Getting Started

This chapter provides an overview of the VPN 3000 Concentrator's Quick Configuration program and describes where to go in the ASDM to configure the counterpart features. Following the outline of configuration tasks, this chapter lists the information needed to run the VPN wizard to configure site-to-site and remote access tunnels.

Quick Configuration Tasks and Counterparts in ASDM

Table 3-1 describes the following configuration tasks and where to perform these tasks in ASDM.

- Configuring IP interfaces
- Configuring system information
- Configuring tunneling protocols and options
- Configuring an address management method
- Configuring authentication
- Configuring an internal server user database
- Configuring IPSec groups
- Configuring an administrator password

Table 3-1 Getting Started Tasks

VPN 3000 Quick Configuration Tasks	ASA Counterpart
Configuring IP interfaces Enter the IP address and subnet mask for private and public ethernet connections. Optionally, enter addresses for the external interface. • Enable/disable • DHCP Client/system name • Static IP addressing (IP addr/subnet mask) • Type of interface (public or private) • MAC address • Filter • Speed • Duplex • MTU	Go to **Configuration > Interfaces**. • Add/Edit – Select Hardware Port – Check Enable Interface • Enter: – VLAN ID – Sub-interface ID – Interface Name – Security Level – Source of IP Address: Static IP or DHCP – IP Address – Subnet Mask – MTU • Click **Configure Hardware Properties...** – Select Duplex type: Full, Half, Auto – Select Speed 10, 100, Auto • Optionally enable traffic between two or more interfaces configured with the same security levels.
Configuring system information • System hostname • Time and date • DNS server information (IP address, Internet domain name, default gateway)	Go to **Configuration > Properties > Device Administration > Device**. • Enter host name and domain name. • Go to **Configuration > Properties > Device Administration > Clock** to enter time and date. • Go to **Configuration > Properties > DNS Client**. – Add Servers (up to 6). – Enter timeout in seconds. – Enter number of retries. – Enable DNS lookup on interfaces.
Configuring tunneling protocols and options • PPTP -- encryption option • L2TP -- encryption option • IPSec (allows remote access only. Can't do site-to-site through QC)	To define Tunnel Groups go to **Configuration > VPN > General > Tunnel Group**. Two default tunnel groups for IPSec: • DefaultL2LGroup for LAN-to-LAN • DefaultRAGroup for Remote Access

Table 3-1 Getting Started Tasks

VPN 3000 Quick Configuration Tasks	ASA Counterpart
Configuring address management method • Client specifies its own IP address. • Assign IP addresses per user (use auth server). • Use DHCP (specify server address or name). • Configure a pool (start/end ranges).	Go to **Configuration > VPN > IP Address Management > Assignment**. Choices: • Use address from authentication server. • Use DHCP. • Use internal address pools. • Configure IP address pools under **Configuration > VPN > IP Address Management > IP Pools**.
Configuring authentication • Choose a server type: internal, RADIUS, NTDomain, SDI, Kerberos/Active Directory. • Fill in information for selected authentication server. Each has its own screen.	Go to **Configuration > Properties > AAA Setup**. • Add server groups. • Add servers to server groups. • Configure authentication prompts.
Configuring internal server user database Enter user information: • User name • Password • Verify password • IP address (if per-user address assignment) • Subnet mask	Go to **Configuration > Properties > Device Administration > User Accounts**. Add user account and enter information: • Under Identity: Username Password Confirm Password Privilege Level • Under VPN Policy (specify or check inherit if from group policy) Group Policy (previously defined) Tunneling Protocols Filter Tunnel Group Lock Store Password on Client System Connection Settings Dedicated IP address (optional)
Configuring IPSec group • Group name • Password • Verify	Go to **Configuration > VPN > General > Tunnel Group**. Add tunnel group of IPSec type.
Configuring administrator password	Go to **Configuration > Properties > Device Administration > Password**.
Testing the VPN Connection steps	

Configuring a VPN Tunnel Using the VPN Wizard

The VPN wizard lets you configure a site-to-site or remote access VPN tunnel from the ASA to either another VPN device or a remote client user. You can use the wizard to define new VPN configurations only. Once you have configured a VPN tunnel using the wizard, you can edit it by using the ASDM features, especially in the **Configuration > Features > VPN** section.

Gathering Information

Before you launch the VPN wizard, gather the information needed to configure the VPN tunnel. To do so, use the section that names the tunnel type you want to configure.

- Site-to-Site VPN Tunnels
- Remote Access Using Locally Stored User Accounts
- Remote Access Using AAA Server Group for Client Authentication

Site-to-Site VPN Tunnels

When you configure a site-to-site VPN tunnel using the VPN wizard, you need to have the following information before you begin.

Note When recording these values, take note of the associated number. These numbers mirror the step numbers that appear in the VPN Wizard that you run after assembling this data.

1. VPN Tunnel Type

   Interface for the site-to-site VPN tunnel (for example, “inside” or “outside”)—Before you can configure a VPN tunnel, you configure interfaces for the security appliance. When you configure the tunnel, you select an interface to associate with the VPN tunnel you are configuring.

2. Remote Site Peer

   IP address of peer device at the other end of the tunnel

   Optional name for the tunnel group (which defaults to the peer’s IP address)

   Authentication type (preshared key or digital certificate). You also need one of the following:

   - If preshared, the name of the key.
   - If digital certificate, the certificate signing algorithm (RSA or DSA), and the name of the trustpoint.

     See “Key Pairs” for the differences between the RSA and DSA algorithm.

     A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

     Note If you choose the digital certificate authentication type, configure the trustpoints (see the “Creating the Trustpoint” section on page 4-54) before running the VPN wizard.

3. IPSec Phase 1 Internet Key Exchange Security Association policy to be used to negotiate the tunnel, which consists of the following:
   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is 3DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

     Diffie Hellman Group, which must be the same for both devices—group 1, group 2, group 5, or group 7. The default is group 2.
4. IPSec Phase 2 Encryption and Authentication policy to be applied to the VPN tunnel. The parameters and options consist of the following:
   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is 3DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.
5. Local Hosts and Networks—Hosts and networks at the local site of the IP connection. You have the following options for specifying the hosts and networks at the local site of the IP connection:
   - IP address. You need the following information if you choose this option:

     Interface name—The interface, such as “inside” or “outside,” to which the host is connected.

     IP address—Any, the address of a specific local host, or a subnet. If you choose any, the IP address and subnet mask become 0.0.0.0.

     Subnet mask—Values range from 255.255.255.255 to 0.0.0.0.
   - Name of the host already present in the ASA configuration.
   - Group containing lists of networks or hosts to protect. You need the following information if you choose this option:

     Name of the host already present in the ASA configuration.

     Name of the group already present in the ASA configuration.

Note To configure host/networks group names, go to **Configuration > Global Objects > Hosts/Networks**.

6. Remote hosts and networks—Hosts and networks at the remote site of the IP connection.

   The options are the same as those for the local hosts and networks.

After preparing the information described in this section, go to “Running the VPN Wizard.”

Remote Access Using Locally Stored User Accounts

Prepare the following information for a remote access VPN tunnel requiring login accounts to be stored in the ASA configuration:

Note When recording these values, take note of the associated number. These numbers mirror the step numbers that appear in the VPN Wizard.

1. VPN Tunnel Type

   Interface for the site-to-site VPN tunnel (for example, “inside” or “outside”)—Before you can configure a VPN tunnel, you configure interfaces for the security appliance. When you configure the tunnel, you select an interface to associate with the VPN tunnel you are configuring.

2. Remote Access Client

   Use the default setting (Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product) to specify the type of VPN client supported for tunnels to this ASA. This release does not support other options.

3. VPN Tunnel Group Name and Authentication Method

   Name for the tunnel group to be used for both the remote clients and the ASA. The group name specifies common connection and client settings to be specified in the next steps.

   Authentication type (preshared key or digital certificate). You also need one of the following:

   - If preshared, the name of the key.
   - If digital certificate, the certificate signing algorithm (RSA or DSA), and the name of the trustpoint.

     See “Key Pairs” for the differences between the RSA and DSA algorithm.

     A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

     Note If you choose the digital certificate authentication type, configure the trustpoints (Configuration > Properties > Certificate > Trustpoint) before running the VPN wizard.

4. Client Authentication, which provides a choice of one of the following options:

   - Authenticate using the local (internal) user database

     This option lets you populate the ASA configuration with user accounts.

   - Authenticate using an AAA server group

     This option let you select an AAA server group to handle client authentication. Go to this same step in the next section if you choose this option.

5. User Accounts

   If you chose “Authenticate using the local (internal) user database,” list the login name and respective password for each user to be inserted into the local database.

6. Address Pool

   You can select the name of an IP address pool already present in the ASA configuration or specify a new one. If you specify a new one, you need a new pool name, the associated IP address range, and optionally a subnet mask.

7. (Optional) Attributes Pushed to Client

   You can choose to push the following attributes to the VPN client when it connects:

   - IP addresses of primary and secondary DNS servers
   - IP addresses of primary and secondary WINS servers
   - Default domain name

8. IPSec Phase 1 Internet Key Exchange Security Association policy to be used to negotiate the tunnel, which consists of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is 3DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

     Diffie Hellman Group, which must be the same for both devices—group 1, group 2, group 5, or group 7. The default is group 2.

9. IPSec Phase 2 Encryption and Authentication policy to be applied to the VPN tunnel. The parameters and options consist of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is 3DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

10. (Optional) Address Translation Exemption and Split Tunneling

    Hosts and networks in the internal network to expose to authenticated remote users of the VPN. Specify none to expose the entire internal network to authenticated remote users in the tunnel, or specify the internal addresses to expose to them and leave Network Address Translation to hide the remainder. You have the following options for specifying the internal addresses of the hosts and networks at the local site of the IP connection:

    - IP address. You need the following information if you choose this option:

      Interface name—The interface, such as “inside” or “outside,” to which the host is connected.

      IP address—Any, the address of a specific local host, or a subnet. If you choose any, the IP address and subnet mask become 0.0.0.0.

      Subnet mask—Values range from 255.255.255.255 to 0.0.0.0.
    - Name of the host already present in the ASA configuration.
    - Group containing lists of networks or hosts to protect. You need the following information if you choose this option:

      Name of the host already present in the ASA configuration.

      Name of the group already present in the ASA configuration.

Note To configure host/networks group names, go to **Configuration > Global Objects > Hosts/Networks**.

Split Tunneling—enable to provide VPN users with unencrypted access to the Internet, or leave disabled.

Note If you enable split tunneling, the hosts identified above also serve as the split tunnel access list.

After preparing the information described in this section, go to "Running the VPN Wizard."

Remote Access Using AAA Server Group for Client Authentication

Prepare the following information for a remote access VPN tunnel requiring client authentication using a AAA server group:

Note When recording these values, take note of the associated number. These numbers mirror the step numbers that appear in the VPN Wizard.

1. VPN Tunnel Type

   Interface for the site-to-site VPN tunnel (for example, "inside" or "outside")—Before you can configure a VPN tunnel, you configure interfaces for the security appliance. When you configure the tunnel, you select an interface to associate with the VPN tunnel you are configuring.

2. Remote Access Client

   Use the default setting (Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product) to specify the type of VPN client supported for tunnels to this ASA. This release does not support other options.

3. VPN Tunnel Group Name and Authentication Method

   Name for the tunnel group to be used for both the remote clients and the ASA. The group name specifies common connection and client settings to be specified in the next steps.

   Authentication type (preshared key or digital certificate). You also need one of the following:

   - If preshared, the name of the key.
   - If digital certificate, the certificate signing algorithm (RSA or DSA), and the name of the trustpoint.

     See "Key Pairs" for the differences between the RSA and DSA algorithm.

     A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

     Note If you choose the digital certificate authentication type, configure the trustpoints (Configuration > Properties > Certificate > Trustpoint) before running the VPN wizard.

4. Client Authentication, which provides a choice of one of the following options:

   - Authenticate using the local (internal) user database

     This option lets you populate the ASA configuration with user accounts. Continue with Step 5 in the previous section if you choose this option.

   - Authenticate using an AAA server group

If you choose this option, select the name of an AAA server group you already added to the configuration or create a new one. The **Configuration > Properties > AAA Setup** path lets you examine and manage the AAA server configuration. The Client Authentication panel in the VPN Wizard that provides these authentication options also provides a **New** button that lets you create a AAA server group. If you choose this option, be ready to give the group a name, choose an authentication protocol (RADIUS, TACACS+, SDI, NT, or Kerberos), specify the IP address of the server, choose the interface (such as "inside" or "outside," and specify the server secret key.

5. Address Pool

   You can select the name of an IP address pool already present in the ASA configuration or specify a new one. If you specify a new one, you need a new pool name, the associated IP address range, and optionally a subnet mask.

6. (Optional) Attributes Pushed to Client

   You can choose to push the following attributes to the VPN client when it connects:

   - IP addresses of primary and secondary DNS servers
   - IP addresses of primary and secondary WINS servers
   - Default domain name

7. IPSec Phase 1 Internet Key Exchange Security Association policy to be used to negotiate the tunnel, which consists of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is 3DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

     Diffie Hellman Group, which must be the same for both devices—group 1, group 2, group 5, or group 7. The default is group 2.

8. IPSec Phase 2 Encryption and Authentication policy to be applied to the VPN tunnel. The parameters and options consist of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is 3DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

9. (Optional) Address Translation Exemption and Split Tunneling

   Hosts and networks in the internal network to expose to authenticated remote users of the VPN. Specify none to expose the entire internal network to authenticated remote users in the tunnel, or specify the internal addresses to expose to them and leave Network Address Translation to hide the remainder. You have the following options for specifying the internal addresses of the hosts and networks at the local site of the IP connection:

   - IP address. You need the following information if you choose this option:

     Interface name—The interface, such as "inside" or "outside," to which the host is connected.

     IP address—Any, the address of a specific local host, or a subnet. If you choose any, the IP address and subnet mask become 0.0.0.0.

     Subnet mask—Values range from 255.255.255.255 to 0.0.0.0.

   - Name of the host already present in the ASA configuration.

– Group containing lists of networks or hosts to protect. You need the following information if you choose this option:

  Name of the host already present in the ASA configuration.

  Name of the group already present in the ASA configuration.

Note To configure host/networks group names, go to **Configuration > Global Objects > Hosts/Networks**.

Split Tunneling—enable to provide VPN users with unencrypted access to the Internet, or leave disabled.

Note If you enable split tunneling, the hosts identified above also serve as the split tunnel access list.

After preparing the information described in this section, go to "Running the VPN Wizard."

Running the VPN Wizard

To run the VPN wizard, follow these steps:

Step 1 Go to **Wizards > VPN Wizard**.

Step 2 Select the type of tunnel to set up: **Site to Site** or **Remote Access**.

Step 3 Select **Inside** or **Outside** next to the VPN Tunnel Interface.

Step 4 Click **Next** and follow the instructions in the VPN wizard. For more information, click **Help**.

Saving the Configuration

As you work, remember to save the changes to Flash memory to retain them, as follows:

- ASDM—Select **File > Save Running Configuration to Flash**.
- CLI—Enter the **write memory** command.

Displaying the Configuration

You can enter either of the following commands to display the current configuration settings:

- hostname# **show config**

  Enter this command to show the startup configuration saved to flash memory.
- hostname# **show running-config**

  Enter this command to show the operating configuration.
- hostname# **show running config all**

  Enter this command to show the operating configuration including attributes that have default values.

Note The first two commands are equivalent if you have saved the configuration changes you made.

You can also type **show run ?** to display a detailed list of the show configuration commands you can enter to retrieve a more refined list.

Using ASDM to Learn the CLI

The ASDM **Options > Preferences** window provides a "Preview commands before sending to the device" option. If you enable this option, ASDM displays the equivalent CLI commands in the Preview CLI Commands window whenever you click **Apply**.

View the commands, click **OK**, and then click **Proceed** in the confirmation window to save the changes to the running configuration.