LAN-to-LAN IPsec tunnelheid tussen Cisco VPN 3000 Concentrator en router met AES-configuratievoorbeeld

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Configureren](#)
[Netwerkdiagram](#)
[Configuraties](#)
[De VPN-concentratie configureren](#)
[Verifiëren](#)
[Controleer de routerconfiguratie](#)
[Controleer de VPN-Concentrator-configuratie](#)
[Problemen oplossen](#)
[Probleemoplossing van de router](#)
[Probleemoplossing voor VPN-centrator](#)
[Gerelateerde informatie](#)

Inleiding

Dit document toont hoe u een IPsec-tunnel kunt configureren tussen een Cisco VPN 3000 Concentrator en een Cisco-router met Advanced Encryption Standard (AES) als het coderingsalgoritme.

AES is een nieuwe Federal Information Processing Standard (FIPS) publicatie die is ontwikkeld door het National Institute of Standards and Technology (NIST) en gebruikt wordt als encryptiemethode. Deze standaard specificeert een AES-symmetrisch encryptie-algoritme dat de Data Encryption Standard (DES) vervangt als een privacy-transformatie voor zowel IPsec als Internet Key Exchange (IKE). AES heeft drie verschillende sleutellengtes, een 128-bits toets (het standaard), een 192-bits toets en een 256-bits toets. De optie AES in Cisco IOS® voegt ondersteuning voor de nieuwe coderingsstandaard AES, met Cipher Block Chaining (CBC) modus, toe aan IPsec.

Raadpleeg de website van het NIST Computer Security Resource Center voor meer informatie over AES.

Raadpleeg LAN-to-LAN IPsec-tunnels tussen Cisco VPN 3000 Concentrator en PIX-firewall

Configuratievoorbeeld voor meer informatie over de LAN-to-LAN tunnelconfiguratie tussen een VPN 3000 Concentrator en PIX-firewall.

Raadpleeg IPsec-tunnelheid tussen PIX 7.x en VPN 3000 Concentrator Configuration Voorbeeld voor meer informatie wanneer PIX softwareversie 7.1 heeft.

Voorwaarden

Vereisten

Dit document vereist een basisbegrip van IPsec-protocol. Raadpleeg een Inleiding naar IPSec-encryptie voor meer informatie over IPsec.

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- **Routervereisten** - De AES-functie is geïntroduceerd in Cisco IOS-softwarerelease 12.2(13)T. Om AES in te schakelen moet uw router IPsec ondersteunen en een IOS-afbeelding uitvoeren met "k9" lange toetsen (het "k9" subsysteem).**Opmerking:** hardwareondersteuning voor AES is ook beschikbaar voor Cisco 2600XM, 2691, 3725 en 3745 AES bespoediging VPN-modules. Deze optie heeft geen gevolgen voor de configuratie en de hardwaremodule wordt automatisch geselecteerd als beide beschikbaar zijn.
- **VPN Concentrator-vereisten** - De softwareondersteuning voor de AES-functie is geïntroduceerd in release 3.6. Hardware ondersteuning wordt geleverd door de nieuwe uitgebreide schaalbare encryptie-processor (SEP-E). Deze eigenschap heeft geen configuratie implicaties.**Opmerking:** In Cisco VPN 3000 Concentrator release 3.6.3 onderhandelen tunnels niet met AES door Cisco bug-ID CSCdy8797 (alleen geregistreerde klanten). Dit is opgelost door middel van release 3.6.4.**Opmerking:** de Cisco VPN 3000 Concentrator gebruikt SEP- of SEP-E-modules, niet beide. Installeer beide niet op hetzelfde apparaat. Als u een SEP-E module op een VPN-centrator installeert die al een SEP-module bevat, schakelt de VPN-centrator de SEP-module uit en gebruikt u alleen de SEP-E module.

Gebruikte componenten

De informatie in dit document is gebaseerd op de software- en hardwareversies:

- Cisco 3600 Series router met Cisco IOS-softwarerelease 12.3(5)SW
- Cisco VPN 3060 Concentrator met softwarerelease 4.0.3

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.

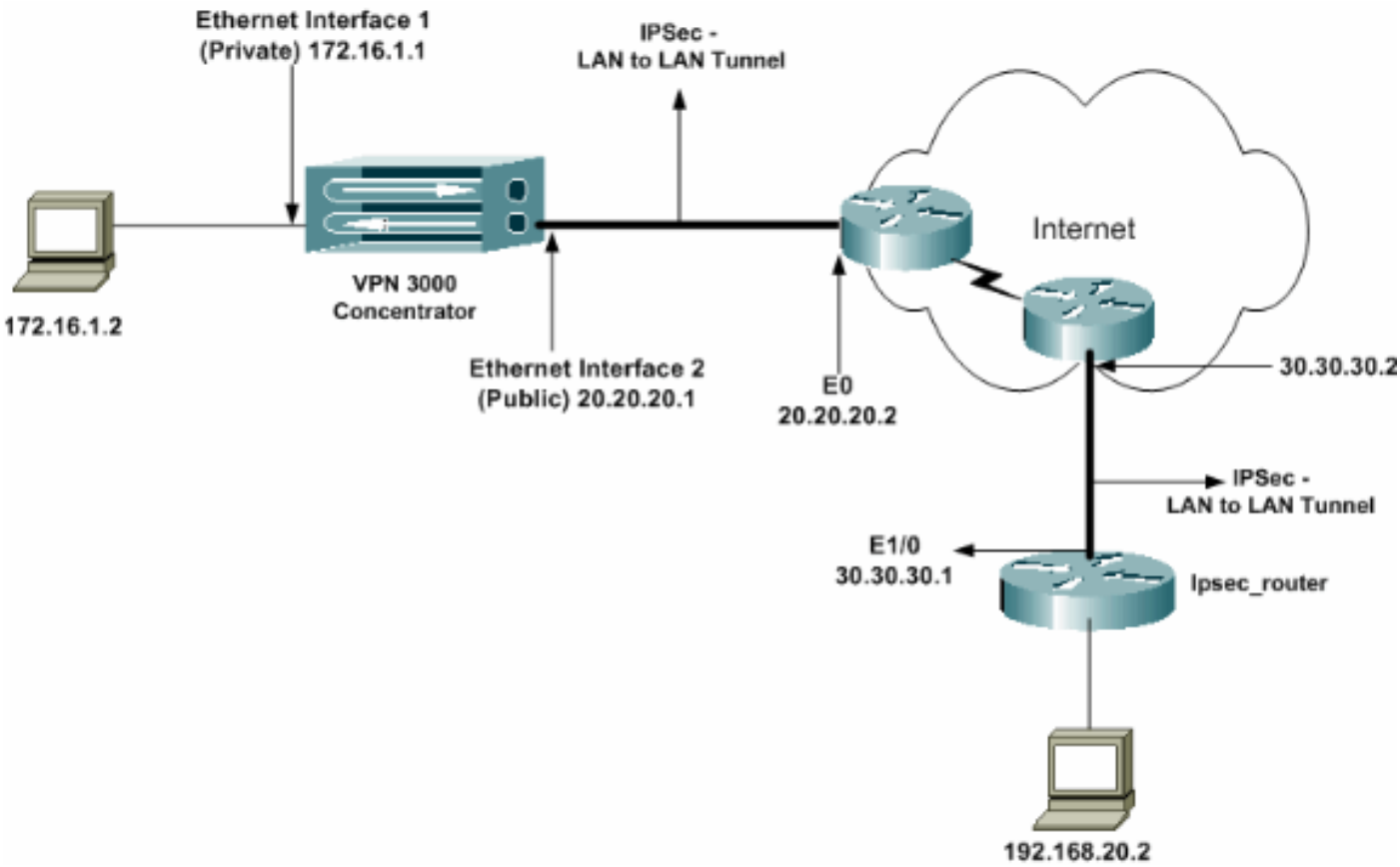
Configureren

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 document gebruikt deze configuraties:

- IPsec-router
- VPN-concentratie

IPsec_router-configuratie

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
```

```
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 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 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
```

```
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Opmerking: Hoewel de syntaxis van ACL ongewijzigd is, zijn de betekeningen voor crypto's iets anders. In crypto ACL's specificeert de **vergunning** dat de overeenkomende pakketten moeten worden versleuteld, terwijl **ontken** aangeeft dat de pakketten niet hoeven te worden versleuteld.

De VPN-concentratie configureren

VPN Concentrators zijn niet voorgeprogrammeerd met IP-adressen in hun fabrieksinstellingen. U moet de troostpoort gebruiken om de eerste configuraties te configureren die een op menu gebaseerde opdrachtregel interface (CLI) zijn. Raadpleeg VPN-centrators configureren via de console voor informatie over de configuratie via de console.

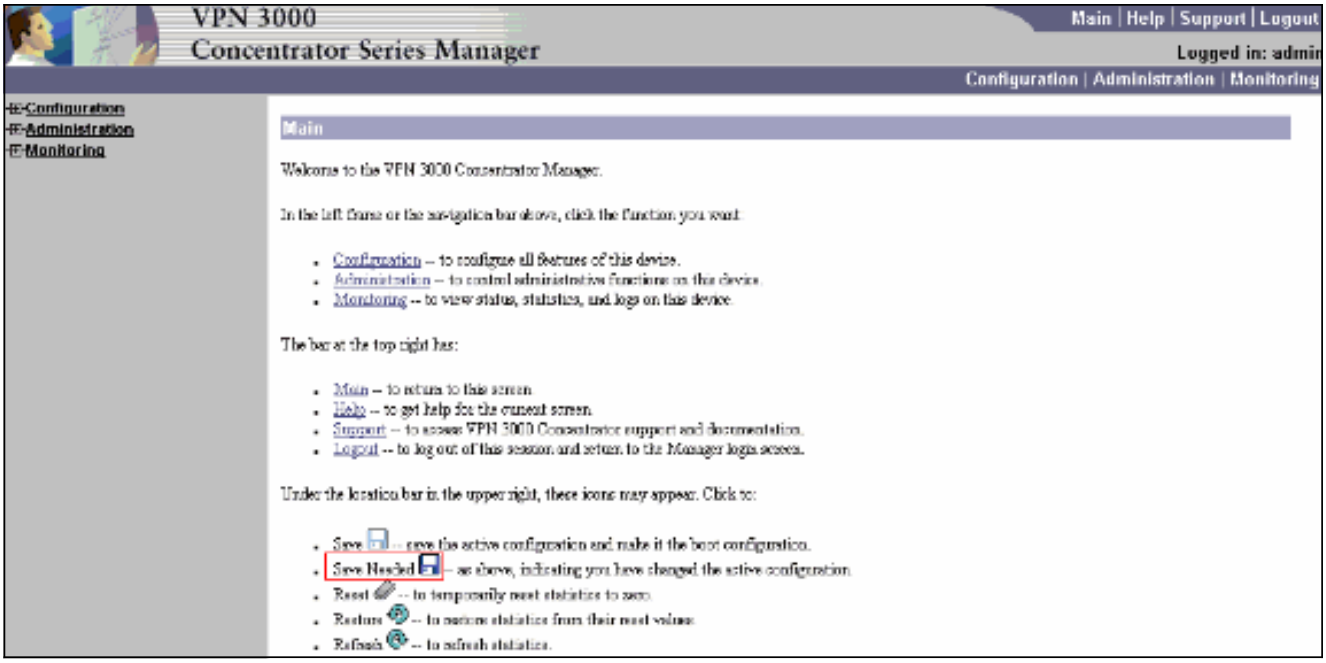
Nadat het IP-adres in de Ethernet 1 (privé) interface is ingesteld, kan de rest worden geconfigureerd met behulp van de CLI of via de browser-interface. De browser interface ondersteunt zowel HTTP als HTTP via Secure Socket Layer (SSL).

Deze parameters worden ingesteld in de console:

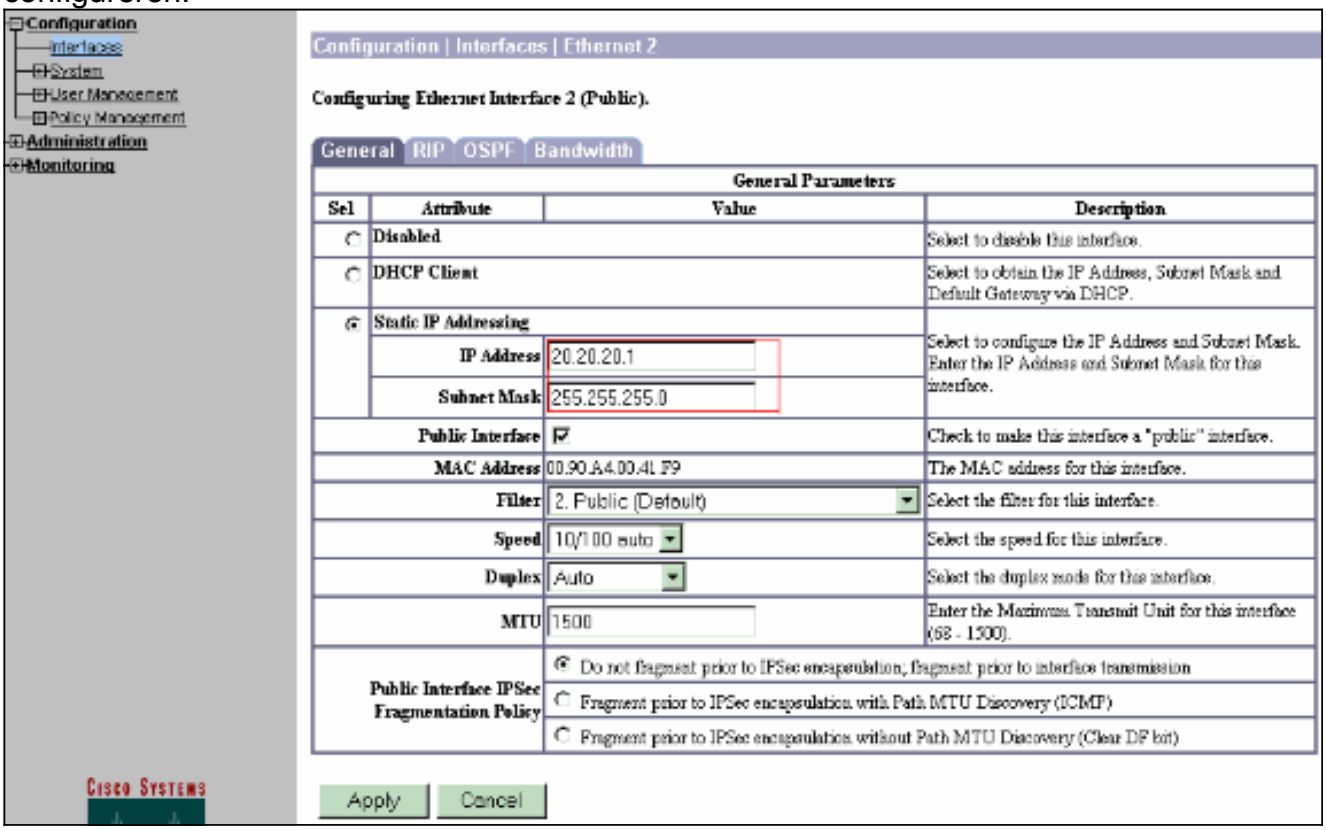
- **Tijd/datum** - Het juiste tijdstip en de juiste datum zijn erg belangrijk. Zij helpen ervoor te zorgen dat de registratie en de boekingen nauwkeurig zijn, en dat het systeem een geldig veiligheidscertificaat kan creëren.
- **Ethernet 1 (privé) interface** - Het IP-adres en -masker (van onze netwerktopologie 172.16.1.1/24).

Op dit punt is de VPN Concentrator toegankelijk via een HTML browser van het binnennetwerk. Raadpleeg voor informatie over het configureren van de VPN-centrator in CLI-modus Quick Configuration via CLI.

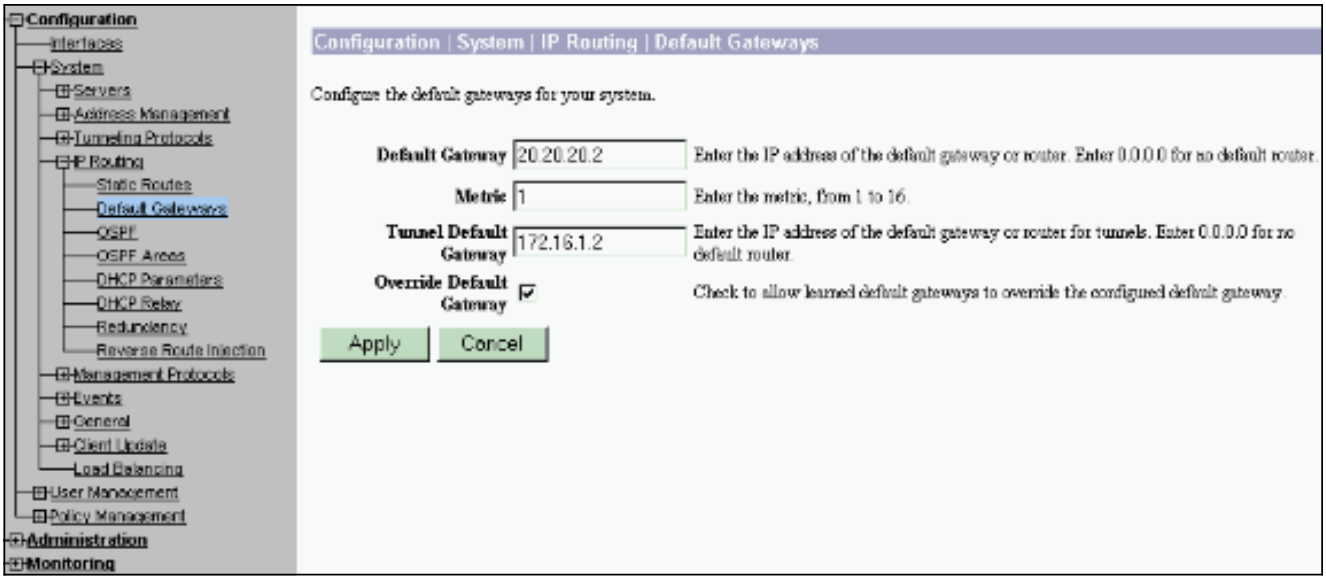
1. Typ het IP-adres van de privé-interface van de webbrowser om de GUI-interface mogelijk te maken.Klik op het pictogram **Save need** om wijzigingen in het geheugen op te slaan. De standaard fabrieksnaam en het wachtwoord zijn "admin" wat hoofdlettergevoelig is.



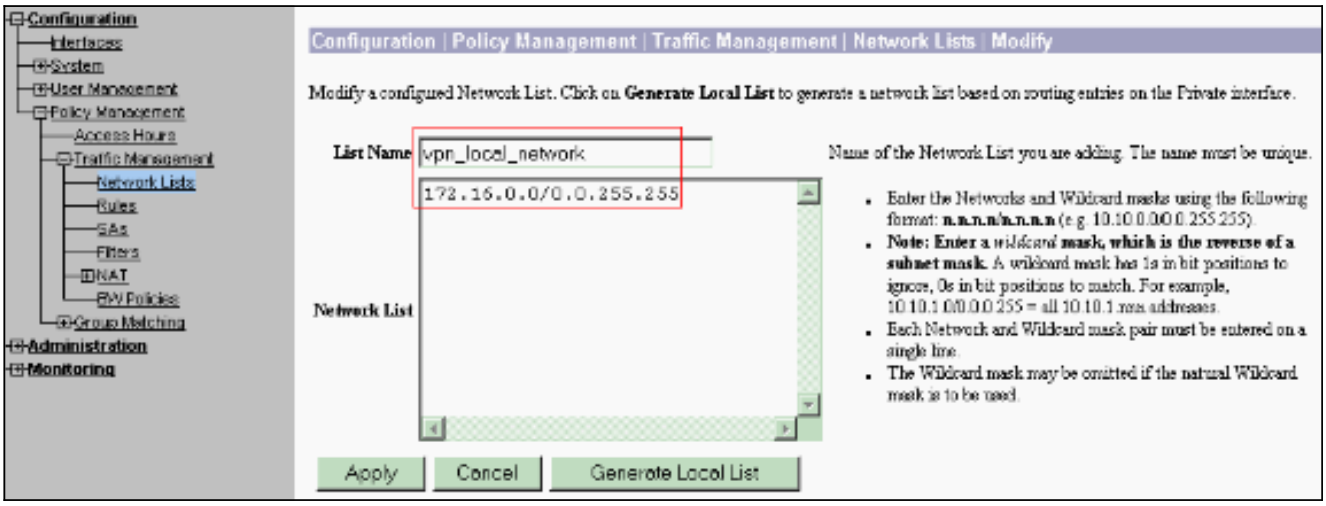
2. Nadat u de GUI hebt opgeroepen, selecteert u **Configuration > Interfaces > Ethernet 2 (Public)** om de Ethernet 2-interface te configureren.



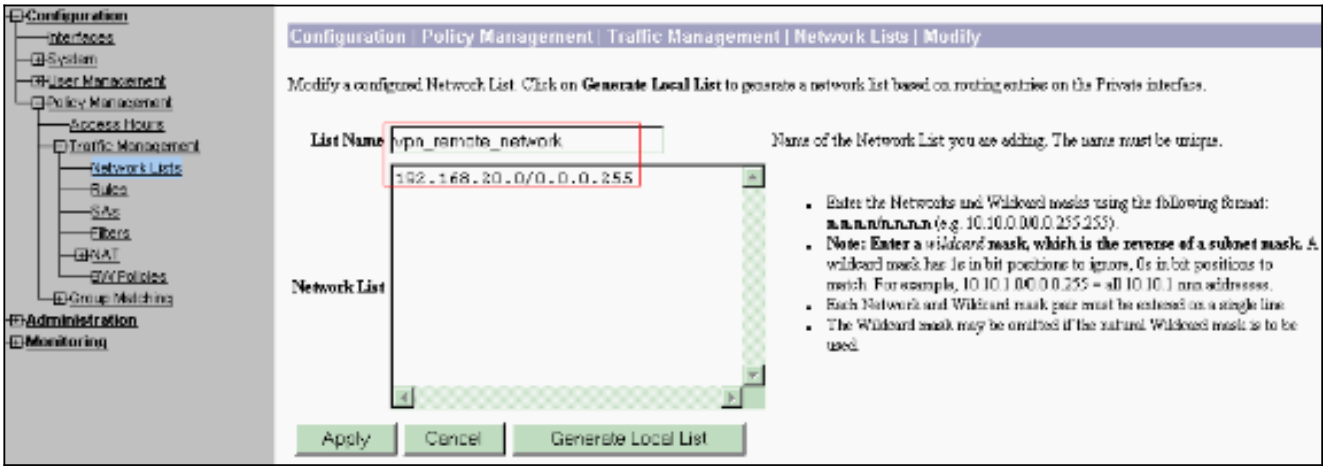
3. Selecteer **Configuration > System > IP-routing > Default gateways** en stel de standaardgateway (Internet) en de tunnelstandaardgateway (binnenin) voor IPsec in om de andere subnetten in het privénetwerk te bereiken.In dit scenario, is er slechts één voorwerp beschikbaar op het binnennetwerk.



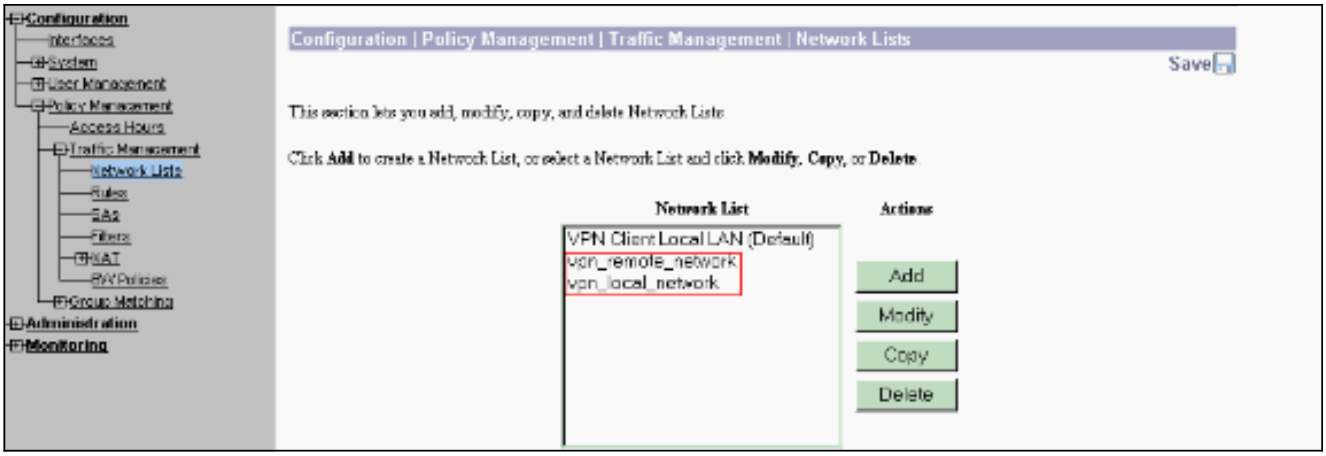
4. Selecteer **Configuration > Policy Management > Traffic Management > Network Lists > Add om de netwerklijsten te definiëren en te versleutelen verkeer te definiëren.**De in de lijst vermelde netwerken zijn bereikbaar voor het externe netwerk. De netwerken in de onderstaande lijst zijn lokale netwerken. U kunt de lokale netwerklijst ook automatisch via RIP genereren wanneer u op **Local List** klikt.



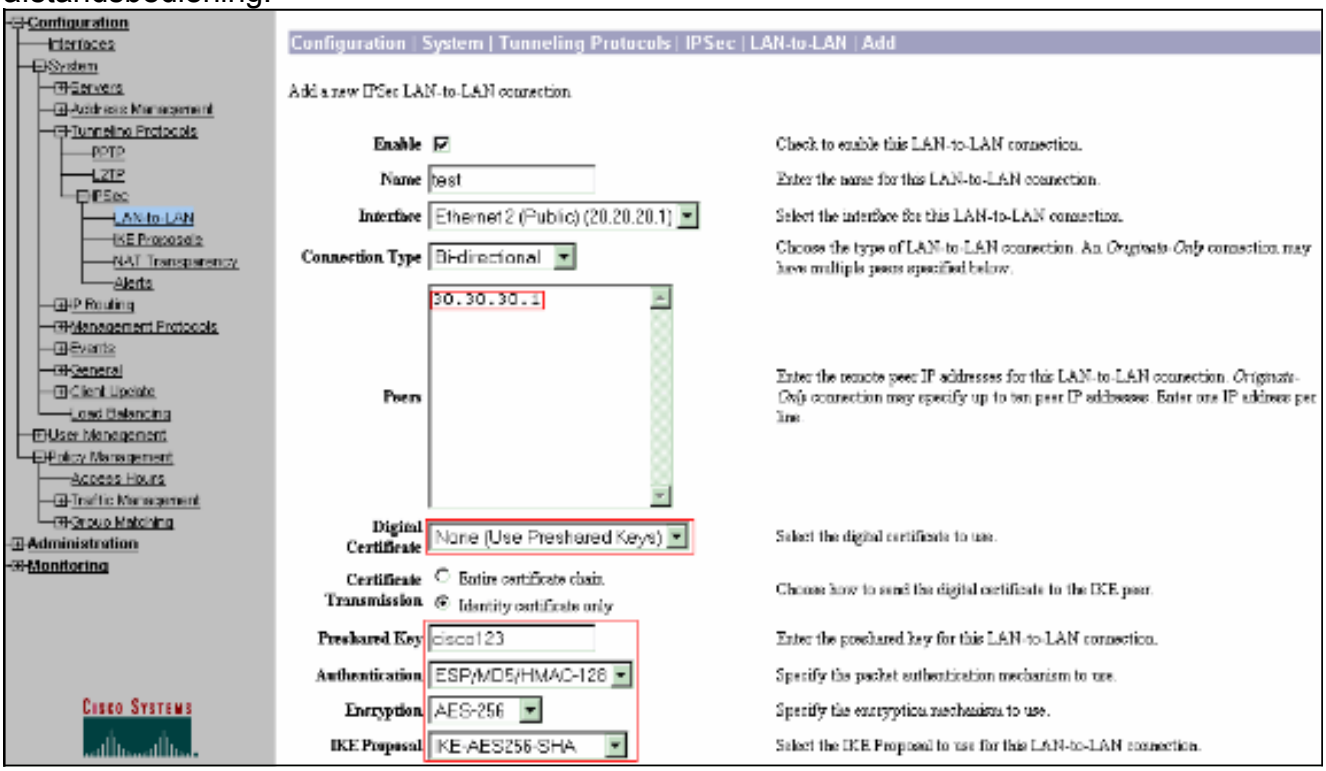
5. De netwerken in deze lijst zijn externe netwerken en moeten handmatig worden ingesteld. Om dit te doen, voer het netwerk/de wildkaart voor elke bereikbare vorm in.

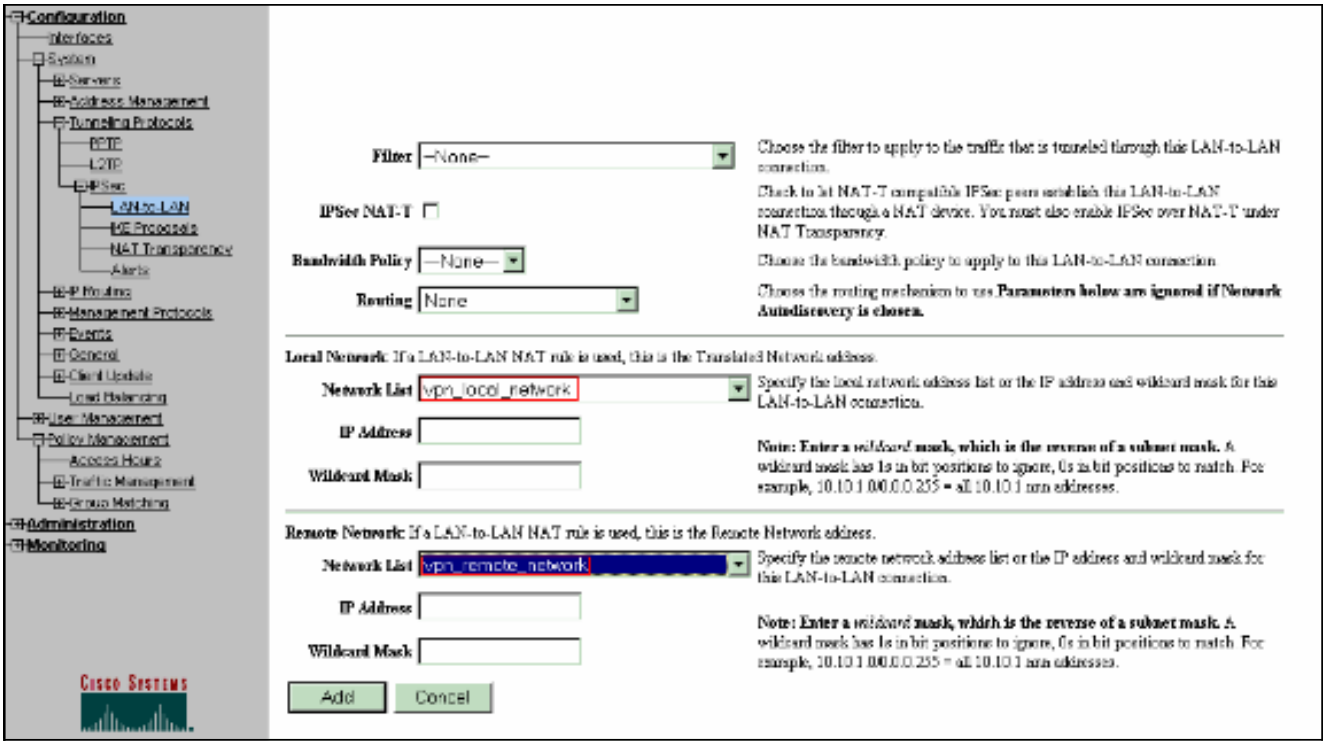


Na voltooiing, zijn dit de twee netwerklijsten:

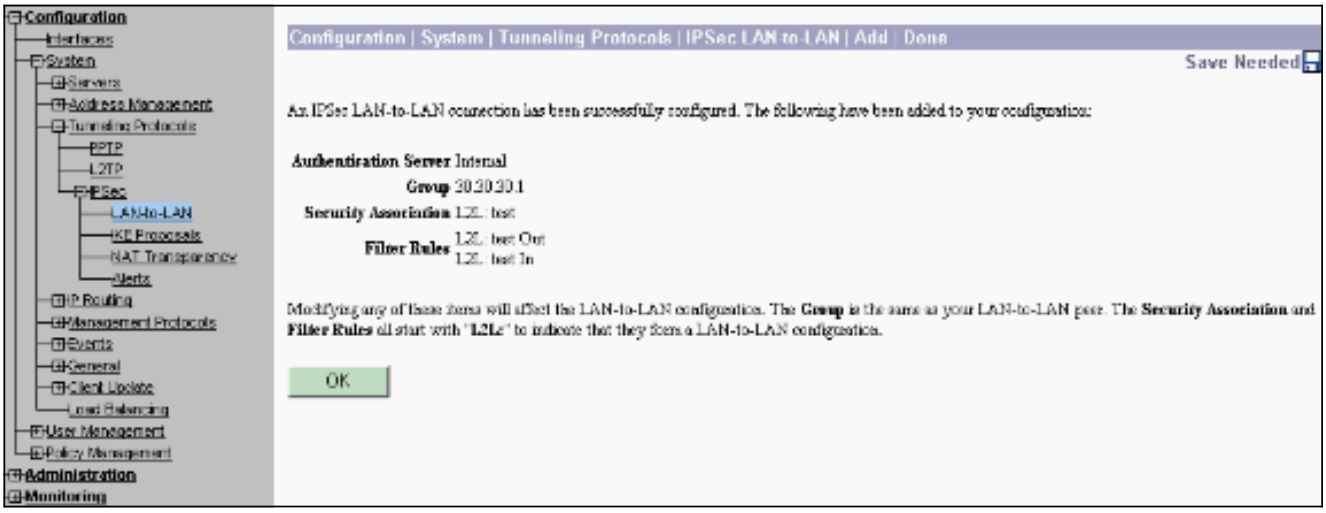


6. Selecteer **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add en definieer de LAN-to-LAN tunnel.**Dit venster heeft drie delen. Het bovenste gedeelte is voor de netwerkinformatie en de onderste twee delen zijn voor de lijsten met lokale en externe netwerken. Selecteer in het gedeelte Network Information de AES-encryptie, het type verificatie, het IKE-voorstel en de vooraf gedeelde toets. In de onderste delen wijst u naar de netwerklijsten die u al hebt gemaakt, zowel lokaal als afstandsbediening.



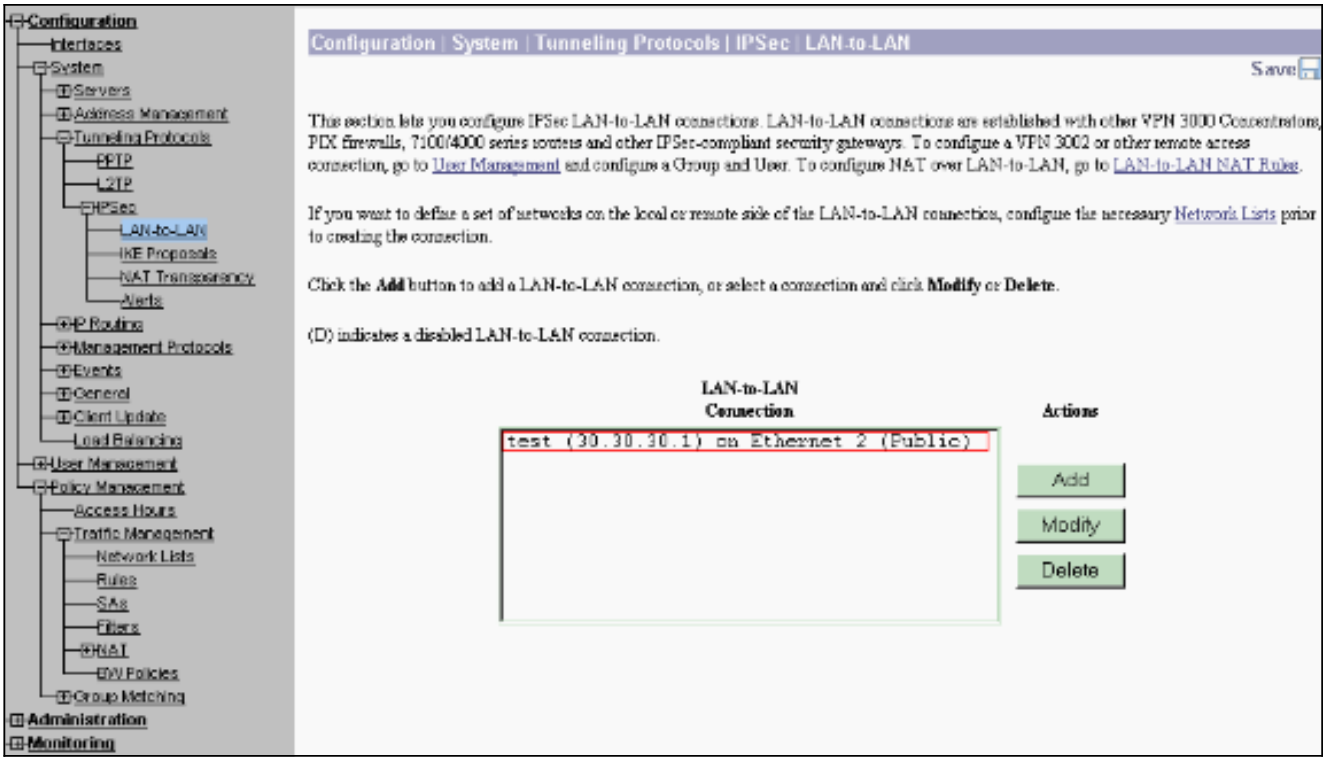


7. Nadat u op **Add** klikt, als uw verbinding correct is, wordt u met het venster IPSec LAN-to-LAN-Add-Ready weergegeven.Dit venster geeft een overzicht van de informatie over de tunnelconfiguratie. Het stelt ook automatisch de groepsnaam, SA Naam en de filternaam in. U kunt alle parameters in deze tabel
bewerken.



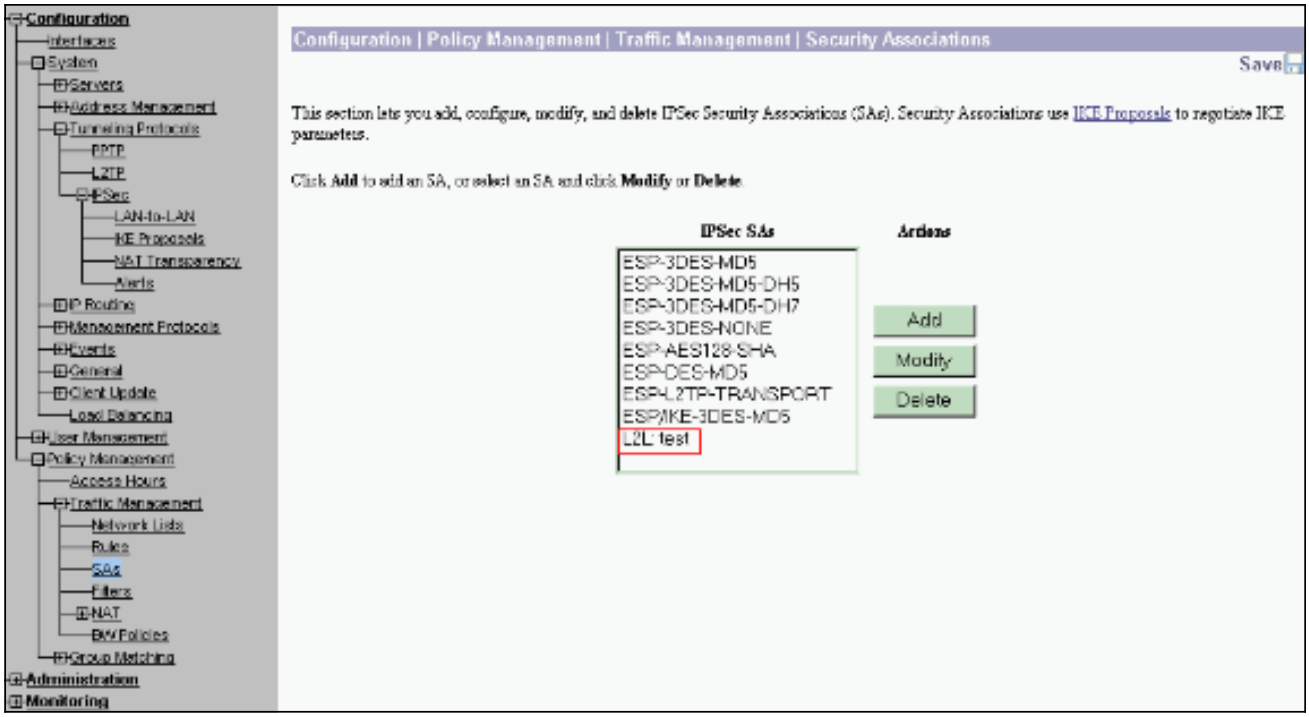
Op dit punt is de IPsec LAN-to-LAN tunnel ingesteld en u kunt aan het werk gaan. Als, om één of andere reden, de tunnel niet werkt, kunt u op misconfiguraties controleren.

8. U kunt de eerder gemaakte LAN-to-LAN IPsec-parameters bekijken of wijzigen wanneer u **Configuration > System > Tunneling-protocollen > IPSec LAN-to-LAN** selecteert.Deze grafiek laat "test" zien aangezien de naam van de tunnel en de openbare interface van het verre uiteinde 30.30.30.1 is zoals in het
scenario.

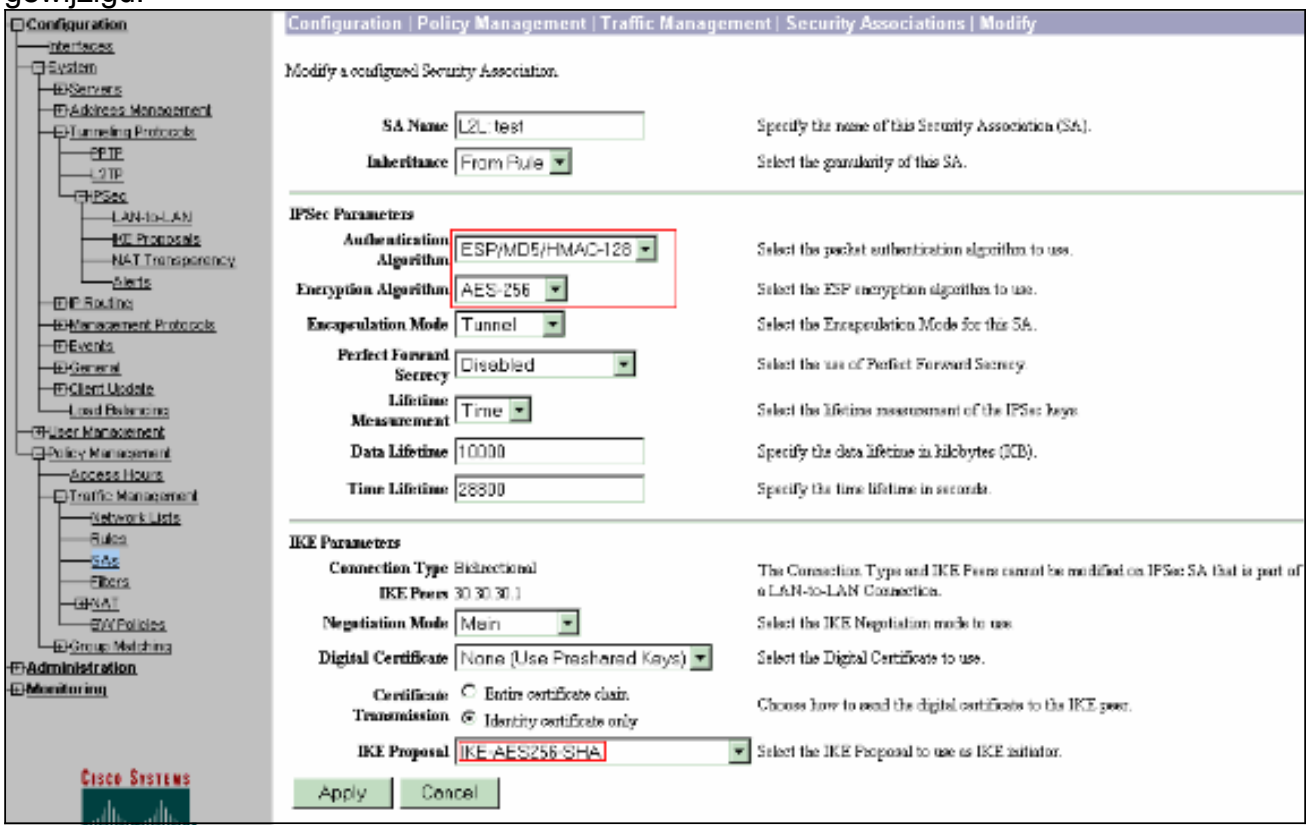


9. Soms komt uw tunnel misschien niet als uw IKE-voorstel in de lijst van Inactieve Voorstellen staat. Selecteer **Configuration > System > Tunneling Protocols > IPSec > IKE Voorstellen om het actieve IKE-voorstel te configureren.**Als uw IKE-voorstel in de lijst "Inactieve voorstellen" staat, kunt u dit inschakelen wanneer u het IKE-voorstel selecteert en op de knop **Activeren** klikt. In deze grafiek staat het geselecteerde voorstel "IKE-AES256-SHA" in de lijst met actieve
voorstellen.

10. Selecteer **Configuration > Policy Management > Traffic Management > Security Associations** om te controleren of de SA-parameters juist
zijn.



11. Klik op de SA naam (in dit geval, **L2L: test**), en klik vervolgens op **Wijzigen** om de SA's te controleren.Als een van de parameters niet overeenkomt met de configuratie van de afstandsbediening, kan deze hier worden gewijzigd.



Verifiëren

Controleer de routerconfiguratie

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

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **toon crypto isakmp sa**-Toont alle huidige IKE SAs bij een peer. De staat QM_IDLE duidt erop dat de SA authentiek blijft met zijn peer en kan worden gebruikt voor daaropvolgende snelle mode uitwisselingen. Het is in een stille staat.

```
ipsec_router#show crypto isakmp sa

 dst            src           state    conn-id   slot

 20.20.20.1     30.30.30.1    QM_IDLE        1      0
```

- **Laat crypto ipsec sa**-displays de instellingen die worden gebruikt door de huidige SAs. Controleer voor de peer IP adressen, de netwerken toegankelijk op zowel de lokale als verre eindpunten, en de transformatie die wordt gebruikt. Er zijn twee ESP SA's, één in elke richting. Aangezien AH-transformatoren worden gebruikt, is deze leeg.

```
ipsec_router#show crypto ipsec sa

interface: Ethernet1/0

       Crypto map tag: vpn, local addr. 30.30.30.1

       protected vrf:

        local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

       remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

       current_peer: 20.20.20.1:500

         PERMIT, flags={origin_is_acl,}

        #pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

        #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

        #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.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

        path mtu 1500, media mtu 1500

        current outbound spi: 54FA9805

       inbound esp sas:

       spi: 0x4091292(67703442)

        transform: esp-256-aes esp-md5-hmac ,

        in use settings ={Tunnel, }

        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

        sa timing: remaining key lifetime (k/sec): (4471883/28110)
```

```
 IV size: 16 bytes

 replay detection support: Y

inbound ah sas:

inbound pcp sas:

 outbound esp sas:

spi: 0x54FA9805(1425709061)

 transform: esp-256-aes esp-md5-hmac ,

 in use settings ={Tunnel, }

 slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn

 sa timing: remaining key lifetime (k/sec): (4471883/28110)

 IV size: 16 bytes

 replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

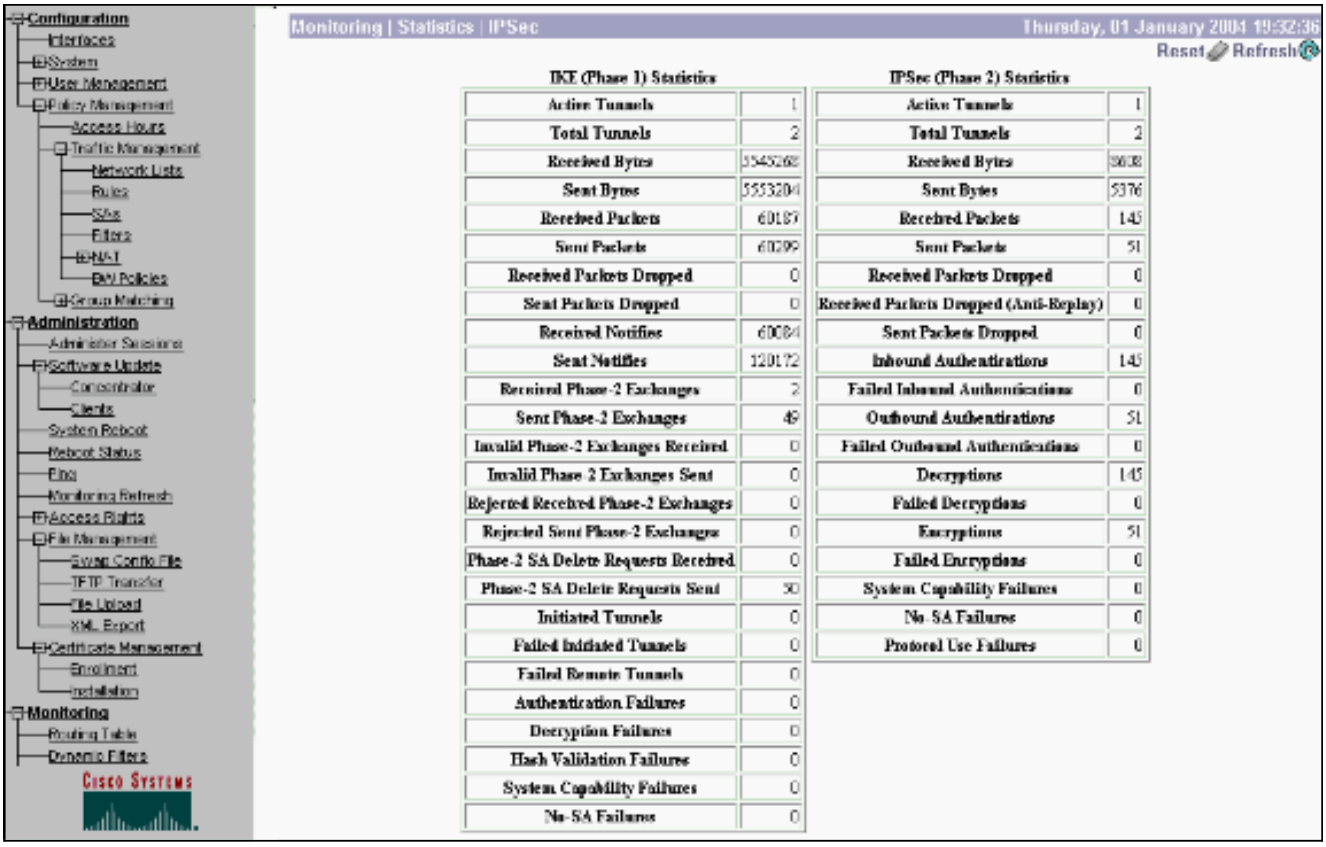
- **tonen de crypto motorverbindingen actief**—Hiermee worden de huidige actieve gecodeerde sessies weergegeven voor alle cryptomotoren. Elke verbinding-ID is uniek. Het aantal pakketten dat versleuteld en gedecrypteerd zijn wordt weergegeven in de laatste twee kolommen.

```
ipsec_router#show crypto engine connections active
   ID     Interface     IP-Address   State   Algorithm          Encrypt Decrypt

    1     Ethernet1/0   30.30.30.1   set     HMAC_SHA+AES_256_C       0       0

 2000     Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C       0      19

 2001     Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C      19       0
```

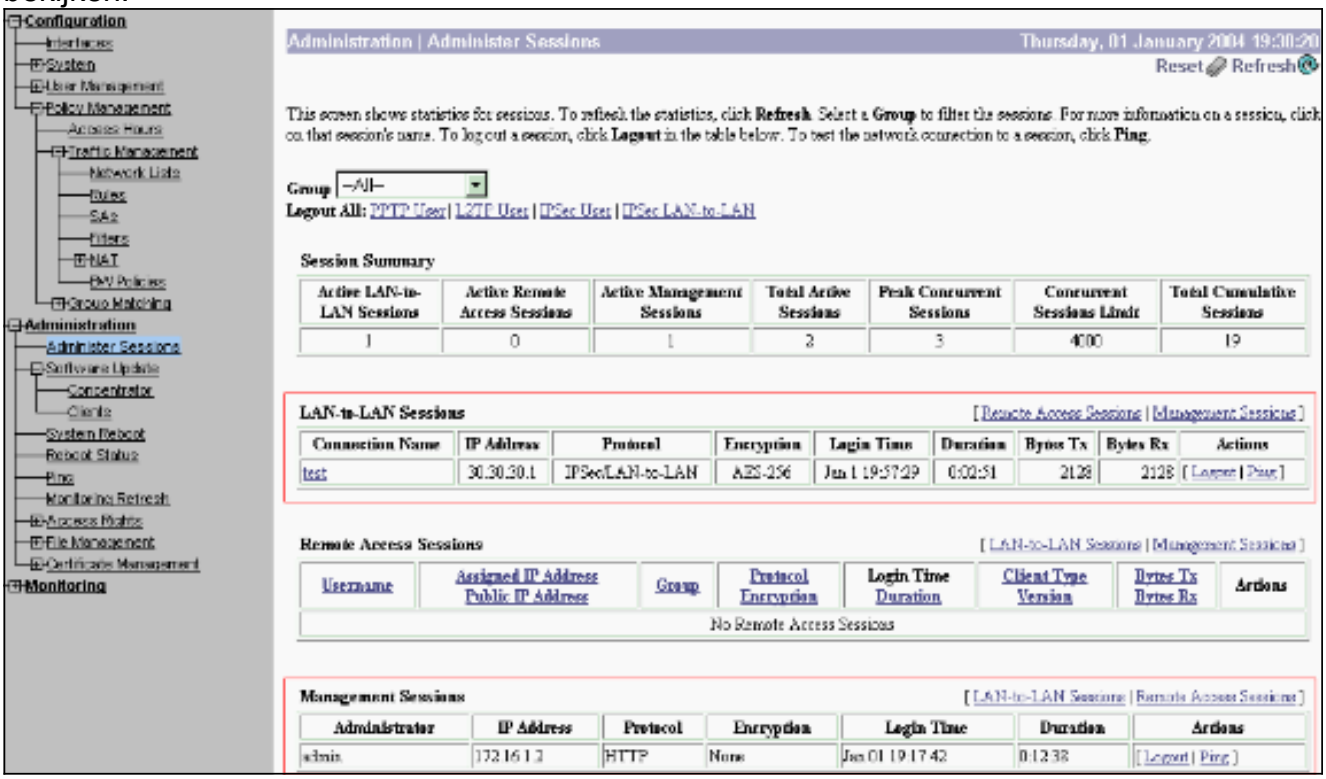
Controleer de VPN-Concentrator-configuratie

Voltooi deze stappen om de VPN-configuratie te controleren.

1. Gelijkaardig om **crypto ipsec te tonen zoals** en **crypto isakmp als** opdrachten op routers **te tonen**, kunt u de IPsec en IKE statistieken bekijken wanneer u **Controle > Statistieken > IPSec op VPN Concentrators selecteert.**



2. Overeenkomstig de **actieve** opdracht **Encrypt-motorverbindingen** op routers kunt u het beheervenster-sessies op VPN-centrator gebruiken om de parameters en statistieken voor alle actieve IPsec LAN-to-LAN verbindingen of tunnels te bekijken.



Problemen oplossen

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

Probleemoplossing van de router

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

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

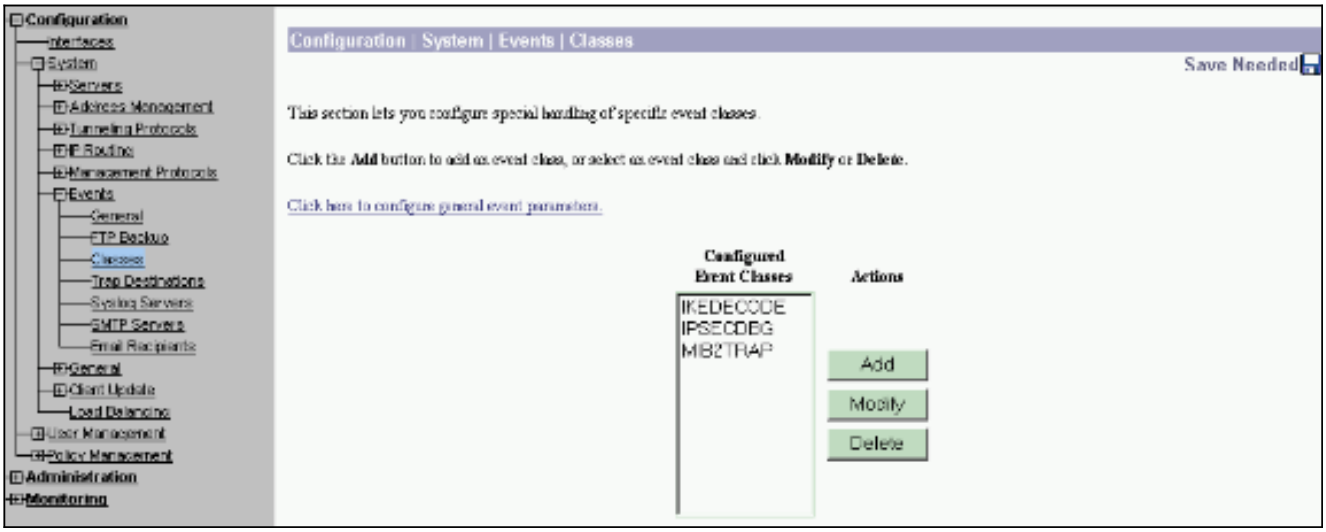
- **debug van crypto motor**-displays het verkeer dat versleuteld wordt. De cryptomotor is het echte mechanisme dat encryptie en decryptie uitvoert. Een cryptomotor kan software zijn of een hardwareversneller.
- **debug van crypto isakmp** — Hiermee geeft u de onderhandelingen over IKE fase 1 weer van de Internet Security Association en Key Management Protocol (ISAKMP).
- **debug crypto ipsec**-displays de IPsec-onderhandelingen van IKE fase 2.

Raadpleeg IPSec-probleemoplossing - Het begrip en het gebruik van **debug** Commands voor meer gedetailleerde informatie en steekproefuitvoer.

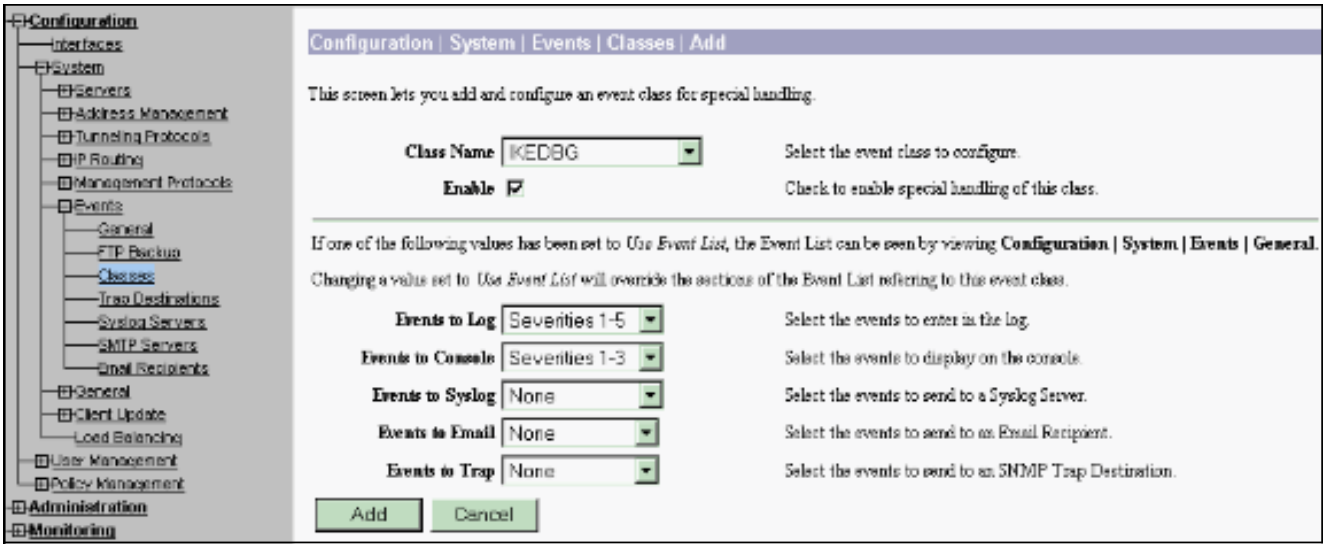
Probleemoplossing voor VPN-centrator

Gelijkaardig aan **debug** bevelen op de routers van Cisco, kunt u de klassen van gebeurtenis configureren om alle alarmen te bekijken.

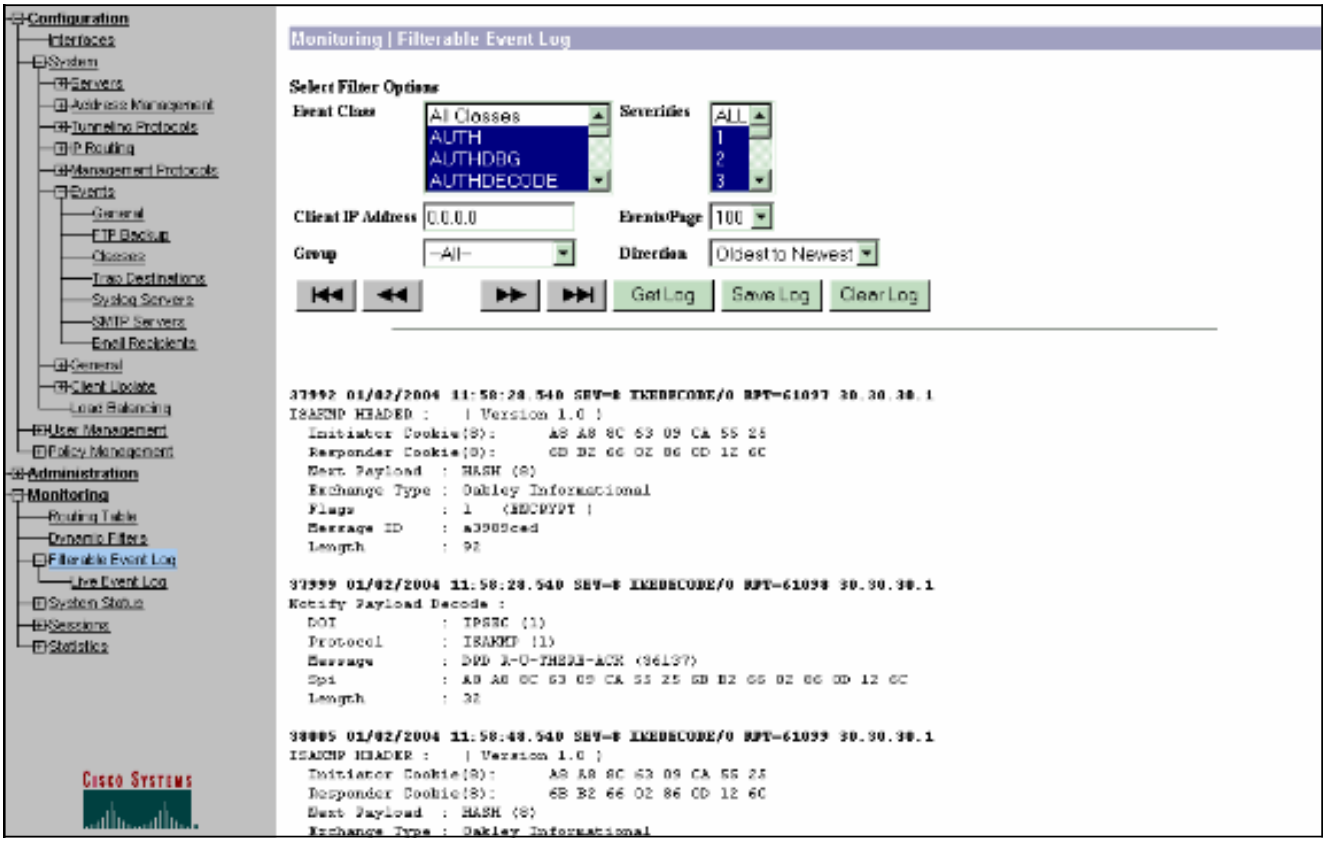
1. Selecteer **Configuration > System > Events > Classes > Add om de logging of Event class in te schakelen.**Deze klassen zijn beschikbaar voor IPsec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. Tijdens het toevoegen kunt u ook het ernst-niveau voor elke klasse selecteren, gebaseerd op het ernst-niveau dat het alarm wordt verzonden.De alarmen kunnen op een van deze manieren worden behandeld:Op logboekOp de console weergegevenNaar de UNIX-bladeserver verzondenAls e-mail verzondenVerstuurd als een val naar een Simple Network Management Protocol-server
(SNMP)



3. Selecteer **Monitoring > Filterable Event Log** om de enabled alarmen te controleren.



Gerelateerde informatie

- Advanced Encryption Standard (AES)
- DES/3DES/AES VPN-encryptie
- IPsec-voorbeeldconfiguratie
- Cisco VPN 3000 Series clientondersteuningspagina
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen