Ejemplo de Configuración de Túnel IPsec entre PIX 7.x y VPN 3000 Concentrator

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de cómo establecer un túnel VPN IPsec de LAN a LAN entre un PIX Firewall 7.x y un Cisco VPN 3000 Concentrator.

Consulte Ejemplo de Configuración de PIX/ASA 7.x Enhanced Spoke-to-Client VPN con autenticación TACACS+ para obtener más información sobre el escenario en el que el túnel LAN-a-LAN entre los PIX también permite que un Cliente VPN acceda al PIX spoke a través del PIX hub.

Consulte Ejemplo de Configuración de Túnel IPsec de LAN a LAN de PIX/ASA 7.x a un Router IOS para obtener más información sobre la situación en la que se encuentra el túnel de LAN a LAN entre el PIX/ASA y un Router IOS.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Este documento requiere una comprensión básica del protocolo IPSec Consulte Introducción al Cifrado IPSec para obtener más información sobre IPsec.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco PIX 500 Series Security Appliance con la versión de software 7.1(1)
- Concentrador VPN 3060 de Cisco con versión de software 4.7.2(B)

Nota: PIX 506/506E no soporta 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Para configurar PIX 6.x, consulte Túnel IPSec de LAN a LAN entre el Concentrador VPN 3000 de Cisco y Ejemplo de Configuración de Firewall PIX.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

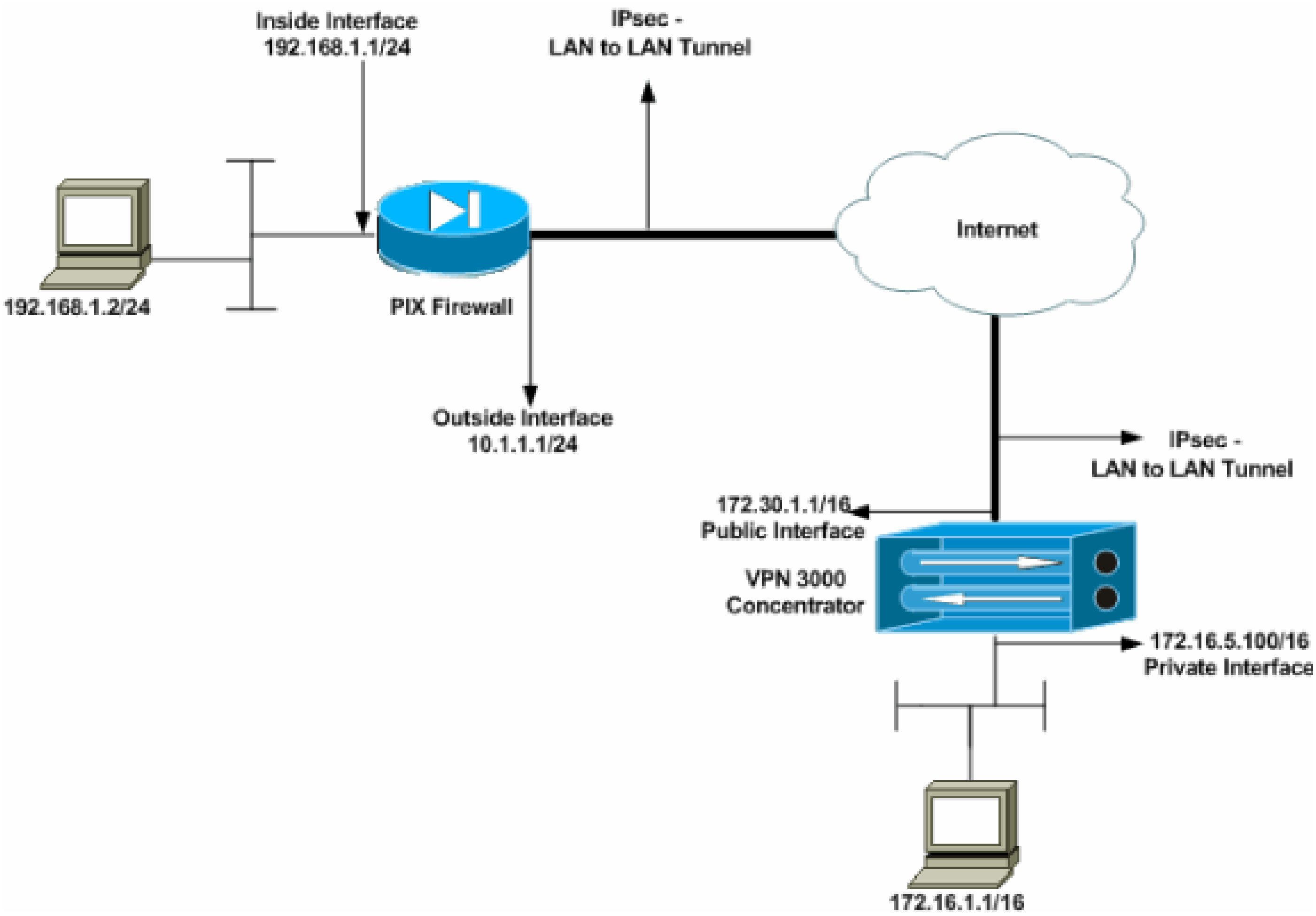
En esta sección encontrará la información para configurar las funciones descritas en este documento.

- Configure el PIX
- Configurar el concentrador VPN 3000

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configure el 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#
```

Configurar el concentrador VPN 3000

Los concentradores VPN no están preprogramados con direcciones IP en sus configuraciones de fábrica. Debe utilizar el puerto de la consola para configurar las configuraciones iniciales que son una interfaz de línea de comandos (CLI) basada en menús. Consulte Configuración de Concentradores VPN a través de la Consola para obtener información sobre cómo configurar a través de la consola.

Después de configurar la dirección IP en la interfaz Ethernet 1 (privada), puede configurar el resto con la CLI o a través de la interfaz del explorador. La interfaz del explorador admite HTTP y HTTP a través de Secure Socket Layer (SSL).

Estos parámetros se configuran a través de la consola:

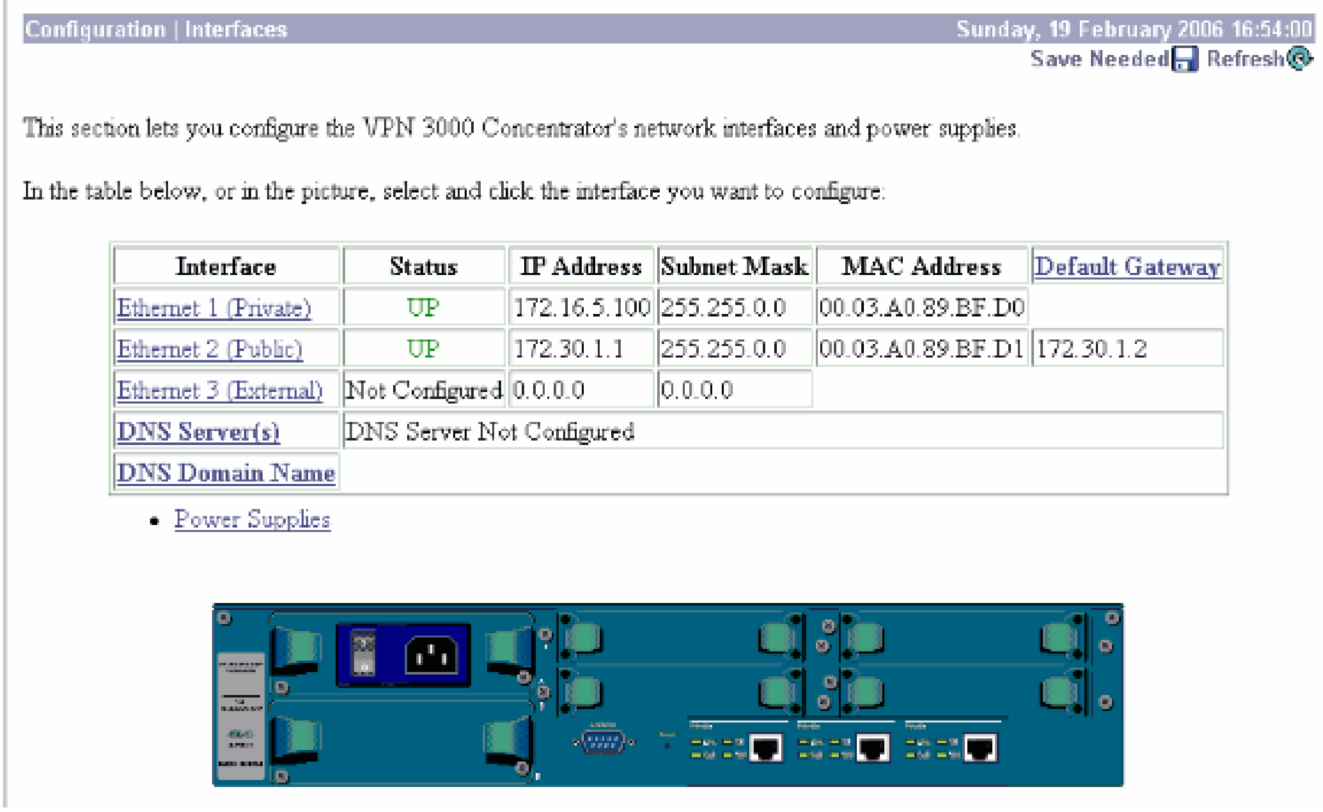
- **Hora/Fecha**: la hora y la fecha correctas son muy importantes. Ayudan a garantizar que las entradas de registro y de contabilidad sean exactas y que el sistema pueda crear un certificado de seguridad válido.
- **Interfaz Ethernet 1 (privada)**: la dirección IP y la máscara (de la topología de red 172.16.5.100/16).

Ahora se puede acceder al concentrador VPN a través de un navegador HTML desde la red interna. Refiérase a Uso de la Interfaz de Línea de Comandos para la Configuración Rápida para obtener información sobre cómo configurar el VPN Concentrator en el modo CLI.

Escriba la dirección IP de la interfaz privada desde el navegador web para habilitar la interfaz GUI.

Haga clic en el icono **guardar** los cambios necesarios para guardar la memoria. El nombre de usuario y la contraseña predeterminados de fábrica son **admin**, que distingue entre mayúsculas y minúsculas.

1. Inicie la GUI y seleccione **Configuration > Interfaces** para configurar la dirección IP para la interfaz pública y el gateway predeterminado.



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

Save Needed Refresh

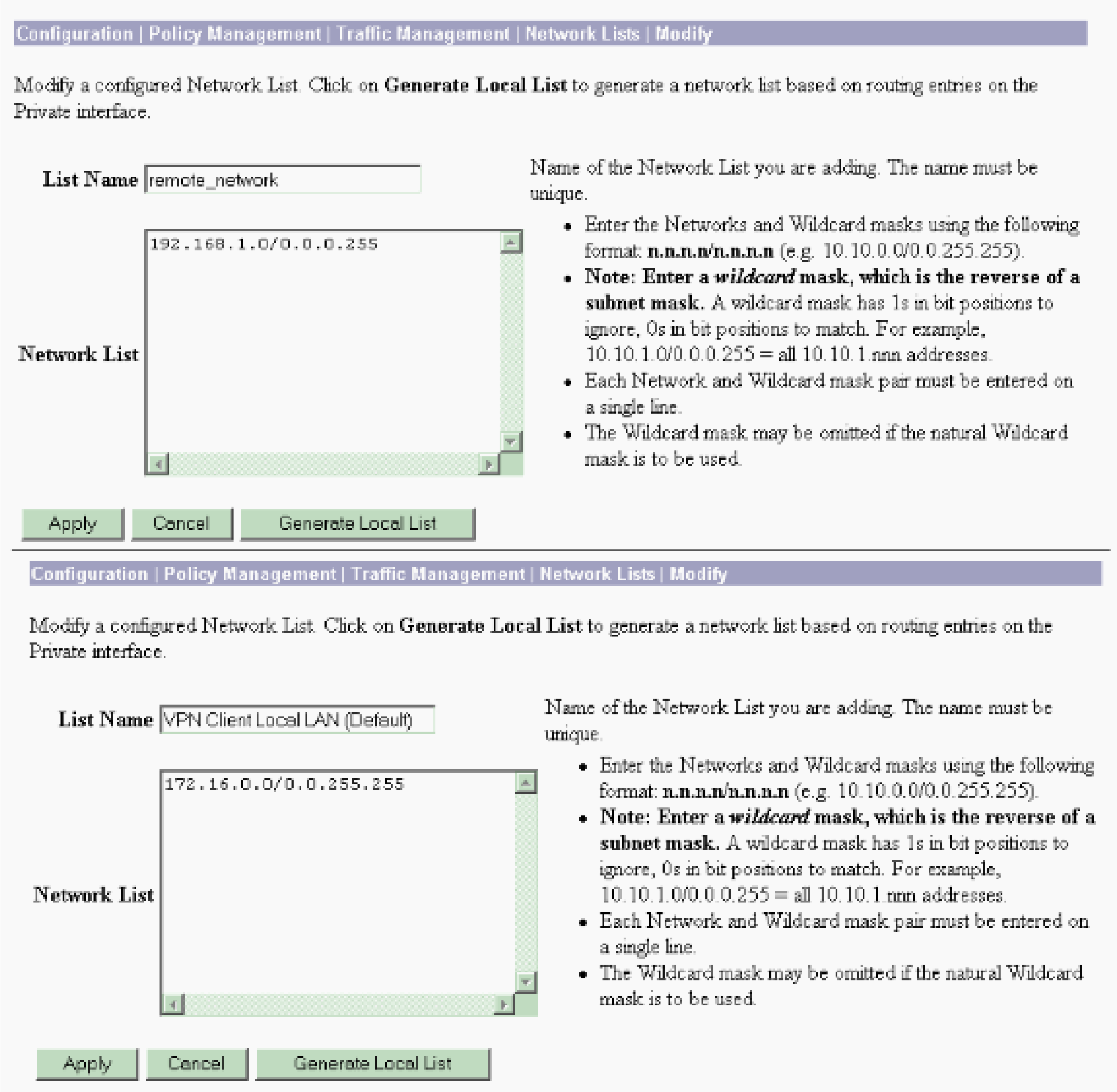
This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

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. Seleccione **Configuration > Policy Management > Traffic Management > Network Lists > Add or Modify** para crear las listas de red que definen el tráfico que se cifrará.Agregue aquí las redes locales y remotas. Las direcciones IP deben reflejar las de la lista de acceso configurada en el PIX remoto.En este ejemplo, las dos listas de red son **remote_network** y **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.

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)

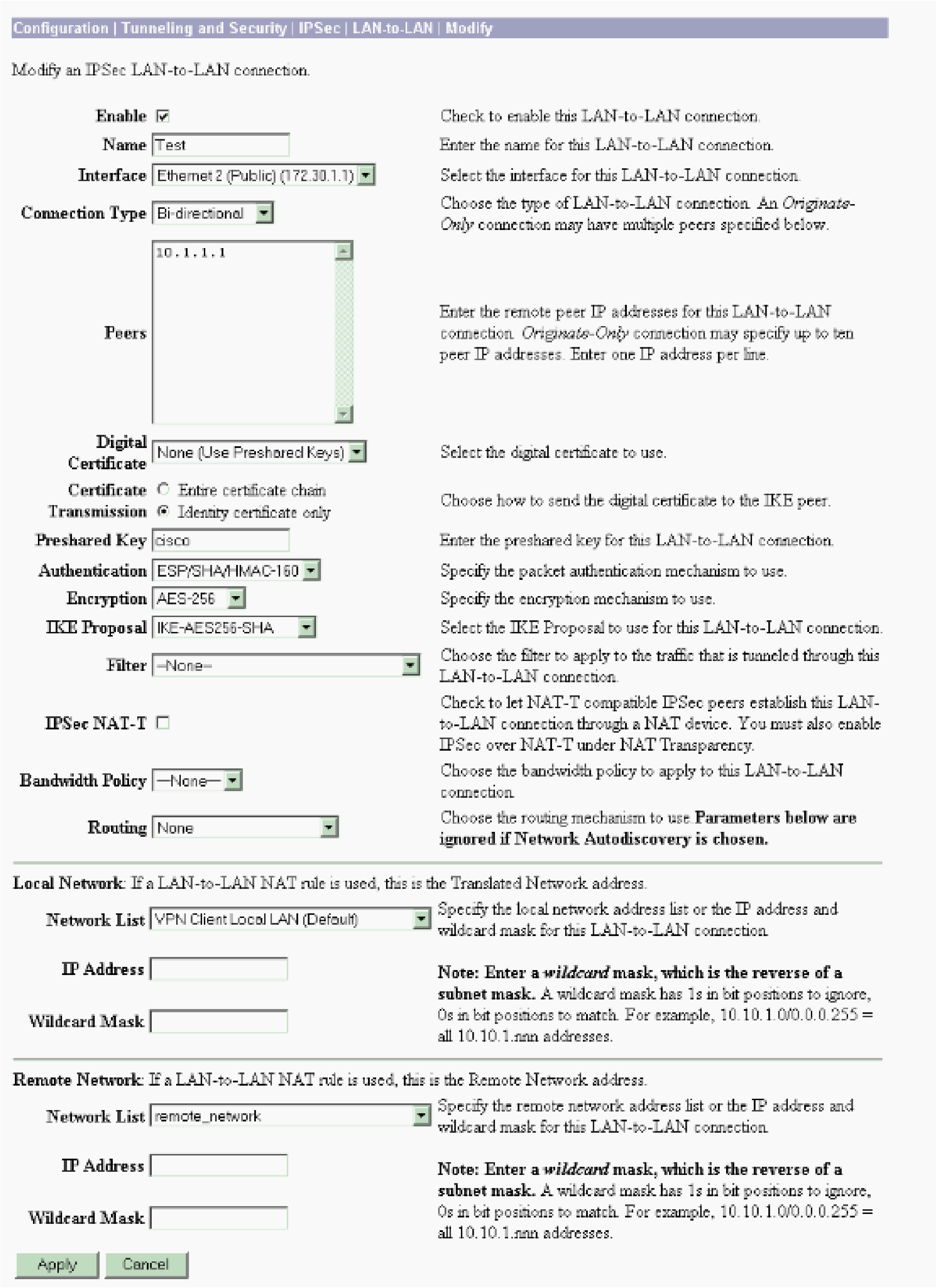
Name of the Network List you are adding. The name must be unique.

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. Seleccione **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add** para configurar el túnel IPsec LAN-to-LAN. Haga clic en Apply (Aplicar) cuando termine.Introduzca la dirección IP del par, las listas de red creadas en el paso 2, los parámetros IPsec e ISAKMP y la clave previamente compartida.En este ejemplo, la dirección IP del peer es **10.1.1.1**, las listas de red son **remote_network** y **VPN Client Local LAN**, y **cisco** es la clave previamente compartida.



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.**

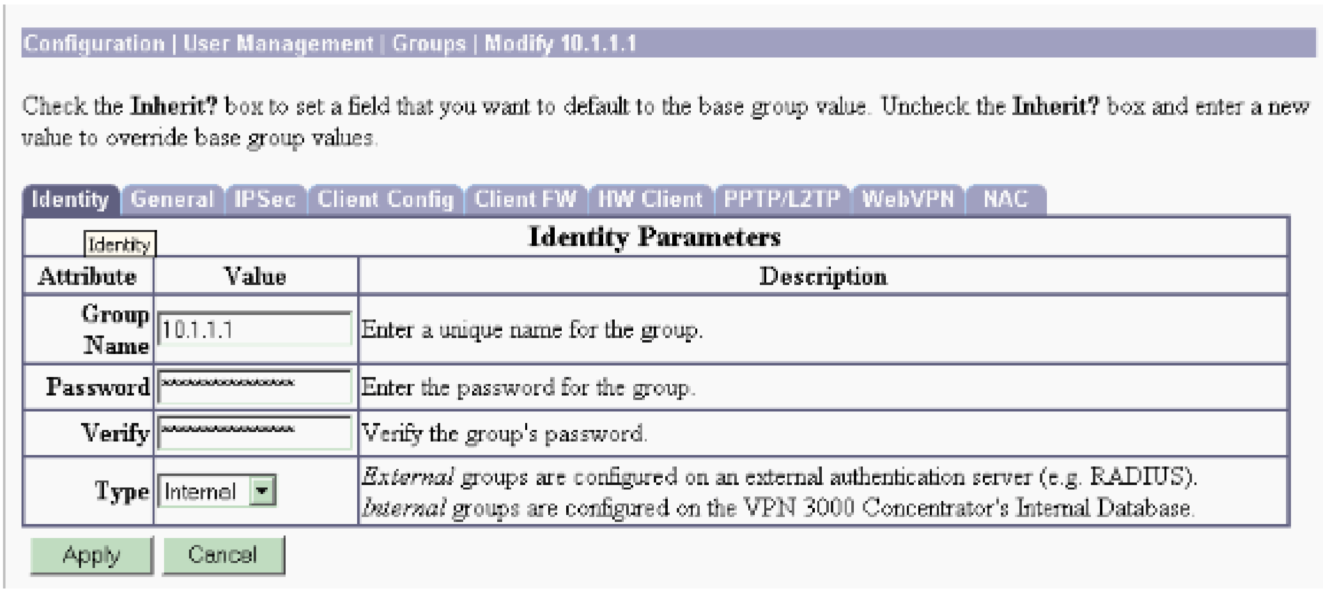
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

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. Seleccione **Configuration > User Management > Groups > Modify 10.1.1.1** para ver la información de grupo generada automáticamente.**Nota:** No modifique esta configuración de grupo.



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	**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.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- Verifique el PIX
- Verifique el concentrador VPN 3000

Verifique el PIX

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show isakmp sa** —Muestra todas las asociaciones de seguridad (SA) IKE actuales en un par. El estado MM_ACTIVE indica que el modo principal se utiliza para configurar el túnel VPN IPsec.En este ejemplo, el Firewall PIX inicia la conexión IPSec. La dirección IP del par es 172.30.1.1 y utiliza el modo principal para establecer la conexión.

```
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
```

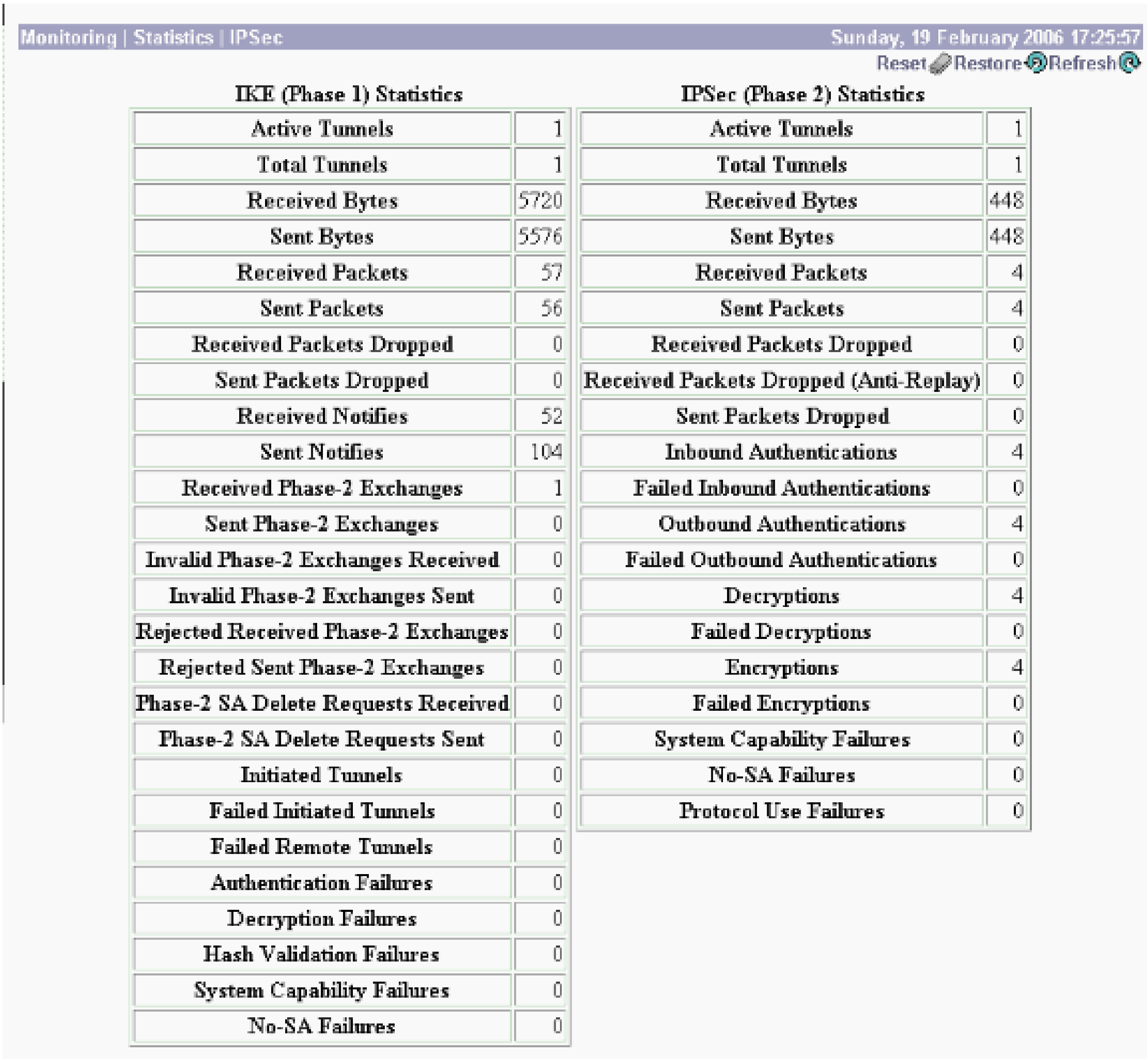
- **show ipsec sa** —Muestra la configuración utilizada por las SAs actuales. Verifique la dirección IP par, las redes accesibles en los extremos remotos y locales y la transformación fijada que se utiliza. Hay dos ESP SA, uno en cada dirección.

```
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
```

Utilice los comandos clear ipsec sa y clear isakmp sa para restablecer el túnel.

Verifique el concentrador VPN 3000

Seleccione **Monitoring > Statistics > IPsec** para verificar si el túnel ha aparecido en el VPN 3000 Concentrator. Esto contiene las estadísticas para los parámetros IKE e IPsec.


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

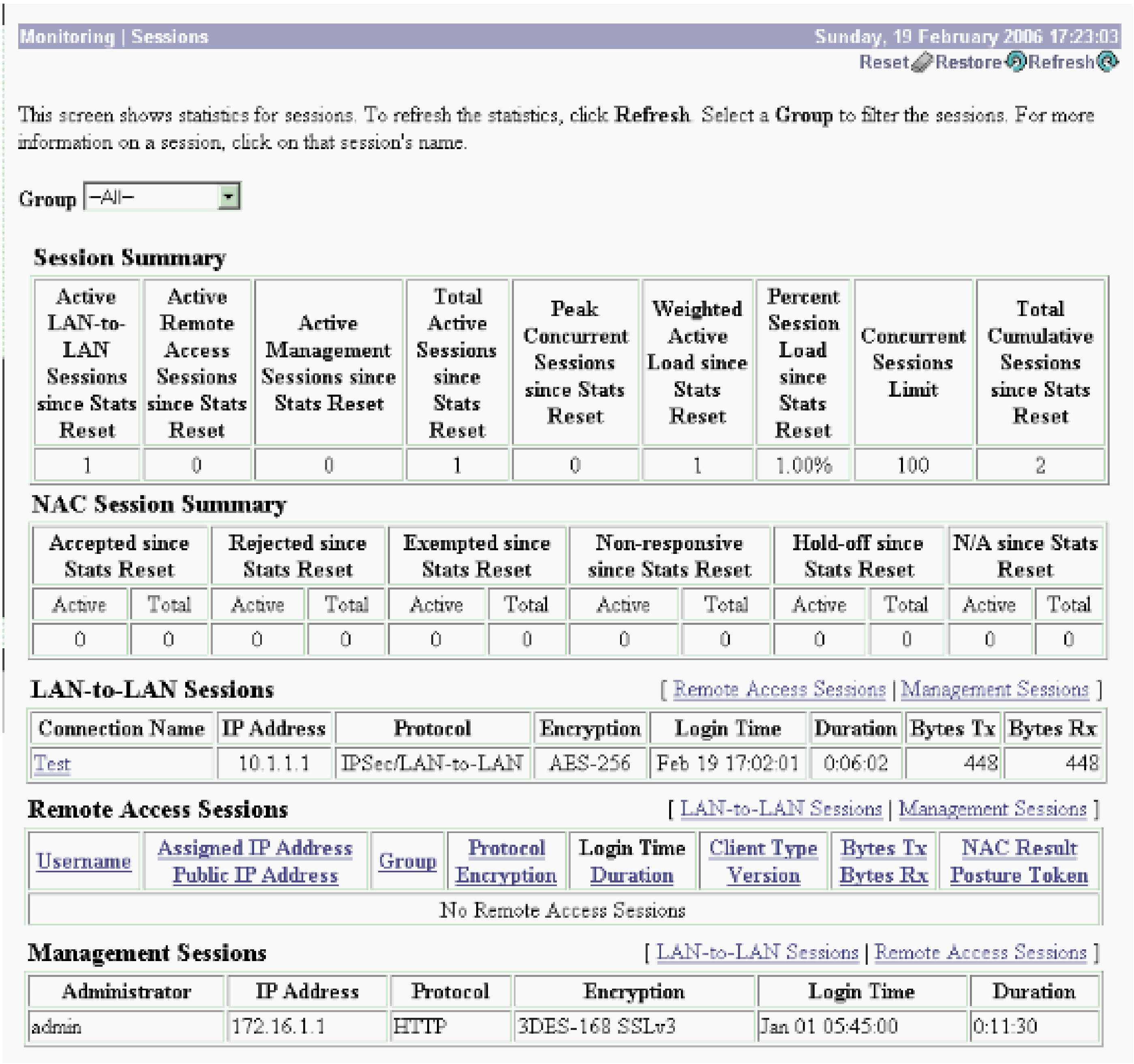
IKE (Phase 1) Statistics

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

Puede supervisar activamente la sesión en **Monitoring > Sessions**. Aquí puede restablecer el túnel IPsec.



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

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Solución de problemas de PIX
- Solución de problemas del concentrador VPN 3000
- PFS

Solución de problemas de PIX

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

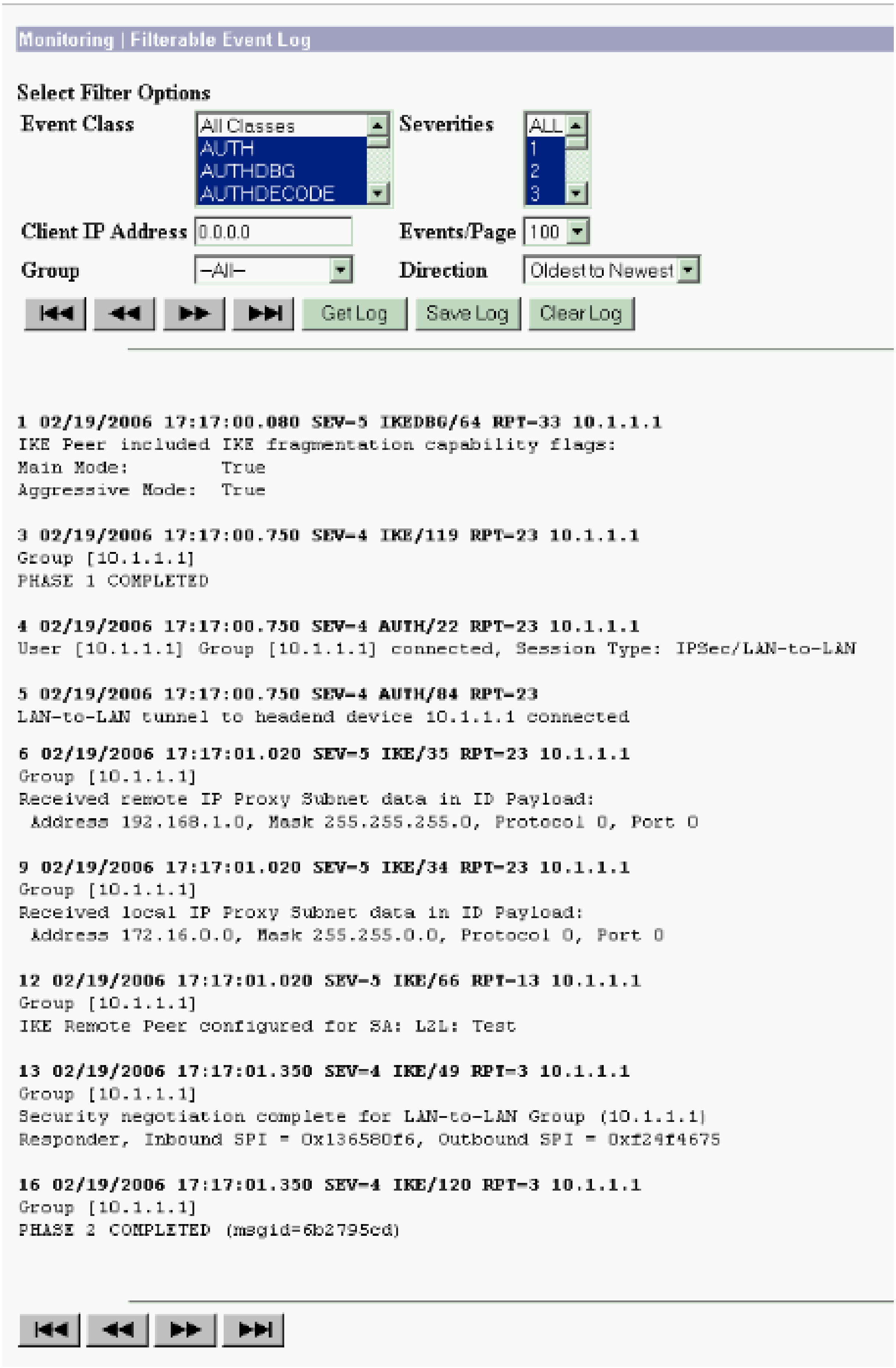
Los comandos **debug** en PIX para los túneles VPN son:

- **debug crypto isakmp** —Depura las negociaciones ISAKMP SA.
- **debug crypto ipsec** —Depura las negociaciones de SA IPSec.

Solución de problemas del concentrador VPN 3000

Al igual que los comandos debug en los routers Cisco, puede configurar las clases de eventos para ver todas las alarmas. Seleccione **Configuration > System > Events > Classes > Add** para activar el registro de clases de eventos.

Seleccione **Monitoring > Filterable Event Log** para supervisar los eventos habilitados.



```
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

En las negociaciones de IPSec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior. Active o desactive el PFS en ambos peers de túnel; de lo contrario, el túnel IPsec de LAN a LAN (L2L) no se establece en el PIX/ASA.

PFS se inhabilita de forma predeterminada. Para habilitar PFS utilice el comando **pfs** con la palabra clave *enable* en el modo de configuración de política de grupo. Para inhabilitar PFS, ingrese la palabra clave disable (inhabilitar).

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

Para quitar el atributo PFS de la configuración en ejecución, ingrese la forma no de este comando. Una política de grupo puede heredar un valor para PFS de otra política de grupo. Ingrese la forma no de este comando para evitar heredar un valor.

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

Información Relacionada

- Página de soporte de Cisco PIX 500 Series Security Appliances
- Cisco VPN 3000 Series Concentrator - Página de soporte
- Referencia de Comandos de Cisco PIX 500 Series Security Appliance
- Soporte Técnico y Documentación - Cisco Systems