Remote Access VPN

Remote Access virtual private network (VPN) allows individual users to connect to your network from a remote location using a computer or other supported iOS or Android device connected to the Internet. This allows mobile workers to connect from their home networks or a public Wi-Fi network, for example.

The following topics explain how to configure remote access VPN for your network.

Remote Access VPN Overview

You can use the FDM to configure remote access VPN over SSL using the AnyConnect Client sofware.

When the AnyConnect Client negotiates an SSL VPN connection with the FTD device, it connects using Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. The client and the FTD device negotiate the TLS/DTLS version to use. DTLS is used if the client supports it.

Maximum Concurrent VPN Sessions By Device Model

There is a maximum limit to the number of concurrent remote access VPN sessions allowed on a device based on the device model. This limit is designed so that system performance does not degrade to unacceptable levels. Use these limits for capacity planning.

Device Model	Maximum Concurrent Remote Access VPN Sessions
ASA 5508-X	100
ASA 5515-X	250
ASA 5516-X	300

Device Model	Maximum Concurrent Remote Access VPN Sessions
ASA 5525-X	750
ASA 5545-X	2500
ASA 5555-X	5000
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
FTDv:	250
ISA 3000	25

Downloading the AnyConnect Client Software

Before you can configure a remote access VPN, you must download the AnyConnect Client software to your workstation. You will need to upload these packages when defining the VPN.

You should download the latest AnyConnect Client version, to ensure that you have the latest features, bug fixes, and security patches. Regularly update the packages on the FTD device.

Note You can upload one AnyConnect Client package per operating system: Windows, Mac, and Linux. You cannot upload multiple versions for a given OS type.

Obtain the AnyConnect Client software packages from software.cisco.com. You need to download the "Full Installation Package" versions of the clients.

How Users Can Install the AnyConnect Client Software

To complete a VPN connection, your users must install the AnyConnect Client software. You can use your existing software distribution methods to install the software directly. Or, you can have users install the AnyConnect Client directly from the FTD device.

Users must have Administrator rights on their workstations to install the software.

Once the AnyConnect Client is installed, if you upload new AnyConnect Client versions to the system, the AnyConnect Client will detect the new version on the next VPN connection the user makes. The system will automatically prompt the user to download and install the updated client software. This automation simplifies software distribution for you and your clients.

If you decide to have users initially install the software from the FTD device, tell users to perform the following steps.

Note Android and iOS users should download the AnyConnect Client from the appropriate App Store.

Procedure

Step 1 Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections.

You identify this interface when you configure the remote access VPN. The system prompts the user to log in.

Step 2 Log into the site.

Users are authenticated using the directory server configured for the remote access VPN. Log in must be successful to continue.

If log in is successful, the system determines if the user already has the required version of the AnyConnect Client. If the AnyConnect Client is absent from the user's computer, or is down-level, the system automatically starts installing the AnyConnect Client software.

When installation is finished, AnyConnect Client completes the remote access VPN connection.

Licensing Requirements for Remote Access VPN

Your base device license must meet export requirements before you can configure remote access VPN. When you register the device, you must do so with a Smart Software Manager account that is enabled for export-controlled features. You also cannot configure the feature using the evaluation license.

In addition, you need to purchase and enable a remote access VPN license, any of the following: AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only. These licenses are treated the same for FTD devices, even though they are designed to allow different feature sets when used with ASA Software-based headends.

To enable the license, select **Device** > **Smart License** > **View Configuration**, then select the appropriate license in the RA VPN License group. You need to have the license available in your Smart Software Manager account. For more information about enabling licenses, see Enabling or Disabling Optional Licenses.

For more information, see the *Cisco AnyConnect Ordering Guide*, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf. There are also other data sheets available on http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html.

Guidelines and Limitations for Remote Access VPN

Please keep the following guidelines and limitations in mind when configuring RA VPN.

- You cannot configure both the FDM access (HTTPS access in the management access list) and remote access SSL VPN on the same interface for the same TCP port. For example, if you configure remote access SSL VPN on the outside interface, you cannot also open the outside interface for HTTPS

connections on port 443. Because you cannot configure the port used by these features in FDM, you cannot configure both features on the same interface.

- The RA VPN outside interface is a global setting. You cannot configure separate connection profiles on different interfaces.
- You cannot use overlapping addresses in the source address of a NAT rule and a remote access VPN address pool.
- (REST API configuration only.) If you configure two-factor authentication using RADIUS and RSA tokens, the default authentication timeout of 12 seconds is too quick to allow successful authentication in most cases. You can increase the authentication timeout value by creating a custom AnyConnect Client profile and applying it to the RA VPN connection profile, as described in Configure and Upload Client Profiles, on page 5. We recommend an authentication timeout of at least 60 seconds, so that users have enough time to authenticate and then paste the RSA token, and for the round-trip verification of the token.

Configuring Remote Access VPN

To enable remote access VPN for your clients, you need to configure a number of separate items. The following procedure provides the end to end process.

Procedure

Step 1 Configure licenses.

You need to enable two licenses:

- When you register the device, you must do so with a Smart Software Manager account that is enabled for export-controlled features. The base license must meet export control requirements before you can configure remote access VPN. You also cannot configure the feature using the evaluation license. For the procedure to register the device, see Registering the Device.
- A remote access VPN license. For details, see Licensing Requirements for Remote Access VPN, on page 3. To enable the license, see Enabling or Disabling Optional Licenses.

Step 2 Configure Certificates.

Certificates are required to authenticate SSL connections between the clients and the device. You can use the pre-defined DefaultInternalCertificate for the VPN, or create your own.

If you use an encrypted connection for the directory realm used for authentication, you must upload a trusted CA certificate.

For more information on certificates and how to upload them, see Configuring Certificates.

Step 3 (Optional.) Configure and Upload Client Profiles, on page 5.

Step 4 Configure the identity source used for authenticating remote users.

You can use the following sources for user accounts that are allowed to log into the remote access VPN.

- Active Directory identity realm—As a primary authentication source. The user accounts are defined in your Active Directory (AD) server. See Configuring AD Identity Realms.

- LocalIdentitySource (the local user database)—As a primary or fallback source. You can define users directly on the device and not use an external server. If you use the local database as a fallback source, ensure that you define the same usernames/passwords as the ones defined in the external server. See Configure Local Users.

Step 5 Configure a Remote Access VPN Connection, on page 6.

Step 6 Allow Traffic Through the Remote Access VPN, on page 9.

Step 7 (Optional.) Control Access to Resources by Remote Access VPN Group, on page 10.

If you do not want all of your remote access users to have the same access to all internal resources, you can apply access control rules to allow or prevent access based on user group membership.

Step 8 Verify the Remote Access VPN Configuration, on page 11.

If you encounter problems completing a connection, see Troubleshooting Remote Access VPNs, on page 13.

Step 9 (Optional.) Enable the identity policy and configure a rule for passive authentication.

If you enable passive user authentication, users who logged in through the remote access VPN will be shown in the dashboards, and they will also be available as traffic-matching criteria in policies. If you do not enable passive authentication, RA VPN users will be available only if they match an active authentication policy. You must enable the identity policy to get any username information in the dashboards or for traffic matching.

Configure and Upload Client Profiles

AnyConnect Client profiles are downloaded to clients along with the AnyConnect Client software. These profiles define many client-related options, such as auto connect on startup and auto reconnect, and whether the end user is allowed to change the option from the AnyConnect Client preferences and advanced settings.

If you configure a fully-qualified hostname (FQDN) for the outside interface when configuring the remote access VPN connection, the system creates a client profile for you. This profile enables the default settings. You need to create and upload client profiles only if you want non-default behavior. Note that client profiles are optional: if you do not upload one, AnyConnect Client will use default settings for all profile-controlled options.

Note You must include the FTD device's outside interface in the VPN profile's server list in order for the AnyConnect Client to display all user controllable settings on the first connection. If you do not add the address or FQDN as a host entry in the profile, then filters do not apply for the session. For example, if you create a certificate match and the certificate properly matches the criteria, but you do not add the device as a host entry in that profile, the certificate match is ignored.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create AnyConnect Client profile objects while editing a profile property by clicking the **Create New AnyConnect Client Profile** link shown in the object list.

Before you begin

Before you can upload client profiles, you must do the following.

- Download and install the stand-alone AnyConnect Client "Profile Editor - Windows / Standalone installer (MSI)." The installation file is for Windows only, and has the file name anyconnect-profileeditor-win-<version>-k9.msi, where <version> is the AnyConnect Client version (the file name is subject to change). For example, anyconnect-profileeditor-win-4.3.04027-k9.msi. You must also install Java JRE 1.6 (or higher) before installing the profile editor. Obtain the AnyConnect Client profile editor from software.cisco.com. Note that this package contains all of the profile editors, not just the one for the VPN client.
- Use the profile editor to create the profiles you need. You should specify the hostname or IP address of the outside interface in the profile. For detailed information, see the editor's online help.

Procedure

Step 1 Select **Objects**, then select **AnyConnect Client Profiles** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To edit an object, click the edit icon ( ) for the object.
- To download the profile associated with an object, click the download icon ( ) for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Enter a name and optionally, a description, for the object.

Step 4 Click **Upload** and select the file you created using the Profile Editor.

Step 5 Click **Open** to upload the profile.

Step 6 Click **OK** to add the object.

Configure a Remote Access VPN Connection

You can create a remote access VPN connection to allow your users to connect to your inside networks when they are on external networks, such as their home network.

Before you begin

Before configuring the remote access (RA) VPN connection:

- Download the required AnyConnect software packages from software.cisco.com to your workstation.
- Optionally, use the AnyConnect Profile Editor to create a client profile. The system will create a default profile for you if you specify a fully-qualified domain name for the outside interface. Client profiles are optional, create one only if you want to customize features controlled by the profile.
- The outside interface, the one that terminates remote access VPN connections, cannot also have a management access list that allows HTTPS connections. Delete any HTTPS rules from the outside interface before configuring RA VPN. See Configuring the Management Access List.

Procedure

Step 1 Click **Device**, then click **Setup Connection Profile** in the Remote Access VPN group.

You can configure one remote access VPN. If you have already configured it, clicking **View Configuration** opens your existing VPN; click the **Edit** button to make changes..

If you want to delete the configuration, click **Clear Configuration**.

Step 2 Define the AnyConnect client configuration.

- **Connection Profile Name**—The name for this connection, up to 50 characters without spaces. For example, MainOffice. You cannot use an IP address as the name.

  Note The name you enter here is what users will see in the connection list in the AnyConnect client. Choose a name that will make sense to your users.

- **Identity Source for User Authentication**—The primary identity source used for authenticating remote users. End users must be defined in this source or the optional fallback source to complete a VPN connection. Select one of the following:
  - An Active Directory (AD) identity realm.
  - LocalIdentitySource (the local user database)—You can define users directly on the device and not use an external server.

- **Fallback Local Identity Source**—If the primary source is an external server, you can select the LocalIdentitySource as a fallback in case the primary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the external server.

- **AnyConnect Packages**—The AnyConnect full installation software images that you will support on this VPN connection. For each package, the filename, including extensions, can be no more than 60 characters. You can upload separate packages for Windows, Mac, and Linux endpoints.

  Download the packages from software.cisco.com. If the endpoint does not already have the right package installed, the system prompts the user to download and install the package after the user authenticates.

Step 3 Click **Next**.

Step 4 Define the device identity and client addressing configuration.

- **Certificate of Device Identity**—Select the internal certificate used to establish the identity of the device. Clients must accept this certificate to complete a secure VPN connection. If you do not already have a certificate, click **Create New Internal Certificate** in the drop-down list. You must configure a certificate.

- **Outside Interface**—The interface to which users connect when making the remote access VPN connection. Although this is normally the outside (Internet-facing) interface, choose whichever interface is between the device and the end users you are supporting with this connection profile.

- **Fully-qualified Domain Name for the Outside Interface**—The name of the interface, for example, ravpn.example.com. If you specify a name, the system can create a client profile for you.

  Note You are responsible for ensuring that the DNS servers used in the VPN and by clients can resolve this name to the outside interface's IP address. Add the FQDN to the relevant DNS servers.

- **IPv4, IPv6 Address Pools**—These options define the address pools for the remote endpoints. Clients are assigned an address from these pools based on the IP version they use to make the VPN connection. Select a network object that defines a subnet for each IP type you want to support. Select **None** (or leave blank) if you do not want to support that IP version. For example, you could define an IPv4 pool as 10.100.10.0/24. The address pool cannot be on the same subnet as the IP address for the outside interface.
- **Primary, Secondary DNS Servers**—The DNS servers clients should use for domain name resolution when connected to the VPN. Click the **OpenDNS** button to load these fields with the OpenDNS public DNS servers. Otherwise, enter the IP addresses of your DNS servers.
- **Domain Search Name**—Enter the domain name for your network, e.g. example.com. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.

Step 5 Click **Next**.

Step 6 Define the connection settings to customize AnyConnect client behavior.

- **Banner Text for Authenticated Clients**—(Optional.) Enter any message you want to show to users at the beginning of their VPN session. For example, legal disclaimers and warnings about appropriate use. The banner can be up to 500 characters, but cannot contain semi-colons (;) or HTML tags.
- **Maximum Connection Time**—The maximum length of time, in minutes, that users are allowed to stay connected to the VPN without logging out and reconnecting, from 1- 4473924 or blank. The default is unlimited (blank), but the idle timeout still applies.
- **Idle Timeout**—The length of time, in minutes, that the VPN connection can be idle before it is automatically closed, from 1-35791394. The default is 30 minutes.
- **Browser Proxy During VPN Sessions**—Whether proxies are used during a VPN session for Internet Explorer web browsers on Windows client devices. Select from the following options:
  - **No change in endpoint settings**—Allow the user to configure (or not configure) a browser proxy, and use the proxy if it is configured.
  - **Disable browser proxy**—Do not use the proxy defined for the browser, if any. No browser connections will go through the proxy.
  - **Auto detect settings**—Enables the use of automatic proxy server detection in the browser.
  - **Use custom settings**—Configures a proxy for the client browser. Enter the IP address and optionally, port, for the HTTP proxy server (the host and port combined cannot exceed 100 characters). You can also click **Add Proxy Exception** if you want to exempt requests to specific web servers from going through the proxy (specifying the port in the exception list is optional). The entire proxy exception list, combining all addresses and ports, cannot be longer than 255 characters.
- **Split Tunneling**—Enable split-tunneling to allow users access to their local networks or the Internet directly at the same time they are using a secure VPN tunnel. Keep split-tunneling disabled for a more secure VPN connection. If you enable split tunneling, you must also select the network objects that represent internal networks remote users will be accessing in the **Inside Networks** list. The networks list must contain the same IP types as the address pools you are supporting. For any networks outside the ones specified, the user's ISP gateway is used for transmitting traffic.
- **NAT Exempt**—Enable NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. If you do not exempt VPN traffic from NAT, ensure that the existing NAT rules for the outside and inside interfaces do not apply to the RA VPN pool of addresses. NAT exempt rules are manual static identity NAT rules for a given source/destination interface and network combination,

but they are not reflected in the NAT policy, they are hidden. If you enable NAT Exempt, you must also configure the following.

- **Inside Interfaces**—Select the interfaces for the internal networks remote users will be accessing. NAT rules are created for these interfaces.
- **Inside Networks**—Select the network objects that represent internal networks remote users will be accessing. The networks list must contain the same IP types as the address pools you are supporting.

- **AnyConnect Client Profiles**—(Optional.) If you configure a fully-qualified domain name for the outside interface, a default profile will be created for you. Alternatively, you can upload your own client profile. Create these profiles using the standalone AnyConnect Profile Editor, which you can download and install from software.cisco.com. If you do not select a client profile, the AnyConnect client uses default values for all options. The items in this list are AnyConnect Client Profile objects rather than the profiles themselves. You can create (and upload) new profiles by clicking **Create New AnyConnect Client Profile** in the drop-down list.

Step 7 Click **Next**.

Step 8 Review the summary.

First, verify that the summary is correct.

Then, click **Instructions** to see what end users need to do to initially install the AnyConnect software and test that they can complete a VPN connection. Click **Copy** to copy these instructions to the clipboard, and then distribute them to your users.

Step 9 Click **Finish**.

What to do next

Ensure that traffic is allowed in the VPN tunnel, as explained in Allow Traffic Through the Remote Access VPN, on page 9.

By default, VPN-terminated traffic bypasses the access control policy, including any advanced inspections defined in that policy, such as URL filtering, intrusion protection, or file policies. If you want VPN traffic to be evaluated and inspected by the access control policy, use FlexConfig to configure the **no sysopt connection permit-vpn** command. You can then configure access control rules to allow traffic between the address pool and the inside networks from the outside to inside interfaces. The system decrypts the VPN traffic before evaluating it with the access control policy, so you can apply intrusion prevention, URL filtering, and so forth.

Allow Traffic Through the Remote Access VPN

Creating the remote access VPN connection is not enough to enable the system to send traffic through the VPN tunnel. You must also configure one of the following:

- Configure the **sysopt connection permit-vpn** command, which exempts traffic that matches the VPN connection from the access control policy. The default for this command is **no sysopt connection permit-vpn**, which means VPN traffic must also be allowed by the access control policy.

  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will

not be applied to the traffic. This also means that no connection events will be generated for the traffic, and thus statistical dashboards will not reflect VPN connections.

Use FlexConfig to configure this command.

- Create access control rules to allow connections from the remote access VPN address pool. This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

  You must use this option if you want to control access based on user group, as described in Control Access to Resources by Remote Access VPN Group, on page 10.

Control Access to Resources by Remote Access VPN Group

If you are familiar with configuring remote access VPN on an ASA, or on the FTD device using the FMC, then you might be used to controlling access to various resources in your network based on remote access VPN groups.

With the FDM, you can configure a single connection profile with a single group policy. However, you can still control access based on user groups by implementing identity policies and user-group-based access control.

The following procedure explains the configuration.

Before you begin

This procedure assumes that you have already configured remote access VPN and the required identity realm. However, you can configure the identity and access control policies first, and then configure RA VPN.

This configuration requires that VPN traffic be subject to the access control policy. In the CLI, use the **show running-config** command to check that the **no sysopt connection permit-vpn** command appears. If it is not in the running configuration, use FlexConfig to configure the command.

Procedure

Step 1 Configure the required user groups in the directory server.

The directory server must have user groups, and those groups must contain the right users, based on the policies you want to deploy. For example, if you want to differentiate between Engineering and Marketing users, and allow group members access to different resources, you must have groups for those users defined in the directory server.

You cannot create user groups directly on the FTD device.

See the documentation for the directory server for information on creating user groups.

Step 2 Choose **Policies** > **Identity**, enable the identity policy, and create a rule to enforce passive authentication for RA VPN users.

The passive authentication rule uses the same realm as the RA VPN connection. At minimum, you must have an identity policy that requires passive authentication for the IP addresses in the RA VPN address pool for the zone that contains the RA VPN outside interface.

If you have a blanket identity policy that requires passive authentication for all addresses and all zones, you do not need any additional rules.

For the information on enabling the policy and creating rules, see Configuring Identity Policies.

You must configure the identity rule because only names collected through identity policy authentication are available for user-based access control policies. Usernames obtained from RA VPN connections only, without an associated identity rule, cannot be used by access control policies. Note that active authentication rules that cover RA VPN users are also sufficient for gathering the required user identity information.

Step 3 Click the **Deploy** button in the menu, then click the **Deploy Now** button, to deploy your changes.

The system needs to establish a connection to the directory server and download users and user groups. Deploying the configuration starts off this user/group download. If you do not deploy, then users and groups will not be selectable in access control rules.

Step 4 Choose **Policies** > **Access Control**, and create group-based access control rules.

You can now create access control rules to differentiate between the directory realm groups for RA VPN users. You can create very general rules, or specifically-targeted rules. For information on creating access control rules, see Configuring Access Control Rules.

For example, rules targeted to specific RA VPN user groups might use the following criteria, based on the tabs in the Add/Edit Access Rule dialog box:

- **Source/Destination**, **Zones**—The **Source** zone should include the RA VPN outside interface. The **Destination** zone can include any relevant inside interfaces.
- **Source/Destination**, **Networks** and **Ports**—Select the RA VPN address pool network object as the **Source** network, and the network (and optionally port) objects that define the controlled resources as the **Destination** network/port. Instead of selecting a destination network/port, you can use the **Application** or **URL** tabs to define the destination resource if that is more appropriate for your requirements.
- **Users**—Select the specific directory groups on this tab. This is the criterion that provides group-based access control.
- **Applications**, **URLs**—You can use these criteria in addition to, or instead of, the destination network/ports criteria on the **Source/Destination** tab. For example, you can select a network object to limit the rule to a specific subnet, and then select applications to control access to those applications on the targeted network.
- **Intrusion Policy**, **File Policy**—Select the options that fit your requirements. These options control threats, they do not control access to specific resources.
- **Logging**—Select the option that fits your requirements. You must enable logging to see any results in the monitoring dashboards or connection events in Event Viewer.

Verify the Remote Access VPN Configuration

After you configure the remote access VPN, and deploy the configuration to the device, verify that you can make remote connections.

If you encounter problems, read through the troubleshooting topics to help isolate and correct the problems. See Troubleshooting Remote Access VPNs, on page 13.

Procedure

Step 1 From an external network, establish a VPN connection using the AnyConnect Client.

Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. If necessary, install the client software and complete the connection. See How Users Can Install the AnyConnect Client Software, on page 2.

Step 2 Log into the device CLI as explained in Logging Into the Command Line Interface (CLI). Alternatively, open the CLI Console.

Step 3 Use the **show vpn-sessiondb** command to view summary information about current VPN sessions.

The statistics should show your active AnyConnect Client session, and information on cumulative sessions, the peak concurrent number of sessions, and inactive sessions. Following is sample output from the command.

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     50
Device Total VPN Capacity   :  10000
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ----------------------------------------
Clientless                  :      0 :          1 :               1
AnyConnect-Parent           :      1 :         49 :               3
SSL-Tunnel                  :      1 :         46 :               3
DTLS-Tunnel                 :      1 :         46 :               3
--------------------------------------------------------------------------------
Totals                      :      3 :        142
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ----------------------------------------
AnyConnect SSL/TLS/DTLS     :        :            :
  Tunneled IPv6             :      1 :         20 :           2
--------------------------------------------------------------------------------
```

Step 4 Use the **show vpn-sessiondb anyconnect** command to view detailed information about current VPN sessions.

Detailed information includes encryption used, bytes transmitted and received, and other statistics. If you use your VPN connection, you should see the bytes transmitted/received numbers change as you re-issue this command.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone  : 0
```

Monitoring Remote Access VPN

To monitor and troubleshoot remote access VPN connections, open the CLI console or log into the device CLI and use the following commands.

- **show vpn-sessiondb** displays information about VPN sessions. You can reset these statistics using the **clear vpn-sessiondb** command.
- **show webvpn** *keyword* displays information about the remote access VPN configuration, including statistics and the AnyConnect images installed. Enter **show webvpn ?** to see the available keywords.
- **show aaa-server** displays statistics about the directory server used with remote access VPN.

Troubleshooting Remote Access VPNs

Remote access VPN connection issues can originate in the client or in the FTD device configuration. The following topics cover the main troubleshooting problems you might encounter.

Troubleshooting SSL Connection Problems

If the user cannot make the initial, non-AnyConnect Client, SSL connection to the outside IP address to download the AnyConnect Client, do the following:

1. From the client workstation, verify that you can ping the IP address of the outside interface. If you cannot, determine why there is no route from the user's workstation to the address.

2. From the client workstation, verify that you can ping the fully-qualified domain name (FQDN) of the outside interface, the one defined in the remote access (RA) VPN connection profile. If you can ping the IP address but not the FQDN, then you need to update the DNS servers used by the client and RA VPN connection profile to add the FQDN-to-IP-address mapping.
3. Verify that the user is accepting the certificate presented by the outside interface. The user should accept it permanently.
4. Examine the RA VPN connection configuration and verify that you selected the correct outside interface. A common mistake is to select an inside interface, the one facing the internal networks, rather than the outside interface, which faces the RA VPN users.
5. If SSL encryption is properly configured, use an external sniffer to verify whether the TCP three-way handshake is successful.

Troubleshooting AnyConnect Client Download and Installation Problems

If the user can make an SSL connection to the outside interface, but cannot download and install the AnyConnect Client package, consider the following:

- Ensure that you uploaded an AnyConnect Client package for the client's operating system. For example, if the user's workstation runs Linux, but you did not upload a Linux AnyConnect Client image, there is no package that can be installed.
- For Windows clients, the user must have Administrator rights to install software.
- For Windows clients, the workstation must enable ActiveX or install Java JRE 1.5 or higher, with JRE 7 recommended.
- For Safari browsers, Java must be enabled.
- Try different browsers, one might fail where another succeeds.

Troubleshooting AnyConnect Client Connection Problems

If the user was able to connect to the outside interface, download, and install the AnyConnect Client, but could not then complete a connection using AnyConnect Client, consider the following:

- If authentication fails, verify that the user is entering the correct username and password, and that the username is defined correctly in the authentication server. The authentication server must also be available through one of the data interfaces.

Note If the authentication server is on an external network, you need to configure a site-to-site VPN connection to the external network, and include the remote access VPN interface address within the VPN. For details, see How to Use a Directory Server on an Outside Network with Remote Access VPN, on page 22.

- If you configured a fully-qualified domain name (FQDN) for the outside interface in the remote access (RA) VPN connection profile, verify that you can ping the FQDN from the client device. If you can ping the IP address but not the FQDN, then you need to update the DNS servers used by the client and RA

VPN connection profile to add the FQDN-to-IP-address mapping. If you are using the default AnyConnect Client profile that is generated when you specify an FQDN for the outside interface, the user will need to edit the server address to use the IP address until DNS is updated.

- Verify that the user is accepting the certificate presented by the outside interface. The user should accept it permanently.
- If the user's AnyConnect Client includes multiple connection profiles, that they are selecting the right one.
- If everything seems right on the client end, make an SSH connection to the FTD device, and enter the **debug webvpn** command. Examine the messages issued during a connection attempt.

Troubleshooting RA VPN Traffic Flow Problems

If the user can make a secure remote access (RA) VPN connection, but cannot send and receive traffic, do the following:

1. Have the client disconnect, then reconnect. Sometimes this eliminates the problem.
2. In the AnyConnect Client, check the traffic statistics to determine whether both the sent and received counters are increasing. If the received packet count stays at zero, the FTD device is not returning any traffic. There is likely a problem in the FTD configuration. Common problems include the following:
   - Access rules are blocking traffic. Check the access control policy for rules that prevent traffic between the inside networks and the RA VPN address pool. You might need to create an explicit Allow rule if your default action is to block traffic.
   - NAT rules are not being bypassed for the RA VPN traffic. Ensure that NAT exempt is configured for the RA VPN connection for every inside interface. Alternatively, ensure that the NAT rules do not prevent communication between the inside networks and interfaces and the RA VPN address pool and outside interface.
   - Routes are misconfigured. Ensure that all defined routes are valid and functioning correctly. For example, if you have a static IP address defined for the outside interface, ensure that the routing table includes a default route (for 0.0.0.0/0 and ::/0).
   - Ensure that the DNS server and domain name configured for the RA VPN are correct, and that the client system is using the correct ones. Verify that the DNS servers are reachable.
   - If you enable split tunneling in the RA VPN, check whether traffic to the specified inside networks is going through the tunnel, while all other traffic is bypassing the tunnel (so that the FTD device does not see it).
3. Make an SSH connection to the FTD device and verify that traffic is being sent and received for the remote access VPN. Use the following commands.
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

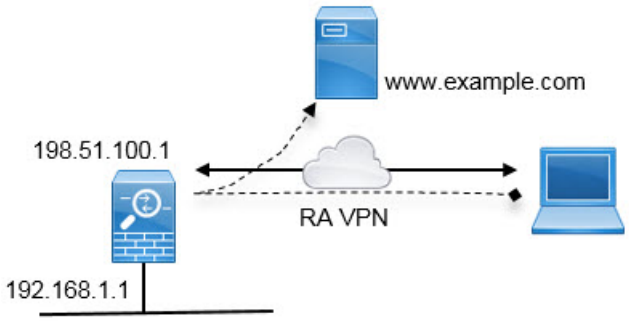
Examples for Remote Access VPN

The following are examples of configuring remote access VPN.

How to Provide Internet Access on the Outside Interface for Remote Access VPN Users (Hair Pinning)

In remote access VPN, you might want users on the remote networks to access the Internet through your device. However, because the remote users are entering your device on the same interface that faces the Internet (the outside interface), you need to bounce Internet traffic right back out of the outside interface. This technique is sometimes called hair pinning.

The following graphic shows an example. There is a remote access VPN configured on the outside interface, 198.51.100.1. You want to split the remote user's VPN tunnel, so that Internet-bound traffic goes back out the outside interface, while traffic to your internal networks continue through the device. Thus, when a remote user wants to go to a server on the Internet, such as www.example.com, the connection first goes through the VPN, then gets routed back out to the Internet from the 198.51.100.1 interface.



The following procedure explains how to configure this service.

Before you begin

This example assumes that you have already registered the device, applied a remote access VPN license, and uploaded the AnyConnect Client image. It also assumes that you have configured the identity realm, which is also used in Identity policies.

This procedure also assumes you are using the default setting for permitting VPN traffic, which subjects the VPN traffic to the access control policy. In the running configuration, this is represented by the **no sysopt connection permit-vpn** command. If you instead enabled **sysopt connection permit-vpn** through FlexConfig, the steps that configure access control rules are not needed.

Procedure

Step 1 Configure the remote access VPN connection profile.

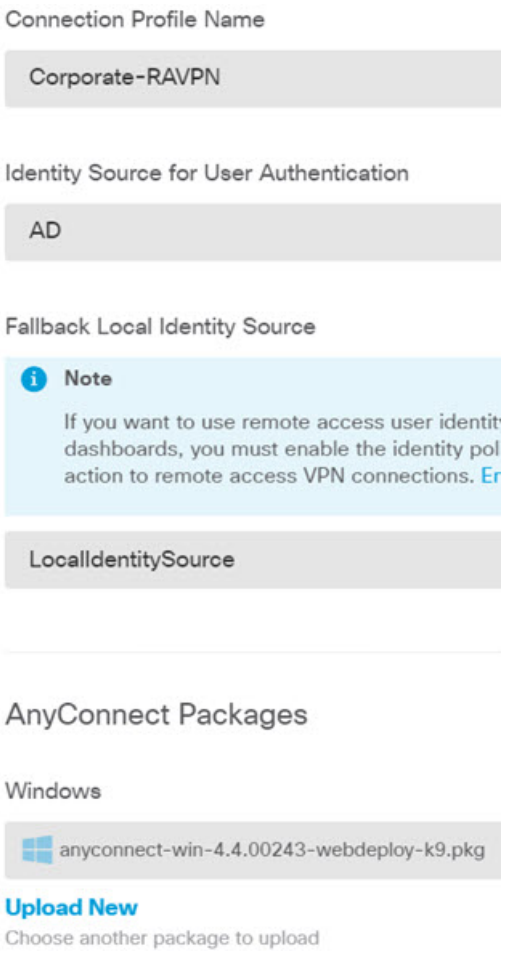
a) Click **Device**, then click **Setup Connection Profile** in the Remote Access VPN group. (Click **View Configuration** if you already configured a profile).

For existing connections, click **Edit** to modify the profile.

b) Configure the connection profile settings:

- **Connection Profile Name**—Enter a name, for example, Corporate-RAVPN.
- **Identity Source for User Authentication**—Select the identity realm used for authenticating remote users. If you have not already configured one, click **Create New Identity Realm** at the bottom of the drop-down list and create it now. Alternatively, you can use the LocalIdentitySource as the primary or fallback source.
- **AnyConnect Packages**—Upload AnyConnect Clients for each operating system you will support. Wait for the upload to complete before continuing.

The connection profile settings should look similar to the following:

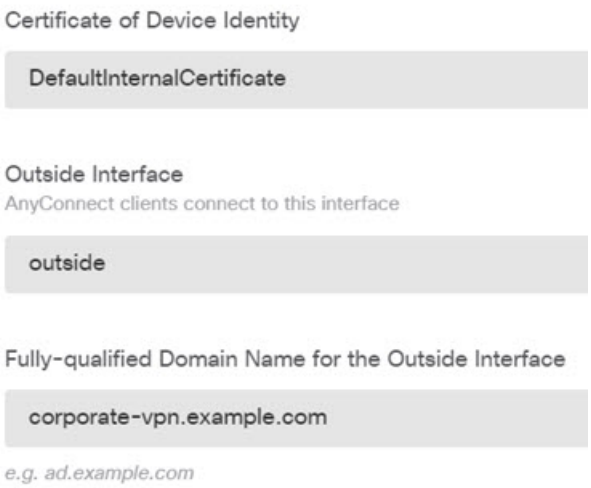


c) Click **Next**, then configure the device identity properties:

- **Certificate of Device Identity**—Select the internal certificate used to establish the identity of the device. Clients must accept this certificate to complete a secure VPN connection. You can use the DefaultInternalCertificate if you do not have your own.
- **Outside Interface**—Select your outside interface, to which remote users will connect. This interface is normally named “outside.”

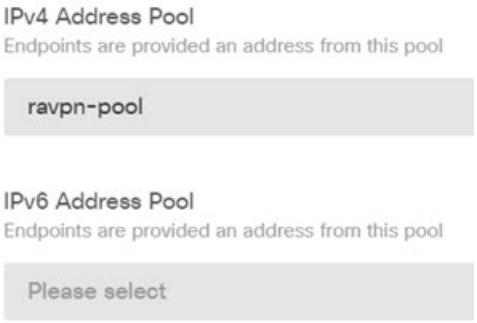
- **Fully-qualified Domain Name for the Outside Interface**—If you have a DNS name for the outside interface, enter it here. For example, corporate-vpn.example.com.

The device identity section of the page might look like the following:



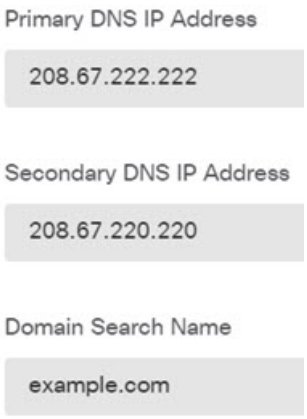
d) Continue down the page and configure the IPv4 Address Pool and optionally, the IPv6 Address Pool.

Select an object that identifies a network. Remote access VPN users are assigned an address from this pool. For example, a network object that specifies 10.1.10.0/24. If the object does not already exist, click Create New Network at the bottom of the list. Also configure a pool for IPv6 if you support those addresses.



e) Scroll down the page and configure the DNS settings for remote connections.

Enter the IP addresses of the DNS servers you use, and your local domain name, for example, example.com. You can click OpenDNS to use the Open DNS servers.

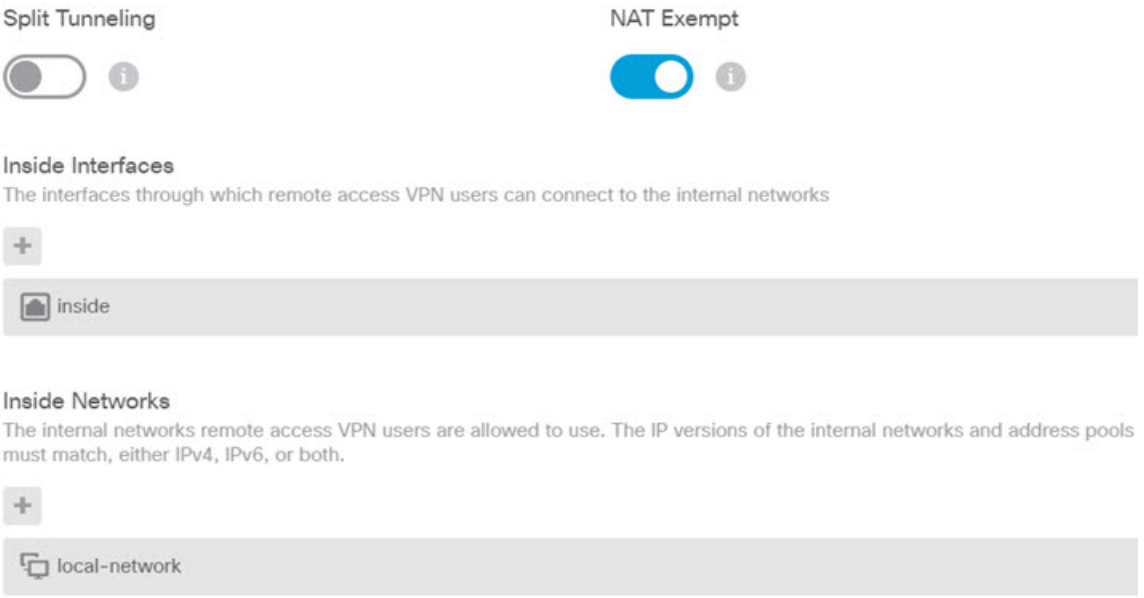


f) Click **Next**, scroll down, and configure the Corporate Resource options.

(You can also configure the banner, connection time and timeout, and proxy settings, but these are not directly related to hair pinning.)

The following settings are critical to making hair pinning possible in the remote access VPN.

- **Split Tunneling**—Disable this feature. You want all traffic to go to the VPN gateway, whereas split tunneling is a way to allow remote clients to directly access local or Internet sites outside of the VPN.
- **NAT Exempt**—Enable this feature. Select the inside interface, then select a network object that defines the internal networks. In this example, the object should specify 192.168.1.0/24. RA VPN traffic going to the internal network will not get address translation. However, because hair-pinned traffic is going out the outside interface, it will still be NAT'ed because the NAT exemption applies to the inside interface only.



g) Optionally, select an **AnyConnect Client Profile**, then click **Next**.

h) Review the RA VPN configuration, then click **Finish**.

Step 2 Configure the NAT rule to translate all connections going out the outside interface to ports on the outside IP address (interface PAT).

When you complete the initial device configuration, the system creates a NAT rule named InsideOutsideNatRule. This rule applies interface PAT to IPv4 traffic from any interface that exits the device through the outside interface. Because the outside interface is included in "Any" source interface, the rule you need already exists, unless you edited it or deleted it.

The following procedure explains how to create the rule you need.

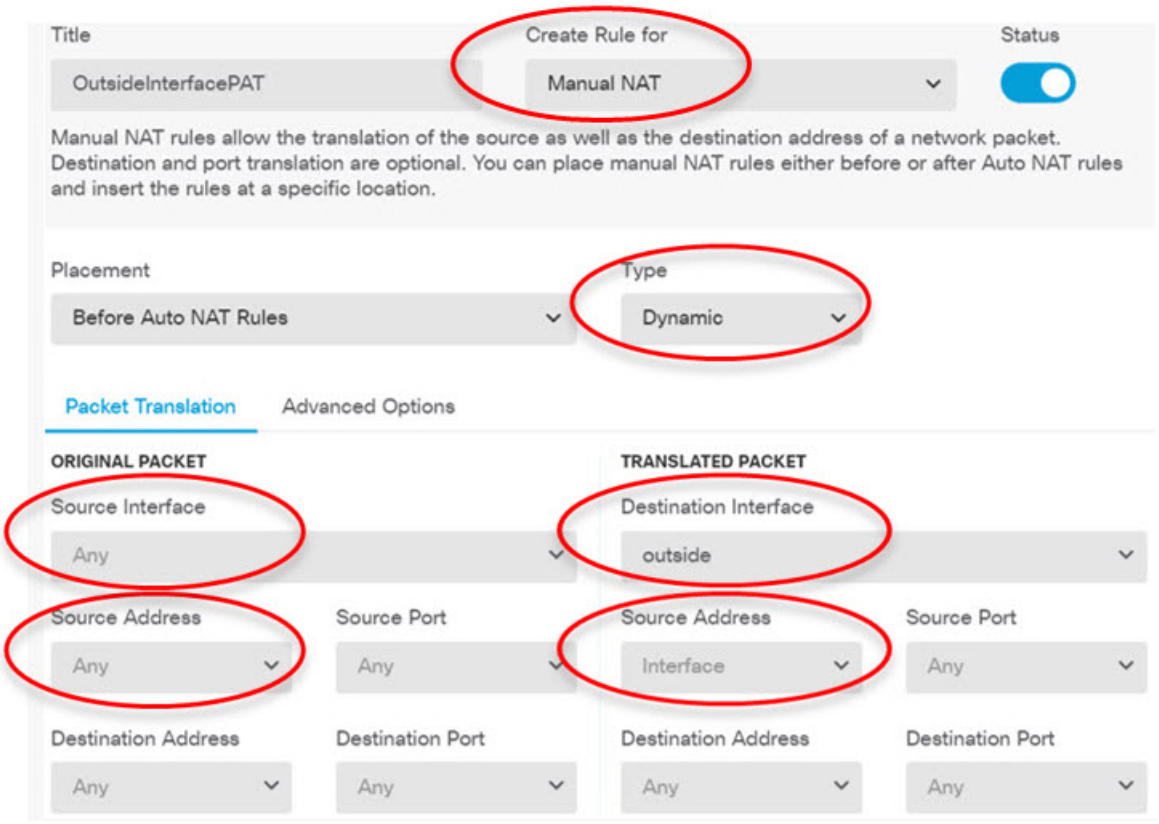
a) Click **Policies** > **NAT**.
b) Do one of the following:

- To edit the InsideOutsideNatRule, mouse over the **Action** column and click the edit icon ( ).
- To create a new rule, click **+**.

c) Configure a rule with the following properties:

- **Title**—For a new rule, enter a meaningful name without spaces. For example, OutsideInterfacePAT.
- **Create Rule For**—**Manual NAT**.
- **Placement**—**Before Auto NAT Rules** (the default).
- **Type**—**Dynamic**.
- **Original Packet**—For **Source Address**, select either Any or any-ipv4. For **Source Interface**, ensure that you select Any (which is the default). For all other Original Packet options, keep the default, Any.
- **Translated Packet**—For **Destination Interface**, select outside. For **Translated Address**, select **Interface**. For all other Translated Packet options, keep the default, Any.

The following graphic shows the simple case where you select Any for the source address.



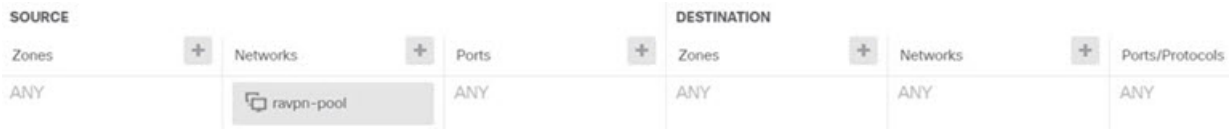
d) Click **OK**.

Step 3 Configure an access control rule to allow access from the remote access VPN address pool.

The following example allows traffic from the address pool to any destination. You can adjust this to meet your specific requirements. You can also precede the rule with block rules to filter out undesirable traffic.

a) Click **Policies** > **Access Control**.
b) Click + to create a new rule.
c) Configure a rule with the following properties:

- **Order**—Select a position in the policy before any other rule that might match these connections and block them. The default is to add the rule to the end of the policy. If you need to reposition the rule later, you can edit this option or simply drag and drop the rule to the right slot in the table.
- **Title**—Enter a meaningful name without spaces. For example, RAVPN-address-pool.
- **Action**—**Allow**. You can select Trust if you do not want this traffic to be inspected for protocol violations or intrusions.
- **Source/Destination** tab—For **Source** > **Network**, select the same object you used in the RA VPN connection profile for the address pool. Leave the default, Any, for all other Source and Destination options.



- **Application**, **URL**, and **Users** tabs—Leave the default settings on these tabs, that is, nothing selected.
- **Intrusion**, **File** tabs—You can optionally select intrusion or file policies to inspect for threats or malware.
- **Logging** tab—You can optionally enable connection logging.

d) Click **OK**.

Step 4 Commit your changes.

a) Click the **Deploy Changes** icon in the upper right of the web page.

b) Click the **Deploy Now** button.

You can wait until deployment completes, or click **OK** and check the task list or deployment history later.

How to Use a Directory Server on an Outside Network with Remote Access VPN

You can configure a remote access VPN to allow mobile workers and telecommuters to securely connect to your internal networks. Security of the connection depends on your directory server, which authenticates the user connection to ensure that only authorized users can gain entry.

If your directory server is on an outside network rather than an inside network, you need to configure a site-to-site VPN connection from the outside interface to the network that includes the directory server. **There is one trick to the site-to-site VPN configuration:** you must include the outside interface address of the remote access VPN device within the "inside" networks of the site-to-site VPN connection, and also in the remote networks for the device behind which the directory server resides. This will be explained further in the following procedure.

Note If you use the data interfaces as a gateway for the virtual management interface, this configuration also enables usage of the directory for identity policies. If you do not use data-interfaces as the management gateway, ensure that there is a route from the management network to the inside network that participates in the site-to-site VPN connection.

This use case implements the following network scenario.

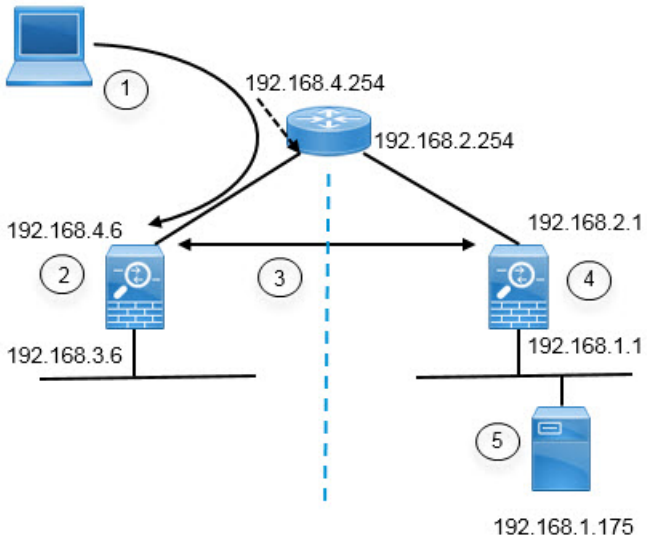


Figure Callout	Description
1	Remote access host that makes a VPN connection to 192.168.4.6. Clients will get an address in the 172.18.1.0/24 address pool.
2	Site A, which hosts the remote access VPN.
3	The site-to-site VPN tunnel between the outside interfaces of the Site A and Site B the FTD devices.
4	Site B, which hosts the directory server.
5	The directory server, on the inside network of Site B.

Before you begin

This use case assumes that you followed the device setup wizard to establish a normal baseline configuration. Specifically:

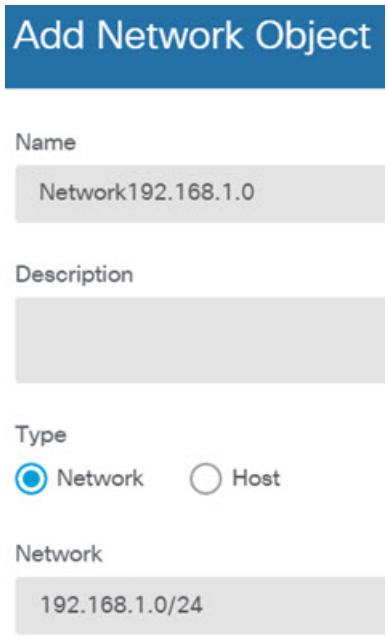
- There is an Inside_Outside_Rule access control rule that allows (or trusts) traffic going from the inside_zone to the outside_zone.
- The inside_zone and outside_zone security zones contain the inside and outside interfaces (respectively).
- There is an InsideOutsideNATRule that performs interface PAT for all traffic coming from inside interfaces going to the outside interface. On devices that use an inside bridge group by default, there might be several rules for interface PAT.
- There is a static IPv4 route for 0.0.0.0/0 that points to the outside interface. This example assumes that you are using static IP addresses for the outside interfaces, but you could also use DHCP and obtain the static route dynamically. For this example, we are assuming the following static routes:
  - Site A: outside interface, gateway is 192.168.4.254.
  - Site B: outside interface, gateway is 192.168.2.254.

Procedure

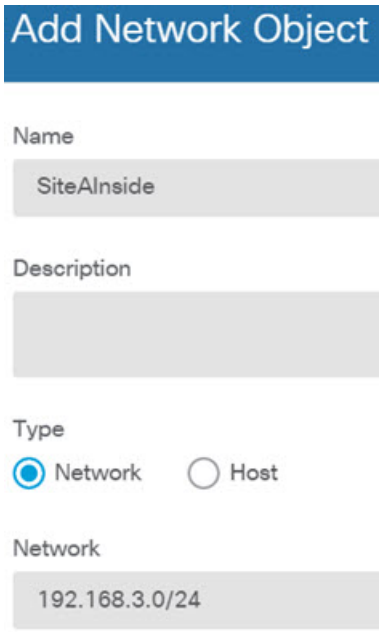
Step 1 Configure the site-to-site VPN connection on **Site B**, which hosts the directory server.

a) Click **Device**, then click **View Configuration** in the Site-to-Site VPN group.
b) Click the + button.
c) Configure the following options for **Endpoint Settings**.

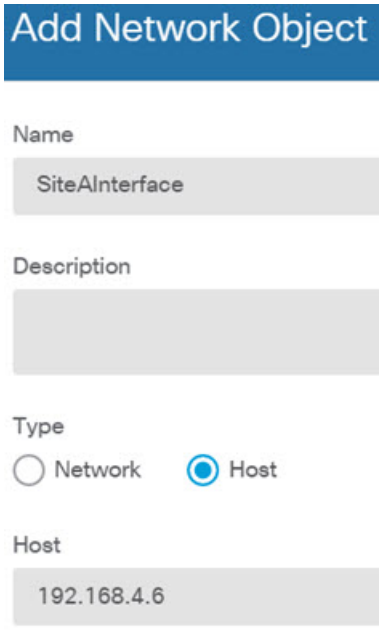
- **Connection Profile Name**—Enter a name, for example, SiteA (to indicate that the connection is to Site A).
- **Local Site**—These options define the local endpoint.
  - **Local VPN Access Interface**—Select the **outside** interface (the one with the 192.168.2.1 address in the diagram).
  - **Local Network**—Click + and select the network object that identifies the local network that should participate in the VPN connection. Because the directory server is on this network, it can participate in the site-to-site VPN. Assuming that the object does not already exist, click **Create New Network** and configure an object for the 192.168.1.0/24 network. After saving the object, select it in the drop-down list and click **OK**.



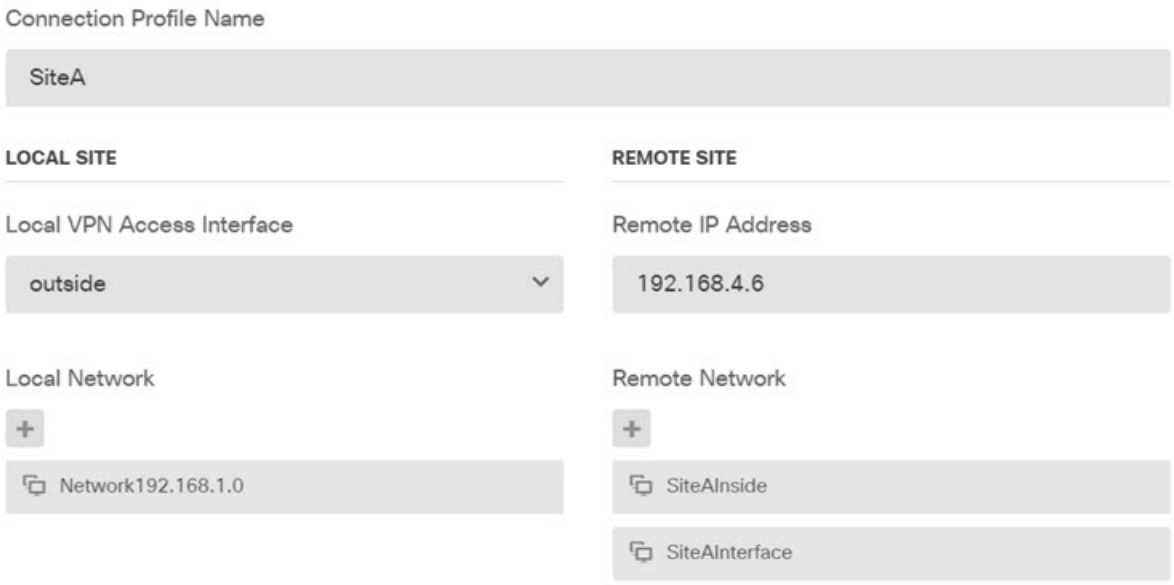
- **Remote Site**—These options define the remote endpoint.
  - **Remote IP Address**—Enter 192.168.4.6, which is the IP address of the remote VPN peer's interface that will host the VPN connection.
  - **Remote Network**—Click + and select the network objects that identify the remote networks that should participate in the VPN connection. Click **Create New Network**, configure the following objects, then select them in the list.
    1. SiteAInside, Network, 192.168.3.0/24.



2. SiteAInterface, Host, 192.168.4.6. **This is key: you must include the remote access VPN connection point address as part of the remote network for the site-to-site VPN connection so that the RA VPN hosted on that interface can use the directory server.**



When you are finished, the endpoint settings should look like the following:



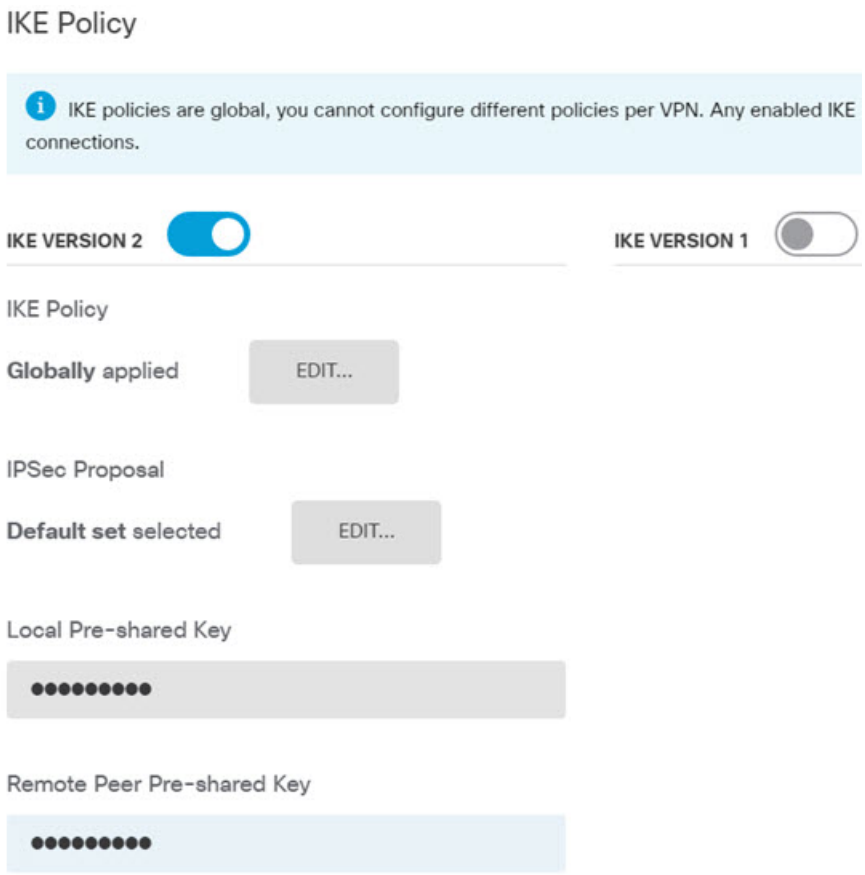
d) Click **Next**.

e) Define the privacy configuration for the VPN.

For this use case, we assume you qualify for export controlled features, which allows the use of strong encryption. Adjust these example settings to meet your needs and your license compliance.

- **IKE Version 2**, **IKE Version 1**—Keep the defaults, **IKE Version 2** enabled, **IKE Version 1** disabled.
- **IKE Policy**—Click **Edit** and enable **AES-GCM-NULL-SHA** and **AES-SHA-SHA**, and disable **DES-SHA-SHA**.
- **IPsec Proposal**—Click **Edit**. In the Select IPSec Proposals dialog box, click **+**, then click **Set Default** to choose the default AES-GCM proposals.
- **Local Preshared Key**, **Remote Peer Preshared Key**—Enter the keys defined on this device and on the remote device for the VPN connection. These keys can be different in IKEv2. The key can be 1-127 alphanumeric characters. **Remember these keys, because you must configure the same strings when creating the site-to-site VPN connection on the Site A device.**

The IKE policy should look like the following:



f) Configure the **Additional Options**.

- **NAT Exempt**—Select the interface that hosts the inside network, in this example, the **inside** interface. Typically, you do not want traffic within a site-to-site VPN tunnel to have their IP addresses translated. This option works only if the local network resides behind a single routed interface (not a bridge group member). If the local network is behind more than one routed interface, or one or more bridge group members, you must manually create the NAT exempt rules. For information on manually creating the required rules, see Exempting Site-to-Site VPN Traffic from NAT.
- **Diffie-Helman Group for Perfect Forward Secrecy**—Select **Group 19**. This option determines whether to use Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.

The options should look like the following.

g) Click **Next**.
h) Review the summary and click **Finish**.

The summary information is copied to the clipboard. You can paste the information in a document and use it to help you configure the remote peer, or to send it to the party responsible for configuring the peer.

i) Click the **Deploy Changes** icon in the upper right of the web page.

j) Click the **Deploy Now** button and wait for deployment to complete successfully.

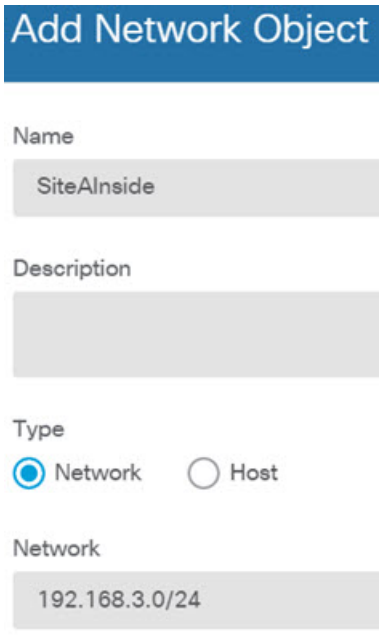
Now the Site B device is ready to host one end of the site-to-site VPN connection.

Step 2 Log out of the **Site B** device and log into the **Site A** device.

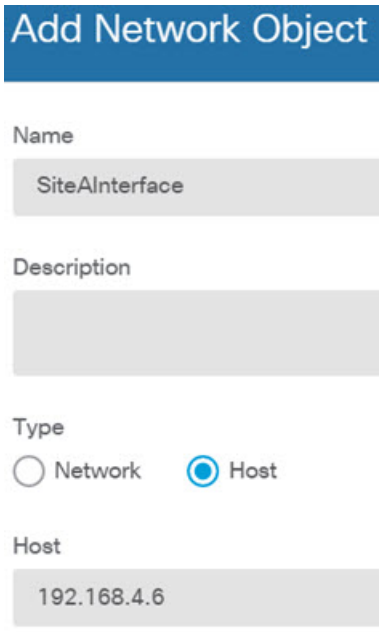
Step 3 Configure the site-to-site VPN connection on **Site A**, which will host the remote access VPN.

a) Click **Device**, then click **View Configuration** in the Site-to-Site VPN group.
b) Click the + button.
c) Configure the following options for **Endpoint Settings**.

- **Connection Profile Name**—Enter a name, for example, SiteB (to indicate that the connection is to Site B).
- **Local Site**—These options define the local endpoint.
  - **Local VPN Access Interface**—Select the **outside** interface (the one with the 192.168.4.6 address in the diagram).
  - **Local Network**—Click + and select the network objects that identify the local networks that should participate in the VPN connection. Click **Create New Network**, configure the following objects, then select them in the list. **Note that you created the same objects in the Site B device, but you have to create them again in the Site A device.**
    1. SiteAInside, Network, 192.168.3.0/24.

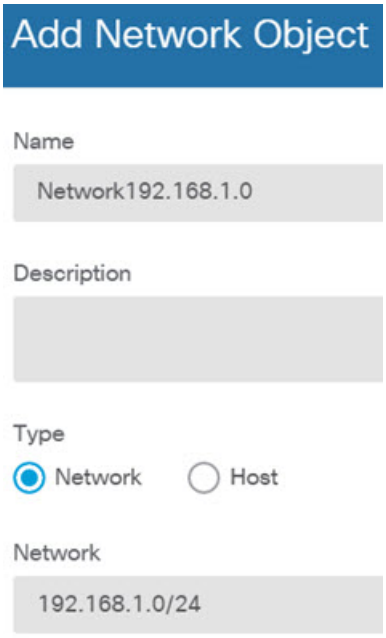


2. SiteAInterface, Host, 192.168.4.6. **This is key: you must include the remote access VPN connection point address as part of the inside network for the site-to-site VPN connection so that the RA VPN hosted on that interface can use the directory server on the remote network.**

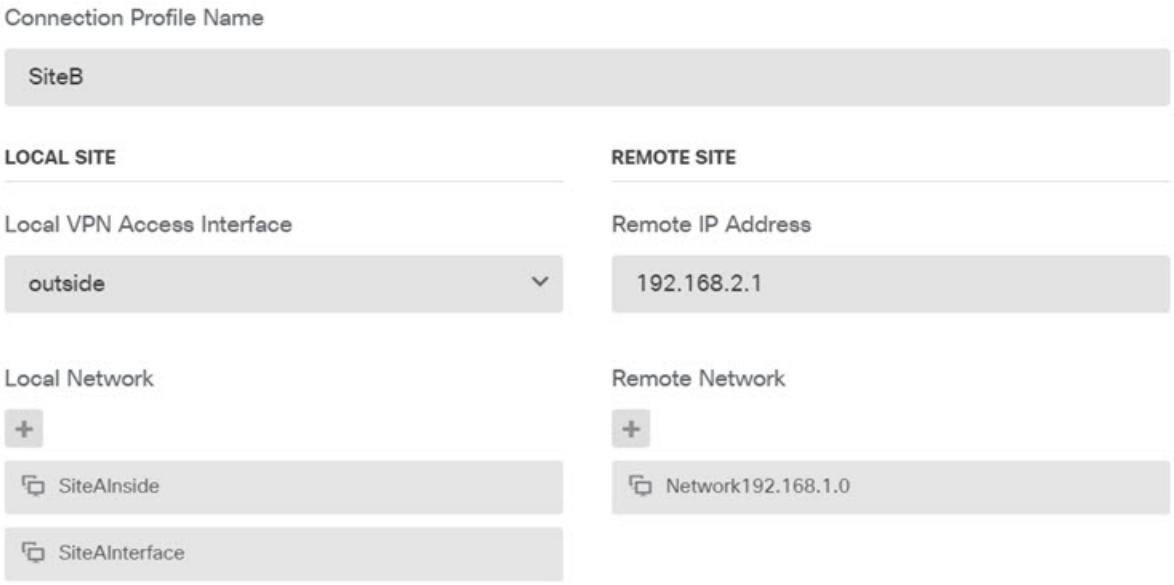


- **Remote Site**—These options define the remote endpoint.
  - **Remote IP Address**—Enter 192.168.2.1, which is the IP address of the remote VPN peer's interface that will host the VPN connection.

- **Remote Network**—Click + and select the network object that identifies the remote network that should participate in the VPN connection, the one that includes the directory server. Click **Create New Network** and configure an object for the 192.168.1.0/24 network. After saving the object, select it in the drop-down list and click **OK**. **Note that you created the same object in the Site B device, but you have to create it again in the Site A device.**



When you are finished, the endpoint settings should look like the following. Notice that the local/remote networks are flipped compared to the Site B settings. This is how the two ends of a point-to-point connection should always look.

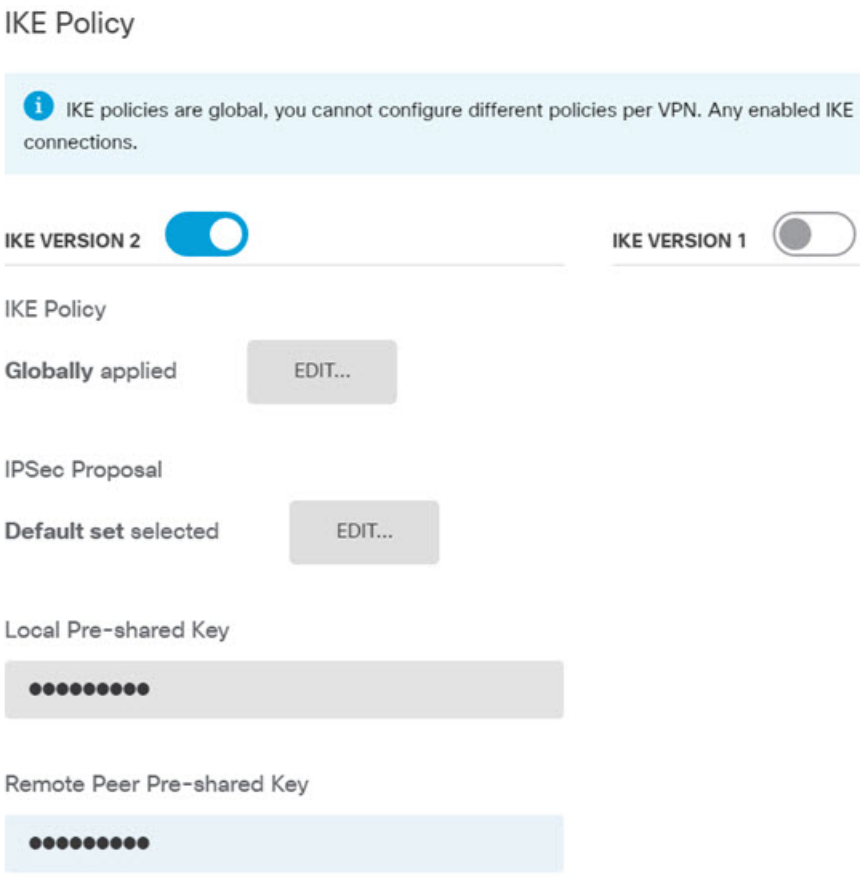


d) Click **Next**.

e) Define the privacy configuration for the VPN.

Configure the same IKE version, policy, and IPsec proposal, and the same preshared keys, as you did for the Site B connection, **but make sure that you reverse the Local and Remote preshared keys**.

The IKE policy should look like the following:



f) Configure the **Additional Options**.

- **NAT Exempt**—Select the interface that hosts the inside network, in this example, the **inside** interface. Typically, you do not want traffic within a site-to-site VPN tunnel to have their IP addresses translated. This option works only if the local network resides behind a single routed interface (not a bridge group member). If the local network is behind more than one routed interface, or one or more bridge group members, you must manually create the NAT exempt rules. For information on manually creating the required rules, see Exempting Site-to-Site VPN Traffic from NAT.
- **Diffie-Helman Group for Perfect Forward Secrecy**—Select **Group 19**.

The options should look like the following.

g) Click **Next**.
h) Review the summary and click **Finish**.
i) Click the **Deploy Changes** icon in the upper right of the web page.

j) Click the **Deploy Now** button and wait for deployment to complete successfully.

Now the Site A device is ready to host the other end of the site-to-site VPN connection. Because Site B is already configured with compatible settings, the two devices should negotiate a VPN connection.

You can confirm the connection by logging into the device CLI and pinging the directory server. You can also use the **show ipsec sa** command to view the session information.

Step 4 Configure the directory server on **Site A**. Click **Test** to verify that there is a connection.

a) Select **Objects**, then select **Identity Sources** from the table of contents.
b) Click **+** > **AD**.
c) Configure the basic realm properties.

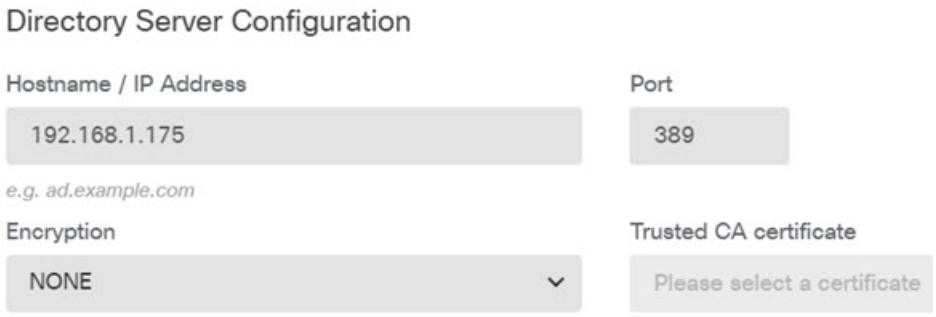
- **Name**—A name for the directory realm. For example, AD.
- **Type**—The type of directory server. Active Directory is the only supported type, and you cannot change this field.
- **Directory Username**, **Directory Password**—The distinguished username and password for a user with appropriate rights to the user information you want to retrieve. For Active Directory, the user does not need elevated privileges. You can specify any user in the domain. The username must be fully qualified; for example, Administrator@example.com (not simply Administrator).

  Note The system generates ldap-login-dn and ldap-login-password from this information. For example, Administrator@example.com is translated as cn=adminisntrator,cn=users,dc=example,dc=com. Note that cn=users is always part of this translation, so you must configure the user you specify here under the common name “users” folder.

- **Base DN**—The directory tree for searching or querying user and group information, that is, the common parent for users and groups. For example, cn=users,dc=example,dc=com. For information on finding the base DN, see Determining the Directory Base DN.
- **AD Primary Domain**— The fully qualified Active Directory domain name that the device should join. For example, example.com.

d) Configure the directory server properties.

- **Hostname/IP Address**—The hostname or IP address of the directory server. If you use an encrypted connection to the server, you must enter the fully-qualified domain name, not the IP address. For this example, enter 192.168.1.175.
- **Port**—The port number used for communications with the server. The default is 389. Use port 636 if you select LDAPS as the encryption method. For this example, keep 389.
- **Encryption**—To use an encrypted connection for downloading user and group information. The default is **None**, which means that user and group information is downloaded in clear text. For RA VPN, you can use **LDAPS**, which is LDAP over SSL. Use port 636 if you select this option. RA VPN does not support STARTTLS. For this example, select **None**.
- **Trusted CA Certificate**—If you select an encryption method, upload a Certificate Authority (CA) certificate to enable a trusted connection between the system and the directory server. If you are using a certificate to authenticate, the name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 192.168.1.175 as the IP address but ad.example.com in the certificate, the connection fails.



e) Click the **Test** button to verify the system can contact the server.

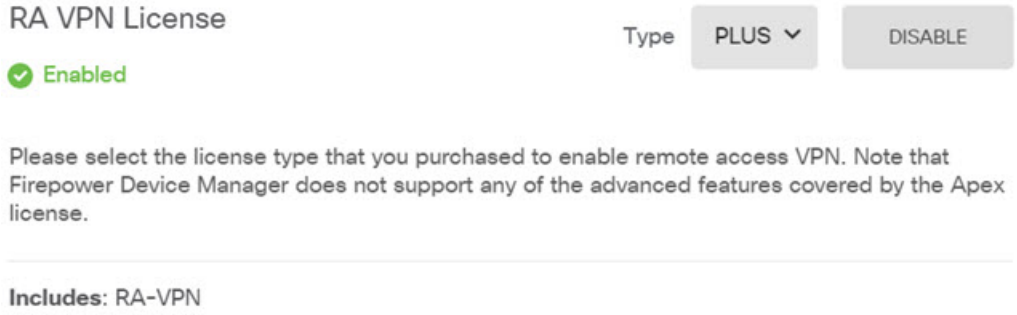
The system uses separate processes to access the server, so you might get errors indicating that the connection works for one type of use but not another, for example, available for Identity policies but not for remote access VPN. If the server cannot be reached, verify that you have the right IP address and host name, that the DNS server has an entry for the hostname, and so forth. Also, verify that the site-to-site VPN connection is working and that you included Site A's outside interface address in the VPN, and that

NAT is not translating traffic for the directory server. You might also need to configure a static route for the server.

f) Click **OK**.

Step 5 Click **Device** > **Smart License** > **View Configuration**, and enable the RA VPN license.

When enabling the RA VPN license, select the type of license you purchased: Plus, Apex (or both), or VPN Only. For more information, see Licensing Requirements for Remote Access VPN, on page 3.



Step 6 Configure the remote access VPN on Site A.

a) Click **Device**, then click **Setup Connection Profile** in the Remote Access VPN group.

b) Define the AnyConnect client configuration.

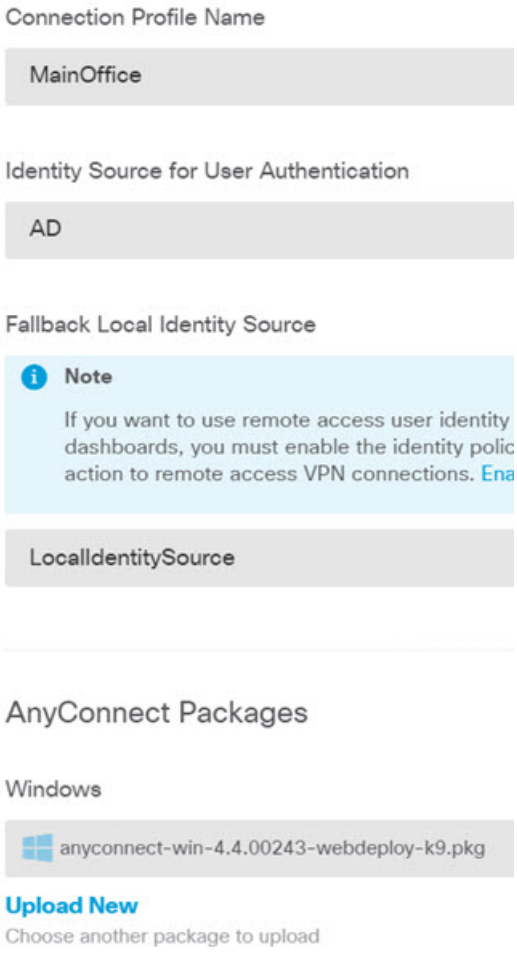
- **Connection Profile Name**—The name for this connection, up to 50 characters without spaces. For example, MainOffice. You cannot use an IP address as the name.

  Note The name you enter here is what users will see in the connection list in the AnyConnect client. Choose a name that will make sense to your users.

- **Identity Source for User Authentication**—Select the directory realm. You can optionally select the local database as the fallback identity source.

- **AnyConnect Packages**—The AnyConnect full installation software images that you will support on this VPN connection. For each package, the filename, including extensions, can be no more than 60 characters. You can upload separate packages for Windows, Mac, and Linux endpoints.

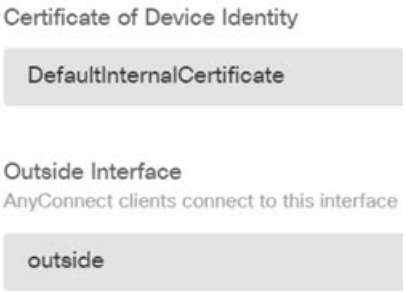
  Download the packages from software.cisco.com (there is a link to the right location at the end of the page). If the endpoint does not already have the right package installed, the system prompts the user to download and install the package after the user authenticates.



c) Click **Next**.

d) Define the device identity and client addressing configuration.

- **Certificate of Device Identity**—Select DefaultInternalCertificate. This is the internal certificate used to establish the identity of the device. Clients must accept this certificate to complete a secure VPN connection. If you have a different certificate that you want use, click **Create New Internal Certificate** in the drop-down list and upload it.
- **Outside Interface**—Select **outside**, the one with the 192.168.4.6 IP address. This is the interface to which users connect when making the remote access VPN connection.



- **Fully-qualified Domain Name for the Outside Interface**—The name of the interface, for example, ravpn.example.com. If you specify a name, the system can create a client profile for you. For this example, we will leave it blank.

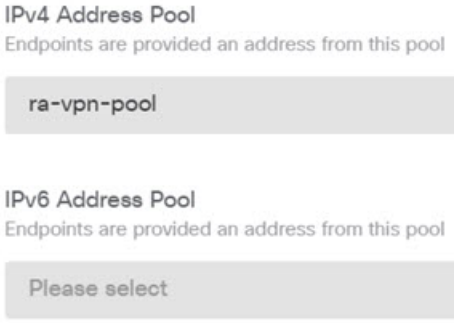
  Note You are responsible for ensuring that the DNS servers used in the VPN and by clients can resolve this name to the outside interface's IP address. Add the FQDN to the relevant DNS servers.

- **IPv4, IPv6 Address Pools**—These options define the address pools for the remote endpoints. For this example, select **Create New Network** in the IPv4 address pool and create an object for the 172.18.1.0/24 network, then select the object. Clients are assigned an address from this pool. Leave the IPv6 pool blank. The address pool cannot be on the same subnet as the IP address for the outside interface.

  The object should look like the following:

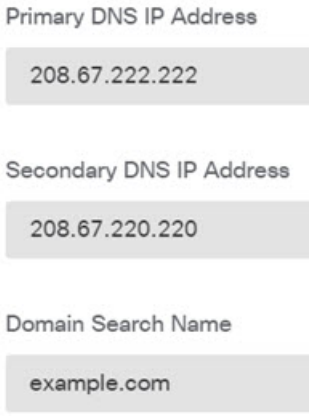
  

  The pool specification should look like the following:

- **Primary, Secondary DNS Servers**—For this example, click the **OpenDNS** button to load these fields with the OpenDNS public DNS servers. RA VPN clients use these DNS servers clients for domain name resolution when connected to the VPN. Optionally, enter the IP addresses of your DNS servers.

- **Domain Search Name**—Enter the domain name for your network, e.g. example.com. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.

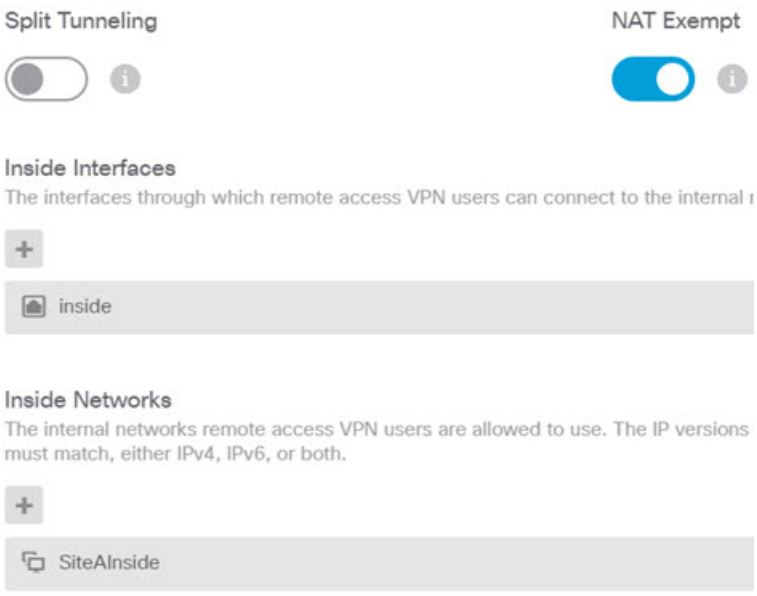


e) Click **Next**.
f) Define the connection settings to customize AnyConnect client behavior.

Keep the default settings for all options, as they are appropriate for most networks.

Because **NAT Exempt** is selected, you need to configure the following options:

- **Inside Interfaces**—Select the **inside** interface. These are the interfaces for the internal networks remote users will be accessing. NAT rules are created for these interfaces.
- **Inside Networks**—Select the SiteAInside network object. These are the network objects that represent internal networks remote users will be accessing.



g) Click **Next**.
h) Review the summary.

First, verify that the summary is correct.

Then, click **Instructions** to see what end users need to do to initially install the AnyConnect software and test that they can complete a VPN connection. Click **Copy** to copy these instructions to the clipboard, and paste them in a text file or email.

i) Click **Finish**.

Step 7 Click the **Deploy Changes** icon in the upper right of the web page.

Step 8 Click the **Deploy Now** button and wait for deployment to complete successfully.

Now the Site A device is ready to accept RA VPN connections. Have an external user install the AnyConnect Client client and complete a VPN connection.

You can confirm the connection by logging into the device CLI and using the **show vpn-sessiondb anyconnect** command to view the session information.

How to Customize the AnyConnect Client Icon and Logo

You can customize the icon and logo for the AnyConnect Client app on Windows and Linux client machines. The names of the icons are pre-defined, and there are specific limits to the file type and size for the images you upload.

Although you can use any filename if you deploy your own executable to customize the GUI, this example assumes you are simply swapping icons and logos without deploying a fully-customized framework.

There are a number of images you can replace, and their file names differ based on platform. For complete information on customization options, file names, types, and sizes, please see the chapter on customizing and localizing the AnyConnect Client and installer in the *Cisco AnyConnect Secure Mobility Client Administrator Guide*. For example, the chapter for the 4.8 client is available at:

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

Before you begin

For the purposes of this example, we will replace the following images for Windows clients. Note that if your image is a different size than the maximum, the system will automatically resize it to the maximum, and stretch the image if necessary.

- app_logo.png

  This application logo image is the application icon, and it can have a maximum size of 128 x 128 pixels.

- company_logo.png

  This company logo image appears in the top-left corner of the tray flyout and Advanced dialogs. The maximum size is 97 x 58 pixels.

- company_logo_alt.png

The alternative company logo image appears in the bottom-right corner of the About dialog box. The maximum size is 97 x 58 pixels.

To upload these files, you must place them on a server that the FTD device can access. You can use a TFTP, FTP, HTTP, HTTPS, or SCP server. The URLs to get images from these files can include paths and uesrname/password, as required by your server setup. This example will use TFTP.

Procedure

Step 1 Upload the image files to each FTD device that is acting as an RA VPN headend that should use the customized icons and logos.

a) Log into the device CLI using an SSH client.

b) In the CLI, enter the **system support diagnostic-cli** command to enter diagnostic CLI mode.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

Note Read the message! You must press **Ctrl+a, then d**, to get out of the diagnostic CLI and back into the normal FTD CLI mode.

c) Note the command prompt. The normal CLI uses > only, whereas the diagnostic CLI's user EXEC mode uses the hostname plus >. In this example, ftdv1>. You need to get into privileged EXEC mode, which uses # as the ending character, for example, ftdv1#. If your prompt already has #, skip this step. Otherwise, enter the enable command, and simply press Enter at the password prompt without entering a password.

```
ftdv1> enable
Password:
ftdv1#
```

d) Use the **copy** command to copy each file from the hosting server to the FTD device's disk0. You can place them in a subdirectory, such as disk0:/anyconnect-images/. You can create a new folder using the **mkdir** command.

For example, if the TFTP server's IP address is 10.7.0.80, and you want to create a new directory, the commands would be similar to the following. Note that responses to the **copy** command are omitted after the first example.

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)
```

```
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

Step 2 Use the **import webvpn** command in the diagnostic CLI to instruct the AnyConnect Client to download these images when installing itself on client machines.

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:**/*directoryname/filename*

This command is for Windows. For Linux, replace the **win** keyword with **linux** or **linux-64**, as appropriate for your clients.

For example, to import the files uploaded in the previous step, and assuming we are still in the diagnostic CLI:

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

Step 3 Verify the configuration:

- To verify the imported files, use the **show import webvpn AnyConnect-customization** command in the diagnostic CLI privileged EXEC mode.
- To verify that the images were downloaded to a client, they should appear when the user runs the client. You can also check the following folder on Windows clients, where %PROGRAMFILES% typically resolves to c:\Program Files.

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

What to do next

If you want to return to the default images, use the **revert webvpn** command (in the diagnostic CLI privileged EXEC mode) for each image you customized. The command is:

revert webvpn AnyConnect-customization type resource platform win name *filename*

As with **import webvpn**, replace **win** with **linux** or **linux-64** if you customized those client platforms, and issue the command separately for each image filename you imported. For example:

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```