Configuring IKE and IPsec Policies

This chapter describes how to configure Internet Protocol Security (IPsec) and the Internet Security Association and Key Management Protocol (ISAKMP, or IKE) standards to build site-to-site and remoteaccess IPsec Virtual Private Networks (VPNs). These policies are used in regular IPsec and other typesof IPsec-based VPN technologies to build VPN tunnels.

Tunneling makes it possible to use a public TCP/IP network, such as the Internet, to create secureconnections between remote users and a private corporate network. Each secure connection is called a tunnel.

IPsec-based VPN technologies use the ISAKMP and IPsec tunneling standards to build and manage tunnels. ISAKMP and IPsec accomplish the following:

- Negotiate tunnel parameters.
- Establish tunnels.
- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint or router.

A device in a VPN functions as a bidirectional tunnel endpoint. It can receive plain packets from theprivate network, encapsulate them, create a tunnel, and send them to the other end of the tunnel wherethey are unencapsulated and sent to their final destination. It can also receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

The following topics explain the basic IKE and IPsec policies and how to configure them:

Overview of IKE and IPsec Configurations

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and to automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection.

An IKE proposal is a set of algorithms that two peers use to secure the IKE negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. For IKE version 1 (IKEv1), IKE proposals contain a single set of algorithms and a modulus group. You can create multiple, prioritized policies at each peer to ensure that at least one policy matches a remote peer's policy. Unlike IKEv1, in an IKEv2 proposal, you can select multiple algorithms and modulus groups from which peers can choose during the Phase 1 negotiation, potentially making it possible to create a single IKE proposal (although you might want different proposals to give higher priority to your most desired options). You can define several IKE proposals per VPN.

You must configure several policies to define the settings required to make successful regular IPsec connections in a site-to-site or remote access VPN. The following procedure provides an overview of the steps required to complete the configuration, and points to other topics that provide detailed information for each step.

Related Topics

- Understanding IKE , on page 5
- Understanding IPsec Proposals , on page 19
- Understanding IKEv1 Preshared Key Policies in Site-to-Site VPNs , on page 48
- Understanding Public Key Infrastructure Policies , on page 51

Step 1 Configure the **IKE Proposal** policy.

In the IKE Proposal policy, you define the IKE proposal policy objects to use for making VPN connections. When defining the IKE proposal object, you select the algorithms to use for encrypting the IKE negotiation and for integrity checking, and the Diffie-Hellman group to use to operate the encryption algorithm. For IKEv1, you also determine whether you are using preshared keys or Public Key Infrastructure, whereas in IKEv2, the IKE proposal does not include a specification for authentication mode.

The following topics explain how to configure the IKE Proposal policy:

- Configuring an IKE Proposal , on page 10
  - Configuring IKEv1 Proposal Policy Objects , on page 11
  - Configuring IKEv2 Proposal Policy Objects , on page 15
- Configuring the IKE Proposal for GET VPN

Step 2 Complete the authentication mode configuration.

Your selection for authentication mode in the IKEv1 proposal, and your decision on which mode to use for IKEv2, controls what other policies are required to complete the authentication mode configuration:

- Preshared keys—For remote access IKEv1 IPsec VPNs, you define the preshared keys in the **Connection Profiles** policy; preshared keys are not supported for IKEv2 in remote access VPNs. For site-to-site VPNs, you define the keys in the **IKEv1 Preshared Keys** or the **IKEv2 Authentication** policy based on the IKE version you are using.

The following topics explain preshared key configuration:

- IPSec Tab (Connection Profiles)
- Configuring IKEv1 Preshared Key Policies , on page 49
- Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70

- Public Key Infrastructure Certificate Authority servers—If you configure IKE to use Certificate Authority (CA) servers, you must configure the **Public Key Infrastructure** policy. You also use this policy to define the Public Key Infrastructure for SSL VPNs. For site-to-site VPNs, the policy is **IKEv1 Public Key Infrastructure** or **IKEv2 Authentication**, based on the IKE version you are using.

The Public Key Infrastructure policy identifies the PKI enrollment object that identifies the Certificate Authority server. For site-to-site VPNs, you can select a single PKI enrollment object; for remote access VPNs, you can select all objects needed for your remote access connections. These trustpoints are then identified in the remote access **Connection Profiles** policy (on the IPsec tab).

The following topics explain public key infrastructure configuration:

- Understanding Public Key Infrastructure Policies , on page 51
- Configuring IKEv1 Public Key Infrastructure Policies in Site-to-Site VPNs , on page 55
- Defining Multiple IKEv1 CA Servers for Site-to-Site VPNs , on page 56
- Configuring Public Key Infrastructure Policies for Remote Access VPNs , on page 58
- IPSec Tab (Connection Profiles)
- Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70

Step 3 Configure the **IPsec Proposal** policy. The IPsec Proposal policy defines the IPsec transform set policy objects used to create a secure IPsec tunnel for the VPN.

The following topics explain how to configure the IPsec Proposal policy:

- Configuring IPsec Proposals in Site-to-Site VPNs , on page 23
  - Selecting the IKE Version for Devices in Site-to-Site VPNs , on page 26
  - Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects , on page 27
- Configuring an IPsec Proposal for Easy VPN
- Configuring an IPsec Proposal on a Remote Access VPN Server (ASA, PIX 7.0+ Devices)
- Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices)

Step 4 Configure the **Global Settings** policy.

The **Global Settings** (remote access) and **VPN Global Settings** (site-to-site) policies define various ISAKMP, IKEv1, IKEv2, IPsec, NAT, fragmentation, and other settings. These settings have default values that are frequently adequate, so normally you need to configure the Global Settings policy only if you want non-default behavior. However, you must configure the policy for remote access IKEv2 IPsec VPNs, because you must specify a remote access global trustpoint on the **IKEv2 Settings** tab.

The following topics explain how to configure the Global Settings policy:

- Configuring VPN Global Settings , on page 31
  - Configuring VPN Global ISAKMP/IPsec Settings , on page 34
  - Configuring VPN Global IKEv2 Settings , on page 38
  - Configuring VPN Global NAT Settings , on page 43
  - Configuring VPN Global General Settings , on page 44
- Configuring Global Settings for GET VPN

Step 5 If you are configuring a remote access IKEv2 IPsec VPN, you must also configure several policies for SSL VPN. IKEv2 shares several configuration settings with SSL VPNs. For information on the other policies you need to configure, see Creating IPSec VPNs Using the Remote Access VPN Configuration Wizard (ASA and PIX 7.0+ Devices).

Comparing IKE Version 1 and 2

There are two versions of IKE: version 1 (IKEv1) and version 2 (IKEv2). When you configure IKE on a device that supports IKEv2, you have the option of configuring either version alone, or both versions together. When the device attempts to negotiate a connection with another peer, it uses whichever versions you allow and that the other peer accepts. If you allow both versions, the device automatically falls back to the other version if negotiations are unsuccessful with the initially chosen version (IKEv2 is always tried first if it is configured). Both peers must support IKEv2 to use it in a negotiation.

Tip Security Manager supports IKEv2 on ASA 8.4(1)+ only. For remote access IPsec VPNs, users must use the AnyConnect 3.0+ client to complete IKEv2 connections, and IKEv2 connections use the same license pool that is used for SSL VPN connections. The legacy VPN Client is used for IKEv1 remote access connections on ASAs. For more information about device support in VPNs, see Understanding Devices Supported by Each IPsec Technology.

IKEv2 differs from IKEv1 in the following ways:

- IKEv2 fixes the Photuris style cookie mechanism.
- IKEv2 has fewer round trips in a negotiation than IKEv1, two round trips versus five for IKEv1 for a basic exchange.
- Transform options are OR'ed, which means that you can specify multiple options in a single proposal rather than creating separate unique proposals for each allowed combination.
- Built-in dead peer detection (DPD).
- Built-in configuration payload and user authentication mode.

- Built-in NAT traversal (NAT-T). IKEv2 uses ports 500 and 4500 for NAT-T.
- Improved re-keying and collision handling.
- A single security association (SA) can protect multiple subnets, which improves scalability.
- Asymmetric authentication in site-to-site VPNs, where each side of a tunnel can have different preshared keys, different certificates, or one side a key and the other side a certificate.
- For remote access IPsec VPNs, you can configure double authentication for IKEv2 connections in the same way that you configure them for remote access SSL VPNs. IKEv1 does not support double authentication.

Related Topics

- Overview of IKE and IPsec Configurations , on page 2
- Configuring an IKE Proposal , on page 10

Understanding IKE

Internet Key Exchange (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 (SA). It provides a common framework for agreeing on the format of SA attributes. This includes negotiating with the peer about the SA, and modifying or deleting the SA. IKE creates the cryptographic keys used to authenticate IPsec peers, negotiates and distributes IPsec encryption keys, and automatically establishes IPsec security associations.

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, creating the first tunnel that enables the peers to communicate securely in Phase 2, protecting later ISAKMP negotiation messages. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec, which protects the data sent between peers. Both phases use proposals when they negotiate a connection.

An IKE proposal is a set of algorithms that two peers use to secure the IKE negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. In remote access IPsec VPNs, you can define several IKE proposals per VPN to create multiple, prioritized policies at each peer to ensure that at least one policy matches a remote peer's policy. For site-to-site VPNs, you can create a single IKE proposal.

To define an IKE proposal, you must specify:

- A unique priority (1 through 65,543, with 1 the highest priority).
- An encryption method for the IKE negotiation, to protect the data and ensure privacy. See Deciding Which Encryption Algorithm to Use , on page 6.
- A Hashed Message Authentication Codes (HMAC) method (called *integrity algorithm* in IKEv2) to ensure the identity of the sender, and to ensure that the message has not been modified in transit. See Deciding Which Hash Algorithm to Use , on page 7.
- For IKEv2, a separate pseudo-random function (PRF) used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. The options are the same as those used for the hash algorithm; see Deciding Which Hash Algorithm to Use , on page 7.

- A Diffie-Hellman group to determine the strength of the encryption-key-determination algorithm. The device uses this algorithm to derive the encryption and hash keys. See Deciding Which Diffie-Hellman Modulus Group to Use , on page 7.
- An authentication method, to ensure the identity of the peers. See Deciding Which Authentication Method to Use , on page 9.
- A limit to the time the device uses an encryption key before replacing it.

Note Configuring IKEv2 Proposal Policy Objects , on page 15

Tip (ASA devices only.) With IKEv1 policies, for each parameter, you set one value. For IKEv2, you can configure multiple encryption, integrity, PRF, and Diffie-Hellman options. The ASA orders the settings from the most secure to the least secure and negotiates with the peer using that order. This allows you to potentially send a single proposal to convey all the allowed transforms instead of the need to send each allowed combination as with IKEv1.

When IKE negotiation begins, the peer that initiates the negotiation sends all of its policies to the remote peer, and the remote peer searches for a match with its own policies, in priority order.

A match between IKE policies exists if they have the same encryption, hash (integrity and PRF for IKEv2), authentication, and Diffie-Hellman values, and an SA lifetime less than or equal to the lifetime in the policy sent. If the lifetimes are not identical, the shorter lifetime—from the remote peer policy—applies. If no match exists, IKE refuses negotiation and the IKE SA is not established.

The following topics explain how to configure IKE proposals:

- Configuring an IKE Proposal , on page 10
- Configuring IKEv1 Proposal Policy Objects , on page 11
- Configuring IKEv2 Proposal Policy Objects , on page 15
- Configuring the IKE Proposal for GET VPN

Deciding Which Encryption Algorithm to Use

When deciding which encryption and hash algorithms to use for the IKE proposal, your choice is limited to algorithms that are supported by the devices in the VPN.

You can choose from the following encryption algorithms:

- DES (Data Encryption Standard) is a symmetric secret-key block algorithm. It is faster than 3DES and uses less system resources, but it is also less secure. If you do not need strong data confidentiality, and if system resources or speed is a concern, you should choose DES.
- 3DES (Triple DES) is more secure because it processes each block of data three times, each time with a different key. However, it uses more system resources and is slower than DES. 3DES is the recommended encryption algorithm, assuming that the devices support it.

- AES (Advanced Encryption Standard) provides greater security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192- and 256-bit keys. A longer key provides higher security but a reduction in performance. When you configure IKE on a router, the router must use Cisco IOS Software 12.3T or later to use AES.

Note AES cannot be used in conjunction with a hardware encryption card.

Related Topics

- Understanding IKE , on page 5
- Configuring an IKE Proposal , on page 10

Deciding Which Hash Algorithm to Use

You can choose from the following hash algorithms. In IKEv2, the hash algorithm is separated into two options, one for the integrity algorithm, and one for the pseudo-random function (PRF).

- SHA (Secure Hash Algorithm) is more resistant to brute-force attacks than MD5. However, it is also more resource intensive than MD5. For implementations that require the highest level of security, use the SHA hash algorithm.

Standard SHA produces a 160-bit digest.

The following options, which are even more secure, are available for IKEv2 configurations on ASA 8.4(2+) devices:

- SHA512—A 512-bit key.
- SHA384—A 384-bit key.
- SHA256—A 256-bit key.

- MD5 (Message Digest 5) produces a 128-bit digest and uses less processing time for an overall faster performance than SHA, but it is considered to be weaker than SHA.

Related Topics

- Understanding IKE , on page 5
- Configuring an IKE Proposal , on page 10

Deciding Which Diffie-Hellman Modulus Group to Use

Security Manager supports the following Diffie-Hellman key derivation algorithms to generate IPsec security association (SA) keys. Each group has a different size modulus. A larger modulus provides higher security, but requires more processing time. You must have a matching modulus group on both peers.

Tip If you select AES encryption, to support the large key sizes required by AES, ISAKMP negotiation should use Diffie-Hellman (DH) Group 5 or later. For IKEv1, ASA devices support groups 2 and 5 only.

- Diffie-Hellman Group 1: 768-bit modulus. Use to generate IPsec SA keys where the prime and generator numbers are 768 bits.

Note Beginning with Cisco Security Manager 4.19, DH group 1 for IKEv1 and IKEv2 is not supported for ASA 9.12(1) and later devices.

- Diffie-Hellman Group 2: 1024-bit modulus. Use to generate IPsec SA keys where the prime and generator numbers are 1024 bits. Cisco VPN Client Version 3.x or later requires a minimum of Group 2.
- Diffie-Hellman Group 5: 1536-bit modulus. Use to generate IPsec SA keys where the prime and generator numbers are 2048 bits. Considered good protection for 128-bit keys, but group 14 is better.
- Diffie-Hellman Group 7: Use to generate IPsec SA keys when the elliptical curve field size is 163 characters. Group 7 is not supported on a Catalyst 6500/7600 device with VPNSM or VPN SPA configuration.
- Diffie-Hellman Group 14: 2048-bit modulus. Considered good protection for 128-bit keys. (ASA 9.0.1+ devices only).

Note Beginning with Cisco Security Manager 4.20, DH group 14 is supported, and is the default DH group, for IKEv1 and IKEv2 on ASA 9.13(1) and later devices.

- Diffie-Hellman Group 15: 3072-bit modulus. Considered good protection for 192-bit keys.
- Diffie-Hellman Group 16: 4096-bit modulus. Considered good protection for 256-bit keys.

Note Beginning with Cisco Security Manager 4.20, DH groups 15 and 16 are supported for IKEv2 on ASA 9.13(1) and later devices.

- Diffie-Hellman Group 19: (256-bit elliptical curve field size). (ASA 9.0.1+ devices only).
- Diffie-Hellman Group 20: (384-bit elliptical curve field size). (ASA 9.0.1+ devices only).
- Diffie-Hellman Group 21: (521-bit elliptical curve field size). (ASA 9.0.1+ devices only).
- Diffie-Hellman Group 24: (2048-bit modulus and 256-bit prime order subgroup). (ASA 9.0.1+ devices only).
- Diffie-Hellman Group 31: (256-bit elliptical curve field size). (ASA 9.16.1+ devices only).

Related Topics

- Understanding IKE , on page 5

- Configuring an IKE Proposal , on page 10

Deciding Which Authentication Method to Use

Security Manager supports two methods for peer device authentication in a VPN communication:

- **Preshared Key**—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. The same shared key must be configured at each peer or the IKE SA cannot be established.

To use IKE successfully with this device authentication method, you must define various preshared key parameters. For more information, see the appropriate topic:

- Site-to-site VPN, IKEv1 configuration—See Configuring IKEv1 Preshared Key Policies , on page 49.
- Site-to-site VPN, IKEv2 configuration—See Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.
- Remote access IPsec VPN, IKEv1—Configured on the IPsec tab of the connection profile. See IPSec Tab (Connection Profiles).
- Remote access IPsec VPN, IKEv2—You cannot use preshared keys when using IKEv2 in a remote access IPSec VPN. You must use certificates.

- **Certificate**—An authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide non-repudiation of communication between two peers, meaning that it can be proved that the communication actually took place. When using this authentication method, peers are configured to obtain digital certificates from a Certification Authority (CA). CAs manage certificate requests and issue certificates to participating IPsec network devices. These services provide centralized key management for the participating devices.

While the use of preshared keys does not scale well, using a CA does improve the manageability and scalability of your IPsec network. With a CA, you do not need to configure keys between all encrypting devices. Instead, each participating device is registered with the CA, and requests a certificate from the CA. Each device that has its own certificate and the public key of the CA can authenticate every other device within a given CA's domain.

To use IKE successfully with the Certificate authentication method, you must define parameters for CA authentication and enrollment. For more information, see the appropriate topic:

- Site-to-site VPN, IKEv1 configuration—See Understanding Public Key Infrastructure Policies , on page 51.
- Site-to-site VPN, IKEv2 configuration— Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.
- Remote access IPsec VPN, IKEv1—Configured on the IPsec tab of the connection profile as explained in IPSec Tab (Connection Profiles). You must also configure the Public Key Infrastructure policy with the same trustpoint; see Understanding Public Key Infrastructure Policies , on page 51.
- Remote access IPsec VPN, IKEv2—Configure the global trustpoint on the IKEv2 Settings tab of the Global Settings policy as explained in Configuring VPN Global IKEv2 Settings , on page 38. You must also configure the Public Key Infrastructure policy with the same trustpoint; see Understanding Public Key Infrastructure Policies , on page 51.

Related Topics

- Understanding IKE , on page 5
- Configuring an IKE Proposal , on page 10

Configuring an IKE Proposal

In Security Manager, an IKE proposal is a mandatory policy when you configure a site-to-site or remote access IPsec VPN. When you use the configuration wizard to create a new IPsec VPN, an IKE Proposal policy is automatically assigned to the VPN; the policy might be the factory default, or it might be a shared policy specifically selected for the VPN. For more information about the IKE (Internet Key Exchange) key management protocol, see Understanding IKE , on page 5.

Use the IKE Proposal policy to examine the current IKE proposals and to configure new proposals except for GET VPN topologies. For GET VPN, see Configuring the IKE Proposal for GET VPN.

Note Beginning with Cisco Security Manager version 4.17, you can configure and deploy IKE Proposal policy on ASA multi-context devices running the software version 9.9(2) or later.

Tips

- For site-to-site VPNs, you can select at most one IKE proposal per IKE version. For remote access IPsec VPNs, you can select multiple proposals for each IKE version; select all IKE proposals that are allowed in the remote access VPN.
- To configure IKEv2 (version 2), the device must be an ASA running ASA Software release 8.4(1) or later.
- The IPsec Proposal policy must enable IKEv1, IKEv2, or both, to match the IKE proposals you configure in this policy. In cases where you cannot configure IKEv2 in the IPsec proposal, such as in Easy VPN topologies, IKEv2 is not supported. For more information, see Understanding IPsec Proposals , on page 19.
- The IKEv1 Proposal objects specify whether preshared keys or certificates are used for authentication. If the IKEv1 Proposal object is of certificate authentication type, ensure that you specify the appropriate CA Server in the IKEv1 Public Key Infrastructure (from Policy Selector) policy. For preshared keys, ensure that the IKEv1 Preshared Key policy is assigned. For IKEv2, the object does not specify whether preshared keys or certificates are used, but other policies must define the authentication requirements. For more information, see Deciding Which Authentication Method to Use , on page 9.
- For Regular IPSec VTI technology, you can specify only one of the IKE Proposals—IKEv1 proposal or IKEv2 proposal. That is, if you have selected IKE version 1 for the Regular IPSec VTI, (in the IKE Proposal window) you must be specifying the IKEv1 Proposal and leave the IKEv2 Proposal field blank and vice versa.

Related Topics

- Deciding Which Hash Algorithm to Use , on page 7
- Deciding Which Diffie-Hellman Modulus Group to Use , on page 7
- Deciding Which Authentication Method to Use , on page 9

Step 1 Do one of the following to open the IKE Proposal policy based on the type of VPN you are configuring:

- For remote access VPNs, do one of the following:
  - (Device View) Select **Remote Access VPN > IPSec VPN > IKE Proposal** from the Policy selector.
  - (Policy View) Select **Remote Access VPN > IPSec VPN > IKE Proposal** from the Policy Type selector. Select an existing policy or create a new one.
- For site-to-site VPNs, do one of the following:
  - Open the Site-to-Site VPN Manager Window, select a topology (other than GET VPN) in the VPNs selector, then select **IKE Proposal** in the Policies selector.
  - (Policy view) Select **Site-to-Site VPN > IKE Proposal** from the Policy Types selector. Select an existing shared policy or create a new one.

Step 2 Click **Select** against the appropriate IKE versions to choose the policy objects that define the settings for an IKE version 1 or version 2 proposal. Configure proposals only for those IKE versions supported in the VPN.

Note Beginning with 4.16, Cisco Security Manager does not support IKEv1 configuration for Firepower 9300 devices with distributed mode.

- To select an IKE proposal for site-to-site VPNs, simply highlight it in the available proposals list. For remote access IPsec VPNs, highlight the desired objects in the available proposals list and click >> to move them to the selected proposals list.
- To remove an IKE proposal for remote access IPsec VPNs, highlight it in the selected proposals list and click << to move it to the available proposals list.
- To create a new IKE proposal, click the **Create (+)** button beneath the available proposals list. The Add IKEv1 or IKEv2 Proposal dialog box opens. For instructions on creating the object, see the following topics:
  - Configuring IKEv1 Proposal Policy Objects , on page 11
  - Configuring IKEv2 Proposal Policy Objects , on page 15
- To edit an object, or to view its settings, select it and click the **Edit (pencil)** button beneath the list.

Configuring IKEv1 Proposal Policy Objects

Use the IKEv1 Proposal dialog box to create, copy, and edit an IKEv1 proposal object.

Internet Key Exchange (IKE) version 1 proposal objects contain the parameters required for IKEv1 proposals when defining remote access and site-to-site VPN policies. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes security associations (SAs) for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. For more information about IKE proposals, see the following topics:

- Overview of IKE and IPsec Configurations , on page 2
- Comparing IKE Version 1 and 2 , on page 4
- Understanding IKE , on page 5
- Deciding Which Encryption Algorithm to Use , on page 6
- Deciding Which Hash Algorithm to Use , on page 7
- Deciding Which Diffie-Hellman Modulus Group to Use , on page 7
- Deciding Which Authentication Method to Use , on page 9

Navigation Path

Select **Manage** > **Policy Objects**, then select **IKE Proposals** > **IKEv1 Proposals** from the Object Type Selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Tip You can also access this dialog box when configuring the IKE Proposal policy as explained in Configuring an IKE Proposal , on page 10.

Related Topics

- Configuring IKEv2 Proposal Policy Objects , on page 15
- Creating Policy Objects
- Policy Object Manager
- Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects , on page 27

Field Reference

Table 1: IKEv1 Proposal Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object. A maximum of 1024 characters is allowed.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 10000. The lower the number, the higher the priority. If you leave this field blank, Security Manager assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.

Element	Description
Encryption Algorithm	The encryption algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations: • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash Algorithm	The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.

Element	Description
Modulus Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: **Tip** For IKEv1, ASA devices support DH group 14 only. • 1—Diffie-Hellman Group 1 (768-bit modulus). **Note** Beginning with Cisco Security Manager 4.19, DH group 1 is not supported for ASA 9.12(1) and later devices. The default value will be Group 2. • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or later). • 7—Diffie-Hellman Group 7 (163-bit elliptical curve field size). • 14—Diffie-Hellman Group 14 (2048-bit modulus, considered good protection for 128-bit keys). **Note** Beginning with Cisco Security Manager 4.20, DH group 14 is supported, and is the default DH group, for IKEv1 on ASA 9.13(1) and later devices. • 15—Diffie-Hellman Group 15 (3072-bit modulus, considered good protection for 192-bit keys). • 16—Diffie-Hellman Group 16 (4096-bit modulus, considered good protection for 256-bit keys). **Note** Although Diffie-Hellman groups 15 and 16 are listed, they are not supported for IKEv1 and will cause a validation error if selected for IKEv1 policies.
Lifetime	The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 2147483647 seconds. The default is 86400.
Authentication Method	The method of authentication to use between the two peers. For information on how this selection determines which other policies you must configure, see Deciding Which Authentication Method to Use , on page 9. Select one of the following: • Preshared Key—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If one of the participating peers is not configured with the same preshared key, the IKE SA cannot be established. • Certificate—An authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. This method provides non-repudiation of communication between two peers, meaning that it can be proved that the communication actually took place. When you use this authentication method, the peers are configured to obtain digital certificates from a Certification Authority (CA).

Element	Description
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects.

Configuring IKEv2 Proposal Policy Objects

Use the IKEv2 Proposal dialog box to create, copy, and edit an IKEv2 proposal object. You can use IKEv2 proposals with ASA Software release 8.4(1)+ only.

Internet Key Exchange (IKE) version 2 proposal objects contain the parameters required for IKEv2 proposals when defining remote access and site-to-site VPN policies. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes security associations (SAs) for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. Unlike IKEv1, in an IKEv2 proposal, you can select multiple algorithms and modulus groups from which peers can choose during the Phase 1 negotiation. For more information about IKE proposals, see the following topics:

- Overview of IKE and IPsec Configurations , on page 2
- Comparing IKE Version 1 and 2 , on page 4
- Understanding IKE , on page 5
- Deciding Which Encryption Algorithm to Use , on page 6
- Deciding Which Hash Algorithm to Use , on page 7
- Deciding Which Diffie-Hellman Modulus Group to Use , on page 7

Tip Unlike IKEv1, you do not specify the authentication method in the IKE proposal. For more information on how to configure the authentication method in IKEv2, see Deciding Which Authentication Method to Use , on page 9.

Navigation Path

Select **Manage** > **Policy Objects**, then select **IKE Proposals** > **IKEv2 Proposals** from the Object Type Selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Tip You can also access this dialog box when configuring the IKE Proposal policy as explained in Configuring an IKE Proposal , on page 10.

Related Topics

- Configuring IKEv1 Proposal Policy Objects , on page 11
- Creating Policy Objects
- Policy Object Manager
- Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects , on page 27

Field Reference

Table 2: IKEv2 Proposal Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object. A maximum of 1024 characters is allowed.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 65535. The lower the number, the higher the priority. If you leave this field blank, Security Manager assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.

Element	Description
Encryption Algorithm	The encryption algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations. Click **Select** and select all of the algorithms that you want to allow in the VPN: • AES-GCM-256—Encrypts according to the Advanced Encryption Standard in Galois/Counter Mode using 256-bit keys. (ASA 5580 and ASA 5500-X Series devices running 9.0.1+ only). • AES-GCM-192—Encrypts according to the Advanced Encryption Standard in Galois/Counter Mode using 192-bit keys. (ASA 5580 and ASA 5500-X Series devices running 9.0.1+ only). • AES-GCM—Encrypts according to the Advanced Encryption Standard in Galois/Counter Mode using 128-bit keys. (ASA 5580 and ASA 5500-X Series devices running 9.0.1+ only). • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • Null—No encryption algorithm.
Integrity (Hash) Algorithm	The integrity portion of the hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Click **Select** and select all of the algorithms that you want to allow in the VPN: **Note** If using AES-GCM, AES-GCM-192, or AES-GCM-256, you must select Null as the Integrity Algorithm. • SHA (Secure Hash Algorithm)—SHA is more resistant to brute-force attacks than MD5. Standard SHA produces a 160-bit digest. The following options, which are even more secure, are available for IKEv2 configurations on ASA 8.4(2+) devices: • SHA512—A 512-bit key. • SHA384—A 384-bit key. • SHA256—A 256-bit key. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA. • Null—No encryption algorithm. For use with AES-GCM, AES-GCM-192, and AES-GCM-256 only.

Element	Description
Prf Algorithm	The pseudo-random function (PRF) portion of the hash algorithm used in the IKE proposal. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Click **Select** and select all of the algorithms that you want to allow in the VPN. The options are described above under Integrity Algorithm.
Modulus Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Click **Select** and select all of the groups that you want to allow in the VPN: • 1—Diffie-Hellman Group 1 (768-bit modulus). **Note** Beginning with Cisco Security Manager 4.19, DH group 1 option is not supported for ASA 9.12(1) and later devices. • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or later). • 14—Diffie-Hellman Group 14 (2048-bit modulus, considered good protection for 128-bit keys). (ASA 9.0.1+ devices only). **Note** Beginning with Cisco Security Manager 4.20, DH group 14 is supported, and is the default DH group, for IKEv1 on ASA 9.13(1) and later devices. • 15—Diffie-Hellman Group 15 (3072-bit modulus, considered good protection for 192-bit keys). (ASA 9.13.1+ devices only). • 16—Diffie-Hellman Group 16 (4096-bit modulus, considered good protection for 256-bit keys). (ASA 9.13.1+ devices only). • 19—Diffie-Hellman Group 19 (256-bit elliptical curve field size). (ASA 9.0.1+ devices only). • 20—Diffie-Hellman Group 20 (384-bit elliptical curve field size). (ASA 9.0.1+ devices only). • 21—Diffie-Hellman Group 21 (521-bit elliptical curve field size). (ASA 9.0.1+ devices only). • 24—Diffie-Hellman Group 24 (2048-bit modulus and 256-bit prime order subgroup). (ASA 9.0.1+ devices only). • 31—Diffie-Hellman Group 31 (256-bit elliptical curve field size). (ASA 9.16.1+ devices only).
Lifetime	The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 120 to 2147483647 seconds. The default is 86400.

Element	Description
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects.

Understanding IPsec Proposals

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers, which can be devices in a site-to-site VPN or a device and user in remote access IPsec VPNs. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms called a transform set.

An IPsec proposal is used in Phase 2 of an IKE negotiation, as explained in Understanding IKE , on page 5. The specific content of the proposal varies according to topology type (site-to-site or remote access) and device type, although the proposals are broadly similar and contain many of the same elements, such as IPsec transform sets.

The following topics explain IPsec proposal concepts and procedures in more detail:

Understanding IPsec Proposals for Site-to-Site VPNs

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. Pure IPsec configurations cannot use routing protocols—the policy created is used for pure IPsec provisioning. You can configure pure IPsec on Cisco IOS routers, PIX Firewalls, Catalyst VPN Service Modules, and Adaptive Security Appliance (ASA) devices.

With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms called a transform set.

In Security Manager, you use an IPsec Proposal policy to define the settings required for a IPsec tunnels. An IPsec proposal is a collection of one or more crypto maps that are applied to the VPN interfaces on the devices. A crypto map combines all the components required to set up IPsec security associations, including transform sets. A crypto map can also be configured with Reverse Route Injection (RRI).

The following topics provide more information:

- Understanding Crypto Maps , on page 20
- Understanding Transform Sets , on page 21
- Understanding Reverse Route Injection , on page 22

Related Topics

- Configuring IPsec Proposals in Site-to-Site VPNs , on page 23

Understanding Crypto Maps

A crypto map combines all components required to set up IPsec security associations (SA), including IPsec rules, transform sets, remote peers, and other parameters that might be necessary to define an IPsec SA. A crypto map entry is a named series of CLI commands. Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set, which is applied to the VPN interfaces on relevant devices. All IP traffic passing through the interface is evaluated against the applied crypto map set.

When two peers try to establish an SA, they must each have at least one compatible crypto map entry. The transform set defined in the crypto map entry is used in the IPsec security negotiation to protect the data flows specified by that crypto map's IPsec rules.

Dynamic crypto map policies are used in site-to-site VPNs when an unknown remote peer tries to initiate an IPsec security association with the local hub. The hub cannot be the initiator of the security association negotiation. Dynamic crypto policies allow remote peers to exchange IPsec traffic with a local hub even if the hub does not know the remote peer's identity. You can create a dynamic crypto policy on individual hubs or on a device group that contains hubs. The policy is written only to the hubs, not to any spokes that might be contained in the group. A dynamic crypto map policy essentially creates a crypto map entry without all the parameters configured. The missing parameters are later dynamically configured (as the result of an IPsec negotiation) to match a remote peer's requirements. The peer addresses for dynamic or static crypto maps are deduced from the VPN topology.

Dynamic crypto map policies apply only in a hub-and-spoke VPN configuration—in a point-to-point or full mesh VPN topology, you can apply only static crypto map policies.

Note (Site-to-site VPNs.) Except for Extranet VPNs, Security Manager can manage an existing VPN tunnel only if the tunnel's peers are managed by Security Manager. In such a case, Security Manager uses the same crypto map name for the tunnel on the peers. On subsequent deployments, only Security Manager tunnels are managed (Security Manager maintains a log of all tunnels that were configured).

Related Topics

- Understanding IPsec Proposals , on page 19
- Understanding Transform Sets , on page 21
- Configuring IPsec Proposals in Site-to-Site VPNs , on page 23

Understanding Transform Sets

A transform set is a combination of security protocols and algorithms that secure traffic in an IPsec tunnel. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers. When such a transform set is found, it is applied to create an SA that protects data flows in the access list for that crypto map, protecting the traffic in the VPN.

There are separate IPsec transform sets for IKEv1 and IKEv2. With IKEv1 transform sets, for each parameter, you set one value. For IKEv2 transform sets, you can configure multiple encryption and integration algorithms for a single proposal. ASA devices order the settings from the most secure to the least secure and negotiate with the peer using that order. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

You can specify a number of transform sets per IPsec proposal policy. If you are defining the policy on a spoke or a group of spokes, you do not usually have to specify more than one transform set. This is because the spoke's assigned hub would typically be a higher performance router capable of supporting any transform set that the spoke supports. However, if you are defining the policy on a hub for dynamic crypto, you should specify more than one transform set to ensure that there will be a transform set match between the hub and the unknown spoke. If more than one of your selected transform sets is supported by both peers, the transform set that provides the highest security is used.

Security Manager provides predefined transform sets that you can use in your tunnel policies. You can also create your own transform sets. For more information, see Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects , on page 27.

Selecting Tunnel Mode for IKEv1 Transform Sets

When defining an IKEv1 transform set, you must specify which IPsec mode of operation to use—tunnel mode or transport mode. You can use the AH and ESP protocols to protect an entire IP payload (Tunnel mode) or just the upper-layer protocols of an IP payload (Transport mode).

In tunnel mode (the default), the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a router to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source's router encrypts packets and forwards them along the IPsec tunnel. The destination's router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to enjoy the benefits of IPsec. Tunnel mode also protects against traffic analysis. With tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

In transport mode, only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. However, by passing the IP header in the clear, transport mode allows an attacker to perform some traffic analysis. For example, an attacker could see when a company's CEO sent many packets to another senior executive. However, the attacker would only know that IP packets were sent; the attacker would not be able to decipher the contents of the packets. With transport mode, the destination of the flow must be an IPsec termination device.

Note You cannot use transport mode for VPN topologies using regular IPsec or Easy VPN.

Related Topics

- Understanding IPsec Proposals , on page 19

- Understanding Crypto Maps , on page 20
- Configuring IPsec Proposals in Site-to-Site VPNs , on page 23

Understanding Reverse Route Injection

Reverse Route Injection (RRI) enables static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities. Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote VPN router as the next hop, the traffic is forced through the crypto process to be encrypted.

After the static route is created on the VPN router, this information is propagated to upstream devices, allowing them to determine the appropriate VPN router to which to send returning traffic in order to maintain IPsec state flows. This is particularly useful if multiple VPN routers are used at a site to provide load balancing or failover, or if the remote VPN devices are not accessible through a default route. Routes are created in either the global routing table or the appropriate virtual route forwarding (VRF) table.

Note Security Manager automatically configures RRI on devices with High Availability (HA) or on the IPsec Aggregator when VRF-Aware IPsec is configured. You can also configure RRI on a device's crypto map in a remote access VPN.

In Security Manager, the following options are available for configuring Reverse Route Injection:

- For dynamic crypto maps, routes are created upon the successful establishment of IPsec security associations (SAs) for those remote proxies. The next hop back to those remote proxies is through the remote VPN router whose address is learned and applied during the creation of the dynamic crypto map template. The routes are deleted after the SAs are deleted.
- The Remote Peer option (available for IOS devices only) enables you to specify an interface or address as the explicit next hop to the remote VPN device. Two routes are created. One route is the standard remote proxy ID and the next hop is the remote VPN client tunnel address. The second route is the actual route to the remote tunnel endpoint, when a recursive lookup is forced to impose that the remote endpoint is reachable via "next-hop." Creation of the second route for the actual next hop is very important for VRF-Aware IPsec when a default route must be overridden by a more explicit route.

Note For devices using a VPN Services Module (VPNSM), the next hop is the interface or subinterface/VLAN on which the crypto map is applied. See Configuring an IPsec Proposal on a Remote Access VPN Server (ASA, PIX 7.0+ Devices) and Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices).

- In the case of Remote Peer IP (available for IOS devices only), one route is created to a remote proxy by way of a user-defined next hop. The next hop can be used to override a default route to properly direct outgoing encrypted packets. This option reduces the number of routes created and supports those platforms that do not readily facilitate route recursion.

Related Topics

- Understanding IPsec Proposals , on page 19

- Understanding Crypto Maps , on page 20
- Configuring IPsec Proposals in Site-to-Site VPNs , on page 23

Configuring IPsec Proposals in Site-to-Site VPNs

Use the IPsec Proposal page to configure the IPsec proposal used during IKE Phase 2 negotiations for site-to-site VPN topologies with the exception of Easy VPN topologies.

IPsec proposals used with Easy VPN topologies, and with remote access VPNs, are significantly different than the basic site-to-site proposal explained in this topic. For information on IPsec proposals in these other topologies, see the following topics:

- Configuring an IPsec Proposal for Easy VPN
- Configuring an IPsec Proposal on a Remote Access VPN Server (ASA, PIX 7.0+ Devices)
- Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices)

Navigation Path

- (Site-to-Site VPN Manager Window) Select a non-Easy VPN topology in the VPNs selector, then select **IPsec Proposal** in the Policies selector. If necessary, click the **IPsec Proposal** tab.
- (Policy view) Select **Site-to-Site VPN > IPsec Proposal** from the Policy Types selector. Select an existing shared policy or create a new one.

Related Topics

- Understanding IKE , on page 5
- Understanding IPsec Proposals for Site-to-Site VPNs , on page 19

Field Reference

Table 3: IPsec Proposal Page, Site-to-Site VPNs (except Easy VPN)

Element	Description
Crypto Map Type (Hub and spoke and full mesh topologies only.)	A crypto map combines all the components required to set up IPsec security associations (SA). When two peers try to establish an SA, they must each have at least one compatible crypto map entry. For more information, see Understanding Crypto Maps , on page 20. Select the type of crypto map you want to generate: • Static—Use a static crypto map in a point-to-point or full mesh VPN topology. • Dynamic—Dynamic crypto maps can only be used in a hub-and-spoke VPN topology. Dynamic crypto map policies allow remote peers to exchange IPsec traffic with a local hub, even if the hub does not know the remote peer's identity.

Element	Description
Enable IKEv1 Enable IKEv2	The IKE versions to use during IKE negotiations. IKEv2 is supported on ASA Software release 8.4(x) only. Similarly, beginning with 4.16, Cisco Security Manager does not support IKEv1 configurations for Firepower 9300 devices configured with distributed mode. Select either or both options as appropriate; you must select IKEv1 if any device in the topology does not support IKEv2. When you select both options in hub-and-spoke or full mesh topologies, Security Manager automatically assigns the IKE version to devices based on the OS type and version used by the device. You can change these assignments by clicking the **IKE Version** tab, then click the Select button beneath the IKEv1 Enabled Peers or IKEv2 Enabled Peers to change which version is assigned to the device. You can change the assignments for devices that support each version only; other devices are not selectable. For more information, see Selecting the IKE Version for Devices in Site-to-Site VPNs , on page 26.
Transform Sets IKEv2 Transform Sets	The transform sets to use for your tunnel policy. Transform sets specify which authentication and encryption algorithms will be used to secure the traffic in the tunnel. The transform sets are different for each IKE version; select objects for each supported version. You can select up to 11 transform sets for each. For more information, see Understanding Transform Sets , on page 21. If more than one of your selected transform sets is supported by both peers, the transform set that provides the highest security will be used. Click **Select** to select the IPsec transform set policy objects to use in the topology. If the required object is not yet defined, you can click the **Create (+)** button beneath the available objects list in the selection dialog box to create a new one. For more information, see Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects , on page 27. **Note** IKEv1 Transform sets can use tunnel mode or transport mode of IPsec operation. However, you cannot use transport mode in IPsec or Easy VPN topologies.
Enable Perfect Forward Secrecy Modulus Group	Whether to use Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices. If you select this option, also select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key in the **Modulus Group** list. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use , on page 7. **Note** DH group 1 is deprecated and will be removed in later ASA version. In later ASA versions, the default value will be Group 2.

Element	Description
Lifetime (sec) Lifetime (kbytes)	The global lifetime settings for the crypto IPsec security association (SA). You can specify the IPsec lifetime in seconds, in kilobytes, or both. • Seconds (sec)—The number of seconds an SA will exist before expiring. The default is 3600 seconds (one hour). • Kilobytes (kbytes)—The volume of traffic (in kilobytes) that can pass between IPsec peers using a given SA before it expires. Valid values depend on the device type. Enter a value within the range 10-2147483647 for an IOS router, and 2560-536870912 for an ASA/PIX7.0+ device. The default value is 4,608,000 kilobytes.
QoS Preclassify	Supported on Cisco IOS routers, except 7600 devices. When selected, enables the classification of packets before tunneling and encryption occur. The Quality of Service (QoS) for VPNs feature enables Cisco IOS QoS services to operate with tunneling and encryption on an interface. The QoS features on the output interface classify packets and apply the appropriate QoS service before the data is encrypted and tunneled, enabling traffic flows to be adjusted in congested environments, and resulting in more effective packet tunneling.
Reverse Route	Supported on ASA devices, PIX 7.0+ devices, and Cisco IOS routers except 7600 devices. Reverse Route Injection (RRI) enables static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. For more information, see Understanding Reverse Route Injection , on page 22. Select one of the following options to configure RRI on the crypto map: • **None**—Disables the configuration of RRI on the crypto map. • **Standard**—(ASA, PIX 7.0+, IOS devices) Creates routes based on the destination information defined in the crypto map access control list (ACL). This is the default option. • **Remote Peer**—(IOS devices only) Creates two routes, one for the remote endpoint and one for route recursion to the remote endpoint via the interface to which the crypto map is applied. • **Remote Peer IP**—(IOS devices only) Specifies an address as the explicit next hop to the remote VPN device. Enter the IP address or a network/host object that specifies the address, or click **Select** to select the network/host object from a list or to create a new object. **Note** If you use network/host objects, you can select the **Allow Value Override per Device** option in the object to override the IP address, if required, for specific devices that use this object.

Element	Description
Enable Dynamic RRI	**Note** This option is supported from ASA 9.7(1) onwards. It is only applicable if IKEV2 is enabled or Static Crypto Maps are selected. When enabled, the crypto map does not install the reverse-route during configuration but defers it till the IPsec security associations (SA) come up.
ESPv3 Settings (ASA 9.0.1+ only) Specify whether incoming ICMP error messages are validated for cryptography and dynamic cryptography maps, set the per-security association policy, or enable traffic flow packets:	
Validate Incoming ICMP error messages	Whether to validate those ICMP error messages received through an IPsec tunnel and destined for an interior host on the private network.
Enable Do Not Fragment (DF) Policy	Define how the IPsec subsystem handles large packets that have the do-not-fragment (DF) bit set in the IP header. Choose one of the following: • Set—Sets and uses the DF bit. • Copy—Maintains the DF bit. • Clear—Ignores the DF bit.
Enable Traffic Flow Confidentiality (TFC) Packets	Enable dummy TFC packets that mask the traffic profile which traverses the tunnel. **Note** You must have an IKEv2 IPsec proposal set on the Tunnel Policy (Crypto Map) Basic tab before enabling TFC. Traffic Flow Confidentiality is not available when IKEv1 is enabled. Use the Burst, Payload Size, and Timeout parameters to generate random length packets at random intervals across the specified SA.

Selecting the IKE Version for Devices in Site-to-Site VPNs

Use the IKE Version tab in the IPsec Proposal page to select which version of IKE to use for each device in a hub-and-spoke or full mesh site-to-site VPN. This tab appears only in the Site-to-Site VPN Manager; you cannot configure the options in Policy view, because they are specific to the actual devices in a VPN topology.

The IKE Version tab contains two lists: IKEv1 Enabled Peers and IKEv2 Enabled Peers. When you configure the IPsec proposal, as described in Configuring IPsec Proposals in Site-to-Site VPNs , on page 23, you select which IKE versions to allow in the VPN (version 1, version 2, or both). Security Manager automatically chooses which IKE version to use for a device based on the OS version used by the device. For example, IOS routers always appear in the IKEv1 Enabled Peers list. If a device supports both IKEv1 and IKEv2, it appears in both lists.

You need to alter the selection only if you are allowing both IKE versions in a VPN and you want to specifically prevent some IKEv2-capable devices from using one of the IKE versions.

To change which IKE version is allowed for a device, click the **Select** button beneath the list from which you want to remove the device (or to add the device after previously removing it). A selection dialog box opens where you can do the following (click **OK** to confirm your choices):

- To remove a device, so that it cannot use the IKE version, highlight it in the Selected Peers list and click << to move it to the Available Peers list.

- To add a device, so that it is allowed to use the IKE version, highlight it in the Available Peers list and click >> to move it to the Selected Peers list.

Tip The selection lists include only those devices that support both IKE versions, because you cannot change the version selection for devices that support a single version. IKEv2 is supported on ASA Software 8.4(1)+.

Navigation Path

(Site-to-Site VPN Manager Window) Select a non-Easy VPN topology in the VPNs selector, then select **IPsec Proposal** in the Policies selector. Click the **IKE Version** tab.

Related Topics

- Understanding IKE , on page 5
- Configuring IPsec Proposals in Site-to-Site VPNs , on page 23

Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects

Use the Add or Edit IPSec Transform Set dialog box to configure IPSec transform sets for use in IKE negotiations.

You can create IPSec transform set objects for use in IPSec proposals when defining IPSec-protected traffic in site-to-site and remote access VPNs. During IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Two different security protocols are included within the IPSec standard:

- Encapsulating Security Protocol (ESP)—Provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.
- Authentication Header (AH)—Provides authentication and anti-replay services. AH does not provide encryption and has largely been superseded by ESP. It is also supported on routers only. AH is IP protocol type 51.

Note We recommend using both encryption and authentication on IPSec tunnels.

There are separate IPsec transform set objects based on the IKE version, IKEv1 or IKEv2:

- When you create an IPSec IKEv1 transform set object, you select the mode in which IPSec should operate, as well as define the required encryption and authentication types. Additionally, you can select whether to include compression in the transform set. You can select single options for the algorithms, so if you want to support multiple combinations in a VPN, you must create multiple IPsec IKEv1 transform set objects.
- When you create an IPSec IKEv2 transform set object, you can select all of the encryption and hash algorithms that you will allow in a VPN. During IKEv2 negotiations, the peers select the most appropriate options that each support.

Note If you configure an IPsec IKEv1 or IKEv2 Proposal on a device, you must use the configured Proposal for that device. For example, in a Site-to-Site (Point-to-Point) VPN configuration, the endpoint (interface) configured with the IPsec Proposal can be used in generating the crypto map. However, if the configured Proposal is not used by Security Manager for that device, in the following preview configuration, Security Manager will generate a negate command and the configured IPsec Proposal will be negated by Security Manager.

Navigation Path

Select **Manage > Policy Objects**, then select **IPSec Transform Sets > IPSec IKEv1 Transform Sets** or **IPSec Transform Sets > IPSec IKEv2 Transform Sets** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Transform Sets , on page 21
- Overview of IKE and IPsec Configurations , on page 2
- Comparing IKE Version 1 and 2 , on page 4
- Understanding IKE , on page 5
- Understanding IPsec Proposals , on page 19
- IPsec Proposal Editor (ASA, PIX 7.0+ Devices)
- IPsec Proposal Editor (IOS, PIX 6.3 Devices)
- Configuring an IPsec Proposal on a Remote Access VPN Server (ASA, PIX 7.0+ Devices)
- Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices)
- Configuring IPsec Proposals in Site-to-Site VPNs , on page 23
- Configuring an IPsec Proposal for Easy VPN
- Configuring IKEv1 Proposal Policy Objects , on page 11
- Creating Policy Objects
- Policy Object Manager

Field Reference

Table 4: IPSec IKEv1 or IKEv2 Transform Set Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object. A maximum of 1024 characters is allowed.

Element	Description
Mode (IKEv1 only.)	The mode in which the IPSec tunnel operates: • Tunnel—Tunnel mode encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet. • Transport—Transport mode encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

Element	Description
ESP Encryption	The Encapsulating Security Protocol (ESP) encryption algorithm that the transform set should use. For more information on the following options, see Deciding Which Encryption Algorithm to Use , on page 6. For IKEv1, select one of the following options. For IKEv2, click **Select** to open a dialog box where you can select all of the options you want to support: **Note** AES-GCM/GMAC can only be configured on 5580 and newer ASA platforms. • (Blank)—Do not use ESP encryption. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option. **Note** Beginning with version 4.22, Cisco Security Manager does not support DES and 3DES ESP Encryption Algorithms for IPsec IKEv1 proposal, because they are no longer considered secure againt modern threats. • AES-128 (AES)—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • ESP-Null (NULL)—A null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this is typically used for testing purposes only. • AES-GCM (IKEv2 only)—Encrypts according to the Advanced Encryption Standard in Galois/Counter Mode using 128-bit keys. (ASA 9.0.1+ devices only). • AES-GCM-192 (IKEv2 only)—Encrypts according to the Advanced Encryption Standard in Galois/Counter Mode using 192-bit keys. (ASA 9.0.1+ devices only). • AES-GCM-256 (IKEv2 only)—Encrypts according to the Advanced Encryption Standard in Galois/Counter Mode using 256-bit keys. (ASA 9.0.1+ devices only). • AES-GMAC (IKEv2 only)—Encrypts according to the Advanced Encryption Standard Galois Message Authentication Codeusing 128-bit keys. • AES-GMAC-192 (IKEv2 only)—Encrypts according to the Advanced Encryption Standard Galois Message Authentication Codeusing 192-bit keys. • AES-GMAC-256 (IKEv2 only)—Encrypts according to the Advanced Encryption Standard Galois Message Authentication Code using 256-bit keys.

Element	Description
ESP Hash Algorithm (IKEv1) ESP Integration Algorithm (IKEv2) AH Hash Algorithm (IKEv1 only)	The hash or integrity algorithm to use in the transform set for authentication. For IKEv1, the default is to use SHA for ESP authentication and to not use AH authentication. For IKEv2, there is no default. The AH hash algorithm is used on routers only. For IKEv1, select one of the following options. For IKEv2, click **Select** to open a dialog box where you can select all of the options you want to support. • None—Does not perform ESP or AH authentication. • SHA, SHA-1 (Secure Hash Algorithm version 1)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5, but requires more processing time. The following options, which are even more secure, are available for IKEv2 configurations on ASA 8.4(2+) devices: • SHA512—A 512-bit key. • SHA384—A 384-bit key. • SHA256—A 256-bit key. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA, but is less secure. • Null—No encryption algorithm. For use with AES-GCM, AES-GCM-192, AES-GCM-256, AES-GMAC, AES-GMAC-192, and AES-GMAC-256 only.
Compression (IKEv1 only, IOS devices only.)	Whether to compress the data in the IPSec tunnel using the Lempel-Ziv-Stac (LZS) algorithm.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects.

Configuring VPN Global Settings

You can define global settings that apply to all devices in your remote access or site-to-site VPN topology. These settings include Internet Key Exchange (IKE), IKEv2, IPsec, NAT, and fragmentation definitions. The global settings typically have defaults that work in most situations, so configuring the Global Settings policy is optional in most cases; configure it only if you need non-default behavior or if you are supporting IKEv2 negotiations in a remote access IPsec VPN.

Note The VPN Global Settings policy for site-to-site VPNs applies to all technologies except GET VPN. For an explanation of global settings for GET VPN, see Configuring Global Settings for GET VPN.

Step 1 Do one of the following to open the global settings policy based on the type of VPN you are configuring:

- For remote access VPNs, do one of the following:
  - (Device View) Select **Remote Access VPN > Global Settings** from the Policy selector.
  - (Policy View) Select **Remote Access VPN > Global Settings** from the Policy Type selector. Select an existing policy or create a new one.
- For site-to-site VPNs, do one of the following:
  - Open the Site-to-Site VPN Manager Window, select a topology in the VPNs selector, then select **VPN Global Settings** in the Policies selector.
  - (Policy view) Select **Site-to-Site VPN > VPN Global Settings** from the Policy Types selector. Select an existing shared policy or create a new one.

Step 2 Select the desired tab and configure the settings as needed:

- **ISAKMP/IPsec Settings**—To configure global settings for IKE and IPsec. For detailed information about the options, see Configuring VPN Global ISAKMP/IPsec Settings , on page 34.
- **IKEv2 Settings**—To configure global settings for IKE version 2 negotiations. For detailed information about the options, see Configuring VPN Global IKEv2 Settings , on page 38.
- **NAT Settings**—To configure NAT behavior. For detailed information about the options, see Configuring VPN Global NAT Settings , on page 43. Also see Understanding NAT in VPNs , on page 42.
- **Address Assignment**—To specify one or more methods of address assignment to remote clients, see Configuring VPN Global Address Assignment Settings , on page 32. The address assignment applies only to remote access VPN.
- **General Settings**—To configure fragmentation behavior and some other miscellaneous options. For detailed information about the options, see Configuring VPN Global General Settings , on page 44.

Configuring VPN Global Address Assignment Settings

Use the Address Assignment tab of the VPN Global Settings page to specify one or more methods of address assignment to remote clients. The available methods are:

- Obtain IP addresses from an authentication server.
- Obtain IP addresses from a DHCP server.
- Obtain IP addresses from an internally configured pool.

Note You can configure address assignment on devices running the ASA software version 7.0(1) or later. By default all the methods are enabled.

Address Assignment is supported for ASA 9.5(2) Remote Access VPN in Multi-context mode.

Navigation Path

- For remote access VPNs, do one of the following:
  - (Device View) Select **Remote Access VPN > Global Settings** from the Policy selector. Click the **Address Assignment** tab.
  - (Policy View) Select **Remote Access VPN > Global Settings** from the Policy Type selector. Select an existing policy or create a new one, then click the **Address Assignment** tab.

Related Topics

- Configuring VPN Global Settings , on page 31

Field Reference

Table 5: VPN Global Settings Page, Address Assignment Tab

Element	Description
IPv4 Address Assignment Priority	
Use Authentication Server	Choose to assign IPv4 addresses retrieved from an authentication server on a per-user basis. If you are using an authentication server (external or internal) that has IPv4 addresses configured, we recommend using this method. If you select this option, use the **Platform** > **Device Admin** > **AAA** policy to define the AAA server groups to use for authenticating user access. This method is available for IPv4 and IPv6 assignment policies.
Use DHCP	Choose to obtain IP addresses from a DHCP server. If you use DHCP, you must configure the server using the **Platform** > **Device Admin** > **Server Access** > **DHCP Server** from the Device Policy selector. You must also define the range of IP addresses that the DHCP server can use. This method is available for IPv4 assignment policies.
Use internal address pools	Choose to have the ASA assign IPv4 addresses from an internally configured pool. Internally configured address pools are the easiest method of address pool assignment to configure. If you use this method, you must configure the IP address pools. To configure IP address pools, on the Device view, select **NAT** > **Address Pools** from the Device Policy Selector. Or on the Policy view, select **NAT (PIX/ASA/FWSM)** > **Address Pools** from the Policy Type selector, then select an existing policy from the Shared Policy selector, or right-click **Address Pools** to create a new policy.
Allow the reuse of an IP address - minutes after it is released	Delays the reuse of an IP address after its return to the address pool. Adding a delay helps to prevent problems firewalls can experience when an IP address is reassigned quickly. By default, this is unchecked, meaning the ASA does not impose a delay. To add a delay, check the box and enter the number of minutes in the range 0 - 480 to delay IP address reassignment. **Note** This feature is available on devices running the ASA software version 8.0(3) or later.

Element	Description
IPv6 Address Assignment Priority - Security Manager 4.12 onwards for ASA devices running version 9.0 or later.	
Use Authentication Server	Choose to assign IPv6 addresses retrieved from an authentication server on a per-user basis. If you are using an authentication server (external or internal) that has IPv6 addresses configured, we recommend using this method. If you select this option, use the **Platform** > **Device Admin** > **AAA** policy to define the AAA server groups to use for authenticating user access.
Use internal address pools	Choose to have the ASA assign IPv6 addresses from an internally configured pool. Internally configured address pools are the easiest method of address pool assignment to configure. If you use this method, you must configure the IP address pools. To configure IPv6 address pools, on the Device view, select **NAT** > **Address Pools** from the Device Policy Selector. Or on the Policy view, select **NAT (PIX/ASA/FWSM)** > **Address Pools** from the Policy Type selector, then select an existing policy from the Shared Policy selector, or right-click **Address Pools** to create a new policy.

Configuring VPN Global ISAKMP/IPsec Settings

Use the ISAKMP/IPsec Settings tab of the VPN Global Settings page to specify global settings for Internet Key Exchange (IKE) and IPsec.

The Internet Key Exchange (IKE) protocol, also called the 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 ISAKMP negotiation is divided into a Phase 1 and Phase 2. Phase 1 creates the first tunnel, which protects ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data.

To set terms for ISAKMP negotiations, you create an IKE proposal. For more information, see Configuring an IKE Proposal , on page 10.

About IKE Keepalive

With IKE keepalive, tunnel peers exchange messages that demonstrate they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals, and any disruption in that interval results in the creation of a new tunnel, using a backup device.

Devices that rely on IKE keepalive for resiliency transmit their keepalive messages regardless of whether they are exchanging other information. These keepalive messages can therefore create a small but additional demand on your network.

A variation on IKE keepalive called keepalive dead-peer detection (DPD) sends keepalive messages between peer devices only when no incoming traffic is received and outbound traffic needs to be sent. If you want to send DPD keepalive messages when no incoming traffic is received regardless of whether there is any outbound traffic, you can specify this using the Periodic option.

Navigation Path

- For remote access VPNs, do one of the following:
  - (Device View) Select **Remote Access VPN > Global Settings** from the Policy selector. Click the **ISAKMP/IPsec Settings** tab.

- (Policy View) Select **Remote Access VPN > Global Settings** from the Policy Type selector. Select an existing policy or create a new one, then click the **ISAKMP/IPsec Settings** tab.

- For site-to-site VPNs, do one of the following:
  - Open the Site-to-Site VPN Manager Window, select a topology in the VPNs selector, then select **VPN Global Settings** in the Policies selector. Click the **ISAKMP/IPsec Settings** tab.
  - (Policy view) Select **Site-to-Site VPN > VPN Global Settings** from the Policy Types selector. Select an existing shared policy or create a new one, then click the **ISAKMP/IPsec Settings** tab.

Related Topics

- Configuring VPN Global Settings , on page 31
- Understanding IKE , on page 5
- Understanding IPsec Proposals , on page 19

Field Reference

Table 6: VPN Global Settings Page, ISAKMP/IPsec Settings Tab

Element	Description
ISAKMP Settings	
Enable Keepalive	Whether to configure dead-peer detection (DPD) settings. If the peer fails to respond, a new tunnel is constructed on the assumption that the peer is no longer available. IKE keepalive is defined on the spokes in a hub-and-spoke VPN topology, on both devices in a point-to-point VPN topology, or in remote access VPN configurations. Configure the following options: • Interval—The number of seconds the peer can be idle before beginning keepalive monitoring. The range is 10-3600 seconds. The default is 10, although the ASA device default for remote access groups is 300. • Retry—The interval in seconds between retries after a keepalive response has not been received. The range is 2-10 seconds for ASA, 2-60 for IOS devices. The default is 2 seconds. • Periodic—(Routers running IOS Software version 12.3(7)T and later, except 7600 devices.) Whether to send DPD keepalive messages at regular intervals regardless of IPsec traffic. This changes how the interval value is used. • Infinite—(ASA only.) Whether to ignore the interval and retry settings and allow the peer to be idle indefinitely.

Element	Description

Identity	During Phase I IKE negotiations, peers must identify themselves to each other. Select one of the following:
	• Address—Use the IP address of the host exchanging ISAKMP identity information. This is the default.
	• Hostname—Use the fully-qualified domain name of the host exchanging ISAKMP identity information.
	• Auto/DN—Use automatic selection or distinguished name based on device type:
	  • Distinguished Name (IOS devices only)—Use a distinguished name (DN) to identify a user group name.
	  • Auto (ASA devices only)—Determine ISAKMP negotiation by connection type; IP address for preshared key or certificate distinguished name for certificate authentication.

SA Requests System Limit	Supported on routers running Cisco IOS Software Release 12.3(8)T and later, except 7600 routers. The maximum number of SA requests allowed before IKE starts rejecting them, from 0 to 99999. The number must equal or exceed the number of peers, or the VPN tunnels might be disconnected.
SA Requests System Threshold	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. The percentage of system resources that can be used before IKE starts rejecting new SA requests. The default is 75 percent.
Enable Aggressive Mode (Site to site VPNs only.)	Supported on ASA devices and PIX 7.0+ devices. When selected, enables you to use aggressive mode in ISAKMP negotiations. Aggressive mode is enabled by default.
IPsec Settings	
Enable Lifetime	Select to enable you to configure the global lifetime settings for the crypto IPsec security associations (SAs) on the devices in your site-to-site or remote access VPN. Configure the following: • Lifetime (secs)—The number of seconds a security association will exist before expiring. The default is 3,600 seconds (1 hour). • Lifetime (kbytes)—The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires. The default is 4,608,000 kilobytes.

Element	Description
Xauth Timeout	Supported on Cisco IOS routers and Catalyst 6500/7600 devices in remote access VPN and Easy VPN topologies only. The number of seconds the device will wait for a system response to the Xauth challenge. When negotiating tunnel parameters for establishing IPsec tunnels in a remote access or Easy VPN configuration, Xauth adds another level of authentication that identifies the user who requests the IPsec connection. Using the Xauth feature, the client waits for a username/password (Xauth) challenge after the IKE SA has been established. When the end user responds to the challenge, the response is forwarded to the IPsec peers for an additional level of authentication.
Max Sessions	Supported on ASA devices and PIX 7.0+ devices. The maximum number of security associations (SAs) that can be enabled simultaneously on the device. The maximum number differs based on device model. For ASA devices, the limits are: • 5505—10 sessions. • 5510—250 sessions. • 5520—750 sessions. • 5540, 5550, 5585-X with SSP-10—5000 sessions. • 5580, 5585-X (other models)—10000 sessions.
Enable IPsec via Sysopt	Supported on ASA devices, and PIX Firewalls versions 6.3 or 7.0+. Whether to bypass the access rules defined on the VPN interface for VPN traffic. By default, the device allows VPN traffic to terminate on an interface; you do not need to allow IKE or ESP (or other types of VPN packets) in an interface access list. By default, you also do not need an interface access list for local IP addresses of decrypted VPN packets. Because the VPN tunnel was terminated successfully using VPN security mechanisms, this feature simplifies configuration and maximizes the device performance without any security risks. (Group policy and per-user authorization access lists still apply to the traffic.) If you deselect this option, the interface access rules are also applied to VPN traffic. The access list applies to the local IP address and not to the original client IP address used before the VPN packet was decrypted. The command applied is **no sysopt connection permit-vpn**.
Enable IPsec inner routing lookup (Security Manager version 4.12 onwards for ASA devices 9.6(2) or later)	To enable per-packet routing lookups for the IPsec inner packets. This checkbox is deselected by default.

Element	Description
Enable SPI Recovery (Site-to-site VPNs only.)	Supported on routers running IOS version 12.3(2)T and later, in addition to Catalyst 6500/7600 devices running version 12.2(18)SXE and later. When selected, enables the SPI recovery feature to configure your device so that if an invalid SPI (Security Parameter Index) occurs, an IKE SA will be initiated. SPI is a number which, together with a destination IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association. When an invalid SPI occurs during IPsec packet processing, the SPI recovery feature enables an IKE SA to be established.
ESPv3 Settings	
Enable PMTU (Path Maximum Transmission Unit) Aging	Supported for IKEv2 on ASA devices versions 9.0.1+. Whether to enable Path Maximum Transmission Unit aging. If you select this option, configure the interval, in minutes, at which the PMTU value is reset to its original value. The value can be from 10 to 30 minutes. The default is 10 minutes.

Configuring VPN Global IKEv2 Settings

Use the IKEv2 Settings tab of the VPN Global Settings page to specify global settings for Internet Key Exchange (IKE) version 2. These settings apply to ASA 8.4(x) devices only.

Internet Key Exchange (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 (SA).

Preventing DoS Attacks by Limiting IKEv2 Open SAs

You can prevent denial-of-service (DoS) attacks for IPsec IKEv2 connections by always cookie challenging incoming security associations (SAs) or by limiting the number of open SAs and cookie challenging any additional connections. By default, the ASA does not limit the number of open SAs and never cookie challenges SAs.

You can also limit the number of SAs allowed, which stops further connections from negotiating to protect against memory or CPU attacks that the cookie-challenge feature may be unable to thwart. Limiting the maximum number of SAs can protect the current connections.

With a DoS attack, an attacker initiates the attack when the peer device sends an SA initiate packet and the ASA sends its response, but the peer device does not respond further. If the peer device does this continually, all the allowed SA requests on the ASA can be used up until it stops responding.

Enabling a threshold percentage for cookie challenges limits the number of open SA negotiations. For example, with the default setting of 50%, when 50% of the allowed SAs are in-negotiation (open), the ASA cookie challenges any additional SA initiate packets that arrive. For the Cisco ASA 5580 with 10,000 allowed IKEv2 SAs, after 5000 SAs become open, any more incoming SAs are cookie-challenged.

If used in conjunction with the **Maximum SAs in Negotiation** option, configure a lower cookie-challenge threshold.

Navigation Path

- For remote access VPNs, do one of the following:
  - (Device View) Select **Remote Access VPN > Global Settings** from the Policy selector. Click the **IKEv2 Settings** tab.
  - (Policy View) Select **Remote Access VPN > Global Settings** from the Policy Type selector. Select an existing policy or create a new one, then click the **IKEv2 Settings** tab.
- For site-to-site VPNs, do one of the following:
  - Open the Site-to-Site VPN Manager Window, select a topology in the VPNs selector, then select **VPN Global Settings** in the Policies selector. Click the **IKEv2 Settings** tab.
  - (Policy view) Select **Site-to-Site VPN > VPN Global Settings** from the Policy Types selector. Select an existing shared policy or create a new one, then click the **IKEv2 Settings** tab.

Related Topics

- Configuring VPN Global Settings , on page 31
- Understanding IKE , on page 5
- Understanding IPsec Proposals , on page 19
- Configuring Group Load Balance Policies (ASA)

Field Reference

Table 7: VPN Global Settings Page, IKEv2 Settings Tab

Element	Description
Maximum SAs	The number of allowed IKEv2 connections (security associations) on the device. The default limit is the maximum number of connections specified by the device license, which differs by device model. Specify a number only if you want to create a limit that is lower than the device license. The range is 1 to 10000.
Maximum SAs in Negotiation	The maximum number of IKEv2 security associations (SAs) that can be in negotiation at any time as a percentage of the maximum allowed SAs. The default is no limit on SAs in negotiation, so it is possible for all available SAs to be in negotiation. The range is 1 to 100%. If you configure this option and also enable custom cookie challenge, configure the cookie challenge threshold lower than this limit.

Element	Description
Enable Cookie Challenge	Whether to send cookie challenges to peer devices in response to SA initiate packets, which can help thwart denial of service (DoS) attacks. The default is to use cookie challenges when 50% of the available SAs are in negotiation. Select one of these options: • **Custom**—Cookie challenge when the number of SAs in negotiation exceeds the total number of allowed SAs on the device based on percentage (SAs in negotiation as a percentage of total allowed SAs). In Custom Cookie Challenge, enter the percentage that triggers cookie challenges for any future SA negotiations. The range is 1 to 100%. The default is 50%. • **Never**—The device never uses cookie challenge. • **Always**—The device always uses cookie challenge, regardless of the percentage of SAs in negotiation.
Remote Access Authentication RA Trustpoint (Remote access VPN only.)	(Required when supporting IKEv2 negotiations.) The PKI enrollment object that identifies the Certificate Authority (CA) server that the device can use to authenticate itself to the remote user. This authorization is required before the user can select a connection profile and log into the VPN. This CA server is used in remote access IKEv2 IPsec VPNs only. Click **Select** to select the object or to create a new one. **Note** Beginning with Cisco Security Manager version 4.17, you can configure remote access authentication on ASA 9.9(2) or later multi-context devices. **Tip** You must also select this PKI enrollment object in the Remote Access VPN > Public Key Infrastructure policy.

Element	Description

Load Balancing Settings
Redirect Connections During
(Remote access VPNs only.)
	If you configure load balancing, using the ASA Group Load Balance policy, you can specify the IKEv2 negotiation phase in which a user can be redirected to another device in the group. Select one of these options:
	• **INIT**—Redirect at unauthenticated initiation requests (the first IKEv2 message IKE_SA_INIT), before any group or user authentication.
	  • Pros—This option allows the main server to do minimal processing and state keeping (using CPU and memory) prior to redirecting the connection.
	  • Cons—This option is not as secure as AUTH (even though security risks are minimal) because anyone can get a redirected IP address without authenticating at all.
	• **AUTH** (the default)—Redirect during authentication (during IKE_AUTH). The device still has not identified or authenticated the user at this point, but it allows the client to authenticate the server to make sure it can trust the redirection that it receives.
	  • Pros—This option is more secure as the reply is encrypted in the IKEv2 tunnel and it allows the client side to authenticate the server before retrying with the redirected IP address, providing better DoS protection than the INIT option.
	  • Cons—This option requires more processing as the IKEv2 tunnel needs to be almost brought up before redirecting, although child SAs and data tunnels do not need to be brought up. The client is not authenticated at all. Note that IKEv1 redirection occurs after group authentication of both sides of the tunnel.

Enable Invalid Selectors Notification	Whether to enable sending an IKE notification to the peer when an inbound packet is received on an SA that does not match the traffic selectors for that SA. This feature is available in Security Manager version 4.9 onwards for ASA devices version 9.4(1) or later.
Fragmentation Settings (ASA devices 9.6(1) or later)	
Enable Fragmentation before Encryption	Whether to enable fragmentation of IKEv2 messages. The Internet Key Exchange Version 2 (IKEv2) fragmentation protocol splits large IKEv2 message into a set of smaller ones, called IKE Fragment Messages. Fragmentation is supported on the ASA devices running the software version 9.6(1) or later.
Local MTU Size (ASA)	Enter the MTU size value. MTU size is used to divide the clear text packet into chunks. The MTU value used includes the IP header plus UDP header size. The default MTU size is 576.

Element	Description
Fragmentation Mode (ASA)	Select one of the following: • CSCO—refers to the current Cisco Proprietary Fragmentation method. • IETF—refers to the method defined by the IETF standard: draft-ietf-ipsecme-ikev2-fragmentation. By default IETF is selected.

Understanding NAT in VPNs

Network Address Translation (NAT) enables devices that use internal IP addresses to send and receive data through the Internet. It converts private, internal LAN addresses into globally routable IP addresses when they try to access data on the Internet. In this way, NAT enables a small number of public IP addresses to provide global connectivity for a large number of hosts.

NAT enhances the stability of your hub-and-spoke VPN tunnels or remote access connections because resources required for VPN connections are not used for other purposes, and the VPN tunnel is kept available for traffic requiring complete security. Sites inside the VPN can use NAT through a split tunnel to exchange non secure traffic with outside devices, and they do not squander VPN bandwidth or overwhelm the hub at the tunnel head-end by directing nonessential traffic through it.

Security Manager supports NAT with dynamic IP addressing only, and applies to it an overload feature that permits what is known as port-level NAT or Port Address Translation (PAT). PAT uses port addressing to associate thousands of private NAT addresses with a small group of public IP address. PAT is used if the addressing requirements of your network exceed the available addresses in your dynamic NAT pool.

Note When you enable PAT on Cisco IOS routers, an additional NAT rule is implicitly created for split-tunneled traffic on deployment. This NAT rule, which denies VPN-tunneled traffic and permits all other traffic (using the external interface as the IP address pool), is not reflected as a router platform policy. You can remove the NAT rule by disabling this feature. For more information, see NAT Page: Dynamic Rules.

You can configure traffic to bypass NAT configuration on site-to-site VPN traffic. To bypass NAT configuration on Cisco IOS routers, make sure the **Do Not Translate VPN Traffic** option is selected in the NAT Dynamic Rule platform policy (see NAT Dynamic Rule Dialog Box). To exclude NAT on PIX Firewalls or ASA devices, make sure this option is selected in the NAT Translation Options platform policy (see Translation Options Page).

About NAT Traversal

NAT traversal is used for the transmission of keepalive messages when there is a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow.

If the IP address of the VPN interface on the spoke is not globally routable, the NAT on the middle device replaces it with a new globally routable IP address. This change is made in the IPsec header, and violates the checksum of the spoke causing a mismatch with the hub's checksum calculation. This results in loss of connectivity between the hub and the spoke.

With NAT traversal, the spoke adds a UDP header to the payload. The NAT on the middle device changes the IP address in the UDP header, leaving the IPsec header and checksum intact. On a middle device that uses static NAT, you must provide the static NAT IP address (globally routable) on the inside interface. The static NAT IP address is provided for all traffic through that interface that requires NAT. However, if the middle

device uses dynamic NAT where the NAT IP address is unknown, you must define dynamic crypto on the hub to serve any connection request from the spoke. Security Manager generates the required tunnel configuration for the spoke.

Note NAT traversal is enabled by default on routers running IOS version 12.3T and later. If you want to disable the NAT traversal feature, you must do this manually on the device or using a FlexConfig (see Managing Flexconfigs).

You can define global NAT settings on the NAT Settings tab of the Global VPN Settings page as described in Configuring VPN Global NAT Settings , on page 43.

Configuring VPN Global NAT Settings

Use the NAT Settings tab of the Global Settings page to define global Network Address Translation (NAT) settings that enable devices that use internal IP addresses to send and receive data through the Internet.

Note For site-to-site VPNs, if you want to bypass NAT configuration on IOS routers, make sure that the **Do Not Translate VPN Traffic** option is selected in the NAT Dynamic Rule platform policy (seeNAT Dynamic Rule Dialog Box). To exclude NAT on PIX Firewalls or ASA devices, make sure this option is selected in the NAT Translation Options platform policy (see Translation Options Page).

Navigation Path

- For remote access VPNs, do one of the following:
  - (Device View) Select **Remote Access VPN > Global Settings** from the Policy selector. Click the **NAT Settings** tab.
  - (Policy View) Select **Remote Access VPN > Global Settings** from the Policy Type selector. Select an existing policy or create a new one, then click the **NAT Settings** tab.
- For site-to-site VPNs, do one of the following:
  - Open the Site-to-Site VPN Manager Window, select a topology in the VPNs selector, then select **VPN Global Settings** in the Policies selector. Click the **NAT Settings** tab.
  - (Policy view) Select **Site-to-Site VPN > VPN Global Settings** from the Policy Types selector. Select an existing shared policy or create a new one, then click the **NAT Settings** tab.

Related Topics

- Understanding NAT in VPNs , on page 42
- Configuring VPN Global Settings , on page 31

Field Reference

Table 8: VPN Global Settings Page, NAT Settings Tab

Element	Description
Enable Traversal Keepalive Interval	Whether to enable NAT traversal keepalive. NAT traversal keepalive is used for the transmission of keepalive messages when there is a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow. If you select this option, configure the interval, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active. The value can be from 5 to 3600 seconds. The default is 10 seconds. **Note** On Cisco IOS routers, NAT traversal is enabled by default. If you want to disable the NAT traversal feature, you must do this manually on the device or by using a FlexConfig.
Enable Traversal over TCP TCP Ports (Remote access VPNs only.)	Supported on ASA and PIX 7.0+ devices. When selected, encapsulates both the IKE and IPsec protocols within a TCP packet and enables secure tunneling through both NAT and PAT devices and firewalls. If you select this option, specify the TCP ports for which you want to enable NAT traversal (NAT-T). You must configure TCP ports on the remote clients and on the VPN device. The client configuration must include at least one of the ports you set for the security appliance. You can enter up to 10 ports. **Tip** These ports are used for IKEv1 connections only. IKEv2 uses ports 500 and 4500 for NAT-T. Ensure that any ports that you specify are opened in the access rules for the applicable interface.
Enable PAT (Port Address Translation) on Split Tunneling for Spokes (Site-to-site VPNs only.)	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. When selected, enables Port Address Translation (PAT) to be used for split-tunneled traffic on spokes in your VPN topology. PAT can associate thousands of private NAT addresses with a small group of public IP address through the use of port addressing. PAT is used if the addressing requirements of your network exceed the available addresses in your dynamic NAT pool. **Note** When you select this option, Security Manager implicitly creates an additional NAT rule for split-tunneled traffic on deployment. This NAT rule, which denies VPN-tunneled traffic and permits all other traffic (using the external interface as the IP address pool), is not reflected as a router platform policy. For information on creating or editing a dynamic NAT rule as a router platform policy, see NAT Page: Dynamic Rules.

Configuring VPN Global General Settings

Use the General Settings tab of the VPN Global Settings page to define fragmentation settings including maximum transmission unit (MTU) handling parameters for site-to-site and remote access VPNs.

Fragmentation breaks a packet into smaller units when it is transmitted over a physical interface that cannot support the original size of the packet. Fragmentation minimizes packet loss in a VPN tunnel, because it enables transmission of secured packets that might otherwise be too large to transmit. This is particularly relevant when using GRE, because any packet of more than 1420 bytes will not have enough room in its header for the additional 80 bytes that the combined use of IPsec and GRE adds to the packet payload.

The maximum transmission unit (MTU) specifies the maximum packet size, in bytes, that an interface can handle. If a packet exceeds the MTU, it is fragmented, typically after encryption. If the DF (Do Not Fragment) bit is set, the packet is dropped. A DF bit is a bit within the IP header that indicates if a device can fragment a packet. You must specify whether the device can clear, set, or copy the DF bit from the encapsulated header.

Because reassembly of an encrypted packet is difficult, fragmentation can degrade network performance. To prevent network performance problems, you can select **Enable Fragmentation Before Encryption** so that fragmentation occurs before encryption.

Navigation Path

- For remote access VPNs, do one of the following:
  - (Device View) Select **Remote Access VPN > Global Settings** from the Policy selector. Click the **General Settings** tab.
  - (Policy View) Select **Remote Access VPN > Global Settings** from the Policy Type selector. Select an existing policy or create a new one, then click the **General Settings** tab.
- For site-to-site VPNs, do one of the following:
  - Open the Site-to-Site VPN Manager Window, select a topology in the VPNs selector, then select **VPN Global Settings** in the Policies selector. Click the **General Settings** tab.
  - (Policy view) Select **Site-to-Site VPN > VPN Global Settings** from the Policy Types selector. Select an existing shared policy or create a new one, then click the **General Settings** tab.

Related Topics

- Configuring VPN Global Settings , on page 31

Field Reference

Table 9: VPN Global Settings Page, General Settings Tab

Element	Description
Fragmentation Settings	

Element	Description
Fragmentation Mode Local MTU Size	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. Fragmentation minimizes packet loss in a VPN tunnel when packets are transmitted over a physical interface that cannot support the original size of the packet. Select the fragmentation mode: • **No Fragmentation**—Do not fragment before IPsec encapsulation. After encapsulation, the device fragments packets that exceed the MTU setting before transmitting them through the public interface. • **End to End MTU Discovery**—Use ICMP messages to determine the maximum MTU. Use this option with IPsec VPNs. End-to-end MTU discovery uses Internet Control Message Protocol (ICMP) messages to determine the maximum MTU that a host can use to send a packet through the VPN tunnel without causing fragmentation. The MTU setting for each link in a transmission path is checked to ensure that no transmitted packet exceeds the smallest MTU in that path. The discovered MTU is used to decide whether fragmentation is necessary. If ICMP is blocked, MTU discovery fails and packets are either lost (if the DF bit is set) or fragmented after encryption (if the DF bit is not set). **Note** (Site-to-site VPNs) For Catalyst 6500/7600 devices, end-to-end path MTU discovery is supported only on images 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXH, 12.2(33)SXI or above. • **Local MTU Handling**—Set the MTU locally on the devices. This option is typically used when ICMP is blocked or in site-to-site IPsec/GRE VPNs. If you select this option, specify the local MTU size, which can be between 68 and 65535 bytes depending on the VPN interface.
DF Bit	Supported on Cisco IOS routers, Catalyst 6500/7600 devices, PIX 7.0+ and ASA devices. A Do Not Fragment (DF) bit within an IP header determines whether a device is allowed to fragment a packet. Select how to handle the DF bit: • **Copy**—Copy the DF bit from the encapsulated header in the current packet to all the device's packets. If the packet's DF bit is set to fragment, all future packets are fragmented. This is the default option. • **Set**—Set the DF bit in the packet you are sending. A large packet that exceeds the MTU is dropped and an ICMP message is sent to the packet's initiator. • **Clear**—Fragment packets regardless of the original DF bit setting. If ICMP is blocked, MTU discovery fails and packets are fragmented only after encryption.

Element	Description
Enable Fragmentation Before Encryption	Supported on Cisco IOS routers, Catalyst 6500/7600 devices, PIX 7.0+ and ASA devices. When selected, enables fragmentation to occur before encryption if the expected packet size exceeds the MTU. Look ahead Fragmentation (LAF) is used before encryption takes place to calculate the packet size that would result after encryption, depending on the transform sets configured on the IPsec SA. If the packet size exceeds the specified MTU, the packet will be fragmented before encryption.
Enable Notification on Disconnection	Supported on ASA and PIX 7.0+ devices. When selected, enables the device to notify qualified peers of sessions that are about to be disconnected. The peer receiving the alert decodes the reason and displays it in the event log or in a pop-up window. This feature is disabled by default. IPsec sessions might be dropped for several reasons, such as a security appliance shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.
Enable Split Tunneling (Site-to-site VPN only.)	When selected (the default), enables you to configure split tunneling in your site-to-site VPN topology. Split tunneling allows you to transmit both secured and unsecured traffic on the same interface. Split tunneling requires that you specify exactly which traffic will be secured and what the destination of that traffic is, so that only the specified traffic enters the IPsec tunnel, while the rest is transmitted unencrypted across the public network.
Enable Spoke-to-Spoke Connectivity through the Hub	Supported on ASA and PIX 7.0+ devices. When selected, enables direct communication between spokes in a hub-and-spoke VPN topology in which the hub is an ASA or PIX 7.0+ device.
Enable Default Route	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. When selected, the device uses the configured external interface as the default outbound route for all incoming traffic.
Do not reboot until all the sessions are terminated (ASA)	Select this option if you want the ASA to postpone a scheduled reboot until all active sessions terminate. This feature is disabled by default. **Note** The **crypto isakmp reload-wait** command in ASA software is supported only in System context for ASA devices that are on multiple context mode. However, since System context is not supported on VPN configurations, Security Manager does not generate this command for devices in VPN configuration, that are on multiple context mode. You must use the FlexConfig policies in System context for the **crypto isakmp reload-wait** command to work on devices that are on multiple context mode. FlexConfig policies allow you to configure device commands that are not otherwise supported by Security Manager. For more information, see Managing Flexconfigs.

Understanding IKEv1 Preshared Key Policies in Site-to-Site VPNs

If you want to use preshared key as your authentication method for IKEv1 negotiations, you must define a shared key for each tunnel between two peers that will be their shared secret for authenticating the connection. The key will be configured on each peer. If the key is not the same on both peers of the tunnel, the connection cannot be established. The peer addresses that are required for configuring the preshared key are deduced from the VPN topology.

Tip You can also use preshared keys for IKEv2 negotiations, but the configuration is different from the one used for IKEv1, as are the rules and requirements. For information on configuring preshared keys for IKEv2 negotiations, see Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.

Preshared keys are configured on spokes. In a hub-and-spoke VPN topology, Security Manager mirrors the spoke's preshared key and configures it on its assigned hub, so that the key on the spoke and hub are the same. In a point-to-point VPN topology, you must configure the same preshared key on both peers. In a full mesh VPN topology, any two devices that are connected must have the same preshared key.

In a preshared key policy, you can use a specific key, or you can use automatically generated keys for peers participating in each communication session. Using automatically generated keys (the default method) is preferred, because security can be compromised if all connections in a VPN use the same preshared key.

Beginning with 4.16, Cisco Security Manager does not support IKEv1 related configuration for Firepower 9300 devices with distributed mode.

While discovering a VPN topology, where one of the devices is in cluster distributed mode (IKEv2 configured), and other is a non-cluster mode (IKEv1 and IKEv2 configured), Cisco Security Manager does not display any error. However, during preview config, the activity validation error is displayed to remove IKEv1 related configuration.

There are three methods for negotiating key information and setting up IKE security associations (SAs):

- Main mode address—Negotiation is based on IP address. Main mode provides the highest security because it has three two-way exchanges between the initiator and receiver. This is the default negotiation method.

This method has three options for creating keys:

- You can create a key for each peer, based on the unique IP address of each peer, providing high security.
- You can create a group preshared key on a hub in a hub-and-spoke VPN topology, to be used for communication with any device in a specified subnet. Each peer is identified by its subnet, even if the IP address of the device is unknown. In a point-to-point or full mesh VPN topology, a group preshared key is created on the peers.
- You can create a wildcard key on a hub in a hub-and-spoke VPN topology, or on a group containing hubs, to be used for dynamic crypto where a spoke does not have a fixed IP address or belong to a specific subnet. All spokes connecting to the hub have the same preshared key, which could compromise security. In a point-to-point or full mesh VPN topology, a wildcard key is created on the peers.

Note If you are configuring DMVPN with direct spoke-to-spoke connectivity, you create a wildcard key on the spokes.

- Main mode fully qualified domain name (FQDN)—Negotiation is based on DNS resolution, with no reliance on IP address. This option can only be used if the DNS resolution service is available for the host. It is useful when managing devices with dynamic IP addresses that have DNS resolution capabilities.
- Aggressive mode—Negotiation is based on hostname (without DNS resolution) and domain name. Aggressive mode is less secure than main mode. However, it provides more security than using group preshared keys if the IP address of the VPN interface on the host is unknown, and the FQDN of the dynamic IP peer is not DNS resolvable. This negotiation method is recommended for use with a GRE Dynamic IP or DMVPN failover and routing policy.

Related Topics

- Deciding Which Authentication Method to Use , on page 9
- Configuring IKEv1 Preshared Key Policies , on page 49

Configuring IKEv1 Preshared Key Policies

Use the IKEv1 Preshared Key page to define the preshared key configuration when using IKEv1 in a site-to-site VPN topology. For information on configuring preshared keys when using IKEv2, see Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.

Note The preshared key policy does not apply to Easy VPN topologies.

Note Beginning with 4.16, Cisco Security Manager does not support IKEv1 preshared key configuration for Firepower 9300 devices with distributed mode.

To open the IKEv1 Preshared Key page:

- (Site-to-Site VPN Manager Window) Select a topology in the VPNs selector, then select **IKEv1 Preshared Key** in the Policies selector.
- (Policy view) Select **Site-to-Site VPN > IKEv1 Preshared Key** from the Policy Types selector. Select an existing shared policy or create a new one.

The following table explains the settings you can configure in this policy.

Table 10: IKEv1 Preshared Key Page

Element	Description
Key Specification Select whether to manually define the key (User Defined) or to have the key automatically generated. There are additional options you can configure when using auto generated keys.	
User Defined	When selected, enables you to use a manually defined preshared key. Enter the required preshared key in the **Key** field, then enter it again in the **Confirm** field.
Auto Generated	When selected, allocates a random key to the participating peers. This ensures security because a different key is generated for every hub-spoke connection. Auto Generated is the default selection. Auto generated is not a useful option when you do not manage all nodes in the VPN, for example, in the case of an Extranet VPN. **Note** The key is allocated during the first deployment to the devices and is used in all subsequent deployments to the same devices, until you select the Regenerate Key (Only in Next Deployment) check box.
Key Length	The required length of the preshared key to be automatically generated, from 1 to 127. The default is 24.
Same Key for All Tunnels	Unavailable in a point-to-point VPN topology. When selected, enables you to use the same auto-generated key for all tunnels. **Note** If you do not select this option, different keys are used for the tunnels, except in cases, such as DMVPN configuration, when different multipoint GRE interfaces in the same network must use the same preshared key.
Regenerate Key (Only in Next Deployment)	When selected, enables Security Manager to generate a new key for the next deployment to the devices. This is useful if it is possible that the secrecy of the keys might be compromised. When you submit the job for deployment, this check box is cleared. It does not remain selected because the new key will only be generated for the upcoming deployment, and not for subsequent deployments (unless you select it again).
Negotiation Method Select the type of negotiation method. The methods are explained in more detail in Understanding IKEv1 Preshared Key Policies in Site-to-Site VPNs , on page 48.	

Element	Description
Main Mode Address	Use this negotiation method for exchanging key information if the IP address of the devices is known. Negotiation is based on IP address. Main mode provides the highest security because it has three two-way exchanges between the initiator and receiver. Main mode address is the default negotiation method. Select one of the following options to define the negotiation address type: • **Peer Address**—Negotiation is based on the unique IP address of each peer. A key is created for each peer, providing high security. This is the default. • **Subnet**—Creates a group preshared key on a hub in a hub-and-spoke topology to use for communication with any device in a specified subnet, even if the IP address of the device is unknown. Each peer is identified by its subnet. In a point-to-point or full mesh VPN topology, a group preshared key is created on the peers. Enter the subnet in the field provided, for example, 10.10.10.0/24. • **Wildcard**—Creates a wildcard key on a hub or on a group of hubs in a hub-and-spoke topology to use when a spoke does not have a fixed IP address or belong to a specific subnet. In this case, all spokes connecting to the hub have the same preshared key, which could compromise security. Use this option if a spoke in your hub-and-spoke VPN topology has a dynamic IP address. In a point-to-point or full mesh VPN topology, a wildcard key is created on the peers. **Note** When configuring DMVPN with direct spoke-to-spoke connectivity, you create a wildcard key on the spokes.
Main Mode FQDN	Select this negotiation method for exchanging key information if the IP address is not known and DNS resolution is available for the devices. Negotiation is based on DNS resolution, with no reliance on IP address.
Aggressive Mode	Available only in a hub-and-spoke VPN topology. Select this negotiation method for exchanging key information if the IP address is not known and DNS resolution might not be available on the devices. Negotiation is based on hostname and domain name. **Note** If direct spoke to spoke tunneling is enabled, you cannot use aggressive mode.

Related Topics

• Understanding IKEv1 Preshared Key Policies in Site-to-Site VPNs , on page 48

Understanding Public Key Infrastructure Policies

Security Manager supports IPsec configuration with Certification Authority (CA) servers that manage certificate requests and issue certificates to devices in your VPN topology. You can create a Public Key Infrastructure (PKI) policy to generate enrollment requests for CA certificates and RSA keys, and manage keys and certificates, providing centralized key management for the participating devices.

CA servers, also known as trustpoints, manage public CA certificate requests and issue certificates to participating IPsec network devices. When you use Certificates as the authentication method for IKE and IPsec proposal policies, peers are configured to obtain digital certificates from a CA server. With a CA server, you do not have to configure keys between all the encrypting devices. Instead, you individually enroll each participating device with the CA server, which is explicitly trusted to validate identities and create a digital certificate for the device. When this has been accomplished, each participating peer can validate the identities of the other participating peers and establish encrypted sessions with the public keys contained in the certificates.

CAs can also revoke certificates for peers that no longer participate in an IPsec VPN topology. Revoked certificates are either managed by an Online Certificate Status Protocol (OCSP) server or are listed in a certificate revocation list (CRL) stored on an LDAP server, which each peer can check before accepting a certificate from another peer.

PKI enrollment can be set up in a hierarchical framework consisting of multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. Subordinate CAs within the hierarchy can enroll with either the root CA or with another subordinate CA. Within a hierarchical PKI, all enrolled peers can validate each other's certificate if the peers share a trusted root CA certificate or a common subordinate CA.

Keep the following in mind:

- PKI policies can be configured on Cisco IOS routers running version 12.3(7)T and later, PIX Firewalls, and Adaptive Security Appliance (ASA) devices for site-to-site and remote access VPNs.
- In site-to-site VPNs, you use the IKEv1 Public Key Infrastructure policy to identify CA servers for IKEv1 negotiations only. For IKEv2 negotiations, you identify the CA servers in the IKEv2 Authentication policy as described in Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.
- To save the RSA key pairs and the CA certificates between reloads permanently to Flash memory on a PIX Firewall release 6.3, you must configure the **ca save all** command. You can do this manually on the device or using a FlexConfig.

CA Server Authentication Methods

You can authenticate the CA server using one of the following methods:

- Using the Simple Certificate Enrollment Protocol (SCEP) to retrieve the CA's certificates from the CA server. Using SCEP, you establish a direct connection between your device and the CA server. Be sure your device is connected to the CA server before beginning the enrollment process. Because this method of retrieving CA certificates for routers is interactive, you can deploy your PKI policy to live devices only, not to files.

Note When using SCEP, you must enter the fingerprint for the CA server. If the value you enter does not match the fingerprint on the certificate, the certificate is rejected. You can obtain the CA's fingerprint by contacting the server directly, or by entering the following address in a web browser: **http://<URLHostName>/certsrv/mscep/mscep.dll**.

- Manually creating an enrollment request that you can submit to a CA server offline, by copying the CA server's certificates from another device.

Use this method if your device cannot establish a direct connection to the CA server or if you want to generate an enrollment request and send it to the server at a later time.

Note This method enables you to deploy the PKI policy either to devices or to files.

For more information, see PKI Enrollment Dialog Box , on page 59.

Note You can also use Cisco Secure Device Provisioning (SDP) to enroll for a certificate for a router. For more information about using SDP for certificate enrollment, see Secure Device Provisioning on Cisco IOS Routers.

The following topics explain Public Key Infrastructure configuration in more detail:

Requirements for Successful PKI Enrollment

The following are prerequisites for configuring a PKI policy in your network:

- For IKEv1, the IKE proposal must specify Certificate for the IKE authentication method. See Configuring IKEv1 Proposal Policy Objects , on page 11.
- The domain name must be defined on the devices for PKI enrollment to be successful (unless you specify the CA server nickname).
- To enroll with the CA server directly, you must specify the server's enrollment URL.
- To enroll with the CA server by means of a TFTP server, you must ensure that the CA certificates file is saved to the TFTP server. After deployment of the PKI policy, you must copy the certificate request from your TFTP server to the CA server.
- You may specify an RSA public key to use in the enrollment request. If you do not specify an RSA key pair, the Fully Qualified domain Name (FQDN) key will be used.

If using RSA keys, once the certificate has been granted, the public key is included in the certificate so that peers can use it to encrypt data sent to the device. The private key is kept on the device and used to decrypt data sent by peers, and to digitally sign transactions when negotiating with peers. You can use an existing key pair or generate a new one. If you want to generate a new key pair to use in the certificate for router devices, you must also specify the modulus to determine the size of the key.

For more information, see PKI Enrollment Dialog Box—Enrollment Parameters Tab , on page 65.

- If you are making a PKI enrollment request on a Cisco Easy VPN IPsec remote access system, you must configure each remote component (spoke) with the name of the user group to which it connects. You specify this information in the Organization Unit (OU) field in the Certificate Subject Name tab of the PKI Enrollment Editor dialog box.

Note You do not need to configure the name of the user group on the hub (Easy VPN server).

For more information, see PKI Enrollment Dialog Box—Certificate Subject Name Tab , on page 68.

- To deploy PKI policies to files (not to live devices), the following prerequisites must be met:
  - Routers must run Cisco IOS Software 12.3(7)T or later.
  - CA authentication certificates must be cut and pasted into the Security Manager user interface (so that CA authentication is not interactive and does not require communication with the live device).
- If you are deploying to live devices, the PKI server must be online.
- Security Manager supports the Microsoft, Verisign, and Entrust PKIs.
- Security Manager supports Cisco IOS Certificate Servers. The Cisco IOS Certificate Server feature embeds a simple certificate server, with limited CA functionality, into the Cisco IOS software. An IOS Certificate Server can be configured as a FlexConfig policy. For more information, see Managing Flexconfigs.
- To configure PKI with AAA authorization that uses the entire subject name on an IOS router, use the predefined FlexConfig object named IOS_PKI_WITH_AAA.

Prerequisites for PKI Enrollment Using TFTP

If you do not have constant direct access to the CA server, you can enroll using TFTP if your devices are routers running Cisco IOS Software 12.3(7)T or later.

On deployment, Security Manager generates the corresponding CA trustpoint command and authenticate command. The trustpoint command is configured with the enrollment URL tftp://<certserver> <file_specification> entry to retrieve the CA certificate using TFTP. If file_specification is not specified, the FQDN of the router is used.

Before using this option, you must make sure that the CA certificates file (.ca) is saved on the TFTP server. To do this, use this procedure:

1. Connect to http://servername/certsrv, where servername is the name of the Windows 2000 web server on which the CA you want to access is located.
2. Select **Retrieve the CA certificate or certificate revocation list**, then click **Next**.
3. Select **Base64 encoded**, then click **Download CA certificate**.
4. Save the .crt file as a .ca file on the TFTP server using your browser's Save As function.

After deployment, you must transfer the certificate request generated by Security Manager on the TFTP server to the CA, and then transfer the device's certificates from the CA to the device.

Transferring the Certificate Request from the TFTP Server to the CA Server

Security Manager creates a PKCS#10 formatted enrollment request (.req) on the TFTP server. You must transfer it to the PKI server using this procedure:

1. Connect to http://servername/certsrv, where servername is the name of the Windows 2000 web server where the CA you want to access is located.

2. Select **Request a certificate**, then click **Next**.
3. Select **Advanced request**, then click **Next**.
4. Select **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**, then click Next.
5. Either select browse for a file (and browse to the TFTP server and select the .req file) or open the just received by TFTP .req file with WordPad/Notepad and copy/paste the contents in the first window.
6. Export the .crt file from the CA and put it on the TFTP server.
7. Configure the 'crypto ca import <label> certificate' to import the device's certificates from the tftp server.

Related Topics

- Configuring IKEv1 Public Key Infrastructure Policies in Site-to-Site VPNs , on page 55
- Configuring Public Key Infrastructure Policies for Remote Access VPNs , on page 58
- PKI Enrollment Dialog Box , on page 59
- Configuring a User Group Policy for Easy VPN

Configuring IKEv1 Public Key Infrastructure Policies in Site-to-Site VPNs

You can create a Public Key Infrastructure (PKI) policy to generate enrollment requests for CA certificates and RSA keys, and to manage keys and certificates. Certification Authority (CA) servers are used to manage these certificate requests and issue certificates to the participating devices in your VPN topology.

In Security Manager, CA servers are predefined as PKI enrollment objects that you can use in your PKI policies. A PKI enrollment object contains the server information and enrollment parameters that are required for creating enrollment requests for CA certificates.

For more information about Public Key Infrastructure policies, see Understanding Public Key Infrastructure Policies , on page 51.

This procedure describes how to specify the CA server that will be used to create an IKEv1 Public Key Infrastructure (PKI) policy in your VPN topology.

Tip For information on specifying CA servers for use in IKEv2 negotiations, see Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.

Before You Begin

For important information about successfully configuring PKI, see Requirements for Successful PKI Enrollment , on page 53.

Related Topics

- Defining Multiple IKEv1 CA Servers for Site-to-Site VPNs , on page 56
- Deciding Which Authentication Method to Use , on page 9
- Filtering Items in Selectors

Step 1 Do one of the following:

- (Site-to-Site VPN Manager Window) Select an existing topology and then select **IKEv1 Public Key Infrastructure** in the Policies selector.
- (Policy view) Select **Site-to-Site VPN > IKEv1 Public Key Infrastructure**, and then select an existing policy or create a new one.

The Public Key Infrastructure page opens, displaying the currently selected CA server, if any, in the **Selected** field.

Step 2 Select the PKI enrollment policy object that defines the desired CA server in the Available CA Servers list. You can do the following to modify the listed objects:

- To add a new PKI enrollment object, click the **Create (+)** button. The Add PKI Enrollment dialog box opens. For detailed information about the attributes of a PKI enrollment object, see PKI Enrollment Dialog Box , on page 59.
- To change the configuration of an existing object, select it and click the **Edit (pencil)** button.

Note If you are making a PKI enrollment request on an Easy VPN topology, you must configure each remote component (spoke) with the name of the user group to which it connects. You specify this information in the Organization Unit (OU) field in the Certificate Subject Name tab of the PKI Enrollment dialog box. You do not need to configure the name of the user group on the hub (Easy VPN server). For more information, see PKI Enrollment Dialog Box—Certificate Subject Name Tab , on page 68.

Defining Multiple IKEv1 CA Servers for Site-to-Site VPNs

You can select only one CA server when defining an IKEv1 Public Key Infrastructure (PKI) policy on a site-to-site VPN. This creates a problem when the devices in the VPN enroll with different CA servers when using IKEv1. For example, the spoke devices might enroll with a different CA server than the hub, or the spokes in one part of the VPN might enroll with a different CA server than the spokes in another part of the VPN.

Tip When using IKEv2, you can configure different CA servers for various devices by creating overrides for the IKEv2 Authentication policy global settings rather than creating device-level overrides for PKI enrollment policy objects. However, you can also use device-level overrides for IKEv2 as described in this topic. For information on configuring CA servers for IKEv2, see Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.

To define an IKEv1 PKI policy, you select a PKI enrollment object that specifies the CA server to which the devices should enroll. Although by default the policy object refers globally to a single CA server, you can use device-level overrides to have the object refer to a different CA server on selected devices.

For example, if PKI enrollment object PKI_1 refers to a CA server named CA_1, you can create a device-level override for selected devices that has PKI_1 refer to a different CA server, for example, CA_2. Theoretically, you can use overrides to define a different CA server for each device in the VPN.

This procedure describes the basic steps for creating overrides for PKI enrollment objects.

Note You can also use device-level overrides when the CA servers are arranged in a PKI hierarchy beneath a common, trusted CA server. To do this, you must ensure that both the global definition of the object and the device-level override specify the trusted CA server in the Trusted CA Hierarchy tab of the PKI Enrollment dialog box. See PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab , on page 69.

Related Topics

- Understanding Public Key Infrastructure Policies , on page 51
- Deciding Which Authentication Method to Use , on page 9

Step 1 To create the PKI enrollment object, open the PKI Enrollment dialog box. You can access this dialog box in two ways:

- From the Public Key Infrastructure policy—Click the **Create (+)** button beneath the Selected field. See Configuring IKEv1 Public Key Infrastructure Policies in Site-to-Site VPNs , on page 55.
- From the Policy Object Manager (select **Manage > Policy Objects**)—Select PKI Enrollments from the Object Type selector, then click the **New Object (+)** button.

Step 2 Define the global definition of the PKI enrollment object, including the CA server to which the object refers. Be sure to select **Allow Value Override per Device**. This option makes the object overridable on individual devices. See PKI Enrollment Dialog Box , on page 59.

Base the global definition of the object on the CA server that is used by the most devices in the VPN. Doing this reduces the number of device-level overrides that are required.

Step 3 When you finish defining the PKI enrollment object, click **OK**. As a result:

- If you accessed the dialog box through the PKI policy, the new object appears in the Selected field of the policy page.
- If you accessed the dialog box using the Policy Object Manager, the new object appears in the work area of the Policy Object Manager window. A green check mark in the Overridable column indicates that device-level overrides can be created for this object. (The check mark does not indicate whether any overrides actually exist.)

Step 4 Create the device-level overrides for the PKI enrollment object. You can do this in one of two ways:

- From Device Properties (with the device selected in Device view, select **Tools > Device Properties**)—This option is recommended when you want to create a device-level override for a single device. In the device properties, select **Policy Object Overrides > PKI Enrollments**, select the PKI enrollment object that you want to override, then click the **Create Override** button. You can then define the content of the override, including the CA server defined by the object.

For more information, see Creating or Editing Object Overrides for a Single Device.

- From the Policy Object Manager—This option is recommended when you want to create a device-level override for multiple devices at the same time. Double-click the green check mark in the Overridable column, select the devices to which the override should apply, then define the content of the override, including the CA server defined by the object.

For more information, see Creating or Editing Object Overrides for Multiple Devices At A Time.

Configuring Public Key Infrastructure Policies for Remote Access VPNs

You can create a Public Key Infrastructure (PKI) policy to generate enrollment requests for CA certificates and RSA keys, and to manage keys and certificates. Certification Authority (CA) servers are used to manage these certificate requests and issue certificates to users who connect to your IPsec or SSL remote access VPN.

In Security Manager, CA servers are predefined as PKI enrollment objects that you can use in your PKI policies. A PKI enrollment object contains the server information and enrollment parameters that are required for creating enrollment requests for CA certificates.

For more information about Public Key Infrastructure policies, see Understanding Public Key Infrastructure Policies , on page 51.

Note Beginning with version 4.12, Security Manager provides support for Public Key Infrastructure policy for ASA multi-context devices running the software version 9.5(2) or later.

This procedure describes how to specify the CA servers that will be used to create a Public Key Infrastructure (PKI) policy in your remote access VPN.

Before You Begin

Keep the following in mind:

- For important information about successfully configuring PKI, see Requirements for Successful PKI Enrollment , on page 53.
- The **IKE Proposal** policy for IPsec remote access VPNs should use an IKE Proposal object that requires certificate authorization when configuring IKEv1.
- For remote access VPNs defined on an ASA or PIX 7.x+ device, be aware that the Public Key Infrastructure policy is directly related to the following policies. Any trustpoints defined in these policies must also be selected in the Public Key Infrastructure policy; they are not automatically added to the policy. You might want to first configure these policies to determine which PKI enrollment objects are required in your remote access VPNs.
  - **Connection Profiles**—When you create a IPsec connection profile for which CA trustpoints should be used, you select the PKI enrollment object that identifies the trustpoint on the IPsec tab.
  - **SSL VPN Access**—You can configure trustpoints for each interface and also a fallback trustpoint.
  - **Global Settings, IKEv2 Settings tab**—For IKEv2 IPsec, you must specify a global trustpoint.

Related Topics

- Deciding Which Authentication Method to Use , on page 9
- Filtering Items in Selectors

Step 1 Do one of the following:

- (Device view) Select **Remote Access VPN > Public Key Infrastructure** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Public Key Infrastructure** from the Policy Type selector. Select an existing policy or create a new one.

The Public Key Infrastructure page opens, displaying the currently available and selected CA servers (PKI enrollment objects), if any.

Step 2 Select the PKI enrollment policy objects that define the desired CA servers in the Available CA Servers list and click >> to move them to the Selected CA Servers list. You can remove undesired objects by selecting them in the selected list and clicking <<.

Note When configuring IKEv2 in a Site-to-Site VPN, and choosing PKI as the authentication method, you are required to specify the object name that must be listed here, under Selected CA Servers (see Step 2 of Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70). Hence, ensure that you include the required CA Servers in the Selected CA Servers list.

For ASA and PIX 7.x+ devices, the list of selected PKI enrollment objects must include all objects that are specified in the connection profiles defined for the remote access VPN. For more information on connection profiles, see Configuring Connection Profiles (ASA, PIX 7.0+). Also, any trustpoints configured for IKEv2 on the Global Settings policy must be included; see Configuring VPN Global IKEv2 Settings , on page 38.

You can do the following to modify the listed objects:

- To add a new PKI enrollment object, click the **Create (+)** button below the list of available servers. The Add PKI Enrollment dialog box opens. For detailed information about the attributes of a PKI enrollment object, see PKI Enrollment Dialog Box , on page 59.
- To change the configuration of an existing object, select it in either list and click the **Edit (pencil)** button.

PKI Enrollment Dialog Box

Use the PKI Enrollment dialog box to view, create, copy, or edit Public-Key Infrastructure (PKI) enrollment objects. A PKI enrollment object represents an external certification authority (CA) server that responds to certificate requests from devices in the network.

You can create PKI enrollment objects to define the properties of a CA server used when devices exchange certificates as part of an IPsec network. When you create a PKI enrollment object, you define a name for the server and the URL for enrollment. You must specify whether the devices you wish to enroll with this server should retrieve the CA server's own certificate using the Simple Certificate Enrollment Process (SCEP) or use a certificate that you have entered manually into the device configuration. You must also select the method of support used by the CA server for revocation checking.

Note You do not have to define enrollment parameters in order to create or import a trustpoint in Security Manager.

In addition, you can optionally define the following:

- Whether the CA server is acting as a Registration Authority (RA) server.
- Enrollment parameters, including retry settings and RSA key pair settings.
- Additional attributes to include in the certificate request.
- The list of trusted CA servers located above this server in the PKI hierarchy.

Navigation Path

Select **Manage > Policy Objects**, then select **PKI Enrollments** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Tip You can also open this dialog box from the **Public Key Infrastructure** policy for remote access or site-to-site VPNs.

Related Topics

- Understanding Public Key Infrastructure Policies , on page 51
- Requirements for Successful PKI Enrollment , on page 53
- Configuring IKEv1 Public Key Infrastructure Policies in Site-to-Site VPNs , on page 55
- Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70
- Configuring Public Key Infrastructure Policies for Remote Access VPNs , on page 58
- Policy Object Manager

Field Reference

Table 11: PKI Enrollment Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects.
Description	An optional description of the object.
CA Information tab	Use this tab to enter settings related to the Certificate Authority server, its certificate, and its level of revocation checking support. For information on the specific settings, see PKI Enrollment Dialog Box—CA Information Tab , on page 61.
Enrollment Parameters tab	Use this tab to enter settings related to PKI enrollment. For information on the specific settings, see PKI Enrollment Dialog Box—Enrollment Parameters Tab , on page 65. **Note** You do not have to define enrollment parameters in order to create or import a trustpoint in Security Manager.

Element	Description
Certificate Subject Name tab	Use this tab to enter optional information to be included in the certificate, including subject attributes. For information on the specific settings, see PKI Enrollment Dialog Box—Certificate Subject Name Tab , on page 68.
Trusted CA Hierarchy tab	Use this tab to define trusted CA servers that are arranged in a hierarchical framework. For information on the specific settings, see PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab , on page 69.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden and Understanding Policy Object Overrides for Individual Devices. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

PKI Enrollment Dialog Box—CA Information Tab

Use the CA Information tab of the PKI Enrollment dialog box to:

- Define the name and location of the external certificate authority (CA) server.
- Manually paste the certificate, if known.
- Define the server's level of support for revocation checking.

Navigation Path

Go to the PKI Enrollment dialog box and click the **CA Information** tab. For information on opening the dialog box, see PKI Enrollment Dialog Box , on page 59.

Related Topics

- PKI Enrollment Dialog Box—Enrollment Parameters Tab , on page 65
- PKI Enrollment Dialog Box—Certificate Subject Name Tab , on page 68
- PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab , on page 69

Field Reference

Table 12: PKI Enrollment Dialog Box—CA Information Tab

Element	Description
CA Server Nickname	The name used to identify the CA server in the certificate request. If you leave this field blank, the domain name is used. You must leave this field blank for Verisign CAs. Also, keep the following in mind: • You cannot configure two CA servers with the same name but different URLs on the same device. • The CA name cannot match the name of a trusted CA configured as part of the same PKI enrollment object (as defined on the PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab , on page 69). • When the device is configured as part of a VPN, do not configure a device-level override that uses the same CA name as that of the CA server used by any of the peers. (This is not a problem when the device and its peers use a tiered PKI hierarchy.)
Enrollment Type	The type of enrollment you want to perform. Security Manager completes the enrollment only if you configure URL enrollment. If you select another type, you must complete the enrollment using your own methods. • Self-Signed Certificate (ASA only)—To configure the **enrollment self** command. • Terminal (ASA only)—To configure the **enrollment terminal** command. • URL—To configure the URL for the CA server so that you can complete automatic enrollment. • None—Do not configure any enrollment command.
Protocols	Specify whether you want to configure an SCEP CA URL or a CMP CA URL.
Enrollment URL (URL enrollment only.)	The URL of the CA server to which devices should attempt to enroll. The URL can be in the following formats: • SCEP—Uses an HTTP URL in the form of **http://CA_name:port**, where CA_name is the host DNS name or IP address of the CA server. The port number is mandatory. • TFTP—Uses the format **tftp://certserver/file_specification**. Use this option when you do not have direct access to the CA server. The TFTP server transfers certificate requests and certificates. • Other supported formats include: bootflash, cns, flash, ftp, null, nvram, rcp, scp, system. **Note** If the CA cgi-bin script location at the CA is not the default (/cgi-bin/pkiclient.exe), you must also include the nonstandard script location in the URL, in the form of **http://CA_name:port/script_location**, where script_location is the full path to the CA scripts.

Element	Description
CA Certificate Source Fingerprint Certificate (URL enrollment only.)	How to obtain the certificate: • **Retrieve CA Certificate Using SCEP** (the default)—Have the router retrieve the certificate from the CA server using the Simple Certificate Enrollment Process (SCEP). Enter the fingerprint for the CA server in hexadecimal format. If the value you enter does not match the fingerprint on the certificate, the certificate is rejected. Using the Fingerprint to verify the authenticity of the CA's certificate helps prevent an unauthorized party from substituting a fake certificate in place of the real one. **Tip** You can obtain the CA's fingerprint by contacting the server directly, or by entering the following address in a web browser: **http://URLHostName/certsrv/mscep/mscep.dll**. Using the fingerprint is supported only on Cisco IOS software releases 12.3(12) or later, 12.3(14)T or later, 12.4 or later (including 15.x), 12.2(33)XNA or later. • **Enter CA Certificate from CA Server Manually**—Copy and Paste up to three certificates from another device into the **Certificate** field (using your browser's Paste function or the Ctrl-V keyboard shortcut). Use this option when you want the PKI enrollment object to represent predefined certificates. Each certificate must begin with the word "certificate" and end with the word "quit".CMP authentication requires base 64 encoded CA certificate for authentication. For CMP, we can configure base 64 encoded CA certificate in this field. Copy and paste the base 64 encoded CA certificate from CA server and end with the word "quit". **Note** Enter the certificate details within the words,----BEGIN CERTIFICATE---- and ----END CERTIFICATE----.
CA Certificate Check	Certificates without the CA flag now cannot be installed on the ASA as CA certificates by default. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. Beginning with version 4.9, you can use Security Manager to configure the ASA to allow installation of these certificates if desired. This feature is supported only in devices running ASA software version 9.4(1) or later. CA Certificate check is enabled by default.

Element	Description
Revocation Check Support	The type of certificate revocation checking to be performed: • Checking Not Performed—This is the default. The device does not perform any revocation checking, even if a CRL is on the device. • CRL Check Required—The device must check a CRL. If no CRL exists on the device and the device cannot obtain one, certificates are rejected and a tunnel cannot be established. • OCSP Check Required—The device must check revocation status from an OCSP server. If this check fails, certificates are rejected. • CRL Check Attempted—The device tries to download the latest CRL from the specified LDAP server. If the download fails, however, certificates are accepted. • OCSP Check Attempted—The device tries to check revocation status from an OCSP server. If this fails, however, certificates are accepted. • CRL or OCSP Check Required—The device first checks for a CRL. If a CRL does not exist or cannot be obtained, the device tries to check revocation status from an OCSP server. If both options fail, certificates are rejected. • OCSP or CRL Check Required—The device first tries to check revocation status from an OCSP server. If this fails, the device checks for a CRL. If both options fail, certificates are rejected. • CRL and OCSP Checks Attempted—The device first checks for a CRL. If a CRL does not exist or cannot be obtained, the device tries to check revocation status from an OCSP server. If both options fail, however, certificates are accepted. • OCSP and CRL Checks Attempted—The device first tries to check revocation status from an OCSP server. If this fails, the device tries to download the latest CRL. If both options fail, however, certificates are accepted.
OCSP Server URL	The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with **http://**
CRL Server URL	The URL of the LDAP server from which the CRL can be downloaded if you require CRL checks. This URL must start with **ldap://** **Note** You must include a port number in the URL when using this AAA server on ASA devices, otherwise LDAP will fail.
Enable Registration Authority Mode (PIX 6.3)	For PIX 6.3 devices, whether the CA server operates in RA (Registration Authority) mode. A Registration Authority is a server that acts as a proxy for the actual CA so that CA operations can continue when the CA server is offline. **Note** Cisco IOS routers configure RA mode automatically, if required.

PKI Enrollment Dialog Box—Enrollment Parameters Tab

Use the Enrollment Parameters tab of the PKI Enrollment dialog box to define the retry settings to use when the device contacts the CA server as well as the settings for generating the RSA key pair to associate with the certificate.

If the PKI enrollment object represents a Microsoft CA, you can define the challenge password required to validate the router's identity.

Note You do not have to define enrollment parameters in order to create or import a trustpoint in Security Manager.

Navigation Path

Go to the PKI Enrollment dialog box and click the **Enrollment Parameters** tab. For information on opening the dialog box, see PKI Enrollment Dialog Box , on page 59.

Related Topics

- PKI Enrollment Dialog Box—CA Information Tab , on page 61
- PKI Enrollment Dialog Box—Certificate Subject Name Tab , on page 68
- PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab , on page 69

Field Reference

Table 13: PKI Enrollment Dialog Box—Enrollment Parameters Tab

Element	Description
Challenge Password Confirm	The password used by the CA server to validate the identity of the device. This password is mandatory for PIX 6.3 devices, but optional for PIX/ASA 7.0+ devices and Cisco IOS routers. You can obtain the password by contacting the CA server directly or by entering the following address in a web browser: **http://URLHostName/certsrv/mscep/mscep.dll**. The password is good for 60 minutes from the time you obtain it from the CA server. Therefore, it is important that you deploy the password as soon as possible after you create it. **Note** Each password is valid for a single enrollment by a single device. Therefore, we do not recommend that you assign a PKI enrollment object where this field is defined to a VPN, unless you first configure a device-level override for each device in the VPN. For more information, see Understanding Policy Object Overrides for Individual Devices.
Retry Period	The interval between certificate request attempts, in minutes. Values can be 1 to 60 minutes. The default is 1 minute.
Retry Count	The number of retries that should be made if no certificate is issued upon the first request. Values can be 1 to 100. The default is 10.

Element	Description
Certificate Auto-Enrollment (IOS devices only)	The percentage of the current certificate's lifetime after which the router requests a new certificate. For example, if you enter 70, the router requests a new certificate after 70% of the lifetime of the current certificate has been reached. Values range from 10% to 100%. If you do not specify a value, the router requests a new certificate after the old certificate expires.
Enable Auto-Enrollment	When enabled, certificates are automatically requested based on configurable triggers. The following specific parameters can also be further configured: • whether or not CMPv2 update will be used • when it will be triggered • whether the current key pair will be used or a new key pair will be generated
Certificate Auto-Enrollment (ASA 9.7.1 onwards)	The percentage of the current certificate's lifetime after which the router requests a new certificate. For example, if you enter 50, the router requests a new certificate after 50% of the lifetime of the current certificate has been reached. Values range from 10% to 99%. If you do not specify a value, the router requests a new certificate after the old certificate expires. **Note** The default value is 70%.
Auto Enroll Regenerate Key (ASA 9.7.1 onwards)	Select to generate a new key while renewing the certificate.
Regenerate Key Pair (ASA 9.7.1 onwards)	Select to regenerate a new key pair before enrolling the trustpoint request.
Shared Key (ASA 9.7.1 onwards)	Specify the user credentials obtained from the CA, out of band. This will be used by the CA and ASA to confirm the authenticity and integrity of the messages that they exchange. The key length cannot exceed 64 characters. **Note** The shared key must be in the format, 'reference: shared key'.
Signing Certificate (ASA 9.7.1 onwards)	Specify the name of the trust point that contains a previously issued device certificate to be used to sign the CMP enrollment request.
Note For the CMP protocol, options like Certificate, Shared Key or Signing Certificate will not be discovered, for security reasons. As a result, the PKI enrollment dialog will be creating a override on rediscovery.	

Element	Description
Key Pair	New key pairs will be automatically generated for all CMP manual and automatic enrollments. To support this, we the ability to configure key pair parameters in the trust point has been added. Select the algorithm - RSA or EDCSA, that should be used to generate the key pair. **Note** The RSA algorithm has the following modulus options: 1024| 2048| 4096| 512|768 and the EDCSA algorithm, has the following elliptic-curve options 256|384|521 to generate a key pair.
Include Device's Serial Number	Whether to include the serial number of the device in the certificate. **Tip** The CA uses the serial number to either authenticate certificates or to later associate a certificate with a particular device. If you are in doubt, include the serial number, as it is useful for debugging purposes.
RSA Key Pair Name (PIX 7.0+, ASA, IOS devices only.)	If the key pair you want to associate with the certificate already exists, this field specifies the name of that key pair. If the key pair does not exist, this field specifies the name to assign to the key pair that will be generated during enrollment. **Note** If you do not specify an RSA key pair, the fully qualified domain name (FQDN) key pair is used instead. On PIX and ASA devices, the key pair must exist on the device before deployment.
RSA Key Size (IOS devices only.)	If the key pair does not exist, defines the desired key size (modulus), in bits. If you want a modulus between 512 and 1024, enter an integer that is a multiple of 64. If you want a value higher than 1024, enter 1536 or 2048. The recommended size is 1024. **Note** The larger the modulus size, the more secure the key. However, keys with larger modulus sizes take longer to generate (a minute or more when larger than 512 bits) and longer to process when exchanged.
RSA Encryption Key Size (IOS devices only.)	The size of the second key, which is used to request separate encryption, signature keys, and certificates.

Element	Description
Source Interface (IOS devices and ASA 9.5(1) or later)	The source address for all outgoing connections sent to a CA or LDAP server during authentication, enrollment, and when obtaining a revocation list. This parameter may be necessary when the CA server or LDAP server cannot respond to the address from which the connection originated (for example, due to a firewall). If you do not define a value in this field, the address of the outgoing interface is used. Enter the name of an interface or interface role, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it. **Note** Security Manager 4.9 supports separate routing table for Management traffic on devices running ASA 9.5(1) or later. This functionality enables to completely segregate management traffic from other data traffic on the ASA. Apart from IOS devices you can now select ASA devices running the software version 9.5(1) or later.

PKI Enrollment Dialog Box—Certificate Subject Name Tab

Use the Certificate Subject Name tab of the PKI Enrollment dialog box to optionally define additional information about the device in certificate requests sent to the CA server. This information is placed in the certificate and can be viewed by any party who receives the certificate from the router.

Enter all information using the standard LDAP X.500 format.

Navigation Path

Go to the PKI Enrollment dialog box and click the **Certificate Subject Name** tab. For information on opening the dialog box, see PKI Enrollment Dialog Box , on page 59.

Related Topics

- PKI Enrollment Dialog Box—CA Information Tab , on page 61
- PKI Enrollment Dialog Box—Enrollment Parameters Tab , on page 65
- PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab , on page 69

Field Reference

Table 14: PKI Enrollment Dialog Box—Certificate Subject Name Tab

Element	Description
Include FQDN	Whether to include the device's fully qualified domain name (FQDN) in the certificate request. The name is taken from the Hostname policy (ensure that you specify both the hostname and domain name in the policy to get a valid fully-qualified domain name). If you do not configure the Hostname policy, the name is derived from the display name for the device in Security Manager, *display_name*.**null**, which is unlikely to give you the desired results.
Include Device's IP Address	The interface whose IP address is included in the certificate request. Enter the name of the interface or interface role, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.
Common Name (CN)	The X.500 common name to include in the certificate.
Organization Unit (OU)	The name of the organization unit (for example, a department name) to include in the certificate. **Note** When you configure PKI enrollment objects for Cisco Easy VPN Remote components, this field must contain the name of the client group to which the component connects. Otherwise, the component will not be able to connect. Although this information is not required for the Easy VPN Server, including it does not create configuration problems. For more information about Easy VPN, see Understanding Easy VPN.
Organization (O)	The organization or company name to include in the certificate.
Locality (L)	The locality to include in the certificate.
State (ST)	The state or province to include in the certificate.
Country (C)	The country to include in the certificate.
Email (E)	The email address to include in the certificate.

PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab

Use the Trusted CA Hierarchy tab of the PKI Enrollment dialog box to define the trusted CA servers within an hierarchical PKI framework. Within this framework, all enrolled peers can validate each other's certificates if they share a trusted root CA certificate or a common subordinate CA.

Select the CA servers (as defined as PKI enrollment objects) to include in the hierarchy in the Available Servers list and click >> to move them to the selected list. You can do the reverse to remove servers.

If the PKI enrollment object you need is not yet defined, click the **Create (+)** button beneath the available servers list to create the object. You can also select an object and click the **Edit** button to change its definition, if needed.

Navigation Path

Go to the PKI Enrollment dialog box and click the **Trusted CA Hierarchy** tab. For information on opening the dialog box, see PKI Enrollment Dialog Box , on page 59.

Related Topics

- PKI Enrollment Dialog Box—CA Information Tab , on page 61
- PKI Enrollment Dialog Box—Enrollment Parameters Tab , on page 65
- PKI Enrollment Dialog Box—Certificate Subject Name Tab , on page 68

Configuring IKEv2 Authentication in Site-to-Site VPNs

When you configure IKE version 2 (IKEv2) in a site-to-site VPN, you must configure the IKEv2 Authentication policy to define authentication settings. Unlike IKEv1, authentication settings are not part of the IKEv2 proposal.

In Security Manager, when you configure IKEv2 authentication for a site-to-site VPN, you configure default settings that will be used in the VPN topology. You can then configure exceptions to the default, specifying different preshared keys or trustpoints for specific segments of the VPN. You can use a mixture of preshared keys and trustpoints, for example, configuring a global preshared key, but trustpoints for selected members of the VPN.

Configuring asymmetric authentication for IKEv2 tunnels

IKEv2 allows you to use asymmetric authentication, unlike IKEv1. This means that two peers can have different preshared keys, different trustpoints, or one peer could use a preshared key and the other peer could use a trustpoint. In Security Manager, you can configure asymmetric authentication by doing any of the following:

- On the Global IKEv2 Authentication Settings tab, you can configure different preshared keys if you elect to auto-generate keys and **do not** select the Same Keys for All Tunnels or the Same Key at Tunnel Endpoints option. A different preshared key is generated for each end of each tunnel.
- On the Override IKEv2 Authentication Settings tab, you can create overrides for the global settings. You add overrides that specify different keys or trustpoints for subsets of local and remote peers. Because you can create more than one override for a device or a specific tunnel, you can configure a set of preshared keys and trustpoints from which peers will authenticate.

Tip The IKEv2 Authentication policy is not a shared policy. You must configure the policy for each VPN topology in which you support IKEv2 negotiations. You cannot configure global IKEv2 authentication options for use by all of your VPN topologies. When using the Create VPN wizard, even if you elect to support IKEv2, the IKEv2 Authentication policy is never configured.

Before You Begin

The IKEv2 Authentication policy is used only if you enable IKEv2 in the VPN in the IKE Proposal and IPsec Proposal policies, and if at least some of the devices in the topology support IKEv2.

To configure IKEv2, the device must be an ASA running ASA Software release 8.4(1) or later. For more information on device support, see Understanding Devices Supported by Each IPsec Technology.

Tip If you support only IKEv2 in the topology, ensure that you unassign the IKEv1 Preshared Keys and IKEv1 Public Key Infrastructure policies to avoid validation warnings.

Related Topics

- Understanding IKE , on page 5
- Deciding Which Authentication Method to Use , on page 9

Step 1 Open the Site-to-Site VPN Manager Window, select a regular IPsec topology (that supports IKEv2) in the VPNs selector, then select **IKEv2 Authentication** in the Policies selector.

For reference information on the policy, see IKEv2 Authentication Policy , on page 72.

Step 2 On the **Global IKEv2 Authentication Settings** tab, configure the authentication type that should be used for devices in the VPN for which no override is configured on the Override IKEv2 Authentication Settings tab. Select the option that is used by most devices in the VPN. You can configure a global preshared key or trustpoint:

- **Global Preshared Keys**—To configure a global preshared key, select **Key Specification** and then configure one of the following options:
  - User Defined—Enter the desired global key and enter it again in the Confirm field.
  - Auto Generated—Enter the length of the key that should be generated and select whether you want to use the same key for all tunnels or the same key at both ends of a single tunnel. If you select neither of these options, unique keys are generated for every end point.

You can also select **Regenerate Key (On Next Deployment)** to have new keys generated. This allows you to periodically re-key the VPN. The check box is cleared after the next successful deployment.

- **Global Trustpoint (CA Servers)**—To configure trustpoint certificate authorization, select **PKI Specification** and enter the name of the PKI enrollment object that identifies the Certificate Authority (CA) server.

Note Ensure that you enter the same object name as deployed in the PKI policy (see Step 2 of Configuring Public Key Infrastructure Policies for Remote Access VPNs , on page 58).

Click **Select** to select the object from a list or to create a new object.

- **Sign IKEv2 Authentication Payload with SHA1**—To enable SHA1 authentication on IKEv2 payload, select the check box. This option is available only from Cisco Security Manager 4.19 and for ASA 9.12(1) or later devices.

Step 3 If you want to override the global IKEv2 authentication configuration for specific devices, click the **Override IKEv2 Authentication Settings** tab and do any of the following:

- To add an override, click the **Add Row (+)** button and fill in the IKEv2 Authentication dialog box. You select the local and remote peers for which to create the override, and then specify the preshared key or CA server that should be used. See IKEv2 Authentication (Override) Dialog Box , on page 74.
- To edit an override, select it in the table and click the **Edit Row (pencil)** button.

- To delete an override, select it in the table and click the **Delete Row (trash can)** button.

Note Override IKEV2 authentication settings are applicable for only Hub & Spoke VPN and Full Mesh VPN topologies.

Note You can configure asymmetric authentication in site-to-site VPNs, where each side of a tunnel can have different preshared keys. To create asymmetric keys for IKEv2 authentication, for each peer device that is part of the site-to-site topology, you must add two rows on the Override IKEv2 Authentication Settings tab. For more information, see IKEv2 Authentication (Override) Dialog Box , on page 74.

IKEv2 Authentication Policy

Use the IKEv2 Authentication policy to configure the device authentication settings for Internet Key Exchange (IKE) version 2 in site-to-site VPNs. These settings apply to ASA 8.4(1)+ devices only. For more information about configuring IKEv2 authentication, see Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.

The policy contains two tabs:

- Global IKEv2 Authentication Settings—The global settings apply to all devices in the VPN unless overrides are configured on the Overrides tab. Configure the global settings to represent the authentication scheme used by most devices in the VPN.
- Override IKEv2 Authentication Settings—The override settings apply unique authentication settings to specific tunnels, allowing you to create unique preshared key and trustpoint combinations that are required by various tunnels in the VPN. The settings you configure on this tab are used first and always take precedence over the global settings.

Navigation Path

Open the Site-to-Site VPN Manager Window, select a regular IPsec topology (that supports IKEv2) in the VPNs selector, then select **IKEv2 Authentication** in the Policies selector.

This policy is not available as a shared policy.

Related Topics

- Understanding IKE , on page 5
- Understanding IPsec Proposals for Site-to-Site VPNs , on page 19
- Filtering Tables
- Table Columns and Column Heading Features

Field Reference

Table 15: IKEv2 Authentication Policy

Element	Description
Global IKEv2 Authentication Settings Tab	

Element	Description

Key Specification	Use a preshared key for authentication in the VPN. Configure one of the following:
	• **User Defined**—Enter the desired global key and enter it again in the Confirm field. The key can be 1 to 128 characters.
	• **Auto Generated**—Have Security Manager generate a key for you. Specify the following options to indicate how the key should be generated:
	  • **Key Length**—The length of the key that should be generated, from 1 to 128.
	  • **Same Keys for All Tunnels**—Select this option to generate the same keys for all tunnels in the VPN. If you do not select this option, different keys or pair of keys (if you select Same Key for Tunnel Endpoints) are used for each tunnel.
	  • **Same Key for Tunnel Endpoints**—Select this option to generate the same key on each end of each tunnel within the VPN. If you do not select this option, different keys are generated on each end of the tunnel.
	  • **Regenerate Key (On Next Deployment)**—Select this option to generate new keys for the next deployment to the devices. This allows you to easily re-key the VPN.
	
	After a successful deployment, this check box is cleared so that keys are not regenerated on the subsequent deployment. Select the option each time you want to re-key the VPN.

PKI Specification	The name of the PKI enrollment policy object that defines the trustpoint for IKEv2 connections. A trustpoint represents a Certificate Authority (CA)/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. Click **Select** to select the PKI enrollment object or to create a new object.
Override IKEv2 Authentication Settings tab	The table lists the IKEv2 authentication overrides defined for the VPN. These policies take precedence over the preshared key/PKI configuration defined in the global settings. Do any of the following to configure overrides: • To add an override, click the **Add Row (+)** button and fill in the IKEv2 Authentication dialog box. You select the local and remote peers for which to create the override, and then specify the preshared key or CA server that should be used. See IKEv2 Authentication (Override) Dialog Box , on page 74. • To edit an override, select it in the table and click the **Edit Row (pencil)** button. • To delete an override, select it in the table and click the **Delete Row (trash can)** button. **Note** You can configure asymmetric authentication in site-to-site VPNs, where each side of a tunnel can have different preshared keys. To create asymmetric keys for IKEv2 authentication, for each peer device that is part of the site-to-site topology, you must add two rows on the Override IKEv2 Authentication Settings tab. For more information, see IKEv2 Authentication (Override) Dialog Box , on page 74

IKEv2 Authentication (Override) Dialog Box

Use the IKEv2 Authentication dialog box to configure overrides to the IKEv2 authentication global settings for a site-to-site VPN. For more information about IKEv2 global and override authentication settings, see Configuring IKEv2 Authentication in Site-to-Site VPNs , on page 70.

Navigation Path

From the Override IKEv2 Authentication Settings tab of the IKEv2 Authentication policy (see IKEv2 Authentication Policy , on page 72), click the **Add Row (+)** button or select an override in the table and click **Edit Row (pencil)**.

Field Reference

Table 16: IKEv2 Authentication Dialog Box

Element	Description
Local Peers Remote Peers	The local and remote sides of the tunnels for which you are defining this override. To add devices to the list, click the **Select** button to the right of the list to open the Local or Remote Peer Selection dialog box. In that dialog box, select the desired peers in the Available list and click >> to move them to the Selected list. You can deselect a device by doing the reverse (using the << button). The list of available devices includes only those devices that support IKEv2 connections, which might not be all of the devices in the VPN.
IKEv2 Authentication Mode	The IKEv2 authentication mode to use between the selected local and remote peers. Select one of the following: • Key Specification—A user-defined preshared key, from 1 to 128 characters. Enter the desired key and enter it again in the Confirm field. • PKI Specification—The name of the PKI enrollment policy object that defines the trustpoint for IKEv2 connections. Click **Select** to select the PKI enrollment object or to create a new object.

Configuring Asymmetric keys for IKEv2 Authentication

You can configure asymmetric authentication in site-to-site VPNs, where each side of a tunnel can have different preshared keys. To create asymmetric keys for IKEv2 authentication, for each peer device that is part of the site-to-site topology, you must add two rows on the Override IKEv2 Authentication Settings tab. Perform the following:

1. Click the **Override IKEv2 Authentication Settings** tab and then click the**Add Row (+)** button. The IKEv2 Authentication dialog box opens. On Peers specification, select the Local Peer device and the Remote Peer device that are part of the site-to-site VPN topology. On **IKEv2 Authentication Mode** select Key Specification and then specify a key and confirm. Security Manager considers this key as the local preshared key for the selected local peer device and the same key as the remote preshared key for the selected remote peer device. Click **OK** to return to the Override IKEv2 Authentication Settings tab.
2. With the **Override IKEv2 Authentication Settings** tab selected, click the **Add Row (+)** button. The IKEv2 Authentication dialog box opens. On Peers specification, for Local Peer, select the Remote Peer

device of Step 1 and for Remote Peer, select the Local Peer device of Step 1. On **IKEv2 Authentication Mode** select Key Specification and then specify a key and confirm. This key must be different from the key that you specified in Step 1.

The following table illustrates the configuration of asymmetric keys for IKEv2 authentication:

	Local Peer Device	Remote Peer Device	Authentication method (Preshared Key)
Add Row 1	Peer1	Peer2	test123
Add Row 2	Peer2	Peer1	sample123