Configuration des listes d'accès IP

Contenu

Introduction

Ce document décrit comment les listes de contrôle d'accès (ACL) IP peuvent filtrer le trafic sur le réseau. Il contient également de brèves descriptions des types de listes de contrôle d'accès IP, de la disponibilité des fonctionnalités et un exemple d'utilisation sur un réseau.

Accédez à l'outil de conseiller de logiciel (clients enregistrés seulement) afin de déterminer le support de certaines des fonctionnalités d'ACL plus avancées IP de Cisco IOS®.

La RFC 1700 contient les numéros affectés de ports connus. La RFC 1918 contient l'attribution d'adresse pour les sites Internet privés, les adresses IP qui ne devraient normalement pas apparaître sur Internet.

Remarque: il est également possible d'utiliser les listes de contrôle d'accès à des fins autres que le filtrage du trafic IP, par exemple pour définir le trafic pour la traduction d'adresses réseau (NAT) ou le chiffrement, ou pour filtrer des protocoles non-IP, par exemple AppleTalk ou IPX. Une discussion relative à ces fonctions sort du cadre de ce document.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document. Les concepts discutés sont présents dans des versions de logiciel 8.3 ou ultérieures de Cisco IOS®. Ceci est noté sous chaque fonctionnalité de liste d'accès.

Composants utilisés

Ce document traite de divers types de listes de contrôle d'accès. Certaines de ces dernières sont présentes puisque des versions du logiciel Cisco IOS 8.3 et autres ont été introduites dans des versions de logiciel ultérieures. Ceci est noté dans la discussion de chaque type.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Concepts relatifs aux listes de contrôle d'accès

Cette section décrit les concepts relatifs aux listes de contrôle d'accès.

Masques

Les masques sont employés avec des adresses IP dans les listes de contrôle d'accès IP pour spécifier ce qui doit être autorisé et refusé. Les masques permettant de configurer des adresses IP sur des interfaces commencent par 255 et ont les valeurs élevées du côté gauche, par exemple une adresse IP 209.165.202.129 avec un masque de 255.255.255.224. Les masques pour les listes de contrôle d'accès IP sont dans l'ordre inverse, par exemple le masque 0.0.0.255. Ce masque est parfois appelé masque inverse ou masque générique. Quand la valeur du masque est décomposée en binaire (0 et 1), les résultats déterminent les bits d'adresse qui doivent être pris

en compte dans le traitement du trafic. Un 0 indique que les bits d'adresse doivent être pris en compte (correspondance exacte) ; un 1 dans le masque revient à « ignorer ». Le tableau ci-dessous explique le concept.

Exemple de masque	
adresse réseau (trafic à traiter)	*10.1.1.0*
masque	*0.0.0.255*
adresse réseau (binaire)	*00001010.00000001.00000001.00000000*
masque (binaire)	*00000000.00000000.00000000.11111111*

Selon le masque binaire, vous pouvez voir que les trois premiers octets doivent correspondre exactement à l'adresse réseau binaire indiquée (00001010.00000001.00000001). Le dernier ensemble de nombres est à « ignorer » (.11111111). Par conséquent, tout le trafic qui commence par 10.1.1 correspond puisque le dernier octet est à « ignorer ». Par conséquent, avec ce masque, les adresses réseau 10.1.1.1 à 10.1.1.255 (10.1.1.x) sont traitées.

Soustrayez le masque normal de 255.255.255.255 afin de déterminer le masque inverse de liste de contrôle d'accès. Dans cet exemple, le masque inverse est déterminé pour l'adresse réseau 172.16.1.0 avec un masque normal de 255.255.255.0.

- 255.255.255.255 - 255.255.255.0 (masque normal) = 0.0.0.255 (masque inverse)

Notez ces équivalents de liste de contrôle d'accès.

- L'équivalent source/source-wildcard de 0.0.0.0/255.255.255.255 signifie « quelconque ».
- L'équivalent source/générique de 10.1.1.2/0.0.0.0 est identique à « hôte 10.1.1.2 ».

Récapitulation des listes de contrôle d'accès

Remarque: les masques de sous-réseau peuvent également être représentés comme notation de longueur fixe. Par exemple, 192.168.10.0/24 représente 192.168.10.0 255.255.255.0.

Cette liste décrit comment récapituler une plage de réseaux en un seul réseau pour l'optimisation des listes de contrôle d'accès. Examinez les réseaux ci-dessous.

```
192.168.32.0/24
192.168.33.0/24
192.168.34.0/24
192.168.35.0/24
192.168.36.0/24
192.168.37.0/24
192.168.38.0/24
192.168.39.0/24
```

Les deux premiers octets et le dernier octet sont les mêmes pour chaque réseau. Le tableau ci-dessous explique comment les récapituler en un seul réseau.

Le troisième octet pour les réseaux précédents peut être écrit comme indiqué dans ce tableau, selon la position de bit d'octet et la valeur d'adresse pour chaque bit.

Décimal	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1
	M	M	M	M	M	D	D	D

Puisque les cinq premiers bits correspondent, les huit réseaux précédents peuvent être récapitulés en un réseau (192.168.32.0/21 ou 192.168.32.0 255.255.248.0). Chacune des huit combinaisons possibles des trois bits de poids faible est appropriée pour les plages de réseaux en question. Cette commande définit une liste de contrôle d'accès qui autorise ce réseau. Si vous soustrayez 255.255.248.0 (masque normal) de 255.255.255.255, le résultat est 0.0.7.255.

```
access-list acl_permit permit ip 192.168.32.0 0.0.7.255
```

Examinez cet ensemble de réseaux pour plus d'explications.

```
access-list acl_permit permit ip 192.168.32.0 0.0.7.255
```

Les deux premiers octets et le dernier octet sont les mêmes pour chaque réseau. Le tableau ci-dessous explique comment les récapituler.

Le troisième octet pour les réseaux précédents peut être écrit comme indiqué dans ce tableau, selon la position de bit d'octet et la valeur d'adresse pour chaque bit.

Décimal	128	64	32	16	8	4	2	1
146	1	0	0	1	0	0	1	0
147	1	0	0	1	0	0	1	1
148	1	0	0	1	0	1	0	0
149	1	0	0	1	0	1	0	1
	M	M	M	M	M	?	?	?

Àla différence de l'exemple précédent, vous ne pouvez pas récapituler ces réseaux en un seul réseau. S'ils sont récapitulés en un seul réseau, ils deviennent 192.168.144.0/21 parce que cinq bits sont semblables dans le troisième octet. Ce réseau récapitulé, 192.168.144.0/21, couvre une plage de réseaux comprise entre 192.168.144.0 et 192.168.151.0. Parmi ces derniers, les réseaux 192.168.144.0, 192.168.145.0, 192.168.150.0 et 192.168.151.0 ne sont pas dans la liste des quatre réseaux donnée. Afin de couvrir les réseaux spécifiques en question, vous avez besoin

d'un minimum de deux réseaux récapitulés. Les quatre réseaux donnés peuvent être récapitulés dans ces deux réseaux :

- Pour les réseaux 192.168.146.x et 192.168.147.x, tous les bits correspondent à l'exception du dernier, qui est à « ignorer ». Il peut être écrit comme 192.168.146.0/23 (ou 192.168.146.0 255.255.254.0).
- Pour les réseaux 192.168.148.x et 192.168.149.x, tous les bits correspondent à l'exception du dernier, qui est à « ignorer ». Il peut être écrit comme 192.168.148.0/23 (ou 192.168.148.0 255.255.254.0).

Cette sortie définit une liste de contrôle d'accès récapitulée pour les réseaux ci-dessus.

```
!--- This command is used to allow access access for devices with IP !--- addresses in the range
from 192.168.146.0 to 192.168.147.254. access-list 10 permit 192.168.146.0 0.0.1.255
```

```
!--- This command is used to allow access access for devices with IP !--- addresses in the range
from 192.168.148.0 to 192.168.149.254 access-list 10 permit 192.168.148.0 0.0.1.255
```

Traiter les listes de contrôle d'accès

Le trafic qui entre dans le routeur est comparé aux entrées de la liste de contrôle d'accès basées sur l'ordre dans lequel les entrées arrivent dans le routeur. De nouvelles instructions sont ajoutées à la fin de la liste. Le routeur continue de chercher jusqu'à ce qu'il trouve une correspondance. Si aucune correspondance n'est trouvée quand le routeur atteint la fin de la liste, le trafic est refusé. Pour cette raison, vous devez avoir les entrées fréquemment consultées en haut de la liste. Il existe un refus implicite pour le trafic qui n'est pas autorisé. Une liste de contrôle d'accès d'entrée unique avec une seule entrée de refus aboutit à un refus de tout le trafic. Vous devez avoir au moins une instruction d'autorisation dans une liste de contrôle d'accès ou tout le trafic est bloqué. Ces deux listes de contrôle d'accès (101 et 102) ont le même effet.

```
!--- This command is used to permit IP traffic from 10.1.1.0 !--- network to 172.16.1.0 network.
All packets with a source !--- address not in this range will be rejected. access-list 101
permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
!--- This command is used to permit IP traffic from 10.1.1.0 !--- network to 172.16.1.0 network.
All packets with a source !--- address not in this range will be rejected. access-list 102
permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

Dans cet exemple, la dernière entrée est suffisante. Vous n'avez pas besoin des trois premières entrées parce que TCP inclut Telnet, et IP inclut TCP, UDP (User Datagram Protocol) et ICMP (Internet Control Message Protocol).

```
!--- This command is used to permit Telnet traffic !--- from machine 10.1.1.2 to machine
```

```
172.16.1.1. access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet


!--- This command is used to permit tcp traffic from !--- 10.1.1.2 host machine to 172.16.1.1
host machine. access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1


!--- This command is used to permit udp traffic from !--- 10.1.1.2 host machine to 172.16.1.1
host machine. access-list 101 permit udp host 10.1.1.2 host 172.16.1.1


!--- This command is used to permit ip traffic from !--- 10.1.1.0 network to 172.16.1.10
network. access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

Définir les ports et les types de messages

Outre la définition de la source et de la destination des listes de contrôle d'accès, il est possible de définir les ports, les types de messages ICMP et d'autres paramètres. Une source utile d'informations pour les ports connus est la RFC 1700. Les types de messages ICMP sont décrits dans la RFC 792.

Le routeur peut afficher un texte descriptif sur certains des ports connus. Utilisez un **?** pour obtenir de l'aide.

```
access-list 102 permit tcp host 10.1.1.1 host 172.16.1.1 eq ?
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
```

Pendant la configuration, le routeur convertit également des valeurs numériques en valeurs plus conviviales. Voici un exemple où vous tapez la valeur numérique du type de message ICMP, ce qui fait que le routeur convertit la valeur numérique en un nom.

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 14
```

devient

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 timestamp-reply
```

Appliquer les listes de contrôle d'accès

Vous pouvez définir des listes de contrôle d'accès sans les appliquer. Toutefois, les listes de contrôle d'accès n'ont aucun effet tant qu'elles ne sont pas appliquées à l'interface du routeur. Il est judicieux d'appliquer la liste de contrôle d'accès sur l'interface la plus proche de la source du trafic. Comme illustré dans cet exemple, quand vous essayez de bloquer le trafic de la source à la destination, vous pouvez appliquer une liste de contrôle d'accès entrante à E0 sur le routeur A au

lieu d'une liste sortante à E1 sur le routeur C. Une liste d'accès a une entrée **deny ip any any** implicitement à la fin de n'importe quelle liste d'accès. Si le trafic est lié à une demande DHCP et qu'il n'est pas explicitement autorisé, le trafic est abandonné parce que, quand vous examinez la demande DHCP dans IP, l'adresse source est s=0.0.0.0 (Ethernet1/0), d=255.255.255.255, len 604, rcvd 2 UDP src=68, dst=67. Notez que l'adresse IP source est 0.0.0.0 et l'adresse de destination est 255.255.255.255. Le port source est 68 et le port de destination 67. Par conséquent, vous devez autoriser ce type de trafic dans votre liste d'accès, sinon le trafic est abandonné en raison d'un refus implicite à la fin de l'instruction.

Remarque: Pour que le trafic UDP puisse passer, il doit également être autorisé explicitement par la liste de contrôle d'accès.

Définir les termes interne, externe, entrant, sortant, source et destination

Le routeur utilise les termes interne, externe, source et destination comme références. Le trafic sur le routeur peut être comparé au trafic sur l'autoroute. Si vous étiez un officier de police en Pennsylvanie et vouliez arrêter un camion allant du Maryland à New York, la source du camion est le Maryland et sa destination est New York. Le barrage de la route pourrait être appliqué à la frontière Pennsylvanie-New York (externe) ou Maryland–Pennsylvanie (interne).

Quand vous faites référence à un routeur, ces termes ont les significations suivantes.

- **Externe** : trafic qui est déjà passé par le routeur et quitte l'interface. La source est l'endroit où il était, de l'autre côté du routeur, et la destination est l'endroit où il va.
- **Interne** : trafic qui arrive sur l'interface, puis passe par le routeur. La source est l'endroit où il était et la destination est l'endroit où il va, de l'autre côté du routeur.
- **Entrant** : si la liste d'accès est entrante, quand le routeur reçoit un paquet, le logiciel Cisco IOS recherche une correspondance dans les instructions de critères de la liste d'accès. Si le paquet est autorisé, le logiciel continue de le traiter. Si le paquet est refusé, le logiciel ignore le paquet.
- **Sortant** : si la liste d'accès est sortante, une fois que le logiciel a reçu un paquet et l'a routé vers l'interface sortante, il recherche une correspondance dans les instructions de critères de la liste d'accès. Si le paquet est autorisé, le logiciel le transmet. Si le paquet est refusé, le logiciel ignore le paquet.

La liste de contrôle d'accès interne a une source sur un segment de l'interface à laquelle elle est appliquée et une destination hors de tout autre interface. La liste de contrôle d'accès externe a une source sur un segment d'une interface autre que celle à laquelle elle est appliquée et une destination hors de l'interface à laquelle elle est appliquée.

Modifier les listes de contrôle d'accès

Lorsque vous modifiez une liste de contrôle d'accès, vous devez être particulièrement vigilant. Par exemple, si vous avez l'intention de supprimer une ligne spécifique d'une liste de contrôle d'accès numérotée qui existe comme illustré ici, toute la liste est supprimée.

```
!--- The access-list 101 denies icmp from any to any network !--- but permits IP traffic from
any to any network. router#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  router(config)#access-list 101 deny icmp any any
  router(config)#access-list 101 permit ip any any
  router(config)#^Z

  router#show access-list
  Extended IP access list 101
      deny icmp any any
      permit ip any any
  router#
  *Mar  9 00:43:12.784: %SYS-5-CONFIG_I: Configured from console by console

  router#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  router(config)#no access-list 101 deny icmp any any
  router(config)#^Z

  router#show access-list
  router#
  *Mar  9 00:43:29.832: %SYS-5-CONFIG_I: Configured from console by console
```

Copiez la configuration du routeur sur un serveur TFTP ou un éditeur de texte, tel que le Bloc-notes, afin de modifier des listes de contrôle d'accès numérotées. Apportez ensuite toutes les modifications nécessaires et recopiez la configuration sur le routeur.

Vous pouvez également procéder ainsi.

```
router#configure terminal
  Enter configuration commands, one per line.
  router(config)#ip access-list extended test
  !--- Permits IP traffic from 2.2.2.2 host machine to 3.3.3.3 host machine. router(config-ext-
nacl)#permit ip host 2.2.2.2 host 3.3.3.3
  !--- Permits www traffic from 1.1.1.1 host machine to 5.5.5.5 host machine. router(config-ext-
nacl)#permit tcp host 1.1.1.1 host 5.5.5.5 eq www
  !--- Permits icmp traffic from any to any network. router(config-ext-nacl)#permit icmp any any
  !--- Permits dns traffic from 6.6.6.6 host machine to 10.10.10.0 network. router(config-ext-
nacl)#permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq domain
  router(config-ext-nacl)#^Z
  1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l

  router#show access-list
  Extended IP access list test
      permit ip host 2.2.2.2 host 3.3.3.3
      permit tcp host 1.1.1.1 host 5.5.5.5 eq www
      permit icmp any any
      permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq domain
```

Toutes les suppressions sont retirées de la liste de contrôle d'accès et tous les ajouts sont apportés à la fin de la liste de contrôle d'accès.

```
router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#ip access-list extended test
   !--- ACL entry deleted. router(config-ext-nacl)#no permit icmp any any
   !--- ACL entry added. router(config-ext-nacl)#permit gre host 4.4.4.4 host 8.8.8.8
   router(config-ext-nacl)#^Z
   1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l
```

```
router#show access-list
Extended IP access list test
    permit ip host 2.2.2.2 host 3.3.3.3
    permit tcp host 1.1.1.1 host 5.5.5.5 eq www
    permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq domain
    permit gre host 4.4.4.4 host 8.8.8.8
```

Vous pouvez également ajouter des lignes de liste de contrôle d'accès à des listes de contrôle d'accès standard ou étendues numérotées par numéro de séquence dans Cisco IOS. Voici un exemple de la configuration :

Configurez la liste de contrôle d'accès étendue de la façon suivante :

```
Router(config)#access-list 101 permit tcp any any
Router(config)#access-list 101 permit udp any any
Router(config)#access-list 101 permit icmp any any
Router(config)#exit
Router#
```

Émettez la commande **show access-list** afin de visualiser les entrées de la liste de contrôle d'accès. Les numéros de séquence tels que 10, 20 et 30 apparaissent également ici.

```
Router#show access-list
Extended IP access list 101
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
```

Ajoutez l'entrée pour la liste d'accès 101 avec le numéro de séquence 5.

Exemple 1 :

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#5 deny tcp any any eq telnet
Router(config-ext-nacl)#exit
Router(config)#exit
Router#
```

Dans la sortie de la commande **show access-list**, la liste de contrôle d'accès avec le numéro de séquence 5 est ajoutée comme première entrée à la liste d'accès 101.

```
Router#show access-list
Extended IP access list 101
    5 deny tcp any any eq telnet
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
Router#
```

Exemple 2 :

```
internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.162.2.9
```

```
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any

internetrouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
internetrouter(config)#ip access-list extended 101
internetrouter(config-ext-nacl)#18 per tcp any host 172.162.2.11
internetrouter(config-ext-nacl)#^Z

internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.162.2.9
    18 permit tcp any host 172.162.2.11
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any
internetrouter#
```

De même, vous pouvez configurer la liste d'accès standard de la façon suivante :

```
internetrouter(config)#access-list 2 permit 172.16.1.2
internetrouter(config)#access-list 2 permit 172.16.1.10
internetrouter(config)#access-list 2 permit 172.16.1.11

internetrouter#show access-lists
Standard IP access list 2
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    10 permit 172.16.1.2

internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#25 per 172.16.1.7
internetrouter(config-std-nacl)#15 per 172.16.1.16

internetrouter#show access-lists
Standard IP access list 2
    15 permit 172.16.1.16
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    25 permit 172.16.1.7
    10 permit 172.16.1.2
```

La principale différence dans une liste d'accès standard est que Cisco IOS ajoute une entrée par ordre décroissant de l'adresse IP, et non sur un numéro de séquence.

Cet exemple illustre les différentes entrées, par exemple comment autoriser une adresse IP (192.168.100.0) ou les réseaux (10.10.10.0).

```
internetrouter#show access-lists
Standard IP access list 19
    10 permit 192.168.100.0
    15 permit 10.10.10.0, wildcard bits 0.0.0.255
    19 permit 201.101.110.0, wildcard bits 0.0.0.255
    25 deny any
```

Ajoutez l'entrée dans la liste d'accès 2 afin d'autoriser l'adresse IP 172.22.1.1 :

```
internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#18 permit 172.22.1.1
```

Cette entrée est ajoutée en haut de la liste afin de donner la priorité à l'adresse IP spécifique plutôt qu'au réseau.

```
internetrouter#show access-lists
Standard IP access list 19
    10 permit 192.168.100.0
    18 permit 172.22.1.1
    15 permit 10.10.10.0, wildcard bits 0.0.0.255
    19 permit 201.101.110.0, wildcard bits 0.0.0.255
    25 deny   any
```

Remarque: Les listes de contrôle d'accès précédentes ne sont pas prises en charge dans un dispositif de sécurité, tel que le pare-feu ASA/PIX.

Directives pour changer les listes d'accès quand elles sont appliquées à des cartes de chiffrement

- Si vous procédez à un ajout à une configuration de liste d'accès existante, il est inutile de supprimer la carte de chiffrement. En cas d'ajout direct sans suppression de la carte de chiffrement, cette opération est prise en charge et acceptable.
- Si vous devez modifier ou supprimer une entrée de liste d'accès à partir de listes d'accès existantes, vous devez supprimer la carte de chiffrement de l'interface. Après avoir supprimé la carte de chiffrement, apportez toutes les modifications nécessaires à la liste d'accès et ajoutez à nouveau la carte de chiffrement. Si vous apportez des modifications telles que la suppression de la liste d'accès sans suppression de la carte de chiffrement, cette opération n'est pas prise en charge et peut avoir comme conséquence un comportement imprévisible.

Dépanner

Comment supprimer une liste de contrôle d'accès d'une interface ?

Passez en mode de configuration et entrez **no** devant la commande **access-group**, comme illustré dans cet exemple, afin de supprimer une liste de contrôle d'accès d'une interface.

```
interface <interface> no ip access-group <acl-number> in|out
```

Que faire quand trop de trafic est refusé ?

Si trop de trafic est refusé, étudiez la logique de votre liste ou essayez de définir et d'appliquer une autre liste plus importante. La commande **show ip access-lists** fournit un nombre de paquets qui indique l'entrée de la liste de contrôle d'accès consultée.

Le mot clé **log** à la fin des entrées individuelles de la liste de contrôle d'accès indique le numéro de la liste de contrôle d'accès et si le paquet a été autorisé ou refusé, en plus des informations spécifiques au port.

Remarque: Le mot clé **log-input** existe dans les versions du logiciel Cisco IOS 11.2 et ultérieures, ainsi que dans certains logiciels basés sur Cisco IOS Version 11.1 créés spécifiquement pour le marché des fournisseurs de services. Des logiciels plus anciens ne prennent pas en charge ce mot clé. L'utilisation de ce mot clé inclut l'interface d'entrée et l'adresse MAC source le cas échéant.

Comment déboguer au niveau du paquet qui utilise un routeur Cisco ?

Cette procédure explique le processus de débogage. Avant de commencer, assurez-vous qu'aucune liste de contrôle d'accès n'est actuellement appliquée, qu'il existe une liste de contrôle d'accès et que la commutation rapide n'est pas désactivée.

Remarque: Faites très attention quand vous déboguez un système avec un trafic intense. Utilisez une liste de contrôle d'accès afin de déboguer un trafic spécifique. Toutefois, soyez sûr du processus et du flux de trafic.

1. Employez la commande **access-list** afin de capturer les données voulues.Dans cet exemple, la capture de données est définie pour l'adresse de destination 10.2.6.6 ou l'adresse source 10.2.6.6.

   ```
   access-list 101 permit ip any host 10.2.6.6
   access-list 101 permit ip host 10.2.6.6 any
   ```

2. Désactivez la commutation rapide sur les interfaces impliquées. Vous voyez seulement le premier paquet si la commutation rapide n'est pas désactivée.

   ```
   config interface
   no ip route-cache
   ```

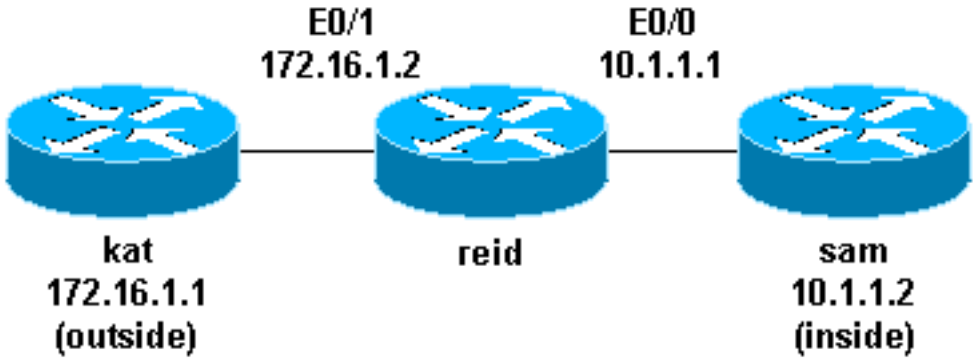
3. Utilisez la commande **terminal monitor** en mode enable afin d'afficher la sortie de la commande **debug** et les messages d'erreur système pour la session et le terminal actuels.
4. Utilisez la commande **debug ip packet 101** ou **debug ip packet 101 detail** afin de commencer le processus de débogage.
5. Exécutez la commande **no debug all** en mode enable et la commande **interface configuration** afin d'arrêter le processus de débogage.
6. Redémarrez la mise en cache.

   ```
   config interface
   ip route-cache
   ```

Types de listes de contrôle d'accès IP

Cette section du document décrit les types de listes de contrôle d'accès.

Diagramme du réseau



ACLs standard

Les listes de contrôle d'accès standard sont le plus ancien type de liste de contrôle d'accès. Elles remontent à l'époque du logiciel Cisco IOS Version 8.3. Les listes de contrôle d'accès standard contrôlent le trafic en comparant l'adresse source des paquets IP aux adresses configurées dans la liste de contrôle d'accès.

Voici le format de la syntaxe de commande d'une liste de contrôle d'accès standard.

```
access-list access-list-number {permit|deny} {host|source source-wildcard|any}
```

Dans toutes les versions de logiciel, *access-list-number* peut être compris entre 1 et 99. Dans le logiciel Cisco IOS Version 12.0.1, les listes de contrôle d'accès standard commencent à utiliser des nombres supplémentaires (1300 à 1999). Ces nombres supplémentaires sont désignés sous le nom de listes de contrôle d'accès IP développées. Le logiciel Cisco IOS Version 11.2 a ajouté la capacité d'utiliser le *nom* de liste dans les listes de contrôle d'accès standard.

Un paramètre *source/source-wildcard* de 0.0.0.0/255.255.255.255 peut être spécifié comme **any**. Le générique peut être omis s'il n'est composé que de zéros. Par conséquent, l'hôte 10.1.1.2 0.0.0.0 est identique à l'hôte 10.1.1.2.

Une fois que la liste de contrôle d'accès est définie, elle doit être appliquée à l'interface (entrante ou sortante). Dans les premières versions de logiciel, « out » était la valeur par défaut si aucun mot clé « out » ni « in » n'était spécifié. La direction a dû être spécifiée dans les versions de logiciel ultérieures.

```
interface <interface>
ip access-group number {in|out}
```

Voici un exemple de l'utilisation d'une liste de contrôle d'accès standard afin de bloquer tout le trafic, à l'exception de celui provenant de la source 10.1.1.x.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
access-list 1 permit 10.1.1.0 0.0.0.255
```

ACLs étendu

Les listes de contrôle d'accès étendues ont été introduites dans le logiciel Cisco IOS Version 8.3. Les listes de contrôle d'accès étendues contrôlent le trafic en comparant les adresses source et de destination des paquets IP aux adresses configurées dans la liste de contrôle d'accès.

Voici le format de la syntaxe de commande des listes de contrôle d'accès étendues. Les lignes sont ici renvoyées à la ligne pour des raisons d'espace.

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***]**

ICMP

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***] [precedence** *precedence***] [tos** *tos***] [log|log-input] [time-range** *time-range-name***]**

TCP

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***]**

UDP

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***]**

Dans des toutes les versions logicielles, l'*access-list-number* peut être de 100 à 199. Dans le logiciel Cisco IOS Version 12.0.1, les listes de contrôle d'accès étendues commencent à utiliser des nombres supplémentaires (2000 à 2699). Ces nombres supplémentaires sont désignés sous le nom de listes de contrôle d'accès IP développées. Le logiciel Cisco IOS Version 11.2 a ajouté la capacité d'utiliser le *nom* de liste dans les listes de contrôle d'accès étendues.

La valeur 0.0.0.0/255.255.255.255 peut être spécifiée comme **any**. Une fois que la liste de contrôle d'accès est définie, elle doit être appliquée à l'interface (entrante ou sortante). Dans les premières versions de logiciel, « out » était la valeur par défaut si aucun mot clé « out » ni « in » n'était spécifié. La direction a dû être spécifiée dans les versions de logiciel ultérieures.

interface <*interface***> ip access-group {***number|name***} {in|out}**

Cette liste de contrôle d'accès étendue est employée pour permettre le trafic sur le réseau 10.1.1.x (intérieur) et pour recevoir des réponses Ping de l'extérieur tout en empêchant des messages Ping non sollicités provenant de personnes de l'extérieur, ce qui autorise tout le reste du trafic.

```
interface Ethernet0/1
ip address 172.16.1.2 255.255.255.0
ip access-group 101 in
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo
```

```
access-list 101 permit ip any 10.1.1.0 0.0.0.255
```

Remarque: Certaines applications, telles que la gestion de réseau, nécessitent des messages Ping pour une fonction de conservation de connexion active. Si tel est le cas, vous pouvez limiter le blocage des messages Ping entrants ou être plus précis en ce qui concerne les IP autorisées/refusées.

Verrou et clé (listes de contrôle d'accès dynamiques)

La fonctionnalité de verrou et clé, également connue sous le nom de listes de contrôle d'accès dynamiques, a été introduite dans le logiciel Cisco IOS Version 11.1. Cette fonctionnalité dépend de Telnet, de l'authentification (locale ou à distance) et des listes de contrôle d'accès étendues.

La configuration de la fonctionnalité de verrou et clé démarre avec l'application d'une liste de contrôle d'accès étendue pour bloquer le trafic par le routeur. Les utilisateurs qui veulent traverser le routeur sont bloqués par la liste de contrôle d'accès étendue jusqu'à ce qu'ils établissent une connexion Telnet au routeur et soient authentifiés. La connexion Telnet est alors supprimée et une liste de contrôle d'accès dynamique d'entrée unique est ajoutée à la liste de contrôle d'accès étendue qui existe. Le trafic est ainsi autorisé pendant une période particulière ; des délais d'attente inactifs et absolus sont possibles.

Voici le format de la syntaxe de commande pour la configuration de la fonctionnalité de verrou et clé avec une authentification locale.

```
username user-name password password interface <interface> ip access-group {number|name}
{in|out}
```

La liste de contrôle d'accès d'entrée unique de cette commande est dynamiquement ajoutée à la liste de contrôle d'accès qui existe après authentification.

```
access-list access-list-number dynamic name {permit|deny} [protocol] {source source-
wildcard|any} {destination destination-wildcard|any} [precedence precedence][tos
tos][established] [log|log-input] [operator destination-port|destination port]

line vty line_range

login local
```

Voici un exemple de base de la fonctionnalité de verrou et clé.

```
username test password 0 test
!--- Ten (minutes) is the idle timeout. username test autocommand access-enable host timeout 10


interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip access-group 101 in

access-list 101 permit tcp any host 10.1.1.1 eq telnet
!--- 15 (minutes) is the absolute timeout. access-list 101 dynamic testlist timeout 15 permit ip
```

```
10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255


line vty 0 4
login local
```

Une fois que l'utilisateur sur 10.1.1.2 a établi une connexion Telnet à 10.1.1.1, la liste de contrôle d'accès dynamique est appliquée. La connexion est alors supprimée et l'utilisateur peut accéder au réseau 172.16.1.x.

Listes de contrôle d'accès nommées IP

Les listes de contrôle d'accès nommées IP ont été introduites dans le logiciel Cisco IOS Version 11.2. Ceci permet de donner des noms à la place des numéros aux listes de contrôle d'accès standard et étendues.

Voici le format de la syntaxe de commande pour les listes de contrôle d'accès nommées IP.

```
ip access-list {extended|standard} name
```

Voici un exemple TCP :

```
{permit|deny} tcp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]] [established] [precedence precedence] [tos tos] [log] [time-range time-range-
name]
```

Voici un exemple de l'utilisation d'une liste de contrôle d'accès nommée afin de bloquer tout le trafic, à l'exception de la connexion Telnet entre l'hôte 10.1.1.2 et l'hôte 172.16.1.1.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group in_to_out in

ip access-list extended in_to_out
permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

Listes de contrôle d'accès réflexives

Les listes de contrôle d'accès réflexives ont été introduites dans le logiciel Cisco IOS Version 11.3. Les listes de contrôle d'accès réflexives permettent de filtrer les paquets IP selon des informations de session de couche supérieure. Elles sont généralement employées pour autoriser le trafic sortant et pour limiter le trafic entrant en réponse aux sessions initialisées à l'intérieur du routeur.

Les listes de contrôle d'accès réflexives peuvent être définies seulement avec les listes de contrôle d'accès nommées IP étendues. Elles ne peuvent pas être définies avec des listes de contrôle d'accès nommées IP standard ou numérotées, ni avec d'autres listes de contrôle d'accès de protocole. Les listes de contrôle d'accès réflexives peuvent être utilisées en même temps que d'autres listes de contrôle d'accès étendues standard et statiques.

Voici la syntaxe pour différentes commandes de liste de contrôle d'accès réflexive.

```
interface
ip access-group {number|name} {in|out} ip access-list extended name permit protocol any any
reflect name [timeoutseconds] ip access-list extended name evaluate name
```

Voici un exemple d'autorisation du trafic sortant et entrant ICMP alors qu'en autorisant uniquement le trafic TCP initialisé de l'intérieur, le reste du trafic est refusé.

```
ip reflexive-list timeout 120

interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group inboundfilters in
 ip access-group outboundfilters out

ip access-list extended inboundfilters
permit icmp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
evaluate tcptraffic

!--- This ties the reflexive ACL part of the outboundfilters ACL, !--- called tcptraffic, to the
inboundfilters ACL. ip access-list extended outboundfilters
permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 reflect tcptraffic
```

Listes de contrôle d'accès basées sur l'heure utilisant des plages temporelles

Les listes de contrôle d'accès basées sur l'heure ont été introduites dans le logiciel Cisco IOS Version 12.0.1.T. Tout en étant semblables aux listes de contrôle d'accès étendues dans leur fonctionnement, elles autorisent un contrôle d'accès basé sur l'heure. Une plage temporelle est créée qui définit des heures spécifiques de la journée et de la semaine afin d'implémenter des listes de contrôle d'accès basées sur l'heure. La plage temporelle est identifiée par un nom et référencée par une fonction. Par conséquent, les restrictions horaires sont imposées à la fonction elle-même. La plage temporelle repose sur l'horloge système du routeur. L'horloge du routeur peut être utilisée, mais la fonctionnalité fonctionne de façon optimale avec la synchronisation du Protocole d'Heure Réseau (NTP).

Voici des commandes de liste de contrôle d'accès basée sur l'heure.

```
!--- Defines a named time range. time-range time-range-name
!--- Defines the periodic times. periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm
!--- Or, defines the absolute times. absolute [start time date] [end time date]
!--- The time range used in the actual ACL. ip access-list name|number
<extended_definition>time-rangename_of_time-range
```

Dans cet exemple, une connexion Telnet est autorisée de l'intérieur vers l'extérieur du réseau les lundi, mercredi et vendredi pendant les heures d'ouverture :

```
interface Ethernet0/0
```

```
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in

access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range EVERYOTHERDAY

time-range EVERYOTHERDAY
periodic Monday Wednesday Friday 8:00 to 17:00
```

Entrées de liste de contrôle d'accès IP commentées

Les entrées de listes de contrôle d'accès IP commentées ont été introduites dans le logiciel Cisco IOS Version 12.0.2.T Les commentaires facilitent la compréhension des listes de contrôle d'accès et peuvent être utilisés pour les listes de contrôle d'accès IP standard ou étendues.

Voici la syntaxe de commande pour les listes de contrôle d'accès nommées IP commentées.

```
ip access-list {standard|extended} access-list-name remark remark
```

Voici la syntaxe de commande pour les listes de contrôle d'accès IP numérotées commentées.

```
access-list access-list-number remark remark
```

Voici un exemple de commentaire d'une liste de contrôle d'accès numérotée.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in

access-list 101 remark permit_telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

Contrôle d'accès basé sur contexte

Le contrôle d'accès basé sur contexte (CBAC) a été introduit dans le logiciel Cisco IOS Version 12.0.5.T et nécessite l'ensemble des fonctionnalités du pare-feu Cisco IOS. Le contrôle CBAC examine le trafic qui transite par le pare-feu afin de détecter et de gérer les informations d'état pour les sessions TCP et UDP. Ces informations d'état sont utilisées afin de créer des ouvertures temporaires dans les listes d'accès du pare-feu. Configurez des listes **ip inspect** dans la direction du flux d'initiation du trafic afin d'autoriser le trafic entrant et d'autres connexions de données pour la session permise, les sessions initialisées à l'intérieur du réseau interne protégé, pour effectuer cette opération.

Voici la syntaxe pour le contrôle CBAC.

```
ip inspect name inspection-name protocol [timeoutseconds]
```

Voici un exemple de l'utilisation du contrôle CBAC pour examiner le trafic sortant. La liste de contrôle d'accès étendue 111 bloque normalement le trafic entrant autre que le trafic ICMP sans les ouvertures du contrôle CBAC pour le trafic entrant.

```
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw tcp timeout 3600
ip inspect name myfw udp timeout 3600
ip inspect name myfw tftp timeout 3600
interface Ethernet0/1
       ip address 172.16.1.2 255.255.255.0
       ip access-group 111 in
       ip inspect myfw out
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 111 permit icmp any 10.1.1.0 0.0.0.255
```

Proxy d'authentification

Le proxy d'authentification a été introduit dans le logiciel Cisco IOS Version 12.0.5.T. Ce proxy nécessite l'ensemble de fonctionnalités du pare-feu Cisco IOS. Le proxy d'authentification est employé pour authentifier les utilisateurs entrants ou sortants, ou les deux. Les utilisateurs qui sont normalement bloqués par une liste de contrôle d'accès peuvent amener un navigateur à passer par le pare-feu et s'authentifier sur un serveur TACACS+ ou RADIUS. Le serveur transmet des entrées de la liste de contrôle d'accès supplémentaires au routeur afin de permettre aux utilisateurs de passer après authentification.

Le proxy d'authentification est semblable à la fonctionnalité de verrou et clé (listes de contrôle d'accès dynamiques). Les différences sont les suivantes :

- La fonctionnalité de verrou et clé est activée par une connexion Telnet au routeur. Le proxy d'authentification est activé par HTTP via le routeur.
- Le proxy d'authentification doit utiliser un serveur externe.
- Le proxy d'authentification peut gérer l'ajout de plusieurs listes dynamiques. La fonctionnalité de verrou et clé ne peut en ajouter qu'une.
- Le proxy d'authentification a un délai d'attente absolu, mais pas inactif. La fonctionnalité de verrou et clé a les deux.

Pour obtenir des exemples de proxy d'authentification, reportez-vous au Manuel de configuration logicielle intégrée sécurisée Cisco.

Listes de contrôle d'accès turbo

Les listes de contrôle d'accès turbo ont été introduites dans le logiciel Cisco IOS Version 12.1.5.T et figurent uniquement sur les plates-formes 7200, 7500 et autres plates-formes haut de gamme. La fonctionnalité de liste de contrôle d'accès turbo est conçue pour traiter les listes de contrôle d'accès plus efficacement afin d'améliorer les performances du routeur.

Utilisez la commande **access-list compiled** pour les listes de contrôle d'accès turbo. Voici un exemple d'une liste de contrôle d'accès compilée.

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq syslog
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq tftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq ntp
```

Une fois que la liste de contrôle d'accès standard ou étendue est définie, utilisez la commande **global configuration** pour la compilation.

```
!--- Tells the router to compile. access-list compiled

Interface Ethernet0/1
ip address 172.16.1.2 255.255.255.0
!--- Applies to the interface. ip access-group 101 in
```

La commande **show access-list compiled** affiche des statistiques sur la liste de contrôle d'accès.

Listes de contrôle d'accès basées sur l'heure distribuées

Les listes de contrôle d'accès basées sur l'heure distribuées ont été introduites dans le logiciel Cisco IOS Version 12.2.2.T afin d'implémenter les listes de contrôle d'accès basées sur l'heure sur des routeurs de la gamme Cisco 7500 compatibles avec VPN. Avant l'introduction de la fonctionnalité de liste de contrôle d'accès basée sur l'heure distribuée, les listes de contrôle d'accès basées sur l'heure n'étaient pas prises en charge sur des cartes de ligne pour les routeurs de la gamme Cisco 7500. Si les listes de contrôle d'accès basées sur l'heure étaient configurées, elles se comportaient comme des listes de contrôle d'accès normales. Si une interface d'une carte de ligne était configurée avec des listes de contrôle d'accès basées sur l'heure, les paquets commutés dans l'interface n'étaient pas distribués commutés via la carte de ligne, mais transférés au processeur de routage pour traitement.

La syntaxe pour les listes de contrôle d'accès basées sur l'heure distribuées est la même que pour les listes de contrôle d'accès basées sur l'heure, avec l'ajout de commandes pour l'état des messages IPC (Inter Processor Communication) entre le processeur de routage et la carte de ligne.

```
debug time-range ipc
show time-range ipc
clear time-range ipc
```

Listes de contrôle d'accès de réception

Les listes de contrôle d'accès de réception sont utilisées afin d'améliorer la sécurité sur les routeurs Cisco 12000 par la protection du processeur GRP (Gigabit Route Processor) du routeur contre tout trafic inutile et potentiellement néfaste. Les listes de contrôle d'accès de réception ont été ajoutées comme dérogation spéciale à la limitation de maintenance pour le logiciel Cisco IOS Version 12.0.21S2 et intégrées à 12.0(22)S. Reportez-vous à GSR : Listes de contrôle d'accès de réception pour plus d'informations.

Listes de contrôle d'accès de protection d'infrastructure

Les listes de contrôle d'accès d'infrastructure sont employées afin de réduire au minimum le risque et l'efficacité d'une attaque directe de l'infrastructure par l'autorisation explicite du trafic

autorisé seulement au matériel d'infrastructure tout en permettant tout autre trafic de transit. Reportez-vous à Protection de votre noyau : Listes de contrôle d'accès de protection d'infrastructure pour plus d'informations.

Listes de contrôle d'accès de transit

Les listes de contrôle d'accès de transit sont employées afin d'améliorer la sécurité du réseau puisqu'elles autorisent uniquement de manière explicite le trafic nécessaire dans votre ou vos réseaux. Reportez-vous à Listes de contrôle d'accès de transit : Filtrage au niveau de votre périphérie pour plus d'informations.

Informations connexes

- RFC 1700
- RFC 1918
- Access Lists Support Page
- Cisco IOS Firewall
- Cisco IOS Software - Support Resources
- Support et documentation techniques - Cisco Systems