Konfigurieren der Service-Verwaltung für Zugriffsregeln auf den Routern RV160X/RV260X

Ziel

In diesem Artikel erfahren Sie, wie Sie Zugriffsregeln für die Router RV160 und RV260 konfigurieren.

Einführung

Zugriffsregeln definieren die Regeln, die der Datenverkehr erfüllen muss, um eine Schnittstelle zu passieren. Eine Zugriffsregel erlaubt oder verweigert Datenverkehr basierend auf dem Protokoll, einer Quell- und Ziel-IP-Adresse oder dem Netzwerk und optional den Quell- und Zielports.

Wenn Sie Zugriffsregeln für Geräte bereitstellen, werden diese zu einem oder mehreren Zugriffskontrolleinträgen (ACEs) für Zugriffskontrolllisten (ACLs), die an Schnittstellen angeschlossen sind. In der Regel sind diese Regeln die erste Sicherheitsrichtlinie, die auf Pakete angewendet wird. Sie sind Ihre erste Verteidigungslinie. Jedes Paket, das an einer Schnittstelle ankommt, wird anhand der von Ihnen festgelegten Kriterien überprüft, ob das Paket weitergeleitet oder verworfen werden soll. Wenn Sie Zugriffsregeln in die ausgehende Richtung definieren, werden auch Pakete analysiert, bevor sie eine Schnittstelle verlassen dürfen.

Anwendbare Geräte

- RV160
- RV260

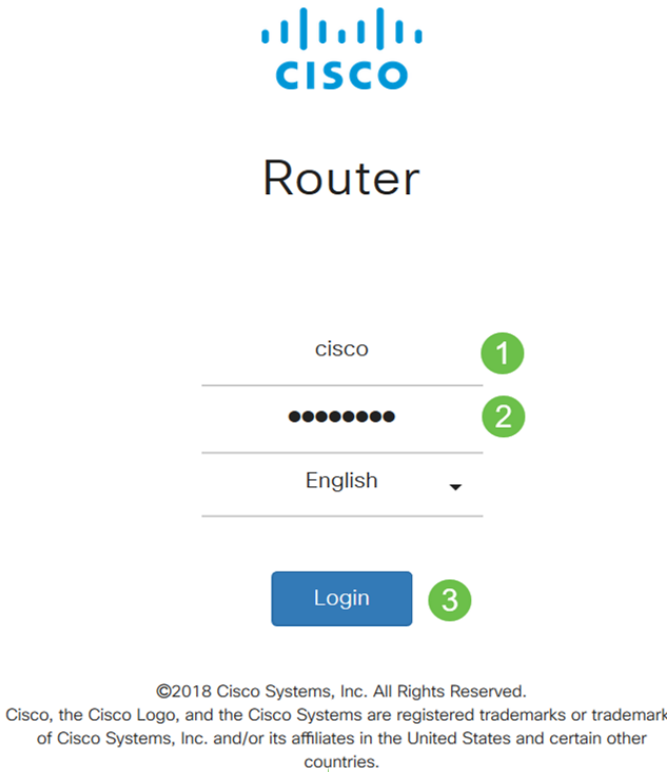
Softwareversion

- 1,0 00,15

Zugriffsregeln konfigurieren

Führen Sie die folgenden Schritte aus, um die Zugriffsregeln für den RV160/RV260 zu konfigurieren.

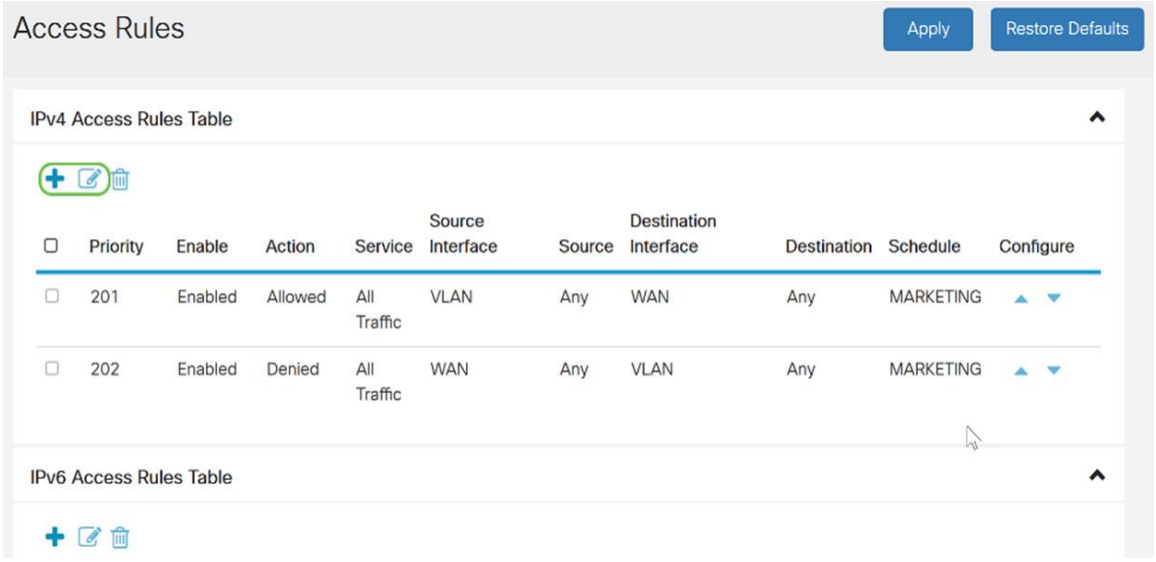
Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres Routers an.



Hinweis: In diesem Artikel wird die RV260W zum Konfigurieren von Zugriffsregeln verwendet. Die Konfiguration kann je nach verwendetem Modell variieren.

Schritt 2: Navigieren Sie zu **Firewall > Zugriffsregeln**.

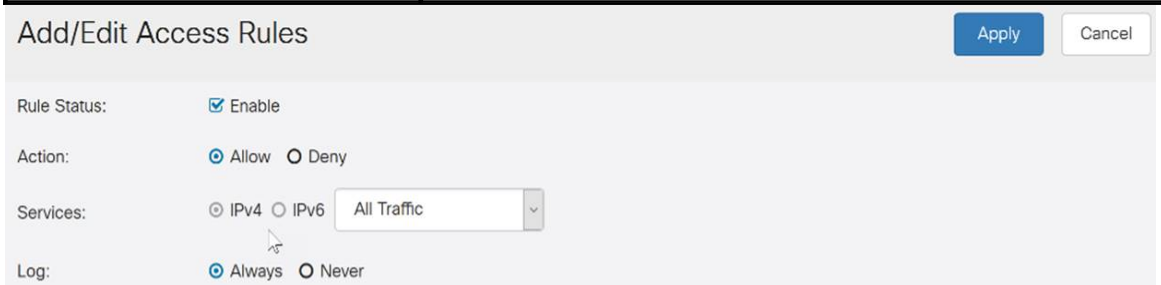
Schritt 3: Klicken Sie in der *Tabelle mit IPv4- oder IPv6-Zugriffsregeln* auf **Hinzufügen**, oder wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**.



Schritt 4: Geben Sie im Abschnitt *Zugriffsregeln hinzufügen/bearbeiten* die folgenden Felder ein.

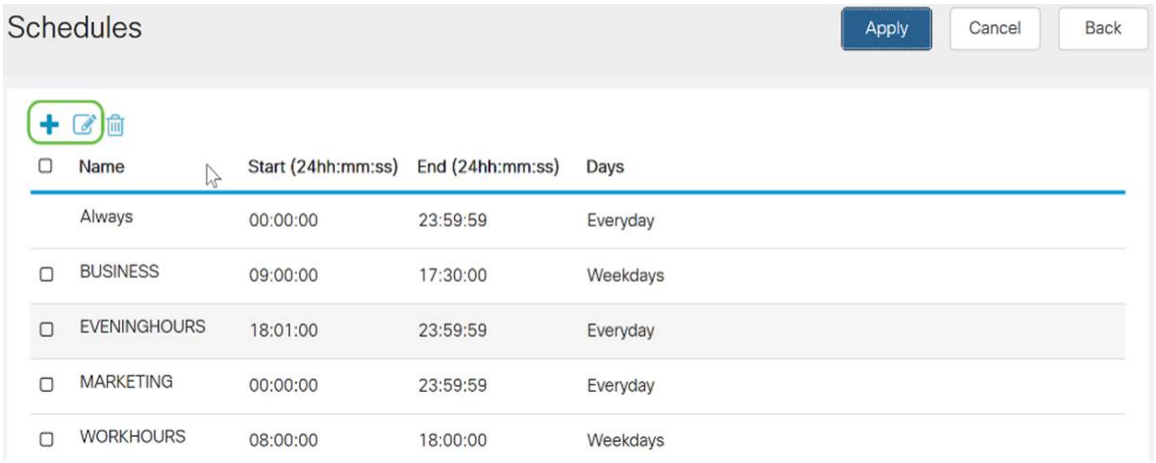
Regelstatus	Aktivieren Sie *Aktivieren,* um die spezifische Zugriffsregel zu aktivieren. Deaktivieren Sie

	diese Option.
Aktion	Wählen Sie *Zulassen* oder *Ablehnen* aus der Dropdown-Liste aus.
Services	· *IPv4*: Wählen Sie den Dienst aus, um die IPv4-Regel anzuwenden. · *IPv6*: Wählen Sie den Service aus, um die IPv6-Regel anzuwenden. · *Services* - Wählen Sie den Service aus der Dropdown-Liste aus.
Protokoll	Wählen Sie eine Option aus der Dropdown-Liste aus. · *Always*: Für Pakete, die den Regeln entsprechen, werden Protokolle angezeigt. · *Nie* - Kein Protokoll erforderlich.
Quellschnittstelle	Wählen Sie die Quellschnittstelle aus der Dropdown-Liste aus.
Quelladresse	Wählen Sie die Quell-IP-Adresse aus, auf die die Regel angewendet wird, und geben Sie Folgendes ein: *Any (Beliebig* ·): Wählen Sie diese Option aus, um alle IP-Adressen abzugleichen. · *Single* - Geben Sie eine IP-Adresse ein. · *Subnetz* - Geben Sie ein Subnetz eines Netzwerks ein. · *IP-Bereich*: Geben Sie den IP-Adressbereich ein.
Zielschnittstelle	Wählen Sie die Quellschnittstelle aus der Dropdown-Liste aus.
Zieladresse	Wählen Sie die Quell-IP-Adresse aus, auf die die Regel angewendet wird, und geben Sie Folgendes ein: *Any (Beliebig* ·): Wählen Sie diese Option aus, um alle IP-Adressen abzugleichen. · *Single* - Geben Sie eine IP-Adresse ein. · *Subnetz* - Geben Sie ein Subnetz eines Netzwerks ein. · *IP-Bereich*: Geben Sie den IP-Adressbereich ein.
Name des Zeitplans	Wählen Sie *aus* der Dropdown-Liste *Always, Business, Evening hours, Marketing oder Work Hours (Immer, Geschäftszeiten, Abendstunden, Marketing oder Arbeitszeiten)* aus, um die Firewall-Regel anzuwenden. Klicken Sie dann *hier*, um die Zeitpläne zu konfigurieren.



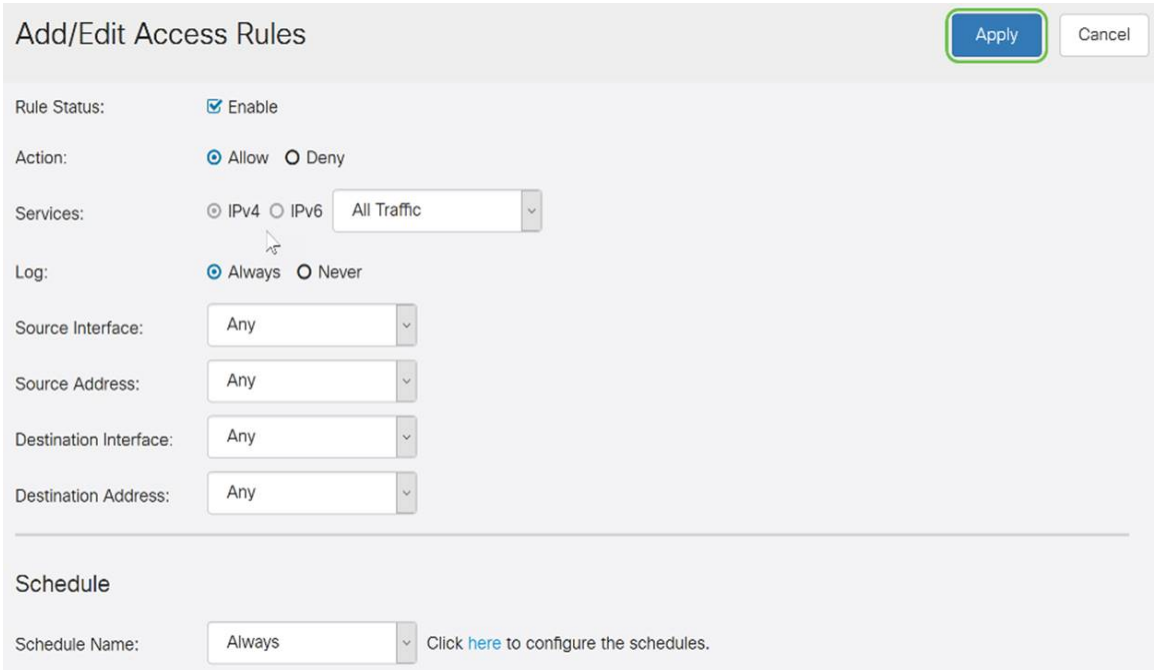
Schritt 5: (Optional) Klicken Sie zum Konfigurieren von Zeitplänen neben *Name* des *Zeitplans* **hier**.

Schritt 6: (Optional) Klicken Sie auf **Hinzufügen**, um einen Zeitplan hinzuzufügen, oder wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**.

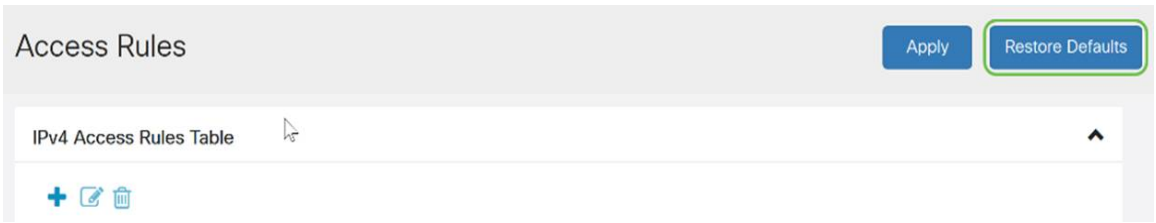


Hinweis: Weitere Informationen zur Konfiguration des Zeitplans erhalten Sie hier.

Schritt 7: (Optional) Klicken Sie auf **Übernehmen**.

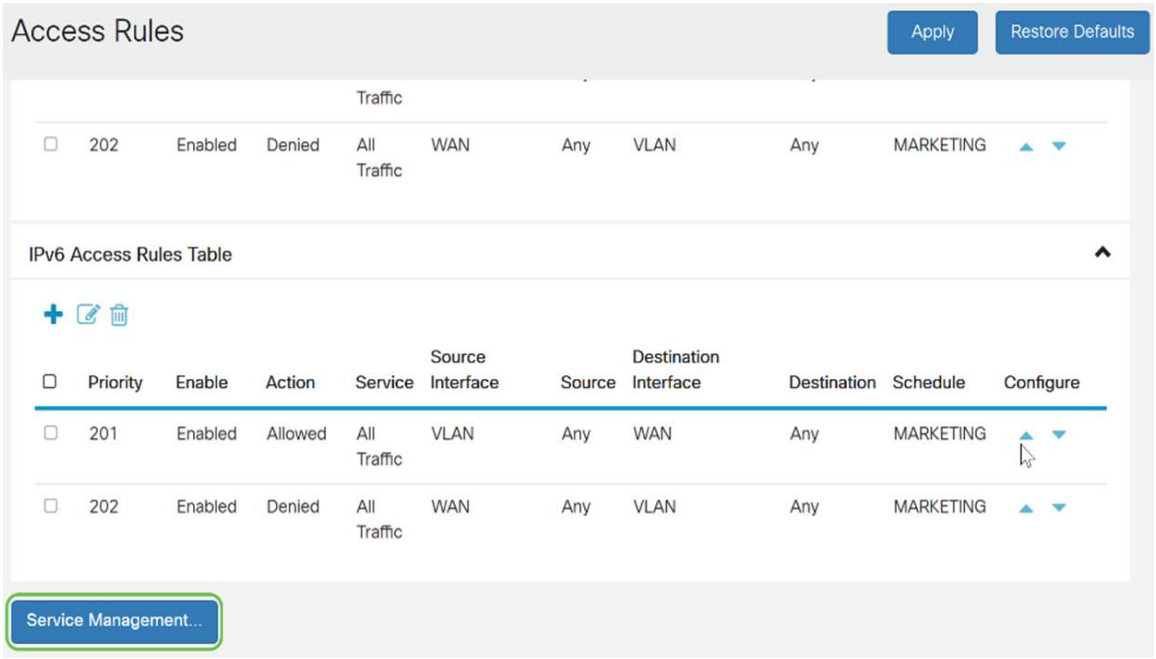


Schritt 8: (Optional) Klicken Sie auf **Standardeinstellungen wiederherstellen**, um die Standardeinstellungen wiederherzustellen.

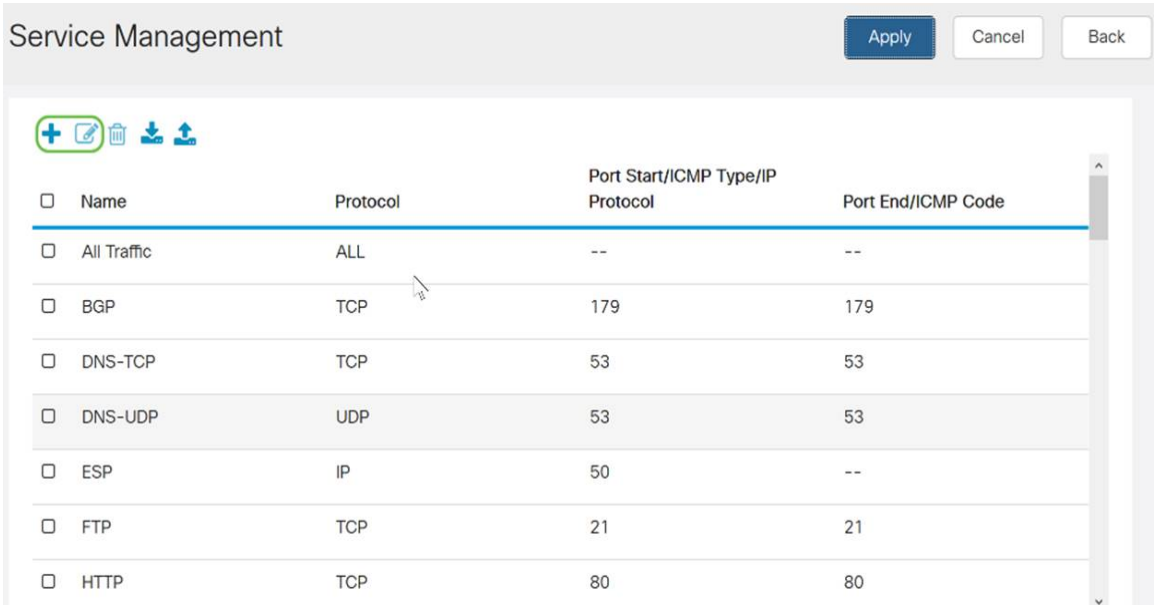


Service-Management

Schritt 1: Zum Hinzufügen oder Bearbeiten eines Eintrags in der Liste Dienste klicken Sie auf **Service Management.**

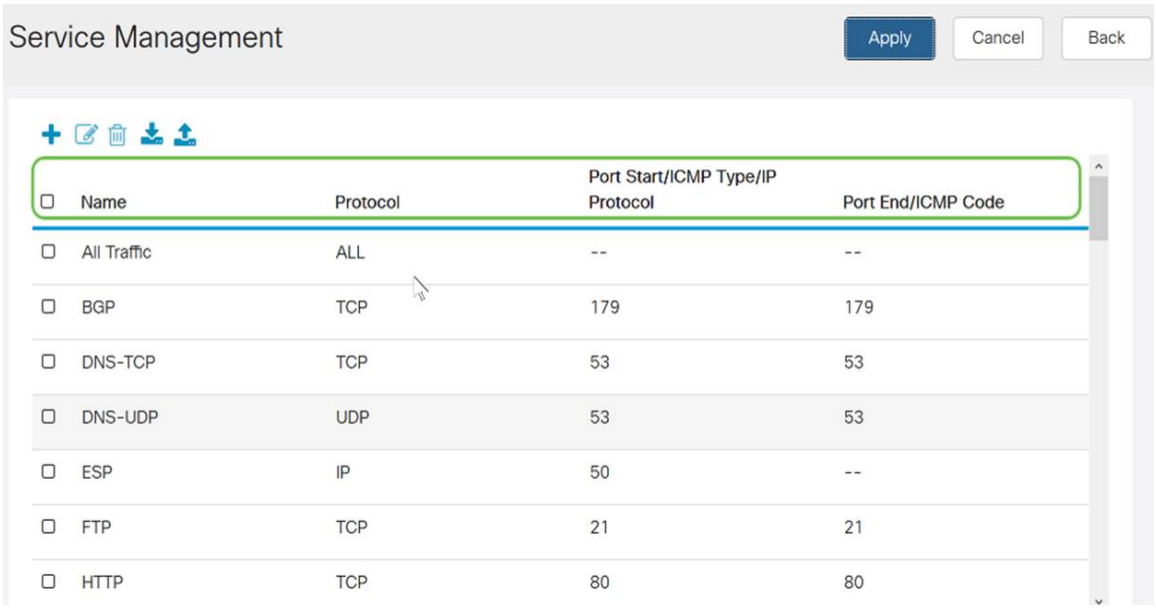


Schritt 2: Um einen Dienst hinzuzufügen, klicken Sie in der Diensttabelle auf **Hinzufügen**. Um einen Dienst zu bearbeiten, wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**. Die Felder können geändert werden.

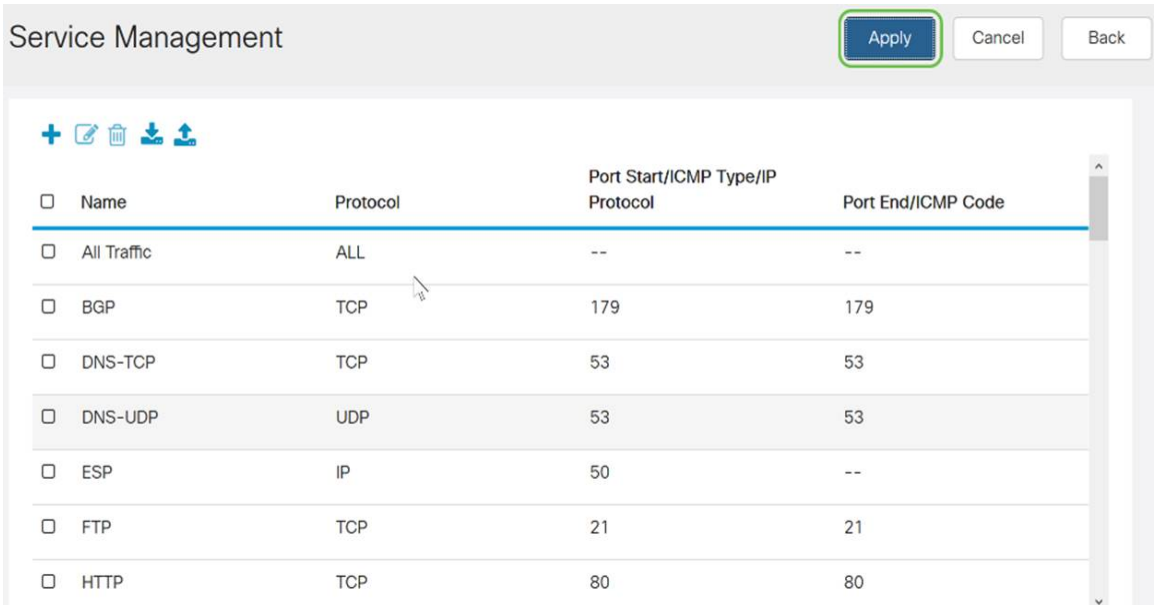


Schritt 3: Sie können viele Dienste in der Liste haben:

- *Name* - Name des Dienstes oder der Anwendung.
- *Protokoll* - Wählen Sie ein Protokoll aus der Dropdown-Liste aus.
- *Port Start/ICMP Type/IP Protocol* - Bereich der für diesen Service reservierten Portnummern.
- *Port-End/ICMP-Code* - Letzte Nummer des Ports, reserviert für diesen Service.



Schritt 4: Wenn Sie Einstellungen hinzugefügt oder bearbeitet haben, klicken Sie auf **Übernehmen**.



Sie sollten jetzt die Zugriffsregeln für Ihren RV160/RV260-Router erfolgreich konfiguriert haben.