Konfiguration einer IPv4-Zugriffsregel auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziel

Anhand einer Zugriffsregel kann der Router anhand der Benutzeranforderung bestimmen, welcher Datenverkehr durch die Firewall geleitet werden darf und welcher Datenverkehr abgelehnt werden soll. Dadurch wird die Sicherheit des Routers erhöht.

In diesem Dokument wird das Verfahren zum Hinzufügen oder Löschen einer Zugriffsregel für die VPN-Router RV016, RV042, RV042G und RV082 erläutert.

Unterstützte Geräte

RV016
â€¢RV042
ãƒ» RV042G
RV082

Software-Version

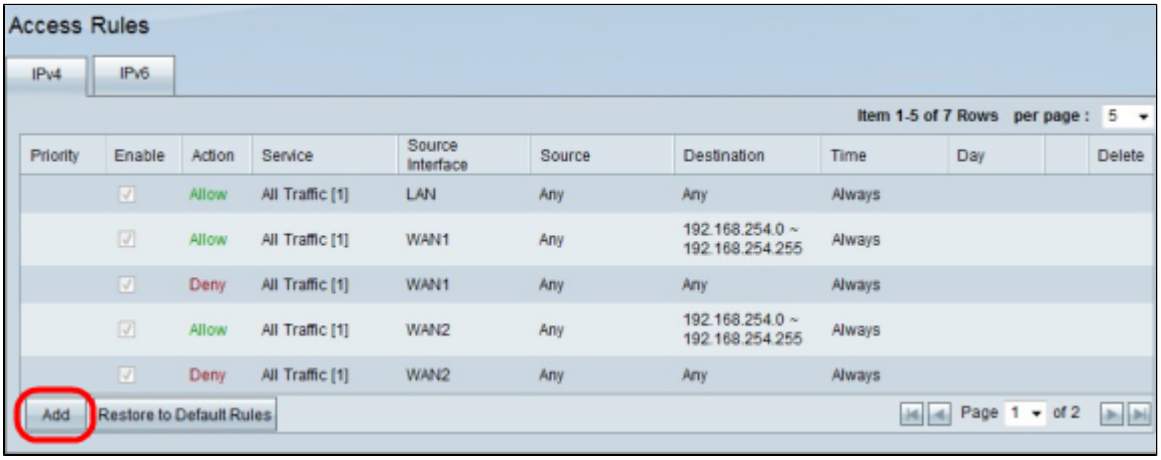
â€¢4.2.1.02

IPv4-Zugriffsregeln verwalten

Die Planung von IPv4-Zugriffsregeln ist eine optionale Konfiguration.

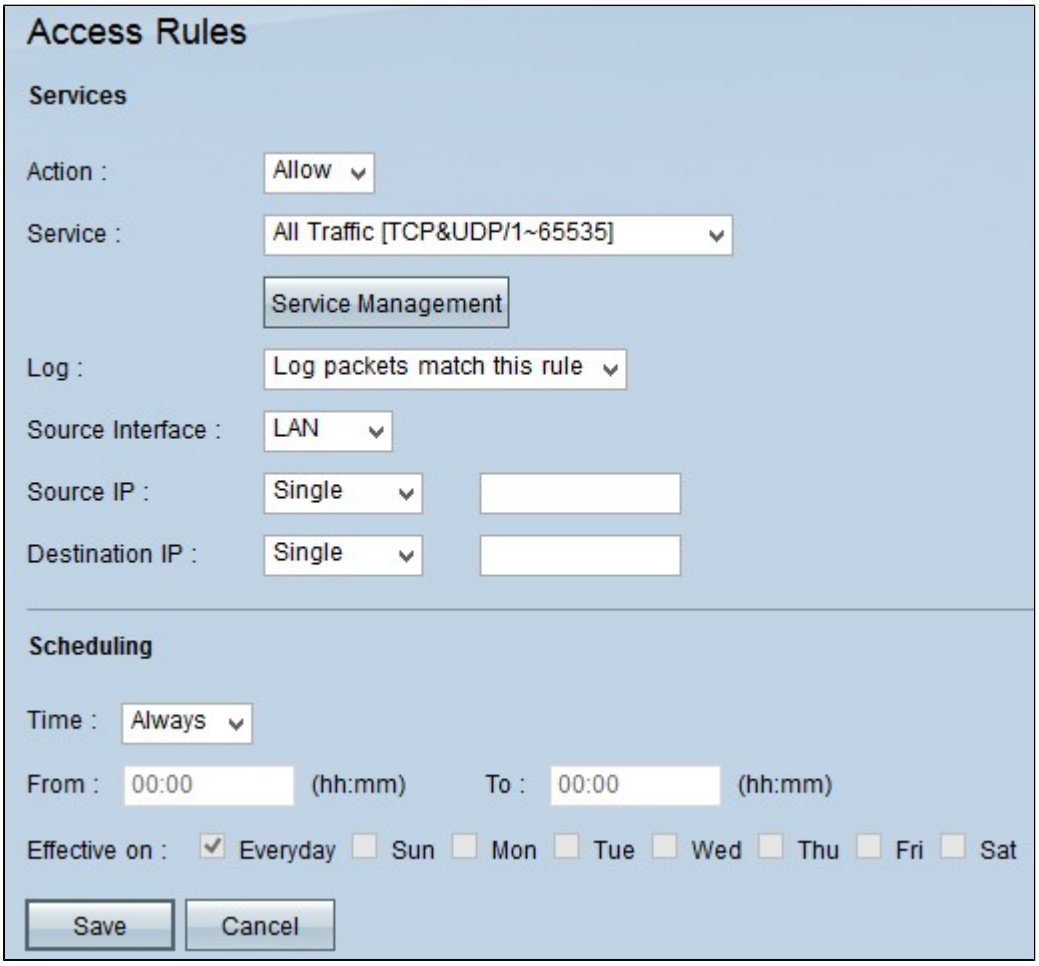
IPv4-Zugriffsregeln hinzufügen oder löschen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Access Rules aus**. Die Seite *IPv4 Access Rules* (IPv4-Zugriffsregeln) wird geöffnet. Klicken Sie auf **Hinzufügen**.



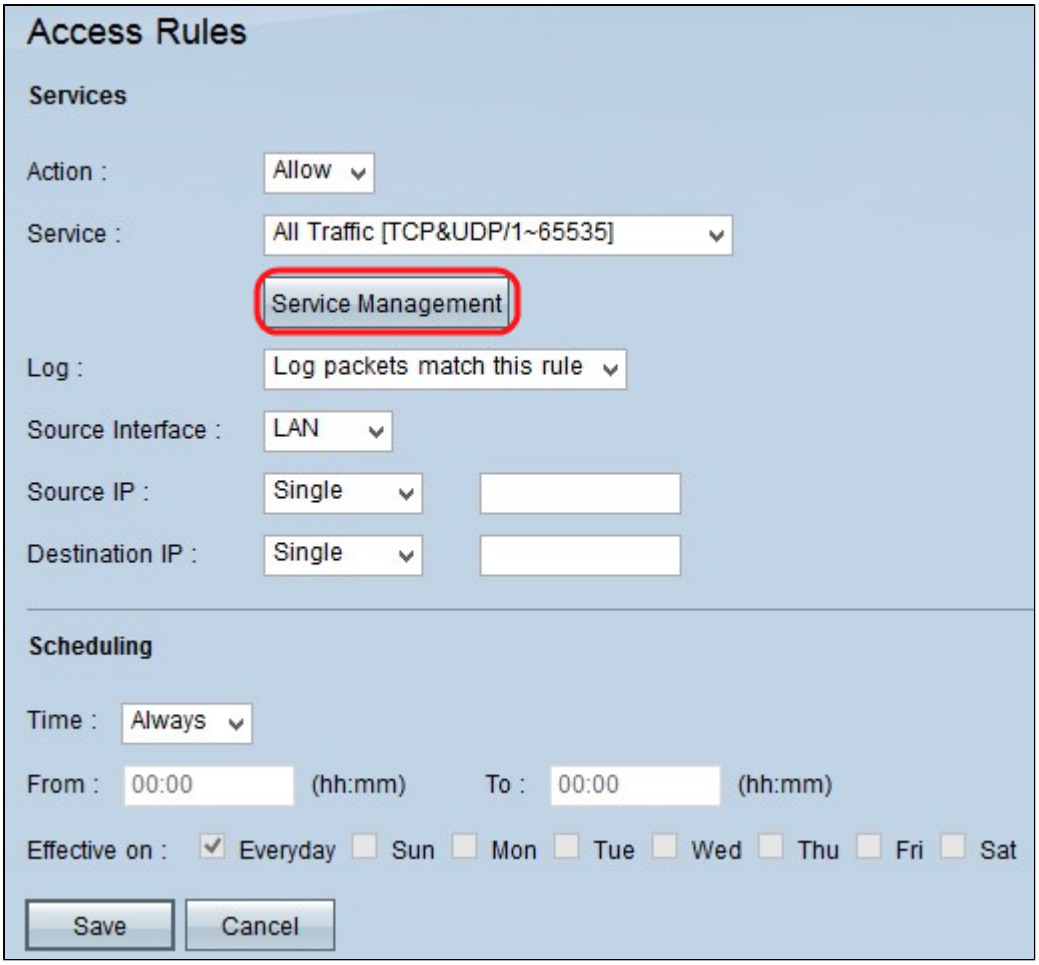
Schritt 2: Die Seite *Zugriffsregeldienst* wird geöffnet. Wählen Sie in der Dropdown-Liste Aktion die Option

Zulassen aus, um den Datenverkehr zuzulassen. Andernfalls wählen Sie **Verweigern**, um den Datenverkehr abzulehnen.



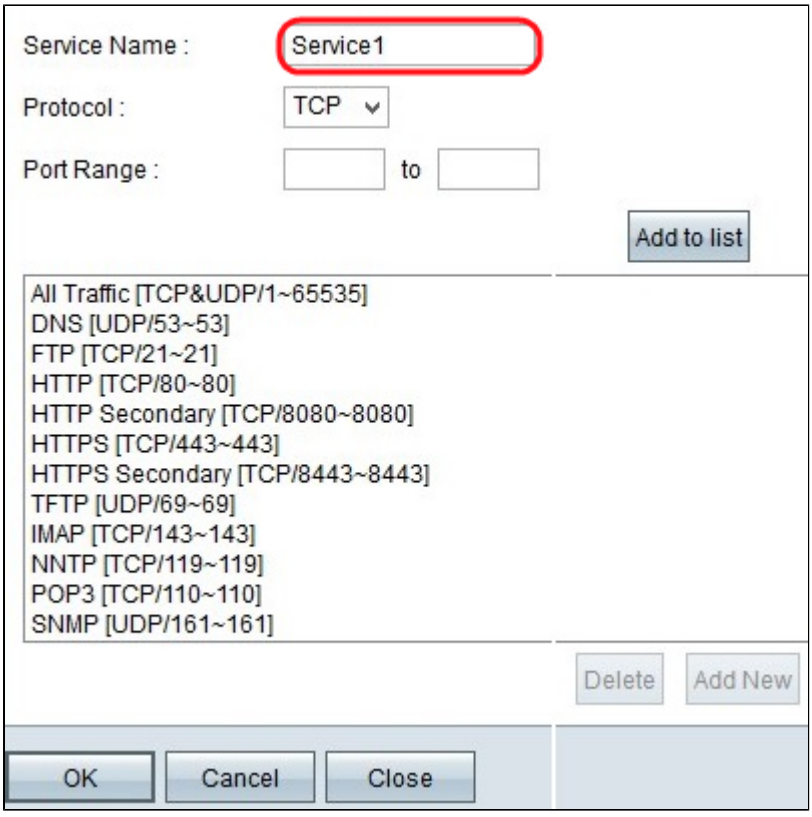
Schritt 3: Wählen Sie den entsprechenden Service aus der Dropdown-Liste aus. Wenn der entsprechende Service nicht verfügbar ist, klicken Sie auf **Service Management (Servicemanagement).**

Hinweis: Wenn der gewünschte Service verfügbar ist, fahren Sie mit Schritt 6 fort.



Schritt 4:

Ein neues Fenster wird angezeigt. Geben Sie im Feld "Servicename" einen Servicenamen ein.

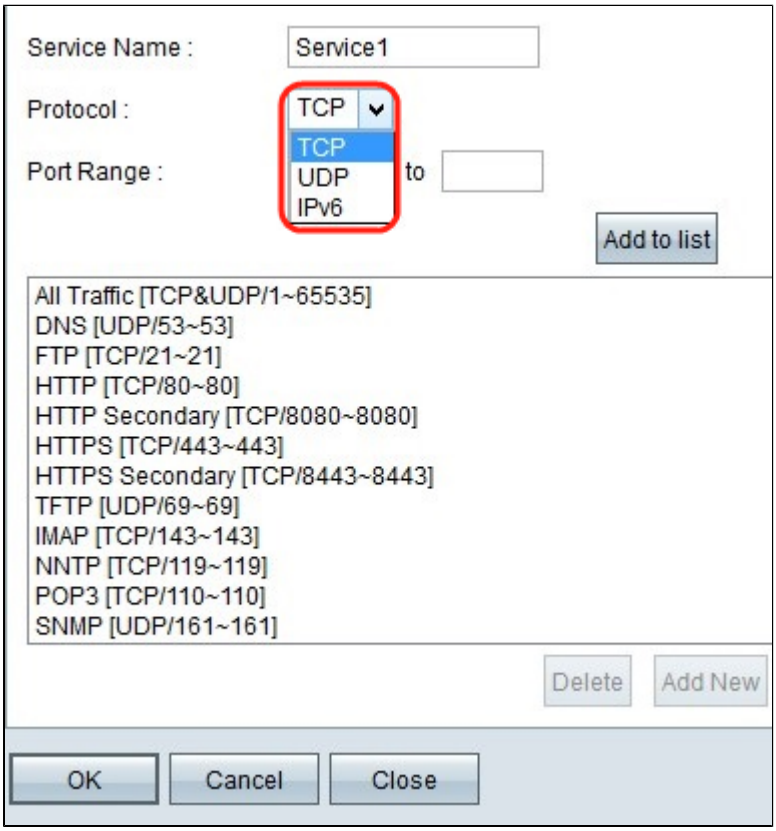


Schritt 5: Wählen Sie den entsprechenden Protokolltyp aus der Dropdown-Liste "Protokoll" aus.

ãƒ» TCP (Transmission Control Protocol) - Ein Transportschichtprotokoll, das von Anwendungen verwendet wird, die eine garantierte Bereitstellung erfordern.

ãƒ» UDP (User Datagram Protocol) â€" Verwendet Datagrammsockets, um die Kommunikation zwischen Host und Host herzustellen. Sie ist schneller als TCP, wird aber wahrscheinlich nicht erfolgreich bereitgestellt.

ãƒ» IPv6 (Internet Protocol Version 6) - Leitet den Internet-Datenverkehr zwischen Hosts in Paketen weiter, die über Netzwerke geroutet werden, die durch Routing-Adressen angegeben werden.

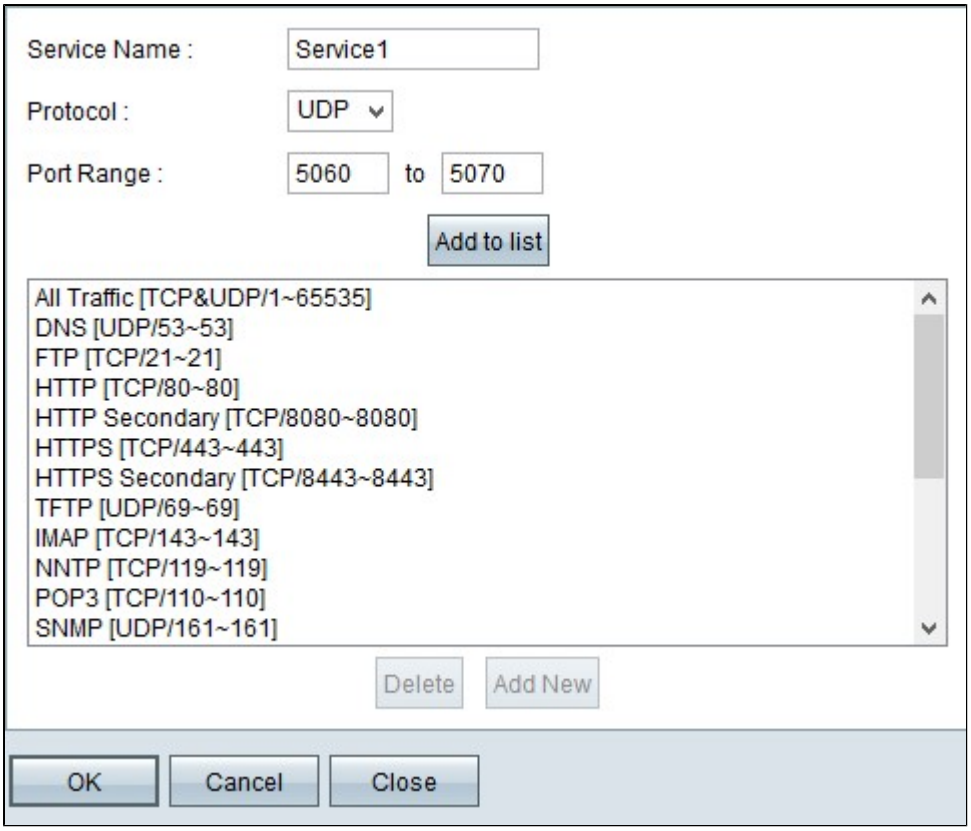


Schritt 6: Geben Sie den Port-Bereich in die Felder Port Range (Port-Bereich) ein. Dieser Bereich hängt vom gewählten Protokoll ab.

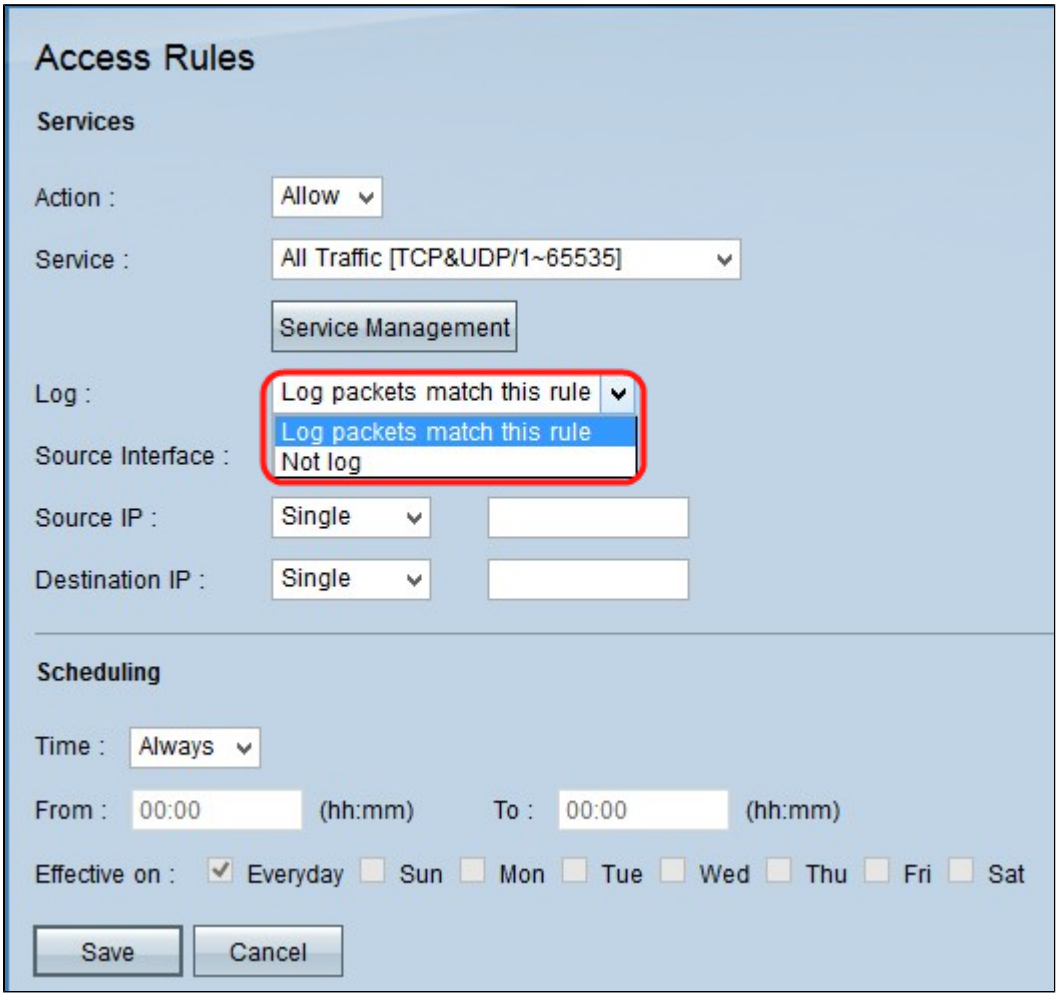
Klicken Sie auf **Zur Liste hinzufügen**. Damit wird der Service der Dropdown-Liste hinzugefügt.

Weitere Optionen sind **Löschen**, **Aktualisieren** oder **Neu hinzufügen**.

Klicken Sie auf **OK**. Das Fenster wird geschlossen, und der Benutzer kehrt zur Seite *Zugriffsregeldienst* zurück.



Schritt 7. Wählen Sie in der Dropdown-Liste Log (Protokoll) die Option **Log Packets match this rule (Pakete mit dieser Regel** protokollieren) aus, um die eingehenden Pakete zu protokollieren, die der Zugriffsregel entsprechen. Andernfalls wählen Sie **Nicht protokollieren**.



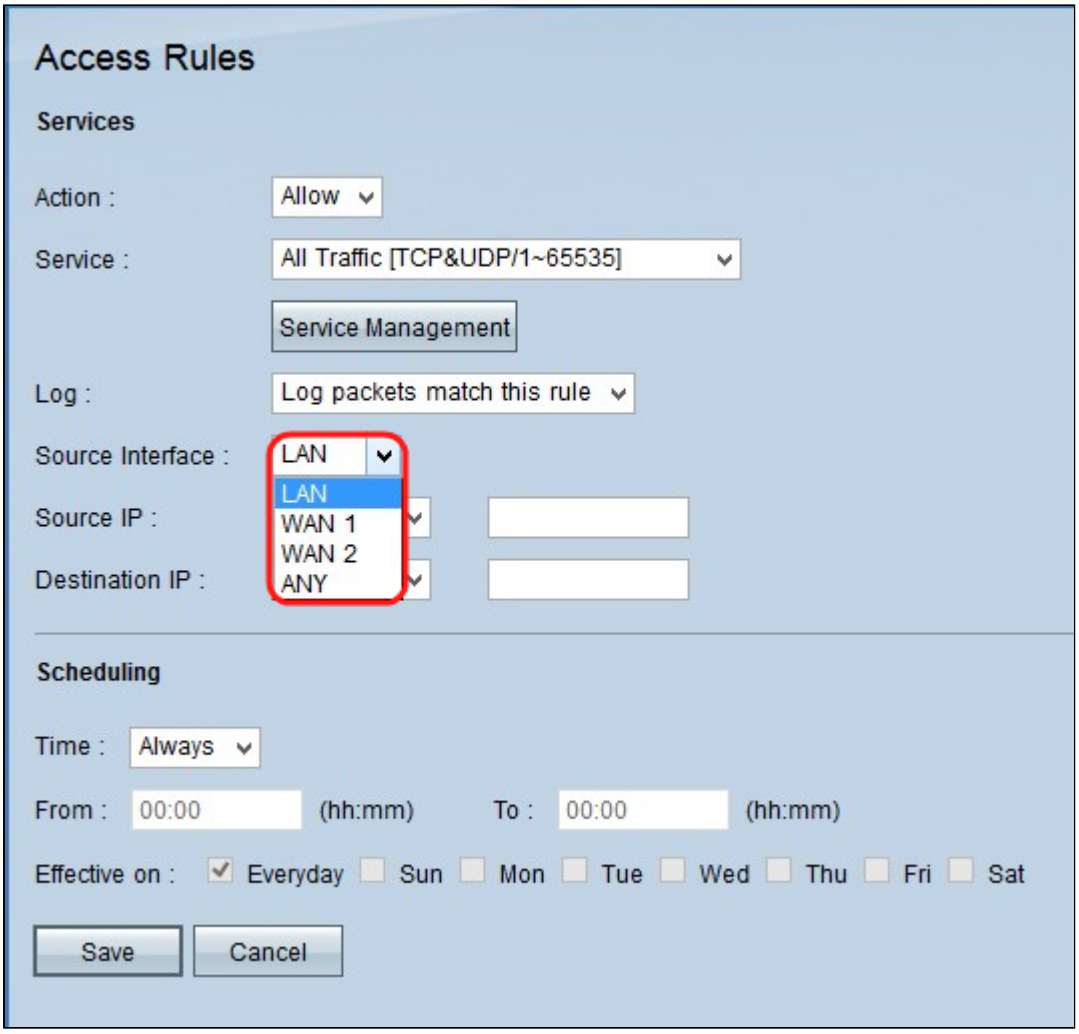
Schritt 8: Wählen Sie in der Dropdown-Liste "Source Interface" (Quellschnittstelle) die Schnittstelle aus, die von dieser Regel betroffen ist. Die Quellschnittstelle ist die Schnittstelle, von der aus der Datenverkehr initiiert wird.

ãƒ» LAN - Das lokale Netzwerk des Routers.

ãƒ» WAN1: Das WAN oder das Netzwerk, von dem der Router über den ISP oder den Next-Hop-Router auf das Internet zugreift.

ãƒ» WAN2 - Das gleiche wie WAN1, mit der Ausnahme, dass es sich um ein sekundäres Netzwerk handelt.

ãƒ» BELIEBIG â€" Ermöglicht die Verwendung jeder beliebigen Schnittstelle.

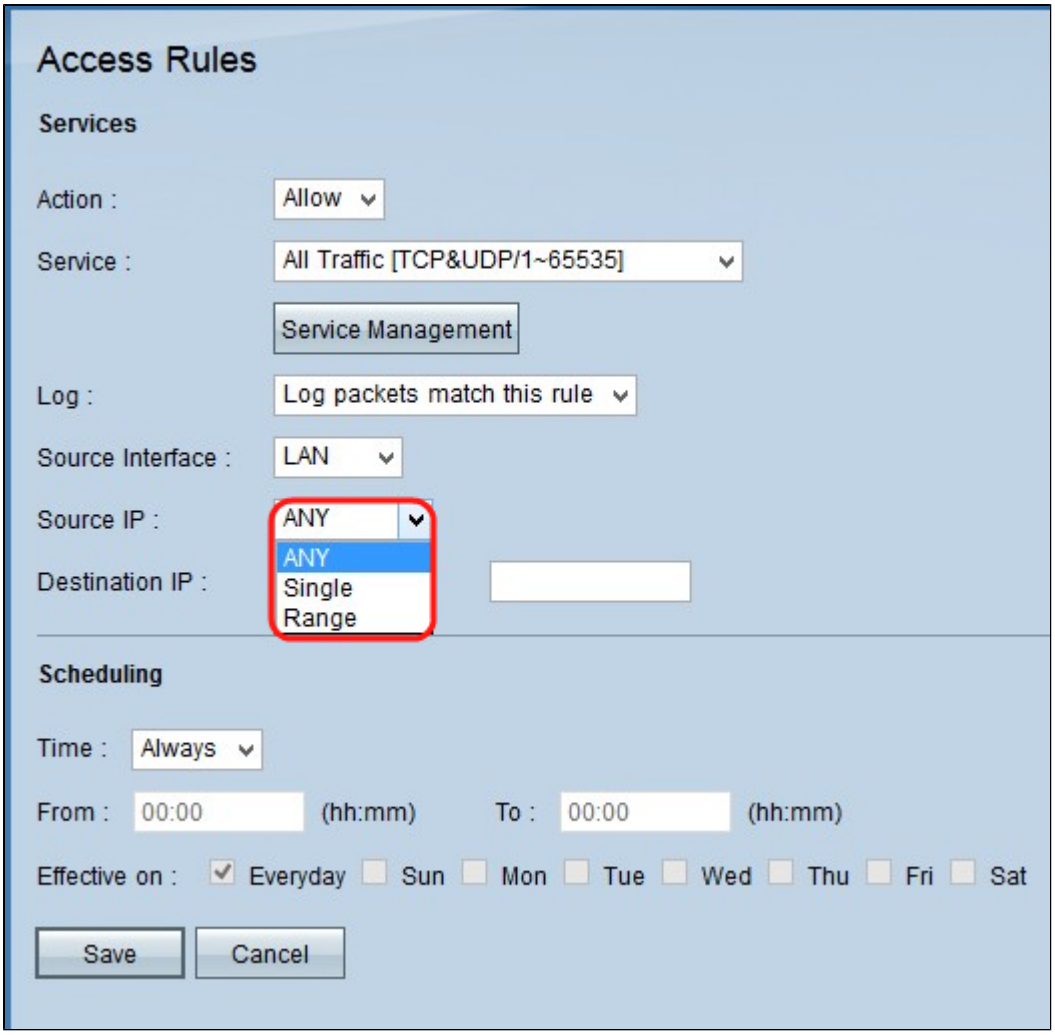


Schritt 9. Wählen Sie in der Dropdown-Liste Source IP (Quell-IP) eine Option aus, um den Bereich der Quell-IP-Adressen anzugeben, die von der Schnittstelle zugelassen oder abgelehnt werden sollen. Pakete, die über die Schnittstelle eingehen, werden durch die Quell- und Ziel-IP-Adresse überprüft.

ãƒ» Any (Beliebig): Die Zugriffsregel wird auf den gesamten Datenverkehr von der Quellschnittstelle angewendet. Rechts neben der Dropdown-Liste werden keine Felder angezeigt.

ãƒ» Single - Die Zugriffsregel wird auf eine einzelne IP-Adresse von der Quellschnittstelle angewendet. Geben Sie die gewünschte IP-Adresse in das Adressfeld ein.

ãƒ» Bereich - Die Zugriffsregel wird von der Quellschnittstelle aus auf ein Subnetz angewendet. Geben Sie die IP-Adresse und die Präfixlänge ein.



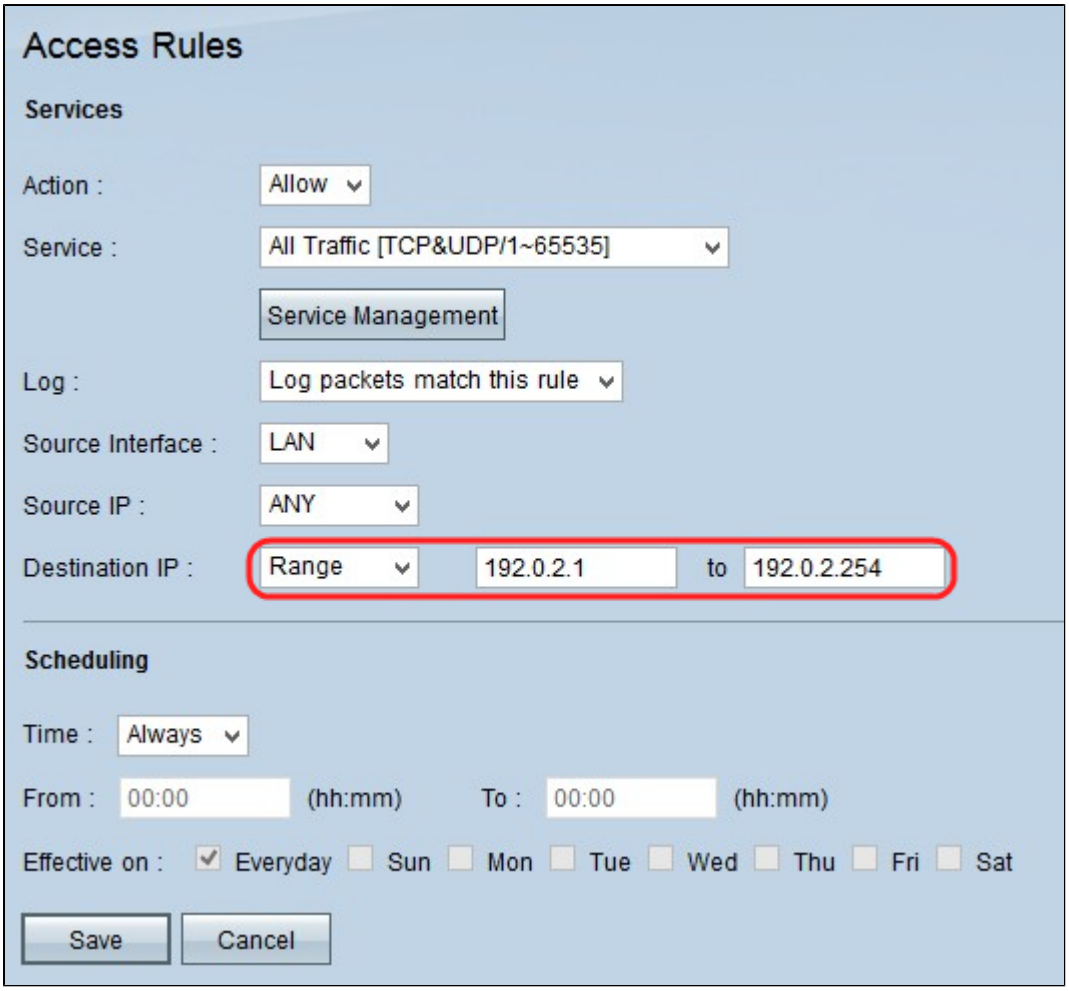
Schritt 9. Wählen Sie in der Dropdown-Liste Destination (Ziel) eine Option aus, um den Bereich der Zieladressen anzugeben, die von der Schnittstelle zugelassen oder abgelehnt werden sollen. Pakete, die über die Schnittstelle eingehen, werden durch die Quell- und Ziel-IP-Adresse überprüft.

ãƒ» Any (Beliebig): Die Zugriffsregel wird auf den gesamten Datenverkehr an die Zielschnittstelle angewendet. Rechts neben der Dropdown-Liste werden keine Felder angezeigt.

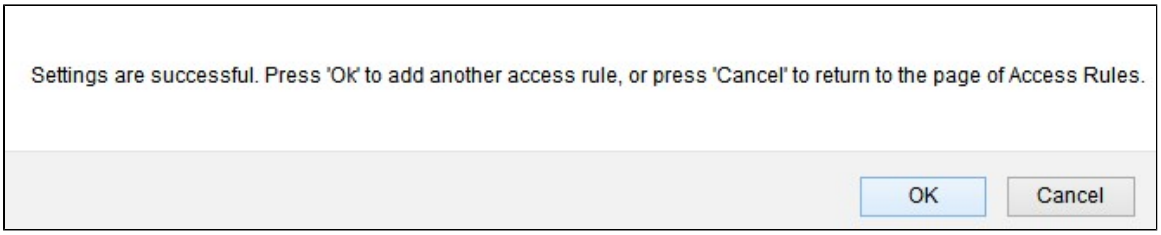
ãƒ» Single (Einfach): Eine Zugriffsregel wird auf eine einzelne IP-Adresse auf die Zielschnittstelle angewendet. Geben Sie die gewünschte IP-Adresse in das Adressfeld ein.

ãƒ» Bereich - Die Zugriffsregel wird in einem Subnetz auf die Zielschnittstelle angewendet. Geben Sie die IP-Adresse und die Präfixlänge ein.

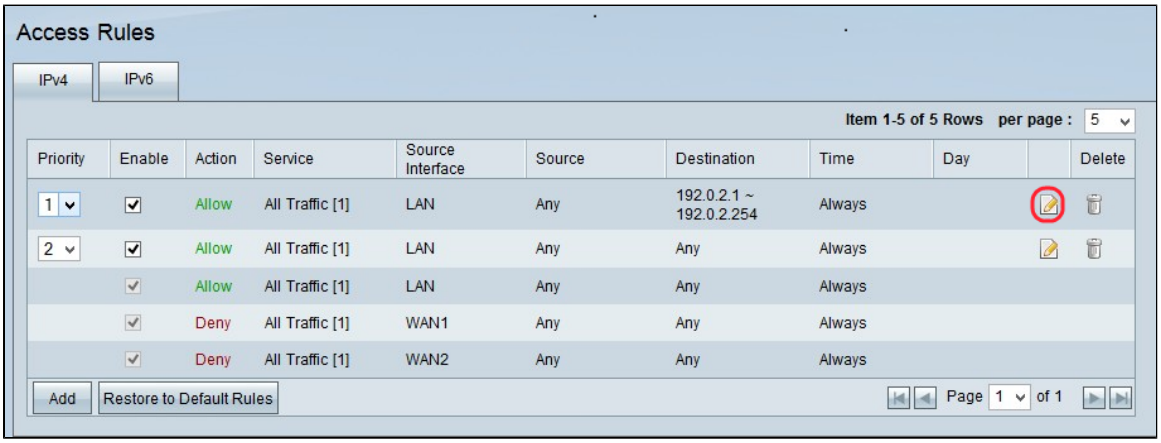
Klicken Sie auf **Speichern**, um alle Änderungen an der Zugriffsregel zu speichern. Es wird ein Bestätigungsfenster mit dem Status der am Gerät vorgenommenen Änderungen angezeigt.



Schritt 10. Klicken Sie auf **OK**, um eine weitere Zugriffsregel hinzuzufügen. Klicken Sie auf **Abbrechen**, um zur Seite *Zugriffsregeln* zurückzukehren.

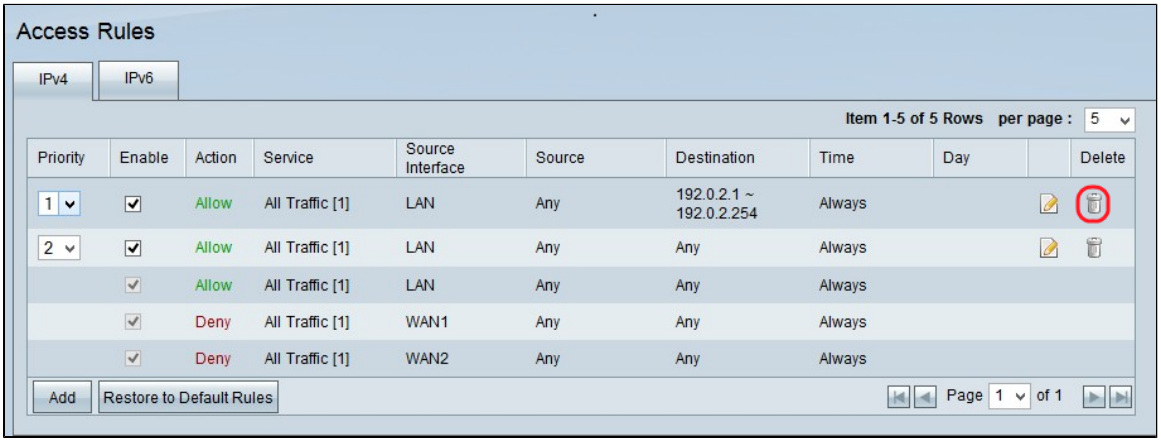


Schritt 11 (optional). Wählen Sie die gewünschte Zugriffsregel aus der Liste aus, und klicken Sie dann auf die **Schaltfläche Bearbeiten**, um die Konfiguration der Zugriffsregel zu bearbeiten.



Schritt 12 (optional). Wählen Sie die gewünschten Zugriffsregeln aus der Liste aus, und klicken Sie dann

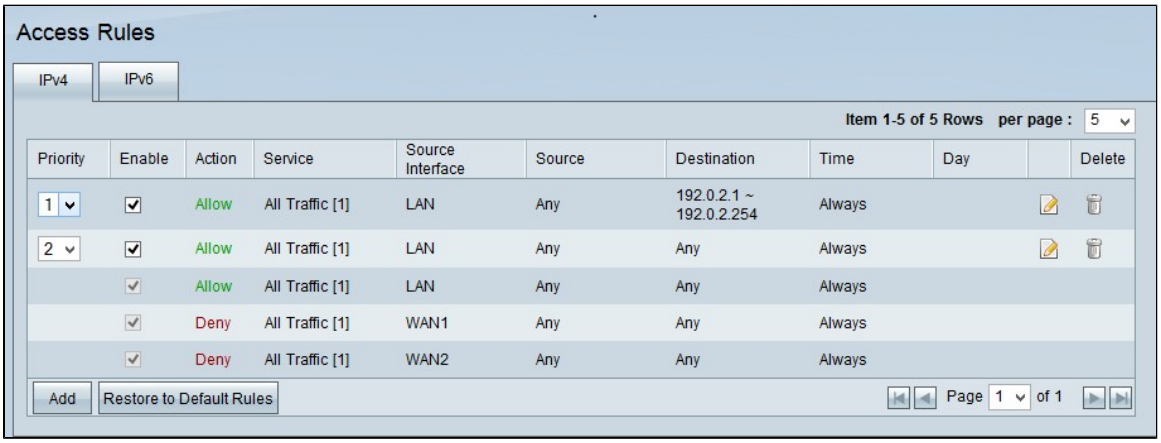
auf die **Schaltfläche Löschen**, um die Zugriffsregel aus der Liste der Zugriffsregeln zu löschen.



IPv4-Zugriffsregeln planen

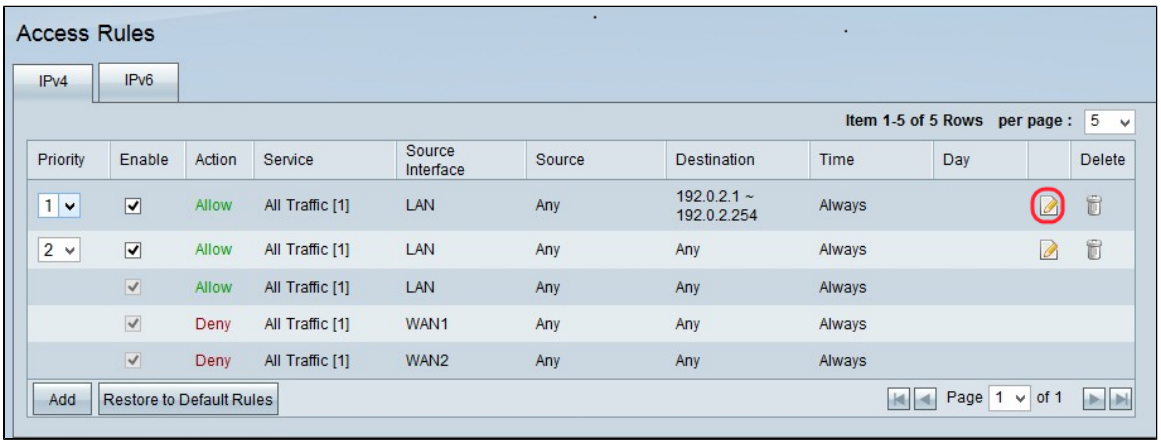
Die Planung von Zugriffsregeln erleichtert die Angabe eines Zeitplans, wenn diese Zugriffsregeln Tag und Uhrzeit sind. Es funktioniert nur mit IPv4.

Schritt 1: Verwenden Sie das Webkonfigurationsprogramm, und wählen Sie **Firewall > Access Rules aus**. Die Seite *IPv4 Access Rules* (IPv4-Zugriffsregeln) wird geöffnet:



Schritt 2: Wählen Sie die Zugriffsregel aus der Tabelle aus, und klicken Sie auf das Symbol **Edit** (**Bearbeiten**), um die Planungsfunktion zu dieser Zugriffsregel hinzuzufügen.

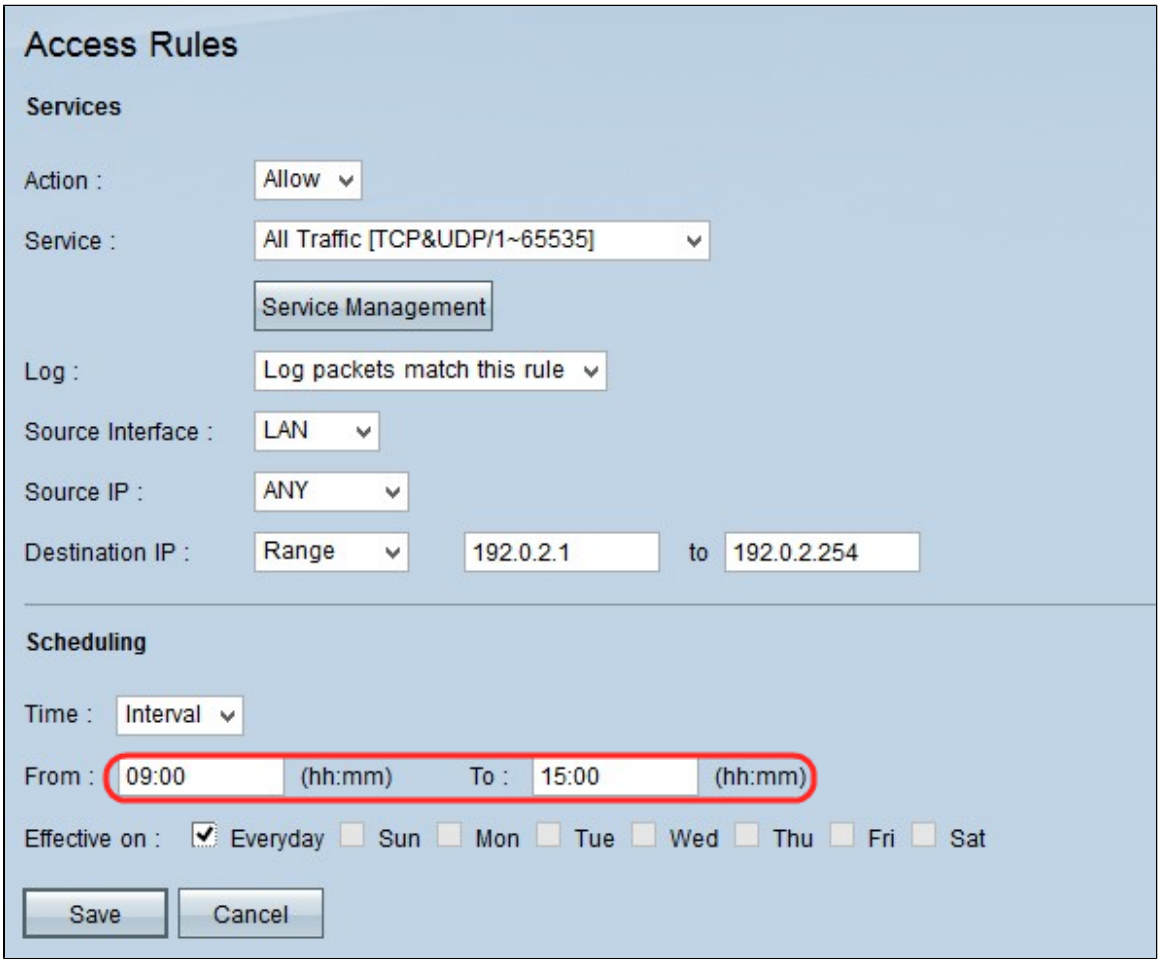
Hinweis: Sie können die Planungsfunktion auch hinzufügen, wenn Sie eine neue Zugriffsregel hinzufügen.



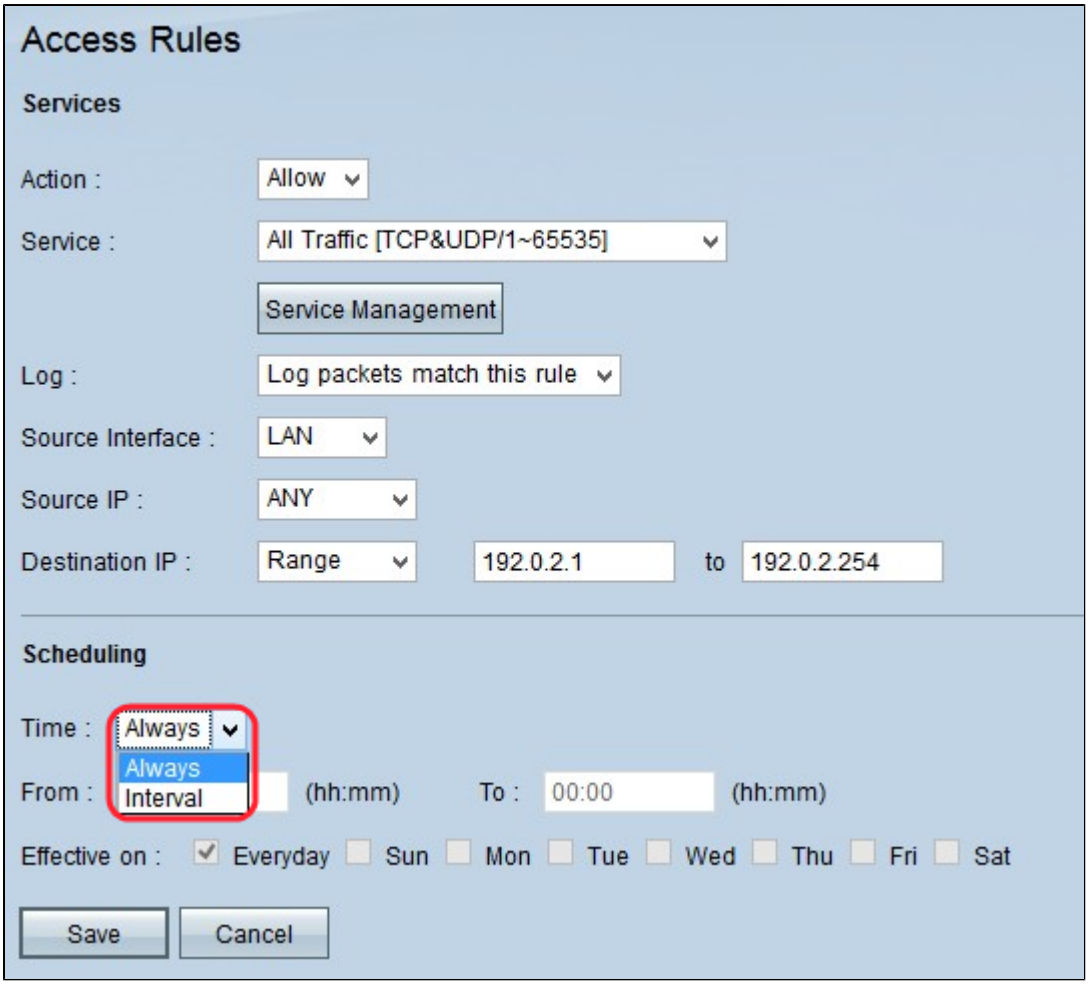
Schritt 3: Wählen Sie die Uhrzeit aus der Dropdown-Liste aus. Sie legt fest, wann die Zeitplanung verwendet werden soll.

ãƒ» Immer â€" Die Zugriffsregel gilt zu jeder Zeit und an allen Wochentagen. Sie ist standardmäßig ausgewählt. Wenn Sie diese Option auswählen, klicken Sie auf *Speichern*, und fahren Sie mit Schritt 6 fort.

ãƒ» Intervall â€" Basierend auf dem vom Benutzer angegebenen Zeitintervall wird die Zugriffsregel angewendet.

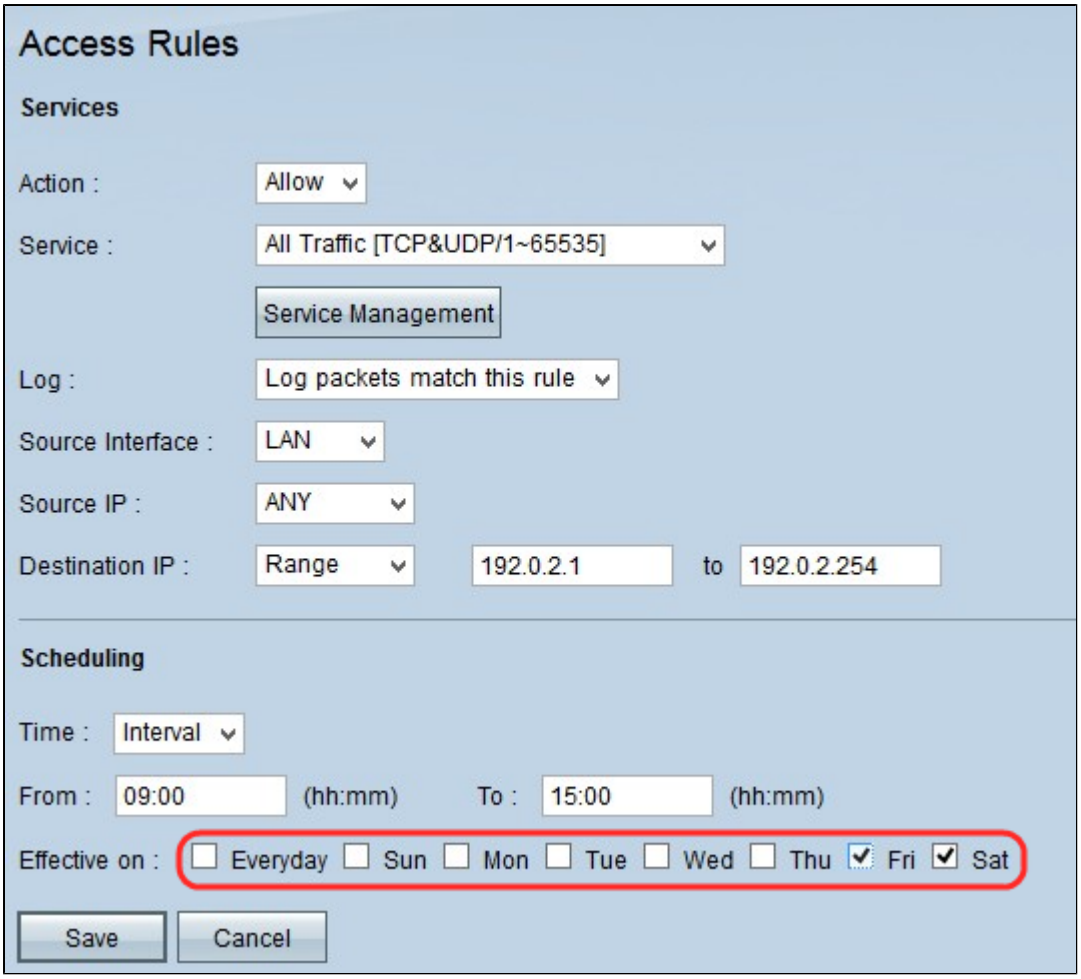


Schritt 4: Geben Sie das Zeitintervall im 24-Stunden-Format ein, während dessen die Zugriffsregel in den Feldern *Von* und *Bis* angewendet wird.

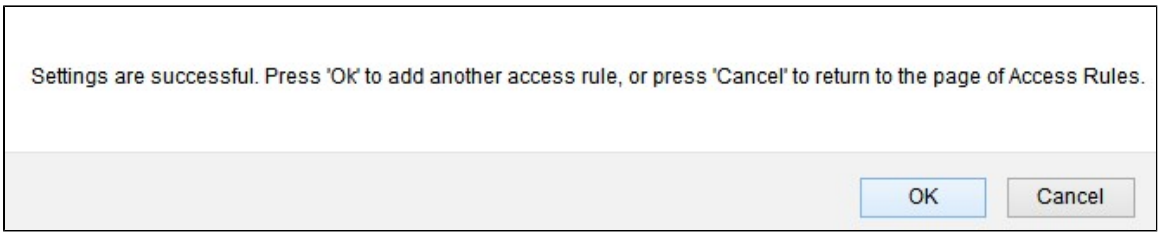


Schritt 5: Aktivieren Sie die Kontrollkästchen neben den Tagen, an denen die Zugriffsregel angewendet werden soll. Die Zugriffsregel gilt nur an den überprüften Tagen. Standardmäßig wird *Everyday (Täglich*) ausgewählt.

Klicken Sie auf **Speichern**, um alle Änderungen an der Zugriffsregel zu speichern. Es wird ein Bestätigungsfenster mit dem Status der am Gerät vorgenommenen Änderungen angezeigt.



Schritt 6: Klicken Sie auf **OK**, um eine weitere Zugriffsregel hinzuzufügen. Klicken Sie auf **Abbrechen**, um zur Seite mit den Zugriffsregeln zurückzukehren.



Schlussfolgerung

Sie haben jetzt IPv4-Zugriffsregeln für Ihren RV016-, RV042-, RV042G- oder RV082-VPN-Router eingerichtet.

Wenn Sie auf den gesamten Support für diese Router zugreifen möchten, sehen Sie sich die Produktseite an, indem Sie hier klicken.

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.