

Konfiguration der Zugriffsregeln auf RV320- und RV325-VPN-Routern

Ziel

Zugriffskontrolllisten (Access Control Lists, ACLs) sind Listen, die das Senden von Datenverkehr an und von bestimmten Benutzern blockieren oder zulassen. Zugriffsregeln können so konfiguriert werden, dass sie jederzeit gültig sind oder auf einem definierten Zeitplan basieren. Eine Zugriffsregel wird auf der Grundlage verschiedener Kriterien konfiguriert, um den Zugriff auf das Netzwerk zuzulassen oder zu verweigern. Die Zugriffsregel wird basierend auf dem Zeitpunkt geplant, zu dem die Zugriffsregeln auf den Router angewendet werden müssen. Dieser Artikel beschreibt und beschreibt den Assistenten für die Einrichtung von Zugriffsregeln, der verwendet wird, um zu bestimmen, ob der Datenverkehr über die Firewall des Routers in das Netzwerk gelangen darf oder nicht, um die Sicherheit im Netzwerk zu gewährleisten.

Anwendbare Geräte | Firmware-Version

- RV320 Dual-WAN VPN-Router | V 1.1.0.09 ([aktueller Download](#))
- RV325 Dual-WAN-VPN-Router mit Gigabit | V 1.1.0.09 ([aktueller Download](#))

Zugriffsregelkonfiguration

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



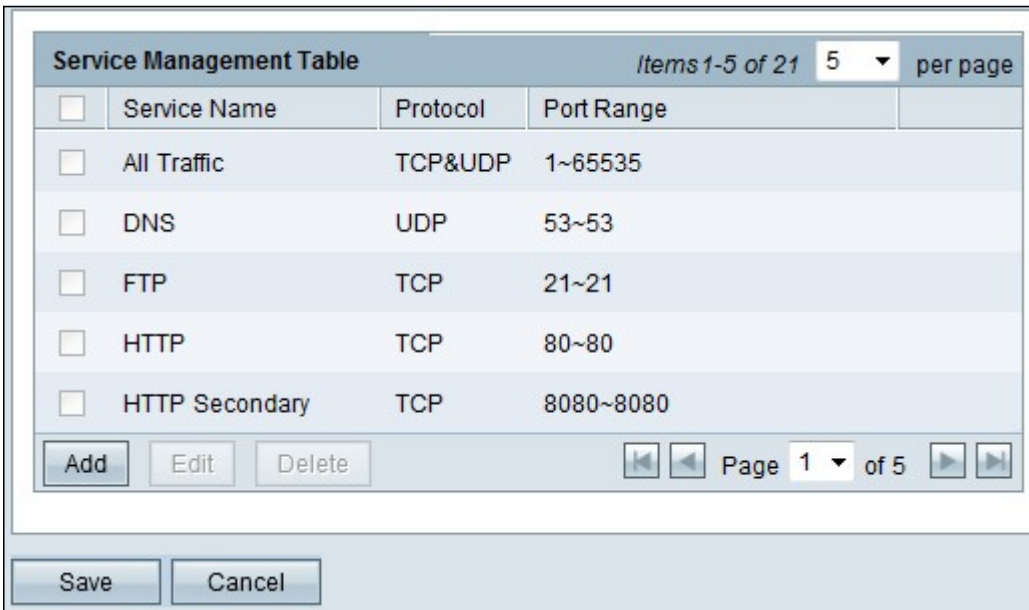
Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Die Tabelle mit Zugriffsregeln enthält die folgenden Informationen:

- Priority (Priorität) - Zeigt die Priorität der Zugriffsregel an
- Enable (Aktivieren) - Zeigt an, ob die Zugriffsregel aktiviert oder deaktiviert ist.
- Aktion - Zeigt an, dass die Zugriffsregel zugelassen oder verweigert ist.
- Service - Zeigt den Typ des Service an.
- SourceInterface - Zeigt an, auf welche Schnittstelle die Zugriffsregel angewendet wird.
- Quelle - Zeigt die IP-Adresse des Quellgeräts an
- Ziel - Zeigt die IP-Adresse des Zielgeräts an.
- Zeit - Zeigt an, wann die Zugriffsregel angewendet werden soll.
- Tag - Zeigt während einer Woche an, in der die Zugriffsregel angewendet wird

Service-Management

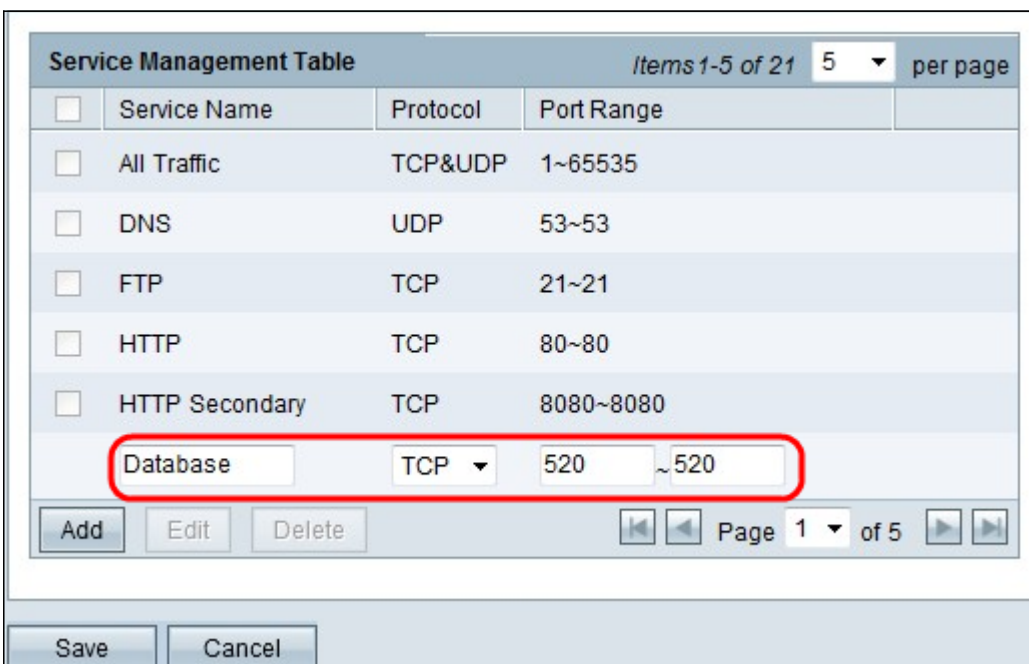
Schritt 1: Klicken Sie auf **Service Management**, um einen neuen Service hinzuzufügen. Die Seite *Service Management Table (Service-Management-Tabelle)* wird geöffnet:



The screenshot shows the 'Service Management Table' interface. At the top, it displays 'Items 1-5 of 21' and '5 per page'. Below this is a table with the following columns: Service Name, Protocol, and Port Range. The table contains five rows of services: All Traffic (TCP&UDP, 1~65535), DNS (UDP, 53~53), FTP (TCP, 21~21), HTTP (TCP, 80~80), and HTTP Secondary (TCP, 8080~8080). Each row has a checkbox to its left. Below the table are three buttons: 'Add', 'Edit', and 'Delete'. At the bottom of the interface are 'Save' and 'Cancel' buttons.

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080

Schritt 2: Klicken Sie auf **Hinzufügen**, um einen neuen Service hinzuzufügen.



The screenshot shows the 'Service Management Table' interface with a new service entry 'Database' highlighted in red. The entry is located in the table below the existing services. The 'Database' entry has a checkbox, the name 'Database', the protocol 'TCP', and the port range '520 ~520'. The 'Add' button is now disabled.

<input type="checkbox"/>	Service Name	Protocol	Port Range
<input type="checkbox"/>	All Traffic	TCP&UDP	1~65535
<input type="checkbox"/>	DNS	UDP	53~53
<input type="checkbox"/>	FTP	TCP	21~21
<input type="checkbox"/>	HTTP	TCP	80~80
<input type="checkbox"/>	HTTP Secondary	TCP	8080~8080
<input type="checkbox"/>	Database	TCP	520 ~520

Schritt 3: Konfigurieren Sie die folgenden Felder.

- Servicenamen - Geben Sie je nach Anforderung einen Namen für den Service an.
- Protokoll - Wählen Sie ein TCP- oder UDP-Protokoll für Ihren Dienst aus.
- Port Range (Port-Bereich) - Geben Sie den Port-Nummernbereich entsprechend Ihrer Anforderungen ein, und die Port-Nummer muss im Bereich (1-65536) liegen.

Schritt 4: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Zugriffsregelkonfiguration auf IPv4

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 5 5 per page

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management...

Page 1 of 1

Schritt 1: Klicken Sie auf **Hinzufügen**, um eine neue Zugriffsregel zu konfigurieren. Das Fenster *Zugriffsregeln bearbeiten* wird angezeigt.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Schritt 2: Wählen Sie in der Dropdown-Liste Aktion die entsprechende Option aus, um den Datenverkehr für die zu erstellende Regel zuzulassen oder zu beschränken. Zugriffsregeln beschränken den Zugriff auf das Netzwerk auf der Grundlage verschiedener Werte.

- Zulassen: Lässt den gesamten Datenverkehr zu.
- Verweigern - Schränkt den gesamten Datenverkehr ein.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From:

To:

Effective on: Mon Tue Wed Thu Fri Sat

Schritt 3: Wählen Sie den gewünschten Service aus der Dropdown-Liste Service aus, der gefiltert werden soll.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Schritt 4: Wählen Sie in der Dropdown-Liste Protokoll die entsprechende Option aus. Die Protokolloption bestimmt, ob das Gerät ein Protokoll des Datenverkehrs speichert, das den festgelegten Zugriffsregeln entspricht.

- Protokollieren von Paketen, die dieser Zugriffsregel entsprechen - Der Router speichert ein Protokoll, das den ausgewählten Service verfolgt.
- Not Log (Nicht protokollieren): Der Router speichert keine Protokolle für die Zugriffsregel.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Schritt 5: Wählen Sie in der Dropdown-Liste Interface (Schnittstelle) die entsprechende Quellschnittstelle aus. An dieser Schnittstelle wird die Zugriffsregel erzwungen.

- LAN - Die Zugriffsregel betrifft nur den LAN-Datenverkehr.
- WAN 1: Die Zugriffsregel betrifft nur den WAN 1-Datenverkehr.
- WAN 2 - Die Zugriffsregel betrifft nur den WAN-2-Datenverkehr.
- Any (Beliebig): Die Zugriffsregel betrifft den gesamten Datenverkehr an einer der Schnittstellen des Geräts.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Schritt 6: Wählen Sie in der Dropdown-Liste Source IP (Quelle-IP) den entsprechenden IP-Quellentyp aus, auf den die Zugriffsregel angewendet wird.

- Any (Beliebig): Jede IP-Adresse des Netzwerks des Geräts hat die Regel auf sie angewendet.
- Single (Einzel): Nur eine einzige angegebene IP-Adresse im Netzwerk des Geräts hat die Regel auf sie angewendet. Geben Sie die gewünschte IP-Adresse in das angrenzende Feld ein.
- Bereich - Nur ein bestimmter Bereich von IP-Adressen im Netzwerk des Geräts wird mit der Regel verknüpft. Wenn Sie Range (Bereich) auswählen, müssen Sie die erste und die letzte IP-Adresse für den Bereich in den angrenzenden Feldern eingeben.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP: To

Destination IP:

- ANY
- Single
- Range

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu

Schritt 7: Wählen Sie aus der Dropdown-Liste den geeigneten Ziel-IP-Typ aus, auf den die Zugriffsregel angewendet wird.

- Any (Beliebig): Bei jeder Ziel-IP-Adresse wird die Regel auf sie angewendet.
- Single (Einzel): Nur eine einzige angegebene IP-Adresse hat die Regel auf sie angewendet. Geben Sie die gewünschte IP-Adresse in das angrenzende Feld ein.
- Bereich - Nur ein bestimmter Bereich von IP-Adressen außerhalb des Netzwerks des Geräts wird mit der Regel verknüpft. Wenn Sie Range (Bereich) auswählen, müssen Sie die erste und die letzte IP-Adresse für den Bereich in den angrenzenden Feldern eingeben.

Scheduling

Time:

- Always
- Interval

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Zeitschoner: Standardmäßig ist die Zeit auf Always eingestellt. Wenn Sie die Zugriffsregel auf einen bestimmten Zeitpunkt oder Tag anwenden möchten, befolgen Sie Schritt 8 bis Schritt 11.

Falls nicht, fahren Sie mit Schritt 12 fort.

Schritt 8: Wählen Sie **Interval** aus der Dropdown-Liste aus, Zugriffsregeln sind für bestimmte Zeiten aktiv. Sie müssen das Zeitintervall eingeben, damit die Zugriffsregel erzwungen werden kann.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Schritt 9: Geben Sie den Zeitpunkt ein, zu dem die Zugriffsliste im Feld Von angewendet werden soll. Das Zeitformat ist hh:mm.

Schritt 10: Geben Sie den Zeitpunkt ein, zu dem die Zugriffsliste im Feld "An" nicht mehr angewendet werden soll. Das Zeitformat ist hh:mm.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Schritt 11: Aktivieren Sie das Kontrollkästchen der bestimmten Tage, an denen die Zugriffsliste angewendet werden soll.

Schritt 12: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 6 5 ▾

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input checked="" type="radio"/>	1 ▾	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100	Any	03:00 ~ 07:00	All week
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management...

Page 1 of 2

Schritt 13: (Optional) Wenn Sie die Standardregeln wiederherstellen möchten, klicken Sie auf

Wiederherstellen auf Standardregeln. Alle von Ihnen konfigurierten Zugriffsregeln gehen verloren.

Zugriffsregelkonfiguration auf IPv6

The screenshot shows the 'Access Rules' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6'. The 'IPv6' tab is selected and highlighted with a red circle. Below the tabs is a table titled 'Access Rules Table' with columns: Priority, Enable, Action, Service, SourceInterface, Source, Destination, Time, and Day. The table contains five rows of default rules. At the bottom, there are buttons for 'Add', 'Edit', 'Delete', 'Restore to Default Rules', and 'Service Management...'. The 'Add' button is highlighted with a red circle.

Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Schritt 1: Klicken Sie auf die Registerkarte IPv6, um IPv6-Zugriffsregeln zu konfigurieren.

This screenshot is identical to the previous one, showing the 'Access Rules' configuration page with the 'IPv6' tab selected. The 'Add' button at the bottom left is highlighted with a red circle.

Schritt 2: Klicken Sie auf Hinzufügen, um eine neue IPv6-Zugriffsregel hinzuzufügen. Das Fenster *Zugriffsregeln bearbeiten* wird angezeigt.

The screenshot shows the 'Edit Access Rules' dialog box. It has several fields with dropdown menus: 'Action' (set to 'Allow'), 'Service' (set to '[TCP&UDP/1~65535]'), 'Log' (set to 'No Log'), 'Source Interface' (set to 'LAN'), 'Source IP / Prefix Length' (set to 'ANY'), and 'Destination IP / Prefix Length' (set to 'ANY'). The 'Action' dropdown menu is open, and the 'Allow' option is highlighted with a red circle. At the bottom, there are three buttons: 'Save', 'Cancel', and 'Back'.

Schritt 3: Wählen Sie in der Dropdown-Liste Aktion die entsprechende Option aus, um die einrichtende Regel zuzulassen oder einzuschränken. Zugriffsregeln beschränken den Zugriff auf das Netzwerk, indem sie den Datenverkehr bestimmter Services oder Geräte zulassen oder verweigern.

- Zulassen: Lässt den gesamten Datenverkehr zu.
- Verweigern - Schränkt den gesamten Datenverkehr ein.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Save Cancel

All Traffic [TCP&UDP/1~65535]
 DNS [UDP/53~53]
 FTP [TCP/21~21]
 HTTP [TCP/80~80]
 HTTP Secondary [TCP/8080~8080]
 HTTPS [TCP/443~443]
 HTTPS Secondary [TCP/8443~8443]
 TFTP [UDP/69~69]
 IMAP [TCP/143~143]
 NNTP [TCP/119~119]
 POP3 [TCP/110~110]
 SNMP [UDP/161~161]
 SMTP [TCP/25~25]
 TELNET [TCP/23~23]
 TELNET Secondary [TCP/8023~8023]
 TELNET SSL [TCP/992~992]
 DHCP [UDP/67~67]
 L2TP [UDP/1701~1701]
 PPTP [TCP/1723~1723]
 IPsec [UDP/500~500]
 Ping [ICMP/255~255]
 data [TCP/520~521]

Schritt 4: Wählen Sie den gewünschten Service aus der Dropdown-Liste Service aus, der gefiltert werden soll.

Hinweis: Um den gesamten Datenverkehr zuzulassen, wählen Sie in der Dropdown-Liste "Service" die Option **All Traffic [TCP&UDP/1~65535]** aus. Die Liste enthält alle Arten von Diensten, die Sie filtern möchten.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface:

Source IP / Prefix Length: ANY ▾

Destination IP / Prefix Length: ANY ▾

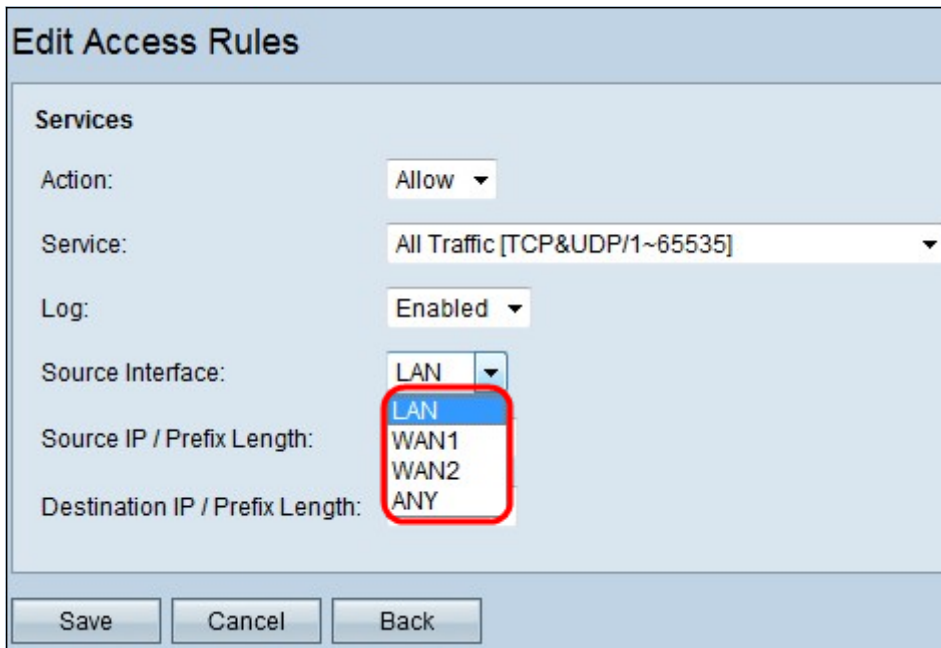
Save Cancel Back

No Log
 Enabled

Schritt 5: Wählen Sie in der Dropdown-Liste Protokoll die entsprechende Option aus. Die

Protokolloption legt fest, ob das Gerät ein Protokoll des Datenverkehrs speichert, das den festgelegten Zugriffsregeln entspricht.

- Enabled (Aktiviert): Ermöglicht dem Router, die Protokollierung für den ausgewählten Service beizubehalten.
- Not Log (Nicht protokollieren): Deaktiviert den Router, um die Protokollierung beizubehalten.



Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length: LAN

Destination IP / Prefix Length: ANY

Save Cancel Back

Schritt 6: Klicken Sie auf die Dropdown-Liste Interface (Schnittstelle), und wählen Sie die entsprechende Quellschnittstelle aus. An dieser Schnittstelle wird die Zugriffsregel erzwungen.

- LAN - Die Zugriffsregel betrifft nur den LAN-Datenverkehr.
- WAN 1: Die Zugriffsregel betrifft nur den WAN 1-Datenverkehr.
- WAN 2 - Die Zugriffsregel betrifft nur den WAN-2-Datenverkehr.
- Any (Beliebig): Die Zugriffsregel betrifft den gesamten Datenverkehr an einer der Schnittstellen des Geräts.



Edit Access Rules

Services

Action: Allow

Service: All Traffic [TCP&UDP/1~65535]

Log: Enabled

Source Interface: LAN

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

Schritt 7: Wählen Sie in der Dropdown-Liste Source IP/Prefix Length den entsprechenden IP-

Quellentyp aus, auf den die Zugriffsregel angewendet wird.

- BELIEBIGE - Für alle Pakete, die von einem Netzwerk des Geräts empfangen werden, wird die Regel auf sie angewendet.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Single ▾ 2607:f0d0:1002:51::4 / 128

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Single (Einzel): Nur eine einzige angegebene IP-Adresse im Netzwerk des Geräts hat die Regel auf sie angewendet. Geben Sie die gewünschte IPv6-Adresse in das angrenzende Feld ein.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Subnetz - Nur die IP-Adressen eines Subnetzes haben die Regel darauf angewendet. Geben Sie die IPv6-Netzwerkadresse und die Präfixlänge des gewünschten Subnetzes in den angrenzenden Feldern ein.

Edit Access Rules

Services

Action: Allow ▾

Service: All Traffic [TCP&UDP/1~65535] ▾

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

- ANY
- Single
- Subnet

Save Cancel Back

Schritt 8: Wählen Sie in der Dropdown-Liste Destination IP/Prefix Length den geeigneten Ziel-IP-Typ aus, auf den die Zugriffsregel angewendet wird.

- Any (Beliebig): Bei jeder Ziel-IP-Adresse wird die Regel auf sie angewendet.
- Single (Einzel): Nur eine einzige angegebene IP-Adresse im Netzwerk des Geräts hat die Regel auf sie angewendet. Geben Sie die gewünschte IPv6-Adresse ein.
- Subnetz - Nur die IP-Adressen eines Subnetzes haben die Regel darauf angewendet. Geben Sie die IPv6-Netzwerkadresse und die Präfixlänge des gewünschten Subnetzes in den angrenzenden Feldern ein.

Schritt 9: Klicken Sie auf **Speichern**, damit die Änderungen wirksam werden.

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)