

# RV130 및 RV130W에서 액세스 규칙 추가 및 구성

## 목표

네트워크 디바이스는 액세스 규칙과 함께 기본적인 트래픽 필터링 기능을 제공합니다. 액세스 규칙은 프로토콜, 소스 및 목적지 IP 주소 또는 네트워크 컨피그레이션을 기반으로 허용 또는 거부 규칙(패킷을 전달하거나 삭제하기 위한)을 지정하는 ACL(Access Control List)의 단일 항목입니다.

이 문서의 목적은 RV130 및 RV130W에 액세스 규칙을 추가하고 구성하는 방법을 보여주는 것입니다.

## 적용 가능한 장치

- RV130
- RV130W

## 소프트웨어 버전

- 버전 1.0.1.3

## 액세스 규칙 추가 및 구성

### 기본 아웃바운드 정책 설정

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

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

2단계. *Default Outbound Policy(기본 아웃바운드 정책)* 영역에서 원하는 라디오 버튼을 클릭하여 아웃바운드 트래픽에 대한 정책을 선택합니다. 정책은 구성된 액세스 규칙 또는 인터넷 액세스 정책이 없을 때마다 적용됩니다. 기본 설정은 **Allow(허용)**이며, 이는 인터넷으로 향하는 모든 트래픽이 통과하도록 허용합니다.

# Access Rules

## Default Outbound Policy

Policy:  Allow  Deny

## Access Rule Table

사용 가능한 옵션은 다음과 같이 정의됩니다.

- 허용 — LAN에서 인터넷으로 나가는 모든 유형의 트래픽을 허용합니다.
- 거부 — LAN에서 인터넷으로 나가는 모든 유형의 트래픽을 차단합니다.

3단계. **저장**을 클릭하여 설정을 저장합니다.

Access Rules

Default Outbound Policy

Policy:  Allow  Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

## 액세스 규칙 추가

1단계. 웹 구성 유틸리티에 로그인하고 Firewall(방화벽) > **Access Rules(액세스 규칙)**를 선택합니다. *Access Rules* 창이 열립니다.

Access Rules

Default Outbound Policy

Policy:  Allow  Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

2단계. 새 **액세스 규칙**을 추가하려면 *Access Rule Table(액세스 규칙 테이블)*에서 Add Row(행 추가)를 클릭합니다.

**Access Rules**

Default Outbound Policy  
Policy:  Allow  Deny

**Access Rule Table**

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

Add Access Rule 페이지가 열립니다.

**Add Access Rule**

Connection Type: Outbound (LAN > WAN) ▼

Action: Always block ▼

Schedule: ▼

Services: All Traffic ▼

Source IP: Any ▼

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP: Any ▼

Start:

Finish:

Log: Never ▼

Rule Status:  Enable

3단계. Connection Type 드롭다운 목록에서 규칙을 적용할 트래픽 유형을 선택합니다.

Connection Type: Outbound (LAN > WAN) ▼

Outbound (LAN > WAN)  
Inbound (WAN > LAN)  
Inbound (WAN > DMZ)

Action:

Schedule: ▼

Services: All Traffic ▼

Source IP: Any ▼

Start:

Finish:

사용 가능한 옵션은 다음과 같이 정의됩니다.

·아웃바운드(LAN > WAN) — 규칙은 로컬 네트워크(LAN)에서 가져온 패킷과 인터넷(WAN)으로 나가는 패킷에 영향을 미칩니다.

·인바운드(WAN > LAN) — 이 규칙은 인터넷(WAN)에서 로컬 네트워크(LAN)로 들어오는 패킷에 영향을 줍니다.

·인바운드(WAN > DMZ) — 규칙은 인터넷(WAN)에서 DMZ(Demilitarized Zone) 하위 네트워크로 들어오는 패킷에 영향을 줍니다.

4단계. *Action* 드롭다운 목록에서 규칙이 일치할 때 수행할 작업을 선택합니다.

The screenshot shows a configuration window for a firewall rule. The 'Action' dropdown menu is expanded, with 'Always block' selected. The 'Connection Type' is set to 'Outbound (LAN > WAN)'. The 'Source IP' is set to 'Any'. The 'Destination IP' is also set to 'Any'. There are input fields for 'Start' and 'Finish' times, with hints provided for the 'Start' field (192.168.1.100) and the 'Finish' field (192.168.1.200). The 'Log' dropdown is set to 'Never'. The 'Rule Status' is currently unchecked, with an 'Enable' checkbox.

사용 가능한 옵션은 다음과 같이 정의됩니다.

·Always Block — 조건에 매칭할 경우 항상 액세스를 거부합니다. 6단계로 건너뛩니다.

·Always Allow — 조건에 매칭할 경우 항상 액세스를 허용합니다. 6단계로 건너뛩니다.

·일정별 차단 — 사전 구성된 일정 동안 조건이 일치하는 경우 액세스를 거부합니다.

·일정별 허용 — 사전 구성된 일정 중에 조건이 일치하는 경우 액세스를 허용합니다.

5단계. 4단계에서 **일정별 차단** 또는 **일정별 허용**을 선택한 경우 일정 드롭다운 목록에서 적절한 **일정**을 선택합니다.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test\_schedule ▾

Services: test\_schedule\_1 ▾

Source IP: Any ▾

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status:  Enable

**참고:** 일정을 만들거나 편집하려면 일정 구성을 클릭합니다. 자세한 내용 [과 지침은 RV130 및 RV130W에서](#) 일정 구성을 참조하십시오.

6단계. Services(서비스) 드롭다운 목록에서 액세스 규칙이 적용되는 서비스 유형을 선택합니다.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test\_schedule ▾

Services: All Traffic ▾

Source IP:

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:  Enable

**참고:** 서비스를 추가하거나 편집하려면 서비스 구성을 클릭합니다. 자세한 내용과 [지침은 RV130 및 RV130W의 서비스 관리](#) 구성을 참조하십시오.

## 아웃바운드 트래픽에 대한 소스 및 목적지 IP 구성

[액세스 규칙](#) 추가의 3단계에서 연결 유형으로 아웃바운드(LAN > WAN)가 선택된 경우 이 절의 단계를 수행합니다.

**참고:** 액세스 규칙 추가의 3단계에서 인바운드 연결 유형을 선택한 경우 다음 섹션으로 건너

됩니다. [인바운드 트래픽에 대한 소스 및 목적지 IP 구성](#)

1단계. Source IP(소스 IP) 드롭다운 목록에서 소스 IP를 정의할 방법을 선택합니다. 아웃바운드 트래픽의 경우 소스 IP는 방화벽 규칙이 적용될 (LAN의) 주소를 나타냅니다.

The screenshot shows a firewall rule configuration window. The 'Source IP' dropdown menu is open, showing three options: 'Any', 'Single Address', and 'Address Range'. The 'Any' option is currently selected and highlighted in blue. The 'Address Range' option is also visible. Other fields in the form include 'Connection Type' (Outbound (LAN > WAN)), 'Action' (Allow by schedule), 'Schedule' (test\_schedule), 'Services' (VOIP), 'Destination IP' (Any), and 'Log' (Never). There are also 'Configure Schedules' and 'Configure Services' buttons.

사용 가능한 옵션은 다음과 같이 정의됩니다.

- Any — 로컬 네트워크의 IP 주소에서 시작되는 트래픽에 적용됩니다. 따라서 시작 및 완료 필드는 비워 둡니다. 이 옵션을 선택하는 경우 4단계로 건너뜁니다.
- 단일 주소 — 로컬 네트워크의 단일 IP 주소에서 시작되는 트래픽에 적용됩니다. 시작 필드에 IP 주소를 입력합니다.
- 주소 범위 — 로컬 네트워크의 IP 주소 범위에서 시작되는 트래픽에 적용됩니다. 범위를 설정하려면 시작 필드에 범위의 시작 IP 주소를 입력하고 마침 필드에 끝 IP 주소를 입력합니다.

2단계. 1단계에서 단일 주소를 선택한 경우 시작 필드에 액세스 규칙에 적용할 IP 주소를 입력한 다음 4단계로 건너뜁니다. 1단계에서 주소 범위를 선택한 경우 시작 필드에 액세스 규칙에 적용할 시작 IP 주소를 입력합니다.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test\_schedule ▾

Services: VOIP ▾

Source IP: Single Address ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status:  Enable

3단계. 1단계에서 주소 범위를 선택한 경우 *Finish* 필드에 액세스 규칙의 IP 주소 범위를 캡슐화할 끝 IP 주소를 입력합니다.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test\_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status:  Enable

4단계. Destination IP(대상 IP) 드롭다운 목록에서 *대상 IP*를 정의할 방법을 선택합니다. 아웃바운드 트래픽의 경우 Destination IP는 로컬 네트워크에서 트래픽이 허용되거나 거부되는 주소(WAN의 주소)를 의미합니다.

Connection Type: Outbound (LAN > WAN) ▾  
 Action: Allow by schedule ▾  
 Schedule: test\_schedule ▾   
 Services: VOIP ▾   
 Source IP: Address Range ▾  
 Start: 10.10.14.100 (Hint: 192.168.1.100)  
 Finish: 10.10.14.175 (Hint: 192.168.1.200)  
 Destination IP: Any ▾  
 Start:   
 Finish:   
 Log: Never ▾  
 Rule Status:  Enable

사용 가능한 옵션은 다음과 같이 정의됩니다.

- Any — 공용 인터넷의 모든 IP 주소로 향하는 트래픽에 적용됩니다. 따라서 시작 및 완료 필드는 비워 둡니다.
- 단일 주소 — 공용 인터넷의 단일 IP 주소로 향하는 트래픽에 적용됩니다. 시작 필드에 IP 주소를 입력합니다.
- Address Range — 공용 인터넷의 IP 주소 범위로 향하는 트래픽에 적용됩니다. 범위를 설정하려면 시작 필드에 범위의 시작 IP 주소를 입력하고 마침 필드에 끝 IP 주소를 입력합니다.

5단계. 4단계에서 **단일 주소**를 선택한 경우 시작 필드에 액세스 규칙에 적용할 IP 주소를 입력합니다. 4단계에서 **Address Range(주소 범위)**를 선택한 경우 Start(시작) 필드에 액세스 규칙에 적용할 시작 IP 주소를 입력합니다.



Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test\_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start: 192.168.1.100

Finish:

Log: Never ▾

Rule Status:  Enable

6단계. 4단계에서 주소 범위를 선택한 경우 액세스 규칙의 IP 주소 범위를 캡슐화할 끝 IP 주소를 *Finish* 필드에 입력합니다.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test\_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status:  Enable

## 인바운드 트래픽에 대한 소스 및 목적지 IP 구성

액세스 규칙 추가의 3단계에서 인바운드(WAN > LAN) 또는 인바운드(WAN > DMZ)가 연결 유형으로 선택된 경우 이 절의 단계를 수행합니다.

1단계. Source IP(소스 IP) 드롭다운 목록에서 소스 IP를 정의할 방법을 선택합니다. 인바운드 트래픽의 경우 소스 IP는 방화벽 규칙이 적용될 주소(WAN의 주소)를 참조합니다.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:  Enable

사용 가능한 옵션은 다음과 같이 정의됩니다.

·Any — 공용 인터넷의 IP 주소에서 시작되는 트래픽에 적용됩니다. 따라서 시작 및 완료 필드는 비워 둡니다. 이 옵션을 선택하는 경우 4단계로 건너뜁니다.

·단일 주소 — 공용 인터넷의 단일 IP 주소에서 시작되는 트래픽에 적용됩니다. 시작 필드에 IP 주소를 입력합니다.

·주소 범위 — 공용 인터넷의 IP 주소 범위에서 시작되는 트래픽에 적용됩니다. 범위를 설정하려면 시작 필드에 범위의 시작 IP 주소를 입력하고 마침 필드에 끝 IP 주소를 입력합니다.

2단계. 1단계에서 단일 주소를 선택한 경우 시작 필드에 액세스 규칙에 적용할 IP 주소를 입력한 다음 4단계로 건너뜁니다. 1단계에서 주소 범위를 선택한 경우 시작 필드에 액세스 규칙에 적용할 시작 IP 주소를 입력합니다.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:  Enable

3단계. 1단계에서 주소 범위를 선택한 경우 *Finish* 필드에 액세스 규칙의 IP 주소 범위를 캡슐화할 끝 IP 주소를 입력합니다.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:  Enable

4단계. Destination IP(대상 IP) 드롭다운 목록 아래의 *Start(시작)* 필드에 *대상 IP*의 단일 주소를 입력합니다. 인바운드 트래픽의 경우 Destination IP는 공용 인터넷에서 트래픽이 허용되거나 거부되는 주소(LAN)를 나타냅니다.

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test\_schedule ▾

Services: All Traffic ▾

Source IP: Address Range ▾

Start: 192.168.1.100 (Hint: 192.168.1.100)

Finish: 192.168.1.200 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start: 10.10.14.2

Finish:

Log: Never ▾

Rule Status:  Enable

**참고:** 액세스 규칙 추가의 3단계에서 Connection Type(연결 유형)으로 Inbound(WAN > DMZ)가 선택된 경우, 대상 IP의 단일 주소는 활성화된 DMZ 호스트의 IP 주소로 자동으로 구성됩니다.

## 액세스 규칙 로깅 및 활성화

1단계. 패킷이 규칙과 일치할 때마다 라우터가 로그를 생성하도록 하려면 *Log* 드롭다운 목록에서 Always를 선택합니다. 규칙이 일치할 때 로깅이 발생하지 않도록 하려면 Never를 선택합니다.

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾  
Never  
Always

Rule Status:

2단계. 액세스 규칙을 활성화하려면 Enable 확인란을 선택합니다.

### Add Access Rule

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:  Enable

3단계. Save(저장)를 클릭하여 설정을 저장합니다.

### Add Access Rule

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start:  (Hint: 192.168.1.100)

Finish:  (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:  Enable

액세스 규칙 테이블이 새로 구성된 액세스 규칙으로 업데이트됩니다.

## Access Rules



Configuration settings have been saved successfully

### Default Outbound Policy

Policy:  Allow  Deny

### Access Rule Table

Filter: Action matches All

	Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/>	Allow by schedule	VOIP	Enabled	Outbound (LAN > WAN)	10.10.14.100 ~ 10.10.14.175	192.168.1.100 ~ 192.168.1.170	Never

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.