VPN 3000 Concentrator 대역폭 관리 컨피그레이션 예

목차

소개

이 문서에서는 Cisco VPN 3000 Concentrator에서 대역폭 관리 기능을 구성하는 데 필요한 단계를 설명합니다.

- Site-to-Site(LAN-to-LAN) VPN 터널
- 원격 액세스 VPN 터널

참고: 원격 액세스 또는 Site-to-Site VPN 터널을 구성하기 전에 먼저 VPN 3000 Concentrator에서 기본 대역폭 정책을 구성해야 합니다.

대역폭 관리의 두 가지 요소는 다음과 같습니다.

- **Bandwidth Policing**(대역폭 폴리싱) - 터널링된 트래픽의 최대 속도를 제한합니다.VPN Concentrator는 이 속도 아래로 수신되는 트래픽을 전송하고 이 속도를 초과하는 트래픽을 삭제합니다.
- **Bandwidth Reservation(대역폭 예약)** - 터널링된 트래픽에 대한 최소 대역폭 속도를 설정합니다.Bandwidth Management를 사용하면 그룹 및 사용자에게 균등하게 대역폭을 할당할 수 있습니다.이렇게 하면 특정 그룹 또는 사용자가 대역폭의 대부분을 소비하지 않습니다.

대역폭 관리는 터널링된 트래픽(L2TP[Layer 2 Tunnel Protocol], PPTP[Point to Point Tunneling Protocol], IPSec)에만 적용되며 공용 인터페이스에 가장 일반적으로 적용됩니다.

대역폭 관리 기능은 원격 액세스 및 사이트 간 VPN 연결에 대한 관리 혜택을 제공합니다.원격 액세스 VPN 터널은 대역폭 폴리싱을 사용하므로 광대역 사용자가 모든 대역폭을 사용하지 않습니다.반대로 관리자는 사이트 간 터널에 대한 대역폭 예약을 구성하여 각 원격 사이트에 대한 최소 대역폭 양을 보장할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

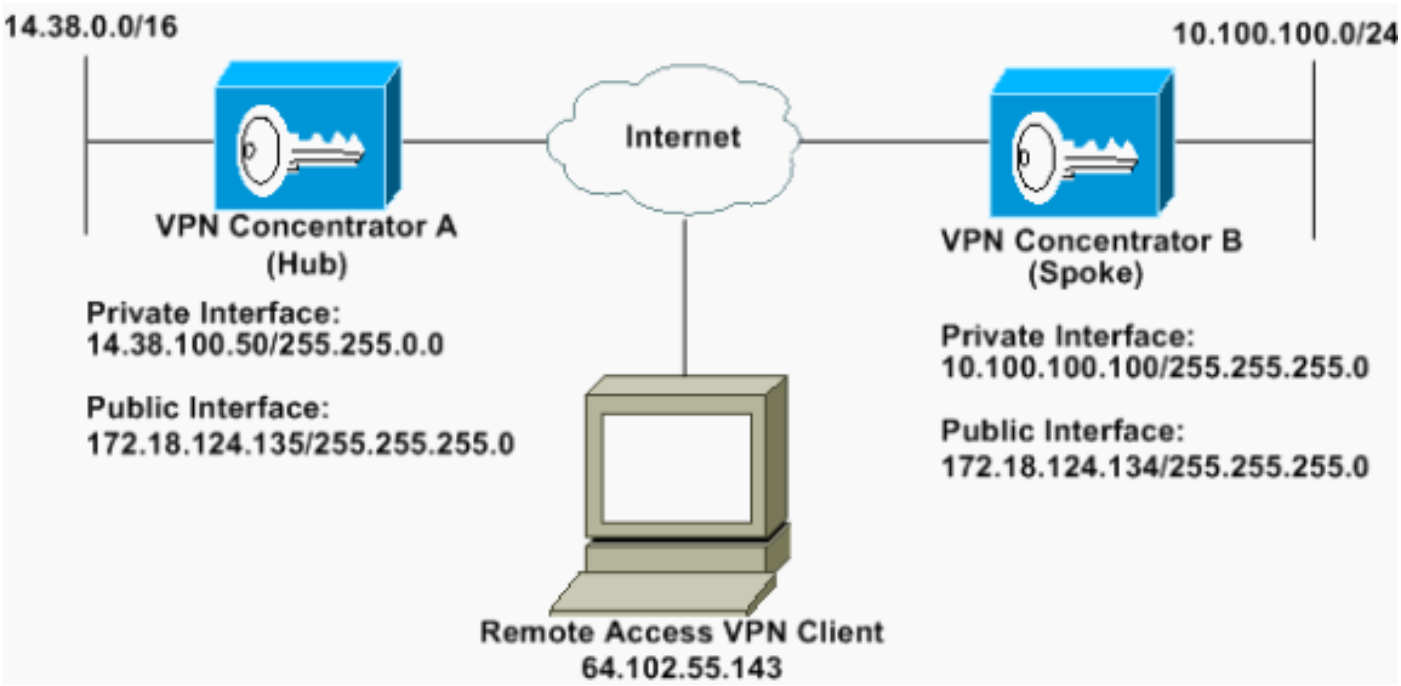
- Cisco VPN 3000 Concentrator with Software 릴리스 4.1.x 이상

참고: 대역폭 관리 기능은 릴리스 3.6에서 도입되었습니다.

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 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

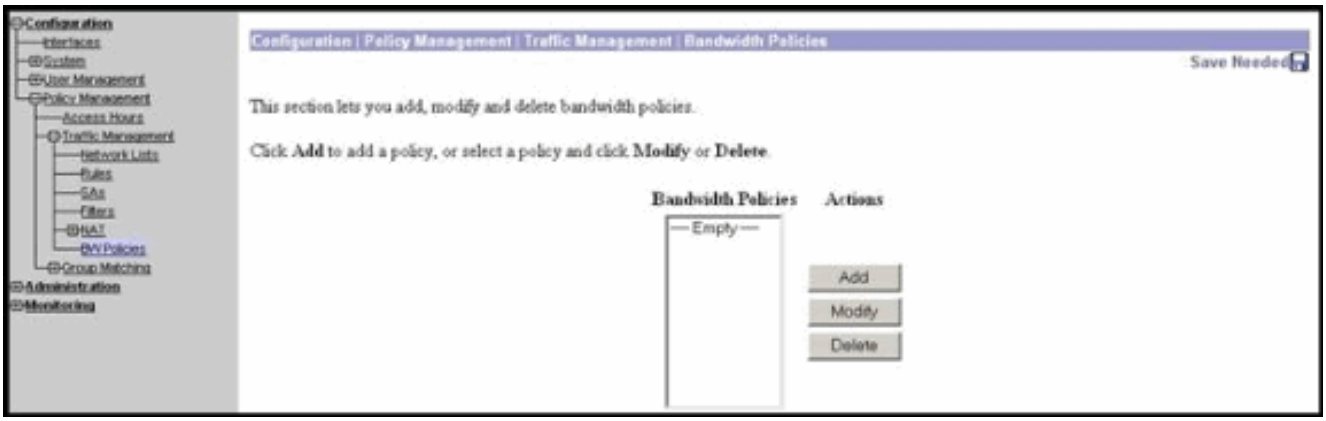
VPN 3000 Concentrator에서 기본 대역폭 정책 구성

LAN-to-LAN 터널 또는 원격 액세스 터널에서 대역폭 관리를 구성하려면 먼저 공용 인터페이스에서 대역폭 관리를 활성화해야 합니다.이 샘플 컨피그레이션에서는 기본 대역폭 정책이 구성됩니다.이 기본 정책은 VPN Concentrator에 속한 그룹에 대역폭 관리 정책이 적용되지 않은 사용자/터널에 적

용됩니다.

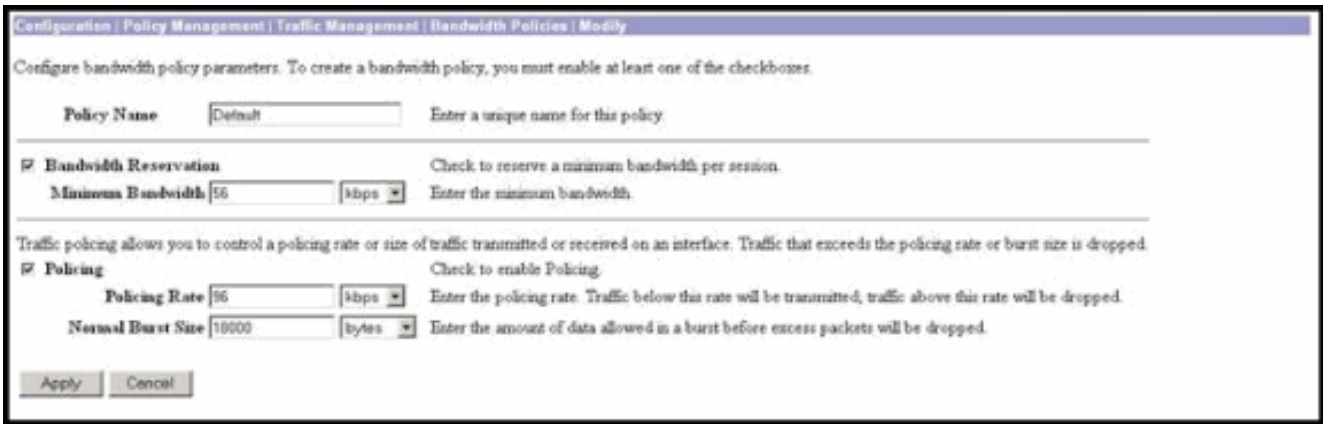
1. 정책을 구성하려면 Configuration(컨피그레이션) **> Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Bandwidth Policies(대역폭 정책)를** 선택하고 **Add(추가)**를 클릭합니다

.



추가를 클릭하면 수정 창이 표시됩니다

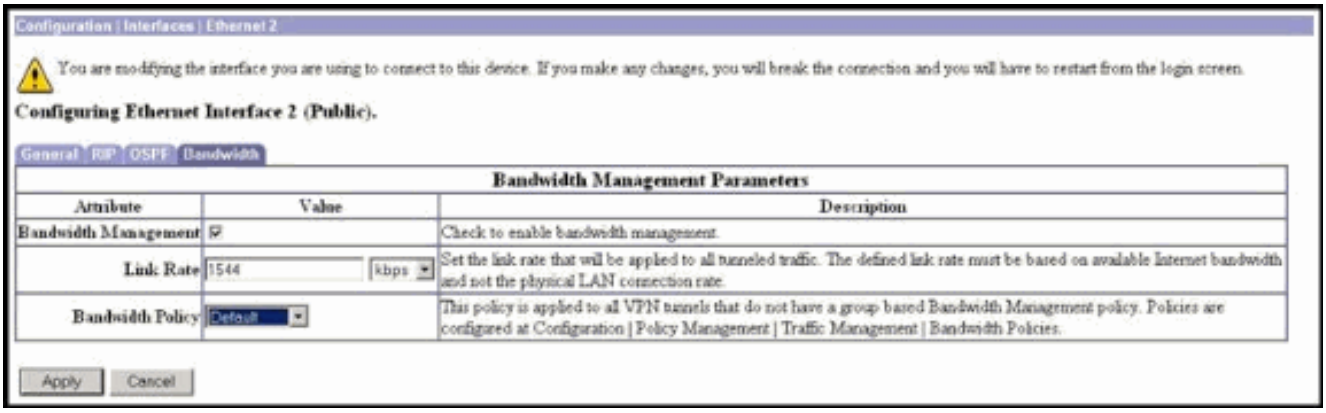
.



2. 수정 창에서 이러한 매개변수를 설정합니다.**Policy Name(정책 이름**) - 정책을 기억하도록 도와주는 고유한 정책 이름을 입력합니다.최대 길이는 32자입니다.이 예에서 이름 'Default'는 정책 이름으로 구성됩니다.**Bandwidth Reservation**(대역폭 예약) - **Bandwidth Reservation(대역폭 예약)** 확인란을 선택하여 각 세션에 대한 최소 대역폭 양을 예약합니다.이 예에서는 대역폭 관리가 구성된 그룹에 속하지 않는 모든 VPN 사용자에 대해 56kbps의 대역폭이 예약됩니다.**Policing**(폴리싱) - 폴리싱을 활성화하려면 Policing(폴리싱) 확인란을 선택합니다.폴리싱 비율 값을 입력하고 측정 단위를 선택합니다.VPN Concentrator는 폴리싱 속도 아래로 이동하는 트래픽을 전송하고 폴리싱 속도 이상으로 이동하는 모든 트래픽을 삭제합니다.대역폭 폴리싱에 96kbps가 구성됩니다.일반 버스트 크기는 VPN Concentrator가 지정된 시간에 전송할 수 있는 순간 버스트의 양입니다.버스트 크기를 설정하려면 다음 공식을 사용합니다.
   `(Policing Rate/8) * 1.5`
   이 공식을 사용하면 버스트 속도는 18000바이트입니다.
3. Apply를 **클릭합니다**.
4. Configuration **> Interfaces > Public Interface**를 선택하고 Bandwidth 탭을 클릭하여 인터페이스에 기본 대역폭 정책을 적용합니다.
5. **Bandwidth Management** 옵션을 활성화합니다.
6. 링크 속도를 지정합니다.연결 속도는 인터넷을 통한 네트워크 연결 속도입니다.이 예에서는 인터넷에 대한 T1 연결이 사용됩니다.따라서 1544kbps가 구성된 링크 속도입니다.
7. Bandwidth Policy 드롭다운 목록에서 정책을 선택합니다.이 인터페이스에 대해 기본 정책이 이전에 구성됩니다.여기서 적용하는 정책은 이 인터페이스의 모든 사용자에 대한 기본 대역폭

정책입니다.이 정책은 해당 그룹에 대역폭 관리 정책이 적용되지 않은 사용자에게 적용됩니다

.

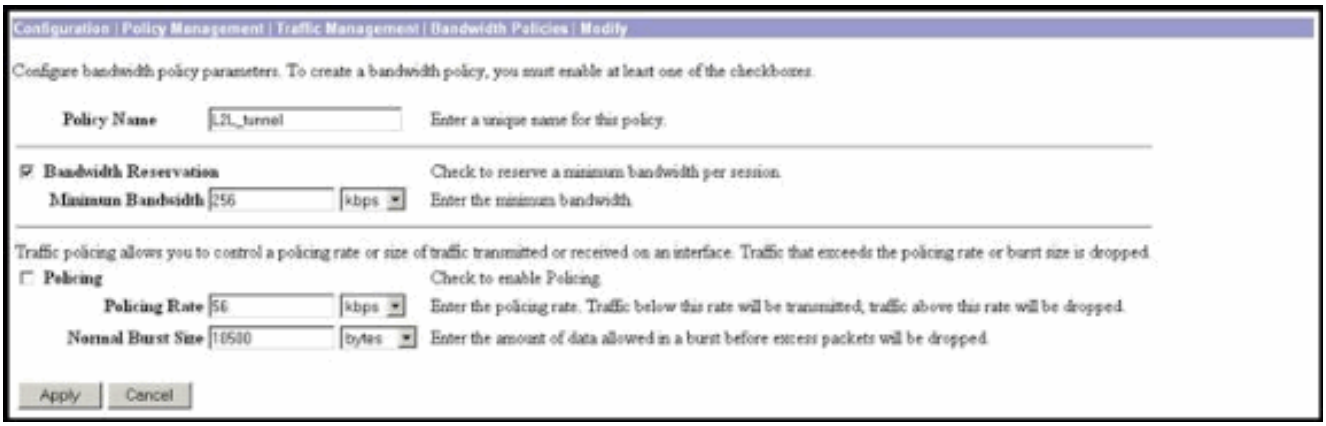


사이트 간 터널에 대한 대역폭 관리 구성

사이트 간 터널에 대한 대역폭 관리를 구성하려면 다음 단계를 완료합니다.

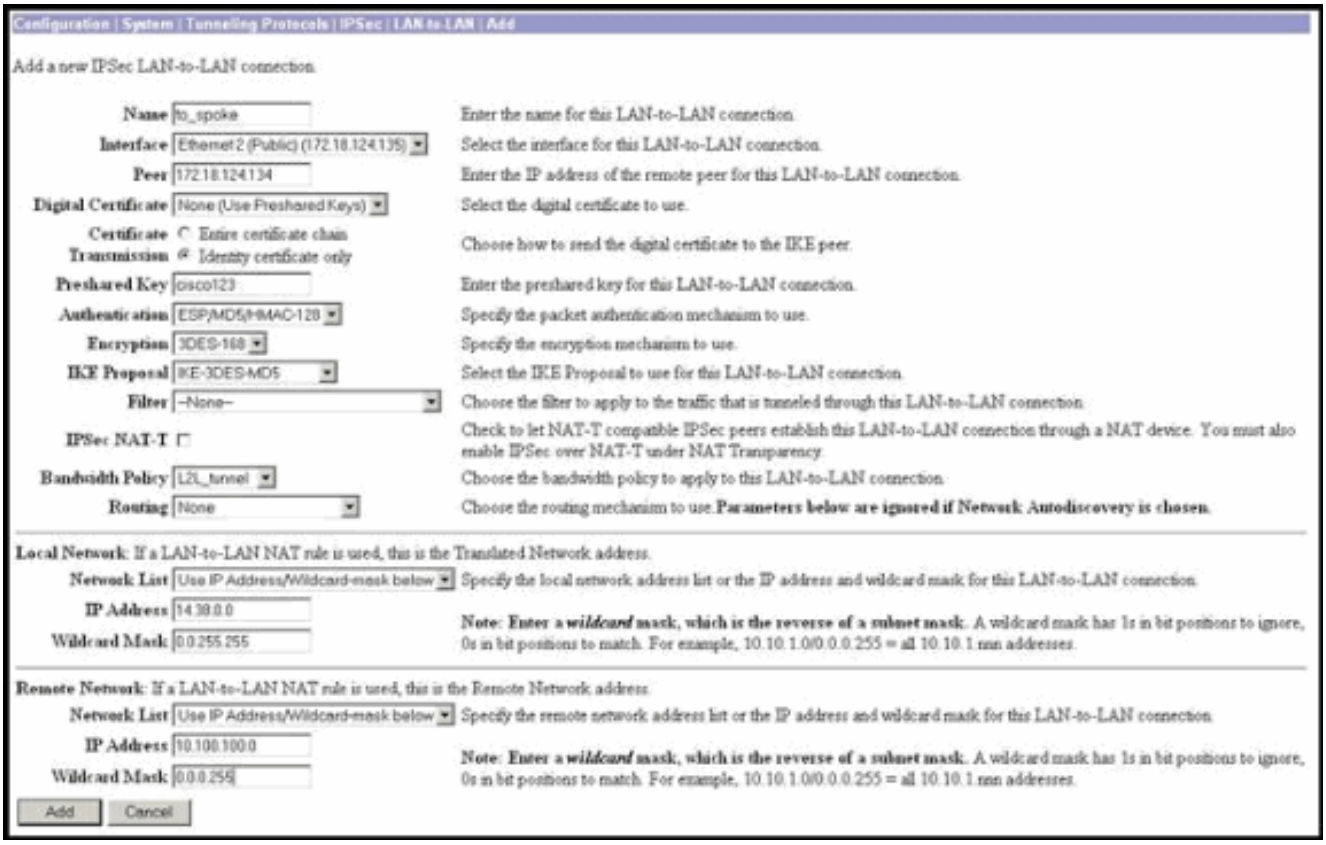
1. Configuration **> Policy Management > Traffic Management > Bandwidth Policies**를 선택하고 **Add**를 클릭하여 새 LAN-to-LAN 대역폭 정책을 정의합니다.이 예에서 'L2L_tunnel'이라는 정책은 256kbps의 대역폭 예약을 사용하여 구성되었습니다

.



2. Bandwidth Policy(대역폭 정책) 드롭다운 메뉴에서 기존 LAN-to-LAN 터널에 대역폭 정책을 적용합니다

.

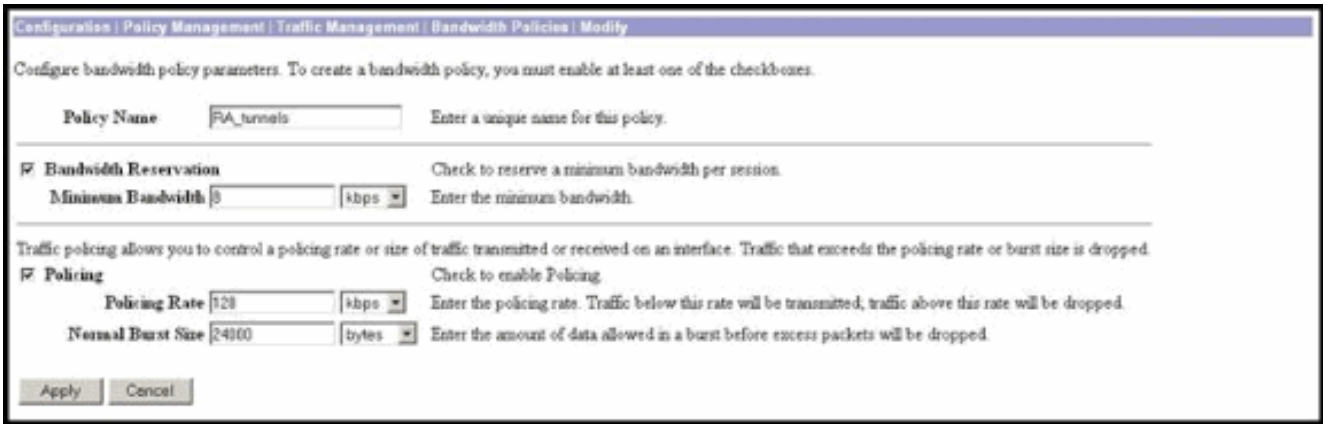


원격 VPN 터널에 대한 대역폭 관리 구성

원격 VPN 터널에 대한 대역폭 관리를 구성하려면 다음 단계를 완료합니다.

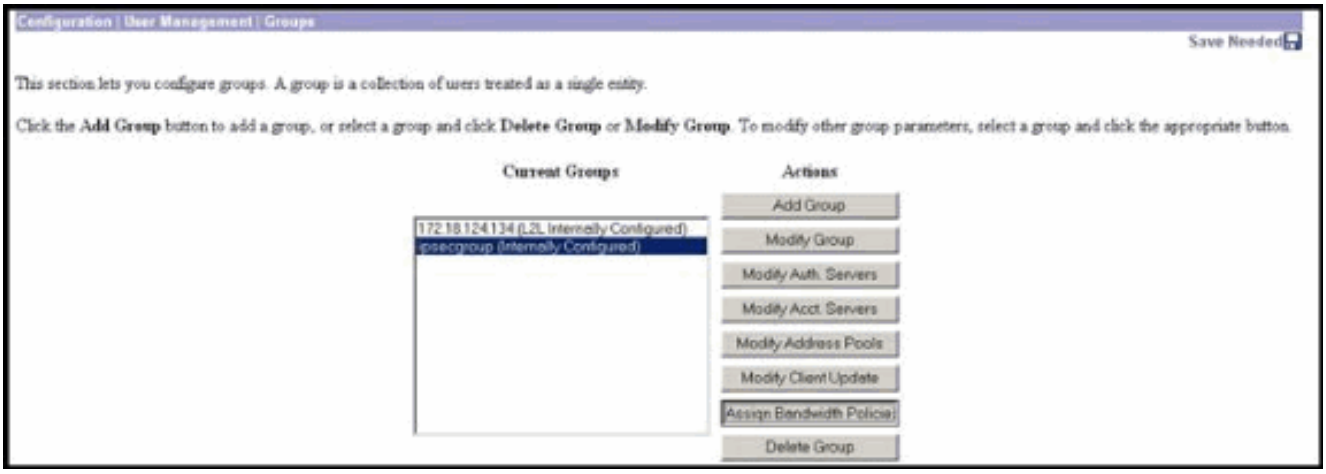
1. Configuration **> Policy Management > Traffic Management > Bandwidth Policies**를 선택하고 **Add**를 클릭하여 새 대역폭 정책을 생성합니다.이 예에서 'RA_tunnels'라는 정책은 8kbps의 대역폭 예약을 사용하여 구성됩니다.트래픽 폴리싱은 128kbps의 폴리싱 속도와 24,000바이트의 버스트 크기로 구성됩니다

.

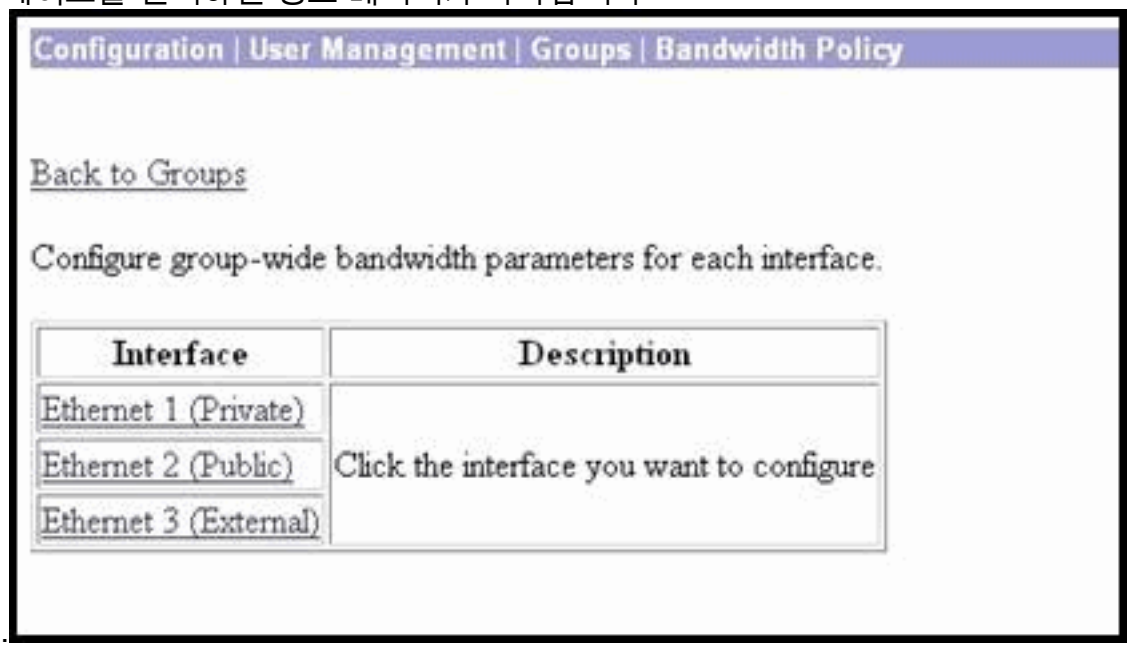


2. 원격 액세스 VPN 그룹에 대역폭 정책을 적용하려면 Configuration(구성) **> User Management(사용자 관리) > Groups(그룹)**를 선택하고 그룹을 선택한 다음 Assign Bandwidth Policies(**대역폭 정책 할당)를 클릭합니다**

.



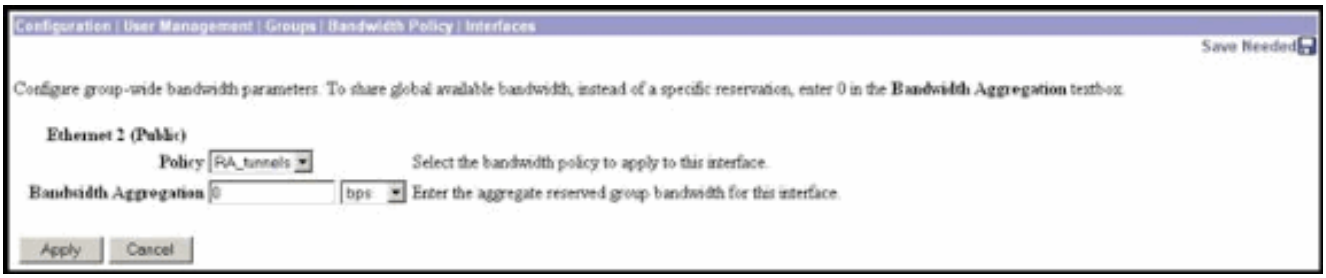
3. 이 그룹에 대한 대역폭 관리를 구성할 인터페이스를 클릭합니다.이 예에서 'Ethernet2 (Public)'는 그룹에 대해 선택된 인터페이스입니다.인터페이스의 그룹에 대역폭 정책을 적용하려면 해당 인터페이스에서 대역폭 관리를 활성화해야 합니다.대역폭 관리가 비활성화된 인터페이스를 선택하면 경고 메시지가 나타납니다



.

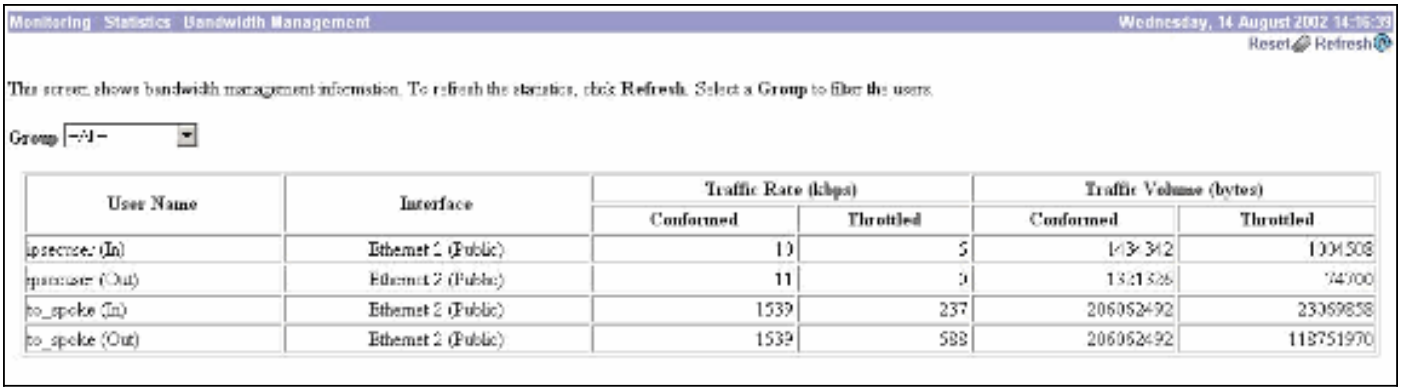
4. 이 인터페이스의 VPN 그룹에 대한 대역폭 정책을 선택합니다.이전에 정의된 RA_tunnels 정책이 이 그룹에 대해 선택됩니다.이 그룹에 대해 예약할 최소 대역폭 값을 입력합니다.대역폭 집계의 기본값은 0입니다. 기본 측정 단위는 bps입니다.그룹이 인터페이스에서 사용 가능한 대역폭을 공유하도록 하려면 **0**을 입력합니다

.



다음을 확인합니다.

Monitoring(**모니터링**) > **Statistics(통계)** > **Bandwidth Management** on the VPN 3000 Concentrator를 선택하여 Bandwidth Management(대역폭 관리)를 모니터링합니다.



문제 해결

VPN 3000 Concentrator에서 대역폭 관리가 구현되는 동안 문제를 해결하려면 Configuration(컨피그레이션) > System(시스템) > Events(이벤트) > Classes(클래스)에서 다음 두 **이벤트 클래스를 활성화합니다**.

- **BMGT**(기록할 심각도 포함:1-9)
- **BMGTDBG**(심각도:1-9)

다음은 가장 일반적인 이벤트 로그 메시지 중 일부입니다.

- 대역폭 이 수정되면 로그에 Exceeds the Aggregate Reservation 오류 메시지가 표시됩니다.

```
1 08/14/2002 10:03:10.840 SEV=4 BMGT/47 RPT=2
The Policy [ RA_tunnels ] with Reservation [ 8000 bps ] being
applied to Group [ipsecgroup ] on Interrface [ 2 ] exceeds
the Aggregate Reservation [ 0 bps ] configured for that group.
```

  이 오류 메시지가 표시되면 그룹 설정으로 돌아가 그룹에서 'RA_tunnel' 정책을 적용 취소합니다.올바른 값으로 'RA_tunnel'을 수정한 다음 정책을 다시 특정 그룹에 적용합니다.
- 인터페이스 대역폭을 찾을 수 없습니다.

```
11 08/14/2002 13:03:58.040 SEV=4 BMGTDBG/56 RPT=1
Could not find interface bandwidth policy 0 for group 1 interface 2.
```

  인터페이스에서 대역폭 정책이 활성화되지 않고 LAN-to-LAN 터널에 적용하려고 하면 이 오류가 발생할 수 있습니다.이 경우 VPN 3000 Concentrator 섹션에서 Configure a Default Bandwidth Policy에 설명된 대로 공용 인터페이스에 정책을 적용합니다.

관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 지원 페이지
- Technical Support - Cisco Systems