

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Antecedentes](#)

[Configuración](#)

[Configuración de ASDM](#)

[Configuración de PIX CLI](#)

[Túnel de sitio a sitio de respaldo](#)

[Borrar asociaciones de seguridad \(SA\)](#)

[Verificación](#)

[Troubleshoot](#)

[PFS](#)

[Acceso a la gestión](#)

[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.

Se forma un túnel mediante IPsec. IPsec es una combinación de estándares abiertos que proporcionan confidencialidad, integridad y autenticación de origen de datos entre pares IPsec.

Nota: En PIX 7.1 y versiones posteriores, el comando `sysopt connection permit-ipsec` se cambia a `sysopt connection permit-vpn`. Este comando permite que el tráfico que ingresa al dispositivo de seguridad a través de un túnel VPN y luego es descifrado, omita las listas de acceso a la interfaz. La política de grupo y las listas de acceso de autorización por usuario siguen aplicándose al tráfico. Para inhabilitar esta función, utilice la forma `no` de este comando. Este comando no está visible en la configuración CLI.

Consulte el [Ejemplo de Configuración del Túnel PIX 6.x: Simple PIX-to-PIX VPN](#) para aprender más sobre el mismo escenario donde el Cisco PIX Security Appliance ejecuta la versión 6.x del

software.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento especifica que este peer inicia el primer intercambio propietario para determinar el peer apropiado al cual conectarse.

- Cisco PIX 500 Series Security Appliance con versión 7.x y posterior
- ASDM versión 5.x y posteriores

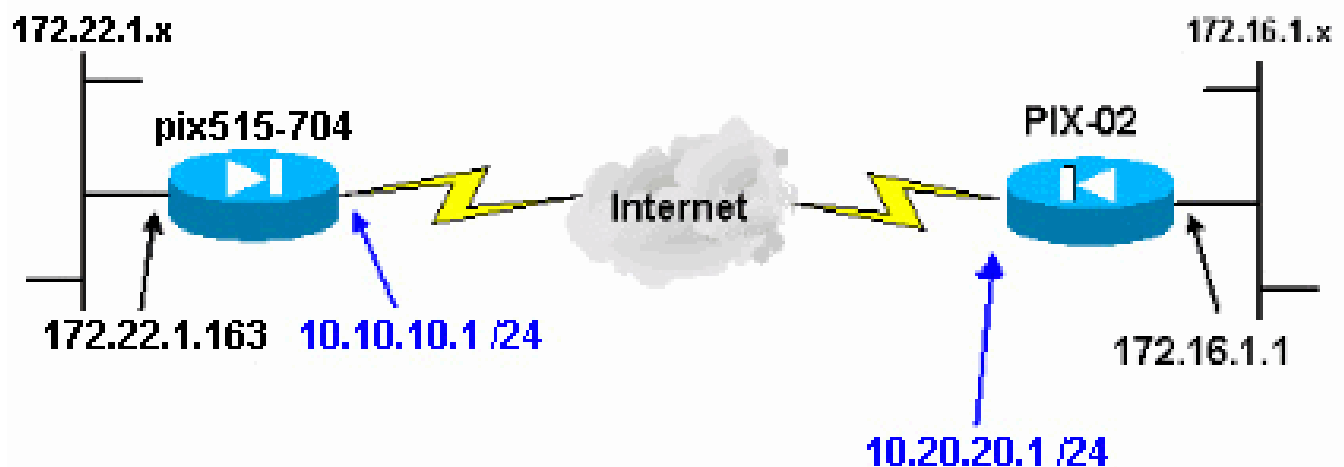
Nota: Consulte [Cómo Permitir el Acceso HTTPS para ASDM](#) para permitir que el ASA sea configurado por el ASDM.

Nota: ASA 5500 Series versión 7.x/8.x ejecuta el mismo software que se ve en PIX versión 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). If your network is live, make sure that you understand the potential impact of any command.

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

La negociación IPsec se puede dividir en cinco pasos e incluye dos fases de Intercambio de claves de Internet (IKE).

1. Un túnel IPsec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPsec.
2. En la Fase 1 IKE, las entidades pares IPsec negocian la política establecida de la Asociación de seguridad (SA) IKE. 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 de IKE, los pares IPsec usan el túnel autenticado y seguro para negociar las transformaciones de IPsec SA. La negociación de la política compartida determina el modo en que se establece el túnel IPsec.
4. Se crea el túnel IPsec y los datos se transfieren entre los pares IPsec según los parámetros IPsec configurados en los conjuntos de transformaciones de IPsec.
5. El túnel IPsec termina cuando los IPsec SAs son borrados o cuando caduca su vigencia.

Nota: La negociación IPsec entre los dos PIX falla si las SA en ambas fases IKE no coinciden en los pares.

Configuración

- [Configuración de ASDM](#)
- [Configuraciones de PIX CLI](#)

Configuración de ASDM

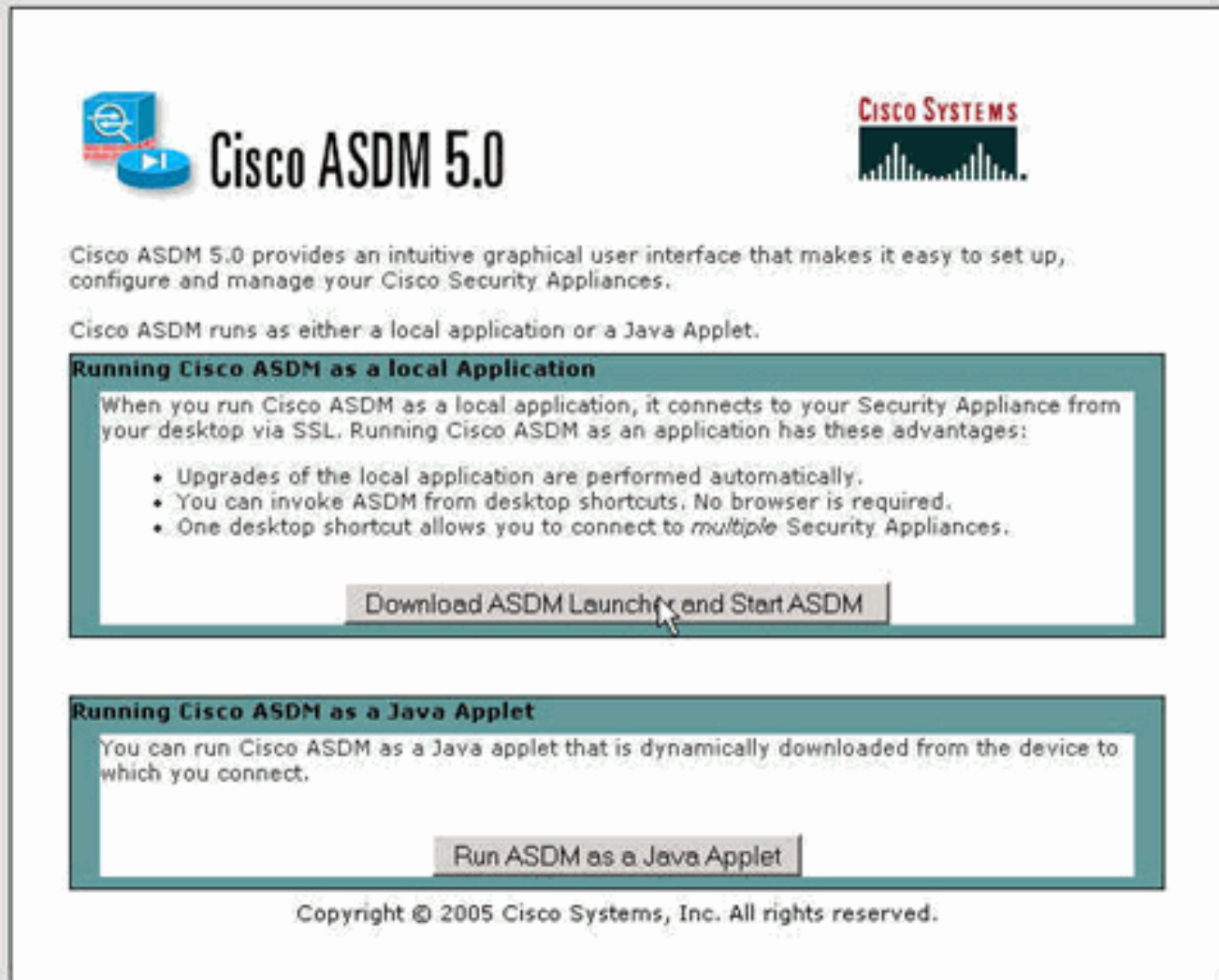
Complete estos pasos:



1. Abra su navegador y escriba `https://<Inside_IP_Address_of_PIX>` para acceder al ASDM en el PIX.

Asegúrese de autorizar cualquier advertencia que le proporcione su navegador en relación con la autenticidad del certificado SSL. El nombre de usuario y la contraseña predeterminados están en blanco.

El PIX presenta esta ventana para permitir la descarga de la aplicación ASDM. En este

ejemplo se carga la aplicación en el equipo local y no se ejecuta en un subprograma Java.



 **Cisco ASDM 5.0** 

Cisco ASDM 5.0 provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or a Java Applet.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- Upgrades of the local application are performed automatically.
- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

[Download ASDM Launcher and Start ASDM](#)

Running Cisco ASDM as a Java Applet

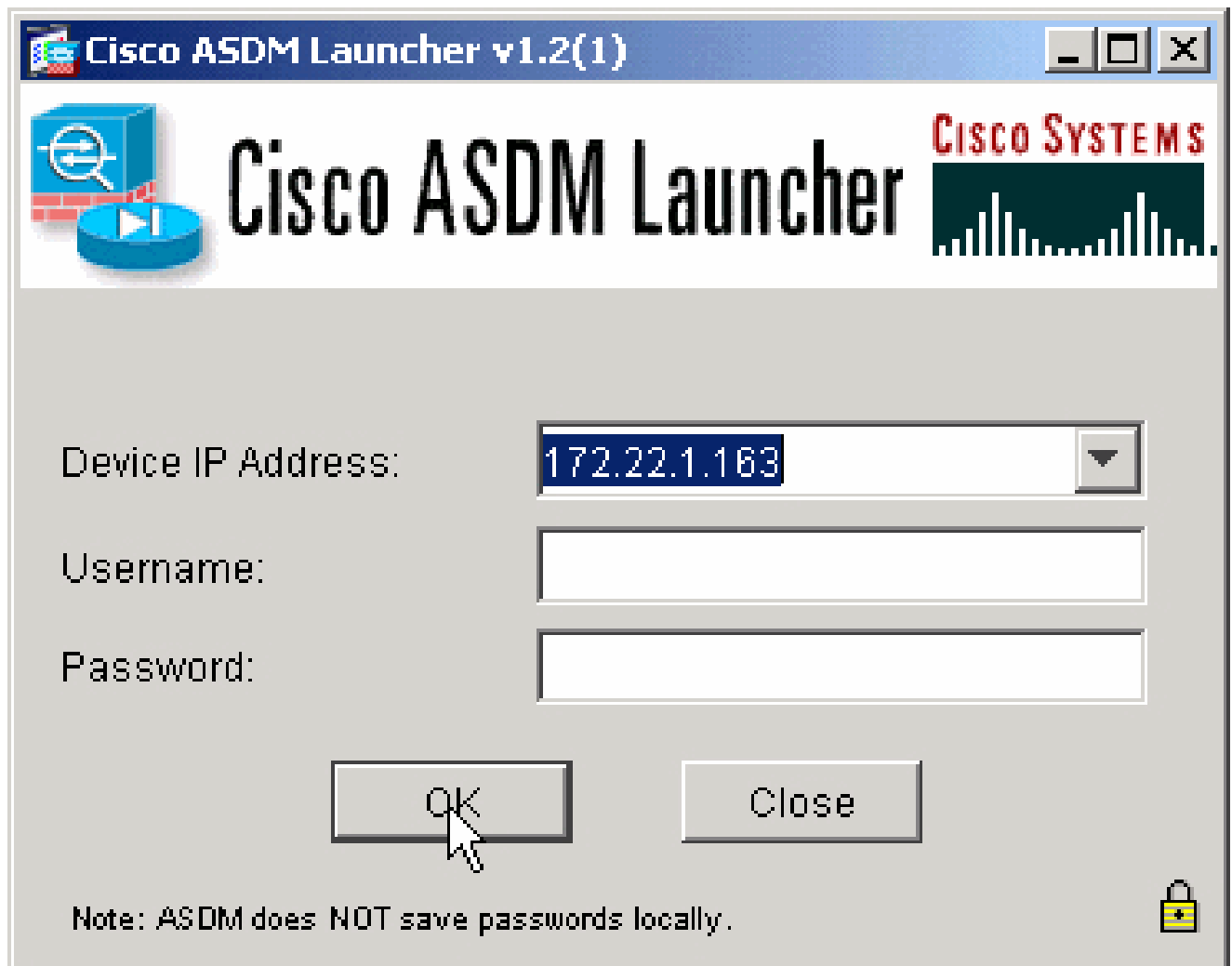
You can run Cisco ASDM as a Java applet that is dynamically downloaded from the device to which you connect.

[Run ASDM as a Java Applet](#)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

2. Haga clic en Download ASDM Launcher and Start ASDM para descargar el instalador para la aplicación ASDM.
3. Una vez que se descarga el punto de ejecución de ASDM, siga las indicaciones para instalar el software y ejecutar el punto de ejecución de ASDM de Cisco.
4. Ingrese la dirección IP para la interfaz que configuró con el comando http - y un nombre de usuario y contraseña si especificó uno.

Este ejemplo utiliza el nombre de usuario y la contraseña predeterminados en blanco.



5. Ejecute el asistente VPN una vez que la aplicación ASDM se conecte al PIX.

Cisco ASDM 5.0 for PIX - 172.22.1.163

File Rules Search Options Tools **Wizards** Help

Home Configuration Monitor **VPN Wizard...** Forward Search Refresh Save Help

Device Information

General License

Host Name: **pix515-704.cisco.com**

PIX Version: **7.0(4)** Device Uptime: **5d 20h 24m 26s**

ASDM Version: **5.0(4)** Device Type: **PIX 515**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **16 MB** Total Memory: **64 MB**

VPN Status

IKE Tunnels: **0** IPSec Tunnels: **0**

System Resources Status

CPU: 1% (17:31:42)

CPU Usage (percent): [Line graph showing 1% usage]

Memory: 20MB (17:31:42)

Memory Usage (MB): [Line graph showing 20MB usage]

Interface Status

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	172.22.1.163/24	up	up	2
outside	10.10.10.1/24	up	up	0

Select an interface to view input and output Kbps

Traffic Status

Connections Per Second Usage

[Line graph showing 0 connections per second]

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

[Line graph showing 0 input and output Kbps]

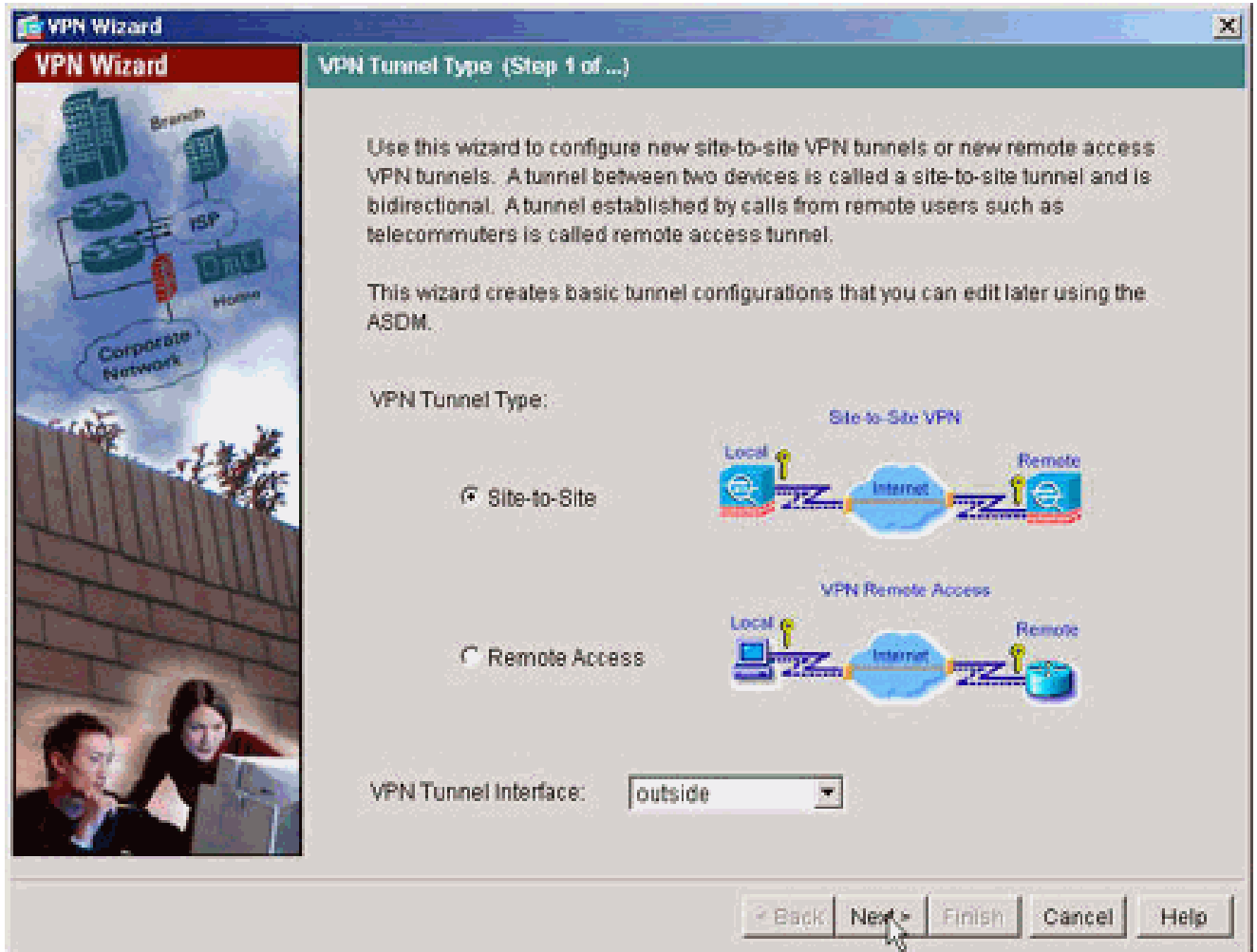
Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

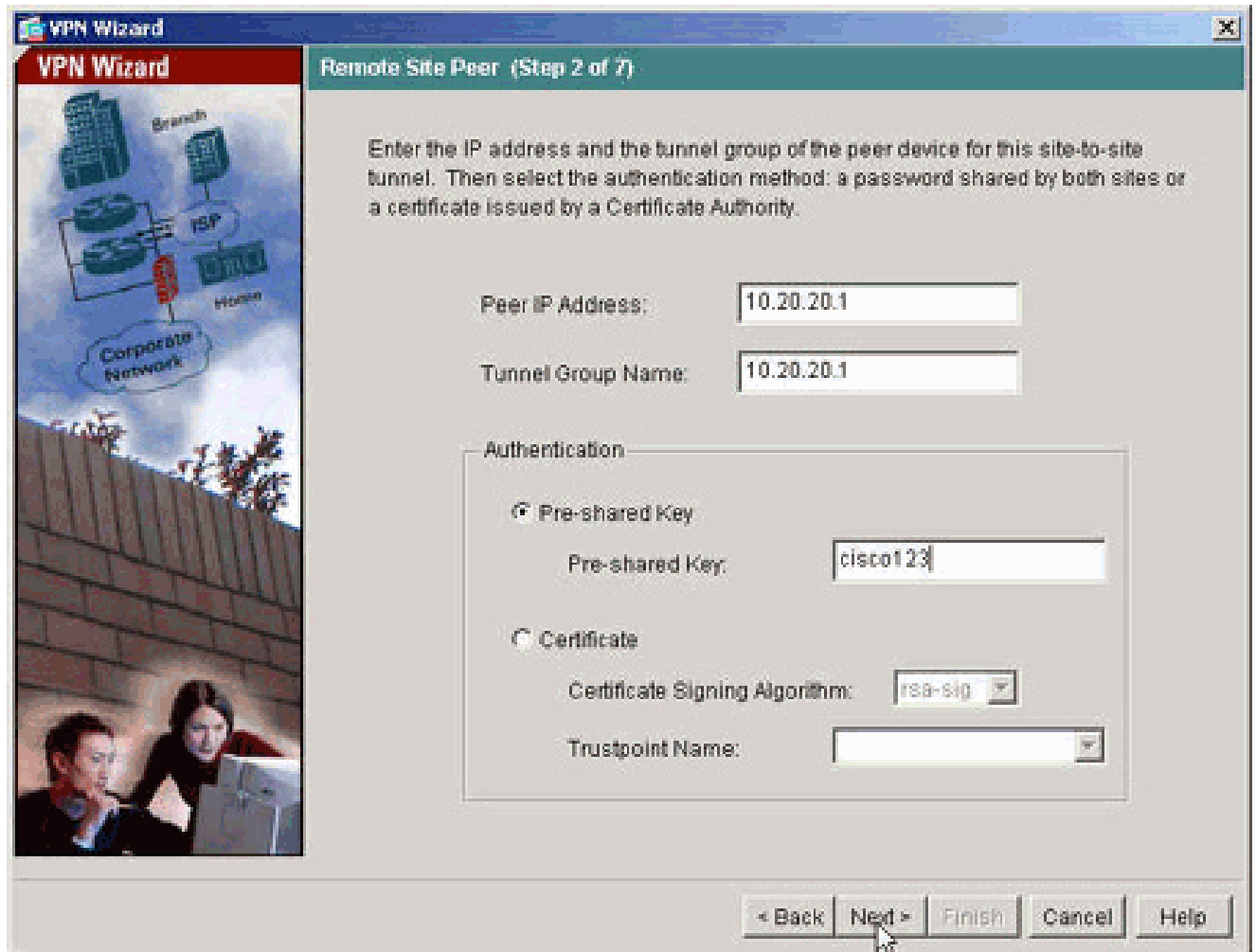
-- Syslog Disabled --

Device configuration loaded successfully. <admin> NA (15) 11/3/05 5:31:42 PM UTC

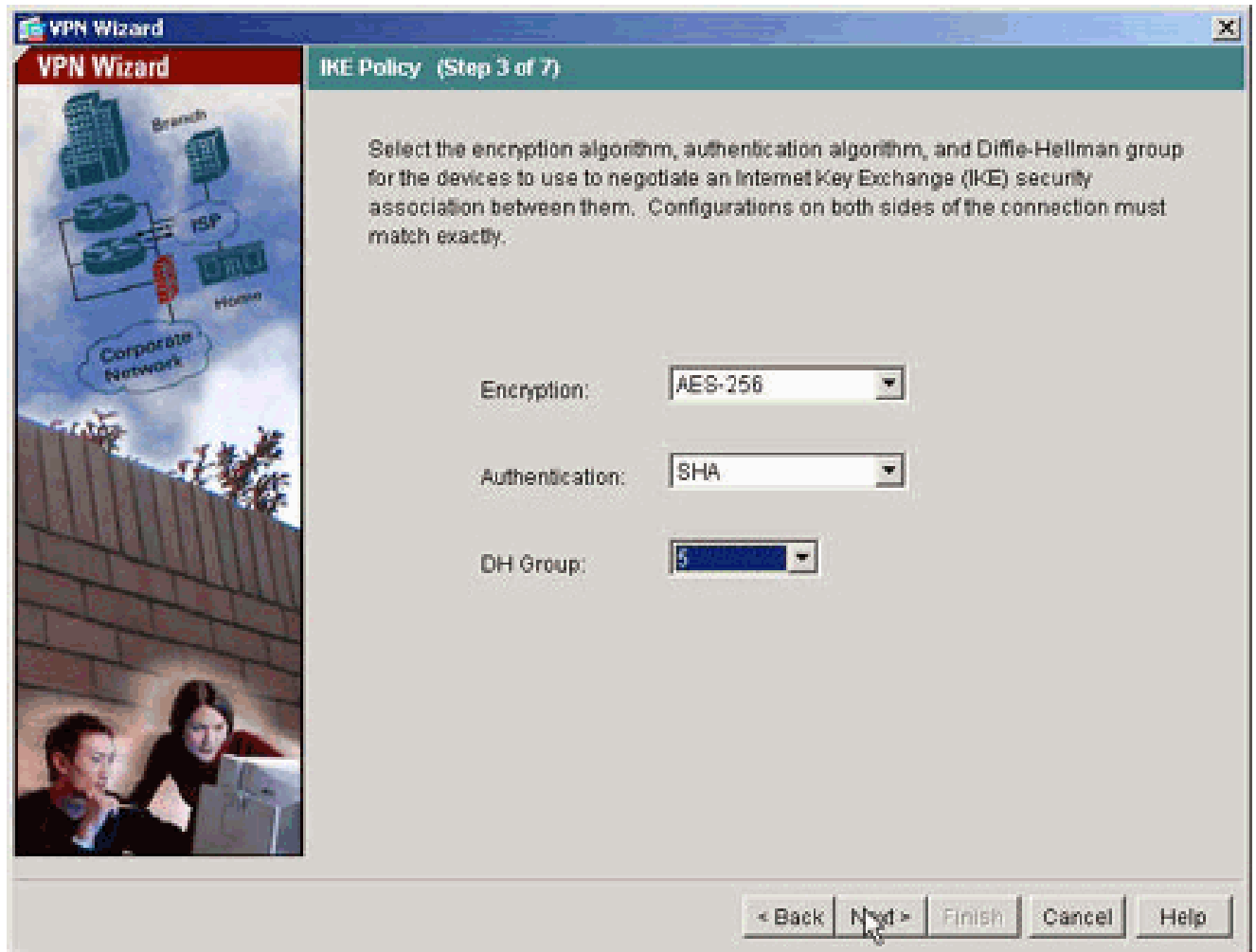
6. Elija el tipo de túnel VPN de sitio a sitio.



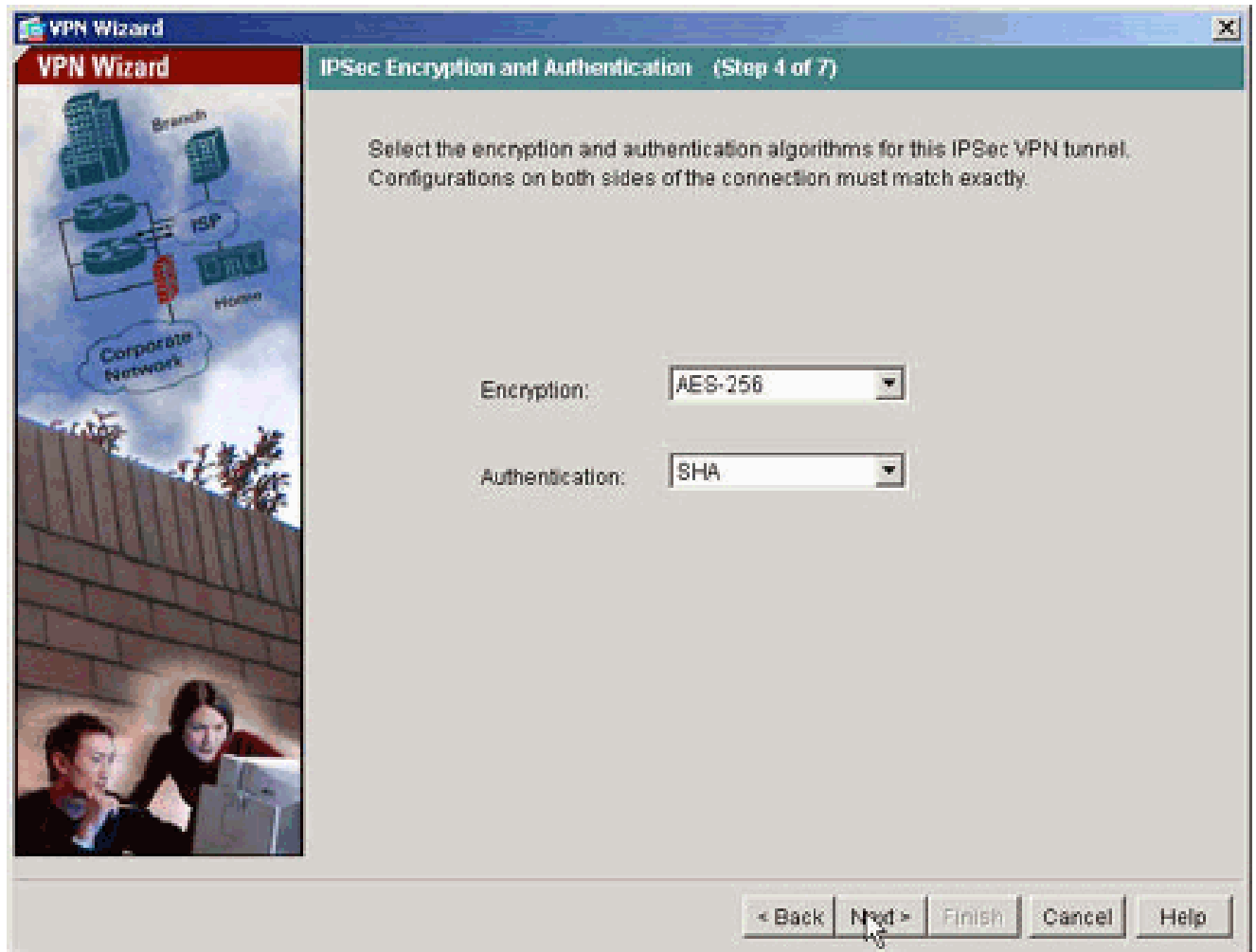
7. Especifique la dirección IP externa del par remoto. Introduzca la información de autenticación que desea utilizar (clave previamente compartida en este ejemplo).



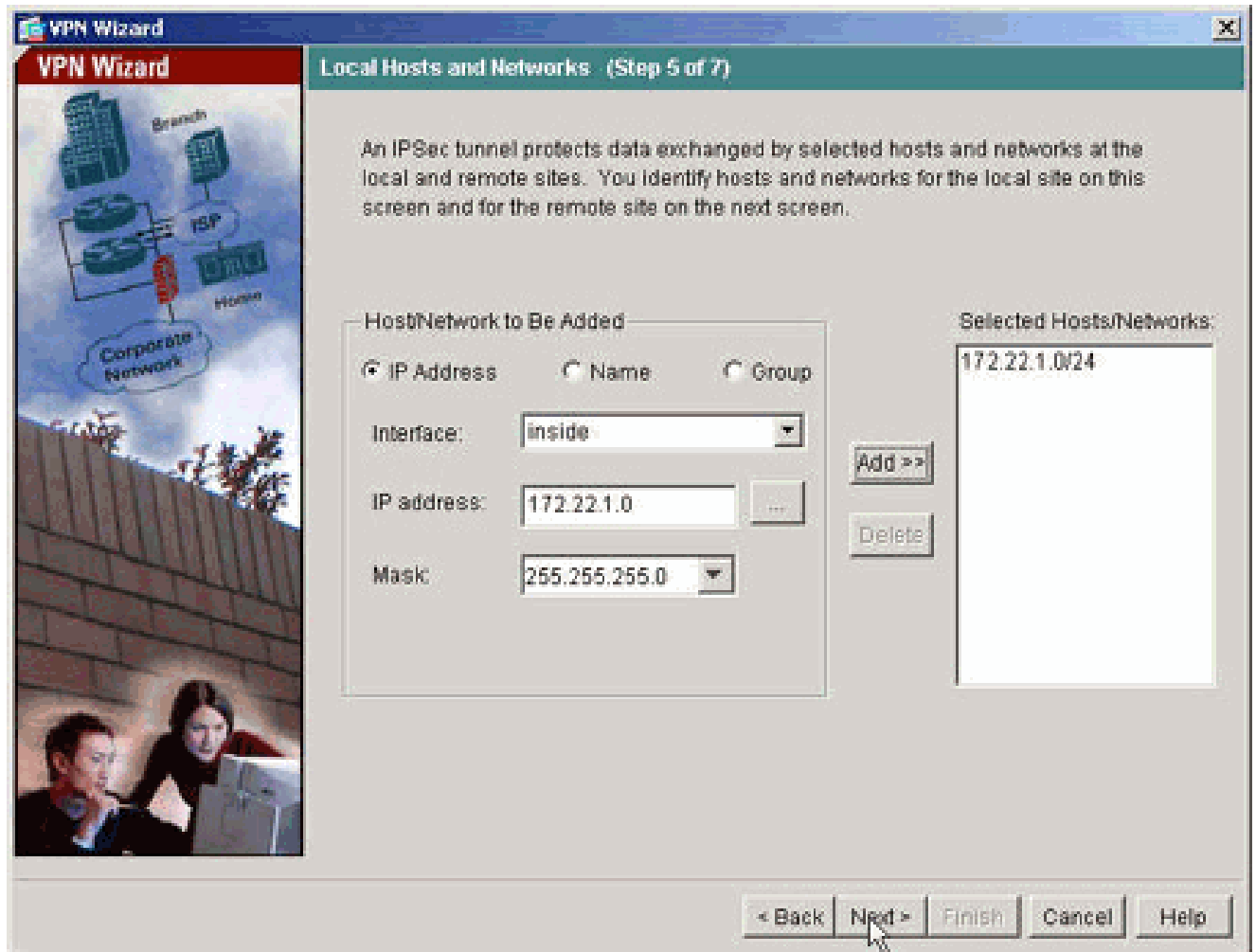
8. Especifique los atributos que se utilizarán para IKE, también conocidos como "fase 1". Estos atributos deben ser los mismos en ambos lados del túnel.



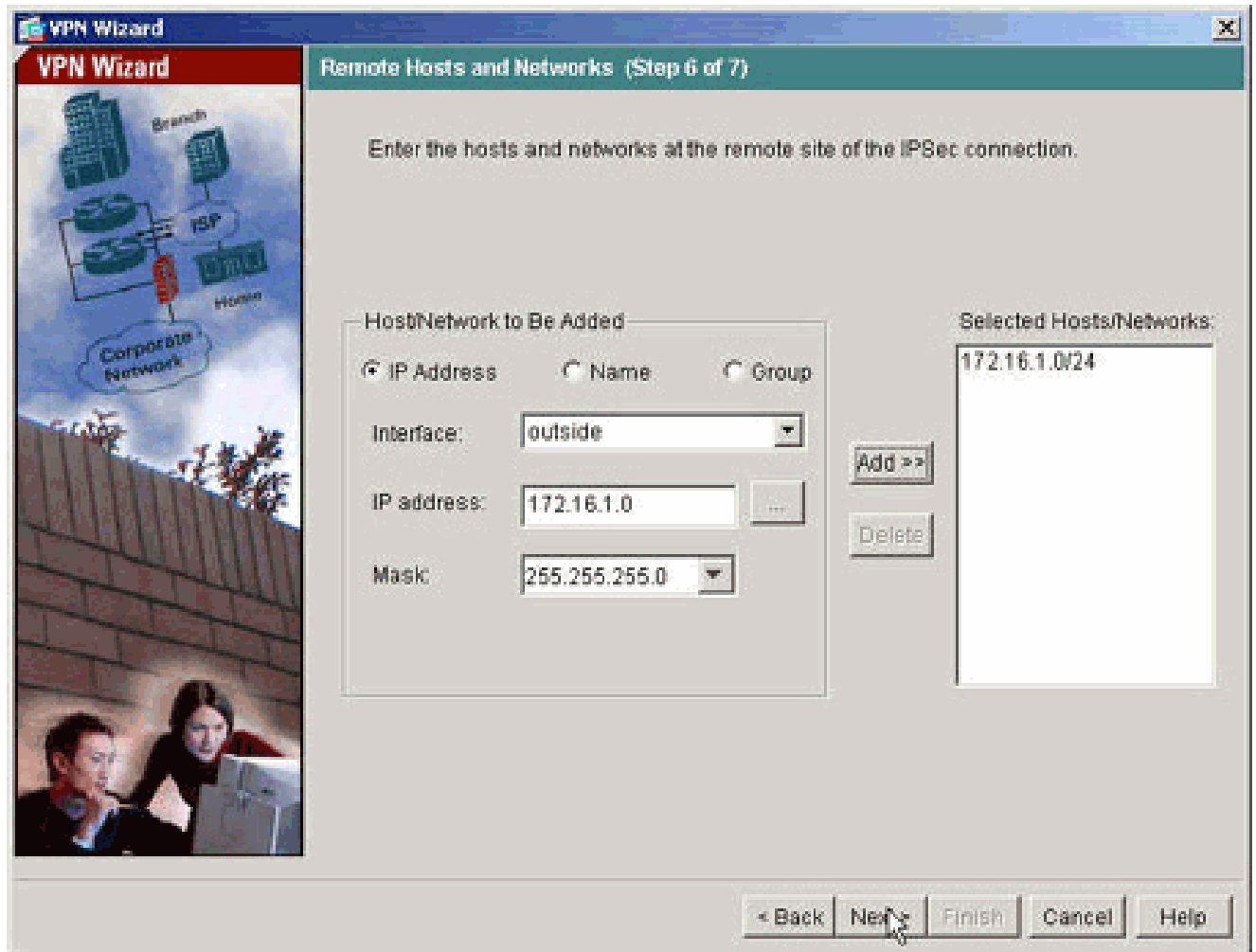
9. Especifique los atributos que se utilizarán para IPsec, también conocidos como "fase 2". Estos atributos deben coincidir en ambos lados.



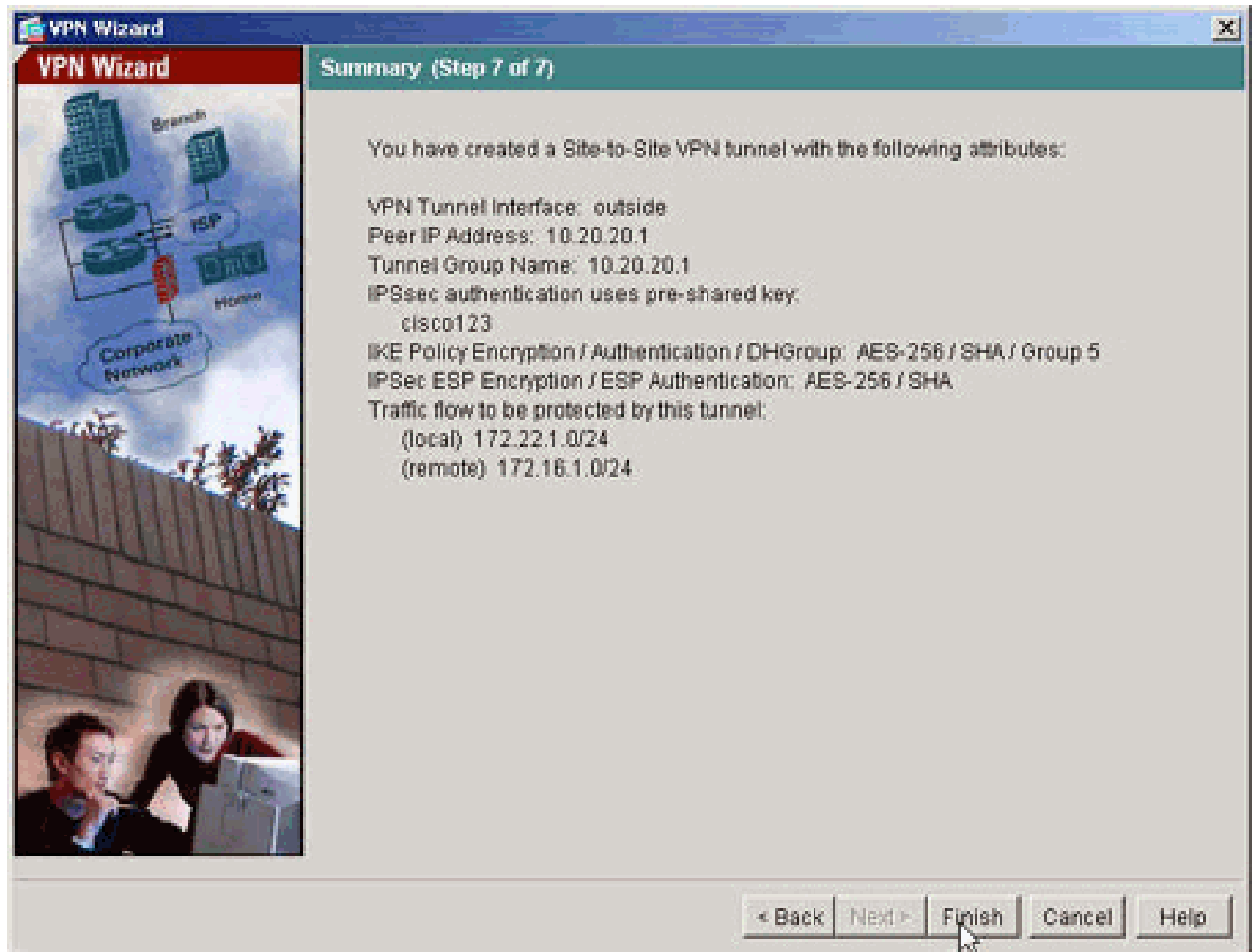
10. Especifique los hosts cuyo tráfico se debe permitir que pase a través del túnel VPN. En este paso, se especifican los hosts locales para pix515-704.



11. Se especifican los hosts y las redes del lado remoto del túnel.



12. En este resumen se muestran los atributos definidos por el Asistente para VPN. Vuelva a comprobar la configuración y haga clic en Finish cuando esté satisfecho con la configuración correcta.



Configuración de PIX CLI

```
<#root>
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

(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 inter

(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"

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 in

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

```
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

<#root>

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 sitio a sitio de respaldo

Para especificar el tipo de conexión para la función de sitio a sitio de copia de seguridad para esta entrada de mapa criptográfico, utilice el comando `crypto map set connection-type` en el modo de configuración global. Utilice la forma `no` de este comando para volver a la configuración predeterminada.

Sintaxis:

<#root>

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

- **answer-only:** especifica que este peer solo responde a las conexiones IKE entrantes primero durante el intercambio propietario inicial para determinar el peer apropiado al que conectarse.
- **bidireccional:** especifica que este par puede aceptar y originar conexiones basadas en esta entrada de mapa criptográfico. Este es el tipo de conexión predeterminado para todas las conexiones de sitio a sitio.
- **originate-only:** especifica que este peer inicia el primer intercambio propietario para determinar el peer apropiado al que conectarse.

El comando `crypto map set connection-type` especifica los tipos de conexión para la función de copia de seguridad de LAN a LAN. Permite especificar varios pares de respaldo en un extremo de la conexión. Esta función sólo funciona entre estas plataformas:

- Dos dispositivos de seguridad Cisco ASA serie 5500
- Dispositivo de seguridad Cisco ASA serie 5500 y un concentrador Cisco VPN 3000
- Dispositivo de seguridad Cisco ASA serie 5500 y un dispositivo de seguridad que ejecuta Cisco PIX Security Appliance Software versión 7.0 o posterior

Para configurar una conexión de LAN a LAN de respaldo, Cisco recomienda que configure un extremo de la conexión como `originate-only` con la palabra clave `originate-only`, y el extremo con varios pares de respaldo como `answer-only` con la palabra clave `answer-only`. En el extremo `originate-only`, utilice el comando `crypto map set peer` para ordenar la prioridad de los peers. El dispositivo de seguridad sólo de origen intenta negociar con el primer par de 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 se configura de esta manera, el peer `originate-only` intenta inicialmente establecer un túnel propietario y negociar con un peer. A partir de entonces, cualquiera de los pares puede establecer una conexión LAN a LAN normal y los datos de cualquier extremo pueden iniciar la conexión de túnel.

Nota: Si configuró VPN con varias direcciones IP de peer para una entrada `crypto`, la VPN se establece con la IP de peer de respaldo una vez que el peer primario deja de funcionar. Sin embargo, una vez que el peer primario regresa, la VPN no se antepone a la dirección IP primaria. Debe eliminar manualmente la SA existente para reiniciar la negociación VPN para conmutarla a la dirección IP principal. Como se indica en la conclusión, el túnel de sitio a sitio no admite VPN preempt.

Tipos de conexión de LAN a LAN de copia de seguridad compatibles

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 mapa criptográfico mymap y establece el tipo de conexión en originate-only.

```
<#root>
```

```
hostname(config)#
```

```
crypto map outside_map 20 connection-type originate-only
```

Borrar asociaciones de seguridad (SA)

En el modo de privilegio del PIX, utilice los siguientes comandos:

- clear [crypto] ipsec sa: elimina las SA de IPsec activas. La palabra clave crypto es opcional.
- clear [crypto] isakmp sa: elimina las IKE SA activas. La palabra clave crypto es opcional.

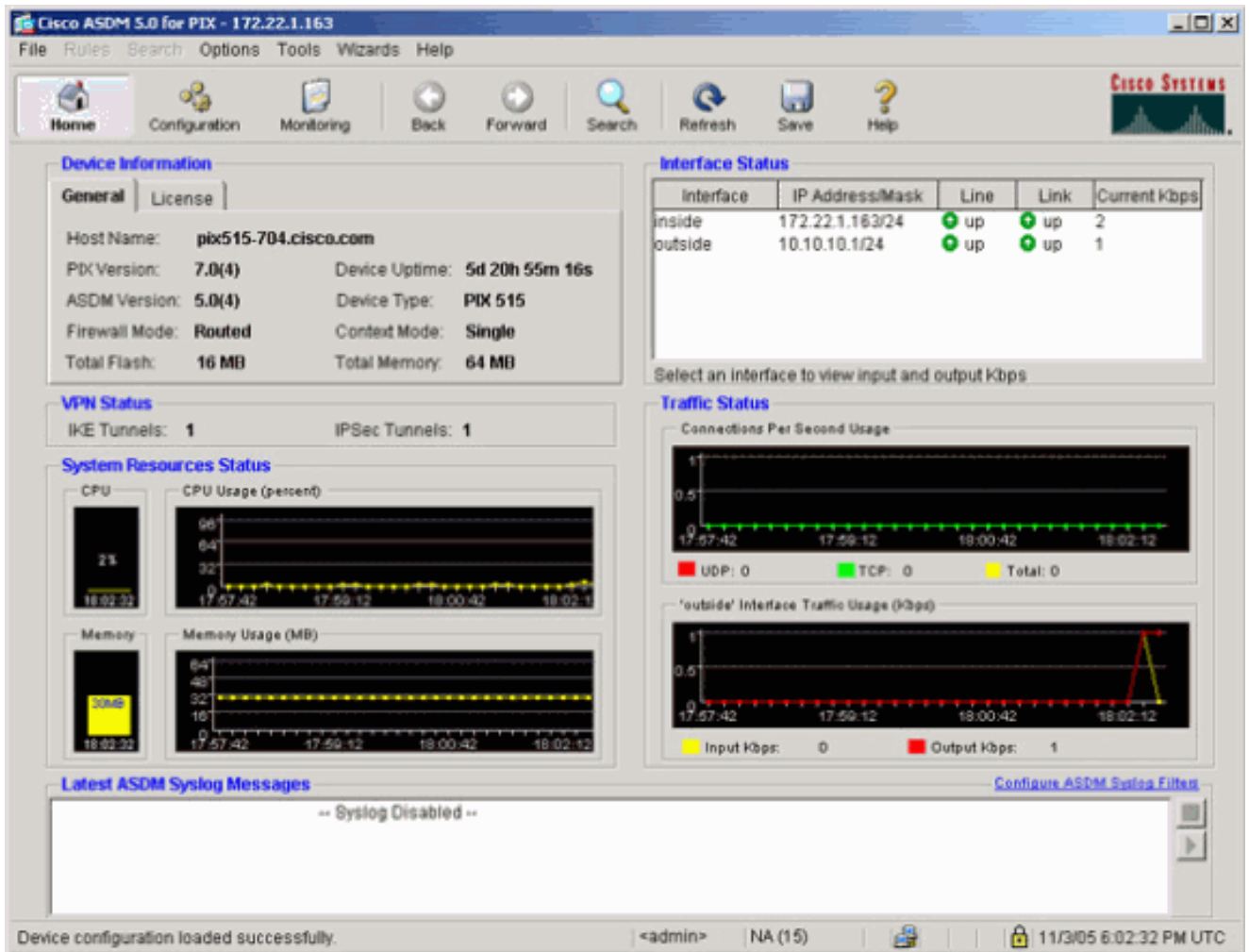
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

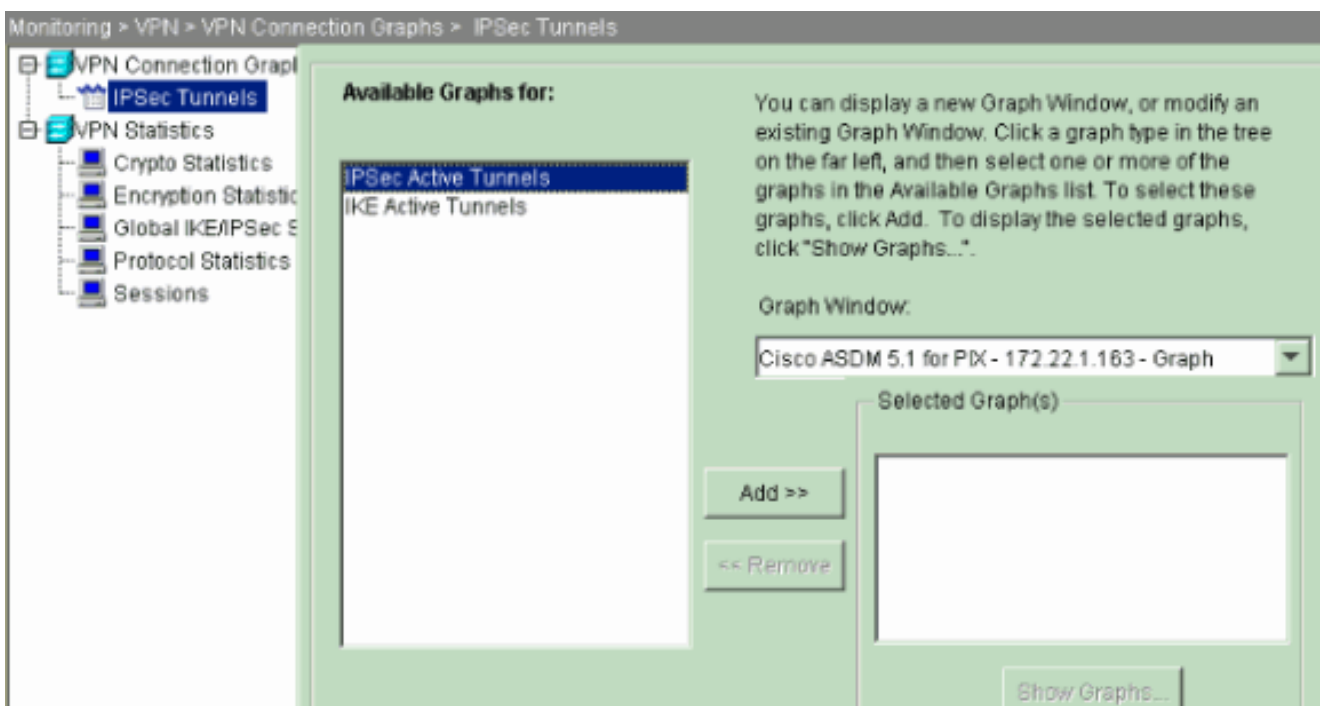
[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

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

1. Vea el estado de VPN en Inicio en el ASDM para verificar la formación del túnel.

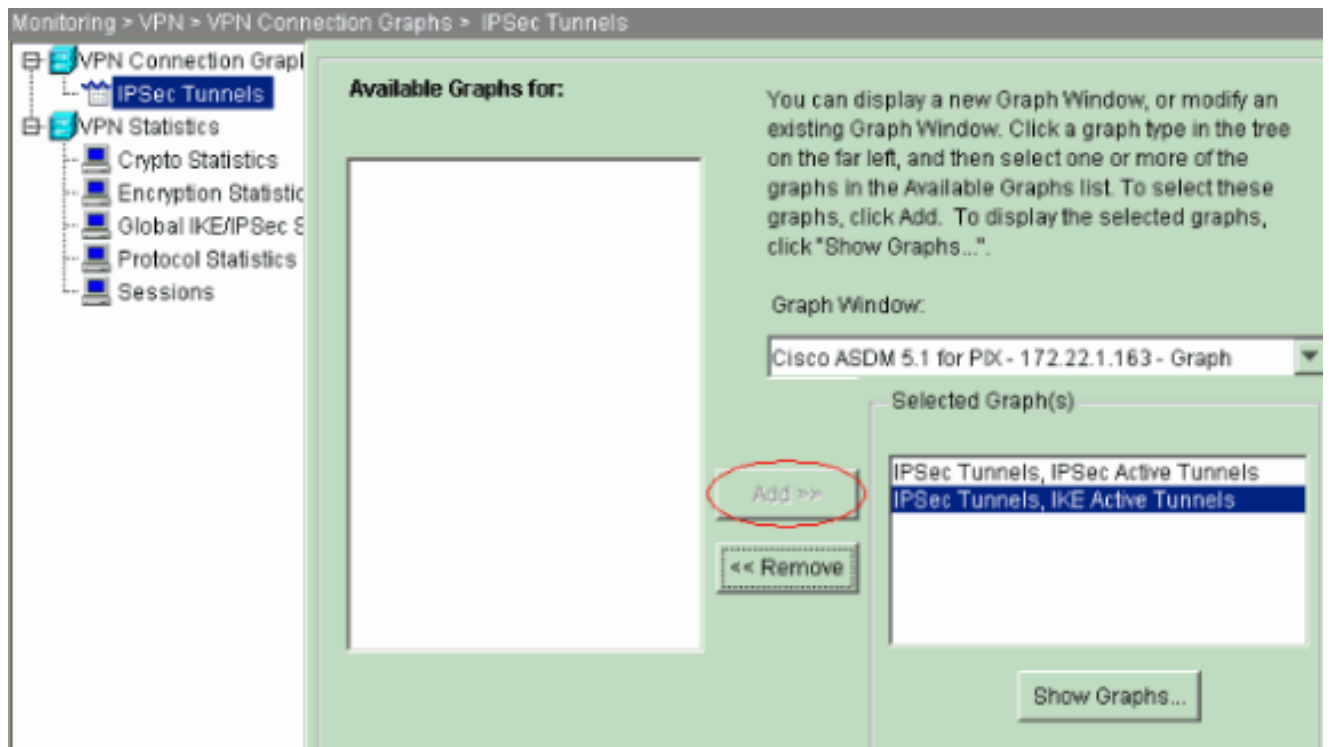


2. Elija Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels para verificar los detalles sobre el establecimiento del túnel.

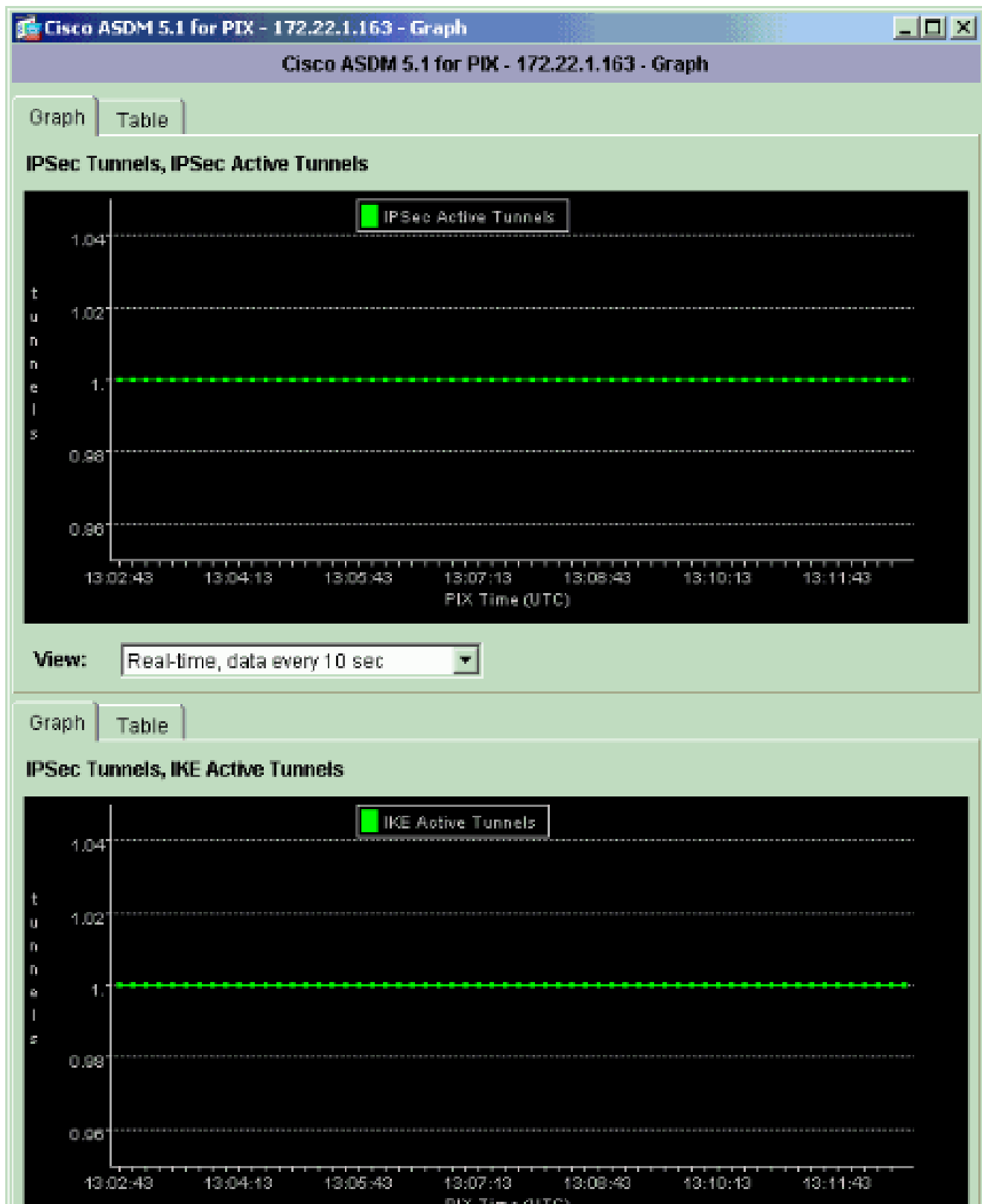


3. Haga clic en Agregar para seleccionar los gráficos disponibles para visualizarlos en la

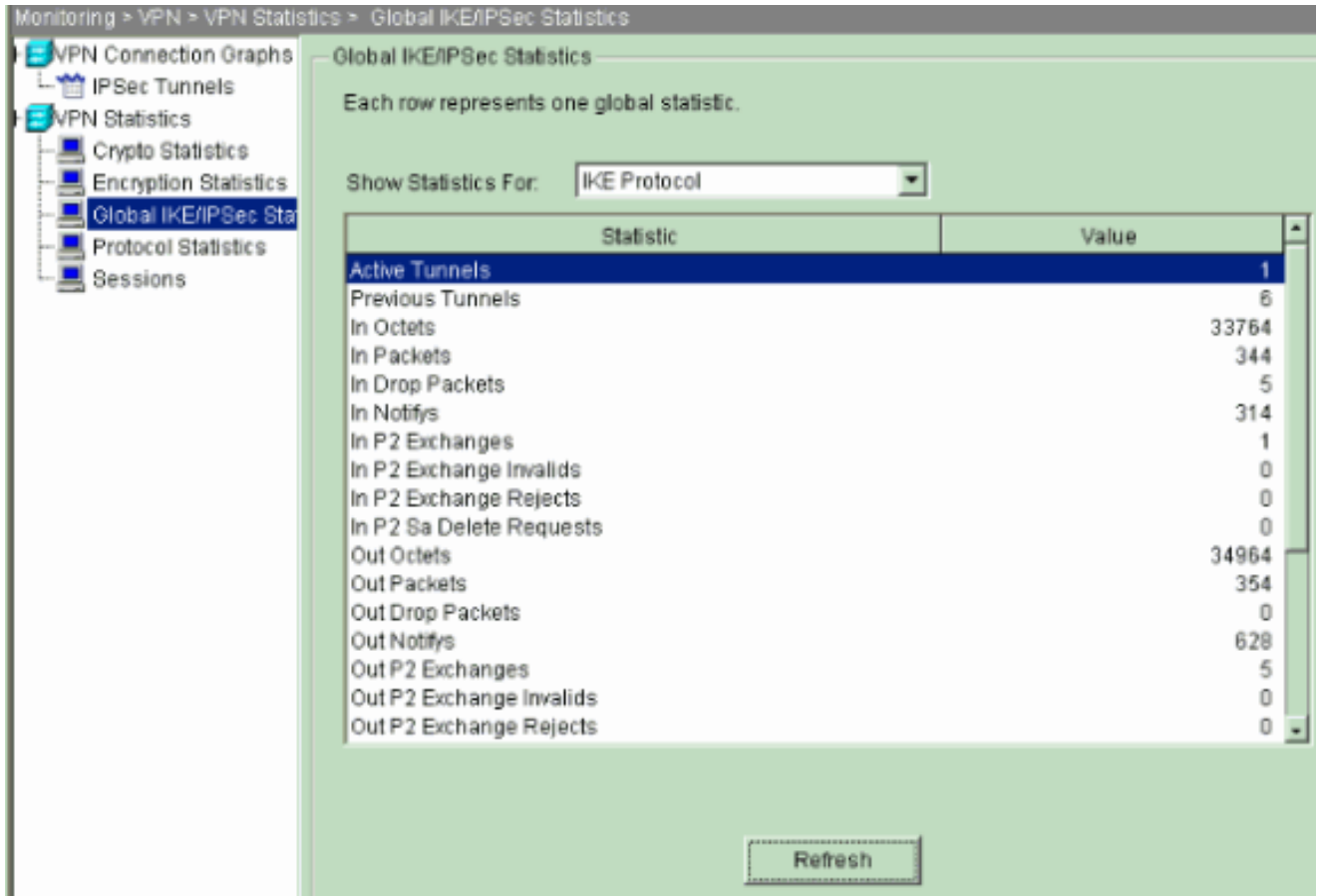
ventana gráfica.



4. Haga clic en Show Graphs para ver los gráficos de los túneles activos IKE e IPsec.



5. Elija Monitoring > VPN > VPN Statistics > Global IKE/IPsec Statistics para conocer la información estadística del túnel VPN.



También puede verificar la formación de túneles mediante CLI. Ejecute el comando `show crypto isakmp sa` para verificar la formación de los túneles y ejecute el comando `show crypto ipsec sa` para observar el número de paquetes encapsulados, cifrados, etc.

```

pix515-704
<#root>
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

```



```

<#root>
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

```

Troubleshoot

PFS

En las negociaciones de IPsec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior. Habilite o inhabilite PFS en ambos peers del túnel; de lo contrario, el túnel IPsec L2L no se establece en PIX/ASA.

PFS se inhabilita de forma predeterminada. Para habilitar PFS utilice el comando pfs con la palabra clave enable en el modo de configuración de política de grupo. Para inhabilitar PFS, ingrese la palabra clave disable (inhabilitar).

```
<#root>
```

```
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.

```
<#root>
```

```
hostname(config-group-policy)#
```

```
no pfs
```

Acceso a la gestión

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 [acceso se configure en el modo global configuration](#).

```
<#root>
```

```
PIX-02(config)#
```

```
management-access inside
```

```
PIX-02(config)#
```

```
show management-access
```

```
management-access inside
```

Comandos de Debug

Nota: Consulte Información importante sobre los comandos de depuración antes de utilizar este tipo de comandos.

debug crypto isakmp: muestra información de depuración sobre las conexiones IPsec y muestra el primer conjunto de atributos que se deniegan debido a incompatibilidades en ambos extremos.

```
debug crypto isakmp

<#root>
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 constructing 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)
```

debug crypto ipsec—Muestra información de depuración acerca de las conexiones IPsec.

```
debug crypto ipsec
```

```
<#root>
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: 121
```

```
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: 121
```

```
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 túneles redundantes entre firewalls mediante 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](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).