Configurez IP utilisé généralement ACLs

Contenu

Introduction

Ce document fournit des exemples de configuration pour les listes de contrôle d'accès (ACL) fréquemment utilisées, qui filtrent les paquets IP sur la base des éléments suivants :

- Adresse source
- Adresse de destination
- Type de paquet
- Toute combinaison de ces éléments

Pour filtrer le trafic réseau, les listes de contrôle d'accès vérifient si les paquets sont acheminés ou bloqués au niveau de l'interface du routeur. Votre routeur examine chaque paquet afin de déterminer si expédier ou relâcher le paquet basé sur les critères que vous spécifiez dans l'ACL. Les critères de la liste ACL incluent :

- Adresse source du trafic
- Adresse de destination du trafic
- Protocole de couche supérieure

Terminez-vous ces étapes afin de construire un ACL comme les exemples dans ce document

affichent :

1. Créez une liste ACL.
2. Appliquez l'ACL à une interface.

L'ACL IP est une collection séquentielle d'autorisation et refuse les conditions qui s'appliquent à un paquet IP. Le routeur teste les paquets en fonction des conditions présentes dans l'ACL, les unes après les autres.

La première correspondance détermine si le logiciel Cisco IOS® doit accepter ou refuser le paquet. Puisque le Logiciel Cisco IOS arrête le test des conditions après la première correspondance, l'ordre des conditions est essentiel. Si aucune condition ne possède de correspondance, le routeur refuse le paquet en raison d'une clause implicite de refus de tous les paquets.

Voici des exemples d'ACL IP qui peuvent être configurées dans le logiciel Cisco IOS :

- ACLs standard
- ACLs étendu
- ACL dynamiques (verrou et clé)
- ACL nommées IP
- Listes de contrôle d'accès réflexives
- ACL basées sur l'heure, qui utilisent des plages temporelles
- Entrées de liste de contrôle d'accès IP commentées
- ACL basées sur le contexte
- Proxy d'authentification
- Listes de contrôle d'accès turbo
- Listes de contrôle d'accès basées sur l'heure distribuées

Ce document traite des normes et des listes de contrôle d'accès fréquemment utilisées (standard et étendues). Reportez-vous à Configurer des listes d'accès IP pour plus d'informations sur les différents types d'ACL pris en charge par le logiciel Cisco IOS et sur les méthodes de configuration et de modification des ACL.

La syntaxe des commandes applicables aux listes de contrôle d'accès standard est la suivante : **access-list access-list-number {permit|deny} {host|source source-wildcard|quels}**.

ACLs standard comparent l'adresse source des paquets IP aux adresses configurées dans l'ACL afin de contrôler le trafic.

ACLs étendu comparent la source et les adresses de destination des paquets IP aux adresses configurées dans l'ACL afin de contrôler le trafic. Vous pouvez également rendre les ACL étendues plus précises et les configurer pour le filtrage du trafic selon des critères tels que :

- Protocol
- Numéros de port
- Valeur de point de code de services différenciés (DSCP - Differentiated services code point)
- Valeur de priorité
- État du bit de numéro de séquence (SYN - Synchronize Sequence Number)

La syntaxe des commandes applicables aux ACL étendues est la suivante :

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
  {deny | permit} protocol source source-wildcard destination
    destination-wildcard
  [precedence precedence] [tos tos] [log | log-input]
    [time-range time-range-name][fragments]
```

Protocole ICMP (Internet Control Message Protocol)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit}
 icmp source source-wildcard destination destination-wildcard [icmp-type
 [icmp-code] | [icmp-message]] [precedenceprecedence] [tos tos] [log |
 log-input] [time-range time-range-name][fragments]
```

Protocole TCP (Transport Control Protocol)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp
 source source-wildcard [operator [port]] destination destination-wildcard
 [operator [port]] [established] [precedence precedence] [tos tos] [log |
 log-input] [time-range time-range-name][fragments]
```

Protocole UDP (User Datagram Protocol)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp
 source source-wildcard [operator [port]] destination destination-wildcard
 [operator [port]] [precedence precedence] [tos tos] [log | log-input]
 [time-range time-range-name][fragments]
```

Conditions préalables

Exigences

Assurez-vous que vous répondez aux exigences suivantes avant d'essayer cette configuration :

- Compréhension de base de l'adressage IP

Reportez-vous à Adressage IP et division en sous-réseaux pour les nouveaux utilisateurs pour plus d'informations.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

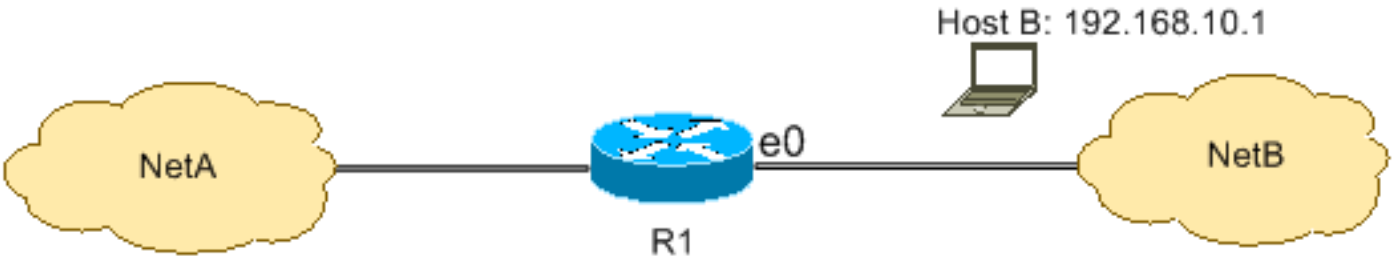
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurer

Ces exemples de configuration utilisent les ACL IP les plus fréquents.

Autoriser l'accès au réseau pour un hôte sélectionné

Cette figure illustre un hôte sélectionné disposant d'une autorisation d'accès au réseau. Tout trafic originaire de l'hôte B et destiné à NetA est autorisé, alors que tout autre trafic originaire de NetB et destiné à NetA est refusé.



La sortie indiquée dans le tableau R1 montre comment le réseau autorise l'accès à l'hôte. Cette sortie indique les éléments suivants :

- La configuration autorise uniquement l'accès à l'hôte portant l'adresse IP 192.168.10.1 sur l'interface Ethernet 0 sur R1.
- Cet hôte a accès aux services IP de NetA.
- Aucun autre hôte de NetB ne dispose d'un accès à NetA.
- Aucune déclaration de refus n'est configurée dans l'ACL.

Par défaut, une clause implicite de refus se trouve à la fin de chaque ACL. Tout ce qui n'est pas explicitement autorisé est refusé.

R1

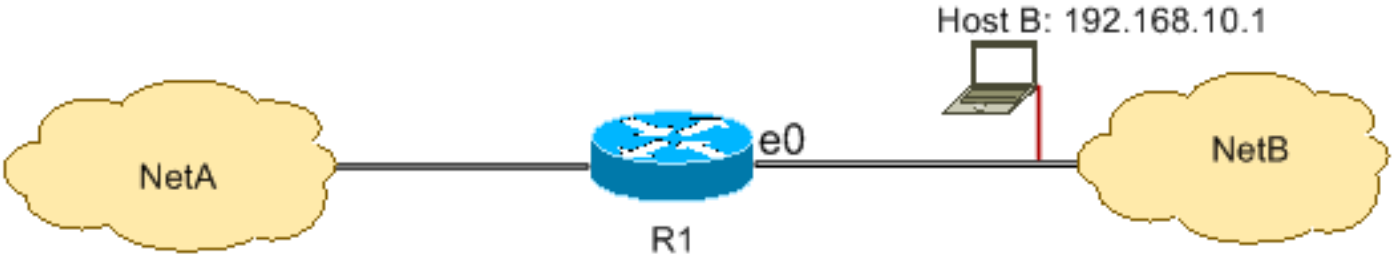
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> **Note**: L'ACL filtre les paquets IP de NetB à NetA, à l'exception des paquets originaires de NetB. On permet encore des paquets originaires de l'hôte B à NetA.

> **Note**: L'ACL **access-list 1 permit 192.168.10.1 0.0.0.0** représente une autre méthode de configuration de la même règle.

Refuser l'accès au réseau pour un hôte sélectionné

Cette figure montre que le trafic originaire de l'hôte B et destiné à NetA est refusé, alors que tout autre trafic originaire de NetB et destiné à accéder à NetA est autorisé.



Cette configuration refuse tous les paquets de l'hôte 192.168.10.1/32 via Ethernet 0 sur R1 et autorise tout le reste. Vous devez utiliser la commande **access list 1 permit any** pour autoriser explicitement tout le reste, parce qu'il existe une clause implicite de refus dans chaque ACL.

R1

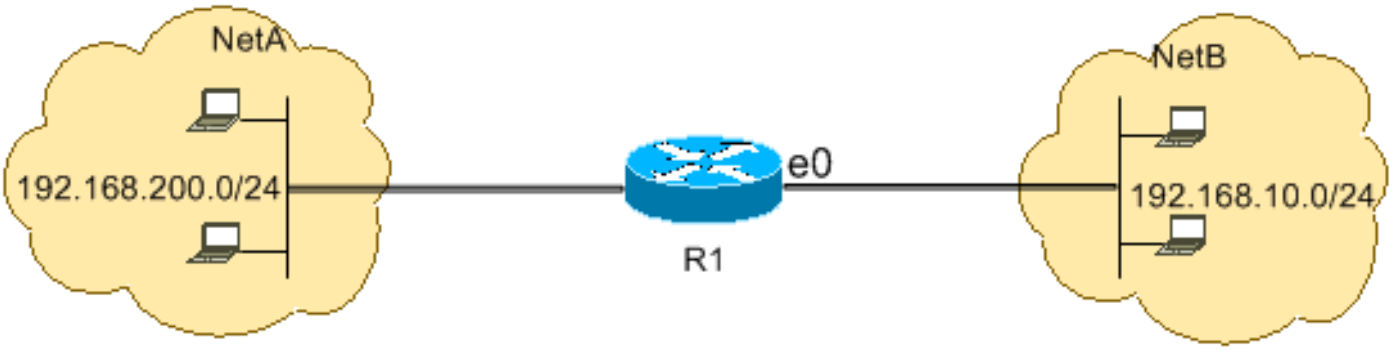
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

> **Note**: L'ordre des déclarations est essentiel pour le bon fonctionnement d'une ACL. Si l'ordre des entrées est inversé, comme l'illustre cette commande, la première ligne correspond à l'adresse source de chaque paquet. Par conséquent, l'ACL n'empêche pas l'hôte 192.168.10.1/32 d'accéder à NetA.

```
access-list 1 permit any
   access-list 1 deny host 192.168.10.1
```

Autoriser l'accès à une plage d'adresses IP contiguës

Cette figure montre que tous les hôtes de NetB portant l'adresse réseau 192.168.10.0/24 peuvent accéder au réseau 192.168.200.0/24 dans NetA.



Cette configuration autorise l'accès à NetA des paquets IP portant une en-tête IP avec une adresse source comprise dans le réseau 192.168.10.0/24 et une adresse de destination comprise dans le réseau 192.168.200.0/24. Il y a une clause implicite de refus en fin d'ACL qui refuse l'accès à tout autre trafic via Ethernet 0 sur R1.

R1

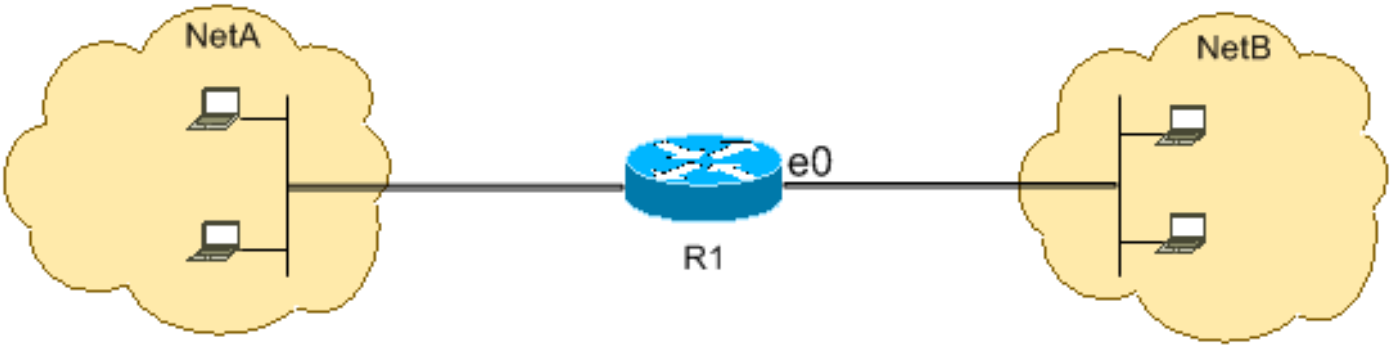
```
hostname R1
!
interface ethernet0
ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0  0.0.0.255
  192.168.200.0  0.0.0.255
```

> **Note**: Dans la commande **access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255**, "0.0.0.255" est le masque réseau 192.168.10.0 inversé par rapport au masque 255.255.255.0. Les ACL utilisent le masque inversé pour savoir quel nombre de bits de l'adresse réseau doit correspondre. Dans ce tableau, l'ACL autorise l'accès de tous les hôtes portant des adresses source comprises dans le réseau 192.168.10.0/24 et des adresses de destination comprises dans le réseau 192.168.200.0/24.

Reportez-vous à la section Masques de la rubrique Configurer des listes d'accès IP pour plus d'informations sur le masque d'une adresse réseau et sur la méthode de calcul de masque inversé requis par les ACL.

Refuser le trafic Telnet (TCP, port 23)

Afin de résoudre les problèmes de sécurité graves, vous pouvez être amené à désactiver l'accès Telnet à votre réseau privé à partir du réseau public. Cette figure montre comment le trafic Telnet de NetB (public) destiné à NetA (privé) est refusé, ce qui permet à NetA de lancer et d'établir une session Telnet avec NetB tandis que tout autre trafic IP est autorisé.



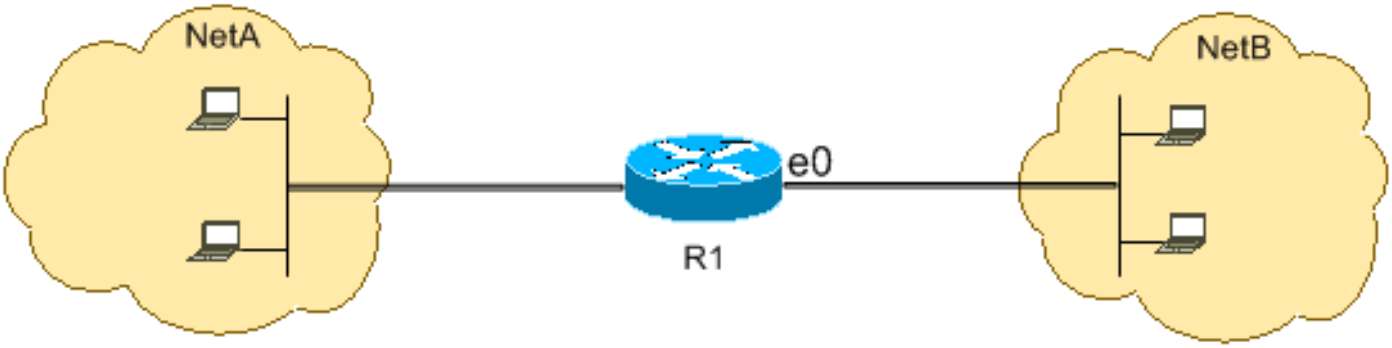
Telnet utilise TCP, port 23. Cette configuration montre que tout le trafic TCP destiné à NetA pour le port 23 est bloqué, et que tout autre trafic IP est autorisé.

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

Autoriser les réseaux internes uniquement pour le lancement d'une session TCP

Cette figure montre que le trafic TCP originaire de NetA et destiné à NetB est autorisé, alors que le trafic TCP originaire de NetB et destiné à NetA est refusé.



Dans cet exemple, l'objectif de l'ACL est le suivant :

- Autoriser les hôtes de NetA de lancer et d'établir une session TCP avec les hôtes de NetB.
- Empêcher les hôtes de NetB de lancer et d'établir une session TCP destinée aux hôtes de NetA.

Cette configuration permet à un datagramme de passer par l'nterface Ethernet 0 sur R1 quand le datagramme possède les caractéristiques suivantes :

- Bits ACK (confirmés) ou RST (réinitialisés) définis (indiquant une session TCP établie)
- Une valeur de port de destination supérieure à 1023

R1

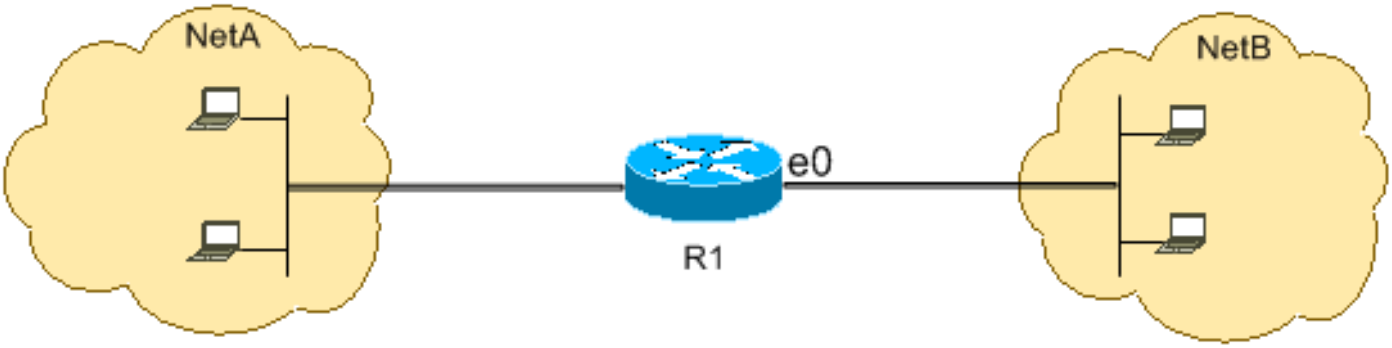
```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Puisque la plupart des ports connus au niveau des services IP utilisent des valeurs inférieures à 1023, tout datagramme dont le port de destination est inférieur à 1023 ou dont le bit ACK/RST n'est pas défini est refusé par l'ACL 102. Par conséquent, quand un hôte de NetB lance une connexion TCP via l'envoi du premier paquet TCP (sans bit de synchronisation/démarrage SYN/RST défini) pour un numéro de port inférieur à 1023, celle-ci est refusée et la session TCP échoue. Les sessions TCP lancées à partir de NetA et destinées à NetB sont autorisées, car le bit ACK/RST a été défini en vue du retour de paquets et de l'utilisation de valeurs de port supérieures à 1023.

Reportez-vous à RFC 1700 pour obtenir la liste complète des ports.

Refuser le trafic FTP (TCP, port 21)

Cette figure montre que le trafic FTP (TCP, port 21) et le trafic de données FTP (port 20) originaires de NetB et destinés à NetA sont refusés, tandis que tout autre trafic est autorisé.



FTP utilise le port 21 et le port 20. Le trafic TCP destiné au port 21 et au port 20 est refusé, et tout le reste est explicitement autorisé.

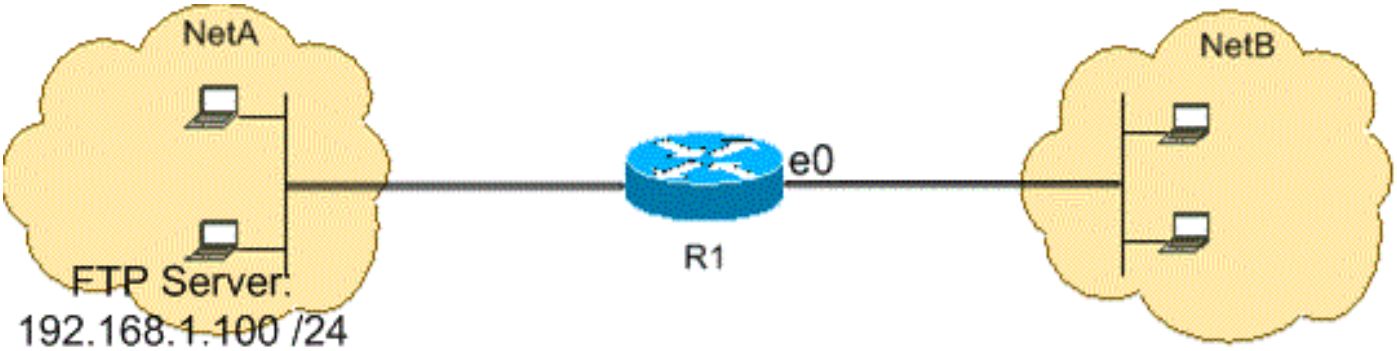
R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

Autoriser le trafic FTPc (FTP actif)

FTP peut fonctionner dans deux modes différents, appelés mode actif et mode passif. Reportez-vous à Fonctionnement FTP pour comprendre comment fonctionnent les modes FTP actif et passif.

Lorsque FTP fonctionne en mode actif, le serveur FTP utilise le port 21 pour le contrôle et le port 20 pour les données. Le serveur FTP (192.168.1.100) est situé dans NetA. Cette figure montre que le trafic FTP (TCP, port 21) et le trafic de données FTP (port 20) originaires de NetB et destinés au serveur FTP (192.168.1.100) sont autorisés, tandis que tout autre trafic IP est refusé.



R1

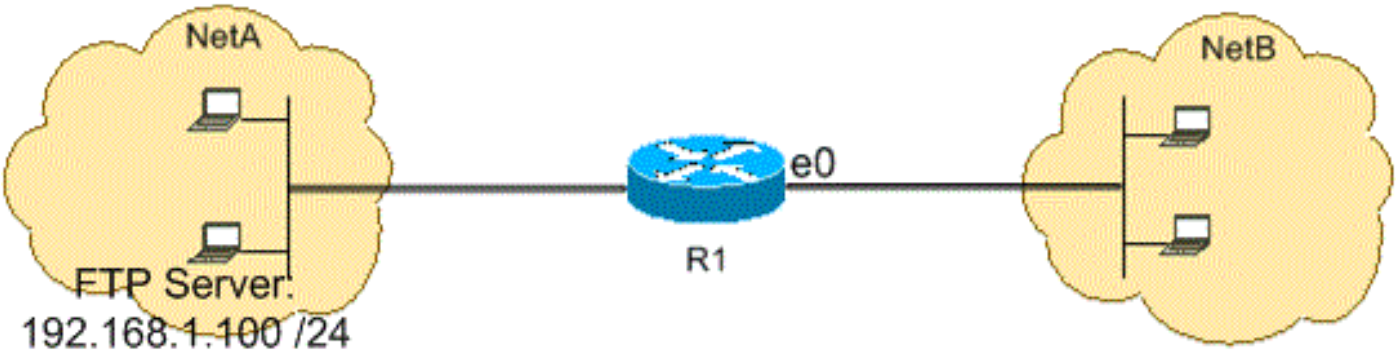
```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
```

```
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any
```

Autoriser le trafic FTP (FTP passif)

FTP peut fonctionner dans deux modes différents, appelés mode actif et mode passif. Reportez-vous à Fonctionnement FTP afin de comprendre comment fonctionnent les modes FTP actif et passif.

Lorsque FTP fonctionne en mode passif, le serveur FTP utilise le port 21 pour le contrôle et les ports dynamiques supérieurs ou égaux à 1024 pour les données. Le serveur FTP (192.168.1.100) est situé dans NetA. Cette figure montre que le trafic FTP (TCP, port 21) et le trafic de données FTP (ports supérieurs ou égaux à 1024) originaires de NetB et destinés au serveur FTP (192.168.1.100) sont autorisés, alors que tout autre trafic IP est refusé.

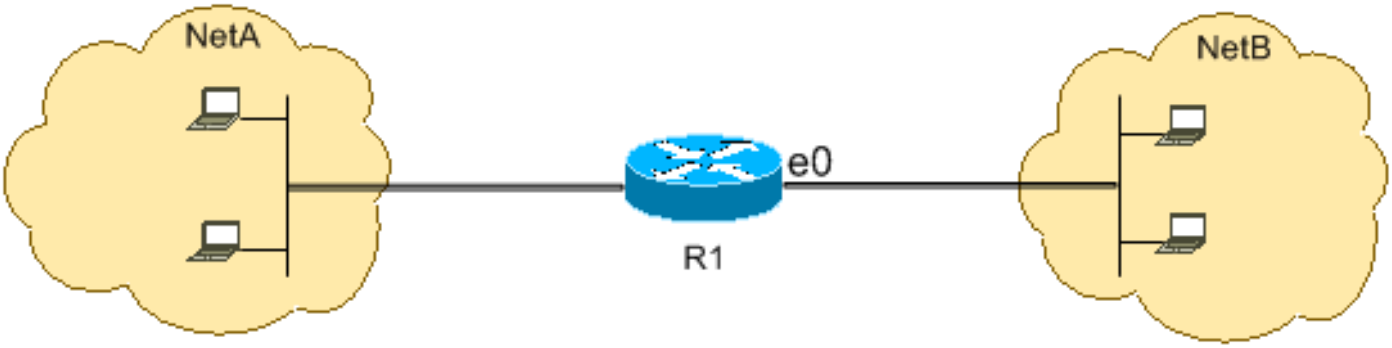


R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established
```

Autoriser les commandes ping (ICMP)

Cette figure montre que le trafic ICMP originaire de NetA et destiné à NetB est autorisé, et que les commandes Ping originaires de NetB et destinées à NetA sont refusées.



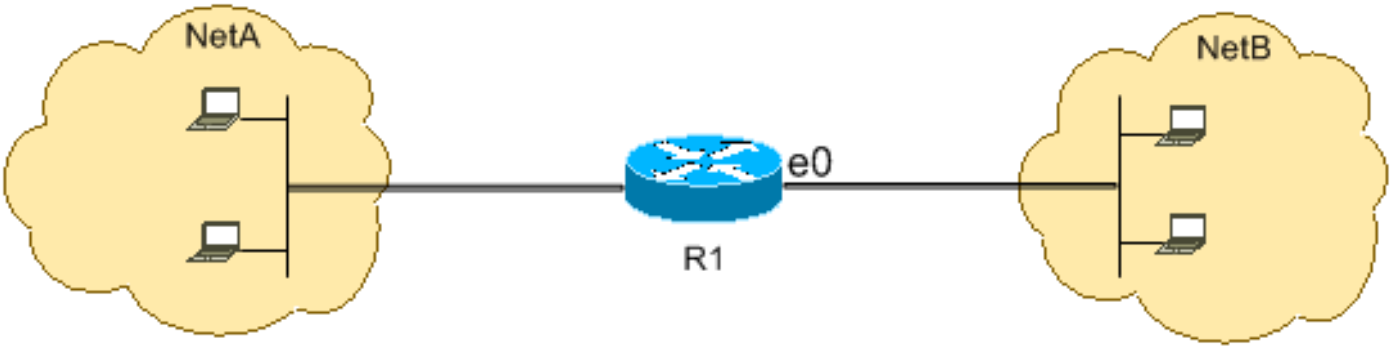
Cette configuration autorise uniquement les paquets à réponse d'écho (réponse ping) à entrer dans l'interface Ethernet 0 de NetB vers NetA. En revanche, elle bloque tous les paquets ICMP à requête d'écho lorsque les commandes ping sont originaires de NetB et destinées à NetA. Par conséquent, les hôtes de NetA peuvent utiliser les commandes Ping sur les hôtes de NetB, alors que les hôtes de NetB ne peuvent pas faire de même avec les hôtes de NetA.

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

Autoriser le trafic HTTP, Telnet, e-mail, POP3, FTP

Cette figure montre que seul le trafic HTTP, Telnet, SMTP (Simple Mail Transfer Protocol), POP3 et FTP est autorisé, et que le reste du trafic originaire de NetB et destiné à NetA est refusé.



Cette configuration autorise le trafic TCP dont les valeurs de port de destination correspondent à WWW (port 80), Telnet (port 23), SMTP (port 25), POP3 (port 110), FTP (port 21) ou données FTP (port 20). Notez qu'une clause implicite de refus figure à la fin des ACL, qui a pour effet de refuser tout trafic ne correspondant pas aux clauses d'autorisation.

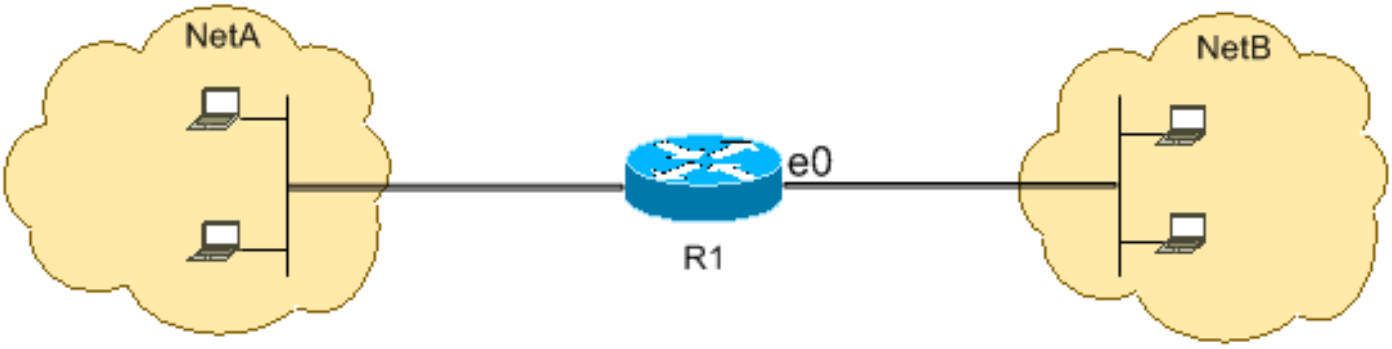
R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
```

```
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

Autoriser le trafic DNS

Cette figure montre que seul le trafic DNS (Domain Name System) est autorisé, et que le reste du trafic originaire de NetB et destiné à NetA est refusé.



Cette configuration autorise le trafic TCP dont la valeur de port de destination est 53. La clause implicite de refus figurant à la fin des ACL a pour effet de refuser tout autre trafic ne correspondant pas aux clauses d'autorisation.

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 112 permit udp any any eq domain
access-list 112 permit udp any eq domain any
access-list 112 permit tcp any any eq domain
access-list 112 permit tcp any eq domain any
```

Autoriser les mises à jour du routage

Lorsque vous vous appliquez une ACL entrante à une interface, assurez-vous que les mises à jour de routage ne sont pas filtrées. Utilisez l'ACL appropriée parmi celles de cette liste pour autoriser les paquets du protocole de routage :

Sélectionnez cette commande afin de permettre le Protocole RIP (Routing Information Protocol) :

```
access-list 102 permit udp any any eq rip
```

Sélectionnez cette commande afin de permettre le Protocole IGRP (Interior Gateway Routing Protocol) :

```
access-list 102 permit igrp any any
```

Sélectionnez cette commande afin de permettre l'Enhanced IGRP (EIGRP) :

```
access-list 102 permit eigrp any any
```

Sélectionnez cette commande afin de permettre le Protocole OSPF (Open Shortest Path First) :

```
access-list 102 permit ospf any any
```

Sélectionnez cette commande afin de permettre le Protocole BGP (Border Gateway Protocol) :

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```

Effectuer le débogage du traffic sur la base de l'ACL

L'utilisation des commandes de **débogage** exige l'allocation de ressources système telles que mémoire et capacité de traitement ; dans des situations extrêmes, cela peut faire caler un système très chargé. Utilisez les commandes de **débogage**avec prudence. Utilisez une ACL afin de définir sélectivement le trafic devant être examiné, afin de diminuer l'impact de la commande thedebug. Ce type de configuration ne filtre aucun paquet.

Cette configuration active la commande **debug ip packet** uniquement pour les paquets entre les hôtes 10.1.1.1 et 172.16.1.1.

```
R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
   R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
   R1(config)#end
   R1#debug ip packet 199 detail
   IP packet debugging is on (detailed) for access list 199
```

Reportez-vous à Informations importantes sur les commandes de débogage pour plus d'informations sur l'impact des commandes de débogage.

Reportez-vous à la section Utilisation de la commande de débogage de la rubrique Compréhension des commandes Ping et traceroute pour plus d'informations sur l'utilisation des ACL avec les commandes de **débogage**.

Filtrage des adresses MAC

Vous pouvez filtrer des trames avec une adresse d'origine ou de destination Mac spécifique. Vous pouvez configurer dans le système le nombre souhaité d'adresses, sans baisse de performances. Afin de filtrer par adresse Mac, utilisez cette commande en mode de configuration globale :

```
Router#config terminal
       bridge irb
       bridge 1 protocol ieee
       bridge 1 route ip
```

Appliquez le protocole de pont à une interface pour laquelle vous avez besoin de filtrer le trafic, grâce à la liste d'accès créée :

```
Router#int fa0/0
       no ip address
       bridge-group 1 {input-address-list 700 | output-address-list 700}
       exit
```

Créez une interface virtuelle de pont, puis appliquez l'adresse IP assignée à l'interface Ethernet :

```
Router#int bvi1
       ip address
       exit
!
!
       access-list 700 deny <mac address> 0000.0000.0000
       access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

Avec cette configuration, le routeur autorise uniquement les adresses MAC configurées sur l'access-list 700. Avec la liste d'accès, vous pouvez refuser les adresses MAC qui ne peuvent pas avoir accès et autoriser tout le reste.

> **Note**: Créez chaque ligne de la liste d'accès pour chaque adresse MAC.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Configuration des listes d'accès IP
- Access Lists Support Page
- Page de support pour le routage IP
- Page d'assistance pour les protocoles de routage IP
- Support et documentation techniques - Cisco Systems