Túnel IPsec dinámico entre un ASA estáticamente dirigido y un router dinámicamente dirigido del Cisco IOS que utiliza el ejemplo de configuración CCP

Contenido

Introducción

Este documento proporciona una configuración de muestra para que cómo permita al dispositivo de seguridad del PIX/ASA para validar las conexiones dinámicas del IPSec del router del ® del Cisco IOS. En este escenario, el túnel IPsec establece cuando el túnel se inicia del extremo del router solamente. El ASA no podía iniciar un túnel VPN debido a la configuración IPSec dinámica.

Esta configuración permite al dispositivo de seguridad PIX para crear un túnel dinámico del LAN a LAN del IPSec (L2L) con un VPN Router remoto. Este router recibe dinámicamente a su IP Address público exterior de su Proveedor de servicios de Internet. El Protocolo de configuración dinámica de host (DHCP) proporciona este mecanismo para afectar un aparato los IP Addresses dinámicamente del proveedor. Esto permite que los IP Addresses sean reutilizados cuando los host los necesitan no más.

La configuración en el router se hace con el uso del Cisco Configuration Professional (CCP). El CCP es una herramienta de Administración de dispositivos GUI basada que permite que usted configure al Routers basado en IOS de Cisco. Refiera a la configuración básica del router usando el Cisco Configuration Professional para más información sobre cómo configurar a un router con

el CCP.

Refiera al sitio para localizar VPN (L2L) con el ASA para más inormation y ejemplos de configuración en el establecimiento del túnel IPsec que utilicen el ASA y al Routers del Cisco IOS.

Refiera al sitio para localizar VPN (L2L) con el IOS para más información y un ejemplo de configuración en el establecimiento dinámico del túnel IPsec con el uso del PIX y del router del Cisco IOS.

prerrequisitos

Requisitos

Antes de que usted intente esta configuración, asegúrese de que el ASA y el router tengan conectividad a Internet para establecer el túnel IPsec.

Componentes Utilizados

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

- Cisco IOS Router1812 que funciona con el Cisco IOS Software Release 12.4
- Software Release 8.0.3 de Cisco ASA 5510

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

En este escenario, la red de 192.168.100.0 está detrás de la red ASA y de 192.168.200.0 está detrás del router del Cisco IOS. Se asume que el router consigue a su dirección pública con el DHCP de su ISP. Pues esto plantea un problema en la configuración de un peer estático en el extremo ASA, usted necesita acercarse a la manera de configuración de criptografía dinámica de establecer un túnel del sitio a localizar entre el ASA y el router del Cisco IOS.

Los usuarios de Internet en el extremo ASA consiguen traducidos a la dirección IP de su interfaz exterior. Se asume que el NAT no está configurado en el extremo del router del Cisco IOS.

Ahora éstos son los pasos principales que se configurarán en el extremo ASA para establecer el túnel dinámico:

1. Configuración relacionada de la fase 1 ISAKMP
2. Configuración nacional de la exención

3. Configuración de la correspondencia cifrada dinámica

El router del Cisco IOS hace una correspondencia de criptografía estática configurar porque el ASA se asume para tener un IP Address público estático. Ahora ésta es la lista de pasos principales que se configurarán en el extremo del router del Cisco IOS para establecer el túnel IPsec dinámico.

1. Configuración relacionada de la fase 1 ISAKMP
2. Configuración relacionada de la correspondencia de criptografía estática

Estos pasos se describen detalladamente en estas configuraciones.

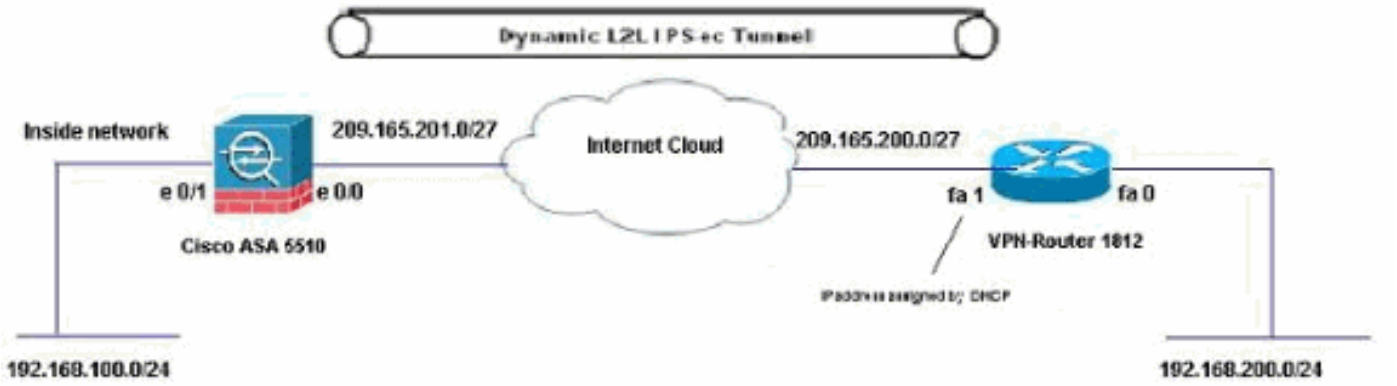
Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

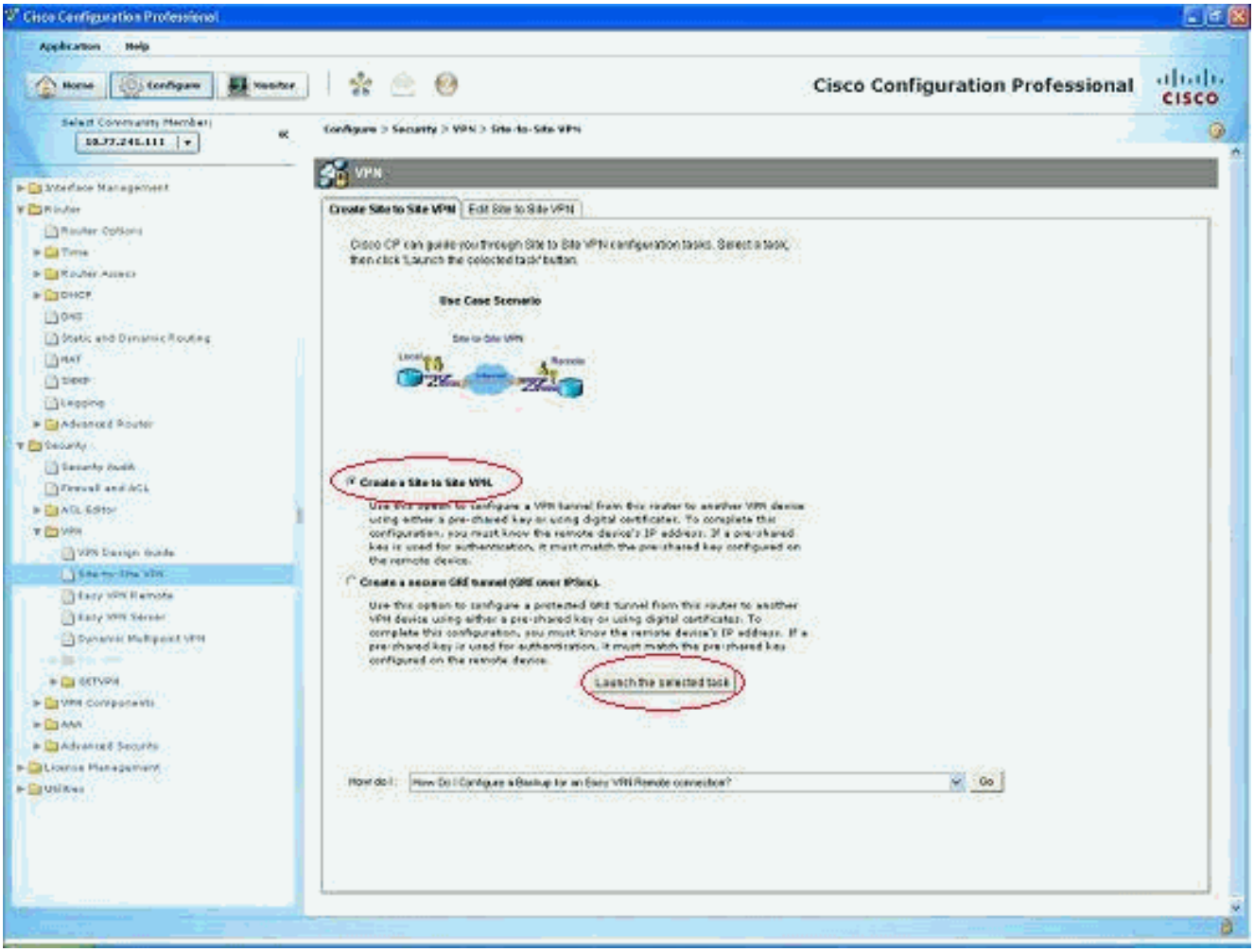
En este documento, se utiliza esta configuración de red:



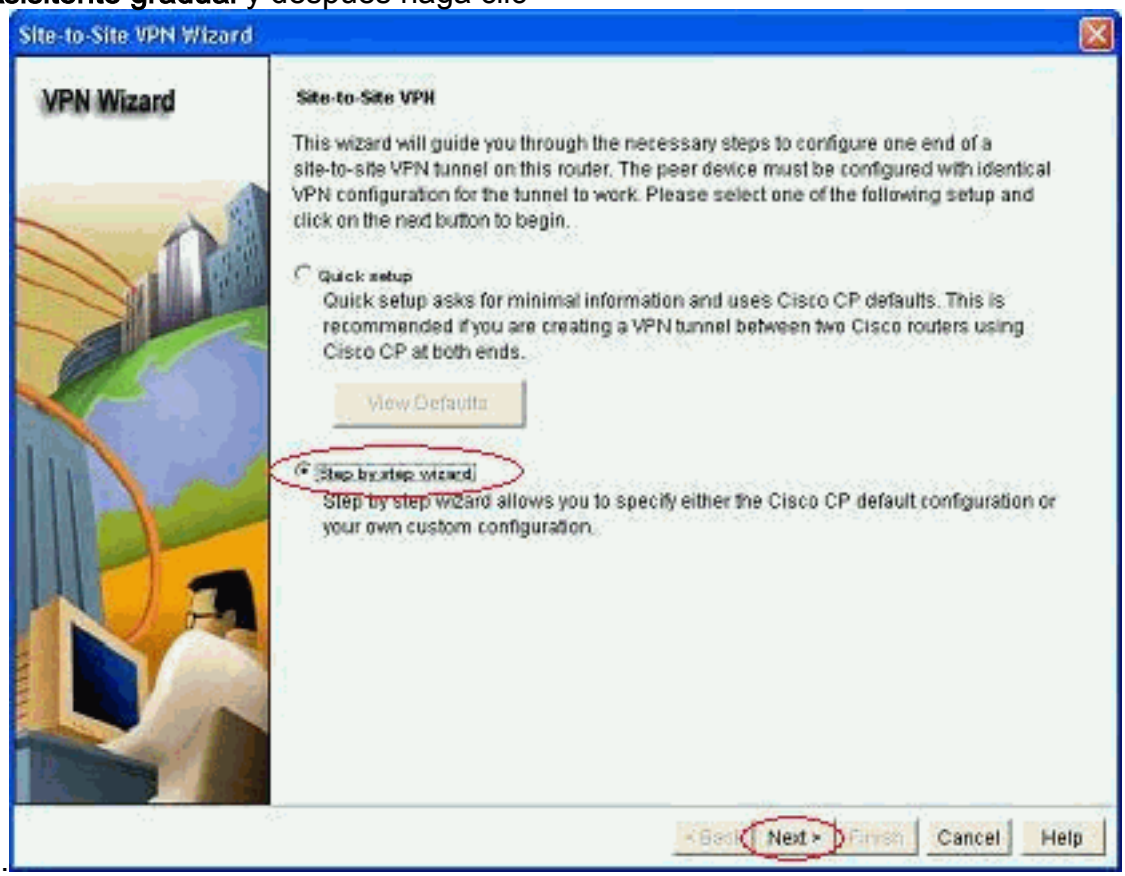
Configuraciones

Ésta es la configuración del IPSec VPN en el VPN Router con el CCP. Complete estos pasos:

1. Abra la aplicación CCP y elija el **> Security (Seguridad) de la configuración > el VPN > el sitio para localizar el VPN**. Haga clic el **lanzamiento la lengueta seleccionada.**



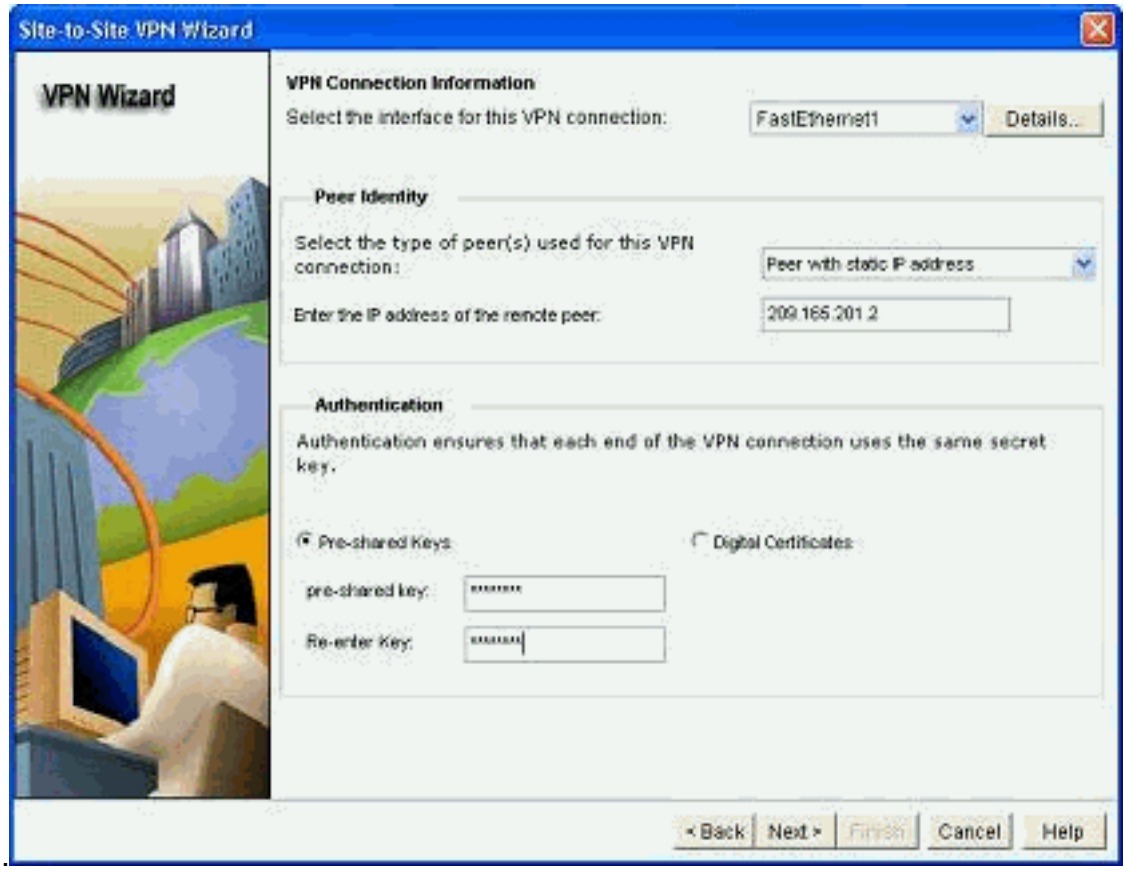
2. Elija al **Asisitente gradual** y después haga clic



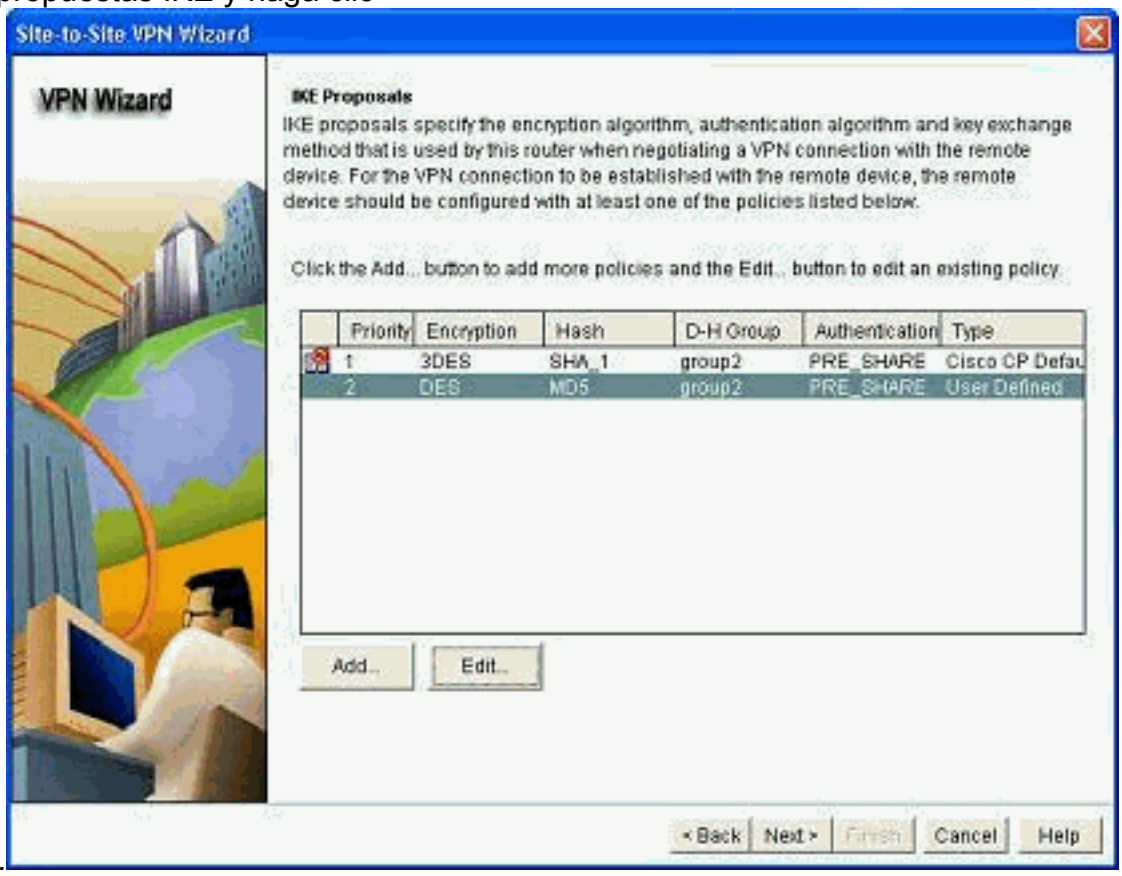
después.

3. Complete la dirección IP del peer remoto junto con los detalles de la

autenticación.

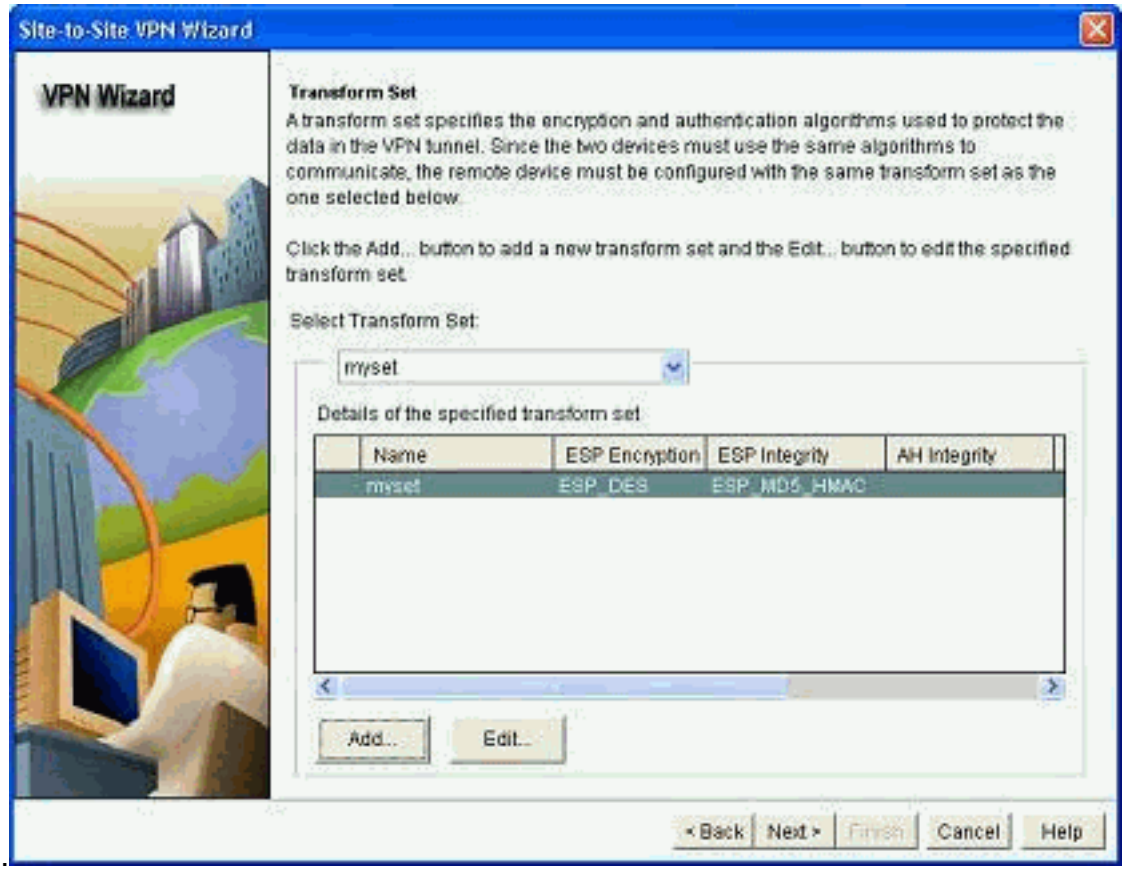


4. Elija las propuestas IKE y haga clic



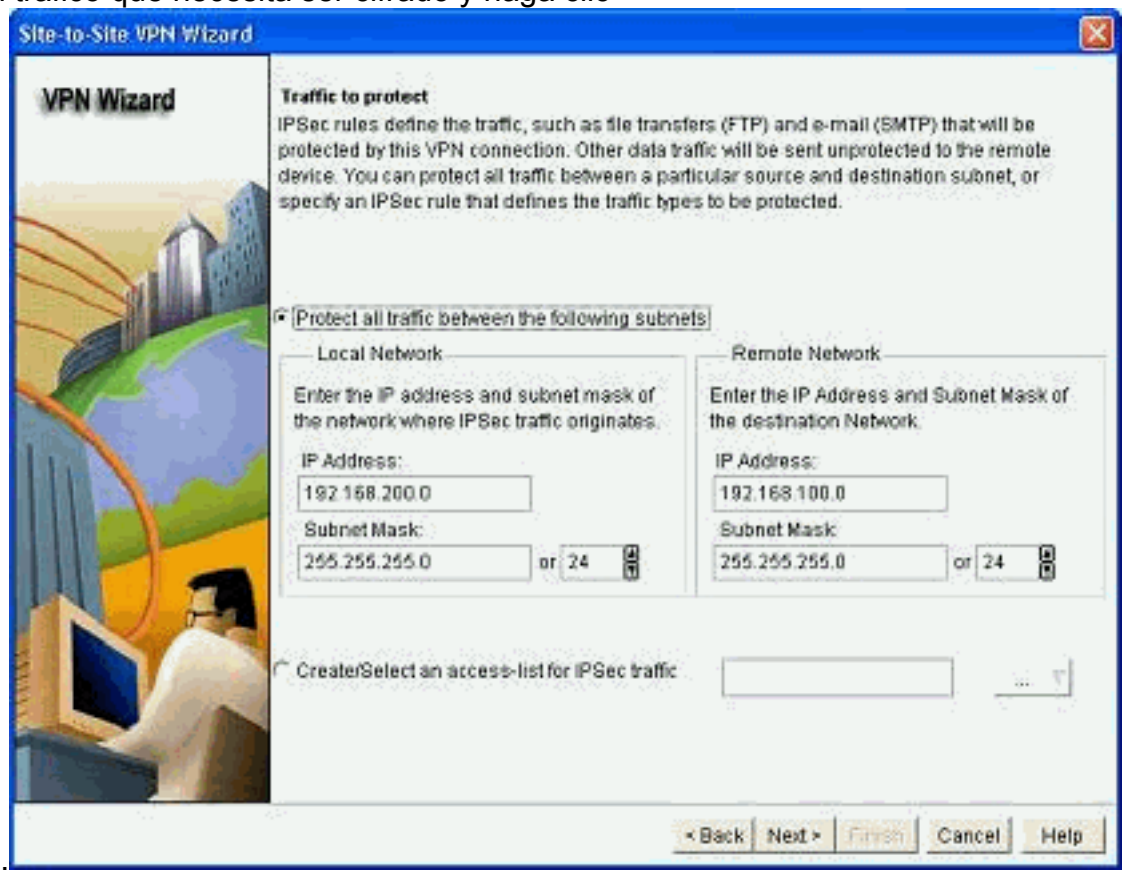
después.

5. Defina los detalles del transforme el conjunto y haga clic



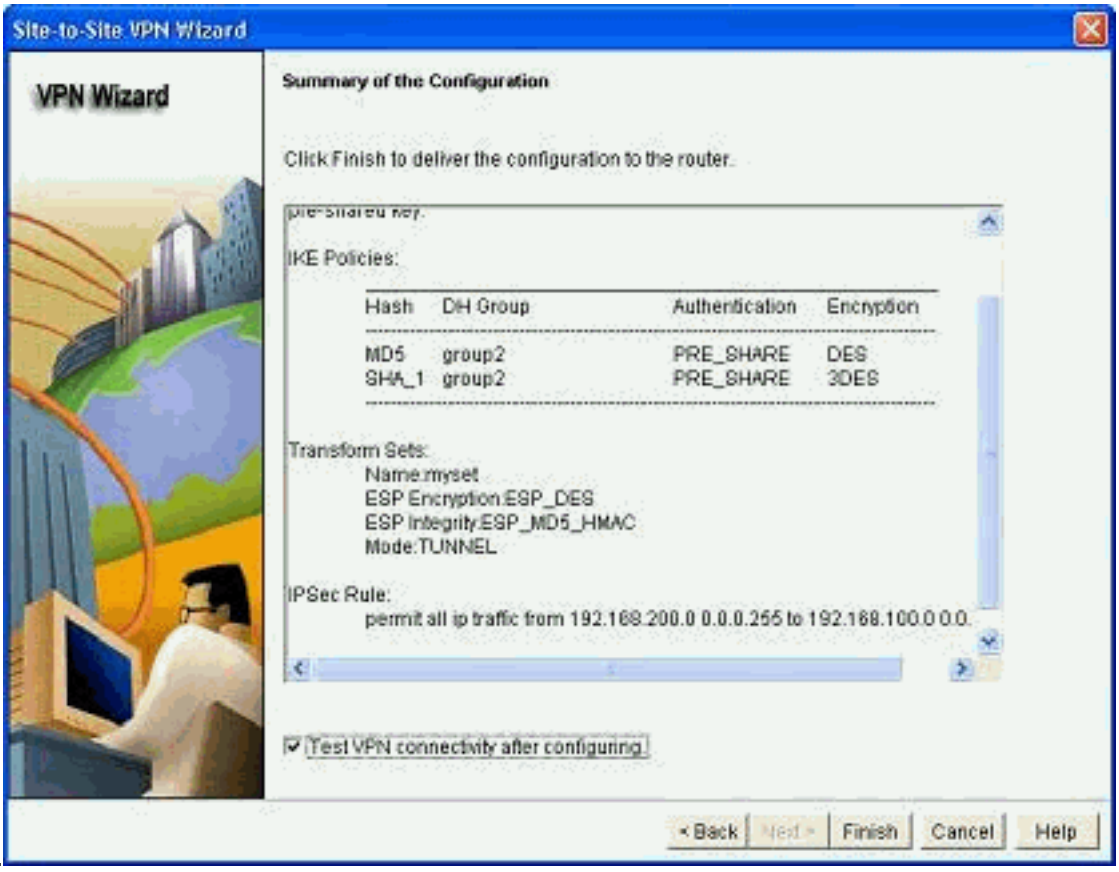
después.

6. Defina el tráfico que necesita ser cifrado y haga clic



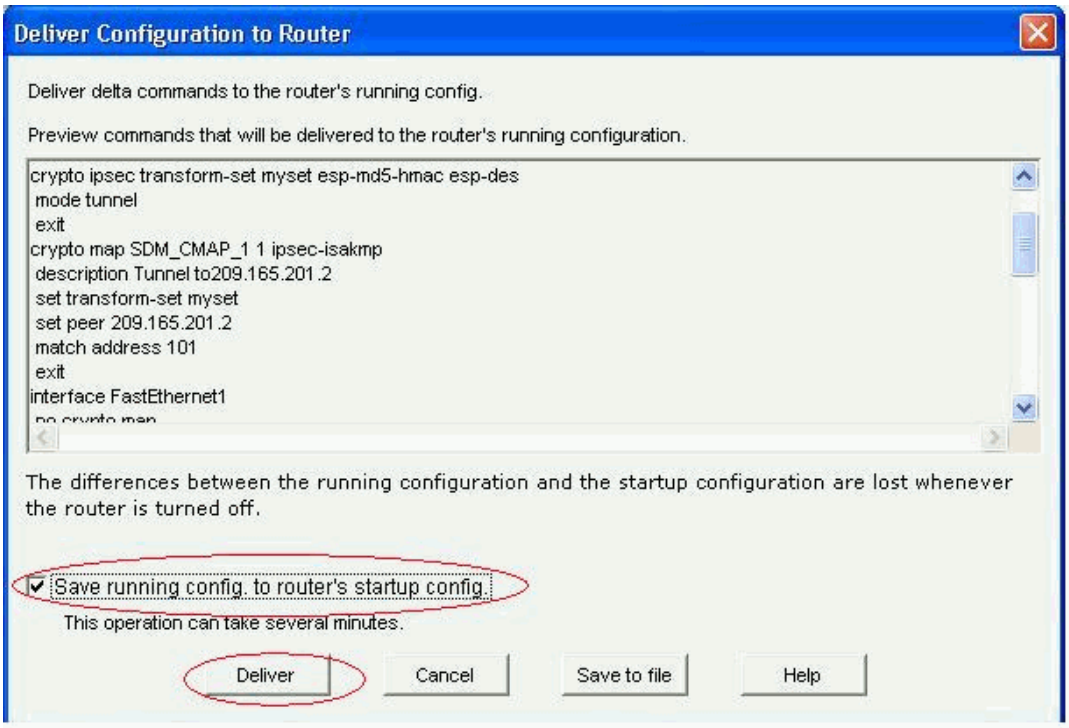
después.

7. Verifique el resumen de la configuración IPSec y del clic en Finalizar

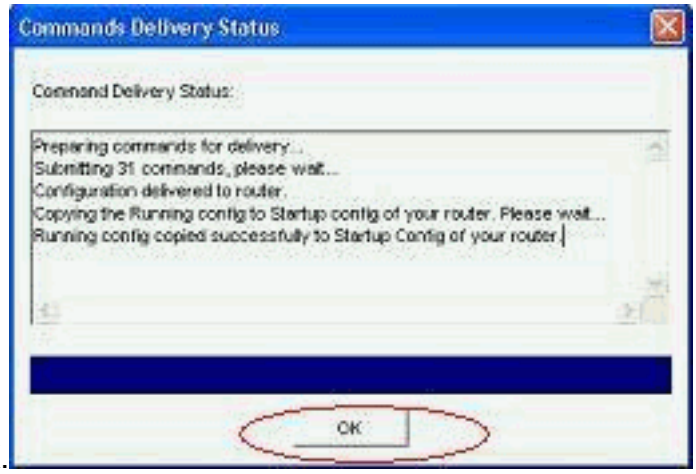


crypto.

8. El tecleo **entrega** para enviar la configuración al VPN Router.



9. Haga clic en OK.



Configuración de CLI

- Ciscoasa
- VPN Router

Ciscoasa

```
ciscoasa(config)#show run : Saved : ASA Version 8.0(3) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif outside
security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive !--- Output suppressed access-list
nonat extended permit ip 192.168.100.0 255.255.255.0
192.168.200.0 255.255.255.0 no pager mtu outside 1500
mtu inside 1500 icmp unreachable rate-limit 1 burst-size
1 asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 ! !--- Define the nat-translation for
Internet users global (outside) 1 interface nat (inside)
1 192.168.100.0 255.255.255.0 ! ! !--- Define the nat-
exemption policy for VPN traffic nat (inside) 0 access-
list nonat ! route outside 0.0.0.0 0.0.0.0 209.165.201.1
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 mgcp-pat
0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00
absolute dynamic-access-policy-record DfltAccessPolicy
no snmp-server location no snmp-server contact snmp-
server enable traps snmp authentication linkup linkdown
coldstart ! !--- Configure the IPsec transform-set
crypto ipsec transform-set myset esp-des esp-md5-hmac !
! !--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset crypto dynamic-map
mymap 1 set reverse-route crypto map dyn-map 10 IPSec-
isakmp dynamic mymap crypto map dyn-map interface
outside ! !--- Configure the phase I ISAKMP policy
crypto isakmp policy 10 authentication pre-share
encryption des hash md5 group 2 lifetime 86400 ! ! !---
Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes pre-
shared-key * ! class-map inspection_default match
```

```
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map 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 prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa(config)#
```

El CCP crea esta configuración en el VPN Router.

VPN Router

```
VPN-Router#show run Building configuration... ! version
12.4 service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname VPN-Router ! ! username cisco
privilege 15 secret 5 $1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQO1 ! ! !--- Output
suppressed no aaa new-model ip subnet-zero ! ip cef !
crypto isakmp enable outside ! crypto isakmp policy 1
encrypt 3des authentication pre-share group 2 ! crypto
isakmp policy 2 hash md5 authentication pre-share group
2 ! ! crypto isakmp key cisco123 address 209.165.201.2 !
! crypto ipsec transform-set myset esp-des esp-md5-hmac
! ! crypto map SDM_CMAP_1 1 IPSec-isakmp description
Tunnel to209.165.201.2 set peer 209.165.201.2 set
transform-set myset match address 101 ! ! ! interface
BRI0 no ip address shutdown ! interface Dot11Radio0 no
ip address shutdown speed basic-1.0 basic-2.0 basic-5.5
6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root ! interface Dot11Radio1 no ip address
shutdown speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
36.0 48.0 54.0 station-role root ! interface
FastEthernet0 ip address 192.168.200.1 255.255.255.0
duplex auto speed auto ! interface FastEthernet1 ip
address dhcp duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet2 no ip address
shutdown ! interface FastEthernet3 no ip address
shutdown ! interface FastEthernet4 no ip address
shutdown ! interface FastEthernet5 no ip address
shutdown ! interface FastEthernet6 no ip address
shutdown ! interface FastEthernet7 no ip address
shutdown ! interface FastEthernet8 no ip address
shutdown ! interface FastEthernet9 no ip address
shutdown ! interface Vlan1 no ip address ! ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1 ! ! !--- Output
suppressed ! ip http server ip http authentication local
ip http secure-server ! access-list 100 permit ip
0.0.0.0 255.255.255.0 0.0.0.0 255.255.255.0 access-list
101 remark CCP_ACL Category=4 access-list 101 remark
IPSEC Rule access-list 101 permit ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 ! ! ! ! control-plane
! ! line con 0 line aux 0 line vty 0 4 privilege level
15 login local transport input telnet ssh line vty 5 15
privilege level 15 login local transport input telnet
ssh ! no scheduler allocate end
```

Verificación

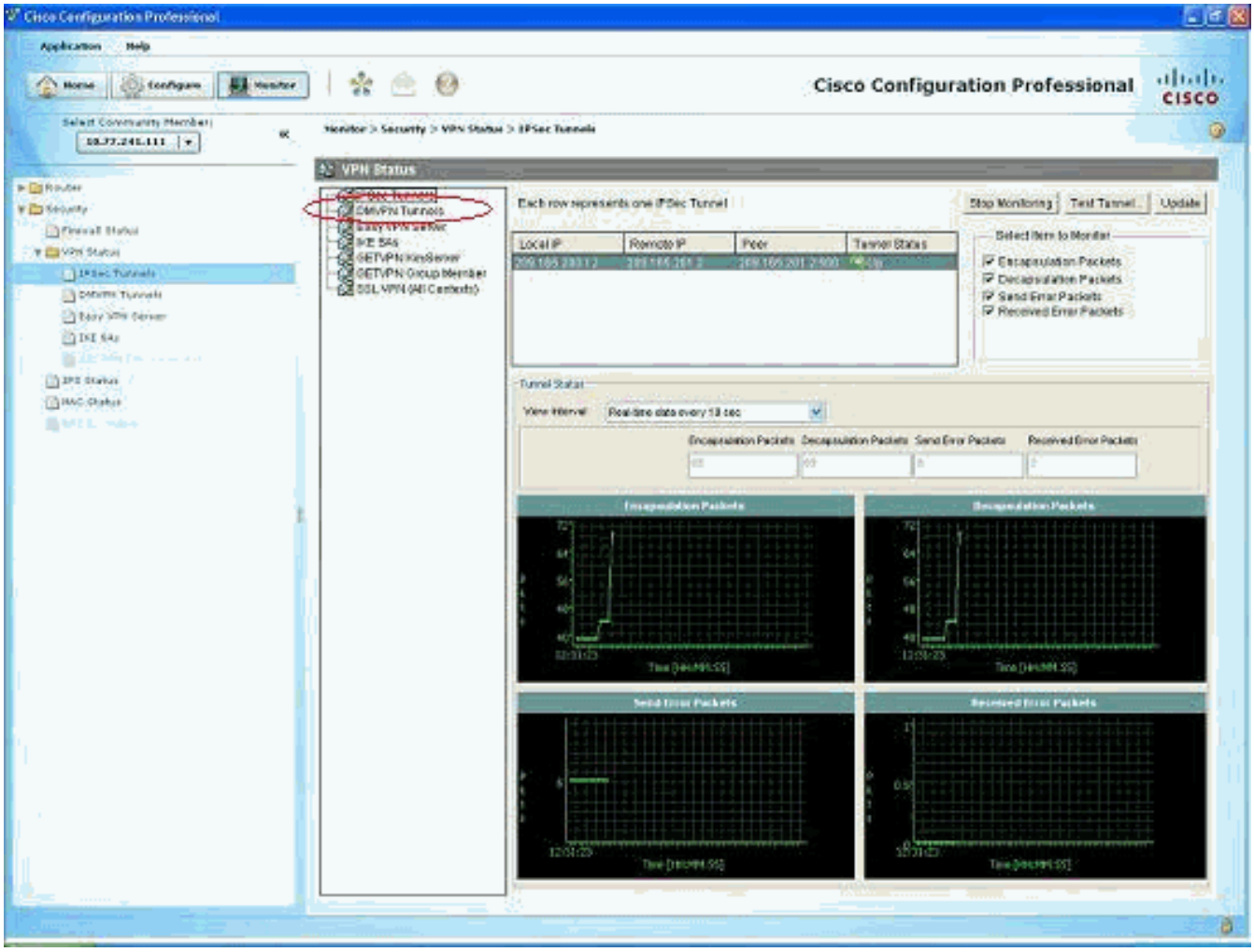
Use esta sección para confirmar que su configuración funciona correctamente.

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

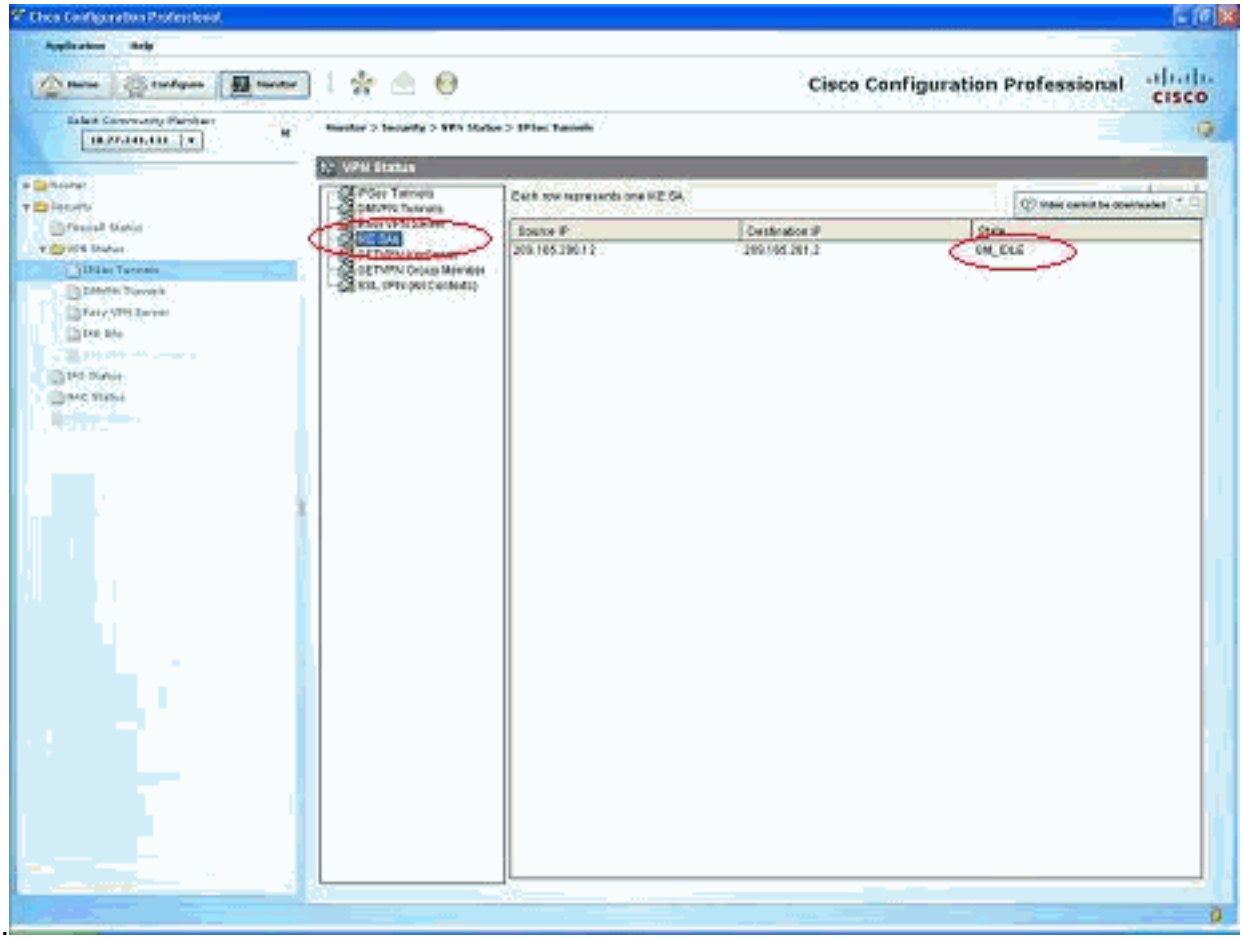
- Verificar los parámetros del túnel con el CCP
- Verificar el estado del túnel con ASA CLI
- Verificar los parámetros del túnel a través del router CLI

Verifique los parámetros del túnel con el CCP

- Monitoree los pasos del tráfico a través del túnel IPsec.



- Monitoree el estatus ISAKMP SA de la fase

I. 

Verifique el estado del túnel con ASA CLI

- Verifique el estatus ISAKMP SA de la fase I.`ciscoasa#`**`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: 209.165.200.12 Type : L2L Role :` **`responder`** `Rekey : no State :` **`MM_ACTIVE`** `ciscoasa#`

  Nota: Observe el papel para ser el respondedor, que estado que el iniciador de este túnel está en el otro extremo, por ejemplo, el VPN Router.
- Verifique los parámetros IPSEC SA de la fase II.`ciscoasa#`**`show crypto ipsec sa`** `interface: outside Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2` **`local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)`** `current_peer: 209.165.200.12` **`#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29 #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29`** `#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 29, #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.: 209.165.201.2, remote crypto endpt.: 209.165.200.12 path mtu 1500, IPSec overhead 58, media mtu 1500 current outbound spi: E7B37960 inbound esp sas: spi: 0xABB49C64 (2880740452) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xE7B37960 (3887298912) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y`

Verifique los parámetros del túnel a través del router CLI

- Verifique el estatus ISAKMP SA de la fase I.`VPN-Router#`**`show crypto isakmp sa`** `dst src state conn-id slot status 209.165.201.2 209.165.200.12` **`QM_IDLE`** `1 0` **`ACTIVE`**
- Verifique los parámetros IPSEC SA de la fase II.`VPN-Router#`**`show crypto ipsec sa`** `interface:`

```
FastEthernet1 Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12 protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) current_peer 209.165.201.2 port 500
PERMIT, flags={origin_is_acl,} #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39 #pkts
decaps: 39, #pkts decrypt: 39, #pkts verify: 39 #pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress
failed: 0 #send errors 6, #recv errors 0 local crypto endpt.: 209.165.200.12, remote crypto
endpt.: 209.165.201.2 path mtu 1500, ip mtu 1500 current outbound spi:
0xABB49C64(2880740452) inbound esp sas: spi: 0xE7B37960(3887298912) transform: esp-des esp-
md5-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): (4481818/3375) IV size: 8 bytes replay
detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xABB49C64(2880740452) transform: esp-des esp-md5-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): (4481818/3371) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound
ah sas: outbound pcp sas:
```

Troubleshooting

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

- Derribar las conexiones crypto existentes.`ciscoasa#clear crypto ipsec sa ciscoasa#clear crypto isakmp sa VPN-Router#clear crypto isakmp`
- Utilice los **comandos debug** para resolver problemas los problemas con el túnel VPN.**Nota:** Si usted habilita el debugging, éste puede interrumpir la operación del router cuando las condiciones de mucha carga de la experiencia del internetworks. Utilice los comandos de depuración con precaución. En general, se recomienda que estos comandos se utilicen sólo bajo la dirección del representante de soporte técnico de su router cuando se intenta resolver problemas específicos.`ciscoasa#debug crypto engine ciscoasa#debug crypto isakmp ciscoasa#debug crypto IPSec ciscoasa# VPN-Router#debug crypto engine Crypto Engine debugging is on VPN-Router#debug crypto isakmp Crypto ISAKMP debugging is on VPN-Router#debug crypto ipsec Crypto IPSEC debugging is on VPN-Router#`

Refiera al isakmp del debug crypto al la comprensión y usar de los comandos debug para más información sobre los commangs del debug.

Información Relacionada

- Página de Soporte de IPSec Negotiation/IKE Protocols
- Documentación para el software de sistema operativo del dispositivo de seguridad de Cisco ASA
- La mayoría de las soluciones del troubleshooting del IPSec comunes VPN
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems