CHAPTER 6

VPN Wizards

The ASA provides Secure Socket Layer (SSL) remote access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. Clientless, browser-based VPN lets users establish a secure, remote-access VPN tunnel to the adaptive security appliance using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. Users have no direct access to resources on the internal network.

The Cisco AnyConnect VPN client provides secure SSL connections to the ASA for remote users with full VPN tunneling to corporate resources. Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept clientless VPN connections. The ASA downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure connection and either remains or uninstalls itself (depending on the ASA configuration) when the connection terminates. In the case of a previously installed client, when the user authenticates, the ASA examines the revision of the client and upgrades the client as necessary.

With the addition of IKEv2 support in release 8.4, the end user can have the same experience independent of the tunneling protocol used by the AnyConnect client session. This addition allows other vendors' VPN clients to connect to the ASAs. This support enhances security and complies with the IPsec remote access requirements defined in federal and public sector mandates.

The VPN wizard lets you configure basic LAN-to-LAN and remote access VPN connections and assign either preshared keys or digital certificates for authentication. Use ASDM to edit and configure advanced features.

VPN Overview

The ASA creates a Virtual Private Network by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. It can create single-user-to-LAN connections and LAN-to-LAN connections.

For LAN-to-LAN connections using both IPv4 and IPv6 addressing, the security appliance supports VPN tunnels if both peers are Cisco ASA 5500 series security appliances, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6). This is also true if both peer inside networks are IPv6 and the outside network is IPv6.

The secure connection is called a tunnel, and the ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA functions as a bidirectional tunnel endpoint: it can receive plain

packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination.

The four VPN wizards described in this section are as follows:

- IPsec IKEv1 Remote Access Wizard
- IPsec Site-to-Site VPN Wizard
- AnyConnect VPN Wizard
- Clientless SSL VPN Wizard

IPsec IKEv1 Remote Access Wizard

Use the IKEv1 Remote Access Wizard to select remote access or LAN-to-LAN and to identify the interface that connects to the remote IPsec peer. The tunnel type is automatically selected when the wizard is started.

Fields

- Remote Access—Click to create a configuration that achieves secure remote access for VPN clients, such as mobile users. This option lets remote users securely access centralized network resources. When you select this option, the VPN wizard displays a series of panes that let you enter the attributes a remote access VPN requires.
- VPN Tunnel Interface—Choose the interface that establishes a secure tunnel with the remote IPsec peer. If the ASA has multiple interfaces, you need to plan the VPN configuration before running this wizard, identifying the interface to use for each remote IPsec peer with which you plan to establish a secure connection.
- Enable inbound IPsec sessions to bypass interface access lists—Enable IPsec authenticated inbound sessions to always be permitted through the security appliance (that is, without a check of the interface access-list statements). Be aware that the inbound sessions bypass only the interface ACLs. Configured group-policy, user, and downloaded ACLs still apply.

Remote Access Client

Remote access users of various types can open VPN tunnels to this ASA. Choose the type of VPN client for this tunnel.

Fields

- VPN Client Type
  - Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product
  - Microsoft Windows client using L2TP over IPsec—Specify the PPP authentication protocol. The choices are PAP, CHAP, MS-CHAP-V1, MS-CHAP-V2, and EAP-PROXY:

    PAP—Passes cleartext username and password during authentication and is not secure.

    CHAP—In response to the server challenge, the client returns the encrypted [challenge plus password] with a cleartext username. This protocol is more secure than the PAP, but it does not encrypt data.

MS-CHAP, Version 1—Similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP.

MS-CHAP, Version 2—Contains security enhancements over MS-CHAP, Version 1.

EAP-Proxy—Enables EAP which permits the ASA to proxy the PPP authentication process to an external RADIUS authentication server.

If a protocol is not specified on the remote client, do no specify it.

Specify if the client will send tunnel group name as username@tunnelgroup.

VPN Client Authentication Method and Tunnel Group Name

Use the VPN Client Authentication Method and Name pane to configure an authentication method and create a connection policy (tunnel group).

Fields

- Authentication Method—The remote site peer authenticates either with a preshared key or a certificate.
  - Pre-shared Key—Click to use a preshared key for authentication between the local ASA and the remote IPsec peer.

    Using a preshared key is a quick and easy way to set up communication with a limited number of remote peers and a stable network. It may cause scalability problems in a large network because each IPsec peer requires configuration information for each peer with which it establishes secure connections.

    Each pair of IPsec peers must exchange preshared keys to establish secure tunnels. Use a secure method to exchange the preshared key with the administrator of the remote site.
  - Pre-shared Key—Type an alphanumeric string between 1 and 128 characters.
  - Certificate—Click to use certificates for authentication between the local ASA and the remote IPsec peer. To complete this section, you must have previously enrolled with a CA and downloaded one or more certificates to the ASA.

    You can efficiently manage the security keys used to establish an IPsec tunnel with digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the public key.

    To use digital certificates, each peer enrolls with a certification authority (CA), which is responsible for issuing digital certificates. A CA can be a trusted vendor or a private CA that you establish within an organization.

    When two peers want to communicate, they exchange certificates and digitally sign data to authenticate each other. When you add a new peer to the network, it enrolls with a CA, and none of the other peers require additional configuration.

    Certificate Signing Algorithm—Displays the algorithm for signing digital certificates, rsa-sig for RSA.
  - Challenge/response authentication (CRACK)—Provides strong mutual authentication when the client authenticates using a popular method such as RADIUS and the server uses public key authentication. The security appliance supports CRACK as an IKE option in order to authenticate the Nokia VPN Client on Nokia 92xx Communicator Series devices.

- Tunnel Group Name—Type a name to create the record that contains tunnel connection policies for this IPsec connection. A connection policy can specify authentication, authorization, and accounting servers, a default group policy, and IKE attributes. A connection policy that you configure with this VPN wizard specifies an authentication method and uses the ASA Default Group Policy.

Client Authentication

Use the Client Authentication pane to select the method by which the ASA authenticates remote users.

Fields

Select one of the following options:

- Authenticate using the local user database—Click to use authentication internal to the ASA. Use this method for environments with a small, stable number of users. The next pane lets you create accounts on the ASA for individual users.
- Authenticate using an AAA server group—Click to use an external server group for remote user authentication.
  - AAA Server Group Name—Choose a AAA server group configured previously.
  - New...—Click to configure a new AAA server group.

User Accounts

Use the User Accounts pane to add new users to the ASA internal user database for authentication purposes.

Fields

- Use the fields in this section to add a user.
  - Username—Enter the username.
  - Password—(Optional) Enter a password.
  - Confirm Password—(Optional) Reenter the password.
- Add—Click to add a user to the database after you have entered the username and optional password.
- Delete—To remove a user from the database, highlight the appropriate username and click **Delete**.

Address Pool

Use the Address Pool pane to configure a pool of local IP addresses that the ASA assigns to remote VPN clients.

Fields

- Tunnel Group Name—Displays the name of the connection policy to which the address pool applies. You set this name in the VPN Client Name and Authentication Method pane.
- Pool Name—Select a descriptive identifier for the address pool.
- New...—Click to configure a new address pool.

- Range Start Address—Type the starting IP address in the address pool.
- Range End Address—Type the ending IP address in the address pool.
- Subnet Mask—(Optional) Choose the subnet mask for these IP addresses.

Attributes Pushed to Client (Optional)

Use the Attributes Pushed to Client (Optional) pane to have the ASA pass information about DNS and WINS servers and the default domain name to remote access clients.

Fields

- Tunnel Group—Displays the name of the connection policy to which the address pool applies. You set this name in the VPN Client Name and Authentication Method pane.
- Primary DNS Server—Type the IP address of the primary DNS server.
- Secondary DNS Server—Type the IP address of the secondary DNS server.
- Primary WINS Server—Type the IP address of the primary WINS server.
- Secondary WINS Server— Type the IP address of the secondary WINS server.
- Default Domain Name—Type the default domain name.

IKE Policy

IKE, also called Internet Security Association and Key Management Protocol (ISAKMP), is the negotiation protocol that lets two hosts agree on how to build an IPsec Security Association. Each IKE negotiation is divided into two sections called Phase1 and Phase 2.

- Phase 1 creates the first tunnel, which protects later IKE negotiation messages.
- Phase 2 creates the tunnel that protects data.

Use the IKE Policy pane to set the terms of the Phase 1 IKE negotiations, which include the following:

- An encryption method to protect the data and ensure privacy.
- An authentication method to ensure the identity of the peers.
- A Diffie-Hellman group to establish the strength of the of the encryption-key-determination algorithm. The ASA uses this algorithm to derive the encryption and hash keys.

Fields

- Encryption—Select the symmetric encryption algorithm the ASA uses to establish the Phase 1 SA that protects Phase 2 negotiations. The ASA supports the following encryption algorithms:

Algorithm	Explanation
DES	Data Encryption Standard. Uses a 56-bit key.
3DES	Triple DES. Performs encryption three times using a 56-bit key.
AES-128	Advanced Encryption Standard. Uses a 128-bit key.
AES-192	AES using a 192-bit key.
AES-256	AES using a 256-bit key.

The default, 3DES, is more secure than DES but requires more processing for encryption and decryption. Similarly, the AES options provide increased security but also require increased processing.

- Authentication—Choose the hash algorithm used for authentication and ensuring data integrity. The default is SHA. MD5 has a smaller digest and is considered to be slightly faster than SHA. There has been a demonstrated successful (but extremely difficult) attack against MD5. However, the Keyed-Hash Message Authentication Code (HMAC) version used by the ASA prevents this attack.
- Diffie-Hellman Group—Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The default, Group 2 (1024-bit Diffie-Hellman), requires less CPU time to execute but is less secure than Group 5 (1536-bit).

Note The default value for the VPN 3000 Series Concentrator is MD5. A connection between the ASA and the VPN Concentrator requires that the authentication method for Phase I and II IKE negotiations be the same on both sides of the connection.

IPsec Settings (Optional)

Use the IPsec Settings (Optional) pane to identify local hosts/networks which do not require address translation. By default, the ASA hides the real IP addresses of internal hosts and networks from outside hosts by using dynamic or static Network Address Translation (NAT). NAT minimizes risks of attack by untrusted outside hosts but may be improper for those who have been authenticated and protected by VPN.

For example, an inside host using dynamic NAT has its IP address translated by matching it to a randomly selected address from a pool. Only the translated address is visible to the outside. Remote VPN clients that attempt to reach these hosts by sending data to their real IP addresses cannot connect to these hosts, unless you configure a NAT exemption rule.

Note If you want all hosts and networks to be exempt from NAT, configure nothing on this pane. If you have even one entry, all other hosts and networks are subject to NAT.

Fields

- Interface—Choose the name of the interface that connects to the hosts or networks you have selected.
- Exempt Networks—Select the IP address of the host or network that you want to exempt from the chosen interface network.
- Enable split tunneling—Select to have traffic from remote access clients destined for the public Internet sent unencrypted. Split tunneling causes traffic for protected networks to be encrypted, while traffic to unprotected networks is unencrypted. When you enable split tunneling, the ASA pushes a list of IP addresses to the remote VPN client after authentication. The remote VPN client encrypts traffic to the IP addresses that are behind the ASA. All other traffic travels unencrypted directly to the Internet without involving the ASA.
- Enable Perfect Forwarding Secrecy (PFS)—Specify whether to use Perfect Forward Secrecy, and the size of the numbers to use, in generating Phase 2 IPsec keys. PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless PFS is enabled. PFS uses Diffie-Hellman techniques to generate the keys.

PFS ensures that a session key derived from a set of long-term public and private keys is not compromised if one of the private keys is compromised in the future.

PFS must be enabled on both sides of the connection.

- Diffie-Hellman Group—Select the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The default, Group 2 (1024-bit Diffie-Hellman), requires less CPU time to execute but is less secure than Group 5 (1536-bit).

Summary

The Summary pane displays all of the attributes of this VPN LAN-to-LAN connection as configured.

Fields

Back—To make changes, click **Back** until you reach the appropriate pane.

Finish—When you are satisfied with the configuration, click **Finish**. ASDM saves the LAN-to-LAN configuration. After you click **Finish**, you can no longer use the VPN wizard to make changes to this configuration. Use ASDM to edit and configure advanced features.

Cancel—To remove the configuration, click **Cancel**.

IPsec Site-to-Site VPN Wizard

Use this wizard to set up new site-to-site VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.

Peer Device Identification

Identify the peer VPN device by its IP address and the interface used to access the peer.

Fields

- Peer IP Address—Configure the IP address of the peer device.
- VPN Access Interface—Use the drop-down to specify the interface for the site-to-site tunnel.

IKE Version

ASA supports both version 1 and version 2 of the IKE (Internet Key Exchange) protocol. This step lets you decide which version or versions to support in this connection profile.

Fields

- IKEv1
- IKEv2

Traffic to Protects

This step lets you identify the local network and remote network These networks protect the traffic using IPsec encryption.

Fields

- Network Type—Choose IPv4 or IPv6.
- Local Networks—Identify the host used in the IPsec tunnel.
- Remote Networks—Identify the networks used in the IPsec tunnel.

Authentication Methods

This step lets you configure the methods to authenticate with the peer device.

Fields

IKE version 1

- Pre-shared Key—Using a preshared key is a quick and easy way to set up communication with a limited number of remote peers and a stable network. It may cause scalability problems in a large network because each IPsec peer requires configuration information for each peer with which it establishes secure connections.

  Each pair of IPsec peers must exchange preshared keys to establish secure tunnels. Use a secure method to exchange the preshared key with the administrator of the remote site.
- Device Certificate—Click to use certificates for authentication between the local ASA and the remote IPsec peer.

  You can efficiently manage the security keys used to establish an IPsec tunnel with digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the public key.

  When two peers want to communicate, they exchange certificates and digitally sign data to authenticate each other. When you add a new peer to the network, it enrolls with a CA, and none of the other peers require additional configuration.

IKE version 2

- Local Pre-shared Key—Specify IPsec IKEv2 authentication methods and encryption algorithms.
- Local Device Certificate—Authenticates VPN access through the security appliance.
- Remote Peer Pre-shared Key—Click to use a preshared key for authentication between the local ASA and the remote IPsec peer.
- Remote Peer Certificate Authentication—When checked, the peer device is allowed to use the certificate to authenticate itself to this device.

Encryption Algorithm

This step lets you select the types of encryption algorithms used to protect the data.

Fields

IKE version 1

- IKE Policy—Specify IKEv1 authentication methods.
- IPsec Proposal—Specify IPsec encryption algorithms.

IKE version 2

- IKE Policy—Specify IKEv2 authentication methods.
- IPsec Proposal—Specify IPsec encryption algorithms.

Miscellaneous

You can enable or disable Perfect Forward Secrecy (PFS). PFS ensures that the key for a given IPsec SA was not derived from any other secret. PFS makes it difficult to break a key by deriving from other keys.

Fields

- Enable inbound IPsec sessions to bypass interface access lists—Enable IPsec authenticated inbound sessions to always be permitted through the security appliance (that is, without a check of the interface access-list statements). Be aware that the inbound sessions bypass only the interface ACLs. Configured group-policy, user, and downloaded ACLs still apply.
- Enable Perfect Forward Secrecy (PFS)—Ensures the key for a given IPsec SA was not derived from any other secret.
- Diffie-Hellman Group—Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The default, Group 2 (1024-bit Diffie-Hellman), requires less CPU time to execute but is less secure than Group 5 (1536-bit).
- Exempt ASA side host/network from address translation—Use the drop-down to choose a host or network to be excluded from address translation.

Summary

Provides a summary of your selections from the previous wizard windows. The supported VPN protocols are included in the summary as well as the IKE version chosen on the VPN Connection Type window.

AnyConnect VPN Wizard

Use this wizard to configure ASA to accept VPN connections from the AnyConnect VPN client. This wizard configures either IPsec (IKEv2) or SSL VPN protocols for full network access. The ASA automatically uploads the AnyConnect VPN client to the end user's device when a VPN connection is established.

Warn the user that running the wizard does not mean the IKEv2 profile automatically applies in predeployment scenarios. Either provide a pointer or the steps necessary to successfully predeploy IKEv2.

Connection Profile Identification

The connection profile identification is used to identify the ASA to the remote acess users.

Fields

- Connection Profile Name—Provide a name that the remote access users will access for VPN connections.
- VPN Access Interface—Choose an interface that the remote access users will access for VPN connections.

VPN Protocols

Specify the VPN protocol allowed for this connection profile.

The AnyConnect client defaults to SSL. If you enable IPsec as a VPN tunnel protocol for the connection profile, you must also create and deploy a client profile with IPsec enabled using the profile editor from ASDM, and deploy the profile.

If you predeploy instead of weblaunch the AnyConnect client, the first client connection uses SSL, and receives the client profile from the ASA during the session. For subsequent connections, the client uses the protocol specified in the profile, either SSL or IPsec. If you predeploy the profile with IPsec specified with the client, the first client connection uses IPsec. For more information about predeploying a client profile with IPsec enabled, see the AnyConnect Secure Mobility Client Administrator Guide.

Fields

- SSL
- IPsec (IKE v2)
- Device Certificate—Identifies the ASA to the remote access clients.

  Note Some AnyConnect features (such as always on, IPsec/IKEv2) require a valid device certificate on the ASA.

- Manage—Choosing **Manage** opens the Manage Identity Certificates window.
  - Add—Choose **Add** to add an identity certificate and its details.
  - Show Details—If you choose a particular certificate and click **Show Details**, the Certificate Details window appears and provides who the certificate was issued to and issued by, as well as specifics about its serial number, usage, associated trustpoints, valid timeframe, and so on.
  - Delete—Highlight the certificate you want to remove and click **Delete**.
  - Export—Highlight the certificate and click **Export** to export the certificate to a file with or without an encryption passphrase.
  - Enroll ASA SSL VPN with Entrust—Gets your Cisco ASA SSL VPN appliance up and running quickly with an SSL Advantage digitial certificate from Entrust.

Client Images

ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network. You can use a regular expression to match the user agent of a browser to an image. You can also minimize connection setup time by moving the most commonly encountered operation system to the top of the list.

Fields

- Add
- Replace
- Delete

Authentication Methods

Specify authentication information on this screen.

Fields

- AAA server group—Enable to let the ASA contact a remote AAA server group to authenticate the user. Select a AAA server group from the list of pre-configured groups or click **New** to create a new group.
- Local User Database Details—Add new users to the local database stored on the ASA.
  - Username—Create a username for the user.
  - Password—Create a password for the user.
  - Confirm Password—Re-type the same password to confirm.
  - Add/Delete—Add or delete the user from the local database.

Client Address Assignment

Provide a range of IP addresses to remote SSL VPN users.

Fields

- IPv4 Address Pools—SSL VPN clients receive new IP addresses when they connect to the ASA. Clientless connections do not require new IP addresses. Address Pools define a range of addresses that remote clients can receive. Select an existing IP Address Pool or click **New** to create a new pool.

  If you select **New**, you will have to provide a starting and ending IP address and subnet mask.
- IPv6 Address Pool—Select an existing IP Address Pool or click **New** to create a new pool.

Note This option is not available with IKEv2 connection profiles.

Network Name Resolution Servers

This step lets you specify which domain names are resolved for the remote user when accessing the internal network.

Fields

- DNS Servers—Enter the IP address of the DNS server.
- WINS Servers—Enter the IP address of the WINS server.
- Domain Name—Type the default domain name.

NAT Exempt

If network translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

Fields

- Exempt VPN traffic from network address translation

AnyConnect Client Deployment

You can install the AnyConnect client program to a client device with one of the following two methods:

- Web launch—Installs automatically when accessing the ASA using a web browser.
- Pre-deployment—Manually installs the AnyConnect client package.

Fields

- Allow Web Launch—A global setting that affects all connections. If it is unchecked (disallowed), AnyConnect SSL connections and clientless SSL connections do not work.

For pre-deployment, the disk0:/test2_client_profile.xml profile bundle contains an .msi file, and you must include this client profile from the ASA in your AnyConnect package to ensure IPsec connection functions as expected.

Summary

Provides a summary of your selections from the previous wizard windows. The supported VPN protocols are part of the summary as well as the IKE version chosen.

Clientless SSL VPN Wizard

This wizard enables clientless, browser-based connections for specific, supported internal resources through a portal page.

SSL VPN Interface

Provide a connection profile and the interface that SSL VPN users connect to.

Fields

- Connection Profile Name
- SSL VPN Interface—The interface users access for SSL VPN connections.
- Digital Certificate—Specifies what the security appliance sends to the remote web browser to authenticate the ASA.
  - Certificate—Choose from the drop-down menu.
- Accessing the Connection Profile
  - Connection Group Alias/URL—The group alias is chosen during login from the Group drop-down list. This URL is entered into the web browser.
  - Display Group Alias list at the login page

User Authentication

Specify authentication information on this screen.

Fields

- Authenticate using a AAA server group—Enable to let the ASA contact a remote AAA server group to authenticate the user.
  - AAA Server Group Name—Select a AAA server group from the list of pre-configured groups or click **New** to create a new group.
- Authenticate using the local user database—Add new users to the local database stored on the ASA.
  - Username—Create a username for the user.
  - Password—Create a password for the user.
  - Confirm Password—Re-type the same password to confirm.
  - Add/Delete—Add or delete the user from the local database.

Group Policy

Group policies configure common attributes for groups of users. Create a new group policy or select an existing one to modify.

Fields

- Create new group policy—Enables you to create a new group policy. Provide a name for the new policy.
- Modify existing group policy—Select an existing group policy to modify.

Bookmark List

Configure a list of group intranet websites that appear in the portal page as links. Some examples include https://intranet.acme.com, rdp://10.120.1.2, vnc://100.1.1.1 and so on.

Fields

- Bookmark List

- Manage

Summary

Provides a summary of your selections from the previous wizard windows.