

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

## 概要

L2TP などのレイヤ 2 トンネリング プロトコルは、トンネリングするトラフィックに暗号化メカニズムを提供しません。代わりに、データを暗号化するために IPSec などの他のセキュリティ プロトコルに依存します。ダイヤルインするユーザに対しては、この文書の設定例を使用して、IPSec を使用し L2TP トラフィックを暗号化します。

L2TP トンネルは、L2TP アクセス コンセントレータ ( LAC ) と L2TP ネットワーク サーバ ( LNS ) との間で確立されます。IPSec トンネルもこれらのデバイス間で確立され、すべての L2TP トンネルのトラフィックは IPSec を使用して暗号化されます。

## 前提条件

### 要件

このドキュメントの内容は、IPsec プロトコルに関する基本的知識が前提となっています。IPSec の詳細については、『[IP Security \( IPSec \) 暗号化の概要](#)』を参照してください。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェア リリース 12.2(24a)
- Cisco 2500 シリーズ ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

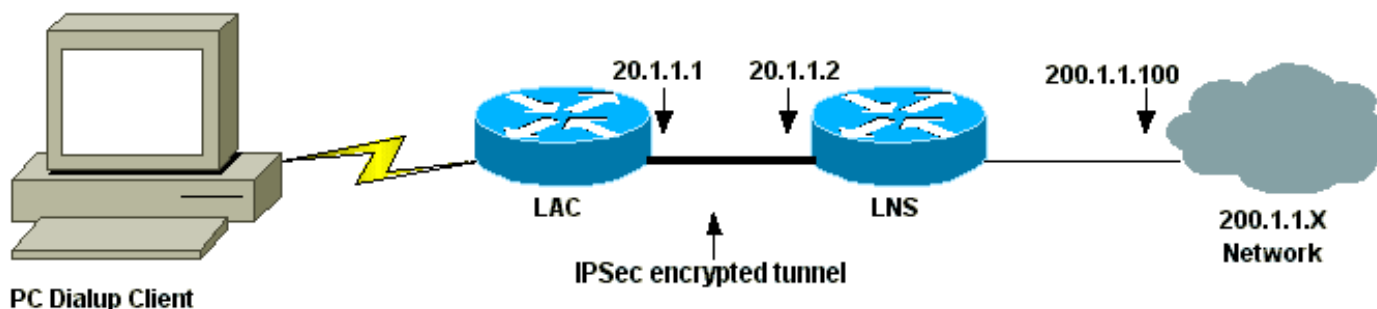
## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。ダイヤルアップユーザは、アナログ電話システムで LAC との PPP セッションを開始します。ユーザが認証された後、LAC は LNS への L2TP トンネルを開始します。トンネルエンドポイントである LAC と LNS は、トンネルが作成される前に相互に認証を行います。トンネルが確立されると、ダイヤルアップユーザに対して L2TP セッションが作成されます。LAC と LNS の間のすべての L2TP トラフィックを暗号化するため、L2TP トラフィックは、IPSec に関する対象トラフィック ( 暗号化されるトラフィック ) として定義されます。



## 設定

このドキュメントでは、次の設定を使用します。

- [LAC 設定](#)
- [LNS の設定](#)

### LAC の設定

```
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 dialup user 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-sharegroup 2lifetime
3600crypto 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 "testtrans" 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 20.1.1.2set transform-set testtrans
match address 101!interface Ethernet0ip address
10.31.1.6 255.255.255.0no ip directed-
broadcast!interface Serial0ip address 20.1.1.1
255.255.255.252no ip directed-broadcastno ip route-
cacheno ip mroute-cacheno fair-queue!-- Assign crypto
map l2tpmap to the interface. crypto map
l2tpmap!interface Async0ip unnumbered Ethernet0no ip
directed-broadcastencapsulation pppno ip route-cacheno
ip mroute-cacheasync mode dedicatedpeer default ip
address pool my_poolppp authentication chap!-- Create
an IP Pool named "my_pool" and !--- specify the IP
range. ip local pool my_pool 10.31.1.100 10.31.1.110ip
classlessip 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 0exec-timeout 0 0transport input
noneline 1autoselect during-loginautoselect pppmodem
InOuttransport input allspeed 38400flowcontrol
hardwareline aux 0line vty 0 4password

```

## LNS の設定

```

Current configuration:!version 12.2service timestamps
debug datetime msec localtime show-timezoneservice
timestamps log datetime msec localtime show-
timezoneservice password-encryption!hostname LNS!enable
password 7 0822455D0A16!-- Usernames and passwords are
used for !--- L2TP tunnel authentication.username LAC
password 7 0107130A550E0A1F205F5Dusername 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

```

```

lauthentication pre-sharegroup 2lifetime 3600crypto
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 "testtrans" 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 20.1.1.1set transform-set testtrans match
address 101!interface Ethernet0ip address 200.1.1.100
255.255.255.0no ip directed-broadcastno keepalive!!---
Create a virtual-template interface !--- used for
"cloning" !--- virtual-access interfaces using address
pool "mypool" !--- with Challenge Authentication
Protocol (CHAP) authentication.interface Virtual-
Templatelip unnumbered Ethernet0no ip directed-
broadcastno ip route-cachepeer default ip address pool
mypoolppp authentication chap!interface Serial0ip
address 20.1.1.2 255.255.255.252no ip directed-
broadcastno ip route-cacheip mroute-cacheip mroute-cache
no fair-queueclockrate 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 200.1.1.1 200.1.1.10ip 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 0exec-timeout 0 0transport
input noneline aux 0line vty 0 4password login!end

```

## 確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、[Output Interpreter Tool](#) ( [登録ユーザ専用](#) ) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

設定を確認するには、次の **show** コマンドを使用します。

- [show crypto isakmp sa](#) か。ピアですべての電流 IKE Security Association ( SA ) を表示する。

```

LAC#show crypto isakmp sadst          src          state          conn-id          slot20.1.1.2
20.1.1.1          QM_IDLE          1          0LAC#

```

- [show crypto ipsec sa](#) か。電流 SA によって使用される設定を表示する。

```

LAC#show crypto ipsec sainterface: 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](#) か。アクティブ L2TP トンネルについての情報を表示する。

```
LAC#show vpdnL2TP Tunnel and Session Information Total tunnels 1 sessions 1LocID RemID Remote
Name State Remote Address Port Sessions26489 64014 LNS est 20.1.1.2
1701 1LocID RemID TunID Intf Username State Last Chg Fastswitch41 9
26489 As1 dialupuser@cisco.com est 00:12:21 enabled%No active L2F tunnels%No
active PPTP tunnels%No active PPPoE tunnelsLAC#
```

## トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。


### トラブルシューティングのためのコマンド

特定の **show** コマンドは、[Output Interpreter Tool](#) ( [登録ユーザ専用](#) ) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注 コマンドを使用する前に、『[debug コマンドに関する重要な情報](#)』を参照してください。

- **debug crypto engine** か。エンジンイベントを表示する。
- **debug crypto ipsec** か。IPSecイベントを表示する。
- **debug crypto isakmp** か。IKE イベントについてのメッセージを表示する。
- **debug ppp authentication** か。CHAP パケット交換および Password Authentication Protocol ( PAP ) 交換を含む認証プロトコルメッセージを、表示する。
- **debug vpdn event** か。正常なトンネル確立の一部またはシャットダウンであるイベントについてのメッセージを表示する。
- **debug vpdn error** か。トンネルは確立されるまたはエラーを表示することを防ぐ確立されたトンネルを閉じますエラーを。
- **debug ppp negotiation** か。PPP オプションがネゴシエートされる PPP 始動の間に送信される PPP パケットを表示する。

## 関連情報

- [IPSec RFC 1825](#) 
- [IPSec に関するサポートページ \( 英語 \)](#)
- [IPsec ネットワーク セキュリティの設定](#)
- [インターネット キー交換セキュリティ プロトコルの設定](#)
- [テクニカルサポート - Cisco Systems](#)