

Configurando L2TP No IPSec Entre o PIX Firewall e o PC com Windows 2000 Usando Certificados

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o cliente L2TP da Microsoft](#)

[Obter certificados para o PIX Firewall](#)

[Configuração de firewall PIX](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Exemplo de saída de depuração](#)

[Depuração válida para registrar-se com o CA](#)

[Depuração inadequada para registro com CA](#)

[Informações Relacionadas](#)

Introduction

O L2TP (Layer 2 Tunneling Protocol) sobre IPsec é suportado no Cisco Secure PIX Firewall Software Release 6.x ou posterior. Os usuários que executam o Windows 2000 podem usar o cliente IPsec nativo e o cliente L2TP para estabelecer um túnel L2TP para o PIX Firewall. O tráfego flui através do túnel L2TP criptografado por Associações de Segurança (SAs - Security Associations) IPsec.

Observação: você não pode usar o cliente IPsec L2TP do Windows 2000 para executar telnet para o PIX.

Observação: o tunelamento dividido não está disponível com L2TP no PIX.

Para configurar L2TP sobre IPsec de clientes remotos Microsoft Windows 2000/2003 e XP para um escritório corporativo PIX/ASA Security Appliance usando chaves pré-compartilhadas com um Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS Server para autenticação de usuário, consulte [L2TP sobre IPsec entre Windows 2000/IP XP PC e PIX/ASA 7.2 usando o](#)

[exemplo de configuração de chave pré-compartilhada.](#)

Para configurar o L2TP sobre IP Security (IPsec) de clientes remotos do Microsoft Windows 2000 e XP para um site corporativo usando um método criptografado, consulte [Configurando o L2TP sobre IPSec de um cliente Windows 2000 ou XP para um Cisco VPN 3000 Series Concentrator usando chaves pré-compartilhadas.](#)

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento se aplicam a estas versões de software e hardware:

- Software PIX Versão 6.3(3)
- Windows 2000 com ou sem SP2 (consulte a dica da Microsoft [Q276360](#) para obter informações sobre SP1.)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

Informações de Apoio

O suporte ao certificado no Cisco Secure PIX versões 6.x ou posterior inclui servidores Baltimore, Microsoft, VeriSign e Entrust. Atualmente, o PIX não aceita solicitações L2TP sem proteção IPsec.

Este exemplo mostra como configurar o PIX Firewall para o cenário mencionado anteriormente neste documento. A autenticação do Internet Key Exchange (IKE) usa o comando **rsa-sig** (certificados). Neste exemplo, a autenticação é feita por um servidor RADIUS.

As opções menos envolvidas para conexões de cliente criptografadas com o PIX estão listadas em [Cisco Hardware and VPN Clients com suporte a IPsec/PPTP/L2TP.](#)

Configurar

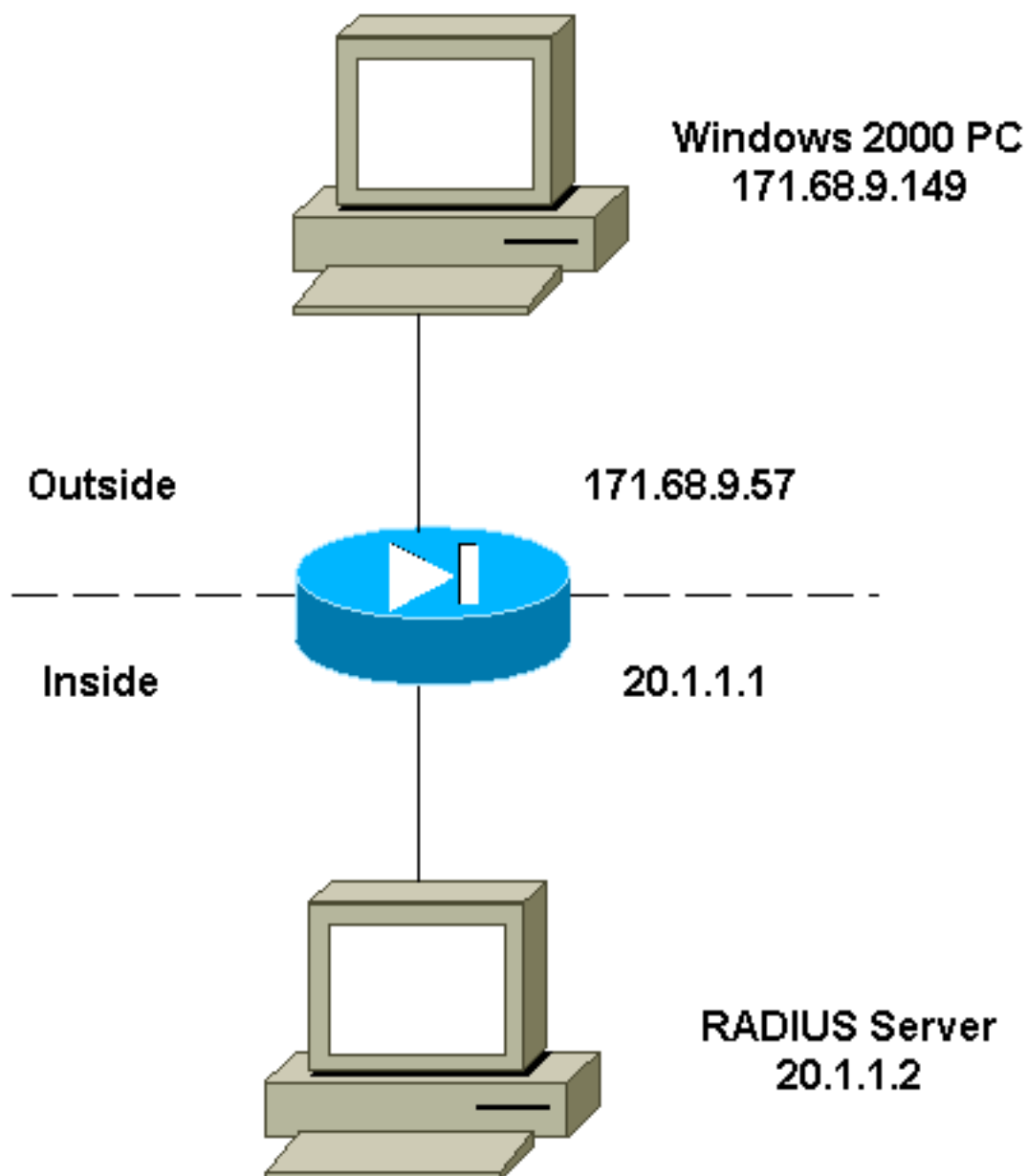
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações

sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurar o cliente L2TP da Microsoft

Informações sobre como configurar o cliente L2TP da Microsoft estão disponíveis no [Guia Passo a Passo da Microsoft para Segurança de Protocolo Internet](#).

Conforme observado no guia passo a passo da Microsoft mencionado, o cliente suporta vários servidores de autoridade de certificação (CA) testados. Informações sobre como configurar a AC da Microsoft estão disponíveis no [Guia passo a passo da Microsoft para configurar uma autoridade de certificado](#).

Obter certificados para o PIX Firewall

Consulte [Exemplos de Configuração de CA](#) para obter detalhes sobre como configurar o PIX para

interoperabilidade com certificados da VeriSign, Entrust, Baltimore e Microsoft.

Configuração de firewall PIX

Este documento utiliza esta configuração.

Firewall de PIX

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-506-2
domain-name sjvpn.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Access Control List (ACL) configured to bypass !---
Network Address Translation (NAT) for the L2TP IP pool.
access-list nonat permit ip 20.1.1.0 255.255.255.0
50.1.1.0 255.255.255.0
!--- ACL configured to permit L2TP traffic (UDP port
1701). access-list l2tp permit udp host 171.68.9.57 any
eq 1701
no pager
logging on
logging console debugging
logging buffered debugging
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 171.68.9.57 255.255.255.0
ip address inside 20.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Pool for L2TP address assignment. ip local pool
l2tp 50.1.1.1-50.1.1.5
pdm history enable
arp timeout 14400
!--- NAT configuration that matches previously defined
!--- ACL for the L2TP IP pool. nat (inside) 0 access-
list nonat
route outside 0.0.0.0 0.0.0.0 171.68.9.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
!--- AAA (RADIUS) server configuration. aaa-server
RADIUS (inside) host 20.1.1.2 cisco timeout 5
no snmp-server location
```

```

no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- sysopt command entry to permit L2TP !--- traffic,
while bypassing all ACLs.

sysopt connection permit-l2tp
no sysopt route dnat
!--- The IPsec configuration. crypto ipsec transform-set
l2tp esp-des esp-md5-hmac
!--- Only transport mode is supported. crypto ipsec
transform-set l2tp mode transport
crypto ipsec security-association lifetime seconds 3600
crypto dynamic-map dyna 20 match address l2tp
crypto dynamic-map dyna 20 set transform-set l2tp
crypto map mymap 10 ipsec-isakmp dynamic dyna
crypto map mymap client authentication RADIUS
crypto map mymap interface outside
!--- The IKE configuration. isakmp enable outside
isakmp policy 20 authentication rsa-sig
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
ca identity sjvpn 171.68.9.149:/certsrv/mscep/mscep.dll
ca configure sjvpn ra 1 20 crloptional
telnet 171.68.9.0 255.255.255.0 inside
telnet 20.1.1.2 255.255.255.255 inside
telnet timeout 60
ssh timeout 5
!--- The L2TP configuration parameters. vpdn group
l2tpipsec accept dialin l2tp
vpdn group l2tpipsec ppp authentication chap
vpdn group l2tpipsec ppp authentication mschap
vpdn group l2tpipsec client configuration address local
l2tp
vpdn group l2tpipsec client configuration dns 20.1.1.250
20.1.1.251
vpdn group l2tpipsec client configuration wins
20.1.1.250
vpdn group l2tpipsec client authentication aaa RADIUS
vpdn group l2tpipsec client accounting RADIUS
vpdn group l2tpipsec l2tp tunnel hello 60
vpdn enable outside
terminal width 80
Cryptochecksum:06a53009d1e9f04740256d9f0fb82837
: end
[OK]

```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\)](#) oferece suporte a determinados comandos `show`. Use a OIT para exibir uma análise da saída do comando `show`.

- **show crypto ca cert** — Exibe informações sobre seu certificado, o certificado da CA e quaisquer certificados da Autoridade de Registro (RA).
Certificate

Status: Available
Certificate Serial Number: 0371630800000000022
Key Usage: General Purpose
Subject Name
Name: PIX-506-2.sjvpn.com
Validity Date:
start date: 16:29:10 Apr 27 2001
end date: 16:39:10 Apr 27 2002

RA Signature Certificate
Status: Available
Certificate Serial Number: 0347dc82000000000002
Key Usage: Signature
CN = scott
OU = tac
O = cisco
L = san jose
ST = ca
C = US
EA =<16> zaahmed@cisco.com
Validity Date:
start date: 18:47:45 Jul 27 2000

end date: 18:57:45 Jul 27 2001

CA Certificate
Status: Available
Certificate Serial Number: 1102485095cbf8b3415b2e96e86800d1
Key Usage: Signature
CN = zakca
OU = vpn
O = cisco
L = sj
ST = california
C = US
EA =<16> zaahmed@cisco.com
Validity Date:
start date: 03:15:09 Jul 27 2000

end date: 03:23:48 Jul 27 2002

RA KeyEncipher Certificate
Status: Available
Certificate Serial Number: 0347df0d0000000000003
Key Usage: Encryption
CN = scott
OU = tac
O = cisco
L = san jose
ST = ca
C = US
EA =<16> zaahmed@cisco.com
Validity Date:
start date: 18:47:46 Jul 27 2000

end date: 18:57:46 Jul 27 2001

- **show crypto isakmp sa** — Exibe todas as SAs IKE atuais em um peer.

```
dst src state pending created  
171.68.9.57 171.68.9.149 QM_IDLE 0 1
```

- **show crypto ipsec sa** — Exibe as configurações usadas pelas SAs atuais.

```
interface: outside
Crypto map tag: mymap, local addr. 171.68.9.57
local ident (addr/mask/prot/port): (171.68.9.57/255.255.255.255/17/1701)
remote ident (addr/mask/prot/port): (171.68.9.149/255.255.255.255/17/1701)
current_peer: 171.68.9.149
dynamic allocated peer ip: 0.0.0.0

PERMIT, flags={reassemble_needed,transport_parent,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 45, #pkts decrypt: 45, #pkts verify 45
#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.: 171.68.9.57, remote crypto endpt.: 171.68.9.149
path mtu 1500, ipsec overhead 36, media mtu 1500
current outbound spi: a8c54ec8
```

```
inbound esp sas:
spi: 0xfbc9db43(4224310083)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (99994/807)
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xa8c54ec8(2831503048)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (99999/807)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

- **show vpdn tunnel** — Exibe informações sobre os túneis L2TP ou L2F (L2F) ativos em uma rede de discagem privada virtual (VPDN).

```
L2TP Tunnel Information (Total tunnels=1 sessions=1)
```

```
Tunnel id 4 is up, remote id is 19, 1 active sessions
Tunnel state is established, time since change 96 secs
Remote Internet Address 171.68.9.149, port 1701
Local Internet Address 171.68.9.57, port 1701
15 packets sent, 38 received, 420 bytes sent, 3758 received
Control Ns 3, Nr 5
Local RWS 16, Remote RWS 8
Retransmission time 1, max 1 seconds
Unsent queuesize 0, max 0
Resend queuesize 0, max 1
Total resends 0, ZLB ACKs 3
```

```
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
```

```
% No active PPTP tunnels
```

```
PIX-506-2# sh uauth
Current Most Seen
Authenticated Users 1 2
Authen In Progress 0 2
vpdn user 'vpnclient' at 50.1.1.1, authenticated
```

- **show vpdn session** — Exibe informações sobre sessões L2TP ou L2F ativas em uma VPDN.
L2TP Session Information (Total tunnels=1 sessions=1)

```
Call id 4 is up on tunnel id 4
Remote tunnel name is zaahmed-pc
Internet Address is 171.68.9.149
Session username is vpnclient, state is established
Time since change 201 secs, interface outside
Remote call id is 1
PPP interface id is 1
15 packets sent, 56 received, 420 bytes sent, 5702 received
Sequencing is off
```

- **show vpdn pppinterface** — Exibe o status e as estatísticas da interface virtual PPP que foi criada para o túnel PPTP para o valor de identificação da interface a partir do comando **show vpdn session**.

```
PPP virtual interface id = 1
PPP authentication protocol is CHAP
Client ip address is 50.1.1.1
Transmitted Pkts: 15, Received Pkts: 56, Error Pkts: 0
MPPE key strength is None
MPPE_Encrypt_Pkts: 0, MPPE_Encrypt_Bytes: 0
MPPE_Decrypt_Pkts: 0, MPPE_Decrypt_Bytes: 0
Rcvd_Out_Of_Seq_MPPE_Pkts: 0
```

- **show uauth** — Exibe informações atuais de autenticação e autorização do usuário.

```
Current Most Seen
Authenticated Users 1 2
Authen In Progress 0 2
vpdn user 'vpnclient' at 50.1.1.1, authenticated
```

Troubleshoot

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

Comandos para Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\)](#) oferece suporte a determinados [comandos show](#). Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos debug.

- **debug crypto ipsec** — Exibe eventos de IPSec.
- **debug crypto isakmp** — Exibe mensagens sobre eventos de IKE.
- **debug crypto engine** — Exibe mensagens de depuração sobre mecanismos de criptografia, que executam criptografia e descriptografia.

- **debug ppp io** — Exibe as informações do pacote para a interface virtual PPTP PPP.
- **debug crypto ca** — Exibe mensagens de depuração trocadas com a CA.
- **debug ppp error** — mostra erros de protocolo e estatísticas de erros associados à negociação e à operação da conexão PPP.
- **debug vpdn error** — Exibe erros que evitam que um túnel de PPP seja estabelecido ou erros que fazem com que um túnel estabelecido seja fechado.
- **debug vpdn packet**—Exibe erros e eventos L2TP que fazem parte do fechamento ou estabelecimento de túnel normal para VPDNs.
- **debug vpdn event** — Exibe mensagens sobre eventos que fazem parte do estabelecimento ou encerramento normal do túnel PPP.
- **debug ppp uauth** — Exibe as mensagens de depuração de autenticação de usuário AAA da interface virtual PPTP PPP.

Exemplo de saída de depuração

Este é um exemplo de uma boa depuração no PIX Firewall.

```
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
ISAKMP: Created a peer node for 171.68.9.149
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth RSA sig
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x0 0xe 0x10
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a MSWIN2K client

ISAKMP (0): SA is doing RSA signature authentication using id type ID_FQDN
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing CERT payload. message ID = 0
ISAKMP (0): processing a CT_X509_SIGNATURE cert
CRYPTO_PKI: status = 0: crl check ignored
PKI: key process suspended and continued
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found
while selecting CRL

CRYPTO_PKI: cert revocation status unknown.
ISAKMP (0): cert approved with warning
ISAKMP (0): processing SIG payload. message ID = 0
ISAKMP (0): processing CERT_REQ payload. message ID = 0
ISAKMP (0): peer wants a CT_X509_SIGNATURE cert
```

ISAKMP (0): SA has been authenticated

ISAKMP (0): ID payload

next-payload : 6

type : 2

protocol : 17

port : 500

length : 23

ISAKMP (0): Total payload length: 27

return status is IKMP_NO_ERROR

crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57

OAK_QM exchange

oakley_process_quick_mode:

OAK_QM_IDLE

ISAKMP (0): processing SA payload. message ID = 3800855889

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES

ISAKMP: attributes in transform:

ISAKMP: SA life type in seconds

ISAKMP: SA life duration (VPI) of 0x0 0x0 0x3 0x84

ISAKMP: SA life type in kilobytes

ISAKMP: SA life duration (VPI) of 0x0 0x1 0x86 0xa0

ISAKMP: encaps is 2

ISAKMP: authenticator is HMAC-MD5

ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,

(key eng. msg.) dest= 171.68.9.57, src= 171.68.9.149,

dest_proxy= 171.68.9.57/255.255.255.255/17/1701 (type=1),

src_proxy= 171.68.9.149/255.255.255.255/17/1701 (type=1),

protocol= ESP, transform= esp-des esp-md5-hmac ,

lifedur= 0s and 0kb,

spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0

ISAKMP (0): processing NONCE payload. message ID = 3800855889

ISAKMP (0): processing ID payload. message ID = 3800855889

ISAKMP (0): ID_IPV4_ADDR src 171.68.9.149 prot 17 port 1701

ISAKMP (0): processing ID payload. message ID = 3800855889

ISAKMP (0): ID_IPV4_ADDR dst 171.68.9.57 prot 17 port 1701IPSEC(key_engine):

got a queue event...

IPSEC(spi_response): getting spi 0xfbc9db43(4224310083) for SA

from 171.68.9.149 to 171.68.9.57 for prot 3

return status is IKMP_NO_ERROR

crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57

OAK_QM exchange

oakley_process_quick_mode:

OAK_QM_AUTH_AWAIT

ISAKMP (0): Creating IPsec SAs

inbound SA from 171.68.9.149 to 171.68.9.57 (proxy 171.68.9.149 to 171.68.9.57)

has spi 4224310083 and conn_id 1 and flags 0

lifetime of 900 seconds

lifetime of 100000 kilobytes

outbound SA from 171.68.9.57 to 171.68.9.149 (proxy 171.68.9.57 to 171.68.9.149)

has spi 2831503048 and conn_id 2 and flags 0

lifetime of 900 seconds

lifetime of 100000 kilobytesIPSEC(key_engine): got a queue event...

IPSEC(initialize_sas): ,

(key eng. msg.) dest= 171.68.9.57, src= 171.68.9.149,

dest_proxy= 171.68.9.57/0.0.0.0/17/1701 (type=1),

src_proxy= 171.68.9.149/0.0.0.0/17/1701 (type=1),

protocol= ESP, transform= esp-des esp-md5-hmac ,

```
lifedur= 900s and 100000kb,
spi= 0xfbc9db43(4224310083), conn_id= 1, keysize= 0, flags= 0x0
IPSEC(initialize_sas): ,
(key eng. msg.) src= 171.68.9.57, dest= 171.68.9.149,
src_proxy= 171.68.9.57/0.0.0.0/17/1701 (type=1),
dest_proxy= 171.68.9.149/0.0.0.0/17/1701 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 900s and 100000kb,
spi= 0xa8c54ec8(2831503048), conn_id= 2, keysize= 0, flags= 0x0

return status is IKMP_NO_ERROR
```

show log

```
603102: PPP virtual interface 1 - user: vpnclient aaa authentication started
603103: PPP virtual interface 1 - user: vpnclient aaa authentication succeed
109011: Authen Session Start: user 'vpnclient', sid 0
603106: L2TP Tunnel created, tunnel_id is 1, remote_peer_ip is 171.68.9.149
ppp_virtual_interface_id is 1, client_dynamic_ip is 50.1.1.1
username is vpnclient
```

[Depuração válida para registrar-se com o CA](#)

```
CI thread sleeps!
Crypto CA thread wakes up!%
% Start certificate enrollment ..
```

```
% The subject name in the certificate will be: PIX-506-2.sjvpn.com
```

```
CI thread wakes up!% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
```

```
PIX-506-2(config)#
PIX-506-2(config)#      Fingerprint:  d8475977 7198ef1f 17086f56 9e3f7a89
```

```
CRYPTO_PKI: transaction PKCSReq completed
CRYPTO_PKI: status:
Crypto CA thread sleeps!
PKI: key process suspended and continued
CRYPTO_PKI: http connection opened
CRYPTO_PKI:  received msg of 711 bytes
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found
while selecting CRL
```

```
CRYPTO_PKI: signed attr: pki-message-type:
13 01 33
CRYPTO_PKI: signed attr: pki-status:
13 01 33
CRYPTO_PKI: signed attr: pki-recipient-nonce:
04 10 70 0d 4e e8 03 09 71 4e c8 24 7a 2b 03 70 55 97
CRYPTO_PKI: signed attr: pki-transaction-id:
13 20 65 66 31 32 32 31 30 33 31 37 30 61 30 38 65 32 33 38
38 35 61 36 30 65 32 35 31 31 34 66 62 37
CRYPTO_PKI: status = 102: certificate request pending
CRYPTO_PKI: http connection opened
CRYPTO_PKI:  received msg of 711 bytes
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found
while selecting CRL
CRYPTO_PKI: signed attr: pki-message-type:
13 01 33
```

```
CRYPTO_PKI: signed attr: pki-status:
13 01 33
CRYPTO_PKI: signed attr: pki-recipient-nonce:
04 10 c8 9f 97 4d 88 24 92 a5 3b ba 9e bc d6 7c 75 57
CRYPTO_PKI: signed attr: pki-transaction-id:
13 20 65 66 31 32 32 31 30 33 31 37 30 61 30 38 65 32 33 38
38 35 61 36 30 65 32 35 31 31 34 66 62 37
CRYPTO_PKI: status = 102: certificate request pending
!--- After approval from CA. Crypto CA thread wakes up! CRYPTO_PKI: resend GetCertInitial, 1
Crypto CA thread sleeps! CRYPTO_PKI: resend GetCertInitial for session: 0 CRYPTO_PKI: http
connection opened The certificate has been granted by CA! CRYPTO_PKI: received msg of 1990 bytes
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found while selecting CRL PKI: key
process suspended and continued CRYPTO_PKI: signed attr: pki-message-type: 13 01 33 CRYPTO_PKI:
signed attr: pki-status: 13 01 30 CRYPTO_PKI: signed attr: pki-recipient-nonce: 04 10 c8 9f 97
4d 88 24 92 a5 3b ba 9e bc d6 7c 75 57 CRYPTO_PKI: signed attr: pki-transaction-id: 13 20 65 66
31 32 32 31 30 33 31 37 30 61 30 38 65 32 33 38 38 35 61 36 30 65 32 35 31 31 34 66 62 37
CRYPTO_PKI: status = 100: certificate is granted CRYPTO_PKI: WARNING: Certificate, private key
or CRL was not found while selecting CRL CRYPTO_PKI: All enrollment requests completed.
CRYPTO_PKI: All enrollment requests completed. CRYPTO_PKI: WARNING: Certificate, private key or
CRL was not found while selecting CRL
```

Depuração inadequada para registro com CA

Neste exemplo, a sintaxe de URL incorreta foi usada no comando **ca identity**:

```
CI thread sleeps!
Crypto CA thread wakes up!
CRYPTO_PKI: http connection opened
msgsym(GETCARACERT, CRYPTO)!
%Error in connection to Certificate Authority: status = FAIL
CRYPTO_PKI: status = 266: failed to verify
CRYPTO_PKI: transaction GetCACert completed
Crypto CA thread sleeps!
```

Se o modo de inscrição foi especificado como CA em vez de como RA, você obtém esta depuração:

```
CI thread sleeps!
Crypto CA thread wakes up!
CRYPTO_PKI: http connection opened
Certificate has the following attributes:

Fingerprint: 49dc7b2a cd5fc573 6c774840 e58cf178

CRYPTO_PKI: transaction GetCACert completed
CRYPTO_PKI: Error: Invalid format for BER encoding while

CRYPTO_PKI: can not set ca cert object.
CRYPTO_PKI: status = 65535: failed to process RA certiifcate
Crypto CA thread sleeps!
```

Neste exemplo, o comando **mode transport** está ausente:

```
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x0 0x70 0x80
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: encaps is 2
ISAKMP: authenticator is HMAC-MD5IPSEC(validate_proposal):
invalid transform proposal flags -- 0x0
```

Nesta saída, o comando **crypto map mymap 10 ipsec-isakmp dynamic dyna** está ausente, e esta mensagem pode aparecer na depuração:

```
no IPSEC cryptomap exists for local address a.b.c.d
```

[Informações Relacionadas](#)

- [Páginas de suporte à tecnologia RADIUS](#)
- [Referências de comando PIX](#)
- [Página de suporte do PIX](#)
- [Página de Suporte de Negociação IPSec/Protocolos IKE](#)
- [Solicitações de Comentários \(RFCs\)](#)