Configurazione del protocollo L2TP (Layer 2 Tunneling Protocol) su IPSec

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Configurazione
Esempio di rete
Configurazioni
Verifica
Risoluzione dei problemi
Comandi per la risoluzione dei problemi
Informazioni correlate

Introduzione

I protocolli di tunneling di livello 2, ad esempio L2TP, non forniscono meccanismi di crittografia per il traffico che gestisce. Per crittografare i dati si basano invece su altri protocolli di protezione, ad esempio IPSec. Utilizzare questa configurazione di esempio per crittografare il traffico L2TP utilizzando IPSec per gli utenti che eseguono chiamate in ingresso.

Il tunnel L2TP viene stabilito tra il L2TP Access Concentrator (LAC) e il L2TP Network Server (LNS). Viene inoltre stabilito un tunnel IPSec tra questi dispositivi e tutto il traffico del tunnel L2TP viene crittografato utilizzando IPSec.

Prerequisiti

Requisiti

Questo documento richiede una conoscenza di base del protocollo IPSec. Per ulteriori informazioni su IPSec, vedere Introduzione alla crittografia IPSec (IP Security).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- Software Cisco IOS® versione 12.2(24a)

- Cisco serie 2500 Router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

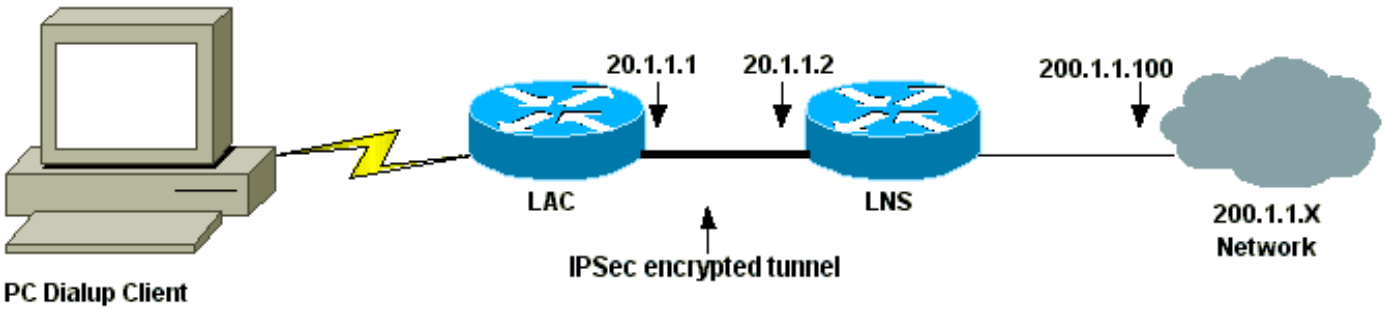
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma. L'utente remoto avvia una sessione PPP con il LAC tramite il sistema telefonico analogico. Dopo che l'utente è stato autenticato, il LAC avvia un tunnel L2TP verso l'LNS. Gli endpoint del tunnel, LAC e LNS, si autenticano a vicenda prima della creazione del tunnel. Una volta stabilito il tunnel, viene creata una sessione L2TP per l'utente della connessione remota. Per crittografare tutto il traffico L2TP tra LAC e LNS, il traffico L2TP viene definito come il traffico interessante (da crittografare) per IPSec.



Configurazioni

Nel documento vengono usate queste configurazioni.

- Configurazione LAC
- Configurazione LNS

Configurazione 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
```

Configurazione 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Utilizzare questi comandi **show** per verificare la configurazione.

- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza (SA) IKE correnti in un 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**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

```
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: visualizza le informazioni sul tunnel L2TP attivo.

```
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#
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

- **debug crypto engine**: visualizza gli eventi del motore.
- **debug crypto ipsec**: visualizza gli eventi IPSec.
- **debug crypto isakmp**: visualizza i messaggi sugli eventi IKE.
- **debug ppp authentication**: visualizza i messaggi del protocollo di autenticazione, inclusi gli scambi di pacchetti CHAP e gli scambi del protocollo PAP (Password Authentication Protocol).
- **debug vpdn event**: visualizza i messaggi relativi agli eventi che fanno parte della normale creazione del tunnel o del normale arresto.
- **debug vpdn error**: visualizza gli errori che impediscono di stabilire un tunnel o gli errori che causano la chiusura di un tunnel stabilito.
- **debug ppp negotiation**: visualizza i pacchetti PPP trasmessi durante l'avvio del protocollo PPP, in cui le opzioni PPP vengono negoziate.

Informazioni correlate

- IPSec RFC 1825
- Pagine di supporto IPSec

- Configurazione di IPSec Network Security
- Configurazione del protocollo di protezione di Internet Key Exchange
- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).