RV34x Series 라우터의 ACL 모범 사례

목표

이 문서의 목적은 RV34x 시리즈 라우터를 사용하여 ACL(Access Control List)을 생성하는 모범 사례를 설명하는 것입니다.

적용 가능한 디바이스 | 펌웨어 버전

- RV340 | 1.0.03.20 **(최신 다운로드)**
- RV340W | 1.0.03.20 **(최신 다운로드)**
- RV345 | 1.0.03.20 **(최신 다운로드)**
- RV345P | 1.0.03.20 **(최신 다운로드)**

소개

네트워크에 대한 더 강력한 제어 기능을 원하십니까?네트워크를 안전하게 유지하기 위해 추가 단계를 수행하시겠습니까?그렇다면 ACL(Access Control List)이 필요할 수 있습니다.

ACL은 네트워크 트래픽 프로필을 종합적으로 정의하는 하나 이상의 ACE(Access Control Entries)로 구성됩니다.그런 다음 이 프로파일은 트래픽 필터링, 우선 순위 또는 사용자 지정 대기열 처리와 같은 Cisco 소프트웨어 기능에서 참조할 수 있습니다.각 ACL에는 소스 주소, 목적지 주소, 프로토콜, 프로토콜별 매개변수 등의 기준을 기반으로 하는 작업 요소(허용 또는 거부)와 필터 요소가 포함됩니다.

입력한 기준에 따라 특정 트래픽이 네트워크에 드나드는 것을 제어할 수 있습니다.라우터가 패킷을 받으면 액세스 목록을 기반으로 패킷을 전달할지 아니면 삭제할지를 결정하기 위해 패킷을 검사합니다.

이러한 보안 수준의 구현은 특정 네트워크 시나리오 및 보안 요구 사항을 고려하여 여러 활용 사례를 기반으로 합니다.

라우터가 라우터의 컨피그레이션을 기반으로 자동으로 액세스 목록을 만들 수 있다는 점에 유의해야 합니다.이 경우 라우터 컨피그레이션을 변경하지 않으면 지울 수 없는 액세스 목록이 표시될 수 있습니다.

액세스 목록을 사용하는 이유

- 대부분의 경우 ACL을 사용하여 네트워크에 액세스하기 위한 기본적인 수준의 보안을 제공합니다.예를 들어 ACL을 구성하지 않으면 기본적으로 라우터를 통과하는 모든 패킷이 네트워크의 모든 부분에 허용될 수 있습니다.
- ACL은 하나의 호스트, IP 주소 범위 또는 네트워크를 허용하고 다른 호스트, IP 주소 범위 또는 네트워크가 동일한 영역(호스트 또는 네트워크)에 액세스하지 못하도록 할 수 있습니다.
- ACL을 사용하여 라우터 인터페이스에서 전달하거나 차단한 트래픽 유형을 결정할 수 있

습니다.예를 들어 SSH(Secure Shell) SFTP(File Transfer Protocol) 트래픽을 허용할 수 있으며 동시에 모든 SIP(Session Initiation Protocol) 트래픽을 차단할 수 있습니다.

액세스 목록 사용 시기

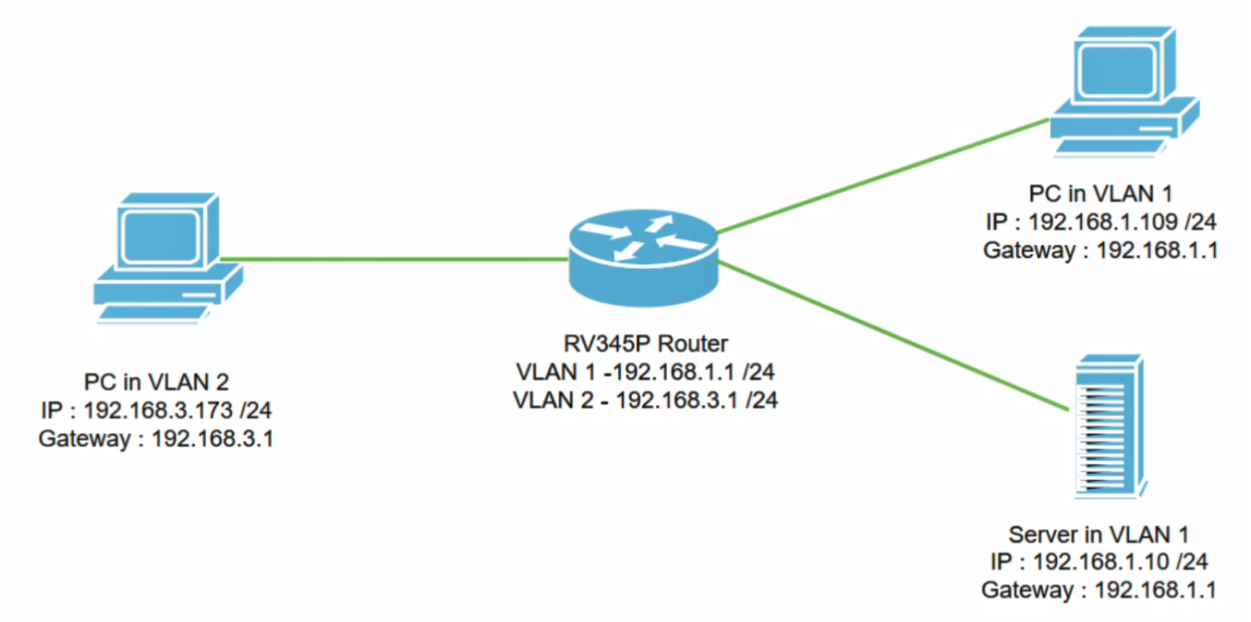
- 내부 네트워크와 인터넷과 같은 외부 네트워크 사이에 있는 라우터에서 ACL을 구성해야 합니다.
- ACL을 사용하여 내부 네트워크의 특정 부분에 들어오거나 나가는 트래픽을 제어할 수 있습니다.
- 인터페이스에서 인바운드 트래픽 또는 아웃바운드 트래픽 또는 둘 다를 필터링해야 하는 경우
- 트래픽을 제어하려면 프로토콜별로 ACL을 정의해야 합니다.

액세스 목록을 사용하여 기본 보안을 구성하는 모범 사례

- 다른 모든 것을 거부하는 프로토콜, 포트 및 IP 주소만 허용하는 ACL을 구현합니다.
- 목적지와 소스 주소가 동일하다고 주장하는 수신 패킷 차단(라우터 자체에 대한 랜드 공격)
- 내부(신뢰할 수 있는) Syslog 호스트에 대한 ACL의 로깅 기능을 설정합니다.
- 라우터에서 SNMP(Simple Network Management Protocol)를 사용하는 경우 SNMP ACL 및 복잡한 SNMP 커뮤니티 문자열을 구성해야 합니다.
- 내부 주소만 내부 인터페이스에서 라우터를 입력하고 내부 주소로 향하는 트래픽만 외부(외부 인터페이스)에서 라우터로 들어갈 수 있도록 허용합니다.
- 멀티캐스트를 사용하지 않는 경우 차단합니다.
- 일부 ICMP(Internet Control Message Protocol) 메시지 유형(리디렉션, 에코)을 차단합니다.
- ACL을 입력하는 순서를 항상 고려하십시오.예를 들어 라우터가 패킷을 전달할지 차단할지 결정할 때 ACL이 생성된 순서대로 각 ACL 문에 대해 패킷을 테스트합니다.

Cisco RV34x Series 라우터의 액세스 목록 구현

네트워크 토폴로지 예



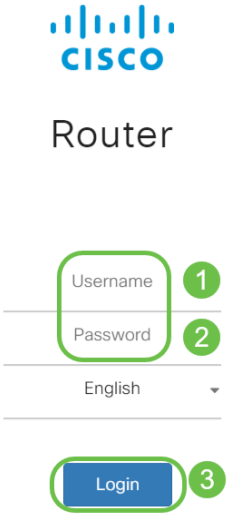
예제 시나리오

이 시나리오에서는 RV345P 라우터와 두 개의 다른 VLAN 인터페이스가 있는 이 네트워크 다이어그램을 복제합니다.VLAN 1과 VLAN2에 PC가 있고 VLAN 1에 서버도 있습니다. VLAN 간 라우팅이 활성화되므로 VLAN 1과 VLAN 2 사용자는 서로 통신할 수 있습니다.이제 액세스 규칙을 적용하여 VLAN 1의 이 서버에 대한 VLAN 2 사용자 간의 통신을 제한합니다.

컨피그레이션 예

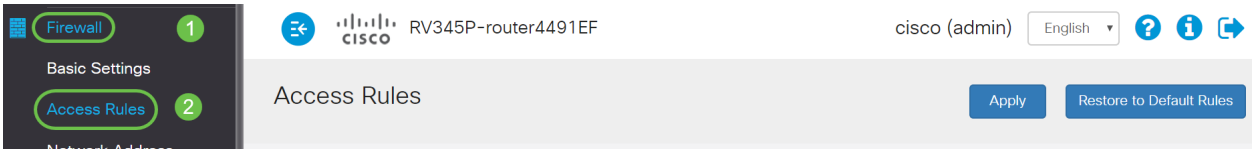
1단계

구성한 자격 증명을 사용하여 라우터의 UI(웹 사용자 인터페이스)에 로그인합니다.



2단계

ACL을 구성하려면 **Firewall(방화벽) > Access Rules(액세스 규칙)**로 이동하고 **더하기 아이콘**을 클릭하여 새 규칙을 추가합니다.



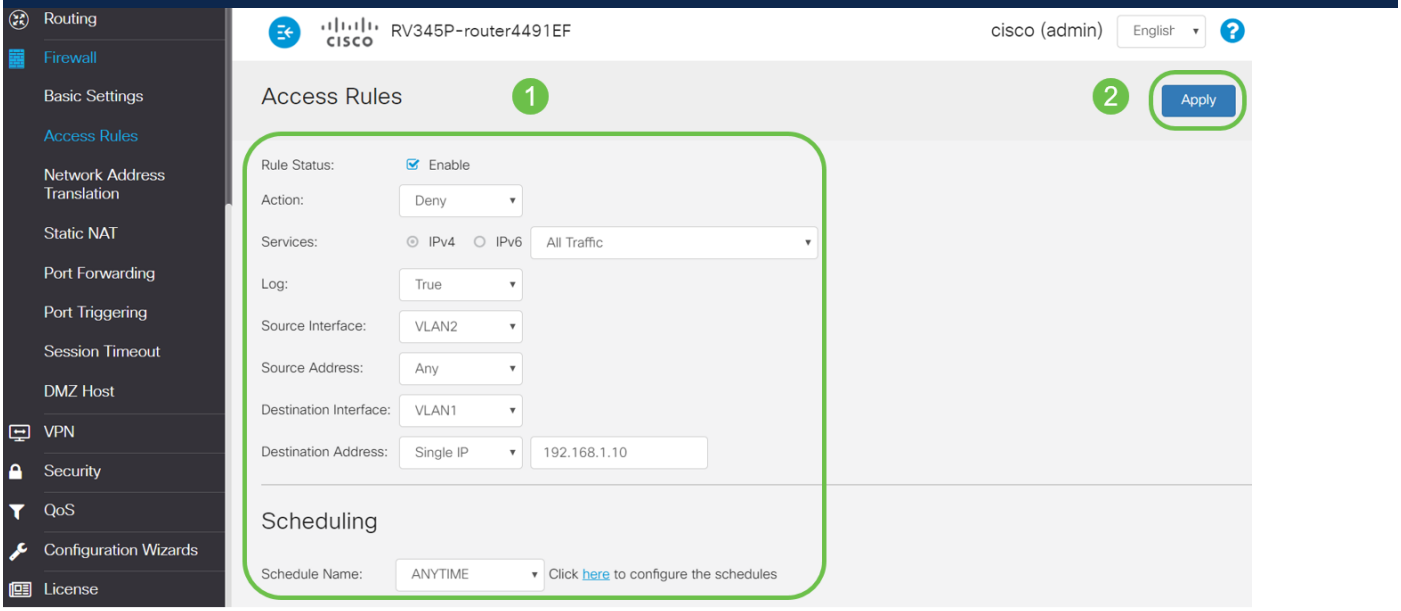
3단계

액세스 *규칙* 매개변수를 구성합니다.서버(IPv4:192.168.1.10/24) VLAN2 사용자로부터의 액세스이 시나리오의 매개변수는 다음과 같습니다.

- *규칙 상태:사용*
- *작업:거부*
- *서비스:모든 트래픽*
- *로그:참*
- *소스 인터페이스:VLAN2*
- *소스 주소:모두*
- *대상 인터페이스:VLAN1*
- *대상 주소:단일 IP 192.168.1.10*
- *일정 이름:언제든지*

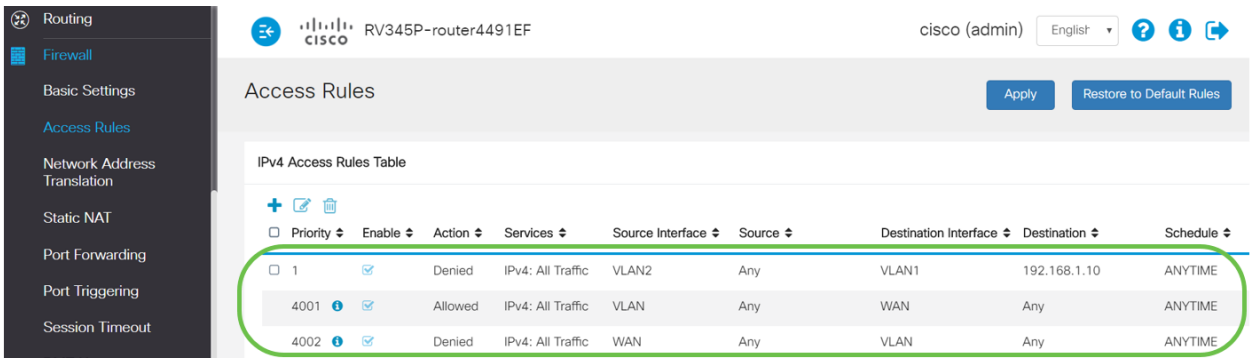
Apply를 **클릭합니다**.

이 예에서는 VLAN2에서 서버로의 모든 디바이스에 대한 액세스를 거부한 다음 VLAN1의 다른 디바이스에 대한 액세스를 허용합니다. 요구 사항은 다를 수 있습니다.



4단계

Access *Rules*(액세스 규칙) 목록은 다음과 같이 표시됩니다.



확인

서비스를 확인하려면 명령 프롬프트를 엽니다.Windows 플랫폼에서는 Windows 단추를 클릭한 다음 컴퓨터의 왼쪽 아래 검색 상자에 **cmd**를 입력한 다음 메뉴에서 **명령 프롬프트**를 선택하여 이 작업을 수행할 수 있습니다.

다음 명령을 입력합니다.

- VLAN2의 PC(192.168.3.173)에서 서버(IP:192.168.1.10). 통신이 허용되지 *않는다는* 의미인 *요청 시간 초과* 알림을 받게 됩니다.
- VLAN2의 PC(192.168.3.173)에서 VLAN1의 다른 PC(192.168.1.109)을 ping합니다. 성공적으로 회신하게 됩니다.

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

결론

Cisco RV34x Series 라우터에서 액세스 규칙을 구성하는 데 필요한 단계를 확인했습니다.이제 이를 적용하여 네트워크에 필요에 맞는 액세스 규칙을 만들 수 있습니다!