

RV34x Series 라우터에서 액세스 규칙 구성

목표

RV340 Dual-WAN VPN Router는 중소기업에 적합한 사용하기 쉽고 유연한 고성능 디바이스입니다. 웹 필터링, 애플리케이션 제어, IP 소스 가드 등의 보안 기능이 추가되었습니다. 새로운 RV340은 소규모 사무실 및 원격 직원에게 매우 안전한 광대역, 유선 연결을 제공합니다. 이러한 새로운 보안 기능은 네트워크에서 허용되는 활동을 세부적으로 조정할 수 있는 편의성도 제공합니다.

RV34x Series Router의 액세스 규칙 또는 정책을 사용하면 규칙을 구성하여 네트워크의 보안을 강화할 수 있습니다. 규칙의 조합이며 ACL(Access Control List)이 있습니다. ACL은 특정 사용자로부터 트래픽을 보내거나 받는 것을 차단하거나 허용하는 목록입니다. 액세스 규칙은 항상 적용되도록 구성하거나 정의된 일정에 따라 구성할 수 있습니다.

ACL은 목록 끝에 암시적 거부가 있으므로 명시적으로 허용하지 않는 한 트래픽은 통과할 수 없습니다. 예를 들어, 특정 주소를 제외한 모든 사용자가 라우터를 통해 네트워크에 액세스하도록 허용하려면 특정 주소를 거부하고 다른 모든 주소를 허용해야 합니다.

이 문서의 목적은 RV34x Series 라우터에서 액세스 규칙을 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스

- RV34x 시리즈

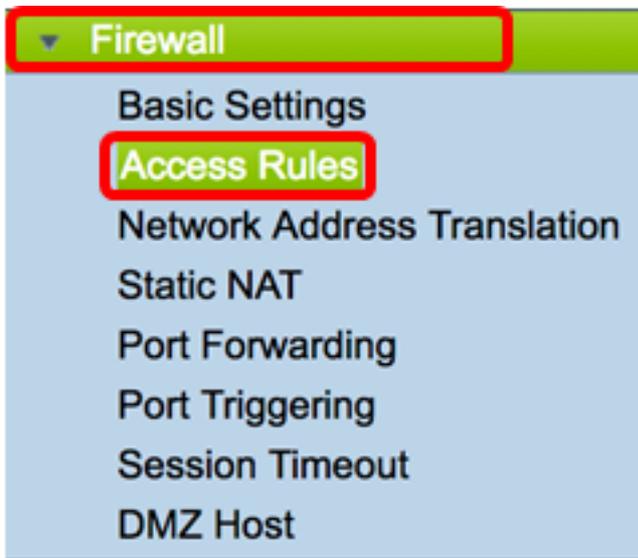
소프트웨어 버전

- 1.0.1.16
 - [이 문서의 게시 이후 UI를 업데이트하는 펌웨어를 사용할 수 있게 되었습니다. 여기를 클릭하여 다운로드 페이지로 이동하여 해당 위치에서 특정 제품을 찾으십시오.](#)

RV34x Series 라우터에서 액세스 규칙 구성

액세스 규칙 생성

1단계. 라우터의 웹 기반 유틸리티에 로그인하고 **Firewall > Access Rules**를 선택합니다.



2단계. IPv4 또는 IPv6 Access Rules 테이블에서 **Add**를 클릭하여 새 규칙을 생성합니다.

참고:RV34x Series Router에서는 최대 202개의 규칙을 구성할 수 있습니다.이 예에서는 IPv4가 사용됩니다.



3단계. Enable **Rule Status** 확인란을 선택하여 규칙을 활성화합니다.



4단계. Action(작업) 드롭다운 메뉴에서 정책이 데이터를 허용할지 또는 거부할지를 선택합니다.

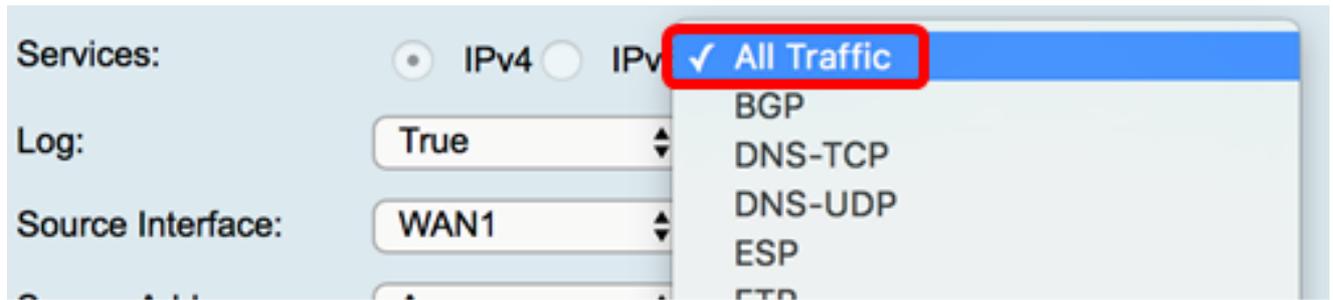
참고:이 예에서는 Allow(허용)가 선택됩니다.



5단계. Services(서비스) 드롭다운 메뉴에서 라우터가 허용하거나 거부할 트래픽 종류를 선택

합니다.

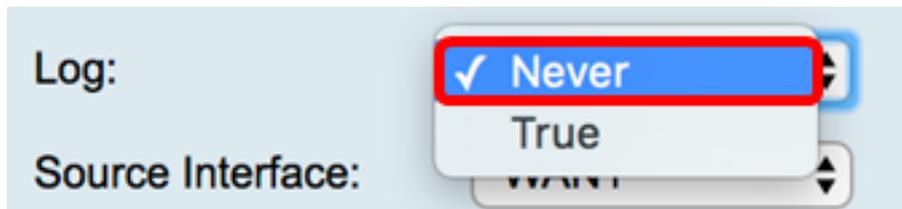
참고:이 예에서는 All traffic(모든 트래픽)이 선택됩니다.모든 트래픽이 허용됩니다.



6단계. Log(로그) 드롭다운 메뉴에서 라우터가 허용 또는 거부된 트래픽을 로깅할지 여부를 확인하는 옵션을 선택합니다.옵션은 다음과 같습니다.

- Never — 라우터는 허용 및 거부된 트래픽을 로깅하지 않습니다.
- True — 라우터가 정책과 일치하는 트래픽을 로깅합니다.

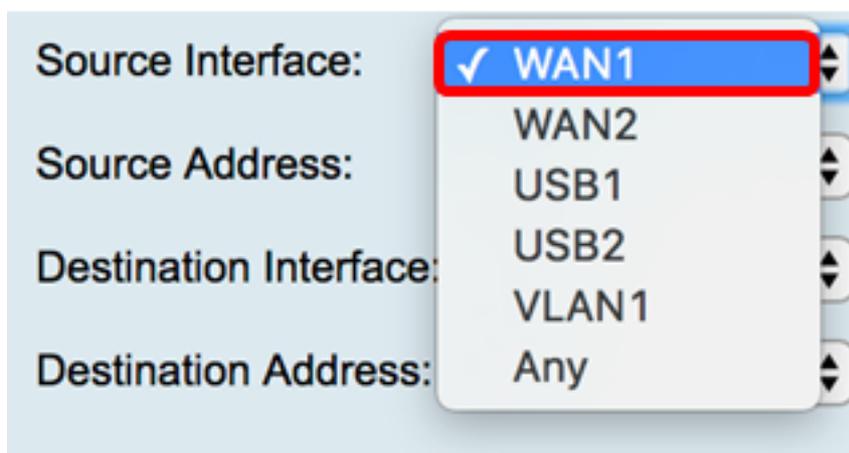
참고:이 예에서는 Never가 선택됩니다.



7단계. Source Interface 드롭다운 메뉴에서 액세스 정책을 적용해야 하는 수신 또는 인바운드 트래픽의 인터페이스를 선택합니다.옵션은 다음과 같습니다.

- WAN1 — 정책은 WAN1의 트래픽에만 적용됩니다.
- WAN2 — 정책은 WAN2의 트래픽에만 적용됩니다.
- USB1 — 정책은 USB1의 트래픽에만 적용됩니다.
- USB2 — 정책은 USB2의 트래픽에만 적용됩니다.
- VLAN1 — 정책은 트래픽 VLAN1에만 적용됩니다.
- Any — 정책이 모든 인터페이스에 적용됩니다.

참고:추가 VLAN(Virtual Local Area Network)이 구성된 경우 VLAN 옵션이 목록에 나타납니다 .이 예에서는 WAN1이 선택됩니다.

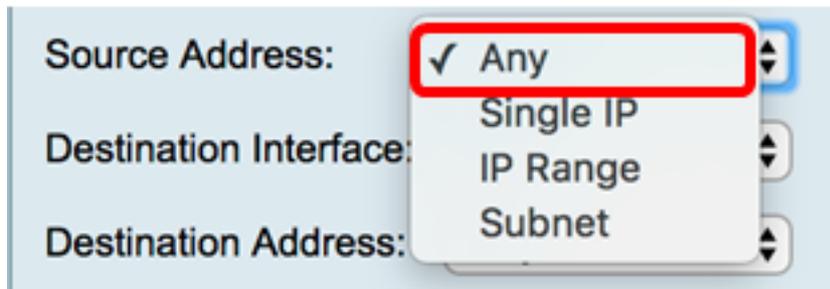


8단계. Source Address 드롭다운 메뉴에서 정책을 적용할 소스를 선택합니다.옵션은 다음과

같습니다.

- Any — 정책이 네트워크의 모든 IP 주소에 적용됩니다.이 옵션을 선택한 경우 [12단계](#)로 건너됩니다.
- 단일 IP — 정책이 단일 호스트 또는 IP 주소에 적용됩니다.이 옵션을 선택한 경우 [9단계](#)로 건너됩니다.
- IP 범위 — 정책이 IP 주소 집합 또는 범위에 적용됩니다.이 옵션을 선택한 경우 [10단계](#)로 건너됩니다.
- 서브넷 — 정책이 전체 하위 네트워크에 적용됩니다.이 옵션을 선택한 경우 [11단계](#)로 건너됩니다.

참고:이 예에서는 Any가 선택됩니다.



Source Address: Any
Destination Interface:
Destination Address:

[9단계](#). (선택 사항) 8단계에서 단일 IP를 선택하고 적용할 정책의 단일 IP 주소를 입력한 다음 [12단계](#)로 건너됩니다.

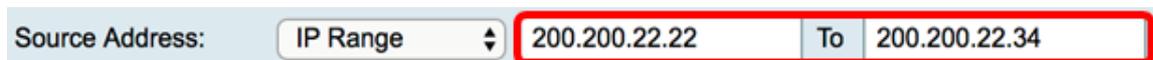
참고:이 예에서는 200.200.22.52이 사용됩니다.



Source Address:

[10단계](#). (선택 사항) 8단계에서 IP 범위를 선택한 경우 각 IP 주소 필드에 시작 및 종료 IP 주소를 입력합니다.

참고:이 예에서 200.200.22.22은 시작 IP 주소로, 200.200.22.34은 끝 IP 주소로 사용됩니다.



Source Address: To

[11단계](#). (선택 사항) 8단계에서 서브넷을 선택한 경우 네트워크 ID와 해당 서브넷 마스크를 입력하여 정책을 적용합니다.

참고:이 예에서는 200.200.22.1이 서브넷 ID로 사용되고 24가 서브넷 마스크로 사용됩니다.



Source Address: /

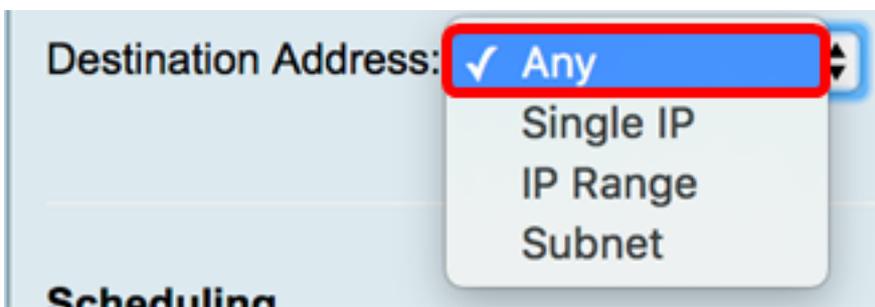
[12단계](#). Destination Interface 드롭다운 메뉴에서 액세스 정책을 적용해야 하는 발신 또는 아웃바운드 트래픽에 대한 인터페이스를 선택합니다. 옵션은 WAN1, WAN2, USB1, USB2, VLAN1 및 Any입니다.

참고:이 예에서는 WAN1이 선택됩니다.



13단계. Destination Address(대상 주소) 드롭다운 메뉴에서 정책을 적용할 대상을 선택합니다. 옵션은 Any, Single IP, IP Range, Subnet입니다.

참고: 이 예에서는 Any가 선택됩니다. [17단계](#)로 건너웁니다.



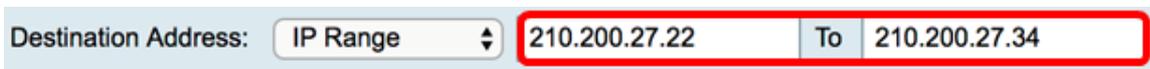
14단계. (선택 사항) 13단계에서 단일 IP를 선택한 경우 적용할 정책에 대해 단일 IP 주소를 입력합니다.

참고: 이 예에서는 210.200.22.52이 사용됩니다.



15단계. (선택 사항) 13단계에서 IP 범위를 선택한 경우 각 IP 주소 필드에 시작 및 종료 IP 주소를 입력합니다.

참고: 이 예에서 210.200.27.22은 시작 IP 주소로, 210.200.27.34은 끝 IP 주소로 사용됩니다. [17단계](#)로 건너웁니다.

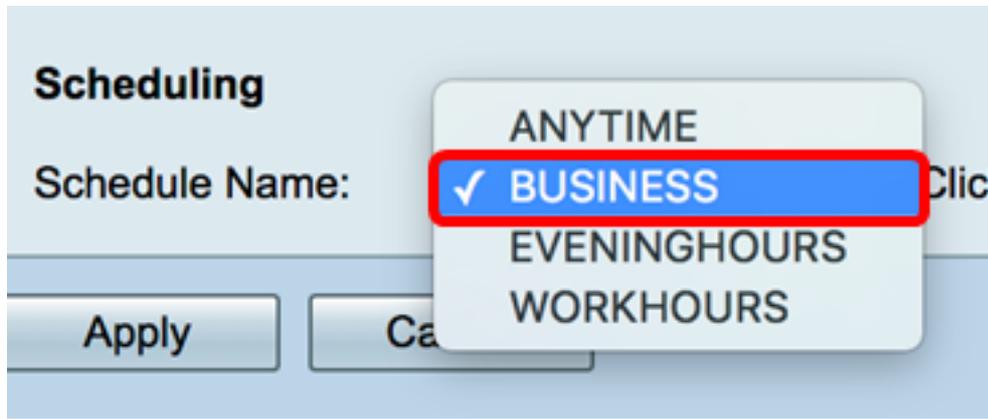


16단계. (선택 사항) 13단계에서 서브넷을 선택한 경우 정책을 적용할 네트워크 주소와 해당 서브넷 마스크를 입력합니다.

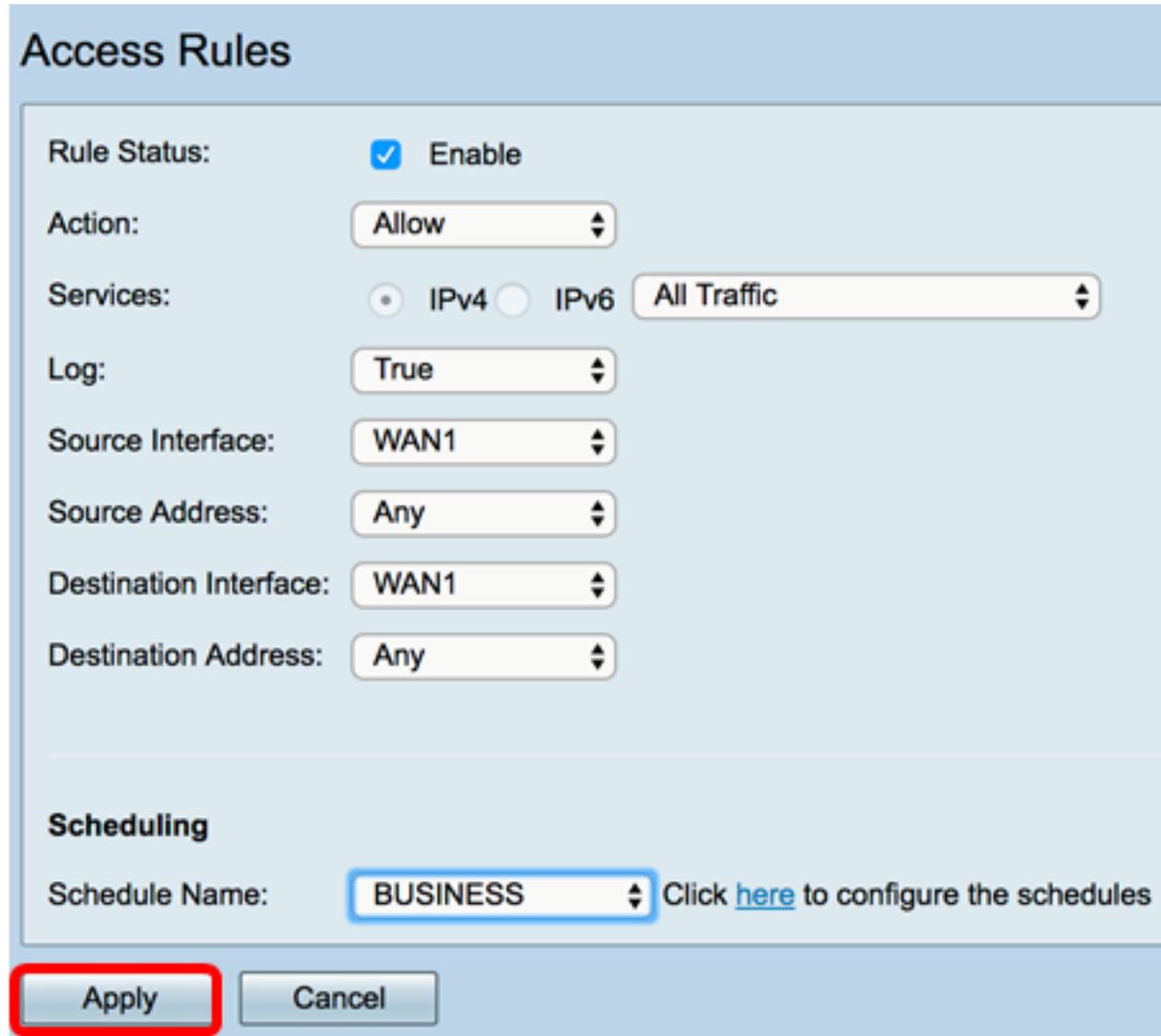
참고: 이 예에서 210.200.27.1은 서브넷 주소로, 24는 서브넷 마스크로 사용됩니다.



[17단계](#). Schedule Name 드롭다운 목록에서 이 정책을 적용할 일정을 선택합니다. 일정을 구성하는 방법을 알아보려면 [여기](#)를 클릭하십시오.



18단계. 적용을 누릅니다.



이제 RV Series Router에서 액세스 규칙을 성공적으로 생성해야 합니다.

액세스 규칙 편집

1단계. IPv4 또는 IPv6 액세스 규칙 테이블에서 구성하려는 액세스 규칙 옆의 확인란을 선택합니다.

참고: 이 예에서 IPv4 Access Rules Table(IPv4 액세스 규칙 테이블)에서 Priority 1(우선순위 1)이 선택됩니다.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

2단계. Edit(수정)를 클릭합니다.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

3단계. (선택 사항) Configure 열에서 원하는 액세스 규칙 행의 Edit 버튼을 클릭합니다.

Schedule	Configure			
BUSINESS	<input checked="" type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
BUSINESS	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>

4단계. 필요한 매개변수를 갱신합니다.

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

Schedule Name: Click [here](#) to configure the schedules

Apply

Cancel

5단계. 적용을 누릅니다.

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

Schedule Name: Click [here](#) to configure the schedules

6단계. (선택 사항) Configure 열에서 액세스 규칙의 우선순위를 변경하려면 이동할 액세스 규칙의 **Up** 또는 **Down** 버튼을 클릭합니다.

참고: 액세스 규칙을 위나 아래로 이동하면 원래 배치 위 또는 아래로 한 단계가 이동합니다. 이 예에서는 우선 순위 1이 아래로 이동합니다.

Priority	Enable	Action	Service	Source Interf...	Source	Destinat...	Destination	Schedule	Configure
1	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	WAN1	Any	USB1	192.168.1.1	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
201	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	VLAN	Any	WAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
202	<input checked="" type="checkbox"/>	Denied	IPv4: All T...	WAN	Any	VLAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>

참고: 이 예에서는 우선 순위 1이 우선 순위 2가 되었습니다.

IPv4 Access Rules Table										
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter...	Source	Destina...	Destination	Schedule	Configure
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	VLAN	Any	WAN	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Tr...	WAN	Any	VLAN	Any	ANYTIME	Edit Delete Up Down

Add Edit Delete

7단계. 적용을 클릭합니다.

Access Rules

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Add Edit Delete

IPv6 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

Add Edit Delete

이제 RV34x Series Router에서 액세스 규칙을 편집했습니다.

액세스 규칙 삭제

1단계. IPv4 또는 IPv6 액세스 규칙 테이블에서 삭제할 액세스 규칙 옆의 확인란을 선택합니다.

참고: 이 예에서 IPv4 Access Rules Table(IPv4 액세스 규칙 테이블)에서 Priority 1(우선순위 1)이 선택됩니다.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

2단계. 테이블 아래에 있는 삭제를 클릭하거나 구성 열에서 삭제 단추를 클릭합니다.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

3단계. 적용을 클릭합니다.

Access Rules

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

IPv6 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

이제 RV34x Series 라우터에서 액세스 규칙을 성공적으로 삭제해야 합니다.

[이 문서와 관련된 비디오 보기...](#)

[여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.](#)