PIX 7.x 和 VPN 3000 集中器之间的 IPSec 隧道配置示例

目录

简介

本文档提供了如何在 PIX 防火墙 7.x 和 Cisco VPN 3000 集中器之间建立 LAN 到 LAN IPSec VPN 隧道的示例配置。

要了解有关 PIX 之间的 LAN 到 LAN 隧道同时允许 VPN Client 通过中央 PIX 访问分支 PIX 的方案的详细信息，请参阅使用 TACACS+ 身份验证增强的 PIX/ASA 7.x 分支到客户端 VPN 配置示例。

要详细了解PIX/ASA和IOS路由器之间的LAN到LAN隧道的场景，请参阅PIX/ASA 7.x安全设备到IOS路由器的LAN到LAN隧道配置示例。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 本文档需要对 IPSec 协议拥有基本的了解。要了解有关 IPsec 的详细信息，请参阅 IPsec 加密简介。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安装有软件版本 7.1(1) 的 Cisco PIX 500 系列安全设备
- 安装有软件版本 4.7.2(B) 的 Cisco VPN 3060 集中器

注意：PIX 506/506E不支持7.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

要配置 PIX 6.x，请参阅在 Cisco VPN 3000 集中器和 PIX 防火墙之间建立 LAN 到 LAN IPSec 隧道的配置示例。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

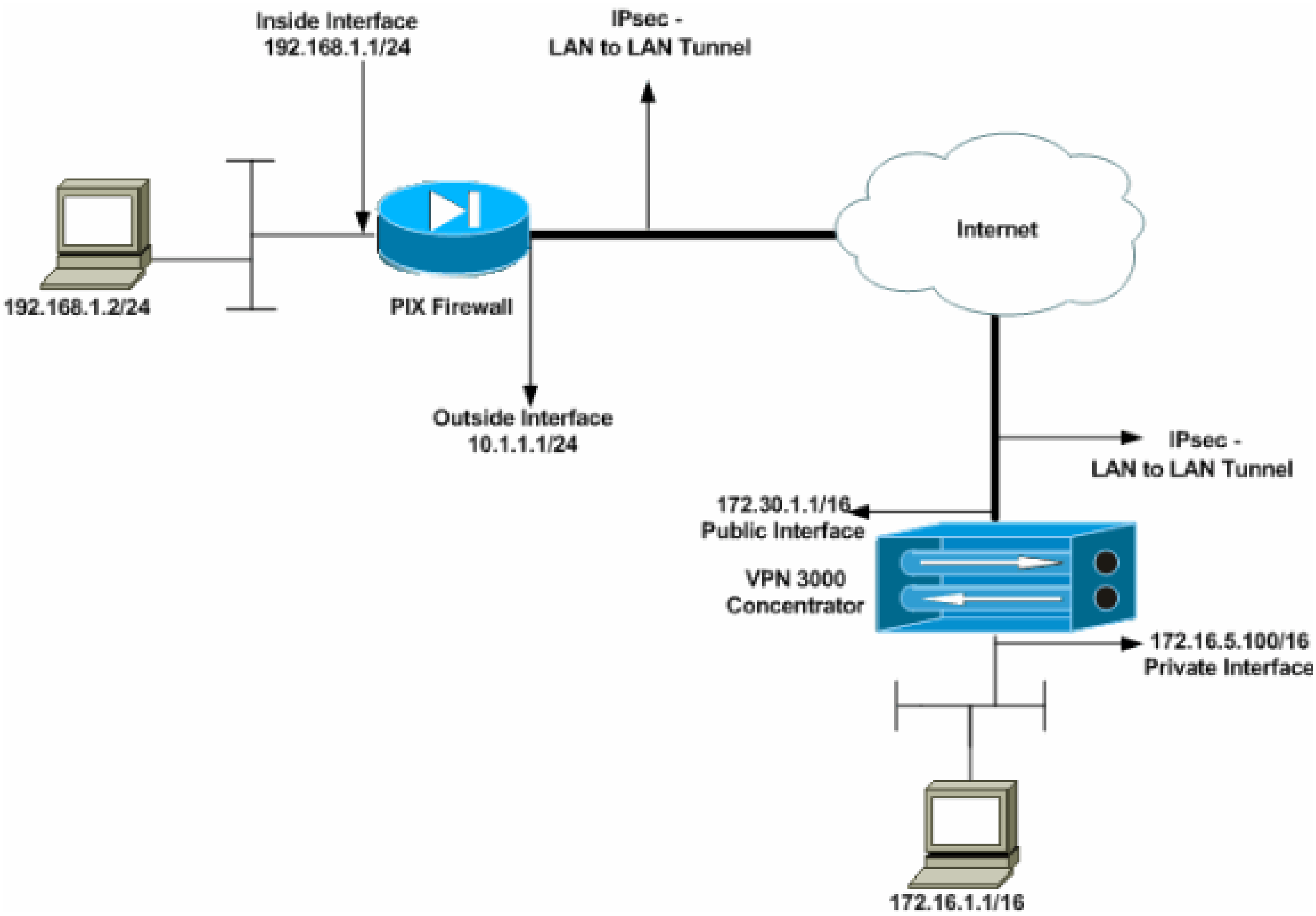
本部分提供有关如何配置本文档所述功能的信息。

- 配置 PIX
- 配置VPN 3000集中器

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置 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#
```

配置VPN 3000集中器

VPN集中器在他们的出厂设置中没有预编程序设置IP地址。必须使用控制台端口配置基于菜单的命令行界面 (CLI) 的初始配置。 有关如何通过控制台进行配置的信息，请参阅通过控制台配置 VPN 集中器。

在以太网 1（专用）接口上配置 IP 地址之后，可在 CLI 中或通过浏览器界面配置其余 IP 地址。浏览器界面支持 HTTP 和使用安全套接字层 (SSL) 的 HTTP。

以下参数通过控制台进行配置：

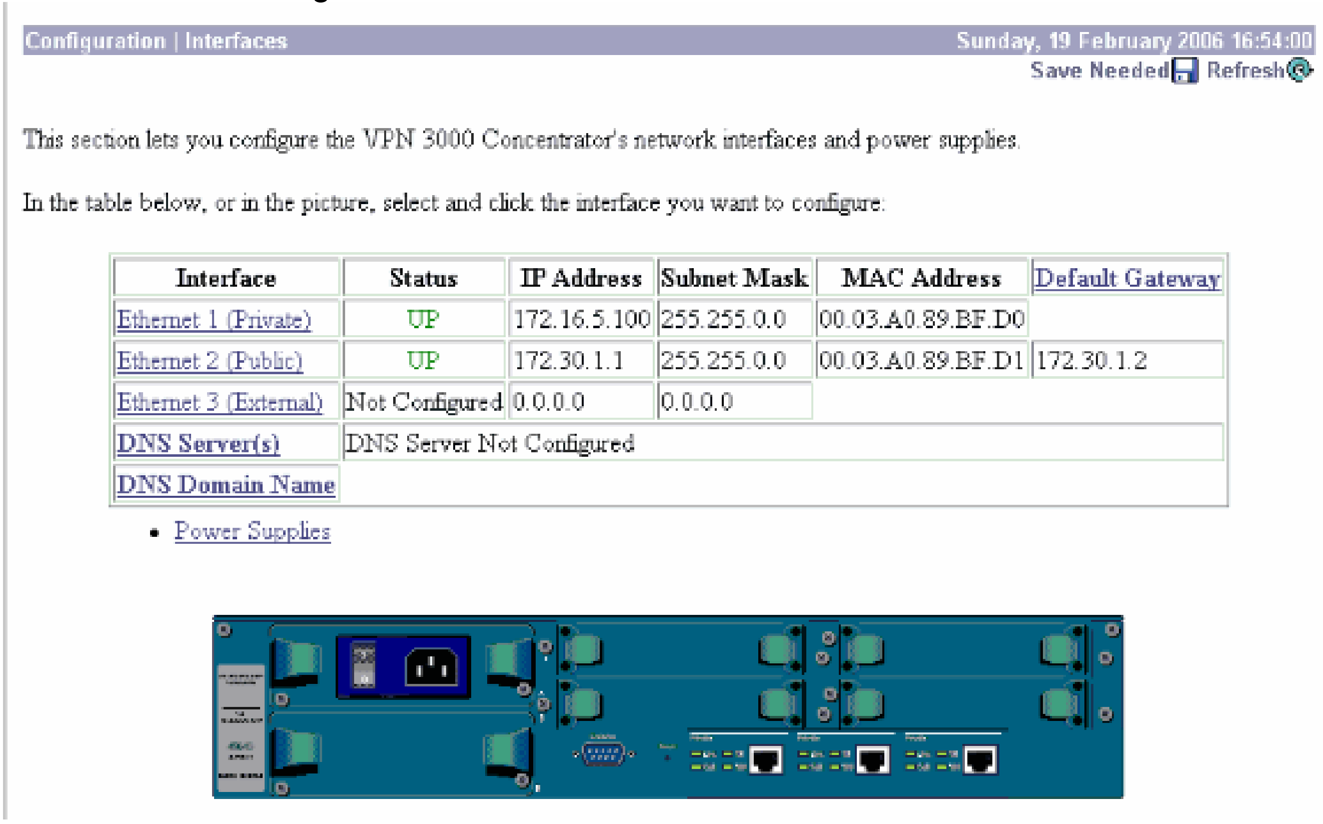
- **时间/日期 - 正确的时间和日期非常重要。**他们帮助保证记录和记帐条目是准确的，并且系统能创建一个有效安全证书。
- **以太网 1（专用）接口 - 网络拓扑 172.16.5.100/16 的 IP 地址和掩码。**

现在，可通过 HTML 浏览器从网络内部访问 VPN 集中器。有关如何在 CLI 模式下配置 VPN 集中器的信息，请参阅使用命令行界面快速配置。

从 Web 浏览器中键入专用接口的 IP 地址，以便启用 GUI 界面。

单击 **save needed 图标将更改保存到内存中。**出厂默认用户名和口令为 admin，且区分大小写。

1. 启动 GUI，选择 **Configuration > Interfaces 以便为公共接口配置 IP 地址和默认网关。**



Configuration | Interfaces

Sunday, 19 February 2006 16:54:00

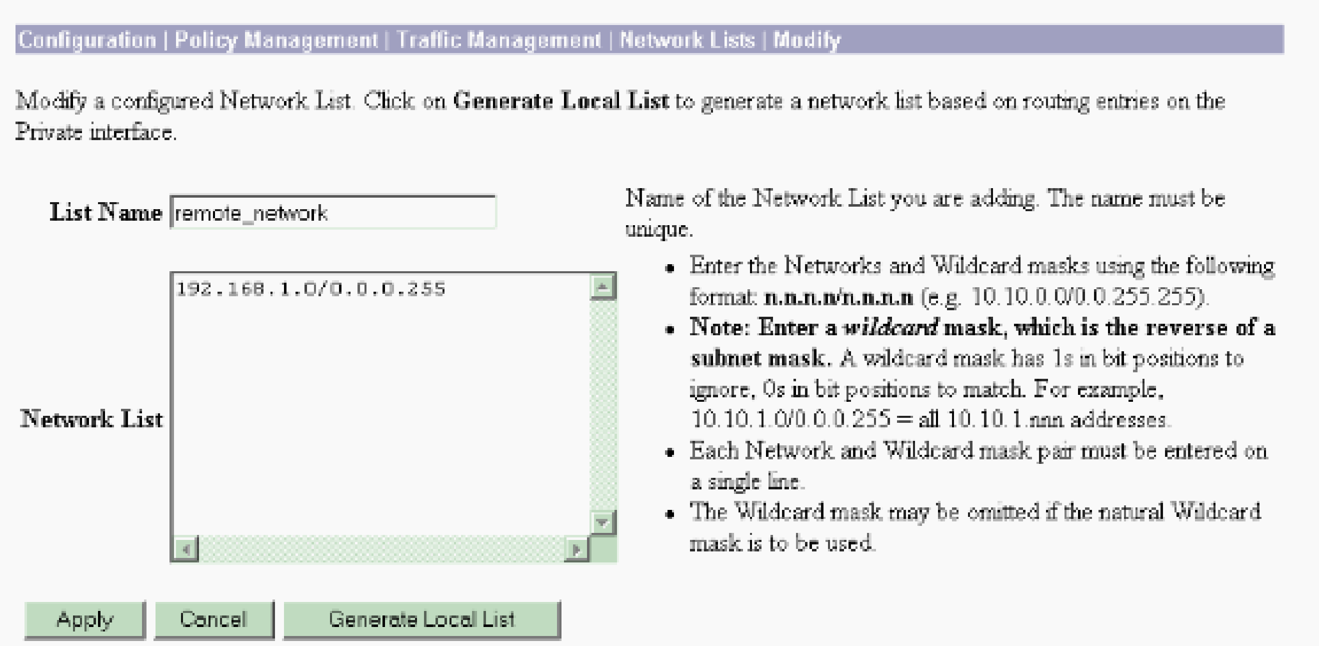
This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

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. 选择 **Configuration > Policy Management > Traffic Management > Network Lists > Add or Modify 创建定义要加密的数据流的网络列表。**请在此处添加本地和远程网络。IP 地址应镜像在远程 PIX 上配置的访问列表中的 IP 地址。在本示例中，这两个网络列表为 **remote_network 和"VPN Client Local LAN"。**



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 remote_network

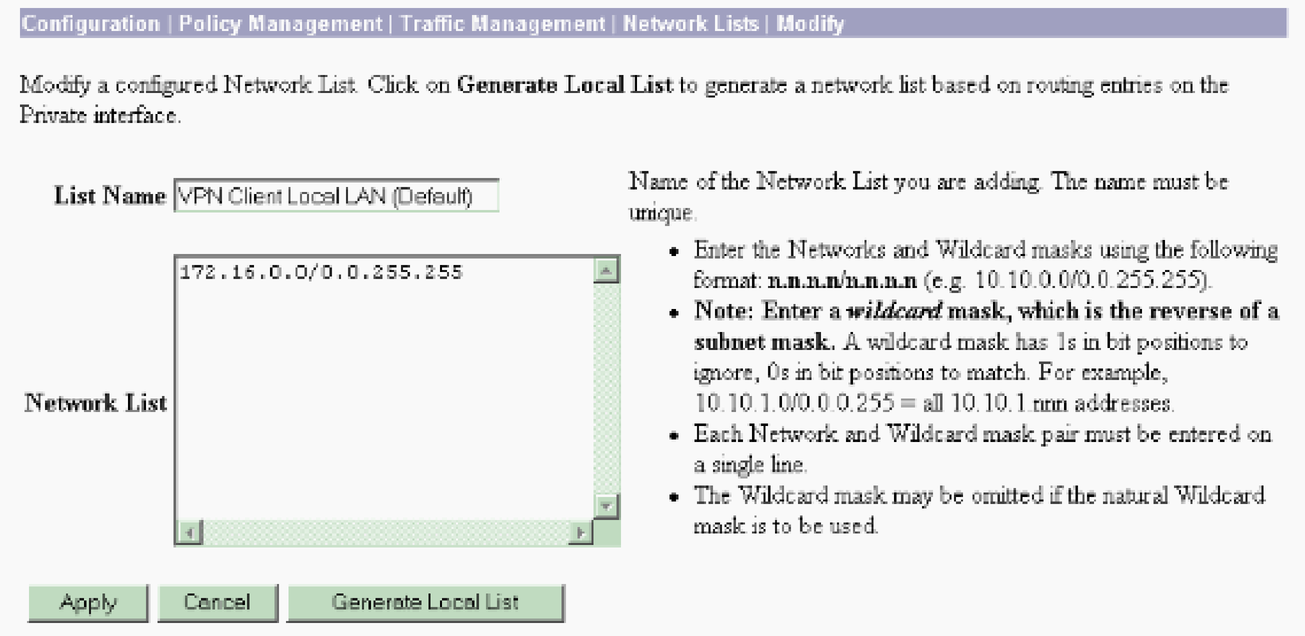
Name of the Network List you are adding. The name must be unique.

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.

Apply
Cancel
Generate Local List



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 VPN Client Local LAN (Default)

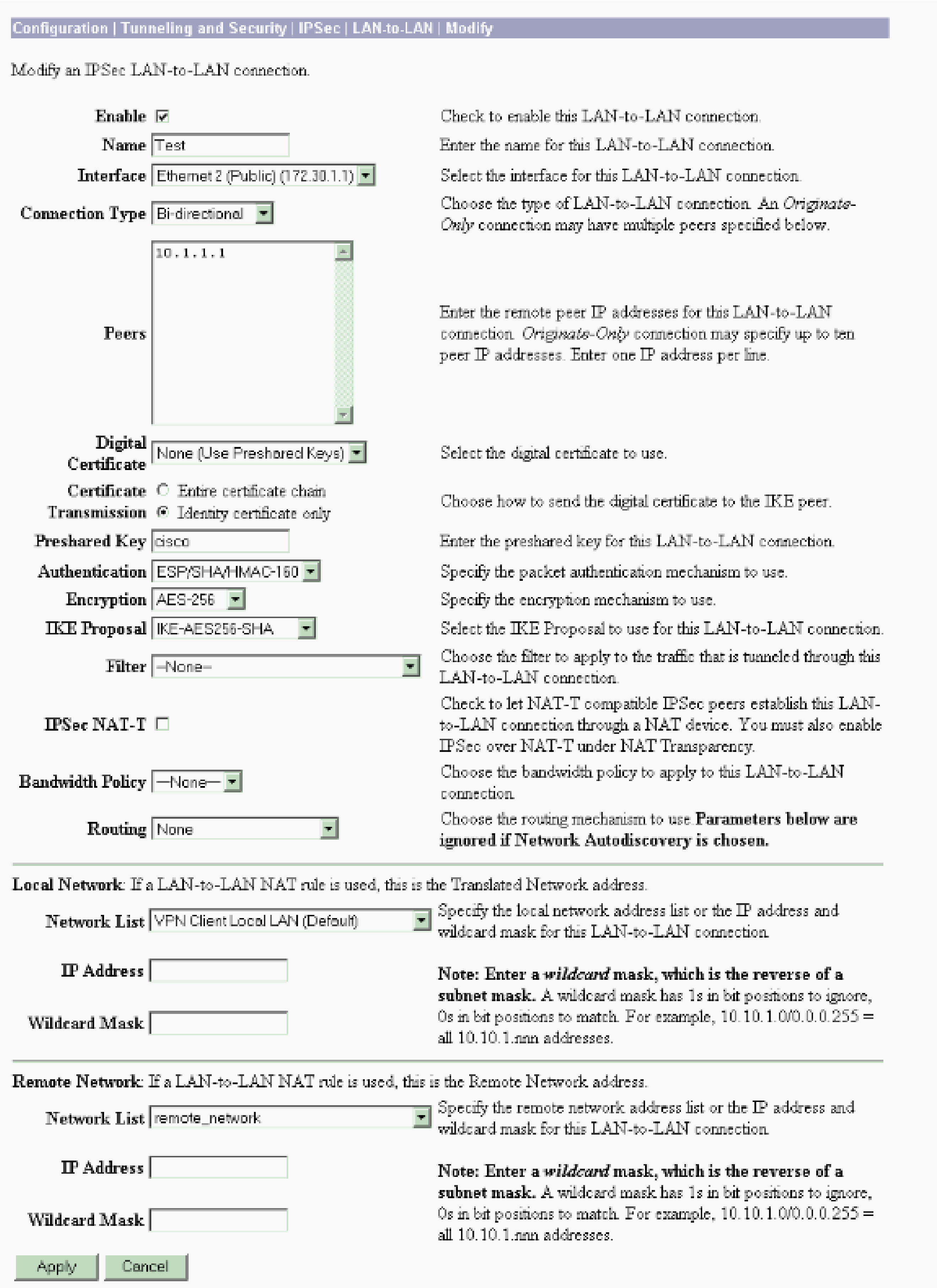
Name of the Network List you are adding. The name must be unique.

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. 选择 **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add 配置 IPsec LAN 到 LAN 隧道。**完成后，单击 **Apply**。输入对等体 IP 地址、在第 2 步中创建的网络列表、IPsec 和 ISAKMP 参数，以及预共享密钥。在本示例中，对等体 IP 地址为 **10.1.1.1**，网络列表为 remote_network 和“VPN Client Local LAN”，预共享密钥为“cisco”。



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Enable	☑	Check to enable this LAN-to-LAN connection.
Name	Test	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.30.1.1)	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional	Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.
Peers	10.1.1.1	Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.
Digital Certificate	None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission	○ Entire certificate chain ● Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key	cisco	Enter the preshared key for this LAN-to-LAN connection.
Authentication	ESP/SHA/HMAC-160	Specify the packet authentication mechanism to use.
Encryption	AES-256	Specify the encryption mechanism to use.
IKE Proposal	IKE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	--None--	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T	□	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	--None--	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing	None	Choose the routing mechanism to use. **Parameters below are ignored if Network Autodiscovery is chosen.**

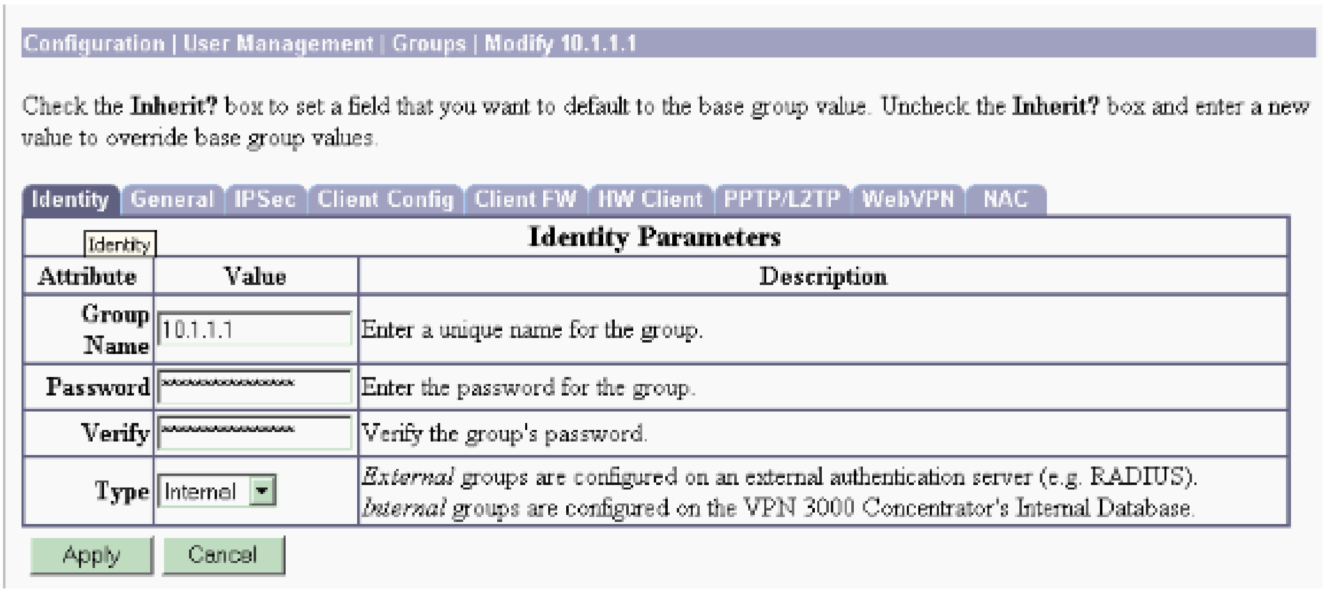
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List	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		**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.
Wildcard Mask		

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

Network List	remote_network	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address		**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.
Wildcard Mask		

4. 选择 **Configuration > User Management > Groups > Modify 10.1.1.1 查看自动生成的组信息。注意：**请勿修改这些组设置。



Configuration | User Management | Groups | Modify 10.1.1.1

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	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

验证

使用本部分可确认配置能否正常运行。

- 验证 PIX
- 验证 VPN 3000 集中器

验证 PIX

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show isakmp sa** - 显示对等体上的所有当前 IKE 安全关联 (SA)。状态 MM_ACTIVE 表示使用主模式设置 IPsec VPN 隧道。在本示例中，PIX 防火墙发起 IPsec 连接。对等体 IP 地址为 172.30.1.1，并使用主模式建立连接。

```
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
```

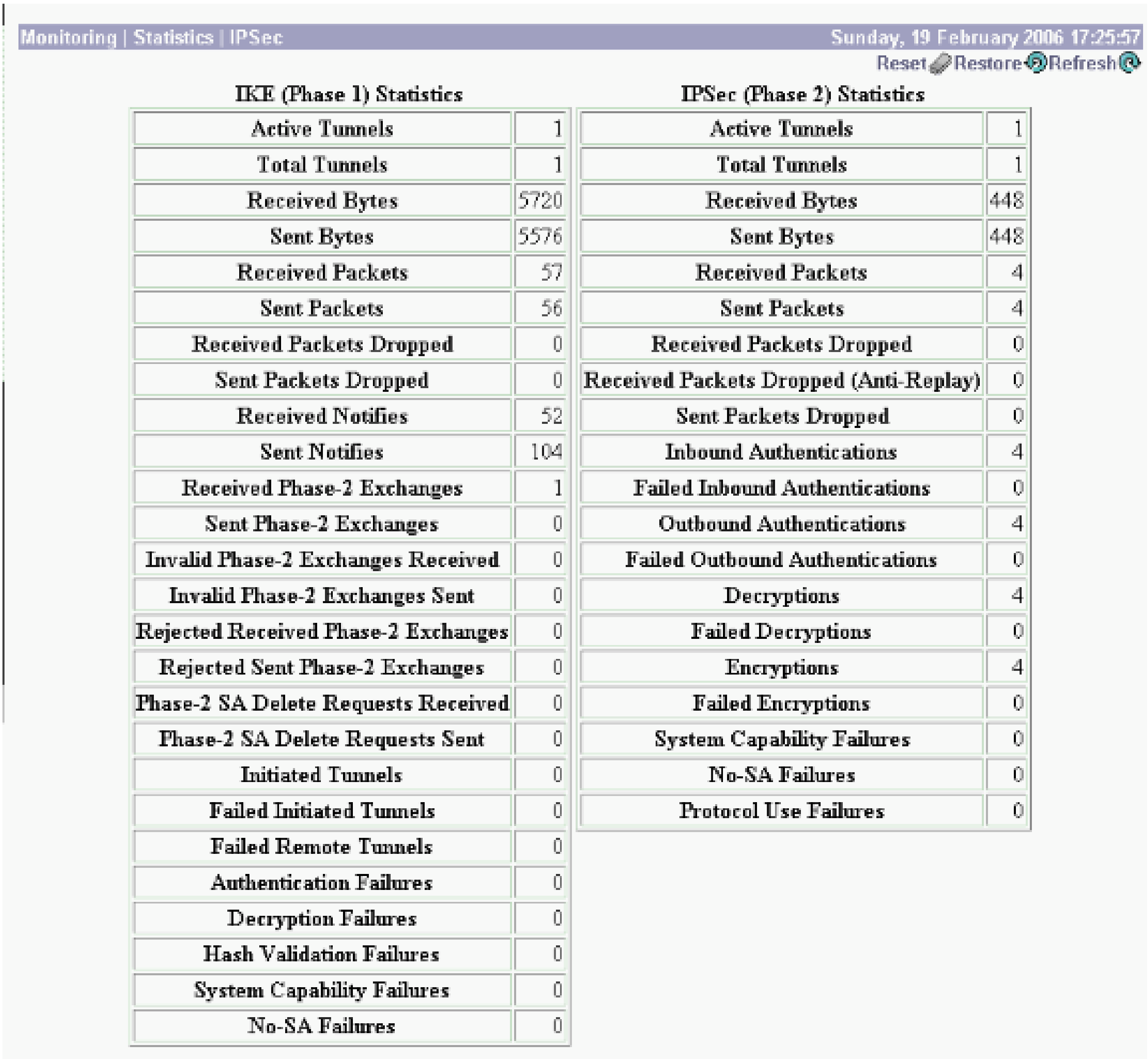
- **show ipsec sa** - 显示当前 SA 使用的设置。检查对等 IP 地址、本地和远程端都可访问的网络，以及所使用的转换集。有两个 ESP SA，每个方向一个。

```
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
```

使用 clear ipsec sa 和 clear isakmp sa 命令重置隧道。

验证 VPN 3000 集中器

选择 **Monitoring > Statistics > IPsec 验证是否已在 VPN 3000 集中器中建立隧道。**这包含 IKE 和 IPsec 参数的统计信息。



Monitoring | Statistics | IPSec
Sunday, 19 February 2006 17:25:57
Reset
Restore
Refresh

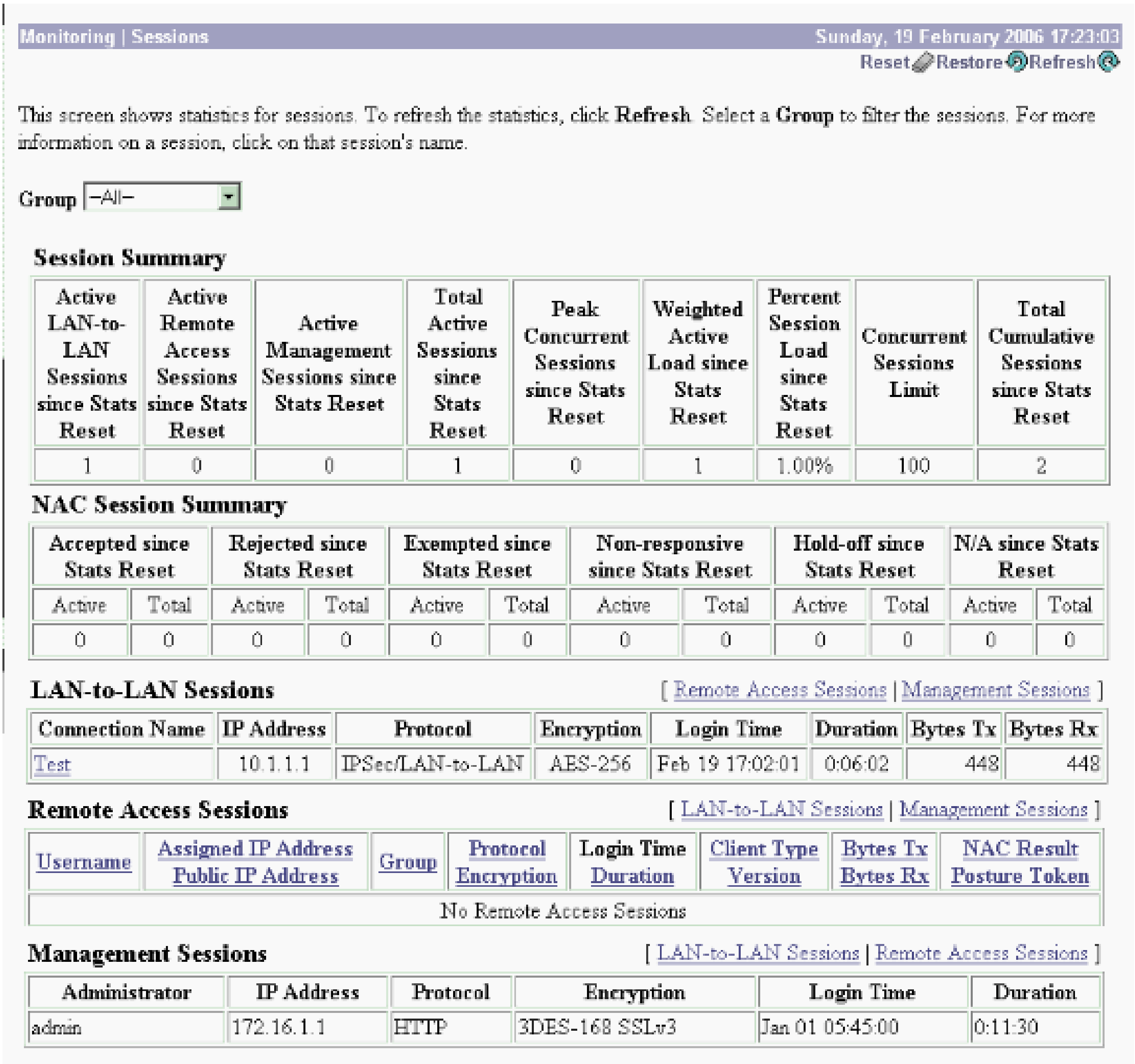
IKE (Phase 1) Statistics

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

选择 **Monitoring > Sessions** 可主动监控会话。可在此处重置 IPsec 隧道。



Monitoring | Sessions — Sunday, 19 February 2006 17:23:03

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 –All–

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

故障排除

本部分提供的信息可用于对配置进行故障排除。

- 排除 PIX 故障
- 排除 VPN 3000 集中器的故障
- PFS

排除 PIX 故障

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命令**的**重要信息。

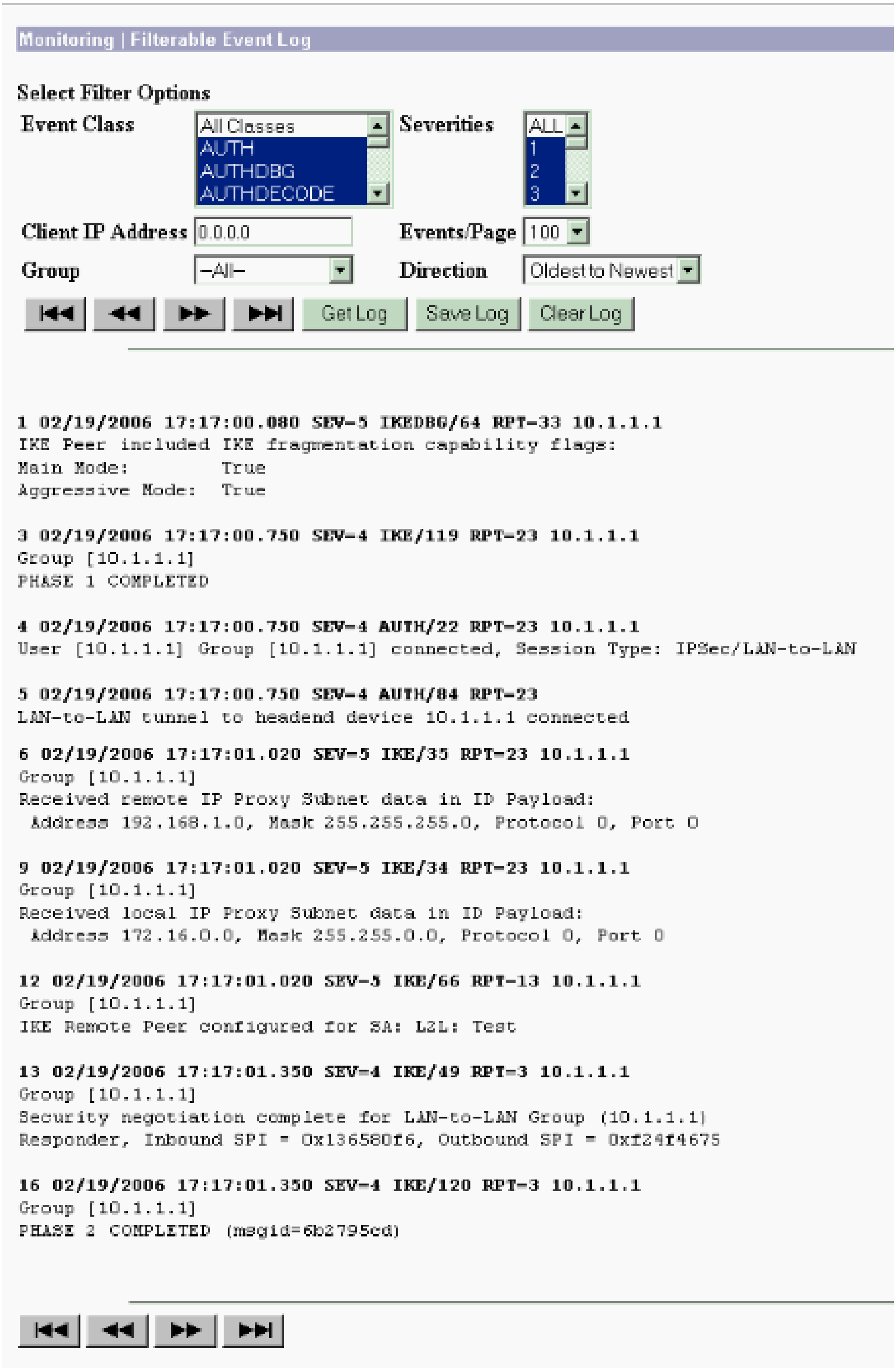
PIX 上用于 VPN 隧道的 **debug 命令包括：**

- debug crypto isakmp - 调试 ISAKMP SA 协商。
- debug crypto ipsec - 调试 IPsec SA 协商。

排除 VPN 3000 集中器的故障

类似于Cisco路由器的debug命令，您能配置事件类型，以查看所有告警。选择 **Configuration > System > Events > Classes > Add 以便对事件类启用日志记录。**

选择 **Monitoring > Filterable Event Log 监控已启用的事件。**



Select Filter Options

Event Class: All Classes, AUTH, AUTHDBG, AUTHDECODE

Severities: ALL, 1, 2, 3

Client IP Address: 0.0.0.0

Events/Page: 100

Group: --All--

Direction: 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

在 IPsec 协商中，完全转发保密 (PFS) 可确保每个新的加密密钥与任何先前密钥不相关。请在两个

隧道对等体上同时启用或禁用 PFS，否则不会在 PIX/ASA 中建立 LAN 到 LAN (L2L) IPsec 隧道。

默认情况下 PFS 处于禁用状态。要启用 PFS，请在组策略配置模式下使用 **pfs 命令并指定 enable 关键字。**要禁用 PFS，请输入 **disable 关键字。**

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

要从正在运行的配置中删除 PFS 属性，请输入此命令的 **no 形式。**一个组策略可以从另一个组策略继承 PFS 的值。请输入此命令的 **no 形式，以防止继承值。**

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

相关信息

- Cisco PIX 500 系列安全设备 - 支持页
- Cisco VPN 3000 系列集中器 - 支持页
- Cisco PIX 500 系列安全设备命令参考
- 技术支持和文档 - Cisco Systems