L2TP Security

The L2TP security feature allows the security features of IP Security (IPSec) to protect the Layer 2 Tunnel Protocol (L2TP) virtual private dialup network (VPDN) tunnel and the PPP sessions within the tunnel. Without L2TP security, only a one-time, optional mutual authentication is performed during tunnel setup, with no authentication of subsequent data packets or control messages.

The enhanced protection provided by L2TP security increases the integrity and confidentiality of tunneled PPP sessions. The security features of IPSec and Internet Key Exchange (IKE) include confidentiality, integrity checking, replay protection, authentication, and key management. Traditional routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Interior Gateway Routing Protocol (IGRP) will run transparently because a real PPP interface is associated with the secure tunnel.

Configuration Information

Configuration information is included in the "Configuring Additional VPDN Features" module in the *Cisco IOS VPDN Configuration Guide*, Release 12.4T, at the following URL:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tvpdn_c/vpc6adht.htm

Command Reference

This section documents modified commands.

- **crypto map (global IPSec)**
- **ip pmtu**
- **l2tp security crypto-profile**

crypto map (global IPSec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map *map-name seq-num* [**ipsec-manual**]

crypto map *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

crypto map *map-name* [**client-accounting-list** *aaalist*]

crypto map *map-name seq-num* [**gdoi**]

no crypto map *map-name seq-num*

Note Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
seq-num	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the "Usage Guidelines" section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
profile-name	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
aaalist	(Optional) List name.
gdoi	(Optional) Indicates that the key management mechanism is Group Domain of Interpretation (GDOI).

Command Default

No crypto maps exist.
Peer discovery is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3T	The following keywords and arguments were added: • **ipsec-manual** • **ipsec-isakmp** • **dynamic** • *dynamic-map-name*
12.0(5)T	The **discover** keyword was added to support Tunnel Endpoint Discovery (TED).
12.2(4)T	The **profile** *profile-name* keyword and argument combination was added to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(15)T	The **client-accounting-list** *aaalist* keyword and argument combination was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(6)T	The **gdoi** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB without support for the **gdoi** keyword.

Usage Guidelines

Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

- What traffic should be protected
- To which IPSec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and SAs should be used or managed (or what the keys are, if IKE is not used)

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named “mymap” is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

Refer to the “Usage Guidelines” section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps do you want it to be evaluated against the dynamic map set.

If a crypto map entry references a dynamic crypto map set, make it the lowest priority map entry by giving the it the highest *seq-num* value of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

TED

TED is an enhancement to the IPSec feature. Defining a dynamic crypto map allows you to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.

Note TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPSec. Thus, TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the L2TP Security feature. The relevant SAs in the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

Note The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPSec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example configures TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPSec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

The following example configures a crypto map for a GDOI group member:

```
crypto map diffint 10 gdoi
 set group diffint
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters crypto map configuration command mode.
crypto isakmp profile	Audits IPSec user sessions.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

ip pmtu

To enable the discovery of the path maximum transmission unit (MTU) for Layer 2 traffic, use the **ip pmtu** command in VPDN group, VPDN template, or pseudowire class configuration mode. To disable path MTU discovery, use the **no** form of this command.

ip pmtu

no ip pmtu

Syntax Description

This command has no arguments or keywords.

Command Default

Path MTU discovery is disabled.

Command Modes

VPDN group configuration
VPDN template configuration
Pseudowire class configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.3(2)T	Support was added for using this command in pseudowire class configuration mode.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

When issued in VPDN group configuration mode, the **ip pmtu** command enables any tunnel associated with the specified virtual private dialup network (VPDN) group to participate in path MTU discovery.

When issued in pseudowire class configuration mode, the **ip pmtu** command enables any Layer 2 Tunnel Protocol Version 3 (L2TPv3) session derived from the specified pseudowire class configuration to participate in path MTU discovery.

Because path MTU checks decrease switching performance, this option is disabled by default.

When the **ip pmtu** command is enabled, the Don't Fragment (DF) bit in the Layer 2 encapsulation header is copied from the inner IP header to the encapsulation header.

The **ip pmtu** command enables the processing of Internet Control Message Protocol (ICMP) unreachable messages that indicate fragmentation errors in the IP backbone network carrying the tunneled traffic. If an IP packet is larger than the MTU of any interface it must pass through and the DF bit is set, the packet is dropped and an ICMP unreachable message is returned. The ICMP unreachable message indicates the MTU of the interface that was unable to forward the packet without fragmentation. This information allows the source host to reduce the size of the packet before retransmission to allow it to fit through that interface.

Examples

The following example configures a VPDN group named dial-in on a Layer 2 Tunnel Protocol (L2TP) tunnel server and uses the **ip pmtu** command to specify that tunnels associated with this VPDN group will participate in path MTU discovery:

```
Router(config)# vpdn-group dial-in
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# l2tp security crypto-profile l2tp
Router(config-vpdn)# no l2tp tunnel authentication
Router(config-vpdn)# lcp renegotiation on-mismatch
Router(config-vpdn)# ip pmtu
```

The following example shows how to enable the discovery of the path MTU for pseudowires that have been created from the pseudowire class named ether-pw:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip pmtu
```

Related Commands

Command	Description
ip dfbit set	Enables the DF bit in the outer L2TPv3 tunnel header.
ip mtu	Sets the MTU size of IP packets sent on an interface.
ip mtu adjust	Enables automatic adjustment of the IP MTU on a virtual access interface.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp security crypto-profile

To configure IP Security (IPSec) protection of Layer 2 Tunnel Protocol (L2TP) sessions associated with a virtual private dialup network (VPDN) group, use the **l2tp security crypto-profile** command in VPDN group or VPDN template configuration mode. To disable IPSec protection for a VPDN group, use the **no** form of this command.

l2tp security crypto-profile *profile-name* [**keep-sa**]

no l2tp security crypto-profile

Syntax Description

profile-name	The name of the crypto profile to be used for IPSec protection of tunneled PPP sessions.
keep-sa	(Optional) Controls the destruction of IPSec security associations (SAs) upon tunnel teardown. By default, any IPSec phase 2 SAs and Internet Key Exchange (IKE) phase 1 SAs are destroyed when the L2TP tunnel is torn down. Issuing the **keep-sa** keyword prevents the destruction of IKE phase 1 SAs.

Command Default

IPSec security is disabled.
IKE phase 1 SAs are destroyed on tunnel teardown.

Command Modes

VPDN group configuration
VPDN template configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Enabling this command for a VPDN group ensures that no L2TP packets will be processed unless they have IPSec protection.

A crypto profile must be configured using the **crypto map** (global IPSec) command before it can be associated with a VPDN group using the **l2tp security crypto-profile** command. The *profile-name* argument must match the name of a profile configured using the **crypto map** command.

The **keep-sa** keyword can be used to prevent the destruction of IKE phase 1 SAs when the L2TP tunnel between the network access server (NAS) and tunnel server is considered permanent, and the IP addresses of the peer devices rarely change. This option is not useful with short-lived tunnels, such as those generated by client-initiated L2TP tunneling.

Examples

The following example configures VPDN group 1, associates it with the crypto profile named l2tp, and prevents the destruction of IKE phase 1 SAs on tunnel teardown:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.0.0.13
 local name LAC
 l2tp security crypto-profile l2tp keep-sa
```

Related Commands

Command	Description
crypto map (global IPSec)	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.