Konfigurieren des Layer 2 Tunneling Protocol (L2TP) über IPSec

Inhalt

Einleitung

Layer-2-Tunneling-Protokolle wie L2TP bieten keine Verschlüsselungsmechanismen für den Datenverkehr, den sie tunneln. Stattdessen vertrauen sie bei der Verschlüsselung ihrer Daten auf andere Sicherheitsprotokolle wie IPSec. Verwenden Sie diese Beispielkonfiguration, um L2TP-Datenverkehr mit IPSec für Benutzer zu verschlüsseln, die sich einwählen.

Zwischen dem L2TP-Zugriffskonzentrator (LAC) und dem L2TP-Netzwerkserver (LNS) wird ein L2TP-Tunnel eingerichtet. Zwischen diesen Geräten wird ein IPSec-Tunnel eingerichtet, und der gesamte L2TP-Tunnelverkehr wird mit IPSec verschlüsselt.

Voraussetzungen

Anforderungen

Dieses Dokument erfordert grundlegende Kenntnisse des IPSec-Protokolls. Weitere Informationen zu IPSec finden Sie unter Einführung in die IP-Sicherheit (IPSec)-Verschlüsselung.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen.

- Cisco IOS® Softwareversion 12.2(24a)

- Router der Cisco 2500 Serie

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn sich Ihr Netzwerk in der Produktionsumgebung befindet, müssen Sie sich bei jedem Befehl zunächst dessen potenzielle Auswirkungen vor Augen führen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

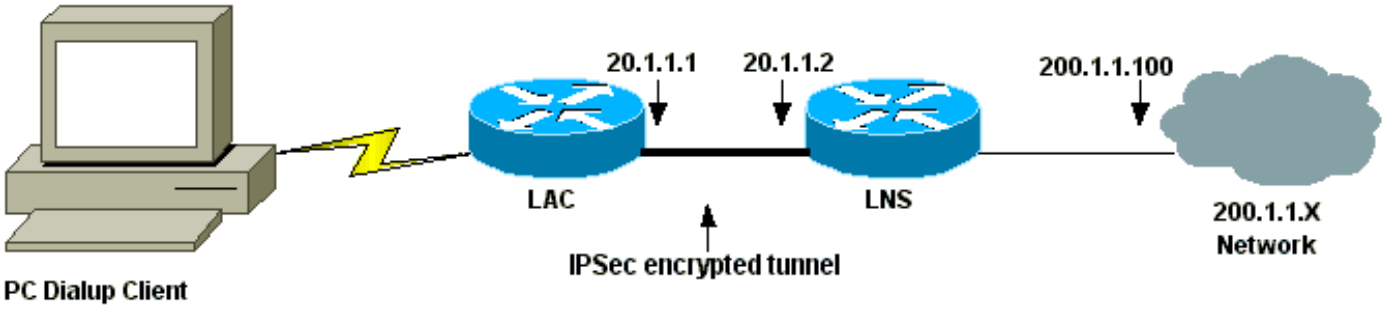
Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das Tool für die Suche nach Befehlen (nur für registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet. Der DFÜ-Benutzer initiiert eine PPP-Sitzung mit der LAC über das analoge Telefonsystem. Nachdem der Benutzer authentifiziert wurde, initiiert der LAC einen L2TP-Tunnel zum LNS. Die Tunnel-Endpunkte LAC und LNS authentifizieren sich gegenseitig, bevor der Tunnel erstellt wird. Sobald der Tunnel eingerichtet ist, wird eine L2TP-Sitzung für den DFÜ-Benutzer erstellt. Zur Verschlüsselung des gesamten L2TP-Verkehrs zwischen dem LAC und dem LNS wird der L2TP-Verkehr als der interessante Verkehr (zu verschlüsselnder Verkehr) für IPSec definiert.



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet.

- LAC-Konfiguration
- LNS-Konfiguration

LAC-Konfiguration
`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-Konfiguration

```
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
```

Überprüfung

Diese Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Einige Befehle des Typs **show werden vom Tool** Output Interpreter unterstützt (nur für registrierte Kunden), mit dem sich Analysen der Ausgabe von Befehlen des Typs **show abrufen lassen.**

Verwenden Sie die Befehle **show**, um die Konfiguration zu überprüfen.

- show crypto isakmp sa - Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) auf einem Peer an.

```
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 - Zeigt die von aktuellen SAs verwendeten Einstellungen an.

```
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 - Zeigt die Informationen zum aktiven L2TP-Tunnel an.

```
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#
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Befehle für die Fehlerbehebung

Einige Befehle des Typs **show werden vom Tool** Output Interpreter unterstützt (nur für registrierte Kunden), mit dem sich Analysen der Ausgabe von Befehlen des Typs **show abrufen lassen.**

Hinweis: Bevor Sie **Debug-**Befehle ausgeben, lesen Sie bitte Wichtige Informationen zu Debug-Befehlen.

- **debug crypto engine**: Zeigt Modulereignisse an.
- **debug crypto ipsec:** Zeigt IPSec-Ereignisse an.
- **debug crypto isakmp:** Zeigt Meldungen zu IKE-Ereignissen an.
- **debug ppp authentication**: Zeigt Authentifizierungsprotokollnachrichten an, einschließlich CHAP-Paketaustausch und PAP-Austausch (Password Authentication Protocol).
- **debug vpdn event**: Zeigt Meldungen zu Ereignissen an, die Teil des normalen Tunnelaufbaus oder -abbaus sind.
- **debug vpdn error (**VPN-Fehler debuggen): Zeigt Fehler an, die verhindern, dass ein Tunnel erstellt wird, oder Fehler, die dazu führen, dass ein erstellter Tunnel geschlossen wird.
- **debug ppp negotiation** (Debug-PPP-Aushandlung): Zeigt PPP-Pakete an, die während des PPP-Starts übertragen werden, wobei PPP-Optionen ausgehandelt werden.

Zugehörige Informationen

- IPSec RFC 1825
- IPSec-Support-Seiten
- Konfigurieren der IPSec-Netzwerksicherheit

- Konfigurieren des Internet Key Exchange Security Protocol
- Technischer Support – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.