Konfiguration der Zugriffsregeln auf dem CVR100W VPN-Router

Ziel

Zugriffskontrolllisten (Access Control Lists, ACLs) sind Listen, die festlegen, ob Pakete an der Router-Schnittstelle zugelassen oder abgelehnt werden. ACLs sind so konfiguriert, dass sie jederzeit oder basierend auf festgelegten Zeitplänen gültig sind. Der CVR100W VPN-Router ermöglicht die Konfiguration von Zugriffsregeln, um die Sicherheit zu erhöhen.

In diesem Dokument wird die Konfiguration der Zugriffsregeln auf dem CVR100W VPN-Router beschrieben.

Anwendbares Gerät

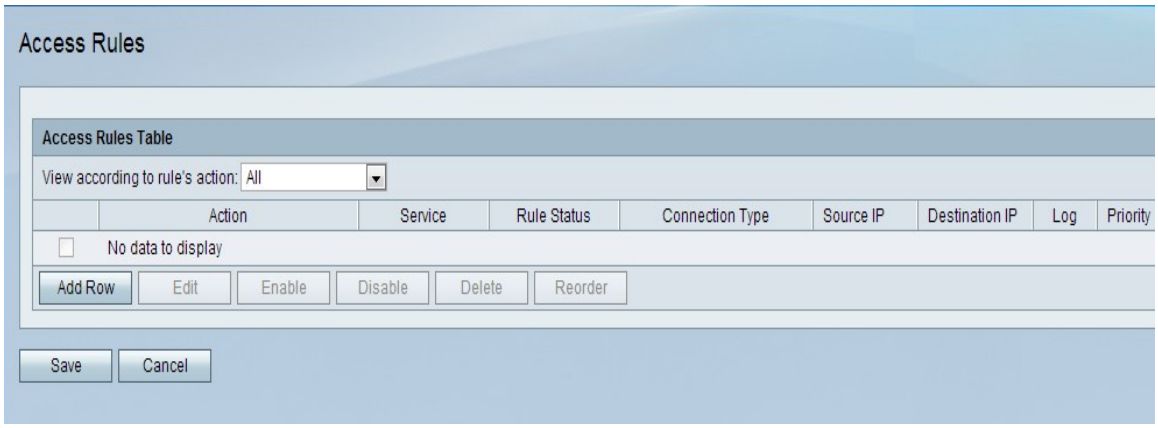
·CVR100W VPN-Router

Softwareversion

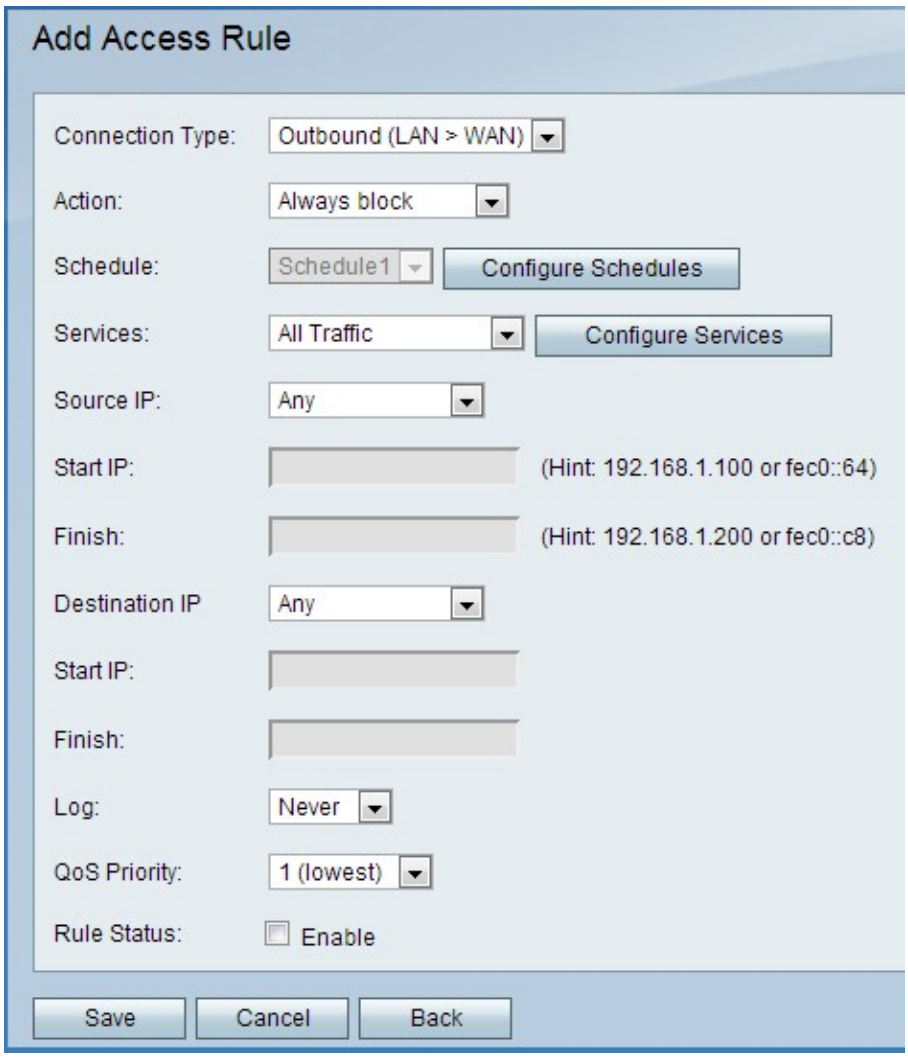
·1.0.1.19

Zugriffsregeln

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Access Control > Access Rules aus**. Die Seite *Zugriffsregeln* wird geöffnet:



Schritt 2: Klicken Sie auf **Zeile hinzufügen**, um eine neue Zugriffsregel hinzuzufügen. Die Seite *Zugriffsregel hinzufügen* wird geöffnet:



Schritt 3: Wählen Sie in der Dropdown-Liste Verbindungstyp den Regeltyp aus, der erstellt werden soll.

·Outbound (LAN > WAN) - Diese Option betrifft Pakete vom sicheren LAN zum unsicheren WAN.

·Inbound (WAN > LAN) - Diese Option betrifft Pakete vom unsicheren WAN zum sicheren LAN.

·Eingehend (WAN > DMZ) - Diese Option betrifft Pakete vom unsicheren WAN zur DMZ. Eine DMZ ist ein Netzwerksegment, das das LAN vom WAN trennt, um eine Sicherheitsebene bereitzustellen.

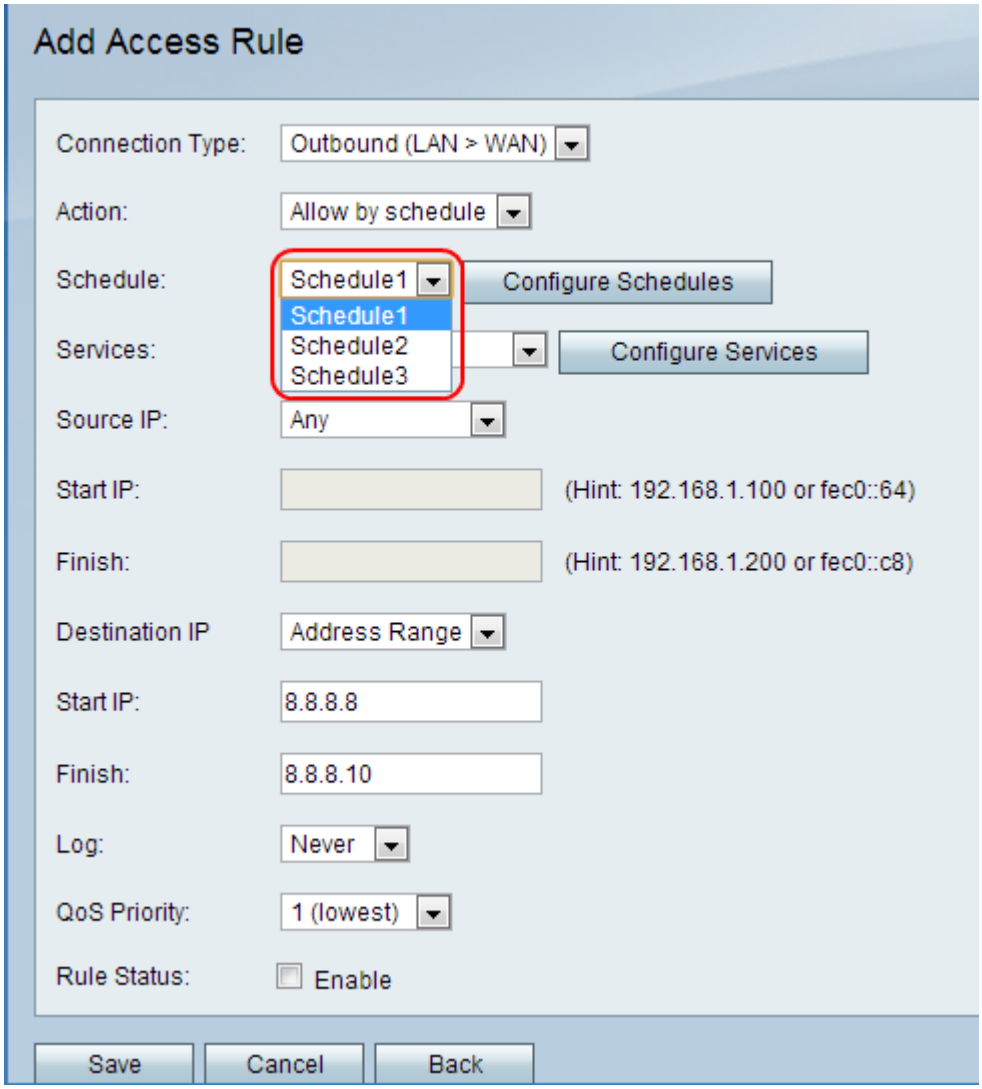
Schritt 4: Wählen Sie in der Dropdown-Liste Aktion die Aktion aus, die auf die Regel angewendet wird.

·Immer blockieren - Pakete immer blockieren.

·Immer zulassen - Pakete immer zulassen.

·Sperren nach Zeitplan - Pakete werden basierend auf einem festgelegten Zeitplan blockiert.

·Planmäßig zulassen - Pakete werden basierend auf einem festgelegten Zeitplan zugelassen.



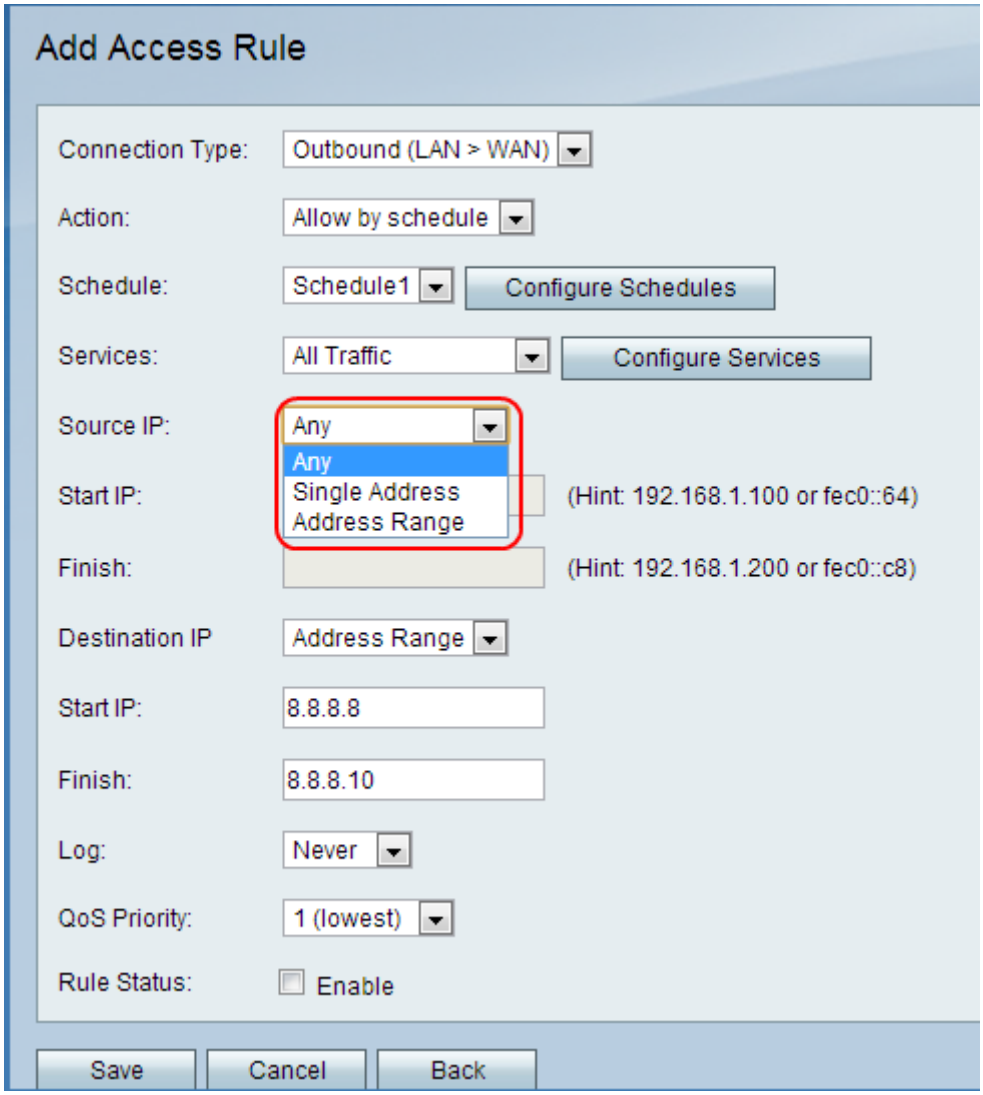
Schritt 5: Wählen Sie in der Dropdown-Liste Schedule (Zeitplan) einen Zeitplan aus, der auf die Regel angewendet werden soll.

Hinweis: Die Dropdown-Liste ist deaktiviert, wenn Sie in Schritt 4 die Option Immer blockieren oder Immer zulassen auswählen.

Schritt 6: (Optional) Um Firewall-Zeitpläne zu konfigurieren, klicken Sie auf **Zeitpläne konfigurieren.** Informationen zum Konfigurieren von Zeitplänen finden Sie im Artikel *Firewall Schedule Management auf dem CVR100W VPN-Router*.

Schritt 7: Wählen Sie in der Dropdown-Liste Dienste einen Service aus, der zugelassen oder blockiert werden soll. Die Dropdown-Liste enthält die Standardservices, die auf dem CVR100W VPN-Router verfügbar sind. Services legen den verwendeten Protokolltyp und den Port fest, für den er gilt.

Schritt 8: (Optional) Klicken Sie zum Konfigurieren von Diensten auf **Dienste konfigurieren** . Informationen zum Konfigurieren von Services finden Sie im Artikel *Service Management auf dem CVR100W VPN-Router*.



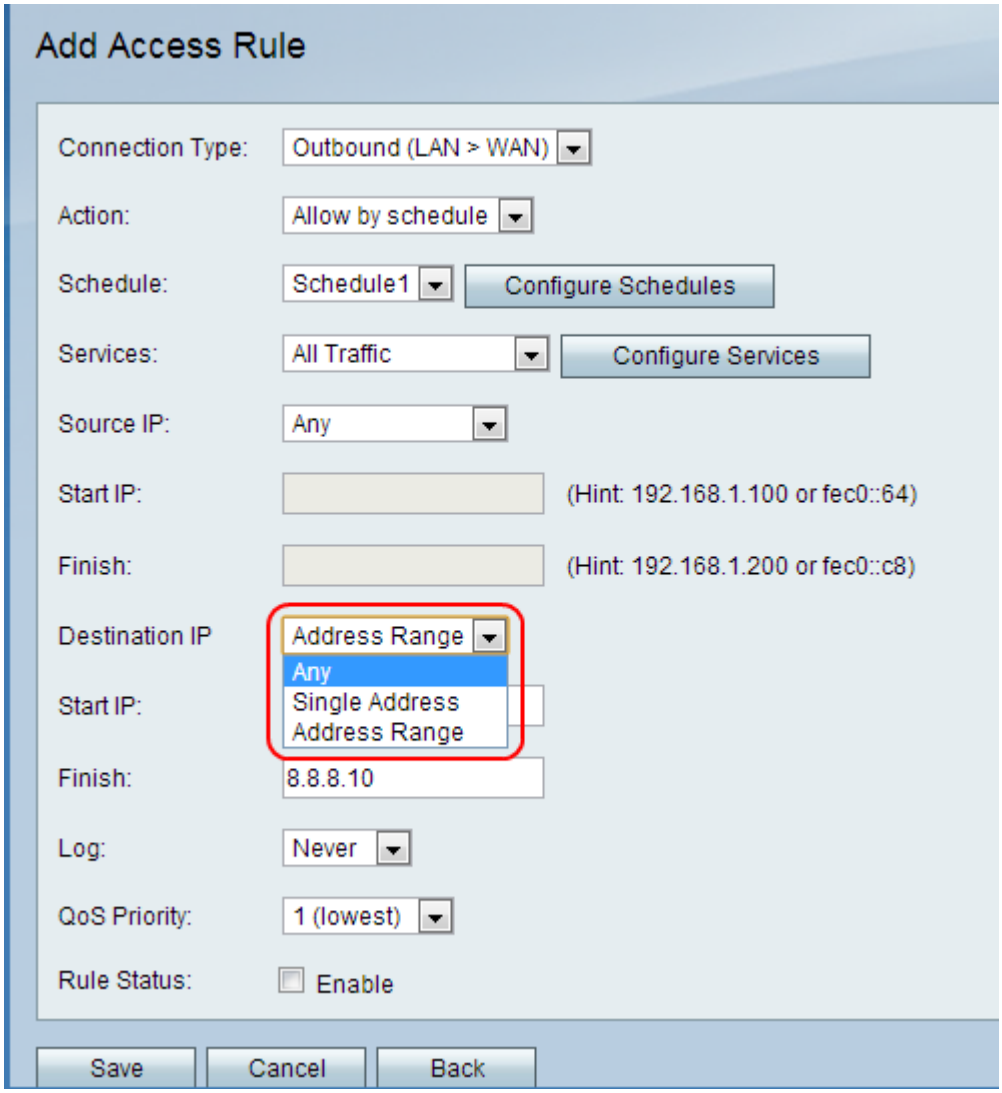
Schritt 9: Wählen Sie in der Dropdown-Liste Source IP (Quell-IP) die Quell-IP-Adressen aus, auf die die Regel angewendet wird.

·Any (Beliebig): Diese Option wendet die Regel auf alle Quell-IP-Adressen an.

·Single Address (Einzeladresse): Diese Option wendet die Regel auf eine einzelne IP-Adresse an. Geben Sie die Quell-IP-Adresse in das Feld Start-IP ein.

·Adressbereich: Diese Option wendet die Regel auf einen Bereich von IP-Adressen an. Geben Sie die Start-IP-Adresse des Adressbereichs in das Feld Start-IP ein, und geben Sie die End-IP-Adresse des Adressbereichs im Feld Beenden der IP-Adresse ein.

Hinweis: Das Feld Start IP (Start-IP) ist deaktiviert, wenn die Option Any (Beliebig) ausgewählt ist. Außerdem wird das Feld "Beenden" abgeblendet, wenn die Option "Alle" oder "Einzeladresse" ausgewählt wurde.



Schritt 10: Wählen Sie in der Dropdown-Liste Destination IP (Ziel-IP) die Ziel-IP-Adressen aus, für die die Regel gilt.

·Any (Beliebig): Diese Option wendet die Regel auf alle Quell-IP-Adressen an.

·Single Address (Einzeladresse): Diese Option wendet die Regel auf eine einzelne IP-Adresse an. Geben Sie die Ziel-IP-Adresse im Feld Start-IP ein.

·Adressbereich: Diese Option wendet die Regel auf einen Bereich von IP-Adressen an. Geben Sie die Start-IP-Adresse des Adressbereichs im Feld Start-IP ein, und geben Sie die End-IP-Adresse des Adressbereichs im Feld Beenden der IP-Adresse ein.

Hinweis: Das Feld Start IP (Start-IP) ist deaktiviert, wenn die Option Any (Beliebig) ausgewählt ist. Außerdem wird das Feld "Beenden" abgeblendet, wenn die Option "Alle" oder "Einzeladresse" ausgewählt wurde.

Schritt 11: Wählen Sie aus der Dropdown-Liste Protokoll eine Protokolloption aus. Protokolle sind generierte Systemdatensätze, die für das Audit- und Sicherheitsmanagement verwendet werden.

·Never (Nie): Deaktiviert Protokolle.

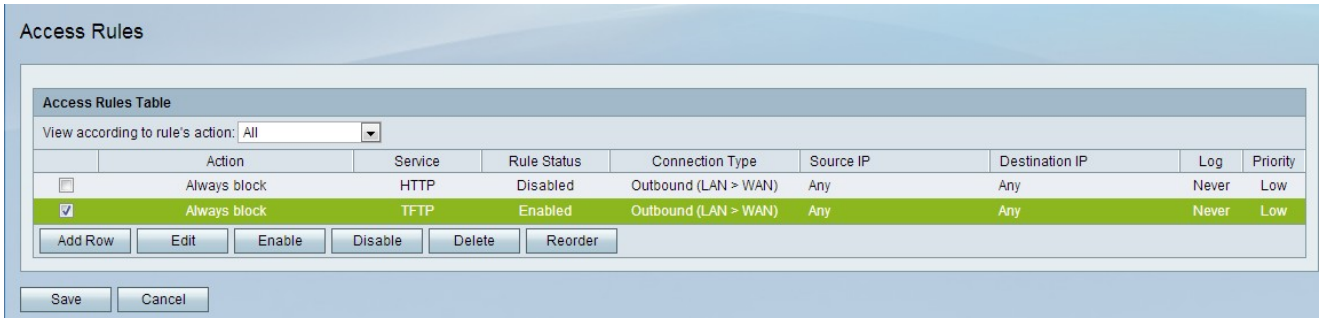
·Immer - Ein Protokoll wird immer erstellt, wenn ein Paket mit der Regel übereinstimmt.

Schritt 12: Wählen Sie aus der Dropdown-Liste "QoS Priority" (QoS-Priorität) eine Priorität

für die ausgehenden IP-Pakete der Regel aus. Priorität Eins ist die niedrigste, Priorität vier die höchste. Pakete in Warteschlangen mit höherer Priorität werden vor Paketen mit niedriger Priorität weitergeleitet.

Schritt 13: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Regelstatus, um die Regel zu aktivieren.

Schritt 14: Klicken Sie auf **Speichern**.



Schritt 15: (Optional) Um eine Zugriffsregel in der Zugriffsliste zu bearbeiten, aktivieren Sie das Kontrollkästchen des Eintrags, klicken Sie auf **Bearbeiten**, bearbeiten Sie die erforderlichen Felder, und klicken Sie auf **Speichern**.

Schritt 16: (Optional) Zum Löschen eines Zugriffsregeleintrags in der Zugriffs-Regeltabelle aktivieren Sie das Kontrollkästchen des Eintrags, klicken Sie auf **Löschen** und dann auf **Speichern**.

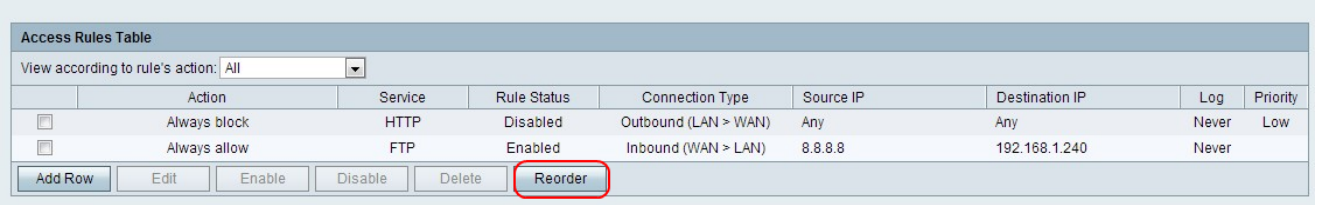
Hinweis: Es wird eine Eingabeaufforderung angezeigt, die besagt, dass Sie speichern müssen, bevor Sie bearbeiten oder löschen können.

Schritt 17: (Optional) Um einen Zugriffsregeleintrag in der Zugriffs-Regeltabelle zu aktivieren, aktivieren Sie das Kontrollkästchen des Eintrags, klicken Sie auf **Aktivieren** und dann auf **Speichern**.

Schritt 18: (Optional) Um einen Zugriffsregeleintrag in der Zugriffs-Regeltabelle zu deaktivieren, aktivieren Sie das Kontrollkästchen des Eintrags, klicken Sie auf **Deaktivieren** und klicken Sie auf **Speichern**.

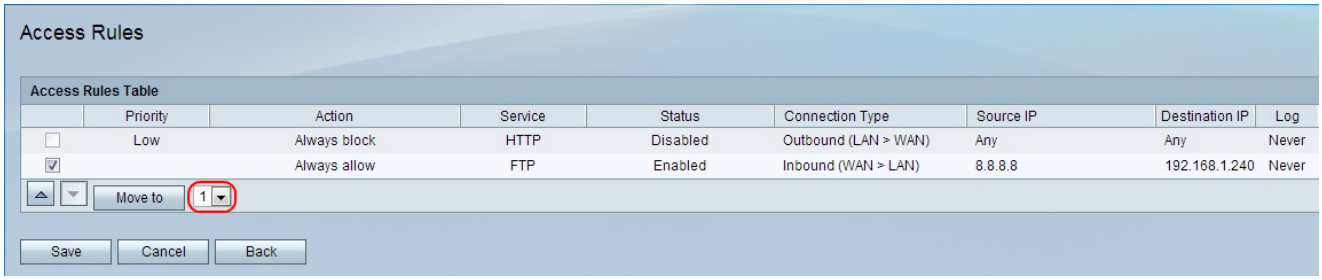
Zugriffsregeln neu ordnen

Zugriffsregeln werden in der Tabelle mit den Zugriffsregeln in einer bestimmten Reihenfolge angezeigt. Die Reihenfolge gibt an, wie die Regeln angewendet werden. Die erste Regel in der Tabelle ist die erste Regel, die angewendet wird. Danach wird die zweite Regel der Liste angewendet. Die Neuanordnung ist eine wichtige Option auf dem CVR100W VPN-Router.



Schritt 1: Klicken Sie auf **Neu anordnen**, um die Zugriffsregeln neu anzuordnen.

Schritt 2: Aktivieren Sie das Kontrollkästchen der Zugriffsregel, die neu bestellt werden soll.



Schritt 3: Wählen Sie aus der Dropdown-Liste eine Position aus, in die Sie die angegebene Regel verschieben möchten.

Schritt 4: Klicken Sie auf **Verschieben zu**, um die Regel neu anzuordnen. Die Regel wird an die angegebene Position in der Tabelle verschoben.

Hinweis: Mithilfe der Nach-oben- und Nach-unten-Tasten können die Zugriffsregeln neu angeordnet werden.

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