

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

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o cliente de Microsoft L2TP](#)

[Obtenha Certificados para o PIX Firewall](#)

[Configuração de firewall PIX](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Exemplo de debug](#)

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

[Depuração inadequada para registro com CA](#)

[Informações Relacionadas](#)

Introdução

O protocolo de tunelamento de camada 2 (L2TP) em IPSec é apoiado no Software Release 6.x ou Mais Recente do firewall PIX segura Cisco. Os usuários que executam o Windows 2000 podem usar o cliente IPSec nativo e o cliente L2TP a fim estabelecer um túnel L2TP ao PIX Firewall. O tráfego corre através do túnel L2TP cifrado pelas associações de segurança IPSec (SA).

Nota: Você não pode usar o telnet do cliente de IPSec do Windows 2000 L2TP ao PIX.

Nota: O Split Tunneling não está disponível com o L2TP no PIX.

A fim configurar o L2TP sobre o IPsec de Microsoft Windows remoto 2000/2003 e os clientes XP a um escritório corporativo da ferramenta de segurança PIX/ASA usando chaves pré-compartilhada com um servidor Radius do Internet Authentication Service de Microsoft Windows 2003 (IAS) para a autenticação de usuário, refira o [L2TP sobre o IPsec entre o exemplo de configuração de utilização de Windows 2000/XP PC e da chave pré-compartilhada PIX/ASA 7.2](#).

A fim configurar o L2TP sobre a Segurança IP (IPsec) do Microsoft Windows 2000 remoto e os clientes XP a uma site corporativo usando um método cifrado, refira [configurar o L2TP sobre o IPsec de um Windows 2000 ou do cliente XP a um concentrador da Cisco VPN 3000 Series usando chaves pré-compartilhada](#).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento aplica aos estes a versão de software e hardware:

- PIX Software Release 6.3(3)
- Windows 2000 com ou sem o SP2 (veja o dica do Microsoft [Q276360](#) para obter informações sobre do SP1.)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

O suporte de certificado em versões 6.x ou mais recente do PIX seguro Cisco inclui Baltimore, Microsoft, Verisign, e confia server. Atualmente, o PIX não aceita pedidos L2TP sem proteção IPSec.

Este exemplo mostra como configurar o PIX Firewall para a encenação mencionada mais cedo neste original. 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 cifradas ao PIX estão listadas no [hardware Cisco e nos clientes VPN que apoiam IPSec/PPTP/L2TP](#).

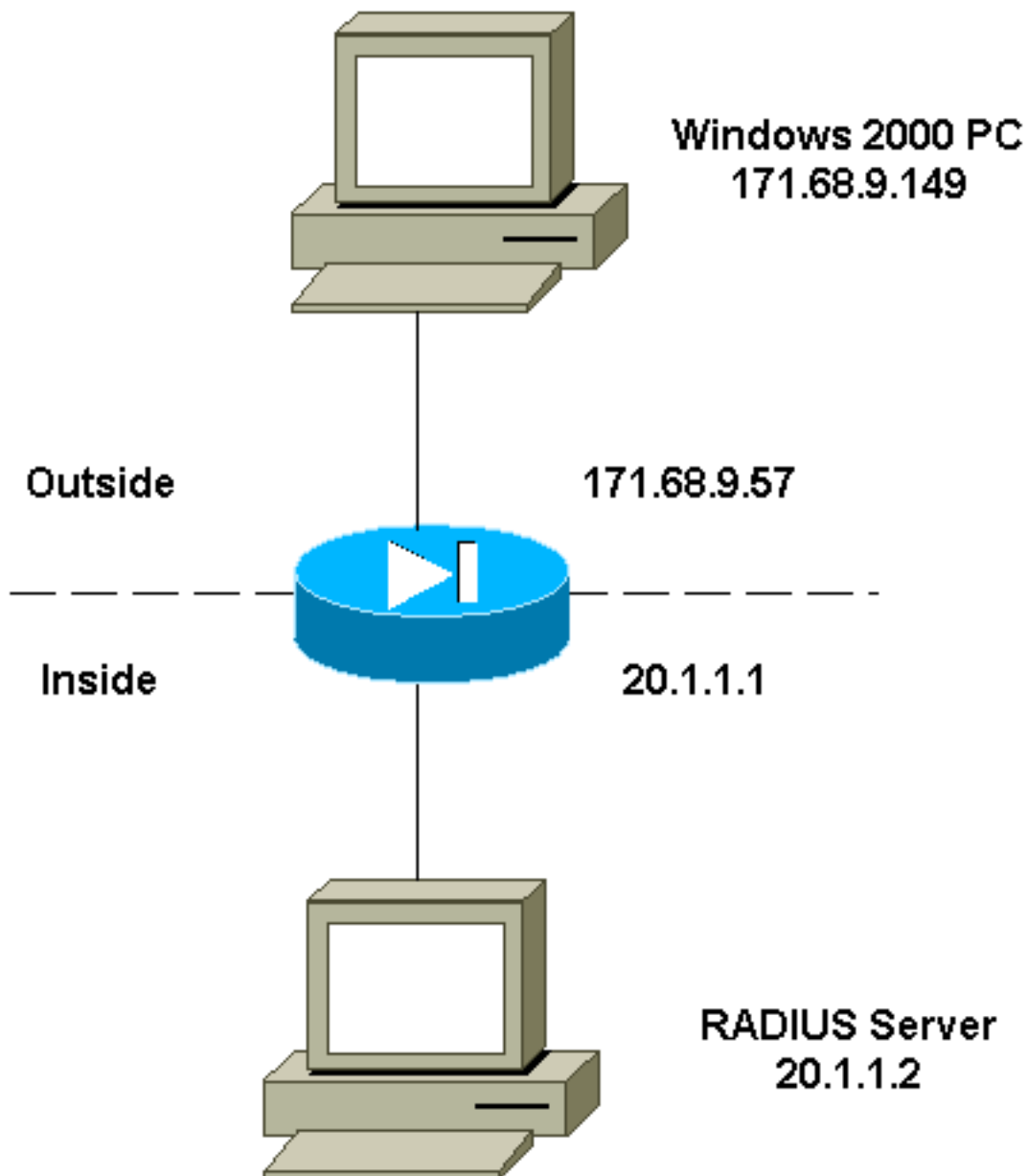
Configurar

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

Nota: Use a ferramenta [Command Lookup Tool](#) ([apenas para 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 de Microsoft L2TP

A informação em como configurar o cliente de Microsoft L2TP é encontrada no [guia passo a passo de Microsoft à segurança de protocolo do Internet](#) .

Como referido no guia passo a passo provido de Microsoft, os suportes ao cliente um número de server testados do Certificate Authority (CA). A informação em como estabelecer Microsoft CA é encontrada no [guia passo a passo de Microsoft a estabelecer um Certificate Authority](#) .

Obtenha Certificados para o PIX Firewall

Refira [exemplos de configuração de CA](#) para detalhes em como configurar o PIX para a Interoperabilidade com os Certificados de Verisign, confie, Baltimore, e Microsoft.

Configuração de firewall PIX

Este original usa 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 \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show crypto ca cert** — Indica a informação sobre seu certificado, o certificado de CA, e todos os Certificados do registration authority (RA autoridade de registro).

```

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]

```

- show crypto isakmp sa – Exibe todas as SAs de IKE atuais em um correspondente.

```

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]

```

- **mostre IPsec cripto sa** — Indica os ajustes usados por SA atuais.

```

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]

```

- **mostre o túnel do vpdn** — A informação dos indicadores sobre L2TP ativo ou Level 2 Forwarding (L2F) escava um túnel em um Virtual Private Dialup Network (VPDN).

```

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]

```

- **mostre a sessão do vpdn** — Informação dos indicadores sobre sessões ativas L2TP ou L2F em um VPDN.

```

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 l2tppsec client authentication aaa RADIUS
vpdn group l2tppsec client accounting RADIUS
vpdn group l2tppsec l2tp tunnel hello 60
vpdn enable outside
terminal width 80
Cryptochecksum:06a53009d1e9f04740256d9f0fb82837
: end
[OK]

```

- **mostre o pppinterface do vpdn** — Indica o estado e as estatísticas da interface virtual PPP que foi criada para o túnel PPTP para o valor de identificação da relação do comando **show vpdn session**.

```

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 dnats
!--- 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]
```

• **uauth da mostra** — Indicadores autenticação de usuário e informação de autorização atuais.

```
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]
```

Troubleshooting

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

Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta 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 IKE.
- **motor do debug crypto** — Os indicadores debugam mensagens sobre as crypto-engines, que executam a criptografia e a descriptografia.
- **debug ppp io** - Exibe as informações de pacotes para a interface virtual PPP PPTP.
- **debug crypto ca** — Os indicadores debugam as mensagens trocadas com 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** — Indica mensagens sobre os eventos que são parte de estabelecimento de túnel normal ou parada programada PPP.
- **debug ppp uauth** - Exibe as mensagens de depuração de autenticação de usuário AAA da interface virtual PPTP PPP.

Exemplo de debug

Esta é uma amostra de um debug correto 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](#)

```
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 inadequada para registro com CA](#)

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

```
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

Se o modo do registro foi especificado como CA em vez como do RA, a seguir você obtém este debuga:

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
```

Neste exemplo, o comando mode transport falta:

```
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
```

Nesta saída, o comando `crypto map mymap 10 ipsec-isakmp dynamic dyna` falta, e esta mensagem pode aparecer debugar:

```
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
```

[Informações Relacionadas](#)

- [Páginas de suporte de tecnologia RADIUS](#)

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