

# Konfigurationsbeispiel für einen IPsec-Tunnel zwischen PIX 7.x und VPN 3000 Concentrator

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurieren des PIX](#)

[Konfigurieren des VPN 3000-Konzentrators](#)

[Überprüfen](#)

[PIX überprüfen](#)

[Überprüfen des VPN 3000-Konzentrators](#)

[Fehlerbehebung](#)

[Fehlerbehebung für PIX](#)

[Fehlerbehebung beim VPN 300 Concentrator](#)

[PFS](#)

[Zugehörige Informationen](#)

## [Einführung](#)

Dieses Dokument enthält eine Beispielkonfiguration zum Einrichten eines LAN-to-LAN IPsec-VPN-Tunnels zwischen einer PIX Firewall 7.x und einem Cisco VPN 3000-Konzentrator.

Unter [Konfigurationsbeispiel für PIX/ASA 7.x Enhanced Spoke-to-Client VPN mit TACACS+-Authentifizierung](#) erfahren Sie mehr über das Szenario, in dem der LAN-zu-LAN-Tunnel zwischen den PIXs auch einem VPN-Client den Zugriff auf die Spoke-PIX über den Hub-PIX ermöglicht.

Weitere Informationen zum Szenario, in dem der LAN-zu-LAN-Tunnel zwischen PIX/ASA 7.x-[Sicherheits-Appliance](#) zwischen [einem IOS-Router und einem LAN-zu-LAN-IPsec-Tunnel](#) zwischen dem PIX/ASA-Router und einem IOS-Router verläuft, finden Sie im [Konfigurationsbeispiel](#) für die [PIX/ASA 7.x Security Appliance](#).

## [Voraussetzungen](#)

### [Anforderungen](#)

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese

Konfiguration durchzuführen:

- Dieses Dokument erfordert ein grundlegendes Verständnis des IPsec-Protokolls. Weitere Informationen zu IPsec finden Sie unter [Einführung in die IPsec-Verschlüsselung](#).

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Security Appliance der Serie PIX 500 mit Softwareversion 7.1(1)
- Cisco VPN 3060 Concentrator mit Softwareversion 4.7.2(B)

**Hinweis:** PIX 506/506E unterstützt 7.x nicht.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Informationen zur Konfiguration von PIX 6.x finden Sie unter [Konfigurationsbeispiel](#) für den [LAN-to-LAN IPSec-Tunnel zwischen dem Cisco VPN 3000 Concentrator und der PIX-Firewall](#).

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## Konfigurieren

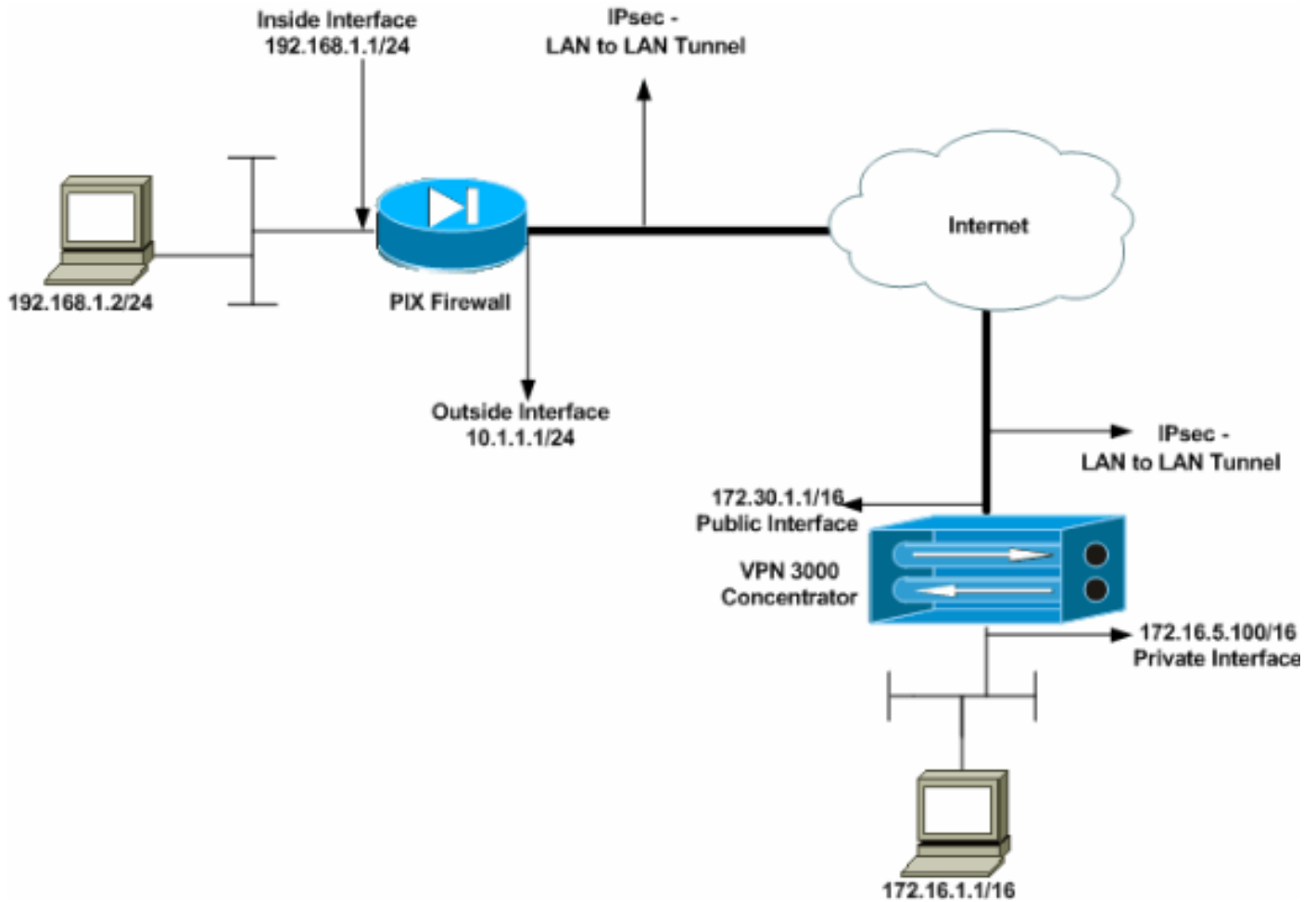
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

- [Konfigurieren des PIX](#)
- [Konfigurieren des VPN 3000-Konzentrators](#)

**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Konfigurieren des PIX

### 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#

```

## Konfigurieren des VPN 3000-Konzentrators

VPN Concentrators sind in den Werkseinstellungen nicht vorprogrammiert und verfügen nicht über IP-Adressen. Sie müssen den Konsolenport verwenden, um die Erstkonfigurationen als menübasierte Befehlszeilenschnittstelle (CLI) zu konfigurieren. Informationen zur Konfiguration über die Konsole finden Sie unter [Konfigurieren von VPN-Concentrators](#) über die [Konsole](#).

Nachdem Sie die IP-Adresse auf der (privaten) Ethernet-1-Schnittstelle konfiguriert haben, können Sie den Rest entweder über die CLI oder über die Browser-Schnittstelle konfigurieren. Die Browserschnittstelle unterstützt sowohl HTTP als auch HTTP über Secure Socket Layer (SSL).

Diese Parameter werden über die Konsole konfiguriert:

- **Uhrzeit/Datum:** Die korrekte Uhrzeit und das richtige Datum sind sehr wichtig. Sie stellen sicher, dass Protokollierungs- und Abrechnungseinträge korrekt sind und dass das System ein gültiges Sicherheitszertifikat erstellen kann.
- **Ethernet 1 (private) Schnittstelle** - Die IP-Adresse und -Maske (aus der Netzwerktopologie 172.16.5.100/16).

Der Zugriff auf den VPN Concentrator erfolgt nun über einen HTML-Browser aus dem internen

Netzwerk. Weitere Informationen zur Konfiguration des VPN-Concentrators im CLI-Modus finden Sie unter [Verwenden der Kommandozeilenschnittstelle für die schnelle Konfiguration](#).

Geben Sie die IP-Adresse der privaten Schnittstelle im Webbrowser ein, um die GUI-Schnittstelle zu aktivieren.

Klicken Sie auf das Symbol **zum Speichern der Änderungen** im Speicher. Der werksseitig voreingestellte Benutzername und das werkseitige Kennwort sind **admin**, wobei die Groß- und Kleinschreibung zu beachten ist.

1. Starten Sie die Benutzeroberfläche, und wählen Sie **Configuration > Interfaces (Konfiguration > Schnittstellen)** aus, um die IP-Adresse für die öffentliche Schnittstelle und das Standard-Gateway zu konfigurieren.


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
<a href="#">Ethernet 1 (Private)</a>	UP	172.16.5.100	255.255.0.0	00.03.A0.89.BF.D0	
<a href="#">Ethernet 2 (Public)</a>	UP	172.30.1.1	255.255.0.0	00.03.A0.89.BF.D1	172.30.1.2
<a href="#">Ethernet 3 (External)</a>	Not Configured	0.0.0.0	0.0.0.0		
<a href="#">DNS Server(s)</a>	DNS Server Not Configured				
<a href="#">DNS Domain Name</a>					

- [Power Supplies](#)



2. Wählen Sie **Configuration > Policy Management > Traffic Management > Network Lists > Add or Modify (Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Netzwerklisten > Hinzufügen oder Ändern)**, um die Netzwerklisten zu erstellen, die den zu verschlüsselnden Datenverkehr definieren. Fügen Sie hier sowohl das lokale als auch das Remote-Netzwerk hinzu. Die IP-Adressen sollten denen in der Zugriffsliste entsprechen, die auf dem Remote-PIX konfiguriert wurde. In diesem Beispiel sind die beiden Netzwerklisten **remote\_network** und **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**

- 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**

- 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. Wählen Sie **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add** aus, um den IPsec LAN-to-LAN-Tunnel zu konfigurieren. Klicken Sie abschließend auf **Apply**. Geben Sie die Peer-IP-Adresse, die in Schritt 2 erstellten Netzwerklisten, die IPsec- und ISAKMP-Parameter und den vorinstallierten Schlüssel ein. In diesem Beispiel ist die Peer-IP-Adresse **10.1.1.1**, die Netzwerklisten sind **remote\_network** und **VPN Client Local LAN**, und **Cisco** ist der vorinstallierte Schlüssel.

Modify an IPSec LAN-to-LAN connection.

<b>Enable</b> <input checked="" type="checkbox"/>	Check to enable this LAN-to-LAN connection.
<b>Name</b> <input type="text" value="Test"/>	Enter the name for this LAN-to-LAN connection.
<b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.30.1.1)"/>	Select the interface for this LAN-to-LAN connection.
<b>Connection Type</b> <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.
<b>Peers</b> <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.
<b>Digital Certificate</b> <input type="text" value="None (Use Preshared Keys)"/>	Select the digital certificate to use.
<b>Certificate Transmission</b> <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
<b>Preshared Key</b> <input type="text" value="cisco"/>	Enter the preshared key for this LAN-to-LAN connection.
<b>Authentication</b> <input type="text" value="ESP/SHA/HMAC-160"/>	Specify the packet authentication mechanism to use.
<b>Encryption</b> <input type="text" value="AES-256"/>	Specify the encryption mechanism to use.
<b>IKE Proposal</b> <input type="text" value="IKE-AES256-SHA"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
<b>Filter</b> <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
<b>IPSec NAT-T</b> <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.
<b>Bandwidth Policy</b> <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
<b>Routing</b> <input type="text" value="None"/>	Choose the routing mechanism to use. <b>Parameters below are ignored if Network Autodiscovery is chosen.</b>

---

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

<b>Network List</b> <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.
<b>IP Address</b> <input type="text"/>	<b>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.</b>
<b>Wildcard Mask</b> <input type="text"/>	

---

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

<b>Network List</b> <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.
<b>IP Address</b> <input type="text"/>	<b>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.</b>
<b>Wildcard Mask</b> <input type="text"/>	

- Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen > Ändern** Sie 10.1.1.1, um die automatisch generierten Gruppeninformationen anzuzeigen. **Hinweis:** Ändern Sie diese Gruppeneinstellungen nicht.



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

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- [PIX überprüfen](#)
- [Überprüfen des VPN 3000-Konzentrators](#)

## PIX überprüfen

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show anzuzeigen**.

- **show isakmp sa**: Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an. Der Status MM\_ACTIVE gibt an, dass der Hauptmodus zum Einrichten des IPsec-VPN-Tunnels verwendet wird. In diesem Beispiel initiiert die PIX-Firewall die IPsec-Verbindung. Die Peer-IP-Adresse ist 172.30.1.1 und verwendet den Hauptmodus, um die Verbindung herzustellen.

```
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
```

- **show ipsec sa**: Zeigt die von aktuellen SAs verwendeten Einstellungen an. Prüfen Sie, ob die Peer-IP-Adressen, die Netzwerke, auf die sowohl die lokalen als auch die Remote-Endgeräte zugreifen können, und das verwendete Transformationssatz verwendet werden. Es gibt zwei ESP-SAs, eine in jede Richtung.

```
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
```

Verwenden Sie die Befehle [clear ipsec sa](#) und [clear isakmp sa](#), um den Tunnel zurückzusetzen.

## [Überprüfen des VPN 3000-Konzentrators](#)

Wählen Sie **Monitoring > Statistics > IPsec** aus, um zu überprüfen, ob der Tunnel im VPN 3000 Concentrator verfügbar ist. Diese enthält die Statistiken für IKE- und IPsec-Parameter.

## 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

Sie können die Sitzung aktiv unter **Überwachung > Sitzungen** überwachen. Sie können den IPsec-Tunnel hier zurücksetzen.

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
<a href="#">Test</a>	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](#) ]

<a href="#">Username</a>	<a href="#">Assigned IP Address</a> <a href="#">Public IP Address</a>	<a href="#">Group</a>	<a href="#">Protocol</a> <a href="#">Encryption</a>	<a href="#">Login Time</a> <a href="#">Duration</a>	<a href="#">Client Type</a> <a href="#">Version</a>	<a href="#">Bytes Tx</a> <a href="#">Bytes Rx</a>	<a href="#">NAC Result</a> <a href="#">Posture Token</a>
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

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- [Fehlerbehebung für PIX](#)
- [Fehlerbehebung beim VPN 300 Concentrator](#)
- [PFS](#)

## Fehlerbehebung für PIX

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe** des Befehls **show** anzuzeigen.

**Hinweis:** Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

Die **Debug**-Befehle für PIX für VPN-Tunnel sind:

- [debug crypto isakmp](#) - Debuggt ISAKMP SA-Verhandlungen.
- [debug crypto ipsec](#) - Debuggt IPsec SA-Verhandlungen.

### Fehlerbehebung beim VPN 300 Concentrator

Ähnlich wie die Debugbefehle auf den Cisco Routern können Sie Ereignisklassen so konfigurieren, dass alle Alarme angezeigt werden. Wählen Sie **Configuration > System > Events > Classes > Add** aus, um die Protokollierung von Ereignisklassen zu aktivieren.

Wählen Sie **Monitoring > Filterable Event Log (Überwachung > Filterbares Ereignisprotokoll)**, um die aktivierten Ereignisse zu überwachen.

## 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](#)

Bei IPsec-Verhandlungen stellt Perfect Forward Secrecy (PFS) sicher, dass jeder neue

kryptografische Schlüssel nicht mit einem vorherigen Schlüssel in Beziehung steht. Aktivieren oder deaktivieren Sie PFS auf beiden Tunnel-Peers, andernfalls wird der LAN-to-LAN (L2L)-IPsec-Tunnel nicht in PIX/ASA eingerichtet.

PFS ist standardmäßig deaktiviert. Um PFS zu aktivieren, verwenden Sie den Befehl **pfs** mit dem **Schlüsselwort *enable*** im Gruppenrichtlinienkonfigurationsmodus. Um PFS zu deaktivieren, geben Sie das *disable*-Schlüsselwort ein.

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

Um das PFS-Attribut aus der aktuellen Konfiguration zu entfernen, geben Sie die **no**-Form dieses Befehls ein. Eine Gruppenrichtlinie kann einen Wert für PFS von einer anderen Gruppenrichtlinie erben. Geben Sie die **no**-Form dieses Befehls ein, um zu verhindern, dass ein Wert geerbt wird.

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

## Zugehörige Informationen

- [Cisco PIX Security Appliances der Serie 500 - Support-Seite](#)
- [Cisco VPN Concentrator der Serie 3000 - Support-Seite](#)
- [Cisco PIX Security Appliance der Serie 500 - Befehlsreferenz](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)