

# Cómo configurar al Cliente Cisco VPN al PIX con el AES

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configuraciones](#)

[Diagrama de la red](#)

[Configure el PIX](#)

[Configure el cliente VPN](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## [Introducción](#)

Este ejemplo de configuración muestra cómo establecer una conexión VPN de acceso remoto desde un Cisco VPN Client a un PIX Firewall, con el Estándar de encriptación avanzado (AES) para el encriptación. Este ejemplo utiliza Cisco Easy VPN para configurar el canal seguro y el firewall PIX se configura como Easy VPN Server.

En el Software Release 6.3 y Posterior del Cisco Secure PIX Firewall, la nueva norma de encriptación internacional AES se soporta para asegurar el sitio a localizar y las conexiones VPN de acceso remoto. Esto está además del Data Encryption Standard (DES) y de los algoritmos de encriptación 3DES. El firewall PIX soporta los tamaños de clave AES de los bits 128, 192, y 256.

El cliente VPN soporta el AES como algoritmo de encriptación que comienza con la versión de Cliente Cisco VPN 3.6.1. El cliente VPN soporta los tamaños de clave de los bits 128 y de los bits 256 solamente.

## [prerrequisitos](#)

### [Requisitos](#)

Esta configuración de muestra asume que el PIX está completamente - operativo y configurado con los comandos necesarios para manejar el tráfico según la política de seguridad de la organización.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software PIX versión 6.3(1)**Nota:** Se espera que esta configuración fue probada en el software PIX versión 6.3(1) y trabaje en todos más adelante las versiones.
- Cliente VPN de Cisco versión 4.0.3(A)**Nota:** Esta configuración fue probada en la versión 4.0.3(A) pero los trabajos del cliente VPN sobre las versiones anteriores de nuevo a 3.6.1 y hasta la versión actual.

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 Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Antecedentes

Las VPN de acceso remoto están abocadas a los requerimientos de la fuerza laboral móvil para la conexión segura a la red de la organización. Los usuarios ambulantes pueden configurar una conexión segura usando el software cliente VPN instalado en sus PC. El cliente VPN inicia una conexión a un dispositivo del sitio central configurado para validar estas peticiones. En este ejemplo, el dispositivo del sitio central es un firewall PIX configurado como Easy VPN Server que utiliza las correspondencias cifradas dinámicas.

El Cisco Easy VPN simplifica el despliegue de VPN haciendo la configuración y la Administración de los VPN fáciles. Consiste en el servidor del Cisco Easy VPN y el telecontrol del Cisco Easy VPN. La configuración mínima se requiere en el Easy VPN Remote. El Easy VPN Remote inicia una conexión. Si la autenticación es acertada, el Easy VPN Server empuja la configuración VPN hacia abajo a ella. Más información sobre cómo configurar un firewall PIX como Easy VPN Server está disponible en el [manejo del Acceso Remoto VPN](#).

Las correspondencias cifradas dinámicas se utilizan para la configuración IPsec cuando algunos parámetros requeridos para configurar el VPN no pueden ser predeterminados, como en el caso de los usuarios ambulantes que obtienen dinámicamente los IP Address asignados. La correspondencia cifrada dinámica actúa como plantilla y los parámetros que falta se determinan durante el IPsec Negotiation. Hay más información disponible sobre los mapas de encriptación dinámicos en [Mapas de encriptación dinámicos](#).

## Configuraciones

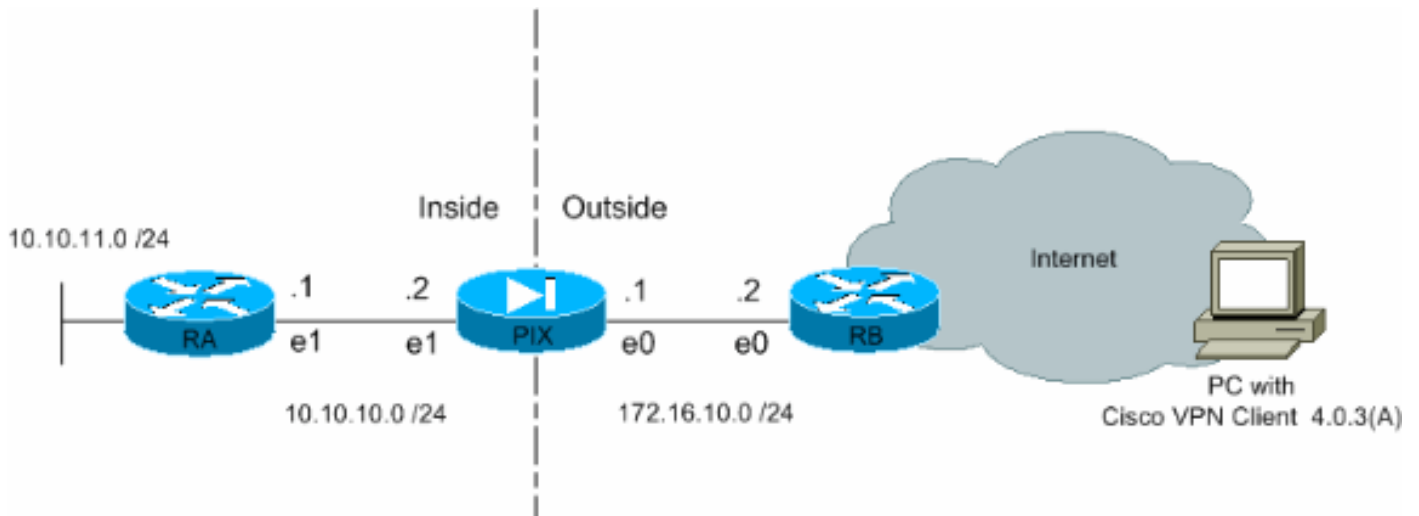
En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener

más información sobre los comandos utilizados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configure el PIX

La configuración necesaria en el firewall PIX se muestra en esta salida. La configuración está para el VPN solamente.

### PIX

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names

!--- Define the access list to enable split tunneling.
access-list 101 permit ip 10.10.10.0 255.255.255.0
10.10.8.0 255.255.255.0 access-list 101 permit ip
10.10.11.0 255.255.255.0 10.10.8.0 255.255.255.0 !---
Define the access list to avoid network address !---
translation (NAT) on IPsec packets. access-list 102
permit ip 10.10.10.0 255.255.255.0 10.10.8.0
```

```

255.255.255.0 access-list 102 permit ip 10.10.11.0
255.255.255.0 10.10.8.0 255.255.255.0 pager lines 24 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 !---
Configure the IP address on the interfaces. ip address
outside 172.16.10.1 255.255.255.0 ip address inside
10.10.10.2 255.255.255.0 no ip address intf2 ip audit
info action alarm ip audit attack action alarm !---
Create a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool vpnpool1 10.10.8.1-10.10.8.254 pdm history
enable arp timeout 14400 !--- Disable NAT for IPsec
packets. nat (inside) 0 access-list 102 route outside
0.0.0.0 0.0.0.0 172.16.10.2 1 route inside 10.10.11.0
255.255.255.0 10.10.10.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h225 1:00:00 timeout h323 0:05:00 mgcp 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-server LOCAL protocol local no snmp-
server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Permit packet that came from an IPsec tunnel
to pass through without !--- checking them against the
configured conduits/access lists. sysopt connection
permit-ipsec !--- Define the transform set to be used
during IPsec !--- security association (SA) negotiation.
Specify AES as the encryption algorithm. crypto ipsec
transform-set trmset1 esp-aes-256 esp-sha-hmac !---
Create a dynamic crypto map entry !--- and add it to a
static crypto map. crypto dynamic-map map2 10 set
transform-set trmset1 crypto map map1 10 ipsec-isakmp
dynamic map2 !--- Bind the crypto map to the outside
interface. crypto map map1 interface outside !--- Enable
Internet Security Association and Key Management !---
Protocol (ISAKMP) negotiation on the interface on which
the IPsec !--- peer communicates with the PIX Firewall.
isakmp enable outside isakmp identity address !---
Define an ISAKMP policy to be used while !---
negotiating the ISAKMP SA. Specify !--- AES as the
encryption algorithm. The configurable AES !--- options
are aes, aes-192 and aes-256. !--- Note: AES 192 is not
supported by the VPN Client. isakmp policy 10
authentication pre-share isakmp policy 10 encryption
aes-256 isakmp policy 10 hash sha isakmp policy 10 group
2 isakmp policy 10 lifetime 86400 !--- Create a VPN
group and configure the policy attributes which are !---
downloaded to the Easy VPN Clients. vpngroup
groupmarketing address-pool vpnpool1 vpngroup
groupmarketing dns-server 10.10.11.5 vpngroup
groupmarketing wins-server 10.10.11.5 vpngroup
groupmarketing default-domain org1.com vpngroup
groupmarketing split-tunnel 101 vpngroup groupmarketing
idle-time 1800 vpngroup groupmarketing password *****
telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:c064abce81996b132025e83e421e1c3 : end

```

**Nota:** En esta configuración, se recomienda que usted para no especificar el aes-192 mientras que usted configura el conjunto de la transformación o la política isakmp. Los clientes VPN no soportan el aes-192 para el cifrado.

**Nota:** Con las versiones anteriores, requirieron a los comandos isakmp client configuration

address-pool y crypto map client-configuration address de la configuración de modo IKE. Sin embargo, con las versiones más nuevas (3.x y posterior) estos comandos ya no son necesarios. Varias agrupaciones de direcciones ahora pueden ser especificadas utilizando el comando vpngroup address-pool.

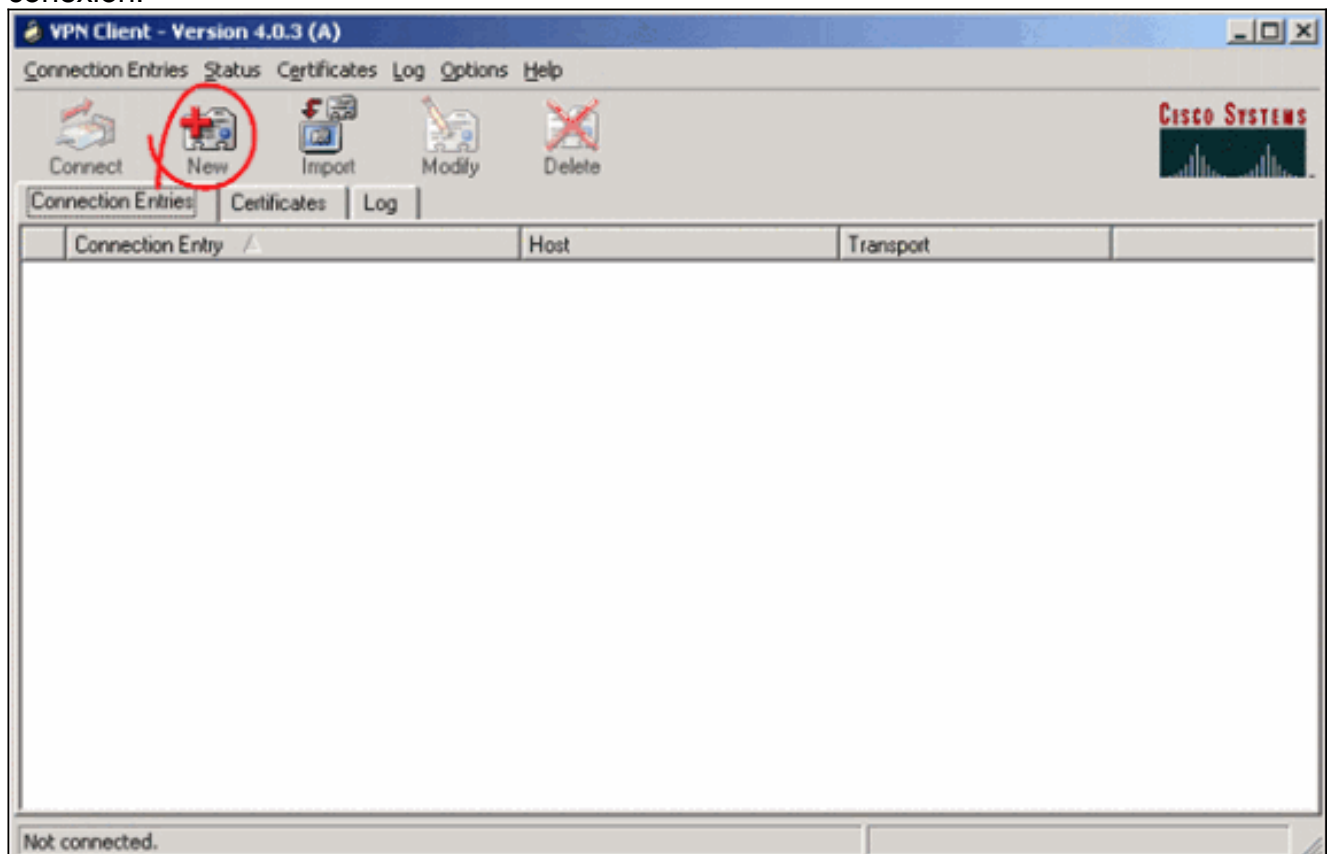
**Nota:** Los nombres del grupo VPN son con diferenciación entre mayúsculas y minúsculas. Esto significa que la autenticación de usuario falla si el nombre del grupo especificado en el PIX y el nombre del grupo en el cliente VPN son diferentes en términos de caso de carta (superior o minúsculo).

**Nota:** Por ejemplo, cuando usted ingresa el nombre del grupo como **GroupMarketing** en un dispositivo y **groupmarketing** en otro dispositivo, el dispositivo no funciona.

## [Configure el cliente VPN](#)

Después de que usted instale al cliente VPN en el PC, cree una nueva conexión tal y como se muestra en de estos pasos:

1. Inicie la aplicación cliente VPN y haga clic en Nuevo para crear una nueva entrada de conexión.



2. Un nuevo cuadro de diálogo tituló al cliente VPN | Cree la nueva entrada de la conexión VPN aparece. Ingrese la información de configuración para la nueva conexión. En Entrada de conexión el campo, asigne un nombre a la nueva entrada se crea que. En el campo Host, ingrese la dirección de IP de la interfaz pública del PIX. Seleccione la lengüeta de la autenticación, y después teclee el nombre del grupo y la contraseña (dos veces - para la confirmación). Esto necesita corresponder con la información ingresada en el PIX usando el **comando vpngroup password**. Haga clic en Save (Guardar) para guardar la información ingresada. La nueva conexión ahora se

**VPN Client | Create New VPN Connection Entry**

Connection Entry: Connect to PIX

Description:

Host: 172.16.10.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication

Name: groupmarketing

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Certificate Authentication

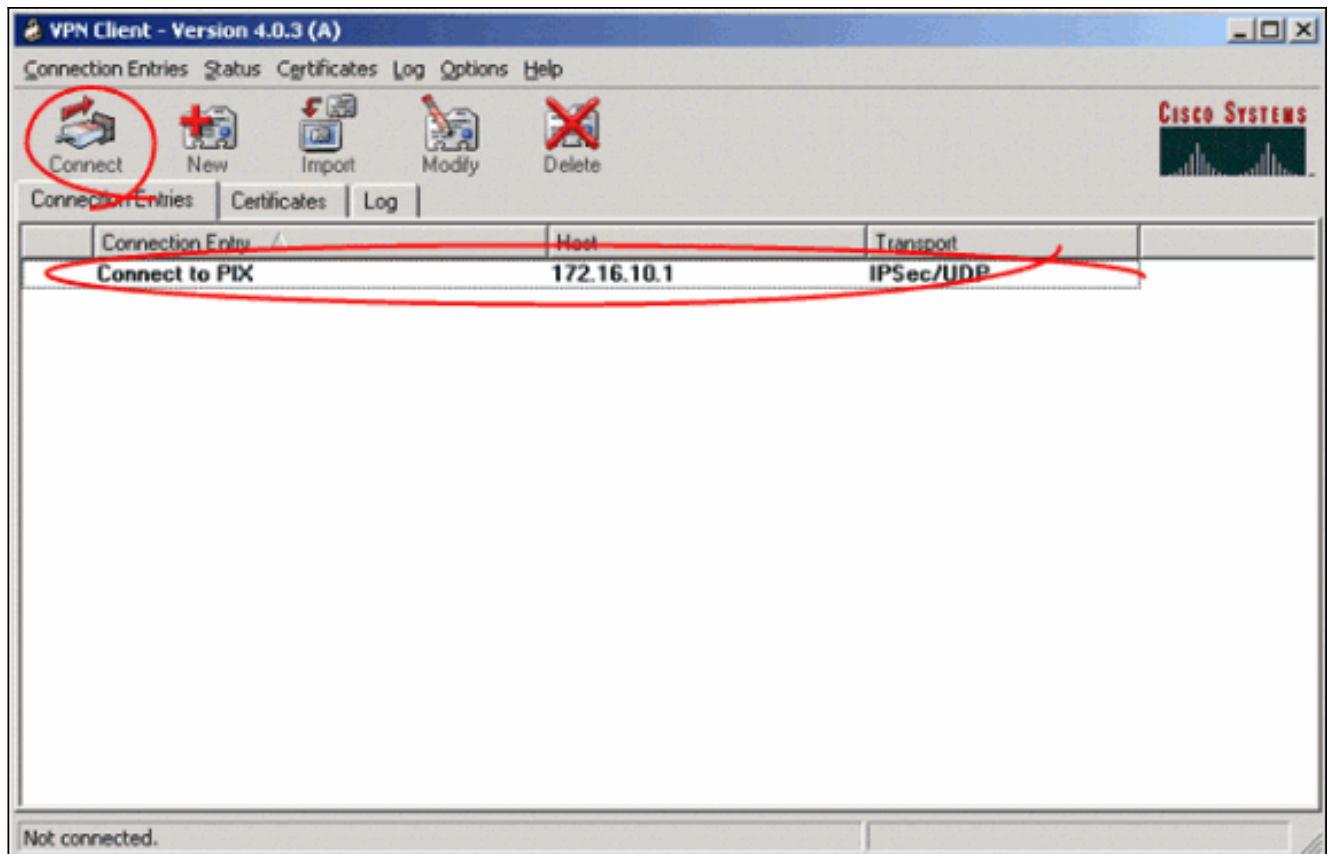
Name:

Send CA Certificate Chain

Erase User Password | **Save** | Cancel

crea.

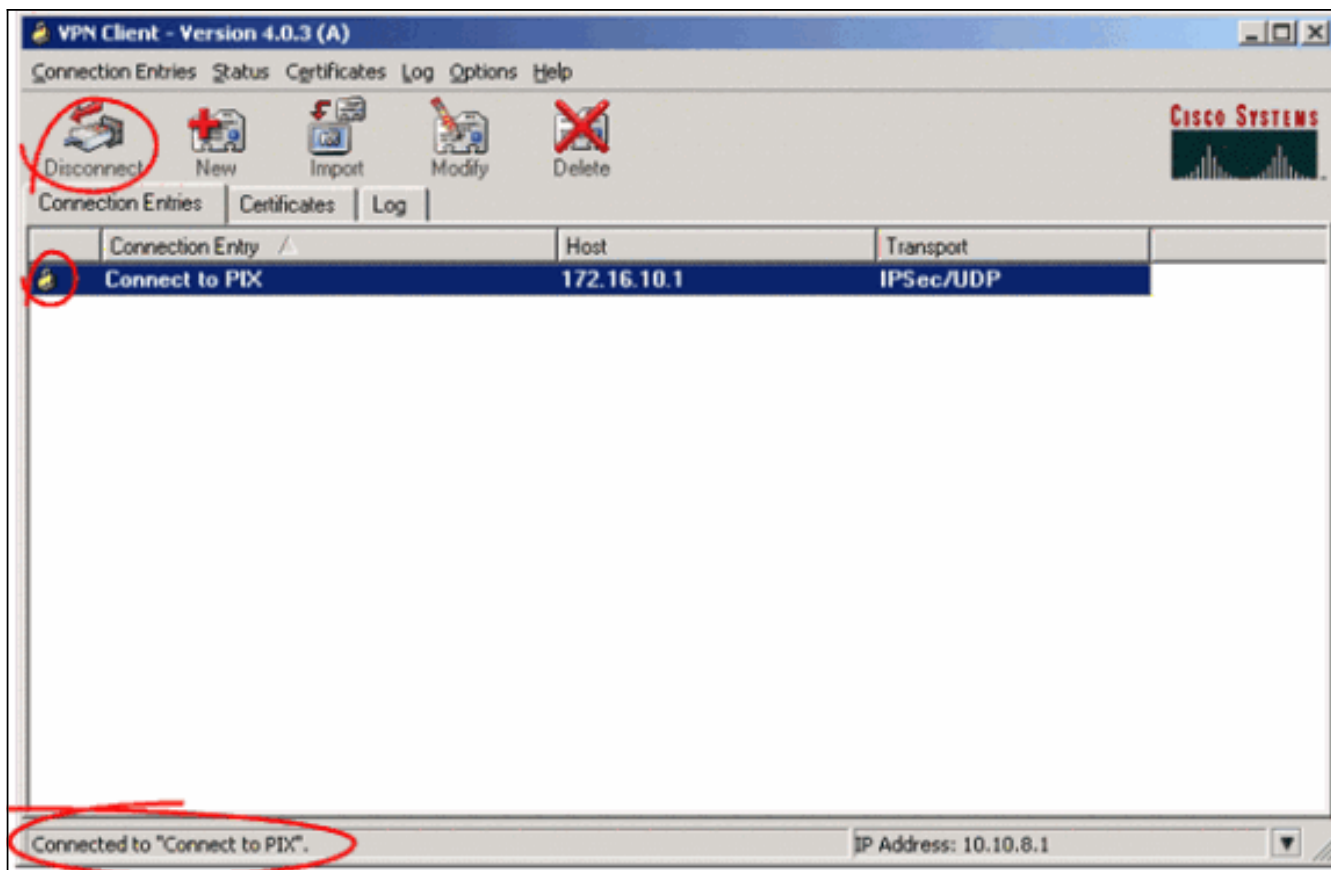
3. Para conectar con el gateway usando la entrada de la nueva conexión, seleccione Entrada de conexión haciendolo clic en una vez y después haga clic el icono de la **conexión**. Un doble clic en la entrada de conexión tiene el mismo efecto.



## Verificación

En el cliente VPN, una conexión establecida al gateway remoto es indicada con éxito por estos elementos:

- Aparece un icono amarillo de candado cerrado contra la entrada de la conexión activa.
- El icono de la conexión en la barra de herramientas (al lado de la lengüeta de las entradas de la conexión) cambia para desconectar.
- La línea del estado en el extremo de la ventana muestra el estatus como “conectado con” seguido por Entrada de conexión el nombre.



**Nota:** En forma predeterminada, una vez establecida la conexión, el cliente VPN se minimiza a un icono de candado cerrado en la bandeja del sistema, en la esquina inferior derecha de la barra de tareas de Windows. Tecleo doble el icono del candado cerrado para hacer la ventana del cliente VPN visible otra vez.

En el firewall PIX, estos **comandos show** pueden ser utilizados para verificar el estatus de las conexiones establecidas.

**Nota:** La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **muestre IPsec crypto sa** — Muestra todo el SA de IPsec actual en el PIX. Además, el resultado muestra la dirección IP real del par remoto, la dirección IP asignada, la interfaz y dirección IP local, y la correspondencia de criptografía aplicada.
 

```
Pixfirewall#show crypto ipsec sa interface: outside Crypto map tag: map1, local addr. 172.16.10.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.10.8.1/255.255.255.255/0/0) current_peer: 172.16.12.3:500 dynamic allocated peer ip: 10.10.8.1 PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.12.3 path mtu 1500, ipsec overhead 64, media mtu 1500 current outbound spi: cbabd0ce inbound esp sas: spi: 0x4d8a971d(1300928285) transform: esp-aes-256 esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: map1 sa timing: remaining key lifetime (k/sec): (4607996/28685) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xcbabd0ce(3417034958) transform: esp-aes-256 esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: map1 sa timing: remaining key lifetime (k/sec): (4608000/28676) IV size: 16 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
```
- **muestre isakmp crypto sa** — Muestra el estatus ISAKMP SA construido entre los pares.
 

```
Pixfirewall#show crypto isakmp sa Total : 1 Embryonic : 0 dst src state pending created 172.16.10.1 172.16.12.3 QM_IDLE 0 1
```



# Troubleshooting

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

Estos comandos debug pueden ayudar a los problemas del troubleshooting con la configuración de VPN.

**Nota:** Consulte [información importante en los comandos debug](#) antes de ejecutar los comandos debug.

- **isakmp del debug crypto** — Muestra ISAKMP SA se construye que y los atributos del IPsec se negocian que. Durante la negociación ISAKMP SA, el PIX puede desechar posiblemente varias ofertas mientras que “no aceptable” antes de que valide uno. Una vez que se conviene en ISAKMP SA, se negocian los atributos del IPsec. De nuevo, varias ofertas se pueden rechazar posiblemente antes de que se valide una, tal y como se muestra en de esta **salida de los debugs**.

```
crypto_isakmp_process_block:src:172.16.12.3, dest:172.16.10.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy ISAKMP: encryption AES-CBC
ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: extended auth pre-share (init) ISAKMP:
life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP: keylength of
256 !--- Proposal is rejected since extended auth is not configured. ISAKMP (0): atts are
not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 2 against priority
10 policy ISAKMP: encryption AES-CBC ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP:
extended auth pre-share (init) ISAKMP: life type in seconds ISAKMP: life duration (VPI) of
0x0 0x20 0xc4 0x9b ISAKMP: keylength of 256 !--- Proposal is rejected since MD5 is not
specified as the hash algorithm. ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy ISAKMP: encryption AES-
CBC ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: auth pre-share ISAKMP: life type in
seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP: keylength of 256 !--- This
proposal is accepted since it matches ISAKMP policy 10. ISAKMP (0): atts are acceptable.
Next payload is 3 ISAKMP (0): processing KE payload. message ID = 0 !--- Output is
suppressed. OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA
payload. message ID = 3348522173 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1,
ESP_AES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: key
length is 256 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration
(VPI) of 0x0 0x20 0xc4 0x9b !--- This proposal is not accepted since transform-set !---
trmset1 does not use MD5. ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0):
skipping next ANded proposal (1) ISAKMP : Checking IPsec proposal 2 ISAKMP: transform 1,
ESP_AES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: key
length is 256 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration
(VPI) of 0x0 0x20 0xc4 0x9b !--- This proposal is accepted since it matches !--- transform-
set trmset1. ISAKMP (0): atts are acceptable. ISAKMP (0): bad SPI size of 2 octets! ISAKMP :
Checking IPsec proposal 3 !--- Output is suppressed.
```

- **IPsec del debug crypto** — Visualiza la información sobre las negociaciones IPsec

```
SA.IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.16.12.3
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal_request): proposal part #1,
```

```
(key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 10.10.8.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfb0cb69(263244649) for SA
    from    172.16.12.3 to    172.16.10.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xfb0cb69(263244649), conn_id= 2, keysize= 256, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.16.10.1, dest= 172.16.12.3,
src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
dest_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xda6c054a(3664512330), conn_id= 1, keysize= 256, flags= 0x4
```

Con las configuraciones mostradas en este documento, el cliente VPN puede conectar con éxito con el sitio central PIX usando el AES. Se observa a veces que aunque el túnel VPN se establezca con éxito, los usuarios no pueden realizar las tareas comunes tales como recursos de red del ping, abrir una sesión al dominio, u hojear la vecindad de la red. Más información sobre resolver problemas tales problemas está disponible en la [vecindad de red de Microsoft del troubleshooting después de establecer un túnel VPN con el Cliente Cisco VPN](#).

## Información Relacionada

- [Advanced Encryption Standard \(AES\)](#)
- [Una Introducción al Cifrado de Seguridad IP \(IPSec\)](#)
- [Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración](#)
- [Página de Soporte de IPSec Negotiation/IKE Protocols](#)
- [Página de Soporte de PIX](#)
- [Página de soporte para cliente Cisco VPN](#)
- [Referencia de Comandos PIX](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)