SDM: IPSec sitio a sitio VPN entre ASA/PIX y un ejemplo de la configuración del router IOS

Contenido

Introducción

Este documento proporciona una configuración de ejemplo del túnel IPsec de LAN a LAN (sitio a sitio) entre Cisco Security Appliances (ASA/PIX) y un router Cisco IOS. Las rutas estáticas se utilizan para simplificar.

Refiera al dispositivo de seguridad del PIX/ASA 7.x a un ejemplo de la configuración del router IOS túnel ipsec de LAN a LAN para aprender un decorado más casi igual donde el dispositivo de seguridad del PIX/ASA funciona con la versión de software *7.x*.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- La Conectividad de punta a punta IP debe ser establecida antes de comenzar esta configuración.

- La licencia del dispositivo de seguridad se debe activar para el cifrado del Data Encryption Standard (DES) (en un nivel mínimo del cifrado).

Componentes Utilizados

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

- Dispositivo de seguridad adaptante de Cisco (ASA) con la versión 8.x y posterior
- Versión 6.x.and ASDM más adelante
- Cisco 1812 Router con el Software Release 12.3 de Cisco IOS®
- Versión 2.5 del administrador de dispositivo Security de Cisco (SDM)

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

Nota: Refiera a la configuración básica del router usando SDM para permitir que al router configure SDM.

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.

Nota: Refiera al profesional de la configuración: IPSec sitio a sitio VPN entre ASA/PIX y un ejemplo de la configuración del router IOS para una configuración similar usando el Cisco Configuration Professional en el router.

Productos relacionados

Esta configuración se puede también utilizar con el dispositivo de seguridad de la serie de Cisco PIX 500, que funciona con la versión 7.x y posterior.

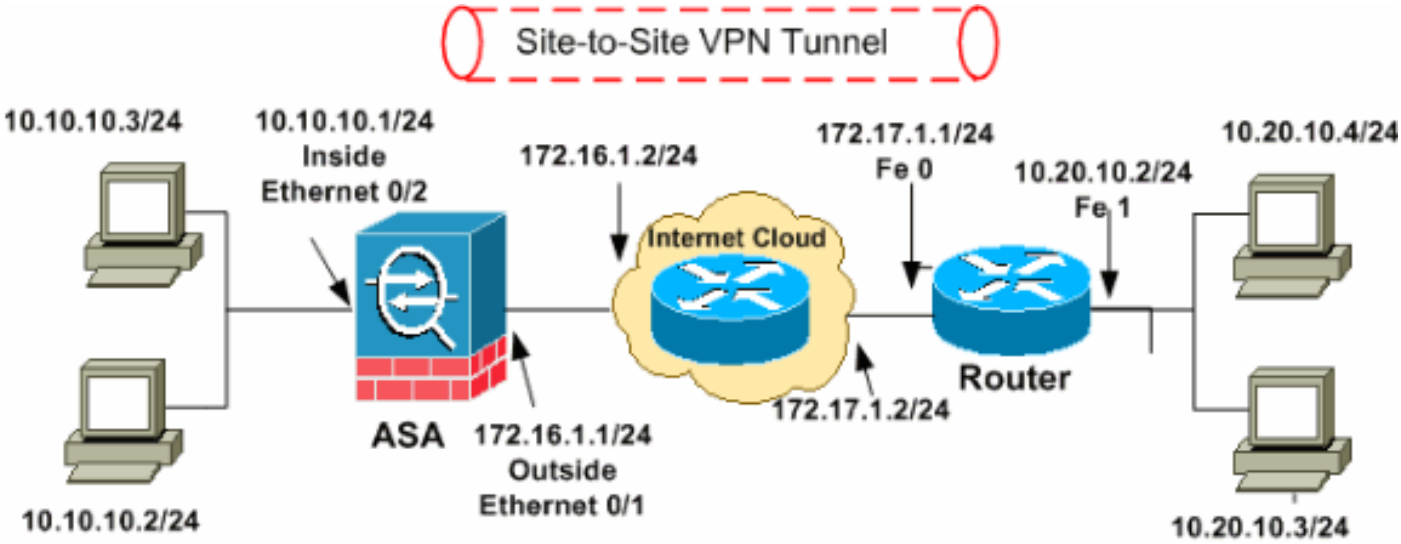
Convenciones

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

Configuración

Diagrama de la red

Este documento utiliza la configuración de la red mostrada en este diagrama.



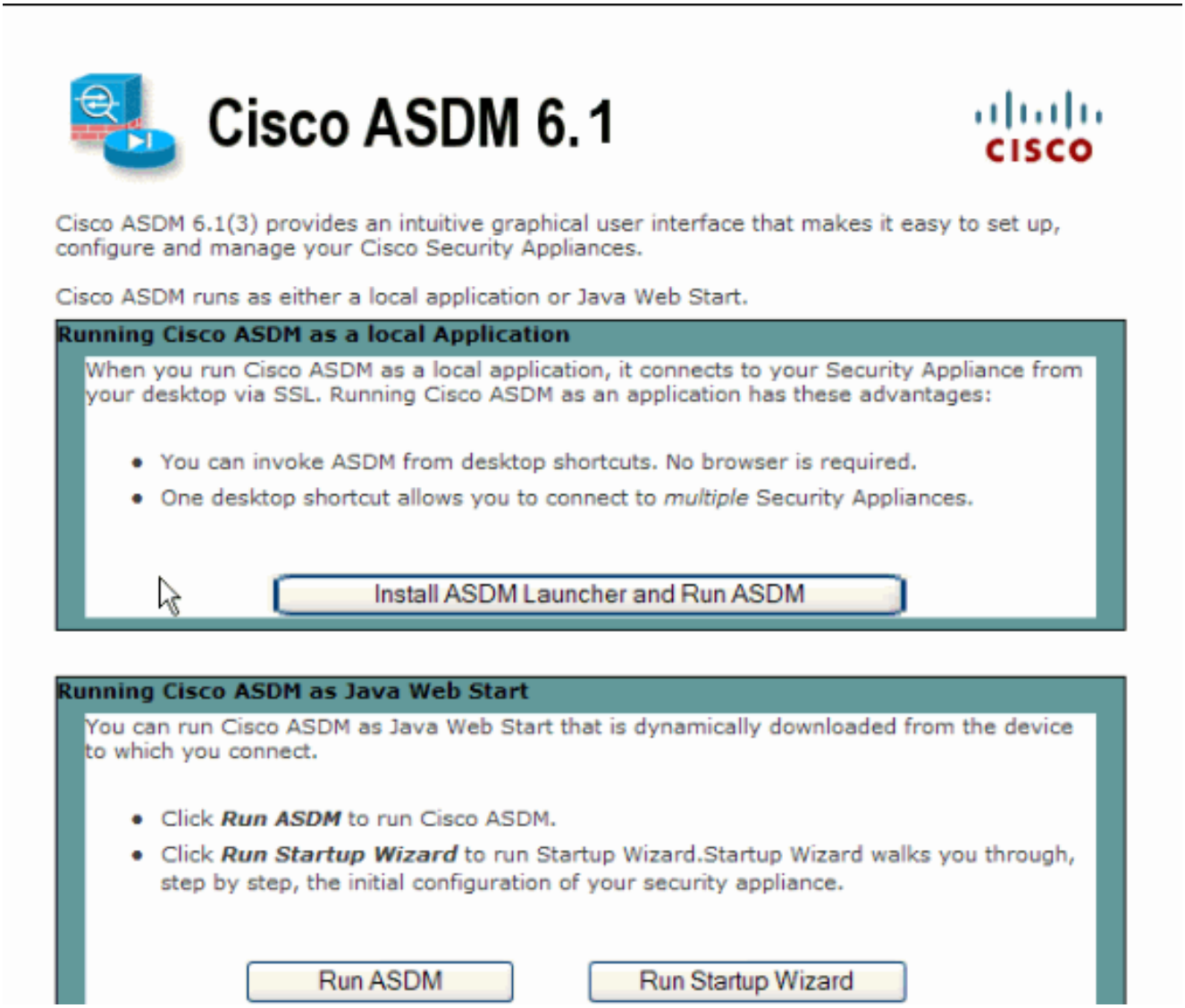
Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918, que se han utilizado en un entorno del laboratorio.

- Configuración del túnel ASDM VPN
- Configuración de SDM del router
- Configuración CLI ASA
- Configuración CLI del router

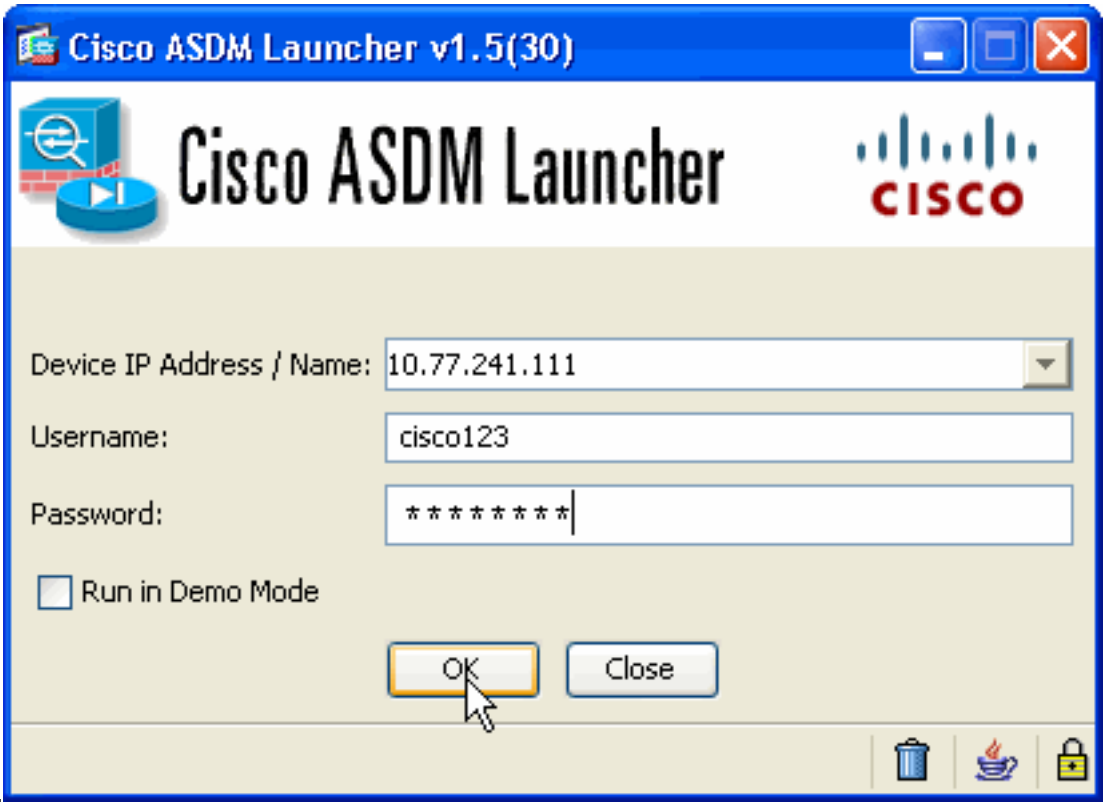
Configuración del túnel ASDM VPN

Complete estos pasos para crear el túnel VPN:

1. Abra su hojeador y ingrese los **<IP_Address de https:// del interfaz del ASA que se ha configurado para ASDM Access>** para tener acceso al ASDM en el ASA.Asegúrese de autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad del certificado SSL. Nombre de usuario y contraseña del valor por defecto es ambos espacio en blanco.El ASA presenta esta ventana para permitir la transferencia directa de la aplicación ASDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en un Java
applet.

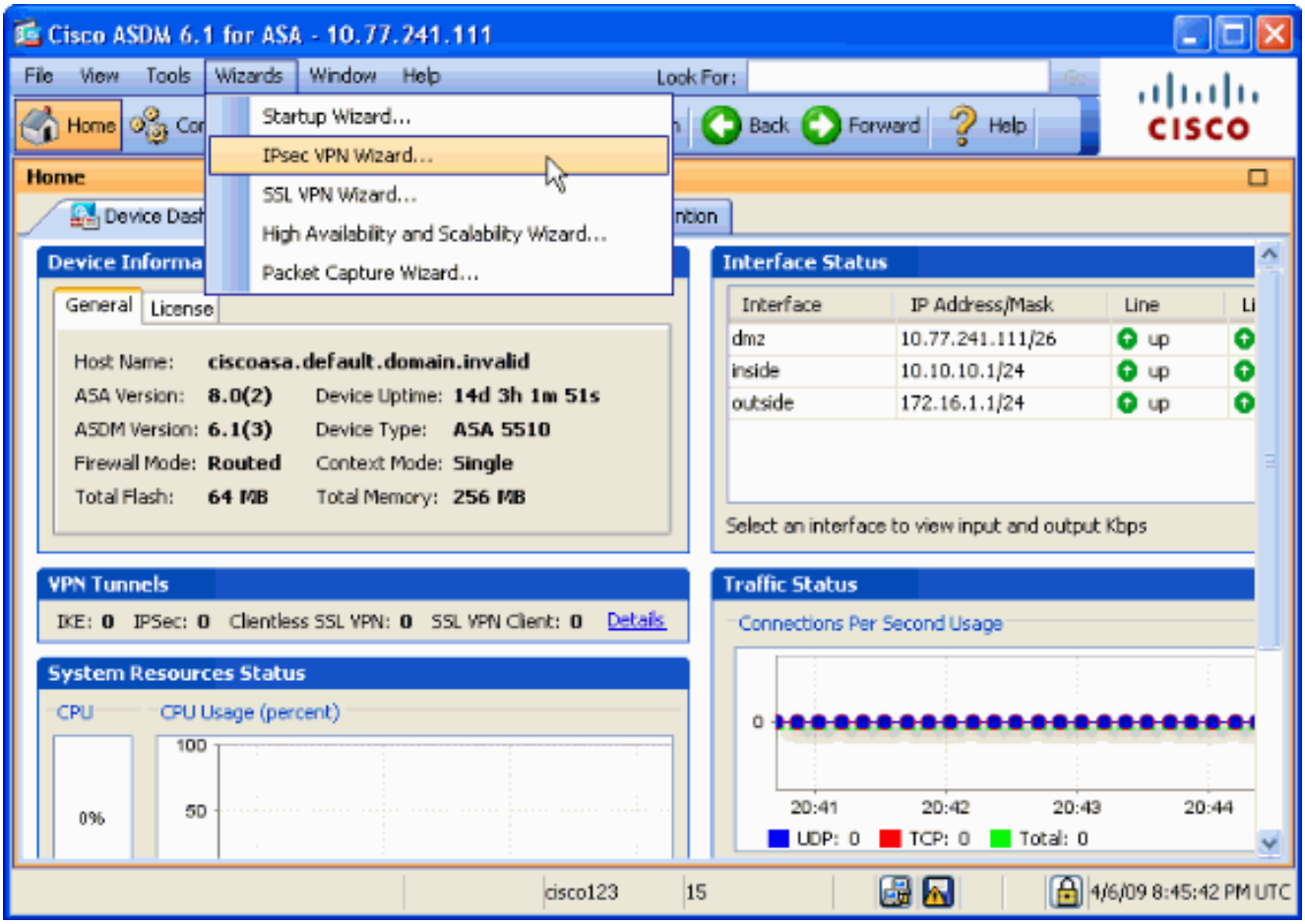


2. Haga clic el **lanzador de la transferencia directa ASDM y comience ASDM** para descargar el instalador para la aplicación ASDM.
3. Una vez que las transferencias directas del lanzador ASDM, completan los pasos ordenados por los mensajes para instalar el software y funcionar con el lanzador de Cisco ASDM.
4. Ingrese el IP address para el interfaz que usted configuró con el **HTTP -** ordene, y un nombre de usuario y contraseña si usted especificó uno.Este ejemplo utiliza **cisco123** para el username y **cisco123** como la

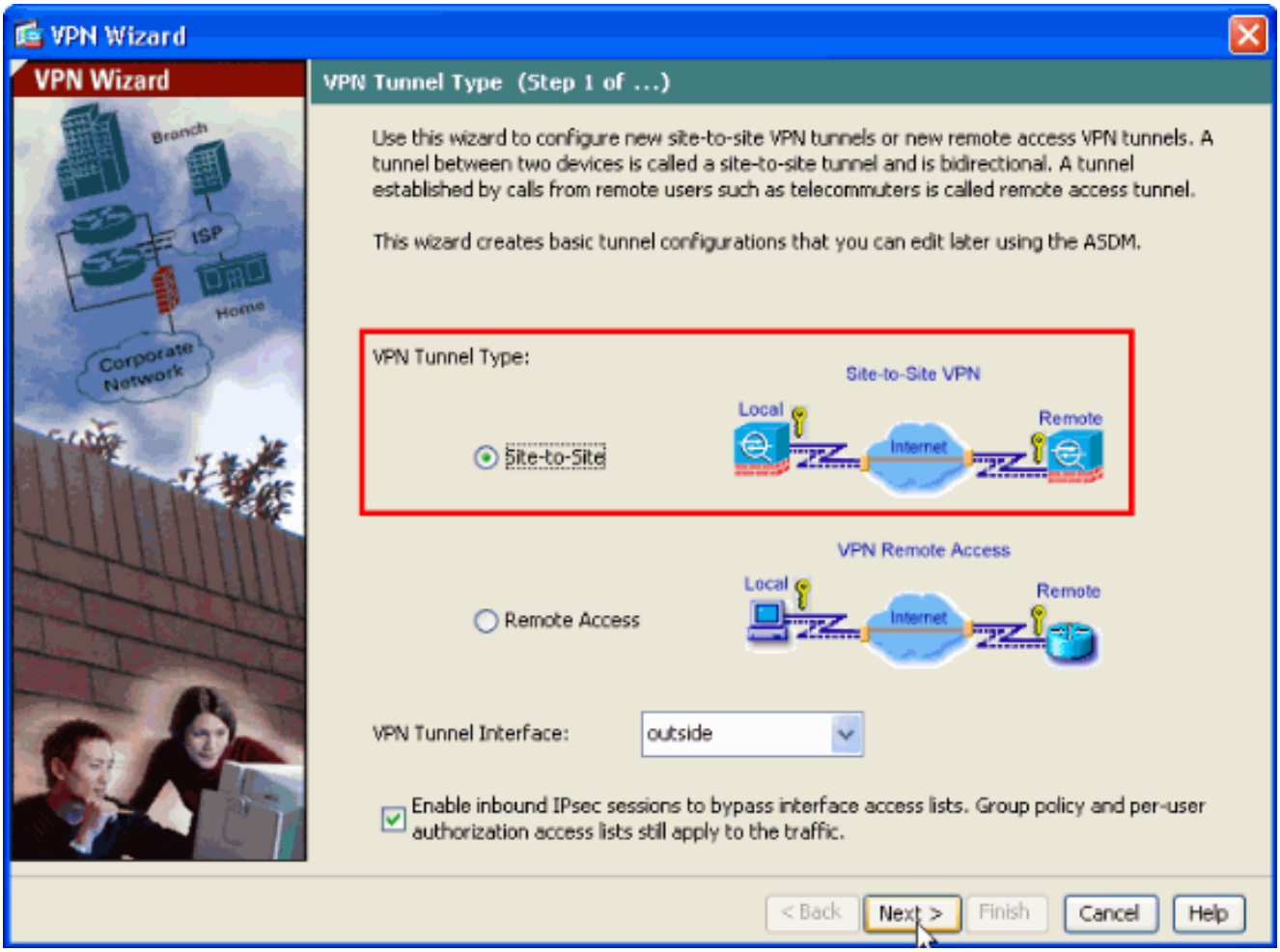


contraseña.

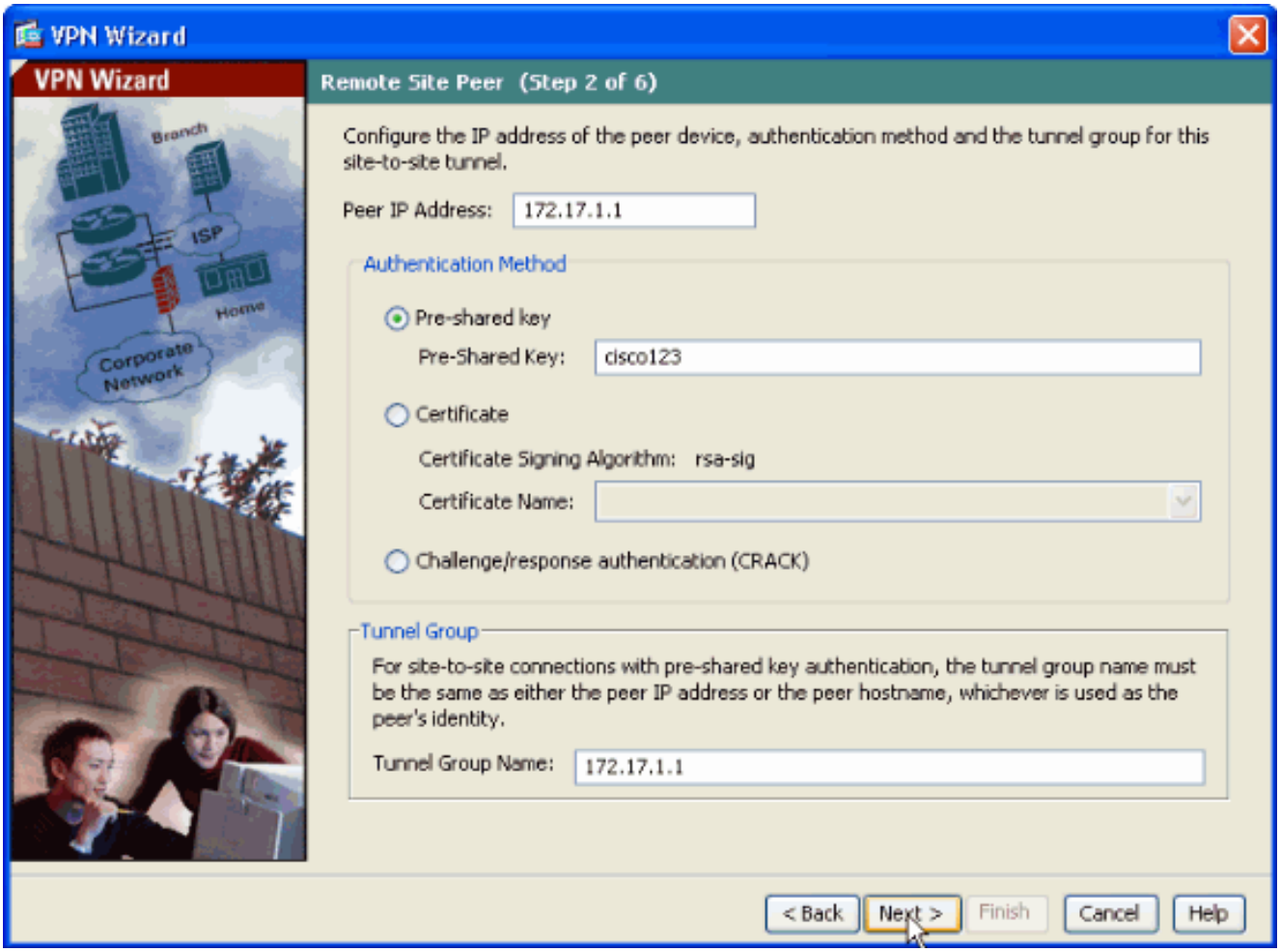
5. Funcione con al **Asisitente de IPsec VPN** una vez que la aplicación ASDM conecta con el ASA.



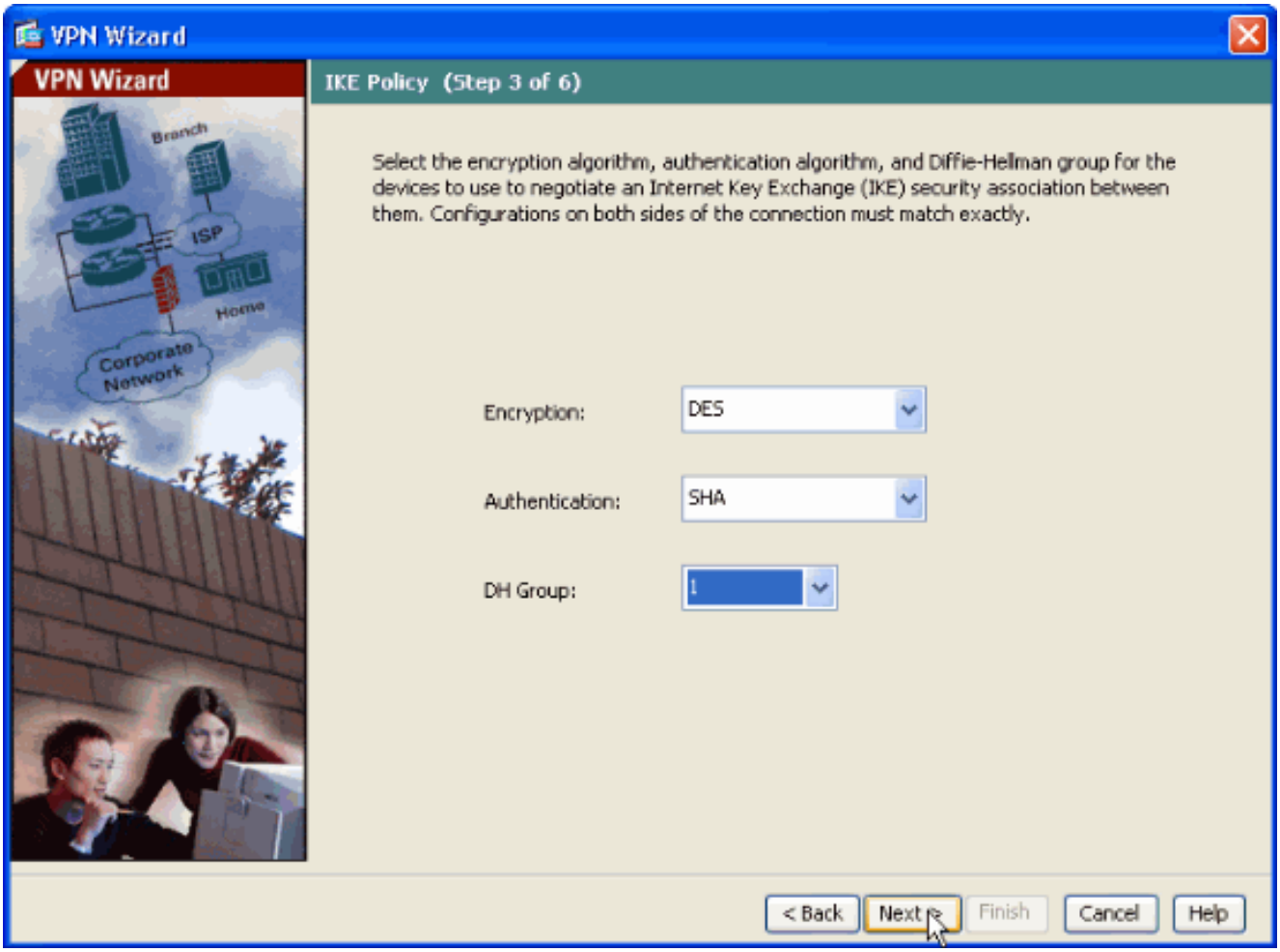
6. Elija **IPSec sitio a sitio el** tipo de túnel VPN y haga clic **después** como se muestra aquí.



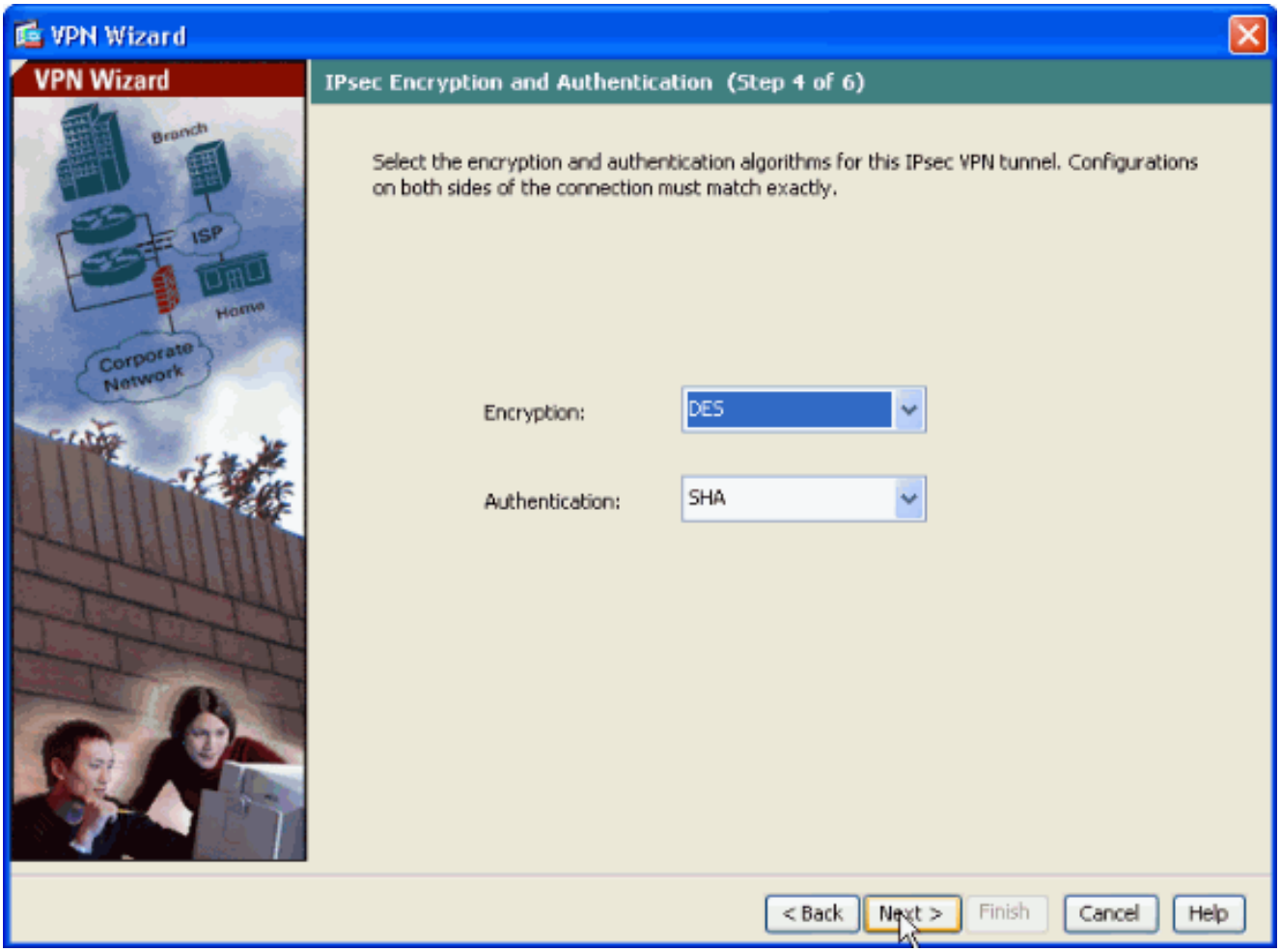
7. Especifique la dirección IP exterior del peer remoto. Ingrese la información de autenticación para utilizar, que es la clave previamente compartida en este ejemplo. La clave previamente compartida usada en este ejemplo es **cisco123**. **El nombre de grupo de túnel** será su dirección IP exterior por abandono si usted configura L2L VPN. Haga clic en Next (Siguiente).



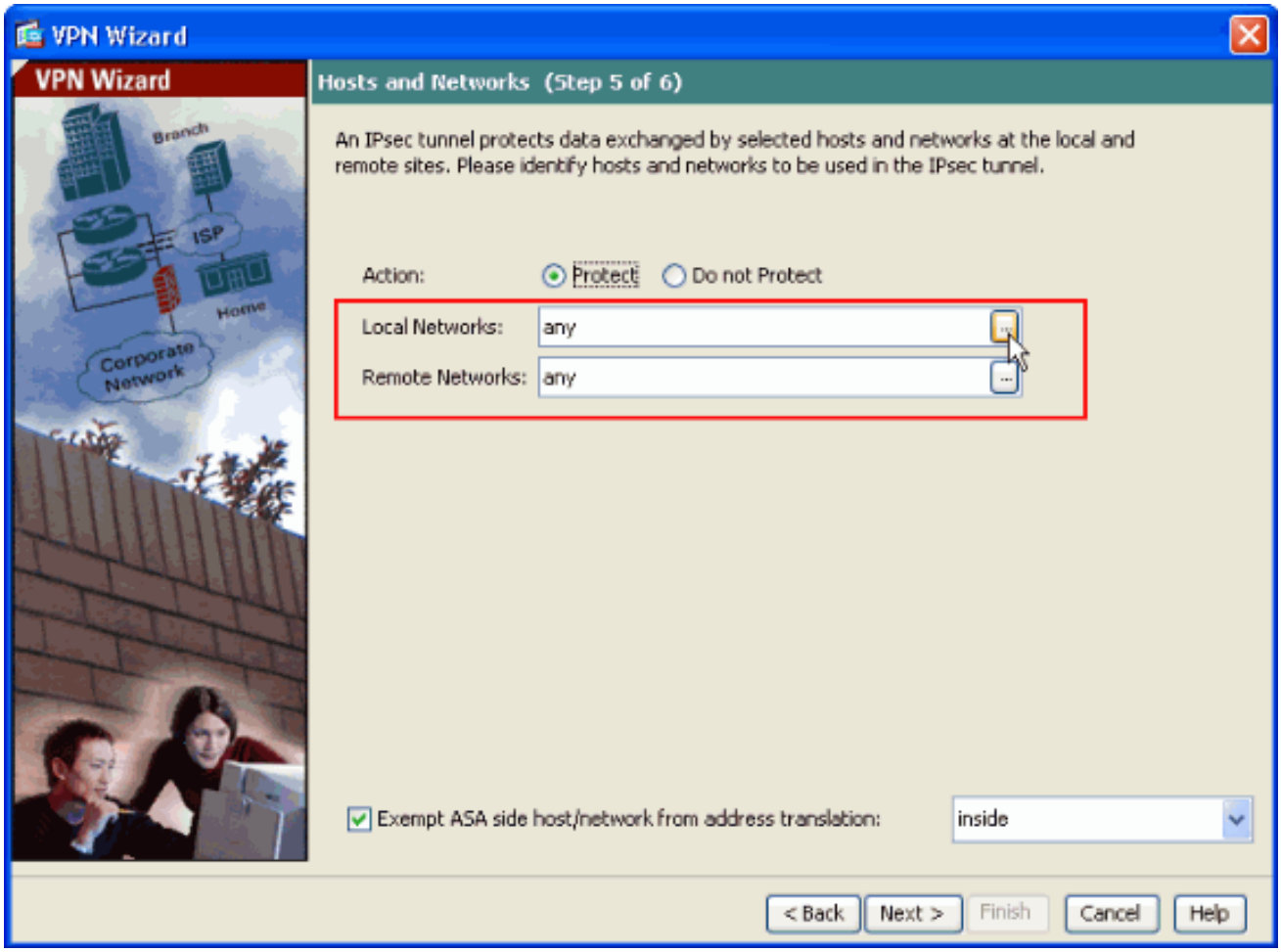
8. Especifique los atributos para utilizar para IKE, también conocido como fase 1. Estos atributos deben ser lo mismo en el ASA y el router IOS. Haga clic en Next (Siguiente).



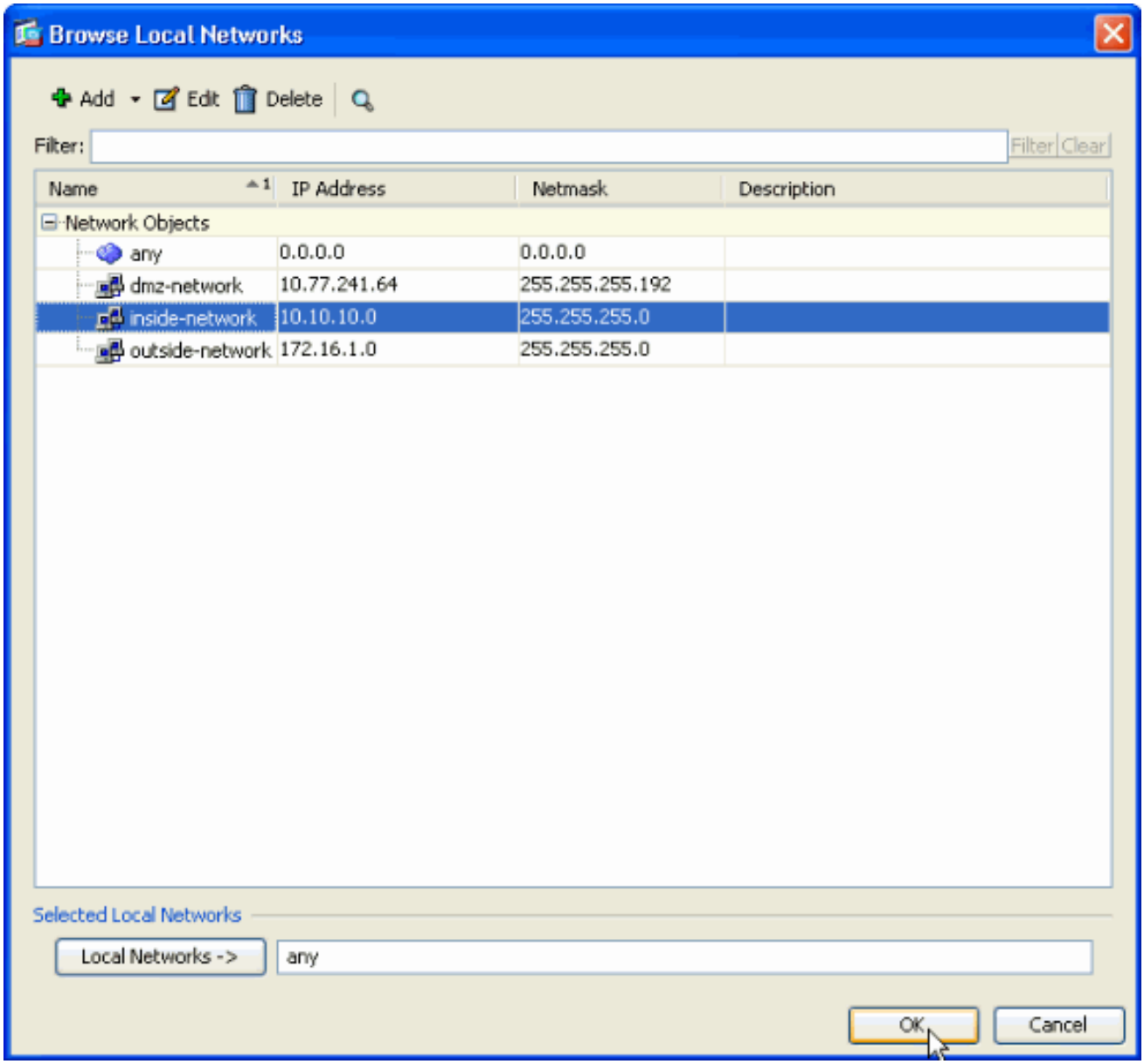
9. Especifique los atributos para utilizar para IPsec, también conocido como fase 2. Estos atributos deben hacer juego en el ASA y el router IOS. Haga clic en Next (Siguiente).



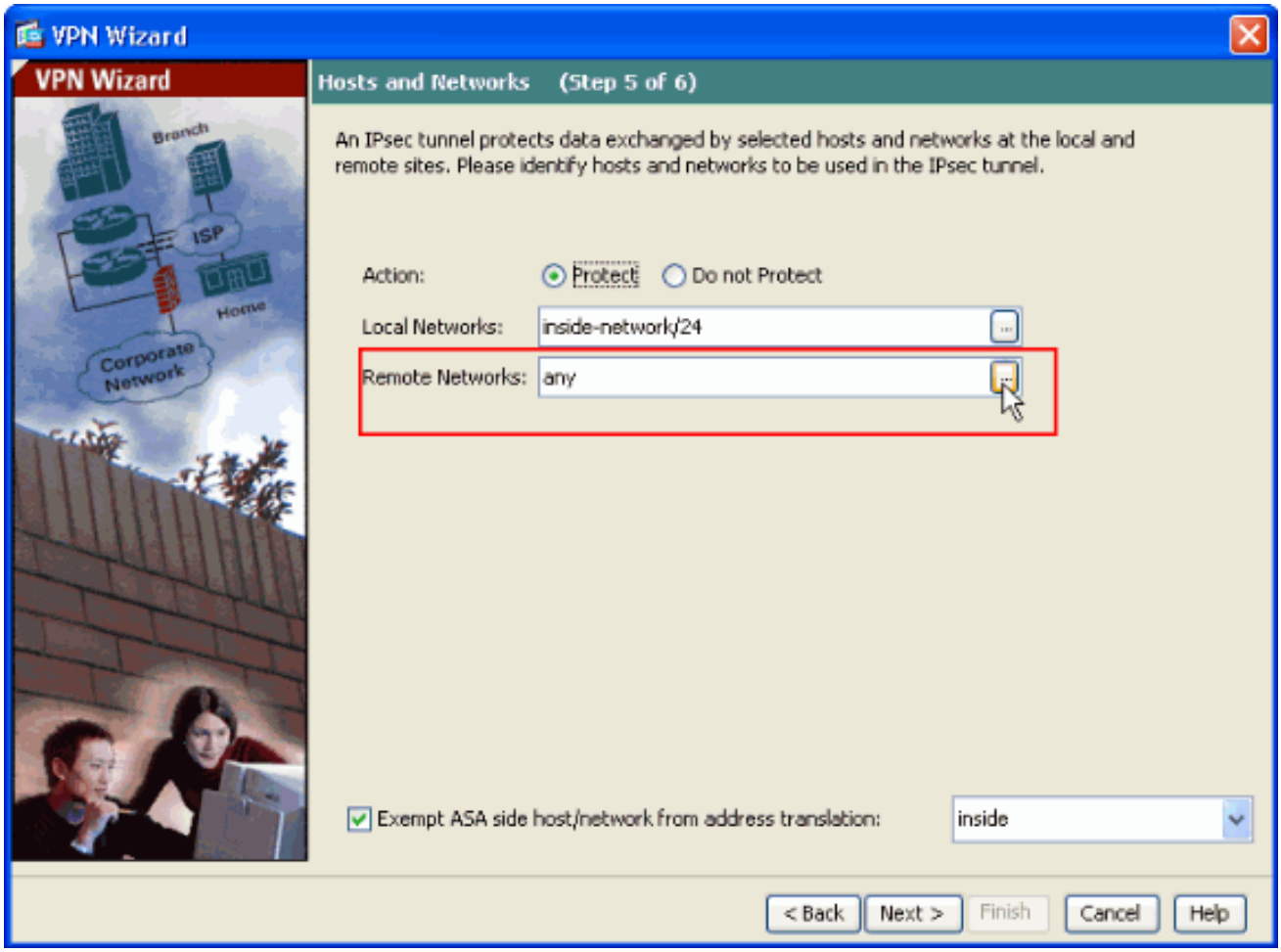
10. Especifique a los host cuyo tráfico se debe permitir pasar a través del túnel VPN. En este paso, usted tiene que proporcionar a las **redes locales y remotas** para el túnel VPN. Haga clic el botón al lado de las **redes locales** como se muestra aquí para elegir el direccionamiento de red local del menú desplegable.



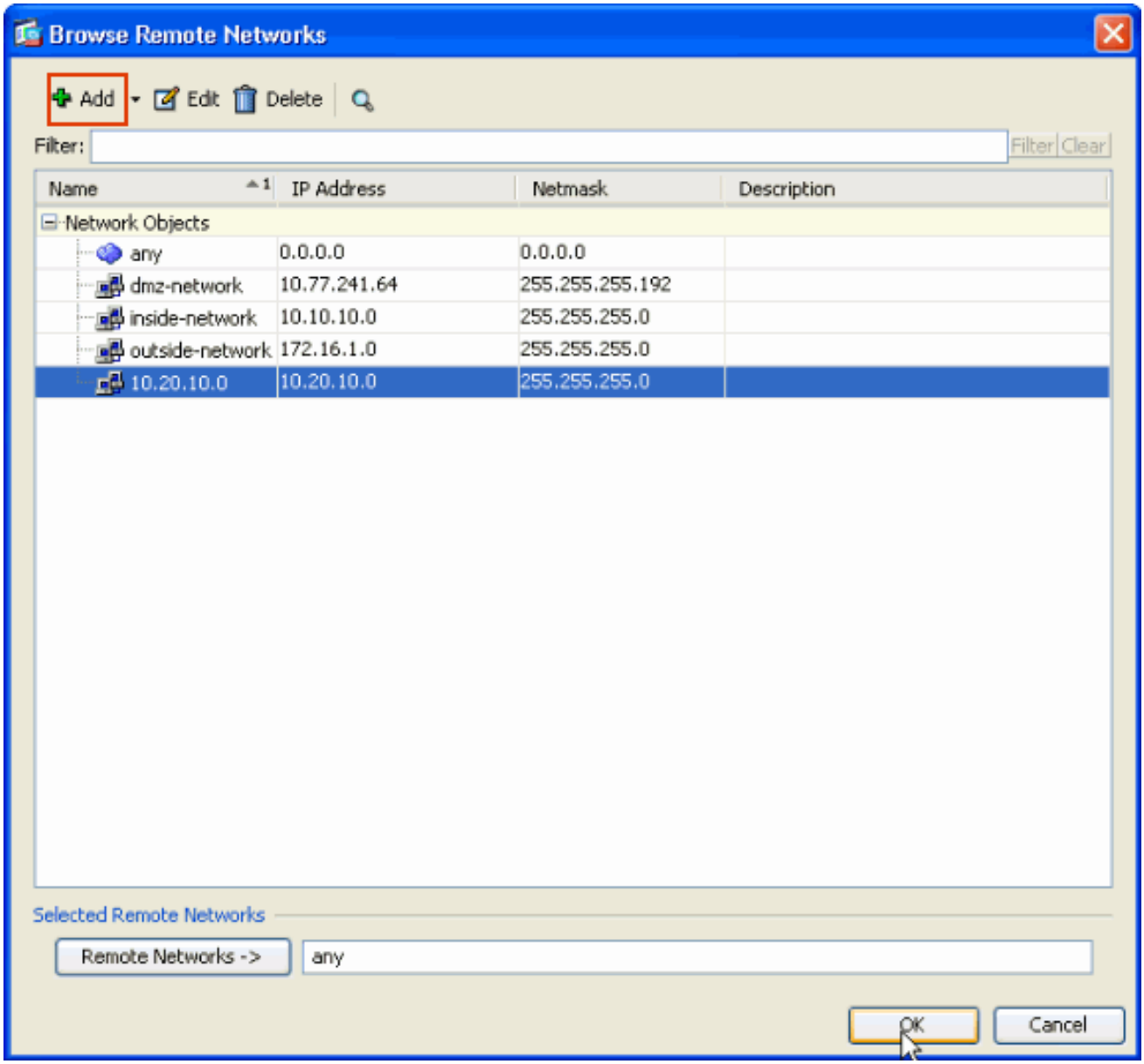
11. Elija el direccionamiento de **red local**, después haga clic la **AUTORIZACIÓN** como se muestra
aquí.



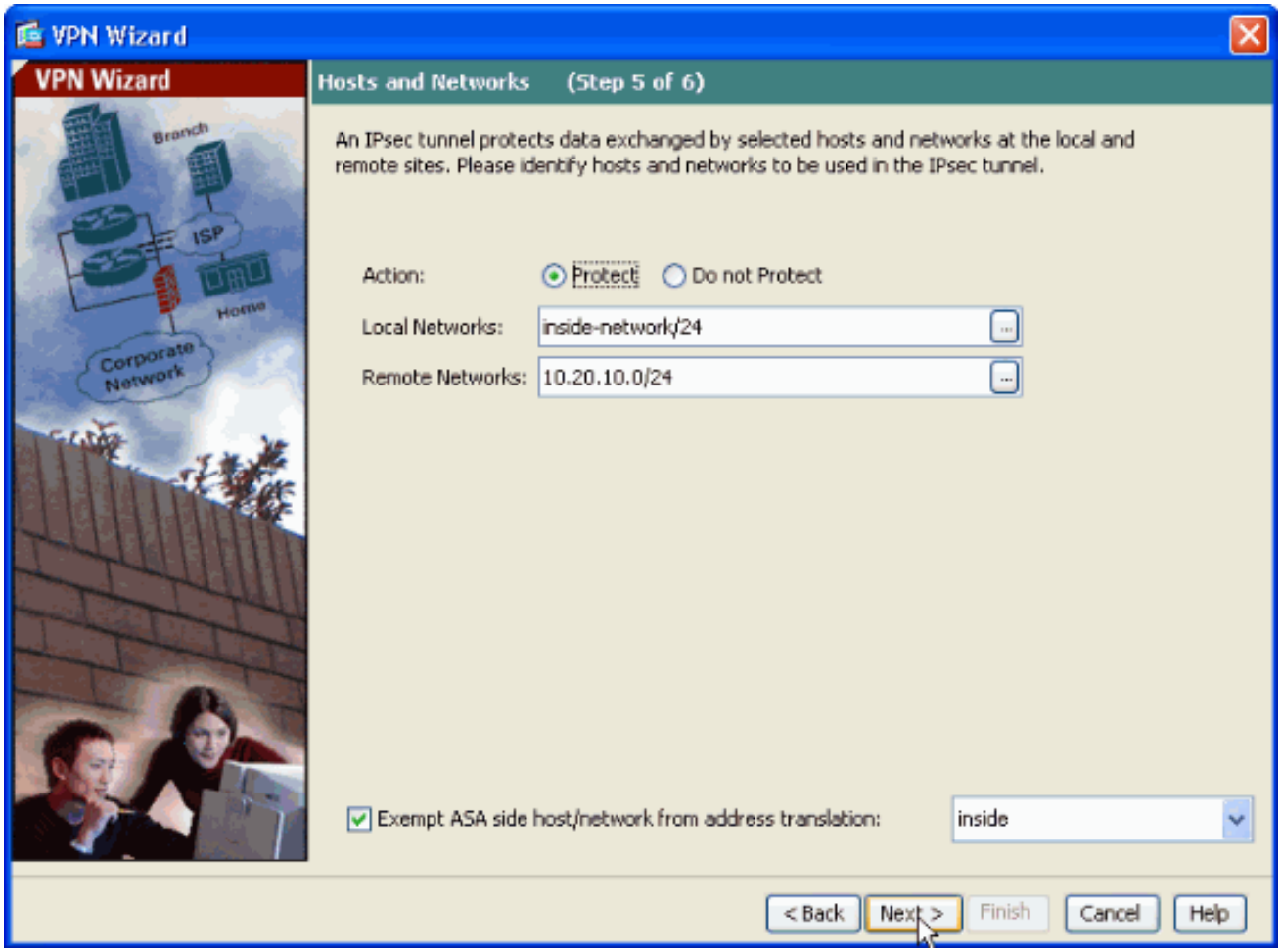
12. Haga clic el botón al lado de las **redes remotas** como se muestra aquí para elegir el direccionamiento de red remota del menú desplegable.



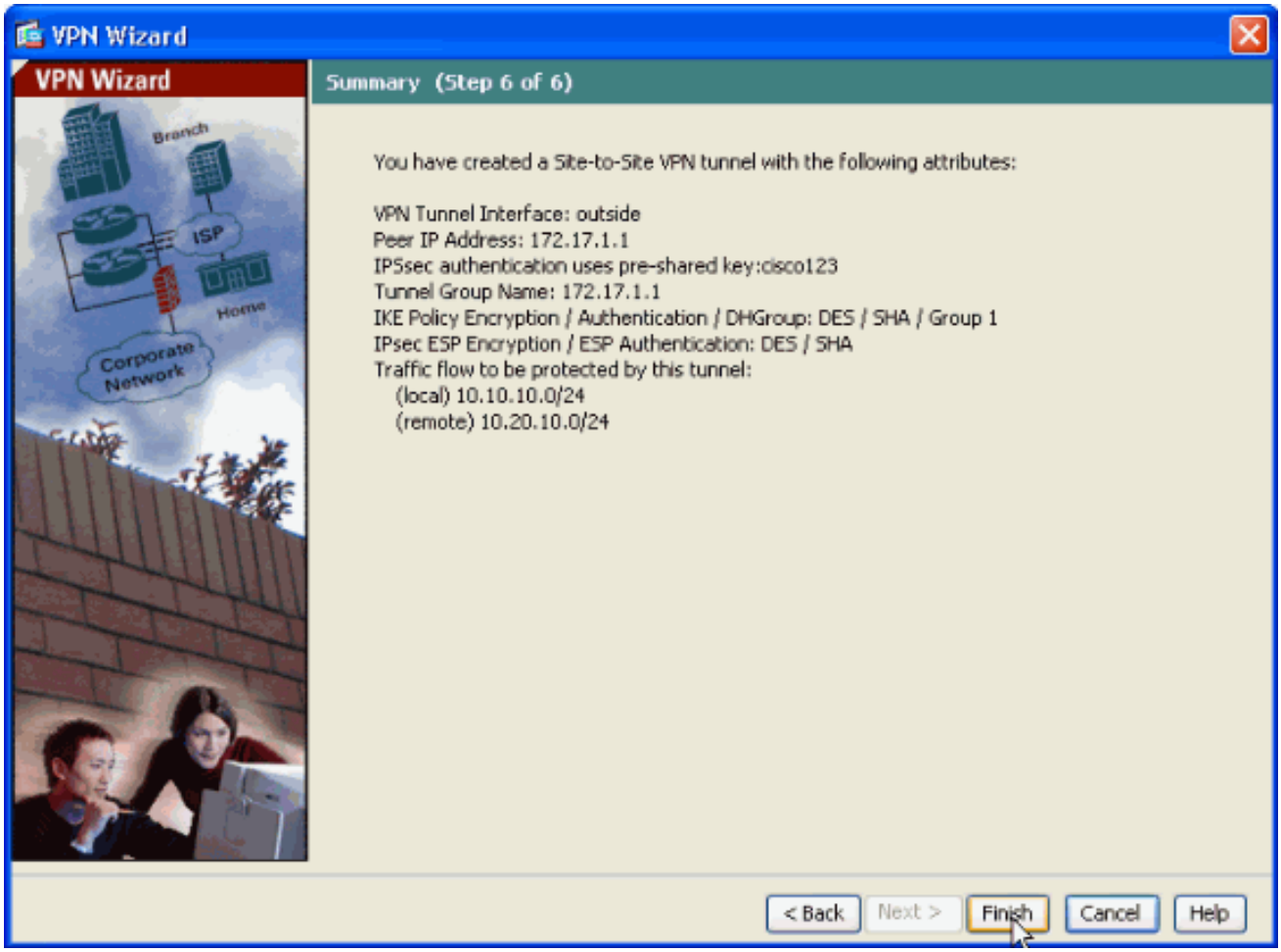
13. Elija el direccionamiento de **red remota**, después haga clic la **AUTORIZACIÓN** como se muestra aquí.**Nota:** Si usted no tiene la red remota en la lista entonces la red tiene que ser agregada a la lista haciendo clic
agrega.



14. Controle el **host/la red exentos del lado ASA del** checkbox de la **traducción de la dirección** para evitar que el tráfico de túnel experimente la **traducción de la dirección de red**. Entonces, haga clic
después.



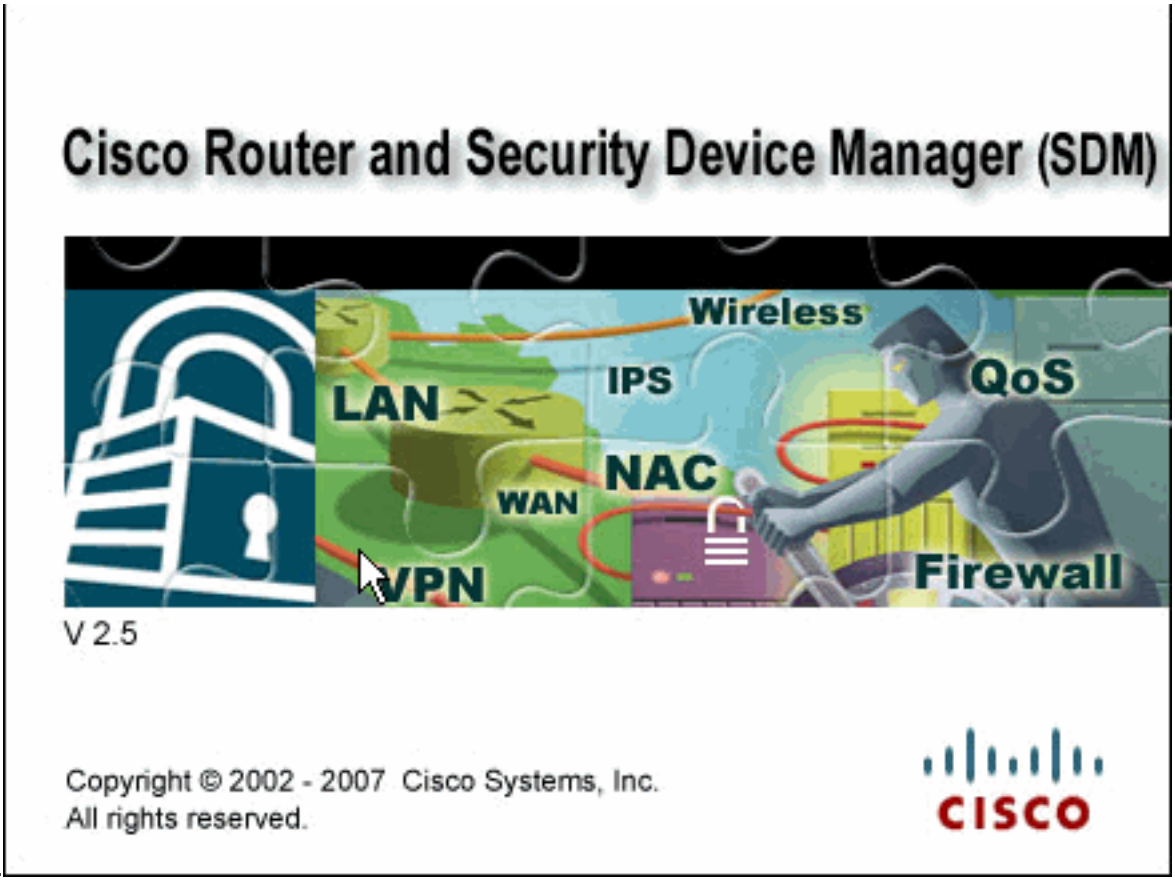
15. Los atributos definidos por el Asisitente VPN se visualizan en este resumen. Compruebe la configuración con minuciosidad y el clic en Finalizar cuando le satisfacen las configuraciones está
correcto.



Configuración de SDM del router

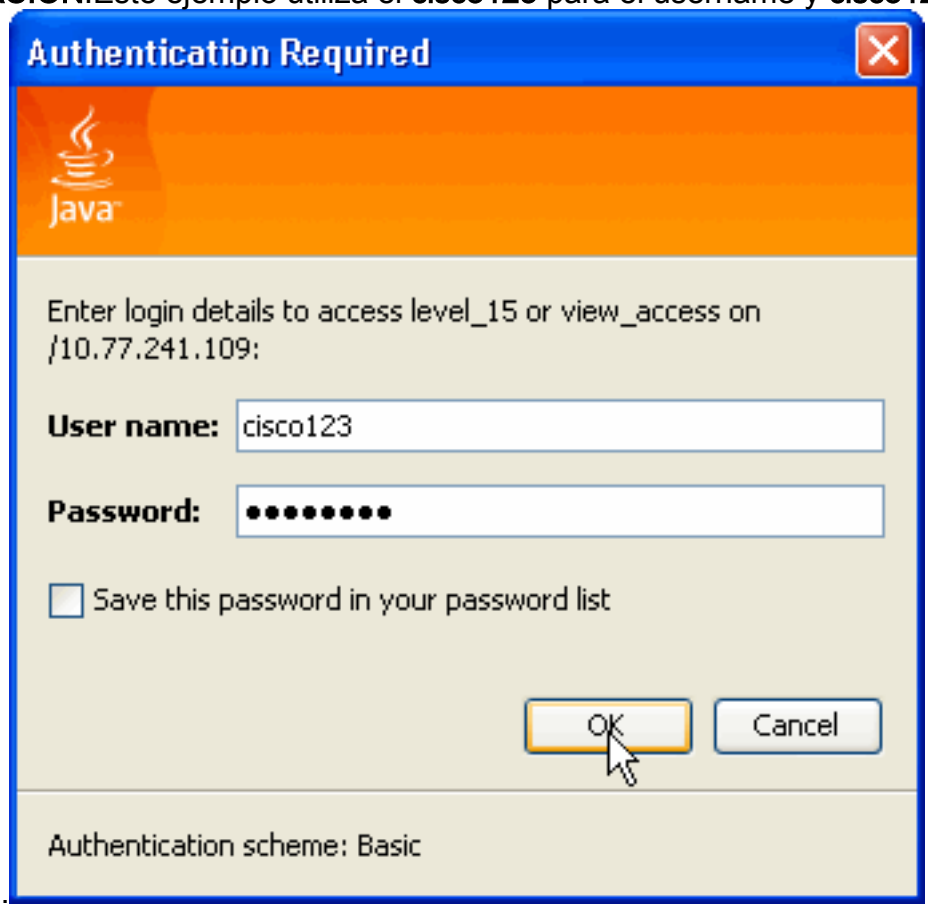
Complete estos pasos para configurar el túnel del VPN de sitio a sitio en el router del Cisco IOS:

1. Abra su hojeador y ingrese los **<IP_Address de https:// del interfaz del ranurador que se ha configurado para SDM Access>** para tener acceso al SDM en el ranurador.Asegúrese de autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad del certificado SSL. Nombre de usuario y contraseña del valor por defecto es ambos espacio en blanco.El router presenta esta ventana para permitir la transferencia directa de la aplicación SDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en un Java



applet.

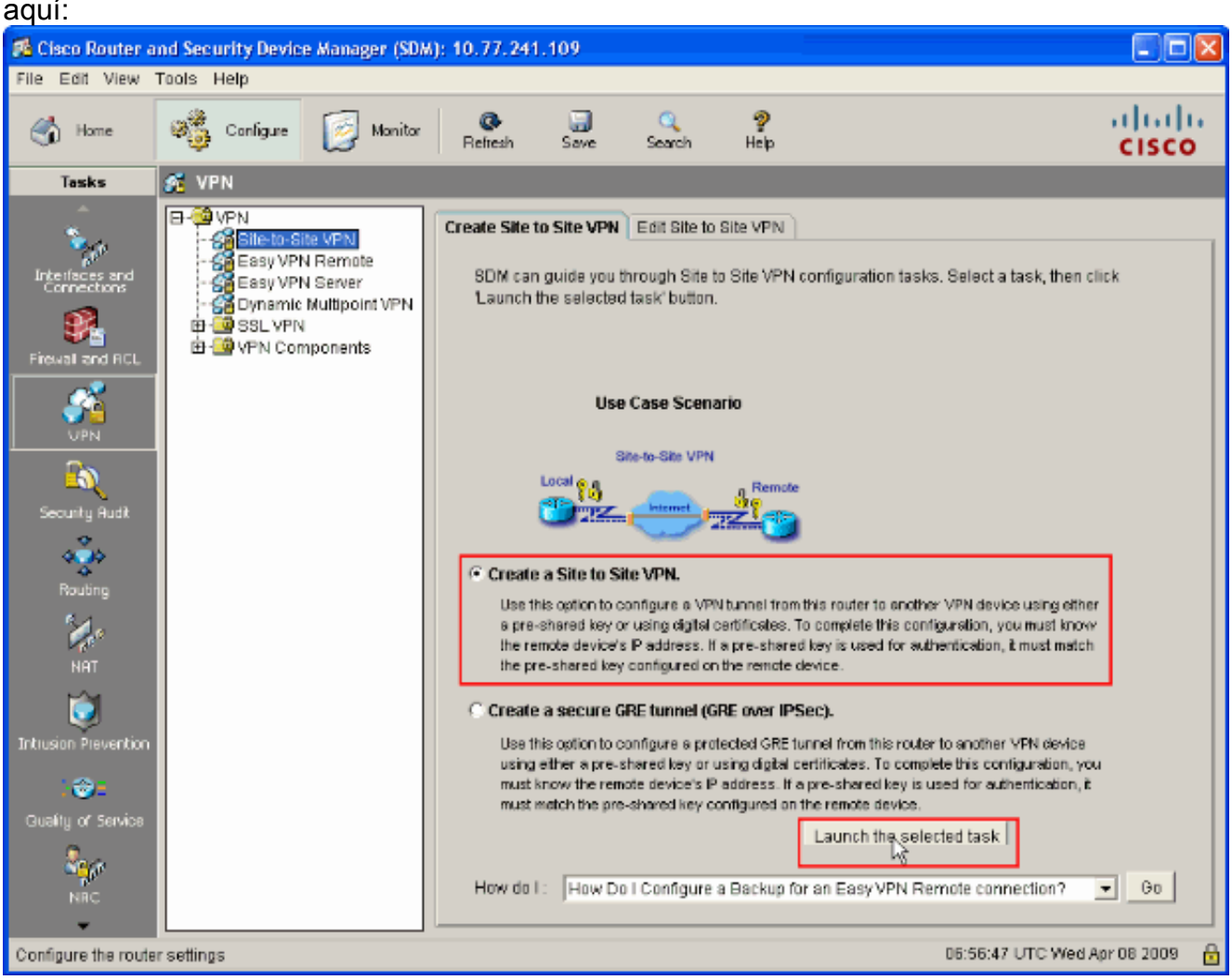
2. La transferencia directa SDM ahora comienza. Una vez que las transferencias directas del lanzador SDM, completan los pasos ordenados por los mensajes para instalar el software y funcionar con el lanzador de Cisco SDM.
3. Ingrese el **nombre de usuario y contraseña** si usted especificó uno y hace clic la **AUTORIZACIÓN**.Este ejemplo utiliza el **cisco123** para el username y **cisco123** como la



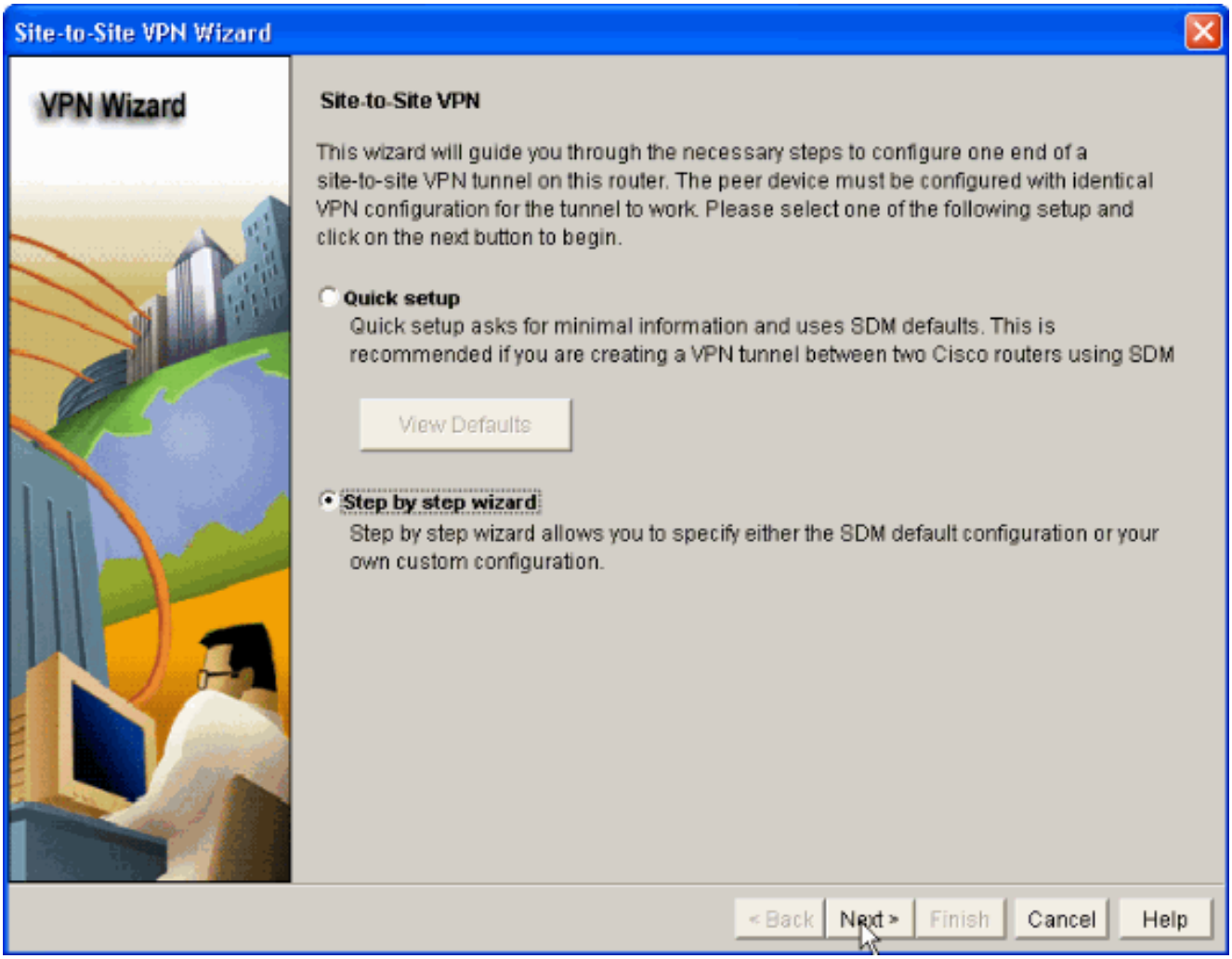
contraseña.

4. Elija **Configuration->VPN->Site-to-Site VPN** y haga clic el botón de radio al lado de **crean un**

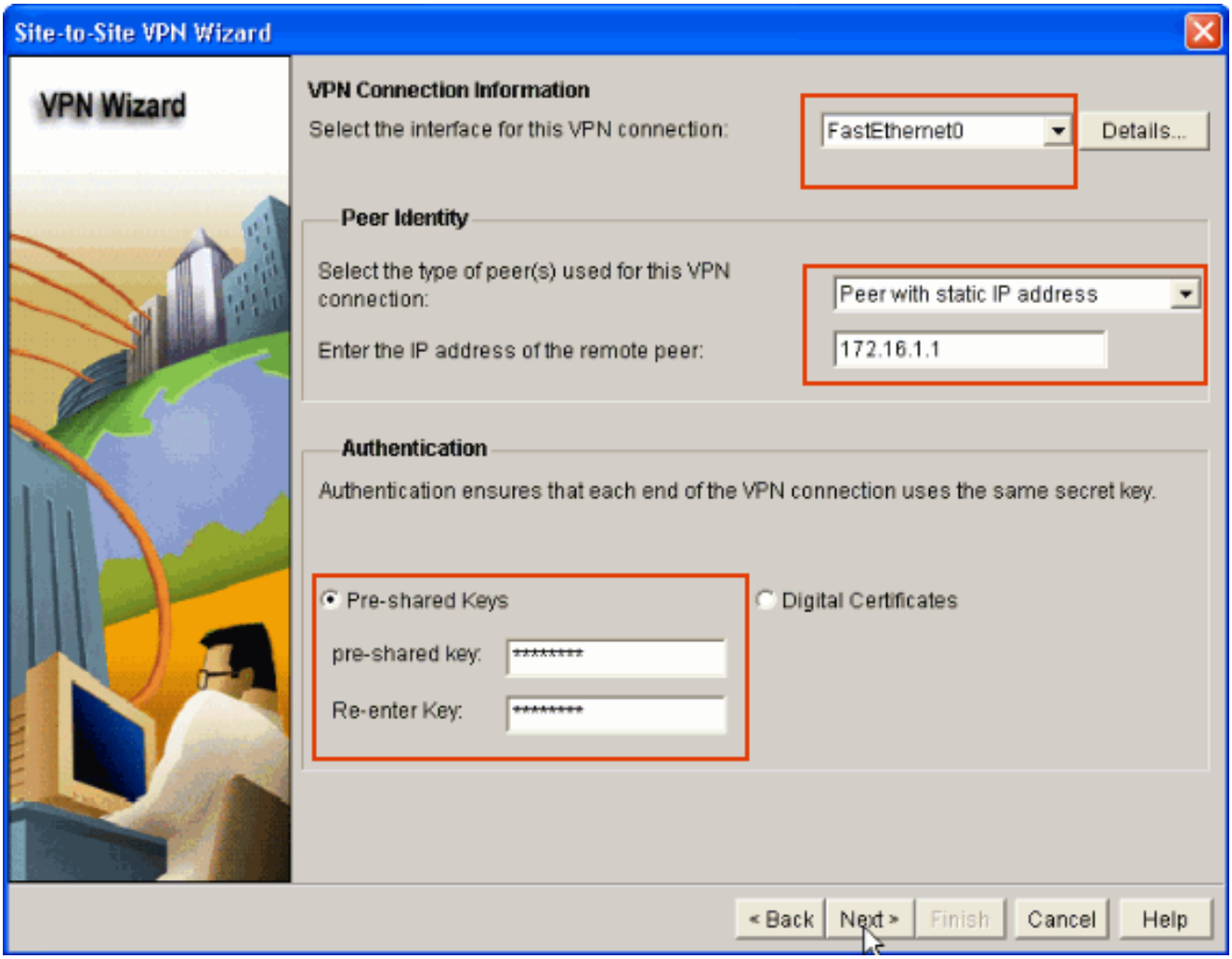
VPN de sitio a sitio en el Home Page SDM. Entonces, **lanzamiento del** tecleo la **tarea seleccionada** como se muestra
aquí:



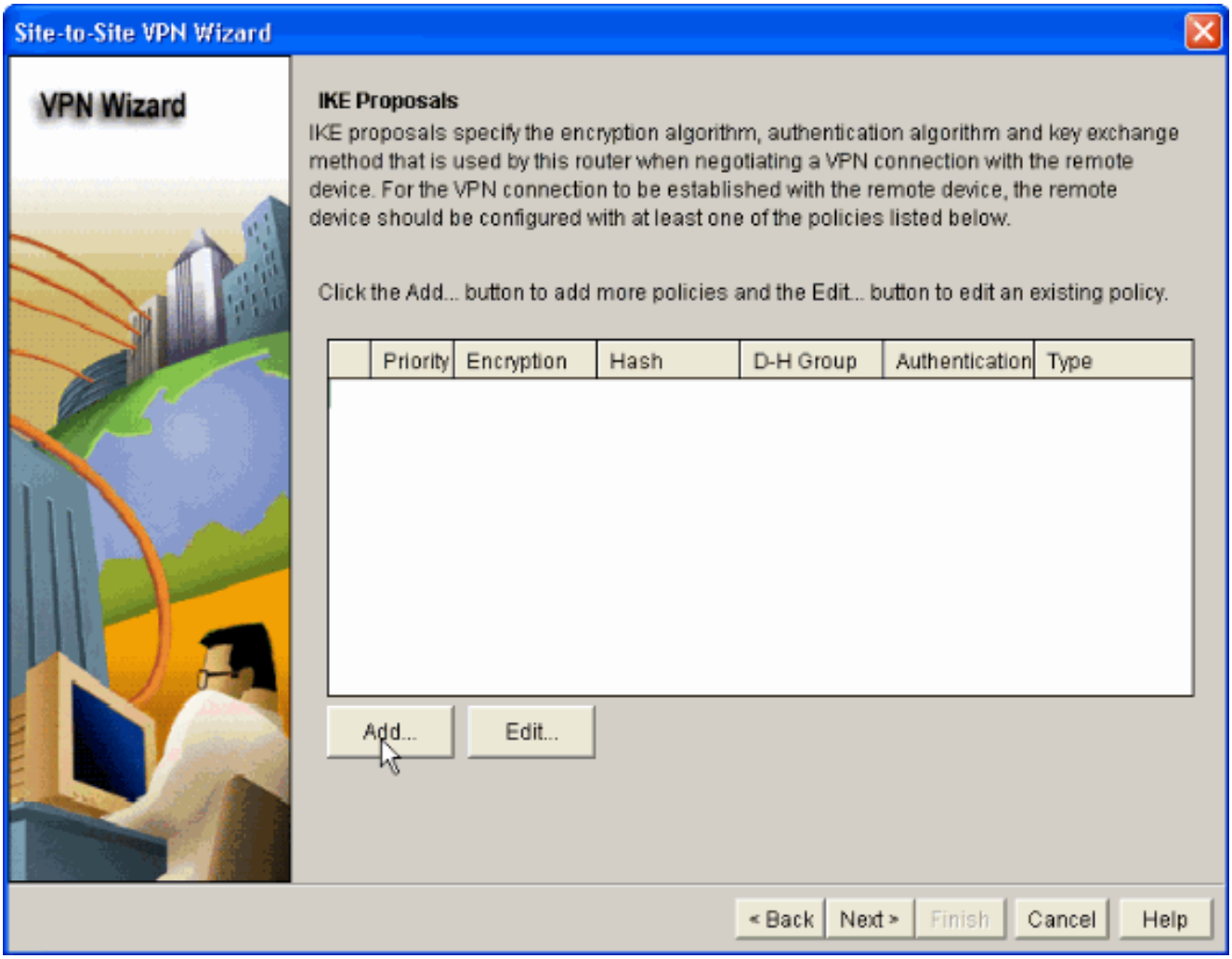
5. Elija al **Asisitente gradual** para proceder con la configuración:



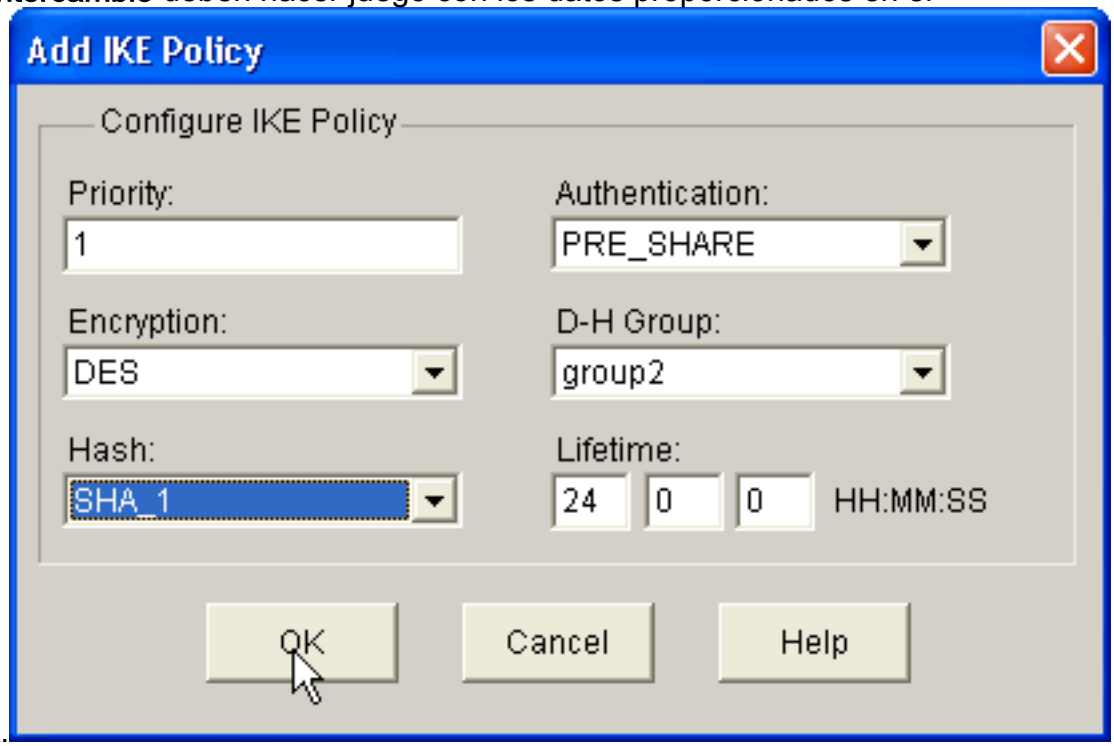
6. En la próxima ventana proporcione a la **información de la conexión VPN** en los espacios respectivos. Seleccione el interfaz del túnel VPN del menú desplegable. Aquí, se elige **FastEthernet0**. En la sección de la **identidad del par**, elija al **par con la dirección IP estática** y proporcione a la dirección IP del peer remoto. Entonces, proporcione a la **clave previamente compartida** (**cisco123** en este ejemplo) en la sección de la autenticación como se muestra. Entonces, haga clic
después.



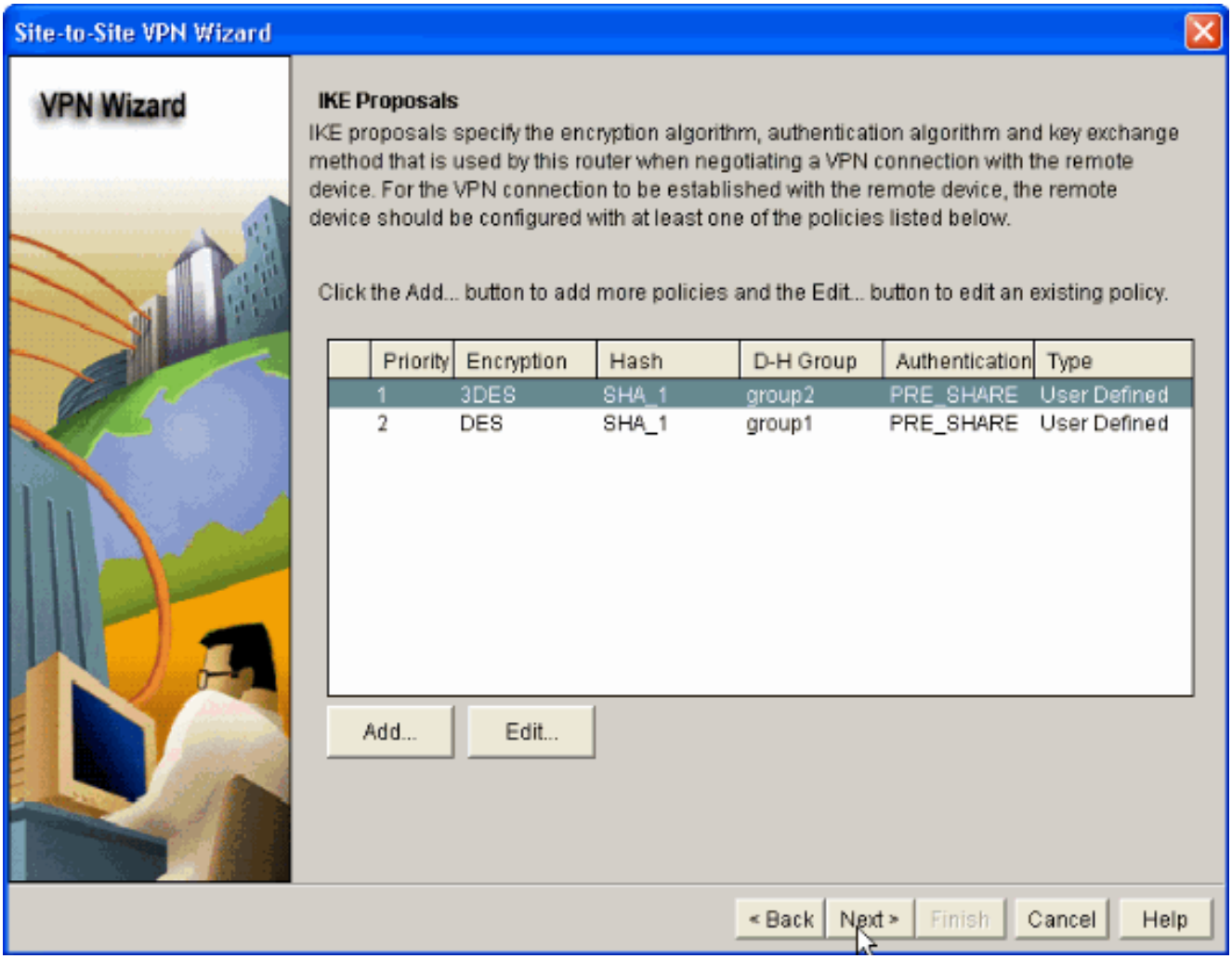
7. El tecleo **agrega** para agregar las propuestas IKE que especifica el **algoritmo de encripción, el algoritmo de la autenticación** y el **método dominante del intercambio**.



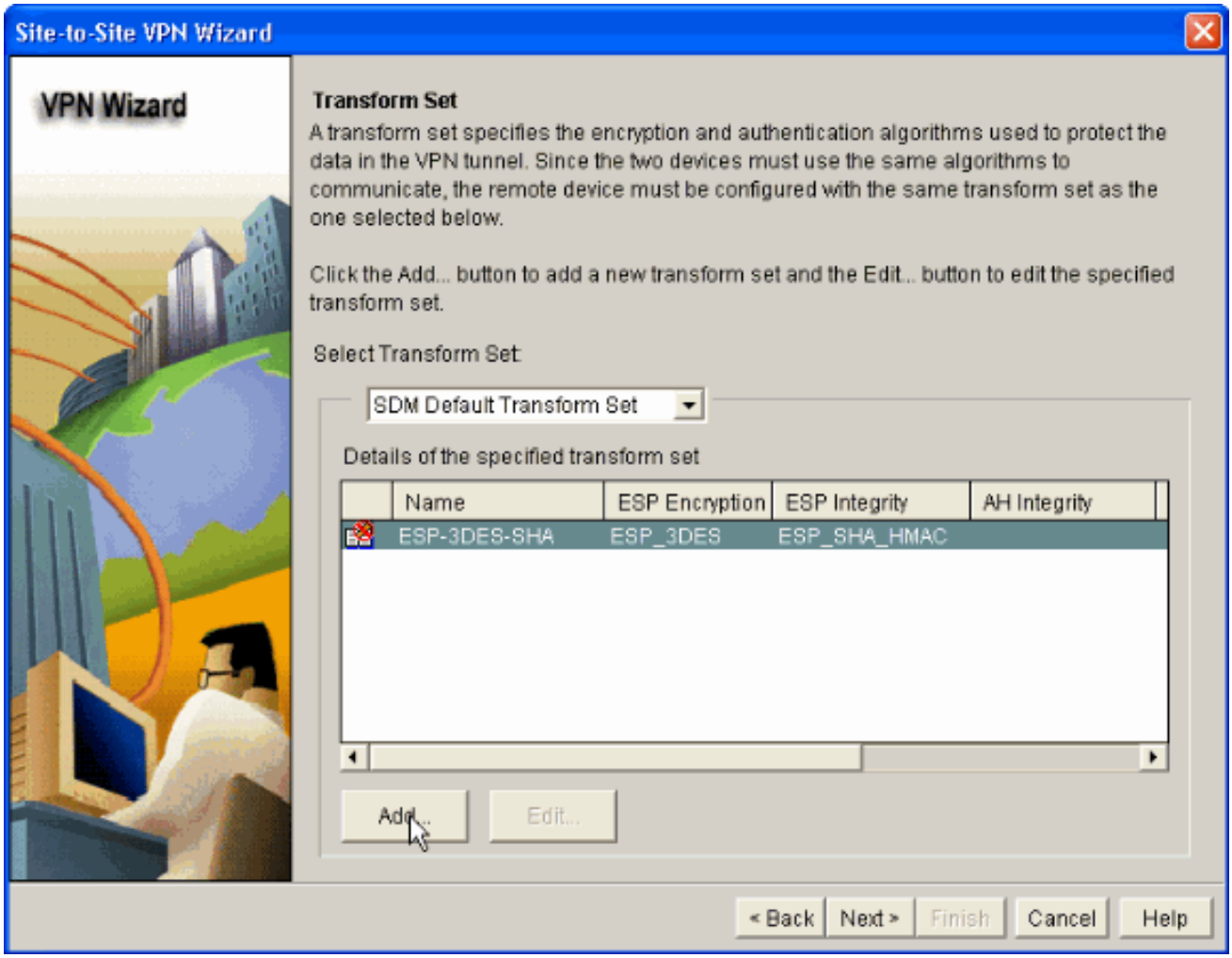
8. Proporcione al **algoritmo de encripción**, al **algoritmo de la autenticación** y al **método dominante del intercambio** como se muestra aquí, después haga clic la **AUTORIZACIÓN**. El **algoritmo de encripción**, el **algoritmo de la autenticación** y los valores **dominantes del método del intercambio** deben hacer juego con los datos proporcionados en el ASA.



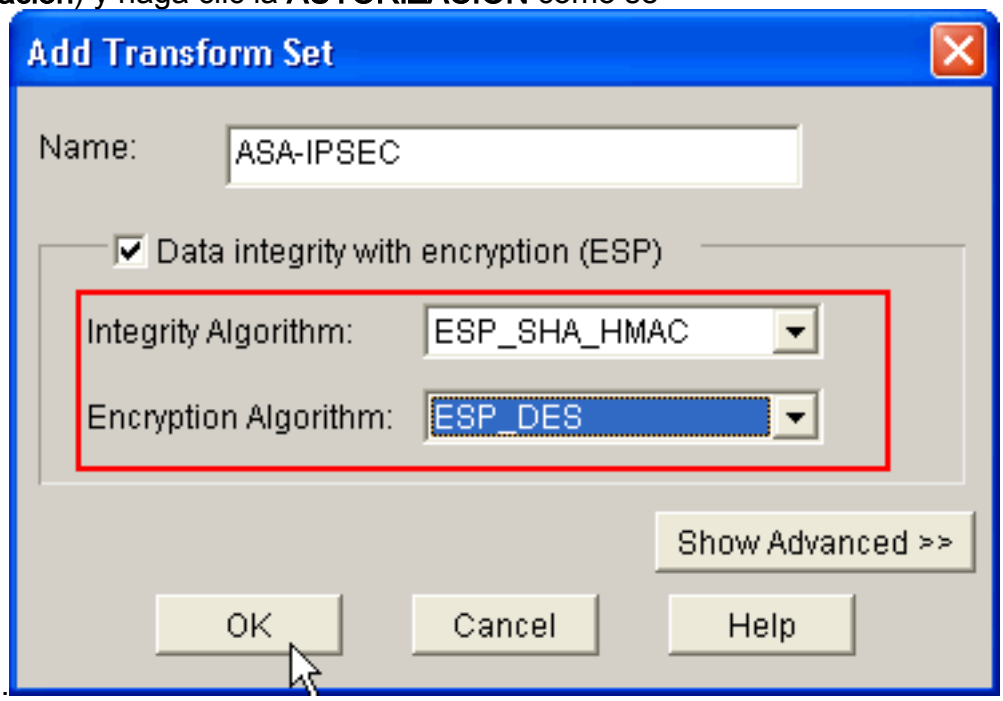
9. Tecleo **después** como se muestra aquí.



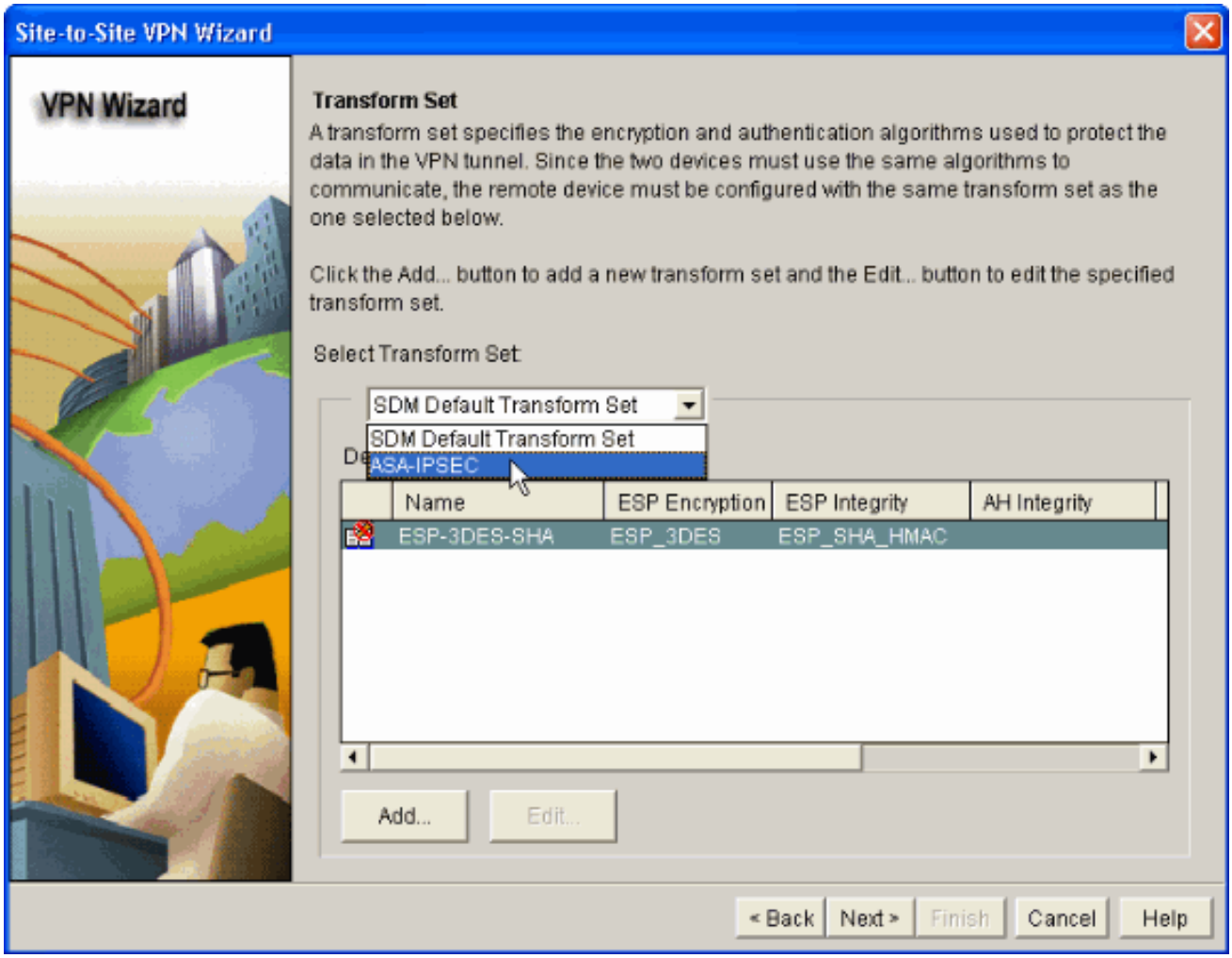
10. En esta nueva ventana los detalles **determinados de la transformación** deben ser proporcionados. El conjunto de la transformación especifica el **cifrado** y los algoritmos de la **autenticación** usados para proteger los **datos en el VPN hacen un túnel**. Entonces, el tecleo **agrega** para proporcionar a estos detalles. Usted puede agregar cualquier número de conjuntos Transform según las necesidades haciendo clic **agrega** y proporcionando a los detalles.



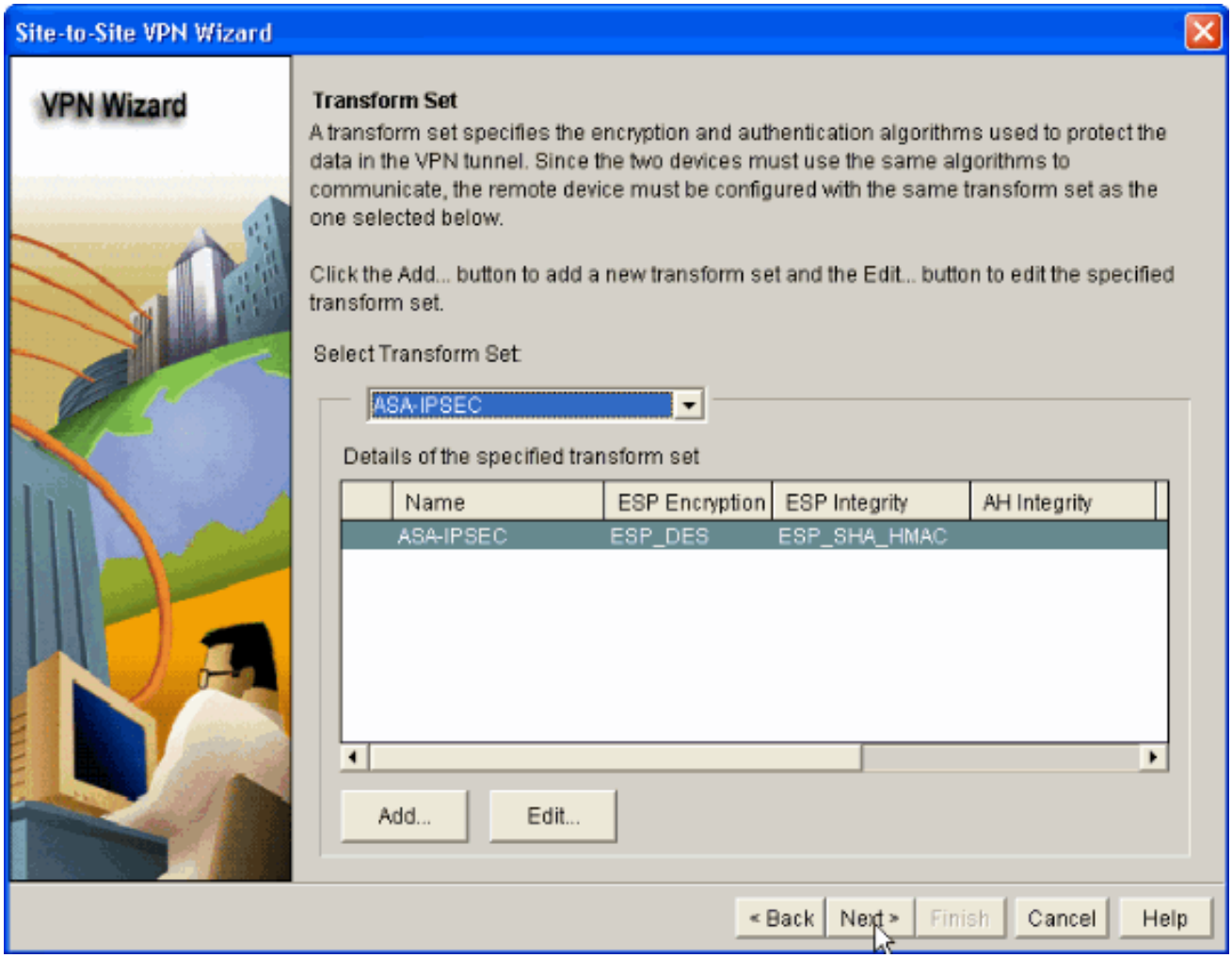
11. Proporcione a los detalles **determinados de la transformación** (**algoritmo del cifrado y de la autenticación**) y haga clic la **AUTORIZACIÓN** como se muestra.



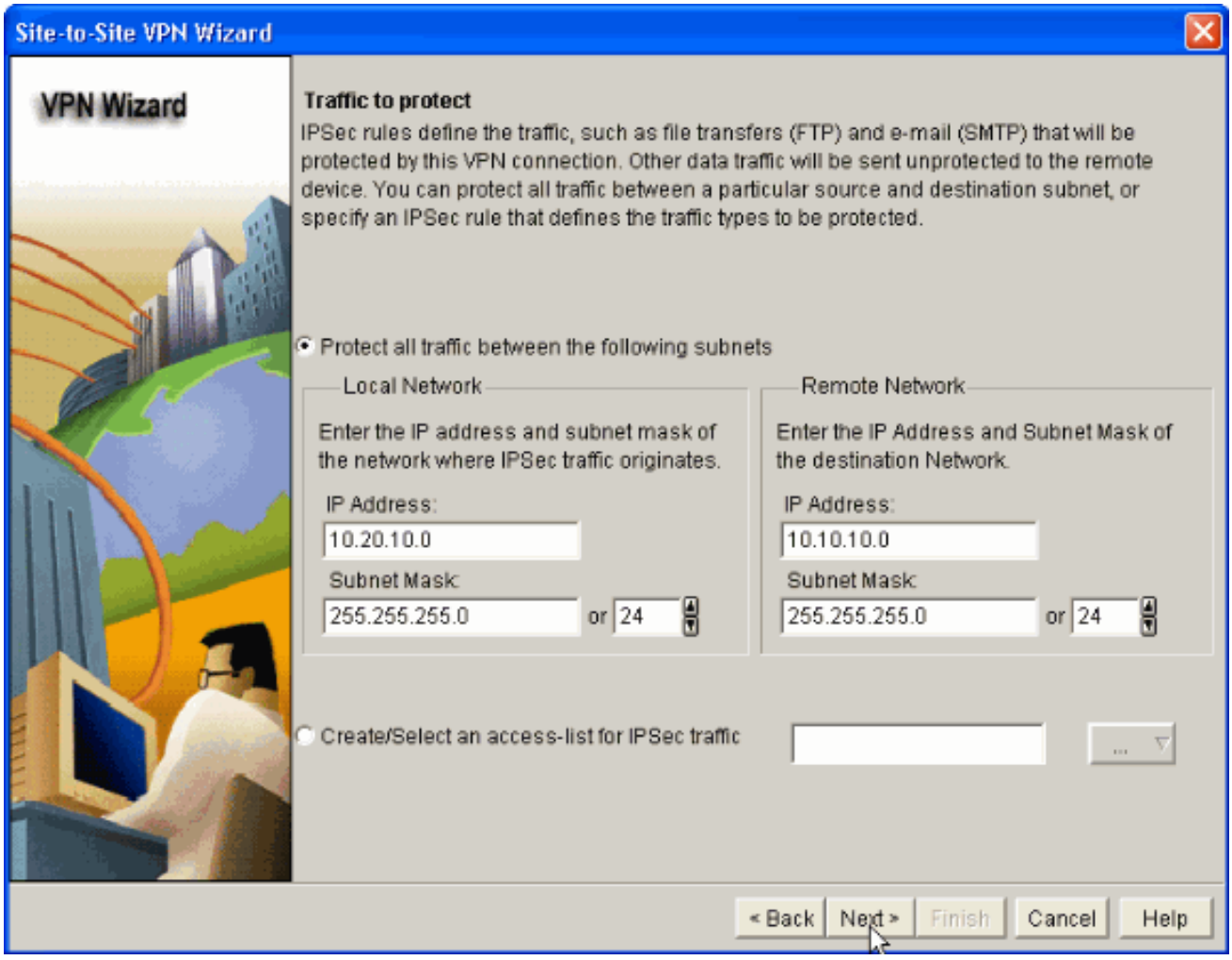
12. Elija requerido **transforman el conjunto** que se utilizará del menú desplegable como se muestra.



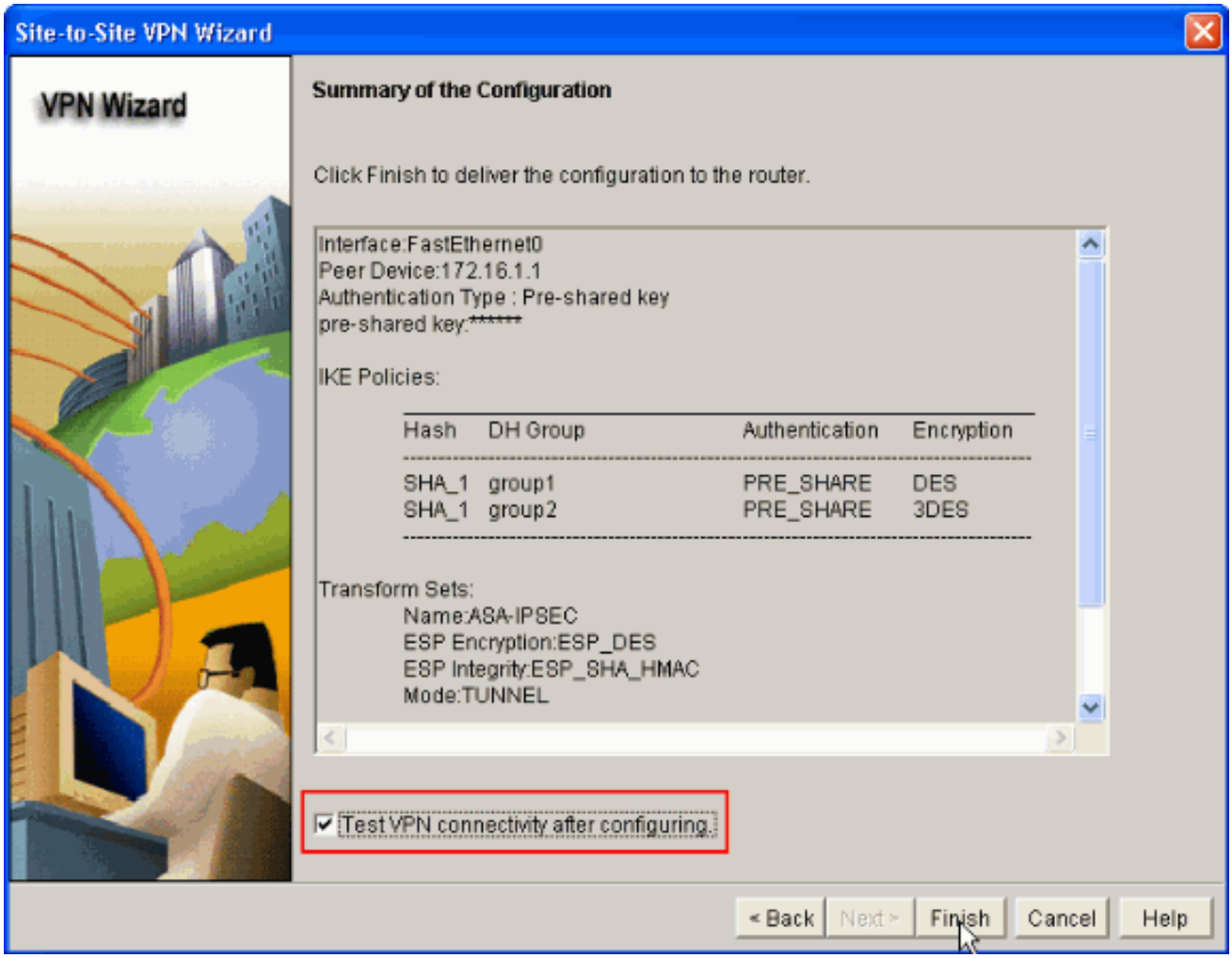
13. Haga clic en Next (Siguiente).



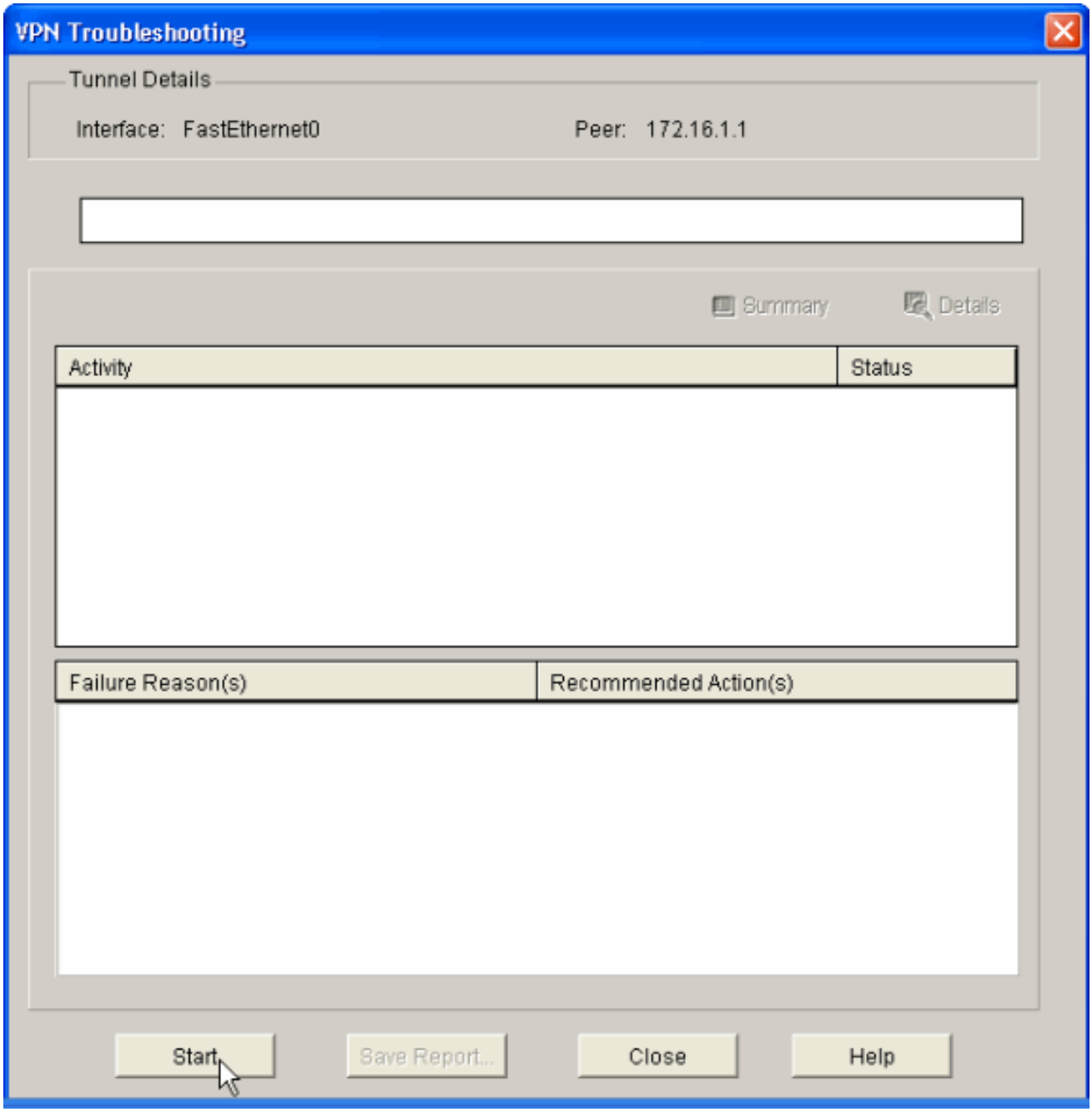
14. En la ventana siguiente proporcione a los detalles sobre el **tráfico que se protegerá** a través del túnel VPN. Proporcione a la **fuente y a las redes de destino del** tráfico que se protegerá para proteger el tráfico entre la fuente y las redes de destino especificadas. En este ejemplo, la red de origen es 10.20.10.0 y la red de destino es 10.10.10.0. Entonces, haga clic
después.



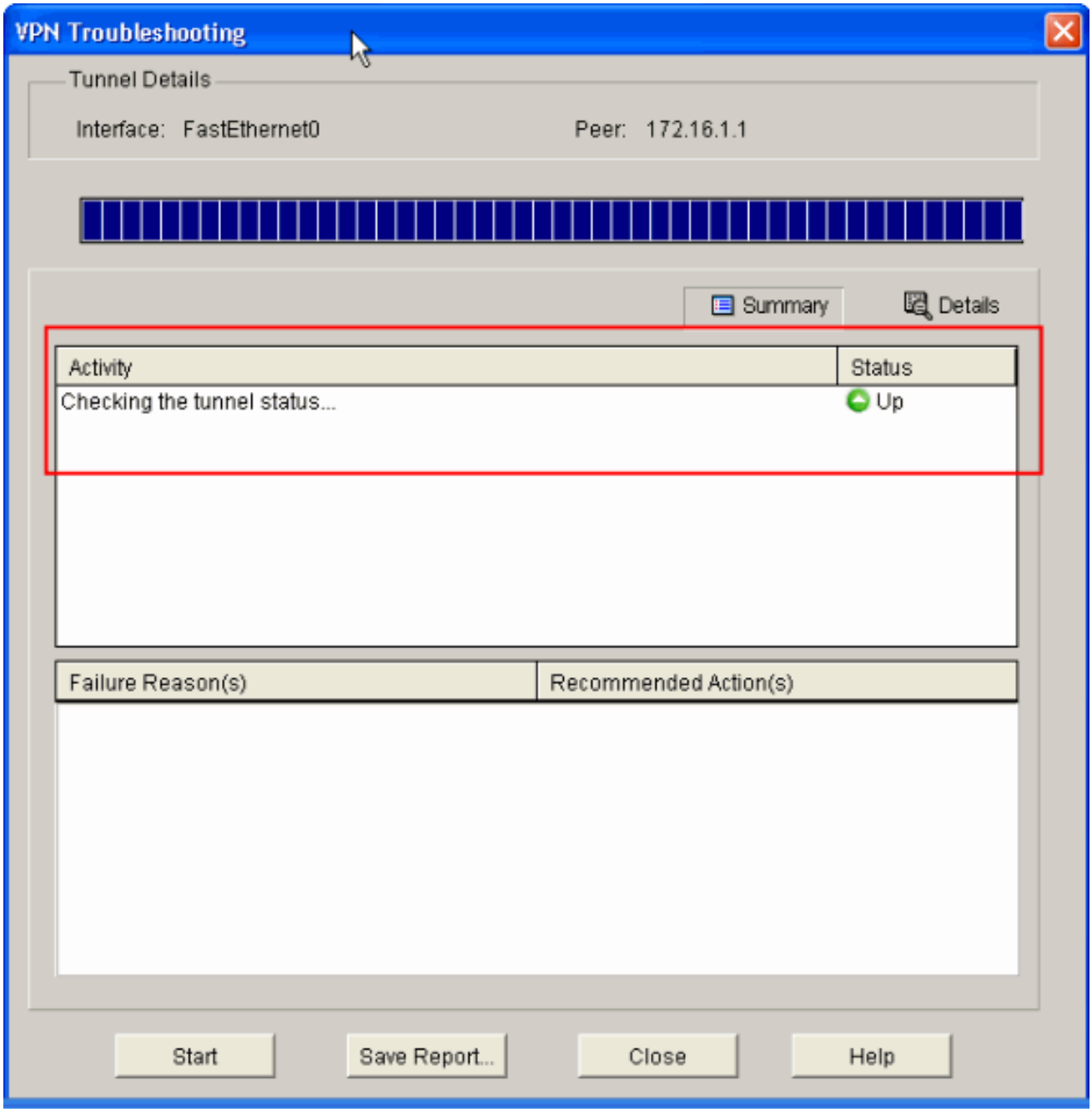
15. Esta ventana muestra el resumen de la configuración del VPN de sitio a sitio hecha. Controle la **conectividad VPN de la prueba después de configurar la** casilla de verificación si usted quiere probar la conectividad VPN. Aquí, se controla el cuadro mientras que la Conectividad necesita ser controlada. Entonces, clic en Finalizar.



16. **Comienzo del** tecleo como se muestra para controlar la conectividad VPN.



17. En la próxima ventana que el resultado de la **conectividad VPN prueba** se proporciona. Aquí, usted puede ver si el túnel está **hacia arriba o hacia abajo**. En este ejemplo de configuración, el túnel está **para arriba** tal y como se muestra en de verde.



Esto completa la configuración en el router del Cisco IOS.

Configuración CLI ASA

ASA

```
ASA#show run
: Saved
ASA Version 8.0(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configure the outside interface. ! interface
Ethernet0/1 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 !--- Configure the inside
interface. ! interface Ethernet0/2 nameif inside
security-level 100 ip address 10.10.10.1 255.255.255.0
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
```

```
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid access-list 100
extended permit ip any any access-list
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0
10.20.10.0 255.255.255.0
!--- 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_1_cryptomap). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_1_cryptomap extended permit ip
10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (outside_cryptomap) 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 disk0:/asdm-613.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 10.10.10.0 255.255.255.0

nat (inside) 0 access-list inside_nat0_outbound
!--- NAT 0 prevents NAT for networks specified in !---
the ACL inside_nat0_outbound.


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
http 0.0.0.0 0.0.0.0 dmz
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-DES-SHA esp-des esp-sha-hmac
!--- Define the transform set for Phase 2. crypto map
outside_map 1 match address outside_1_cryptomap
!--- Define which traffic should be sent to the IPsec
peer. crypto map outside_map 1 set peer 172.17.1.1
!--- Sets the IPsec peer crypto map outside_map 1 set
```

```
transform-set ESP-DES-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. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. crypto
isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 1
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!



tunnel-group 172.17.1.1 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 command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 172.17.1.1 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 threat-detection basic-threat
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic ! !
!-- Output suppressed! username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

Configuración CLI del router

Router

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
```

```
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 2
 authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ASA-IPSEC
esp-des esp-sha-hmac
!

!--- !--- Indicates that IKE is used to establish !---
the IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1

!--- !--- Sets the IP address of the remote end. set
peer 172.16.1.1

!--- !--- Configures IPsec to use the transform-set !---
"ASA-IPSEC" defined earlier in this configuration. set
transform-set ASA-IPSEC

!--- !--- Specifies the interesting traffic to be
encrypted. match address 100
!
!
!
!--- Configures the interface to use the !--- crypto map
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

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 el OIT para ver un análisis de la **salida del comando show**.

- Dispositivo de seguridad PIX - comandos show
- IOS del telecontrol

Dispositivo de seguridad ASA/PIX - comandos show

- **show crypto isakmp sa** — Muestra todas las IKE SAs actuales en un par.

```
ASA#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: 172.17.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

- **muestre ipsec crypto sa** — Muestra todo el SA de IPSec actual en un par.

```
ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

     #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F

    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

Comandos show del router remotos IOS

- **show crypto isakmp sa** — Muestra todas las IKE SAs actuales en un par.

```
Router#show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

- **muestre ipsec crypto sa** — Muestra todo el SA de IPSec actual en un par.

```
Router#show crypto ipsec sa
interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **muestre el active de las conexiones del motor de criptografía** — Conexiones actuales e información de las demostraciones sobre los paquetes encriptados y desencriptados (router solamente).

```
Router#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   3 FastEthernet0        172.17.1.1      set    HMAC_SHA+DES_56_CB        0        0
2001 FastEthernet0        172.17.1.1      set    DES+SHA                   0       59
2002 FastEthernet0        172.17.1.1      set    DES+SHA                  59        0
```

Troubleshooting

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

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

Nota: Consulte Información Importante sobre Comandos Debug y Troubleshooting de Seguridad IP - Comprensión y Uso de Comandos debug antes de usar los comandos **debug** .

- **ponga a punto el ipsec crypto 7** — Visualiza los IPSec Negotiations de la fase 2.**isakmp crypto 7 de la depuración** — Visualiza negociaciones ISAKMP de la fase 1.
- **ipsec crypto de la depuración** — Visualiza los IPSec Negotiations de la fase 2.**isakmp crypto de la depuración** — Visualiza negociaciones ISAKMP de la fase 1.

Refiera a la mayoría del L2L y de las soluciones comunes del troubleshooting de IPSec VPN del Acceso Remoto para más información sobre el Sitio-sitio VPN del troubleshooting.

Información Relacionada

- Cisco PIX Firewall Software
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Profesional de la configuración: IPSec sitio a sitio VPN entre ASA/PIX y un ejemplo de configuración del router IOS
- Referencias de Comandos de Secure PIX firewall
- Router de Cisco y Administrador de dispositivo de seguridad
- Pedidos los comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems