# Meilleures pratiques de liste de contrôle d'accès sur un routeur de la gamme RV34x

## Objectif

L'objectif de cet article est de décrire les meilleures pratiques pour créer des listes de contrôle d'accès (ACL) avec votre routeur de la gamme RV34x.

## Périphériques pertinents | Version du micrologiciel

- RV340 | 1.0.03.20 (télécharger la dernière version)
- RV340W | 1.0.03.20 (télécharger la dernière version)
- RV345 | 1.0.03.20 (télécharger la dernière version)
- RV345P | 1.0.03.20 (télécharger la dernière version)

## Introduction

Voulez-vous davantage de contrôle sur votre réseau ? Voulez-vous prendre des mesures supplémentaires pour sécuriser votre réseau ? Si c'est le cas, une liste de contrôle d'accès (ACL) peut être exactement ce dont vous avez besoin.

Une liste de contrôle d'accès se compose d'une ou plusieurs entrées de contrôle d'accès (ACE) qui définissent collectivement le profil de trafic réseau. Ce profil peut ensuite être référencé par les fonctions logicielles Cisco telles que le filtrage du trafic, la priorité ou la mise en file d'attente personnalisée. Chaque liste de contrôle d'accès inclut un élément d'action (permit ou deny) et un élément de filtre basé sur des critères tels que l'adresse source, l'adresse de destination, le protocole et les paramètres spécifiques au protocole.

En fonction des critères que vous avez entrés, vous pouvez contrôler le trafic entrant et/ou sortant d'un réseau. Lorsqu'un routeur reçoit un paquet, il examine le paquet pour déterminer s'il doit transférer ou abandonner le paquet en fonction de votre liste d'accès.

La mise en oeuvre de ce niveau de sécurité est basée sur différents cas d'utilisation, compte tenu de scénarios de réseau et de besoins de sécurité particuliers.

Il est important de noter que le routeur peut créer automatiquement une liste d'accès en fonction des configurations de votre routeur. Dans ce cas, il se peut que vous ne puissiez pas effacer les listes d'accès à moins de modifier les configurations des routeurs.

### Pourquoi utiliser des listes d'accès

- Dans la plupart des cas, nous utilisons des listes de contrôle d'accès pour fournir un

niveau de sécurité de base pour accéder à notre réseau. Par exemple, si vous ne configurez pas de listes de contrôle d'accès, par défaut, tous les paquets passant par le routeur peuvent être autorisés à toutes les parties de notre réseau.
- Les listes de contrôle d'accès peuvent autoriser un hôte, une plage d'adresses IP ou des réseaux et empêcher un autre hôte, une plage d'adresses IP ou des réseaux d'accéder à la même zone (hôte ou réseau).
- Àl'aide de listes de contrôle d'accès, vous pouvez déterminer les types de trafic que vous avez transférés ou bloqués sur les interfaces du routeur. Par exemple, vous pouvez autoriser le trafic SFTP (Secure Shell) et en même temps bloquer tout le trafic SIP (Session Initiation Protocol).

### Quand utiliser les listes de contrôle d'accès

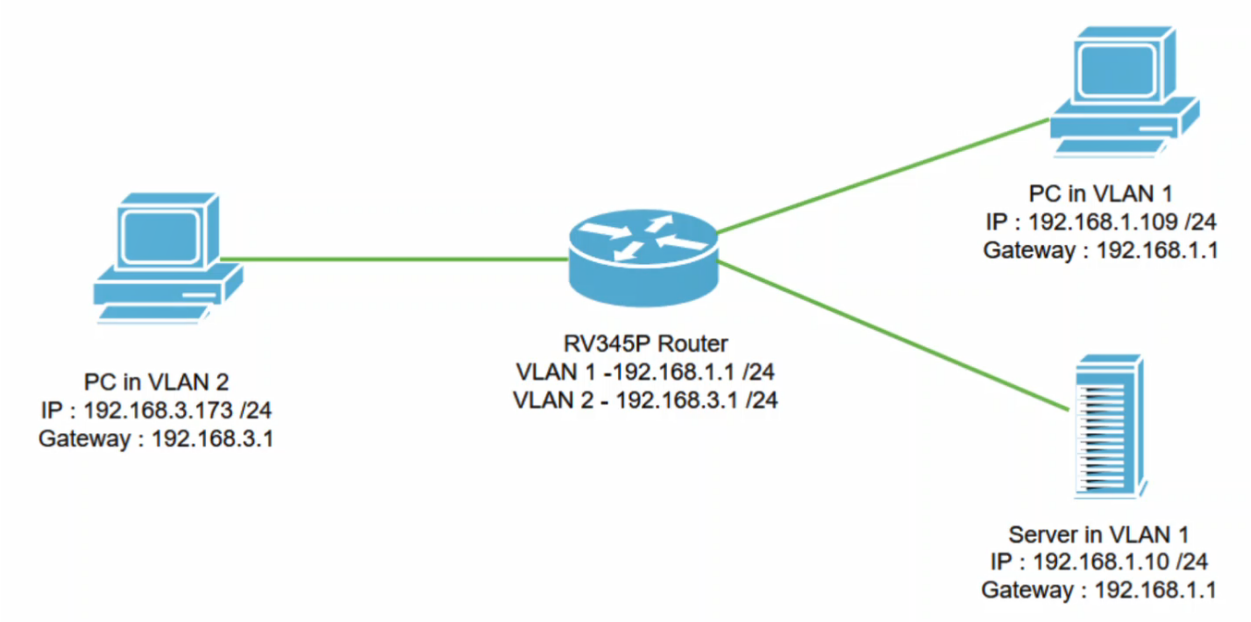
- Vous devez configurer des listes de contrôle d'accès dans les routeurs situés entre notre réseau interne et un réseau externe tel qu'Internet.
- Vous pouvez utiliser des listes de contrôle d'accès pour contrôler le trafic entrant ou sortant d'une partie spécifique de notre réseau interne.
- Lorsque vous devez filtrer le trafic entrant ou sortant, ou les deux sur une interface.
- Vous devez définir des listes de contrôle d'accès par protocole pour contrôler le trafic.

### Meilleures pratiques de configuration de la sécurité de base avec les listes d'accès

- Implémenter des listes de contrôle d'accès qui autorisent uniquement les protocoles, les ports et les adresses IP qui refusent tout le reste.
- Bloquez les paquets entrants qui prétendent avoir la même adresse de destination et d'origine (attaque terrestre sur le routeur lui-même).
- Activez la fonctionnalité de journalisation sur les listes de contrôle d'accès à un hôte Syslog interne (approuvé).
- Si vous utilisez le protocole SNMP (Simple Network Management Protocol) sur le routeur, vous devez configurer une liste de contrôle d'accès SNMP et une chaîne de communauté SNMP complexe.
- Autoriser uniquement les adresses internes à entrer dans le routeur à partir des interfaces internes et autoriser uniquement le trafic destiné aux adresses internes à entrer dans le routeur à partir de l'extérieur (interfaces externes).
- Bloquer la multidiffusion si elle n'est pas utilisée.
- Bloquez certains types de messages ICMP (Internet Control Message Protocol) (redirection, écho).
- Considérez toujours l'ordre dans lequel vous entrez les listes de contrôle d'accès. Par exemple, lorsque le routeur décide de transférer ou de bloquer un paquet, il teste le paquet par rapport à chaque instruction de liste de contrôle d'accès dans l'ordre dans lequel les listes de contrôle d'accès ont été créées.

## Implémentation de listes d'accès dans les routeurs de la gamme Cisco RV34x

### Exemple de topologie de réseau



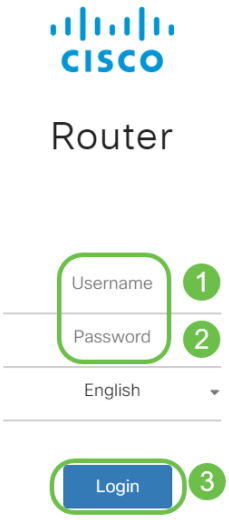

## Exemple de scénario

Dans ce scénario, nous répliquerons ce schéma de réseau, où nous avons un routeur RV345P et deux interfaces VLAN différentes. Nous avons un PC dans VLAN 1 et dans VLAN2, et nous avons également un serveur dans VLAN 1. Le routage inter-VLAN est activé, de sorte que les utilisateurs de VLAN 1 et VLAN 2 peuvent communiquer entre eux. Nous allons maintenant appliquer la règle d'accès pour restreindre la communication entre l'utilisateur du VLAN 2 vers ce serveur dans le VLAN 1.

## Exemple de configuration

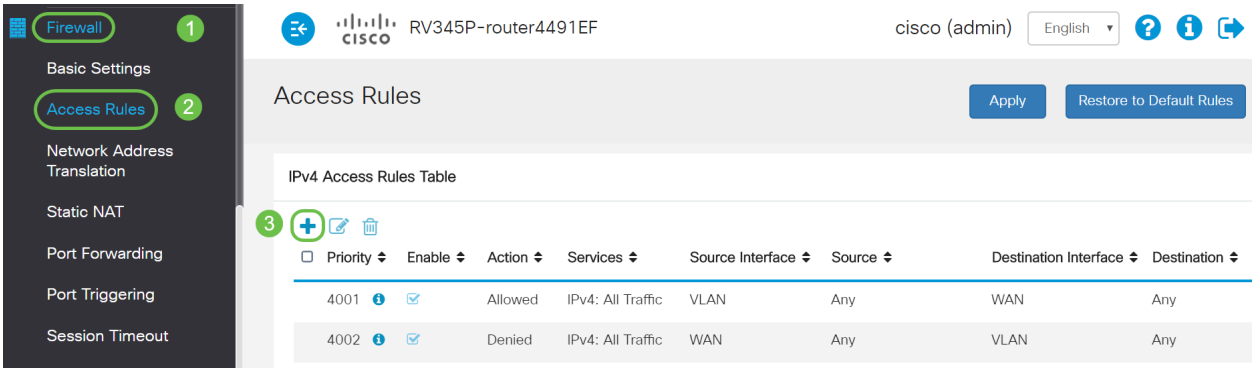
### Étape 1

Connectez-vous à l'interface utilisateur Web du routeur à l'aide des informations d'identification que vous avez configurées.




### Étape 2

Pour configurer la liste de contrôle d'accès, accédez à **Firewall > Access Rules** et cliquez sur l'**icône plus** pour ajouter une nouvelle règle.



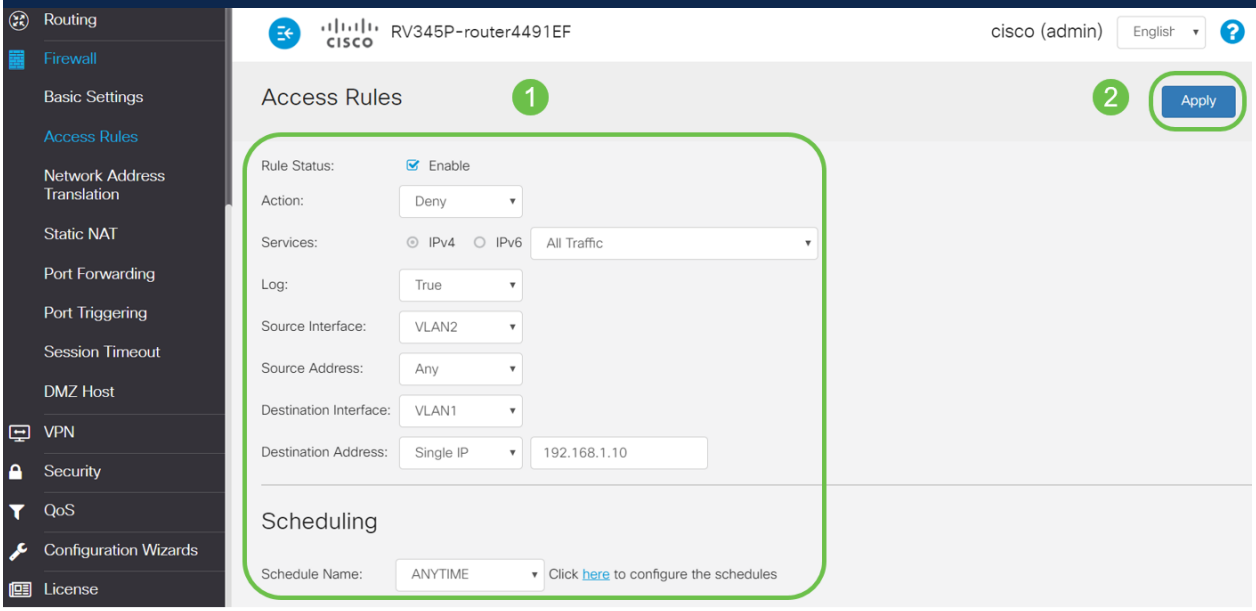

## Étape 3

Configurez les paramètres *des règles d'accès*. Appliquer une liste de contrôle d'accès pour restreindre le serveur (IPv4 : 192.168.1.10/24) accès des utilisateurs de VLAN2. Pour ce scénario, les paramètres seront les suivants :

- *État de la règle : Activer*
- *Action : Refuser*
- *Services : Tout le trafic*
- *Journal : Vrai*
- *Interface source : VLAN2*
- *Adresse source: tous les modèles*
- *Interface de destination : VLAN1*
- *Adresse de destination: Adresse IP unique 192.168.1.10*
- *Nom de la planification : À tout moment*

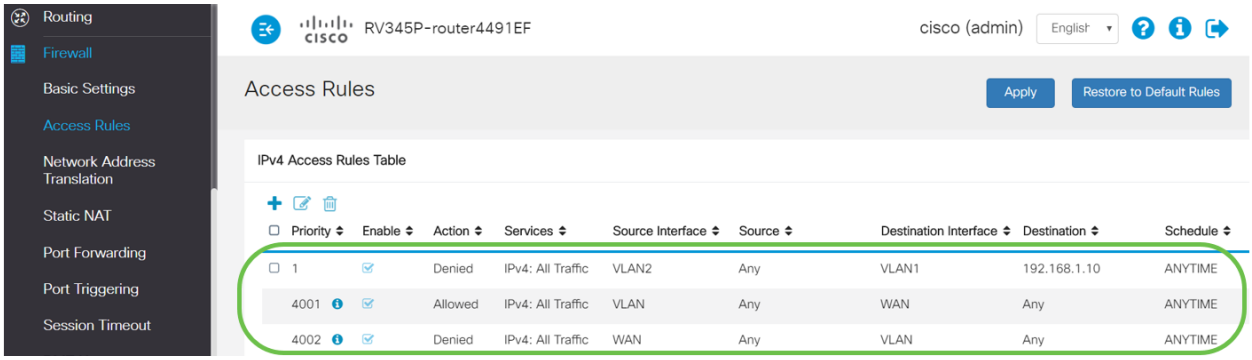
Cliquez sur Apply.

Dans cet exemple, nous avons refusé l'accès de n'importe quel périphérique de VLAN2 au serveur, puis nous avons autorisé l'accès aux autres périphériques de VLAN1. Vos besoins peuvent varier.




## Étape 4

La liste *Règles d'accès* s'affiche comme suit :




## Vérification

Pour vérifier le service, ouvrez l'invite de commandes. Sur les plates-formes Windows, cela peut être réalisé en cliquant sur le bouton Windows, puis en tapant **cmd** dans la zone de recherche inférieure gauche de l'ordinateur et en sélectionnant **Invite de commandes** dans le menu.

Entrez les commandes suivantes :

- Sur le PC (192.168.3.173) dans VLAN2, envoyez une requête ping au serveur (IP : 192.168.1.10). Vous recevrez une notification de *délai d'attente de la demande*, ce qui signifie que la communication n'est pas autorisée.
- Sur le PC (192.168.3.173) dans VLAN2, envoyez une requête ping à l'autre PC (192.168.1.109) dans VLAN1. Vous obtiendrez une réponse réussie.

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

## Conclusion

Vous avez vu les étapes nécessaires pour configurer la règle d'accès sur un routeur de la gamme Cisco RV34x. Vous pouvez désormais appliquer cette règle pour créer une règle d'accès dans votre réseau qui correspondra à vos besoins !