IPSec을 통한 L2TP(Layer 2 Tunneling Protocol) 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[구성](#)
[네트워크 다이어그램](#)
[설정](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[트러블슈팅 명령](#)
[관련 정보](#)

소개

L2TP와 같은 레이어 2 터널링 프로토콜은 터널링하는 트래픽에 대해 암호화 메커니즘을 제공하지 않습니다. 대신 IPSec과 같은 다른 보안 프로토콜을 사용하여 데이터를 암호화합니다. 이 샘플 컨피그레이션을 사용하여 전화를 건 사용자에 대해 IPSec을 사용하여 L2TP 트래픽을 암호화합니다.

L2TP 터널은 L2TP LAC(Access Concentrator)와 L2TP LNS(Network Server) 간에 설정됩니다. 이러한 디바이스 간에는 IPSec 터널도 설정되며 모든 L2TP 터널 트래픽은 IPSec을 사용하여 암호화됩니다.

사전 요구 사항

요구 사항

이 문서에서는 IPSec 프로토콜에 대한 기본적인 이해가 필요합니다. IPSec에 대한 자세한 내용은 IPSec(IP 보안) 암호화 소개를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 이러한 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.2(24a)
- Cisco 2500 Series 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업 중인 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

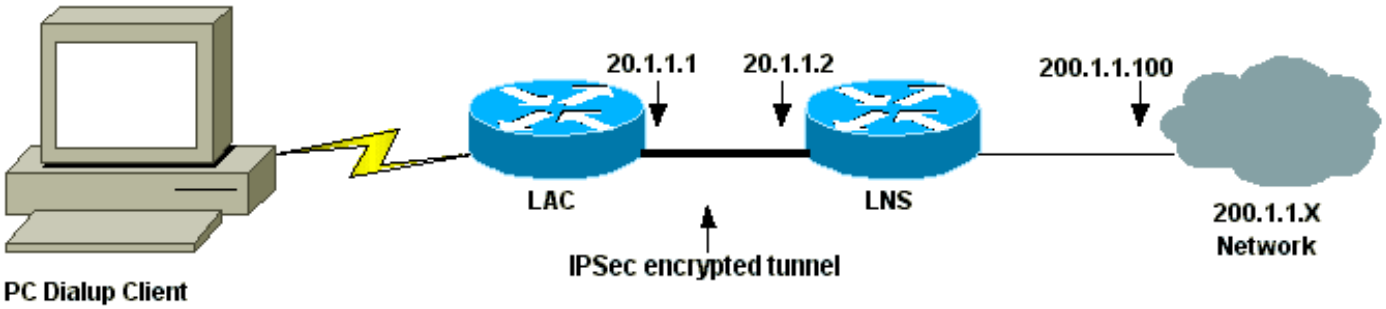
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 나와 있는 네트워크 설정을 사용합니다. 전화 접속 사용자는 아날로그 전화 시스템을 통해 LAC와의 PPP 세션을 시작합니다. 사용자가 인증되면 LAC는 LNS에 대한 L2TP 터널을 시작합니다. 터널 엔드포인트, LAC 및 LNS는 터널을 생성하기 전에 서로 인증합니다. 터널이 설정되면 전화 접속 사용자에 대해 L2TP 세션이 생성됩니다. LAC와 LNS 간의 모든 L2TP 트래픽을 암호화하기 위해 L2TP 트래픽은 IPSec에 대한 관심 트래픽(암호화 대상 트래픽)으로 정의됩니다.



설정

이 문서에서는 이러한 구성을 사용합니다.

- LAC 컨피그레이션
- LNS 컨피그레이션

LAC 컨피그레이션

```
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 컨피그레이션

```
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
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

이 show **명령**을 사용하여 컨피그레이션을 확인합니다.

- show crypto isakmp sa — 피어의 모든 현재 IKE SA(보안 연계)를 표시합니다.

```
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 - 현재 SA에서 사용되는 설정을 표시합니다.

```
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 - 활성 L2TP 터널에 대한 정보를 표시합니다.

```
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#
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

트러블슈팅 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

참고: debug 명령을 **실행하기** 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto engine** - 엔진 이벤트를 표시합니다.
- **debug crypto ipsec** - IPSec 이벤트를 표시합니다.
- **debug crypto isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.
- **debug ppp authentication**(디버그 **ppp 인증**) - CHAP 패킷 교환 및 PAP(Password Authentication Protocol) 교환을 비롯한 인증 프로토콜 메시지를 표시합니다.
- **debug vpdn event** - 정상적인 터널 설정 또는 종료의 일부인 이벤트에 대한 메시지를 표시합니다.
- **debug vpdn error**(디버그 vpdn 오류) - 터널이 설정되지 않도록 하는 오류 또는 설정된 터널이 닫히도록 하는 오류를 표시합니다.
- **debug ppp negotiation** - PPP 시작 중에 전송된 PPP 패킷을 표시합니다. 여기서 PPP 옵션이 협상됩니다.

관련 정보

- IPSec RFC 1825
- IPSec 지원 페이지
- IPSec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- Technical Support - Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.