PIX 7.x와 VPN 3000 Concentrator 간 IPsec 터널 컨피그레이션 예

목차

소개

이 문서에서는 PIX Firewall 7.x와 Cisco VPN 3000 Concentrator 간에 LAN-to-LAN IPsec VPN 터널을 설정하는 방법에 대한 샘플 컨피그레이션을 제공합니다.

PIX 간 LAN-to-LAN 터널을 통해 VPN 클라이언트가 허브 PIX를 통해 스포크 PIX에 액세스할 수 있는 시나리오에 대한 자세한 내용은 PIX/ASA 7.x Enhanced Spoke-to-Client VPN with TACACS+ Authentication Configuration 예를 참조하십시오.

PIX/ASA와 IOS 라우터 간의 LAN-to-LAN 터널 터널이 PIX/ASA와 IOS 라우터 간에 있는 시나리오에 대한 자세한 내용은 PIX/ASA 7.x Security Appliance to an IOS Router LAN-to-LAN 터널 구성 예를 참조하십시오.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 이 문서에서는 IPsec 프로토콜에 대한 기본적인 이해가 필요합니다.IPsec에 대한 자세한 내용은 IPsec 암호화 소개를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco PIX 500 Series Security Appliance, 소프트웨어 버전 7.1(1)
- Cisco VPN 3060 Concentrator 소프트웨어 버전 4.7.2(B)

참고: PIX 506/506E는 7.x를 지원하지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

PIX 6.x를 구성하려면 Cisco VPN 3000 Concentrator와 PIX Firewall Configuration Example 간의 LAN-to-LAN IPSec 터널을 참조하십시오.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

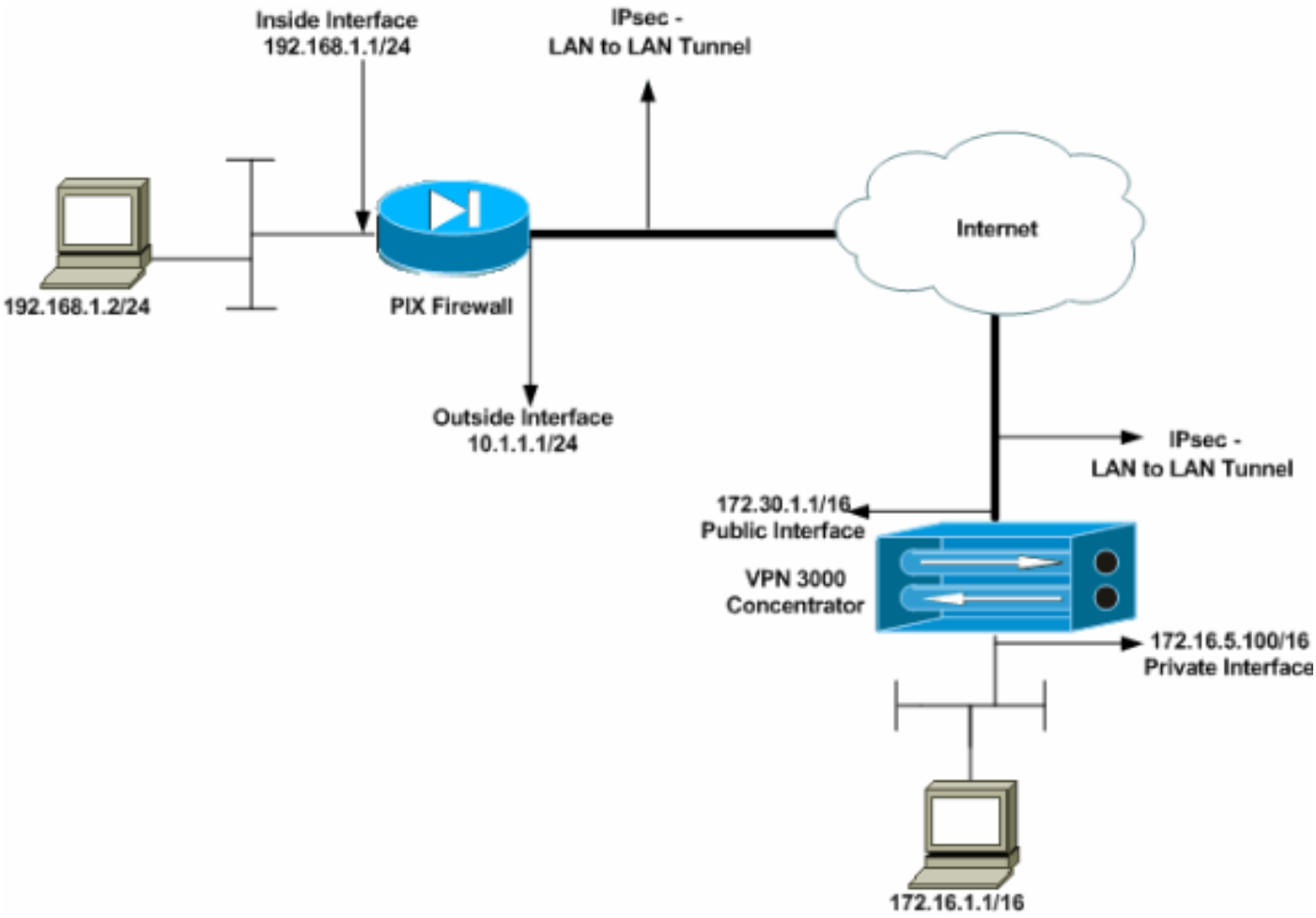
이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

- PIX 구성
- VPN 3000 Concentrator 구성

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



PIX 구성

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-121
tunnel-group 172.30.1.1 ipsec-attributes
 pre-shared-key *
!--- Output is suppressed. ! : end PIX7#
```

VPN 3000 Concentrator 구성

VPN Concentrator는 공장 설정에서 IP 주소로 사전 프로그래밍되지 않습니다.메뉴 기반 CLI(Command Line Interface)인 초기 컨피그레이션을 구성하려면 콘솔 포트를 사용해야 합니다. 콘솔을 통해 구성하는 방법에 대한 자세한 내용은 콘솔을 통해 VPN Concentrator 구성을 참조하십시오.

이더넷 1(프라이빗) 인터페이스에서 IP 주소를 구성한 후 CLI 또는 브라우저 인터페이스를 통해 나머지는 구성할 수 있습니다.브라우저 인터페이스는 SSL(Secure Socket Layer)을 통한 HTTP 및 HTTP를 모두 지원합니다.

이러한 매개변수는 콘솔을 통해 구성됩니다.

- **Time/Date(시간/날짜)** - 올바른 시간과 날짜가 매우 중요합니다.이를 통해 로깅 및 어카운팅 엔트리가 정확하며 시스템이 유효한 보안 인증서를 생성할 수 있는지 확인할 수 있습니다.
- **Ethernet 1 (private) interface**—IP 주소 및 마스크(네트워크 토폴로지 172.16.5.100/16에서).

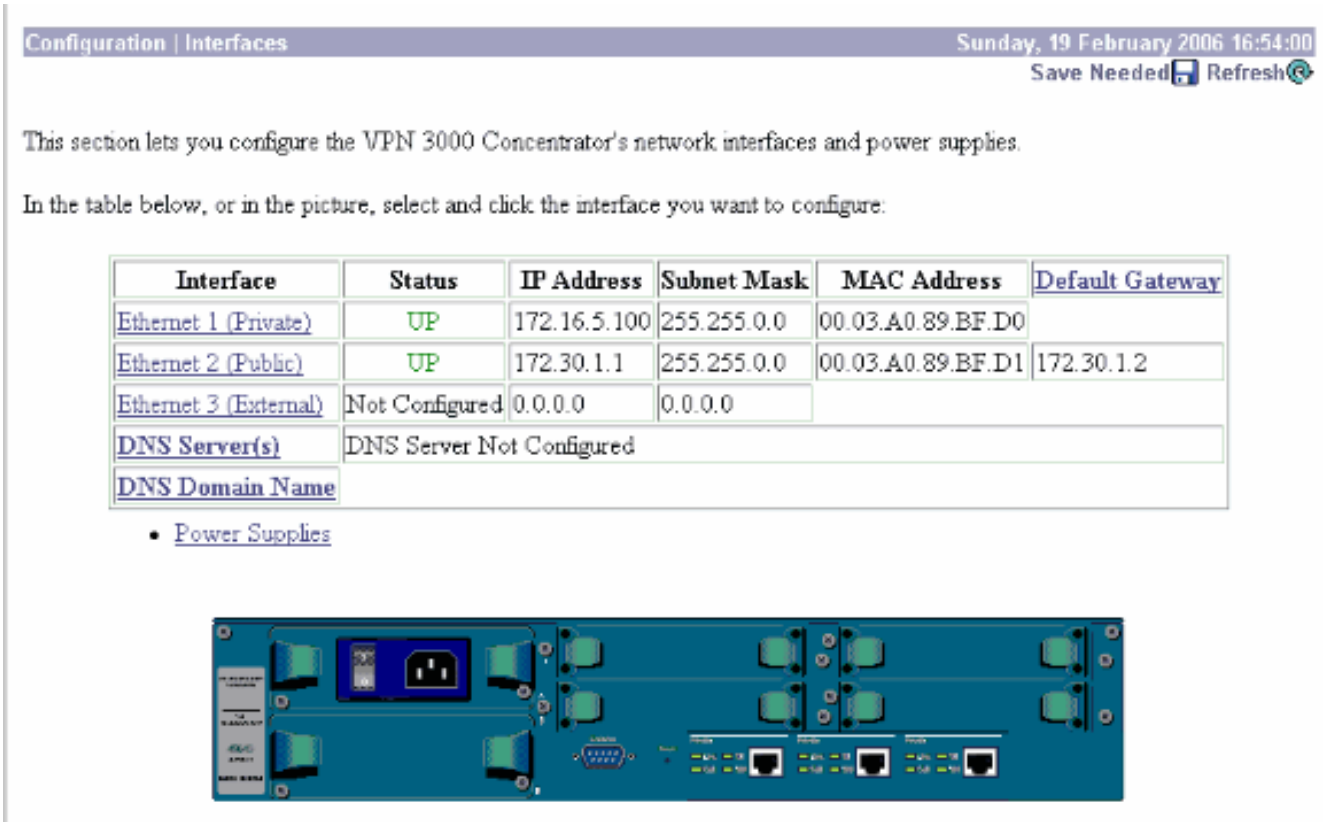
이제 내부 네트워크에서 HTML 브라우저를 통해 VPN Concentrator에 액세스할 수 있습니다.CLI 모드에서 VPN Concentrator를 구성하는 방법에 대한 자세한 내용은 빠른 컨피그레이션을 위한 명령줄 인터페이스 사용을 참조하십시오.

GUI 인터페이스를 활성화하려면 웹 브라우저에서 프라이빗 인터페이스의 IP 주소를 입력합니다.

변경 사항을 메모리에 저장하려면 **필요한 저장** 아이콘을 클릭합니다.공장 기본 사용자 이름 및 비밀번호는 **admin**이며 대/소문자를 구분합니다.

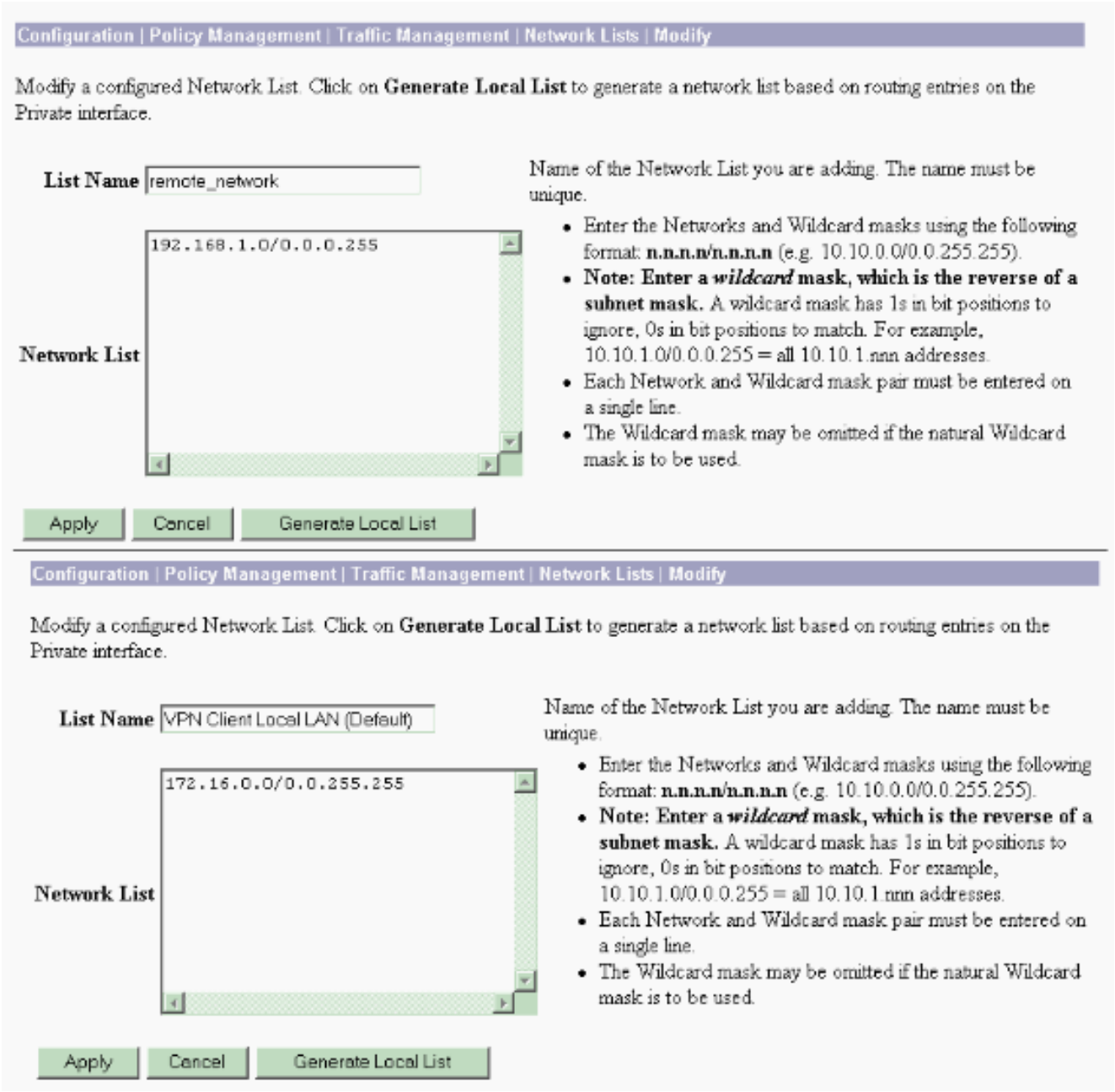
1. GUI를 시작하고 **Configuration > Interfaces**를 선택하여 공용 인터페이스 및 기본 게이트웨이의 IP 주소를 구성합니다

   .



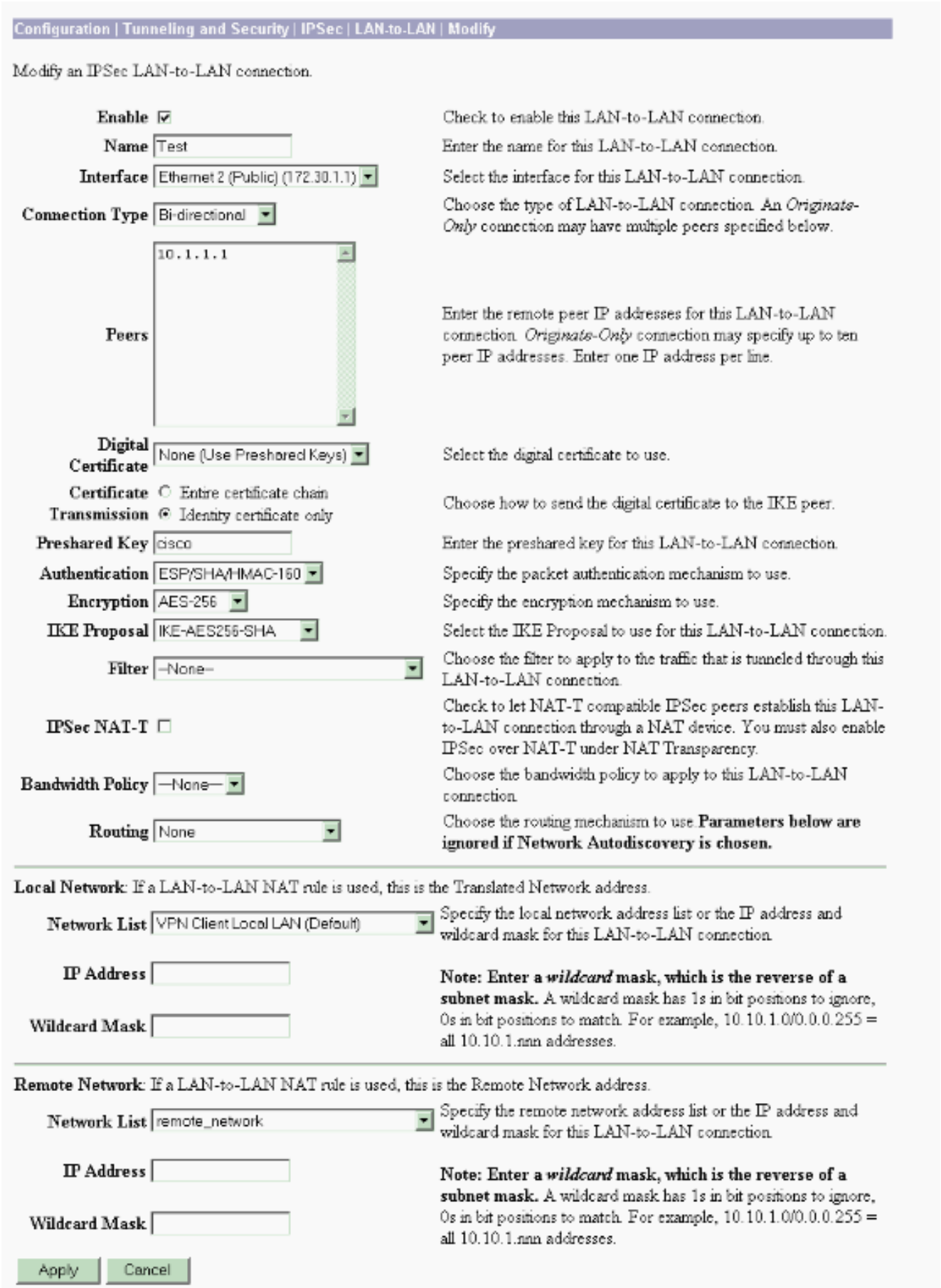
2. Configuration **> Policy Management > Traffic Management > Network Lists > Add 또는 Modify를 선택하여** 암호화할 트래픽을 정의하는 네트워크 목록을 생성합니다.여기에 로컬 및 원격 네트워크를 모두 추가합니다.IP 주소는 원격 PIX에 구성된 액세스 목록의 주소를 미러링해야 합니다.이 예에서 두 네트워크 목록은 **remote_network** 및 **VPN Client Local LAN입니다**

   .



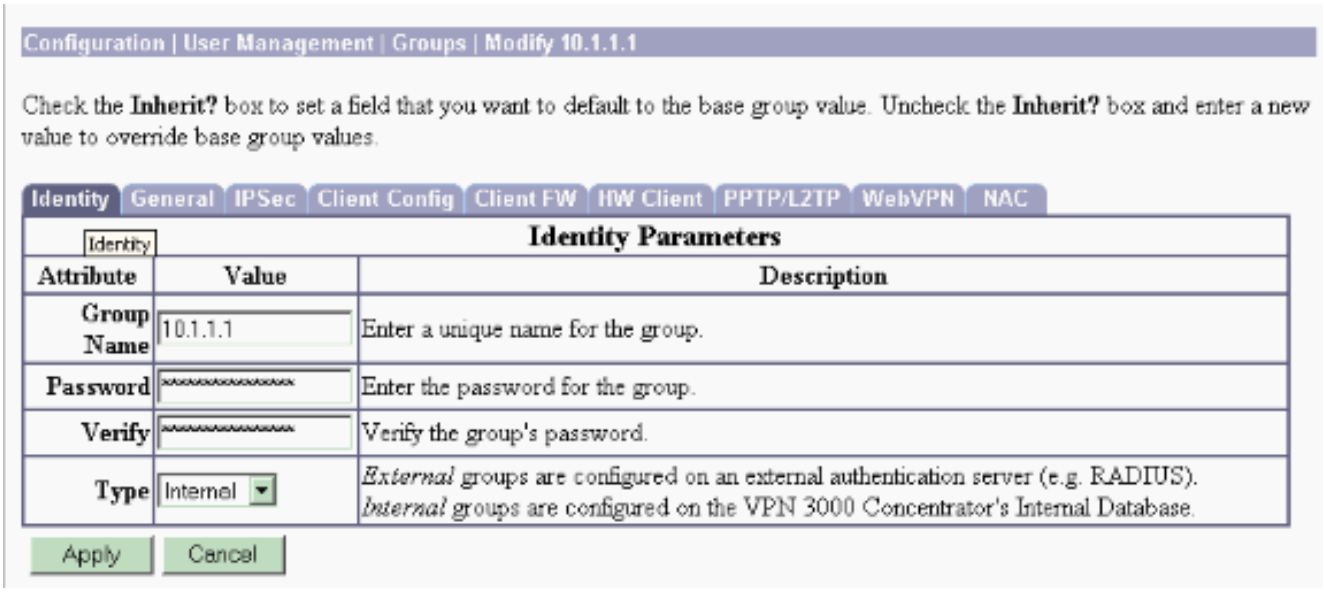
3. Configuration **> System > Tunneling Protocols > IPSec LAN-to-LAN > Add**를 선택하여 IPsec LAN-to-LAN 터널을 구성합니다.완료되면 **Apply**를 클릭합니다.피어 IP 주소, 2단계에서 생성된 네트워크 목록, IPsec 및 ISAKMP 매개변수, 사전 공유 키를 입력합니다.이 예에서 피어 IP 주소는 **10.1.1.1**이고, 네트워크 목록은 **remote_network** 및 **VPN Client Local LAN**, **cisco**는 사전 공유 키입니다

.



4. Configuration **> User Management > Groups > Modify 10.1.1.1을 선택하여** 자동으로 생성된 그룹 정보를 확인합니다.**참고:** 이러한 그룹 설정은 수정하지 마십시오

.



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 | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

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.

Apply | Cancel

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- PIX 확인
- VPN 3000 Concentrator 확인

PIX 확인

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show isakmp sa** - 피어의 현재 IKE SA(Security Association)를 모두 표시합니다.MM_ACTIVE 상태는 Main Mode가 IPsec VPN 터널을 설정하는 데 사용됨을 나타냅니다.이 예에서는 PIX 방화벽이 IPsec 연결을 시작합니다.피어 IP 주소는 172.30.1.1 이며 주 모드를 사용하여 연결을 설정합니다.

```
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** - 현재 SA에서 사용하는 설정을 표시합니다.피어 IP 주소, 로컬 및 원격 모두에서 액세스할 수 있는 네트워크, 사용되는 변형 집합을 확인합니다.ESP SA는 각 방향에 하나씩 2개 있습니다.

```
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)
```

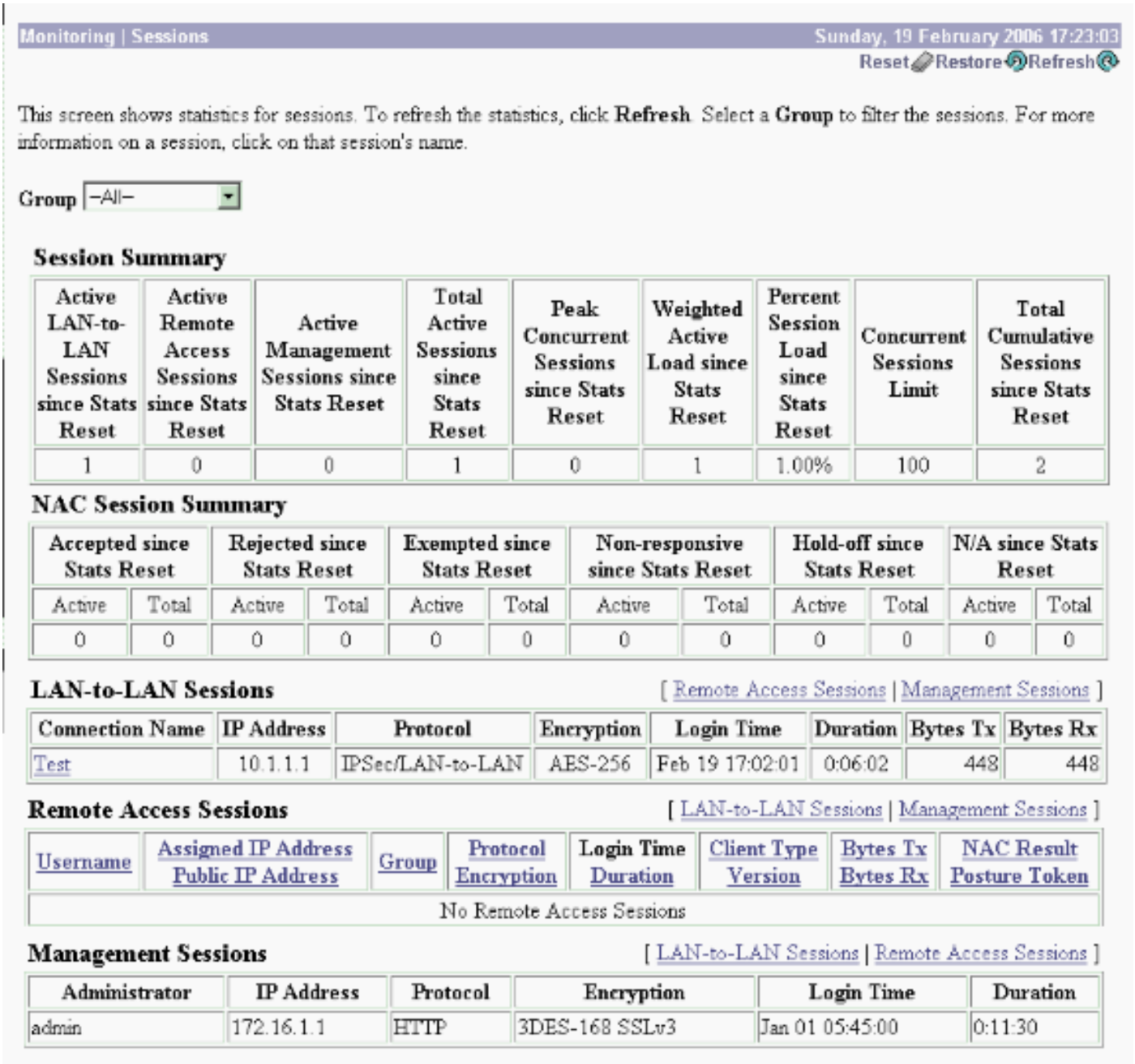
```
    current_peer: 172.30.1.1

    #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 및 clear isakmp sa 명령을 사용하여 터널을 재설정합니다.

VPN 3000 Concentrator 확인

Monitoring(**모니터링**) > **Statistics(통계)** > **IPsec**을 선택하여 터널이 VPN 3000 Concentrator에 나타나는지 확인합니다.여기에는 IKE 및 IPsec 매개변수 모두에 대한 통계가 포함됩니다.

Monitoring(모니터링) > **Sessions(세션)**에서 세션을 능동적으로 모니터링할 수 있습니다.여기에서 IPsec 터널을 재설정할 수 있습니다.



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

Reset Restore Refresh

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

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- PIX 문제 해결
- VPN 3000 Concentrator 문제 해결
- PFS

PIX 문제 해결

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

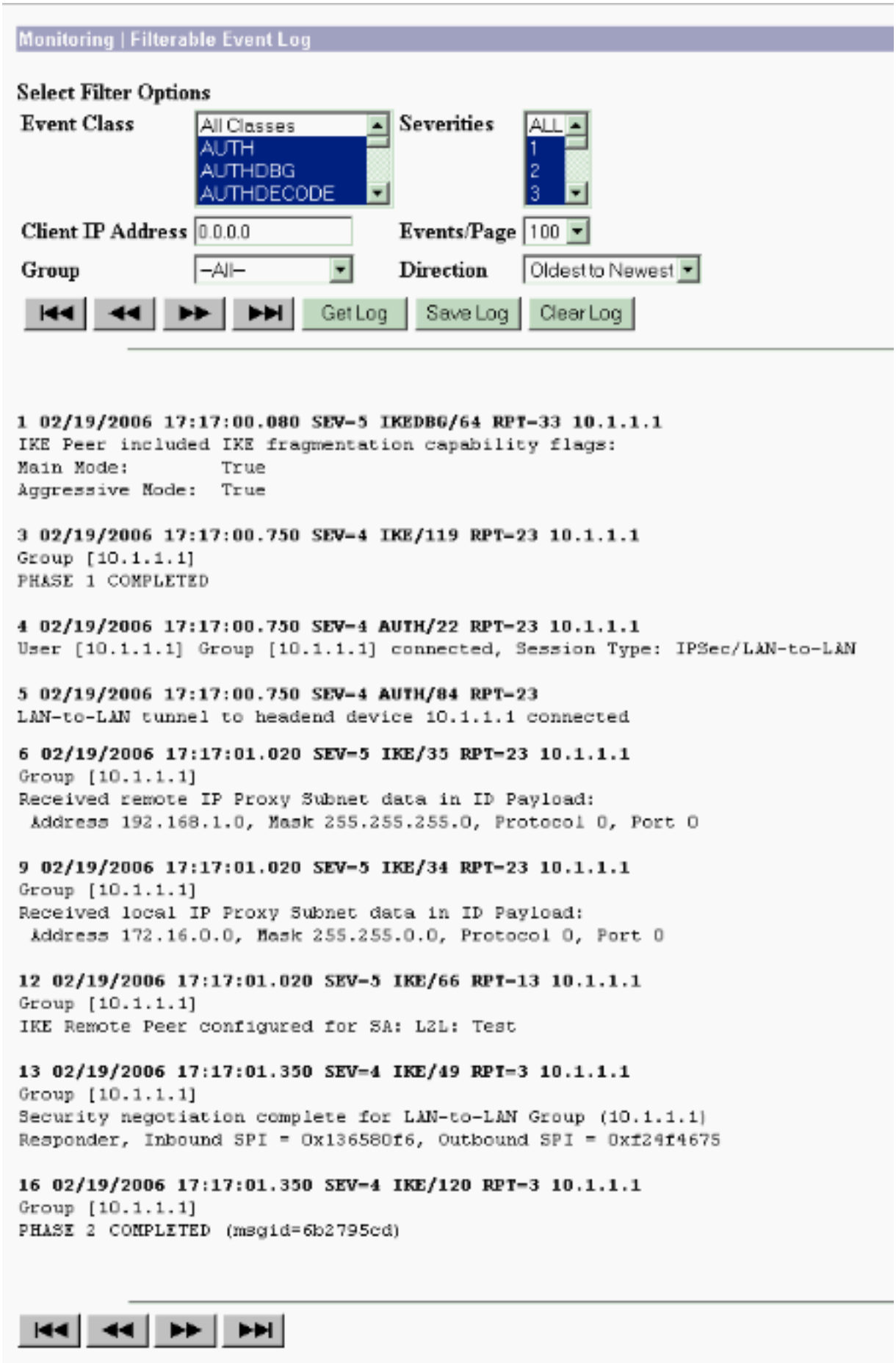
VPN 터널용 PIX의 **debug** 명령은 다음과 같습니다.

- debug crypto isakmp—ISAKMP SA 협상을 디버깅합니다.
- debug crypto ipsec - IPsec SA 협상을 디버깅합니다.

VPN 3000 Concentrator 문제 해결

Cisco 라우터의 debug 명령과 마찬가지로 모든 경보를 표시하도록 이벤트 클래스를 구성할 수 있습니다.Configuration **> System > Events > Classes > Add를 선택하여** 이벤트 클래스 로깅을 설정합니다.

Monitoring **> Filterable Event Log를 선택하여 활성화된** 이벤트를 모니터링합니다.



PFS

IPsec 협상에서 PFS(Perfect Forward Secrecy)는 각 새 암호화 키가 이전 키와 관련이 없도록 합니

다.두 터널 피어에서 PFS를 활성화 또는 비활성화하십시오. 그렇지 않으면 PIX/ASA에서 LAN-to-LAN(L2L) IPsec 터널이 설정되지 않습니다.

PFS는 기본적으로 비활성화되어 있습니다.PFS를 활성화하려면 그룹 정책 컨피그레이션 모드에서 enable **키워드**와 함께 pfs 명령을 사용합니다.PFS를 비활성화하려면 disable 키워드**를 *입력합니다*.**

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

실행 중인 컨피그레이션에서 PFS 특성을 제거하려면 이 명령의 **no** 형식을 입력합니다.그룹 정책은 다른 그룹 정책에서 PFS에 대한 값을 상속할 수 있습니다.값 상속을 방지하려면 이 명령의 **no** 형식을 입력합니다.

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

관련 정보

- Cisco PIX 500 Series 보안 어플라이언스 - 지원 페이지
- Cisco VPN 3000 Series Concentrator - 지원 페이지
- Cisco PIX 500 Series Security Appliance 명령 참조
- 기술 지원 및 문서 – Cisco Systems