Konfiguration einer IPv6-Zugriffsregel für die VPN-Router RV016, RV042, RV042G und RV082

Ziel

Mithilfe einer Zugriffsregel kann der Router bestimmen, welcher Datenverkehr die Firewall passieren darf. Dies trägt dazu bei, die Sicherheit des Routers zu erhöhen.

In diesem Artikel wird erläutert, wie Sie eine IPv6-Zugriffsregel für die VPN-Router RV016, RV042, RV042G und RV082 hinzufügen.

Anwendbare Geräte

RV016
RV042
RV042G
RV082

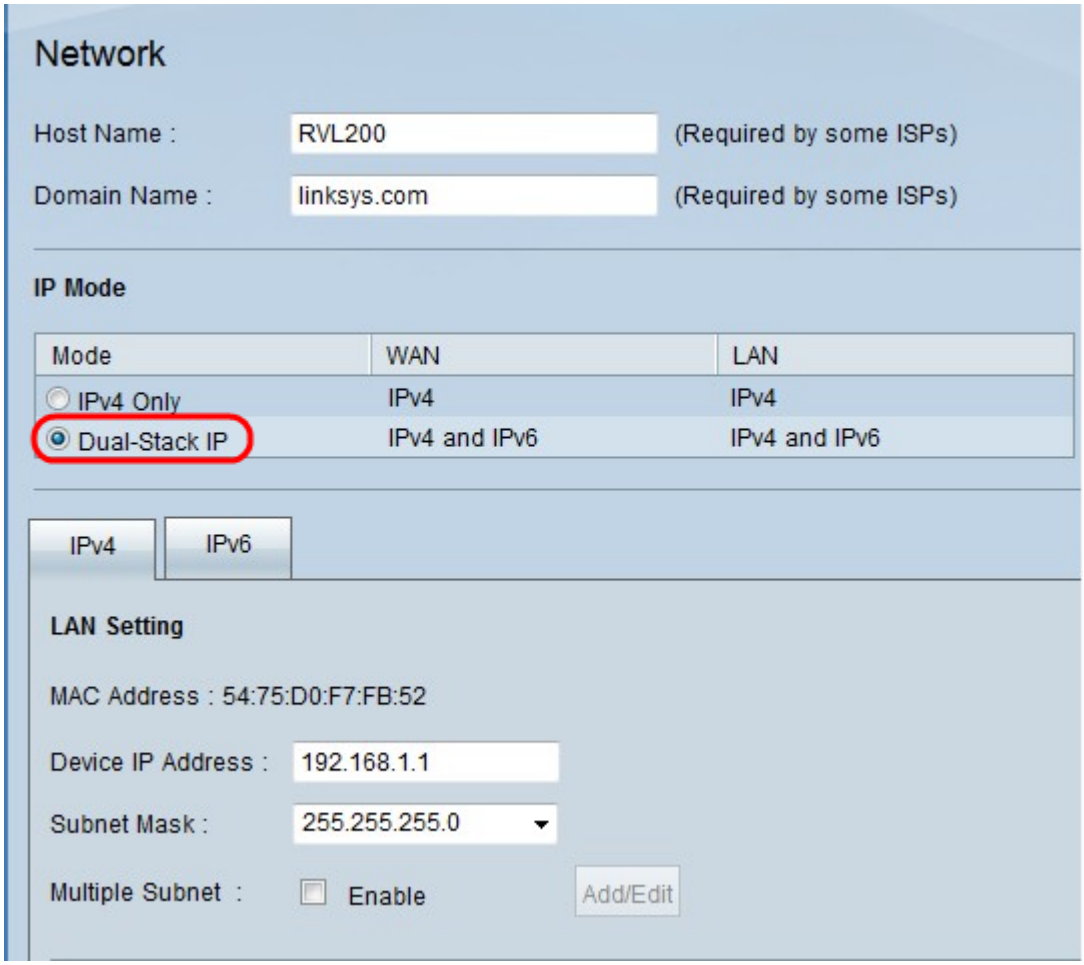
Softwareversion

·v4.2.1.02

Konfiguration einer IPv6-Zugriffsregel

IPv6-Modus aktivieren

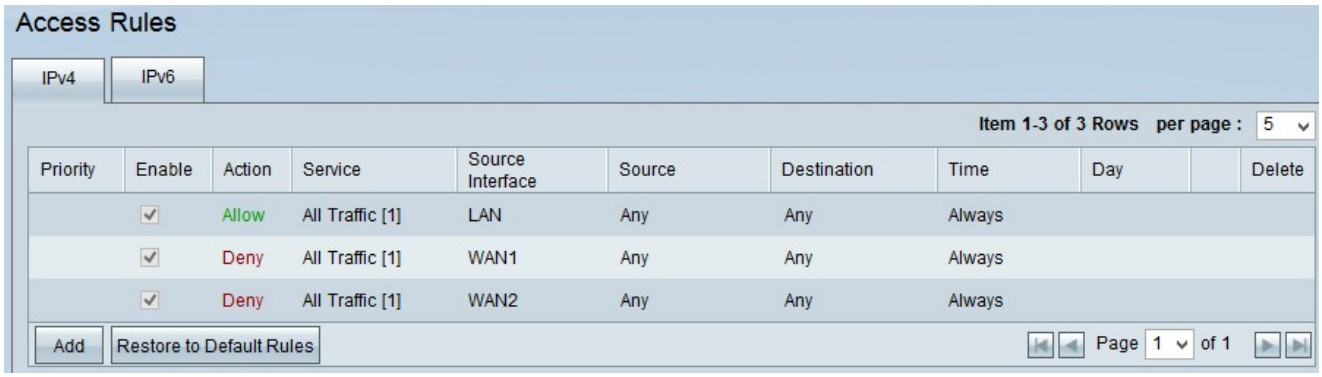
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Setup > Network (Setup > Netzwerk)**. Die Seite *Netzwerk* wird geöffnet:



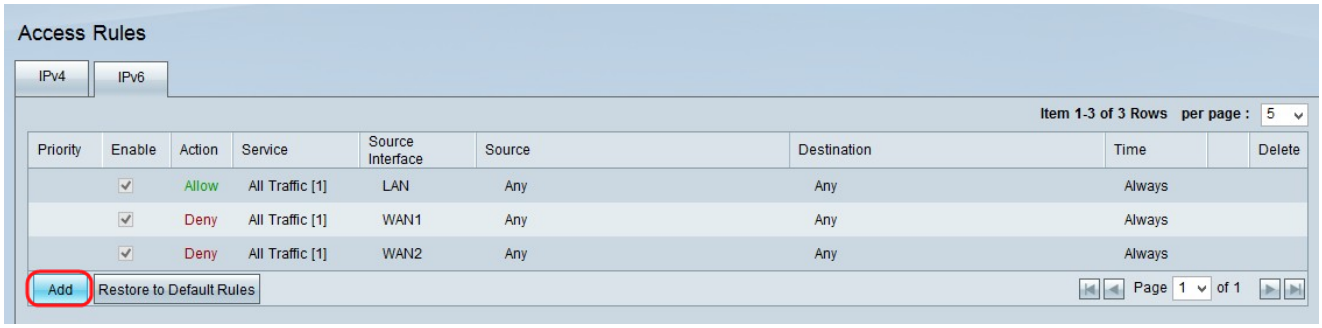
Schritt 2: Klicken Sie auf das Optionsfeld **Dual-Stack IP**. Dadurch können IPv4 und IPv6 gleichzeitig ausgeführt werden. Wenn IPv6-Kommunikation möglich ist, ist dies die bevorzugte Kommunikation.

Konfiguration von IPv6-Zugriffsregeln

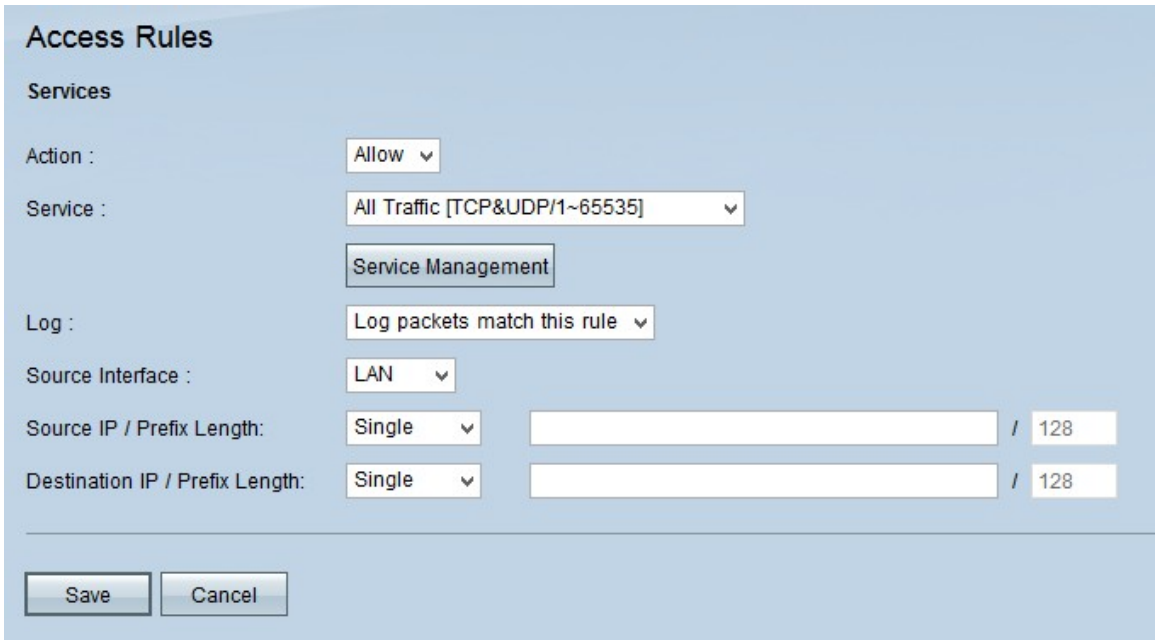
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Access Rules aus**. Die Seite *Zugriffsregeln* wird geöffnet:



Schritt 2: Klicken Sie auf die Registerkarte IPv6. Daraufhin wird die Seite *IPv6-Zugriffsregeln* geöffnet.



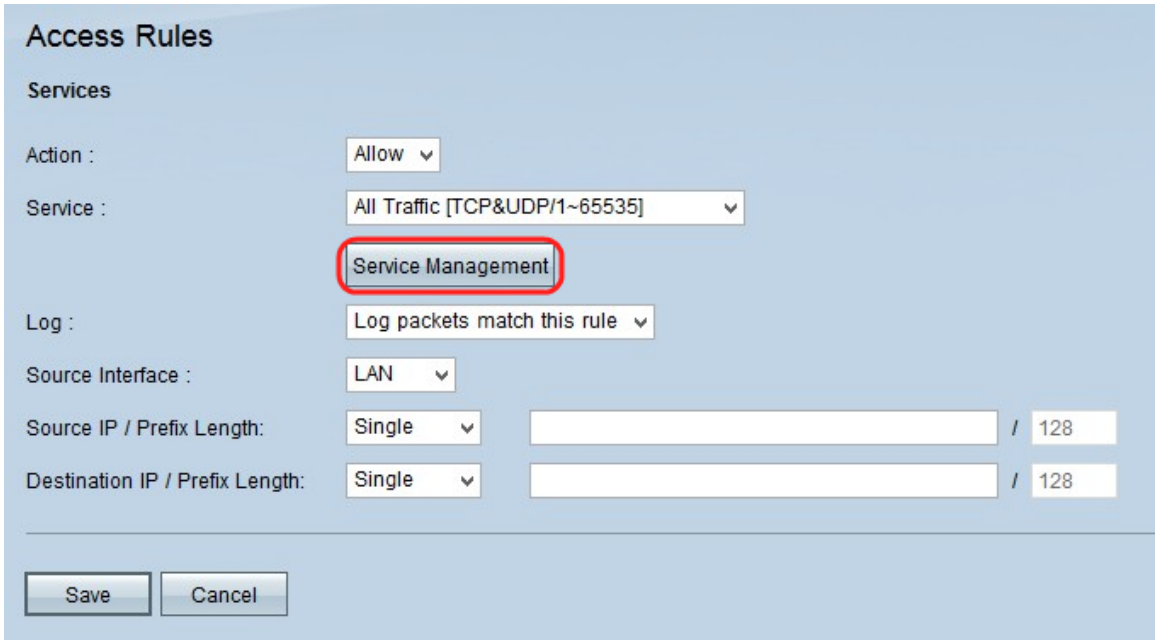
Schritt 3: Klicken Sie auf **Hinzufügen**, um die Zugriffsregeln hinzuzufügen. Die Seite *Zugriffsregeln* wird angezeigt, um die Zugriffsregeln für IPv6 zu konfigurieren.



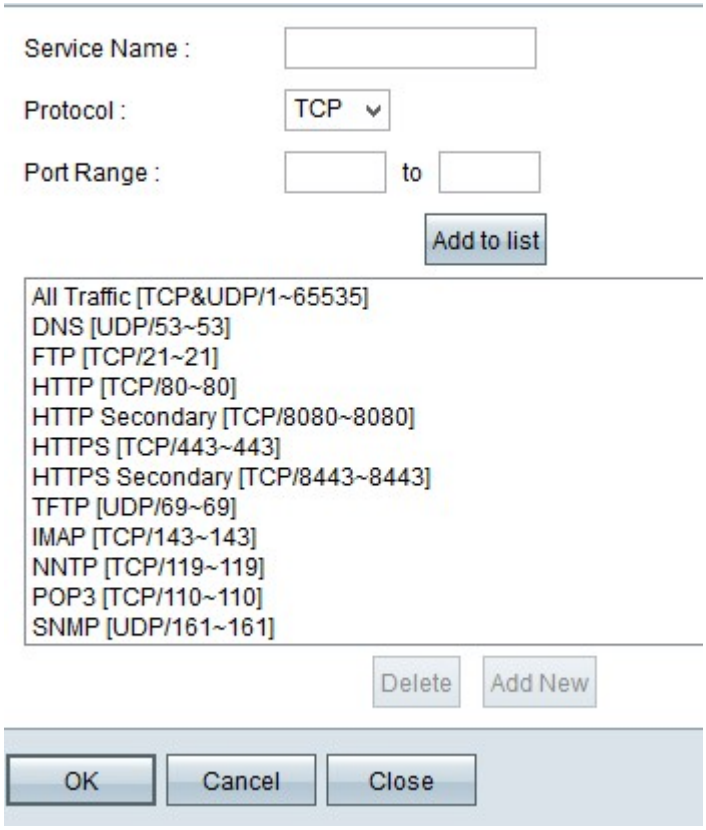
Schritt 4: Wählen Sie **Zulassen** aus der Dropdown-Liste Aktion aus, wenn der Datenverkehr zugelassen werden soll. Wählen Sie **Verweigern**, um den Datenverkehr abzulehnen.

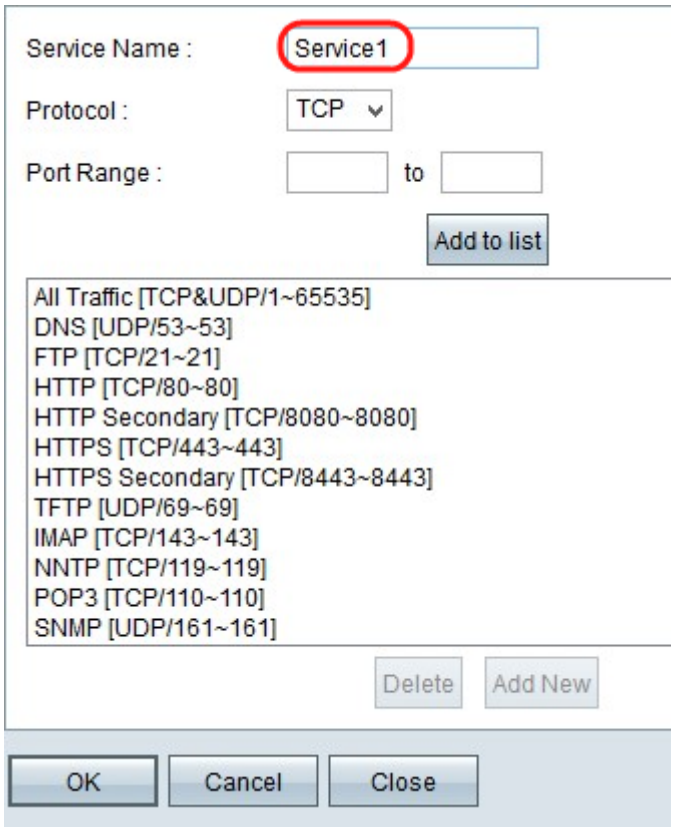
Schritt 5: Wählen Sie den entsprechenden Service in der Dropdown-Liste Service aus.

Zeitgeber: Wenn der gewünschte Service verfügbar ist, fahren Sie mit Schritt 12 fort.

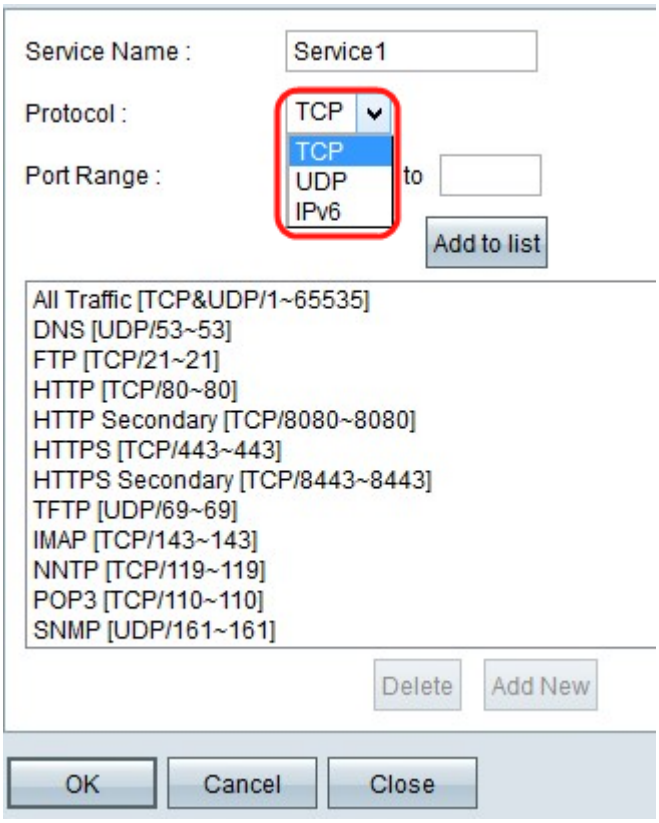


Schritt 6: Wenn der entsprechende Service nicht verfügbar ist, klicken Sie auf **Service Management.** Das Fenster *Service Management* (Dienstverwaltung) wird angezeigt.





Schritt 7: Geben Sie im Feld Dienstname einen Namen für den neuen Dienst ein.

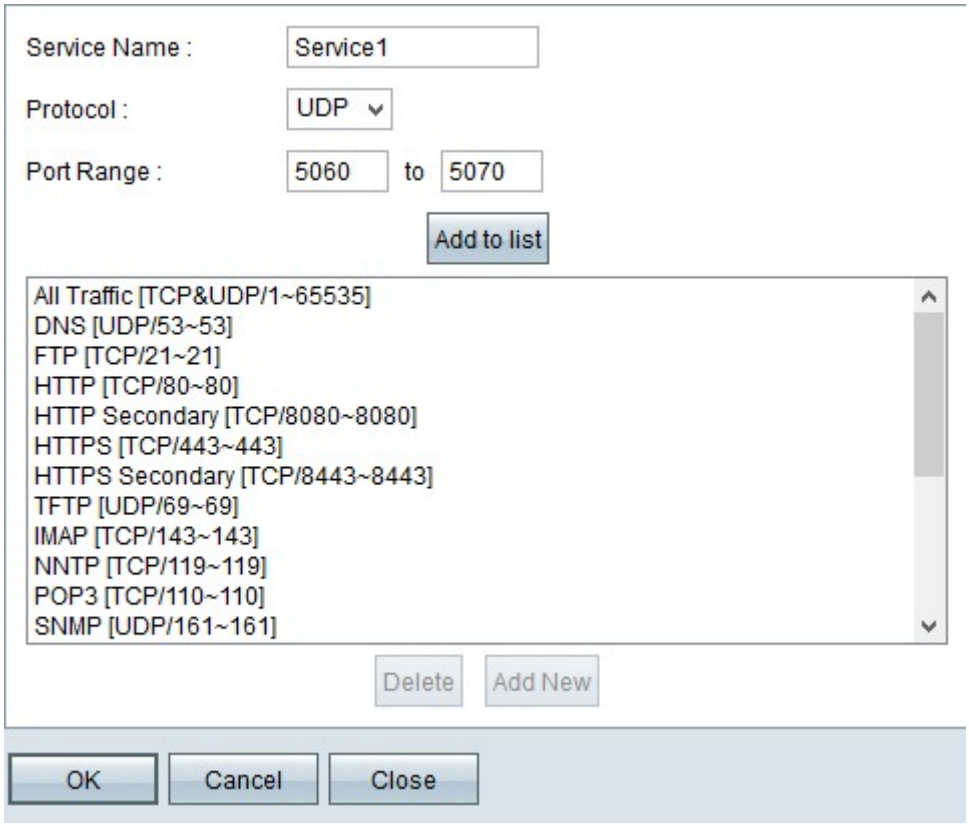


Schritt 8: Wählen Sie in der Dropdown-Liste Protocol (Protokoll) den entsprechenden Protokolltyp aus.

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

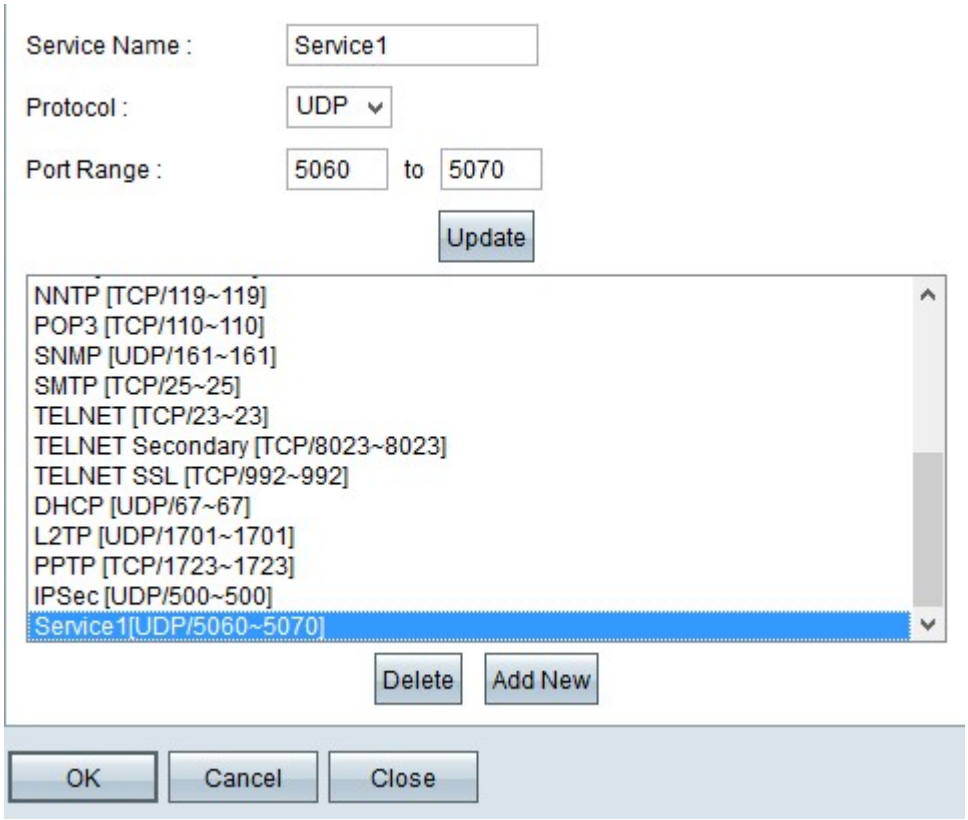
·UDP (User Datagram Protocol) - Verwendet Datagram-Sockets, um die Kommunikation zwischen Host und Host herzustellen. Die UDP-Bereitstellung ist nicht garantiert.

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



Schritt 9: Geben Sie den Port-Bereich im Feld Port Range (Port-Bereich) ein. Dieser Bereich hängt vom Protokoll ab, das im oben genannten Schritt ausgewählt wurde.

Schritt 10: Klicken Sie auf **Zur Liste hinzufügen**. Damit wird der Service der Dropdown-Liste Service hinzugefügt.

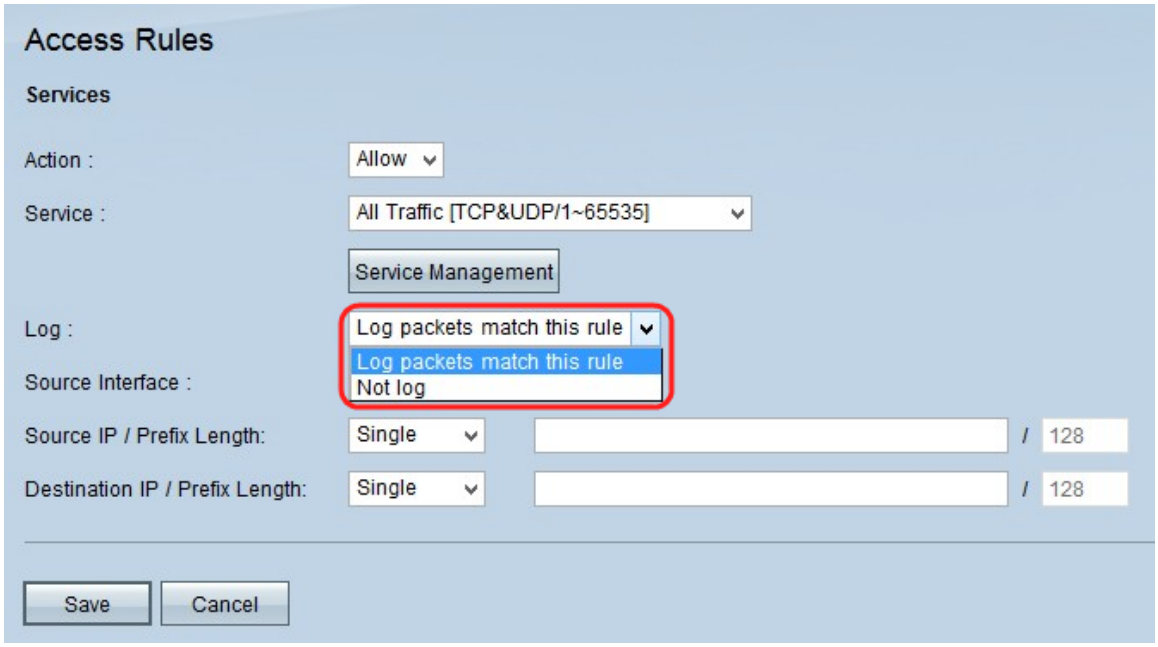


Hinweis: Wenn Sie einen Service aus der Liste der Dienste löschen möchten, wählen Sie den Service aus der Liste der Dienste aus, und klicken Sie dann auf **Löschen**. Wenn Sie den Serviceeintrag aktualisieren möchten, wählen Sie den zu aktualisierenden Service aus der

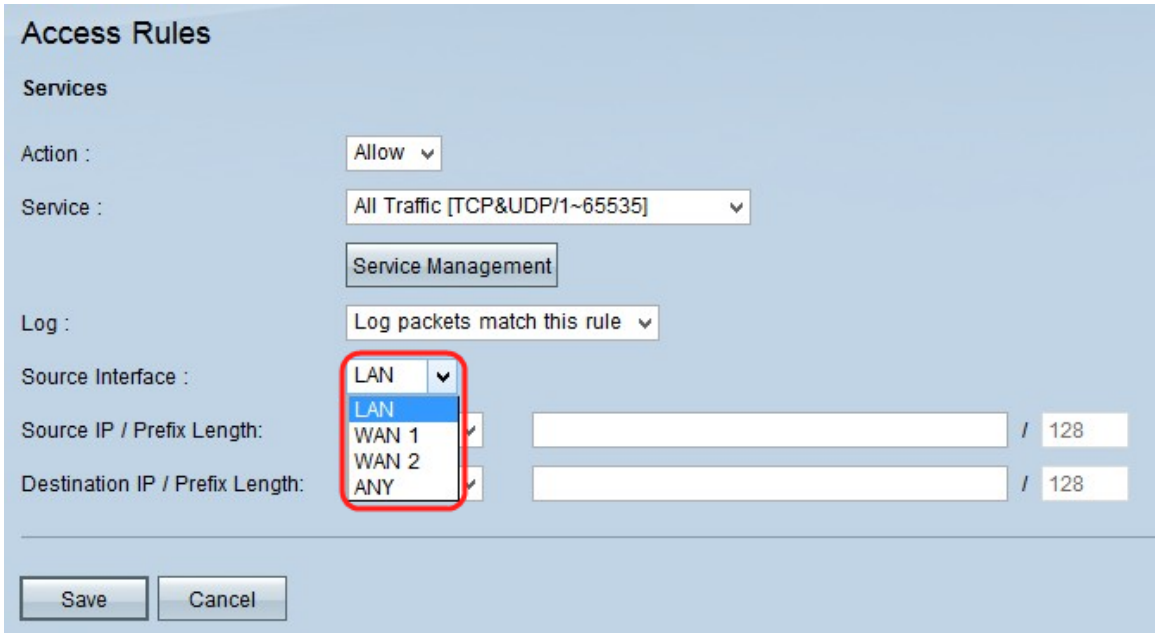
Liste aus, und klicken Sie dann auf **Aktualisieren**. Wenn Sie der Liste einen weiteren neuen Dienst hinzufügen möchten, klicken Sie auf **Neu hinzufügen**.

Schritt 11: Klicken Sie auf **OK**. Dadurch wird das Fenster geschlossen, und der Benutzer kehrt zur Seite *Zugriffsregel* zurück.

Hinweis: Wenn Sie auf **Neu hinzufügen** klicken, befolgen Sie die Schritte 7 bis 11.



Schritt 12: Wenn Sie Pakete, die der Zugriffsregel entsprechen, protokollieren möchten, wählen Sie **Protokollpakete aus, die dieser Regel** in der Dropdown-Liste Protokoll **entsprechen**. Andernfalls wählen Sie **Nicht protokollieren aus**.



Schritt 13: Wählen Sie aus der Dropdown-Liste Quellschnittstelle die Schnittstelle aus, die von dieser Regel betroffen ist. Die Quellschnittstelle ist die Schnittstelle, von der der Datenverkehr initiiert wird.

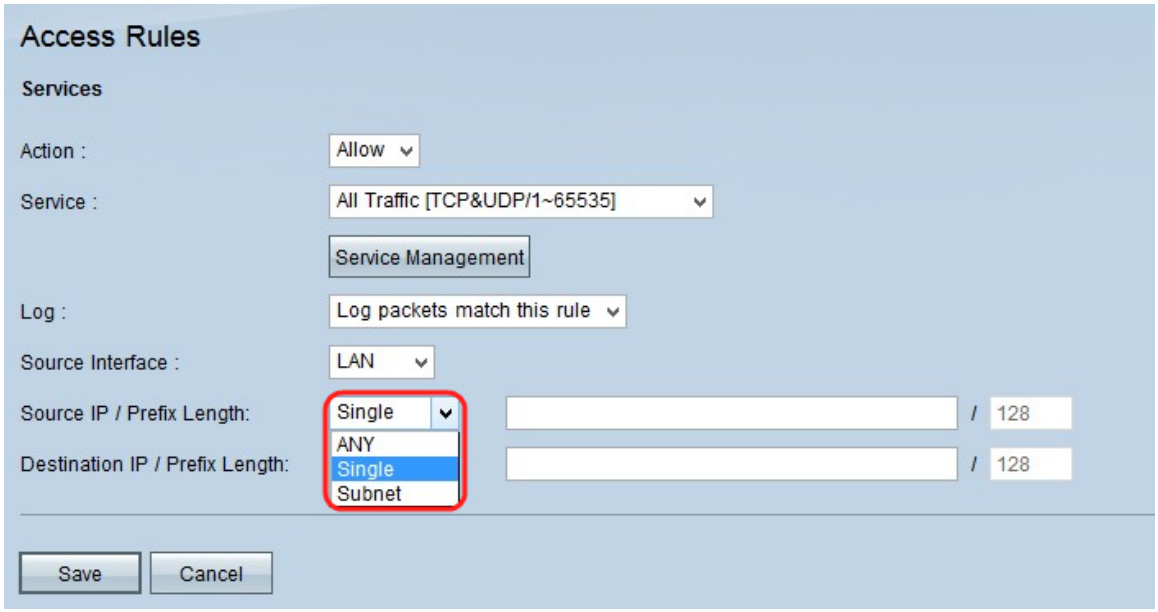
·LAN - Das lokale Netzwerk des Routers.

·WAN1 - Das Wide Area Network oder das Netzwerk, von dem aus der Router eine

Internetverbindung vom ISP oder dem nächsten Hop-Router erhält.

·WAN2 - dasselbe wie WAN1, jedoch ein sekundäres Netzwerk.

·ANY - Ermöglicht die Verwendung beliebiger Schnittstellen.

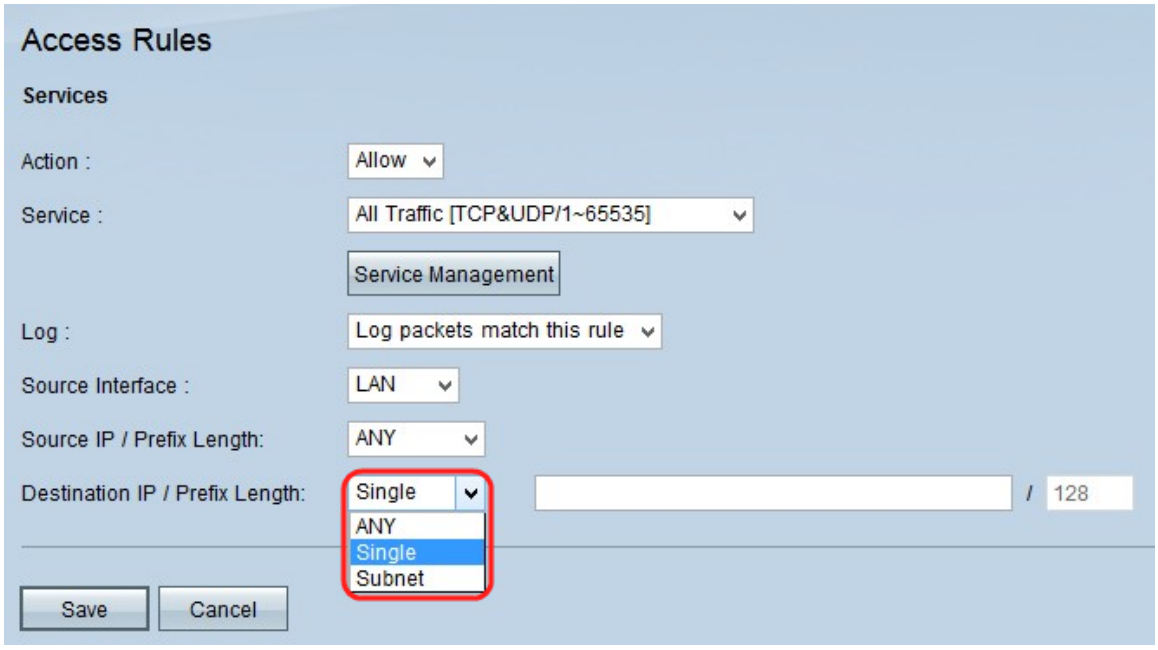


Schritt 14: Wählen Sie in der Dropdown-Liste Source IP (Quelle-IP) eine Option aus, um die Quell-IP-Adresse anzugeben, auf die die Zugriffsregel angewendet wird.

·Any (Beliebig): Zugriffsregeln werden auf den gesamten Datenverkehr von der Quellschnittstelle angewendet. Rechts neben der Dropdown-Liste sind keine Felder verfügbar.

·Single (Single): Die Zugriffsregel wird auf eine einzige IP-Adresse von der Quellschnittstelle angewendet. Geben Sie die gewünschte IP-Adresse in das Adressfeld ein.

·Subnetz - Zugriffsregel wird auf ein Subnetz-Netzwerk von der Quellschnittstelle angewendet. Geben Sie die IP-Adresse und die Präfixlänge ein.



Schritt 15: In der Dropdown-Liste Destination IP (Ziel-IP) Wählen Sie eine Option aus, um die Ziel-IP-Adresse anzugeben, auf die die Zugriffsregel angewendet wird.

·Any (Beliebig): Zugriffsregeln werden auf den gesamten Datenverkehr zur Zielschnittstelle angewendet. Rechts neben der Dropdown-Liste sind keine Felder verfügbar.

·Single (Einzel): Die Zugriffsregel wird auf eine einzige IP-Adresse für die Zielschnittstelle angewendet. Geben Sie die gewünschte IP-Adresse in das Adressfeld ein.

·Subnetz - Zugriffsregel wird auf ein Subnetz-Netzwerk zur Zielschnittstelle angewendet. Geben Sie die IP-Adresse und die Präfixlänge ein.

Schritt 16: Klicken Sie auf **Speichern**, um alle Änderungen der IPv6-Zugriffsregel zu speichern.

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.