Configuración de L2TP sobre IPSec entre PIX Firewall y Windows 2000 PC con certificados

Contenido

Introducción

El Layer 2 Tunneling Protocol (L2TP) a través de IPSec se soporta en la versión 6.x o posterior de Cisco Secure PIX Firewall Software. Los usuarios con Windows 2000 pueden utilizar el cliente de IPSec nativo y el cliente de L2TP para establecer un túnel L2TP hasta el firewall PIX. El tráfico pasa por el túnel L2TP cifrado mediante Asociaciones de Seguridad IPSec (SA).

Nota: Usted no puede utilizar al cliente IPSec para Telnet del Windows 2000 L2TP al PIX.

Nota: La tunelización dividida no está disponible con el L2TP en el PIX.

Para configurar el L2TP sobre el IPSec de Microsoft Windows remoto 2000/2003 y los clientes de XP a una oficina corporativa del dispositivo de seguridad del PIX/ASA usando las claves previamente compartidas con un servidor de RADIUS del Internet Authentication Service de Microsoft Windows 2003 (IAS) para la autenticación de usuario, refiera al L2TP sobre el IPSec entre Windows 2000/XP PC y PIX/ASA 7.2 usando el ejemplo de configuración de la clave previamente compartida.

Para configurar el L2TP sobre la seguridad IP (IPSec) del Microsoft Windows 2000 remoto y a los

clientes de XP a un sitio corporativo usando un método cifrado, refiera a configurar el L2TP sobre el IPSec de un Windows 2000 o de un cliente de XP a un concentrador del Cisco VPN de la serie 3000 usando las claves previamente compartidas.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se aplica a estas versiones de software y hardware:

- Software PIX versión 6.3(3)
- Windows 2000 con o sin el SP2 (véase la recomendación de Microsoft Q276360 para la información sobre el SP1.)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

El Soporte de certificado en las versiones incluye 6.x del Secure PIX de Cisco o más adelante Baltimore, Microsoft, Verisign, y confía los servidores. Actualmente, el PIX no valida las peticiones L2TP fuera protección IPSec.

Este ejemplo muestra cómo configurar el firewall PIX para el escenario mencionado anterior en este documento. La autenticación del Internet Key Exchange (IKE) utiliza el **comando rsa-sig** (Certificados). En este ejemplo, la autenticación es hecha por un servidor de RADIUS.

Las opciones menos vinculadas para las conexiones cliente cifradas al PIX son mencionadas en el Cisco Hardware y los clientes VPN que soportan IPSec/PPTP/L2TP.

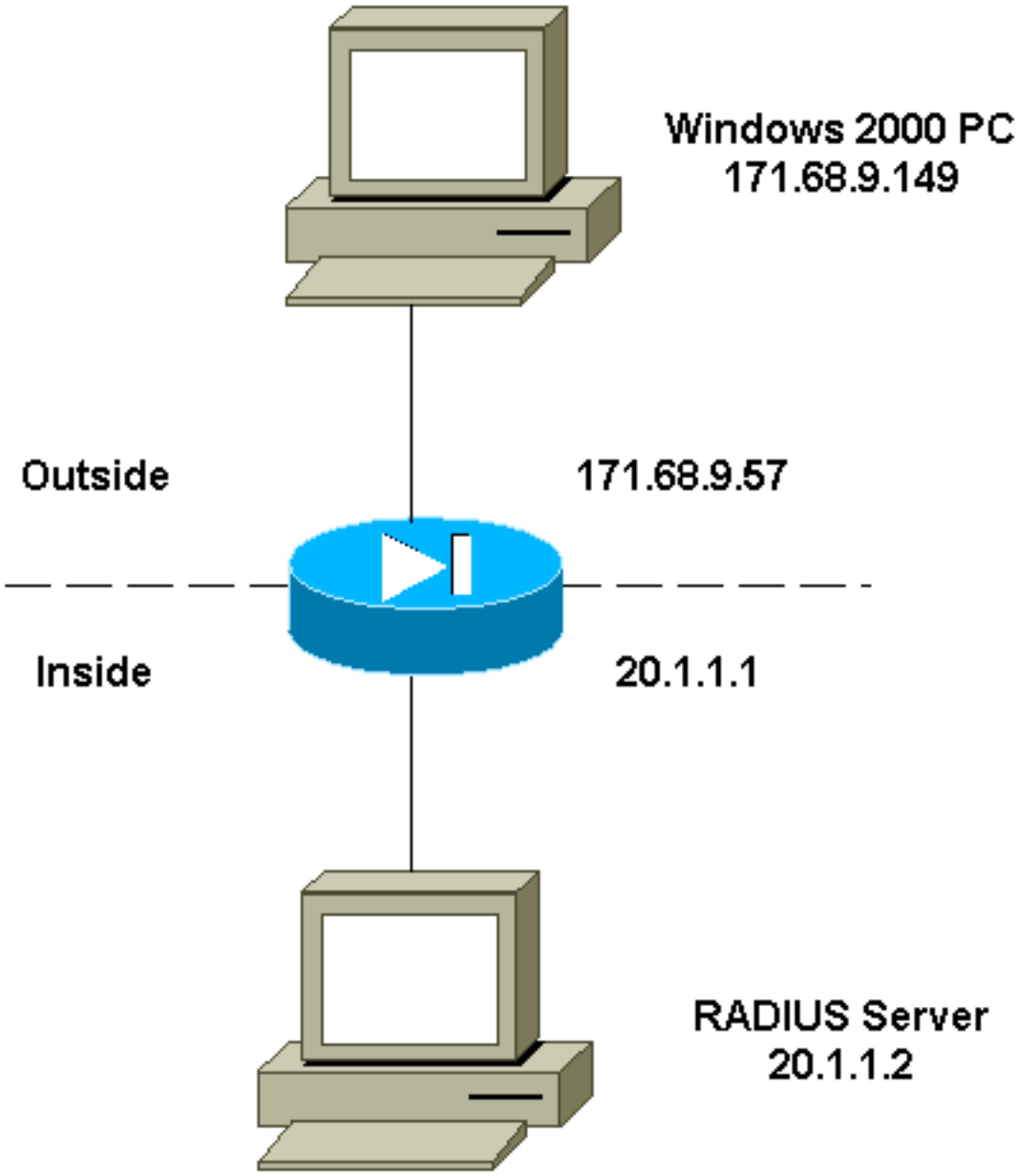
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configure al cliente de Microsoft L2TP

La información sobre cómo configurar al cliente de Microsoft L2TP se encuentra en el guía paso a paso de Microsoft a la seguridad de protocolos en Internet .

Como se apunta en el guía paso a paso referido de Microsoft, los soportes de cliente varios servidores probados del Certificate Authority (CA). La información sobre cómo configurar Microsoft CA se encuentra en el guía paso a paso de Microsoft a configurar un Certificate Authority .

Consiga los Certificados para el firewall PIX

Refiera a los ejemplos de configuración de CA para los detalles en cómo configurar el PIX para la Interoperabilidad con los Certificados de Verisign, confíelos, Baltimore, y Microsoft.

Configuración de Firewall de PIX

Este documento utiliza esta configuración.

Firewall 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]
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto ca cert** — Visualiza la información sobre su certificado, el certificado de CA, y cualquier Certificados del registration authority (RA).

  ```
  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 — Muestra todas las asociaciones actuales de seguridad (SA) IKE de un par.

```
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 ipsec sa — Muestra la configuración actual utilizada por las SA actuales

```
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]
```

- **muestre el túnel del vpdn** — La información de las visualizaciones sobre L2TP activo o el Level 2 Forwarding (L2F) hace un túnel en un 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]
```

- **muestre la sesión del vpdn** — Información de las visualizaciones sobre las sesiones activas L2TP o L2F en un 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]
```

- **muestre el pppinterface del vpdn** — Visualiza el estatus y las estadísticas de la interfaz virtual PPP que fue creada para el túnel PPTP por el valor de identificación de la interfaz del **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 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]
```

- uauth de la demostración — Visualiza la información de autenticación y autorización del Usuario usuario actual.

```
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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **IPSec del debug crypto** — Eventos del IPSec de las visualizaciones.
- debug crypto isakmp — Muestra mensajes acerca de eventos IKE.
- **motor del debug crypto** — Mensajes del debug de las visualizaciones sobre los motores de criptografía, que realizan el cifrado y el desciframiento.
- debug ppp io — Muestra la información de paquete para la interfaz virtual PPTP PPP.
- **debug crypto ca** — Mensajes del debug de las visualizaciones intercambiados por CA.
- debug ppp error — Muestra los errores de protocolo y las estadísticas de error relacionadas con la negociación y operación de conexiones PPP.
- debug vpdn error — Muestra errores que evitan que se establezca un túnel PPP o errores que provocan que un túnel establecido se cierre.
- debug vpdn packet - Muestra errores L2TP y eventos que son una parte del establecimiento normal de túneles o apagado para las VPDN.
- **debug vpdn event** — Visualiza los mensajes sobre los eventos que son establecimiento del túnel normal de la parte de PPP o apagan.
- debug ppp uauth - Muestra los mensajes de depuración de autenticación de usuario de AAA de la interfaz virtual de PPTP PPP.

Ejemplo de resultado del comando debug

Esto es una muestra de un debug correcta en el firewall PIX.

```
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
```

Depuración correcta para registro con 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
```

Depuración incorrecta para registro con CA

En este ejemplo, la sintaxis de URL incorrecta fue utilizada en el **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
```

Si el modo de la inscripción fue especificado como CA en vez como de RA, después usted consigue este debug:

```
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
```

En este ejemplo, el 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
```

En esta salida, el comando crypto map mymap 10 ipsec-isakmp dynamic dyna falta, y este mensaje puede aparecer en el debug:

```
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
```

Información Relacionada

- Páginas de soporte de tecnología RADIUS
- Referencia de Comandos PIX
- Página de Soporte de PIX
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Solicitudes de Comentarios (RFC)