在 IPSec 上配置第二层隧道协议 (L2TP)

目录

简介

第 2 层隧道协议（如 L2TP）不会为以隧道传输的流量提供加密机制。相反，这些协议会依靠其他安全协议（如 IPSec）来加密其数据。使用此配置示例，可借助 IPSec 为拨入的用户加密 L2TP 流量。

L2TP 隧道建立在 L2TP 接入集中器 (LAC) 和 L2TP 网络服务器 (LNS) 之间。IPSec 隧道也建立在这些设备之间，并使用 IPSec 对所有 L2TP 隧道流量进行加密。

先决条件

要求

本文档需要对 IPSec 协议拥有基本的了解。有关 IPSec 的详细信息，请参见 IP 安全 (IPSec) 加密简介。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IOS® 软件版本 12.2(24a)
- Cisco 2500 系列路由器

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

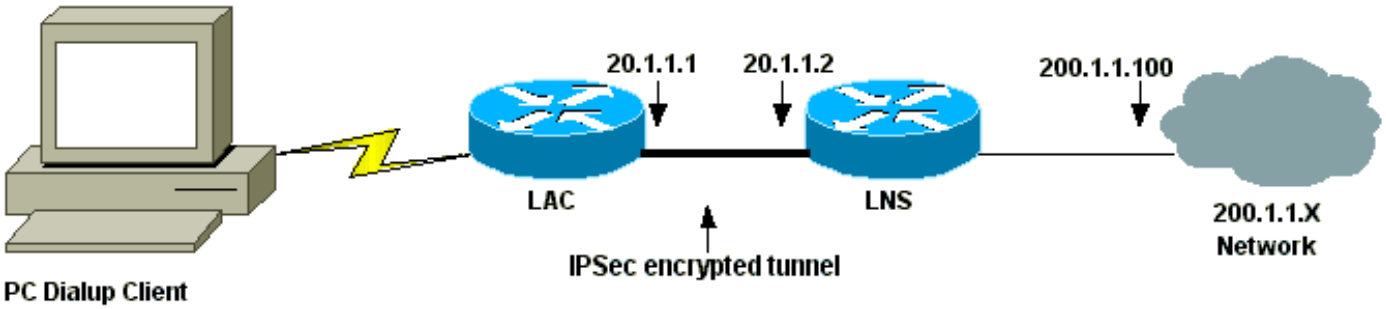
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中所用命令的其他信息，请使用命令查找工具(仅限注册用户)(仅限注册客户)。

网络图

本文档使用此图所示的网络设置。拨号用户通过模拟电话系统启动与 LAC 的 PPP 会话。在对用户进行身份验证之后，LAC 会启动连接 LNS 的 L2TP 隧道。在创建隧道之前，隧道端点、LAC 和 LNS 之间会互相进行身份验证。一旦建立隧道，就为拨号用户创建 L2TP 会话。为了加密 LAC 和 LNS 之间的所有 L2TP 流量，L2TP 流量被定义为 IPSec 的关注流量（将被加密的流量）。



配置

本文档使用以下配置。

- LAC 配置
- LNS 配置

LAC 配置

```
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
!
!--- 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 "testrans" 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 配置

```
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 "testrans" 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-
Template1 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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

使用这些 show 命令可验证配置。

- show crypto isakmp sa - 显示对等体上的所有当前 IKE 安全关联 (SA)。

```
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 - 显示当前 SA 使用的设置。

```
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 — 显示有关活动L2TP隧道的信息。

```
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#
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

注：在发出debug命令之前，请参阅有关Debug命令的重要信息。

- **debug crypto engine — 显示引擎事件。**
- **debug crypto ipsec — 显示 IPSec 事件。**
- **debug crypto isakmp — 显示关于 IKE 事件的消息。**
- **debug ppp authentication — 显示身份验证协议消息，包括 CHAP 数据包交换和口令身份验证协议 (PAP) 交换。**
- **debug vpdn event — 显示属于正常隧道建立或关闭一部分的事件的相关消息。**
- **debug vpdn error — 显示导致隧道无法建立的错误或导致已建立的隧道关闭的错误。**
- **debug ppp negotiation — 显示在 PPP 启动期间传输的 PPP 数据包，在此启动期间将协商 PPP 选项。**

相关信息

- IPSec RFC 1825
- IPSec 支持页
- 配置 IPSec 网络安全
- 配置 Internet 密钥交换安全协议
- 技术支持 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。