

Assistant de configuration des règles d'accès sur la gamme de routeurs VPN RV32x

Objectif

L'Assistant de configuration des règles d'accès est une méthode simple et pratique qui permet de configurer les configurations initiales sur le routeur RV32x. Il guide l'utilisateur dans un processus pas à pas pour configurer le périphérique. 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, qui est utilisé pour déterminer le trafic autorisé à pénétrer dans le réseau via le pare-feu, ce qui aide à sécuriser le réseau.

Périphérique applicable

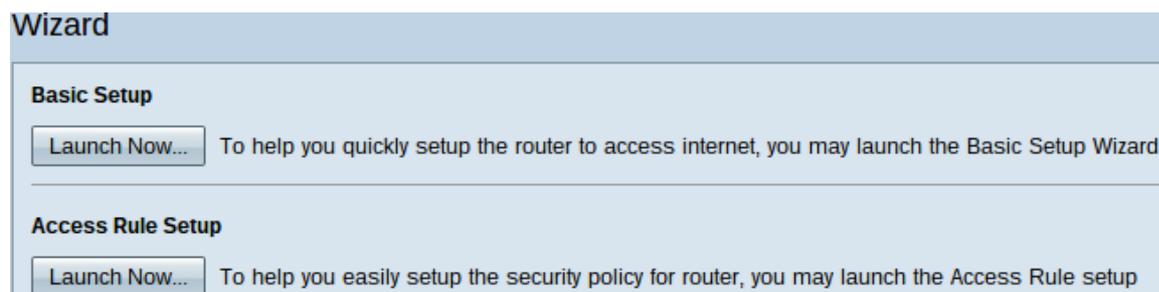
Routeur VPN double WAN · RV320
Routeur VPN double WAN Gigabit · RV325

Version du logiciel

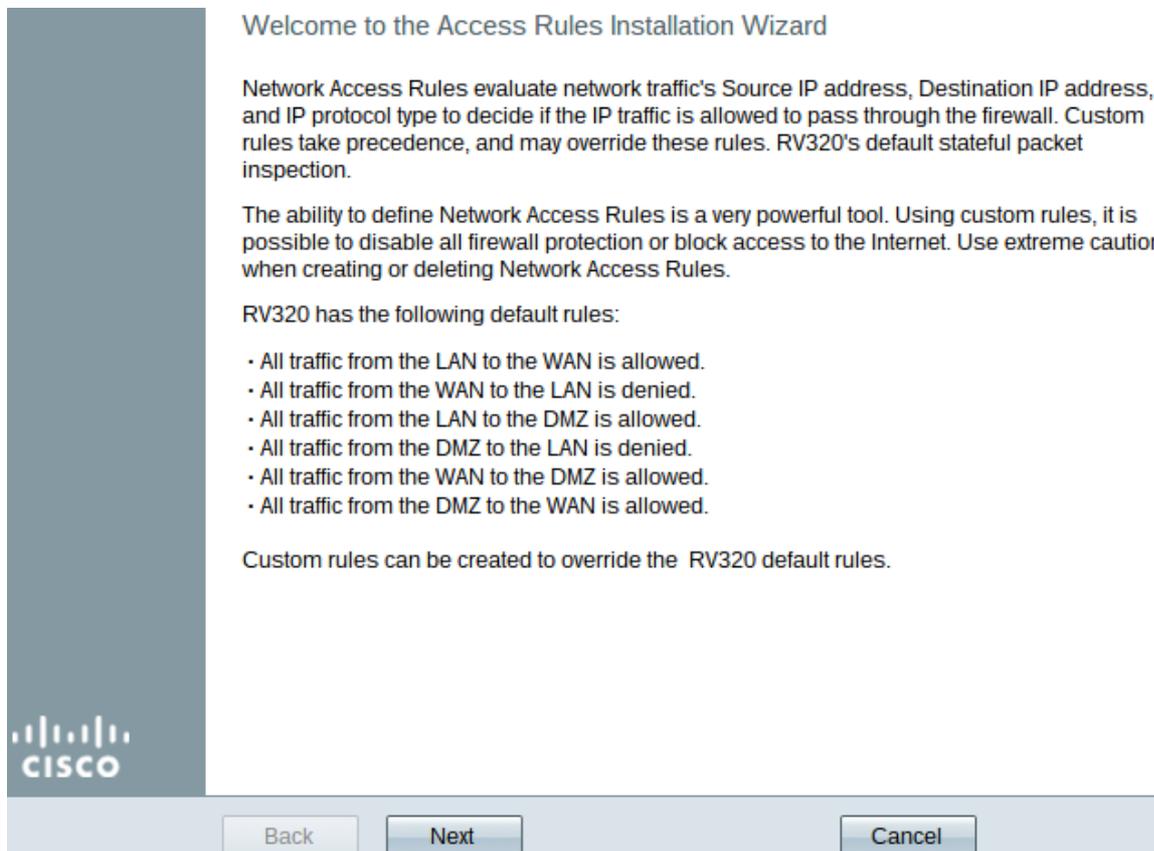
•v 1.1.0.09

Assistant Configuration des règles d'accès

Étape 1. Connectez-vous à l'utilitaire de configuration du routeur et choisissez **Wizard**. La page *Assistant* s'ouvre :



Étape 2. Cliquez sur le bouton **Lancer maintenant** sous la zone Configuration de la règle d'accès pour commencer l'Assistant Configuration de la règle d'accès. La boîte de dialogue *Assistant Installation de règle d'accès* apparaît.



Étape 3. Cliquez sur **Suivant** pour poursuivre l'exécution de l'Assistant.

Action

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: <input type="text" value="Deny"/>
Destination IP	
Schedule	
Summary	
Finish	



Étape 1. Sélectionnez la case d'option appropriée dans la liste déroulante Action pour autoriser ou restreindre la règle que vous êtes sur le point de configurer. Les règles d'accès limitent l'accès au sous-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.

Étape 2. Cliquez sur **Suivant** pour continuer l'Assistant.

Service

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

Étape 1. Sélectionnez le service approprié à filtrer pour être autorisé ou restreint 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.

Étape 2. Cliquez sur **Suivant** pour continuer la configuration.

Journal

✓ 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

Étape 1. 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.

·les paquets de journal correspondent à cette règle d'accès : permet au routeur de conserver le suivi des journaux pour le service sélectionné.

·Not Log : désactive le routeur pour conserver le suivi des journaux.

Étape 2. Cliquez sur **Suivant** pour continuer la configuration.

Interface source

✓ 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:

Source IP

Destination IP

Schedule

Summary

Finish

Étape 1. Cliquez sur la liste déroulante Interface et sélectionnez l'interface source appropriée. Cette interface est l'endroit où la règle d'accès est 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.

Étape 2. Cliquez sur **Suivant** pour continuer la configuration.

Adresse IP source

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

Service

Log 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.

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Étape 1. Choisissez le type d'IP source approprié auquel la règle d'accès est appliquée dans la liste déroulante disponible.

·Any : la règle s'applique à toute adresse IP du réseau du périphérique.

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.

·unique : seule une adresse IP spécifiée sur le réseau du périphérique a la règle qui lui est appliquée. Saisissez l'adresse IP souhaitée.

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

·Range : seule une plage d'adresses IP spécifiée sur le réseau a la règle appliquée à ces adresses. Si vous choisissez Plage, vous devez entrer les adresses IP de début et de fin de la plage.

Étape 2. Cliquez sur **Suivant** pour continuer la configuration.

Adresse IP de destination

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

Schedule

Summary

Finish

Étape 1. 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.

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.

·unique : seule une adresse IP spécifiée à laquelle la règle s'applique. Saisissez l'adresse IP souhaitée.

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

·Range : seule une plage d'adresses IP spécifiée qui sort du réseau du périphérique à laquelle la règle est appliquée à ces adresses. Si vous choisissez Plage, vous devez entrer les adresses IP de début et de fin de la plage.

Étape 2. Cliquez sur **Suivant** pour continuer la configuration.

Programmer

- ✓ 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

Étape 1. Cliquez sur la case d'option appropriée pour choisir l'heure à laquelle vous voulez appliquer la règle d'accès sur le routeur.

·Always : les règles d'accès sont toujours actives sur le routeur. Si vous choisissez cette option, passez à l'étape 5. Il s'agit de la configuration par défaut.

Intervalle · : les règles d'accès sont actives pendant certaines périodes spécifiques. Si vous choisissez cette option, vous devez saisir l'intervalle de temps pour l'application de la règle d'accès.

✓ 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

Étape 2. Saisissez l'heure à partir de laquelle vous voulez appliquer la liste d'accès dans le champ De. Le format de l'heure est **hh:mm**.

Étape 3. Saisissez l'heure jusqu'à laquelle vous souhaitez appliquer la liste d'accès dans le champ À. Le format de l'heure est hh : mm.

Étape 4. Cochez la case des jours spécifiques où vous souhaitez appliquer la liste de contrôle d'accès.

Étape 5. Cliquez sur **Suivant** pour continuer la configuration.

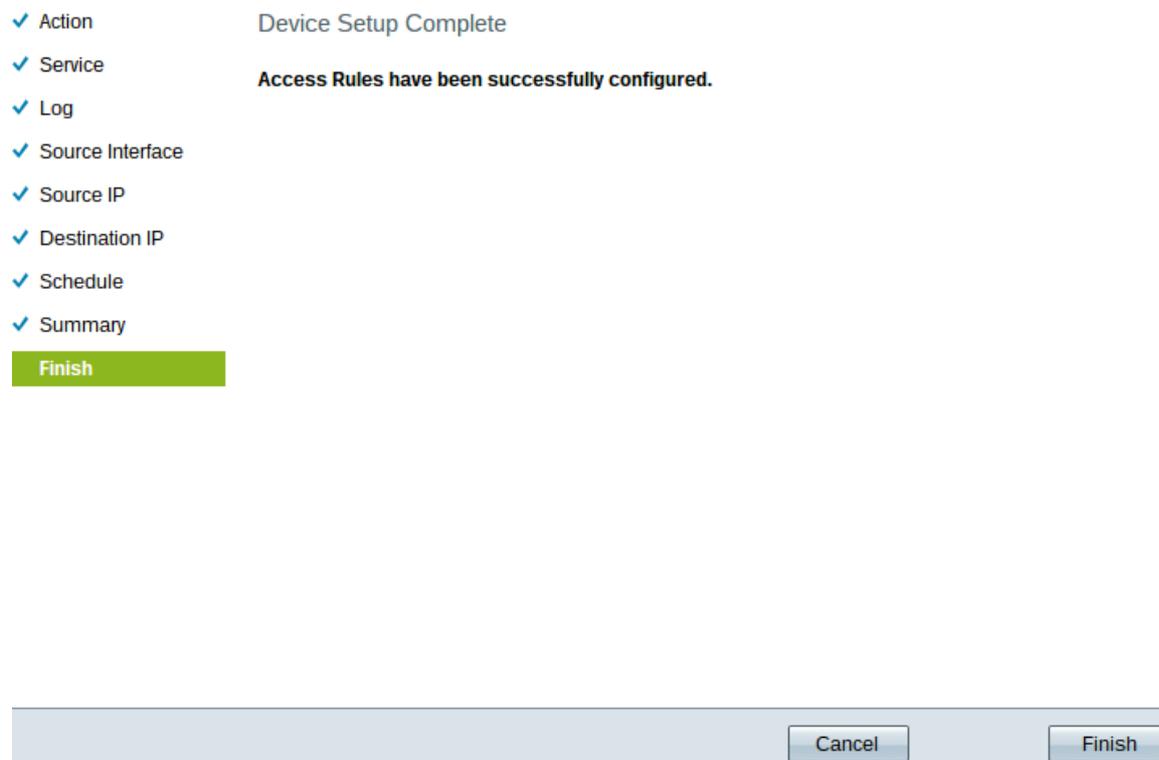
Résumé

✓ 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

Note: La page *Récapitulatif* affiche une vue d'ensemble de tous les paramètres qui viennent d'être configurés sur le routeur RV320 par l'Assistant de configuration d'accès.

Étape 1. Cliquez sur **Submit** pour soumettre vos modifications à la configuration de l'Assistant.

Terminer



Étape 1. Cliquez sur **Terminer** pour finaliser l'Assistant de configuration des règles d'accès.