تكوين بروتوكول الاتصال النفقي للطبقة 2 (L2TP) عبر IPSec

المحتويات

المقدمة

لا توفر بروتوكولات الاتصال النفقي من الطبقة 2، مثل L2TP، آليات تشفير لحركة مرور البيانات بأنفاق تقنية المعلومات. وبدلا من ذلك، فإنهم يعتمدون على بروتوكولات الأمان الأخرى، مثل IPSec، لتشفير بياناتهم. أستخدم نموذج التكوين هذا لتشفير حركة مرور L2TP باستخدام IPSec للمستخدمين الذين يطلبون الدخول.

يتم إنشاء نفق L2TP بين مركز الوصول إلى L2TP (LAC) وخادم شبكة L2TP (LNS). كما يتم إنشاء نفق IPSec بين هذه الأجهزة ويتم تشفير حركة مرور نفق L2TP بالكامل باستخدام IPSec.

المتطلبات الأساسية

المتطلبات

يتطلب هذا المستند فهما أساسيا لبروتوكول IPSec. لمعرفة المزيد حول IPSec، يرجى الرجوع إلى مقدمة لتشفير أمان IP (IPSec).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية.

- برنامج IOS® الإصدار 12.2(24a) من Cisco
- الموجّهات من السلسلة 2500 من Cisco

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير

المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، راجع اصطلاحات تلميحات Cisco التقنية.

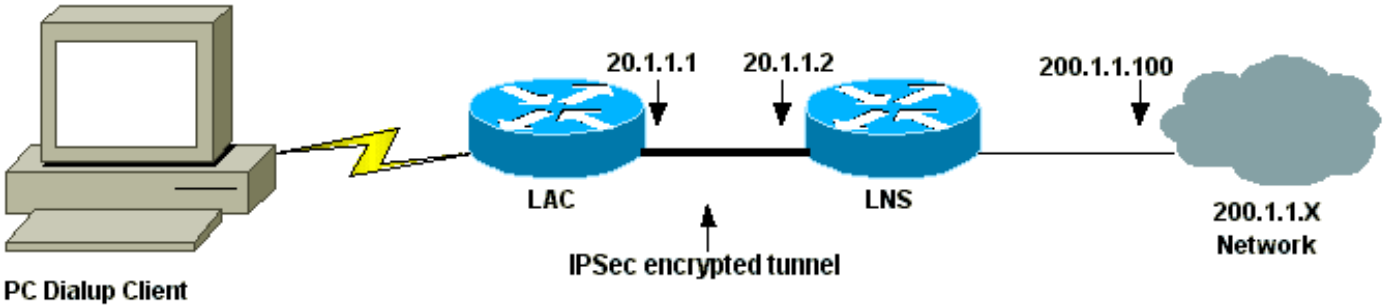
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي. يقوم مستخدم الطلب الهاتفي ببدء جلسة PPP مع LAC عبر نظام الهاتف التناظري. بعد مصادقة المستخدم، تبدأ LAC نفق L2TP إلى LNS. نقاط نهاية النفق، LAC و LNS، مصادقة بعضها البعض قبل إنشاء النفق. وبمجرد إنشاء النفق، يتم إنشاء جلسة عمل ل L2TP لمستخدم الاتصال. لتشفير كل حركة مرور L2TP بين LAC و LNS، يتم تعريف حركة مرور L2TP على أنها حركة المرور المفيدة (حركة المرور التي سيتم تشفيرها) ل IPSec.



التكوينات

يستخدم هذا المستند هذه التكوينات.

- تكوين LAC
- تكوين LNS

تكوين 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
```

تكوين 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
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

استعملت هذا **عرض** أمر أن يدقق التشكيل.

- show crypto isakmp sa — يعرض جميع اقترانات أمان (IKE (SAs الحالية في نظير.

```
LAC#show crypto isakmp sa
dst             src             state          conn-id     slot
QM_IDLE         1        0        20.1.1.1         20.1.1.2

#LAC
```

- show crypto ipSec — يعرض الإعدادات المستخدمة من قبل موجهات الخدمات (SAs) الحالية.

```
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 — يعرض المعلومات حول نفق L2TP النشط.

```
LAC#show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name   State  Remote Address  Port  Sessions
```

```
LNS            est     20.1.1.2        1701  1 64014 26489

LocID RemID TunID Intf           Username                State  Last Chg Fastswitch
As1           dialupuser@cisco.com   est     00:12:21 enabled 26489     9    41

No active L2F tunnels%

No active PPTP tunnels%

No active PPPoE tunnels%
#LAC
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug crypto engine**—يعرض أحداث المحرك.
- **debug crypto ipSec**—يعرض أحداث IPSec.
- **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.
- **debug ppp authentication**—يعرض رسائل بروتوكول المصادقة، بما في ذلك عمليات تبادل حزم CHAP وعمليات تبادل بروتوكول مصادقة كلمة المرور (PAP).
- **debug vpdn event** —يعرض رسائل حول الأحداث التي تعد جزءا من إنشاء النفق العادي أو إيقاف تشغيله.
- **debug vpdn خطأ**—يعرض الأخطاء التي تمنع إنشاء نفق أو الأخطاء التي تتسبب في إغلاق نفق تم إنشاؤه.
- **debug ppp negotiation**—يعرض حزم PPP المرسلة أثناء بدء تشغيل PPP، حيث يتم التفاوض حول خيارات PPP.

معلومات ذات صلة

- IPSec RFC 1825
- صفحات دعم IPSec
- تكوين أمان شبكة IPSec
- تكوين بروتوكول أمان Internet Key Exchange
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).