



CHAPTER 32

VPN

The security appliance 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 security appliance uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The security appliance 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 security appliance performs the following VPN functions:

- Establishes tunnels.
- Negotiates tunnel parameters.
- Enforces VPN policies.
- Authenticates users.
- Authorizes users for specific levels of use and access.
- Performs accounting functions.
- Assigns user addresses.
- Encrypts and decrypts data.
- Manages security keys.
- Manages data transfer across the tunnel.
- Manages data transfer inbound and outbound as a tunnel endpoint or router.

The security appliance invokes various standard protocols to accomplish these functions.

VPN Wizard

The VPN wizard lets you configure basic LAN-to-LAN and remote access VPN connections. Use ASDM to edit and configure advanced features.

**Note**

The VPN wizard lets you assign either preshared keys or digital certificates for authentication. However, to use certificates, you must enroll with a certification authority and configure a trustpoint prior to using the wizard. Use the ASDM Device Administration > Certificate panels and online Help to accomplish these tasks.

VPN Overview

The security appliance 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 security appliance uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The security appliance 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 security appliance performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

VPN Tunnel Type

Use the VPN Tunnel Type panel to select the type of VPN tunnel to define, remote access or LAN-to-LAN, and to identify the interface that connects to the remote IPsec peer.

Fields

- **Site-to-Site**—Click to create a LAN-to-LAN VPN configuration. Use between two IPsec security gateways, which can include security appliances, VPN concentrators, or other devices that support site-to-site IPsec connectivity. When you select this option, the VPN wizard displays a series of panels that let you to enter the attributes a site-to-site VPN requires.
- **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 panels that let you enter the attributes a remote access VPN requires.
- **VPN Tunnel Interface**—Select the interface that establishes a secure tunnel with the remote IPsec peer. If the security appliance 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.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Remote Site Peer

Use the Remote Site Peer panel for the following tasks:

1. Providing the IP address of the remote IPsec peer that terminates this VPN tunnel.
2. Selecting and configuring an authentication method.
3. Creating a connection policy (tunnel group).

Fields

- Peer IP Address—Type the IP address of the remote IPsec peer that terminates the VPN tunnel. The peer might be another security appliance, a VPN concentrator, or any other gateway device that supports IPsec.
- 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 security appliance 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 the preshared key. Maximum 127 characters.
- Certificate—Click to use certificates for authentication between the local security appliance 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 security appliance.

Digital certificates are an efficient way to manage the security keys used to establish an IPsec tunnel. 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 owner's 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.
- Certificate Name—Select the name that identifies the certificate the security appliance sends to the remote peer. This list displays trustpoints with a certificate of the type previously selected in the certificate signing algorithm list.
- 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 policy that you configure with this VPN wizard specifies an authentication method, and uses the security appliance Default Group Policy.

By default, ASDM populates this box with the value of the Peer IP address. You can change this name. Maximum 64 characters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

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 panel 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 security appliance uses this algorithm to derive the encryption and hash keys.

Fields

- Encryption—Select the symmetric encryption algorithm the security appliance uses to establish the Phase 1 SA that protects Phase 2 negotiations. The security appliance 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—Select 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 security appliance prevents this attack.
- 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). Group 7 is for use with the Movian VPN client, but works with any peer that supports Group 7 (ECC).

**Note**

The default value for the VPN 3000 Series Concentrator is MD5. A connection between the security appliance 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.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Hosts and Networks

Use the Hosts and Networks panel to identify local and remote hosts and networks that can use this LAN-to-LAN IPsec tunnel to send and receive data.

For IPsec to succeed, both peers in the LAN-to-LAN connection must have compatible entries for hosts and networks. The hosts and networks you configure as Local Hosts and Networks in this panel must be configured as Remote Hosts and Networks on the device at the remote site for the LAN-to-LAN connection. The local security appliance and the remote device must have at least one transform set in common for this LAN-to-LAN connection.

Fields

- Action—Decide whether or not to protect data travelling between the local and remote network.
- Local networks—Select the local hosts and networks.
- Remote networks—Select the remote hosts and networks.
- Exempt ASA side host/network from address translation—Allows traffic to pass through the security appliance without address translation.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Summary

The Summary panel 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 panel.

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**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Remote Access Client

Use the Remote Access Client panel to identify the type of remote access users this connection serves.

Fields

- Cisco VPN Client Release 3.x or higher, or other Easy VPN Remote product—Click for IPsec connections, including compatible software and hardware clients other than those named here.
- Microsoft Windows client using L2TP over IPsec—Click to enable connections from Microsoft Windows and Microsoft Windows Mobile clients over a public IP network. L2TP uses PPP over UDP (port 1701) to tunnel the data. Enable one or more of the following PPP authentication protocols:
 - 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 security appliance to proxy the PPP authentication process to an external RADIUS authentication server.
- Client will send the tunnel group name as username@tunnelgroup—Check to enable the security appliance to associate different users that are establishing L2TP over IPsec connections with different tunnel groups. Since each tunnel group has its own AAA server group and IP address pools, users can be authenticated through methods specific to their tunnel group.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

VPN Client Authentication Method and Name

Use the VPN Client Authentication Method and Name panel to configure an authentication method and create a 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 security appliance 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 the preshared key.
- Certificate—Click to use certificates for authentication between the local security appliance 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 security appliance.

Digital certificates are an efficient way to manage the security keys used to establish an IPsec tunnel. 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 owner's 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 Name—Select the name that identifies the certificate the security appliance sends to the remote peer.
- 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.
- 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 tunnel group that you configure with this VPN wizard specifies an authentication method, and uses the security appliance Default Group Policy.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	—	•	—	—

Client Authentication

Use the Client Authentication panel to select the method by which the security appliance authenticates remote users.

Fields

Select one of the following options:

- Authenticate using the local user database—Click to use authentication internal to the security appliance. Use this method for environments with a small, stable number of users. The next panel lets you create accounts on the security appliance for individual users.

- Authenticate using an AAA server group—Click to use an external server group for remote user authentication.
- AAA Server Group Name—Select a AAA server group configured previously.
- New ...—Click to configure a new AAA server group.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

New Authentication Server Group

User the New Authentication Server Group panel to define one or more new AAA servers.

Fields

To configure a new AAA server group that contains just one server, provide the following information:

- Server Group Name—Type a name for the server group. You associate this name with users whom you want to authenticate using this server.
- Authentication Protocol—Select the authentication protocol the server uses. Options include TACACS+, RADIUS, SDI, NT, and Kerberos.
- Server IP Address—Type the IP address for the AAA server.
- Interface—Select the security appliance interface on which the AAA server resides.
- Server Secret Key—Type a case-sensitive, alphanumeric keyword of up to 127 characters. The server and security appliance use the key to encrypt data that travels between them. The key must be the same on both the security appliance and server. You can use special characters, but not spaces.
- Confirm Server Secret Key—Type the secret key again.

To add more servers to this new group, or to change other AAA server settings, go to Configuration > Features > Properties > AAA.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

User Accounts

Use the User Accounts panel to add new users to the security appliance internal user database for authentication purposes.

Fields

Provide the following information:

- User to Be Added—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.
- Username—Displays the names of all users in the database.
- Delete—To remove a user from the database, highlight the appropriate username and click **Delete**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Address Pool

Use the Address Pool panel to configure a pool of local IP addresses that the security appliance assigns to remote VPN clients.

Fields

- Name—Displays the name of the tunnel group to which the address pool applies. You set this name in the VPN Client Name and Authentication Method panel.
- 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) Select the subnet mask for these IP addresses

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Attributes Pushed to Client

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

Fields

Provide information for remote access clients to use.

- 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 panel.
- 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. Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

IPsec Settings (Optional)

Use the IPsec Settings (Optional) panel to identify local hosts/networks which do not require address translation. By default, the security appliance 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 panel. If you have even one entry, all other hosts and networks are subject to NAT.

Fields

- **Host/Network to Be Added**—Complete these fields to exempt a particular host or network from NAT.
 - **Interface**—Select the name of the interface that connects to the hosts or networks you have selected.
 - **IP address**—Select the IP address of the host or network. Either type the IP address or click the adjacent ... button to view a diagram of the network and select a host or network.
- **Add**—Click to add the host or network the Selected Hosts/Networks list after you have completed the applicable fields.
- **Selected Hosts/Networks**—Displays the hosts and networks that are exempt from NAT. If you want all hosts and networks to be exempt from NAT, leave this list empty.
- **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 security appliance 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 security appliance. All other traffic travels unencrypted directly to the Internet without involving the security appliance.
- **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). Group 7 is for use with the Movian VPN client, but works with any peer that supports Group 7 (ECC).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

