Configurando o Protocolo de Túnel da Camada 2 (L2TP) sobre IPSec

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Verificar](#)
[Troubleshoot](#)
[Comandos para Troubleshooting](#)
[Informações Relacionadas](#)

Introduction

Os protocolos de tunelamento de Camada 2, como o L2TP, não fornecem mecanismos de criptografia para o tráfego que enviam por túnel. Em vez disso, eles confiam em outros protocolos de segurança, como o IPSec, para criptografar seus dados. Use esta configuração de exemplo para criptografar o tráfego de L2TP utilizando o IPSec para usuários que discaram.

O túnel L2TP é estabelecido entre o Concentrador de Acesso L2TP (LAC) e o Servidor de Rede L2TP (LNS). Um túnel IPSec também é estabelecido entre esses dispositivos e todo o tráfego do túnel L2TP é criptografado usando IPSec.

Prerequisites

Requirements

Este documento requer uma compreensão básica do protocolo de IPSec. Para saber mais sobre o IPSec, consulte Uma introdução à criptografia de segurança de IP (IPSec).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- Software Cisco IOS® versão 12.2(24a)
- Cisco 2500 Series Routers

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

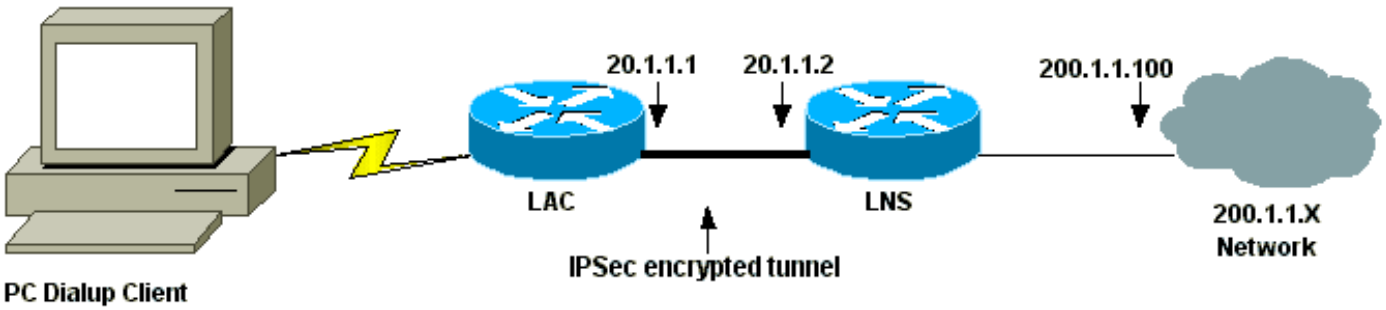
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama. O usuário de discagem inicia uma sessão PPP com o LAC no sistema de telefone analógico. Depois que o usuário é autenticado, o LAC inicia um túnel L2TP para o LNS. Os pontos finais do túnel, LAC e LNS, autenticam-se um ao outro antes que o túnel seja criado. Depois que o túnel é estabelecido, uma sessão L2TP for criada para o usuário de discagem. Para criptografar todo o trafego L2TP entre o LAC e o LNS, o tráfego L2TP é definido como o tráfego interessante (tráfego a ser criptografado) para IPSec.



Configurações

Este documento utiliza estas configurações.

- Configuração do LAC
- Configuração de LNS

Configuração do 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
```

Configuração de 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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Use estes comandos **show** para verificar a configuração.

- **show crypto isakmp sa — Exibe todas as associações de segurança atuais (SAs) de IKE em um 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 — Exibe as configurações usadas pelas SAs atuais.

```
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 — Exibe as informações sobre o túnel L2TP ativo.

```
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#
```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Observação: antes de emitir comandos **debug**, consulte **Informações importantes sobre comandos debug**.

- **debug crypto engine** — Exibe eventos do mecanismo.
- **debug crypto ipsec** — Exibe eventos de IPSec.
- **debug crypto isakmp — Exibe mensagens sobre eventos de IKE.**
- **debug ppp authentication** — Exibe mensagens de protocolo de autenticação, incluindo trocas de pacotes CHAP e trocas de Password Authentication Protocol (PAP).
- **debug vpdn event — Exibe mensagens sobre eventos que são parte do estabelecimento ou fechamento do túnel normal.**
- **debug vpdn error — Exibe erros que impedem que um túnel seja estabelecido ou erros que fazem com que o túnel estabelecido seja fechado.**
- **debug ppp negotiation** — Exibe pacotes PPP transmitidos durante a inicialização de PPP, em que as opções de PPP são negociadas.

Informações Relacionadas

- IPSec RFC 1825
- Páginas de Suporte do IPSec
- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet

- Suporte Técnico - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.