Layer 2 Tunneling Protocol (L2TP) configureren via IPSec

Inhoud

Inleiding

Layer 2-tunnelprotocollen, zoals L2TP, bieden geen encryptiemechanismen voor het verkeer dat met deze tunnels wordt afgesproken. In plaats daarvan maken ze gebruik van andere beveiligingsprotocollen, zoals IPSec, om hun gegevens te versleutelen. Gebruik deze voorbeeldconfiguratie om L2TP-verkeer te versleutelen met IPSec voor gebruikers die inbellen.

L2TP-tunnel is ingesteld tussen de L2TP Access Concentrator (LAC) en de L2TP Network Server (LNS). Er is ook een IPSec-tunnel tot stand gebracht tussen deze apparaten en al het L2TP-tunnelverkeer is versleuteld met IPSec.

Voorwaarden

Vereisten

Dit document vereist een basisbegrip van het IPSec-protocol. Als u meer wilt weten over IPSec, raadpleegt u Een inleiding tot IP security (IPSec) encryptie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies.

- Cisco IOS®-softwarerelease 12.2(24a)XR
- Cisco 2500 Series routers

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een live netwerk werkt, zorg er dan voor dat u de potentiële impact van iedere opdracht begrijpt voor u deze gebruikt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

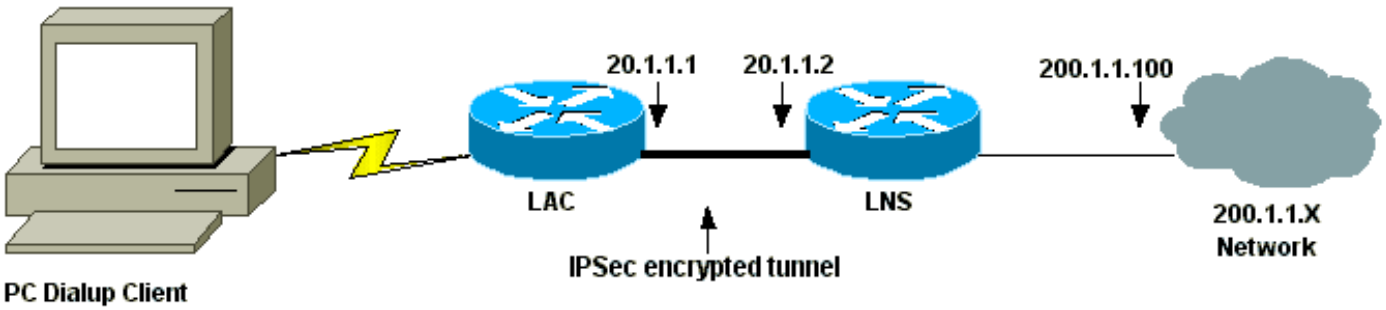
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik Command Lookup Tool (alleen voor geregistreerde klanten) voor meer informatie over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Dit document gebruikt de netwerkinstallatie die in dit diagram wordt getoond. De inbelgebruiker start een PPP-sessie met de LAC via het analoge telefoonsysteem. Nadat de gebruiker is geverifieerd, start de LAC een L2TP-tunnel naar de LNS. De tunneleindpunten, LAC en LNS, verifiëren elkaar voordat de tunnel wordt gemaakt. Zodra de tunnel tot stand is gebracht, wordt er een L2TP-sessie voor de dialup-gebruiker gemaakt. Om al het L2TP-verkeer tussen de LAN's en LAN's te versleutelen, wordt het L2TP-verkeer gedefinieerd als het interessante verkeer (verkeer dat moet worden versleuteld) voor IPSec.



Configuraties

Dit document gebruikt de volgende configuraties.

- LAC-configuratie
- LAN-configuratie

LAC-configuratie

```
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
```

LAN-configuratie

```
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
```

Verifiëren

Deze sectie bevat informatie die u kunt gebruiken om te controleren of uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Gebruik deze **showbevelen** om de configuratie te verifiëren.

- crypto isakmp sa tonen — Toont alle huidige IKE security associaties (SA's) aan een 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#
```

- toon crypto ipsec sa —Hier worden de instellingen weergegeven die door de huidige SA's worden gebruikt.

```
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#
```

- toon vpdn —Hier wordt de informatie over de actieve L2TP-tunnel weergegeven.

```
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#
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Opmerking: Voordat u **debug-**opdrachten uitgeeft, raadpleegt u Belangrijke informatie over debug-opdrachten.

- **debug crypto engine**—Hier worden motorgebeurtenissen weergegeven.
- **debug crypto ipsec**—Hier worden IPSec-gebeurtenissen weergegeven.
- **debug crypto isakmp**—Hier worden berichten over IKE-gebeurtenissen weergegeven.
- **debug ppp-verificatie**—Hier worden verificatieprotocolberichten weergegeven, waaronder CHAP-pakketuitwisselingen en PAP-uitwisselingen (Password Authentication Protocol).
- **debug vpdn gebeurtenis**-Hier worden berichten weergegeven over gebeurtenissen die deel uitmaken van de normale tunnelinstelling of afsluiten.
- **debug vpdn fout**-Hier worden fouten weergegeven die verhinderen dat een tunnel wordt gemaakt of fouten die ervoor zorgen dat een bestaande tunnel wordt gesloten.
- **debug ppp-onderhandeling**—Hier worden PPP-pakketten weergegeven die tijdens het opstarten van PPP worden verzonden, waar PPP-opties worden onderhandeld.

Gerelateerde informatie

- IPsec RFC 1825
- Ondersteuning van IPSec-pagina's
- IPsec-netwerkbeveiliging configureren

- Internet Key Exchange Security Protocol configureren
- Technische ondersteuning – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.