

Access Rule Setup-Assistent für RV32x VPN-Router

Ziel

Der Setup-Assistent für Zugriffsregeln ist eine praktische und einfache Anleitung zum Einrichten der Erstkonfigurationen auf dem RV32x-Router. Der Benutzer wird schrittweise durch die Konfiguration des Geräts geführt. 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, mit dem bestimmt wird, welcher Datenverkehr über die Firewall in das Netzwerk gelangen darf und so zum Schutz des Netzwerks beiträgt.

Anwendbares Gerät

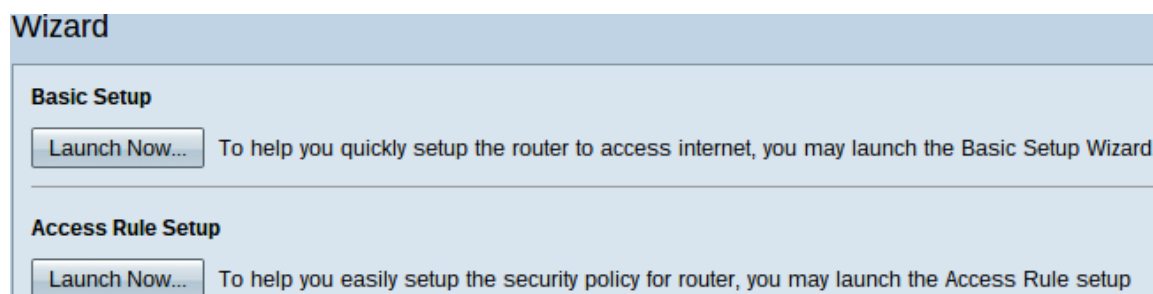
- RV320 Dual-WAN VPN-Router
- RV325 Gigabit Dual-WAN VPN-Router

Softwareversion

- v1.1.0.09

Assistent zum Einrichten von Zugriffsregeln

Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **Assistent aus**. Die Seite *Assistent* wird geöffnet:



Schritt 2: Klicken Sie auf die Schaltfläche **Jetzt starten** unterhalb des Bereichs Zugriffsregeleinrichtung, um den Assistenten für die Einrichtung von Zugriffsregeln zu starten. Das Dialogfeld *Installationsassistent für Zugriffsregeln* wird angezeigt.

Welcome to the Access Rules Installation Wizard


Network Access Rules evaluate network traffic's Source IP address, Destination IP address, and IP protocol type to decide if the IP traffic is allowed to pass through the firewall. Custom rules take precedence, and may override these rules. RV320's default stateful packet inspection.

The ability to define Network Access Rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block access to the Internet. Use extreme caution when creating or deleting Network Access Rules.

RV320 has the following default rules:

- All traffic from the LAN to the WAN is allowed.
- All traffic from the WAN to the LAN is denied.
- All traffic from the LAN to the DMZ is allowed.
- All traffic from the DMZ to the LAN is denied.
- All traffic from the WAN to the DMZ is allowed.
- All traffic from the DMZ to the WAN is allowed.

Custom rules can be created to override the RV320 default rules.



Back Next Cancel

Schritt 3: Klicken Sie auf **Weiter**, um mit dem Assistenten fortzufahren.

Aktion

Action Select the Action.

Service Select **Allow** or **Deny** depending on the intent of the rule. For example, to configure the router to allow all FTP traffic access to the Internet from the LAN, select Allow. Or, to restrict all FTP traffic access Internet from the LAN, select Deny.

Log

Source Interface

Source IP Action:

Destination IP

Schedule

Summary

Finish

Back Next Cancel

Schritt 1: Wählen Sie in der Dropdown-Liste Aktion das entsprechende Optionsfeld aus, um die zu erstellende Regel zuzulassen oder einzuschränken. Zugriffsregeln beschränken den Zugriff auf das Subnetzwerk, indem sie den Datenverkehr bestimmter Services oder Geräte

zulassen oder verweigern.

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

Schritt 2: Klicken Sie auf **Weiter**, um mit dem Assistenten fortzufahren.

Service

✓ Action	Select the Service.
Service	Select the service that will be allowed or denied from the Service menu.
Log	
Source Interface	Service: <input type="text" value="POP3 [TCP/110~110]"/>
Source IP	
Destination IP	
Schedule	
Summary	
Finish	

<input type="button" value="Back"/>	<input type="button" value="Next"/>	<input type="button" value="Cancel"/>
-------------------------------------	-------------------------------------	---------------------------------------

Schritt 1: Wählen Sie in der Dropdown-Liste Service den entsprechenden Service aus, den Sie filtern müssen, um zugelassen oder eingeschränkt zu werden.

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

Schritt 2: Klicken Sie auf **Weiter**, um mit der Einrichtung fortzufahren.

Protokoll

✓ Action

✓ Service

Log

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Select the Log.

You can select **Log packets matching this rule** or **Not log**.

Log:

Back

Next

Cancel

Schritt 1: 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.

·Protokollpakete stimmen mit dieser Zugriffsregel überein - Ermöglicht es dem Router, die Protokollierung für den ausgewählten Dienst beizubehalten.

·Not Log (Nicht protokollieren): Deaktiviert den Router, um die Protokollierung beizubehalten.

Schritt 2: Klicken Sie auf **Weiter**, um mit der Einrichtung fortzufahren.

Quellschnittstelle

✓ Action	Select the Source Interface.
✓ Service	Select the source, either WAN, LAN, DMZ or Any from the Source Interface menu. For example, to allow all FTP traffic to access the Internet from the LAN, select the LAN as source.
✓ Log	
Source Interface	Interface: <input type="text" value="WAN 2"/>
Source IP	
Destination IP	
Schedule	
Summary	
Finish	

Schritt 1: 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.

Schritt 2: Klicken Sie auf **Weiter**, um mit der Einrichtung fortzufahren.

Quell-IP

Action Select the Source IP type and enter the IP address.

Service For example, to allow all users on LAN side to access the Internet, select Any. To allow certain users on LAN side to access the Internet, select Single or Range and enter the IP address.

Log

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Schritt 1: Wählen Sie aus der Dropdown-Liste 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.

Select the Source IP type and enter the IP address.

For example, to allow all users on LAN side to access the Internet, select Any. To allow certain users on LAN side to access the Internet, select Single or Range and enter the IP address.

·Single (Einzel): Nur eine einzige angegebene IP-Adresse des Netzwerks des Geräts hat die Regel auf das Gerät angewendet. Geben Sie die gewünschte IP-Adresse ein.

Select the Source IP type and enter the IP address.

For example, to allow all users on LAN side to access the Internet, select Any. To allow certain users on LAN side to access the Internet, select Single or Range and enter the IP address.

To

·Bereich - Nur ein bestimmter Bereich von IP-Adressen im Netzwerk hat die Regel auf sie angewendet. Wenn Sie Range (Bereich) auswählen, müssen Sie die Start- und End-IP-Adressen für den Bereich eingeben.

Schritt 2: Klicken Sie auf **Weiter**, um mit der Einrichtung fortzufahren.

Ziel-IP

Action Select the Destination IP type and enter the IP address.

Service Select the destination, either Any, Single or Range * from the Destination IP pull-down menu.

Log For example, to allow access to the DMZ port from the Internet, select Single or Range and enter the IP address of DMZ port.

Source Interface

Source IP

Destination IP

Schritt 1: Wählen Sie aus der Dropdown-Liste den geeigneten Ziel-IP-Typ aus, auf den die Zugriffsregel angewendet wird.

·Any (Beliebig): Für jede Ziel-IP-Adresse wird die Regel angewendet.

Select the Destination IP type and enter the IP address.

Select the destination, either Any, Single or Range * from the Destination IP pull-down menu. For example, to allow access to the DMZ port from the Internet, select Single or Range and enter the IP address of DMZ port.

·Single (Einzel): Nur eine angegebene IP-Adresse, auf die die Regel angewendet wurde. Geben Sie die gewünschte IP-Adresse ein.

Select the Destination IP type and enter the IP address.

Select the destination, either Any, Single or Range * from the Destination IP pull-down menu. For example, to allow access to the DMZ port from the Internet, select Range and enter the IP address of DMZ port.

To

·Bereich - Nur ein bestimmter Bereich von IP-Adressen, der aus dem Netzwerk des Geräts ausgeht, wird von der Regel abgedeckt. Wenn Sie Range (Bereich) auswählen, müssen Sie die Start- und End-IP-Adressen für den Bereich eingeben.

Schritt 2: Klicken Sie auf **Weiter**, um mit der Einrichtung fortzufahren.

Zeitplan

- ✓ Action
- ✓ Service
- ✓ Log
- ✓ Source Interface
- ✓ Source IP
- ✓ Destination IP

Schedule

Summary

Finish

When it works

Select the scheduling for this rule to be enforced.

- Always :**
Select **Always** from the Apply this rule menu if the rule is always in effect.
- Interval :**
Select **Interval** to define the specific time and day of week range for this rule to be enforced.

Back

Next

Cancel

Schritt 1: Klicken Sie auf das entsprechende Optionsfeld, um die Uhrzeit auszuwählen, zu der die Zugriffsregel auf den Router angewendet werden soll.

·Immer - Zugriffsregeln sind immer auf dem Router aktiv. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 5 fort. Dies ist die Standardeinstellung.

·Intervall - Zugriffsregeln sind für bestimmte Zeiten aktiv. Wenn Sie diese Option wählen, müssen Sie das Zeitintervall eingeben, damit die Zugriffsregel erzwungen werden kann.

✓ Action Enter the Scheduling

✓ Service

✓ Log

✓ Source Interface

✓ Source IP

✓ Destination IP

Schedule

Summary

Finish

Time Setting

Enter the time of day (in 24-hour format) to begin and end enforcement.

From: (hh:mm)

To: (hh:mm)

Date Setting

Enter the day of week to begin and end enforcement.

Everyday Sun Mon Tue Wed Thu Fri Sat

Schritt 2: Geben Sie die Uhrzeit ein, ab der die Zugriffsliste im Feld Von angewendet werden soll. Das Zeitformat ist **hh:mm**.

Schritt 3: Geben Sie die Zeit ein, bis die Zugriffsliste im Feld "An" angewendet werden soll. Das Zeitformat ist hh:mm.

Schritt 4: Aktivieren Sie das Kontrollkästchen der bestimmten Tage, an denen die Zugriffsliste angewendet werden soll.

Schritt 5: Klicken Sie auf **Weiter**, um mit der Einrichtung fortzufahren.

Zusammenfassung

✓ Action	Summary
✓ Service	Please review the following settings and ensure the data is correct.
✓ Log	Action: Deny
✓ Source Interface	Service: All Traffic [TCP&UDP/1~65535]
✓ Source IP	Log: Not log
✓ Destination IP	Source Interface: WAN 2
✓ Schedule	Source IP: 192.0.2.4
Summary	Destination IP: Any
Finish	Schedule : From 04:30 To 17:14 , Sun , Tue

Hinweis: Die Seite *Zusammenfassung* zeigt eine Gesamtansicht aller Einstellungen an, die gerade vom Access Setup Wizard (Zugriffseinrichtung-Assistent) auf dem RV320 konfiguriert wurden.

Schritt 1: Klicken Sie auf **Senden**, um Ihre Änderungen an der Assistentenkonfiguration zu senden.

Beenden

Device Setup Complete

Access Rules have been successfully configured.

- ✓ Action
- ✓ Service
- ✓ Log
- ✓ Source Interface
- ✓ Source IP
- ✓ Destination IP
- ✓ Schedule
- ✓ Summary

Finish

Cancel Finish

Schritt 1: Klicken Sie auf **Fertig stellen**, um den Assistenten zur Einrichtung von Zugriffsregeln abzuschließen.