

VPN Wizards

- VPN Overview, on page 1
- IPsec Site-to-Site VPN Wizard, on page 2
- **AnyConnect Client VPN Wizard**, on page 4
- IPsec IKEv1 Remote Access Wizard, on page 6
- IPsec IKEv2 Remote Access Wizard, on page 10

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.

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 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.

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

- AnyConnect Client VPN Wizard, on page 4

  The Cisco AnyConnect VPN client provides secure SSL or IPsec (IKEv2) 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.

  The AnyConnect Client VPN wizard will be available only in the User Contexts when ASA is in multi-context mode. The Storage and Resource Class for the required context must be configured from the System Context.

Storage per context is required to have Cisco AnyConnect Client Package and Profile files. Resource Class is required for license allotment for each context. The license utilized is AnyConnect Client Premium.

Note The rest of the configuration for this wizard remains the same as single-context.

- IPsec IKEv2 Remote Access Wizard, on page 10

  IKEv2 allows other vendors' VPN clients to connect to the ASAs. This enhances security and complies with the IPsec remote access requirements defined in federal and public sector mandates.

  The IPSec IKEv2 Remote Access wizard will be available only in the User Contexts when ASA is in multi-context mode. Resource Class for the required context must be configured from the System Context for license allotment. The license utilized is the AnyConnect Client Premium.

Note The rest of the configuration for this wizard remains the same as single-context.

- IPsec IKEv1 Remote Access Wizard, on page 6
- IPsec Site-to-Site VPN Wizard, on page 2

  For LAN-to-LAN connections using both IPv4 and IPv6 addressing, the ASA supports VPN tunnels if both peers are ASAs, 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.

IPsec Site-to-Site VPN Wizard

A tunnel between two ASA 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

- Peer IP Address—Configure the IP address of the other site (peer device).
- VPN Access Interface—Select the interface to use for the site-to-site tunnel.
- Crypto Map Type—Specify the type of maps that will be used for this peer, static or dynamic.

Traffic to Protect

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

- Local Networks—Identify the host used in the IPsec tunnel.
- Remote Networks—Identify the networks used in the IPsec tunnel.

Security

This step lets you configure the methods to authenticate with the peer device. You can either choose the simple configuration, and supply a preshared key. Or you can choose Customized Configuration for more advanced options, as follows:

- IKE Version—Check the IKEv1 or IKEv2 check box according to which version you want to use.
- IKE version 1 Authentication Methods
  - 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 Authentication Methods
  - 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—Enter 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 Algorithms—This tab lets you choose the types of encryption algorithms used to protect the data.
  - IKE Policy—Specify IKEv1/IKEv2 authentication methods.
  - IPsec Proposal—Specify IPsec encryption algorithms.
- Perfect Forward Secrecy
  - 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 14 (2048 -bit Diffie-Hellman).

NAT Exempt

- Exempt ASA side host/network from address translation—Use the drop-down list to choose a host or network to be excluded from address translation.

AnyConnect Client 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.

Connection Profile Identification

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

- 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 *Secure Client Administrator Guide*.

- SSL
- IPsec (IKE v2)
- Device Certificate—Identifies the ASA to the remote access clients. Some AnyConnect Client 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 ASA SSL VPN appliance up and running quickly with an SSL Advantage digital certificate from Entrust.

Client Images

ASA can automatically upload the latest AnyConnect Client 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.

Authentication Methods

Specify authentication information on this screen.

- 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 AnyConnect Client users.

- 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 choose **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 IPv6 address pools can not be created for IKEv2 connection profiles.

Network Name Resolution Servers

Specify which domain names are resolved for the remote user when accessing the internal network.

- 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.

AnyConnect Client Deployment

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

- Web launch—The AnyConnect Client package installs automatically when accessing the ASA using a web browser.



Note Web launch is not supported in multiple-context mode.

- Pre-deployment—Manually install the AnyConnect Client package.

Allow Web Launch is a global setting that affects all connections. If it is unchecked (disallowed), AnyConnect Client 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 Client package to ensure IPsec connection functions as expected.

IPsec IKEv1 Remote Access Wizard



Note The Cisco VPN Client is end-of-life and end-of-support. You must upgrade to the Secure Client.

Use the IKEv1 Remote Access Wizard to configure secure remote access for VPN clients, such as mobile users, and to identify the interface that connects to the remote IPsec peer.

- VPN Tunnel Interface—Choose the interface to use for remote access clients. If the ASA has multiple interfaces, stop now and configure the interfaces on the ASA before running this wizard.
- Enable inbound IPsec sessions to bypass interface access lists—Enable IPsec authenticated inbound sessions to always be permitted through the ASA (that is, without checking 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.

- VPN Client Type

- 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 the 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 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 the 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).

- 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 pre-shared 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.

- 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 choose the method by which the ASA authenticates remote users. 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.

Address Pool

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

- Tunnel Group Name—Displays the name of the connection profile (tunnel group) to which this address pool applies. You set this name in the VPN Client and Authentication Method pane (step 3).
- 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.

- 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 includes an encryption method to protect the data and ensure privacy, an authentication method to ensure the identity of the peers, and 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.

- 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 DH Group 14 (2048 -bit) is considered as more secure than Group 2 and Group 5.

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.

- 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 DH Group 14 (2048 -bit) is considered as more secure than Group 2 and Group 5.

Summary

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.

IPsec IKEv2 Remote Access Wizard

Use the IKEv2 Remote Access Wizard to configure secure remote access for VPN clients, such as mobile users, and to identify the interface that connects to the remote IPsec peer.

Connection Profile Identification

Enter a **Connection Profile Name** and choose the **VPN Access Interface** that will be used for IPsec IKEv2 remote access.

- Connection Profile 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.
- VPN Access 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.

Standards Based IPSec (IKEv2) Authentication Page

IKE Peer Authentication—The remote site peer authenticates either with a preshared key or a certificate or peer authentication using EAP.

- Pre-shared Key—Type an alphanumeric string between 1 and 128 characters.

  Using a pre-shared 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.

- Enable Certificate Authentication—Allows you to use certificates for authentication if checked.
- Enable peer authentication using EAP—Allows you to use EAP for authentication if checked. You must use certificates for local authentication if you check this check box.
- Send an EAP identity request to the client—Enables you to send an EAP request for authentication to the remote access VPN client.

Mobike RRC

- Enable Return Routability Check for mobike—Enable Return Routability checking for dynamic IP address changes in IKE/IPSEC security associations on which mobike is enabled.

IKE Local Authentication

- Enable local authentication, and select either preshared key or certificate
  - Preshared 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.

Authentication Methods

Only Radius authentication is supported for IPsec IKEv2 remote access.

- AAA Server Group—Choose a AAA server group configured previously.
- New—Click to configure a new AAA server group.
- AAA Server Group Details—Use this area to modify the AAA server group if desired.

Client Address Assignment

Create or select IPv4 and IPv6 address pools. Remote access clients will be assigned addresses from either IPv4 or IPv6 pools. IPv4 addresses take precedence if both are configured. See *Configuring Local IP Address Pools* for more information.

Network Name Resolution Servers

Specify how domain names are resolved for the remote user when accessing the internal network.

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

NAT Exempt

- Exempt VPN traffic from Network Address Translation—If NAT is enabled on the ASA this must be checked.