CHAPTER 61

Configuring L2TP over IPsec

This chapter describes how to configure L2TP over IPsec on the adaptive security appliance. This chapter includes the following topics:

Information About L2TP over IPsec

Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol which 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 a PC with a bundled L2TP client such as Microsoft Windows 2000.

The primary benefit of configuring L2TP with 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, enabling remote access from virtually anyplace with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN). No additional client software, such as Cisco VPN client software, is required.

To configure L2TP over IPsec, first configure IPsec transport mode to enable IPsec with L2TP. Then configure L2TP with a virtual private dial-up network VPDN group.

The configuration of L2TP with IPsec supports certificates using the pre-shared keys or RSA signature methods, and the use of dynamic (as opposed to static) crypto maps. This summary of tasks assumes completion of IKE, as well as pre-shared keys or RSA signature configuration. See “Chapter 37, “Configuring Digital Certificates,”” for the steps to configure pre-shared keys, RSA, and dynamic crypto maps.

Note L2TP with IPsec on the adaptive security appliance allows the LNS to interoperate with the Windows 2000 L2TP client. Interoperability with LACs from Cisco and other vendors is currently not supported. Only L2TP with IPsec is supported, native L2TP itself is not supported on adaptive security appliance. The minimum IPsec security association lifetime supported by the Windows 2000 client is 300 seconds. If the lifetime on theadaptive security appliance is set to less than 300 seconds, the Windows 2000 client ignores it and replaces it with a 300 second lifetime.

IPsec Transport and Tunnel Modes

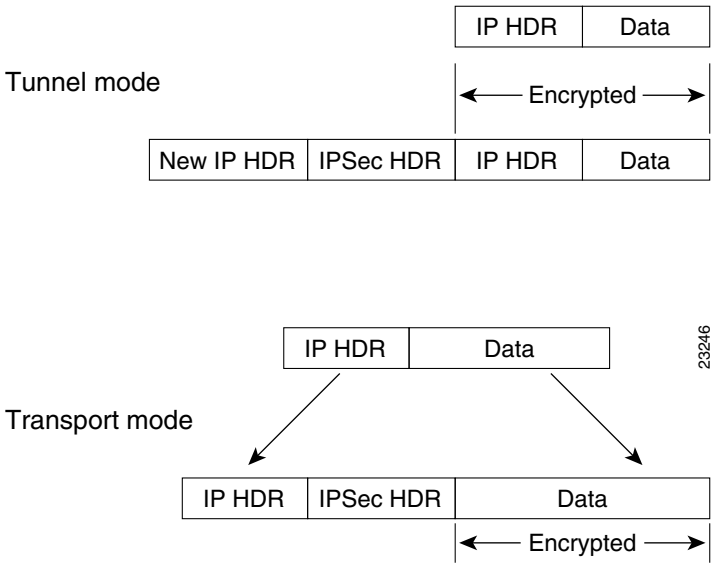
By default, the adaptive security appliance uses IPsec tunnel mode—the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. 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 2000 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 61-1 illustrates the differences between IPsec Tunnel and Transport modes.

Therefore, In order for Windows 2000 L2TP/IPsec clients to connect to the adaptive security appliance, you must configure IPsec transport mode for a transform set using the **crypto ipsec transform-set trans_name mode transport** command. This command is the configuration procedure that follows, **.**

With this capability (transport), 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 will be encrypted, limiting the examination of the packet. Unfortunately, transmitting the IP header in clear text, transport mode allows an attacker to perform some traffic analysis.

Figure 61-1 IPsec in Tunnel and Transport Modes



Licensing Requirements for L2TP over IPsec

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASA 5505	Base License: 10 sessions (25 combined IPSec and SSL VPN[1]). Security Plus License: 25 sessions (25 combined IPSec and SSL VPN[1]).
ASA 5510	Base and Security Plus License: 250 sessions (250 combined IPSec and SSL VPN[1]).
ASA 5520	Base and Security Plus License: 750 sessions (750 combined IPSec and SSL VPN[1]).
ASA 5540	Base and Security Plus License: 5000 sessions (5000 combined IPSec and SSL VPN[1]).
ASA 5550, 5580	Base and Security Plus License: 5000 sessions (5000 combined IPSec and SSL VPN[1]).

1. Although the maximum IPSec and SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.

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.

Configuring L2TP over IPsec

This section describes prerequisites, restrictions, and detailed tasks to configure the adaptive security appliance to accept L2TP over IPsec connections.

Prerequisites

Apple iPhone and MAC OS X Compatibility

The adaptive security appliance requires the following IKE (ISAKMP) policy settings for successful Apple iPhone or MAC OS X connections:

- IKE 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).

The following example shows configuration file commands that ensure iPhone and OS X compatibility:

```
tunnel-group DefaultRAGroup general-attributes
    address-pool pool
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 trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp identity auto
crypto isakmp enable outside
crypto isakmp policy 10
    authentication pre-share
    encryption 3des
    hash sha
    group 2
    lifetime 86400
crypto isakmp nat-traversal 3600
```

For more information about setting IKE policies, see *Configuring IPSec and ISAKMP.*

L2TP/IPsec Connections to Specific Connection Profiles

You can allow users to connect to specific connection profiles (tunnel groups) instead of the default connection profile (DefaultRAGroup). This allows the client to retrieve AAA and PPP attributes from that specific connection profile rather than the default connection profile. To do this, users send their username as *username@groupname*.

However, because the client and the adaptive security appliance negotiate the PPP authentication type and pre-shared key prior to the new connection profile being selected, you must ensure these settings match in the default connection profile and the new one the client switches to.

The following example an example configuration with shows the preshared key *123* and the PPP authentication type *pap* configured in the default connection profile, and then configured in a connection profile named *usersupliedgroupname*:

Example:

```
tunnel-group DefaultRAGroup ipsec-attributes
    pre-shared-key 123
tunnel-group DefaultRAGroup ppp-attributes
    authentication pap

tunnel-group usersuppliedgroupname type ipsec-ra
tunnel-group usersuppliedgroupname general-attributes
    address-pool  20
    authentication-server-group radius
    strip-group
tunnel-group usersuppliedgroupname ipsec-attributes
    pre-shared-key 123
tunnel-group usersuppliedgroupname ppp-attributes
    authentication pap
```

Restrictions

- The adaptive security appliance does not establish an L2TP/IPsec tunnel with Windows 2000 if either the Cisco VPN Client Version 3.x or the Cisco VPN 3000 Client Version 2.5 is installed. To work around this problem, disable the *Cisco VPN Service* for the Cisco VPN Client Version 3.x, or the *ANetIKE Service* for the Cisco VPN 3000 Client Version 2.5 from the Services panel in Windows 2000 (click **Start>Programs>Administrative Tools>Services**). Then restart the IPSec Policy Agent Service from the **Services** panel and reboot the PC.
- The adaptive security appliance 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 connection profile (tunnel group) configured with the **authentication eap-proxy** or **authentication chap** commands, and the adaptive security appliance is configured to use the local database, that user will not be able to connect.
- L2TP over IPsec connections on the adaptive security appliance support only the PPP authentication types shown in Table 61-1:

Table 61-1 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

Detailed Steps

	Command	Purpose
Step 1	**crypto ipsec transform-set** *transform_name algorithm* **Example:** hostname(config)# crypto ipsec transform-set sales_l2tp_transform esp-3des	Creates a transform with a specific algorithm.
Step 2	**crypto ipsec transform-set** *trans_name* **mode transport** **Example:** hostname(config)# crypto ipsec transform-set trans_name mode transport	Instructs IPSec to use transport mode rather than tunnel mode.
Step 3	**vpn-tunnel-protocol l2tp-ipsec** **Example:** hostname(config)# group-policy sales_policy attributes hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec	Specifies L2TP over IPSec as a valid VPN tunneling protocol for a group policy.
Step 4	**dns value** [**none** | *IP_primary* [*IP_secondary*] **Example:** hostname(config)# group-policy sales_policy 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)# 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	**tunnel-group** *name* **type ipsec-ra** **Example:** hostname(config)# tunnel-group sales_tunnel type ipsec-ra	Creates a tunnel group.
Step 7	**default-group-policy** *name* **Example:** hostname(config)# tunnel-group sales_tunnel general-attributes hostname(config-tunnel-general)# default-group-policy sales_policy	Links the name of the group policy to the tunnel group.
Step 8	**authentication-server-group** *server_group* **Example:** hostname(config-tunnel-general)# authentication-server-group sales_server	Specifies a method to authenticate users attempting L2TP over IPSec connections, for the tunnel group.

	Command	Purpose

Step 9	**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 tunnel group.

Step 10	**address-pool** *pool_name*
	
	Example:
	`hostname(config)# tunnel-group sales general-attributes`
	`hostname(config-tunnel-general)# address-pool sales_addresses`
		(Optional) Specifies the local address pool used to allocate the IP address to the client, for the tunnel group.

Step 11	**authentication** *auth_type*
	
	Example:
	`hostname(config)# tunnel-group name ppp-attributes`
	`hostname(config-ppp)# authentication pap`
		Specifies the PPP authentication protocol for the tunnel group. See Table 61-2 for the types of PPP authencation and their characteristics.

Step 12	**l2tp tunnel hello** *seconds* **Example:** `hostname(config)# l2tp tunnel hello 100`	Configures the interval (in seconds) between hello messages.

Step 13	**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.

Table 61-2 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.
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.

Configuration Examples for L2TP over IPsec

The following example shows how to configure L2TP over IPsec:

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
aaa-server sales_server protocol radius
crypto ipsec transform-set sales_l2tp_transform esp-3des esp-sha-hmac
crypto ipsec transform-set sales_l2tp_transform mode transport
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
l2tp tunnel hello 100

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 sales_tunnel type remote-access
tunnel-group sales_tunnel general-attributes
 address-pool sales_addresses
 authentication-server-group none
 accounting-server-group sales_server
 default-group-policy sales_policy
tunnel-group sales_tunnel ppp-attributes
 authentication pap
```

Feature History for L2TP over IPsec

Table 61-3 lists the release history for this feature.

Table 61-3 Feature History for L2TP over IPsec

Feature Name	Releases	Feature Information
L2TP over IPsec	7.2(1)	L2TP/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 with 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, enabling remote access from virtually anyplace with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 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**.