CHAPTER 65

Configuring L2TP over IPsec

This chapter describes how to configure L2TP over IPsec/IKEv1 on the ASA. This chapter includes the following topics:

- Information About L2TP over IPsec/IKEv1, page 65-1
- Licensing Requirements for L2TP over IPsec, page 65-3
- Guidelines and Limitations, page 65-7
- Configuring L2TP over IPsec, page 65-9
- Feature History for L2TP over IPsec, page 65-19

Information About L2TP over IPsec/IKEv1

Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clients to use the public IP network to securely communicate with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data.

L2TP protocol is based on the client/server model. The function is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator (LAC). The LNS typically runs on a network gateway such as a router, while the LAC can be a dial-up Network Access Server (NAS) or an endpoint device with a bundled L2TP client such as Microsoft Windows, Apple iPhone, or Android.

The primary benefit of configuring L2TP with IPsec/IKEv1 in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, which enables remote access from virtually anyplace with POTS. An additional benefit is that no additional client software, such as Cisco VPN client software, is required.

Note L2TP over IPsec supports only IKEv1. IKEv2 is not supported.

The configuration of L2TP with IPsec/IKEv1 supports certificates using the preshared keys or RSA signature methods, and the use of dynamic (as opposed to static) crypto maps. This summary of tasks assumes completion of IKEv1, as well as pre-shared keys or RSA signature configuration. See Chapter 38, "Configuring Digital Certificates," for the steps to configure preshared keys, RSA, and dynamic crypto maps.

Note L2TP with IPsec on the ASA allows the LNS to interoperate with native VPN clients integrated in such operating systems as Windows, MAC OS X, Android, and Cisco IOS. Only L2TP with IPsec is supported, native L2TP itself is not supported on ASA.

The minimum IPsec security association lifetime supported by the Windows client is 300 seconds. If the lifetime on the ASA is set to less than 300 seconds, the Windows client ignores it and replaces it with a 300 second lifetime.

IPsec Transport and Tunnel Modes

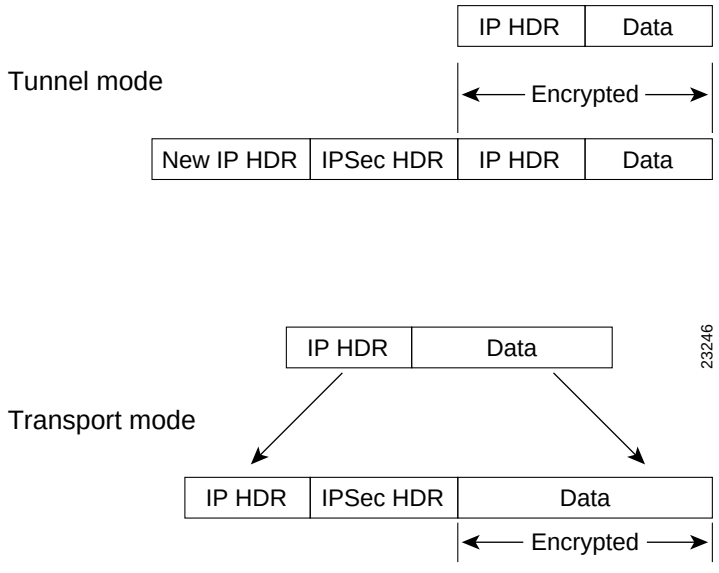
By default, the ASA uses IPsec tunnel mode—the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts 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.

However, the Windows L2TP/IPsec client uses IPsec 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. Figure 65-1 illustrates the differences between IPsec tunnel and transport modes.

In order for Windows L2TP and IPsec clients to connect to the ASA, you must configure IPsec transport mode for a transform set using the **crypto ipsec transform-set trans_name mode transport** command. This command is used in the configuration procedure.

With this transport capability, 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 the examination of the packet. Unfortunately, if the IP header is transmitted in clear text, transport mode allows an attacker to perform some traffic analysis.

Figure 65-1 IPsec in Tunnel and Transport Modes



Licensing Requirements for L2TP over IPsec

The following table shows the licensing requirements for this feature:

Note This feature is not available on No Payload Encryption models.

Model	License Requirement[1]
ASA 5505	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license and Security Plus license: 2 sessions. *Optional permanent or time-based licenses: 10 or 25 sessions.* *Shared licenses are not supported.*[2] – AnyConnect Essentials license[3]: 25 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: – Base license: 10 sessions. – Security Plus license: 25 sessions.
ASA 5510	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base and Security Plus license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.* *Optional Shared licenses*[2]*: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 250 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license and Security Plus license: 250 sessions.
ASA 5520	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.* *Optional Shared licenses*[2]*: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 750 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 750 sessions.

Model	License Requirement[1]
ASA 5540	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 2500 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 2500 sessions.
ASA 5550	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 5000 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 5000 sessions.
ASA 5580	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 10000 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 10000 sessions.

Model	License Requirement[1]
ASA 5512-X	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 250 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 250 sessions.
ASA 5515-X	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 250 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 250 sessions.
ASA 5525-X	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 750 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 750 sessions.
ASA 5545-X	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 2500 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 2500 sessions.

Model	License Requirement[1]
ASA 5555-X	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 5000 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 5000 sessions.
ASA 5585-X with SSP-10	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 5000 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 5000 sessions.
ASA 5585-X with SSP-20, -40, and -60	• IPsec remote access VPN using IKEv2 (use one of the following): – AnyConnect Premium license: Base license: 2 sessions. *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.* *Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* – AnyConnect Essentials license[3]: 10000 sessions. • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2: Base license: 10000 sessions.

1. The maximum combined VPN sessions of *all* types cannot exceed the maximum sessions shown in this table. For the ASA 5505, the maximum combined sessions is 10 for the Base license, and 25 for the Security Plus license.
2. A shared license lets the ASA act as a shared license server for multiple client ASAs. The shared license pool is large, but the maximum number of sessions used by each individual ASA cannot exceed the maximum number listed for permanent licenses.

3. The AnyConnect Essentials license enables AnyConnect VPN client access to the ASA. This license does not support browser-based SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium license instead of the AnyConnect Essentials license.

   Note: With the AnyConnect Essentials license, VPN users can use a Web browser to log in, and download and start (WebLaunch) the AnyConnect client.

   The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium SSL VPN Edition license.

   The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given ASA: AnyConnect Premium license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium licenses on different ASAs in the same network.

   By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command.

   For a detailed list of the features supported by the AnyConnect Essentials license and AnyConnect Premium license, see *AnyConnect Secure Mobility Client Features, Licenses, and OSs*:

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

Prerequisites for Configuring L2TP over IPsec

Configuring L2TP over IPsec has the following prerequisites:

- You can configure the default group policy (DfltGrpPolicy) or a user-defined group policy for L2TP/IPsec connections. In either case, the group policy must be configured to use the L2TP/IPsec tunneling protocol. If the L2TP/IPsec tunning protocol is not configured for your user-defined group policy, configure the DfltGrpPolicy for the L2TP/IPsec tunning protocol and allow your user-defined group policy to inherit this attribute.
- You need to configure the default connection proflie (tunnel group), DefaultRAGroup, if you are performing “pre-shared key” authentication. If you are performing certificate-based authentication, you can use a user-defined connection profile that can be chosen based on certificate identifiers.
- IP connectivity needs to be established between the peers. To test connectivity, try to ping the IP address of the ASA from your endpoint and try to ping the IP address of your endpoint from the ASA.
- Make sure that UDP port 1701 is not blocked anywhere along the path of the connection.
- If a Windows 7 endpoint device authenticates using a certificate that specifies a SHA signature type, the signature type must match that of the ASA, either SHA1 or SHA2.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single context mode. Multiple context mode is not supported.

Firewall Mode Guidelines

Supported only in routed firewall mode. Transparent mode is not supported.

Failover Guidelines

L2TP over IPsec sessions are not supported by stateful failover.

IPv6 Guidelines

There is no native IPv6 tunnel setup support for L2TP over IPsec.

Authentication Guidelines

The ASA only supports the PPP authentications PAP and Microsoft CHAP, Versions 1 and 2, on the local database. EAP and CHAP are performed by proxy authentication servers. Therefore, if a remote user belongs to a tunnel group configured with the **authentication eap-proxy** or **authentication chap** commands, and the ASA is configured to use the local database, that user will not be able to connect.

Supported PPP Authentication Types

L2TP over IPsec connections on the ASA support only the PPP authentication types shown in Table 65-1.

Table 65-1 *AAA Server Support and PPP Authentication Types*

AAA Server Type	Supported PPP Authentication Types
LOCAL	PAP, MSCHAPv1, MSCHAPv2
RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TACACS+	PAP, CHAP, MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

Table 65-1 PPP Authentication Type Characteristics

Keyword	Authentication Type	Characteristics
`chap`	CHAP	In response to the server challenge, the client returns the encrypted [challenge plus password] with a cleartext username. This protocol is more secure than the PAP, but it does not encrypt data.
`eap-proxy`	EAP	Enables EAP which permits the security appliance to proxy the PPP authentication process to an external RADIUS authentication server.
`ms-chap-v1` `ms-chap-v2`	Microsoft CHAP, Version 1 Microsoft CHAP, Version, 2	Similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.
`pap`	PAP	Passes cleartext username and password during authentication and is not secure.

Configuring L2TP over IPsec

This section provides the required ASA IKEv1 (ISAKMP) policy settings that allow native VPN clients, integrated with the operating system on an endpoint, to make a VPN connection to the ASA using L2TP over IPsec protocol.

- IKEv1 phase 1—3DES encryption with SHA1 hash method.
- IPsec phase 2—3DES or AES encryption with MD5 or SHA hash method.
- PPP Authentication—PAP, MS-CHAPv1, or MSCHAPv2 (preferred).
- Pre-shared key (only for iPhone).

Detailed CLI Configuration Steps

	Command	Purpose
Step 1	**crypto ipsec transform-set** *transform_name ESP_Encryption_Type ESP_Authentication_Type* **Example:** `hostname(config)# crypto ipsec transform-set my-transform-set esp-des esp-sha-hmac`	Creates a transform set with a specific ESP encryption type and authentication type.
Step 2	**crypto ipsec transform-set** *trans_name* **mode transport** **Example:** `hostname(config)# crypto ipsec transform-set my-transform-set mode transport`	Instructs IPsec to use transport mode rather than tunnel mode.
Step 3	**vpn-tunnel-protocol** *tunneling_protocol* **Example:** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec`	Specifies L2TP/IPsec as the vpn tunneling protocol.
Step 4	**dns value** [**none** | *IP_primary* [*IP_secondary*] **Example:** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2`	(Optional) Instructs the adaptive security appliance to send DNS server IP addresses to the client for the group policy.
Step 5	**wins-server value** [**none** | *IP_primary* [*IP_secondary*]] **Example:** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4`	(Optional) Instructs the adaptive security appliance to send WINS server IP addresses to the client for the group policy.

	Command	Purpose
Step 6	**tunnel-group** *name* **type remote-access** **Example:** `hostname(config)# tunnel-group sales-tunnel type remote-access`	Creates a connection profile (tunnel group).
Step 7	**default-group-policy** *name* **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy`	Links the name of a group policy to the connection profile (tunnel group).
Step 8	**ip local pool** *pool_name starting_address-ending_address* **mask** *subnet_mask* **Example:** `hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0`	(Optional) Creates an IP address pool.
Step 9	**address-pool** *pool_name* **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# address-pool sales_addresses`	(Optional) Associates the pool of IP addresses with the connection profile (tunnel group).
Step 10	**authentication-server-group** *server_group* **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL`	Specifies a method to authenticate users attempting L2TP over IPsec connections, for the connection profile (tunnel group). If you are not using the ASA to perform local authentication, and you want to fallback to local authentication, add LOCAL to the end of the command.
Step 11	**authentication** *auth_type* **Example:** `hostname(config)# tunnel-group name ppp-attributes` `hostname(config-ppp)# authentication ms-chap-v1`	Specifies the PPP authentication protocol for the tunnel group. See Table 65-1 for the types of PPP authencation and their characteristics.
Step 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **Example:** `hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes` `hostname(config-tunnel-ipsec)# pre-shared-key cisco123`	Sets the pre-shared key for your connection profile (tunnel group).

	Command	Purpose
Step 13	**accounting-server-group** *aaa_server_group* **Example:** `hostname(config)# tunnel-group sales_tunnel general-attributes` `hostname(config-tunnel-general)# accounting-server-group sales_aaa_server`	(Optional) Generates a AAA accounting start and stop record for an L2TP session for the connection profile (tunnel group).
Step 14	**l2tp tunnel hello** *seconds* **Example:** `hostname(config)# l2tp tunnel hello 100`	Configures the interval (in seconds) between hello messages. The range is 10 through 300 seconds. The default is 60 seconds.
Step 15	**crypto isakmp nat-traversal** *seconds* **Example:** `hostname(config)# crypto isakmp enable` `hostname(config)# crypto isakmp nat-traversal 1500`	(Optional) Enables NAT traversal so that ESP packets can pass through one or more NAT devices. If you expect multiple L2TP clients behind a NAT device to attempt L2TP over IPsec connections to the adaptive security appliance, you must enable NAT traversal. To enable NAT traversal globally, check that ISAKMP is enabled (you can enable it with the **crypto isakmp enable** command) in global configuration mode, and then use the **crypto isakmp nat-traversal** command.
Step 16	**strip-group** **strip-realm** **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# strip-group` `hostname(config-tunnel-general)# strip-realm`	(Optional) Configures tunnel group switching. The goal of tunnel group switching is to give users a better chance at establishing a VPN connection when they authenticate using a proxy authentication server. Tunnel group is synonymous with connection profile.

	Command	Purpose
Step 17	**username** *name* **password** *password* **mschap** **Example:** `hostname(config)# username jdoe password j!doe1 mschap`	This example shows creating a user with the username `jdoe`, the password `j!doe1`. The mschap option specifies that the password is converted to Unicode and hashed using MD4 after you enter it. This step is needed only if you are using a local user database.
Step 18	**crypto isakmp policy** *priority* **Example:** `hostname(config)# crypto isakmp policy 5`	The crypto isakmp policy command creates the IKE Policy for Phsase 1 and assigns it a number. There are several different configurable parameters of the IKE policy that you can configure. The isakamp policy is needed so the ASA can complete the IKE negotiation. See the "Creating IKE Policies to Respond to Windows 7 Proposals" section on page 65-13 for configuration examples for Windows 7 native VPN clients.

Creating IKE Policies to Respond to Windows 7 Proposals

Windows 7 L2TP/IPsec clients send several IKE policy proposals to establish a VPN connection with the ASA. Define one of the following IKE policies to facilitate connections from Windows 7 VPN native clients.

	Command	Purpose
Step 1	Detailed CLI Configuration Steps, page 65-9	Follow the Detailed CLI Configuration Steps procedure through step Step 18. Add the additional steps in this table to configure the IKE policy for Windows 7 native VPN clients.
Step 1	**show run crypto isakmp** **Example:** `hostname(config)# show run crypto isakmp`	Displays the attributes and the number of any existing IKE policies.
Step 2	**crypto isakmp policy** number **Example:** `hostname(config)# crypto isakmp policy` *number* `hostname(config-isakmp-policy)#`	Allows you to configure an IKE policy. The number argument specifies the number of the IKE policy you are configuring. This number was listed in the output of the `show run crypto isakmp` command.
Step 3	**authentication** **Example:** `hostname(config-isakmp-policy)# authentication pre-share`	Sets the authentication method the ASA uses to establish the identity of each IPsec peer to use preshared keys.
Step 4	**encryption** *type* **Example:** `hostname(config-isakmp-policy)# encryption {3des|aes|aes-256}`	Choose a symmetric encryption method that protects data transmitted between two IPsec peers. For Windows 7 choose either **3des**, **aes**, for 128-bit AES, or **aes-256**.
Step 5	**hash** **Example:** `hostname(config-isakmp-policy)# hash sha`	Choose the hash algorithm that ensures data integrity. For Windows 7, specify **sha** for the SHA-1 algorithm.
Step 6	**group** **Example:** `hostname(config-isakmp-policy)# group 5`	Choose the Diffie-Hellman group identifier. For Windows 7, specify 5 for the 1536-bit Diffie-Hellman group.
Step 7	**lifetime** **Example:** `hostname(config-isakmp-policy)# lifetime 86400`	Specify the SA lifetime in seconds. For Windows 7, specify 86400 seconds to represent 24 hours.

Detailed CLI Configuration Steps

	Command	Purpose
Step 1	`crypto ipsec` *ike_version* `transform-set` *transform_name ESP_Encryption_Type ESP_Authentication_Type* **Example:** `crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac`	Creates a transform set with a specific ESP encryption type and authentication type.
Step 2	`crypto ipsec` *ike_version* `transform-set` *trans_name* `mode transport` **Example:** `crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport`	Instructs IPsec to use transport mode rather than tunnel mode.
Step 3	**vpn-tunnel-protocol** *tunneling_protocol* **Example:** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec`	Specifies L2TP/IPsec as the vpn tunneling protocol.
Step 4	**dns value** [**none** | *IP_primary* [*IP_secondary*] **Example:** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2`	(Optional) Instructs the adaptive security appliance to send DNS server IP addresses to the client for the group policy.
Step 5	**wins-server value** [**none** | *IP_primary* [*IP_secondary*]] **Example:** `hostname(config)# group-policy DfltGrpPolicy attributes` `hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4`	(Optional) Instructs the adaptive security appliance to send WINS server IP addresses to the client for the group policy.
Step 6	**ip local pool** *pool_name starting_address-ending_address* **mask** *subnet_mask* **Example:** `hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0`	(Optional) Creates an IP address pool.
Step 7	**address-pool** *pool_name* **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# address-pool sales_addresses`	(Optional) Associates the pool of IP addresses with the connection profile (tunnel group).

	Command	Purpose
Step 8	**tunnel-group** *name* **type remote-access** **Example:** `hostname(config)# tunnel-group sales-tunnel type remote-access`	Creates a connection profile (tunnel group).
Step 9	**default-group-policy** *name* **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy`	Links the name of a group policy to the connection profile (tunnel group).
Step 10	**authentication-server-group** *server_group* [local] **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL`	Specifies a method to authenticate users attempting L2TP over IPsec connections, for the connection profile (tunnel group). If you are not using the ASA to perform local authentication, and you want to fallback to local authentication, add LOCAL to the end of the command.
Step 11	**authentication** *auth_type* **Example:** `hostname(config)# tunnel-group` *name* `ppp-attributes` `hostname(config-ppp)# authentication ms-chap-v1`	Specifies the PPP authentication protocol for the tunnel group. See Table 65-1 for the types of PPP authencation and their characteristics.
Step 12	**tunnel-group** *tunnel group name* **ipsec-attributes** **Example:** `hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes` `hostname(config-tunnel-ipsec)# ikev1 pre-shared-key` *cisco123*	Sets the pre-shared key for your connection profile (tunnel group).
Step 13	**accounting-server-group** *aaa_server_group* **Example:** `hostname(config)# tunnel-group sales_tunnel general-attributes` `hostname(config-tunnel-general)# accounting-server-group sales_aaa_server`	(Optional) Generates a AAA accounting start and stop record for an L2TP session for the connection profile (tunnel group).
Step 14	**l2tp tunnel hello** *seconds* **Example:** `hostname(config)# l2tp tunnel hello 100`	Configures the interval (in seconds) between hello messages. The range is 10 through 300 seconds. The default interval is 60 seconds.

	Command	Purpose
Step 15	**crypto isakmp nat-traversal** *seconds* **Example:** `hostname(config)# crypto isakmp enable` `hostname(config)# crypto isakmp nat-traversal 1500`	(Optional) Enables NAT traversal so that ESP packets can pass through one or more NAT devices. If you expect multiple L2TP clients behind a NAT device to attempt L2TP over IPsec connections to the adaptive security appliance, you must enable NAT traversal. To enable NAT traversal globally, check that ISAKMP is enabled (you can enable it with the **crypto isakmp enable** command) in global configuration mode, and then use the **crypto isakmp nat-traversal** command.
Step 16	`strip-group` `strip-realm` **Example:** `hostname(config)# tunnel-group DefaultRAGroup general-attributes` `hostname(config-tunnel-general)# strip-group` `hostname(config-tunnel-general)# strip-realm`	(Optional) Configures tunnel group switching. The goal of tunnel group switching is to give users a better chance at establishing a VPN connection when they authenticate using a proxy authentication server. Tunnel group is synonymous with connection profile.
Step 17	**username** *name* **password** *password* **mschap** **Example:** `asa2(config)# username jdoe password j!doe1 mschap`	This example shows creating a user with the username `jdoe`, the password `j!doe1`. The mschap option specifies that the password is converted to Unicode and hashed using MD4 after you enter it. This step is needed only if you are using a local user database.
Step 18	**crypto ikev1 policy** *priority* **group** *Diffie-Hellman Group* **Example:** `hostname(config)# crypto ikev1 policy 5` `hostname(config-ikev1-policy)# group 5`	The crypto isakmp policy command creates the IKE Policy for Phase 1 and assigns it a number. There are several different configurable parameters of the IKE policy that you can configure. You can also specify a Diffie-Hellman Group for the policy. The isakamp policy is needed so the ASA can complete the IKE negotiation. See the "Creating IKE Policies to Respond to Windows 7 Proposals" section on page 65-17 for configuration examples for Windows 7 native VPN clients.

Creating IKE Policies to Respond to Windows 7 Proposals

Windows 7 L2TP/IPsec clients send several IKE policy proposals to establish a VPN connection with the ASA. Define one of the following IKE policies to facilitate connections from Windows 7 VPN native clients.

	Command	Purpose
Step 1	Detailed CLI Configuration Steps, page 65-14	Follow the Detailed CLI Configuration Steps procedure through step Step 18. Add the additional steps in this table to configure the IKE policy for Windows 7 native VPN clients.
Step 1	**show run crypto ikev1** **Example:** `hostname(config)# show run crypto ikev1`	Displays the attributes and the number of any existing IKE policies.
Step 2	**crypto ikev1 policy** number **Example:** `hostname(config)# crypto ikev1 policy` *number* `hostname(config-ikev1-policy)#`	Allows you to configure an IKE policy. The number argument specifies the number of the IKE policy you are configuring. This number was listed in the output of the `show run crypto ikev1` command.
Step 3	**authentication** **Example:** `hostname(config-ikev1-policy)# authentication pre-share`	Sets the authentication method the ASA uses to establish the identity of each IPsec peer to use preshared keys.
Step 4	**encryption** *type* **Example:** `hostname(config-ikev1-policy)# encryption {3des|aes|aes-256}`	Choose a symmetric encryption method that protects data transmitted between two IPsec peers. For Windows 7 choose either **3des**, **aes**, for 128-bit AES, or **aes-256**.
Step 5	**hash** **Example:** `hostname(config-ikev1-policy)# hash sha`	Choose the hash algorithm that ensures data integrity. For Windows 7, specify **sha** for the SHA-1 algorithm.
Step 6	**group** **Example:** `hostname(config-ikev1-policy)# group 5`	Choose the Diffie-Hellman group identifier. You can specify 5 for aes, aes-256, or 3des encryption types. You can specify 2 only for 3des encryption types.
Step 7	**lifetime** **Example:** `hostname(config-ikev1-policy)# lifetime 86400`	Specify the SA lifetime in seconds. For Windows 7, specify 86400 seconds to represent 24 hours.

Configuration Example for L2TP over IPsec Using ASA 8.2.5

The following example shows configuration file commands that ensure ASA compatibility with a native VPN client on any operating system:

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
    wins-server value 209.165.201.3 209.165.201.4
    dns-server value 209.165.201.1 209.165.201.2
    vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
    default-group-policy sales_policy
    address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
    pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
    no authentication pap
    authentication chap
    authentication ms-chap-v1
    authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
    authentication pre-share
    encryption 3des
    hash sha
    group 2
    lifetime 86400
```

Configuration Example for L2TP over IPsec Using ASA 8.4.1 and later

The following example shows configuration file commands that ensure ASA compatibility with a native VPN client on any operating system:

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
    wins-server value 209.165.201.3 209.165.201.4
    dns-server value 209.165.201.1 209.165.201.2
    vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
    default-group-policy sales_policy
    address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
    pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
    no authentication pap
    authentication chap
    authentication ms-chap-v1
    authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
```

```
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
    authentication pre-share
    encryption 3des
    hash sha
    group 2
    lifetime 86400
```

Feature History for L2TP over IPsec

Table 65-2 lists the release history for this feature.

Table 65-2 Feature History for L2TP over IPsec

Feature Name	Releases	Feature Information
L2TP over IPsec	7.2(1)	L2TP over IPsec provides the capability to deploy and administer an L2TP VPN solution alongside the IPsec VPN and firewall services in a single platform. The primary benefit of configuring L2TP over IPsec in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, which enables remote access from virtually anyplace with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows with Microsoft Dial-Up Networking (DUN). No additional client software, such as Cisco VPN client software, is required. The following commands were introduced or modified: **authentication eap-proxy**, **authentication ms-chap-v1**, **authentication ms-chap-v2**, **authentication pap**, **l2tp tunnel hello**, **vpn-tunnel-protocol l2tp-ipsec**.