配置使用IPSec的第2層隧道協定(L2TP)

目錄

簡介

第2層通道通訊協定（例如L2TP）不為其所通道流量的加密機制。相反，它們依靠其他安全協定（如IPSec）來加密其資料。使用此示例配置為撥入使用者使用IPSec加密L2TP流量。

在L2TP訪問集中器(LAC)和L2TP網路伺服器(LNS)之間建立L2TP隧道。在這些裝置之間還建立了IPSec隧道，並且所有L2TP隧道流量都使用IPSec進行加密。

必要條件

需求

本文檔需要對IPSec協定有基本的瞭解。要瞭解有關IPSec的詳細資訊，請參閱IP安全(IPSec)加密簡介。

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- Cisco IOS®軟體版本12.2(24a)
- Cisco 2500系列路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

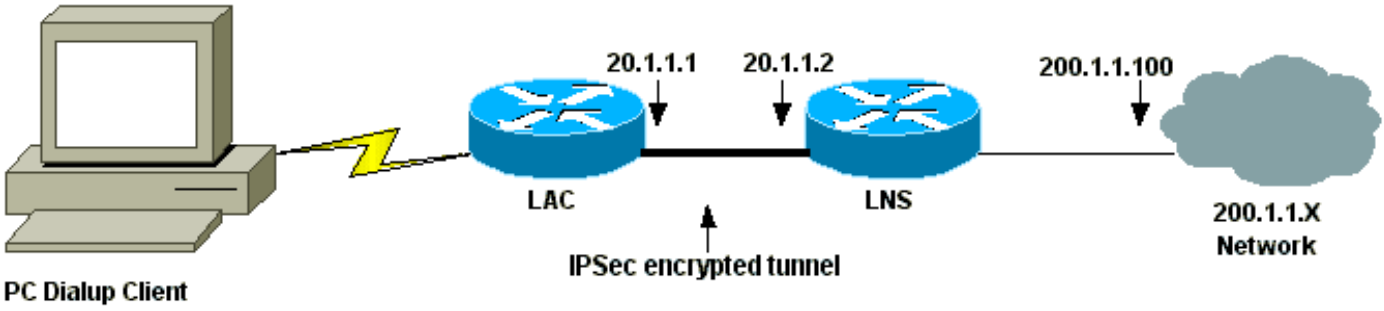
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用下圖中所示的網路設定。撥號使用者通過模擬電話系統發起與LAC的PPP會話。在使用者通過身份驗證後，LAC發起到LNS的L2TP隧道。通道端點LAC和LNS會在通道建立之前相互進行驗證。建立通道後，系統會為撥號使用者建立L2TP作業階段。為了加密LAC和LNS之間的所有L2TP流量，L2TP流量被定義為IPSec的相關流量（要加密的流量）。



組態

本檔案會使用這些設定。

- LAC配置
- LNS配置

LAC配置

```
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配置

```
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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

使用這些**show**命令驗證設定。

- show crypto isakmp sa — 顯示對等體上的所有當前IKE安全關聯(SA)。

```
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 — 顯示當前SA使用的設定。

```
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 — 顯示有關活動L2TP隧道的資訊。

```
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#
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出**debug指令之前，請先參閱**有關Debug指令的重要資訊。

- **debug crypto engine** — 顯示引擎事件。
- **debug crypto ipsec** — 顯示IPSec事件。
- **debug crypto isakmp** — 顯示有關IKE事件的消息。
- **debug ppp authentication** — 顯示身份驗證協定消息，包括CHAP資料包交換和密碼身份驗證協定(PAP)交換。
- **debug vpdn event** — 顯示有關屬於正常隧道建立或關閉的事件的消息。
- **debug vpdn error** — 顯示阻止建立隧道的錯誤或導致關閉已建立隧道的錯誤。
- **debug ppp negotiation** — 顯示在PPP啟動期間傳輸的PPP資料包，其中協商了PPP選項。

相關資訊

- IPSec RFC 1825
- IPSec支援頁面
- **配置IPSec網路安全**
- **配置Internet金鑰交換安全協定**
- 技術支援 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。