

Configuration de la règle d'accès via l'Assistant sur les routeurs VPN RV016, RV082, RV042 et RV042G

Objectif

La règle d'accès est utilisée 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. 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 du moment où les règles d'accès doivent être appliquées au routeur.

Cet article explique comment configurer les règles d'accès via un assistant sur les routeurs VPN RV016, RV082, RV042 et RV042G.

Note: Vous pouvez configurer la règle d'accès via le pare-feu. Pour en savoir plus sur la configuration de la règle d'accès via le pare-feu, consultez *Configuration d'une règle d'accès IPv4 sur les routeurs RV016, RV082, RV042 et RV042G VPN* pour la règle d'accès IPv4 et *Configuration d'une règle d'accès IPv6 sur RV000004044404400402 Routeurs VPN 016 et RV042G* pour règle d'accès IPv6. Vous pouvez également planifier la règle d'accès via le pare-feu. Pour en savoir plus sur la planification de la règle d'accès via le pare-feu, reportez-vous à *Schedule Access Rule sur RV016, RV082, RV042 et RV042G*.

Périphériques pertinents

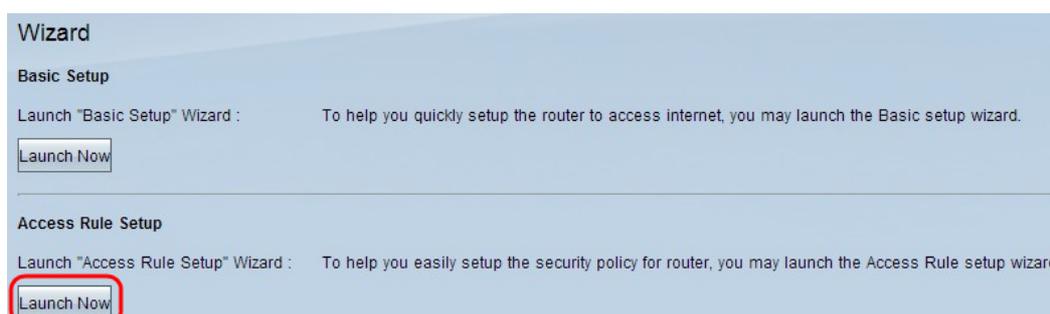
- RV042
- RV042G
- RV082
- RV016

Version du logiciel

- v 4.2.1.02

Configuration de la règle d'accès

Étape 1. Utilisez l'utilitaire de configuration du routeur pour sélectionner **Wizard**. La page *Assistant* s'ouvre :



Étape 2. Cliquez sur **Lancer maintenant** de la section Configuration des règles d'accès pour configurer l'Assistant Installation des règles d'accès. La page explique les règles d'accès et les règles par défaut du routeur. La fenêtre Assistant Installation des règles d'accès s'ouvre :

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 RV042G'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 all access to the Internet. Use extreme caution when creating or deleting Network Access Rules.

RV042G 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 RV042G default rules.

Back Next Cancel

Étape 3. Cliquez sur **Suivant** pour continuer la configuration.

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 from the LAN to the Internet. Thus select Allow. Or, to restrict all FTP traffic access from the LAN to the Internet. Thus select Deny.

Log

Source Interface

Source IP Action:

Destination IP

Schedule

Summary

Finish

Back Next Cancel

Étape 4. Sélectionnez la case d'option appropriée dans la liste déroulante Action pour

autoriser ou limiter le trafic FTP du LAN/WAN à Internet.

·Allow : permet à tout le trafic FTP d'accéder à Internet à partir du LAN/WAN.

·Refuser : limite l'accès à l'ensemble du trafic FTP sur Internet à partir du LAN/WAN.

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

✓ Action Select the Service.

Service Select the service that will be allowed or denied from the Service menu.

Log

Source Interface

Source IP

Destination IP

Schedule

Summary

Finish

Service:

All Traffic [TCP&UDP/1~65535] ▼

All Traffic [TCP&UDP/1~65535] ▲

DNS [UDP/53~53]

FTP [TCP/21~21]

HTTP [TCP/80~80]

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]

Back Next Cancel

Étape 6. Sélectionnez le service approprié que vous devez autoriser ou refuser dans la liste déroulante Service.

Étape 7. Cliquez sur **Suivant** pour continuer la configuration.

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

Select the Log.

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

Log:

- Log packets match this rule
- Log packets match this rule
- Not log

Étape 8. Sélectionnez l'option Journal appropriée dans la liste déroulante Journal.

- 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 9. Cliquez sur **Next** pour continuer.

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

Select the Source Interface.

Select the source, either WAN, LAN, DMZ or Any from the Source Interface menu. For example, allow all FTP traffic access from the LAN to the Internet. Thus select the LAN as source.

Interface:

- LAN
- LAN
- WAN 1
- WAN 2
- ANY

Étape 10. Sélectionnez l'interface source appropriée dans la liste déroulante Interface.

·LAN : l'interface source est Local Area Network. La règle d'accès affecte uniquement le trafic LAN.

·WAN 1 — L'interface source est Wide Area Network 1. La règle d'accès affecte uniquement le trafic WAN 1.

·WAN 2 : l'interface source est le réseau étendu 2. La règle d'accès affecte uniquement le trafic WAN 2.

·Any : l'interface source peut être n'importe quel réseau. La règle d'accès affecte tout trafic.

Étape 11. Cliquez sur **Next pour continuer**.

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

✓ Service For example, allow all users on LAN side to access the Internet. Thus select Any. Allow certain user(s) on LAN side to access the Internet. Thus select Single or Range and enter the IP address.

✓ Log

✓ Source Interface

Source IP

Destination IP

Schedule

Summary

Finish



Étape 12. Choisissez l'adresse IP source appropriée ou une plage d'adresses IP auxquelles la règle d'accès est appliquée dans la liste déroulante Source IP.

·Any : tout utilisateur possédant une adresse IP peut accéder à Internet.

·unique : seul l'utilisateur unique possédant une adresse IP unique peut accéder à Internet. Si vous choisissez Single, vous devez entrer l'adresse IP spécifique.

·Range : seuls les utilisateurs disposant de la plage d'adresses IP peuvent accéder à Internet. Si vous choisissez Plage, vous devez entrer les adresses IP de début et de fin.

Étape 13. Faites défiler la page vers le bas et cliquez sur **Suivant** pour continuer la configuration.

✓ 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. For example, allows Internet can access the DMZ port, thus select Single or Range and enter the IP address of DMZ port.

✓ Log

✓ Source Interface

✓ Source IP

Destination IP

Schedule

Summary

Finish



Étape 14. Choisissez l'adresse IP de destination ou la plage d'adresses IP appropriée pour la règle d'accès dans la liste déroulante Destination IP.

·Any : l'interface de destination peut avoir n'importe quelle adresse IP.

·Single : l'interface de destination peut être l'adresse IP unique spécifique. Si vous choisissez Single, vous devez saisir l'adresse IP unique spécifique.

·Range : l'interface de destination peut être l'une des adresses IP de la plage donnée. Si vous choisissez Plage, vous devez entrer les adresses IP de début et de fin.

Étape 15. Faites défiler la page vers le bas et cliquez sur **Suivant** pour continuer la configuration.

✓ Action When it works

✓ Service Select the scheduling for this rule to be enforced.

✓ Log

✓ Source Interface

✓ Source IP

✓ Destination IP

Schedule

Summary

Finish

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.

Étape 16. 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 s'appliquent toujours sur le routeur. Si vous choisissez cette option, passez de l'étape 17 à l'étape 19. La valeur par défaut est Always.

Intervalle : les règles d'accès sont appliquées pendant certaines périodes spécifiques en fonction du moment où elles sont définies. 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 17. Saisissez l'heure à partir de laquelle vous souhaitez appliquer le planning de la liste d'accès dans le champ De. Le format de l'heure est hh : mm.

Étape 18. Saisissez l'heure jusqu'à laquelle vous souhaitez appliquer le planning de la liste d'accès dans le champ À. Le format de l'heure est hh : mm.

Étape 19. Cochez cette case lorsque vous souhaitez appliquer le planning de la liste d'accès.

Étape 20. Faites défiler la page vers le bas et cliquez sur **Suivant** pour continuer la configuration. La fenêtre Résumé contenant des informations détaillées sur la règle d'accès s'ouvre :

✓ Action	Summary
✓ Service	Action: Allow
✓ Log	Service: All Traffic [TCP&UDP/1~65535]
✓ Source Interface	Log: Log packets match this rule
✓ Source IP	Source Interface: LAN
✓ Destination IP	Source IP: Any
✓ Schedule	Destination IP: Any
Summary	Schedule: From 03:10 to 10:10 , Mon , Tue , Fri
Finish	

Étape 21. Faites défiler la page vers le bas et cliquez sur **Installer** pour installer le programme d'installation.

Étape 22. Cliquez sur **OK** pour enregistrer les paramètres et revenir à la page Assistant.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.