RV016, RV042, RV042G 및 RV082 VPN 라우터에 대한 IPv6 액세스 규칙 구성

목표

액세스 규칙은 라우터가 방화벽을 통과할 수 있는 트래픽을 결정하는 데 도움이 됩니다. 이렇게 하면 라우터에 보안을 추가할 수 있습니다.

이 문서에서는 RV016, RV042, RV042G 및 RV082 VPN 라우터에 IPv6 액세스 규칙을 추가하는 방법에 대해 설명합니다.

적용 가능한 디바이스

· RV016
· RV042
· RV042G
· RV082

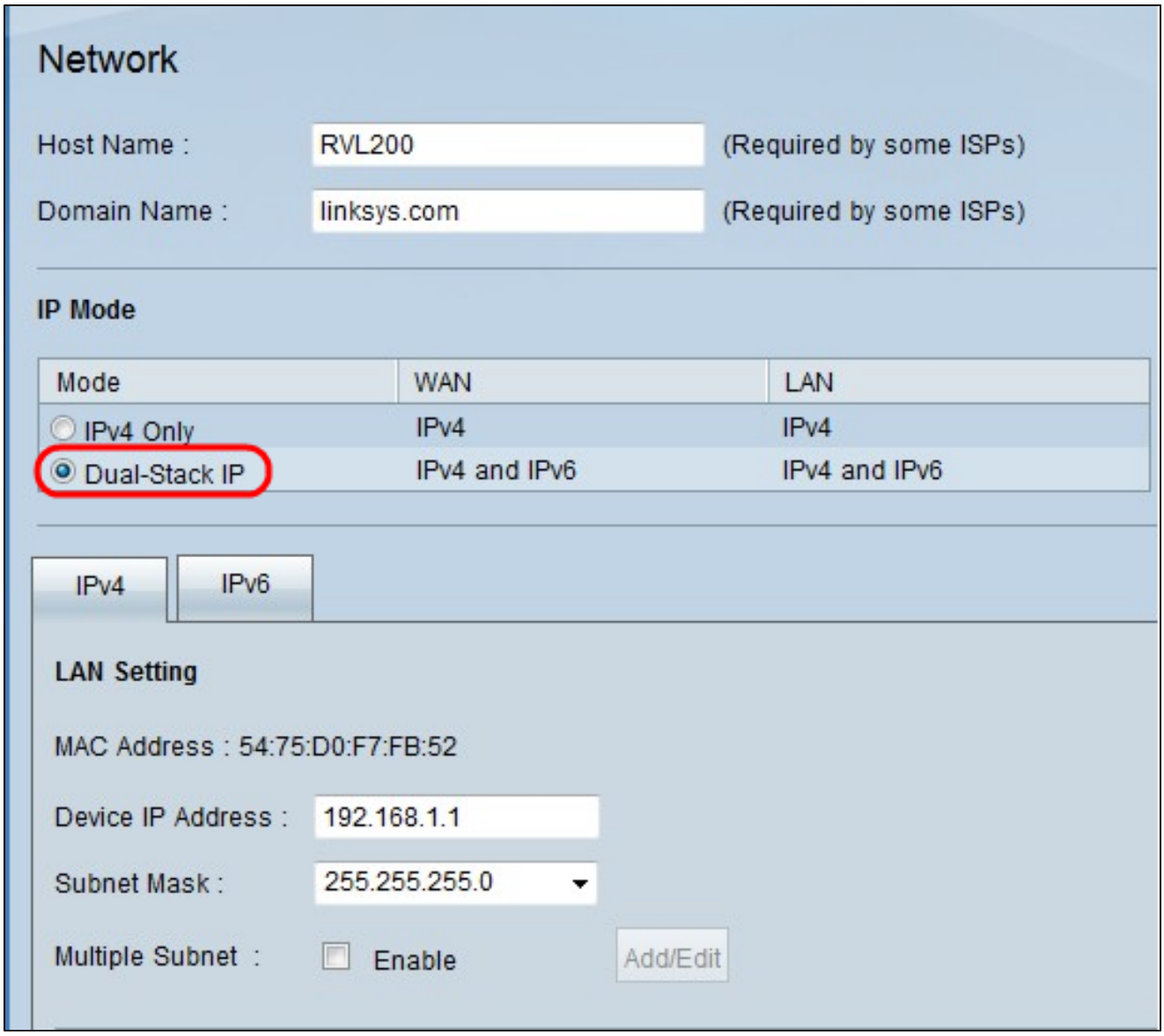
소프트웨어 버전

· v4.2.1.02

IPv6 액세스 규칙 컨피그레이션

IPv6 모드 활성화

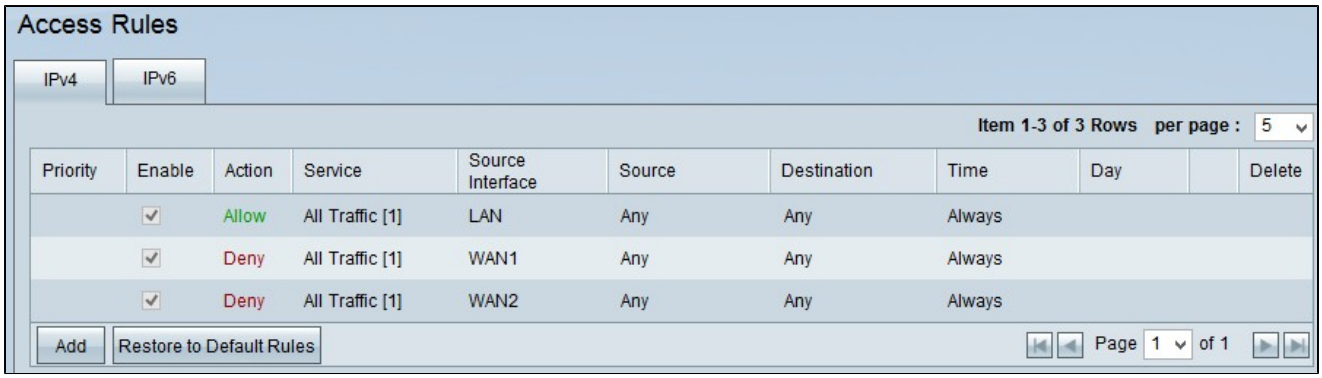
1단계. 웹 컨피그레이션 유틸리티에 로그인하고 Setup(설정) > Network(네트워크)를 선택합니다. Network(네트워크) 페이지가 열립니다.



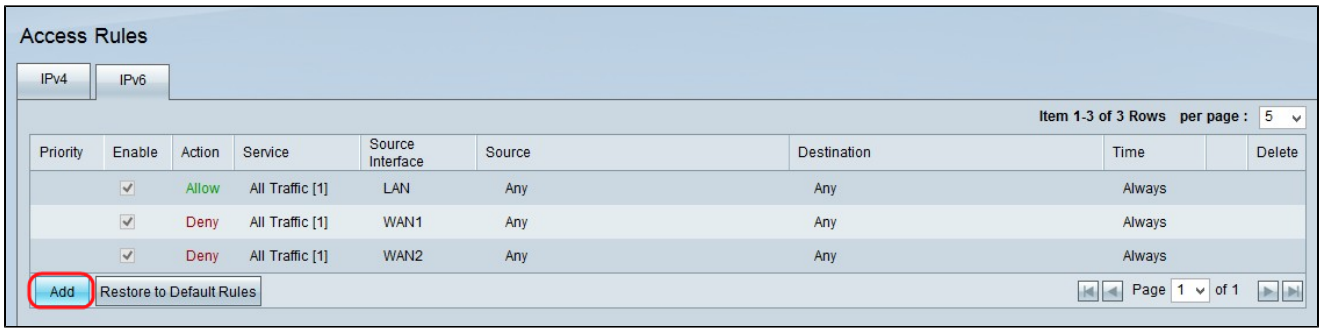
2단계. Dual-Stack IP 라디오 버튼을 클릭합니다. 이렇게 하면 IPv4와 IPv6를 동시에 실행할 수 있습니다. IPv6 통신이 가능한 경우 기본 통신입니다.

IPv6 액세스 규칙 컨피그레이션

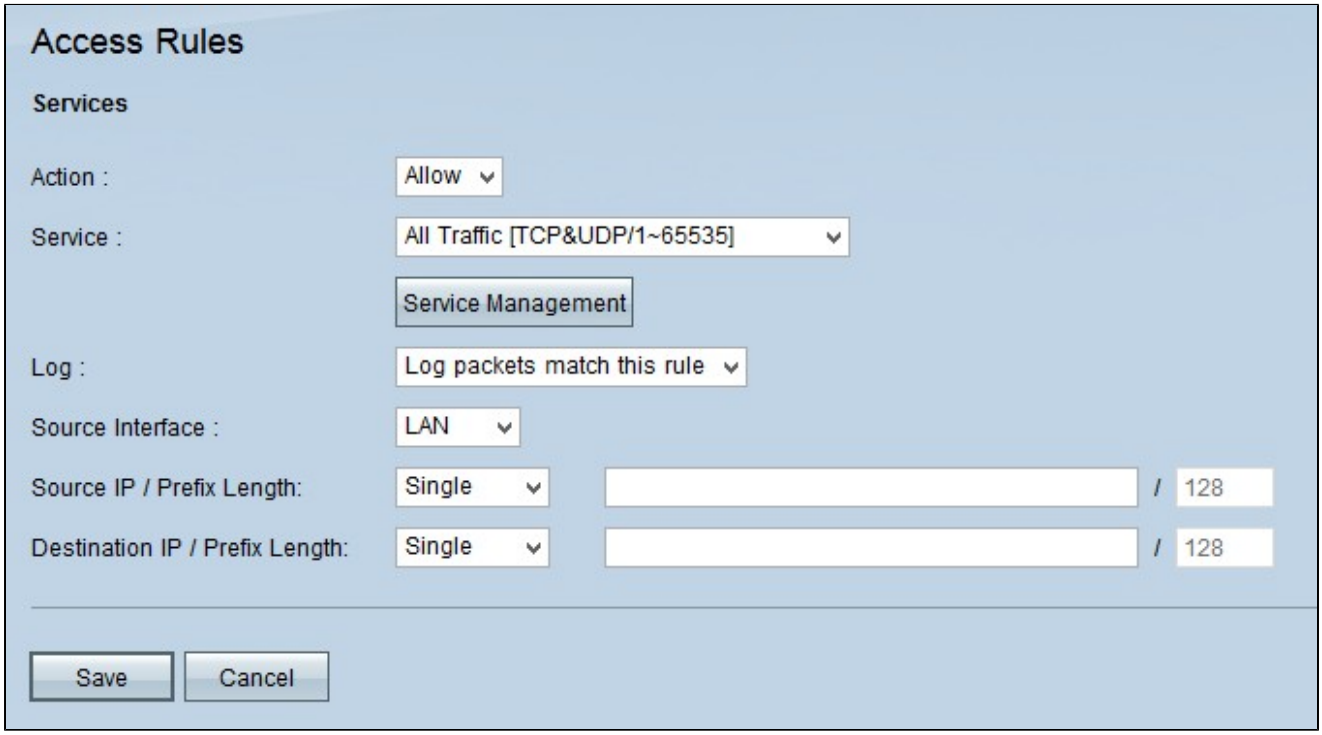
1단계. 웹 컨피그레이션 유틸리티에 로그인하고 Firewall(방화벽) > Access Rules(액세스 규칙)를 선택합니다. Access Rules 페이지가 열립니다.



2단계. IPv6 탭을 클릭합니다. 그러면 IPv6 Access Rules(IPv6 액세스 규칙) 페이지가 열립니다.



3단계. Add(추가)를 클릭하여 액세스 규칙을 추가합니다. IPv6에 대한 액세스 규칙을 구성하기 위해 Access Rules 페이지가 표시됩니다.

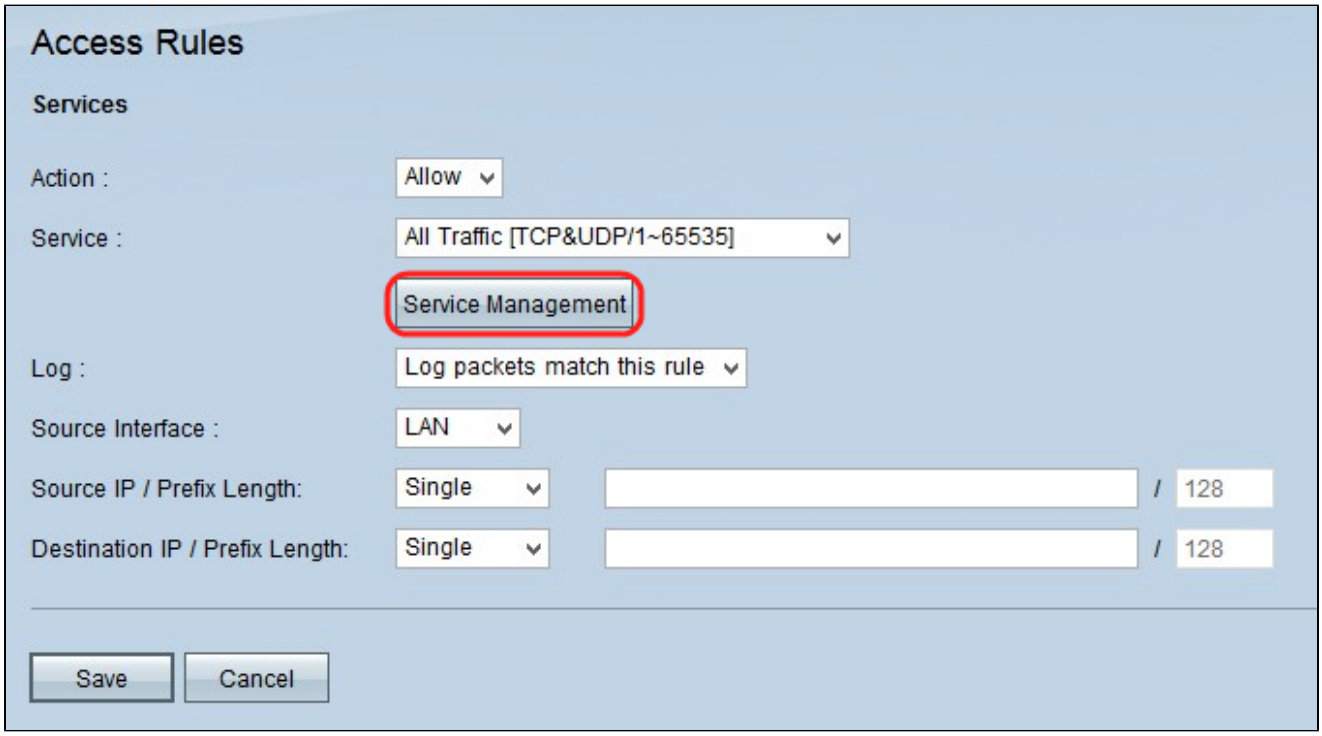


4단계. 트래픽을 허용하려면 Action(작업) 드롭다운 목록에서 Allow(허용)를 선택합니다. 트래

픽을 거부하려면 Deny를 선택합니다.

5단계. Service(서비스) 드롭다운 목록에서 적절한 서비스를 선택합니다.

시간 절약: 원하는 서비스를 사용할 수 있는 경우 12단계로 건너뜁니다.



6단계. 적절한 서비스를 사용할 수 없는 경우 서비스 관리를 클릭합니다. Service Management 창이 나타납니다.

Service Name :

Protocol : TCP

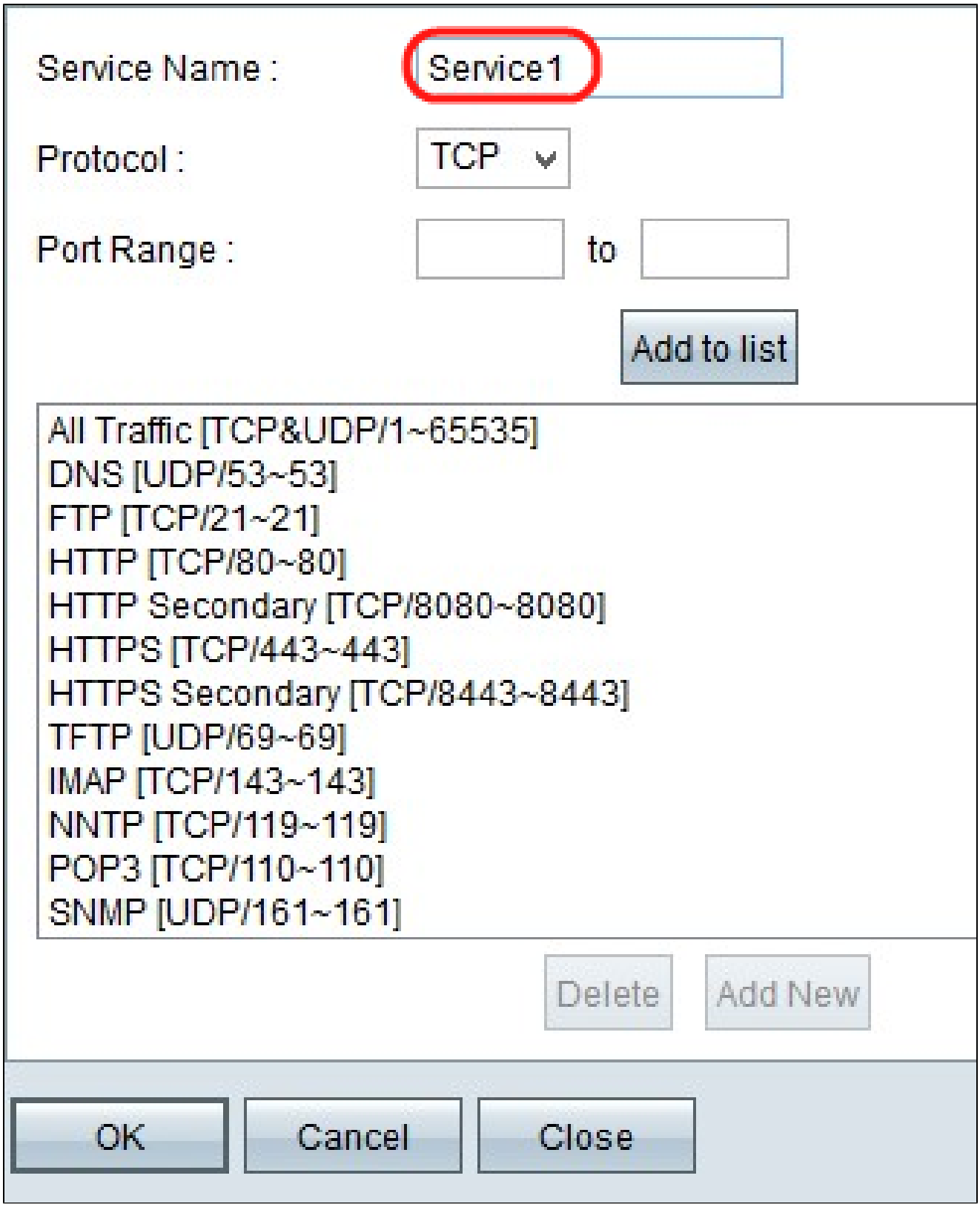
Port Range : to

Add to list

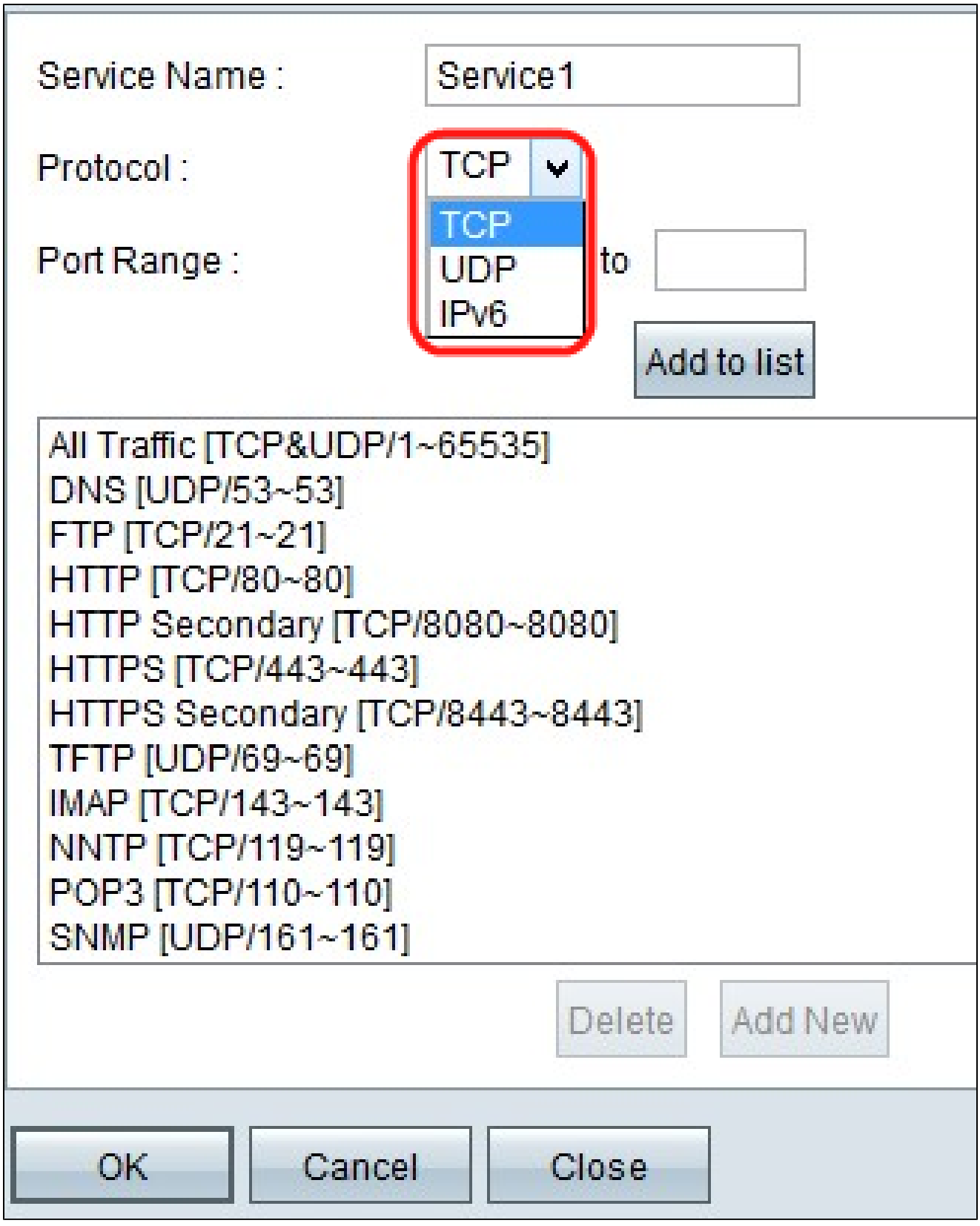
All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]

Delete Add New

OK Cancel Close



7단계. Service Name(서비스 이름) 필드에 새 서비스의 이름을 입력합니다.

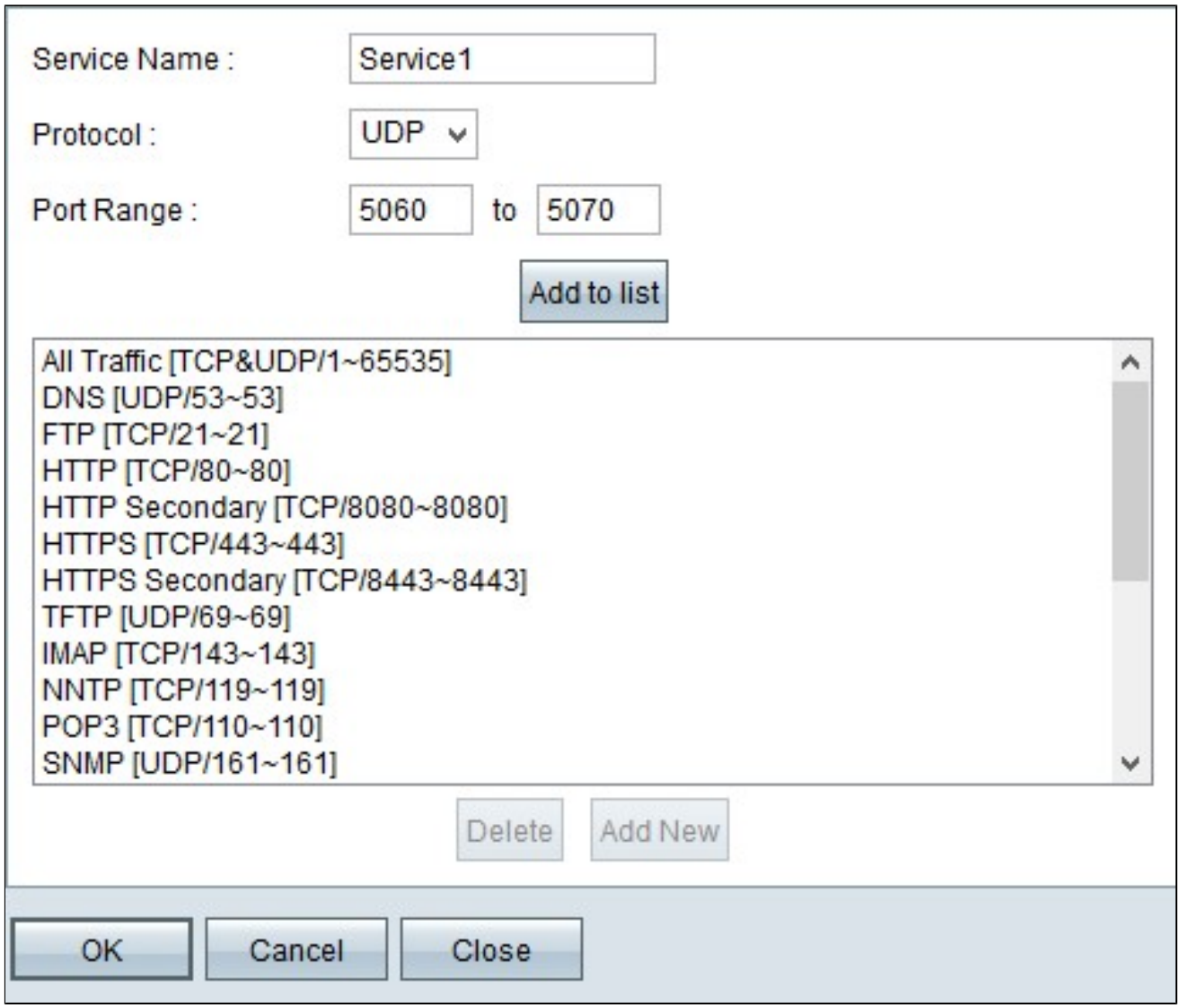


8단계. Protocol 드롭다운 목록에서 적절한 프로토콜 유형을 선택합니다.

· TCP(Transmission Control Protocol) — 보장된 전송이 필요한 애플리케이션에서 사용하는 전송 계층 프로토콜입니다.

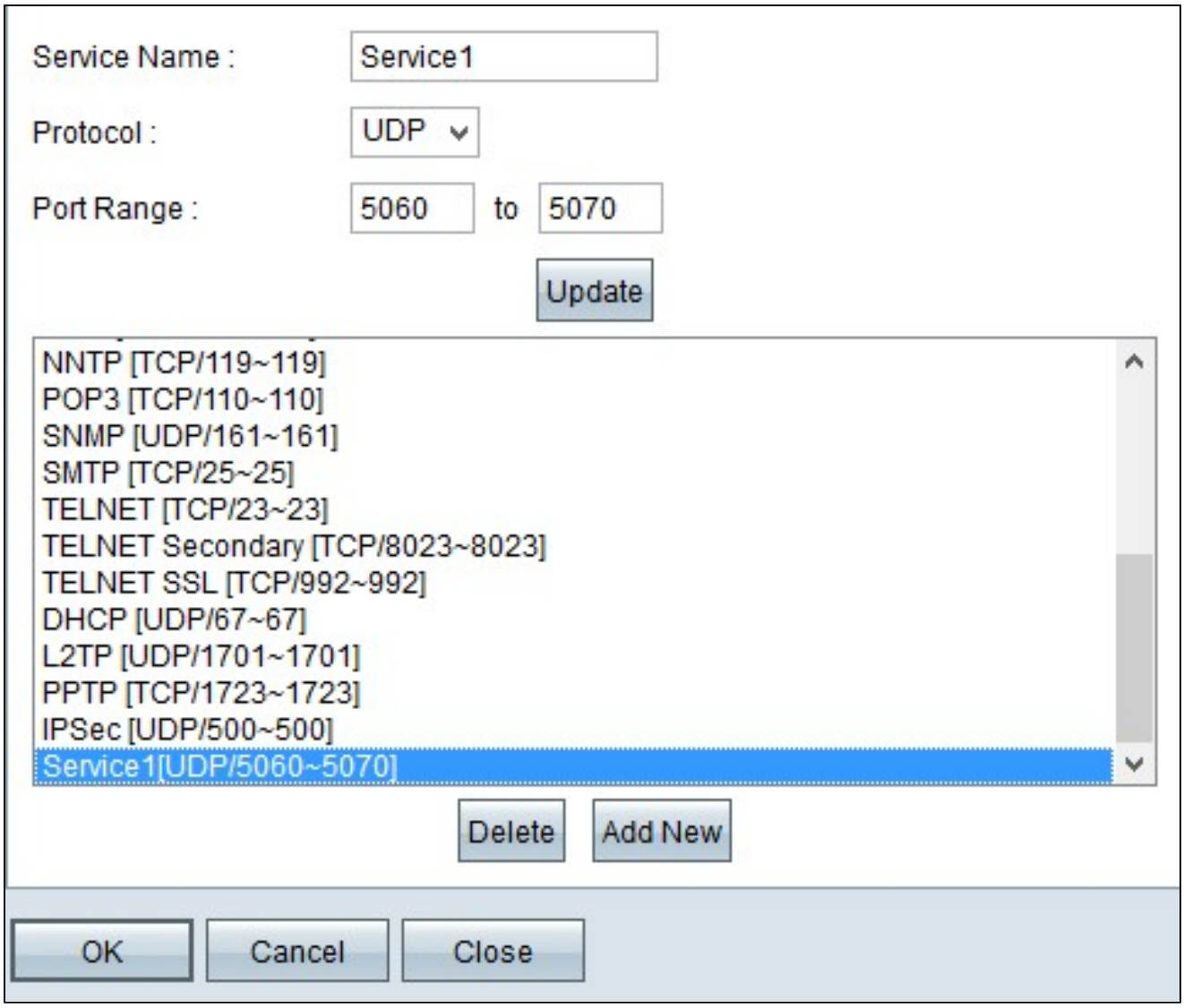
· UDP(User Datagram Protocol) - 데이터그램 소켓을 사용하여 호스트 간 통신을 설정합니다. UDP 전달은 보장되지 않습니다.

· IPv6(Internet Protocol version 6) — 라우팅 주소로 지정된 네트워크를 통해 라우팅되는 패킷의 호스트 간에 인터넷 트래픽을 디렉션합니다.



9단계. Port Range(포트 범위) 필드에 포트 범위를 입력합니다. 이 범위는 위 단계에서 선택한 프로토콜에 따라 달라집니다.

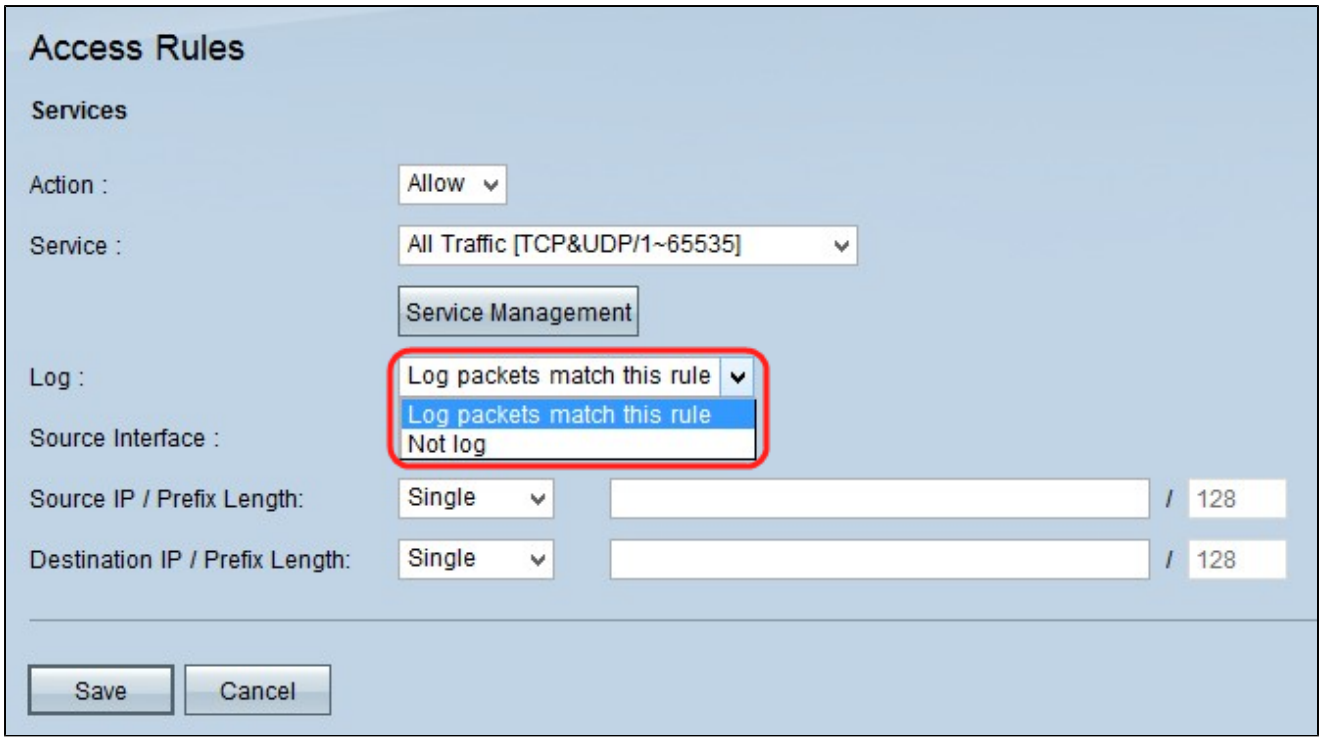
10단계. 목록에 추가를 클릭합니다. 이렇게 하면 서비스가 Service(서비스) 드롭다운 목록에 추가됩니다.



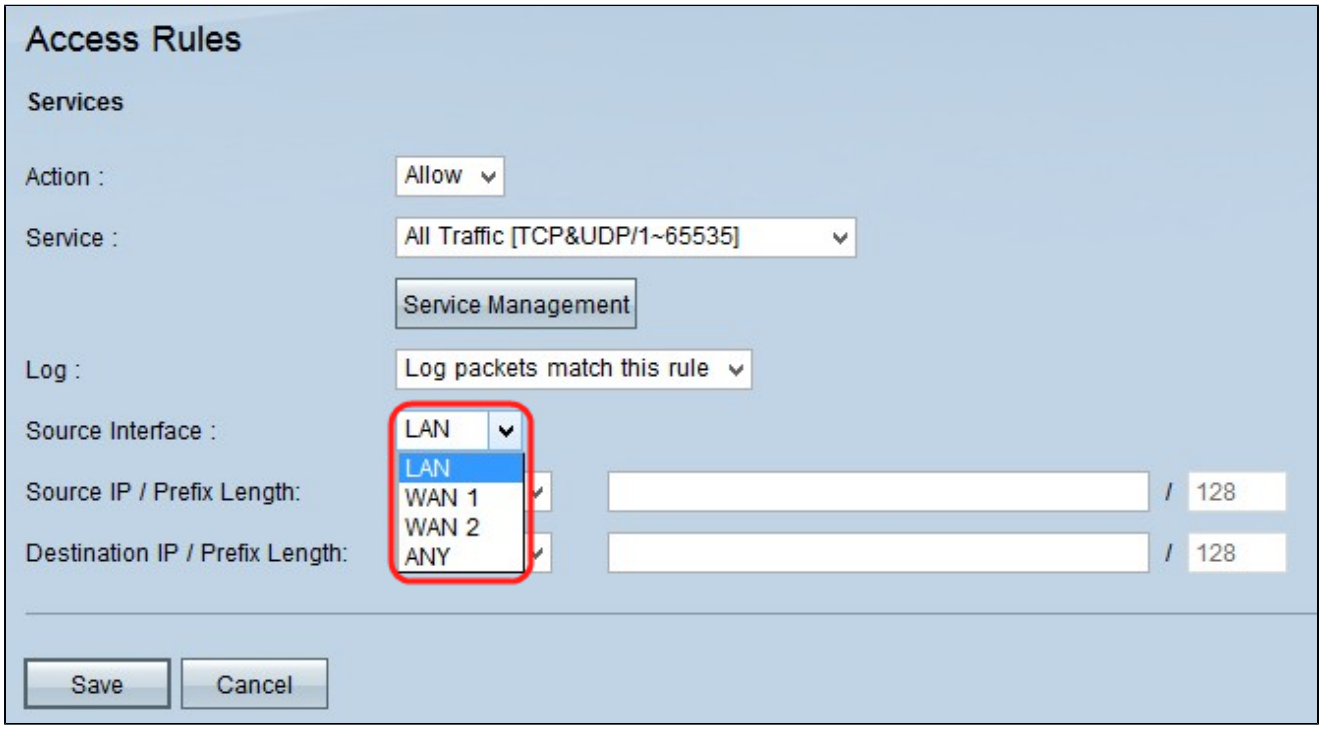
참고: 서비스 목록에서 서비스를 삭제하려면 서비스 목록에서 서비스를 선택하고 삭제를 클릭합니다. 서비스 항목을 업데이트하려면 서비스 목록에서 업데이트할 서비스를 선택한 다음 업데이트를 클릭합니다. 목록에 다른 새 서비스를 추가하려면 Add New(새로 추가)를 클릭합니다.

11단계. OK(확인)를 클릭합니다. 그러면 창이 닫히고 사용자가 Access Rule(액세스 규칙) 페이지로 돌아갑니다.

참고: Add New(새로 추가)를 클릭하면 7~11단계를 수행합니다.



12단계. 액세스 규칙과 일치하는 패킷을 기록하려면 Log packets match this rule in the Log 드롭다운 목록에서 Log packets를 선택합니다. 그렇지 않으면 Not Log를 선택합니다.



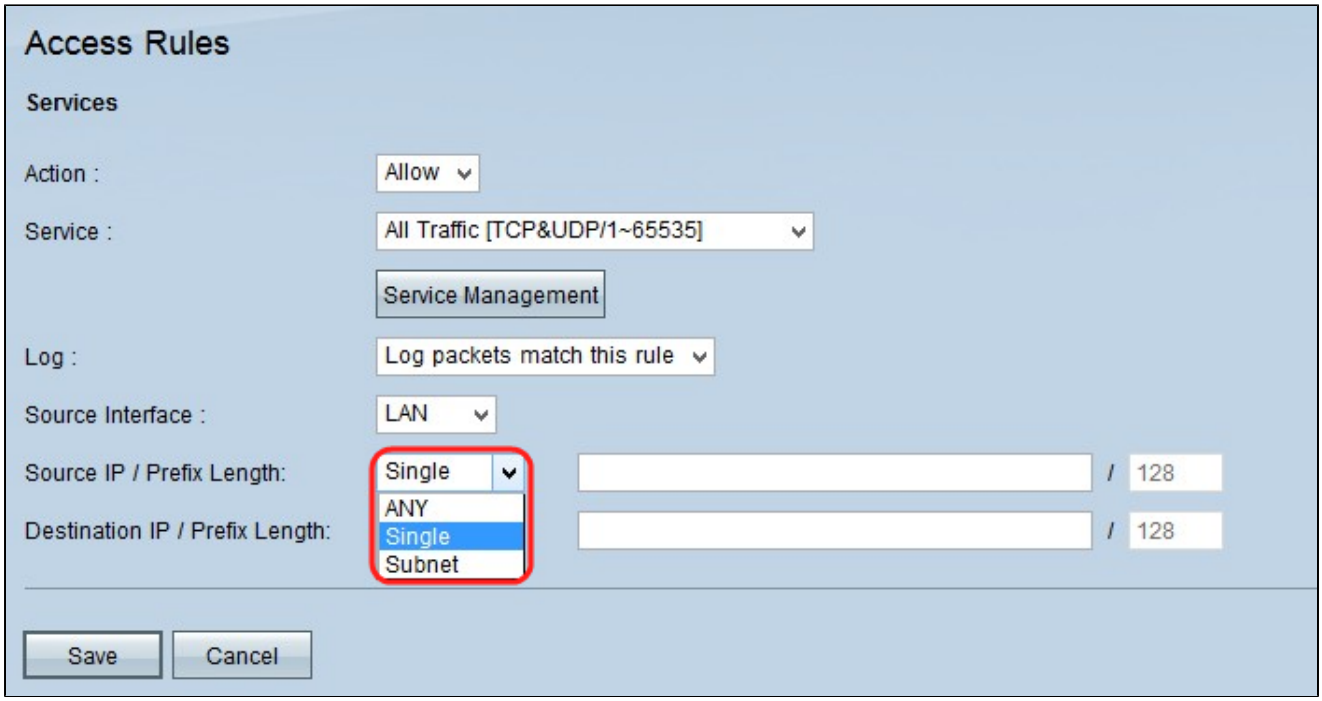
13단계. Source Interface 드롭다운 목록에서 이 규칙의 영향을 받는 인터페이스를 선택합니다. 소스 인터페이스는 트래픽이 시작되는 인터페이스입니다.

· LAN — 라우터의 로컬 영역 네트워크.

· WAN1 — WAN(Wide Area Network) 또는 라우터가 ISP 또는 다음 홉 라우터에서 인터넷을 가져오는 네트워크.

· WAN2 — 보조 네트워크라는 점을 제외하고 WAN1과 동일합니다.

· ANY — 모든 인터페이스를 사용할 수 있습니다.

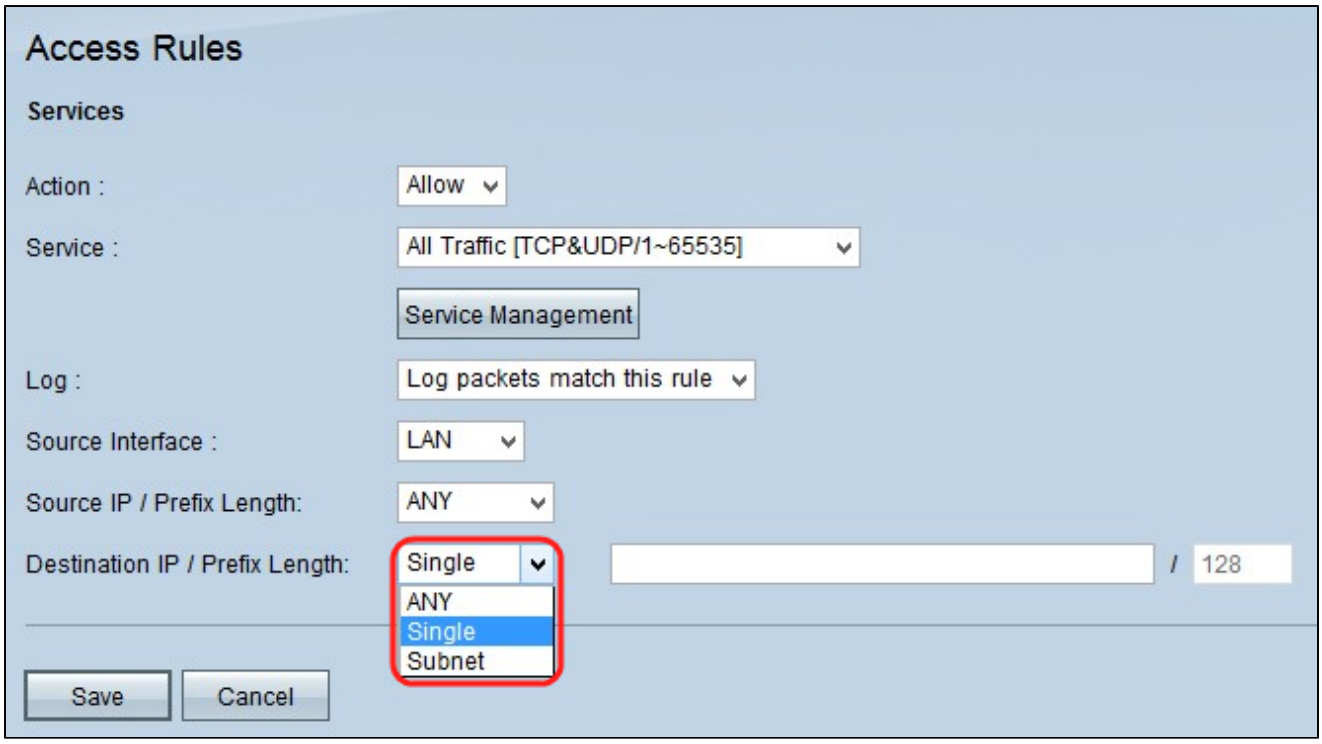


14단계. Source IP 드롭다운 목록에서 액세스 규칙이 적용되는 소스 IP 주소를 지정하는 옵션을 선택합니다.

· Any — 액세스 규칙이 소스 인터페이스의 모든 트래픽에 적용됩니다. 사용 가능한 드롭다운 목록 오른쪽에 필드가 없습니다.

· Single — 액세스 규칙이 소스 인터페이스의 단일 IP 주소에 적용됩니다. 주소 필드에 원하는 IP 주소를 입력합니다.

· 서브넷 — 액세스 규칙이 소스 인터페이스의 서브넷 네트워크에 적용됩니다. IP 주소 및 접두사 길이를 입력합니다.



15단계. Destination IP(대상 IP) 드롭다운 목록에서 액세스 규칙이 적용되는 대상 IP 주소를 지정하는 옵션을 선택합니다.

· Any — 액세스 규칙이 목적지 인터페이스에 대한 모든 트래픽에 적용됩니다. 사용 가능한 드롭다운 목록 오른쪽에 필드가 없습니다.

· Single — 액세스 규칙이 단일 IP 주소에 적용되어 대상 인터페이스에 적용됩니다. 주소 필드에 원하는 IP 주소를 입력합니다.

· 서브넷 — 액세스 규칙이 서브넷 네트워크에서 대상 인터페이스에 적용됩니다. IP 주소 및 접두사 길이를 입력합니다.

16단계. IPv6 액세스 규칙에서 수행한 모든 변경 사항을 저장하려면 Save를 클릭합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.