

IKE

- Configure IKE, on page 1
- Configure IPsec, on page 9

Configure IKE

IKE, also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. To configure the ASA for Virtual Private Networks, you set global IKE parameters that apply system wide, and you also create IKE policies that the peers negotiate to establish a VPN connection.

Procedure

Step 1 Enable IKE, on page 1.

Step 2 Set IKE Parameters for Site-to-Site VPN, on page 2.

Step 3 Configure IKE Policies, on page 5.

Enable IKE

Procedure

Step 1 To enable IKE for VPN connections:

a) In ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access >AnyConnect Connection Profiles**.

b) In the Access Interfaces area, check **Allow Access** under IPsec (IKEv2) Access for the interfaces you will use IKE on.

Step 2 To enable IKE for Site-to-Site VPN:

a) In ASDM, choose **Configuration > Site-to-Site VPN > Connection Profiles**.

b) Select the interfaces you want to use IKEv1 and IKEv2 on.

IKE Parameters for Site-to-Site VPN

In ASDM, choose **Configuration > Site-to-Site VPN > Advanced > IKE Parameters**.

NAT Transparency

- Enable IPsec over NAT-T

  IPsec over NAT-T lets IPsec peers establish both remote access and LAN-to-LAN connections through a NAT device. It does this by encapsulating IPsec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPsec traffic when necessary. This feature is enabled by default.

  - The ASA can simultaneously support standard IPsec, IPsec over TCP, NAT-T, and IPsec over UDP, depending on the client with which it is exchanging data.
  - When both NAT-T and IPsec over UDP are enabled, NAT-T takes precedence.
  - When enabled, IPsec over TCP takes precedence over all other connection methods.

  The ASA implementation of NAT-T supports IPsec peers behind a single NAT/PAT device as follows:

  - One LAN-to-LAN connection.
  - Either a LAN-to-LAN connection or multiple remote access clients, but not a mixture of both.

  To use NAT-T you must:

  - Create an ACL for the interface you will be using to open port 4500 (Configuration > Firewall > Access Rules).
  - Enable IPsec over NAT-T in this pane.
  - On the Fragmentation Policy parameter in the Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies pane, edit the interface you will be using to Enable IPsec pre-fragmentation. When this is configured, it is still alright to let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do.

- Enable IPsec over TCP

  IPsec over TCP enables a VPN client to operate in an environment in which standard ESP or IKE cannot function, or can function only with modification to existing firewall rules. IPsec over TCP encapsulates both the IKE and IPsec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls. This feature is disabled by default.

Note This feature does not work with proxy-based firewalls.

IPsec over TCP works with remote access clients. It works on all physical and VLAN interfaces. It is a client to ASA feature only. It does not work for LAN-to-LAN connections.

- The ASA can simultaneously support standard IPsec, IPsec over TCP, NAT-Traversal, and IPsec over UDP, depending on the client with which it is exchanging data.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

You enable IPsec over TCP on both the ASA and the client to which it connects.

You can enable IPsec over TCP for up to 10 ports that you specify. If you enter a well-known port, for example port 80 (HTTP) or port 443 (HTTPS), the system displays a warning that the protocol associated with that port will no longer work. The consequence is that you can no longer use a browser to manage the ASA through the IKE-enabled interface. To solve this problem, reconfigure the HTTP/HTTPS management to different ports.

You must configure TCP port(s) on the client as well as on the ASA. The client configuration must include at least one of the ports you set for the ASA.

Identity Sent to Peer

Choose the **Identity** that the peers will use to identify themselves during IKE negotiations:

Address	Uses the IP addresses of the hosts exchanging ISAKMP identity information.
Hostname	Uses the fully-qualified domain name of the hosts exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
Key ID	Uses the remote peer uses the **Key Id String** that you specify to look up the preshared key.
Automatic	Determines IKE negotiation by connection type: • IP address for preshared key • Cert DN for certificate authentication.

Session Control

- Disable Inbound Aggressive Mode Connections

  Phase 1 IKE negotiations can use either Main mode or Aggressive mode. Both provide the same services, but Aggressive mode requires only two exchanges between the peers, rather than three. Aggressive mode is faster, but does not provide identity protection for the communicating parties. It is therefore necessary that they exchange identification information prior to establishing a secure SA in which to encrypt in formation. This feature is disabled by default.

- Alert Peers Before Disconnecting
  - Client or LAN-to-LAN sessions may be dropped for several reasons, such as: a ASA shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.
  - The ASA can notify qualified peers (in LAN-to-LAN configurations) of sessions that are about to be disconnected, and it conveys to them the reason. The peer or client receiving the alert decodes the reason and displays it in the event log or in a pop-up pane. This feature is disabled by default.
  - This pane lets you enable the feature so that the ASA sends these alerts, and conveys the reason for the disconnect.

Qualified clients and peers include the following:

- Security appliances with Alerts enabled.
- VPN clients running 4.0 or later software (no configuration required).

- Wait for All Active Sessions to Voluntarily Terminate Before Rebooting

  You can schedule a ASA reboot to occur only when all active sessions have terminated voluntarily. This feature is disabled by default.

- Number of SAs Allowed in Negotiation for IKEv1

  Limits the maximum number of SAs that can be in negotiation at any time.

IKE v2 Specific Settings

Additional session controls are available for IKE v2, that limit the number of open SAs. By default, the ASA does not limit the number of open SAs:

- Cookie Challenge—Enables the ASA to send cookie challenges to peer devices in response to SA initiate packets.
  - % threshold before incoming SAs are cookie challenged—The percentage of the total allowed SAs for the ASA that are in-negotiation, which triggers cookie challenges for any future SA negotiations. The range is zero to 100%. The default is 50%.
- Number of Allowed SAs in Negotiation—Limits the maximum number of SAs that can be in negotiation at any time. If used in conjunction with Cookie Challenge, configure the cookie challenge threshold lower than this limit for an effective cross-check.
- Maximum Number of SAs Allowed—Limits the number of allowed IKEv2 connections on the ASA. By default, the limit is the maximum number of connections specified by the license.
- Maximum Number of Queues Allowed—Limits the number of allowed queues on the ASA.
- Notify Invalid Selector—Allows an administrator to enable or disable the sending of an IKE notification to the peer when an inbound packet that is received on an SA does not match the traffic selectors for that SA. Sending this notification is disabled by default.
- Enable Fragmentation—Enables fragmentation for an IKEv2 VPN on an ASA.
- Fragmentation MTU—Specify a maximum transmission unit (MTU) size between 200 and 1500 bytes.
- Preferred Fragmentation Method:
  - IETF RFC-7383—Select this method when both peers specify support and preference during negotiation. Using this method, encryption is done after fragmentation providing individual protection for each IKEv2 fragment message.
  - Cisco proprietary method—Select this method when it is the only method provided by a peer, such as the AnyConnect Client, or if both peers specify support and preference during negotiation. Using this method fragmentation is done after encryption. The receiving peer cannot decrypt or authenticate the message until all fragments are received. This method does not interoperate with non-Cisco peers.

Preventing DoS Attacks with IKE v2 Specific Settings

You can prevent denial-of-service (DoS) attacks for IPsec IKEv2 connections by configuring Cookie Challenge, which challenges the identify of incoming Security Associations (SAs), or by limiting the number of open SAs. 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 and/or CPU attacks that the cookie-challenge feature may be unable to thwart and protects 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 challenging 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 5585-X with 10000 allowed IKEv2 SAs, after 5000 SAs become open, any more incoming SAs are cookie-challenged.

If used in conjunction with the **Number of SAs Allowed in Negotiation**, or the Maximum Number of SAs Allowed, configure the cookie-challenge threshold lower than these settings for an effective cross-check.

You can also limit the life on all SAs at the IPsec level by choosing Configuration > Site-to-Site VPN > Advanced > System Options.

IKE Policies

Configuration > Site-to-Site VPN > Advanced > IKE Policies

Use this pane to Add, Edit, or Delete IKEv1 and IKEv2 Policies.

To set the terms of the IKE negotiations, you create one or more IKE policies, which include the following:

- A unique priority (1 through 65,543, with 1 the highest priority).
- An authentication method, to ensure the identity of the peers.
- An encryption method, to protect the data and ensure privacy.
- An HMAC method to ensure the identity of the sender, and to ensure that the message has not been modified in transit.
- A Diffie-Hellman group to establish the strength of the of the encryption-key-determination algorithm. The ASA uses this algorithm to derive the encryption and hash keys.
- A limit for how long the ASA uses an encryption key before replacing it.

Each IKE negotiation is divided into two sections called Phase1 and Phase 2. Phase 1 creates the first tunnel, which protects later IKE negotiation messages. Phase 2 creates the tunnel that protects data.

For IKEv1, you can only enable one setting for each parameter. For IKEv2, each proposal can have multiples settings for Encryption, D-H Group, Integrity Hash, and PRF Hash.

If you do not configure any IKE policies, the ASA uses the default policy, which is always set to the lowest priority, and which contains the default value for each parameter. If you do not specify a value for a specific parameter, the default value takes effect.

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, 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.

Fields

- IKEv1 Policies—Displays parameter settings for each configured IKE policy.
  - Priority #—Shows the priority of the policy.
  - Encryption—Shows the encryption method.
  - Hash—Shows the hash algorithm.
  - D-H Group—Shows the Diffie-Hellman group.
  - Authentication—Shows the authentication method.
  - Lifetime (secs)—Shows the SA lifetime in seconds.
- IKEv2 Policies—Displays parameter settings for each configured IKEv2 policy.
  - Priority #—Shows the priority of the policy.
  - Encryption—Shows the encryption method.
  - Integrity Hash—Shows the hash algorithm.
  - PRF Hash—Shows the pseudo random function (PRF) hash algorithm.
  - D-H Group—Shows the Diffie-Hellman group.
  - Lifetime (secs)—Shows the SA lifetime in seconds.

Add or Edit an IKEv1 Policy

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKE Policy

Priority #—Type a number to set a priority for the IKE policy. The range is 1 to 65535, with 1 the highest priority.

Encryption—Choose an encryption method. This is a symmetric encryption method that protects data transmitted between two IPsec peers.The choices follow:

des	56-bit DES-CBC. Less secure but faster than the alternatives. The default.
3des	168-bit Triple DES.
aes	128-bit AES.
aes-192	192-bit AES.
aes-256	256-bit AES.

Hash—Choose the hash algorithm that ensures data integrity. It ensures that a packet comes from whom you think it comes from, and that it has not been modified in transit.

sha	SHA-1	The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	

Authentication—Choose the authentication method the ASA uses to establish the identity of each IPsec peer. Preshared keys do not scale well with a growing network, but are easier to set up in a small network. The choices follow:

pre-share	Preshared keys.
rsa-sig	A digital certificate with keys generated by the RSA signatures algorithm.

D-H Group—Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other.

1	Group 1 (768-bit)	The default, Group 2 (1024-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 1or 5.
2	Group 2 (1024-bit)	
5	Group 5 (1536-bit)	

Lifetime (secs)—Either check Unlimited or enter an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the ASA sets up future IPsec security associations less quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Time Measure—Choose a time measure. The ASA accepts the following values:.

120 - 86,400 seconds
2 - 1440 minutes
1 - 24 hours
1 day

Add or Edit an IKEv2 Policy

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKEv2 Policy

Priority #—Type a number to set a priority for the IKEv2 policy. The range is 1 to 65535, with 1 the highest priority.

Encryption—Choose an encryption method. This is a symmetric encryption method that protects data transmitted between two IPsec peers.The choices follow:

des	Specifies 56-bit DES-CBC encryption for ESP.
3des	(Default) Specifies the triple DES encryption algorithm for ESP.
aes	Specifies AES with a 128-bit key encryption for ESP.

aes-192	Specifies AES with a 192-bit key encryption for ESP.
aes-256	Specifies AES with a 256-bit key encryption for ESP.
aes-gcm	Specifies AES-GCM/GMAC 128-bit support for symmetric encryption and integrity.
aes-gcm-192	Specifies AES-GCM/GMAC 192-bit support for symmetric encryption and integrity.
aes-gcm-256	Specifies AES-GCM/GMAC 256-bit support for symmetric encryption and integrity.
NULL	Indicates no encryption.

D-H Group—Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other.

1	Group 1 (768-bit)	The default, Group 2 (1024-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 2 or 5.
2	Group 2 (1024-bit)	
5	Group 5 (1536-bit)	
14	Group 14	
19	Group 19	
20	Group 20	
21	Group 21	
24	Group 24	

Integrity Hash—Choose the hash algorithm that ensures data integrity for the ESP protocol. It ensures that a packet comes from whom you think it comes from, and that it has not been modified in transit.

sha	SHA 1	The default is SHA 1. MD5 has a smaller digest and is considered to be slightly faster than SHA 1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	
sha256	SHA 2, 256-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	**SHA 2, 384-bit digest**	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	**SHA 2, 512-bit digest**	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.
null		Indicates that AES-GCM or AES-GMAC is configured as the encryption algorithm. You must choose the null integrity algorithm if AES-GCM has been configured as the encryption algorithm.

Pseudo-Random Function (PRF)—Specify the PRF used for the construction of keying material for all of the cryptographic algorithms used in the SA..

sha	SHA-1	The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	
sha256	SHA 2, 256-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	SHA 2, 384-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	SHA 2, 512-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

Lifetime (secs)—Either check Unlimited or enter an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the ASA sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

The ASA accepts the following values:.

120 - 86,400 seconds
2 - 1440 minutes
1 - 24 hours
1 day

Configure IPsec

The ASA uses IPsec for LAN-to-LAN VPN connections, and provides the option of using IPsec for client-to-LAN VPN connections. In IPsec terminology, a “peer” is a remote-access client or another secure gateway.The ASA supports LAN-to-LAN IPsec connections with Cisco peers (IPv4 or IPv6), and with third-party peers that comply with all relevant standards.

During tunnel establishment, the two peers negotiate security associations that govern authentication, encryption, encapsulation, and key management. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPsec SA).

A LAN-to-LAN VPN connects networks in different geographic locations. In IPsec LAN-to-LAN connections, the ASA can function as initiator or responder. In IPsec client-to-LAN connections, the ASA functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The ASA supports these IPsec attributes:

- Main mode for negotiating phase one ISAKMP security associations when using digital certificates for authentication

- Aggressive mode for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication
- Authentication Algorithms:
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- Authentication Modes:
  - Preshared Keys
  - X.509 Digital Certificates
- Diffie-Hellman Groups 1,2 and 5.
- Encryption Algorithms:
  - AES-128, -192, and -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

Procedure

Step 1 Configure Crypto Maps, on page 10.
Step 2 Configure IPsec Pre-Fragmentation Policies, on page 18.
Step 3 Configure IPsec Proposals (Transform Sets), on page 20.

Crypto Maps

Configuration > Site-to-Site VPN > Advanced > Crypto Maps

This pane shows the currently configured crypto maps, which are defined in IPsec rules. Here you can add, edit, delete and move up, move down, cut, copy, and paste an IPsec rule.

Note You cannot edit, delete, or copy an implicit rule. The ASA implicitly accepts the traffic selection proposal from remote clients when configured with a dynamic tunnel policy. You can override it by giving a specific traffic selection.

You can also **Find** (filter the display of) rules by selecting Interface, Source, Destination, Destination Service, or Rule Query, selecting is or contains, and entering the filter parameter. Click ... to launch a browse dialog box that displays all existing entries that you can choose. Use **Diagram** to display the rules pictorially.

The IPsec rules specify the following:

- Type: Priority—Displays the type of rule (static or dynamic) and its priority.
- Traffic Selection
  - #—Indicates the rule number.
  - Source—Indicates the IP addresses that are subject to this rule when traffic is sent to the IP addresses listed in the Remote Side Host/Network column. In detail mode (see the Show Detail button), an address column might contain an interface name with the word any, such as inside:any. any means that any host on the inside interface is affected by the rule.
  - Destination—Lists the IP addresses that are subject to this rule when traffic is sent from the IP addresses listed in the Security Appliance Side Host/Network column. In detail mode (see the Show Detail button), an address column might contain an interface name with the word any, such as outside:any. any means that any host on the outside interface is affected by the rule. Also in detail mode, an address column might contain IP addresses in square brackets, for example, [209.165.201.1-209.165.201.30]. These addresses are translated addresses. When an inside host makes a connection to an outside host, the ASA maps the inside host's address to an address from the pool. After a host creates an outbound connection, the ASA maintains this address mapping. This address mapping structure is called an xlate, and remains in memory for a period of time.
  - Service—Specifies the service and protocol specified by the rule (TCP, UDP, ICMP, or IP).
  - Action—Specifies the type of IPsec rule (protect or do not protect).
- Transform Set—Displays the transform set for the rule.
- Peer—Identifies the IPsec peer.
- PFS—Displays perfect forward secrecy settings for the rule.
- NAT-T Enabled—Indicates whether NAT Traversal is enabled for the policy.
- Reverse Route Enabled—Indicates whether Reverse Route Injection (RRI) is enabled for the policy. RRI is done upon configuration and is considered static, remaining in place until the configuration changes or is removed. The ASA automatically adds static routes to the routing table and announces these routes to its private network or border routers using OSPF.
  - Dynamic— If dynamic is specified, RRIs are created upon the successful establishment of IPsec security associations (SA's) and deleted after the IPsec SA's are deleted.

Note Dynamic RRI applies to IKEv2 based static crypto maps only.

- Connection Type—(Meaningful only for static tunnel policies.) Identifies the connection type for this policy as bidirectional, originate-only, or answer-only).
- SA Lifetime—Displays the SA lifetime for the rule.
- CA Certificate—Displays the CA certificate for the policy. This applies to static connections only.
- IKE Negotiation Mode—Displays whether IKE negotiations use main or aggressive mode.
- Description—(Optional) Specifies a brief description for this rule. For an existing rule, this is the description you typed when you added the rule. An implicit rule includes the following description: "Implicit rule." To edit the description of any but an implicit rule, right-click this column, and choose Edit Description or double-click the column.
- Enable Anti-replay window size—Sets the anti-replay window size, between 64 and 1028 in multiples of 64. One side-effect of priority queueing in a hierarchical QoS policy with traffic shaping (see "Rule Actions > QoS Tab") is packet re-ordering. For IPsec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings becomes false alarms in the case of priority queueing. Configuring the anti-replay pane size helps you avoid possible false alarms.
- Enable IPsec Inner Routing Lookup—By default lookups are not done for packets sent through the IPsec tunnel, per-packet adjacency lookups are done only for the outer ESP packets, In some network topologies, when a routing update has altered the inner packet's path, but the local IPsec tunnel is still up, packets through the tunnel may not be routed correctly and fail to reach their destination. To prevent this, enable per-packet routing lookups for the IPsec inner packets.

Create or Edit an IPsec Rule Tunnel Policy (Crypto Map) - Basic Tab

Use this pane to define a new Tunnel Policy for an IPsec rule. The values you define here appear in the IPsec Rules table after you click **OK**. All rules are enabled by default as soon as they appear in the IPsec Rules table.

The Tunnel Policy pane lets you define a tunnel policy that is used to negotiate an IPsec (Phase 2) security association (SA). ASDM captures your configuration edits, but does not save them to the running configuration until you click **Apply**.

Every tunnel policy must specify a transform set and identify the security appliance interface to which it applies. The transform set identifies the encryption and hash algorithms that perform IPsec encryption and decryption operations. Because not every IPsec peer supports the same algorithms, you might want to specify a number of policies and assign a priority to each. The security appliance then negotiates with the remote IPsec peer to agree on a transform set that both peers support.

Tunnel policies can be *static* or *dynamic*. A static tunnel policy identifies one or more remote IPsec peers or subnetworks to which your security appliance permits IPsec connections. A static policy can be used whether your security appliance initiates the connection or receives a connection request from a remote host. A static policy requires you to enter the information necessary to identify permitted hosts or networks.

A dynamic tunnel policy is used when you cannot or do not want to provide information about remote hosts that are permitted to initiate a connection with the security appliance. If you are only using your security appliance as a VPN client in relation to a remote VPN central-site device, you do not need to configure any dynamic tunnel policies. Dynamic tunnel policies are most useful for allowing remote access clients to initiate a connection to your network through a security appliance acting as the VPN central-site device. A dynamic tunnel policy is useful when the remote access clients have dynamically assigned IP addresses or when you do not want to configure separate policies for a large number of remote access clients.

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Basic

- Interface—Choose the interface name to which this policy applies.
- Policy Type—Choose the type, static or dynamic, of this tunnel policy.
- Priority—Enter the priority of the policy.
- IKE Proposals (Transform Sets)--Specifies IKEv1 and IKEv2 IPsec proposals:
  - IKEv1 IPsec Proposal—Choose the proposal (transform set) for the policy and click **Add** to move it to the list of active transform sets. Click **Move Up** or **Move Down** to rearrange the order of the proposals in the list box. You can add a maximum of 11 proposals to a crypto map entry or a dynamic crypto map entry.
  - IKEv2 IPsec Proposal—Choose the proposal (transform set) for the policy and click **Add** to move it to the list of active transform sets. Click **Move Up** or **Move Down** to rearrange the order of the proposals in the list box. You can add a maximum of 11 proposals to a crypto map entry or a dynamic crypto map entry.
- Peer Settings - Optional for Dynamic Crypto Map Entries—Configure the peer settings for the policy.
  - Connection Type—(Meaningful only for static tunnel policies.) Choose bidirectional, originate-only, or answer-only to specify the connection type of this policy. For LAN-to-LAN connections, choose bidirectional or answer-only (not originate-only). Choose answer-only for LAN-to-LAN redundancy. If you choose Originate Only, you can specify up to 10 redundant peers. For uni-directional, you can specify originate only or answer only, and neither are enabled by default.
  - IP Address of Peer to Be Added—Enter the IP address of the IPsec peer you are adding.
- Enable Perfect Forwarding Secrecy—Check to enable perfect forward secrecy for the policy. PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless you specify Perfect Forward Secrecy.
- Diffie-Hellman Group—When you enable PFS you must also choose a Diffie-Hellman group which the ASA uses to generate session keys. The choices are as follows:
  - Group 1 (768-bits) = Use perfect forward secrecy, and use Diffie-Hellman Group 1 to generate IPsec session keys, where the prime and generator numbers are 768 bits. This option is more secure but requires more processing overhead.
  - Group 2 (1024-bits) = Use perfect forward secrecy, and use Diffie-Hellman Group 2 to generate IPsec session keys, where the prime and generator numbers are 1024 bits. This option is more secure than Group 1 but requires more processing overhead.
  - Group 5 (1536-bits) = Use perfect forward secrecy, and use Diffie-Hellman Group 5 to generate IPsec session keys, where the prime and generator numbers are 1536 bits. This option is more secure than Group 2 but requires more processing overhead.
  - Group 14 (2048-bits) = Use perfect forward secrecy and use Diffie-Hellman Group 14 for IKEv2.
  - Group 19= Use perfect forward secrecy and use Diffie-Hellman Group 19 for IKEv2 to support ECDH.
  - Group 20= Use perfect forward secrecy and use Diffie-Hellman Group 20 for IKEv2 to support ECDH.

- Group 21= Use perfect forward secrecy and use Diffie-Hellman Group 21 for IKEv2 to support ECDH.
- Group 24= Use perfect forward secrecy and use Diffie-Hellman Group 24 for IKEv2.

Create or Edit IPsec Rule Tunnel Policy (Crypto Map) - Advanced Tab

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Advanced

- Enable NAT-T— Enables NAT Traversal (NAT-T) for this policy.
- Enable Reverse Route Injection—Enables Reverse Route Injection for this policy. Reverse Route Injection (RRI) is used to populate the routing table of an internal router that runs dynamic routing protocols such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP) if you run ASA, or Routing Information Protocol (RIP) for remote VPN Clients or LAN to LAN sessions. RRI is done upon configuration and is considered static, remaining in place until the configuration changes or is removed. The ASA automatically adds static routes to the routing table and announces these routes to its private network or border routers using OSPF. Do not enable RRI if you specify any source/destination (0.0.0.0/0.0.0.0) as the protected network, because this will impact traffic that uses your default route.
  - Dynamic— If dynamic is specified, RRIs are created upon the successful establishment of IPsec security associations (SA's) and deleted after the IPsec SA's are deleted. Typically, RRI routes are used to Initiate a tunnel if one is not present and traffic needs to be encrypted. With dynamic RRI support, no routes are present before the tunnel is brought up. Therefore, an ASA with dynamic RRI configured would typically work only as a responder.



Note Dynamic RRI applies to IKEv2 based static crypto maps only.

- Security Association Lifetime Settings—Configures the duration of a Security Association (SA). This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys.
  - Time—Specifies the SA lifetime in terms of hours (hh), minutes (mm) and seconds (ss).
  - Traffic Volume—Defines the SA lifetime in terms of kilobytes of traffic. Enter the number of kilobytes of payload data after which the IPsec SA expires. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.
- Static Type Only Settings—Specifies parameters for static tunnel policies.
  - Device Certificate—Choose the certificate to use. If you choose something other than None (Use Preshared Keys), which is the default. The Send CA certificate chain check box becomes active when you choose something other than None.
  - Send CA certificate chain—Enables transmission of the entire trust point chain.
  - IKE Negotiation Mode—Chooses the IKE negotiation mode, Main or Aggressive. This parameter sets the mode for exchanging key information and setting up the SAs. It sets the mode that the initiator of the negotiation uses; the responder auto-negotiates. Aggressive Mode is faster, using fewer packets and fewer exchanges, but it does not protect the identity of the communicating parties. Main Mode is slower, using more packets and more exchanges, but it protects the identities of the

communicating parties. This mode is more secure and it is the default selection. If you choose Aggressive, the Diffie-Hellman Group list becomes active.

- Diffie-Hellman Group—Choose the Diffie-Hellman group to apply. The choices are as follows: Group 1 (768-bits), Group 2 (1024-bits), or Group 5 (1536-bits).

- ESP v3—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—Choose 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:

    Clear DF bit—Ignores the DF bit.

    Copy DF bit—Maintains the DF bit.

    Set DF bit—Sets and uses 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 IKE v2 IPsec proposal set on the Tunnel Policy (Crypto Map) Basic tab before enabling TFC.

Use the Burst, Payload Size, and Timeout parameters to generate random length packets at random intervals across the specified SA.

Create or Edit IPsec Rule Traffic Selection Tab

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Traffic Selection

This pane lets you define what traffic to protect (permit) or not protect (deny).

- Action—Specify the action for this rule to take. The selections are protect and do not protect.
- Source—Specify the IP address, network object group or interface IP address for the source host or network. A rule cannot use the same address as both the source and destination. Click ... to launch the Browse Source dialog box that contains the following fields:
  - Add/Edit—Choose IP Address or Network Object Group to add more source addresses or groups.
  - Delete—Click to delete an entry.
  - Filter—Enter an IP Address to filter the results displayed.
  - Name—Indicates that the parameters that follow specify the name of the source host or network.
  - IP Address—Indicates that the parameters that follow specify the interface, IP address, and subnet mask of the source host or network.

- Netmask—Chooses a standard subnet mask to apply to the IP address. This parameter appears when you choose the IP Address option button.
- Description—Enter a description.
- Selected Source—Click **Source** to include the selected entry as a source.

- Destination—Specify the IP address, network object group or interface IP address for the destination host or network. A rule cannot use the same address as both the source and destination. Click ... to launch the Browse Destination dialog box that contains the following fields:
  - Add/Edit—Choose IP Address or Network Object Group to add more destination addresses or groups.
  - Delete—Click to delete an entry.
  - Filter—Enter an IP Address to filter the results displayed.
  - Name—Indicates that the parameters that follow specify the name of the destination host or network.
  - IP Address—Indicates that the parameters that follow specify the interface, IP address, and subnet mask of the destination host or network.
  - Netmask—Chooses a standard subnet mask to apply to the IP address. This parameter appears when you choose the IP Address option button.
  - Description—Enter a description.
  - Selected Destination—Click **Destination** to include the selected entry as a destination.
- Service—Enter a service or click ... to launch the browse service dialog box where you can choose from a list of services.
- Description—Enter a description for the Traffic Selection entry.
- More Options
  - Enable Rule—Click to enable this rule.
  - Source Service—Enter a service or click **...** to launch the browse service dialog box where you can choose from a list of services.
  - Time Range—Define a time range for which this rule applies.
  - Group—Indicates that the parameters that follow specify the interface and group name of the source host or network.
  - Interface—Choose the interface name for the IP address. This parameter appears when you choose the IP Address option button.
  - IP address—Specifies the IP address of the interface to which this policy applies. This parameter appears when you choose the IP Address option button.
  - Destination—Specify the IP address, network object group or interface IP address for the source or destination host or network. A rule cannot use the same address as both the source and destination. Click **...** for either of these fields to launch the Browse dialog box that contains the following fields:

- Name—Choose the interface name to use as the source or destination host or network. This parameter appears when you choose the Name option button. This is the only parameter associated with this option.
- Interface—Choose the interface name for the IP address. This parameter appears when you click the Group option button.
- Group—Choose the name of the group on the specified interface for the source or destination host or network. If the list contains no entries, you can enter the name of an existing group. This parameter appears when you click the Group option button.

• **Protocol and Service**—Specifies protocol and service parameters relevant to this rule.



Note "Any - any" IPsec rules are not allowed. This type of rule would prevent the device and its peer from supporting multiple LAN -to-LAN tunnels.

- TCP—Specifies that this rule applies to TCP connections. This selection also displays the Source Port and Destination Port group boxes.
- UDP—Specifies that this rule applies to UDP connections. This selection also displays the Source Port and Destination Port group boxes.
- ICMP—Specifies that this rule applies to ICMP connections. This selection also displays the ICMP Type group box.
- IP—Specifies that this rule applies to IP connections. This selection also displays the IP Protocol group box.
- Manage Service Groups—Displays the Manage Service Groups pane, on which you can add, edit, or delete a group of TCP/UDP services/ports.
- Source Port and Destination Port —Contains TCP or UDP port parameters, depending on which option button you chose in the Protocol and Service group box.
- Service—Indicates that you are specifying parameters for an individual service. Specifies the name of the service and a boolean operator to use when applying the filter.
- Boolean operator (unlabeled)—Lists the boolean conditions (equal, not equal, greater than, less than, or range) to use in matching the service specified in the service box.
- Service (unlabeled)—Identifies the service (such as https, ldaps, or any) to be matched. If you specified the range service operator this parameter becomes two boxes, into which you enter the start and the end of the range.
- ... —Displays a list of services from which you can choose the service to display in the Service box.
- Service Group—Indicates that you are specifying the name of a service group for the source port.
- Service (unlabeled)—Choose the service group to use.
- ICMP Type—Specifies the ICMP type to use. The default is any. Click the **...** button to display a list of available types.

• Options

- Time Range—Specify the name of an existing time range or create a new range.
- ... —Displays the Add Time Range pane, on which you can define a new time range.
- Please enter the description below (optional)—Provides space for you to enter a brief description of the rule.

IPsec Pre-Fragmentation Policies

Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies

The IPsec pre-fragmentation policy specifies how to treat packets that exceed the maximum transmission unit (MTU) setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the ASA and the client rejects or drops IP fragments. For example, suppose a client wants to FTP get from an FTP server behind a ASA. The FTP server transmits packets that when encapsulated would exceed the ASA's MTU size on the public interface. The selected options determine how the ASA processes these packets. The pre-fragmentation policy applies to all traffic travelling out the ASA public interface.

The ASA encapsulates all tunneled packets. After encapsulation, the ASA fragments packets that exceed the MTU setting before transmitting them through the public interface. This is the default policy. This option works for situations where fragmented packets are allowed through the tunnel without hindrance. For the FTP example, large packets are encapsulated and then fragmented at the IP layer. Intermediate devices may drop fragments or just out-of-order fragments. Load-balancing devices can introduce out-of-order fragments.

When you enable pre-fragmentation, the ASA fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the ASA clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site. In our example, the ASA overrides the MTU and allows fragmentation by clearing the DF bit.

Note Changing the MTU or the pre-fragmentation option on any interface tears down all existing connections. For example, if 100 active tunnels terminate on the public interface, and you change the MTU or the pre-fragmentation option on the external interface, all of the active tunnels on the public interface are dropped.

Use this pane to view or **Edit** an existing IPsec pre-fragmentation policy and do-not-fragment (DF) bit policy for an interface selected on the parent pane.

Fields

- **Interface**—Identifies the chosen interface. You cannot change this parameter using this dialog box.
- **Pre-fragmentation Enabled**—Enables or disables IPsec pre-fragmentation. The ASA fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the ASA clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent, non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site.
- **DF Bit Setting Policy**—The do-not-fragment bit policy: Copy, Clear, or Set.

Configure IKEv2 Fragmentation Options

On the ASA, IKEv2 fragmentation can be enabled or disabled, the MTU (Maximum Transmission Unit) used when fragmenting IKEv2 packets can be specified, and a preferred fragmentation method can be configured by the administrator on the following screen:

Configuration > **Site-to-Site VPN** > **Advanced** > **IKE parameters**

By default, all methods of IKEv2 fragmentation are enabled, the MTU is 576 for IPv4, or 1280 for IPv6, and the preferred method is the IETF standard RFC-7383.

Specify the MTU with the following considerations:

- The MTU value used should include the IP(IPv4/IPv6) header + UDP header size.
- If not specified by the administrator the default MTU is 576 for IPv4, or 1280 for IPv6.
- Once specified, the same MTU will be used for both IPv4 and IPv6.
- Valid range is 68-1500.



Note You must consider the ESP overhead while configuring the MTU. The packet size increases after encryption due to the ESP overhead that is added to the MTU during the encryption. If you get the "packet too big" error, ensure that you check the MTU size and configure a lower MTU.

One of the following supported fragmentation methods can be configured as the preferred fragmentation method for IKEv2:

- IETF RFC-7383 standard based IKEv2 fragmentation.
  - This method will be used when both peers specify support and preference during negotiation.
  - Using this method, encryption is done after fragmentation providing individual protection for each IKEv2 Fragment message.
- Cisco proprietary fragmentation.
  - This method will be used if it is the only method provided by a peer, such as the AnyConnect Client, or if both peers specify support and preference during negotiation.
  - Using this method fragmentation is done after encryption. The receiving peer cannot decrypt or authenticate the message until all fragments are received.
  - This method does not interoperate with non-Cisco peers.

Before you begin

- Path MTU Discovery is not supported, the MTU needs to be manually configured to match the needs of the network.
- This configuration is global and will affect future SAs established after the configuration has been applied. Older SAs will not be affected. Same behavior holds true when fragmentation is disabled.
- A maximum of a 100 fragments can be received.

Procedure

Step 1 In ASDM go to **Configuration** > **Site-to-Site VPN** > **Advanced** > **IKE parameters**.

Step 2 Select or deselect the **Enable fragmentation** field.

Step 3 Specify the **Fragmentation MTU** size.

Step 4 Specify the **Preferred fragmentation method**.

IPsec Proposals (Transform Sets)

Configuration > Site-to-Site VPN > Advanced > IPsec Proposals (Transform Sets)

A transform is a set of operations done on a data flow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with 3DES encryption and the HMAC-MD5 authentication algorithm (ESP-3DES-MD5).

Use this pane to view, **Add**, **Edit**, or **Delete** IKEv1 and IKEv2 transform sets described below. Each table displays the name and details of the configured transform sets.

IKEv1 IPsec Proposals (Transform Sets)

- **Mode**—Mode for applying ESP encryption and authentication. This determines what part of the original IP packet has ESP applied.
  - **Tunnel mode**—(default) Applies ESP encryption and authentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destination addresses.The entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPsec tunnel. The destination 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 receive 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.
  - **Transport mode**—Only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. With transport mode, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header is encrypted, which limits examination of the packet.
- **ESP Encryption**—Encapsulating Security Protocol (ESP) encryption algorithms for the transform sets. ESP provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data being protected.
- **ESP Authentication**— ESP authentication algorithms for the transform set.

IKEv2 IPsec Proposals

- **Mode**—Mode for applying ESP encryption and authentication. This determines what part of the original IP packet has ESP applied.
  - **Tunnel mode**—(default) Encapsulation mode will be tunnel mode. Tunnel mode applies ESP encryption and authentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destination addresses.The entire original IP datagram is encrypted, and it becomes the payload in a new IP packet.

    This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPsec tunnel. The destination 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 receive 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.
  - **Transport mode**— Encapsulation mode will be transport mode with option to fallback on tunnel mode, if peer does not support it. In Transport mode only the IP payload is encrypted, and the original IP headers are left intact.

    This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. With transport mode, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header is encrypted, which limits examination of the packet.
  - **Transport Required**— Encapsulation mode will be transport mode only, falling back to tunnel mode is not allowed.



Note Transport mode is not recommended for Remote Access VPNs.

Examples of negotiation of the encapsulation mode is as follows:

- If the initiator proposes transport mode, and the responder responds with tunnel mode, the initiator will fall back to Tunnel mode.
- If the initiator proposes tunnel mode, and responder responds with transport mode, the responder will fallback to Tunnel mode.
- If the initiator proposes tunnel mode and responder has transport-require mode, then NO PROPOSAL CHOSEN will be sent by the responder.
- Similarly if initiator has transport-require, and responder has tunnel mode, NO PROPOSAL CHOSEN will be sent by the responder.

- **Encryption**—Shows the Encapsulating Security Protocol (ESP) encryption algorithms for the IKEv2 IPsec Proposal. ESP provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data being protected.

- **Integrity Hash**—Shows the hash algorithm that ensures data integrity for the ESP protocol. It ensures that a packet comes from whom you would expect and that no modifications were made in transit. It ensures that a packet comes from who you would expect and that no modifications were made in transit. You must choose the null integrity algorithm if AES-GCM/GMAC has been configured as the encryption algorithm.

IPsec Profile

- **Name**—IPsec profile name.
- **IKE v1 IPsec Proposal**—IKE v1 IPsec proposal or the IKE v2 IPsec proposal created for the IPsec profile.
- **Responder only**—Tunnel acts only as a responder.
- **Lifetime**—Security association lifetime duration values in kilobytes and seconds.
- **PFS**—Indicates if PFS is enabled or not.
- **Trustpoint**—Certificate used while initiating the tunnel connection.
- **Local-Identity**—Local IKE identity for the VPN tunnel.
- **Reverse-route**—Indicates if Reverse Route Injection (RRI) is enabled for this IPsec profile.

Security Association (SA) Strength Enforcement—Check this check box to permit connection where the IKEv2 encryption cipher strength is at least equal to the strength of any of its child IPsec SA's encryption ciphers.