PIX/ASA 7.x y superior: Ejemplo de Configuración de Túnel VPN PIX-to-PIX

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Diagrama de la red
Convenciones
Antecedentes
Configuración
Configuración de ASDM
Configuración CLI PIX
Túnel de reserva del sitio a localizar
Borre las asociaciones de seguridad (los SA)
Verificación
Troubleshooting
PFS
Acceso de administración
Comandos de Debug
Información Relacionada

Introducción

Este documento describe el procedimiento para configurar los túneles VPN entre dos firewalls PIX mediante ASDM (Cisco Adaptive Security Device Manager). ASDM es una herramienta de configuración basada en la aplicación diseñada para ayudarle a instalar, configurar y monitorear su firewall PIX con una GUI. Los firewalls PIX se colocan en dos sitios diferentes.

Un túnel se forma usando el IPSec. El IPSec es una combinación de estándares abiertos que proporcionen la confidencialidad de los datos, la integridad de los datos, y la autenticación del origen de los datos entre los peeres IPSec.

Nota: En PIX 7.1 y posterior, cambian al **comando sysopt connection permit-ipsec a la conexión permiso-VPN del sysopt**. Este comando permite que el tráfico que ingresa el dispositivo de seguridad a través de un túnel VPN y después se desencripta, desvíe las Listas de acceso de la interfaz. La directiva del grupo y por usuario las Listas de acceso de la autorización todavía se aplica al tráfico. Para inhabilitar esta característica, no utilice la **ninguna** forma de este comando. Este comando no es visible en la configuración CLI.

Refiera a PIX 6.x: Ejemplo de configuración del Túnel VPN PIX a PIX sencillo para aprender un

escenario más casi igual donde el dispositivo de seguridad del Cisco PIX funciona con la versión de software 6.x.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento especifica que este par inicia el primer intercambio propietario para determinar al par apropiado a quien conectar.

- Dispositivo de seguridad de la serie del Cisco PIX 500 con la versión 7.x y posterior
- Versión 5.x.and del ASDM más adelante

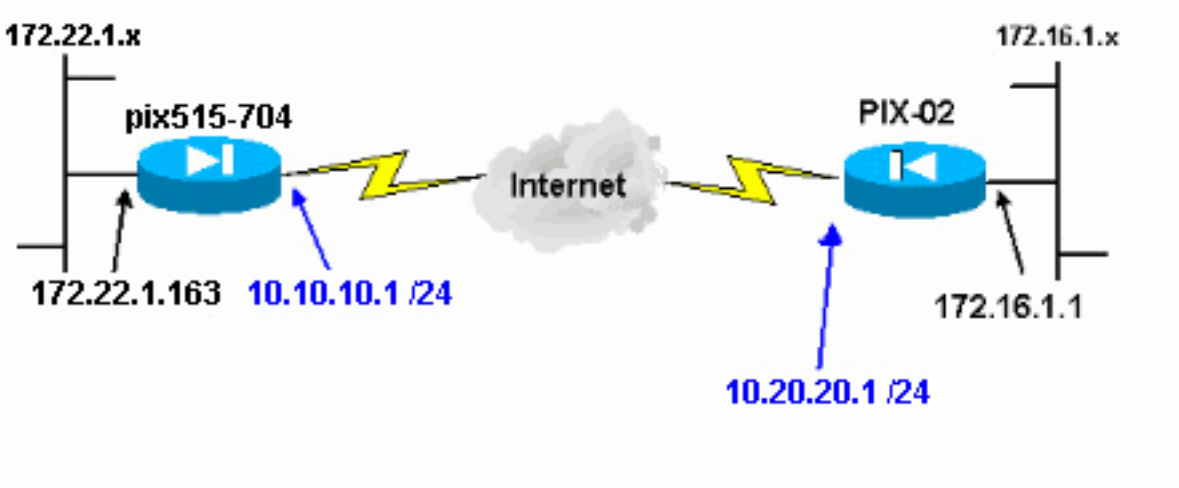
Nota: Consulte Cómo Permitir el Acceso HTTPS para el ASDM para que el ASA sea configurado por el ASDM.

Nota: La versión 7.x/8.x de las 5500 Series ASA funciona con el mismo software considerado en la versión de PIX 7.x/8.x. Las configuraciones en este documento son aplicables a ambas líneas de producto.

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El IPSec Negotiation se puede analizar en cinco pasos, e incluye dos fases del Internet Key Exchange (IKE).

1. Un túnel IPsec es iniciado por el tráfico interesante. El tráfico se considera interesante cuando viaja entre los peeres IPSec.
2. En la fase 1 IKE, los peeres IPSec negocian la directiva establecida de la asociación de seguridad IKE (SA). Una vez que se autentican los pares, se crea un túnel seguro por medio de la Asociación de Seguridad en Internet y del Protocolo de administración de clave (ISAKMP).
3. En la fase 2 IKE, los peeres IPSec utilizan el túnel seguro y autenticado para negociar IPSec SA transforman. La negociación de la política compartida determina cómo se establece el túnel IPsec.
4. Se crea el túnel IPsec y los datos se transfieren entre los peeres IPSec basados en los parámetros de IPSec configurados en el IPSec transforman los conjuntos.
5. El túnel IPsec termina cuando se borra el SA de IPSec o cuando expira su curso de la vida.**Nota:** El IPSec Negotiation entre los dos PIXes falla si los SA en ambas fases IKE no hacen juego en los pares.

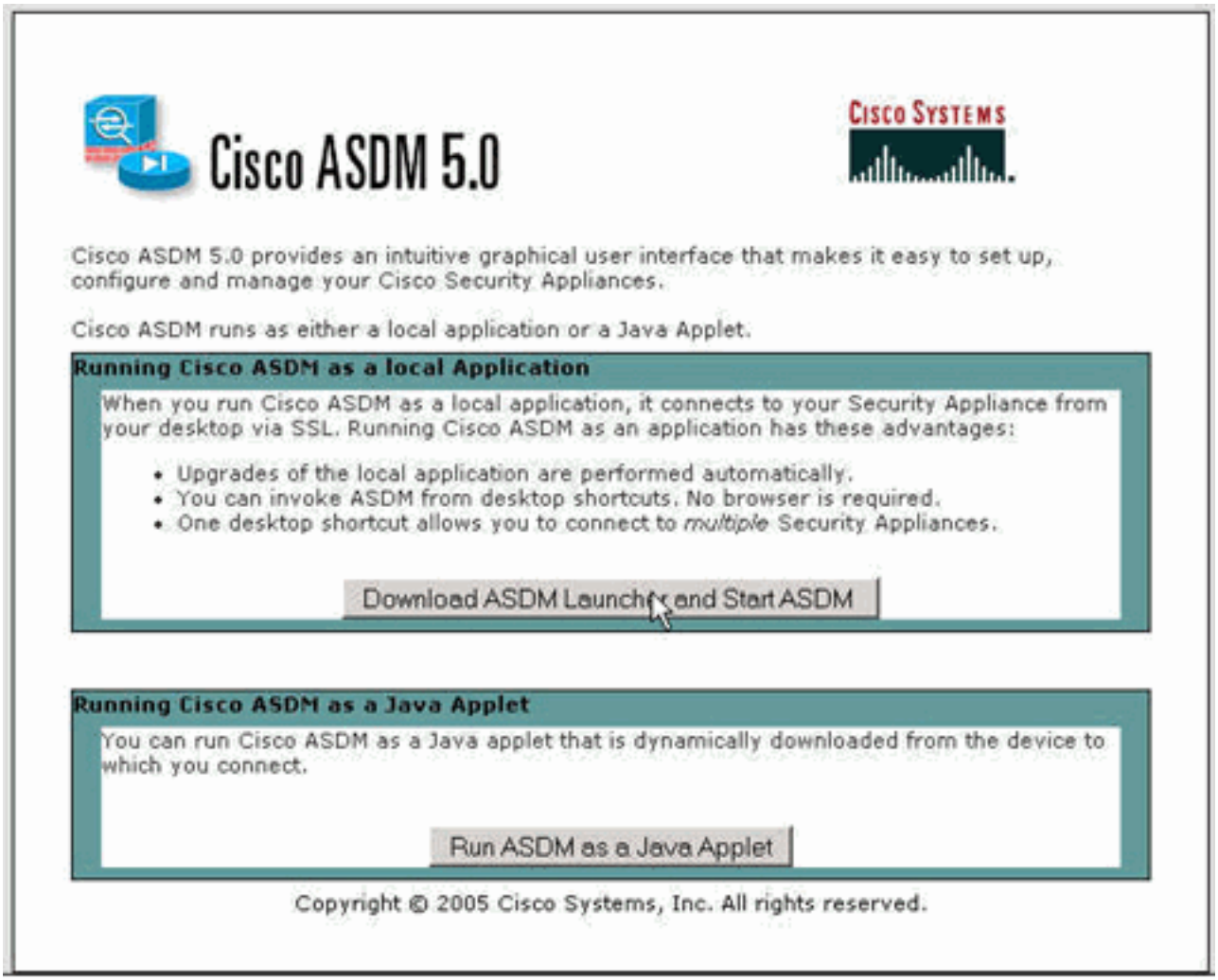
Configuración

- Configuración de ASDM
- Configuraciones CLI PIX

Configuración de ASDM

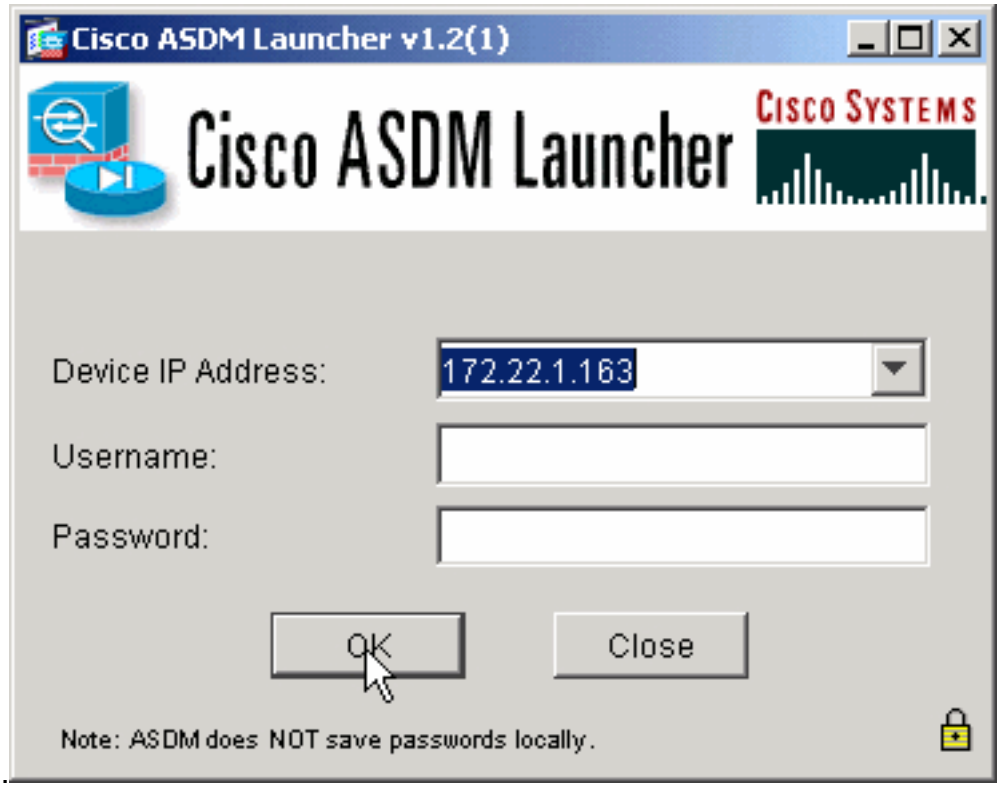
Complete estos pasos:

1. Abra su **<Inside_IP_Address_of_PIX> de https:// del** navegador y del tipo para acceder el ASDM en el PIX.Esté seguro de autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad de certificados SSL. Nombre de usuario predeterminado y la contraseña son ambos espacio en blanco.El PIX presenta esta ventana para permitir la descarga de la aplicación ASDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en los subprogramas
   java.

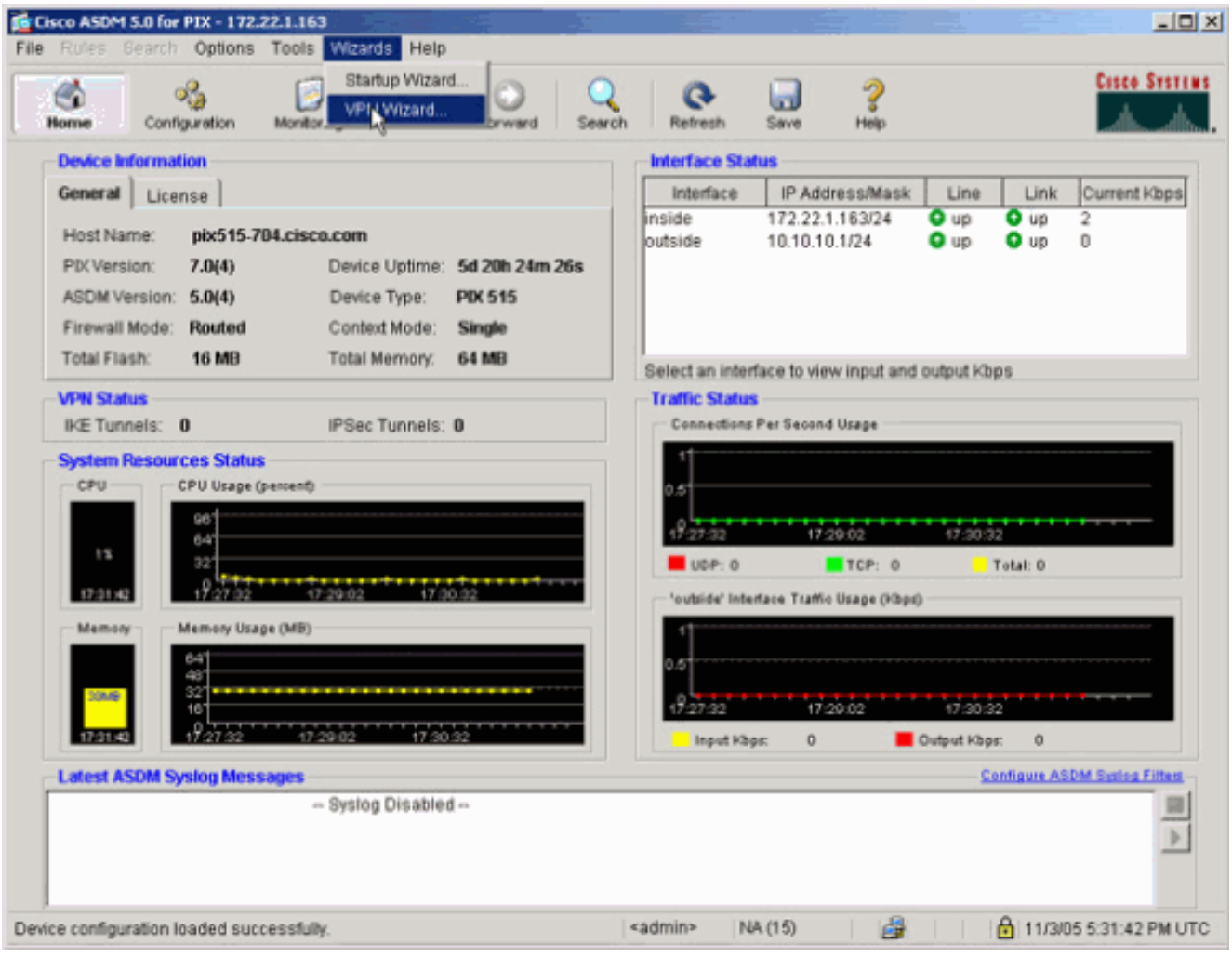


2. Haga clic el **activador de ASDM de la descarga y comience el ASDM** para descargar el instalador para la aplicación ASDM.
3. Una vez que el activador de ASDM descarga, siga los prompts para instalar el software y funcionar con el Cisco ASDM launcher.
4. Ingrese el IP Address para la interfaz que usted configuró con el **HTTP -** ordene y un nombre de usuario y contraseña si usted especificó uno.Este ejemplo utiliza el nombre de usuario y contraseña en blanco

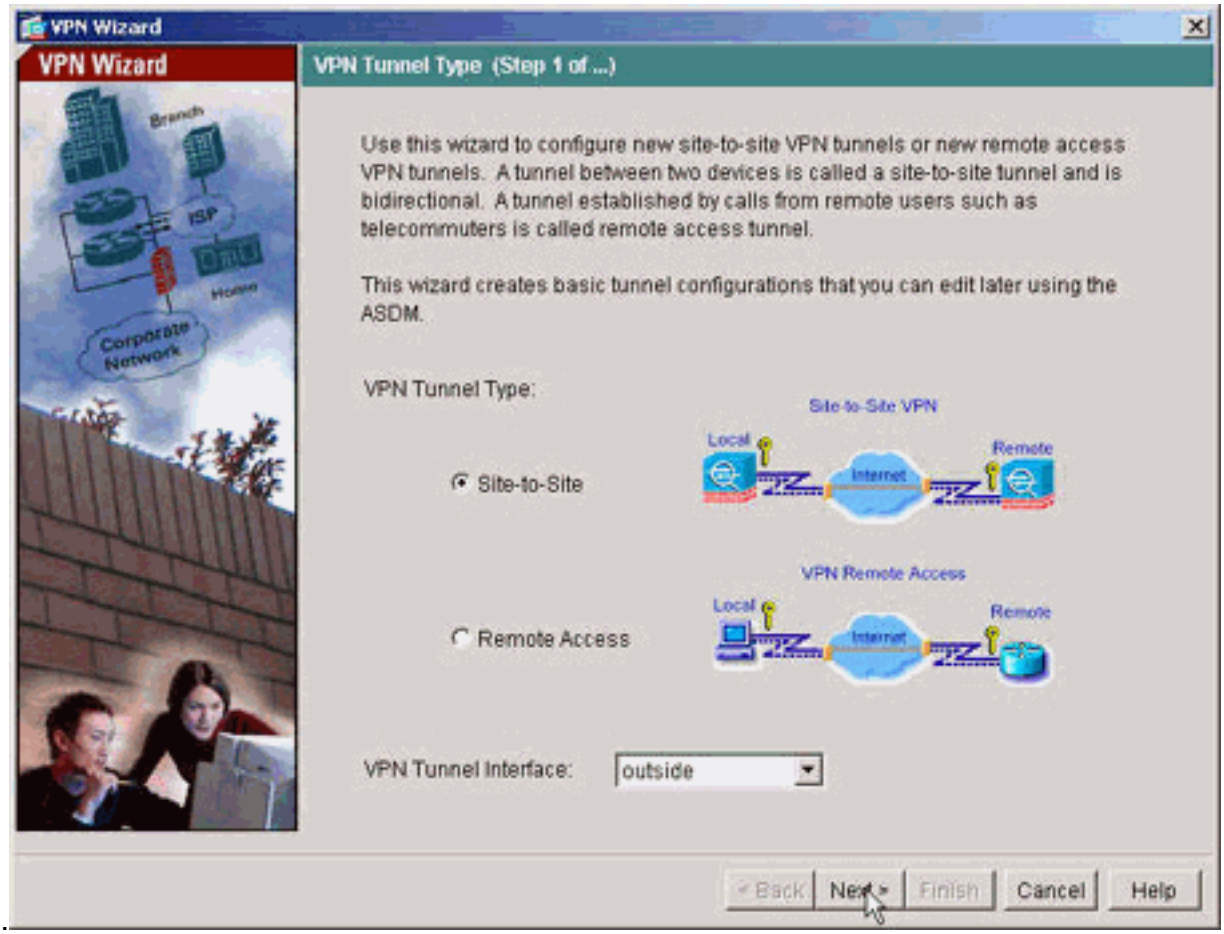
predeterminado.



5. Funcione con al Asistente VPN una vez que la aplicación ASDM conecta con el PIX.

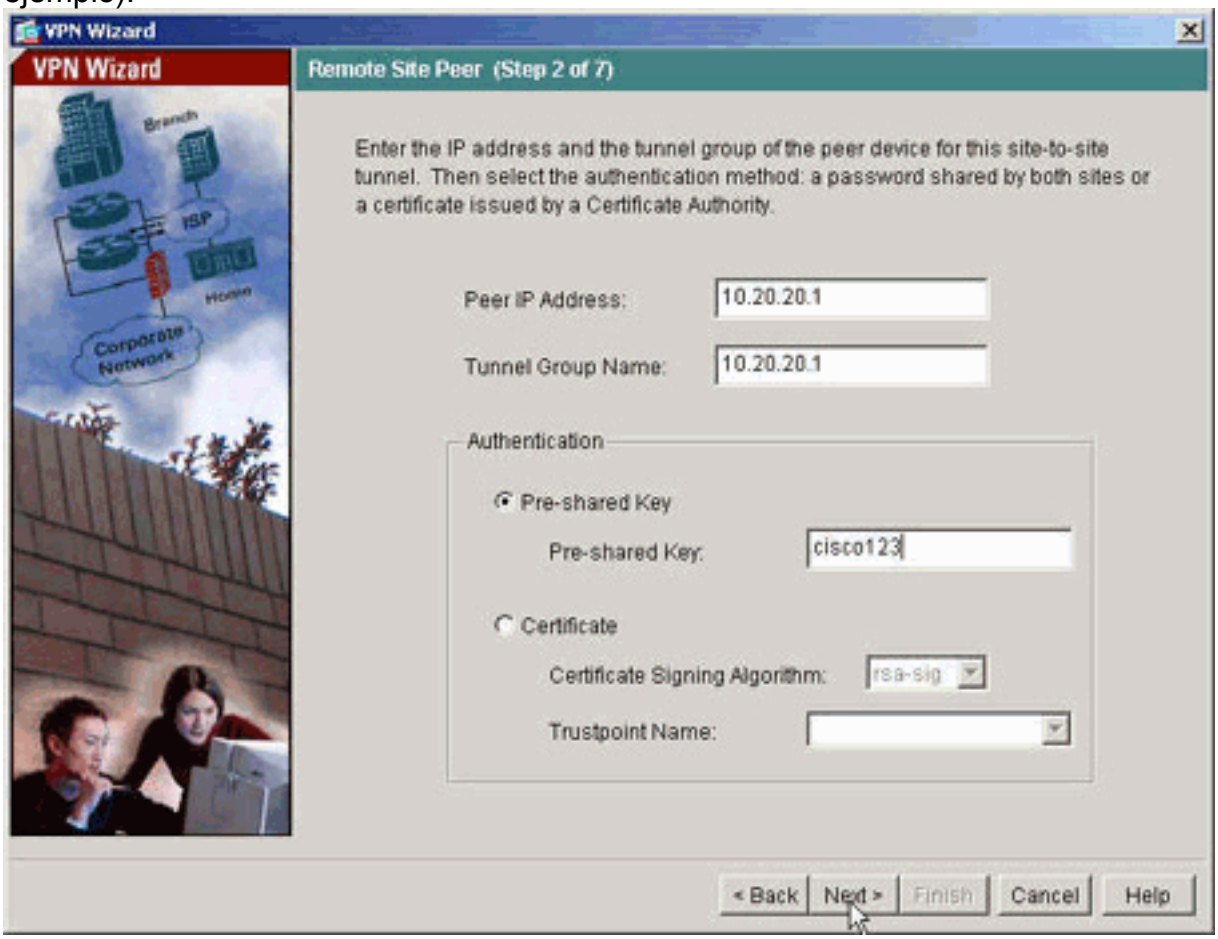


6. Elija el tipo de túnel del **VPN de sitio a**



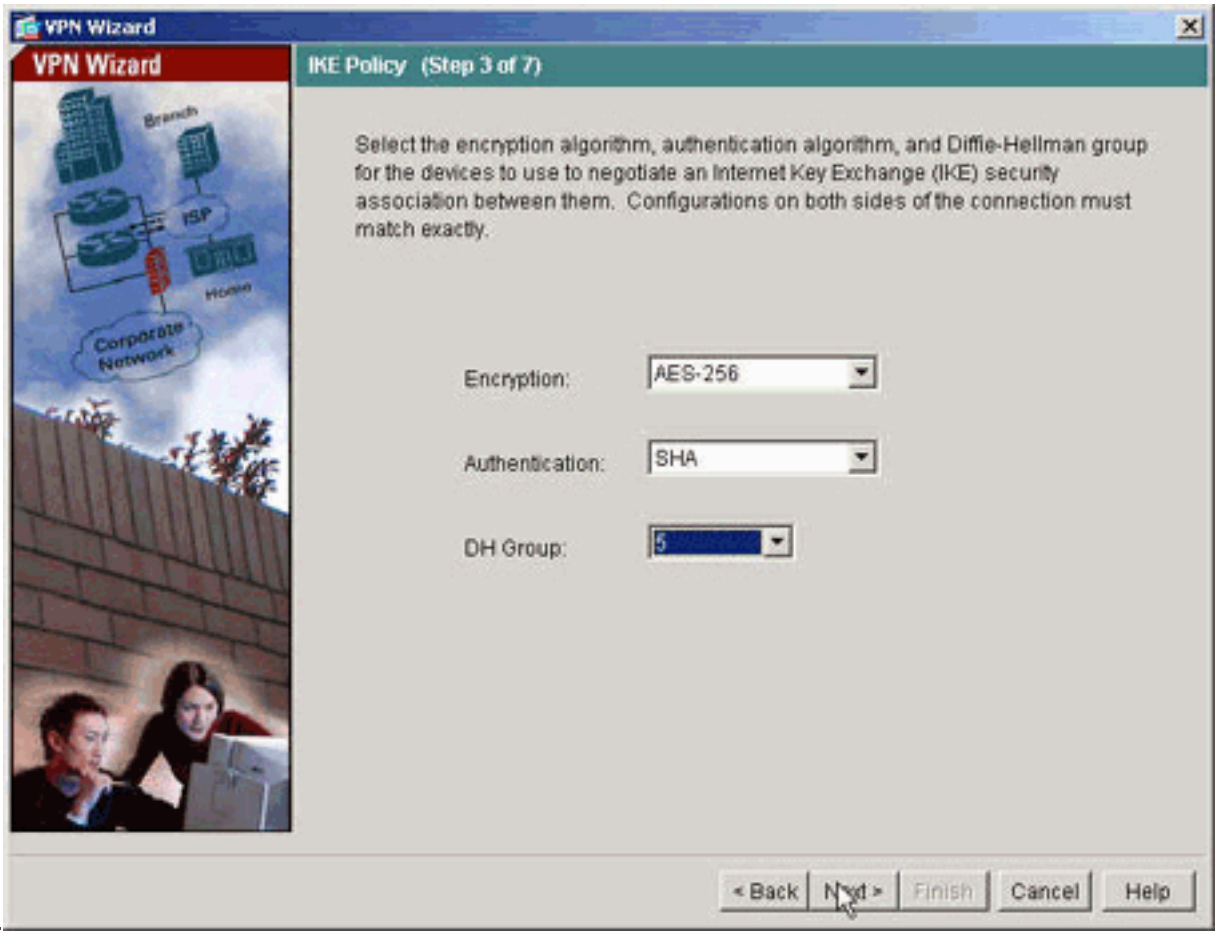
sitio.

7. Especifique el IP Address externo del peer remoto. Ingrese la información de autenticación para utilizar (clave previamente compartida en este ejemplo).



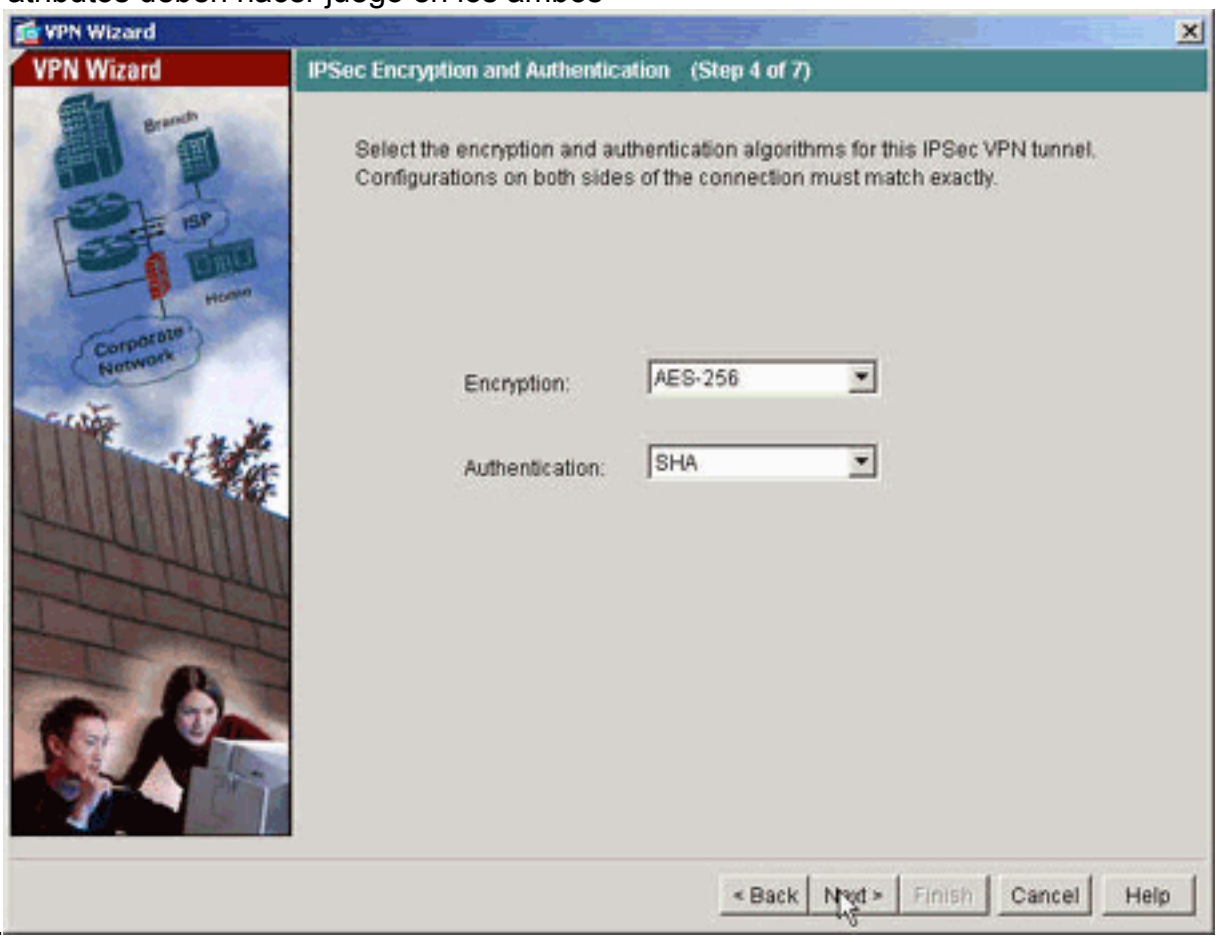
8. Especifique los atributos para utilizar para el IKE, también conocido como “fase el 1". Estos

atributos deben ser lo mismo a ambos lados del



túnel.

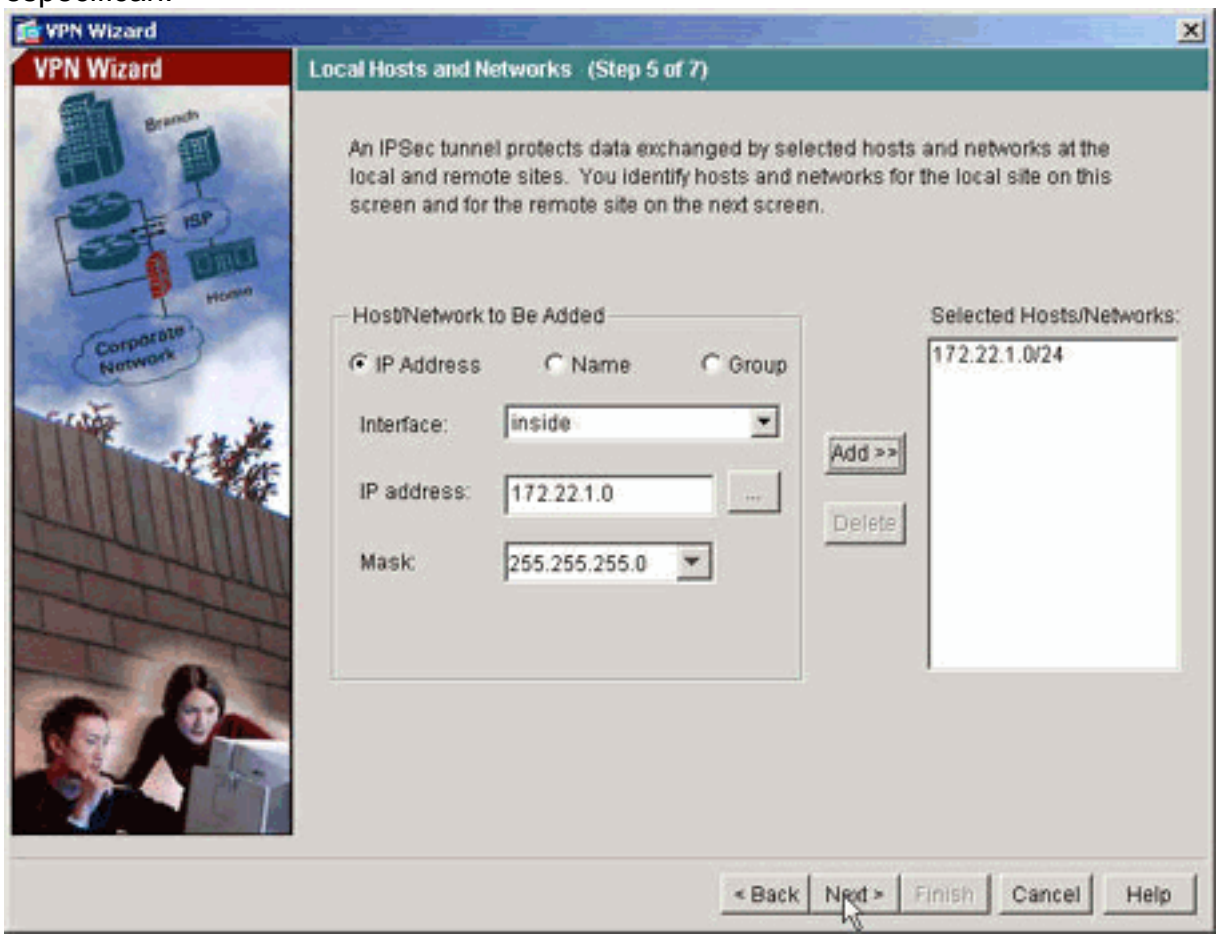
9. Especifique los atributos para utilizar para el IPSec, también conocido como “fase el 2". Estos atributos deben hacer juego en los ambos



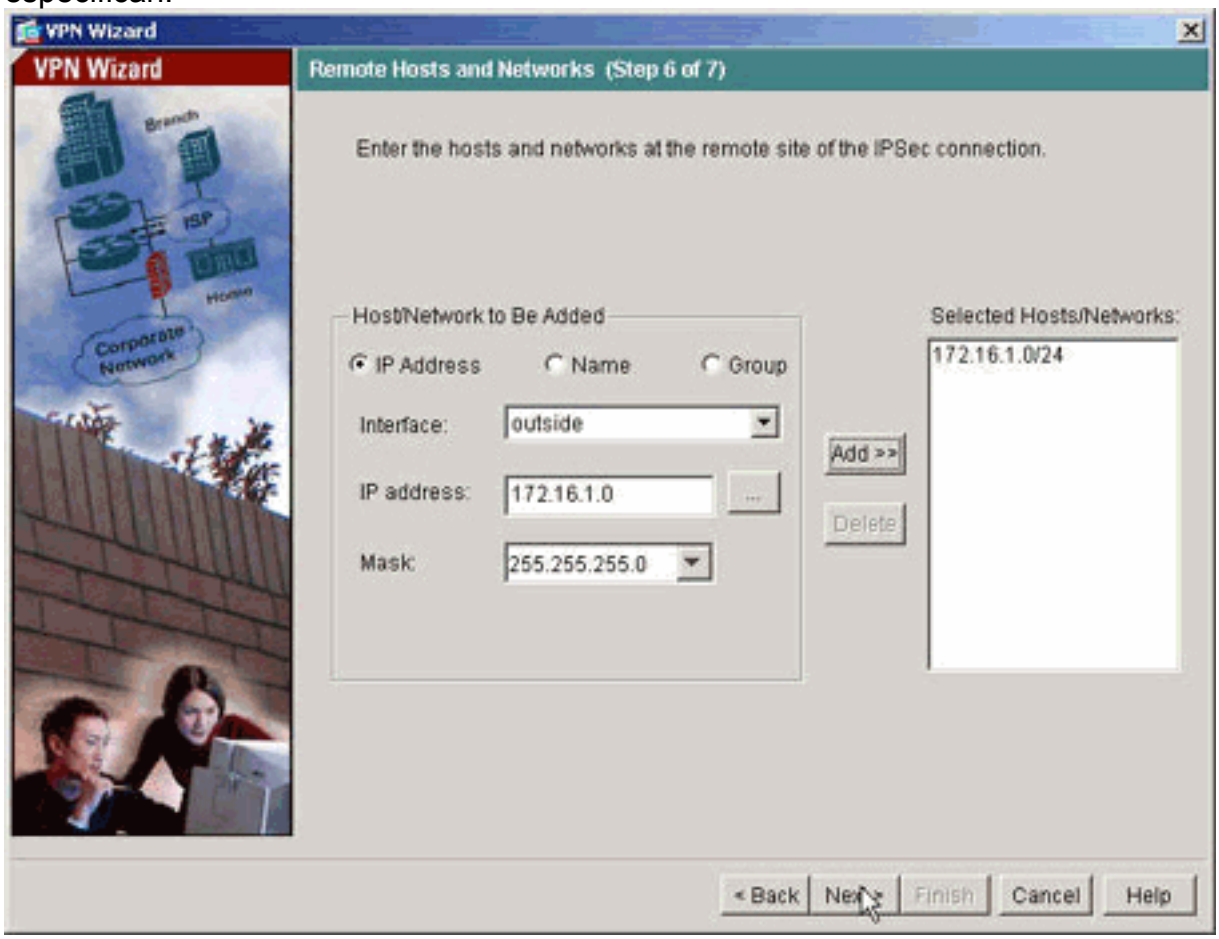
lados.

10. Especifique a los host cuyo tráfico se debe permitir pasar a través del túnel VPN. En este

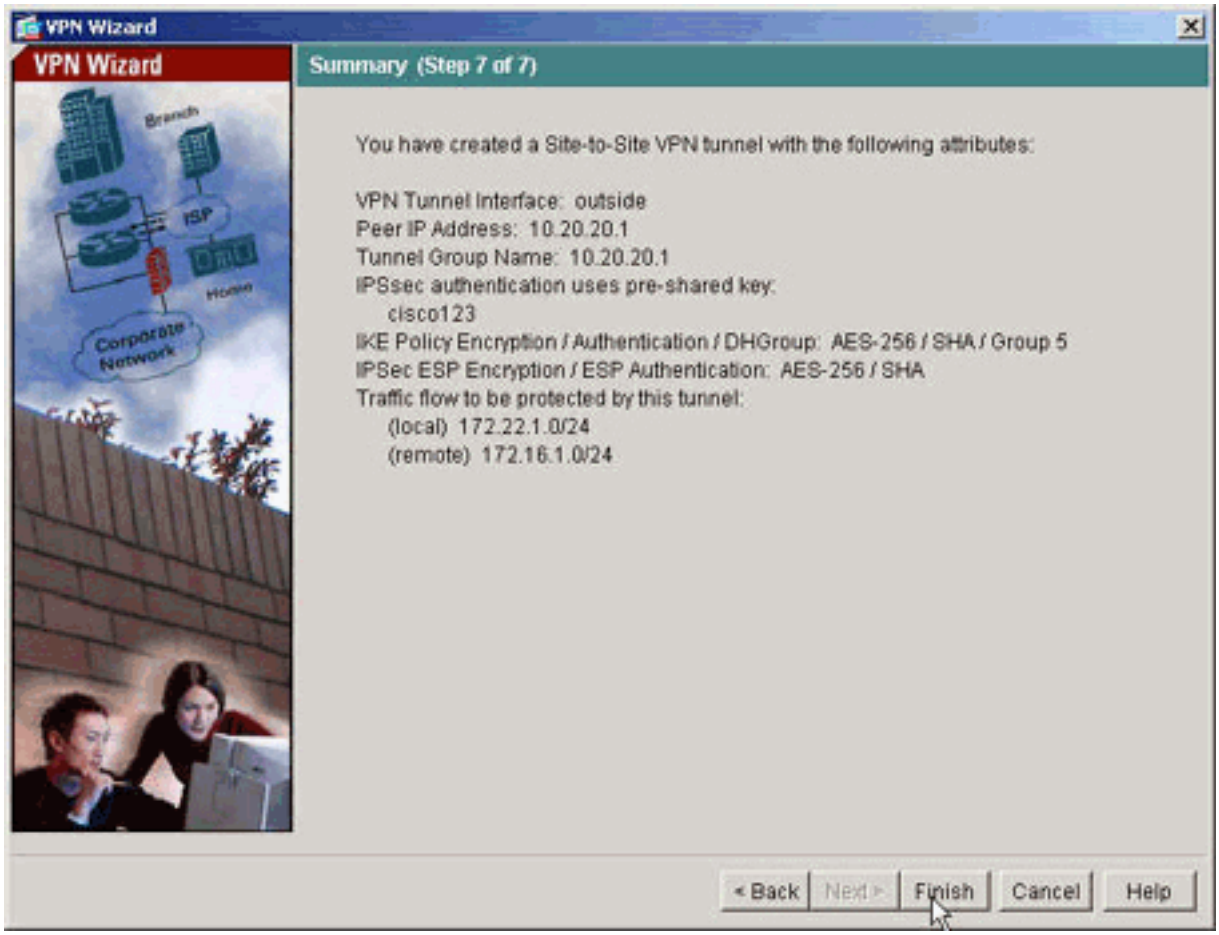
paso, los host locales a pix515-704 se especifican.



11. Los host y las redes en el lado remoto del túnel se especifican.



12. Los atributos definidos por el Asistente VPN se visualizan en este resumen. Compruebe la configuración con minuciosidad y el clic en Finalizar cuando le satisfacen las configuraciones está correcto.



Configuración CLI PIX

pix515-704

```
pixfirewall#show run : Saved PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 ip
address 10.10.10.1 255.255.255.0 !--- Configure the
outside interface. ! interface Ethernet1 nameif inside
security-level 100 ip address 172.22.1.163 255.255.255.0
!--- Configure the inside interface. ! !-- Output
suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list inside_nat0_outbound
extended permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
command. !--- This prevents traffic which matches the
access list from undergoing !--- network address
translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and !--- sent
across the VPN tunnel. This ACL is intentionally !---
the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration. access-list outside_cryptomap_20 extended
permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
```

```
(outside_cryptomap_20) is used with the crypto map !--- outside_map to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is intentionally the same as (inside_nat0_outbound). !--- Two separate access lists should always be used in this configuration. pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image flash:/asdm-511.bin !--- Enter this command to specify the location of the ASDM image. asdm history enable arp timeout 14400 nat (inside) 0 access-list inside_nat0_outbound !--- NAT 0 prevents NAT for networks specified in the ACL inside_nat0_outbound. route outside 0.0.0.0 0.0.0.0 10.10.10.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable !--- Enter this command in order to enable the HTTPS server for ASDM. http 172.22.1.1 255.255.255.255 inside !--- Identify the IP addresses from which the security appliance !--- accepts HTTPS connections. no snmp-server location no snmp-server contact !--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac !--- Define the transform set for Phase 2. crypto map outside_map 20 match address outside_cryptomap_20 !--- Define which traffic should be sent to the IPsec peer. crypto map outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec peer crypto map outside_map 20 set transform-set ESP-AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-256-SHA" !--- to be used with the crypto map entry "outside_map". crypto map outside_map interface outside !--- Specifies the interface to be used with !--- the settings defined in this configuration. !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- Policy 65535 is included in the config by default. !--- The configuration commands here define the Phase !--- 1 policy parameters that are used. isakmp enable outside isakmp policy 10 authentication pre-share isakmp policy 10 encryption aes-256 isakmp policy 10 hash sha isakmp policy 10 group 5 isakmp policy 10 lifetime 86400 isakmp policy 65535 authentication pre-share isakmp policy 65535 encryption 3des isakmp policy 65535 hash sha isakmp policy 65535 group 2 isakmp policy 65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-l2l !--- In order to create and manage the database of connection-specific records !--- for ipsec-l2l–IPsec (LAN-to-LAN) tunnels, use the tunnel-group !--- command in global configuration mode. !--- For L2L connections the name of the tunnel group MUST be the IP !--- address of the IPsec peer. tunnel-group 10.20.20.1 ipsec-attributes pre-shared-key * !--- Enter the pre-shared-key in order to configure the authentication method. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map global_policy class inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end
```

PIX-02

```
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.20.20.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on pix515-704. access-list
outside_cryptomap_20 extended permit ip 172.16.1.0
255.255.255.0 172 .22.1.0 255.255.255.0 !--- Note that
this ACL is a mirror of the outside_cryptomap_20 !---
ACL on pix515-704. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image flash:/asdm-511.bin
no asdm history enable arp timeout 14400 nat (inside) 0
access-list inside_nat0_outbound timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
http server enable http 0.0.0.0 0.0.0.0 inside no snmp-
server location no snmp-server contact crypto ipsec
transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20 crypto map outside_map 20 set peer
10.10.10.1 crypto map outside_map 20 set transform-set
ESP-AES-256-SHA crypto map outside_map interface outside
isakmp enable outside isakmp policy 10 authentication
pre-share isakmp policy 10 encryption aes-256 isakmp
policy 10 hash sha isakmp policy 10 group 5 isakmp
policy 10 lifetime 86400 tunnel-group 10.10.10.1 type
ipsec-l2l tunnel-group 10.10.10.1 ipsec-attributes pre-
shared-key * telnet timeout 5 ssh timeout 5 console
timeout 0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:6774691244870705f858ad4e9b810874 : end
pixfirewall#
```

Túnel de reserva del sitio a localizar

Para especificar el Tipo de conexión para la característica de reserva del sitio a localizar para esta entrada de correspondencia de criptografía, utilice el comando **determinado del Tipo de conexión de la correspondencia de criptografía** en el modo de configuración global. No utilice la `ninguna` forma de este comando para volver a la configuración predeterminada.

Sintaxis:

```
crypto map map-name seq-num set connection-type {answer-only | originate-only | bidirectional}
```

- **respuesta-solamente** — Esto especifica que este par responde solamente a las conexiones entrantes IKE primero durante el intercambio propietario inicial para determinar al par apropiado a quien conectar.
- **bidireccional** — Esto especifica que este par puede validar y originar las conexiones basadas en esta entrada de correspondencia de criptografía. Éste es el tipo de conexión predeterminada para todas las conexiones del sitio a localizar.
- **origine-solamente** — Esto especifica que este par inicia el primer intercambio propietario para determinar al par apropiado a quien conectar.

El comando **determinado del Tipo de conexión de la correspondencia de criptografía** especifica los Tipos de conexión para la característica de reserva del LAN a LAN. Permite que especifiquen a los pares del backup múltiple en un extremo de la conexión. Esta característica trabaja solamente entre estas Plataformas:

- Dos dispositivos de seguridad de las 5500 Series de Cisco ASA
- Dispositivo de seguridad de las 5500 Series de Cisco ASA y un Cisco VPN 3000 Concentrator
- Dispositivo de seguridad de las 5500 Series de Cisco ASA y un dispositivo de seguridad que ejecuta la versión de software 7.0 del dispositivo de seguridad del Cisco PIX o más adelante

Para configurar una conexión de LAN a LAN de reserva, Cisco recomienda que usted configura un extremo de la conexión como origina-solamente con la palabra clave del `originar-solamente`, y el extremo con los pares del backup múltiple como respuesta-solamente con la palabra clave de la `respuesta-solamente`. En el extremo del originar-solamente, utilice el **comando set peer de la correspondencia de criptografía** para ordenar la prioridad de los pares. El dispositivo de seguridad del originar-solamente intenta negociar con el primer par en la lista. Si no responde ese par, el dispositivo de seguridad funciona su manera abajo de la lista hasta que o responda un par o no hay pares en la lista.

Cuando está configurado de esta manera, el par del originar-solamente intenta inicialmente establecer un túnel propietario y negociar con un par. Después de eso, cualquier par puede establecer una conexión de LAN a LAN normal y los datos de cualquier extremo pueden iniciar la conexión del túnel.

Nota: Si usted configuró el VPN con los IP Addresses del peer múltiple para una entrada crypto, el VPN consigue establecido con el IP del backup peer una vez que va el peer primario abajo. Sin embargo, una vez que se vuelve el peer primario, el VPN no se apropia al IP Address principal. Usted debe borrar manualmente el SA existente para reinitiate la negociación VPN para cambiarla al IP Address principal. Mientras que la conclusión dice, el VPN se apropia no se soporta en el túnel del sitio a localizar.

Tipos de conexión de LAN a LAN de reserva soportados

Lado remoto	Lado central
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

Ejemplo:

Este ejemplo, ingresado en el modo de configuración global, configura el **mymap de la correspondencia de criptografía** y fija el Tipo de conexión *para originar-solamente*.

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

Borre las asociaciones de seguridad (los SA)

En el modo del privilegio del PIX, utilice el siguiente los comandos:

- **clear [crypto] ipsec sa** — Borra el IPSec activo SA. La palabra clave crypto es opcional.
- **clear [crypto] isakmp sa** — Borra el IKE activo SA. La palabra clave crypto es opcional.

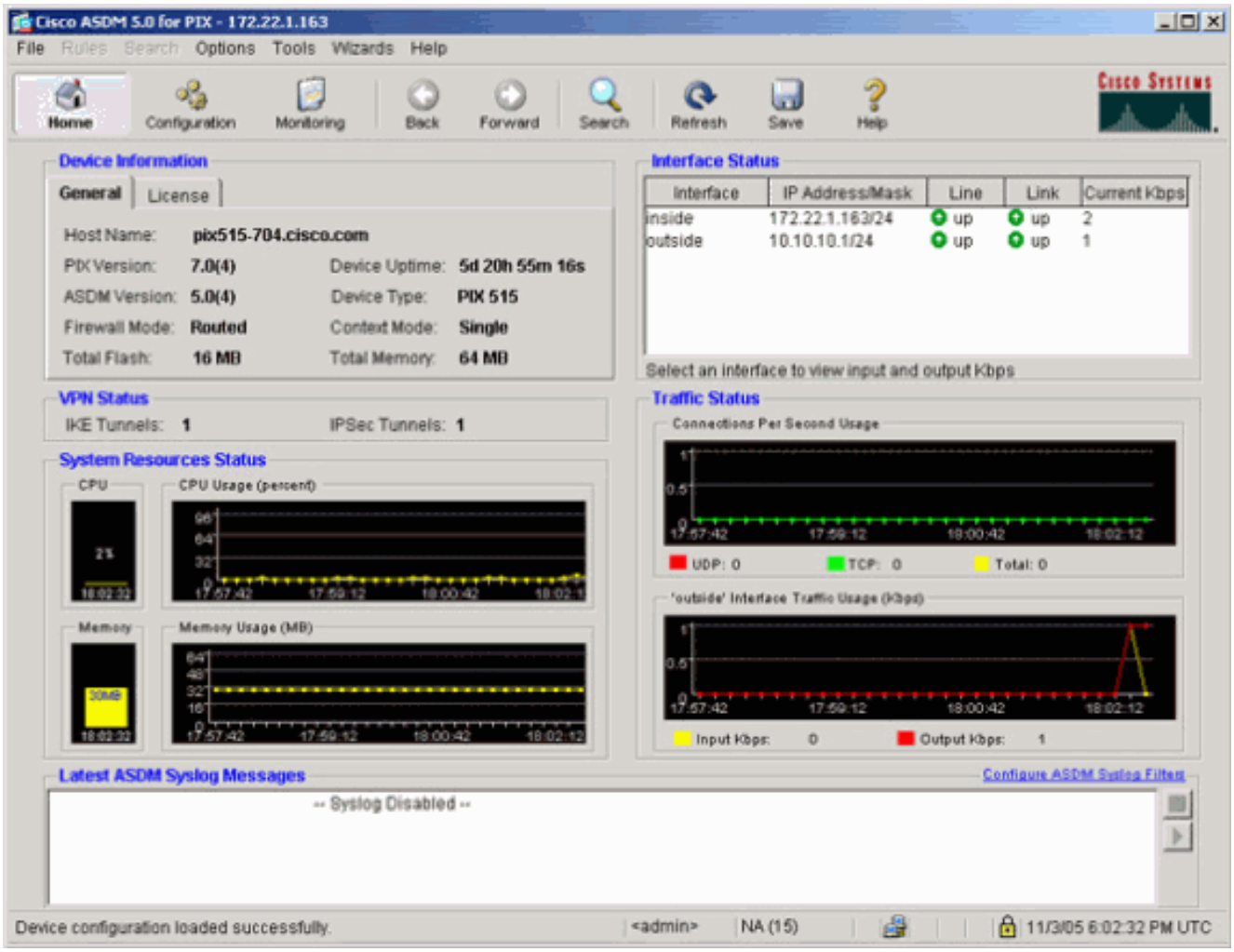
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

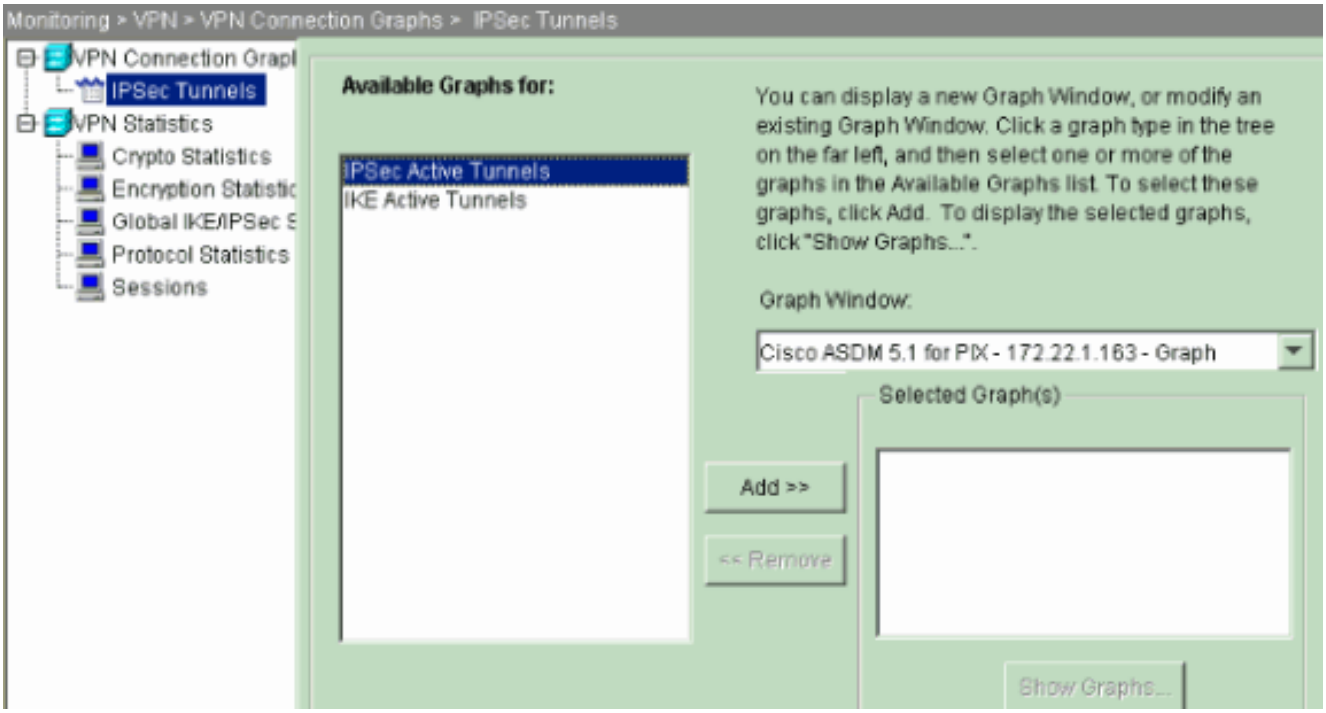
La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Si hay tráfico interesante al par, el túnel se establece entre pix515-704 y el PIX-02.

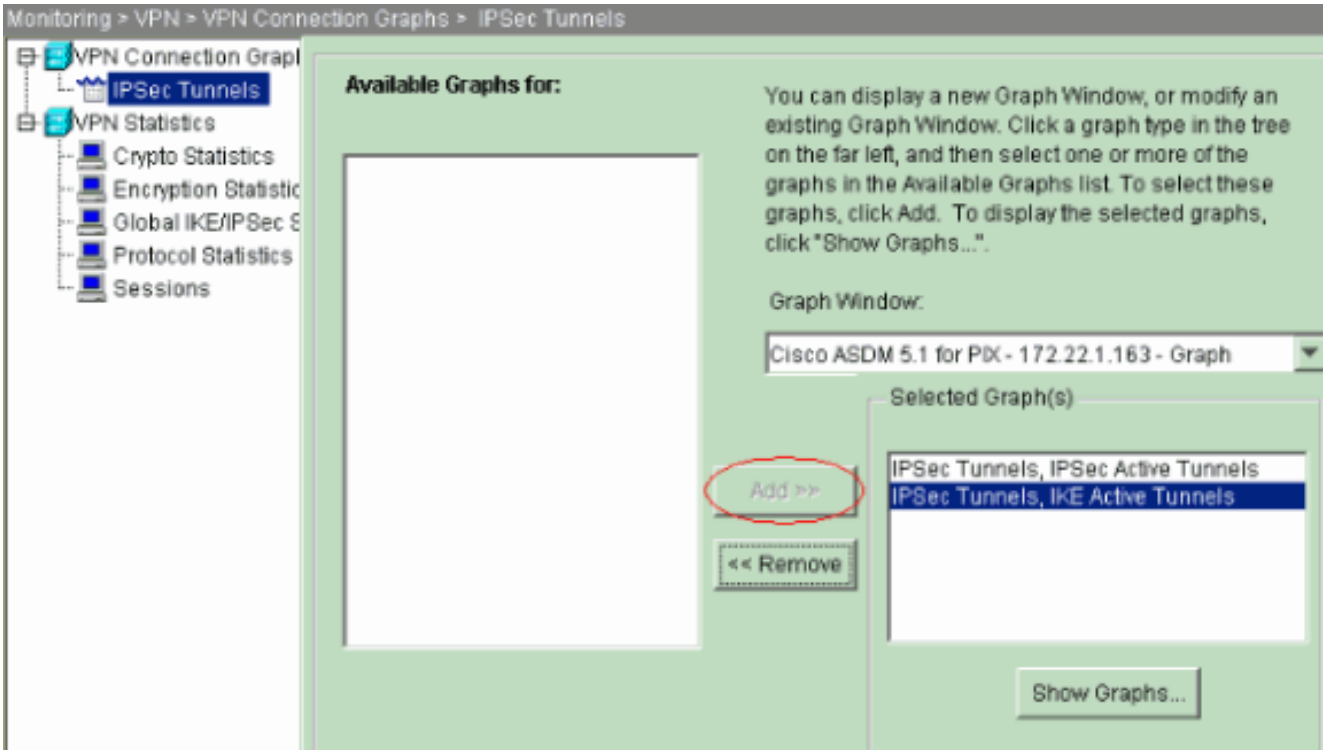
1. Vea el estado del VPN bajo **hogar** en el ASDM para verificar la formación del túnel.



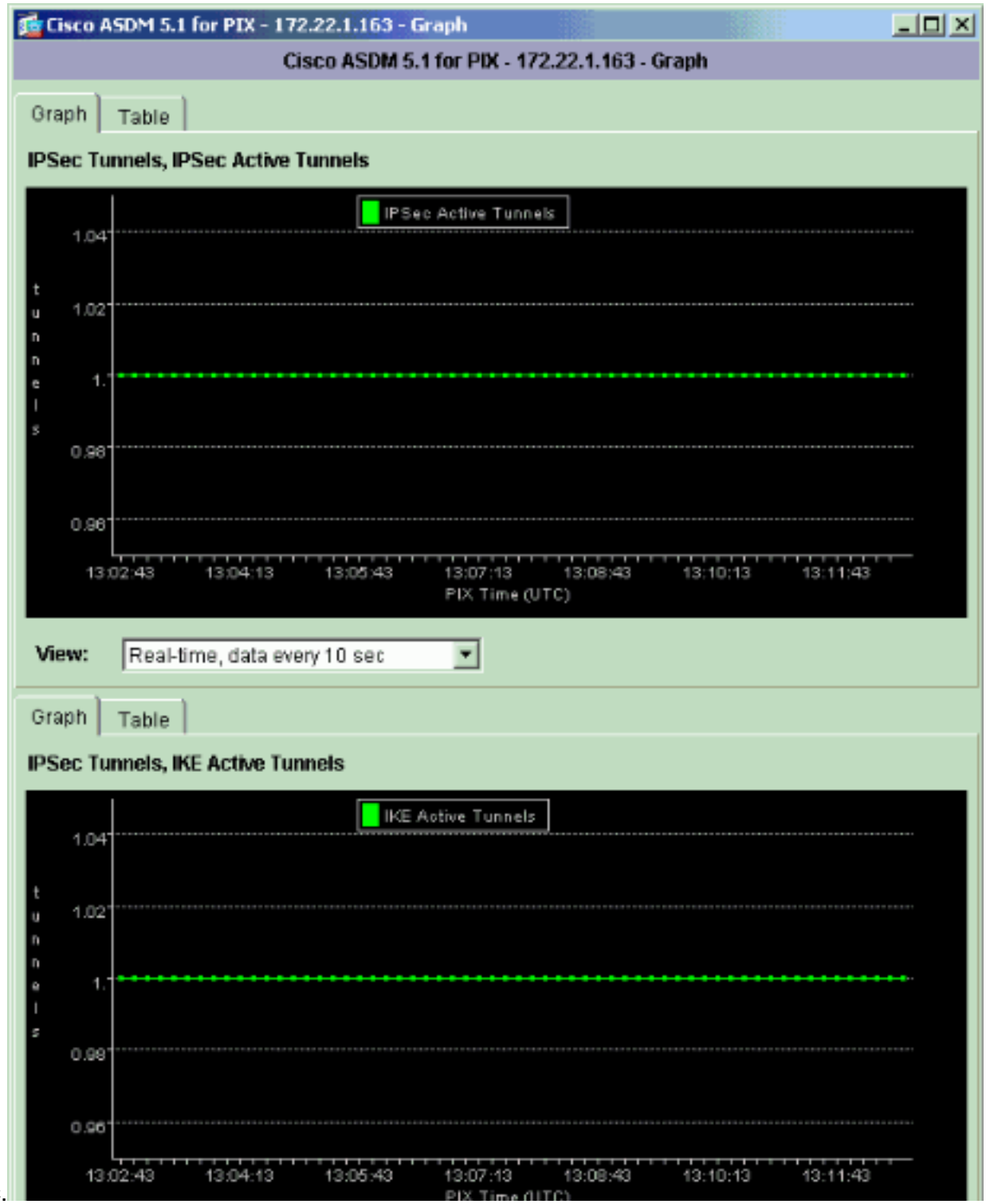
2. Elija la **supervisión > el VPN > la conexión VPN representa gráficamente > los túneles IPsec** para verificar los detalles sobre el establecimiento del túnel.



3. El tecleo **agrega** para seleccionar los gráficos disponibles para ver en la ventana del gráfico.

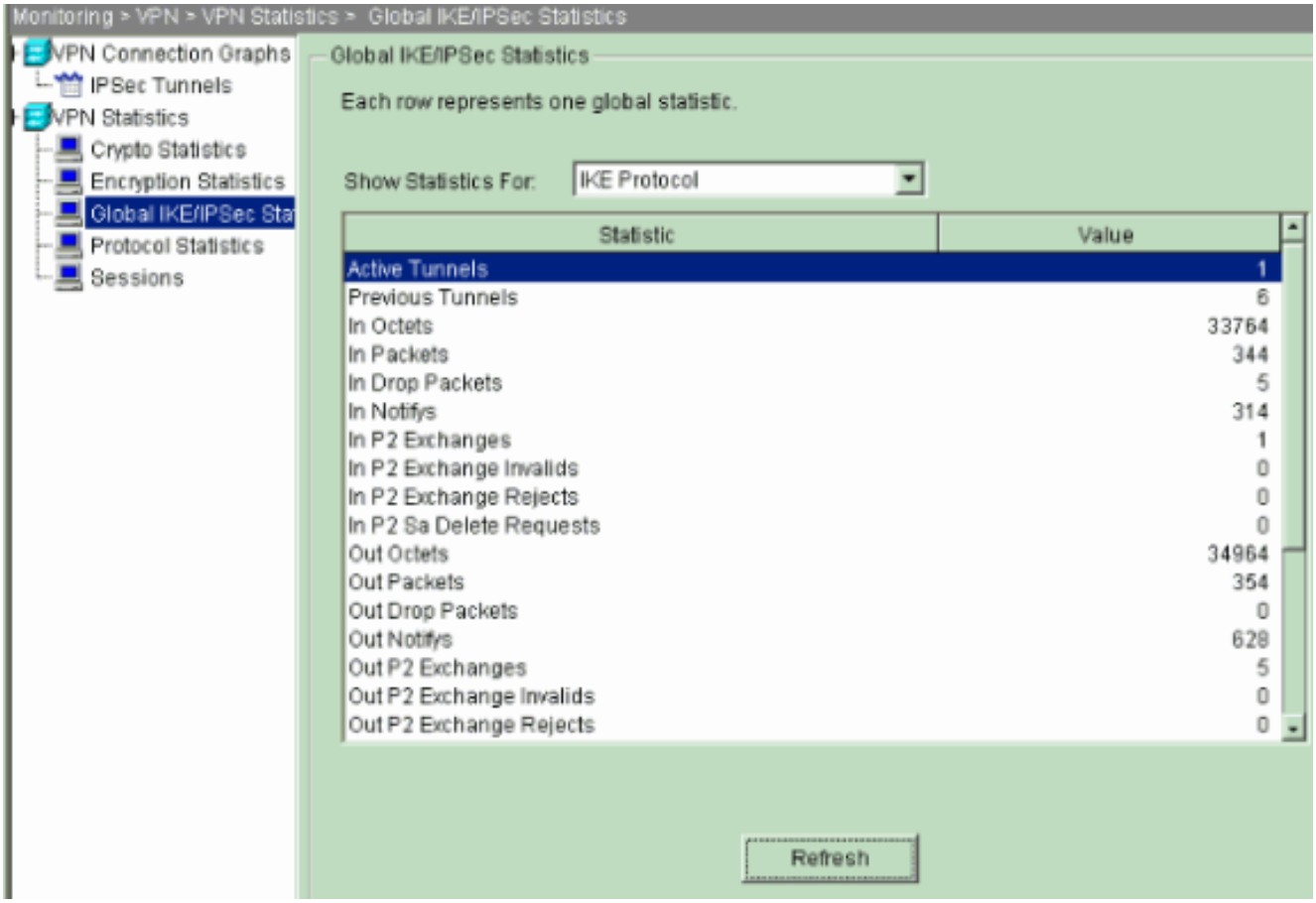


4. Haga clic los **gráficos de la demostración** para ver los gráficos de los túneles activos IKE y del



IPSec.

5. Elija la **supervisión > el VPN > los VPN statistics (Estadísticas de la VPN) > las estadísticas globales IKE/IPSec** para saber sobre la información estadística del túnel VPN.



Usted puede también verificar la formación de túneles usando el CLI. Publique el **comando show crypto isakmp sa** de marcar la formación de túneles y de publicar el **comando show crypto ipsec sa** de observar el número de paquetes encapsulado, cifrado, y así sucesivamente.

pix515-704

```
pixfirewall(config)#show crypto isakmp sa Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey
SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.20.20.1
Type : L2L Role : initiator Rekey : no State : MM_ACTIVE
```

pix515-704

```
pixfirewall(config)#show crypto ipsec sa interface:
outside Crypto map tag: outside_map, seq num: 20, local
addr: 10.10.10.1 access-list outside_cryptomap_20 permit
ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
local ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 10.20.20.1 #pkts encaps: 20, #pkts
encrypt: 20, #pkts digest: 20 #pkts decaps: 20, #pkts
decrypt: 20, #pkts verify: 20 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 20, #pkts comp
failed: 0, #pkts decomp failed: 0 #send errors: 0, #recv
errors: 0 local crypto endpt.: 10.10.10.1, remote crypto
endpt.: 10.20.20.1 path mtu 1500, ipsec overhead 76,
media mtu 1500 current outbound spi: 44532974 inbound
esp sas: spi: 0xA87AD6FA (2826622714) transform: esp-
aes-256 esp-sha-hmac in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (3824998/28246) IV
size: 16 bytes replay detection support: Y outbound esp
sas: spi: 0x44532974 (1146300788) transform: esp-aes-256
esp-sha-hmac in use settings ={L2L, Tunnel, } slot: 0,
conn_id: 1, crypto-map: outside_map sa timing: remaining
```

```
key lifetime (kB/sec): (3824998/28245) IV size: 16 bytes
replay detection support: Y
```

Troubleshooting

PFS

En las negociaciones de IPSec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior. El permiso o la neutralización PFS en ambos los peeres de túnel, si no el túnel IPsec L2L no se establece en el PIX/ASA.

PFS se inhabilita de forma predeterminada. Para habilitar el PFS utilice los **pfs** ordenan con la palabra clave del *permiso* en el modo de configuración de la grupo-directiva. Para inhabilitar PFS, ingrese la palabra clave disable (inhabilitar).

```
hostname(config-group-policy)#pfs {enable | disable}
```

Para quitar el atributo PFS de la configuración en ejecución, ingrese la forma no de este comando. Una política de grupo puede heredar un valor para PFS de otra política de grupo. Ingrese la forma no de este comando para evitar heredar un valor.

```
hostname(config-group-policy)#no pfs
```

Acceso de administración

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

La interfaz interior de PIX no se puede pingear del otro extremo del túnel a menos que el comando del gestión-accesso se configure en el modo global configuration.

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access
inside
```

Comandos de Debug

Nota: Consulte información importante en los comandos debug antes de ejecutar los comandos debug.

isakmp del debug crypto — La información del debug de las visualizaciones sobre las conexiones del IPSec, y muestra el primer conjunto de los atributos que se niegan debido a las incompatibilidades en los ambos extremos.

debug crypto isakmp

```
pixfirewall(config)#debug crypto isakmp 7 Nov 27
12:01:59 [IKEv1 DEBUG]: Pitcher: received a key acquire
message, spi 0x0 Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE Initiator: New Phase 1, Intf 2, IKE Peer
10.20.20.1 local Proxy Address 172.22.1.0, remote Proxy
Address 172.16.1.0, Crypto map (outside_map) Nov 27
12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing
ISAKMP SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP =
10.20.20.1, constructing Fragmentation VID + extended
capabilities payload Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total
```

length : 148 Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 112 Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley proposal is acceptable Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Fragmentation VID Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer included IKE fragmentation capability flags : **Main Mode**: True Aggressive Mode: True Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Cisco Unity VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing xauth V6 VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send Altiga/ Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ISA_KE payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Cisco Unity client VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received xauth V6 VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating keys for Initiator... Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing dpd vid payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 119 Nov 27

12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 96 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Received DPD VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Oakley begin quick mode Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, **PHASE 1 COMPLETED** Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive type for this connection: DPD Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Starting phase 1 rekey timer: 73440000 (ms) Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, IKE got SPI from key engine: SPI = 0x44ae0956 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, oakley constucting quick mode Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing blank hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPSec SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPSec nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing proxy ID Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Transmitting Proxy Id: Local subnet: 172.22.1.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 172.16.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing qm hash payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, loading all IPSEC SAs Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, Security negotiation complete for LAN-to-LAN Group (10.20.20.1) Initiator, Inbound SPI = 0x44ae0956, Outbound SPI =

```
0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group =
10.20.20.1, IP = 10.20.20.1, oakley constructing final
quick mode Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1,
IKE_DECODE SENDING Message (msgid=d723766b) with
payloads : HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, IKE got a KEY_ADD msg for SA: SPI =
0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group =
10.20.20.1, IP = 10.20.20.1, Pitcher: received
KEY_UPDATE, spi 0x44ae0956 Nov 27 12:02:00 [IKEv1]:
Group = 10.20.20.1, IP = 10.20.20.1, Starting P2 Rekey
timer to expire in 24480 seconds Nov 27 12:02:00
[IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 2
COMPLETED (msgid=d723766b)
```

IPSec del debug crypto — Información del debug de las visualizaciones sobre las conexiones del IPSec.

debug crypto ipsec

```
pix1(config)#debug crypto ipsec 7 exec mode
commands/options: <1-255> Specify an optional debug
level (default is 1) <cr> pix1(config)# debug crypto
ipsec 7 pix1(config)# IPSEC: New embryonic SA created @
0x024211B0, SCB: 0x0240AEB0, Direction: inbound SPI :
0x2A3E12BE Session ID: 0x00000001 VPIF num : 0x00000001
Tunnel type: l2l Protocol : esp Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0, SCB:
0x0240B710, Direction: outbound SPI : 0xB283D32F Session
ID: 0x00000001 VPIF num : 0x00000001 Tunnel type: l2l
Protocol : esp Lifetime : 240 seconds IPSEC: Completed
host OBSA update, SPI 0xB283D32F IPSEC: Updating
outbound VPN context 0x02422618, SPI 0xB283D32F Flags:
0x00000005 SA : 0x0240B7A0 SPI : 0xB283D32F MTU : 1500
bytes VCID : 0x00000000 Peer : 0x00000000 SCB :
0x0240B710 Channel: 0x014A45B0 IPSEC: Completed outbound
VPN context, SPI 0xB283D32F VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
Rule ID: 0x01FA0290 IPSEC: New outbound permit rule, SPI
0xB283D32F Src addr: 10.10.10.1 Src mask:
255.255.255.255 Dst addr: 10.20.20.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0xB283D32F Use SPI: true IPSEC:
Completed outbound permit rule, SPI 0xB283D32F Rule ID:
0x0240AF40 IPSEC: Completed host IBSA update, SPI
0x2A3E12BE IPSEC: Creating inbound VPN context, SPI
0x2A3E12BE Flags: 0x00000006 SA : 0x024211B0 SPI :
0x2A3E12BE MTU : 0 bytes VCID : 0x00000000 Peer :
0x02422618 SCB : 0x0240AEB0 Channel: 0x014A45B0 IPSEC:
Completed inbound VPN context, SPI 0x2A3E12BE VPN
handle: 0x0240BF80 IPSEC: Updating outbound VPN context
0x02422618, SPI 0xB283D32F Flags: 0x00000005 SA :
0x0240B7A0 SPI : 0xB283D32F MTU : 1500 bytes VCID :
0x00000000 Peer : 0x0240BF80 SCB : 0x0240B710 Channel:
0x014A45B0 IPSEC: Completed outbound VPN context, SPI
0xB283D32F VPN handle: 0x02422618 IPSEC: Completed
outbound inner rule, SPI 0xB283D32F Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
Rule ID: 0x0240AF40 IPSEC: New inbound tunnel flow rule,
SPI 0x2A3E12BE Src addr: 172.16.1.0 Src mask:
255.255.255.0 Dst addr: 172.22.1.0 Dst mask:
255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore
```

```
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use
protocol: false SPI: 0x00000000 Use SPI: false IPSEC:
Completed inbound tunnel flow rule, SPI 0x2A3E12BE Rule
ID: 0x0240B108 IPSEC: New inbound decrypt rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound decrypt rule, SPI 0x2A3E12BE Rule ID:
0x02406E98 IPSEC: New inbound permit rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound permit rule, SPI 0x2A3E12BE Rule ID:
0x02422C78
```

Información Relacionada

- Creación de túnel redundante entre los Firewall usando el PDM
- Cisco PIX Firewall Software
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems