

IPsec-tunnels tussen PIX 7.x en VPN 3000 Concentrator-configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[PIX configureren](#)

[De VPN 3000-concentratie configureren](#)

[Verifiëren](#)

[Controleer de PIX](#)

[Controleer de VPN-concentratie 3000](#)

[Problemen oplossen](#)

[Probleemoplossing voor PIX](#)

[Probleemoplossing voor VPN 3000 Concentrator](#)

[PFS](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document biedt een voorbeeldconfiguratie voor het maken van een LAN-to-LAN IPsec VPN-tunnel tussen een PIX-firewall 7.x en een Cisco VPN 3000 Concentrator.

Raadpleeg [PIX/ASA 7.x Enhanced Spoke-to-Client VPN met het Configuratievoorbeeld van TACACS+ verificatie](#) om meer te weten te komen over het scenario waarin de LAN-to-LAN tunnel tussen de PIX-apparaten ook een VPN-client toestaat om de opgenomen PIX te benaderen via de hub PIX.

Raadpleeg [PIX/ASA 7.x security applicatie voor een IOS Router LAN-to-LAN IPsec Tunnel Configuration Voorbeeld](#) om meer te weten te komen over het scenario waarin de LAN-to-LAN tunnel tussen de PIX/ASA en een IOS-router.

[Voorwaarden](#)

[Vereisten](#)

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

- Dit document vereist een basisbegrip van IPsec-protocol. Raadpleeg [een Inleiding naar IPsec-encryptie](#) voor meer informatie over IPsec.

[Gebruikte componenten](#)

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

- Cisco PIX 500 Series security applicatie met softwareversie 7.1(1)
- Cisco VPN 3060 Concentrator met softwareversie 4.7.2(B)

Opmerking: PIX 506/506E ondersteunt 7.x niet.

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.

Raadpleeg voor de configuratie van PIX 6.x [LAN-to-LAN IPSec-tunnelbanden tussen de Cisco VPN 3000 Concentrator en het configuratievoorbeeld van de PIX-firewall](#).

[Conventies](#)

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

[Configureren](#)

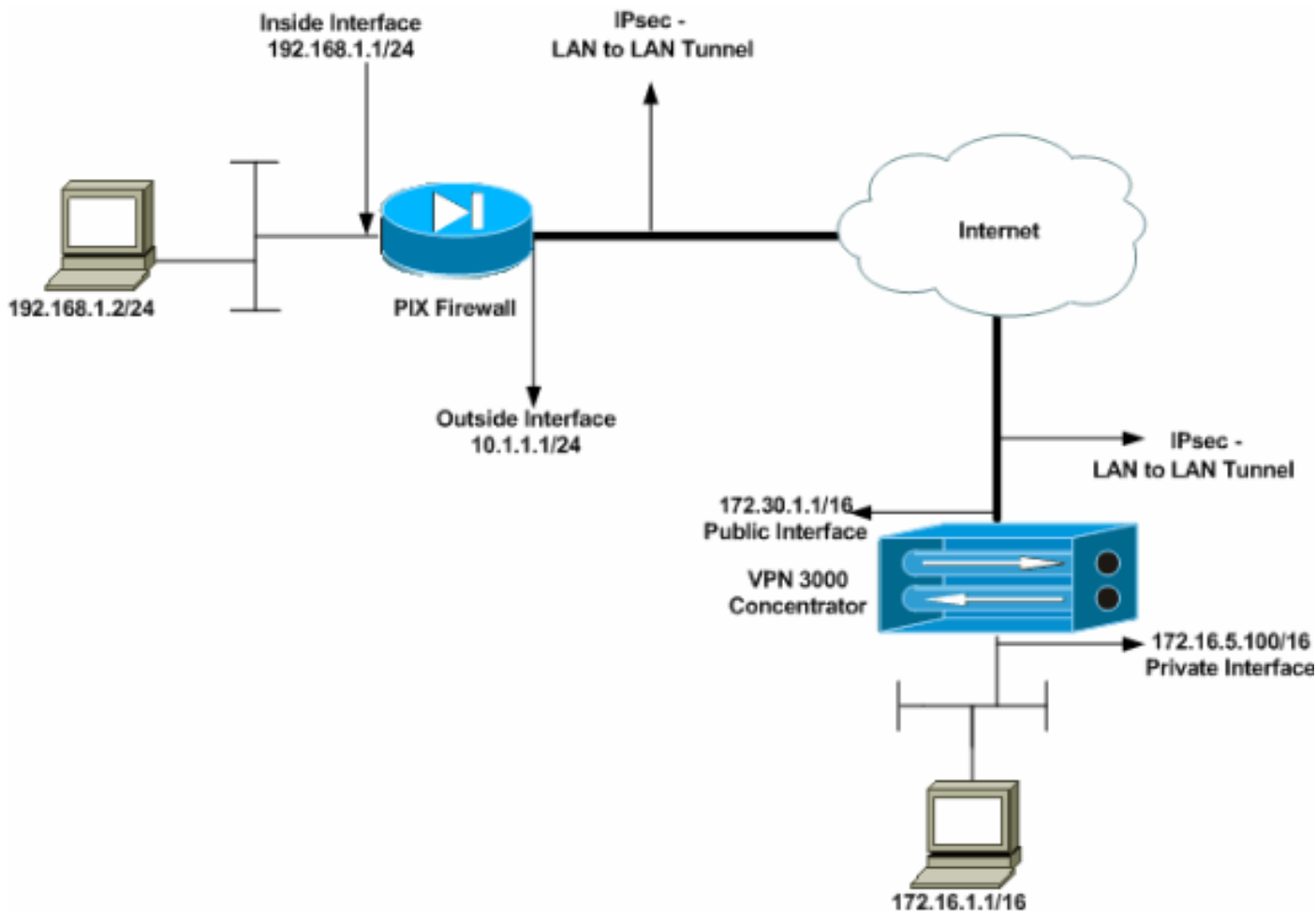
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

- [PIX configureren](#)
- [De VPN 3000-concentratie configureren](#)

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

[Netwerkdigram](#)

Het netwerk in dit document is als volgt opgebouwd:



[PIX configureren](#)

PIX

```

PIX7#show running-config
: Saved
:
PIX Version 7.1(1)
!
hostname PIX7
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside interface of the PIX. !---
By default, the security level for the outside interface
is 0. interface Ethernet0
  nameif outside
  security-level 0
  ip address 10.1.1.1 255.255.255.0
!
!--- Configures the inside interface of the PIX. !--- By
default, the security level for the inside interface is
100. interface Ethernet1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
!--- Defines the IP addresses that should not be NATed.
access-list nonat extended permit ip 192.168.1.0
255.255.255.0 172.16.0.0 255.255.0.0
access-list outside extended permit icmp any any

```

```

!--- Defines the IP addresses that can communicate via
the IPsec tunnel. access-list 101 extended permit ip
192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list OUT extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-504.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list nonat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
!--- Output is suppressed. !--- These are the IPsec
parameters that are negotiated with the client. crypto
ipsec transform-set my-set esp-aes-256 esp-sha-hmac
crypto map mymap 20 match address 101
crypto map mymap 20 set peer 172.30.1.1
crypto map mymap 20 set transform-set my-set
crypto map mymap interface outside
!--- These are the Phase I parameters negotiated by the
two peers. isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- A tunnel group consists of a set of records !---
that contain tunnel connection policies. The two
attributes !--- are General and IPsec. Use the remote
peer IP address as the !--- name of the Tunnel group. In
this example 172.30.1.1 is the peer IP address. !---
Refer to Tunnel Group for more information. tunnel-group
172.30.1.1 type ipsec-l2l
tunnel-group 172.30.1.1 ipsec-attributes
pre-shared-key *
!--- Output is suppressed. ! : end PIX7#

```

[De VPN 3000-concentratie configureren](#)

VPN Concentrators zijn niet voorgeprogrammeerd met IP-adressen in hun fabrieksinstellingen. U moet de console poort 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 u het IP-adres op de Ethernet 1 (privé) interface configureren kunt u de rest configureren met ofwel de CLI ofwel 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** - De juiste tijd en 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 de netwerktopologie 172.16.5.100/16).

De VPN Concentrator is nu toegankelijk via een HTML browser van het binnennetwerk.

Raadpleeg [de Opdracht-Lijn Interface voor Quick Configuration](#) voor informatie over de manier waarop u de VPN Concentrator in CLI-modus kunt configureren.

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.

1. Start de GUI en selecteer **Configuration > Interfaces** om het IP-adres voor de openbare interface en de standaardgateway te configureren.


Configuration | Interfaces Sunday, 19 February 2006 16:54:00
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	172.16.5.100	255.255.0.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	172.30.1.1	255.255.0.0	00.03.A0.89.BF.D1	172.30.1.2
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. Selecteer **Configuratie > Beleidsbeheer > Verkeersbeheer > Netwerklijsten > Toevoegen of wijzigen** om de netwerklijsten te maken die het te versleutelen verkeer definiëren. Voeg hier zowel de lokale als de externe netwerken toe. De IP-adressen moeten die in de toeganglijst spiegelen die in de afstandsbediening zijn geconfigureerd. In dit voorbeeld zijn de twee netwerklijsten **Remote_network** en **VPN Client Local LAN**.

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

192.168.1.0/0.0.0.255

- 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.

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

172.16.0.0/0.0.255.255

- 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.

3. Selecteer **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add** om de IPSec LAN-to-LAN tunnel te configureren. Klik op **Toepassen** wanneer u klaar bent. Voer het IP-adres van de peer in, de netwerklijsten die in stap 2 zijn gemaakt, de parameters IPsec en ISAKMP en de vooraf gedeelde toets. In dit voorbeeld is het peer IP-adres **10.1.1**, de netwerklijsten zijn **Remote_network** en **VPN Client Local LAN** en **cisco** is de pre-gedeelde sleutel.

Modify an IPSec LAN-to-LAN connection.

Enable <input checked="" type="checkbox"/>	Check to enable this LAN-to-LAN connection.
Name <input type="text" value="Test"/>	Enter the name for this LAN-to-LAN connection.
Interface <input type="text" value="Ethernet 2 (Public) (172.30.1.1)"/>	Select the interface for this LAN-to-LAN connection.
Connection Type <input type="text" value="Bi-directional"/>	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.
Peers <input type="text" value="10.1.1.1"/>	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.
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.
Preshared Key <input type="text" value="cisco"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication <input type="text" value="ESP/SHA/HMAC-160"/>	Specify the packet authentication mechanism to use.
Encryption <input type="text" value="AES-256"/>	Specify the encryption mechanism to use.
IKE Proposal <input type="text" value="IKE-AES256-SHA"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T <input type="checkbox"/>	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.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List <input type="text" value="VPN Client Local LAN (Default)"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> 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.
Wildcard Mask <input type="text"/>	

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List <input type="text" value="remote_network"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> 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.
Wildcard Mask <input type="text"/>	

- Selecteer **Configuratie > Gebruikersbeheer > Groepen > Wijzigen 10.1.1.1** om de automatisch gegenereerde groepsinformatie te bekijken. **Opmerking:** wijzig deze groepsinstellingen niet.

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	10.1.1.1	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Apply Cancel

Verifiëren

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

- [Controleer de PIX](#)
- [Controleer de VPN-concentratie 3000](#)

Controleer de PIX

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

- [toon isakmp sa](#)-displays alle huidige IKE security associaties (SA's) bij een peer. De status MM_ACTIVE betekent dat de hoofdmodus wordt gebruikt om de IPsec VPN-tunnel in te stellen. In dit voorbeeld initieert de PIX-firewall de IPsec-verbinding. Het peer IP-adres is 172.30.1.1 en gebruikt hoofdmodus om de verbinding tot stand te brengen.

```
PIX7#show 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: 172.30.1.1
   Type    : L2L                Role    : initiator
   Rekey   : no                State   : MM_ACTIVE
```

- [Laat ipsec sa](#)-displays de instellingen die worden gebruikt door de huidige SA's. 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.

```
PIX7#show ipsec sa
```

```
interface: outside
Crypto map tag: mymap, seq num: 20, local addr: 10.1.1.1

access-list 101 permit ip 192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
```


current_peer: 172.30.1.1

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
```

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 172.30.1.1

```
path mtu 1500, ipsec overhead 76, media mtu 1500
current outbound spi: 136580F6
```

inbound esp sas:

```
spi: 0xF24F4675 (4065281653)
transform: esp-aes-256 esp-sha-hmac
in use settings ={L2L, Tunnel,}
slot: 0, conn_id: 1, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (3824999/28747)
IV size: 16 bytes
replay detection support: Y
```

outbound esp sas:

```
spi: 0x136580F6 (325419254)
transform: esp-aes-256 esp-sha-hmac
in use settings ={L2L, Tunnel,}
slot: 0, conn_id: 1, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (3824999/28745)
IV size: 16 bytes
replay detection support: Y
```

Gebruik de [opdrachten ipsec](#) en [isakmp als](#) resuset om de tunnel te resetten.

[Controleer de VPN-concentratie 3000](#)

Selecteer **Controle > Statistieken > IPsec** om te controleren of de tunnel in de VPN 3000 Concentrator is gegroeid. Dit bevat de statistieken voor zowel IKE als IPsec-parameters.

IKE (Phase 1) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	5720
Sent Bytes	5576
Received Packets	57
Sent Packets	56
Received Packets Dropped	0
Sent Packets Dropped	0
Received Notifies	52
Sent Notifies	104
Received Phase-2 Exchanges	1
Sent Phase-2 Exchanges	0
Invalid Phase-2 Exchanges Received	0
Invalid Phase-2 Exchanges Sent	0
Rejected Received Phase-2 Exchanges	0
Rejected Sent Phase-2 Exchanges	0
Phase-2 SA Delete Requests Received	0
Phase-2 SA Delete Requests Sent	0
Initiated Tunnels	0
Failed Initiated Tunnels	0
Failed Remote Tunnels	0
Authentication Failures	0
Decryption Failures	0
Hash Validation Failures	0
System Capability Failures	0
No-SA Failures	0

IPSec (Phase 2) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	448
Sent Bytes	448
Received Packets	4
Sent Packets	4
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	4
Failed Inbound Authentications	0
Outbound Authentications	4
Failed Outbound Authentications	0
Decryptions	4
Failed Decryptions	0
Encryptions	4
Failed Encryptions	0
System Capability Failures	0
No-SA Failures	0
Protocol Use Failures	0

U kunt de sessie actief controleren bij **Bewaking > Sessies**. U kunt de IPsec-tunnel hier opnieuw instellen.

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group

Session Summary

Active LAN-to-LAN Sessions since Stats Reset	Active Remote Access Sessions since Stats Reset	Active Management Sessions since Stats Reset	Total Active Sessions since Stats Reset	Peak Concurrent Sessions since Stats Reset	Weighted Active Load since Stats Reset	Percent Session Load since Stats Reset	Concurrent Sessions Limit	Total Cumulative Sessions since Stats Reset
1	0	0	1	0	1	1.00%	100	2

NAC Session Summary

Accepted since Stats Reset		Rejected since Stats Reset		Exempted since Stats Reset		Non-responsive since Stats Reset		Hold-off since Stats Reset		N/A since Stats Reset	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	0	0

LAN-to-LAN Sessions

[[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Test	10.1.1.1	IPSec/LAN-to-LAN	AES-256	Feb 19 17:02:01	0:06:02	448	448

Remote Access Sessions

[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
No Remote Access Sessions							

Management Sessions

[[LAN-to-LAN Sessions](#) | [Remote Access Sessions](#)]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	172.16.1.1	HTTP	3DES-168 SSLv3	Jan 01 05:45:00	0:11:30

Problemen oplossen

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

- [Probleemoplossing voor PIX](#)
- [Probleemoplossing voor VPN 3000 Concentrator](#)
- [PFS](#)

Probleemoplossing voor PIX

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.

De **debug** opdrachten in PIX voor VPN-tunnels zijn:

- [debug crypto isakmp](#)—Debugs ISAKMP SA onderhandelingen.
- [debug van crypto ipsec](#) — Debugs IPsec SA onderhandelingen.

[Probleemoplossing voor VPN 3000 Concentrator](#)

Overeenkomstig met debug-opdrachten op de Cisco-routers kunt u Event Classes configureren om alle alarmen weer te geven. Selecteer **Configuration > System > Events > Classes > Add** om de vastlegging van Event Classes in te schakelen.

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

Select Filter Options

Event Class	<input type="text" value="All Classes"/>	Severities	<input type="text" value="ALL"/>
	<input type="text" value="AUTH"/>		<input type="text" value="1"/>
	<input type="text" value="AUTHDBG"/>		<input type="text" value="2"/>
	<input type="text" value="AUTHDECODE"/>		<input type="text" value="3"/>
Client IP Address	<input type="text" value="0.0.0.0"/>	Events/Page	<input type="text" value="100"/>
Group	<input type="text" value="-All-"/>	Direction	<input type="text" value="Oldest to Newest"/>

```

1 02/19/2006 17:17:00.080 SEV-5 IKEDBG/64 RPT-33 10.1.1.1
IKE Peer included IKE fragmentation capability flags:
Main Mode:      True
Aggressive Mode: True

3 02/19/2006 17:17:00.750 SEV-4 IKE/119 RPT-23 10.1.1.1
Group [10.1.1.1]
PHASE 1 COMPLETED

4 02/19/2006 17:17:00.750 SEV-4 AUTH/22 RPT-23 10.1.1.1
User [10.1.1.1] Group [10.1.1.1] connected, Session Type: IPSec/LAN-to-LAN

5 02/19/2006 17:17:00.750 SEV-4 AUTH/84 RPT-23
LAN-to-LAN tunnel to headend device 10.1.1.1 connected

6 02/19/2006 17:17:01.020 SEV-5 IKE/35 RPT-23 10.1.1.1
Group [10.1.1.1]
Received remote IP Proxy Subnet data in ID Payload:
  Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

9 02/19/2006 17:17:01.020 SEV-5 IKE/34 RPT-23 10.1.1.1
Group [10.1.1.1]
Received local IP Proxy Subnet data in ID Payload:
  Address 172.16.0.0, Mask 255.255.0.0, Protocol 0, Port 0

12 02/19/2006 17:17:01.020 SEV-5 IKE/66 RPT-13 10.1.1.1
Group [10.1.1.1]
IKE Remote Peer configured for SA: L2L: Test

13 02/19/2006 17:17:01.350 SEV-4 IKE/49 RPT-3 10.1.1.1
Group [10.1.1.1]
Security negotiation complete for LAN-to-LAN Group (10.1.1.1)
Responder, Inbound SPI = 0x136580f6, Outbound SPI = 0xf24f4675

16 02/19/2006 17:17:01.350 SEV-4 IKE/120 RPT-3 10.1.1.1
Group [10.1.1.1]
PHASE 2 COMPLETED (msgid=6b2795cd)

```

[PFS](#)

Bij IPsec-onderhandelingen zorgt Perfect Forward SecRITY (PFS) ervoor dat elke nieuwe

cryptografische toets geen verband houdt met een eerdere toets. Schakel PFS op beide tunnelpeers in of uit, anders wordt de LAN-to-LAN (L2L) IPsec-tunnel niet in de PIX/ASA.

PFS wordt standaard uitgeschakeld. Om PFS toe te laten gebruik de opdracht **pfs** met het toelaten sleutelwoord in **groep-beleid configuratiewijze**. Om PFS uit te schakelen, voer het *in*.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Om de PFS eigenschap uit de actieve configuratie te verwijderen, dient u de **geen** vorm van deze opdracht in te voeren. Een groepsbeleid kan een waarde voor PFS van een ander groepsbeleid erven. Typ **geen** formulier van deze opdracht om te voorkomen dat een waarde wordt geërfd.

```
hostname(config-group-policy)#no pfs
```

[Gerelateerde informatie](#)

- [Cisco PIX 500 Series security applicaties - ondersteuningspagina](#)
- [Cisco VPN 3000 Series Concentrator - ondersteuningspagina](#)
- [Cisco PIX 500 Series security applicatie, referentie voor opdracht](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)