CHAPTER 28

Configuring L2TP over IPSec

This chapter describes how to configure IPSec over L2TP on the security appliance, and includes the following topics:

- L2TP Overview, page 28-1
- Configuring L2TP over IPSec Connections, page 28-2
- Viewing L2TP over IPSec Connection Information, page 28-5

L2TP Overview

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 anywhere 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 39, “Certificate Configuration,”” for the steps to configure pre-shared keys, RSA, and dynamic crypto maps.

Note

L2TP with IPSec on the 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 security appliance.

The minimum IPSec security association lifetime supported by the Windows 2000 client is 300 seconds. If the lifetime on thesecurity 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 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 28-1 illustrates the differences between IPSec Tunnel and Transport modes.

Therefore, in order for Windows 2000 L2TP/IPSec clients to connect to the 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, “Configuring L2TP over IPSec Connections” section on page 28-2.

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 28-1 IPSec in Tunnel and Transport Modes

Configuring L2TP over IPSec Connections

To configure the security appliance to accept L2TP over IPSec connections, follow these steps:
The 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. 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 machine.

**Step 1** Specify IPSec to use transport mode rather than tunnel mode with the `mode` keyword of the `crypto ipsec transform-set` command:

```
hostname(config)# crypto ipsec transform-set trans_name mode transport
```

**Step 2** (Optional) Specify the local address pool used to allocate the IP address to the client using the `address-pool` command in tunnel-group general-attributes mode:

```
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# address-pool pool_name
```

**Step 3** (Optional) Instruct the security appliance to send DNS server IP addresses to the client with the `dns value` command from group policy configuration mode:

```
hostname(config)# group-policy group_policy_name attributes
hostname(config-group-policy)# dns value [none | IP_primary [IP_secondary]]
```

**Step 4** (Optional) Instruct the security appliance to send WINS server IP addresses to the client using the `wins-server` command from group policy configuration mode:

```
hostname(config-group-policy)# wins-server value [none | IP_primary [IP_secondary]]
```

**Step 5** (Optional) Generate a AAA accounting start and stop record for an L2TP session using the `accounting-server-group` command from tunnel group general-attributes mode:

```
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# accounting-server-group aaa_server_group
```

**Step 6** Configure L2TP over IPSec as a valid VPN tunneling protocol for a group or user with the `vpn-tunnel-protocol l2tp-ipsec` command:

For a group, enter group-policy attributes mode:

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

For a user, enter username attributes mode:

```
hostname(config)# username user_name attributes
hostname(config-username)# vpn-tunnel-protocol l2tp-ipsec
```

**Step 7** Create a tunnel group with the `tunnel-group` command, and link the name of the group policy to the tunnel group with the `default-group-policy` command from tunnel group general-attributes mode:

```
hostname(config)# tunnel-group name type ipsec-ra
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# group-policy group_policy_name
```

**Step 8** Configure the PPP authentication protocol using the `authentication type` command from tunnel group ppp-attributes mode. Table 28-1 shows the types of PPP authentication, and their characteristics.

```
hostname(config)# tunnel-group name ppp-attributes
hostname(config-ppp)# authentication pap
```
Chapter 28 Configuring L2TP over IPSec

Step 9 Specify a method to authenticate users attempting L2TP over IPSec connections. Use the authentication-server-group command from tunnel-group general-attributes mode to configure the security appliance to use an authentication server or its own local database.

Using an Authentication Server

To use an authentication server, use the authentication server group keyword:

```
hostname(config)# tunnel-group name general-attributes
hostname(config-tunnel-general)# authentication-server-group auth_server_group
```

Using the Local Database

To use the local database, enter the LOCAL keyword.

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

Note

The 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 tunnel group configured with the authentication eap-proxy or authentication chap commands, and the security appliance is configured to use the local database, that user will not be able to connect.

Step 10 Create a user in the local database with the username command from global configuration mode.

If the user is an L2TP client using Microsoft CHAP, Version 1 or Version 2, and the security appliance is configured to authenticate against the local database, you must include the mschap keyword. For Example:

```
hostname(config)# username t_wmith password eu5d93h mschap
```

Step 11 Configure the interval (in seconds) between hello messages using the l2tp tunnel hello command in global configuration mode:

```
hostname(config)# l2tp tunnel hello seconds
```
Step 12  (Optional) If you expect multiple L2TP clients behind a NAT device to attempt L2TP over IPSec connections to the security appliance, you must enable NAT traversal so that ESP packets can pass through one or more NAT devices.

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. For example:

```
hostname(config)# crypto isakmp enable
hostname(config)# crypto isakmp nat-traversal 30
```

Tunnel Group Switching

Tunnel Group Switching enables the security appliance to associate different users that are establishing L2TP over IPSec connections with different tunnel groups. Since each tunnel group has its own AAA server group and IP address pools, users can be authenticated through methods specific to their tunnel group.

With this feature, instead of sending just a username, the user sends a username and a group name in the format `username@group_name`, where `@` represents a delimiter that you can configure, and the group name is the name of a tunnel group that has been configured on the security appliance.

To enable Tunnel Group Switching, you must enable Strip Group processing using the `strip-group` command from tunnel-group general-attributes mode. When enabled, the security appliance selects the tunnel group for user connections by obtaining the group name from the username presented by the VPN client. The security appliance then sends only the user part of the username for authorization and authentication. Otherwise (if disabled), the security appliance sends the entire username, including the realm.

In the following example, Strip Group processing is enabled for the tunnel-group `telecommuters`:

```
asal(config)# tunnel-group telecommuters general-attributes
asal(config-tunnel-general)# strip-group
```

Viewing L2TP over IPSec Connection Information

The `show vpn-sessiondb` command includes protocol filters that you can use to view detailed information about L2TP over IPSec connections. The full command from global configuration mode is `show vpn-sessiondb detailed remote filter protocol l2tpOverIpsec`.

The following example shows the details of a single L2TP over IPSec connection:

```
hostname# show vpn-sessiondb detail remote filter protocol L2TPOverIPSec
```

Session Type: Remote Detailed

- **Username**: b_smith
- **Index**: 1
- **Assigned IP**: 90.208.1.200  **Public IP**: 70.208.1.212
- **Protocol**: L2TP over IPSec  **Encryption**: 3DES
- **Hashing**: SHA1
- **Bytes Tx**: 418464  **Bytes Rx**: 424440
- **Client Type**:  **Client Ver**: 
- **Group Policy**: DfltGrpPolicy
- **Tunnel Group**: DefaultRAGroup
- **Login Time**: 13:24:48 UTC Thu Mar 30 2006
- **Duration**: 1h:09m:18s
- **Filter Name**: ACSACL-IP-ACL4Clients-440fa5aa
- **NAC Result**: N/A
- **Posture Token**: 

```
```
Viewing L2TP over IPSec Connection Information

IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1

IKE:
- Session ID: 1
- UDP Src Port: 500
- IKE Neg Mode: Main
- Encryption: 3DES
- Rekey Int (T): 28800 Seconds
- D/H Group: 2
- IKE:
  - Session ID: 1
  - UDP Dst Port: 500
  - Auth Mode: preSharedKeys
  - Hashing: SHA1
  - Rekey Left(T): 24643 Seconds

IPSec:
- Session ID: 2
- Local Addr: 80.208.1.2/255.255.255.255/17/1701
- Remote Addr: 70.208.1.212/255.255.255.255/17/1701
- Encryption: 3DES
- Hashing: SHA1
- Idle Time Out: 30 Minutes
- Bytes Tx: 419064
- Bytes Rx: 425040
- Pkts Tx: 4201
- Pkts Rx: 4227

L2TPOverIPSec:
- Session ID: 3
- Username: l2tp
- Assigned IP: 90.208.1.200
- Encryption: none
- Idle Time Out: 30 Minutes
- Bytes Tx: 301386
- Bytes Rx: 306480
- Pkts Tx: 4198
- Pkts Rx: 4224

The following example shows the details of a single L2TP over IPSec over NAT connection:

```
hostname# show vpn-sessiondb detail remote filter protocol L2TPOverIPSecOverNatT
```

Session Type: Remote Detailed

- Username: v_gonzalez
- Index: 2
- Assigned IP: 90.208.1.202
- Public IP: 70.208.1.2
- Protocol: L2TPOverIPSecOverNatT
- Encryption: 3DES
- Hashing: MD5
- Bytes Tx: 1009
- Bytes Rx: 2241
- Client Type: DfltGrpPolicy
- Group Policy: DfltGrpPolicy
- Tunnel Group: l2tpcert
- Login Time: 14:35:15 UTC Thu Mar 30 2006
- Duration: 0h:00m:07s
- Filter Name: N/A
- NAC Result: N/A
- NAC Result: N/A
- IKE: 1
- IPSecOverNatT Sessions: 1
- L2TPOverIPSecOverNatT Sessions: 1

IKE:
Using L2TP Debug Commands

You can display L2TP debug information using the `debug l2tp` command in privileged EXEC mode. To disable the display of debug information, use the `no` form of this command:

```
    debug l2tp {data | error | event | packet} level
```

data displays data packet trace information.

error displays error events.

event displays L2TP connection events.

packet displays packet trace information.

level sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

The following example enables L2TP debug messages for connection events. The `show debug` command reveals that L2TP debug messages are enabled.

```
    hostname# debug l2tp event 1
    hostname# show debug
    debug l2tp event enabled at level 1
    hostname#
```

Enabling IPSec Debug

IPSec debug information can be added to a Windows 2000 client by adding the following registry:

```
    Step 1  Run the Windows 2000 registry editor: REGEDIT.
```
Step 2  Locate the following registry entry:
MyComputer\HKEY_LOCAL_MACHINE\CurrentControlSet\Services\PolicyAgent

Step 3  Create the key by entering oakley.

Step 4  Create the DWORD by entering EnableLogging.

Step 5  Set the “Enable Logging” value to “1”.

Step 6  Stop and Start the IPSec Policy Agent (click Start>Programs>Administrative Tools>Services). The debug file will be found at “%windir%\debug\oakley.log”.

Getting Additional Information

Additional information on various topics can be found at www.microsoft.com:
http://support.microsoft.com/support/kb/articles/Q240/2/62.ASP
How to Configure an L2TP/IPSec Connection Using Pre-Shared Keys Authentication:
http://support.microsoft.com/support/kb/articles/Q253/4/98.ASP
How to Install a Certificate for Use with IP Security (IPSec):
How to use a Windows 2000 Machine Certificate for L2TP over IPSec VPN Connections:
http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp#heading3
How to Create a Custom MMC Console and Enabling Audit Policy for Your Computer:
http://support.microsoft.com/support/kb/articles/Q259/3/35.ASP