Dynamische IPsec-tunnelheid tussen een automatisch geadresseerde ASA en een dynamisch geadresaliseerde Cisco IOS-router die gebruik maakt van Configuratievoorbeeld

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor de manier waarop u PIX/ASA security applicatie kunt inschakelen om dynamische IPsec-verbindingen van de Cisco IOS® router te accepteren. In dit scenario, bevestigt de IPsec tunnel wanneer de tunnel van het routereind slechts van start gaat. ASA kon geen VPN-tunnel starten vanwege de dynamische IPsec-configuratie.

Deze configuratie stelt de PIX security applicatie in staat om een dynamische IPsec LAN-to-LAN (L2L) tunnel te maken met een externe VPN-router. Deze router ontvangt dynamisch zijn buiten openbare IP-adres van zijn internetserviceprovider. Dynamic Host Configuration Protocol (DHCP) biedt dit mechanisme om IP-adressen dynamisch van de provider toe te wijzen. Dit staat IP adressen toe om opnieuw te worden gebruikt wanneer de hosts deze niet langer nodig hebben.

De configuratie van de router wordt uitgevoerd met het gebruik van Cisco Configuration Professional (CCP). CCP is een op GUI gebaseerd apparaatbeheer waarmee u Cisco IOS-gebaseerde routers kunt configureren. Raadpleeg de basisrouterconfiguratie met Cisco Configuration Professional voor meer informatie over de manier waarop u een router met CTP

kunt configureren.

Raadpleeg Site naar Site VPN (L2L) met ASA voor meer informatie en configuratievoorbeelden in IPsec-tunnelinstellingen die ASA en Cisco IOS-routers gebruiken.

Raadpleeg Site naar Site VPN (L2L) met IOS voor meer informatie en een configuratievoorbeeld voor dynamische IPSec-tunnelvestiging met gebruik van PIX- en Cisco IOS-router.

Voorwaarden

Vereisten

Voordat u deze configuratie probeert, moet u ervoor zorgen dat zowel de ASA als de router internetconnectiviteit hebben om de IPSEC-tunnel op te zetten.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-router 18.12 met Cisco IOS-softwarerelease 12.4
- Cisco ASA 5510 softwarerelease 8.0.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

In dit scenario ligt het 192.168.100.0-netwerk achter de ASA en 192.168.200.0-netwerk achter de Cisco IOS-router. Het wordt verondersteld dat de router zijn openbare adres door DHCP van zijn ISP krijgt. Aangezien dit een probleem vormt in de configuratie van een statisch peer op het ASA-eind, moet u de manier van dynamische crypto configuratie benaderen om een site-to-site tunnel tussen ASA en de Cisco IOS-router op te zetten.

Internetgebruikers aan het ASA-eind worden vertaald naar het IP-adres van de externe interface. Er wordt vanuit gegaan dat NAT niet is geconfigureerd op het Cisco IOS-routereinde.

Dit zijn nu de belangrijkste stappen die op het ASA-eind moeten worden geconfigureerd om dynamische tunnel op te bouwen:

1. Configuratie fase 1 van ISAKMP
2. NAT-vrijstellingsconfiguratie
3. Dynamische configuratie van cryptografische kaarten

De Cisco IOS router heeft een statische crypto kaart geconfigureerd omdat de ASA verondersteld wordt een statisch openbaar IP-adres te hebben. Dit is nu de lijst van belangrijkste stappen die op

het eind van de Cisco IOS router moeten worden gevormd om dynamische IPSEC-tunnel op te zetten.

1. Configuratie fase 1 van ISAKMP
2. Statische cryptografische kaart

Deze stappen worden in deze configuraties uitvoerig beschreven.

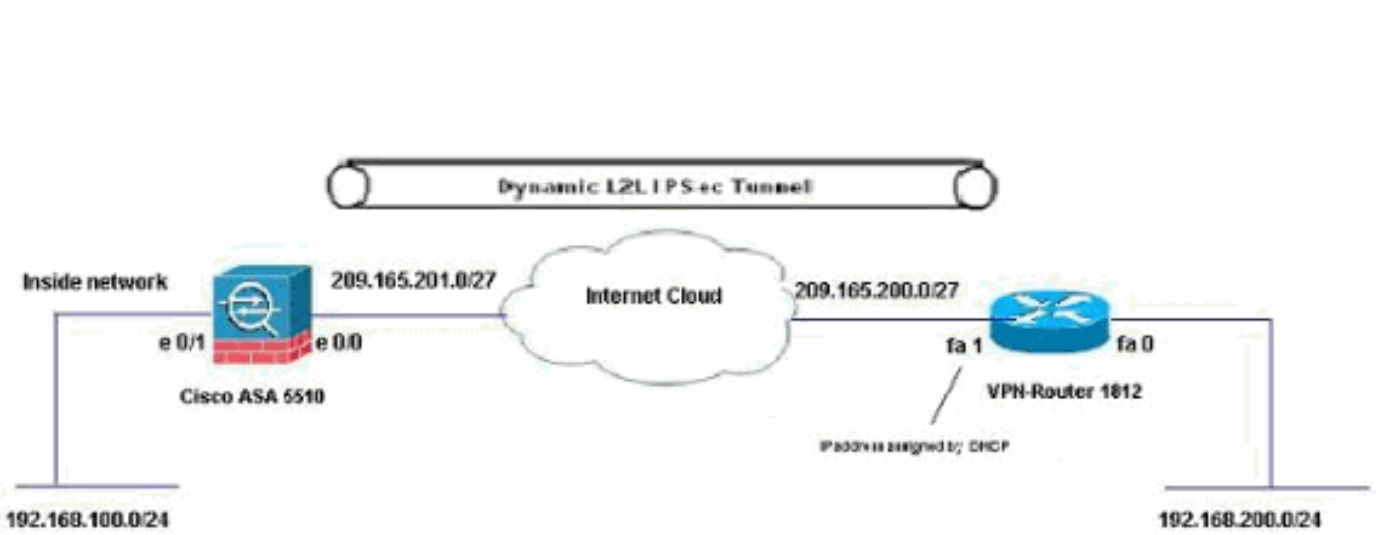
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

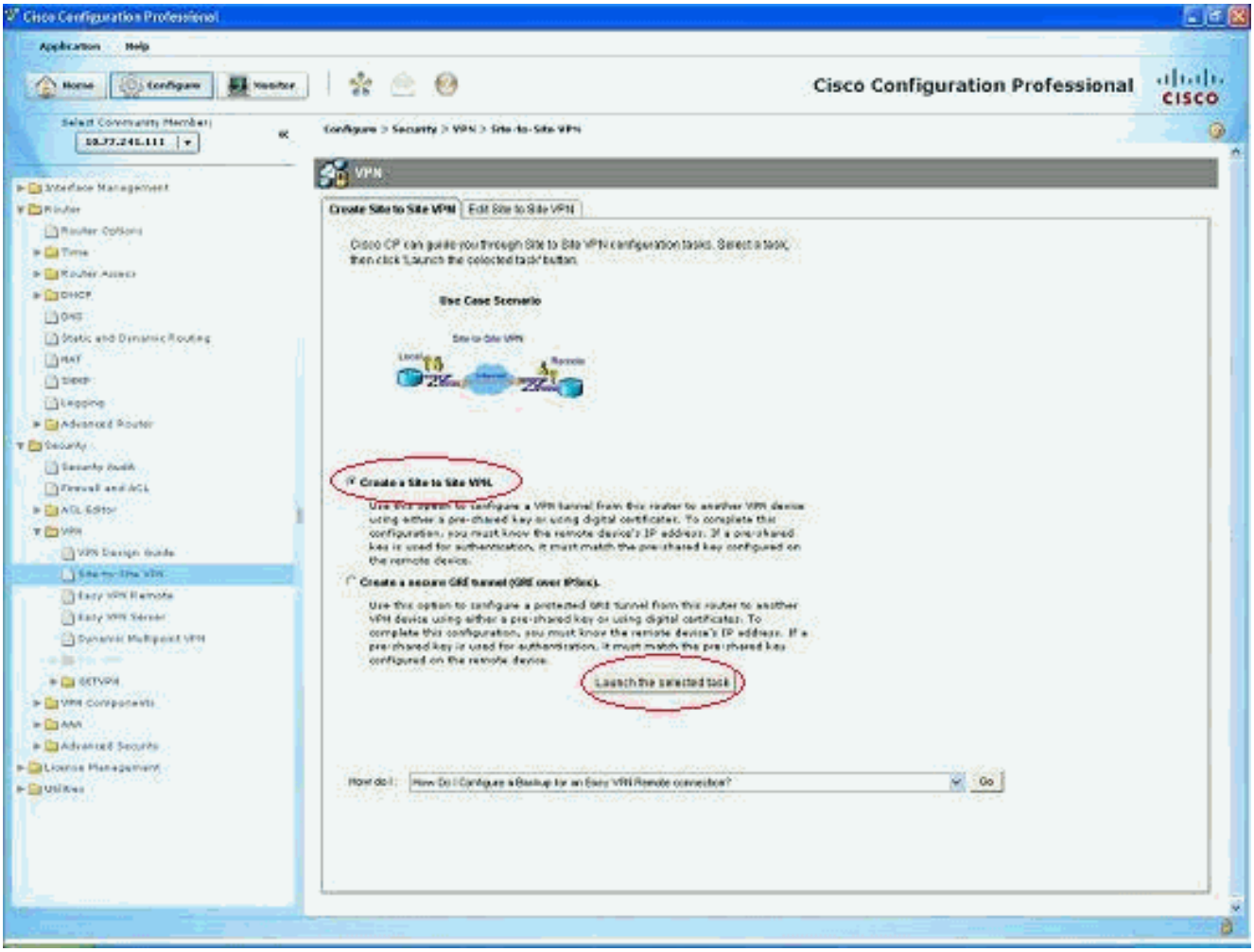
Het netwerk in dit document is als volgt opgebouwd:



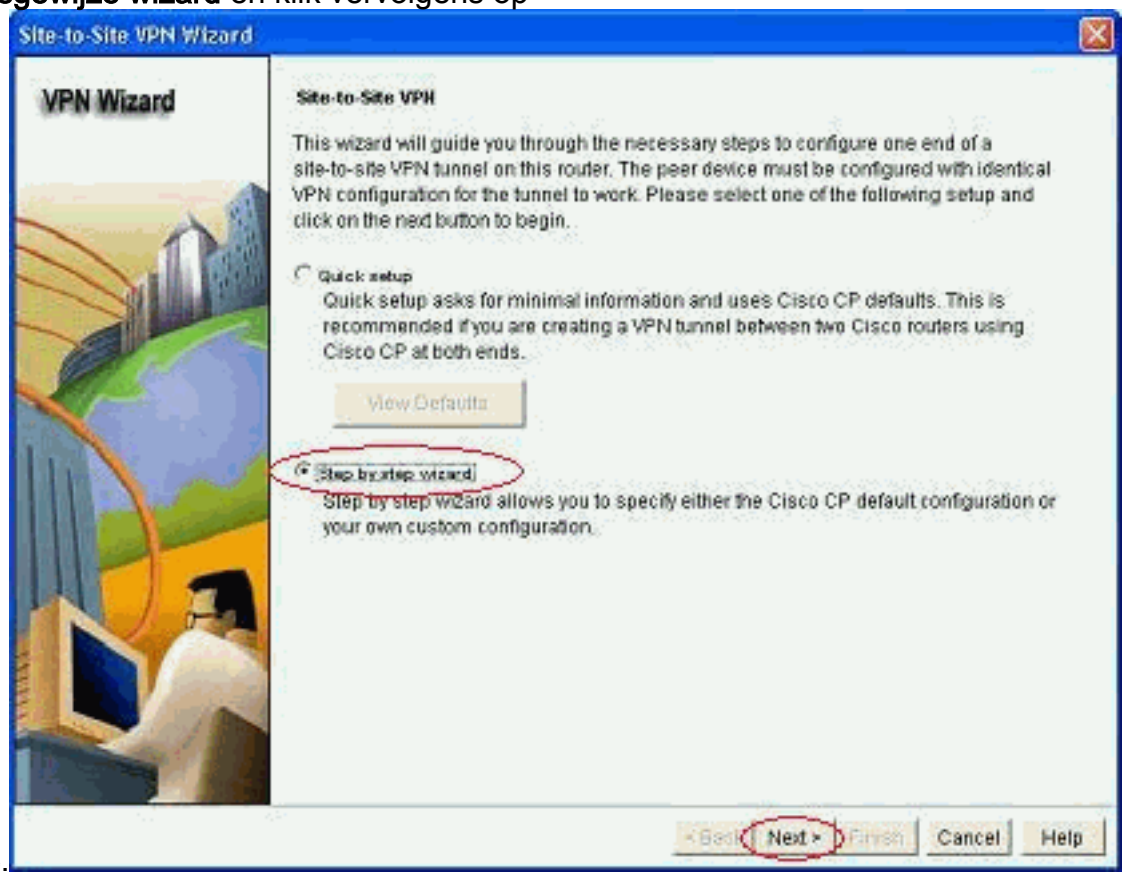
Configuraties

Dit is de configuratie van IPsec VPN op de VPN-router met CCP. Voer de volgende stappen uit:

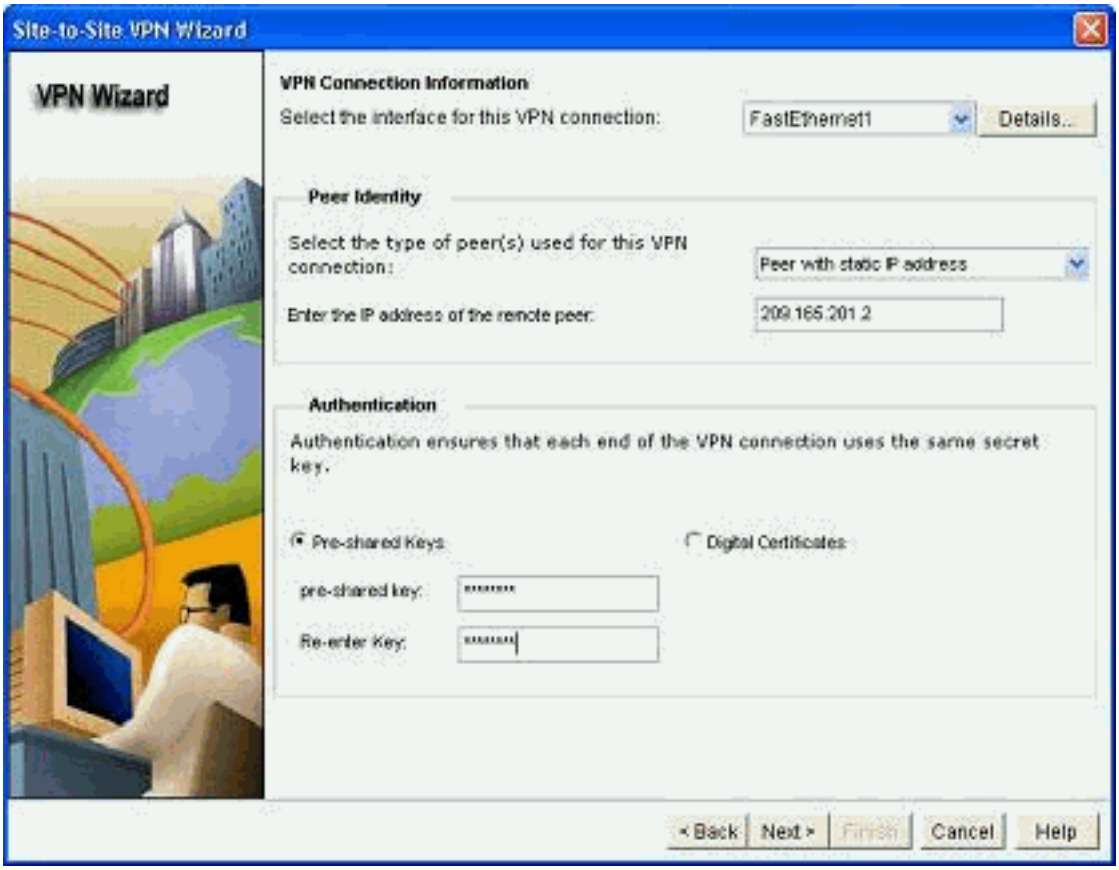
1. Open de CCP-toepassing en kies **Configureren > Beveiliging > VPN > Site VPN**. Klik op het **tabblad**
Start.



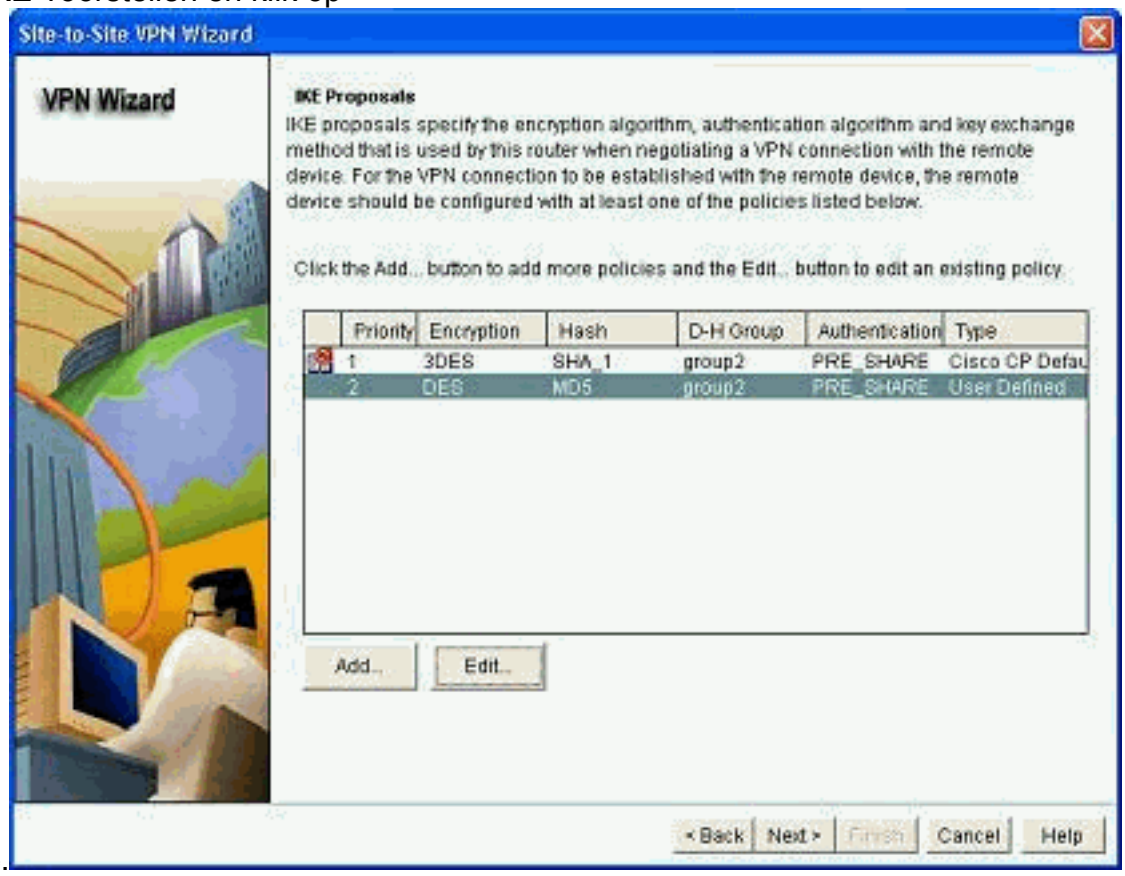
2. Kies **stapsgewijze wizard** en klik vervolgens op **Volgende**.



3. Vul het externe peer IP-adres in samen met de verificatiegegevens.

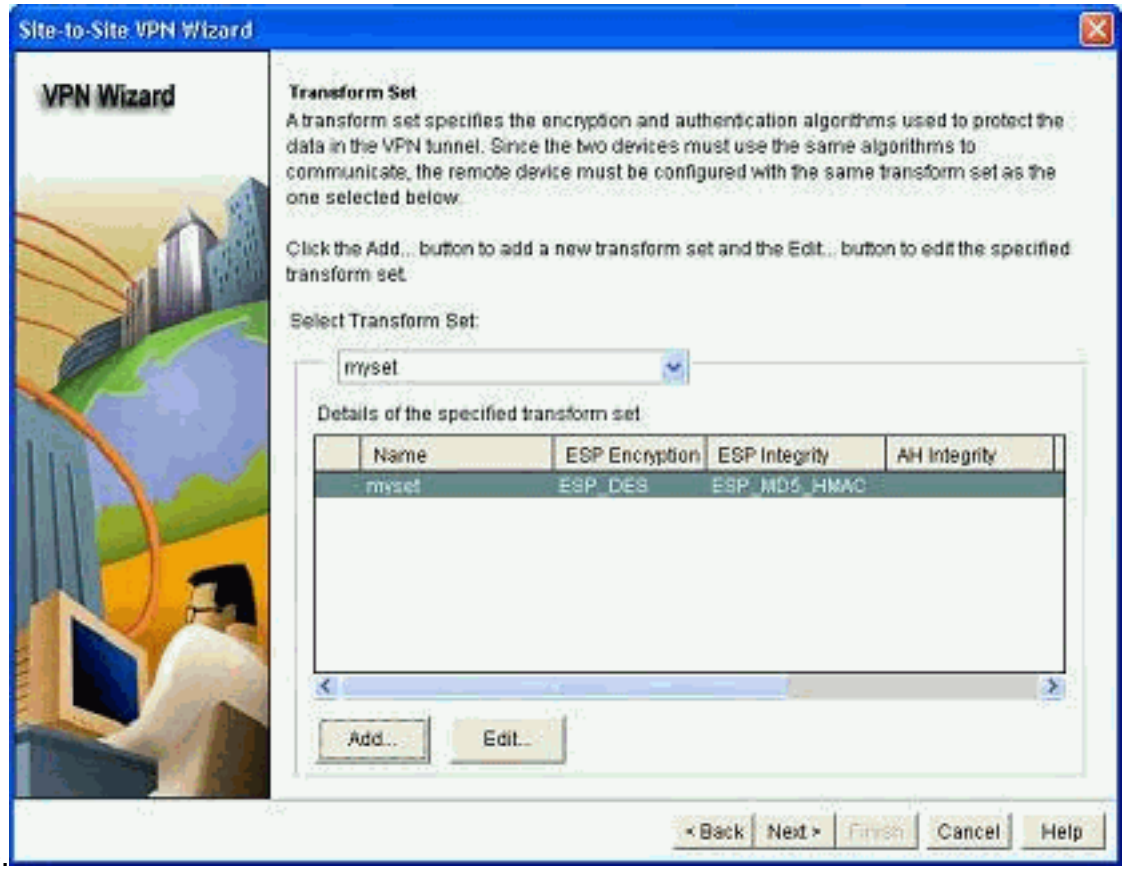


4. Kies de IKE-voorstellen en klik op Volgende.



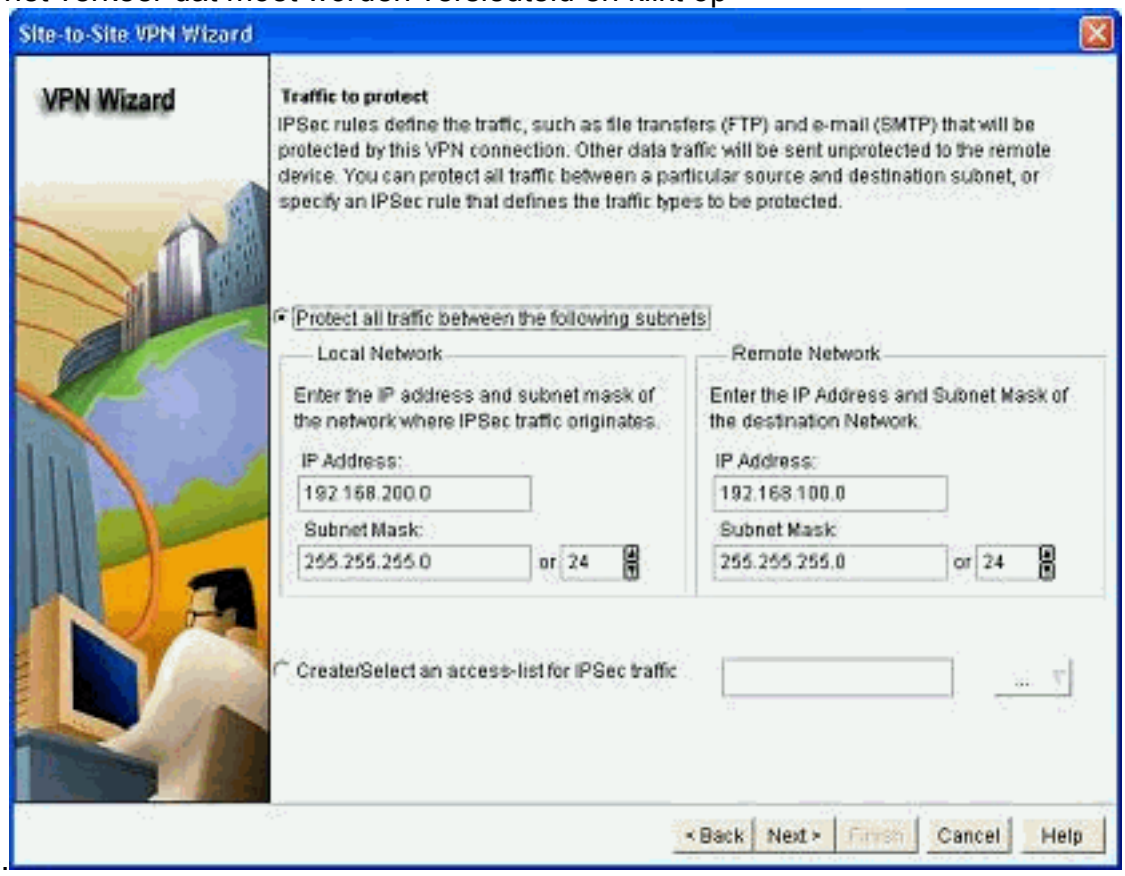
5. Defineer de transformatie-ingestelde details en klik op

Volgende.



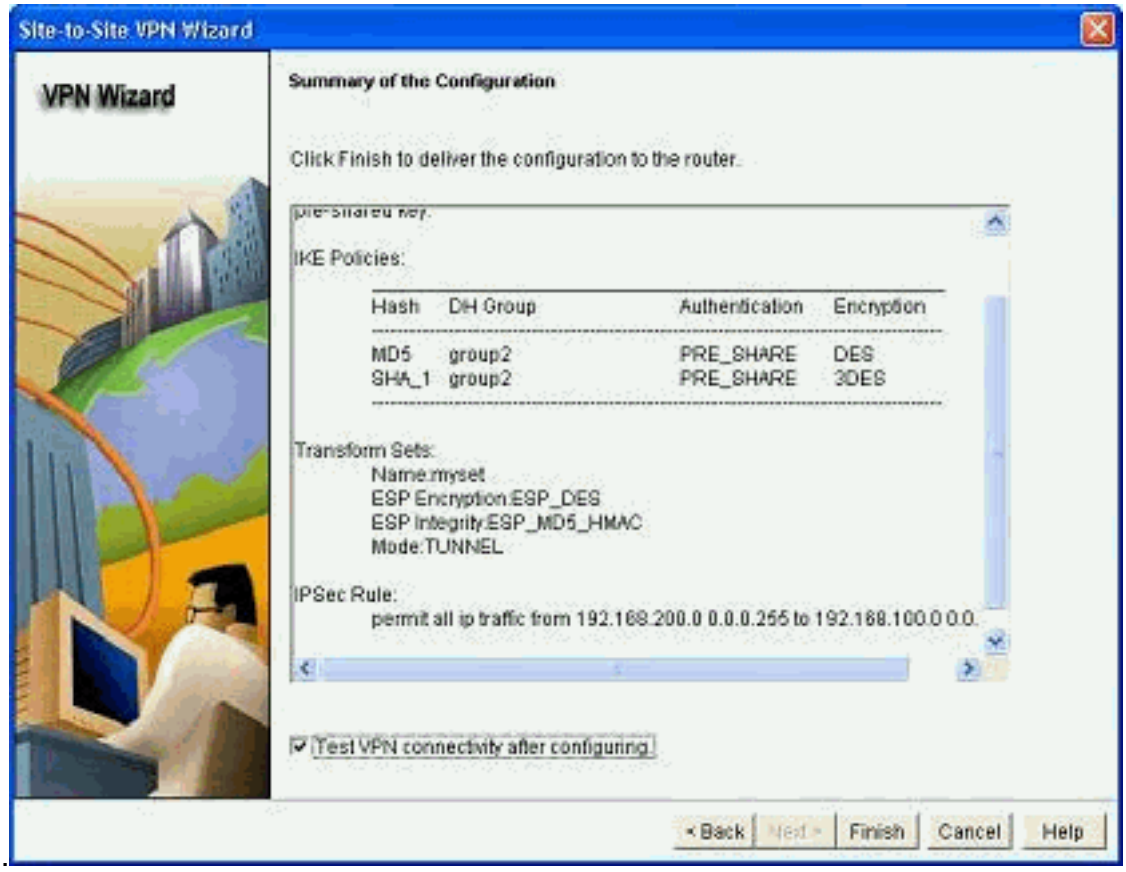
6. Defineert het verkeer dat moet worden versleuteld en klikt op

Volgende.



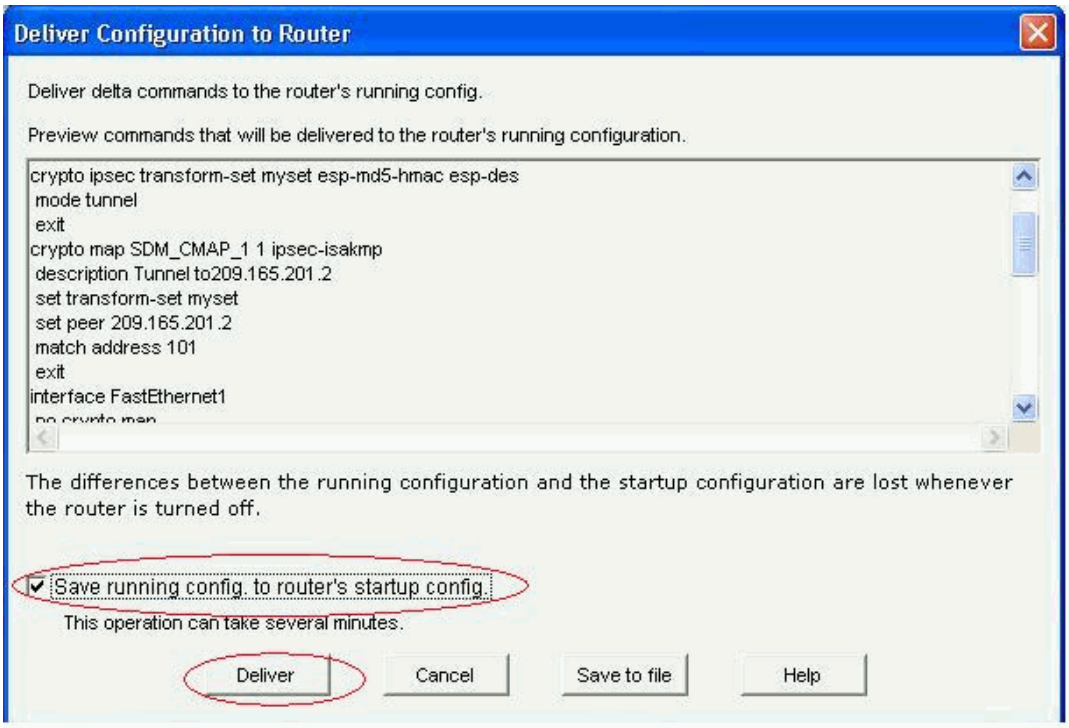
7. Controleer de samenvatting van de configuratie van crypto IPsec en klik op

Volgende.

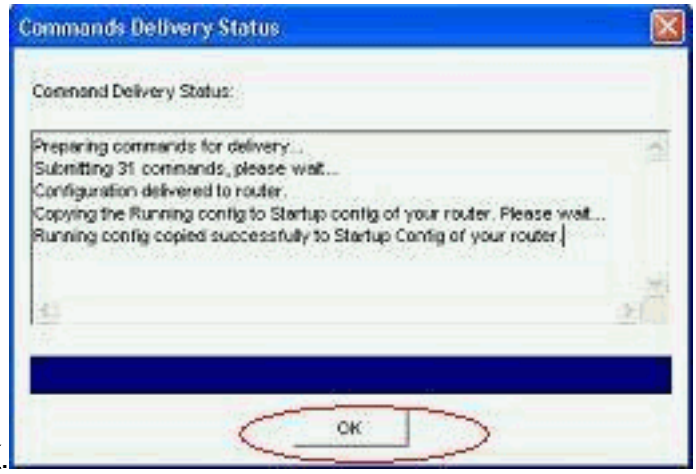


Voltooien.

8. Klik op **Delivery** om de configuratie naar de VPN-router te sturen.



9. Klik op **OK**.



CLI-configuratie

- 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)#
```

CCP maakt deze configuratie op de 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
```

Verifiëren

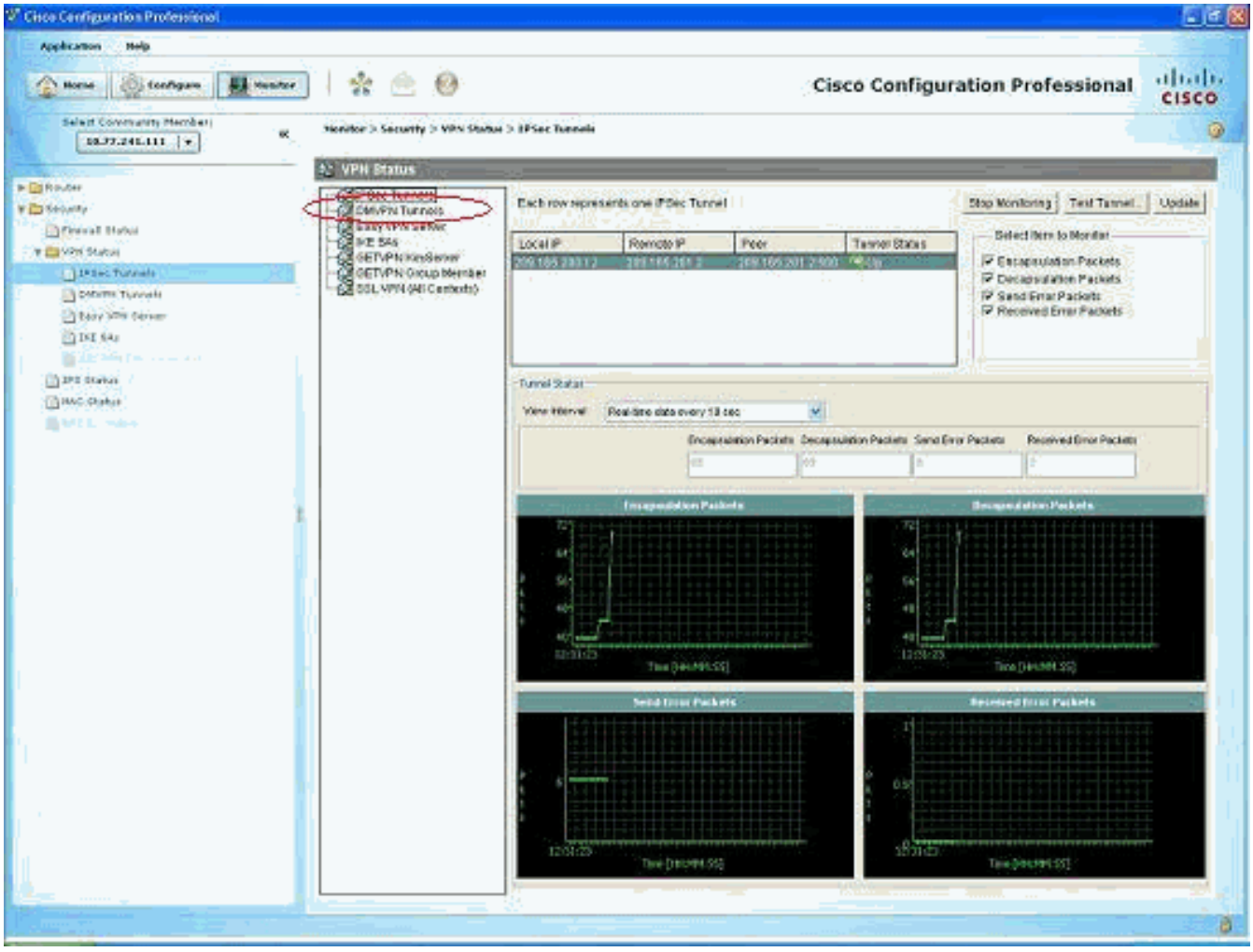
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

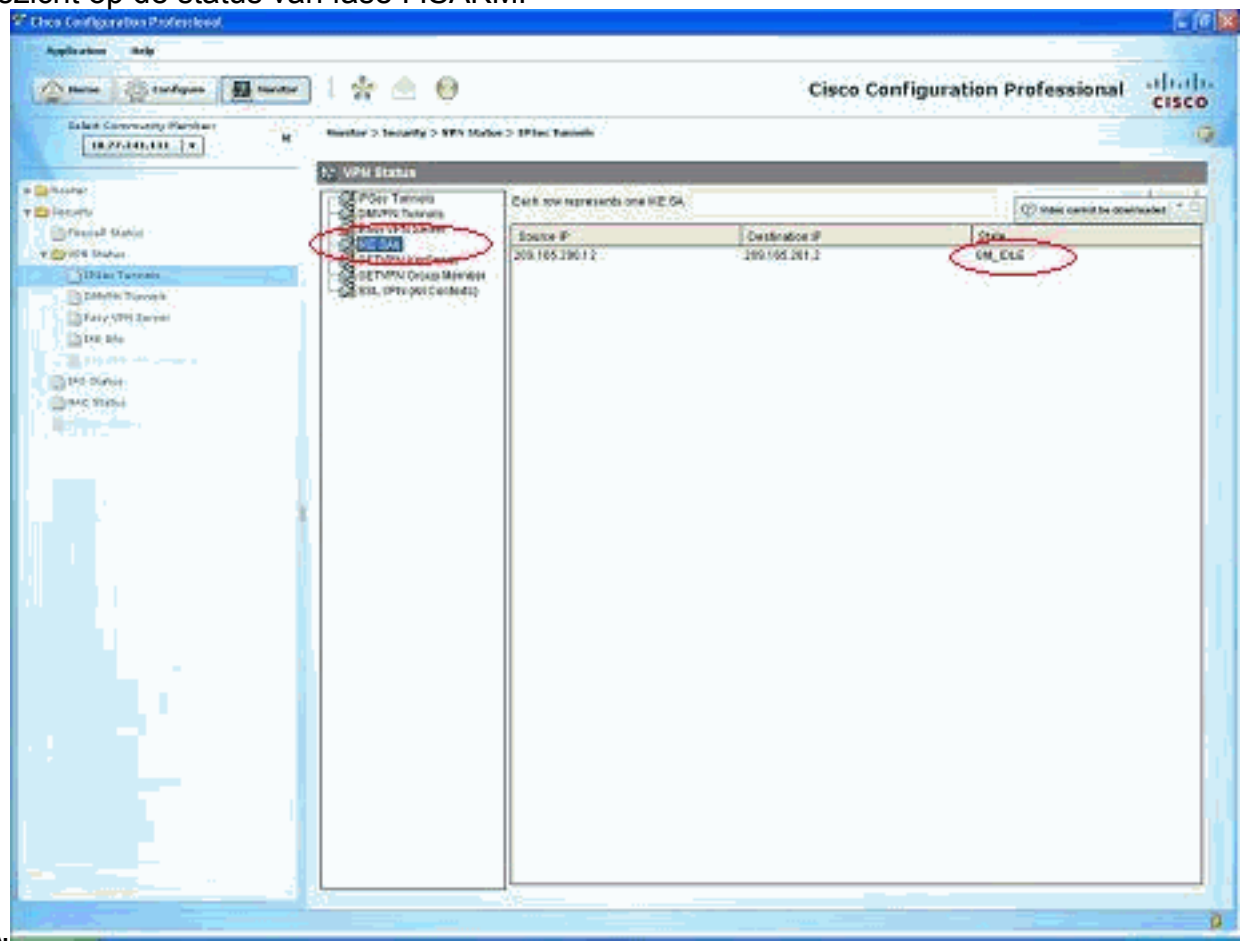
- Verifieer de tunnelparameters door CTP
- Verificatie van de tunnelstatus door ASA CLI
- Verifieer de tunnelparameters door router CLI

Controleer tunnelparameters door CTP

- Controleer het verkeer door de IPsec-tunnel.



- Toezicht op de status van fase I ISAKMP SA.



Controleer de tunnelstatus via ASA CLI

- Controleer de status van fase I ISAKMP SA.

```
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#
```

Opmerking: Neem de Rol in om responder te zijn, wat stelt dat de initiatiefnemer van deze tunnel aan het andere eind is, bijvoorbeeld, de VPN-router.

- Controleer de parameters van fase II IPSEC SA.

```
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
```

Controleer de tunnelparameters door router CLI

- Controleer de status van fase I ISAKMP SA.

```
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
```

- Controleer de parameters van fase II IPSEC SA.

```
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:
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- De bestaande cryptoverbindingen afbreken.

```
ciscoasa#clear crypto ipsec sa
ciscoasa#clear crypto isakmp sa

VPN-Router#clear crypto isakmp
```

- Gebruik **debug** opdrachten om problemen met de VPN-tunnel op te lossen.**Opmerking:** Als u het foutoptreden toelaat, kan dit de werking van de router verstoren wanneer internetwerken hoge belastingsomstandigheden ervaren.**Gebruik debug opdrachten met voorzichtigheid. In het algemeen wordt aanbevolen deze opdrachten alleen te gebruiken onder de richting van uw vertegenwoordiger voor technische ondersteuning van de router wanneer er problemen worden opgelost.**

```
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#
```

Raadpleeg crypto-oplossing voor kreuken in Begrip en het gebruik van debug Commands voor meer informatie over debug-communicatie.

Gerelateerde informatie

- Ondersteuning van IPSEC-onderhandeling/IKE-protocollen
- Documentatie voor Cisco ASA security applicatie S-software
- Meest gebruikelijke oplossingen voor probleemoplossing in IPSEC VPN
- Verzoeken om opmerkingen (RFC's)