L2TP over IPsec

This chapter describes how to configure L2TP over IPsec/IKEv1 on the ASA.

- About L2TP over IPsec/IKEv1 VPN, on page 1
- Licensing Requirements for L2TP over IPsec, on page 3
- Prerequisites for Configuring L2TP over IPsec, on page 3
- Guidelines and Limitations, on page 3
- Configuring L2TP over Eclipse with CLI, on page 5
- Feature History for L2TP over IPsec, on page 10

About L2TP over IPsec/IKEv1 VPN

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 41, “Digital Certificates,” in the general operations configuration guide for the steps to configure preshared keys, RSA, and dynamic crypto maps.

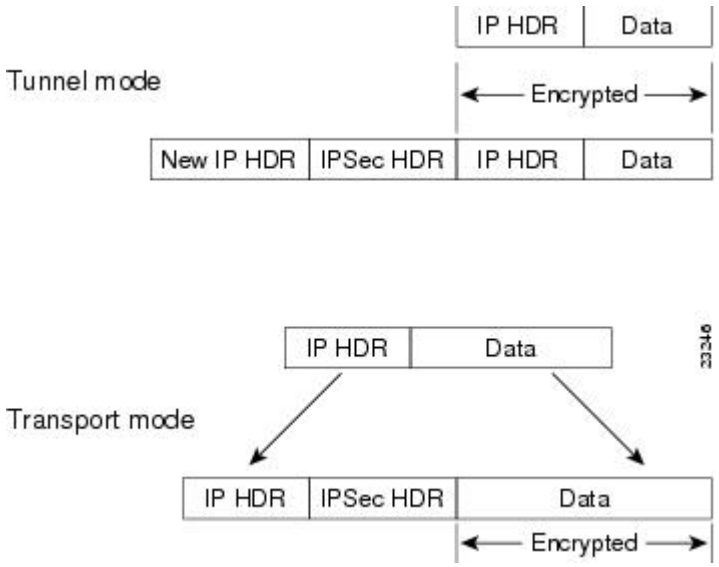
Note L2TP with IPsec on the ASA allows the LNS to interoperate with native VPN clients integrated in such operating systems as Windows, MAC OS X, Android, and Cisco IOS. Only L2TP with IPsec is supported, native L2TP itself is not supported on ASA. The minimum IPsec security association lifetime supported 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. The following figure illustrates the differences between IPsec tunnel and transport modes.

Figure 1: IPsec in 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**.**

Note ASA cannot push more than 28 ACE in split-tunnel access-list.

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.

Licensing Requirements for L2TP over IPsec

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

IPsec remote access VPN using IKEv2 requires an AnyConnect Plus or Apex license, available separately. IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2 uses the Other VPN license that comes with the base license. See Cisco ASA Series Feature Licenses for maximum values per model.

Prerequisites for Configuring L2TP over IPsec

Configuring L2TP over IPsec has the following prerequisites:

- Group Policy-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.
- Connection Profile-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.

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.

Software Limitation on All Platforms

We currently only support 4096 L2TP over IPsec tunnels.

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 as shown:

Table 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 2: 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.

Keyword	Authentication Type	Characteristics
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 Eclipse with CLI

You must configure IKEv1 (ISAKMP) policy settings to allow native VPN clients to make a VPN connection to the ASA using the L2TP over Eclipse protocol.

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

Procedure

Step 1 Create a transform set with a specific ESP encryption type and authentication type.

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-aes esp-sha-hmac
```

Step 2 Instruct Eclipse to use transport mode rather than tunnel mode.

crypto ipsec ike_version transform-set *trans_name* **mode transport**

Example:

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```

Step 3 Specify L2TP/Eclipse as the vpn tunneling protocol.

vpn-tunnel-protocol *tunneling_protocol*

Example:

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

Step 4 (Optional) Instruct the adaptive security appliance to send DNS server IP addresses to the client for the group policy.

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
```

Step 5 (Optional) Instruct the adaptive security appliance to send WINS server IP addresses to the client for the group policy.

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
```

Step 6 (Optional) Create an IP address pool.

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
```

Step 7 (Optional) Associate the pool of IP addresses with the connection profile (tunnel group).

address-pool *pool_name*

Example:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

Step 8 Link the name of a group policy to the connection profile (tunnel group).

default-group-policy name

Example:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
```

Step 9 Specify an authentication server to verify users attempting L2TP over the IPsec connections. If you want the authentication to fallback to local authentication when the server is not available, add LOCAL to the end of the command.

authentication-server-group *server_group* [**local**]

Example:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL
```

Step 10 Specify a method to authenticate users attempting L2TP over Eclipse 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.

authentication *auth_type*

Example:

```
hostname(config)# tunnel-group DefaultRAGroup ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

Step 11 Set the pre-shared key for your connection profile (tunnel group).

tunnel-group *tunnel group name* **ipsec-attributes**

Example:

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

Step 12 (Optional) Generate a AAA accounting start and stop record for an L2TP session for the connection profile (tunnel group).

accounting-server-group *aaa_server_group*

Example:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# accounting-server-group sales_aaa_server
```

Step 13 Configure the interval (in seconds) between hello messages. The range is 10 through 300 seconds. The default interval is 60 seconds.

l2tp tunnel hello *seconds*

Example:

```
hostname(config)# l2tp tunnel hello 100
```

Step 14 (Optional) Enable 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 Eclipse connections to the adaptive security appliance, you must enable NAT traversal.

crypto isakmp nat-traversal *seconds*

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.

Example:

```
hostname(config)# crypto ikev1 enable
hostname(config)# crypto isakmp nat-traversal 1500
```

Step 15 (Optional) Configure 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.

strip-group

strip-realm

Example:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
```

Step 16 (Optional) Create 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.

username *name* **password** *password* **mschap**

Example:

```
asa2(config)# username jdoe password j!doe1 mschap
```

Step 17 Create the IKE Policy for Phase 1 and assign it a number.

crypto ikev1 policy *priority*

group *Diffie-Hellman Group*

There are several different parameters of the IKE policy that you can configure. You can also specify a Diffie-Hellman Group for the policy. The isakamp policy is used by the ASA to complete the IKE negotiation.

Example:

```
hostname(config)# crypto ikev1 policy 14
hostname(config-ikev1-policy)# group14
```

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.

Follow the procedure Configuring L2TP over IPsec for ASA. Add the additional steps in this task to configure the IKE policy for Windows 7 native VPN clients.

Procedure

Step 1 Display the attributes and the number of any existing IKE policies.

Example:

```
hostname(config)# show run crypto ikev1
```

Step 2 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.

crypto ikev1 policy *number*

Step 3 Set the authentication method the ASA uses to establish the identity of each IPsec peer to use preshared keys.

Example:

```
hostname(config-ikev1-policy)# authentication pre-share
```

Step 4 Choose a symmetric encryption method that protects data transmitted between two IPsec peers. For Windows 7, choose **aes** for 128-bit AES, or **aes-256**.

encryption {|**aes**|**aes-256**}

Step 5 Choose the hash algorithm that ensures data integrity. For Windows 7, specify **sha** for the SHA-1 algorithm.

Example:

```
hostname(config-ikev1-policy)# hash sha
```

Step 6 Choose the Diffie-Hellman group identifier. You can specify 14 for aes,aes-256 encryption types.

Example:

```
hostname(config-ikev1-policy)# group 14
```

Step 7 Specify the SA lifetime in seconds. For Windows 7, specify 86400 seconds to represent 24 hours.

Example:

```
hostname(config-ikev1-policy)# lifetime 86400
```

Configuration Example for L2TP over IPsec

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 trans esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set trans 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 aes
 hash sha
```

```
group 14
lifetime 86400
```

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.

Feature Name	Releases	Feature Information
Deprecations of IKE/IPsec encryption and integrity/PRF ciphers DH group 14 support for IKEv1	9.13(1)	The following encryption/integrity/PRF ciphers are deprecated and will be removed in the later release - 9.14(1): • 3DES encryption • DES encryption • MD5 integrity Added DH group 14 (default) support for IKEv1. The group 2 and group 5 command options was deprecated and will be removed in the later release- 9.14(1).