VPN Overview

The ASA 1000V 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 LAN-to-LAN connections.

The secure connection is called a tunnel, and the ASA 1000V 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 1000V 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.

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**
- 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.
  
  - IKE version 2
    - Local Pre-shared Key—Specify IPsec IKEv2 authentication methods and encryption algorithms.
    - Remote Peer Pre-shared Key—Click to use a preshared key for authentication between the local ASA 1000V and the remote IPsec peer.

**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.