Configuration des règles d'accès sur un routeur de la gamme RV34x

Objectif

Le routeur VPN double WAN RV340 est un périphérique hautes performances, flexible et facile à utiliser, adapté aux petites entreprises. Avec des fonctions de sécurité supplémentaires, telles que le filtrage Web, le contrôle des applications et la protection de la source IP. Le nouveau routeur RV340 offre une connectivité filaire haut débit hautement sécurisée aux petits bureaux et aux employés distants. Ces nouvelles fonctions de sécurité facilitent également le réglage précis de l'activité autorisée sur le réseau.

Les règles d'accès ou les stratégies sur le routeur de la gamme RV34x permettent de configurer les règles pour accroître la sécurité du réseau. Une combinaison de règles et vous avez une liste de contrôle d'accès (ACL). Les listes de contrôle d'accès sont des listes qui bloquent ou autorisent l'envoi du trafic à destination et en provenance de certains utilisateurs. Les règles d'accès peuvent être configurées pour être en vigueur à tout moment ou en fonction de calendriers définis.

Les listes de contrôle d'accès ont un refus implicite à la fin de la liste. Par conséquent, à moins que vous ne l'autorisiez explicitement, le trafic ne peut pas passer. Par exemple, si vous voulez autoriser tous les utilisateurs à accéder à un réseau via le routeur, à l'exception des adresses particulières, vous devez refuser ces adresses et autoriser toutes les autres.

L'objectif de cet article est de vous montrer comment configurer les règles d'accès sur un routeur de la gamme RV34x.

Périphériques pertinents

• Gamme RV34x

Version du logiciel

- 1.0.1.16
 - <u>Un micrologiciel mettant à jour l'interface utilisateur est disponible depuis la publication de cet article, cliquez ici pour accéder à la page de téléchargement, localisez votre produit spécifique là.</u>

Configurer une règle d'accès sur un routeur de la gamme RV34x

Créer une règle d'accès

Étape 1. Connectez-vous à l'utilitaire Web du routeur et choisissez **Firewall > Access Rules**.



Étape 2. Dans le tableau Règles d'accès IPv4 ou IPv6, cliquez sur **Ajouter** pour créer une nouvelle règle.

Note: Sur le routeur de la gamme RV34x, il est possible de configurer jusqu'à 202 règles. Dans cet exemple, IPv4 est utilisé.

A	Access Rules									
	IPv4 Access Rules Table									
		Priority	Enable	Action	Service					
		201	\checkmark	Allowed	IPv4: All Traffic					
		202	\checkmark	Denied	IPv4: All Traffic					
		Add	E	dit	Delete					

Étape 3. Cochez la case Activer l'état de la règle pour activer la règle.





Étape 4. Dans le menu déroulant Action, choisissez si la stratégie autorise ou refuse les données.

Note: Dans cet exemple, Allow est sélectionné.



Étape 5. Dans le menu déroulant Services, sélectionnez le type de trafic que le routeur autorise ou refuse.

Note: Dans cet exemple, tout le trafic est sélectionné. Tout le trafic sera autorisé.

Services:	IPv4 IPv	✓ All Traffic
Log:	True 💠	BGP DNS-TCP
Source Interface:	WAN1 \$	DNS-UDP ESP
~ ···	· · ·	FTD

Étape 6. Dans le menu déroulant Log (Journal), sélectionnez une option pour déterminer si le routeur enregistre le trafic autorisé ou refusé. Les options sont les suivantes :

- Jamais : le routeur ne consigne jamais le trafic autorisé et refusé.
- True : le routeur enregistre le trafic correspondant à la stratégie.

Note: Dans cet exemple, Jamais est sélectionné.

Log:	✓ Never
	True
Source Interface:	••••••

Étape 7. Dans le menu déroulant Interface source, sélectionnez une interface pour le trafic entrant ou entrant où la stratégie d'accès doit être appliquée. Les options sont les suivantes

- WAN1 : la stratégie s'applique uniquement au trafic provenant du WAN1.
- WAN2 : la stratégie s'applique uniquement au trafic provenant du WAN2.
- USB1 : la stratégie s'applique uniquement au trafic provenant d'USB1.
- USB2 La stratégie s'applique uniquement au trafic provenant d'USB2.
- VLAN1 : la stratégie s'applique uniquement au trafic VLAN1.
- Any : la stratégie s'applique à n'importe quelle interface.

Note: Si un réseau local virtuel (VLAN) supplémentaire a été configuré, l'option VLAN apparaît dans la liste. Dans cet exemple, WAN1 est choisi.

Source Interface:	✓ WAN1	÷
Onumer Addresses	WAN2	_
Source Address:	USB1	Ð
Destination Interface:	USB2	
Dootmatorration	VLAN1	P
Destination Address:	Any	\$

Étape 8. Dans le menu déroulant Adresse source, sélectionnez une source pour appliquer la stratégie. Les options sont les suivantes :

- Any : la stratégie s'applique à toute adresse IP du réseau. Si cette option est sélectionnée, passez à l'<u>étape 12</u>.
- Single IP : la stratégie s'applique à un seul hôte ou adresse IP. Si cette option est sélectionnée, passez à l'<u>étape 9</u>.
- IP Range : la stratégie s'applique à un ensemble ou une plage d'adresses IP. Si cette option est sélectionnée, passez à l'<u>étape 10</u>.
- Sous-réseau : la stratégie s'applique à un sous-réseau entier. Si cette option est sélectionnée, passez à l'<u>étape 11</u>.

Note: Dans cet exemple, Any est sélectionné.

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

<u>Étape 9.</u> (Facultatif) Une adresse IP unique a été choisie à l'étape 8, saisissez une adresse IP unique pour la stratégie à appliquer, puis passez à l'<u>étape 12</u>.

Note: Pour cet exemple, 200.200.22.52 est utilisé.

Source Address:	Single IP	\$	200.200.22.52	1
oouroe Address.	Olingio II	•	200.200.22.02	

Étape 10. (Facultatif) Si la plage IP a été choisie à l'étape 8, saisissez les adresses IP de début et de fin dans les champs d'adresse IP respectifs.

Note: Dans cet exemple, 200.200.22.22 est utilisé comme adresse IP de début et 200.200.22.34 comme adresse IP de fin.

Source Address:	IP Range	\$ 200.200.22.22	То	200.200.22.34

Étape 11. (Facultatif) Si le sous-réseau a été choisi à l'étape 8, saisissez l'ID réseau et son masque de sous-réseau respectif pour appliquer la stratégie.

Note: Dans cet exemple, 200.200.22.1 est utilisé comme ID de sous-réseau et 24 comme masque de sous-réseau.

Source Address:	Subnet	\$ 200.200.22.1	1	24

<u>Étape 12.</u> Dans le menu déroulant Interface de destination, sélectionnez une interface pour le trafic sortant ou sortant où la stratégie d'accès doit être appliquée. Les options disponibles sont WAN1, WAN2, USB1, USB2, VLAN1 et Any.

Note: Dans cet exemple, WAN1 est choisi.

Destination Interface	✓ WAN1	
	WAN2	5
Destination Address:	USB1	E L
	USB2	
	VLAN1	
	Any	
Scheduling		

Étape 13. Dans le menu déroulant Adresse de destination, sélectionnez une destination pour appliquer la stratégie. Les options sont Any, Single IP, IP Range, Subnet.

Note: Dans cet exemple, Any est sélectionné. Passez à <u>l'étape 17</u>.



Étape 14. (Facultatif) Si une adresse IP unique a été choisie à l'étape 13, saisissez une adresse IP unique pour la stratégie à appliquer.

Note: Dans cet exemple, 210.200.22.52 est utilisé.

Destination Address:	Single IP	\$ 210.200.22.52	

Étape 15. (Facultatif) Si vous avez choisi IP Range à l'étape 13, saisissez les adresses IP de début et de fin dans les champs d'adresse IP respectifs.

Note: Dans cet exemple, 210.200.27.22 est utilisé comme adresse IP de début et 210.200.27.34 comme adresse IP de fin. Passez à <u>l'étape 17</u>.

Destination Address:	IP Range	\$ 210.200.27.22	То	210.200.27.34

Étape 16. (Facultatif) Si Subnet a été sélectionné à l'étape 13, saisissez l'adresse réseau et son masque de sous-réseau respectif pour appliquer la stratégie.

Note: Dans cet exemple, 210.200.27.1 est utilisé comme adresse de sous-réseau et 24 comme masque de sous-réseau.

Destination Address:	Subnet 🗘	210.200.27.1	1	24

<u>Étape 17.</u> Dans la liste déroulante Nom du programme, sélectionnez un programme pour appliquer cette stratégie. Pour savoir comment configurer un planning, cliquez <u>ici</u>.



Étape 18. Cliquez sur Apply.

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

Vous devez maintenant avoir créé une règle d'accès sur un routeur de la gamme RV.

Modifier une règle d'accès

Étape 1. Dans le tableau des règles d'accès IPv4 ou IPv6, cochez la case en regard de la règle d'accès que vous voulez configurer.

Note: Dans cet exemple, dans le tableau des règles d'accès IPv4, la priorité 1 est choisie.

IPv	IPv4 Access Rules Table											
	Priority	Enable	Action	Service	Source Interface							
\bigcirc	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								

Étape 2. Cliquez sur Edit.

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							

Étape 3. (Facultatif) Dans la colonne Configure, cliquez sur le bouton **Edit** dans la ligne de la règle d'accès souhaitée.

Schedule	Configure)		
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

Étape 4. Mettre à jour les paramètres nécessaires.

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

Étape 5. Cliquez sur Apply.

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
Scheduling	
Schedule Name:	BUSINESS Click here to configure the schedules
Apply Can	cel

Étape 6. (Facultatif) Pour modifier la priorité d'une règle d'accès dans la colonne Configurer, cliquez sur le bouton **Haut** ou **Bas** de la règle d'accès à déplacer.

Note: Lorsqu'une règle d'accès est déplacée vers le haut ou vers le bas, elle déplace une étape au-dessus ou au-dessous de son emplacement d'origine. Dans cet exemple, la priorité 1 sera déplacée vers le bas.

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

Note: Dans cet exemple, la priorité 1 est désormais la priorité 2.

IPv	IPv4 Access Rules Table												
	Priority	Enable	Action	Service	Source Inter	Source	Destina	Destination	Schedule	Configure			
	1	V	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit	Delete	Up	Down
	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			Down
0	202	V	Denied	IPv4: All Tr	WAN	Any	VLAN	Any	ANYTIME	Edit	Delete		Down
	Add	E	dit	Delete									

Étape 7.	Cliquez su	r Apply.
----------	------------	----------

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

Vous devez maintenant avoir correctement modifié une règle d'accès sur un routeur de la gamme RV34x.

Supprimer une règle d'accès

Étape 1. Dans le tableau Règles d'accès IPv4 ou IPv6, cochez la case en regard de la règle d'accès que vous voulez supprimer.

Note: Dans cet exemple, dans le tableau des règles d'accès IPv4, la priorité 1 est choisie.

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								

Étape 2. Cliquez sur **Supprimer** situé sous le tableau ou cliquez sur le bouton Supprimer dans la colonne Configurer.

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							

Étape 3. Cliquez sur Apply.

cce	ess Rule	es			
IPv	4 Access	Rules Tab	le		
	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		Denied	IPv4: All Traffic	WAN
	Add	E	dit	Delete	
IPv6 Access Rules Table					
	Priority	Enable	Action	Service	Sourc
	201	\checkmark	Allowed	IPv6: All Traffic	VLAN
	202		Denied	IPv6: All Traffic	WAN
	Add	E	dit	Delete	
_					
Ap	oply	Restore t	o Default R	ules Service Mar	nagement

Vous devez maintenant avoir supprimé une règle d'accès sur le routeur de la gamme RV34x.

Afficher une vidéo relative à cet article...

Cliquez ici pour afficher d'autres présentations techniques de Cisco