

RV320 및 RV325 VPN 라우터의 액세스 규칙 컨피그레이션

목표

ACL(Access Control Lists)은 특정 사용자에게 트래픽을 보내거나 받는 것을 차단하거나 허용하는 목록입니다. 액세스 규칙은 항상 적용되도록 구성하거나 정의된 일정에 따라 구성할 수 있습니다. 액세스 규칙은 네트워크에 대한 액세스를 허용하거나 거부하기 위해 다양한 기준에 따라 구성됩니다. 액세스 규칙은 액세스 규칙을 라우터에 적용해야 하는 시간을 기반으로 예약됩니다. 이 문서에서는 라우터의 방화벽을 통해 네트워크에 트래픽이 들어갈 수 있는지 아니면 네트워크의 보안을 보장하지 않는지 확인하는 데 사용되는 액세스 규칙 설정 마법사에 대해 간략하게 설명하고 설명합니다.

적용 가능한 디바이스 | 펌웨어 버전

- RV320 Dual WAN VPN Router | V 1.1.0.09([최신 다운로드](#))
- RV325 Gigabit Dual WAN VPN Router | V 1.1.0.09([최신 다운로드](#))

액세스 규칙 컨피그레이션

1단계. 웹 컨피그레이션 유틸리티에 로그인하고 방화벽>액세스 규칙을 선택합니다. Access Rules 페이지가 열립니다.

Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
1	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
1	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
1	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
1	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

액세스 규칙 테이블에는 다음 정보가 포함됩니다.

- Priority — 액세스 규칙의 우선순위를 표시합니다.
- Enable — 액세스 규칙의 활성화 여부를 표시합니다.
- Action — 액세스 규칙이 허용되거나 거부되었음을 표시합니다.
- 서비스 — 서비스 유형을 표시합니다.
- SourceInterface — 액세스 규칙이 적용되는 인터페이스를 표시합니다.
- Source — 소스 디바이스의 IP 주소를 표시합니다.
- Destination — 대상 디바이스의 IP 주소를 표시합니다.
- 시간 — 액세스 규칙을 적용할 시간을 표시합니다.
- 일 — 액세스 규칙이 적용되는 1주일 동안 표시됩니다.

서비스 관리

1단계. 서비스 관리를 클릭하여 새 서비스를 추가합니다. 서비스 관리 테이블 페이지가 열립니다.

Service Management Table				Items 1-5 of 21	5	per page
<input type="checkbox"/>	Service Name	Protocol	Port Range			
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535			
<input type="checkbox"/>	DNS	UDP	53~53			
<input type="checkbox"/>	FTP	TCP	21~21			
<input type="checkbox"/>	HTTP	TCP	80~80			
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080			

Page 1 of 5

2단계. 추가를 클릭하여 새 서비스를 추가합니다.

Service Management Table				Items 1-5 of 21	5	per page
<input type="checkbox"/>	Service Name	Protocol	Port Range			
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535			
<input type="checkbox"/>	DNS	UDP	53~53			
<input type="checkbox"/>	FTP	TCP	21~21			
<input type="checkbox"/>	HTTP	TCP	80~80			
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080			
<input type="checkbox"/>	Database	TCP	520 ~ 520			

Page 1 of 5

3단계. 다음 필드를 구성합니다.

- 서비스 이름 — 요구 사항에 따라 서비스 이름을 지정합니다.
- 프로토콜 — 서비스에 대한 프로토콜 TCP 또는 UDP를 선택합니다.
- 포트 범위 — 요구 사항에 따라 포트 번호 범위를 입력하고 포트 번호는 범위(1-65536)에 있어야 합니다.

4단계. **Save(저장)**를 클릭하여 변경 사항을 저장합니다.

IPv4의 액세스 규칙 컨피그레이션

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 5 5 per page

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Page 1 of 1

1단계. Add를 클릭하여 새 액세스 규칙을 구성합니다.Edit Access Rules 창이 나타납니다.

Edit Access Rules

Services

Action: (dropdown menu with 'Allow' selected and 'Deny' below it, circled in red)

Service: (dropdown menu)

Log: (dropdown menu)

Source Interface: (dropdown menu)

Source IP: (dropdown menu)

Destination IP: (dropdown menu)

Scheduling

Time: (dropdown menu)

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

2단계. 설정하려는 규칙에 대한 트래픽을 허용하거나 제한하려면 Action 드롭다운 목록에서 적절한 옵션을 선택합니다. 액세스 규칙은 다양한 값에 따라 네트워크에 대한 액세스를 제한합니다.

- 허용 — 모든 트래픽을 허용합니다.
- 거부 — 모든 트래픽을 제한합니다.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From:

To:

Effective on:

Mon Tue Wed Thu Fri Sat

3단계. Service(서비스) 드롭다운 목록에서 필터링해야 하는 적절한 서비스를 선택합니다.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

4단계. 로그 드롭다운 목록에서 적절한 로그 옵션을 선택합니다.log 옵션은 디바이스에서 액세스 규칙 집합에 해당하는 트래픽 로그를 유지할지 여부를 결정합니다.

- 이 액세스 규칙과 일치하는 패킷 로깅 — 라우터는 선택한 서비스를 추적하는 로그를 유지합니다.
- Not Log — 라우터가 액세스 규칙에 대한 로그를 보관하지 않습니다.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

5단계. Interface 드롭다운 목록에서 적절한 소스 인터페이스를 선택합니다. 이 인터페이스는 액세스 규칙이 적용되는 인터페이스입니다.

- LAN — 액세스 규칙은 LAN 트래픽에만 영향을 줍니다.
- WAN 1 — 액세스 규칙은 WAN 1 트래픽에만 적용됩니다.
- WAN 2 — 액세스 규칙은 WAN 2 트래픽에만 적용됩니다.
- Any — 액세스 규칙은 디바이스의 인터페이스에 있는 모든 트래픽에 영향을 줍니다.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

6단계. Source IP 드롭다운 목록에서 액세스 규칙이 적용되는 적절한 소스 IP 유형을 선택합니다.

- Any — 디바이스 네트워크의 모든 IP 주소에 규칙이 적용됩니다.
- 단일 — 디바이스의 네트워크에 지정된 단일 IP 주소에만 규칙이 적용됩니다. 인접한 필드에 원하는 IP 주소를 입력합니다.
- 범위 — 디바이스의 네트워크에 지정된 IP 주소 범위만 규칙을 적용합니다. Range(범위)를 선택하는 경우 인접 필드에 범위의 첫 번째 및 마지막 IP 주소를 입력해야 합니다.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP: To

Destination IP:

- ANY
- Single
- Range

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu

7단계. 사용 가능한 드롭다운 목록에서 액세스 규칙이 적용되는 적절한 대상 IP 유형을 선택합니다.

- Any — 모든 대상 IP 주소에 규칙이 적용됩니다.
- 단일 — 지정된 단일 IP 주소에만 규칙이 적용됩니다. 인접한 필드에 원하는 IP 주소를 입력합니다.
- 범위 — 디바이스의 네트워크 외부에 지정된 IP 주소 범위만 규칙을 적용합니다. Range(범위)를 선택하는 경우 인접 필드에 범위의 첫 번째 및 마지막 IP 주소를 입력해야 합니다.

Scheduling

Time:

- Always
- Interval

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

시간 절약: 기본적으로 시간은 Always로 설정됩니다. 특정 시간 또는 일에 액세스 규칙을 적용하려면 8단계에서 11단계로 이동합니다. 그렇지 않은 경우 12단계로 건너뛩니다.

8단계. 드롭다운 목록에서 Interval(간격)을 선택하고, Access 규칙은 특정 시간에 대해 활성화됩니다. 액세스 규칙을 적용할 시간 간격을 입력해야 합니다.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

9단계. 시작 필드에 액세스 목록을 적용할 시간을 입력합니다.시간 형식은 hh:mm입니다.

10단계. 더 이상 To 필드에 액세스 목록을 적용하지 않을 시간을 입력합니다.시간 형식은 hh:mm입니다.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

11단계. 액세스 목록을 적용할 특정 요일의 확인란을 선택합니다.

12단계. 변경 사항을 저장하려면 저장을 누릅니다.

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 6 5 ▾

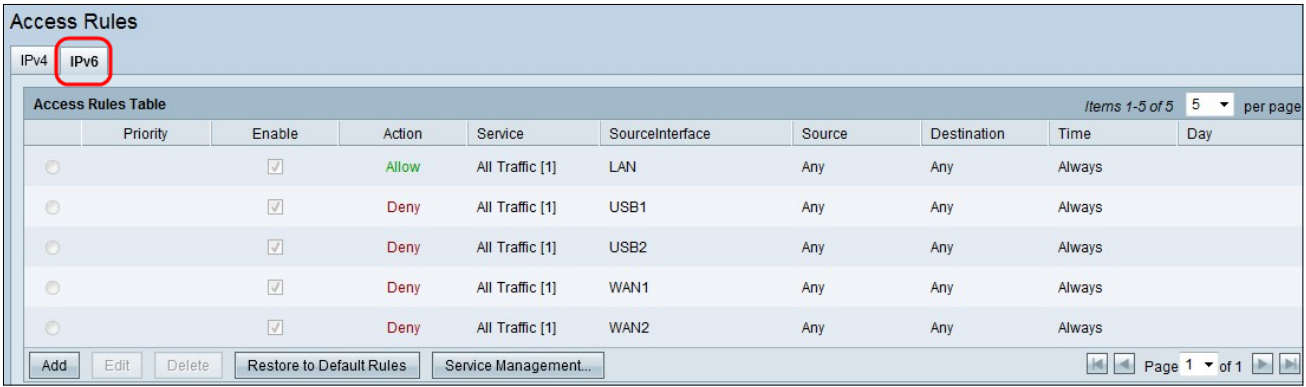
	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input checked="" type="radio"/>	1 ▾	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100	Any	03:00 ~ 07:00	All week
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management...

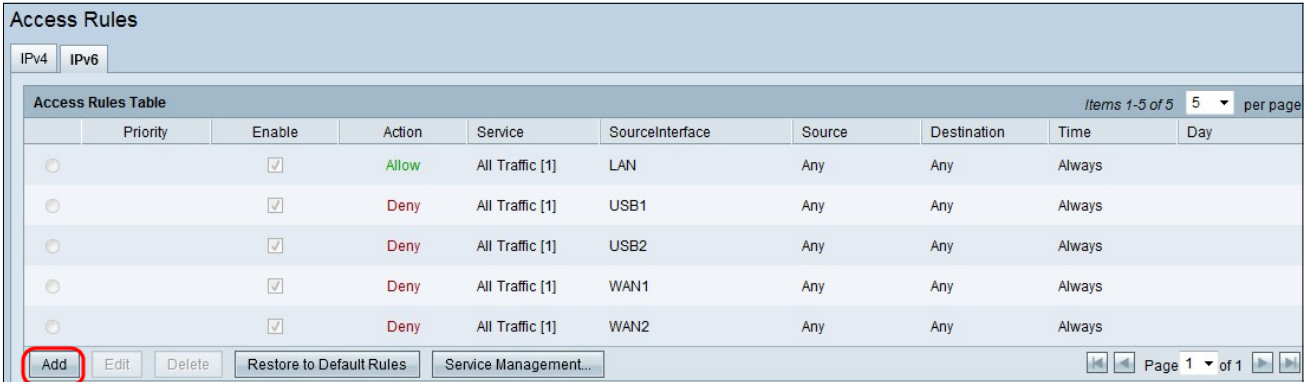
Page 1 of 2

13단계(선택 사항) 기본 규칙을 복원하려면 **Restore to Default Rules**를 클릭합니다.사용자가 구성한 모든 액세스 규칙이 손실됩니다.

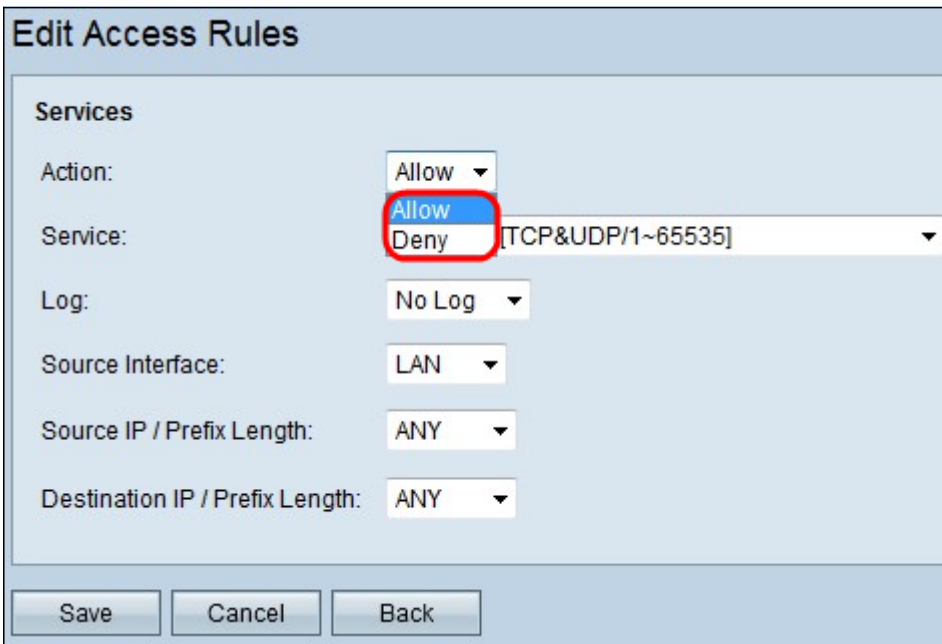
IPv6의 액세스 규칙 컨피그레이션



1단계. IPv6 탭을 클릭하여 IPv6 액세스 규칙을 구성합니다.



2단계. 새 IPv6 액세스 규칙을 추가하려면 Add를 클릭합니다. Edit Access Rules 창이 나타납니다.



3단계. 설정해야 하는 규칙을 허용하거나 제한하려면 조치 드롭다운 목록에서 적절한 옵션을 선택합니다. 액세스 규칙은 특정 서비스 또는 디바이스의 트래픽 액세스를 허용하거나 거부하여 네트워크에 대한 액세스를 제한합니다.

- 허용 — 모든 트래픽을 허용합니다.
- 거부 — 모든 트래픽을 제한합니다.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Save Cancel

- 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]
- SMTP [TCP/25~25]
- TELNET [TCP/23~23]
- TELNET Secondary [TCP/8023~8023]
- TELNET SSL [TCP/992~992]
- DHCP [UDP/67~67]
- L2TP [UDP/1701~1701]
- PPTP [TCP/1723~1723]
- IPSec [UDP/500~500]
- Ping [ICMP/255~255]
- data [TCP/520~521]

4단계. Service(서비스) 드롭다운 목록에서 필터링해야 하는 적절한 서비스를 선택합니다.

참고: 모든 트래픽을 허용하려면 작업이 허용으로 설정된 경우 서비스 드롭다운 목록에서 **All Traffic [TCP&UDP/1~65535]**를 선택합니다. 목록에는 필터링할 수 있는 모든 유형의 서비스가 포함되어 있습니다.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface:

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

- No Log
- Enabled

5단계. 로그 드롭다운 목록에서 적절한 로그 옵션을 선택합니다. log 옵션은 디바이스에서 액세스 규칙 집합에 해당하는 트래픽 로그를 유지할지 여부를 결정합니다.

- Enabled(활성화됨) — 선택한 서비스에 대한 로그 추적을 라우터에서 유지할 수 있습니다.

- Not Log(로그 없음) — 로그 추적을 유지하기 위해 라우터를 비활성화합니다.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length: LAN

Destination IP / Prefix Length: ANY

Save Cancel Back

6단계. Interface(인터페이스) 드롭다운 목록을 클릭하고 적절한 소스 인터페이스를 선택합니다. 이 인터페이스는 액세스 규칙이 적용되는 인터페이스입니다.

- LAN — 액세스 규칙은 LAN 트래픽에만 영향을 줍니다.
- WAN 1 — 액세스 규칙은 WAN 1 트래픽에만 적용됩니다.
- WAN 2 — 액세스 규칙은 WAN 2 트래픽에만 적용됩니다.
- Any — 액세스 규칙은 디바이스의 인터페이스에 있는 모든 트래픽에 영향을 줍니다.

Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

7단계. Source IP/Prefix Length 드롭다운 목록에서 액세스 규칙이 적용되는 적절한 소스 IP 유형을 선택합니다.

- ANY — 디바이스의 네트워크에서 수신되는 모든 패킷에는 규칙이 적용됩니다.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Single ▾ 2607:f0d0:1002:51::4 / 128

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- 단일 — 디바이스의 네트워크에 지정된 단일 IP 주소에만 규칙이 적용됩니다. 인접한 필드에 원하는 IPv6 주소를 입력합니다.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- 서브넷 — 서브넷의 IP 주소에만 규칙이 적용됩니다. 인접 필드에 원하는 서브넷의 IPv6 네트워크 주소 및 접두사 길이를 입력합니다.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

ANY
Single
Subnet

Save Cancel Back

8단계. Destination IP / Prefix Length 드롭다운 목록에서 액세스 규칙이 적용되는 적절한 대상 IP 유형을 선택합니다.

- Any — 모든 대상 IP 주소에 규칙이 적용됩니다.
- 단일 — 디바이스의 네트워크에 지정된 단일 IP 주소에만 규칙이 적용됩니다. 원하는 IPv6 주소를 입력합니다.
- 서브넷 — 서브넷의 IP 주소에만 규칙이 적용됩니다. 인접 필드에 원하는 서브넷의 IPv6 네트워크 주소 및 접두사 길이를 입력합니다.

9단계. 저장을 눌러 변경 사항을 적용합니다.

이 문서와 관련된 비디오 보기...

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