

# PIX 7.x および VPN 3000 コンセントレータ間の IPsec トンネルの設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[PIX の設定](#)

[VPN 3000 コンセントレータの設定](#)

[確認](#)

[PIX の確認](#)

[VPN 3000 コンセントレータの確認](#)

[トラブルシューティング](#)

[PIX のトラブルシューティング](#)

[VPN 3000 コンセントレータのトラブルシューティング](#)

[PFS](#)

[関連情報](#)

## 概要

このドキュメントでは、PIX ファイアウォール 7.x と Cisco VPN 3000 コンセントレータ間に LAN-to-LAN IPsec VPN トンネルを確立する方法について、設定例を示して説明します。

複数の PIX 間の LAN-to-LAN トンネルが、VPN クライアントがハブ PIX を介してスポーク PIX にアクセスすることを許可するシナリオの詳細については、『[TACACS+ 認証を使用した PIX/ASA 7.x 拡張 Spoke-to-Client VPN の設定例](#)』を参照してください。

PIX/ASA と IOS ルータ間に LAN-to-LAN トンネルを確立するシナリオの詳細は、『[IOS ルータの LAN-to-LAN IPsec トンネルに対する PIX/ASA 7.x セキュリティ アプライアンスの設定例](#)』を参照してください。

## 前提条件

### 要件

この設定を行う前に、次の要件が満たされていることを確認します。

- このドキュメントは、IPSec プロトコルに関する基本的知識を前提とします。IPsec に関する知識を深めるには、『[IP Security \(IPSec\) 暗号化の概要](#)』を参照してください。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 7.1(1) が稼働している Cisco PIX 500 シリーズ セキュリティ アプリアンス
- ソフトウェア バージョン 4.7.2(B) が稼働している Cisco VPN 3060 コンセントレータ

注：PIX 506/506Eは7.xをサポートしていません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

PIX 6.x を設定するには、『[コンセントレータ、Cisco VPN 3000 コンセントレータ、PIX ファイアウォール間の接続](#)』を参照してください。

## 表記法

ドキュメント表記の詳細については、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## 設定

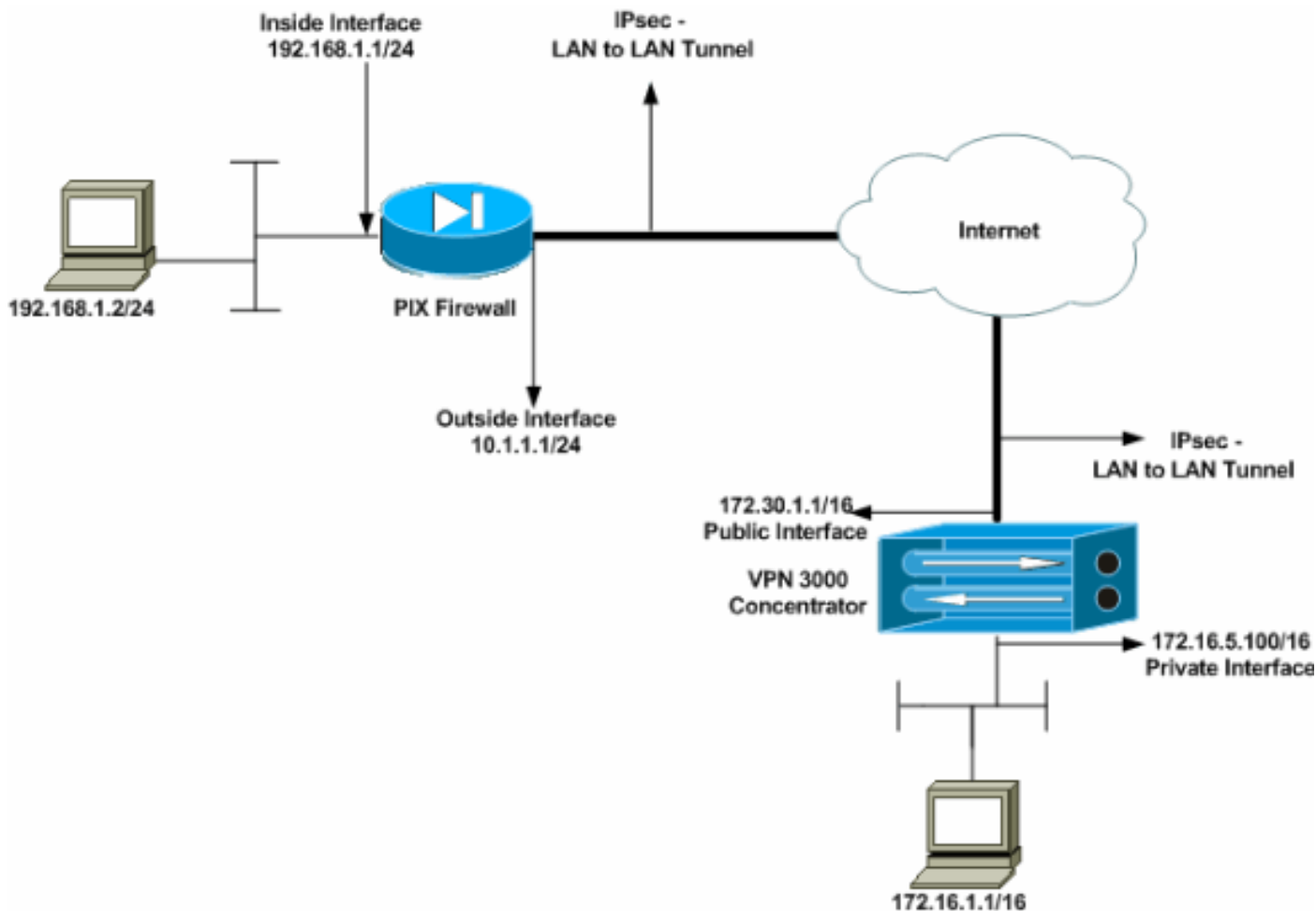
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

- [PIX の設定](#)
- [VPN 3000 コンセントレータの設定](#)

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

## ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



## PIX の設定

### 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#

```

## VPN 3000 コンセントレータの設定

VPN コンセントレータは、工場出荷時に IP アドレスが事前にプログラムされていません。メニューベースのコマンドライン インターフェイス ( CLI ) で初期設定を行うには、コンソールポートを使用する必要があります。コンソール経由で設定を行う方法の詳細は、『[コンソール経由での VPN コンセントレータの設定](#)』を参照してください。

イーサネット 1 ( プライベート ) インターフェイス上の IP アドレスを設定し終わったら、CLI またはブラウザ インターフェイスのいずれかを使用して、残りの項目を設定できます。ブラウザ インターフェイスでは HTTP と HTTP over Secure Socket Layer ( SSL ) の両方がサポートされています。

次のパラメータは、コンソールを使用して設定されます。



- **時間/日付**：時間と日付を正確に設定することはきわめて重要です。これによりロギングとアカウントのエントリが正確になり、システムが有効なセキュリティ認証を作成するのに役立ちます。
- **イーサネット 1 ( プライベート ) インターフェイス**：IP アドレスおよびマスク ( ネットワーク トポロジ 172.16.5.100/16 )。

これで、内部ネットワークから HTML ブラウザを使用して、VPN コネクタにアクセスできるようになります。CLI モードでの VPN コネクタの設定方法の詳細は、『[クイックコンフィギュレーションでのコマンドラインインターフェイスの使用](#)』を参照してください。

GUI インターフェイスをイネーブルにするために、Web ブラウザからプライベート インターフェイスの IP アドレスを入力します。

[save needed] アイコンをクリックして、変更をメモリに保存します。工場出荷時のデフォルトのユーザ名およびパスワードは、**admin** です（大文字と小文字は区別されます）。

1. GUI を起動し、[Configuration] > [Interfaces] を選択して、パブリック インターフェイスおよびデフォルト ゲートウェイの IP アドレスを設定します。

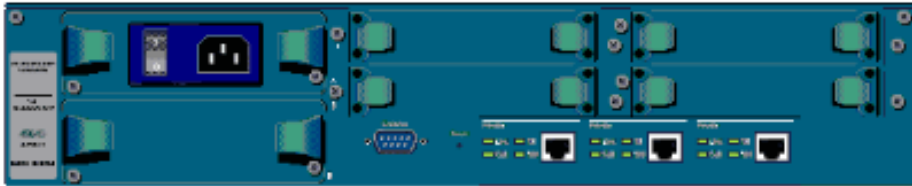
Configuration | Interfaces Sunday, 19 February 2006 16:54:00  
Save Needed  Refresh 

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. [Configuration] > [Policy Management] > Traffic Management] > [Network Lists] > [Add or Modify] を選択して、暗号化されるトラフィックを定義するネットワーク リストを作成します。ローカルとリモートの両方のネットワークをここに追加します。IP アドレスは、リモート PIX に設定されたアクセス リストのアドレスと一致させる必要があります。次の例では、2 つのネットワーク リストは、それぞれ **remote\_network** と **VPN Client Local LAN** です。

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. [Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN] > [Add] を選択して、IPsec LAN-to-LAN トンネルを設定します。終了したら **[Apply]** をクリックします。ピアの IP アドレス、ステップ 2 で作成したネットワーク リスト、IPsec と ISAKMP のパラメータ、および事前共有鍵を入力します。次の例では、ピアの IP アドレスは 10.1.1.1、ネットワーク リストは **remote\_network** と **VPN Client Local LAN**、そして **cisco** が事前共有鍵です。

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"/>	

4. [Configuration] > [User Management] > [Groups] > [Modify 10.1.1.1] を選択して、自動生成されたグループに関する情報を表示します。注：これらのグループ設定は変更しないでください。



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

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

- [PIX の確認](#)
- [VPN 3000 コンセントレータの確認](#)

## PIX の確認

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show isakmp sa** : ピアにおける現在の IKE Security Associations ( SA; セキュリティ アソシエーション ) をすべて表示します。MM\_ACTIVE というステータスは、IPsec VPN トンネルのセットアップにメイン モードが使用されていることを示します。次の例では、PIX ファイアウォールによって IPsec 接続が開始されています。ピアの IP アドレスは 172.30.1.1 であり、メイン モードを使用して接続を確立します。

```
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** : 現在の SA で使用されている設定を表示します。ピア IP アドレス、ローカルとリモートの両端のアクセスが可能なネットワーク、および使用されている変換セットをチェックします。2 つの ESP SA が、各方向に 1 つずつあります。

```
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
```

[clear ipsec sa および clear isakmp sa コマンドを使用して、トンネルをリセットします。](#)

## [VPN 3000 コンセントレータの確認](#)

[Monitoring] > [Statics] > [IPsec] を選択して、VPN 3000 コンセントレータでトンネルがアップ状態になっているかどうかを確認します。IKE パラメータと IPsec パラメータの両方に関する統計情報が表示されます。

## 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

[Monitoring] > [Sessions] では、セッションをアクティブに監視できます。たとえば、ここで IPsec トンネルをリセットできます。

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

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- [PIX のトラブルシューティング](#)
- [VPN 3000 コンセントレータのトラブルシューティング](#)
- [PFS](#)

### PIX のトラブルシューティング

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

次に、PIX で VPN トンネルに使用できる debug コマンドを示します。

- [debug crypto isakmp](#) : ISAKMP SA ネゴシエーションをデバッグします。
- [debug crypto ipsec](#) : IPsec SA ネゴシエーションをデバッグします。

## VPN 3000 コンセントレータのトラブルシューティング

Cisco ルータの debug コマンドと同様に、イベント クラスを設定してすべてのアラームを表示できます。[Configuration] > [System] > [Events] > [Class] > [Add] を選択して、イベント クラスのロギングをオンにします。

[Monitoring] > [Filterable Event Log] を選択して、イネーブルなイベントを監視します。

## 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](#)

IPSec のネゴシエーションでは、Perfect Forward Secrecy ( PFS; 完全転送秘密 ) によって、それ

それぞれの新しい暗号鍵が以前の鍵とは独立したものであることが保証されます。両方のトンネルピアで PFS をイネーブルまたはディセーブルにします。そうでないと、PIX/ASA で LAN-to-LAN ( L2L ) の IPSec トンネルが確立されません。

PFS はデフォルトでディセーブルになっています。PFS をイネーブルにするには、グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して pfs コマンドを使用します。PFS を無効にするには、**disable** キーワードを指定します。

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

実行コンフィギュレーションから PFS アトリビュートを削除するには、このコマンドの no 形式を入力します。グループポリシーでは PFS に関する値を他のグループポリシーから継承できます。値を継承しないようにするには、このコマンドの no 形式を使用します。

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

## [関連情報](#)

- [Cisco PIX 500 シリーズ セキュリティ アプライアンス サポート ページ](#)
- [Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス、コマンド リファレンス](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)