

De Cisco VPN 3000 Concentrator configureren op een Cisco-router

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[VPN-configuratie](#)

[Verifiëren](#)

[Op de router](#)

[Op VPN-concentratie](#)

[Problemen oplossen](#)

[Op de router](#)

[Probleem - kan de tunnel niet openen](#)

[PFS](#)

[Gerelateerde informatie](#)

[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-software release 12.3.2(1)**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](#).

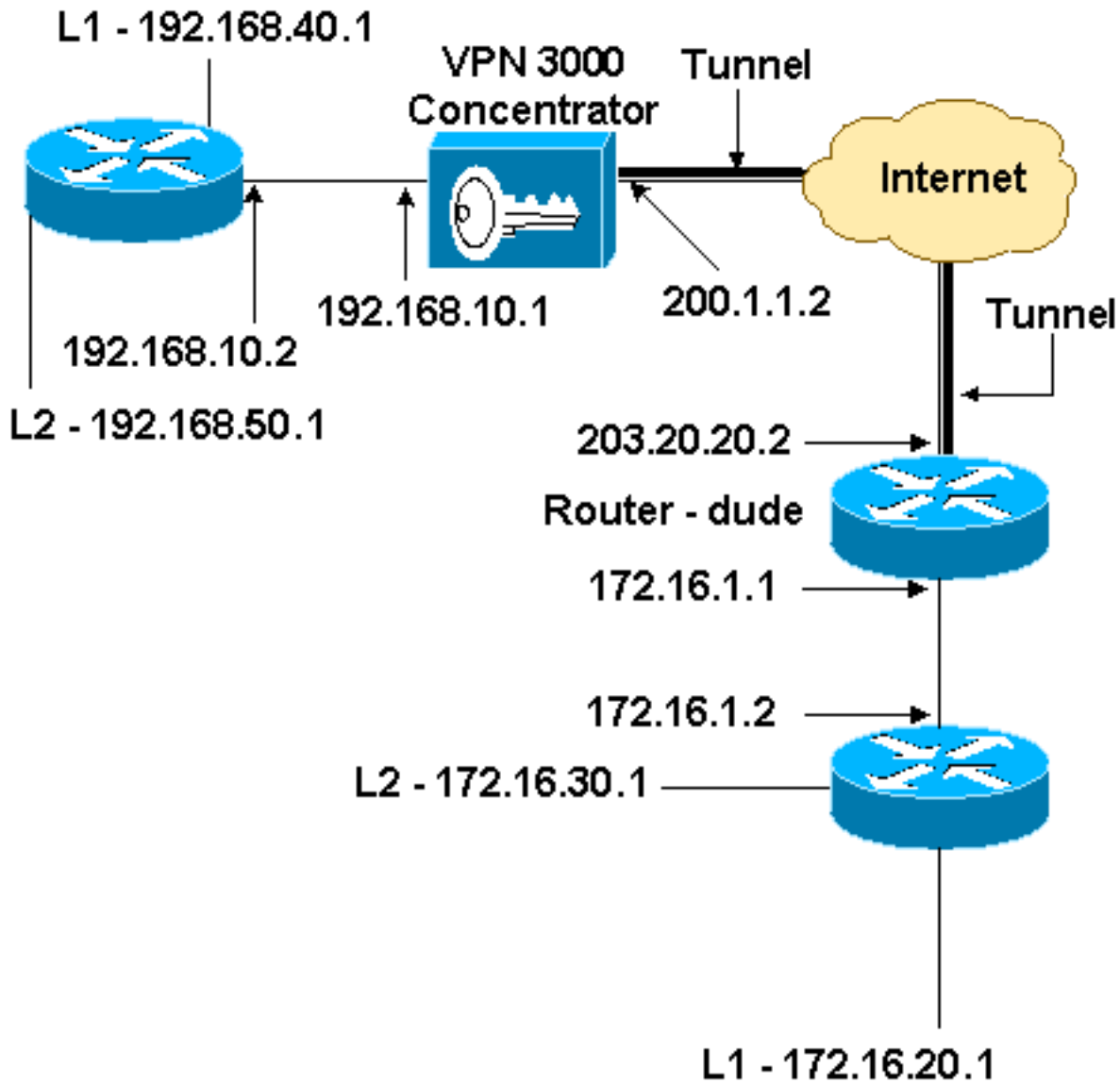
[Configureren](#)

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

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

[Netwerkdigram](#)

Het netwerk in dit document is als volgt opgebouwd.



Configuratie

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.

Configuration | Interfaces Thursday, 03 July 2003 14:04:38
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

• [Power Supplies](#)

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.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

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

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: n.n.n.n/n.n.n.n (e.g. 10.10.0.0/0.0.255.255).
- **Note:** Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Dit zijn de verafgelegen netwerken:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

Apply Cancel Generate Local List

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.

Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default) vpn_local_subnet router_subnet	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

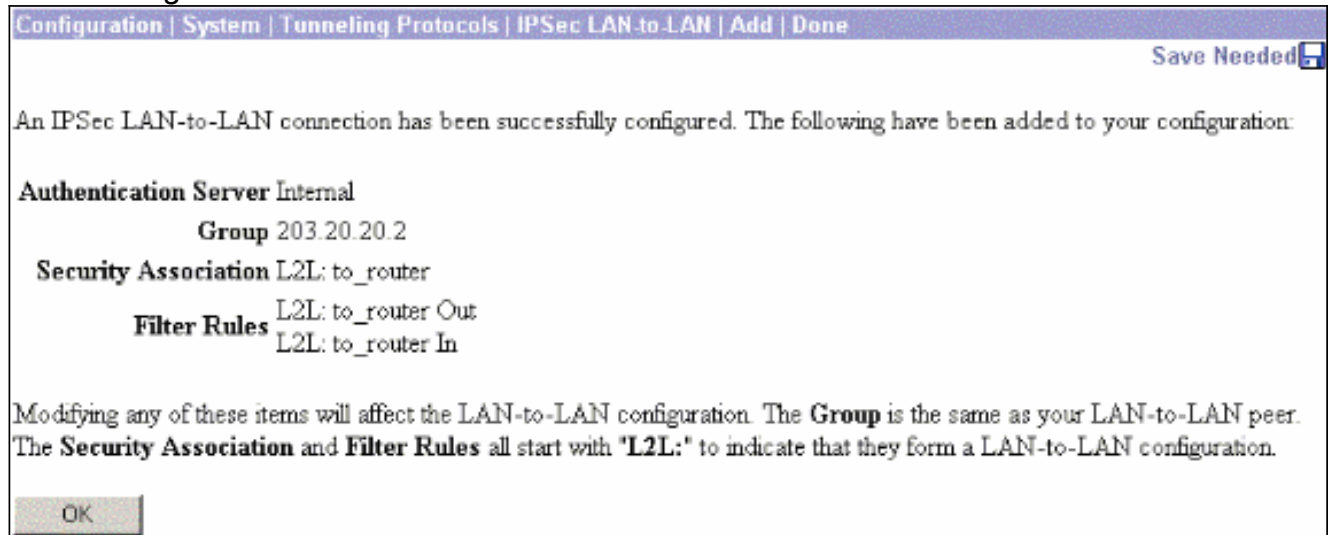
5. Kies Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN en definieer de LAN-to-LAN tunnel.

Add a new IPSec LAN-to-LAN connection.

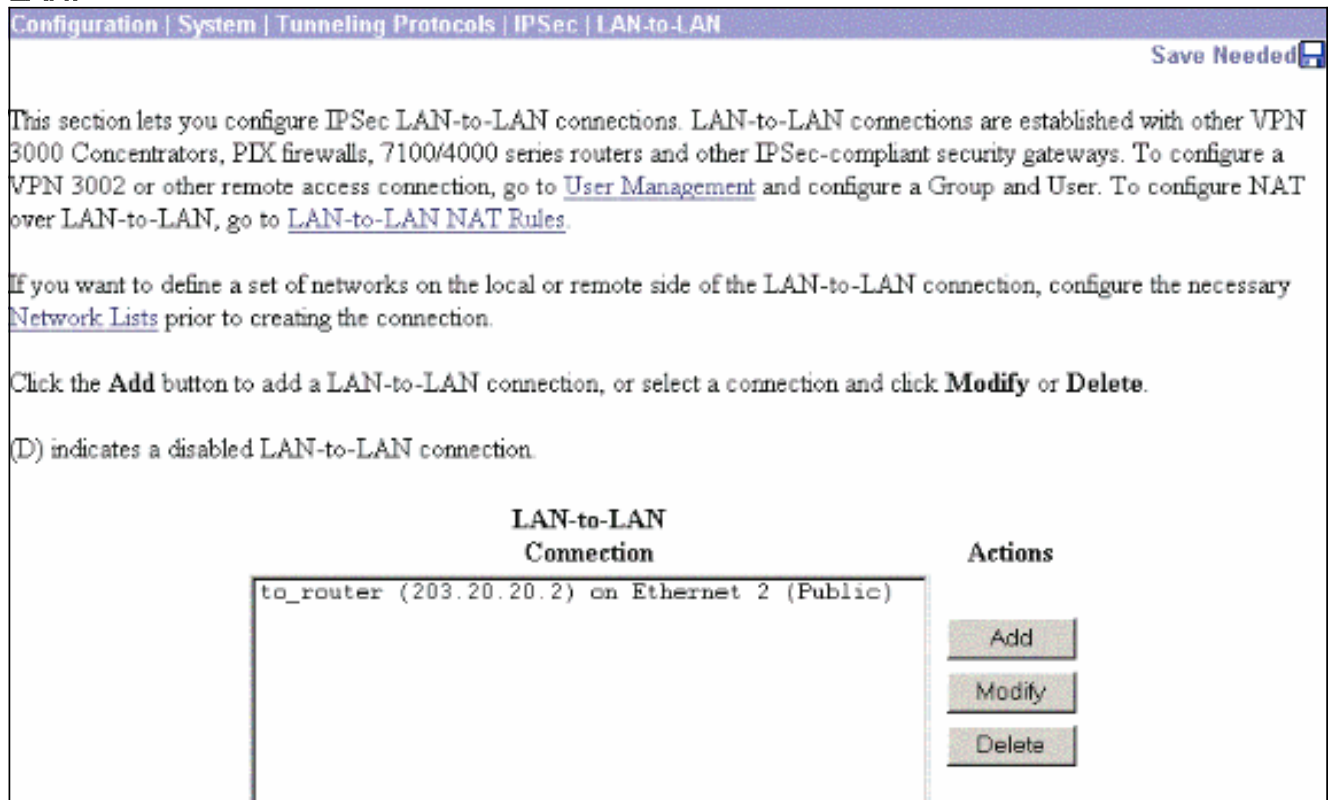
<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> <p>203.20.20.2</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p>
<p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="None"/></p>	<p>Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="vpn_local_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="router_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

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.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5	<< Activate	IKE-3DES-SHA-DSA
IKE-3DES-MD5	Deactivate >>	IKE-3DES-MD5-RSA-DH1
IKE-3DES-MD5-DH1	Move Up	IKE-DES-MD5-DH7
IKE-DES-MD5	Move Down	CiscoVPNClient-3DES-MD5-RSA
IKE-3DES-MD5-DH7	Add	CiscoVPNClient-3DES-SHA-DSA
IKE-3DES-MD5-RSA	Modify	CiscoVPNClient-3DES-MD5-RSA-DH5
CiscoVPNClient-3DES-MD5-DH5	Copy	CiscoVPNClient-3DES-SHA-DSA-DH5
CiscoVPNClient-AES128-SHA	Delete	CiscoVPNClient-AES256-SHA
IKE-AES128-SHA		IKE-AES256-SHA

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

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs	Actions
ESP-3DES-MD5	Add Modify Delete
ESP-3DES-MD5-DH5	
ESP-3DES-MD5-DH7	
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	
L2L: to_router	

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

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	Bidirectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	203.20.20.2	
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

[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](#)