

Konfigurieren von Zugriffsregeln auf Routern der Serien RV160 und RV260

Ziel

Ihr Router ist für den Empfang von Daten aus dem externen Netzwerk zuständig und stellt die erste Verteidigungslinie in Bezug auf die Sicherheit Ihres lokalen Netzwerks dar. Durch die Aktivierung von Zugriffsregeln auf Ihrem Router können Sie Pakete basierend auf bestimmten Parametern wie IP-Adresse oder Portnummer filtern. Mit den unten aufgeführten Schritten soll dieses Dokument Ihnen zeigen, wie Sie Zugriffsregeln konfigurieren, um die in Ihr Netzwerk eingehenden Pakete besser kontrollieren zu können. In diesem Dokument werden auch einige Best Practices für die Verwendung von Zugriffsregeln beschrieben, um das volle Potenzial für die bestmögliche Sicherheit auszuschöpfen.

Anwendbare Geräte

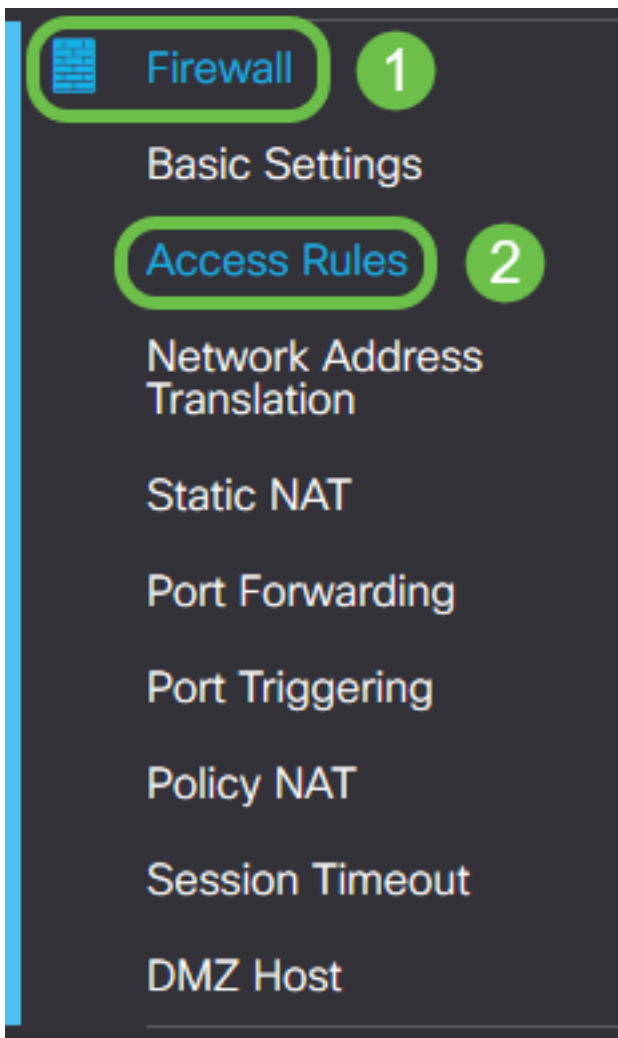
- RV160x
- RV260x

Softwareversion

- 1,0 00,13

Zugriffsregeln konfigurieren

Schritt 1: Wählen Sie im Navigationsbereich auf der linken Seite des Konfigurationsprogramms **Firewall > Access Rules** aus.



Die Seite "Zugriffsregeln" wird angezeigt. Auf dieser Seite gibt es Tabellen mit Listen von Zugriffsregeln und ihren Attributen für IPv4 bzw. IPv6. Hier können Sie eine neue Zugriffsregel hinzufügen, eine vorhandene Regel bearbeiten oder eine vorhandene Regel entfernen.

Hinzufügen/Bearbeiten einer Zugriffsregel

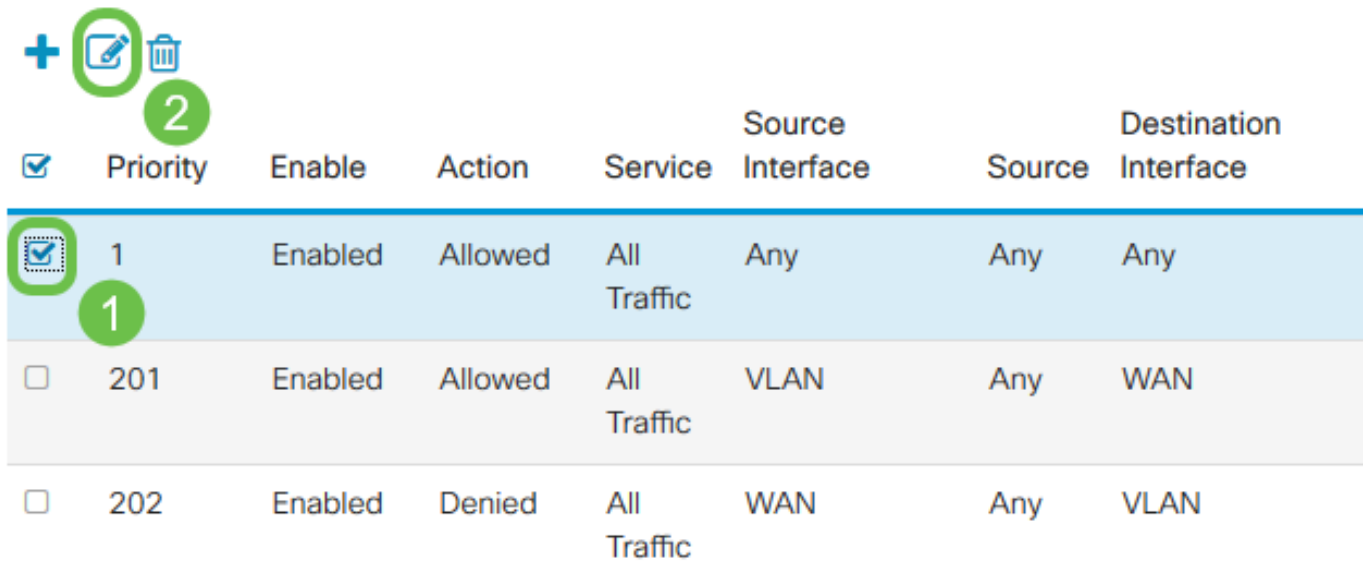
Schritt 2: Um eine neue Zugriffsregel hinzuzufügen, klicken Sie auf das blaue Symbol, um die Tabelle mit den IPv4-Zugriffsregeln oder IPv6-Zugriffsregeln in Abhängigkeit vom Protokoll hinzuzufügen, für das Sie die Regel anwenden möchten. In diesem Fall wird IPv4 verwendet.

IPv4 Access Rules Table



Um einen vorhandenen Eintrag zu bearbeiten, aktivieren Sie das Kontrollkästchen neben der Zugriffsregel, die Sie ändern möchten. Wählen Sie dann das blaue Bearbeitungssymbol oben in der entsprechenden Tabelle aus. Es kann jeweils nur eine Regel zur Bearbeitung ausgewählt werden.

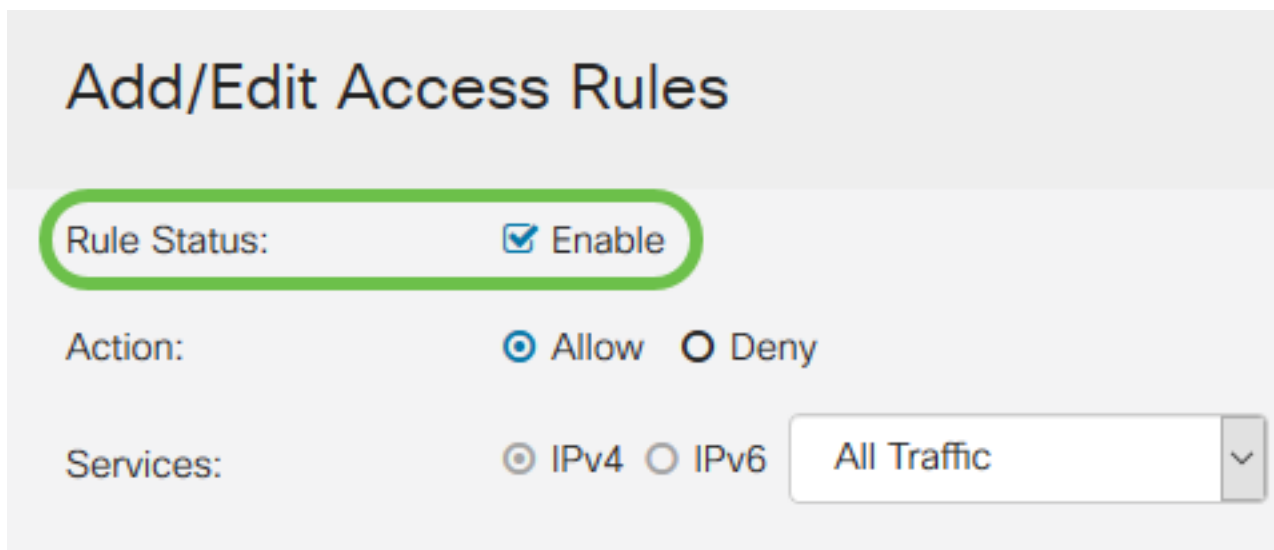
IPv4 Access Rules Table



<input checked="" type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	Any	Any	Any
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN

Die Seite *Zugriffsregeln hinzufügen/bearbeiten* wird angezeigt.

Schritt 3: Aktivieren/Deaktivieren Sie das Kontrollkästchen Regelstatus, um die Zugriffsregel während des Betriebs zu aktivieren oder zu deaktivieren. Dies ist nützlich, wenn Sie eine Zugriffsregel speichern möchten, um sie zu einem späteren Zeitpunkt anzuwenden.



Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6

Schritt 4: Wählen Sie im Feld *Aktion* aus, ob die Regel den Zugriff auf den eingehenden Netzwerkverkehr zulassen oder verweigern soll.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Hinweis: Es wird empfohlen, für die beste Sicherheit Zugriffsregeln festzulegen, die nur den Datenverkehr zulassen, den Sie erwarten, anstatt nur unerwünschten Datenverkehr zu verweigern. So können Sie Ihr Netzwerk besser vor unbekanntem Bedrohungen schützen.

Schritt 5: Wählen Sie im Feld *Services* aus dem Dropdown-Menü den Netzwerkdiensttyp aus, auf den die Zugriffsregel angewendet werden soll.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Hinweis: Das Optionsfeld IPv4 oder IPv6 wird automatisch entsprechend der Tabelle ausgewählt, auf die Sie die Zugriffsregel auf der Seite *Zugriffsregeln* angewendet haben.

Schritt 6: Wählen Sie im Feld *Log (Protokoll)* aus, ob der Router eine Protokollmeldung generieren soll, sobald Pakete, die in Ihr Netzwerk eingehen, mit den angewendeten Regeln übereinstimmen.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Schritt 7: Wählen Sie aus der Dropdown-Liste *Source Interface* (*Quellschnittstelle*) die Netzwerkschnittstelle für eingehende Pakete aus, auf die die Zugriffsregel angewendet wird.

Log: Always Never

Source Interface: Any

Source Address: WAN
USB
VLAN1
Any

Destination Interface: Any

Destination Address: Any

Schritt 8: Wählen Sie aus der Dropdown-Liste *Quelladresse* den Typ der eingehenden Adresse aus, auf die die Zugriffsregel angewendet wird. Folgende Optionen sind verfügbar:

- Any (Alle): Die Regel gilt für alle eingehenden IP-Adressen.
- Einzel: Die Regel gilt für eine einzelne definierte IP-Adresse.
- Subnetz - Die Regel gilt für ein definiertes Subnetz eines Netzwerks
- IP Range (IP-Bereich): Die Regel gilt für einen bestimmten Bereich von IP-Adressen.

Hinweis: Wenn Sie Single (Einzel), Subnet (Subnetz) oder IP Range (IP-Bereich) auswählen, werden rechts neben dem Dropdown-Menü entsprechende Felder angezeigt, in denen Sie Adressdetails eingeben können. In diesem Beispiel wird ein IP-Bereich eingegeben, um zu veranschaulichen.

Source Interface: Any

Source Address: IP Range 1.2.3.1 To 1.2.3.100 (1.2.3.1 To 1.2.3.4)

Destination Interface: Any
Single
Subnet
IP Range

Destination Address:

Schritt 9: Wählen Sie aus der Dropdown-Liste *Destination Interface* (Zielschnittstelle) die Netzwerkschnittstelle für ausgehende Pakete aus, auf die die Zugriffsregel angewendet wird.

Log: Always Never

Source Interface: Any

Source Address: Any

Destination Interface: Any

Destination Address: WAN
USB
VLAN1
Any

Schedule

Schritt 10: Wählen Sie aus der Dropdown-Liste *Destination Address* (Zieladresse) den Typ der ausgehenden Adresse aus, auf die die Zugriffsregel angewendet wird. Folgende Optionen sind verfügbar:

- Any (Alle): Die Regel gilt für alle ausgehenden IP-Adressen.
- Einzel: Die Regel gilt für eine einzelne definierte IP-Adresse.
- Subnetz - Die Regel gilt für ein definiertes Subnetz eines Netzwerks
- IP Range (IP-Bereich): Die Regel gilt für einen bestimmten Bereich von IP-Adressen.

Hinweis: Wenn Sie Single (Einzel), Subnet (Subnetz) oder IP Range (IP-Bereich) auswählen, werden rechts neben dem Dropdown-Menü entsprechende Felder angezeigt, in denen Sie Adressdetails eingeben können. In diesem Beispiel wird ein Subnetz eingegeben, um zu veranschaulichen.

Destination Interface: Any

Destination Address: Subnet 1.2.3.4 / 16 (1.2.3.4 / 32)

Schedule

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

Schritt 11: Wählen Sie aus der Dropdown-Liste *Schedule Name* (Name des Zeitplans) den Zeitplan aus, für den die Zugriffsregel gelten soll.

Schedule

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

Hinweis: Zur Erhöhung der Sicherheit empfiehlt es sich, den nicht kritischen Netzwerkzugriff auf die Geschäftszeiten zu beschränken, um sicherzustellen, dass unerwünschte Verbindungen verweigert werden, wenn Ihr Unternehmen nicht in Betrieb ist.

Hinweis: Klicken Sie auf den Link rechts im Dropdown-Menü *Schedule Name* (*Planungsname*), um die Zeitpläne für Zugriffsregeln zu konfigurieren. Weitere Informationen zur Konfiguration dieser Zeitpläne finden Sie [hier](#).

Schritt 12: Wenn Sie mit der Konfiguration der Zugriffsregel zufrieden sind, klicken Sie zur Bestätigung auf **Übernehmen**.

Add/Edit Access Rules [Apply](#) [Cancel](#)

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

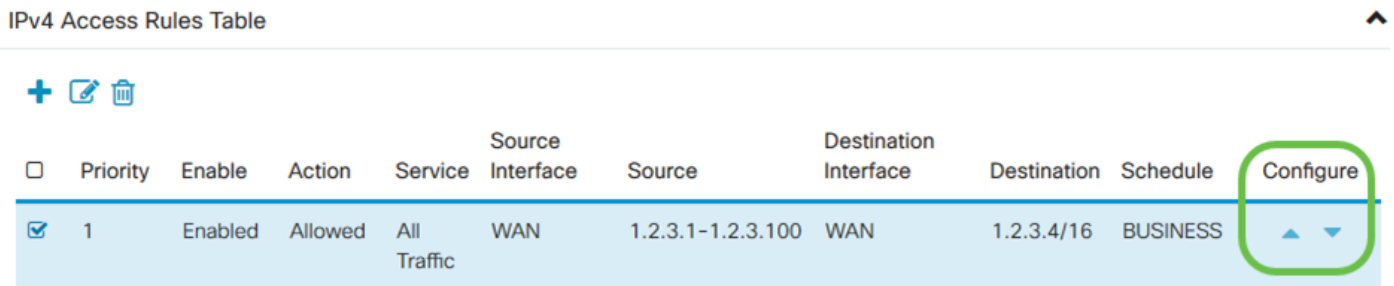
Source Interface: WAN


Sie kehren nun zur Hauptseite *für Zugriffsregeln* zurück.

Hinweis: Wenn eine neue Zugriffsregel erstellt wird, wird ihre Priorität am Ende der Liste platziert. Das bedeutet, dass bei Konflikten zwischen einer Zugriffsregel und einer anderen für einen bestimmten Parameter die Einschränkungen der Regel höherer Priorität Vorrang haben. Um eine Regel mit Priorität nach oben oder unten zu verschieben, können Sie die blauen Pfeile in der

Spalte Konfigurieren verwenden.

IPv4 Access Rules Table



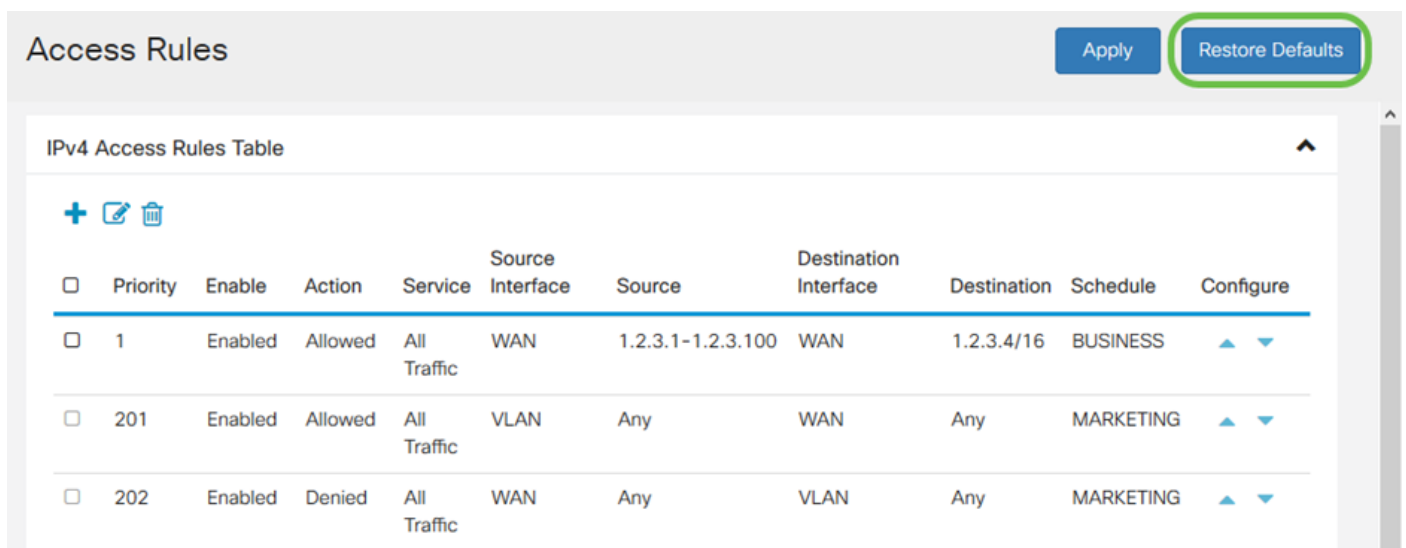
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	




Schritt 13 (optional). Wenn Sie die Liste der Zugriffsregeln auf die Standardeinstellungen zurücksetzen möchten, klicken Sie in der rechten oberen Ecke der Seite auf **Standardeinstellungen wiederherstellen**.

Access Rules

Apply **Restore Defaults**

IPv4 Access Rules Table

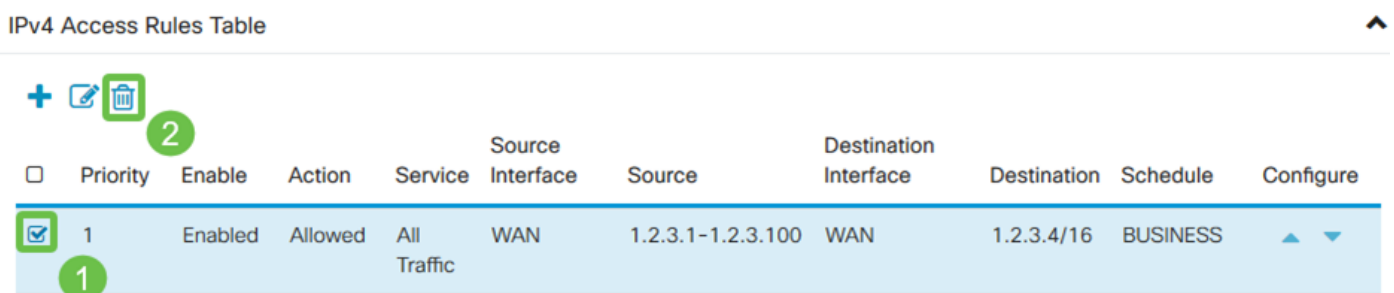



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN	Any	MARKETING	
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN	Any	MARKETING	

Entfernen einer Zugriffsregel

Schritt 14: Um eine Zugriffsregel aus der Liste zu entfernen, aktivieren Sie einfach das Kontrollkästchen für die entsprechende Regel, die Sie entfernen möchten. Wählen Sie dann das blaue Abfallimersymbol oben in der Liste aus. Mehrere Zugriffsregleinträge können gleichzeitig entfernt werden.

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	

Service-Management

Mit der Dienstverwaltung können Sie vorhandene Netzwerkdienste nach Portnummer, Protokoll und anderen Details hinzufügen oder bearbeiten. Diese Netzwerkserviceskalierung ist bei der Konfiguration der Zugriffsregeln im Dropdown-Menü "Services" (Dienste) verfügbar. Über das Konfigurationsmenü der Service-Management-Liste können Sie benutzerdefinierte Services erstellen, die dann auf die Zugriffsregeln angewendet werden können, um die Kontrolle über den in Ihr Netzwerk eingehenden Datenverkehr zu verbessern. Weitere Informationen zur Konfiguration der Service-Verwaltung erhalten Sie [hier](#).

Schlussfolgerung

Zugriffsregeln sind bei entsprechender Anwendung ein nützliches Tool zum Sichern Ihrer WAN-Verbindung. Der obige Leitfaden und die vorgestellten Vorgehensweisen helfen Ihnen bei der Konfiguration sicherer Zugriffsregeln für Ihren RV160x- oder RV260x-Router.