Konfigurieren von Zugriffsregeln auf einem Router der Serie RV34x

Ziel

Der RV340 Dual-WAN VPN-Router ist ein benutzerfreundliches, flexibles und leistungsstarkes Gerät, das sich hervorragend für kleine und mittlere Unternehmen eignet. Mit zusätzlichen Sicherheitsfunktionen wie Webfilterung, Anwendungskontrolle und IP Source Guard. Die neue RV340 bietet sichere kabelgebundene Breitbandverbindungen für kleine Büros und Remote-Mitarbeiter. Diese neuen Sicherheitsfunktionen erleichtern zudem die Feinabstimmung der zulässigen Aktivitäten im Netzwerk.

Zugriffsregeln oder Richtlinien auf dem Router der Serie RV34x ermöglichen die Konfiguration von Regeln zur Erhöhung der Sicherheit im Netzwerk. Eine Kombination von Regeln und eine Zugriffssteuerungsliste (ACL). 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 definierten Zeitplänen basieren.

ACLs verfügen am Ende der Liste über eine implizite Verweigerung. Wenn Sie diese also nicht explizit zulassen, kann der Datenverkehr nicht weitergeleitet werden. Wenn Sie z. B. allen Benutzern den Zugriff auf ein Netzwerk über den Router gestatten möchten, mit Ausnahme bestimmter Adressen, dann müssen Sie die jeweiligen Adressen verweigern und dann alle anderen zulassen.

In diesem Artikel erfahren Sie, wie Sie Zugriffsregeln auf einem Router der Serie RV34x konfigurieren.

Anwendbare Geräte

• Serie RV34x

Softwareversion

- 1,0/1,16
 - <u>Seit der Veröffentlichung dieses Artikels ist eine Firmware-Aktualisierung der</u> <u>Benutzeroberfläche verfügbar. Klicken Sie hier, um zur Download-Seite zu gelangen, und</u> <u>suchen Sie dort Ihr Produkt.</u>

Konfigurieren einer Zugriffsregel für einen Router der Serie RV34x

Erstellen einer Zugriffsregel

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Firewall > Access Rules aus**.



Schritt 2: Klicken Sie in der Tabelle mit den IPv4- oder IPv6-Zugriffsregeln auf **Hinzufügen**, um eine neue Regel zu erstellen.

Hinweis: Auf dem Router der Serie RV34x können bis zu 202 Regeln konfiguriert werden. In diesem Beispiel wird IPv4 verwendet.

A	cce	ess Rule	es		
	IPv	4 Access I	Rules Tab	ole	
		Priority	Enable	Action	Service
		201	\checkmark	Allowed	IPv4: All Traffic
		202	\checkmark	Denied	IPv4: All Traffic
		Add	E	dit	Delete

Schritt 3: Aktivieren Sie das Kontrollkästchen **Regelstatus aktivieren**, um die Regel zu aktivieren.



Schritt 4: Wählen Sie im Dropdown-Menü Aktion aus, ob die Richtlinie Daten zulassen oder ablehnen soll.

Hinweis: In diesem Beispiel wird Allow ausgewählt.



Schritt 5: Wählen Sie im Dropdown-Menü Services (Dienste) die Art des Datenverkehrs aus, der vom Router zugelassen oder abgelehnt wird.

Hinweis: In diesem Beispiel wird der gesamte Datenverkehr ausgewählt. Der gesamte Datenverkehr wird zugelassen.

Services:	IPv4 IPv	✓ All Traffic
Log:	True 🖨	BGP DNS-TCP
Source Interface:	WAN1 \$	DNS-UDP ESP
· · · ·		CTD .

Schritt 6: Wählen Sie im Dropdown-Menü Log (Protokoll) eine Option aus, um zu bestimmen, ob der Router den zulässigen oder abgelehnten Datenverkehr protokolliert. Folgende Optionen stehen zur Verfügung:

- Niemals Der Router protokolliert niemals Datenverkehr, der zugelassen und abgelehnt wurde.
- True Der Router protokolliert den Datenverkehr, der der Richtlinie entspricht.

Hinweis: In diesem Beispiel wird Nie ausgewählt.

Log:	✓ Never	
Source Interface:	True	-

Schritt 7: Wählen Sie im Dropdown-Menü Source Interface (Quellschnittstelle) eine Schnittstelle für den eingehenden oder eingehenden Datenverkehr aus, auf die die Zugriffsrichtlinie angewendet werden soll. Folgende Optionen sind verfügbar:

- WAN1 Die Richtlinie gilt nur für den Datenverkehr von WAN1.
- WAN2 Die Richtlinie gilt nur für den Datenverkehr von WAN2.
- USB1: Die Richtlinie gilt nur für den Datenverkehr von USB1.
- USB2: Die Richtlinie gilt nur für den Datenverkehr von USB2.
- VLAN1 Die Richtlinie gilt nur für das Verkehrs-VLAN1.
- Any (Beliebig): Die Richtlinie gilt für jede Schnittstelle.

Hinweis: Wenn ein zusätzliches VLAN (Virtual Local Area Network) konfiguriert wurde, wird die VLAN-Option in der Liste angezeigt. In diesem Beispiel wird WAN1 ausgewählt.

Source Interface:	✓ WAN1	÷
Ocurre Address	WAN2	5
Source Address:	USB1	₽
Destination Interface:	USB2	
	VLAN1	P
Destination Address:	Any	\$

Schritt 8: Wählen Sie im Dropdown-Menü Quelladresse eine Quelle aus, um die Richtlinie anzuwenden. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Die Richtlinie gilt für alle IP-Adressen im Netzwerk. Wenn Sie diese Option auswählen, fahren Sie mit <u>Schritt 12 fort</u>.
- Single IP (Einzelne IP): Die Richtlinie gilt für einen einzelnen Host oder eine einzelne IP-Adresse. Wenn Sie diese Option auswählen, fahren Sie mit <u>Schritt 9 fort</u>.
- IP Range (IP-Bereich): Die Richtlinie gilt für einen Satz oder Bereich von IP-Adressen. Wenn Sie diese Option auswählen, fahren Sie mit <u>Schritt 10 fort</u>.
- Subnetz Die Richtlinie gilt für ein gesamtes Subnetz. Wenn Sie diese Option auswählen, fahren Sie mit <u>Schritt 11 fort</u>.

Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

Source Address:	✔ Any	ŧ
Destination Interface:	Single IP IP Range	Ð
Destination Address:	Subnet	•

<u>Schritt 9:</u> (Optional) In Schritt 8 wurde eine einzelne IP ausgewählt. Geben Sie eine einzelne IP-Adresse für die Richtlinie ein, und fahren Sie dann mit <u>Schritt 12</u> fort.

Hinweis: In diesem Beispiel wird 200.200.22.52 verwendet.

Source Address:	Single IP	\$ 200.200.22.52	
		· · · · · · · · · · · · · · · · · · ·	

<u>Schritt 10:</u> (Optional) Wenn IP Range (IP-Bereich) in Schritt 8 ausgewählt wurde, geben Sie die Start- und End-IP-Adressen in die entsprechenden IP-Adressfelder ein.

Hinweis: In diesem Beispiel wird 200.200.22.22 als Start-IP-Adresse und 200.200.22.34 als End-IP-Adresse verwendet.

Source Address:	IP Range	\$ 200.200.22.22	То	200.200.22.34

Schritt 11: (Optional) Wenn in Schritt 8 Subnetz ausgewählt wurde, geben Sie die Netzwerk-

ID und die entsprechende Subnetzmaske ein, um die Richtlinie anzuwenden.

Hinweis: In diesem Beispiel wird 200.200.22.1 als Subnetz-ID und 24 als Subnetzmaske verwendet.

Source Address:	Subnet 🛟		200.200.22.1	1	24
		-			

<u>Schritt 12:</u> Wählen Sie im Dropdown-Menü Destination Interface (Zielschnittstelle) eine Schnittstelle für den ausgehenden oder ausgehenden Datenverkehr aus, auf die die Zugriffsrichtlinie angewendet werden soll. Die Optionen sind WAN1, WAN2, USB1, USB2, VLAN1 und Any.

Hinweis: In diesem Beispiel wird WAN1 ausgewählt.

Destination Interface	✓ WAN1	
	WAN2	
Destination Address:	USB1	Ð
	USB2	
	VLAN1	
	Any	
Scheduling		

Schritt 13: Wählen Sie im Dropdown-Menü Destination Address (Zieladresse) ein Ziel aus, das die Richtlinie anwendet. Die Optionen sind Any (Beliebig), Single IP (eine IP-Adresse), IP Range (IP-Bereich) und Subnet (Subnetz).

Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt. Fahren Sie mit Schritt 17 fort.

Destination Address:	🗸 Any
	Single IP
	IP Range
	Subnet
Schoduling	

Schritt 14: (Optional) Wenn in Schritt 13 eine einzelne IP-Adresse ausgewählt wurde, geben Sie eine einzige IP-Adresse für die Richtlinie ein, die angewendet werden soll.

Hinweis: In diesem Beispiel wird 210.200.22.52 verwendet.

Destination Address:	Single IP	\$ 210.200.22.52

Schritt 15: (Optional) Wenn IP Range (IP-Bereich) in Schritt 13 ausgewählt wurde, geben Sie die Start- und End-IP-Adressen in die entsprechenden IP-Adressfelder ein.

Hinweis: In diesem Beispiel wird 210.200.27.22 als Start-IP-Adresse und 210.200.27.34 als End-IP-Adresse verwendet. Fahren Sie mit <u>Schritt 17 fort</u>.

	Destination Address:	IP Range	\$	210.200.27.22	То	210.200.27.34
--	----------------------	----------	----	---------------	----	---------------

Schritt 16: (Optional) Wenn in Schritt 13 Subnetz ausgewählt wurde, geben Sie die Netzwerkadresse und die entsprechende Subnetzmaske ein, um die Richtlinie anzuwenden.

Hinweis: In diesem Beispiel wird 210.200.27.1 als Subnetzadresse und 24 als Subnetzmaske verwendet.

Destination Address:	Subnet		210.200.27.1	1	24
		_			

Schritt 17: Wählen Sie in der Dropdown-Liste Schedule Name (Name des Zeitplans) einen Zeitplan für die Anwendung dieser Richtlinie aus. Um zu erfahren, wie Sie einen Zeitplan konfigurieren, klicken Sie hier.

Scheduling		
ochedding	ANYTIME	
Schedule Name:	✓ BUSINESS	Clic
	EVENINGHOURS	-
Apply Ca	WORKHOURS	

Schritt 18: Klicken Sie auf Übernehmen.

Access Rules	
Rule Status:	Enable
Action:	Allow \$
Services:	IPv4 IPv6 All Traffic
Log:	True 💠
Source Interface:	WAN1 \$
Source Address:	Any \$
Destination Interface:	WAN1 \$
Destination Address:	Any 🗘
Scheduling	
Schedule Name:	BUSINESS Click here to configure the schedules
Apply Can	cel

Sie sollten jetzt erfolgreich eine Zugriffsregel für einen Router der RV-Serie erstellt haben.

Bearbeiten einer Zugriffsregel

Schritt 1: Aktivieren Sie in der Tabelle mit den IPv4- oder IPv6-Zugriffsregeln das Kontrollkästchen neben der Zugriffsregel, die Sie konfigurieren möchten.

Hinweis: In diesem Beispiel wird in der Tabelle mit den IPv4-Zugriffsregeln die Priorität 1 ausgewählt.

IPv	IPv4 Access Rules Table										
	Priority	Enable	Action	Service	Source Interface						
0	1	\checkmark	Allowed	IPv4: All Traffic	WAN1						
	2	\checkmark	Denied	IPv4: BGP	WAN1						
	3	\checkmark	Allowed	IPv4: FTP	WAN1						
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN						
	202	\checkmark	Denied	IPv4: All Traffic	WAN						
	Add	E	dit	Delete							

Schritt 2: Klicken Sie auf Bearbeiten.

IPv	IPv4 Access Rules Table											
	Priority	Enable	Action	Service	Source Interface							
	1	\checkmark	Allowed	IPv4: All Traffic	WAN1							
	2	\checkmark	Denied	IPv4: BGP	WAN1							
	3	\checkmark	Allowed	IPv4: FTP	WAN1							
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN							
	202	\checkmark	Denied	IPv4: All Traffic	WAN							
	Add	E	dit	Delete								

Schritt 3: (Optional) Klicken Sie in der Spalte Konfigurieren auf die Schaltfläche **Bearbeiten** in der Zeile der gewünschten Zugriffsregel.

Schedule	Configure	9		
BUSINESS	Edit	Delete	Up	Down
BUSINESS	Edit	Delete	Up	Down
ANYTIME	Edit	Delete	Up	Down
ANYTIME	Edit	Delete	Up	Down
ANYTIME	Edit	Delete	Up	Down

Schritt 4: Aktualisieren Sie die erforderlichen Parameter.

Access Rules	
Rule Status:	Enable
Action:	Allow \$
Services:	IPv4 IPv6 All Traffic
Log:	True 💠
Source Interface:	WAN1 \$
Source Address:	Any 🗘
Destination Interface:	USB1 \$
Destination Address:	Single IP \$ 192.168.1.1
Scheduling	
Schedule Name:	BUSINESS Click here to configure the schedules
Apply Can	cel

Schritt 5: Klicken Sie auf Übernehmen.

Access Rules	
Rule Status:	Enable
Action:	Allow \$
Services:	IPv4 IPv6 All Traffic
Log:	True 💠
Source Interface:	WAN1 \$
Source Address:	Any 🗘
Destination Interface:	USB1 ¢
Destination Address:	Single IP \$ 192.168.1.1
Scheduling	
Schedule Name:	BUSINESS Click here to configure the schedules
Apply Can	cel

Schritt 6: (Optional) Um die Priorität einer Zugriffsregel in der Spalte Konfigurieren zu ändern, klicken Sie auf die **Nach-oben** oder **Nach-unten**-Schaltfläche der Zugriffsregel, die Sie verschieben möchten.

Hinweis: Wenn eine Zugriffsregel nach oben oder unten verschoben wird, bewegt sie sich einen Schritt über oder unter die ursprüngliche Position. In diesem Beispiel wird Priorität 1 deaktiviert.

IPv	IPv4 Access Rules Table												
	Priority	Enable	Action	Service	Source Interf	Source	Destinat	Destination	Schedule	Configure			
	1		Allowed	IPv4: All T	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit	Delete	Up	Down
	2	1	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit	Delete	Up	Down
	3	1	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit	Delete	Up	Down
	201	1	Allowed	IPv4: All T	VLAN	Any	WAN	Any	ANYTIME				Down
	202	V	Denied	IPv4: All T	WAN	Any	VLAN	Any	ANYTIME	Edit	Delete		Down
	Add	E	dit 🛛	Delete									

Hinweis: In diesem Beispiel ist Priorität 1 jetzt Priorität 2.

IP	IPv4 Access Rules Table												
	Priority	Enable	Action	Service	Source Inter	Source	Destina	Destination	Schedule	Configure	1		
	1	V	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit	Delete	Up	Down
\square	2	V	Allowed	IPv4: All Tr	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit	Delete	Up	Down
	3	V	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit	Delete	Up	Down
	201	V	Allowed	IPv4: All Tr	VLAN	Any	WAN	Any	ANYTIME	Edit	Delete		Down
\bigcirc	202	V	Denied	IPv4: All Tr	WAN	Any	VLAN	Any	ANYTIME	Edit	Delete		Down
	Add	E	dit										

Schritt 7: Klicken Sie auf Übernehmen.

ccess Rules										
IPv4 Access Rules Table										
	Priority	Enable	Action	Service	Source Int					
	1	V	Denied	IPv4: BGP	WAN1					
	2	V	Allowed	IPv4: All Traffic	WAN1					
	3	V	Allowed	IPv4: FTP	WAN1					
	201	V	Allowed	IPv4: All Traffic	VLAN					
	202	V	Denied	IPv4: All Traffic	WAN					
	Add) E	dit	Delete						
IPv	6 Access	Rules Tab	le							
	Priority	Enable	Action	Service	Source Int					
\bigcirc	201	\checkmark	Allowed	IPv6: All Traffic	VLAN					
	202	\checkmark	Denied	IPv6: All Traffic	WAN					
	Add	E	dit	Delete						
Apply Restore to Default Rules Service Management										

Sie sollten jetzt eine Zugriffsregel für einen Router der Serie RV34x erfolgreich bearbeitet haben.

Löschen einer Zugriffsregel

Schritt 1: Aktivieren Sie in der Tabelle mit den IPv4- oder IPv6-Zugriffsregeln das Kontrollkästchen neben der Zugriffsregel, die Sie löschen möchten.

Hinweis: In diesem Beispiel wird in der Tabelle mit den IPv4-Zugriffsregeln die Priorität 1 ausgewählt.

IPv	IPv4 Access Rules Table											
	Priority	Enable	Action	Service	Source Interface							
	1	\checkmark	Allowed	IPv4: All Traffic	WAN1							
	2	\checkmark	Denied	IPv4: BGP	WAN1							
	3	\checkmark	Allowed	IPv4: FTP	WAN1							
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN							
	202	\checkmark	Denied	IPv4: All Traffic	WAN							
	Add	E	dit	Delete								

Schritt 2: Klicken Sie unter der Tabelle auf **Löschen**, oder klicken Sie in der Spalte Konfigurieren auf die Schaltfläche Löschen.

IPv4 Access Rules Table									
	Priority	Enable	Action	Service	Source Interface				
	1	\checkmark	Allowed	IPv4: All Traffic	WAN1				
	2	\checkmark	Denied	IPv4: BGP	WAN1				
	3	\checkmark	Allowed	IPv4: FTP	WAN1				
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN				
	202	\checkmark	Denied	IPv4: All Traffic	WAN				
	Add	E	dit	Delete					

Schritt 3: Klicken Sie auf Übernehmen.

cce	ess Rule	es								
IPv4 Access Rules Table										
	Priority	Enable	Action	Service	Sourc					
	1	\checkmark	Denied	IPv4: BGP	WAN1					
	2	\checkmark	Allowed	IPv4: FTP	WAN1					
	201	\checkmark	Allowed	IPv4: All Traffic	VLAN					
	202	\checkmark	Denied	IPv4: All Traffic	WAN					
	Add	E	dit	Delete						
IPV	Briority	Finable	Action	Sanica	Source					
	Phonty	Enable	Action		Sourc					
	201	\checkmark	Allowed	IPv6: All Traffic	VLAN					
	202		Denied	IPv6: All Traffic	WAN					
	Add	Ε	dit	Delete						
Ap	oply	Restore t	o Default R	Rules Service Man	agement					

Sie sollten jetzt eine Zugriffsregel für den Router der Serie RV34x erfolgreich gelöscht haben.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.