

Cómo Configurar Cisco VPN Client a PIX con AES

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configuraciones](#)

[Diagrama de la red](#)

[Configure el PIX](#)

[Configure el cliente VPN](#)

[Verificación](#)

[Troubleshoot](#)

[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 la versión 6.3 y posteriores del software Cisco Secure PIX Firewall, el nuevo estándar internacional de cifrado AES es compatible para proteger las conexiones VPN de sitio a sitio y de acceso remoto. Esto se añade a los algoritmos estándar de cifrado de datos (DES) y 3DES. El firewall PIX soporta tamaños de clave AES de 128, 192 y 256 bits.

El cliente VPN admite AES como algoritmo de cifrado que comienza con Cisco VPN Client versión 3.6.1. VPN Client soporta tamaños de clave de 128 bits y 256 bits solamente.

[Prerequisites](#)

[Requirements](#)

Esta configuración de ejemplo 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:** Esta configuración se probó en la versión 6.3(1) del software PIX y se espera que funcione en todas las versiones posteriores.
- Cisco VPN Client versión 4.0.3(A)**Nota:** Esta configuración se probó en VPN Client versión 4.0.3(A) pero funciona en versiones anteriores de nuevo a 3.6.1 y hasta la versión actual.

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

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 móviles pueden configurar una conexión segura mediante el software VPN Client instalado en sus PC. El cliente VPN inicia una conexión a un dispositivo de sitio central configurado para aceptar estas solicitudes. En este ejemplo, el dispositivo del sitio central es un firewall PIX configurado como servidor Easy VPN que utiliza mapas criptográficos dinámicos.

Cisco Easy VPN simplifica la implementación de VPN facilitando la configuración y gestión de VPN. Se compone del servidor Cisco Easy VPN y del Cisco Easy VPN Remote. Se requiere una configuración mínima en el Easy VPN remoto. Easy VPN Remote inicia una conexión. Si la autenticación se realiza correctamente, el servidor Easy VPN le envía la configuración VPN. Hay más información disponible sobre cómo configurar un Firewall PIX como servidor Easy VPN en [Administración de Acceso Remoto VPN](#).

Los mapas criptográficos dinámicos se utilizan para la configuración de IPSec cuando algunos parámetros requeridos para configurar la VPN no pueden ser predeterminados, como ocurre con los usuarios móviles que obtienen direcciones IP asignadas dinámicamente. El mapa criptográfico dinámico actúa como una plantilla y los parámetros faltantes se determinan durante la negociación IPSec. Hay más información disponible sobre los mapas de encriptación dinámicos en [Mapas de encriptación dinámicos](#).

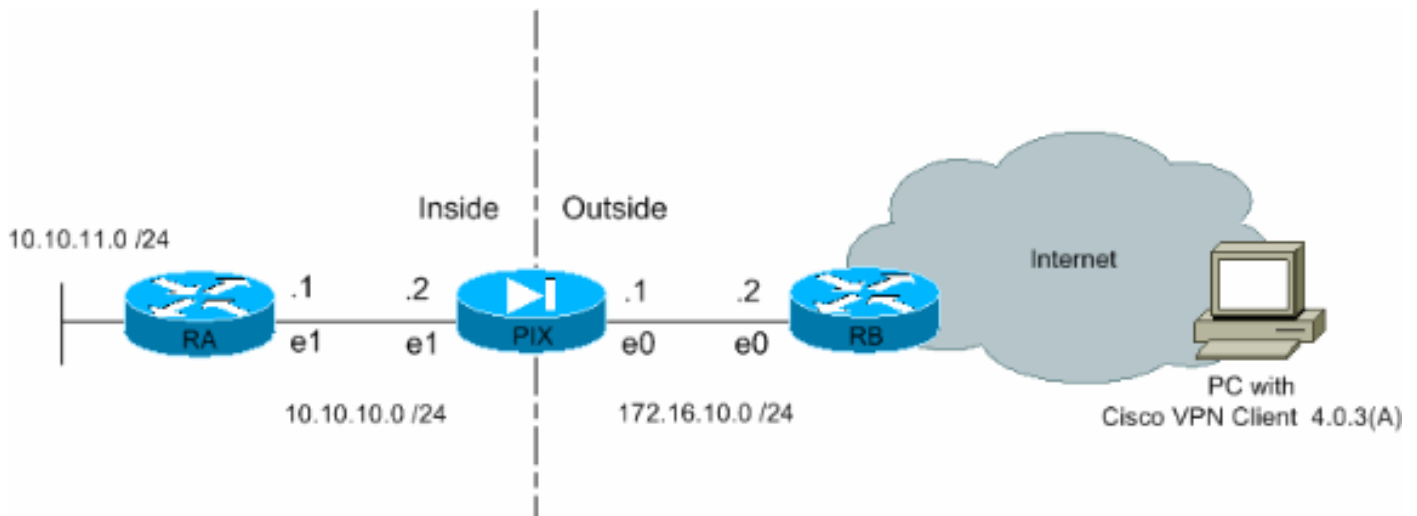
Configuraciones

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

Nota: Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) 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 este resultado. La configuración es sólo para VPN.

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:c064abce81996b132025e83e421ee1c3 : end

```

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

Nota: Con las versiones anteriores, los comandos IKE Mode Configuration **isakmp client configuration address-pool** y **crypto map client-configuration address** fueron necesarios. 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**.

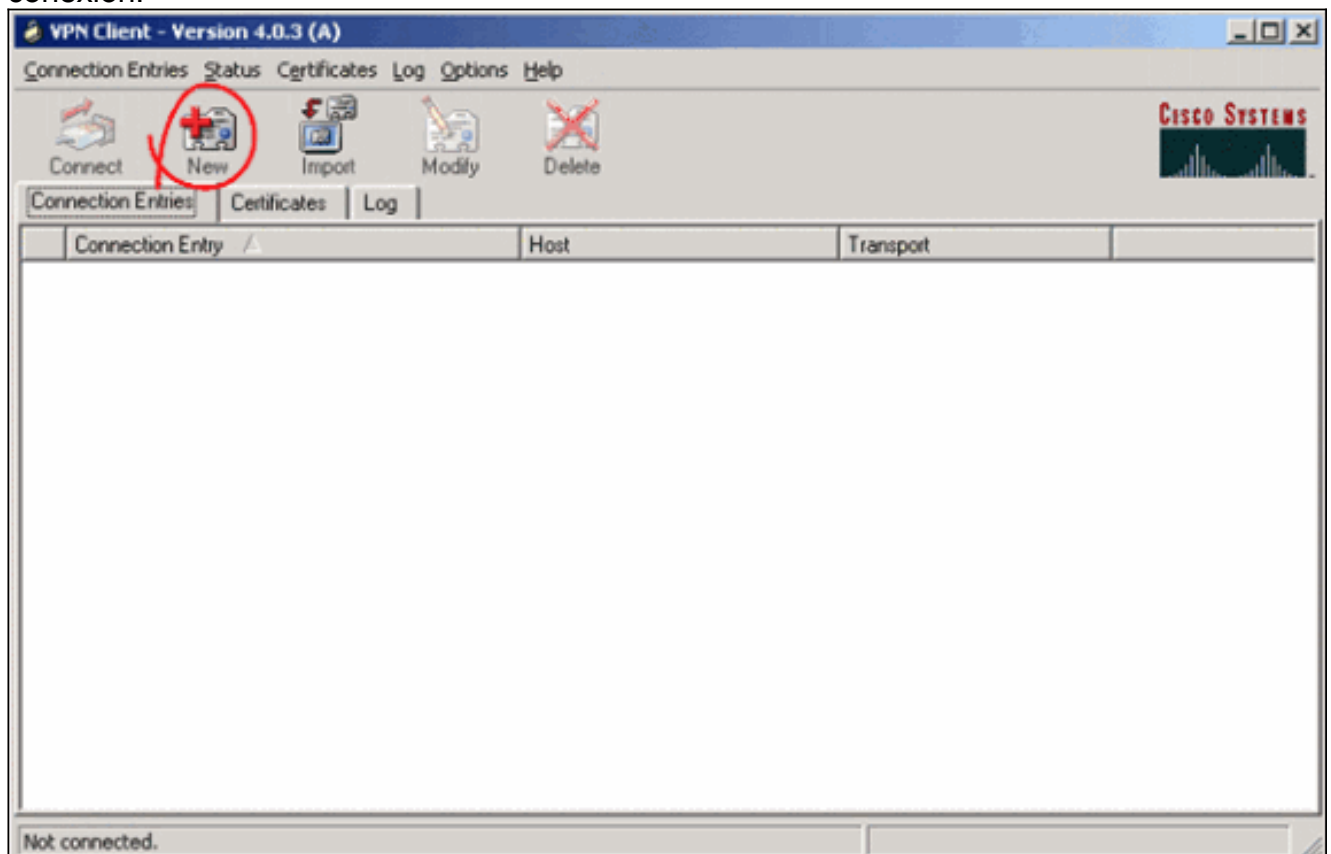
Nota: Los nombres de grupos VPN distinguen entre mayúsculas y minúsculas. Esto significa que la autenticación de usuario falla si el nombre de grupo especificado en el PIX y el nombre de grupo en el VPN Client son diferentes en términos de letra mayúscula o minúscula.

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

[Configure el cliente VPN](#)

Después de instalar VPN Client en el PC, cree una nueva conexión como se muestra en 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 titulado VPN Client | Aparece la opción Crear nueva entrada de conexión VPN. Ingrese la información de configuración para la nueva conexión. En el campo Connection Entry (Entrada de conexión), asigne un nombre a la nueva entrada creada. En el campo Host, ingrese la dirección de IP de la interfaz pública del PIX. Seleccione la ficha Authentication (Autenticación) y, a continuación, escriba el nombre del grupo y la contraseña (dos veces - para obtener confirmación). Esto necesita coincidir con la información ingresada en el PIX usando el comando **vpngroup password**. Haga clic en Save (Guardar) para guardar la información ingresada. Se ha creado la nueva

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication

Name:

Password:


Confirm Password:

Certificate Authentication

Name:

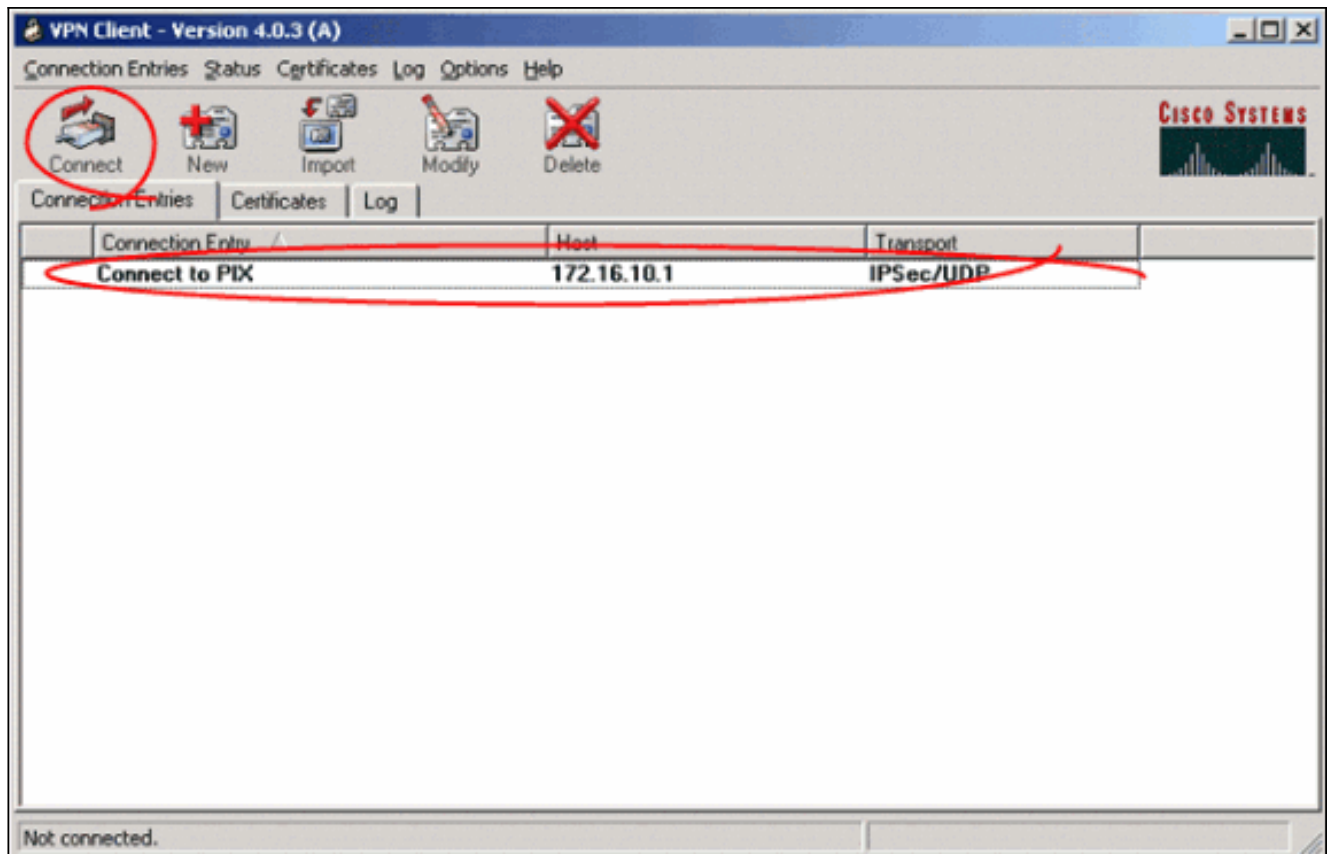
Send CA Certificate Chain

Erase User Password | Save | Cancel



conexión.

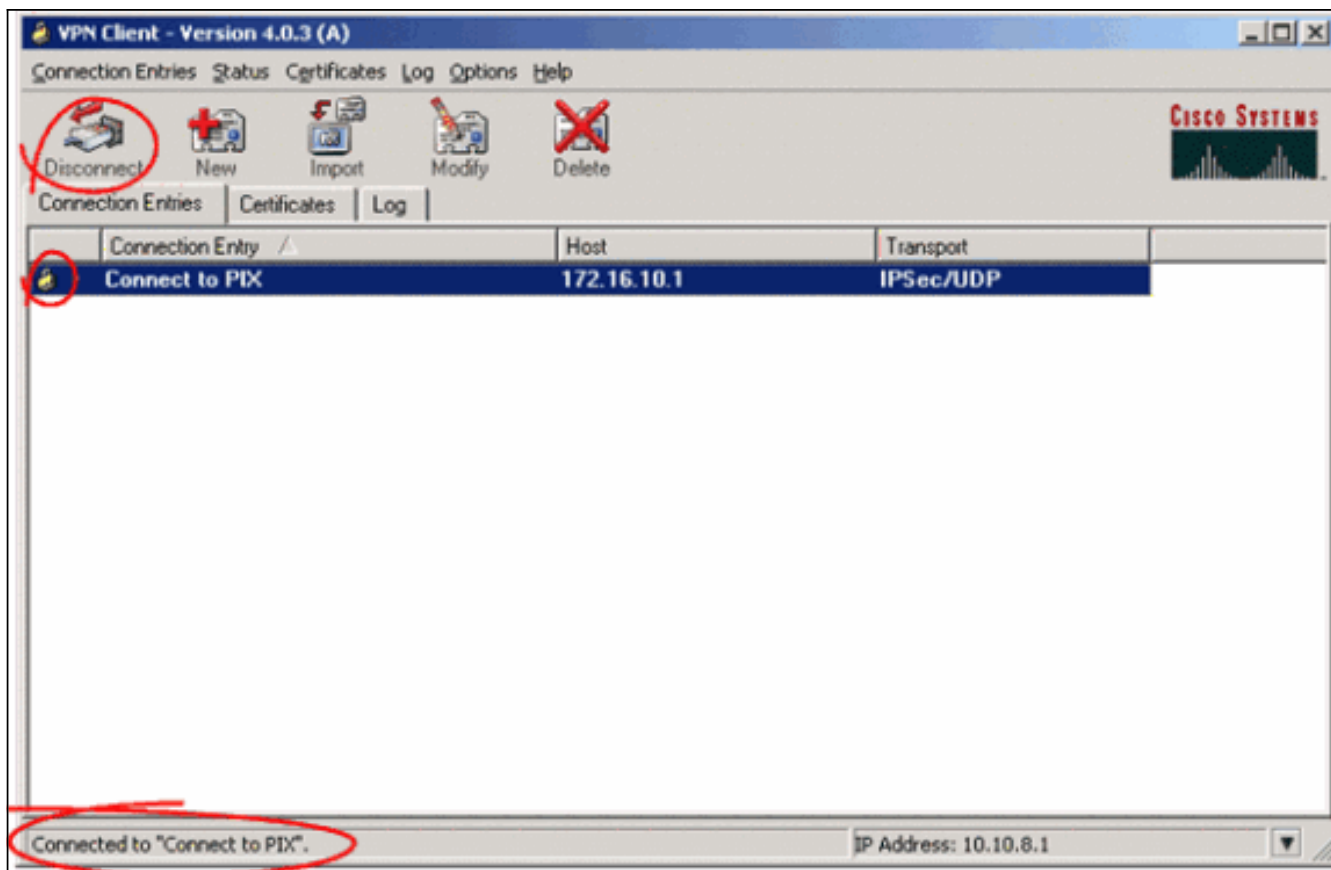
3. Para conectarse a la gateway mediante la nueva entrada de conexión, seleccione la entrada de conexión haciendo clic en ella una vez y luego haga clic en el icono **Connect**. Un doble clic en la entrada de conexión tiene el mismo efecto.



Verificación

En VPN Client, se indica una conexión establecida correctamente con el gateway remoto mediante estos elementos:

- Aparece un icono amarillo de candado cerrado contra la entrada de la conexión activa.
- El icono Conectar de la barra de herramientas (junto a la ficha Entradas de conexión) cambia a Desconectar.
- La línea de estado al final de la ventana muestra el estado como "Conectado" seguido del nombre de la entrada de conexión.



Nota: De forma predeterminada, una vez establecida la conexión, el VPN Client minimiza a un icono de bloqueo cerrado en la bandeja del sistema, en la esquina inferior derecha de la barra de tareas de Windows. Haga doble clic en el icono de bloqueo cerrado para hacer que la ventana VPN Client vuelva a ser visible.

En el Firewall PIX, estos comandos **show** se pueden utilizar para verificar el estado de las conexiones establecidas.

Nota: Ciertos comandos **show** son soportados por la [Herramienta Output Interpreter](#) (sólo para clientes registrados) , que le permite ver un análisis del resultado del comando [show](#).

- **show crypto ipsec sa**—Muestra todas las SAs IPsec actuales 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:
```

- **show crypto isakmp sa:** muestra el estado de ISAKMP SA generado entre peers.

```
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

Troubleshoot

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

Estos comandos debug pueden ayudar en la resolución de problemas con la configuración de VPN.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de ejecutar los comandos debug.

- **debug crypto isakmp:** muestra la SA ISAKMP que se genera y los atributos IPsec que se negocian. Durante la negociación ISAKMP SA, el PIX posiblemente puede descartar varias propuestas como "no aceptables" antes de que acepte una. Una vez que se haya acordado el ISAKMP SA, se negocian los atributos IPsec. Una vez más, es posible que se rechacen varias propuestas antes de que se acepte una, como se muestra en este resultado **debug**.

```
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.
```

- **debug crypto ipsec:** muestra información sobre las negociaciones SA de IPsec.

```
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 VPN Client puede conectarse exitosamente al PIX del sitio central usando AES. A veces se observa que, aunque el túnel VPN se establece correctamente, los usuarios no pueden realizar tareas comunes como hacer ping en los recursos de red, iniciar sesión en el dominio o navegar por el vecindario de la red. Hay más información disponible sobre la resolución de tales problemas en [Solución de problemas de vecindad de red de Microsoft 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](#)