

Configuring Layer 2 Tunneling Protocol (L2TP) over IPSec

Document ID: 14122

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

Layer 2 tunneling protocols, such as L2TP, do not provide encryption mechanisms for the traffic it tunnels. Instead, they rely on other security protocols, such as IPSec, to encrypt their data. Use this sample configuration to encrypt L2TP traffic using IPSec for users who dial in.

L2TP tunnel is established between the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). An IPSec tunnel is also established between these devices and all L2TP tunnel traffic is encrypted using IPSec.

Prerequisites

Requirements

This document requires a basic understanding of IPSec protocol. To learn more about IPSec, please refer to [An Introduction to IP Security \(IPSec\) Encryption](#).

Components Used

The information in this document is based on these software and hardware versions.

- Cisco IOS® Software Release 12.2(24a)
- Cisco 2500 Series Routers

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, see the [Cisco Technical Tips Conventions](#).

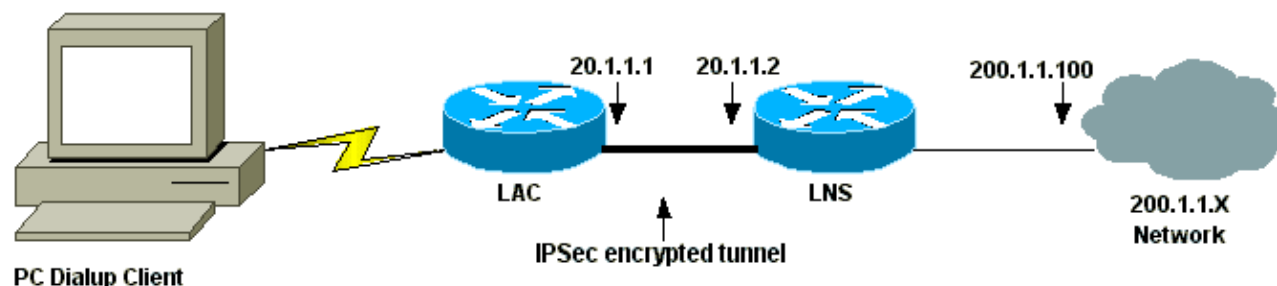
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses the network setup shown in this diagram. The dial up user initiates a PPP session with the LAC over the analog telephone system. After the user is authenticated, the LAC initiates an L2TP tunnel to the LNS. The tunnel end points, LAC and LNS, authenticate each other before the tunnel is created. Once the tunnel is established, an L2TP session is created for the dialup user. To encrypt all the L2TP traffic between the LAC and LNS, the L2TP traffic is defined as the interesting traffic (traffic to be encrypted) for IPSec.



Configurations

This document uses these configurations.

- LAC Configuration
- LNS Configuration

LAC Configuration
<pre>Current configuration: ! version 12.2 service timestamps debug datetime msec localtime show-timezone service timestamps log datetime msec localtime show-timezone service password-encryption ! hostname LAC ! enable password 7 094F471A1A0A ! !--- Usernames and passwords are used !--- for L2TP tunnel authentication. username LAC password 7 0107130A550E0A1F205F5D username LNS password 7 001006080A5E07160E325F !--- Username and password used for authenticating !--- the dial up user. username dialupuser password 7 14131B0A00142B3837 ip subnet-zero !</pre>

```

!--- Enable VDPN.

vpdn enable
vpdn search-order domain
!

!--- Configure vpdn group 1 to request dialin to the LNS,
!--- define L2TP as the protocol, and initiate a tunnel to the LNS 20.1.1.2.
!--- If the user belongs to the domain cisco.com,
!--- use the local name LAC as the tunnel name.

vpdn-group 1
  request-dialin
  protocol l2tp
  domain cisco.com
  initiate-to ip 20.1.1.2
  local name LAC
!

!--- Create Internet Key Exchange (IKE) policy 1,
!--- which is given highest priority if there are additional
!--- IKE policies. Specify the policy using pre-shared key
!--- for authentication, Diffie-Hellman group 2, lifetime
!--- and peer address.

crypto isakmp policy 1
  authentication pre-share
  group 2
  lifetime 3600
  crypto isakmp key cisco address 20.1.1.2
!

!--- Create an IPSec transform set named "testtrans"
!--- with the DES for ESP with transport mode.
!--- Note: AH is not used.

crypto ipsec transform-set testtrans esp-des
!

!--- Create crypto map l2tpmap (assigned to Serial 0), using IKE for
!--- Security Associations with map-number 10
!--- and using "testtrans" transform-set as a template.
!--- Set the peer and specify access list 101, which is used
!--- to determine which traffic (L2TP) is to be protected by IPSec.

crypto map l2tpmap 10 ipsec-isakmp
  set peer 20.1.1.2
  set transform-set testtrans
  match address 101
!
interface Ethernet0
  ip address 10.31.1.6 255.255.255.0
  no ip directed-broadcast
!
interface Serial0
  ip address 20.1.1.1 255.255.255.252
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  no fair-queue

!--- Assign crypto map l2tpmap to the interface.

crypto map l2tpmap

```

```

!
interface Async1
ip unnumbered Ethernet0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
async mode dedicated
peer default ip address pool my_pool
ppp authentication chap
!

!--- Create an IP Pool named "my_pool" and
!--- specify the IP range.

ip local pool my_pool 10.31.1.100 10.31.1.110
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0

!--- Specify L2TP traffic as interesting to use with IPsec.

access-list 101 permit udp host 20.1.1.1 eq 1701 host 20.1.1.2 eq 1701
!

line con 0
exec-timeout 0 0
transport input none
line 1
autoselect during-login
autoselect ppp
modem InOut
transport input all
speed 38400
flowcontrol hardware
line aux 0
line vty 0 4
password

```

LNS Configuration

```

Current configuration:
!
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname LNS
!
enable password 7 0822455D0A16

!--- Usernames and passwords are used for
!--- L2TP tunnel authentication.

username LAC password 7 0107130A550E0A1F205F5D
username LNS password 7 120D10191C0E00142B3837

!--- Username and password used to authenticate
!--- the dial up user.

username dialupuser@cisco.com password 7 104A0018090713181F
!

ip subnet-zero

```

```

!
!---- Enable VDPN.

vpdn enable
!

!---- Configure VPDN group 1 to accept
!---- an open tunnel request from LAC,
!---- define L2TP as the protocol, and identify virtual-template 1
!---- to use for cloning virtual access interfaces.

vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname LAC
  local name LNS

!

!---- Create IKE policy 1, which is
!---- given the highest priority if there are additional IKE policies.
!---- Specify the policy using the pre-shared key for authentication,
!---- Diffie-Hellman group 2, lifetime and peer address.

crypto isakmp policy 1
  authentication pre-share
  group 2
  lifetime 3600
  crypto isakmp key cisco address 20.1.1.1
!
!

!---- Create an IPSec transform set named "testtrans"
!---- using DES for ESP with transport mode.
!---- Note: AH is not used.

crypto ipsec transform-set testtrans esp-des
!

!---- Create crypto map l2tpmap
!---- (assigned to Serial 0), using IKE for
!---- Security Associations with map-number 10
!---- and using "testtrans" transform-set as a template.
!---- Set the peer and specify access list 101, which is used
!---- to determine which traffic (L2TP) is to be protected by IPSec.

crypto map l2tpmap 10 ipsec-isakmp
  set peer 20.1.1.1
  set transform-set testtrans
  match address 101
!
interface Ethernet0
  ip address 200.1.1.100 255.255.255.0
  no ip directed-broadcast
  no keepalive
!

!---- Create a virtual-template interface
!---- used for "cloning"
!---- virtual-access interfaces using address pool "mypool"
!---- with Challenge Authentication Protocol (CHAP) authentication.

interface Virtual-Templat1

```

```

ip unnumbered Ethernet0
no ip directed-broadcast
no ip route-cache
peer default ip address pool mypool
ppp authentication chap
!
interface Serial0
ip address 20.1.1.2 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no fair-queue
clockrate 1300000

!--- Assign crypto map l2tpmap to the interface.

crypto map l2tpmap
!

!--- Create an IP Pool named "mypool" and
!--- specify the IP range.

ip local pool mypool 200.1.1.1 200.1.1.10
ip classless
!

!--- Specify L2TP traffic as interesting to use with IPsec.

access-list 101 permit udp host 20.1.1.2 eq 1701 host 20.1.1.1 eq 1701
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
password
login
!
end

```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Use these **show** commands to verify the configuration.

- **show crypto isakmp sa** Displays all current IKE security associations (SAs) at a peer.

```

LAC#show crypto isakmp sa
dst          src          state          conn-id  slot
20.1.1.2    20.1.1.1    QM_IDLE        1        0

LAC#

```

- **show crypto ipsec sa** Displays the settings used by current SAs.

```

LAC#show crypto ipsec sa

interface: Serial0

```

Crypto map tag: l2tpmap, local addr. 20.1.1.1

local ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/0/0)

current_peer: 20.1.1.2

PERMIT, flags={transport_parent,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 20.1.1.1, remote crypto endpt.: 20.1.1.2

path mtu 1500, ip mtu 1500, ip mtu interface Serial0

current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/17/1701)

remote ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/17/1701)

current_peer: 20.1.1.2

PERMIT, flags={origin_is_acl, reassembly_needed, parent_is_transport,}

#pkts encaps: 1803, #pkts encrypt: 1803, #pkts digest 0

#pkts decaps: 1762, #pkts decrypt: 1762, #pkts verify 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#send errors 5, #recv errors 0

local crypto endpt.: 20.1.1.1, remote crypto endpt.: 20.1.1.2

path mtu 1500, ip mtu 1500, ip mtu interface Serial0

current outbound spi: 43BE425B

inbound esp sas:

spi: 0xCB5483AD(3411313581)

transform: esp-des ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap

sa timing: remaining key lifetime (k/sec): (4607760/1557)

IV size: 8 bytes

replay detection support: N

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x43BE425B(1136542299)

transform: esp-des ,

in use settings ={Tunnel, }

slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap

sa timing: remaining key lifetime (k/sec): (4607751/1557)

IV size: 8 bytes

replay detection support: N

outbound ah sas:

outbound pcp sas:

LAC#

- **show vpdn** Displays the information about the active L2TP tunnel.

LAC#**show vpdn**

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID	RemID	Remote Name	State	Remote Address	Port	Sessions
26489	64014	LNS	est	20.1.1.2	1701	1

LocID	RemID	TunID	Intf	Username	State	Last Chg	Fastswitch
41	9	26489	As1	dialupuser@cisco.com	est	00:12:21	enabled

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels

LAC#

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug crypto engine** Displays engine events.
- **debug crypto ipsec** Displays IPSec events.
- **debug crypto isakmp** Displays messages about IKE events.
- **debug ppp authentication** Displays authentication protocol messages, including CHAP packet exchanges and Password Authentication Protocol (PAP) exchanges.
- **debug vpdn event** Displays messages about events that are part of normal tunnel establishment or shutdown.
- **debug vpdn error** Displays errors that prevent a tunnel from being established or errors that cause an established tunnel to be closed.
- **debug ppp negotiation** Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.

Related Information

- [Configuring and Troubleshooting Cisco Network Layer Encryption](#)
- [IPSec RFC 1825](#)
- [IPSec Support Pages](#)
- [Configuring IPSec Network Security](#)
- [Configuring Internet Key Exchange Security Protocol](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 14122
