Настройка L2TP (туннельного протокола уровня 2) поверх IPSec

Содержание

Введение

Протоколы туннелирования 2-го уровня, в том числе L2TP, не предусматривают механизмы шифрования для трафика, проходящего через туннель. Шифрование данных они делегируют другим протоколам безопасности, таким как IPSec. В рассматриваемом примере конфигурации шифрование трафика L2TP для входящих подключений пользователей по коммутируемым каналам выполняется посредством IPSec.

Туннель L2TP устанавливается между концентратором доступа L2TP (LAC) и сетевым сервером L2TP (LNS). Между этими устройствами также устанавливается туннель IPSec, и весь трафик туннеля L2TP шифруется по протоколу IPSec.

Предварительные условия

Требования

Данный документ требует базовых знаний протокола IPSec. Дополнительные сведения о протоколе IPSec можно найти в документе Обзор протокола шифрования для защиты IP-пакетов (IPSec).

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования.

- ПО Cisco IOS®, выпуск 12.2(24a)
- Маршрутизаторы Cisco серии 2500

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме. Удаленный пользователь инициирует PPP-сеанс с LAC по аналоговой телефонной системе. После прохождения пользователем аутентификации LAC инициирует установление туннеля L2TP с LNS. Оконечные точки туннеля, LAC и LNS, перед созданием туннеля выполняют аутентификацию друг друга. После установления туннеля для пользователя удаленного доступа создается сеанс L2TP. Чтобы зашифровать весь трафик L2TP между LAC и LNS, трафик L2TP определяется как представляющий интерес (трафик, который нужно зашифровать) для IPSec.

Конфигурации

Эти конфигурации используются в данном документе.

- Конфигурация LAC
- Конфигурация LNS

Конфигурация LAC

```
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
```

Конфигурация LNS

```
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
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Для проверки конфигурации используйте следующие команды show.

- show crypto isakmp sa – отображает все текущие сопоставления безопасности IKE (SA) на одноранговом узле.

```
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 — отображает настройки, используемые текущими SA.

```
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– показывает сведения об активном туннеле L2TP.

```
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#
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- **debug crypto engine– показывает события ядра.**
- **debug crypto ipsec– показывает события IPSec.**
- **debug crypto isakmp – отображает сообщения о событиях IKE.**
- **debug ppp authentication– показывает сообщения протокола аутентификации, включая информацию об обмене пакетами CHAP и обмене по протоколу аутентификации по паролю (PAP).**
- **debug vpdn event– показывает сообщения о событиях, являющихся частью обычного**

процесса установки или завершения работы туннеля.
- debug vpdn error– показывает ошибки, не позволяющие установить туннель или вызывающие закрытие установленного туннеля.
- "debug ppp negotiation" – отображаются PPP-пакеты, передаваемые при запуске PPP с согласованием параметров.

Дополнительные сведения

- RFC IPSec 1825
- Страницы поддержки IPSec
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Техническая поддержка - Cisco Systems