De Cisco VPN 3000 Concentrator configureren op een Cisco-router

Inhoud

Inleiding

Deze voorbeeldconfiguratie toont hoe u een privaat netwerk achter een router kunt aansluiten die Cisco IOS® software aan een privaat netwerk achter de Cisco VPN 3000 Concentrator draait. De apparaten op de netwerken kennen elkaar door hun privé adressen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- Cisco 2611 router met Cisco IOS-softwarerelease 12.3.2(1a**Opmerking:** Zorg dat Cisco 2600 Series routers is geïnstalleerd met een crypto IPsec VPN-afbeelding die de VPN-functie

ondersteunt.
- Cisco VPN 3000 Concentrator met 4.0.1 B

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 Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

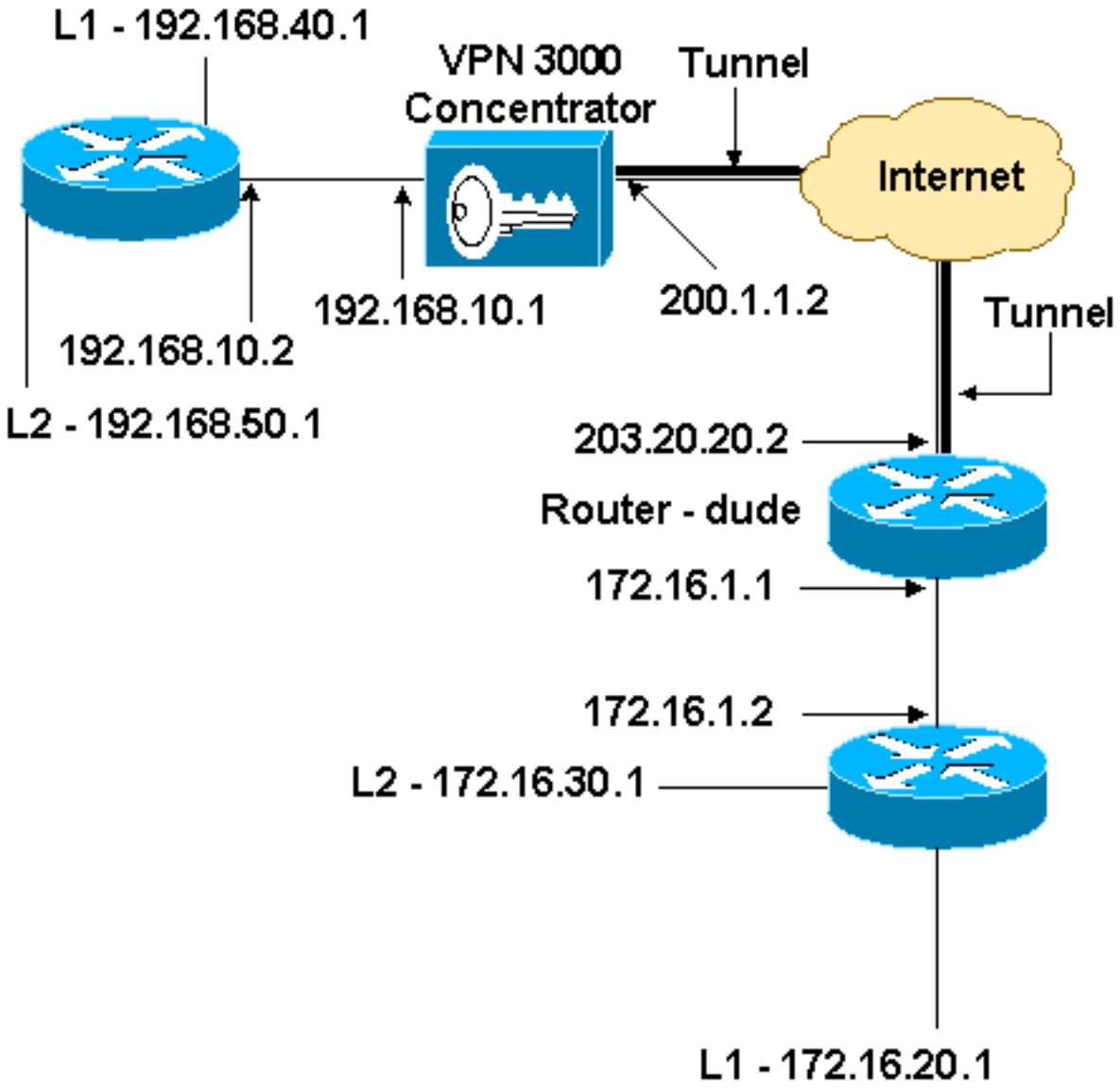
Configureren

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

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd.



Configuraties

Dit document gebruikt deze configuratie.

Routerconfiguratie

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
```

```
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
```

```
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

VPN-configuratie

In deze lab-instelling wordt eerst de VPN-Concentrator benaderd via de console-poort en wordt een minimale configuratie toegevoegd, zodat de verdere configuratie kan worden uitgevoerd via de grafische gebruikersinterface (GUI).

Kies **Beheer > Systeem opnieuw opstarten > Start > Herstart met Fabric-/standaardconfiguratie** om te voorkomen dat er een bestaande configuratie in VPN-centrator is.

De VPN Concentrator verschijnt in Quick Configuration en deze items worden ingesteld na de herstart:

- Tijd/datum
- Interfaces/maskers in **configuratie > interfaces** (publiek=200.1.1.2/24, privé=192.168.10.1/24)
- Standaard gateway in **configuratie > Systeem > IP-routing > Default_Gateway** (20.1.1.1)

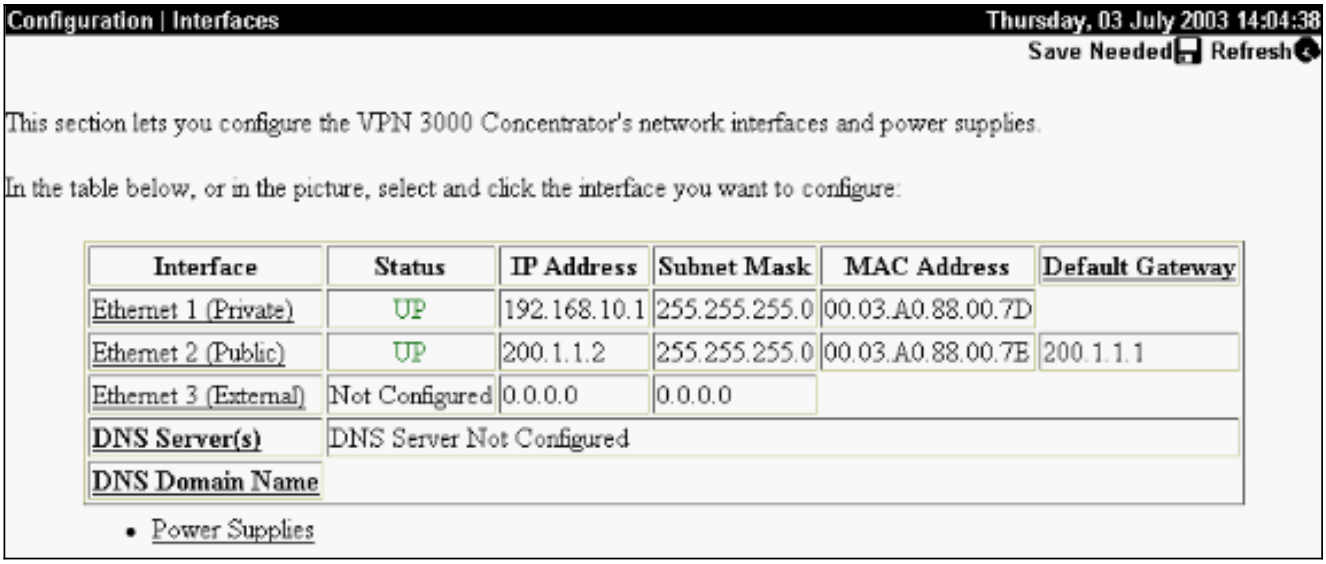
Op dit punt is de VPN Concentrator toegankelijk via HTML van het binnennetwerk.

Opmerking: Omdat de VPN-centrator van buiten wordt beheerd, moet u ook selecteren:

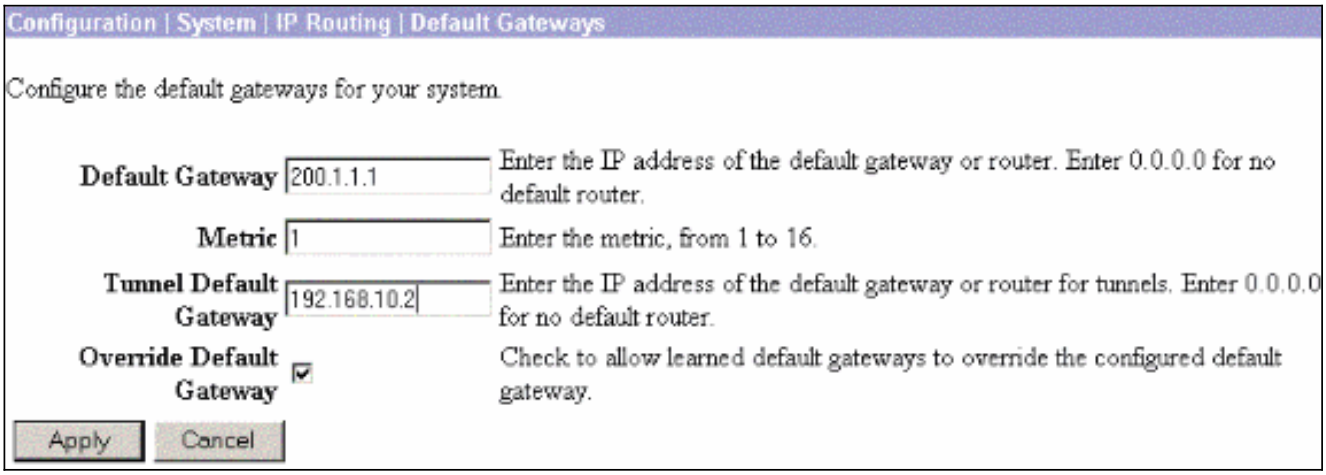
- **Configuratie > Interfaces > 2-publiek > Selecteer IP-filter > 1. Private (standaard)**.
- **Beheer > toegangsrechten > Toegangscontrolelijst > Manager** toevoegen aan het IP-adres van de *externe* manager.

Dit is niet nodig, tenzij u de VPN-centrator van *buiten* beheert.

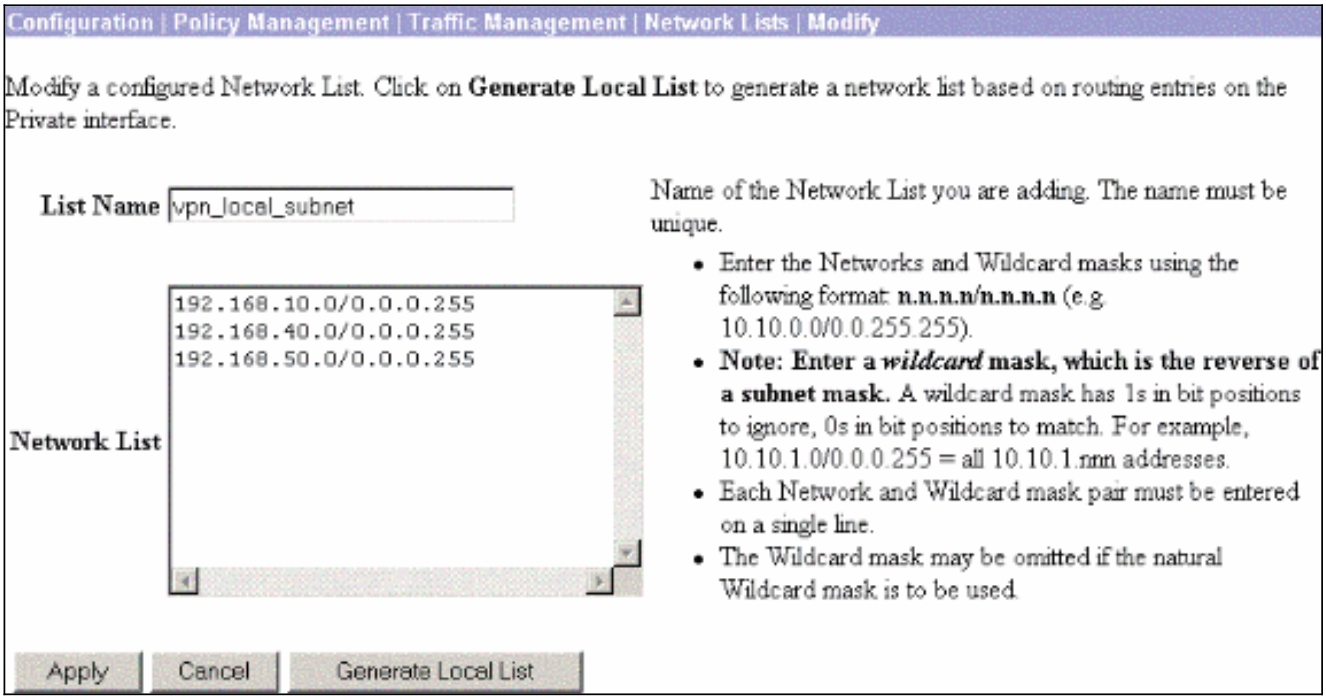
1. Kies **Configuration > Interfaces** om de interfaces opnieuw te controleren nadat u de GUI hebt opgeroepen.



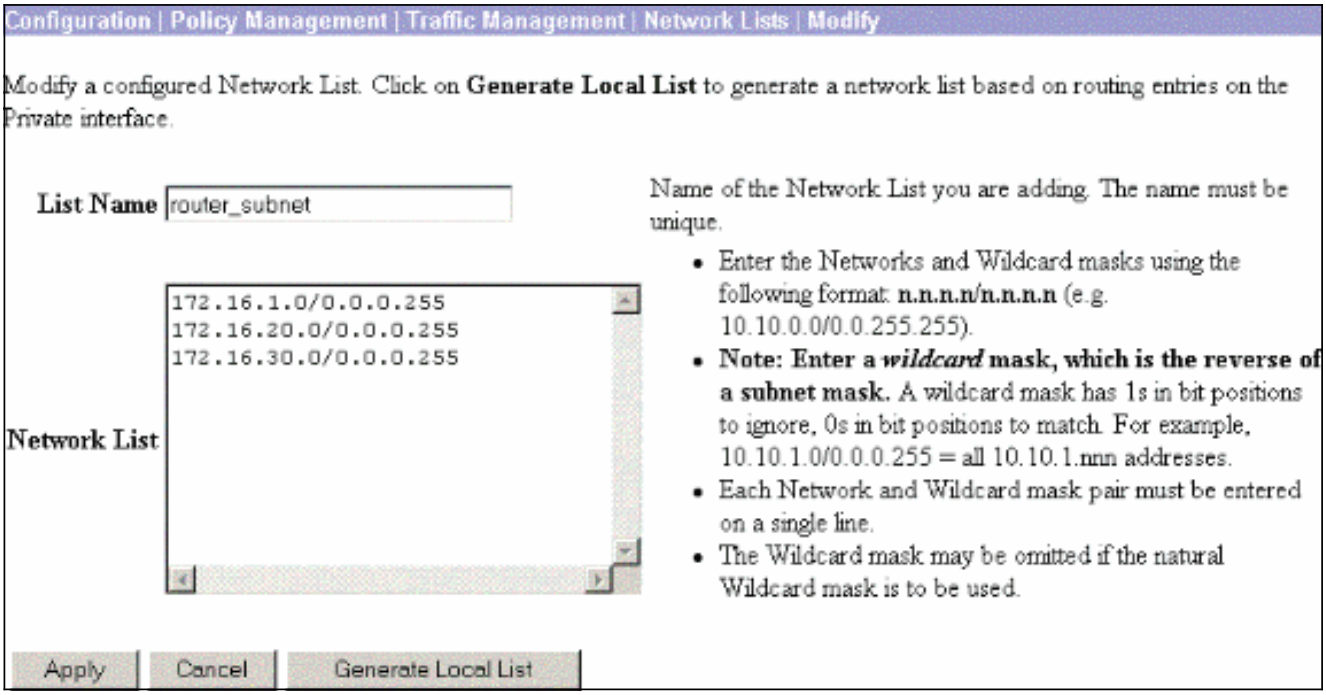
2. Kies Configuration > System > IP-routing > Default gateways om de standaard (Internet) gateway en de **Tunnel Default** (interne) **gateway voor IPsec te** configureren **om de andere subnetten in het privénetwerk te bereiken.**



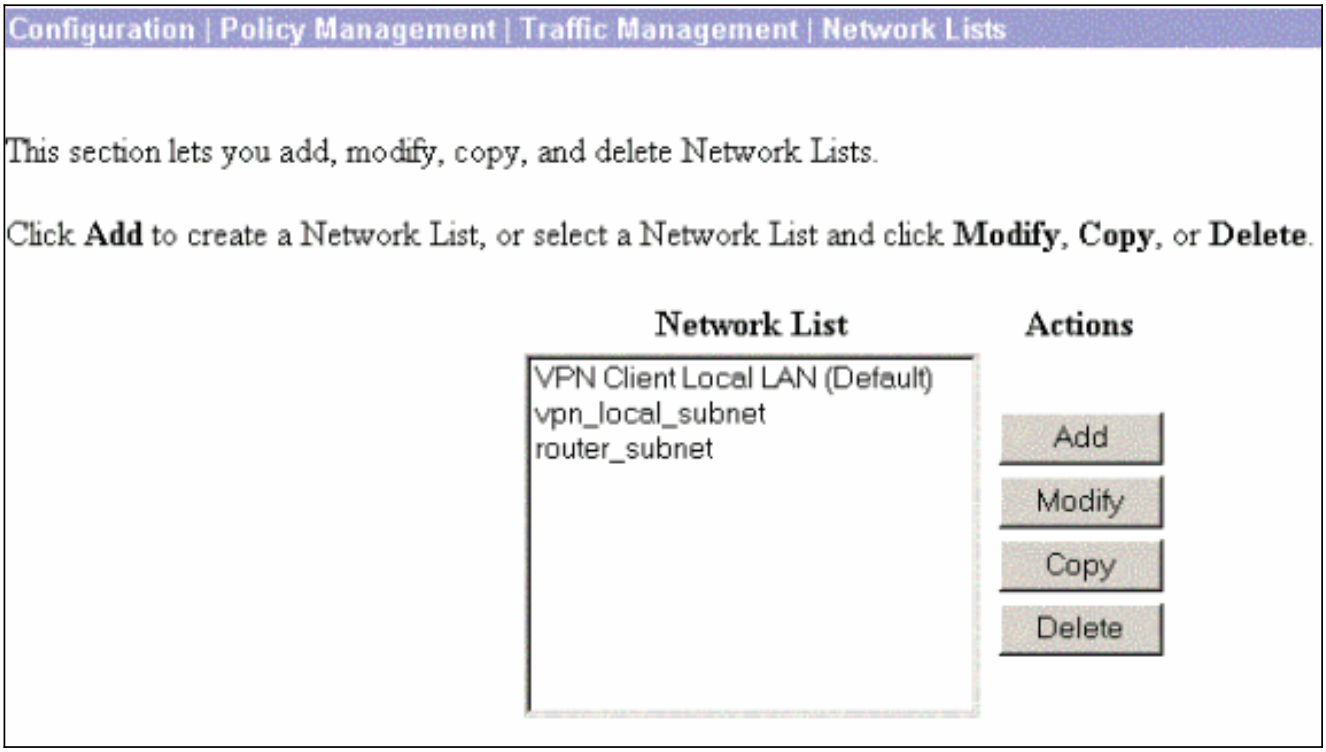
3. Kies **Configuration > Policy Management > Network Lists** om de netwerklijsten te maken die het te versleutelen verkeer definiëren.Dit zijn de lokale netwerken:



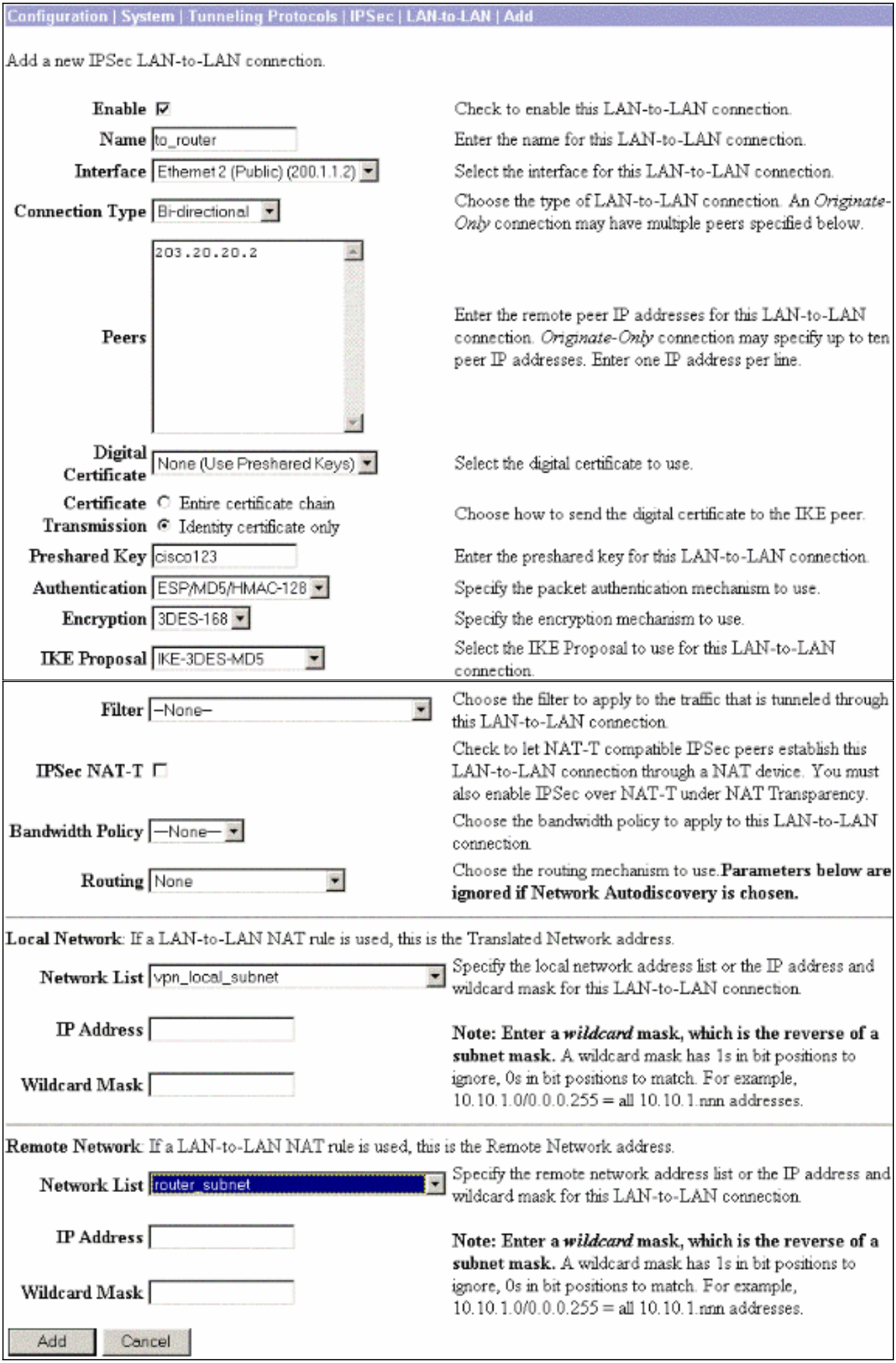
Dit zijn de verafgelegen
netwerken:



4. Na voltooiing, zijn dit de twee netwerklijsten:**Opmerking:** Als de IPsec-tunnel niet omhoog komt, controleer dan of de interessante verkeersovereenkomsten aan beide kanten overeenkomen. Het interessante verkeer wordt gedefinieerd door de toegangslijst in de router- en PIX-boxen. Ze worden gedefinieerd door netwerklijsten in de VPN-concentrators.

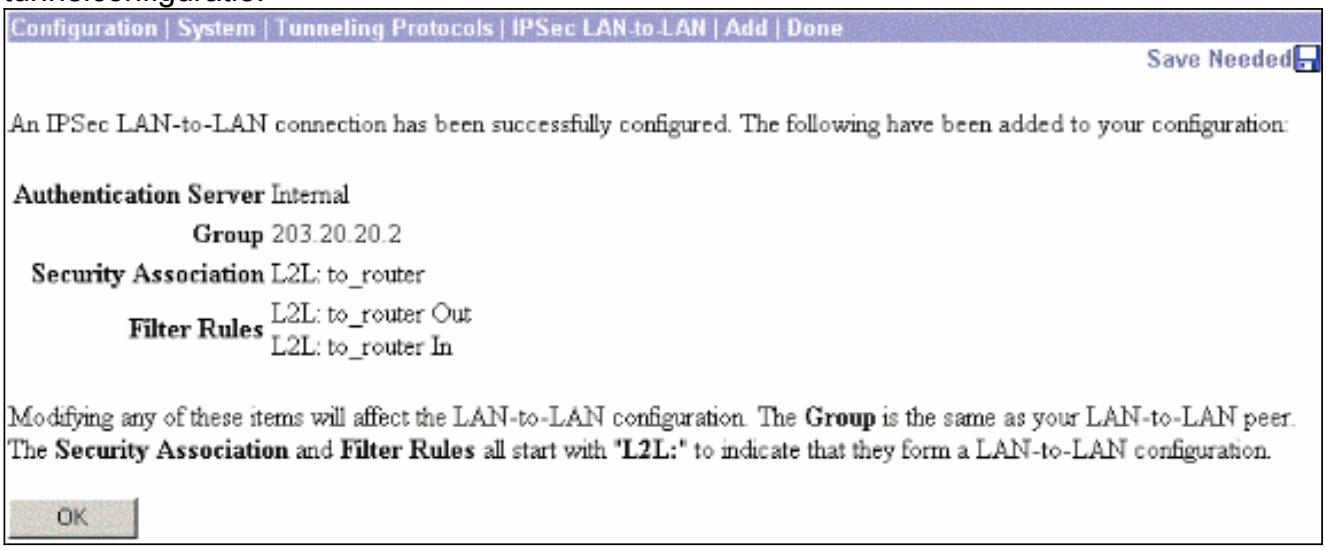


5. Kies **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** en definieer de LAN-to-LAN
tunnel.

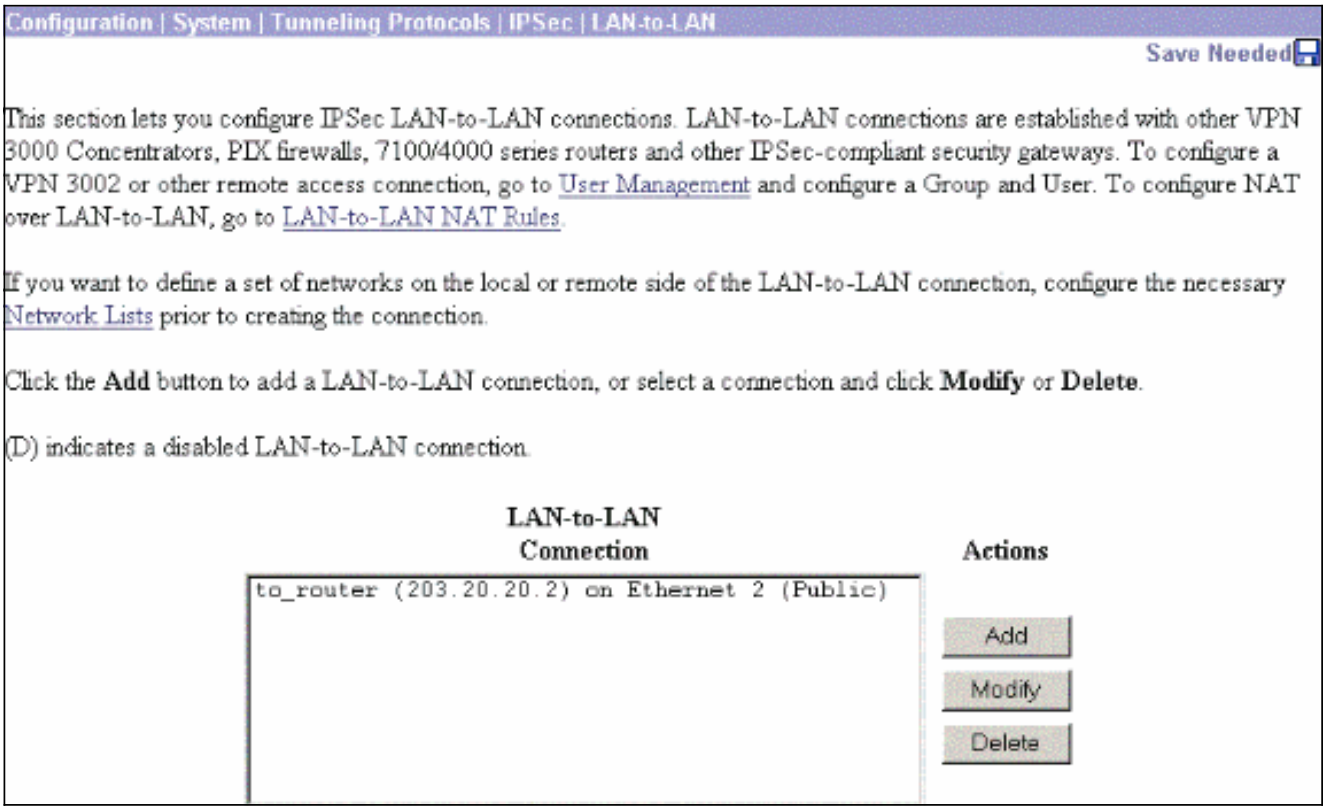


6. Nadat u op **Toepassen** klikt, wordt dit venster weergegeven met de andere configuratie die

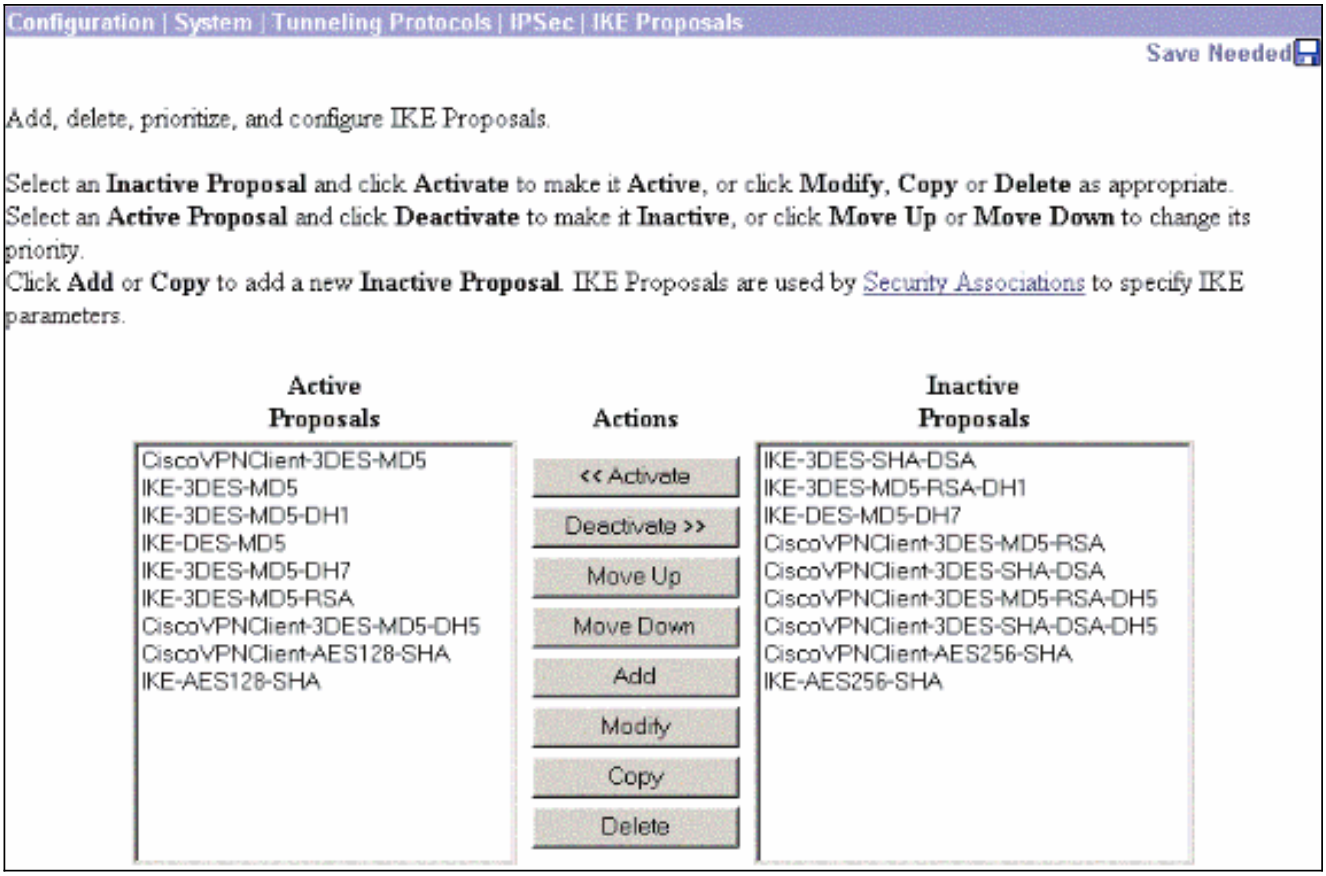
automatisch wordt gemaakt als resultaat van de LAN-to-LAN tunnelconfiguratie.



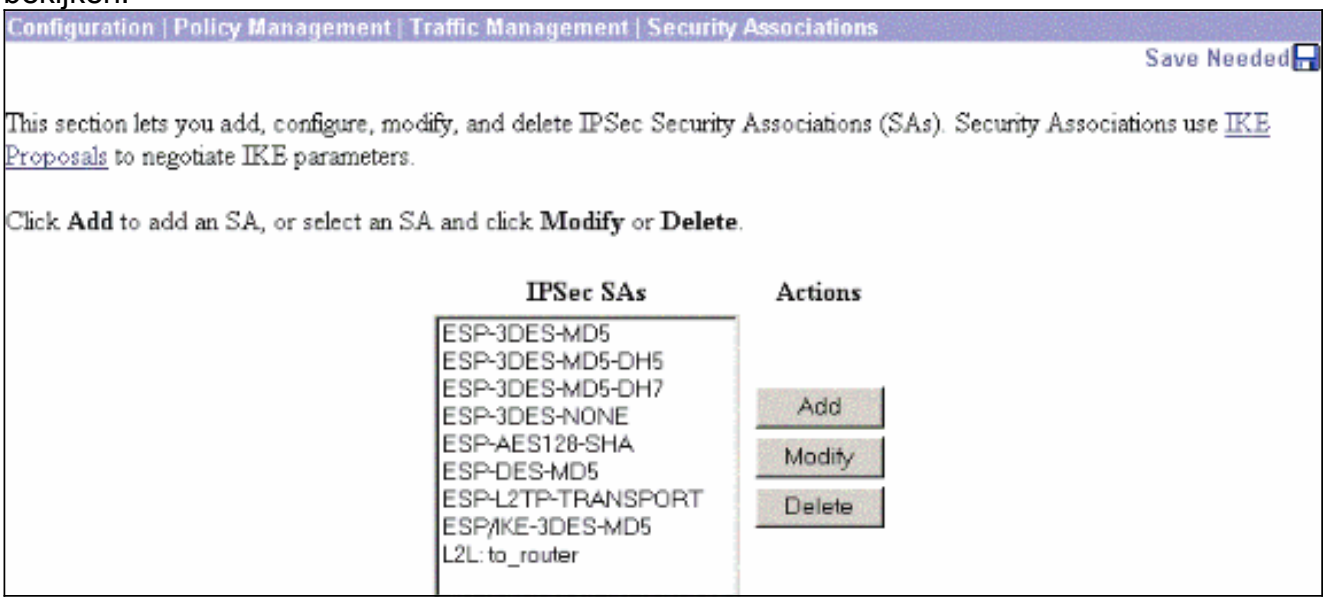
De eerder gemaakte LAN-to-LAN IPsec parameters kunnen worden bekeken of gewijzigd in **Configuration > System > Tunneling**-protocollen **> IPSec LAN-to-LAN.**



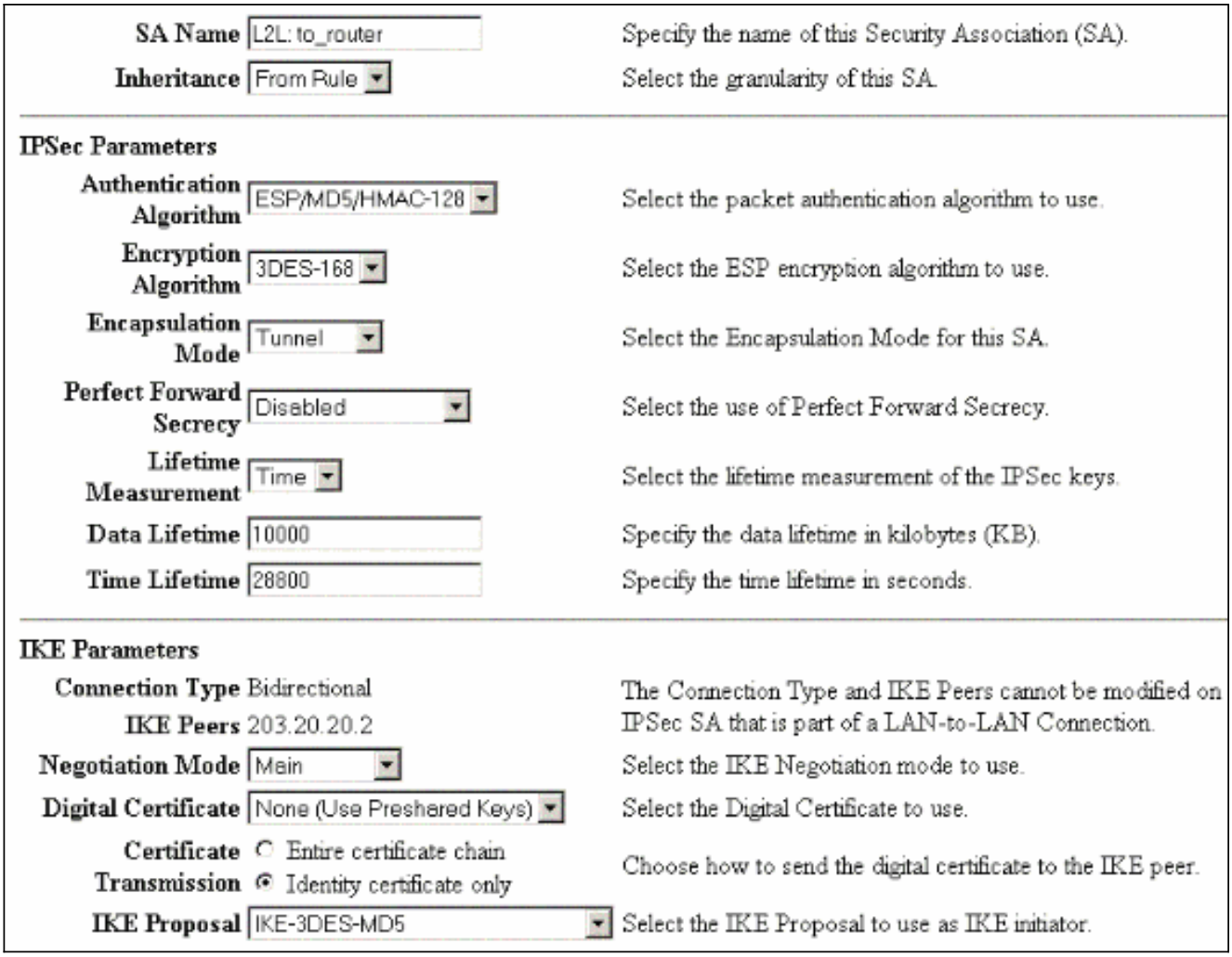
7. Kies **Configuration > System > Tunneling Protocols > IPSec > IKE-voorstellen om het actieve IKE-voorstel te bevestigen.**



8. Kies **Configuration > Policy Management > Traffic Management > Security Associations** om de lijst met beveiligingsassociaties te bekijken.



9. Klik op de naam van de Security Association en klik vervolgens op **Wijzigen** om de Security Associaties te controleren.



Verifiëren

Deze sectie maakt een lijst van de **show** opdrachten die in deze configuratie gebruikt worden.

Op de router

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw 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.

- **tonen crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige Security Associations.
- **toon crypto isakmp sa**-toont alle huidige internet Key Exchange Security Associations bij een peer.
- **tonen de crypto motor verbinding actief** - toont de huidige actieve gecodeerde sessies voor alle crypto motoren.

U kunt het IOS Opname Gereedschap gebruiken (alleen geregistreerde klanten) om meer informatie over bepaalde opdrachten te zien.

Op VPN-concentratie

Kies **Configuration > System > Events > Classes > Wijzigen om de vastlegging aan te zetten.** Deze opties zijn beschikbaar:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Ernst naar logboek = 1-13

Ernst naar console = 1-3

Selecteer **Monitoring > Event Log** om het eventlogboek op te halen.

Problemen oplossen

Op de router

Raadpleeg Belangrijke informatie over Debug Commands voordat u een debug-opdracht probeert.

- **debug van crypto motor**-displays het verkeer dat versleuteld wordt.
- **debug crypto ipsec**-displays de IPsec onderhandelingen van fase 2.
- **debug crypto isakmp** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

Probleem - kan de tunnel niet openen

Fout

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Oplossing

Voltooi deze actie om het gewenste aantal gelijktijdige logins te configureren of de simultane logins voor deze SA in te stellen op 5:

Ga naar **Configuratie > Gebruikersbeheer > Groepen > Wijzigen 10.19.187.229 > Algemeen > Simultaneouts** en wijzig het aantal logins in 5.

PFS

Bij IPsec-onderhandelingen zorgt Perfect Forward SecRITY (PFS) ervoor dat elke nieuwe cryptografische toets geen verband houdt met een eerdere toets. Schakel PFS in of uit op beide tunnelpeers. Anders wordt de LAN-to-LAN (L2L) IPsec-tunnel niet in routers tot stand gebracht.

Om te specificeren dat IPsec naar PFS zou moeten vragen wanneer nieuwe Security Associaties gevraagd worden voor deze crypto map-ingang, of dat IPsec PFS vereist wanneer het verzoeken

om nieuwe Security Associaties ontvangt, gebruik de **set pfs** opdracht in crypto kaart configuratie modus. Om aan te geven dat IPsec geen PFS zou moeten vragen, gebruik de **geen** vorm van deze opdracht.

```
set pfs [group1 | group2]
no set pfs
```

Voor de **ingestelde pfs**-opdracht:

- *groep1* —Specificeert dat IPsec de 768-bits Diffie-Hellman prime modulus groep gebruikt wanneer de nieuwe Diffie-Hellman beurs wordt uitgevoerd.
- *groep2* —Specificeert dat IPsec de 1024-bits Diffie-Hellman prime modulus groep gebruikt wanneer de nieuwe Diffie-Hellman beurs wordt uitgevoerd.

Standaard wordt PFS niet gevraagd. Als er geen groep met deze opdracht is gespecificeerd, **wordt *groep1*** standaard gebruikt.

Voorbeeld:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Raadpleeg de Cisco IOS Security Opdracht Referentie voor meer informatie over de **ingestelde PDF** opdracht.

Gerelateerde informatie

- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 hardwareclients
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems