunneling Role Settings

Use role-level settings to specify split-tunneling, auto-launch, auto-uninstall, Graphical Identification and Authentication (GINA) options.

To specify VPN tunneling split-tunneling, auto-launch, auto-uninstall, and GINA installation options:

1. In the admin console, choose **Users > User Roles > Role Name > VPN Tunneling**.
2. Under Options, select one of the following Split Tunneling options:
   - **Enable** - This option activates split-tunneling and adds (or modifies) routes for specific subnets to go to the tunnel, allowing access to the protected subnets. The subnets are specified in the Users > Resource Policies > VPN Tunneling > Split-tunneling Networks window. In the case of subnet overlap (for example, the specified split-tunnel subnet conflicts with an existing endpoint route), the Route Precedence option (described below) is used.
   - **Disable** - All network traffic from the client goes through the VPN tunnel, allowing access to the protected network. When the session is established, predefined local subnet and host-to-host routes that might cause split-tunneling behavior are removed, and all network traffic from the client goes through the VPN tunnel. With split tunneling disabled, users cannot access local LAN resources during an active VPN session.
3. Under **VPN client options**, select:
   - **Route precedence** - This option defines how the directly-connected subnet routes and the indirectly-connected subnet routes are modified. The exact effect depends on whether split-tunneling is enabled.
   - **Tunnel Routes** - The route table associated with the Pulse virtual adapter take precedence. Pulse overwrites the physical interface routes if there is conflict between the Pulse virtual adapter and the physical adapters. Pulse restores the original routes when the connection is ended.
   - **Tunnel Routes with local subnet access (Pulse on Windows and Mac OS X only)** - Network traffic addressed to the networks defined in the split tunnel resource policies goes through the VPN tunnel. Network traffic that is addressed to the directly-connected (local) subnet goes to the local subnet. The default route is set to the local subnet, so all other network traffic is subject to the original endpoint routing table.
   - **Endpoint Routes** - The route table associated with the endpoint's physical adapter take precedence.

Note: Setting route precedence to Endpoint Routes allows users to access the local subnet regardless of whether split tunneling is enabled or disabled.

- **Route Monitor** - Specify whether you want route monitoring enabled.
  - **Yes** - VPN tunneling ends the connection only if the route change affects the VPN tunnel traffic. For example, if the route metric is changed higher, it should not disconnect VPN tunneling.
  - **No -** Route tables are allowed to change on the client endpoint.
- **Traffic Enforcement** - When Traffic Enforcement is enabled, Pulse creates rules on the endpoint's firewall (Mac and Win) that ensure that all traffic conforms to the split tunneling configuration. For example, a local program might bypass the routing tables and bind traffic to the physical interface instead of allowing it to go through the Pulse virtual interface. If you enable traffic enforcement, you ensure that all traffic is bound by the split tunneling configuration.
  - **IPv4** - All IPv4 traffic should go through tunnel according to routes.
  - **IPv6** - All IPv6 traffic should go through tunnel according to routes.

- **Enable TOS Bits Copy** - Select this option to control the client behavior in networks that employ quality of service (QoS) protocols. When you enable this check box, the Pulse Secure client copies IP Type of Service (TOS) bits from the inner IP header to outer the IP Header. Note that enabling this option might require a reboot of the client endpoint when the client software is installed for the first time on Windows endpoints. Pulse Secure clients support TOS bit copy only for IPsec transport and not for SSL transport.
- **Multitask** - Select this option if you want VPN tunneling to operate in multicast mode.
- **Auto-launch** - Select this option to activate VPN tunneling automatically when the endpoint is started.

4. Under Options for VPN client on Windows, select:

   - **Launch client during Windows Interactive User Logon** - When this option is enabled, the Pulse Secure client starts when the user logs into Windows. Note that this setting is not the same as the Pulse connection settings that control machine authentication and credential provider authentication. Choose one of the following options:

     Require client to start when logging into Windows

     Allow user to decide whether to start client when logging into Windows

5. For Session Scripts, specify the following:

   - **Windows: Session start script** - Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse connects with Connect Secure. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
   - **Windows: Session end script** - Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse disconnects from Connect Secure. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.
   - **Select the Skip if Windows Interactive User Logon Enabled** option to bypass the specified Windows session start script.

   If the client signs in to their Windows Domain via the GINA/Credential Provider automatic sign-in function, a script is executed by the Windows client. In this case, the sign-in script may be identical to the specified VPN Tunneling start script. You can use this option, therefore, as a way to avoid executing the same script twice.

   Windows only supports scripts with the .bat or .cmd extension (referring to batch files, not the .cmd applications within MSDOS). To run a .vbs script, the user must have a batch file to call the .vbs script. Similarly, to run an .exe application (like C:\WINDOWS\system32\mstsc.exe), the user must have a batch file to call the .exe application.

   - **Options for VPN client on Mac** apply only to Pulse on Apple OS X endpoints:
     - **Mac: Session start script** - Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse connects with Connect Secure. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
     - **Mac: Session end script** - Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse disconnects from Connect Secure. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.

- **Linux**: **Session start script** - Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse connects with Connect Secure. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
- **Linux**: **Session end script -** Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse disconnects from Connect Secure. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.

When VPN tunneling launches, start and end scripts are copied to the client and, upon session termination, are removed from the client. Scripts can be accessed locally or remotely via file share or other permanently-available local network resource. Macintosh clients only support running start and end script located on the local machine.

> **Note:** The client should be a member of the same domain as the remote server to allow VPN tunneling to copy start and end scripts. If the client credentials are unknown to the server, the script copy fails, and VPN tunneling does not prompt the user to enter username and password.

The client makes a copy of the end script after the tunnel has been set up and stores the script in a temporary directory to ensure that, if the network connection were to fail, the end script can still be used to terminate the VPN tunnel session.

6. Click **Save Changes.**

About VPN Tunneling Resource Policies

VPN tunneling resource policies specify a variety of session parameters you can use to determine the method of access for remote clients. You can configure the following types of resource policies and apply them to one or more user roles:

- **Access resource policies** - This policy type specifies which resources users may access when using VPN tunneling, such as Web, file, and server machines on the corporate intranet.
- **Packet logging resource policies** - This policy type allows you to compile client-side VPN tunneling packet logs on the system to help diagnose and resolve connection issues. Connection profiles resource policies-This policy type specifies which option (DHCP or system-managed IP address pool) The system uses to assign an IP address to the client-side VPN tunneling agent. You can also use this feature to specify the transport protocol and encryption method for the VPN tunneling session.
- **Split Tunneling resource policies** - This policy type enables you to specify one or more network IP address/netmask combinations for which the system handles traffic passed between the remote client and the corporate intranet.

  A few notes about specifying resources for a VPN tunneling resource policy:

  - You cannot specify a hostname for a VPN tunneling resource policy. You can only specify an IP address.
  - You can specify protocols (such as tcp, udp, icmp) for VPN tunneling. For all other access feature resource policies, specifying protocols is not supported.
  - If the protocol is missing, all protocols are assumed. If a protocol is specified, then the delimiter ":// " is required. No special characters are allowed.

- You cannot mix port lists and port ranges, such as 80, 443, 8080-8090 for VPN tunneling resource policies.
- If you specify a port, you must specify a protocol.
- If the port number is missing, the default port * is assigned for http.

Defining VPN Tunneling Access Control Policies

Use the VPN Tunneling Access Control tab to write a resource policy that controls resources users can connect to when using VPN tunneling.

To write a VPN tunneling access resource policy:

1. In the admin console, choose **System > Configuration > VPN Tunneling**.
2. In the Enable/Disable FQDN ACL section, select the **Check to Enable FQDN ACL** check box and save changes.

Note: Ensure that there is no DNS latency/delay in your network that may lead to performance issues.

3. Choose **Users > Resource Policies > VPN Tunneling > Access Control.**
4. On the Access Control page, click **New Policy**.
5. On the New Policy page, enter:
   - A name to label this policy.
   - A description of the policy. (optional)
6. In the Resources section, specify the IPv4/IPv6/FQDN Resources for which this policy applies, one per line.

Note: When a packet is fragmented, fragment #1 contains more information than all subsequent fragments. Fragment #1 contains the IP address, protocol, and port information. All subsequent fragmented packets contain just the IP address and protocol information. Therefore, the VPN Tunneling ACL evaluates the first packet fragment different from the subsequent packet fragments. For the subsequent packet fragments, the system applies the VPN Tunneling ACL based on just the IP address and protocol since the port number is not available.

7. In the Roles section, specify:
   - **Policy applies to ALL roles** - To apply this policy to all users.
   - **Policy applies to SELECTED roles** - To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
   - **Policy applies to all roles OTHER THAN those selected below** - To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
   - **Allow access** - Select this option to grant access to the resources specified in the Resources list.

- **Deny access** - Select this option to deny access to the resources specified in the Resources list.
- **Use Detailed Rules** - Select this option to define resource policy rules that put additional restrictions on the specified resources.

9. Click **Save Changes.**
10. On the Access Policies page, order the policies according to how you want to evaluate them. Keep in mind that once the system matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Writing a Detailed Rule for VPN Tunneling Access Control Policies

IPv6/FQDN support for ACLs - Layer 3 feature can be configured in the same way as IPv4, in the following 2 ways:

- Simple Rules
- Detailed Rules

Simple Rules: Admin can configure IPv4/IPv6/FQDN addresses with allow/deny rules. These rules permit/deny access to an IPv4/IPv6/FQDN resource based on the IPv4/IPv6/FQDN address configured.

Detailed rules: Admin can configure IPv4/IPv6/FQDN addresses with allow/deny rules with conditions. These rules permit/deny access to an IPv4/IPv6/FQDN resource based on the IPv4/IPv6/FQDN address configured when the condition matches.

Every entry in the ACL policy corresponds to 2 entries in the FORWARD chain in iptables/ip6tables. One in the inbound direction and the other in the outbound direction.

To create/edit VPN Tunneling Access Control policy with IPv4/IPv6/FQDN resources with detailed rules:

1. On the New Policy page for a resource policy, enter the required resource and role information.
2. In the Action section, select U**se Detailed Rules** and then click **Save Changes.**
3. On the **Detailed Rules** tab, click **New Rule.**
4. On the Detailed Rule page:

   In the Action section, specify:

   - **Allow Access** - This option will permit accessing an IPv4/IPv6/FQDN resource based on the IPv4/IPv6/FQDN address configured.
   - **Deny Access** - This option will not allow accessing an IPv4/IPv6/FQDN resource based on the IPv4/IPv6/FQDN address configured.

   In the Resources section, specify:

   In the IPv4 Resources section, specify the IPv4 resources and

   In the IPv6 Resources section, specify the IPv6 resources

   In the FQDN Resources section, specify the FQDN name. FQDN-based split tunneling lets the admin configure split tunneling rules by directly specifying the domain names. This is helpful while configuring rules to ignore or tunnel cloud services. For FQDN resources wild card domains are allowed.

Note: Admin can either configure IPv4 resources or IPv6 resources or FQDN resources or all three.

Note: FQDN is not supported on IPv6. FQDN resource will be given preference over IPv4 incase of conflict.

Note: FQDN resources are supported only with the Device DNS option enabled in the connection profile. Allow the DNS IP address under the IPv4 address resource access list or select the option Auto allow DNS/WINS IP in the connection profile.

In the Conditions section, specify one or more expressions to evaluate in order to perform the action (optional):

- **Boolean expressions**: Using system variables, write one or more boolean expressions using the NOT, OR, or AND operators.
- **Custom expressions:** Using the custom expression syntax, write one or more custom expressions.

When specifying a time condition, the specified time range cannot cross midnight. The workaround is to break the time range into two conditions.

5. Click **Save Changes.**
6. On the **Detailed Rules** tab, order the rules according to how you want the system to evaluate them. Keep in mind that once the system matches the resource requested by the user to a resource in a rule's Resource list, it performs the specified action and stops processing rules (and other resource policies).

Creating VPN Tunneling Connection Profiles

Use the **Users > Resource Policies > VPN Tunneling > Connection Profiles** page to create VPN tunneling connection profiles. When the system receives a client request to start a VPN tunneling session, it assigns an IP address to the client-side agent. The system assigns this IP address based on the DHCP Server or IP Address Pool policies that apply to a user's role. In addition, this feature allows you to specify the transport protocol, encryption method, and whether or not to employ data compression for the VPN tunneling session.

Nodes in a multi-site cluster share configuration information, which means that devices in different networks share an IP address pool. Since any node may receive the client request to start the VPN tunneling session, you need to specify an IP filter for that node that filters out only those network addresses available to that node. When the cluster node receives a request to create a VPN tunnel, it assigns the IP address for the session from the filtered IP address pool.

To write a VPN tunneling connection profile:

1. In the admin console, choose **Users > Resource Policies > VPN Tunneling > Connection Profiles**.
2. On the Connection Profiles page, click **New Profile** and configure the settings described in Table 4.
3. Save the configuration.
4. On the Connection Profiles page, order the profiles according to how you want to evaluate them. Keep in mind that once the system matches the resource requested by the user to a resource in a profile's (or a detailed rule's) Resource list, it performs the specified action and stops processing profiles. See Table 4.

Table 4 VPN Tunneling Connection Profile Settings

Setting	Guidelines
Name	A name to label this policy.
Description	A description of the policy (optional).
IPv4 address assignment	
DHCP servers	Specify the hostname or IP address of a network Dynamic Host Configuration Protocol (DHCP) server responsible for handling client-side IP address assignment. You can specify up to three DHCP servers by listing each one on a separate line. When multiple DHCP servers are listed, the system sends a DHCP Discover message to all listed DHCP servers and then waits five seconds for a response. If multiple DHCP servers respond, the system chooses the one with the longest lease period. The system sends a DHCP release packet to the DHCP server when the VPN tunneling session ends. DHCP provides a framework for passing configuration information to hosts. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. You can specify the DHCP options to forward by entering the option number, its value and type and then clicking Add. For a complete list of DHCP options, see the "RFC2132 - DHCP Options and BOOTP Vendor Extensions" article available on the Internet. To delete an option, select the check box next to the option number then click the Delete button.
DHCP options	By default, the client's hostname is sent by Connect Secure to the DHCP server in the DHCP hostname option (option12.) Passing the useruid in the DHCP hostname option is no longer supported. As an alternative, you can configure the following entry in the DHCP options table. For example: option number=12, option value=<username><authMethod>, option type=String Or you can pass a value by adding an entry in the DHCP options table for hostname with whatever value you want. For example: option number=12, option value=foo, option type=String

Setting	Guidelines
IPv4 address pool	Specify IP addresses or a range of IP addresses for the system to assign to clients that run the VPN tunneling service. Use the canonical format: ip_range. The last component of the IP address is a range delimited by a hyphen (-). No special characters are allowed. The ip_range can be specified as shown in the following list: • a.b.c.d - Specifies a single IP address. • a.b.c.d-e.f.g.h - Specifies all IP addresses from the first address to the last address, inclusive. • a.b.c.d-f.g.h - An abbreviated form that specifies the range a.b.c.d through a.f.g.h • a.b.c.d-g.h - An abbreviated form that specifies the range a.b.c.d through a.b.g.h. • a.b.c.d-h - An abbreviated form that specifies the range a.b.c.d through a.b.c.h. • a.b.c.d/mask - Specifies all addresses in a network. For example, to allocate all addresses in the range 172.20.0.0 through 172.20.3.255, specify 172.20.0.0-3.255. Or, to allocate all addresses in a class C network, specify 10.20.30.0/24. **Note:** Be sure to specify a sufficient number of addresses in the IP address pool for all of the endpoints in your deployment. When all of the addresses in the pool have been assigned to endpoints, additional endpoints are unable to obtain a virtual IP address and are blocked from accessing protected resources. The system logs a message in the Event log when an IP address cannot be assigned to an endpoint. We recommend that you set up your network so that the client-side IP address pool, or the DHCP server specified in the VPN tunneling connection profile, resides on the same subnet as Connect Secure. If your network topology dictates that the system internal IP interface and the IP address pool or DHCP server reside on different subnets, you need to add static routes to your intranet's gateway router(s) to ensure that your Enterprise resources and Connect Secure can see each other on the internal network. If you are running a multi-unit cluster across a LAN, make sure that the IP address pool contains addresses that are valid for each node in the cluster. Then, configure an IP filter for each node to apply to this IP address pool. The system does not support a common IP address pool for VPN tunneling for an Active/Active cluster. In A/A VPN tunneling deployments, we recommend that you split the IP pool into node-specific sub-pools. Furthermore, you are advised to perform static route configuration on the backend router infrastructure in a coordinated fashion, with static routes to each sub-pool pointing to the internal IP address of the hosting cluster node as the next-hop gateway. IP address pool also supports attribute substitution. For example, you can enter a RADIUS role mapping attribute in this field, such as <userAttr.Framed-IP-Address>.
IPv6 address assignment	
Enable IPv6 address assignment to clients	Select this option to enable IPv6 connections. **Note:** IPv6 must be enabled on internal interface for IPv6 addresses to be allocated to clients.
IPv6 address pool	Specify IPv6 address ranges for this profile, one per line. Like the IPv4 address pool, the configuration supports entering ip_range values. We recommend using the IPv6 network prefix / netmask style (such as 2001:DB8::6:0/112).
Connection settings	

Setting	Guidelines
Transport	Select one of the following options for transport, encryption, and compression settings: • **ESP** - Use a UDP encapsulated ESP transfer method to securely transfer data between the client and Connect Secure. ESP uses an LZO compression algorithm. You can use the default settings or configure data transfer parameters by defining the UDP port, ESP-to-SSL fallback time-out value, and ESP encryption key lifetime values. • **SSL** - Use the standard SSL transport method. SSL uses a deflate compression method. In SSL mode, compression is controlled by the Enable GZIP compression option on the System Maintenance Options page. **Note:** To support IPv6 connections, be sure to set MTU greater than 1380. We recommend 1500. If the MTU value on the external interface is lower than 1380 and IPv6 address assignment is enabled, the transport setting for the connection profile is ignored. To avoid IP fragmentation, the session falls back to SSL mode for both IPv6 and IPv4 traffic.
	If you select ESP mode, configure the following transport and compression settings: • **UDP port -** Port through which you intend to direct UDP connection traffic. The default port number is 4500. **Note:** Whether you specify a custom port number or choose to use the default port number (4500), you must also ensure that other devices along the encrypted tunnel allow UDP traffic to pass between Connect Secure and the clients. For example, if you employ an edge router and a firewall between the Internet and your corporate intranet, you must ensure that port 4500 is enabled on both the router and the firewall and that port 4500 is configured to pass UDP traffic. IKEv2 uses port 500 exclusively. Do not configure port 500 in your VPN Tunneling profiles. • **ESP to SSL fallback timeout -** Period of time (in seconds) to fall back to the SSL connection already established following UDP connection failure. The default is 15 seconds. **Note:** A nonconfigurable idle timeout of 60 seconds also affects when fallback occurs. After the tunnel is established through ESP, the client sends keepalives after 60 seconds of inactivity on the ESP channel (the idle timeout). The total time to fallback is therefore the idle timeout (60 seconds) plus the fallback timeout. For example, if ESP to SSL fallback timeout is set to 25 seconds, it takes approximately 60+25 or 85 seconds for the VPN tunneling client to switch. • **Key lifetime (time based)** - Period of time (in minutes) the system continues to employ the same ESP encryption key for this connection profile. Both the local and remote sides of the encrypted transmission tunnel use the same encryption key only for a limited period of time to help prevent unauthorized access. The default is 20 minutes. • **Key lifetime (bytes transferred)** - Maximum amount of data that is transferred on the tunnel for an ESP encryption key. The default is 0 bytes, meaning no limit. **Note:** When either of the key lifetime limits is reached, a new key is exchanged between Connect Secure and the client. The reason for changing keys is to help prevent unauthorized access, however, changing the encryption key too frequently can increase CPU overhead on the system.

Setting	Guidelines
	• **Replay Protection -** Activates replay protection. When enabled, this option protects against hostile "repeat attacks" from the network. When packets arrive from the client, the system checks the IP header information to verify that a packet featuring the same IP header information has not already been received. If one has been received, the packet is rejected. This option is enabled by default. If you activate the Enable TOS Bits Copy option, IP packets with different TOS bits may be reordered when passing through gateway routers on your network. To ensure that any packets received out of order are not automatically dropped when they reach the system, you can disable the Replay Protection option. Note: We recommend that you leave replay protection enabled if you are not expecting more than one source of packets from the client (for example, if only one application is transmitting and receiving traffic over the VPN tunnel). • **Compression -** Use compression for the secure connection. Compression is useful for a slow link but may cause issues in extremely large deployments since extra cycles are spent compressing the data. If you have selected ESP, select one the following encryption settings: • **AES128/MD5 (maximize performance) -** Uses Advanced Encryption Standard (AES) 128-bit encryption on the data channel and the MD5 authentication method for VPN tunneling sessions. • **AES128/SHA1 -** Uses AES 128-bit encryption on the data channel and the SHA1 authentication method during VPN tunneling sessions. • **AES256/MD5** - Uses AES 256-bit encryption on the data channel and the MD5 authentication method for VPN tunneling sessions. • **AES256/SHA1 (maximize security)** - Uses AES 256-bit encryption on the data channel and the SHA1 authentication method during VPN tunneling sessions. • **AES256/SHA256 (maximize security) -** Uses AES 256-bit encryption on the data channel and the SHA2 authentication method during VPN tunneling sessions. This option is limited to PSA hardware. Note: The MD5 authentication algorithm creates digital signatures. The MD5 authentication method translates an input string (like a user's ID or sign-in password, for example) into a fixed, 128-bit fingerprint (also called a "message digest") before it is transmitted to or from the system.
DNS settings	
IVE DNS Settings	In the DNS Settings section, select an option that determines the settings sent to the client: • **IVE DNS Settings -** Send the system DNS settings. • **Manual DNS Settings -** Override standard DNS settings with the settings you provide: - **Primary DNS** - Enter the IP address for the primary DNS. - **Secondary DNS** - Enter the IP address for the secondary DNS. - **DNS Domain(s) -** Enter the DNS domain(s), such as "yourcompany.com, yourcompany.net". - **WINS**-Enter the WINS resolution name or IP address. • **DHCP DNS Settings -** Send to the client the values the DHCP server sends to Connect Secure. There is no fallback to the DNS settings if the DHCP Server does not send any values.

Setting	Guidelines
Auto-allow	Select **Auto-allow IP's in DNS/WINS settings (only for split-tunnel enabled mode)** if you want to create an allow rule for the DNS server. For example, if you have defined policies to allow requests from IP address 10.0.0.0 but your DNS server has an address of 172.125.125.125 the DNS server requests will be dropped. If you select this option, the system creates a rule to allow the DNS requests.
DNS search order	Select the DNS server search order. Applicable only if split tunneling is enabled: • Search client DNS first, then the device • Search the device's DNS servers first, then the client • Search device DNS only. **Note:** DNS search order does not work with iOS clients. The DNS name resolution fields (located on the System > Network > Overview window) must be configured, otherwise all DNS queries will go to the client's DNS server. Pulse Secure client 5.0 and greater supports all DNS search order options. Prior versions of Pulse Secure client support only Search client DNS first, then the device and Search the device's DNS servers first, then the client. For the Search client DNS first, then the device and Search the device's DNS servers first, then the client options, DNS configured on the system are added to the end user's system along with the existing DNS already available on the end user's system. So, either the device DNS servers or client DNS servers get precedence at the end user's systems. When the Search device DNS only option is selected, DNS on the end user's system are replaced with device DNS. This option is recommended to avoid ISP's DNS hijacking. Note that this option is applicable only for Windows platforms; non-Windows clients will use the Search the device's DNS servers first, then the client search order if this option is selected. When using this option, you must ensure that packets to the system DNS are going through the tunnel. To do this, add the required routes to the split tunnel networks policy (Users > Resource Policies > VPN Tunneling > Split-Tunneling Networks), or select the Auto-allow IPs in DNS/WINS settings option. For the Search device DNS only option, the client software (Pulse), removes the DNS information of the available adapters on the client system after the tunnel is created. Once the tunnel is created, the client does not monitor the presence of new adapters and does not monitor if changes are made to the DNS settings of existing adapters. Because of this, the Search device DNS only option may not work properly if any of the following occurs after the tunnel is created: • A new interface appears with a DNS server that does DNS hijacking. • A third-party application adds DNS to the adapters whose DNS was removed by the client as part of the tunnel set up process. • Third-party applications change the TCP/IP option from "Use the following DNS servers" to "Obtain DNS servers automatically" for those adapters whose DNS was removed by the client software as part of the tunnel set up process. • End users enable the interfaces that are in the disabled state during the tunnel set up process. **Note:** On Windows 8, selecting either the first or second radio button sends DNS requests to both the client's and Pulse Secure gateway's DNS at the same time. On Windows 10, selecting the first radio button will have the same effect as the second button.
Proxy Server Settings	
Proxy server settings	Select one of the following options:

Setting	Guidelines
	• **No proxy server -** Specifies that the new profile requires no proxy server. • **Automatic (URL for PAC file on another server) -** Specify the URL of the server on which the PAC file resides, and the frequency (in minutes) with which the client polls the server for an updated version of the PAC file. You can configure VPN tunneling to check for an updated PAC files as often as every 10 minutes. The default (and minimum) update period is 10 minutes. The PAC file should reside on a Web server, not on the local PC. The PAC file update method runs on a 10-minute interval. Specifying a frequency update period that is a multiple of 10 will get an exact result. If you specify the update frequency at a value that is not a multiple of 10, it is rounded up to the next interval. For example, if you specify the update frequency at 15 minutes, the system updates a PAC file every 20 minutes. Note: VPN tunneling limits the size of internal (server side) PAC files. The logical maximum size is 256 KB. The actual maximum size that can be used in your deployment might be smaller, reduced according to the size of other VPN tunneling settings in use, such as the number of split tunnel networks and DNS suffix entries. • **Manual configuration** - Specify the IP address or the hostname of the server and provide the port assignment. • **Preserve client-side proxy settings -** By default, VPN tunneling may change proxy settings when needed. For example, VPN tunneling may temporarily change the proxy settings of the browser so that traffic intended for the VPN session uses the temporary proxy settings. Select the Preserve client-side proxy settings option to prevent the client-side proxy settings from being overridden by VPN tunneling. If you select this option, HTTP and FTP traffic path can change after VPN tunneling establishing the connection. Please analyze the proxy logic and split-tunnel option, and make sure it directs the traffic as intended. • **Disable client-side proxy settings -** Disables the client's proxy settings after the VPN tunnel is established. In the use case where the client proxy configuration (proxy.pac) is hosted on a LAN server and users are outside the office network, proxy.pac is not accessible and users access the Internet directly. However, after a VPN tunnel is established, proxy.pac becomes accessible, and that causes all Internet requests to go through the tunnel to the proxy server. When you select Disable client-side proxy settings, client requests are served through the Pulse server directly. When the tunnel is disconnected, the client proxy settings are restored.
Roles	Specify one of the following options: • **Policy applies to ALL roles** - To apply this policy to all users. • **Policy applies to SELECTED roles** - To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • **Policy applies to all roles OTHER THAN those selected below -** To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

Defining Split Tunneling Network Policies

Use the Split Tunneling Network tab to write a VPN tunneling resource policy that specifies one or more network IP address/netmask combinations for which the system handles traffic passed between the remote client and the corporate intranet. You can also specify traffic that should not pass through the VPN tunnel.

When split-tunneling is used, VPN tunneling modifies routes on clients so that traffic meant for the corporate intranet networks flow through the tunnel and all other traffic goes through the local physical adapter. The system tries to resolve all DNS requests through the physical adapter first and then routes those that fail to the VPN tunneling adapter.

For example:

- If split tunnel is disabled, all split tunnel configuration is ignored, including the exclude route. The default route goes to the tunnel allowing access to the protected network.
- Split tunneling is enabled and the included route contains 10.204.64.0/18 and the exclude traffic contains 10.204.68.0/24. In this scenario, networks from 10.204.64.0/18 to 10.204.127.0/18 will pass through the VPN tunnel with the exception of the 10.204.68.0/24 network, which will not pass through the VPN tunnel.
- If split tunneling is enabled and the include route contains 10.204.64.0/24 (subnet of the excluded route) and the exclude route contains 10.204.64.0/18 (super set of the included route) then the included network's traffic will still be routed through the VPN tunnel.

Note: If split tunneling is enabled and there are no include routes configured to be sent to the client, VPN tunneling adds a default route to send traffic through the tunnel.

In addition to using subnets to define the traffic flow, the split tunneling resource policy supports a dynamic per session resource list based on user attributes. The authentication server can be any type, but must be able to pass user attributes during authentication or authorization. Below is one example scenario. The exact steps depend on your implementation and will vary from this example.

1. A user enters their credentials to initiate a session.
2. Connect Secure contacts the back-end authentication server, for example using a RADIUS Access-Request message.
3. The RADIUS server checks the policies and contacts other back-end resources (if configured) to authenticate the user and to retrieve parameters for the user session.
4. The back-end server manager or policy manager sends the attribute list to the RADIUS server along with a list of hosts and IP subnets. Note that Steps 3 and 4 vary depending on your deployment.
5. The RADIUS server returns the list of internal hosts and subnets to the system as part of the RADIUS Access-Accept message.
6. The system is configured with the split tunneling resource policy for that user session based on the received subnet information from the RADIUS server and returns the policy to the client. The client uses this information to make the local split tunnel decisions.

   To write a split tunneling networks resource policy:

   a. In the admin console, choose **Users > Resource Policies > VPN Tunneling > Split-tunneling Networks**.

   b. On the Connect Split Tunneling page, click **New Policy**.

   c. On the New Policy page, enter:

      - A name to label this policy.

- A description of the policy (optional).

d. In the Resources section, specify:

- One or more network IP address/netmask combinations for which the system handles traffic passed between the remote client and the corporate intranet. You may also use the '/' (slash) notation to specify these networks.
- A user attribute, for example <userAttr.Framed-Route>, to send to the back-end authentication server.
- You can specify both IP address/netmask combinations and user attributes in the Resources section.
- Please note the following:
- If a user attribute is configured in the resource list, it is dynamically resolved from the user session data.
- Invalid entries (including "*") are ignored.
- If a configured user attribute is not resolved at runtime for the resource lists, the device acts as if split tunneling is disabled.
- FQDN (Fully qualified domain name) based split tunneling lets the admin configure split tunneling rules by directly specifying the domain names. This is helpful while configuring rules to ignore or tunnel cloud services. For FQDN resources wild card domains are be allowed.

e. In the Roles section, specify:

- **Policy applies to ALL roles** - To apply this policy to all users.
- **Policy applies to SELECTED roles** - To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
- **Policy applies to all roles OTHER THAN those selected below -** To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

f. In the Action section:

- **Allow access** - Network IP address/netmask combinations specified in the Resources list pass through the VPN tunnel.
- **Exclude access** - Network IP address/netmask combinations specified in the Resources list do not pass through the VPN tunnel.
- **Use Detailed Rules (available after you click 'Save Changes')** - Select this option to define resource policy rules that put additional restrictions on the specified resources.

g. Click **Save Changes.**

h. On the Split Tunneling Policies page, order the policies according to how you want to evaluate them. Keep in mind that once the system matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

VPN Tunneling Resource Policy Configuration Use Case

This topic describes a real-world VPN tunneling application and the steps necessary to configure the appropriate resource policy providing access to remote users on the network.

Large financial institutions (also called Fortune Companies) require a robust client sign-in application like VPN tunneling to help provide remote employees seamless network connection to a large range of enterprise resources at the corporate headquarters. Often, remote users need to be able to access multiple applications on their laptops/client machines beyond simple e-mail or meeting scheduling applications. These remote super users or power users require secure, encrypted access to powerful server applications like Microsoft OutlookTM, OracleTM databases, and the RemedyTM case management system.

For this scenario, let's assume the following:

- There is a small collection of remote users who will all access their financial institution's enterprise resources via the same device.
- All the users have the same user_role_remote role assigned to their user ID
  - Host Checker and Cache Cleaner are configured and verifying the users' machines upon logging into a device and launching their VPN tunneling sessions
  - All users require access to three large servers at the corporate headquarters with the following attributes:
    - outlook.acme.com at IP address 10.2.3.201
    - oracle.financial.acme.com at IP address 10.2.3.202
    - case.remedy.acme.com at IP address 10.2.3.99
  - Because the Company wants to manage their IP address pool very strictly, each device provides IP addresses to remote users (our particular device controls the IP addresses between 10.2.3.128 and 10.2.3.192)
  - The company is interested in the most secure access possible, simultaneously accepting only the least possible amount of client down-time

To configure a VPN tunneling resource policy providing appropriate access to the Fortune Company remote users:

1. Create a new VPN tunneling resource policy where you specify the three servers to which you want to grant remote users access:
   a. In the Resources section, specify the IP address ranges necessary to allow access to the three servers (outlook.acme.com, oracle.financial.acme.com, and case.remedy.acme.com) separated by carriage returns.

      udp://10.2.3.64-127:80,443

      udp://10.2.3.192-255:80,443

Note: Configuring your resource as 10.1.1.1-128:* is not supported. Doing so will result in an error.

   b. In the Roles section, select the **Policy applies** to **SELECTED** roles option and ensure that only the "user_role_remote" role appears in the Selected roles list.
   c. In the Action section, select the **Allow access** option.

2. Create a new VPN tunneling connection profile where you define the transport and encryption method for the data tunnel between the client(s) and system:
   a. In the IP address assignment section, select the I**P address pool** option and enter 10.2.3.128-192 in the associated text field.
   b. In the Connection Settings section, select the **ESP transport** option and the AES/SHA1 encryption option.
   c. In the Roles section, select the **Policy applies** to **SELECTED** roles option and ensure that only the "user_role_remote" role appears in the Selected roles list.

About VPN Tunneling Bandwidth Management Policies

Bandwidth management controls the rate of traffic sent or received on a network interface. Bandwidth management discards excess packets and ensures that a user is allocated a specified amount of bandwidth. Traffic less than or equal to the specified rate is guaranteed to be sent. Traffic exceeding the rate is either dropped or delayed.

The total guaranteed bandwidth and spare bandwidth amounts are tracked and updated as users log in and out. Spare bandwidth is defined as the administrator-configured maximum minus the total guaranteed bandwidth for logged-in users.

Guaranteed bandwidth and maximum bandwidths are defined at the role level. This limit applies to each user in the role and ensures that each user receives at least the guaranteed amount of bandwidth but no more than the configured maximum amount. When users are mapped to multiple roles, the higher limit is used. If you do not define a guaranteed bandwidth to a role, users in that role can still log in, but they are not guaranteed any bandwidth. That is, their guaranteed bandwidth is set to zero.

To ensure the system does not allow more bandwidth than the total available, the ability to start VPN tunnels is restricted. Users can start a VPN tunnel only if the guaranteed bandwidth for their role is available. Once users start a session, they are never dropped due to bandwidth restrictions. A privilege level controls this restriction as shown in Table 5.

Table 5 Privilege Levels and Percent of Maximum Bandwidth

Privilege Level	Percent of Maximum Bandwidth
Low	Limited to 50%
Medium	Limited to 75%
High	Limited to 90%
Maximum	Limited to 100%

For example, users assigned to a low privilege level are able to launch a VPN tunnel if the total current bandwidth usage is less than 50% of the configured Maximum Bandwidth. Users assigned to the maximum privilege level are able to launch a VPN tunnel at any time as long as there is any system bandwidth available.

When a user attempts to launch a VPN connection, the sum of the Guaranteed Minimum Bandwidth of all open VPN connections is divided by the configured Total Bandwidth. If the resulting value is less than the configured privilege level of this user, then the user's VPN connection is established. Otherwise, the connection request is denied. For example, if the user's privilege is 75% and the calculated current consumption is 70%, the user's VPN connection is established. If the calculated current consumption is 80%, the user's connection request is denied and the user receives a 23791 error code.

Note: We recommend that average employees be given Low or Medium privilege levels. Higher privilege employees can be assigned the Maximum privilege level to ensure intranet access as long as there is bandwidth available.

If a user does not have the bandwidth to set up any VPN tunnels, the user can still log in but is restricted in what they can do. For example, they may only be able to access web e-mail, etc.

A guaranteed minimum bandwidth is the bandwidth a user gets once a VPN connection is established. If the remaining VPN bandwidth is smaller than the guaranteed minimum bandwidth, the user's VPN connection request is denied and the user receives an 23791 error code. The Guaranteed Minimum Bandwidth must be smaller than the Maximum Bandwidth.

Maximum bandwidth is the bandwidth a user can use through the VPN connection. This is a limit on how much the user can use if there is bandwidth available. For example, if the user's maximum bandwidth is 100 kbps, the user cannot use more than 100 kbps regardless how much available bandwidth.

Statistics for bandwidth management are recorded in the system snapshots.

Note: Before using VPN tunneling bandwidth management policies, you must specify the maximum bandwidth and VPN maximum bandwidth values for the appliance.

User is Mapped to Multiple Roles

The following decision process is made when a user is mapped to multiple roles:

- Calculate the Bandwidth management policies based on the privilege level defined.
  - The current used bandwidth percentage is calculated and compared with the privilege levels of the Bandwidth management policy of the mapped roles.
  - All bandwidth management polices with the privilege levels that disallow the user to set up VPN tunnels are discarded.
- Compare the matched bandwidth management policies and choose the one with the highest guaranteed minimum bandwidth. If more than one policy with the highest guaranteed minimum bandwidth exists, the policy with the highest maximum bandwidth wins.

For example, a user is mapped to 3 roles and the bandwidth management policy for each role is as follows:

IIf the current total used bandwidth is at 80%:

	Role 1	Role 2	Role 3
Minimum guaranteed bandwidth	100 mbps	200 mbps	100 mbps

	Role 1	Role 2	Role 3
Maximum guaranteed bandwidth	500 mbps	400 mbps	400 mbps
Privilege level	Medium	High	Maximum

- Since role 1's privilege is not enough to allow this user to set up a VPN tunnel, role 1's bandwidth management policy is ignored.
  - Role 2's policy has higher minimum guaranteed bandwidth than role 3 so role 2 wins. The user receives a 200 mbps minimum guaranteed bandwidth and 400 mpbs maximum guaranteed bandwidth.

However, if the current total used bandwidth is 92%, only role 3's privilege allows the user to set up NC tunnel, so role 3's bandwidth management policy is used. Thus the user has a 100 mbps minimum guaranteed bandwidth and 400 mbps maximum guaranteed bandwidth.

Writing a VPN Tunneling Bandwidth Management Resource Policy

To write a VPN tunneling bandwidth management resource policy:

1. In the admin console, choose **Users > Resource Policies > VPN Tunneling > Bandwidth Manage**ment.
2. On the Bandwidth Management page, click **New Policy.**
3. On the New Policy page, enter:
   - A name to label this policy.
   - A description of the policy (optional).
4. In the Bandwidth Management Settings section, specify:

- **Admission Privilege Level -** Select the percentage of the maximum bandwidth that allows users to start a VPN session. Only when the bandwidth is below this percentage can users log in.
- **Guaranteed Minimum Bandwidth** - Specify the user's minimum bandwidth once they start a VPN session.
- **Maximum Bandwidth** - Specify the user's maximum bandwidth once they start a VPN session.

Note: The maximum bandwidth must be less than or equal to the maximum rated value for the appliance.

5. In the Roles section, specify:
   - **Policy applies to ALL roles -** To apply this policy to all users.
   - **Policy applies to SELECTED roles** - To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
   - **Policy applies to all roles OTHER THAN those selected below -** To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

6. Click **Save Changes.**

Configuring the VPN Tunnel Server

You use the System > Network > VPN tunneling page to configure VPN tunnel server options. This topic includes the following information:

- "Specifying IP Filters" on page 42
- "Specifying the VPN Tunneling Server Base IP Address" on page 42

Specifying IP Filters

The VPN Tunneling Server uses the filter list to assign IP addresses to clients requesting a VPN client session. A filter is an IP address/netmask combination. For example: 10.11.0.0/255.255.0.0 or 10.11.0.0/16.

To add an IP address to the VPN tunneling filter list:

1. In the admin console, choose **System > Network > VPN tunneling**.
2. Specify an IP address/netmask combination and then click **Add**.

Specifying the VPN Tunneling Server Base IP Address

Note: Only change the VPN tunneling server base IP address when instructed to do so by the Pulse Secure Support team.

To change the VPN tunneling server base IP address:

1. In the admin console, choose **System > Network > VPN tunneling**.
2. In the **VPN Tunnel Server IP Address** text box, specify the base IP address used by the VPN tunneling server to assign IP addresses to the tunnel interfaces created for VPN Tunneling sessions. If your service is deployed in a cluster, the base IP address you specify will be common to all cluster nodes. Be sure to configure a base IP address that does not encroach on the IP address pool for VPN Tunneling Connection Profiles or for or the IP addresses for the external or internal interface. Take DHCP servers into consideration.

For IPv6 addresses, no additional configuration is required. The base IPv6 address used by the VPN tunneling server will be generated by prepending the network prefix fd00:: to IPv4 address configured for this.

3. Save the configuration.

VPN Tunneling Installer Overview

To download the VPN tunneling application as a Windows executable file, go to Maintenance > System > Installers.

VPN tunneling Installation Process Dependencies

During installation, VPN tunneling interacts with a number of system components, performing checks and validations along the way. The following list provides the order of execution during installation, which may be helpful if you need to debug a VPN tunneling installation process.

1. Start Pre-Installation Process:
2. Parse command line arguments.
3. Set appropriate variables via command line.
4. Process commands, as necessary.
5. If the command line entry responds with help or version information, the VPN tunneling installation program quits, following the command line processing. Typically occurs when you run the VPN tunneling installer as a standalone installer.
6. Validate System:
   - Check OS. If VPN Tunneling does not support this OS version, display error and abort validation process.
   - Check Administrator privileges.
   - 3rd-party GINA component - if GINA is to be registered, check whether there is any existing registered GINA component. If yes, abort installation.
7. If there is an existing VPN tunneling installation, trigger the uninstall in upgrade mode of the existing VPN tunneling.
8. Wait until the existing VPN tunneling uninstallation process completes (in upgrade mode).
9. If the uninstallation process times-out, display error message and abort the VPN tunneling installation, otherwise, continue the VPN tunneling installation.
10. Write logging registry keys for VPN tunneling components.
11. Start VPN tunneling installation.
12. Shared component installation:
    a. Check sharedDll registry value of the shared components to see if this is the first instance of shared component installation.
    b. Check if Neo_CleanInst flag is set.
    c. If steps a or b are true, ensure the sharedDll registry value is clean.
    d. Stop service if still running.
    e. Check installation and driver
       - If driver is installed and it is a clean installation, uninstall the driver.
       - If driver is installed and it is not a clean installation, compare driver versions.
       - If it is an upgrade, set the driver install flag, otherwise, do not install the driver (keep the current higher version driver).

13. VPN tunneling component installation:
    a. If the driver install flag is set or if it is a clean install, install the driver.
    b. Call the shared component installation macro for the VPN tunneling service and GINA component. This macro performs a version comparison, ensures a proper upgrade, and increments the sharedDll registry key value.
    c. Copy other VPN tunneling binary files.
    d. Call the NCCopyFile macro for the files that might be locked by msGINA. This macro takes care of renaming old files and mark them delete on reboot.
    e. Register GINA if GINA flag is set.
    f. Save locale and GINA settings in user's config.ini file.
    g. Start the NCService.
    h. Create program shortcut.
    i. Create Uninstall registry keys.
    j. Start VPN tunneling user interface.
    k. End VPN tunneling installation process.
14. Start Post-Installation Process:
    a. Print product version and append the install log to admin log file
    b. Reboot, if the reboot flag was set.

VPN Tunneling Uninstallation Process Dependencies

During uninstallation, VPN tunneling interacts with a number of system components, performing checks and validations along the way. The following list provides the order of execution during uninstallation, which may be helpful if you need to debug a VPN tunneling uninstallation process.

1. Start Pre-Uninstall Process:
    - Parse command line inputs, including:
        - Locale
        - Clean uninstall flag
        - Upgrade flag
2. Start uninstall operation.
3. Check Administrator privileges.
4. Unregister GINA if already registered.
5. If uninstalling in upgrade mode, stop the VPN tunneling service.
6. If the uninstallation is not in upgrade mode, check the current sharedDll registry key value. If the value is 1, this is the only instance using the shared components, so:

a. Uninstall the driver.

b. Delete the driver file.

c. Stop and unregister the VPN tunneling service.

7. Call the shared components macro to uninstall shared components. This macro decrements the SharedDLL registry key value and removes the source file.

Note: If the uninstall process is in upgrade mode, this step is not executed because the uninstall is triggered from a VPN tunneling installation process and the shared component macro in the installation process will handle the shared component upgrade operations.

8. Delete other VPN tunneling files, including:
   - dsNcAdmin.dll
   - dsNcDiag.dll
   - versioninfo.ini
9. Call the NCDeleteFile macro to delete the files that may be locked by msGINA.
10. Delete VPN tunneling registry keys.
11. Remove VPN tunneling program file directories.
12. End the uninstall process.
13. Print the product version and append the VPN tunneling installation log to the Admin log.
14. Reboot, if the reboot flag was set.