Hinzufügen und Konfigurieren von Zugriffsregeln für den RV130 und den RV130W

Ziel

Netzwerkgeräte bieten grundlegende Funktionen zur Datenverkehrsfilterung mit Zugriffsregeln. Eine Zugriffsregel ist ein einzelner Eintrag in einer Zugriffskontrollliste (ACL), der eine Zulassen- oder Ablehnungsregel (zum Weiterleiten oder Verwerfen eines Pakets) basierend auf dem Protokoll, einer Quell- und Ziel-IP-Adresse oder der Netzwerkkonfiguration angibt.

In diesem Dokument wird erläutert, wie Sie eine Zugriffsregel für den RV130 und den RV130W hinzufügen und konfigurieren.

Unterstützte Geräte

- RV130
- RV130W

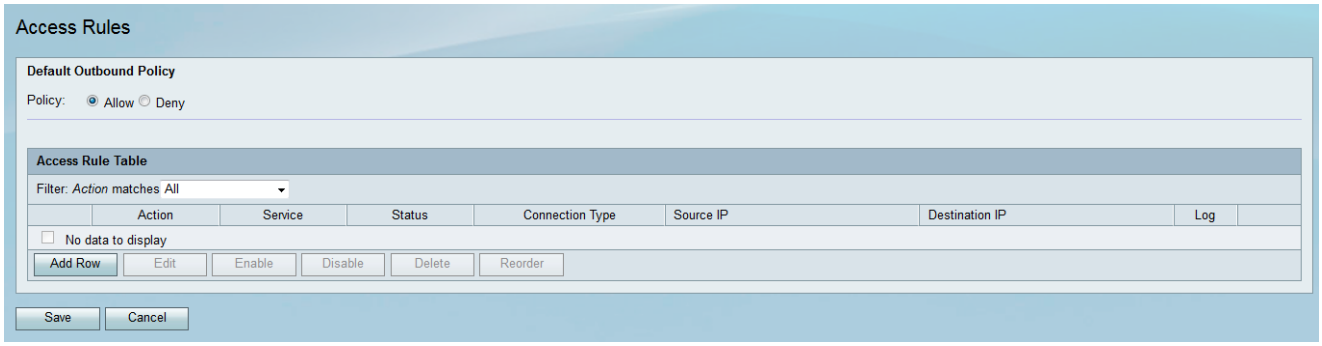
Softwareversionen

- Version 1.0.1.3

Hinzufügen und Konfigurieren einer Zugriffsregel

Festlegen der ausgehenden Standardrichtlinie

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

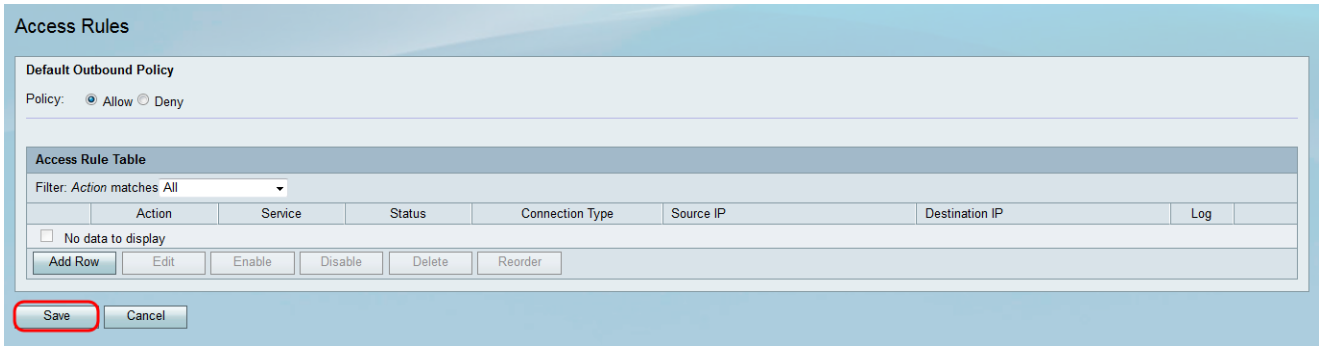


Schritt 2: Klicken Sie im Bereich *Default Outbound Policy (Standardrichtlinie für ausgehenden* Datenverkehr) auf das gewünschte Optionsfeld, um eine Richtlinie für ausgehenden Datenverkehr auszuwählen. Die Richtlinie wird immer dann angewendet, wenn keine Zugriffsregeln oder Internetzugriffsrichtlinien konfiguriert sind. Die Standardeinstellung ist **Allow**, wodurch der gesamte Internet-Datenverkehr durchgelassen wird.

Die verfügbaren Optionen sind wie folgt definiert:

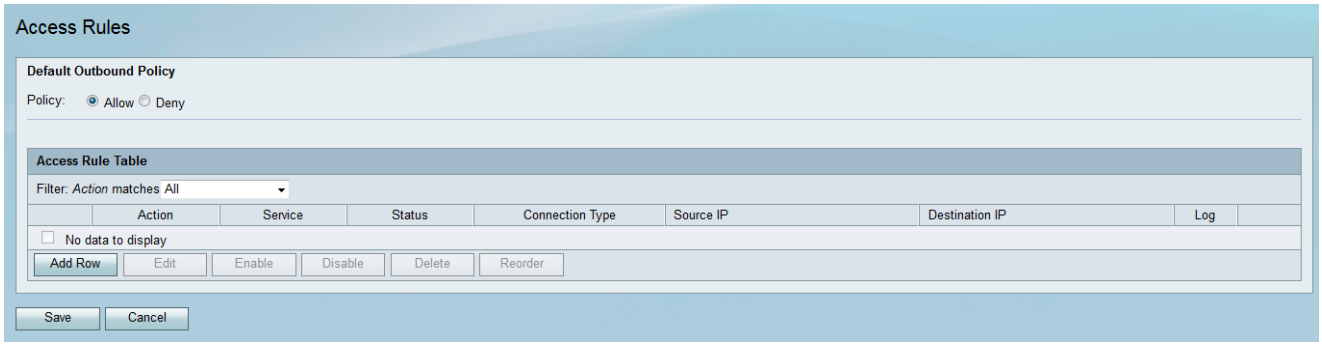
- Zulassen — Alle Arten von Datenverkehr, der vom LAN zum Internet ausgeht, zulassen.
- Verweigern - Blockiert alle Arten von Datenverkehr, der vom LAN zum Internet ausgeht.

Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

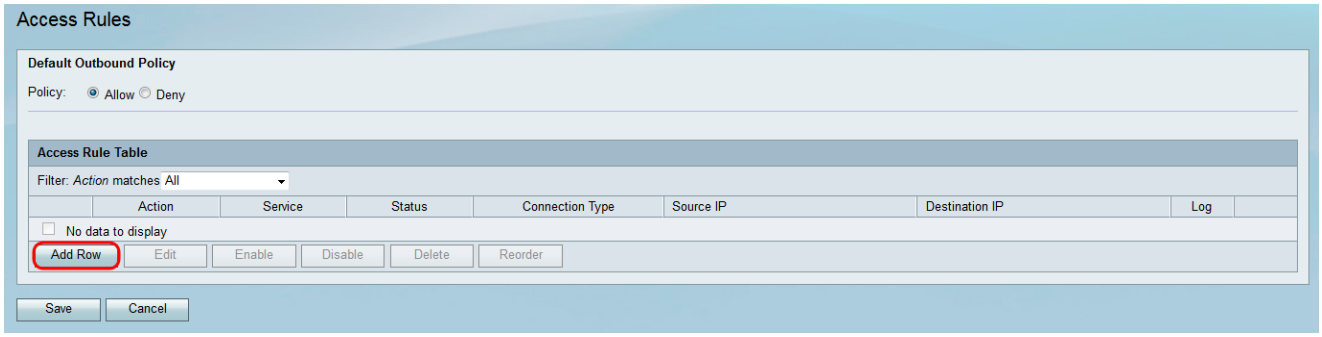


Hinzufügen einer Zugriffsregel

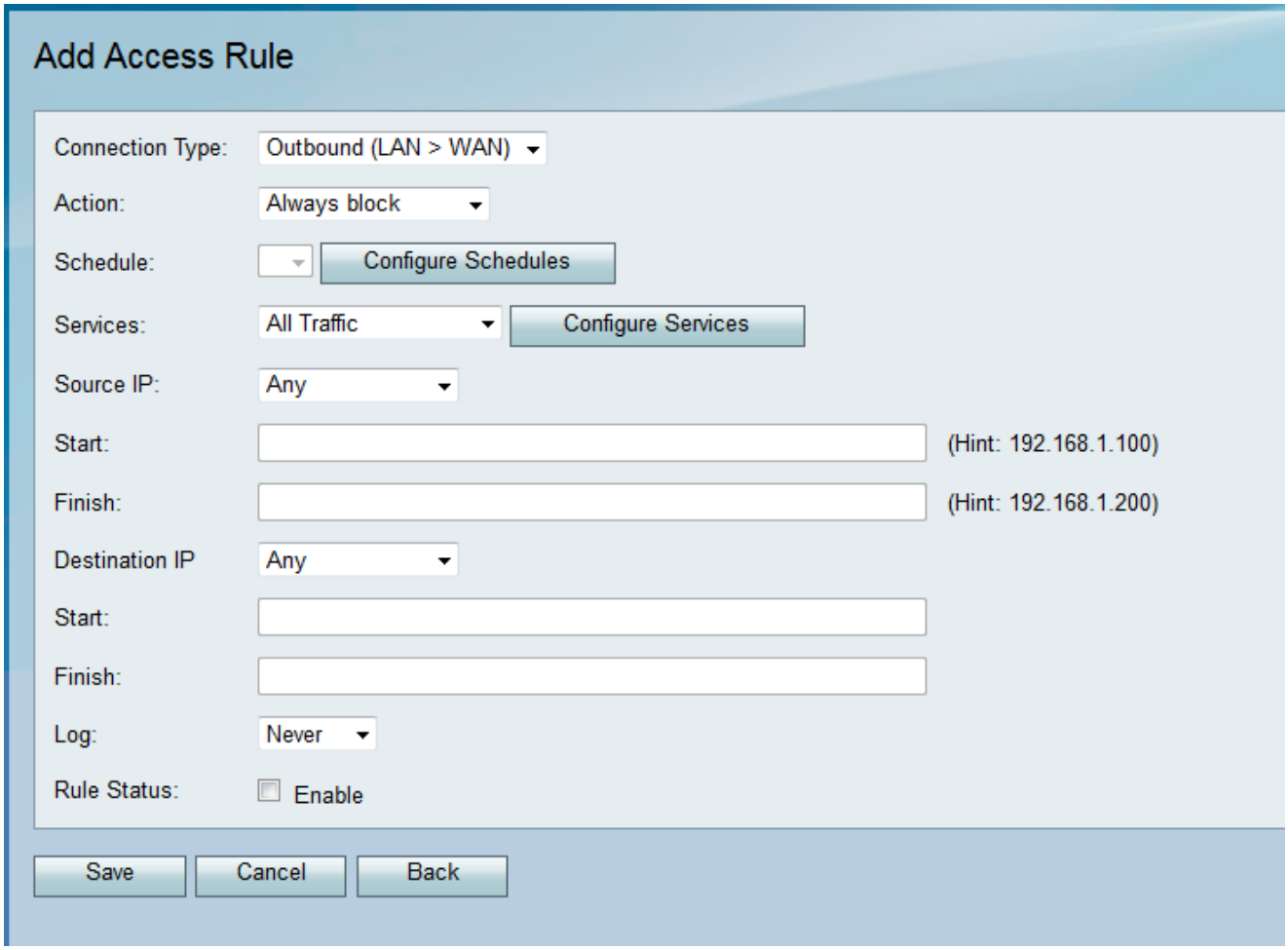
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Access Rules**. Das Fenster *Zugriffsregeln* wird geöffnet:



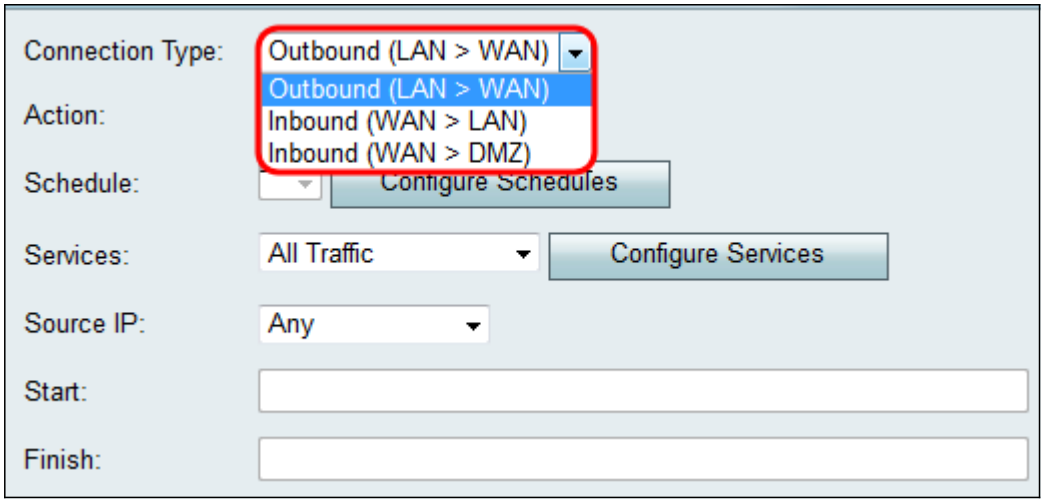
Schritt 2: Klicken Sie in der *Zugriffsregeltabelle* auf **Zeile hinzufügen**, um eine neue Zugriffsregel hinzuzufügen.



Die Seite *Zugriffsregel hinzufügen* wird geöffnet:



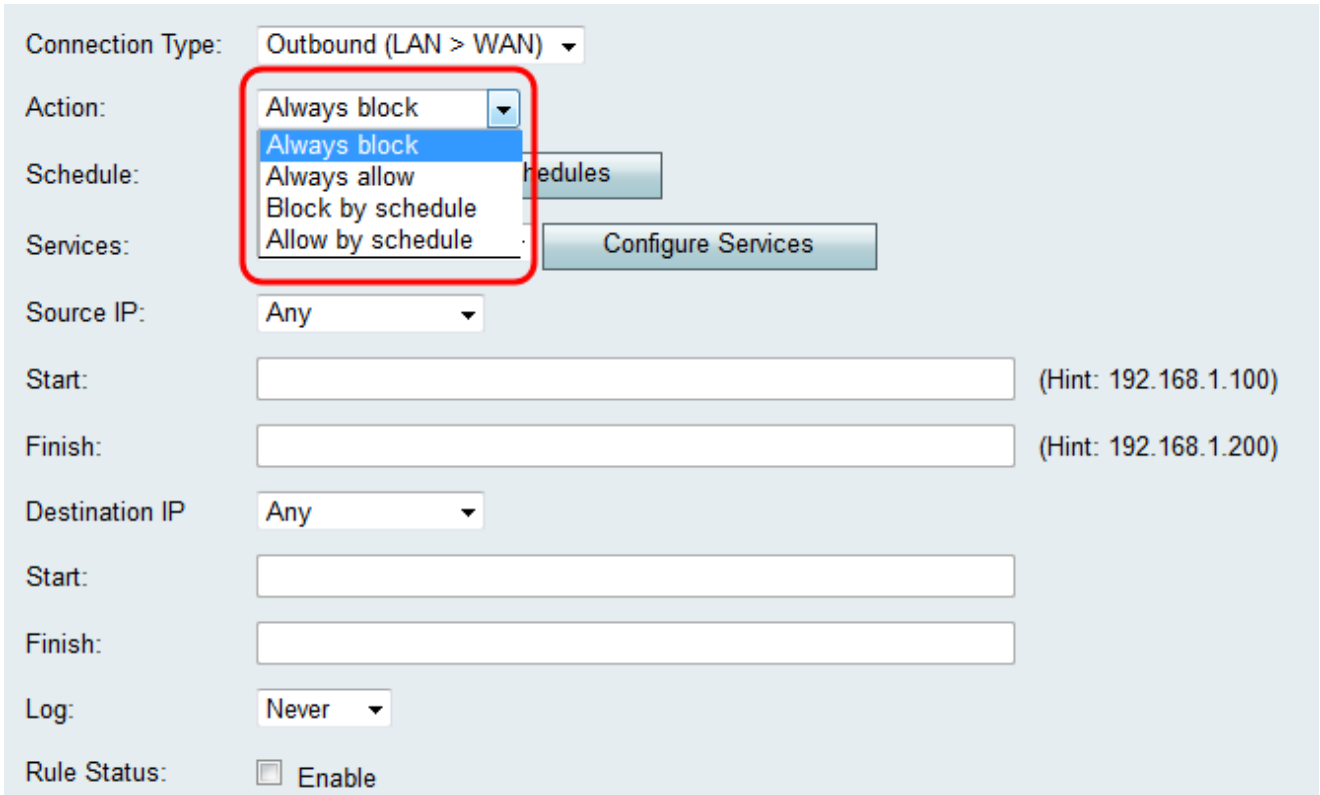
Schritt 3: Wählen Sie aus der Dropdown-Liste *Verbindungstyp* den Typ des Datenverkehrs aus, für den die Regel gilt.



Die verfügbaren Optionen sind wie folgt definiert:

- Ausgehend (LAN > WAN): Die Regel betrifft Pakete, die aus dem lokalen Netzwerk (LAN) stammen und an das Internet (WAN) gesendet werden.
- Eingehend (WAN > LAN): Die Regel betrifft Pakete, die aus dem Internet (WAN) kommen und in das lokale Netzwerk (LAN) gelangen.
- Inbound (WAN > DMZ) (Eingehend (WAN > DMZ)): Die Regel betrifft Pakete, die aus dem Internet (WAN) in das Subnetz der demilitarisierten Zone (DMZ) gelangen.

Schritt 4: Wählen Sie aus der Dropdown-Liste "*Aktion*" die Aktion aus, die beim Zuordnen einer Regel ausgeführt werden soll.



Die verfügbaren Optionen sind wie folgt definiert:

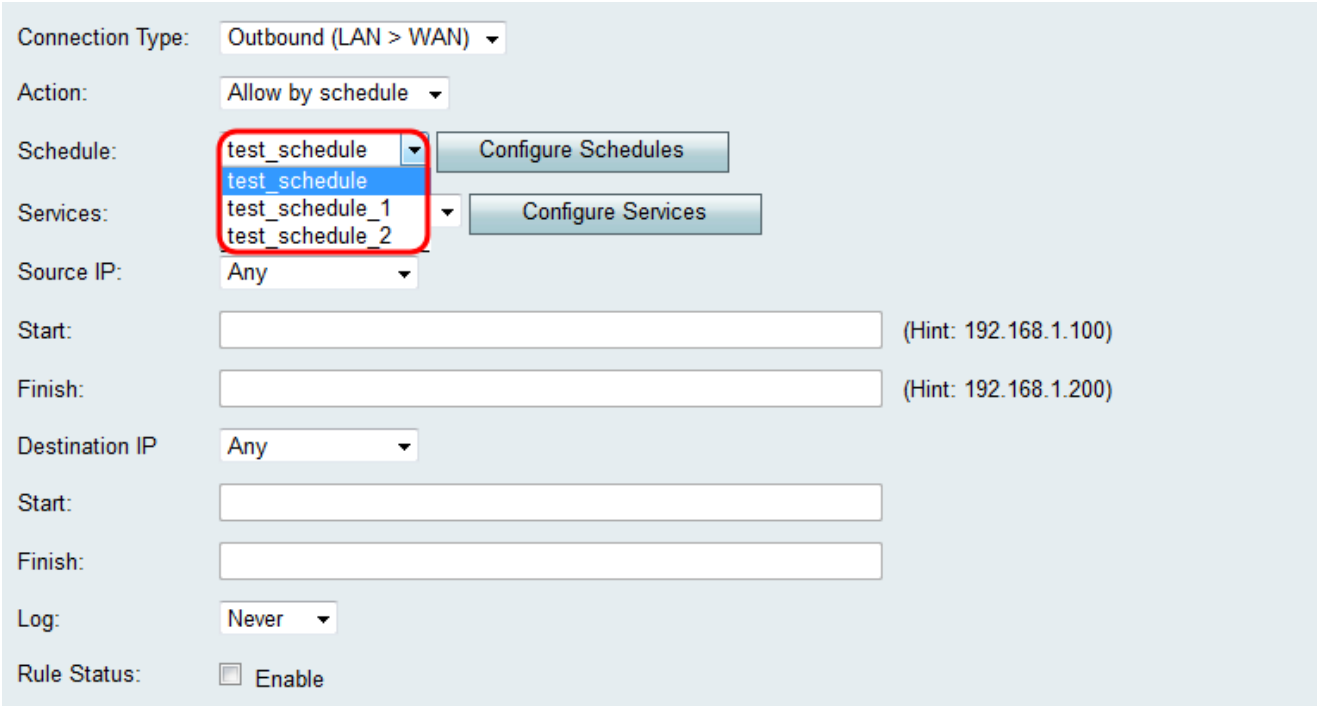
- Immer blockieren - Verweigern Sie den Zugriff immer, wenn die Bedingungen übereinstimmen. Fahren Sie mit Schritt 6 fort.

- Immer zulassen - Erlauben Sie den Zugriff immer, wenn die Bedingungen übereinstimmen. Fahren Sie mit Schritt 6 fort.

- Block by schedule (Nach Zeitplan blockieren): Verweigern Sie den Zugriff, wenn die Bedingungen während eines vorkonfigurierten Zeitplans übereinstimmen.

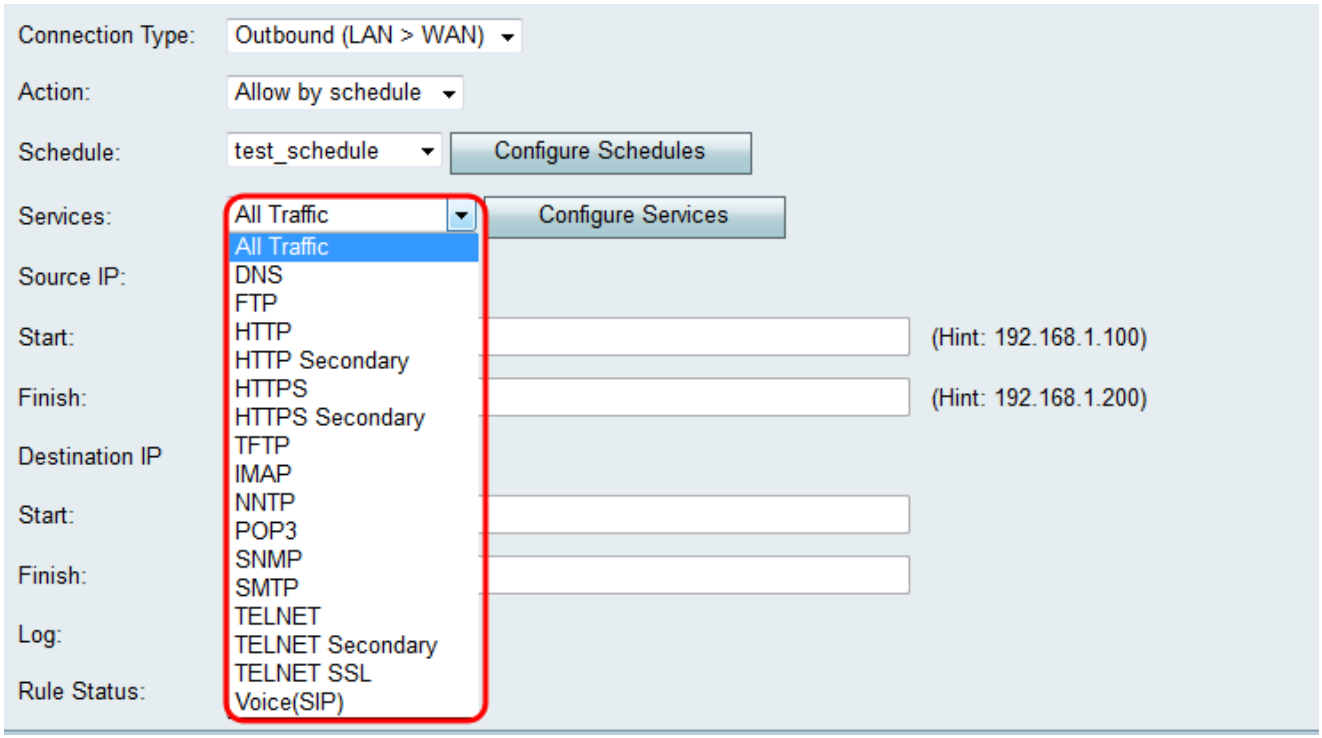
- Nach Zeitplan zulassen - Erlauben Sie den Zugriff, wenn die Bedingungen während eines vorkonfigurierten Zeitplans übereinstimmen.

Schritt 5: Wenn Sie in Schritt 4 die Option **Nach Zeitplan blockieren** oder Nach **Zeitplan zulassen** gewählt haben, wählen Sie den entsprechenden Zeitplan aus der Dropdown-Liste *Zeitplan*.



Anmerkung: Klicken Sie zum Erstellen oder Bearbeiten eines Zeitplans auf **Zeitpläne konfigurieren**. Weitere Informationen und Richtlinien finden Sie unter *Configuring Schedules on the RV130 and RV130W* (*Zeitpläne konfigurieren*).

Schritt 6: Wählen Sie aus der Dropdown-Liste "*Services*" den Servicetyp aus, für den die Zugriffsregel gilt.



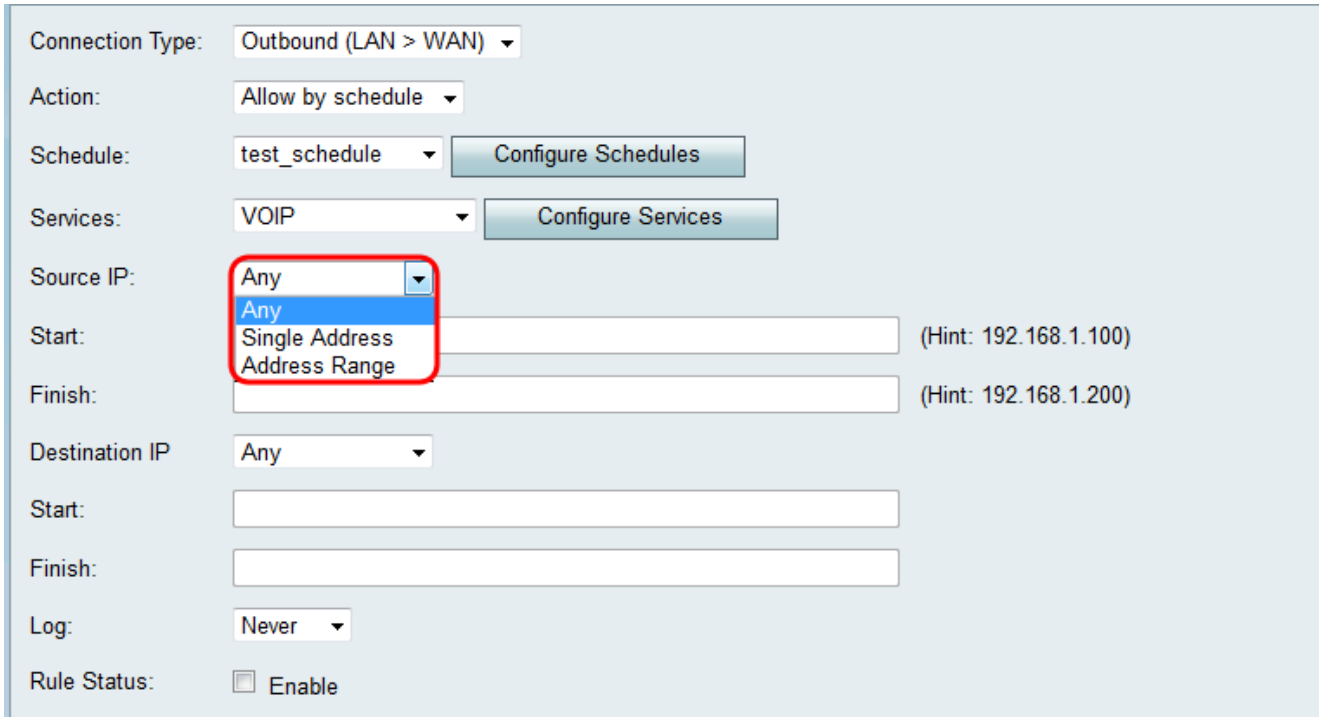
Anmerkung: Wenn Sie einen Service hinzufügen oder bearbeiten möchten, klicken Sie auf **Services konfigurieren**. Weitere Informationen und Richtlinien finden Sie unter *Service Management Configuration auf dem RV130 und RV130W*.

Konfigurieren der Quell- und Ziel-IP für ausgehenden Datenverkehr

Führen Sie die Schritte in diesem Abschnitt aus, wenn **Outbound (LAN > WAN)** als Verbindungstyp in Schritt 3 von *Hinzufügen einer Zugriffsregel* ausgewählt wurde.

Anmerkung: Wenn in Schritt 3 des Hinzufügens einer Zugriffsregel ein eingehender Verbindungstyp ausgewählt wurde, fahren Sie mit dem nächsten Abschnitt fort: *Konfigurieren der Quell- und Ziel-IP für eingehenden Datenverkehr*.

Schritt 1: Wählen Sie aus der Dropdown-Liste "*Quell-IP"* aus, wie die Quell-IP definiert werden soll. Für ausgehenden Datenverkehr bezieht sich die Quell-IP auf die Adresse(n) (im LAN), auf die die Firewall-Regel angewendet würde.



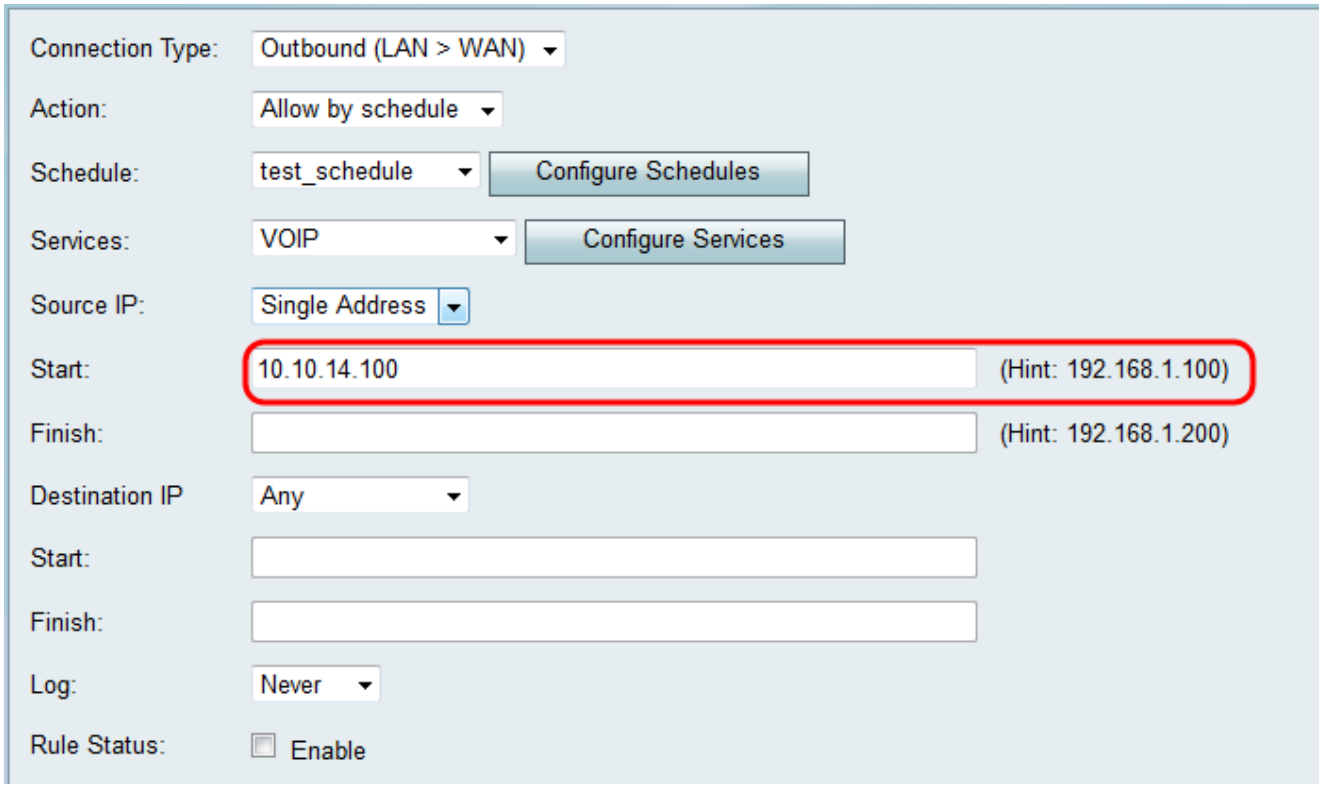
Die verfügbaren Optionen sind wie folgt definiert:

- Beliebig - Gilt für Datenverkehr, der von einer beliebigen IP-Adresse im lokalen Netzwerk ausgeht. Lassen Sie daher die Felder *Start* und *Ende* leer. Fahren Sie mit Schritt 4 fort, wenn Sie diese Option auswählen.

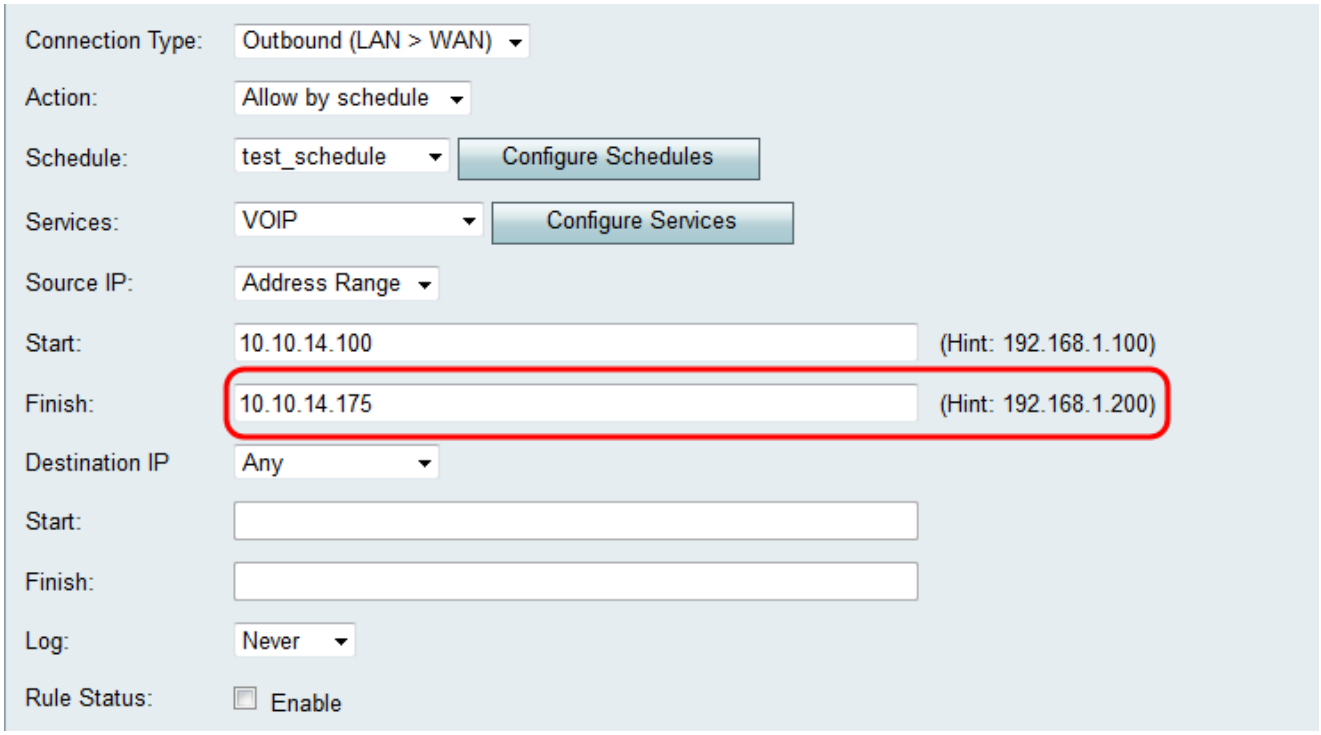
- Einzelne Adresse - Gilt für Datenverkehr, der von einer einzigen IP-Adresse im lokalen Netzwerk ausgeht. Geben Sie die IP-Adresse in das Feld *Start* ein.

- Adressbereich - Gilt für Datenverkehr, der von einem IP-Adressbereich im lokalen Netzwerk ausgeht. Geben Sie die Start-IP-Adresse des Bereichs im Feld *Start* und die End-IP-Adresse im Feld *Ende* ein, um den Bereich festzulegen.

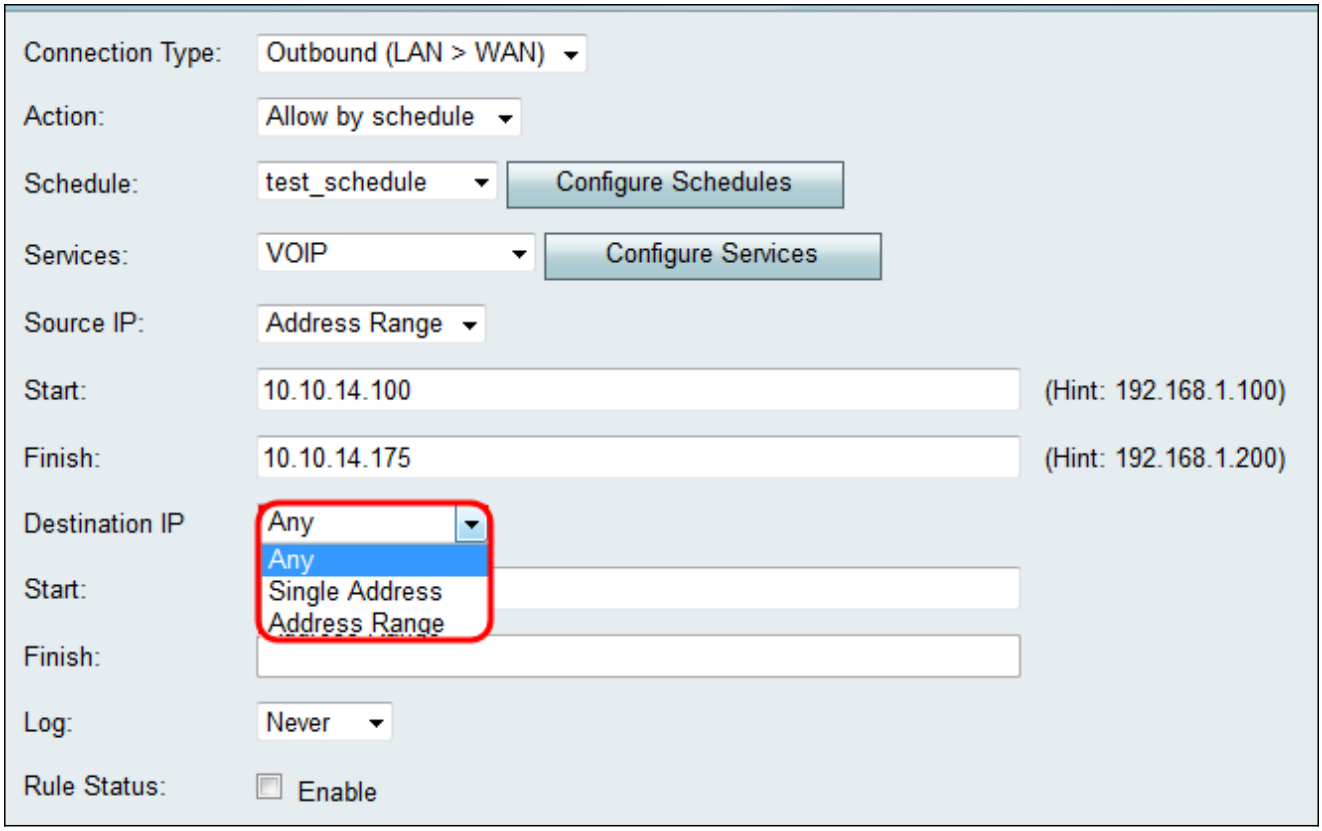
Schritt 2. Wenn Sie in Schritt 1 die Option **Einzelne Adresse** gewählt haben, geben Sie im Feld *Start* die IP-Adresse ein, die auf die Zugriffsregel angewendet wird, und fahren Sie dann mit Schritt 4 fort. Wenn Sie in Schritt 1 die Option **Adressbereich** gewählt haben, geben Sie im Feld *Start* eine Start-IP-Adresse ein, die auf die Zugriffsregel angewendet wird.



Schritt 3: Wenn Sie in Schritt 1 den **Adressbereich** ausgewählt haben, geben Sie die End-IP-Adresse ein, die den IP-Adressbereich für die Zugriffsregel im Feld *Beenden* kapselt.



Schritt 4: Wählen Sie aus der Dropdown-Liste Destination IP (Ziel-IP) aus, wie die Ziel-*IP* definiert werden soll. Bei ausgehendem Datenverkehr bezieht sich die Ziel-IP-Adresse(n) auf die Adresse(n) (im WAN), zu der bzw. denen Datenverkehr vom lokalen Netzwerk zugelassen oder abgelehnt wird.



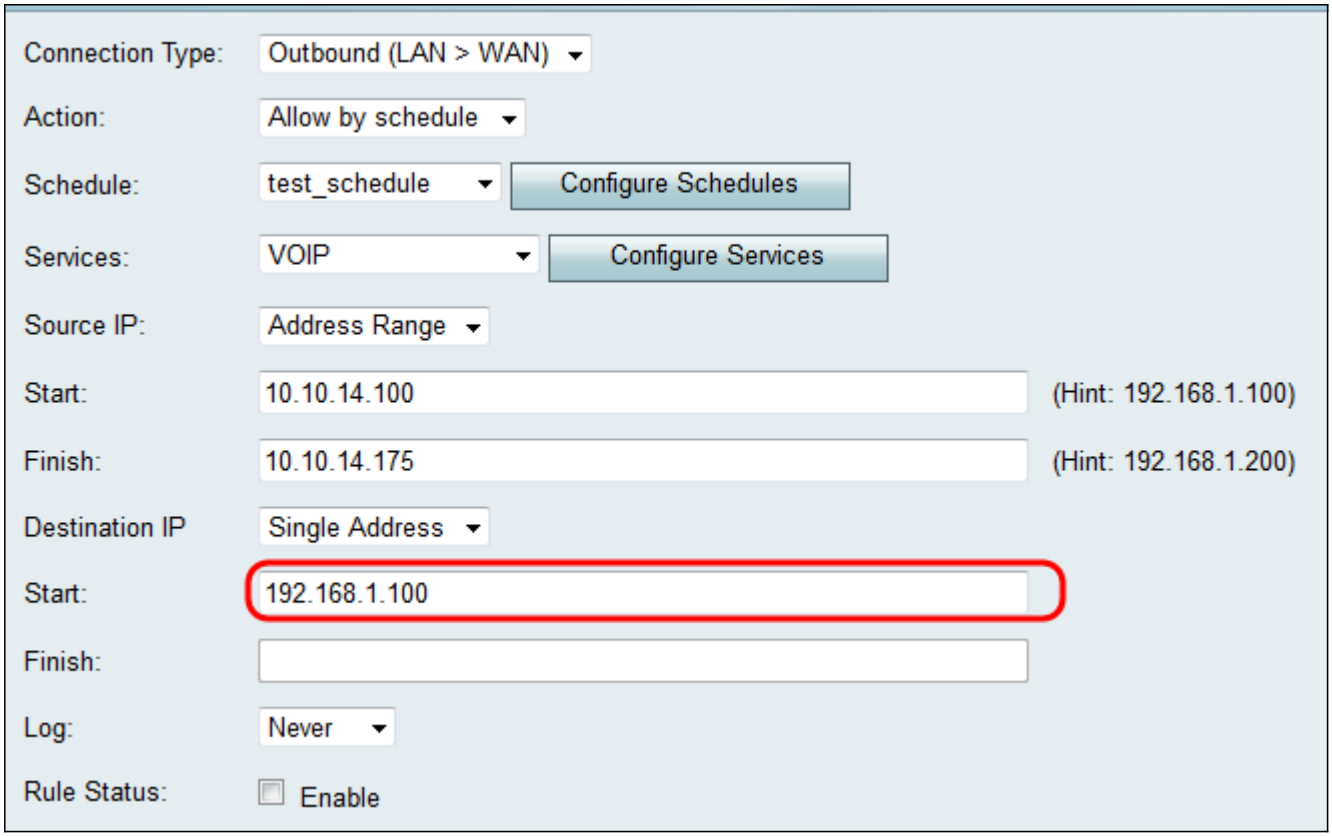
Die verfügbaren Optionen sind wie folgt definiert:

- Beliebig - Gilt für Datenverkehr, der zu einer beliebigen IP-Adresse im öffentlichen Internet führt. Lassen Sie daher die Felder *Start* und *Ende* leer.

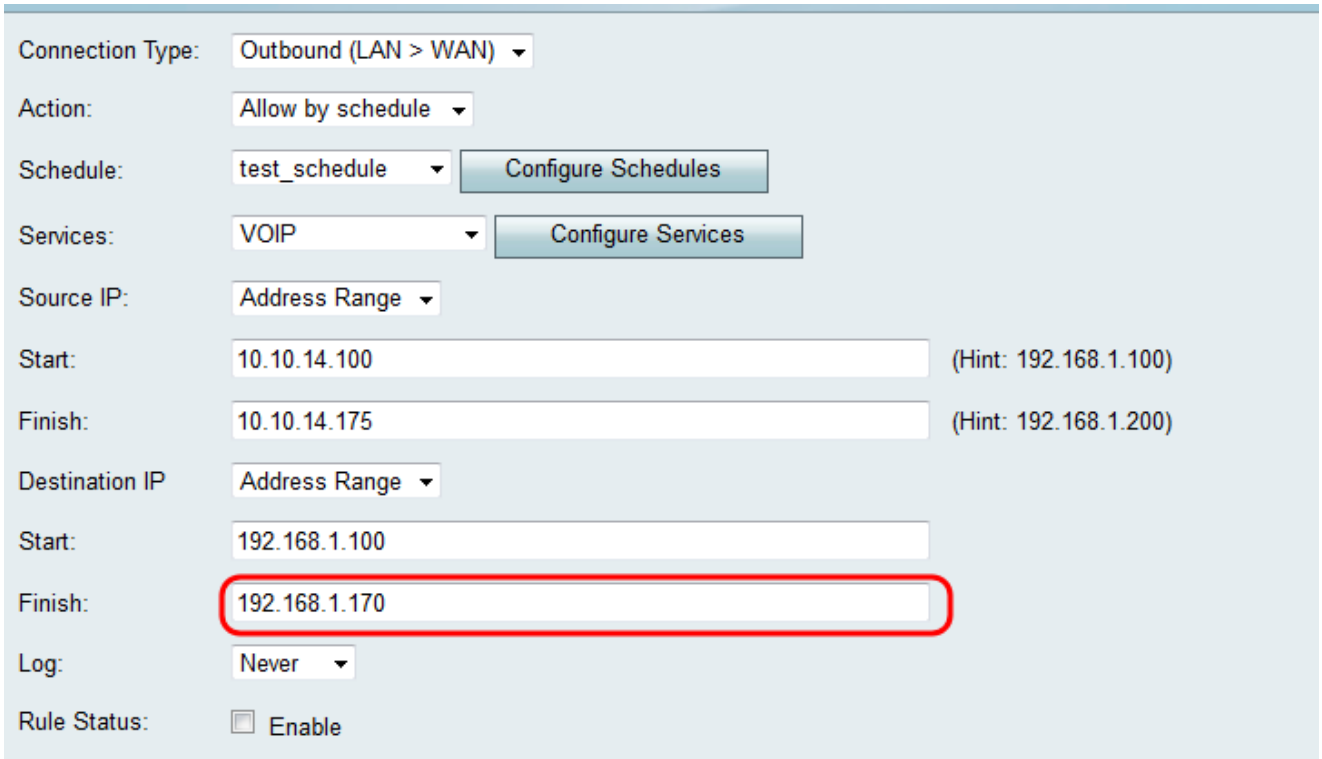
- Eine Adresse - Gilt für Datenverkehr, der zu einer einzigen IP-Adresse im öffentlichen Internet führt. Geben Sie die IP-Adresse in das Feld *Start* ein.

- Adressbereich - Gilt für Datenverkehr, der zu einem IP-Adressbereich im öffentlichen Internet führt. Geben Sie die Start-IP-Adresse des Bereichs im Feld *Start* und die End-IP-Adresse im Feld *Ende* ein, um den Bereich festzulegen.

Schritt 5: Wenn Sie in Schritt 4 die Option **Single Address (Einzeladresse)** gewählt haben, geben Sie die IP-Adresse ein, die auf die Zugriffsregel im Feld *Start* angewendet wird. Wenn Sie in Schritt 4 die Option **Adressbereich** ausgewählt haben, geben Sie eine Start-IP-Adresse ein, die auf die Zugriffsregel im Feld *Start* angewendet wird.



Schritt 6. Wenn Sie in Schritt 4 den **Adressbereich** ausgewählt haben, geben Sie die End-IP-Adresse ein, die den IP-Adressbereich für die Zugriffsregel im Feld *Beenden* kapselt.

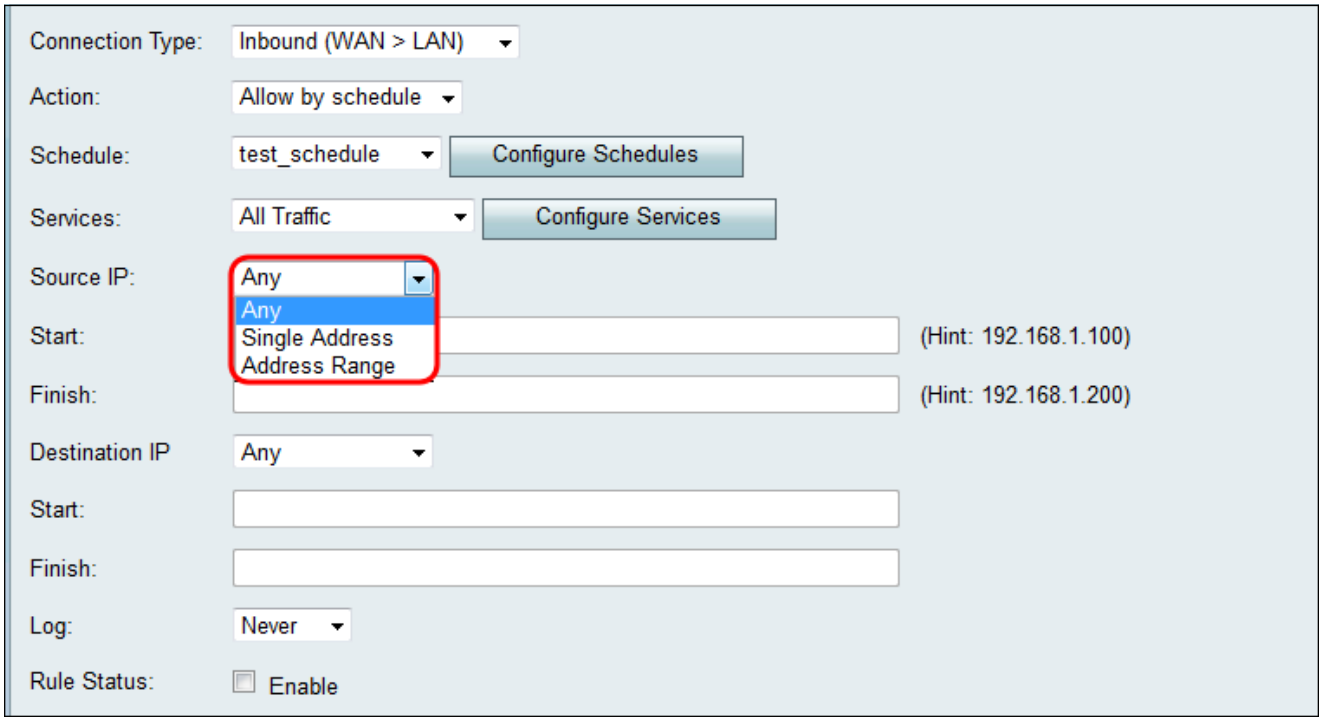


Konfigurieren der Quell- und Ziel-IP für eingehenden Datenverkehr

Führen Sie die Schritte in diesem Abschnitt aus, wenn in Schritt 3 unter *Hinzufügen einer Zugriffsregel* die Option **Eingehend (WAN > LAN)** oder **Eingehend (WAN > DMZ)** als Verbindungstyp ausgewählt wurde.

Schritt 1: Wählen Sie aus der Dropdown-Liste "*Quell-IP*" aus, wie die Quell-IP definiert

werden soll. Beim eingehenden Datenverkehr bezieht sich die Quell-IP auf die Adresse(n) (im WAN), auf die die Firewall-Regel angewendet würde.



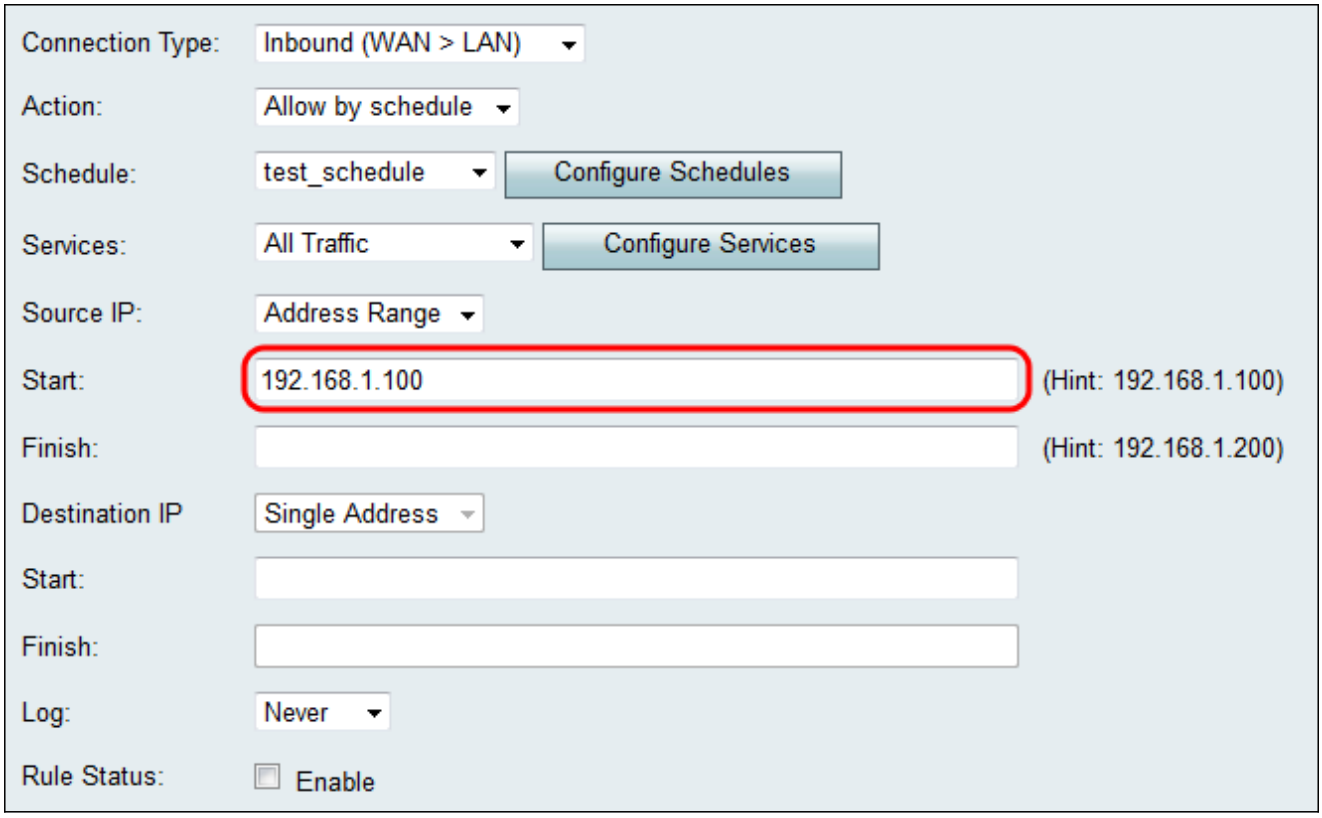
Die verfügbaren Optionen sind wie folgt definiert:

- Beliebig - Gilt für Datenverkehr, der von einer beliebigen IP-Adresse im öffentlichen Internet stammt. Lassen Sie daher die Felder *Start* und *Ende* leer. Fahren Sie mit Schritt 4 fort, wenn Sie diese Option auswählen.

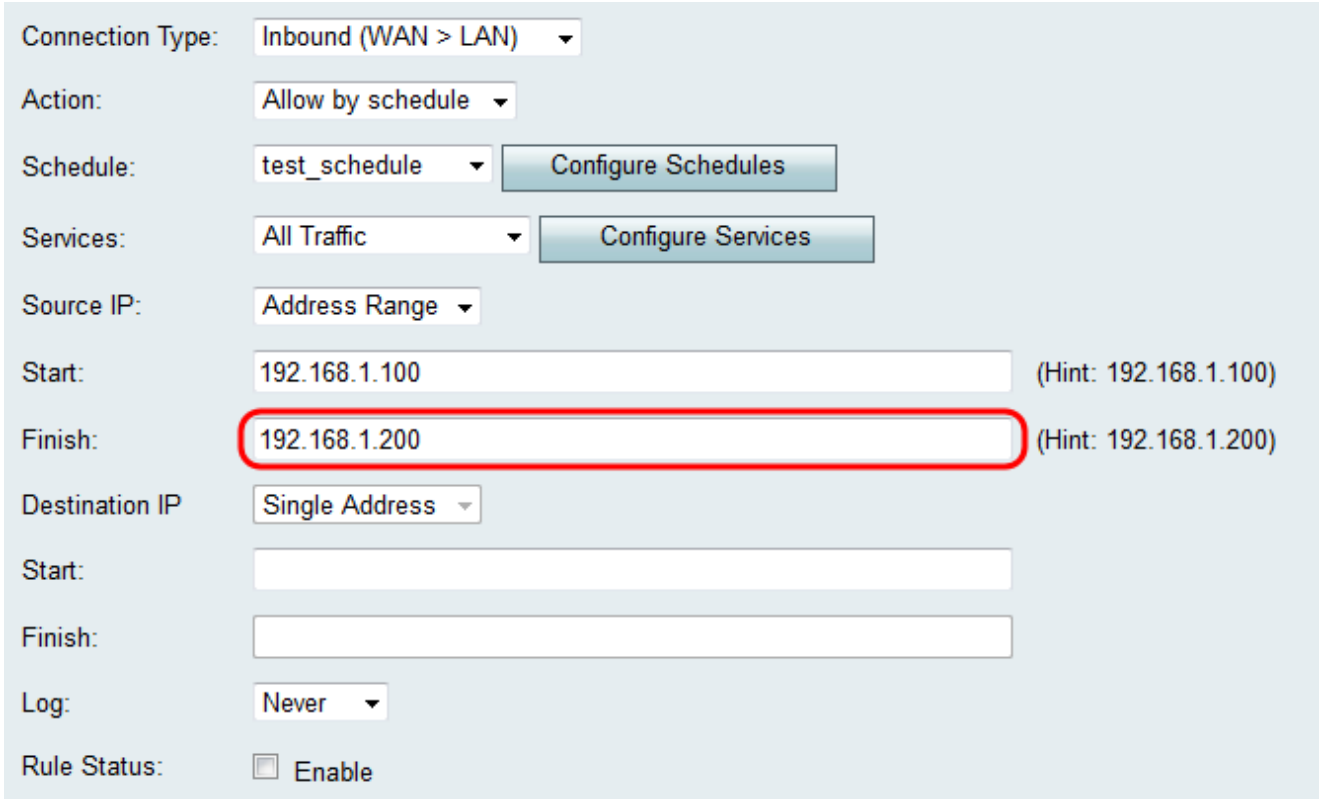
- Eine Adresse - Gilt für Datenverkehr, der von einer einzigen IP-Adresse im öffentlichen Internet ausgeht. Geben Sie die IP-Adresse in das Feld *Start* ein.

- Adressbereich - Gilt für Datenverkehr, der von einem IP-Adressbereich im öffentlichen Internet ausgeht. Geben Sie die Start-IP-Adresse des Bereichs im Feld *Start* und die End-IP-Adresse im Feld *Ende* ein, um den Bereich festzulegen.

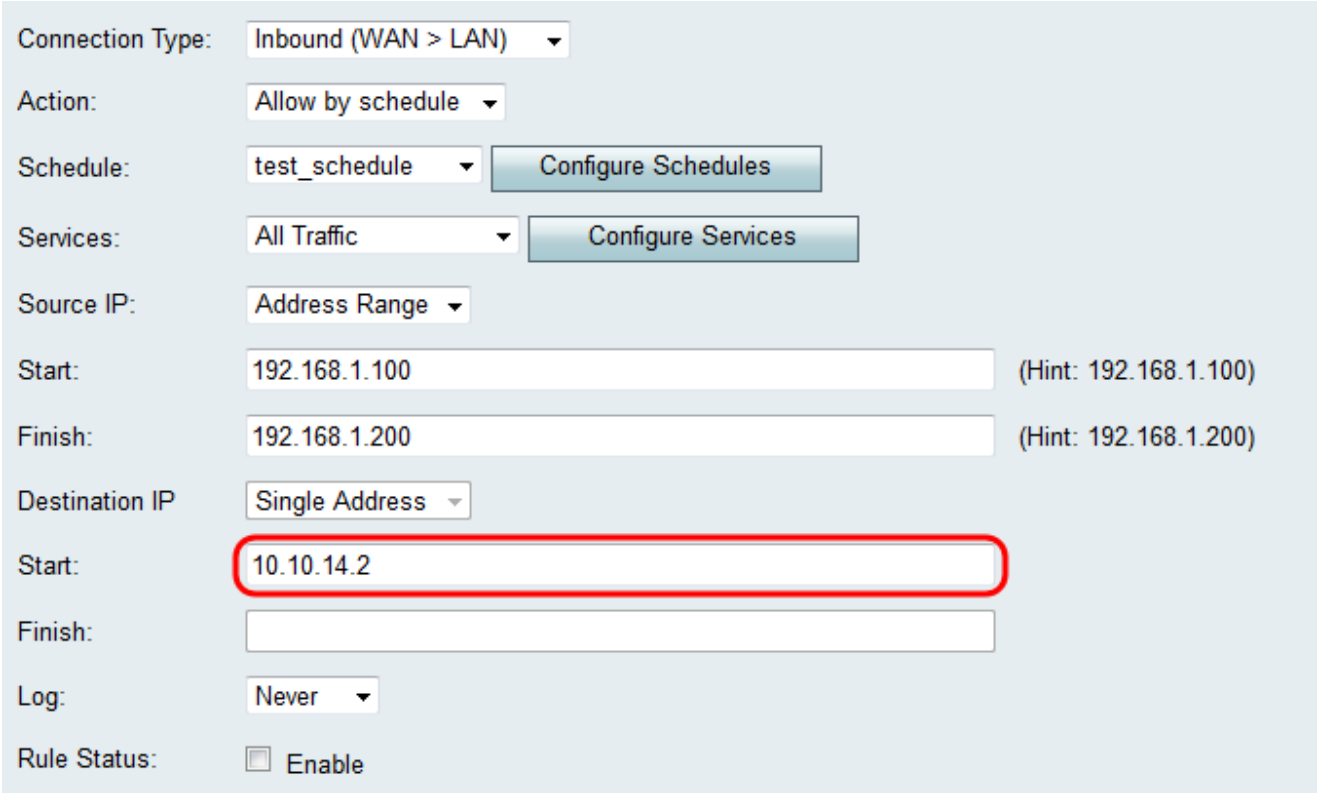
Schritt 2. Wenn Sie in Schritt 1 die Option **Einzelne Adresse** gewählt haben, geben Sie im Feld *Start* die IP-Adresse ein, die auf die Zugriffsregel angewendet wird, und fahren Sie dann mit Schritt 4 fort. Wenn Sie in Schritt 1 die Option **Adressbereich** gewählt haben, geben Sie im Feld *Start* eine Start-IP-Adresse ein, die auf die Zugriffsregel angewendet wird.



Schritt 3: Wenn Sie in Schritt 1 den **Adressbereich** ausgewählt haben, geben Sie die End-IP-Adresse ein, die den IP-Adressbereich für die Zugriffsregel im Feld *Beenden* kapselt.



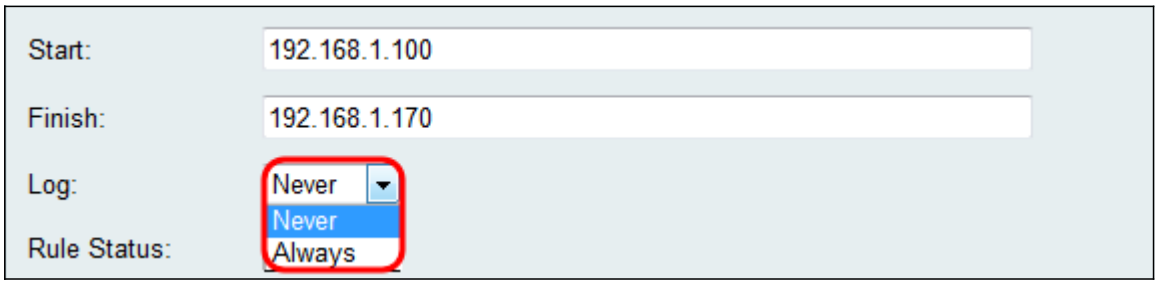
Schritt 4: Geben Sie eine einzelne Adresse für die Ziel-IP in das Feld *Start* unterhalb der Dropdown-Liste *Ziel-IP* ein. Für eingehenden Datenverkehr bezieht sich die Ziel-IP-Adresse auf die Adresse (im LAN), für die Datenverkehr aus dem öffentlichen Internet zugelassen oder abgelehnt wird.



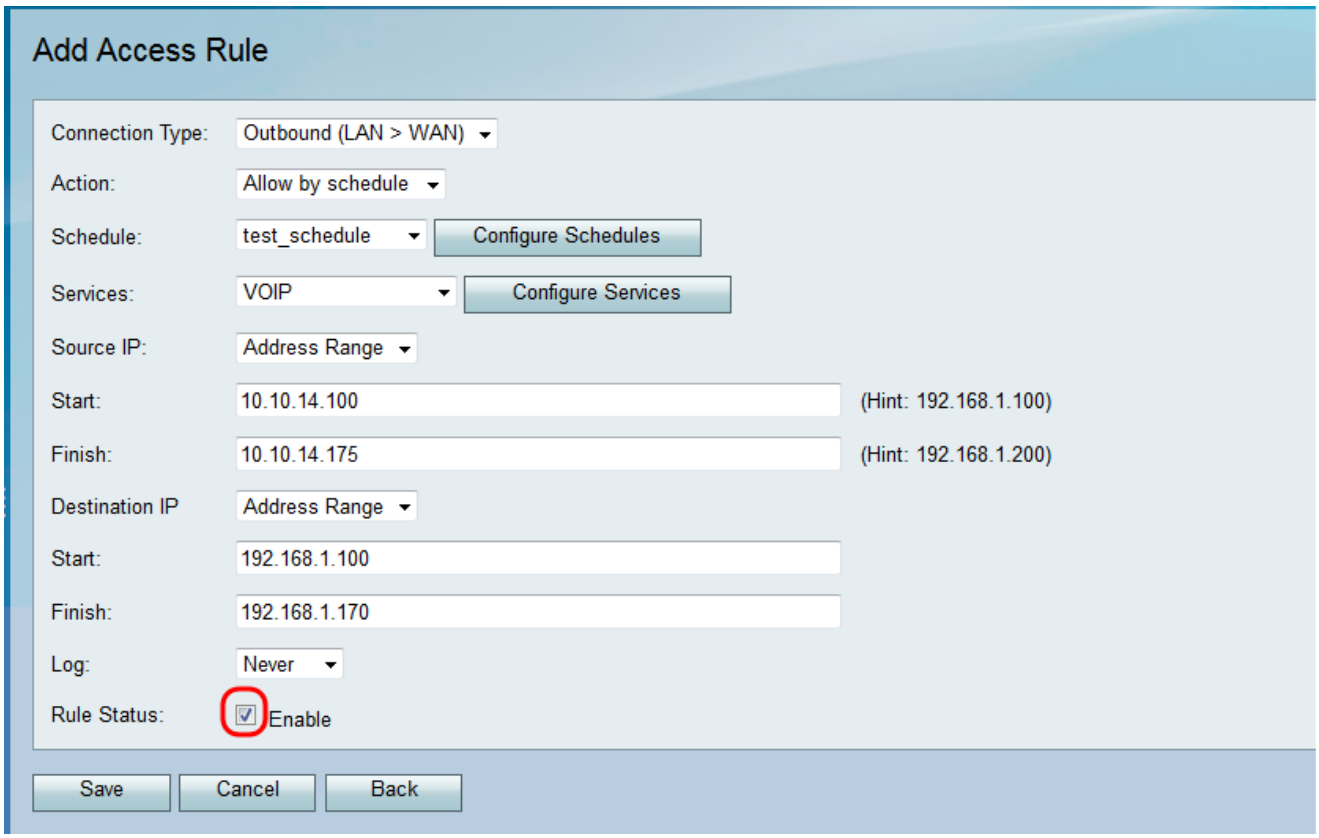
Anmerkung: Wenn in Schritt 3 des *Hinzufügens einer Zugriffsregel* als Verbindungstyp "**Inbound" (WAN > DMZ)** ausgewählt wurde, wird die einzelne Adresse für die Ziel-IP automatisch mit der IP-Adresse des aktivierten DMZ-Hosts konfiguriert.

Protokollieren und Aktivieren der Zugriffsregel

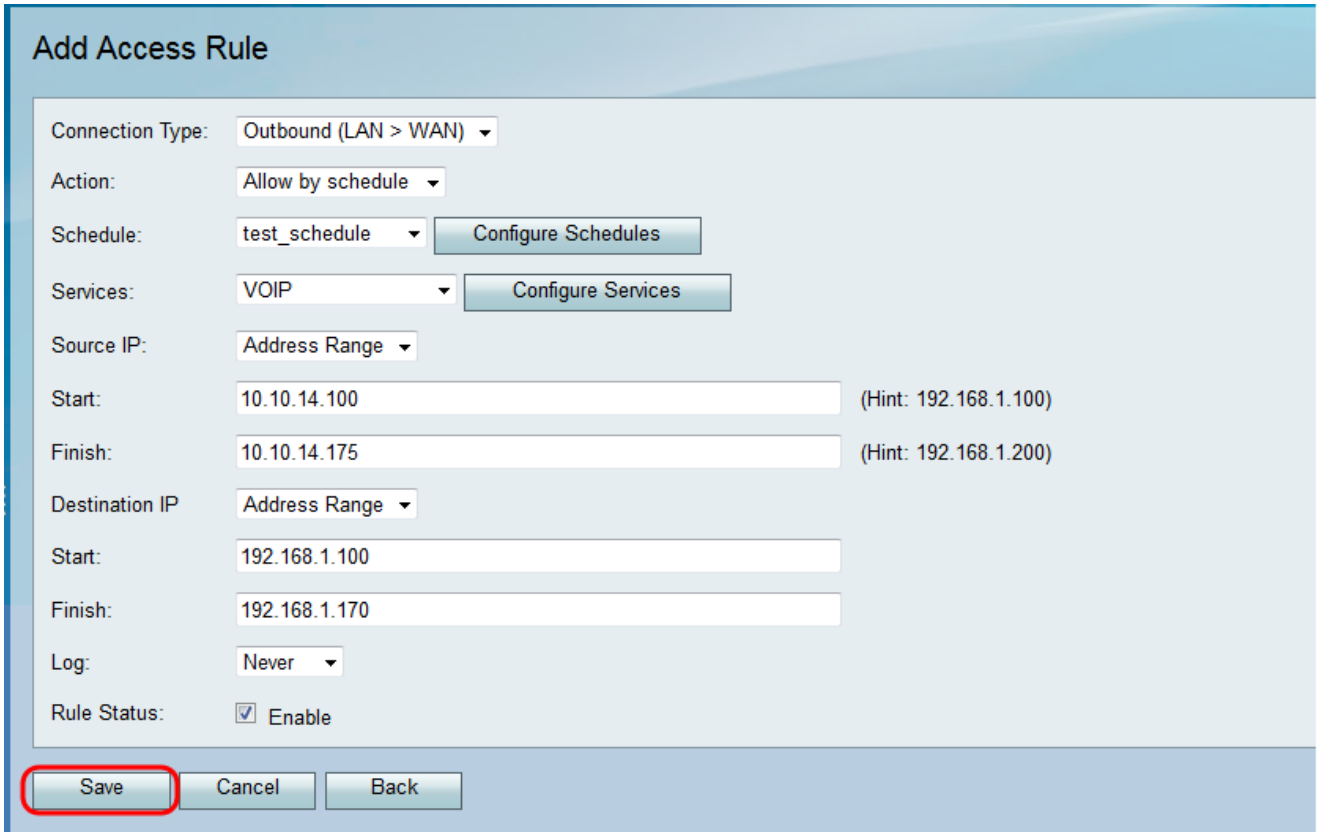
Schritt 1: Wählen Sie in der Dropdown-Liste *Protokoll* die Option **Immer aus,** wenn der Router Protokolle erstellen soll, sobald ein Paket mit einer Regel übereinstimmt. Wählen Sie **Nie,** wenn die Protokollierung bei Übereinstimmung mit einer Regel nie erfolgen soll.



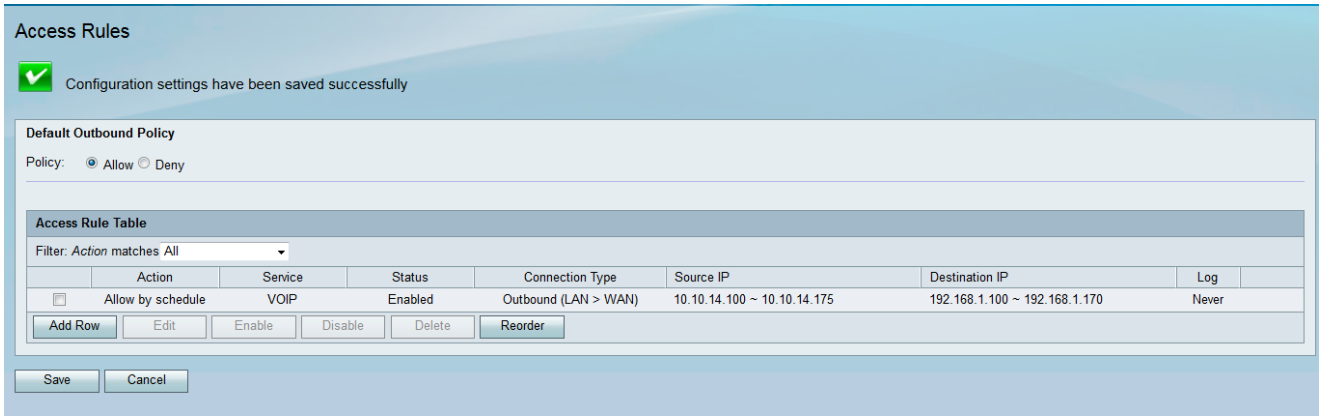
Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Zugriffsregel zu aktivieren.



Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.



Die *Zugriffsregeltabelle* wird mit der neu konfigurierten Zugriffsregel aktualisiert.


Access Rules
Configuration settings have been saved successfully
Default Outbound Policy
Policy: Allow Deny
Access Rule Table
Filter: Action matches All
Action
Service
Status
Connection Type
Source IP
Destination IP
Log
Allow by schedule
VOIP
Enabled
Outbound (LAN > WAN)
10.10.14.100 ~ 10.10.14.175
192.168.1.100 ~ 192.168.1.170
Never
Add Row
Edit
Enable
Disable
Delete
Reorder
Save
Cancel

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.