

# Configuration des règles d'accès sur les routeurs VPN RV320 et RV325

## Objectif

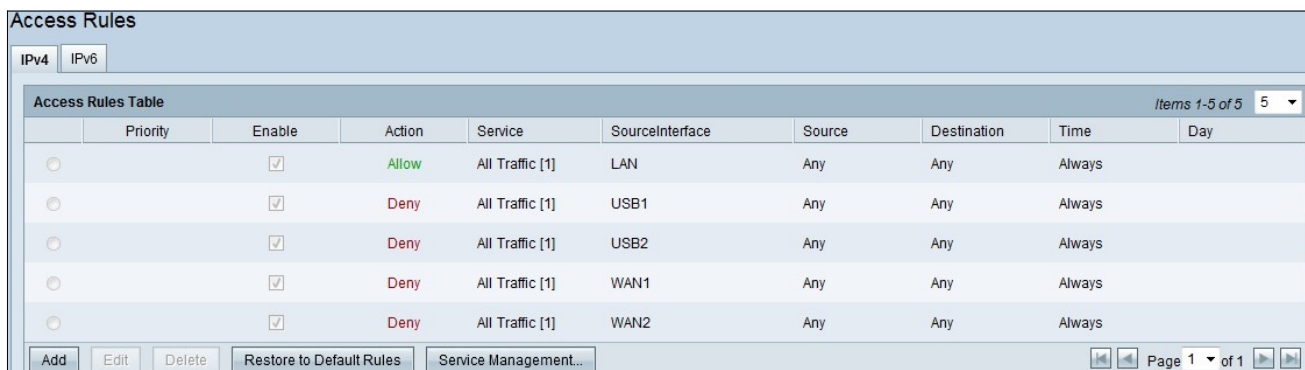
Les listes de contrôle d'accès (ACL) sont des listes qui bloquent ou autorisent l'envoi du trafic à destination et en provenance de certains utilisateurs. Les règles d'accès peuvent être configurées pour être en vigueur à tout moment ou en fonction d'un planning défini. Une règle d'accès est configurée en fonction de différents critères afin d'autoriser ou de refuser l'accès au réseau. La règle d'accès est planifiée en fonction de l'heure à laquelle les règles d'accès doivent être appliquées au routeur. Cet article décrit et décrit l'Assistant de configuration des règles d'accès utilisé pour déterminer si le trafic est autorisé à entrer dans le réseau via le pare-feu du routeur ou non pour assurer la sécurité du réseau.

## Périphériques pertinents | Version du micrologiciel

- Routeur VPN double WAN RV320 | V 1.1.0.09 ([Télécharger la dernière version](#))
- Routeur VPN double WAN Gigabit RV325 | V 1.1.0.09 ([Télécharger la dernière version](#))

## Configuration de la règle d'accès

Étape 1. Connectez-vous à l'utilitaire de configuration Web, puis choisissez **Firewall>Access Rules**. La page *Règles d'accès* s'ouvre :



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	

Le tableau Règles d'accès contient les informations suivantes :

- Priority : affiche la priorité de la règle d'accès.
- Enable : indique si la règle d'accès est activée ou désactivée.
- Action : indique que la règle d'accès est autorisée ou refusée.
- Service : affiche le type de service.
- SourceInterface : indique à quelle interface la règle d'accès est appliquée.
- Source : affiche l'adresse IP du périphérique source.
- Destination : affiche l'adresse IP du périphérique de destination.
- Time : indique l'heure à laquelle la règle d'accès doit être appliquée.
- Day : affiche une semaine au cours de laquelle la règle d'accès est appliquée

## Gestion des services

Étape 1. Cliquez sur **Gestion des services** pour ajouter un nouveau service. La page *du tableau Gestion des services* s'ouvre :

The screenshot shows a web interface titled "Service Management Table". At the top right, it indicates "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, each with a checkbox in the first column:

<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

Below the table are three buttons: "Add", "Edit", and "Delete". To the right of these buttons are navigation arrows and a page indicator "Page 1 of 5". At the bottom of the interface are "Save" and "Cancel" buttons.

Étape 2. Cliquez sur **Ajouter** pour ajouter un nouveau service.

This screenshot is identical to the previous one, but with a new row added to the table. The new row is highlighted with a red border and contains the following data:

<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

Étape 3. Configurez les champs suivants.

- Nom du service : en fonction de vos besoins, indiquez un nom pour le service.
- Protocol : choisissez un protocole TCP ou UDP pour votre service.
- Port Range : saisissez la plage de numéros de port en fonction de vos besoins et le numéro de port doit être compris dans la plage (1-65536).

Étape 4. Cliquez sur **Enregistrer** pour enregistrer les modifications

## Configuration des règles d'accès sur 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	

Page 1 of 1

Étape 1. Cliquez sur **Add** pour configurer une nouvelle règle d'accès. La fenêtre *Modifier les règles d'accès* apparaît.

**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

Étape 2. Choisissez l'option appropriée dans la liste déroulante Action pour autoriser ou limiter le trafic de la règle que vous êtes sur le point de configurer. Les règles d'accès limitent l'accès au réseau en fonction de différentes valeurs.

- Allow : autorise tout le trafic.
- Deny : limite tout le trafic.

### 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

Étape 3. Sélectionnez le service approprié à filtrer dans la liste déroulante Service.

### 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

Étape 4. Sélectionnez l'option Journal appropriée dans la liste déroulante Journal. L'option log détermine si le périphérique conserve un journal du trafic correspondant aux règles d'accès définies.

- Journaliser les paquets correspondant à cette règle d'accès — Le routeur conserve un journal qui suit le service sélectionné.
- Not Log : le routeur ne conserve pas de journaux pour la règle d'accès.

### 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

Étape 5. Dans la liste déroulante Interface, sélectionnez l'interface source appropriée. Cette interface est l'endroit où la règle d'accès serait appliquée.

- LAN : la règle d'accès affecte uniquement le trafic LAN.
- WAN 1 : la règle d'accès affecte uniquement le trafic WAN 1.
- WAN 2 : la règle d'accès affecte uniquement le trafic WAN 2.
- Any : la règle d'accès affecte tout le trafic de l'une des interfaces du périphérique.

### 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

Étape 6. Sélectionnez le type d'IP source approprié auquel la règle d'accès est appliquée dans la liste déroulante Source IP.

- Any : la règle s'applique à toute adresse IP du réseau du périphérique.
- Single : seule une adresse IP spécifiée sur le réseau du périphérique a la règle appliquée. Saisissez l'adresse IP souhaitée dans le champ adjacent.
- Plage : seule une plage spécifiée d'adresses IP sur le réseau du périphérique a la règle appliquée à ces adresses. Si vous choisissez Plage, vous devez entrer les première et dernière adresses IP de la plage dans les champs adjacents.

### 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

Étape 7. Sélectionnez le type d'adresse IP de destination auquel la règle d'accès est appliquée dans la liste déroulante disponible.

- Any : la règle s'applique à toute adresse IP de destination.
- Single : seule une adresse IP spécifiée a la règle appliquée. Saisissez l'adresse IP souhaitée dans le champ adjacent.
- Plage : seule une plage d'adresses IP spécifiée en dehors du réseau du périphérique a la règle appliquée. Si vous choisissez Plage, vous devez entrer les première et dernière adresses IP de la plage dans les champs adjacents.

**Scheduling**

Time: 

- Always
- Interval

From:  (hh:mm)

To:  (hh:mm)

Effective on:  Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Économiseur de temps** : Par défaut, l'heure est définie sur Always. Si vous voulez appliquer la règle d'accès à une heure ou un jour spécifique, suivez les étapes 8 à 11. Sinon, passez à l'étape



12.

Étape 8. Choisissez **Intervalle** dans la liste déroulante, les règles d'accès sont actives pendant certaines périodes spécifiques. vous devez entrer l'intervalle de temps pour que la règle d'accès soit appliquée.

**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

Étape 9. Saisissez l'heure à laquelle vous voulez commencer à appliquer la liste d'accès dans le champ De. Le format de l'heure est hh : mm.

Étape 10. Saisissez l'heure à laquelle vous ne voulez plus appliquer la liste d'accès dans le champ À. Le format de l'heure est 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

Étape 11. Cochez la case des jours spécifiques où vous souhaitez appliquer la liste de contrôle d'accès.

Étape 12. Cliquez sur **Enregistrer** pour enregistrer les modifications.

**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

Étape 13. (Facultatif) Pour restaurer les règles par défaut, cliquez sur **Restaurer les règles par**

défaut. Toutes les règles d'accès configurées par vous sont perdues.

## Configuration des règles d'accès sur IPv6



The screenshot shows the 'Access Rules' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6'. The 'IPv6' tab is 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 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.

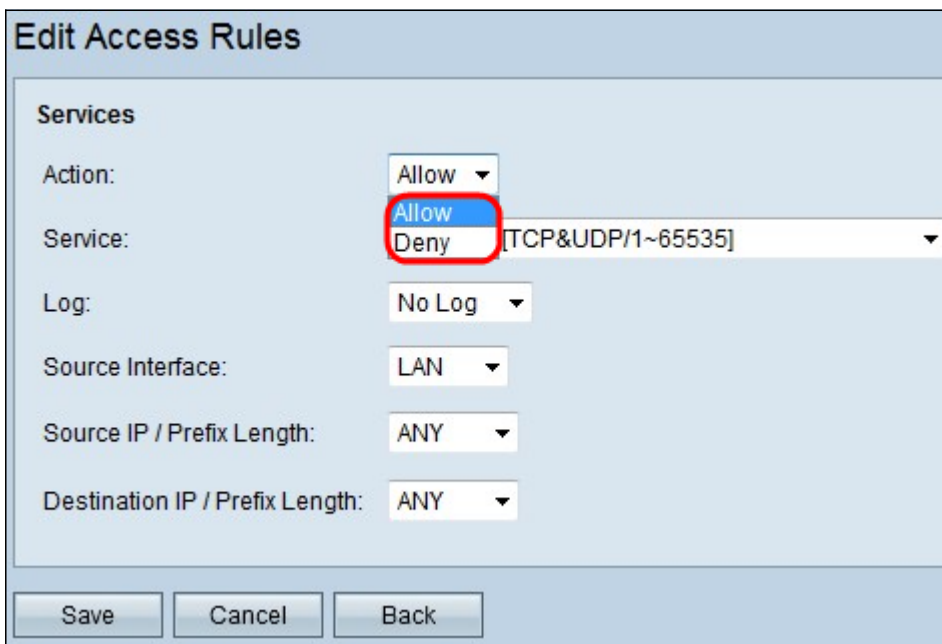
Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any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

Étape 1. Cliquez sur l'onglet IPv6 pour configurer les règles d'accès IPv6.



The screenshot shows the 'Access Rules' configuration page with the 'IPv6' tab selected. The table and buttons are the same as in the previous screenshot. The 'Add' button is highlighted with a red circle.

Étape 2. Cliquez sur Ajouter pour ajouter une nouvelle règle d'accès IPv6. La fenêtre *Modifier les règles d'accès* apparaît.



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 is highlighted with a red circle. At the bottom, there are buttons for 'Save', 'Cancel', and 'Back'.

Étape 3. Sélectionnez l'option appropriée dans la liste déroulante Action pour autoriser ou restreindre la règle à configurer. Les règles d'accès limitent l'accès au réseau en autorisant ou en refusant l'accès au trafic à partir de services ou de périphériques spécifiques.

- Allow : autorise tout le trafic.
- Deny : limite tout le trafic.

### Edit Access Rules

**Services**

Action:

Service:

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

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]

Étape 4. Sélectionnez le service approprié à filtrer dans la liste déroulante Service.

**Note:** Pour autoriser tout le trafic, choisissez **All Traffic [TCP&UDP/1~65535]** dans la liste déroulante service si l'action a été définie pour autoriser. La liste contient tous les types de services que vous souhaitez filtrer.

### Edit Access Rules

**Services**

Action:

Service:

Log:

Source Interface:

Source IP / Prefix Length:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Étape 5. Sélectionnez l'option Journal appropriée dans la liste déroulante Journal. L'option log détermine si le périphérique conserve un journal du trafic correspondant aux règles d'accès définies.

- Enabled : permet au routeur de conserver le suivi des journaux pour le service sélectionné.
- Not Log : désactive le routeur pour conserver le suivi des journaux.

### Edit Access Rules

**Services**

Action: Allow ▾

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

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: LAN  
WAN1  
WAN2  
ANY

Destination IP / Prefix Length:

Save Cancel Back

Étape 6. Cliquez sur la liste déroulante Interface et sélectionnez l'interface source appropriée. Cette interface est l'endroit où la règle d'accès serait appliquée.

- LAN : la règle d'accès affecte uniquement le trafic LAN.
- WAN 1 : la règle d'accès affecte uniquement le trafic WAN 1.
- WAN 2 : la règle d'accès affecte uniquement le trafic WAN 2.
- Any : la règle d'accès affecte tout le trafic de l'une des interfaces du périphérique.

### 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  
Single  
Subnet

Save Cancel Back

Étape 7. Choisissez le type d'IP source approprié auquel la règle d'accès est appliquée dans la liste déroulante Longueur IP/préfixe source.

- ANY : la règle s'applique à tous les paquets reçus d'un réseau du périphérique.

### Edit Access Rules

**Services**

Action:

Service:

Log:

Source Interface:

Source IP / Prefix Length:   /

Destination IP / Prefix Length:

- Single : seule une adresse IP spécifiée dans le réseau du périphérique a la règle appliquée. Saisissez l'adresse IPv6 souhaitée dans le champ adjacent.

### Edit Access Rules

**Services**

Action:

Service:

Log:

Source Interface:

Source IP / Prefix Length:   /

Destination IP / Prefix Length:

- Sous-réseau : seules les adresses IP d'un sous-réseau ont la règle qui leur est appliquée. Saisissez l'adresse réseau IPv6 et la longueur de préfixe du sous-réseau souhaité dans les champs adjacents.

**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

Étape 8. Sélectionnez le type d'IP de destination auquel la règle d'accès est appliquée dans la liste déroulante Destination IP / Prefix Length.

- Any : la règle s'applique à toute adresse IP de destination.
- Single : seule une adresse IP spécifiée sur le réseau du périphérique a la règle appliquée. Saisissez l'adresse IPv6 souhaitée.
- Sous-réseau : seules les adresses IP d'un sous-réseau ont la règle qui leur est appliquée. Saisissez l'adresse réseau IPv6 et la longueur de préfixe du sous-réseau souhaité dans les champs adjacents.

Étape 9. Cliquez sur **Enregistrer** pour que les modifications soient effectives.

**Afficher une vidéo relative à cet article...**

[Cliquez ici pour afficher d'autres présentations techniques de Cisco](#)