필터 및 RADIUS 필터 할당을 사용하여 차단을 위한 Cisco VPN 3000 Concentrator 구성

목차

소개

이 샘플 컨피그레이션에서는 필터를 사용하여 사용자가 네트워크 내에서 하나의 서버(10.1.1.2)에만 액세스하고 다른 모든 리소스에 대한 액세스를 차단하도록 허용하고자 합니다. Cisco VPN 3000 Concentrator는 필터를 사용하여 네트워크 리소스에 대한 IPsec, PPTP(Point-to-Point Tunneling Protocol) 및 L2TP 클라이언트 액세스를 제어하도록 설정할 수 있습니다. 필터는 라우터의 액세스 목록과 유사한 규칙으로 구성됩니다. 라우터가 구성된 경우:

```
access-list 101 permit ip any host 10.1.1.2
access-list 101 deny ip any any
```

VPN Concentrator는 규칙을 사용하여 필터를 설정하는 것과 같습니다.

첫 번째 VPN Concentrator 규칙은 **permit_server_rule**이며, 이는 라우터의 permit ip any **host 10.1.1.2** 명령과 같습니다. 두 번째 VPN Concentrator 규칙은 **deny_server_rule**이며 이는 라우터의 deny ip any 명령과 같습니다.

VPN Concentrator 필터는 **filter_with_2_rules**이며, 라우터의 101 액세스 목록과 같습니다. permit_**server_rule** 및 **deny_server_rule**(그 순서대로)을 사용합니다. 필터를 추가하기 전에 클라이언트가 제대로 연결할 수 있다고 가정합니다. VPN Concentrator의 풀에서 IP 주소를 수신합니다.

PIX/ASA 7.x ASDM을 참조하십시오. PIX/ASA 7.x가 VPN 사용자의 액세스를 차단하는 시나리오에 대해 자세히 알아보려면 Network Access of Remote Access VPN Users(원격 액세스 VPN 사용자의 네트워크 액세스)를 제한합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

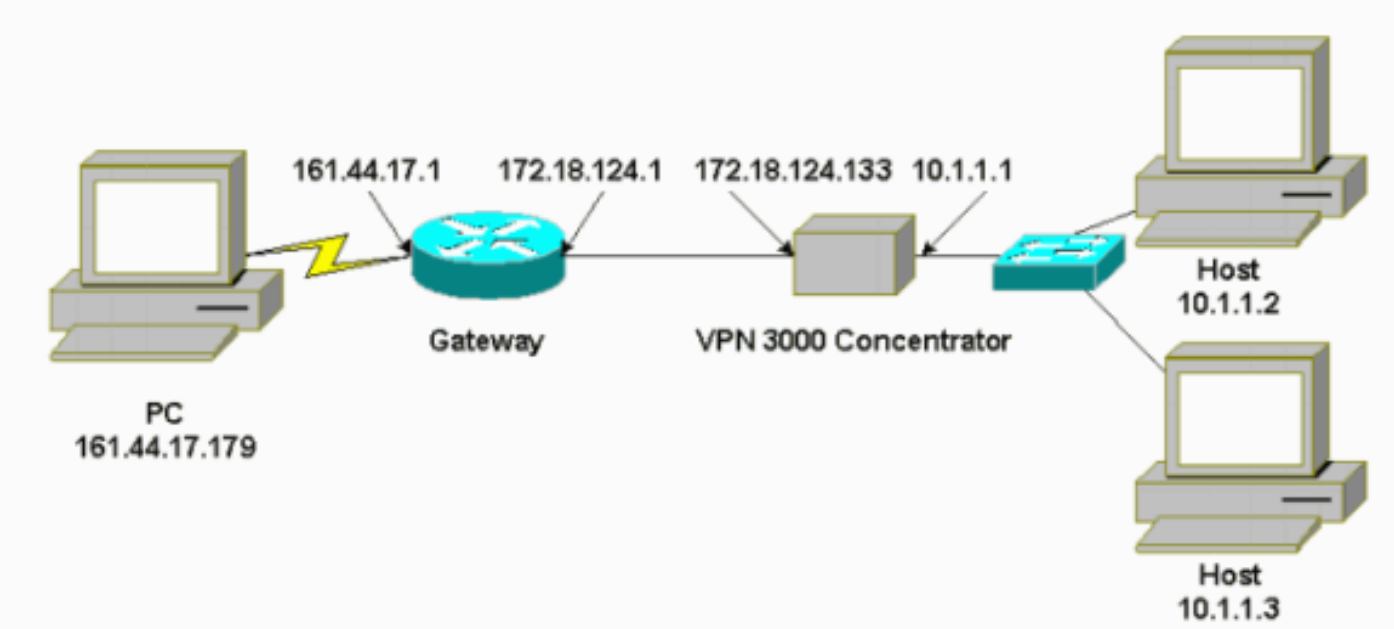
사용되는 구성 요소

이 문서의 정보는 Cisco VPN 3000 Concentrator 버전 2.5.2.D를 기반으로 합니다.

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.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



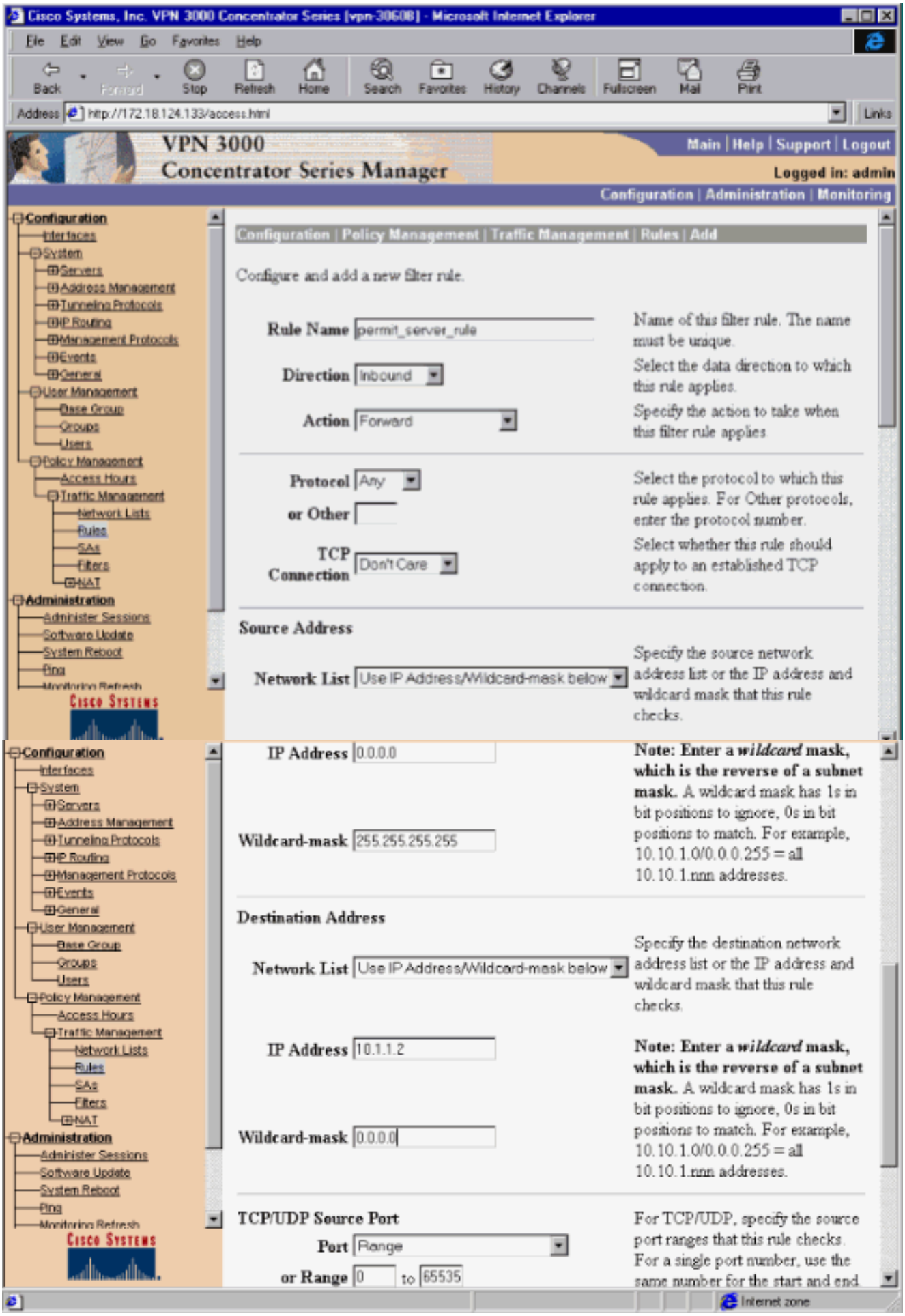
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

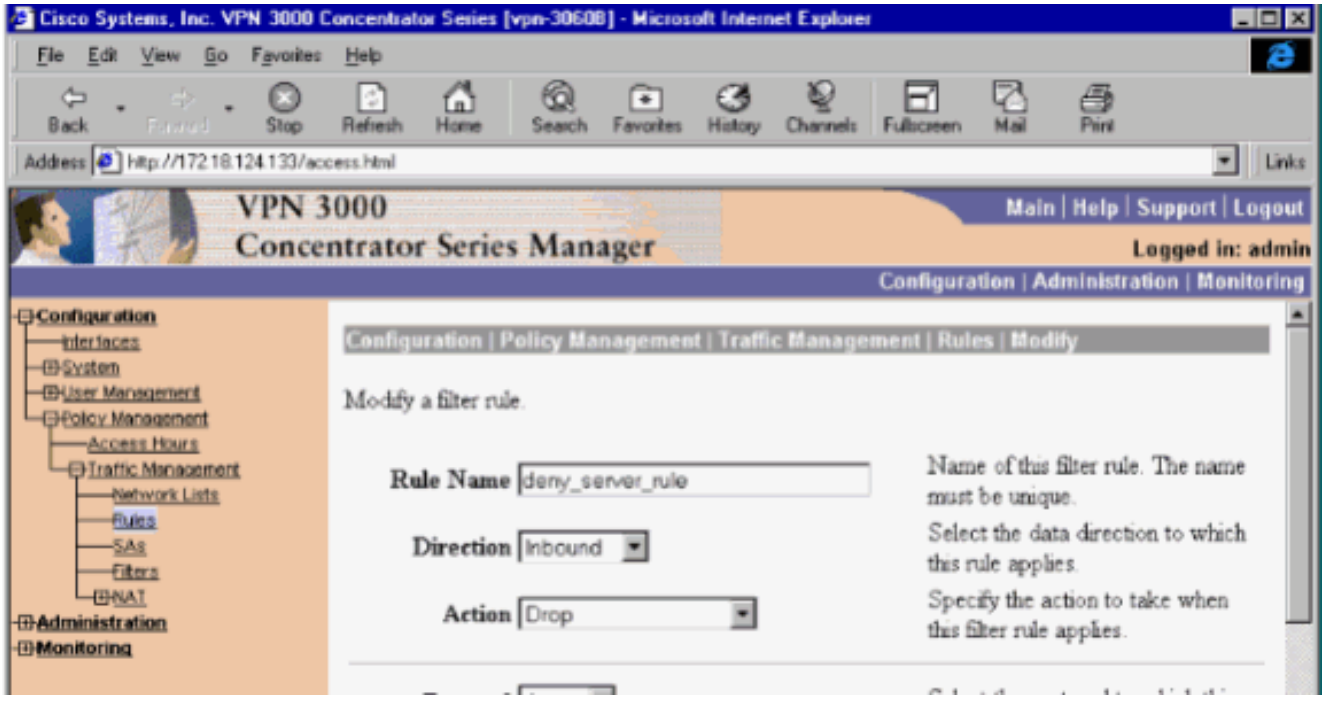
VPN 3000 구성

VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

1. Configuration(**구성) >Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Rules(규칙) > Add(추가)를** 선택하고 다음 설정으로 **permit_server_rule**이라는 첫 번째 VPN Concentrator 규칙을 정의합니다.방향 - **인바운드**작업 - **전달**소스 주소 - **255.255.255.255**대상 주소 - **10.1.1.2**와일드카드 마스크 - **0.0.0.0**

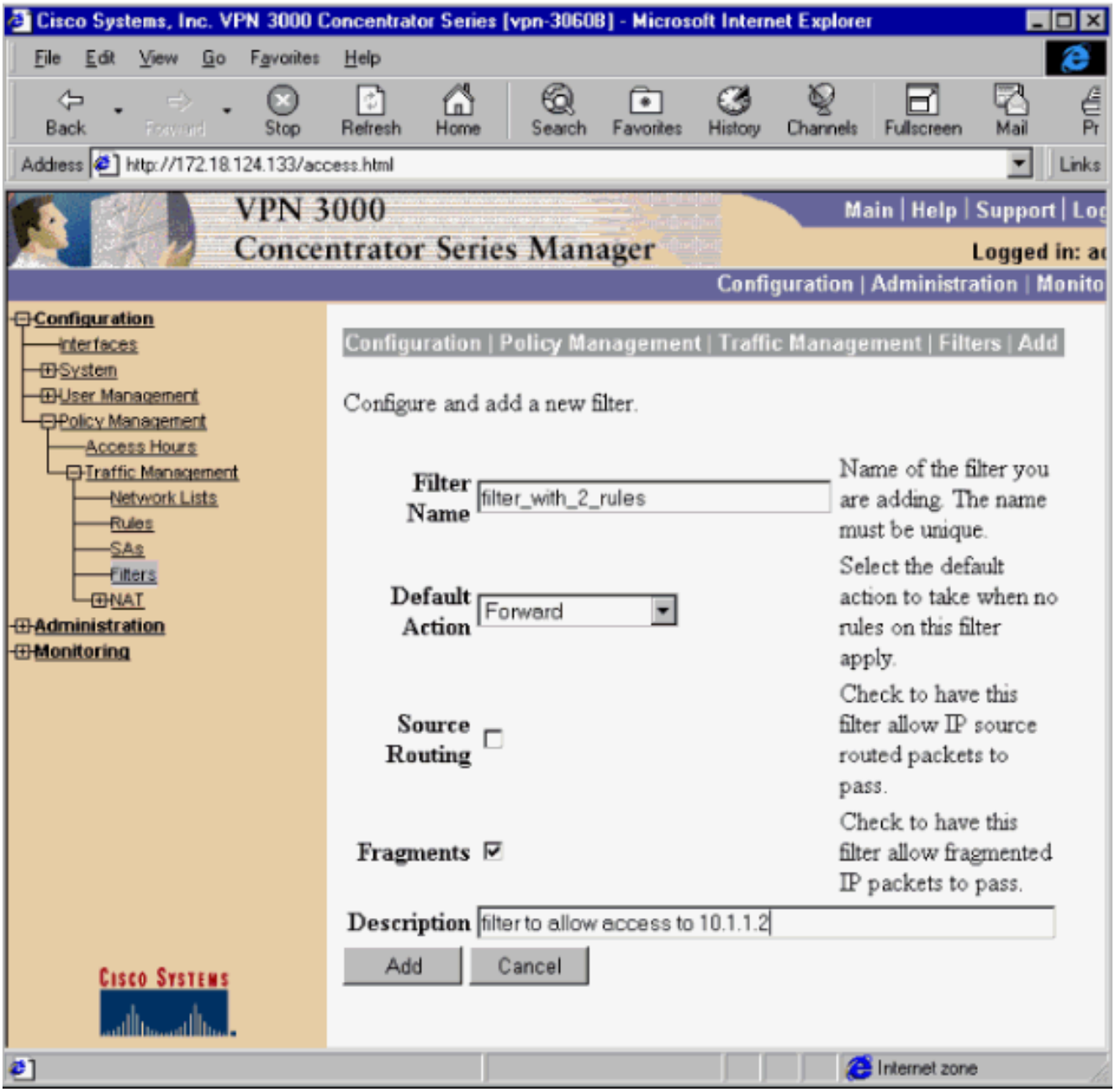


2. 동일한 영역에서 다음 기본값으로 deny_**server_rule**이라는 두 번째 VPN Concentrator 규칙을 정의합니다.방향 - **인바운드**작업 - **삭제**모든 항목의 소스 및 대상 주소 (255.255.255.255):



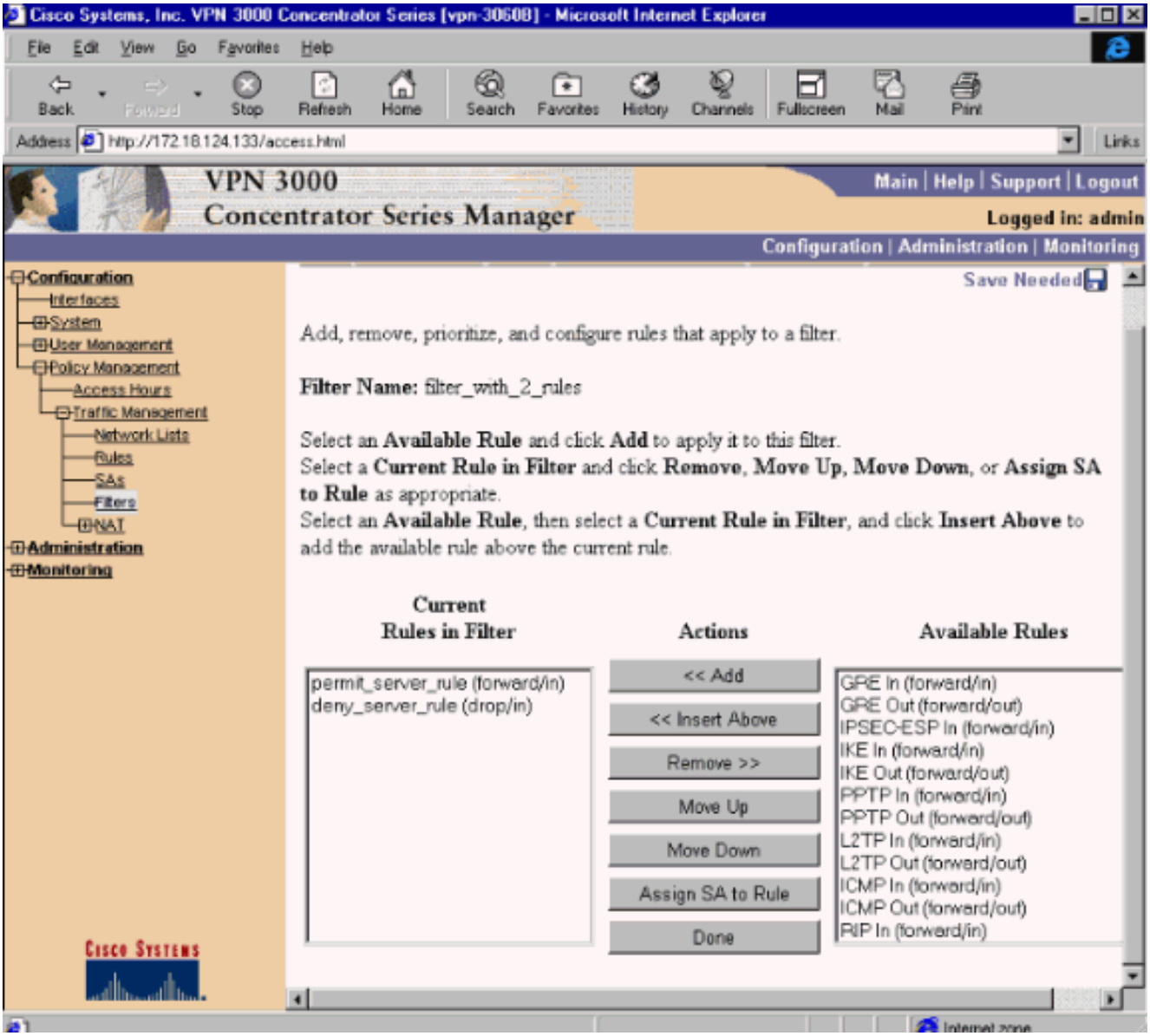
3. Configuration **> Policy Management > Traffic Management > Filters를 선택하고 filter_with_2_rules** 필터를 추가합니다

.



4. filter_with_2_rules에 두 규칙을 추가합니다

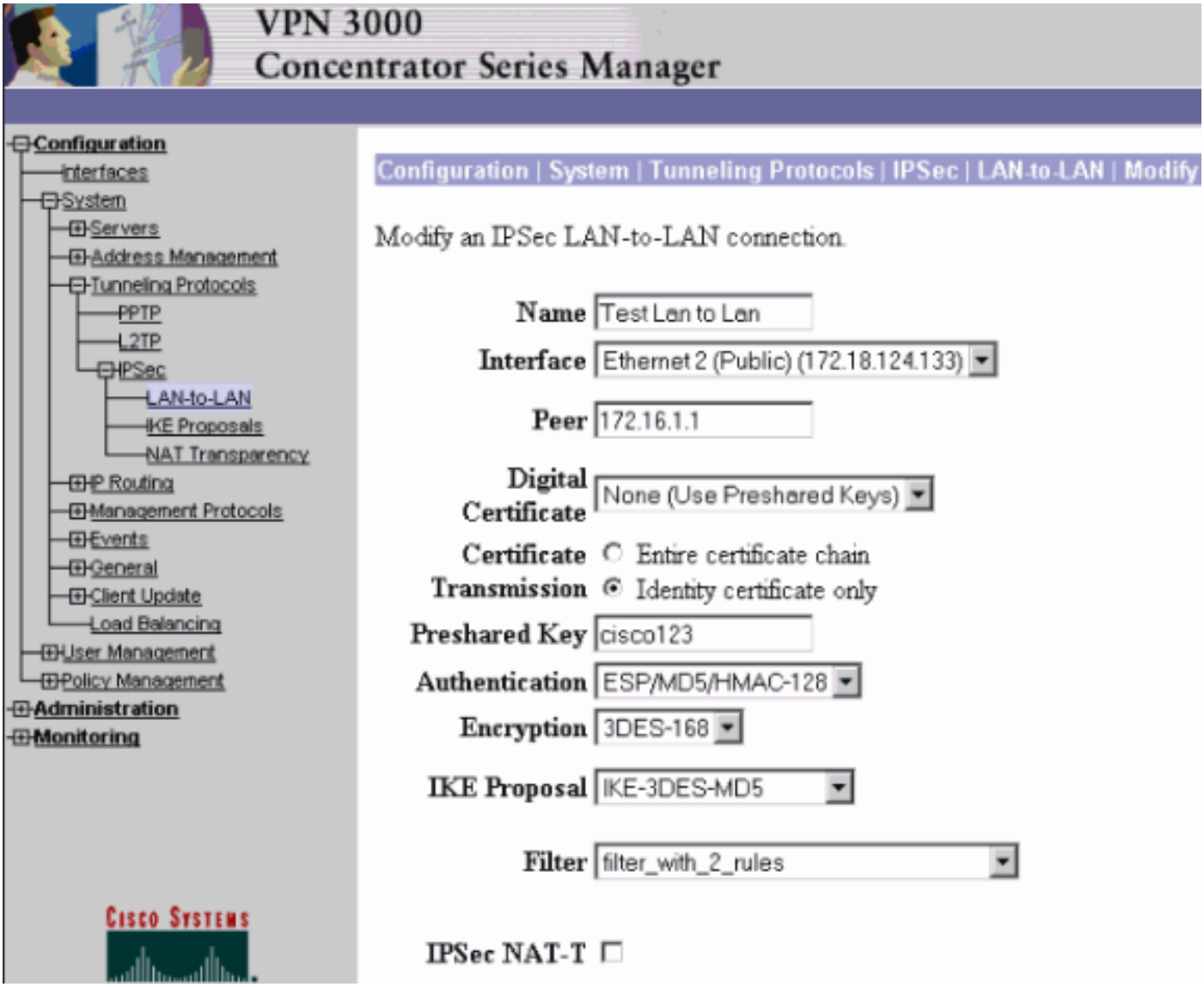
.



5. Configuration **> User Management > Groups**를 선택하고 그룹에 필터를 적용합니다
.

LAN-to-LAN VPN 터널용 필터

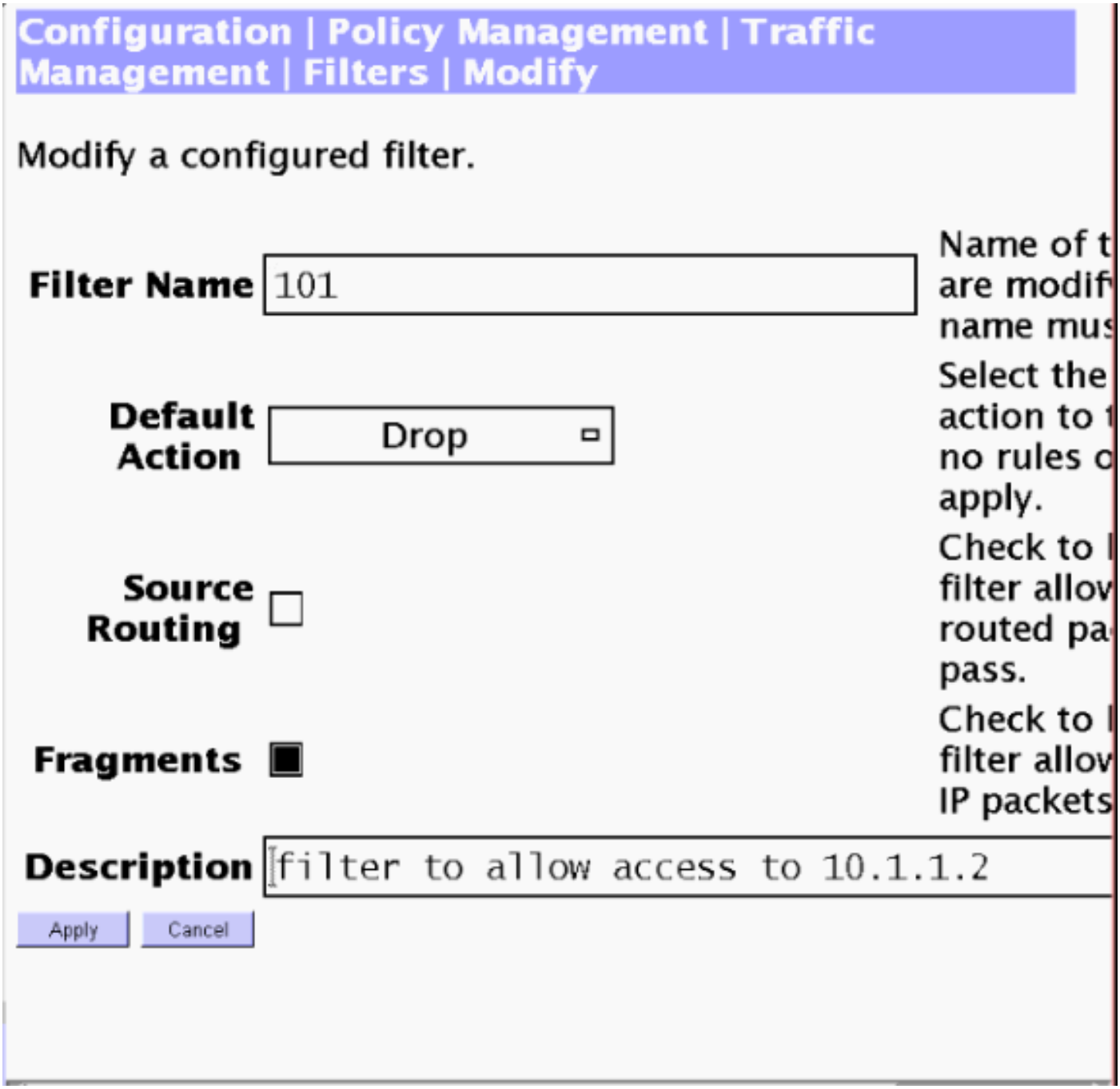
VPN Concentrator 코드 3.6 이상에서 각 LAN-to-LAN IPsec VPN 터널에 대한 트래픽을 필터링할 수 있습니다. 예를 들어, 172.16.1.1 주소를 사용하여 다른 VPN Concentrator에 LAN-to-LAN 터널을 구축하고 다른 모든 트래픽을 거부하는 동시에 호스트 10.1.1.2 터널 액세스를 허용하려는 경우 Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec > LAN-to-LAN > Modify(수정)를 선택하고 **Filter(필터)** 아래에서 filter_with_2_rules를 선택할 수 있습니다.



VPN 3000 구성 - RADIUS 필터 할당

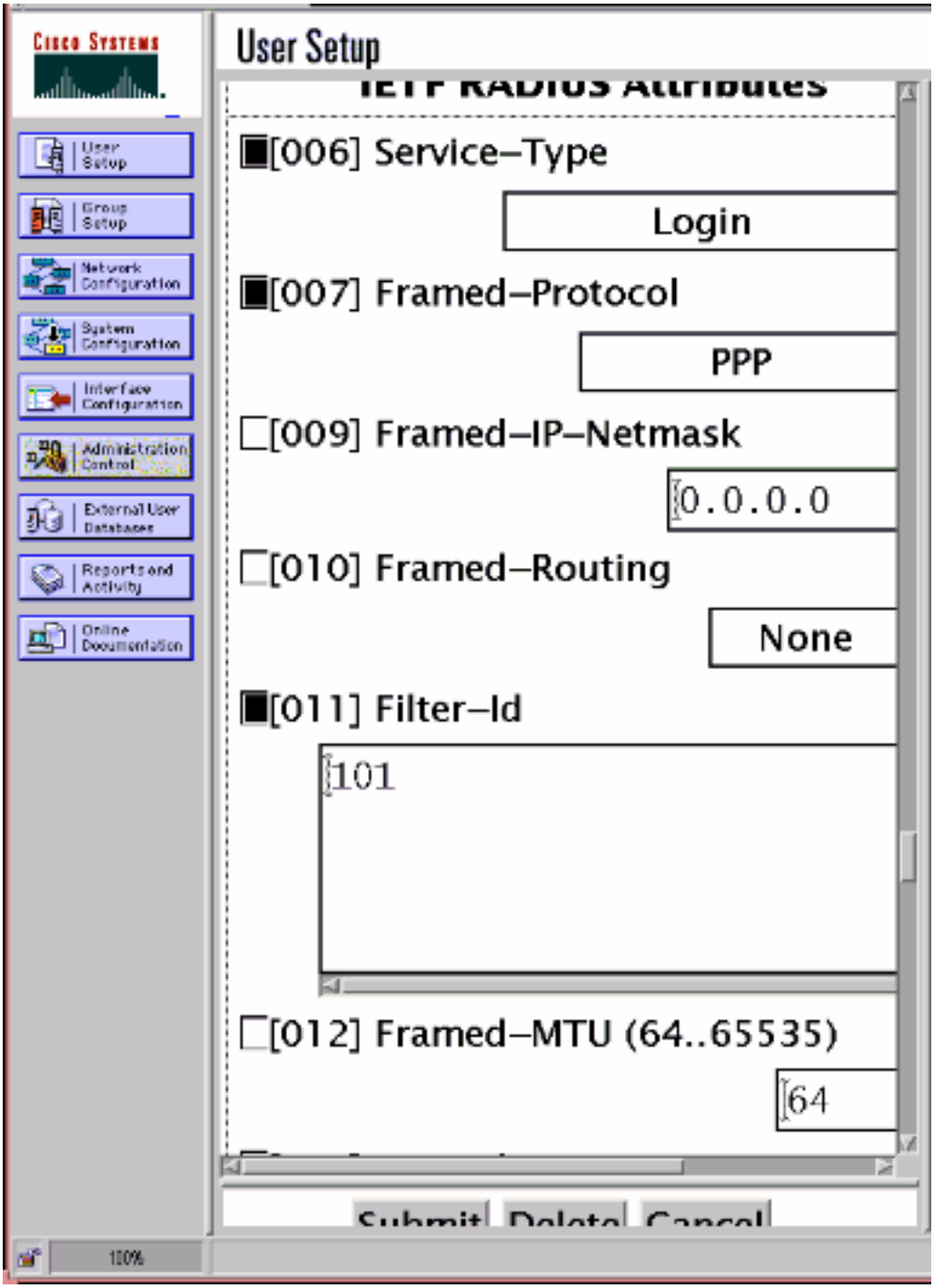
또한 VPN Concentrator에서 필터를 정의한 다음 RADIUS 서버에서 필터 번호(RADIUS 용어로 특성 11은 필터 ID)를 전달하여 사용자가 RADIUS 서버에서 인증되면 필터 ID가 해당 연결과 연결될 수 있습니다. 이 예에서는 VPN Concentrator 사용자에 대한 RADIUS 인증이 이미 작동 중이며 Filter-id만 추가되어야 한다고 가정합니다.

이전 예와 같이 VPN Concentrator에서 필터를 정의합니다.



CSNT 서버 구성 - RADIUS 필터 할당

Cisco Secure NT 서버에서 특성 11, Filter-id를 **101로 구성합니다**.



디버그 - RADIUS 필터 할당

AUTHDECODE(1-13 Severity)가 VPN Concentrator에 있는 경우, 로그에 Cisco Secure NT 서버가 11(0x0B) 특성:

```
207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=228
0000: 020C002B 768825C5 C29E439F 4C8A727A     ...+v.%...C.L.rz
0010: EA7606C5 06060000 00020706 00000001     .v..............
0020: 0B053130 310806FF FFFFFF                   ..101......
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

문제 해결 목적으로만, **구성 > 시스템 > 이벤트 > 클래스**를 선택하고 **심각도 = 13**인 FILTERDBG 클래스**를** 로그**에** 추가할 수 있습니다. 규칙에서 기본 작업을 전달(또는 삭제)에서 전달 및 **로그**(또는 삭제 및 로그)로 변경합니다. 이벤트 로그가 Monitoring(모니터링) **> Event Log(이벤트 로그)**에서 검색되면 다음과 같은 항목이 표시되어야 합니다.

```
221 12/21/2000 14:20:17.190 SEV=9 FILTERDBG/1 RPT=62
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8

222 12/21/2000 14:20:18.690 SEV=9 FILTERDBG/1 RPT=63
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

관련 정보

- IPSec 협상/IKE 프로토콜
- VPN 3000 Concentrator FAQ
- RADIUS 지원
- Cisco VPN 3000 Concentrator 지원
- Cisco VPN 3000 클라이언트 지원
- Windows용 Cisco Secure ACS 지원
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems