Konfigurieren von Zugriffsregeln auf einem Router der Serie RV34x

Ziel

Der RV340 Dual-WAN VPN-Router ist ein benutzerfreundliches, flexibles und leistungsstarkes Gerät, das sich hervorragend für kleine und mittlere Unternehmen eignet. Mit zusätzlichen Sicherheitsfunktionen wie Webfilterung, Anwendungskontrolle und IP Source Guard. Die neue RV340 bietet sichere kabelgebundene Breitbandverbindungen für kleine Büros und Remote-Mitarbeiter. Diese neuen Sicherheitsfunktionen erleichtern zudem die Feinabstimmung der zulässigen Aktivitäten im Netzwerk.

Zugriffsregeln oder Richtlinien auf dem Router der Serie RV34x ermöglichen die Konfiguration von Regeln zur Erhöhung der Sicherheit im Netzwerk. Eine Kombination von Regeln und eine Zugriffssteuerungsliste (ACL). ACLs sind Listen, die das Senden von Datenverkehr an und von bestimmten Benutzern blockieren oder zulassen. Zugriffsregeln können so konfiguriert werden, dass sie jederzeit gültig sind oder auf definierten Zeitplänen basieren.

ACLs verfügen am Ende der Liste über eine implizite Verweigerung. Wenn Sie diese also nicht explizit zulassen, kann der Datenverkehr nicht weitergeleitet werden. Wenn Sie z. B. allen Benutzern den Zugriff auf ein Netzwerk über den Router gestatten möchten, mit Ausnahme bestimmter Adressen, dann müssen Sie die jeweiligen Adressen verweigern und dann alle anderen zulassen.

In diesem Artikel erfahren Sie, wie Sie Zugriffsregeln auf einem Router der Serie RV34x konfigurieren.

Anwendbare Geräte

- Serie RV34x

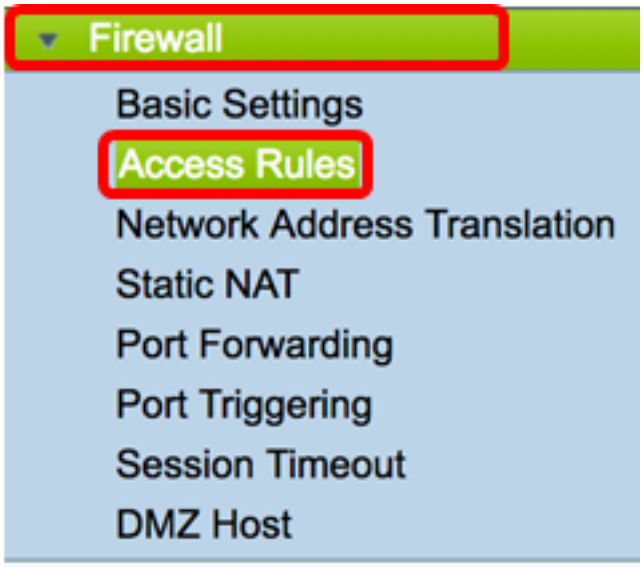
Softwareversion

- 1,0/1,16
  - Seit der Veröffentlichung dieses Artikels ist eine Firmware-Aktualisierung der Benutzeroberfläche verfügbar. Klicken Sie hier, um zur Download-Seite zu gelangen, und suchen Sie dort Ihr Produkt.

Konfigurieren einer Zugriffsregel für einen Router der Serie RV34x

Erstellen einer Zugriffsregel

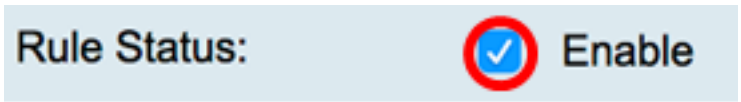
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Firewall > Access Rules aus**.



Schritt 2: Klicken Sie in der Tabelle mit den IPv4- oder IPv6-Zugriffsregeln auf **Hinzufügen**, um eine neue Regel zu erstellen.

Hinweis: Auf dem Router der Serie RV34x können bis zu 202 Regeln konfiguriert werden. In diesem Beispiel wird IPv4 verwendet.

Schritt 3: Aktivieren Sie das Kontrollkästchen **Regelstatus aktivieren**, um die Regel zu aktivieren.

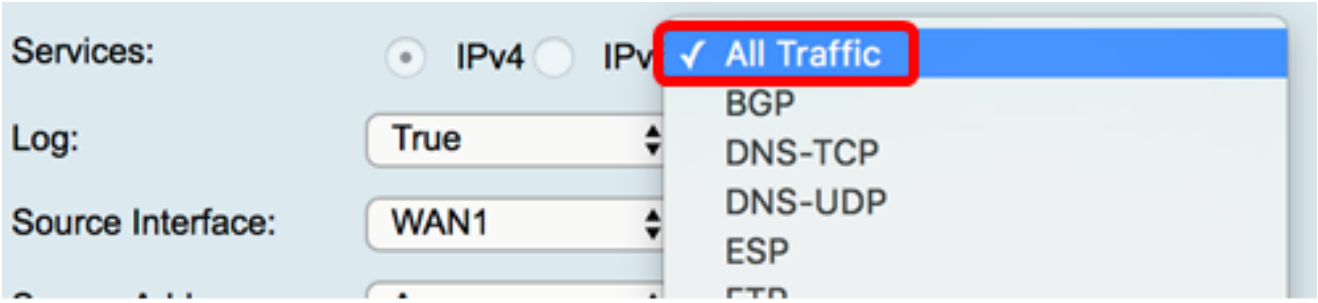


Schritt 4: Wählen Sie im Dropdown-Menü Aktion aus, ob die Richtlinie Daten zulassen oder ablehnen soll.

Hinweis: In diesem Beispiel wird Allow ausgewählt.

Schritt 5: Wählen Sie im Dropdown-Menü Services (Dienste) die Art des Datenverkehrs aus, der vom Router zugelassen oder abgelehnt wird.

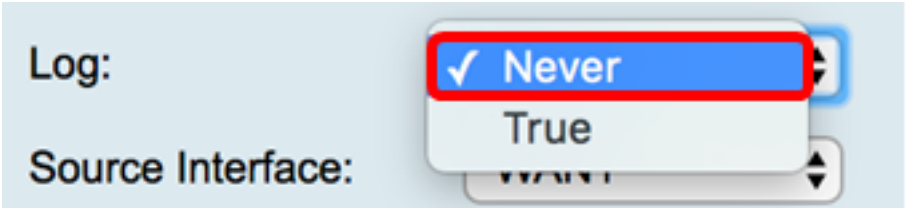
Hinweis: In diesem Beispiel wird der gesamte Datenverkehr ausgewählt. Der gesamte Datenverkehr wird zugelassen.



Schritt 6: Wählen Sie im Dropdown-Menü Log (Protokoll) eine Option aus, um zu bestimmen, ob der Router den zulässigen oder abgelehnten Datenverkehr protokolliert. Folgende Optionen stehen zur Verfügung:

- Niemals - Der Router protokolliert niemals Datenverkehr, der zugelassen und abgelehnt wurde.
- True - Der Router protokolliert den Datenverkehr, der der Richtlinie entspricht.

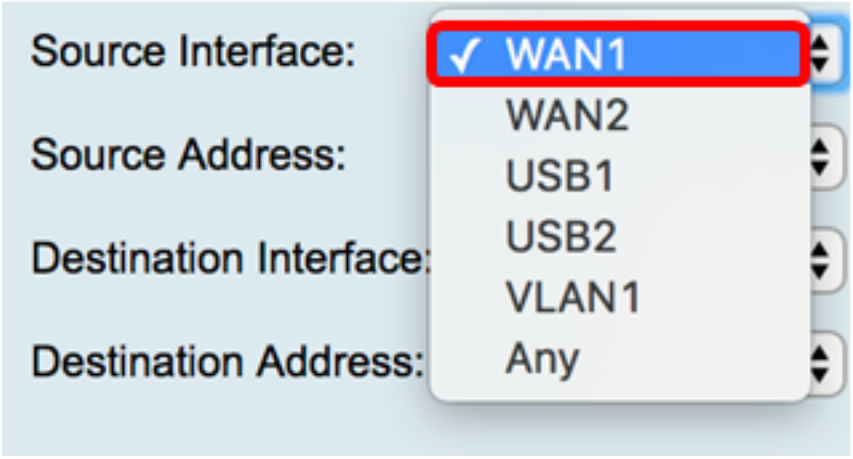
Hinweis: In diesem Beispiel wird Nie ausgewählt.



Schritt 7: Wählen Sie im Dropdown-Menü Source Interface (Quellschnittstelle) eine Schnittstelle für den eingehenden oder eingehenden Datenverkehr aus, auf die die Zugriffsrichtlinie angewendet werden soll. Folgende Optionen sind verfügbar:

- WAN1 - Die Richtlinie gilt nur für den Datenverkehr von WAN1.
- WAN2 - Die Richtlinie gilt nur für den Datenverkehr von WAN2.
- USB1: Die Richtlinie gilt nur für den Datenverkehr von USB1.
- USB2: Die Richtlinie gilt nur für den Datenverkehr von USB2.
- VLAN1 - Die Richtlinie gilt nur für das Verkehrs-VLAN1.
- Any (Beliebig): Die Richtlinie gilt für jede Schnittstelle.

Hinweis: Wenn ein zusätzliches VLAN (Virtual Local Area Network) konfiguriert wurde, wird die VLAN-Option in der Liste angezeigt. In diesem Beispiel wird WAN1 ausgewählt.



Schritt 8: Wählen Sie im Dropdown-Menü Quelladresse eine Quelle aus, um die Richtlinie anzuwenden. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Die Richtlinie gilt für alle IP-Adressen im Netzwerk. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 12 fort.
- Single IP (Einzelne IP): Die Richtlinie gilt für einen einzelnen Host oder eine einzelne IP-Adresse. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 9 fort.
- IP Range (IP-Bereich): Die Richtlinie gilt für einen Satz oder Bereich von IP-Adressen. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 10 fort.
- Subnetz - Die Richtlinie gilt für ein gesamtes Subnetz. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 11 fort.

Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

Schritt 9: (Optional) In Schritt 8 wurde eine einzelne IP ausgewählt. Geben Sie eine einzelne IP-Adresse für die Richtlinie ein, und fahren Sie dann mit Schritt 12 fort.

Hinweis: In diesem Beispiel wird 200.200.22.52 verwendet.

Schritt 10: (Optional) Wenn IP Range (IP-Bereich) in Schritt 8 ausgewählt wurde, geben Sie die Start- und End-IP-Adressen in die entsprechenden IP-Adressfelder ein.

Hinweis: In diesem Beispiel wird 200.200.22.22 als Start-IP-Adresse und 200.200.22.34 als End-IP-Adresse verwendet.

Schritt 11: (Optional) Wenn in Schritt 8 Subnetz ausgewählt wurde, geben Sie die Netzwerk-

ID und die entsprechende Subnetzmaske ein, um die Richtlinie anzuwenden.

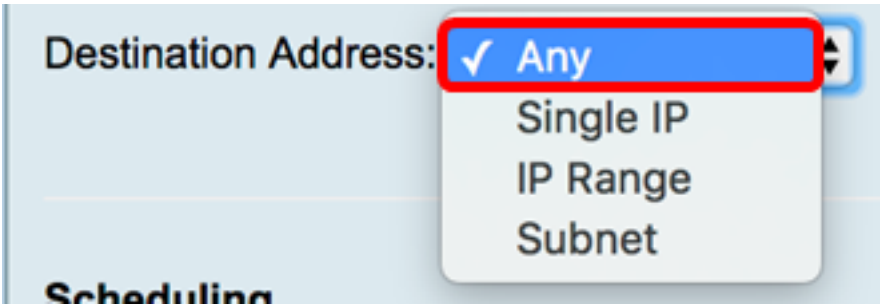
Hinweis: In diesem Beispiel wird 200.200.22.1 als Subnetz-ID und 24 als Subnetzmaske verwendet.

Schritt 12: Wählen Sie im Dropdown-Menü Destination Interface (Zielschnittstelle) eine Schnittstelle für den ausgehenden oder ausgehenden Datenverkehr aus, auf die die Zugriffsrichtlinie angewendet werden soll. Die Optionen sind WAN1, WAN2, USB1, USB2, VLAN1 und Any.

Hinweis: In diesem Beispiel wird WAN1 ausgewählt.

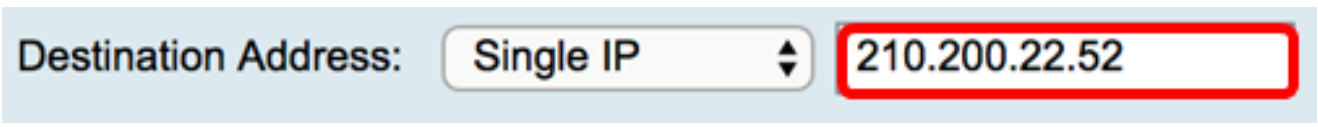
Schritt 13: Wählen Sie im Dropdown-Menü Destination Address (Zieladresse) ein Ziel aus, das die Richtlinie anwendet. Die Optionen sind Any (Beliebig), Single IP (eine IP-Adresse), IP Range (IP-Bereich) und Subnet (Subnetz).

Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt. Fahren Sie mit Schritt 17 fort.



Schritt 14: (Optional) Wenn in Schritt 13 eine einzelne IP-Adresse ausgewählt wurde, geben Sie eine einzige IP-Adresse für die Richtlinie ein, die angewendet werden soll.

Hinweis: In diesem Beispiel wird 210.200.22.52 verwendet.



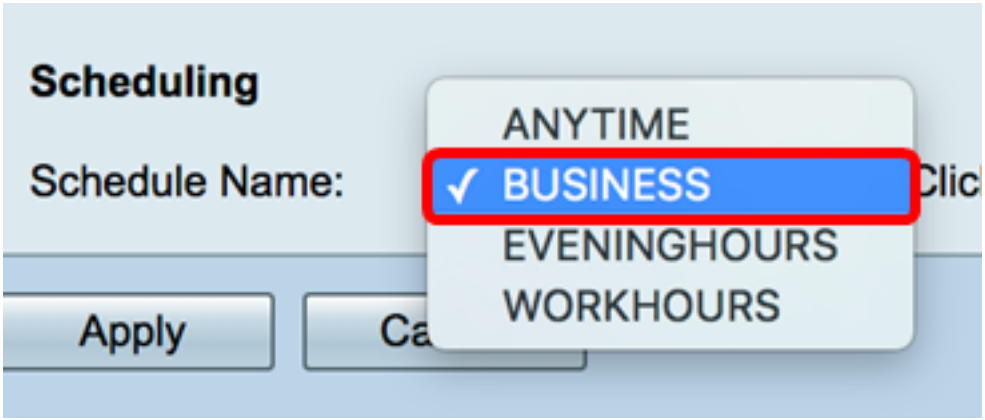
Schritt 15: (Optional) Wenn IP Range (IP-Bereich) in Schritt 13 ausgewählt wurde, geben Sie die Start- und End-IP-Adressen in die entsprechenden IP-Adressfelder ein.

Hinweis: In diesem Beispiel wird 210.200.27.22 als Start-IP-Adresse und 210.200.27.34 als End-IP-Adresse verwendet. Fahren Sie mit Schritt 17 fort.

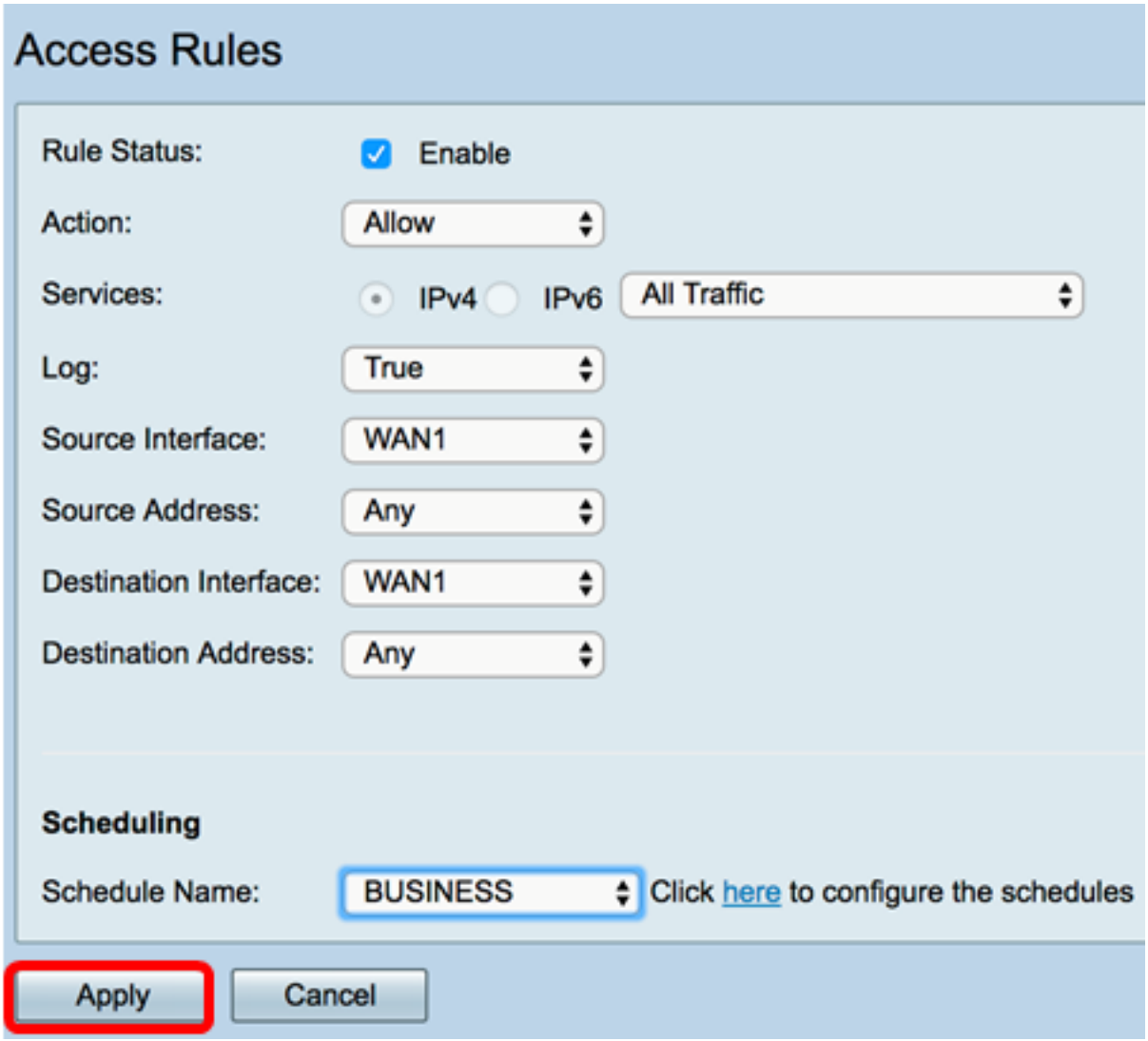
Schritt 16: (Optional) Wenn in Schritt 13 Subnetz ausgewählt wurde, geben Sie die Netzwerkadresse und die entsprechende Subnetzmaske ein, um die Richtlinie anzuwenden.

Hinweis: In diesem Beispiel wird 210.200.27.1 als Subnetzadresse und 24 als Subnetzmaske verwendet.

Schritt 17: Wählen Sie in der Dropdown-Liste Schedule Name (Name des Zeitplans) einen Zeitplan für die Anwendung dieser Richtlinie aus. Um zu erfahren, wie Sie einen Zeitplan konfigurieren, klicken Sie hier.



Schritt 18: Klicken Sie auf **Übernehmen**.

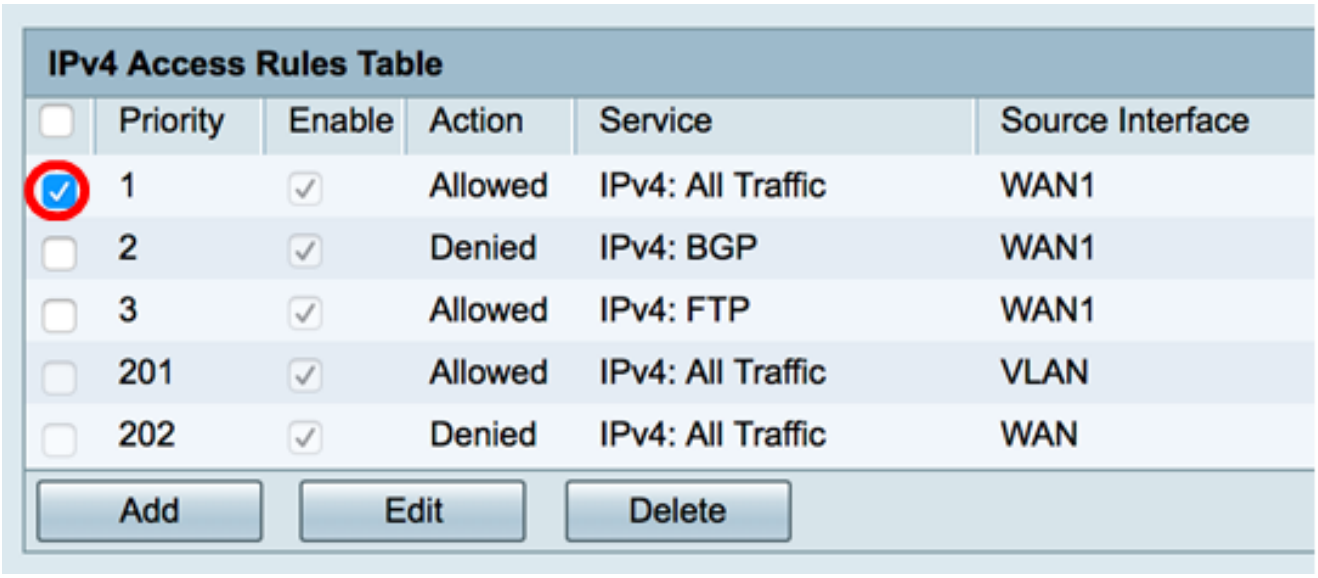


Sie sollten jetzt erfolgreich eine Zugriffsregel für einen Router der RV-Serie erstellt haben.

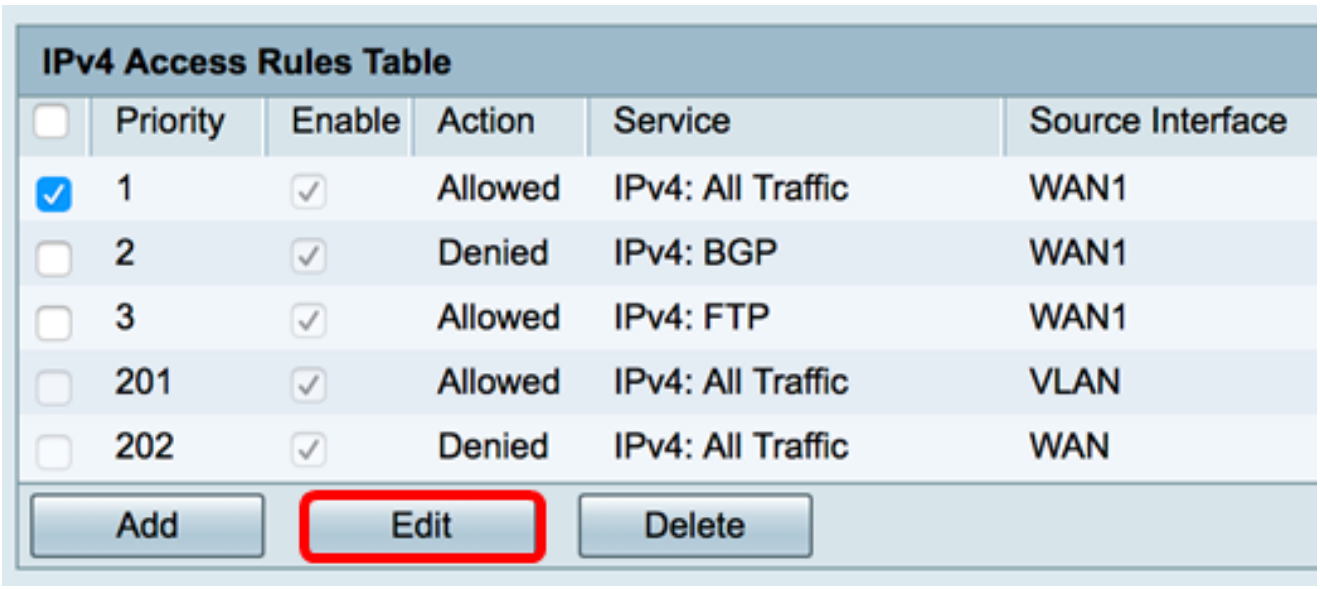
Bearbeiten einer Zugriffsregel

Schritt 1: Aktivieren Sie in der Tabelle mit den IPv4- oder IPv6-Zugriffsregeln das Kontrollkästchen neben der Zugriffsregel, die Sie konfigurieren möchten.

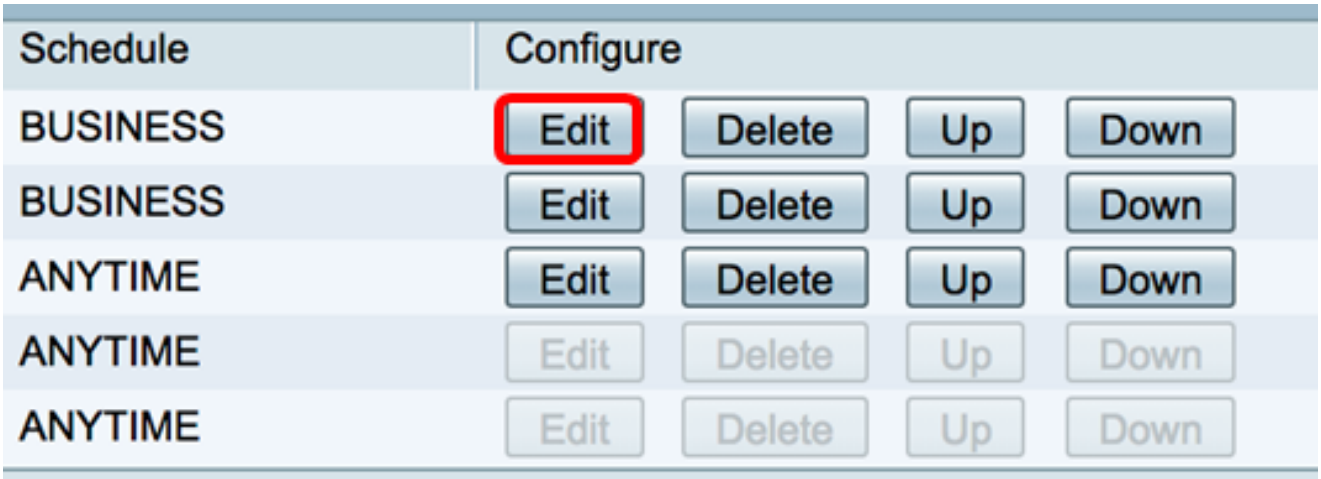
Hinweis: In diesem Beispiel wird in der Tabelle mit den IPv4-Zugriffsregeln die Priorität 1 ausgewählt.



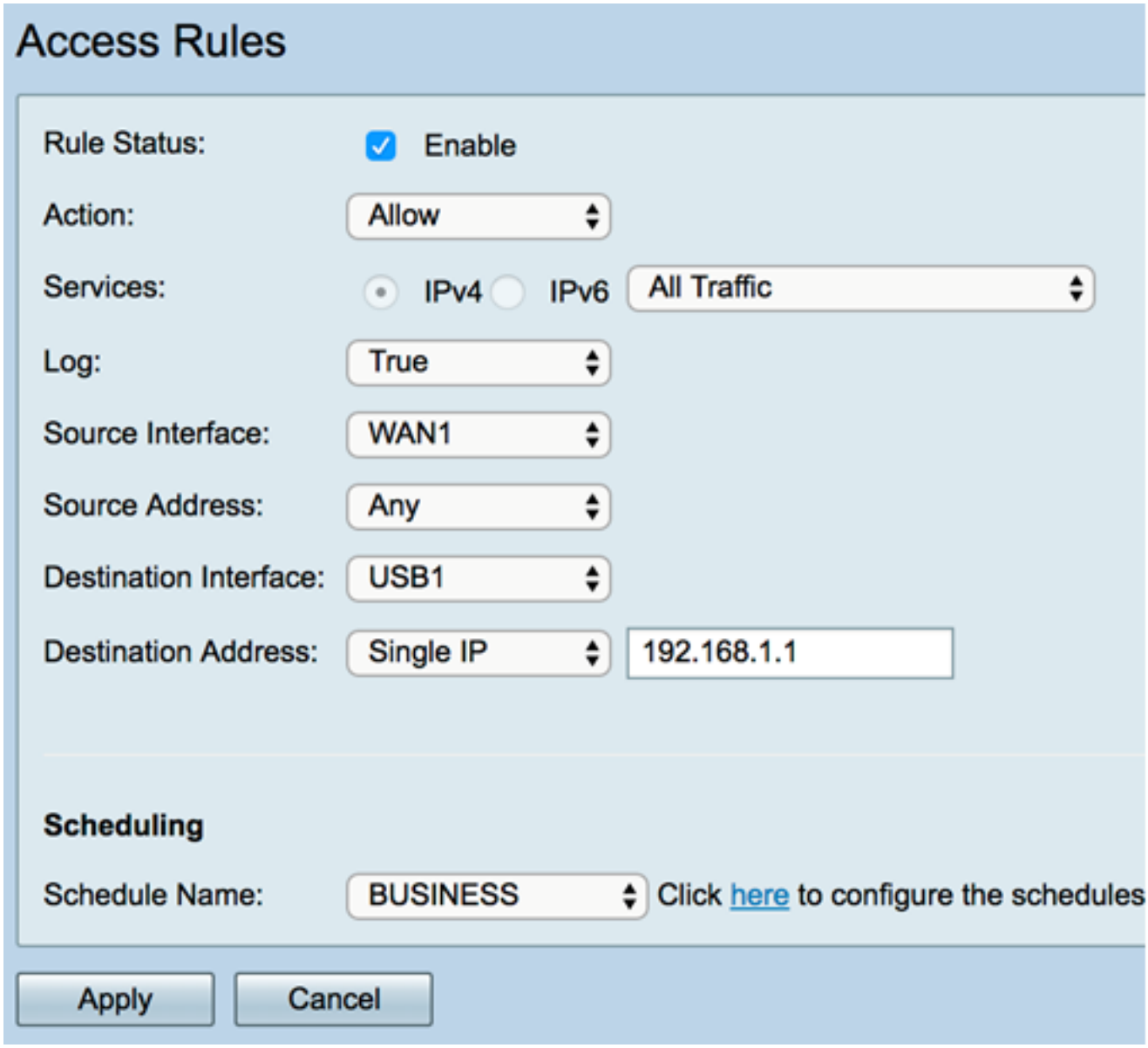
Schritt 2: Klicken Sie auf **Bearbeiten**.



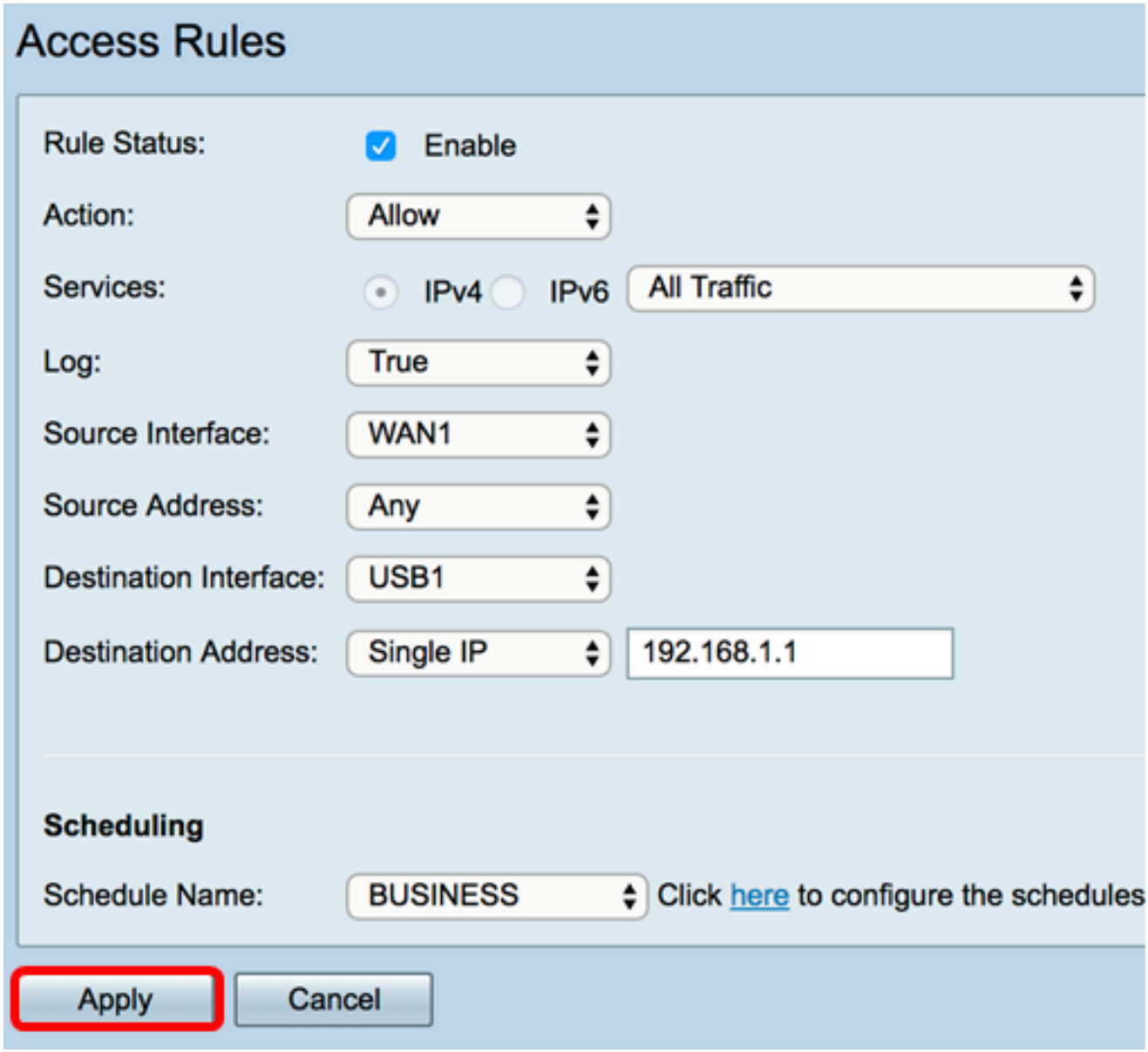
Schritt 3: (Optional) Klicken Sie in der Spalte Konfigurieren auf die Schaltfläche **Bearbeiten** in der Zeile der gewünschten Zugriffsregel.



Schritt 4: Aktualisieren Sie die erforderlichen Parameter.



Schritt 5: Klicken Sie auf **Übernehmen**.



Schritt 6: (Optional) Um die Priorität einer Zugriffsregel in der Spalte Konfigurieren zu ändern, klicken Sie auf die **Nach-oben** oder **Nach-unten**-Schaltfläche der Zugriffsregel, die Sie verschieben möchten.

Hinweis: Wenn eine Zugriffsregel nach oben oder unten verschoben wird, bewegt sie sich einen Schritt über oder unter die ursprüngliche Position. In diesem Beispiel wird Priorität 1 deaktiviert.

Hinweis: In diesem Beispiel ist Priorität 1 jetzt Priorität 2.

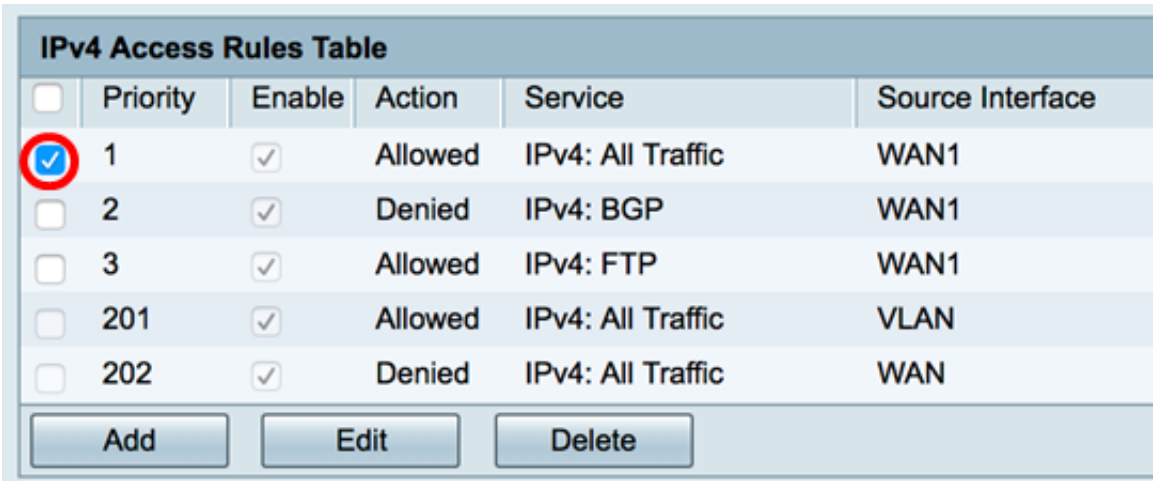
Schritt 7: Klicken Sie auf **Übernehmen**.

Sie sollten jetzt eine Zugriffsregel für einen Router der Serie RV34x erfolgreich bearbeitet haben.

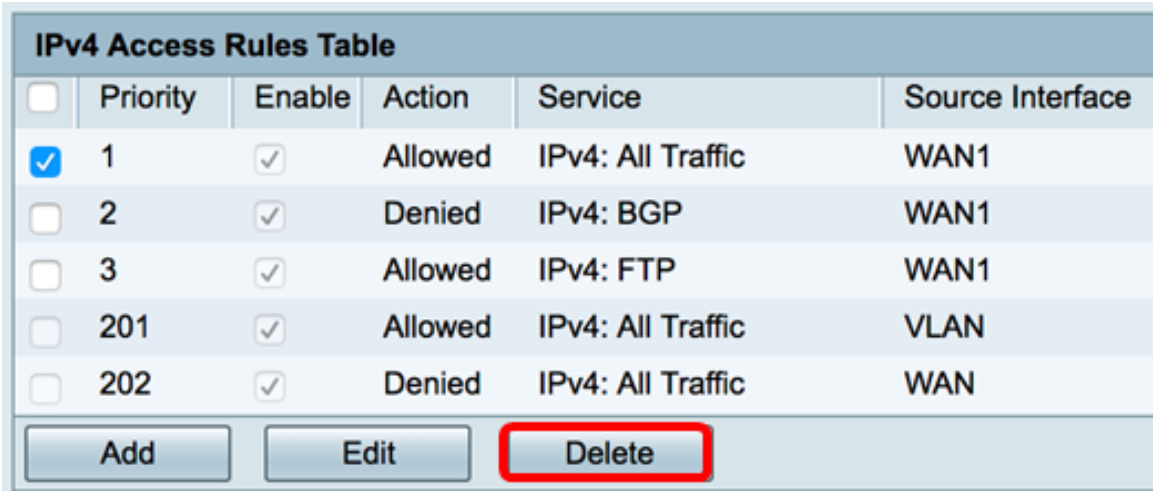
Löschen einer Zugriffsregel

Schritt 1: Aktivieren Sie in der Tabelle mit den IPv4- oder IPv6-Zugriffsregeln das Kontrollkästchen neben der Zugriffsregel, die Sie löschen möchten.

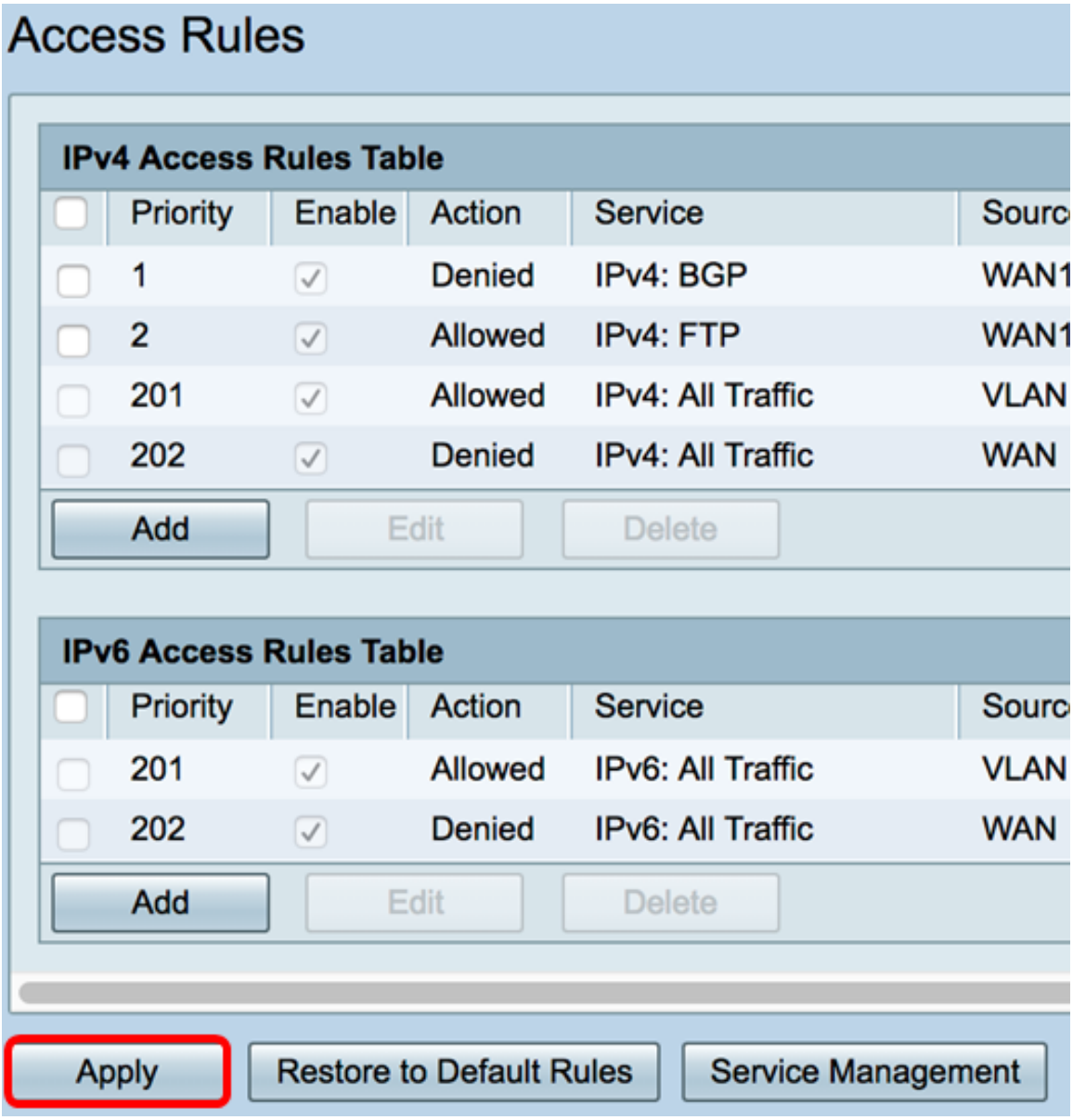
Hinweis: In diesem Beispiel wird in der Tabelle mit den IPv4-Zugriffsregeln die Priorität 1 ausgewählt.



Schritt 2: Klicken Sie unter der Tabelle auf **Löschen**, oder klicken Sie in der Spalte Konfigurieren auf die Schaltfläche Löschen.



Schritt 3: Klicken Sie auf **Übernehmen**.



Sie sollten jetzt eine Zugriffsregel für den Router der Serie RV34x erfolgreich gelöscht haben.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.