Règles d'accès

Ce chapitre décrit comment contrôler l'accès au réseau par l'intermédiaire de l'ASA ou vers l'ASA à l'aide des règles d'accès. Vous utilisez des règles d'accès pour contrôler l'accès au réseau en mode de pare-feu routé et transparent. En mode transparent, vous pouvez utiliser à la fois des règles d'accès (pour le trafic de couche 3) et des règles EtherType (pour le trafic de couche 2).

Remarque Pour accéder à l'interface ASA pour l'accès de gestion, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès de gestion en suivant le guide de configuration sur les opérations générales.

Contrôle d'accès au réseau

Les règles d'accès déterminent le trafic autorisé par l'ASA. Il existe plusieurs couches de règles qui fonctionnent ensemble pour mettre en œuvre votre politique de contrôle d'accès :

- Règles d'accès étendues (trafic de couche 3+) affectées aux interfaces : vous pouvez appliquer des ensembles de règles (ACL) distincts dans les directions entrantes et sortantes. Une règle d'accès étendue autorise ou refuse le trafic en fonction des critères du trafic de source et de destination.
- Règles d'accès étendues (trafic de couche 3+) attribuées aux interfaces virtuelles de pont (BVI; mode routé) : si vous nommez un BVI, vous pouvez appliquer des ensembles de règles distincts dans les sens entrant et sortant, et vous pouvez également appliquer des ensembles de règles aux interfaces de membre du groupe de pont. Lorsque la BVI et l'interface membre ont des règles d'accès, l'ordre de traitement dépend de la direction. En entrée, les règles d'accès de l'interface membre sont évaluées en premier, puis les règles d'accès de la BVI. En sortie, les règles de la BVI sont prises en compte en premier, puis les règles de l'interface membre.

- Règles d'accès étendues attribuées globalement : vous pouvez créer un seul ensemble de règles globales, qui sert de contrôle d'accès par défaut. Les règles globales sont appliquées après les règles d'interface.
- Règles d'accès de gestion (trafic de couche 3+) : vous pouvez appliquer un seul ensemble de règles pour couvrir le trafic dirigé vers une interface, qui est généralement le trafic de gestion. Dans l'interface de ligne de commande, il s'agit de groupes d'accès « plan de contrôle ». Pour le trafic ICMP dirigé vers le périphérique, vous pouvez également configurer les règles ICMP.
- Règles EtherType (trafic de couche 2) affectées aux interfaces (interfaces membres de groupes de ponts uniquement) : vous pouvez appliquer des ensembles de règles distincts dans les directions entrantes et sortantes. Les règles EtherType contrôlent l'accès réseau pour le trafic non IP. Une règle EtherType autorise ou refuse le trafic en fonction de l'EtherType. Vous pouvez également appliquer des règles d'accès étendues aux interfaces membres de groupes de ponts pour contrôler le trafic de couche 3+.

Renseignements généraux sur les règles

Les rubriques suivantes fournissent des renseignements généraux sur les règles d'accès et les règles EtherType.

Règles d'accès d'interface et règles d'accès globales

Vous pouvez appliquer une règle d'accès à une interface spécifique ou appliquer une règle d'accès globalement à toutes les interfaces. Vous pouvez configurer des règles d'accès globales en liaison avec les règles d'accès d'interface. Si vous le faites, les règles d'accès de l'interface entrante spécifiques sont toujours traitées avant les règles d'accès globales générales. Les règles d'accès globales s'appliquent uniquement au trafic entrant.

Règles entrantes et sortantes

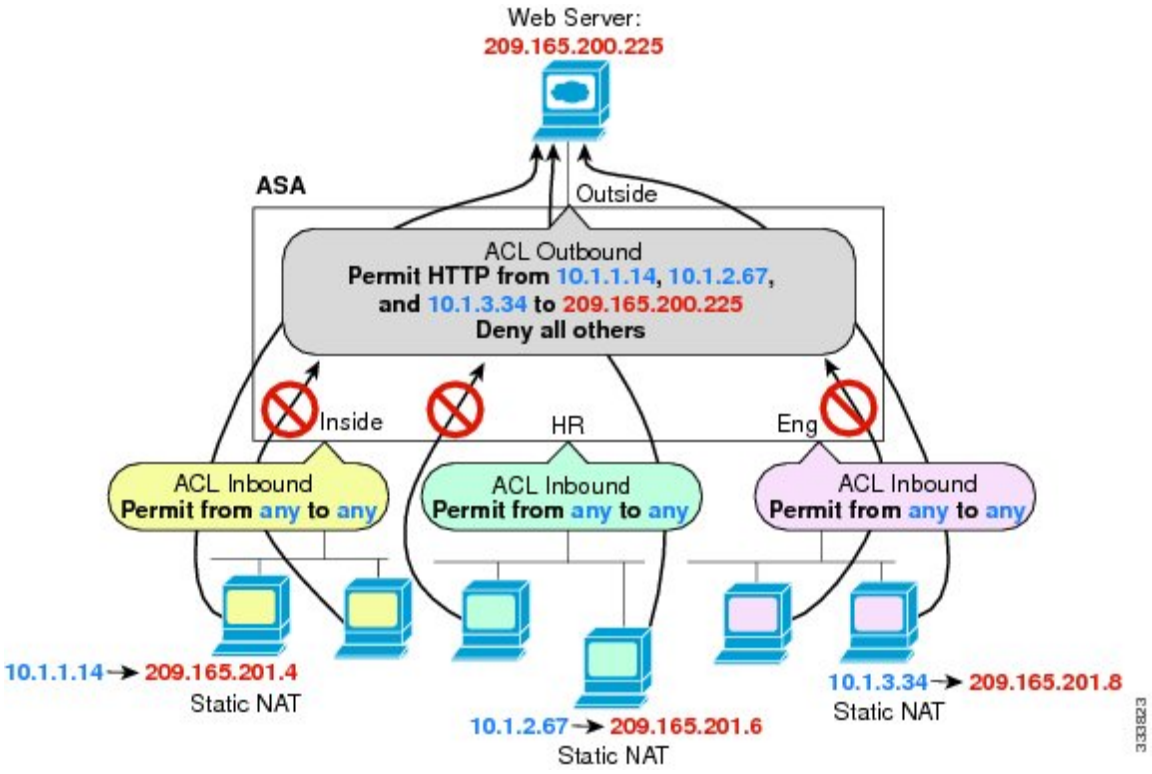
Vous pouvez configurer des règles d'accès en fonction de la direction du trafic :

- Entrantes : les règles entrantes s'appliquent au trafic lorsqu'il entre dans une interface. Les règles d'accès globales et de gestion sont toujours entrantes.
- Sortantes : les règles sortantes s'appliquent au trafic lorsqu'il quitte une interface.

Remarque « entrantes » et « sortantes » font référence à l'application d'une liste de contrôle d'accès sur une interface, soit au trafic entrant dans l'ASA sur une interface, soit au trafic sortant de l'ASA sur une interface. Ces termes ne font pas référence au déplacement du trafic d'une interface de sécurité inférieure vers une interface de sécurité plus élevée, communément appelée entrante, ou d'une interface de niveau supérieur vers une interface de niveau inférieur, communément appelée sortante.

Une liste de contrôle d'accès sortante est utile, par exemple, si vous souhaitez autoriser uniquement certains hôtes des réseaux internes à accéder à un serveur Web sur le réseau externe. Plutôt que de créer plusieurs listes de contrôle d'accès entrantes pour restreindre l'accès, vous pouvez créer une seule liste de contrôle d'accès sortante qui autorise uniquement les hôtes spécifiés. (Voir la figure suivante.) L'ACL sortante empêche tout autre hôte d'atteindre le réseau externe.

Illustration 1 : ACL sortante



Consultez les commandes suivantes pour cet exemple :

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14 host 209.165.200.225
 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67 host 209.165.200.225
 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34 host 209.165.200.225
 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

Ordre des règles

L'ordre des règles est important. Lorsque l'ASA décide de transférer ou d'abandonner un paquet, l'ASA teste le paquet par rapport à chaque règle dans l'ordre dans lequel les règles sont répertoriées dans l'ACL appliquée. Une fois qu'une correspondance est trouvée, aucune autre règle n'est vérifiée. Par exemple, si vous créez une règle d'accès au début qui autorise explicitement tout le trafic pour une interface, aucune autre règle n'est jamais vérifiée.

Autorisations implicites

Le trafic IPv4 et IPv6 de monodiffusion est autorisé par défaut d'une interface à sécurité supérieure vers une interface à sécurité inférieure. Cela inclut le trafic entre les interfaces routées standard et les interfaces virtuelles de pont (BVI) en mode routé.

Pour les interfaces de membre de groupes de ponts, cette autorisation implicite d'une interface de sécurité supérieure à inférieure s'applique aux interfaces du même groupe de ponts uniquement. Il n'y a pas

d'autorisations implicites entre une interface de membre de groupe de ponts et une interface routée ou un membre d'un groupe de ponts différent.

Les interfaces de membre de groupe de ponts (mode routé ou transparent) autorisent également les éléments suivants par défaut :

- ARP dans les deux sens. (Vous pouvez contrôler le trafic ARP à l'aide de l'inspection ARP, mais vous ne pouvez pas le contrôler à l'aide de la règle d'accès.)
- BPDU dans les deux sens. (Vous pouvez les contrôler à l'aide des règles Ethertype.)

Pour les autres trafics, vous devez utiliser une règle d'accès étendue (IPv4 et IPv6) ou une règle EtherType (non IP).

Refus implicite

Les listes de contrôle d'accès ont un refus implicite à la fin de la liste, donc, sauf si vous l'autorisez explicitement, le trafic ne peut pas passer. Par exemple, si vous souhaitez autoriser tous les utilisateurs à accéder à un réseau par l'intermédiaire de l'ASA, à l'exception d'adresses particulières, vous devez refuser les adresses particulières, puis autoriser tous les autres.

Pour les listes de contrôle d'accès de gestion (plan de commande), qui contrôlent le trafic vers le boîtier, il n'y a pas de refus implicite à la fin d'un ensemble de règles de gestion pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès normales.

Pour les listes de contrôle d'accès EtherType, le refus implicite à la fin de la liste de contrôle d'accès n'affecte pas le trafic IP ni les ARP ; par exemple, si vous autorisez EtherType 8037, le refus implicite à la fin de l'ACL ne bloque pas le trafic IP que vous avez précédemment autorisé avec une liste de contrôle d'accès étendue (ou implicitement autorisé d'une interface de haute sécurité à une interface de sécurité faible). Toutefois, si vous refusez explicitement tout le trafic avec une règle EtherType, le trafic IP et ARP est refusé; seul le trafic de protocole physique, tel que la négociation automatique, est toujours autorisé.

Si vous configurez une règle d'accès globale, le refus implicite survient *après* le traitement de la règle globale. Consultez l'ordre des opérations suivant :

1. Critères d'accès de l'interface
2. Pour les interfaces de membre de groupes de ponts, la règle d'accès de l'interface virtuelle de pont (BVI).
3. Critères d'accès globaux
4. Refus implicite.

NAT et critères d'accès

Les critères d'accès utilisent toujours les adresses IP réelles pour déterminer une correspondance, même si vous configurez la NAT. Par exemple, si vous configurez la NAT pour un serveur interne, 10.1.1.5, de sorte qu'il ait une adresse IP routable publiquement à l'extérieur, 209.165.201.5, alors le critère d'accès permettant au trafic externe d'accéder au serveur interne doit faire référence à l'adresse IP réelle du serveur (10.1.1.5), et non à l'adresse mappée (209.165.201.5).

Interfaces de niveau de sécurité identiques et règles d'accès

Chaque interface a un niveau de sécurité, et la vérification du niveau de sécurité est effectuée avant que les règles d'accès ne soient prises en compte. Ainsi, même si vous autorisez une connexion dans une règle d'accès,

elle peut être bloquée en raison d'une vérification de même niveau de sécurité au niveau de l'interface. Vous pouvez vous assurer que votre configuration autorise les connexions au même niveau de sécurité afin que vos règles d'accès soient toujours prises en compte dans les décisions en matière d'autorisation ou de refus.

- Les connexions entre les interfaces d'entrée et de sortie de même niveau de sécurité sont soumises à la vérification same-security-traffic inter-interface.

  Pour autoriser ces connexions, entrez la commande **same-security-traffic permit inter-interface**.

  Pour autoriser ces connexions, choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** puis sélectionnez l'option **Enable traffic between two or more interfaces which are configured with the same security levels (Activer le trafic entre deux interfaces ou plus qui sont configurées avec les mêmes niveaux de sécurité**).

- Les connexions avec les mêmes interfaces d'entrée et de sortie sont soumises à la même vérification intra-interface de sécurité et de trafic.

  Pour autoriser ces connexions, entrez la commande **same-security-traffic permit intra-interface**.

  Pour autoriser ces connexions, choisissez **Configuration Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** , puis sélectionnez l'option **Enable traffic between two or more hosts connected to the same interface (Activer le trafic entre deux hôtes ou plus connectés à la même interface)**.

Règles d'accès étendues

Cette section décrit les renseignements sur les règles d'accès étendues.

Règles de contrôle d'accès étendues pour le retour du trafic

Pour les connexions TCP, UDP et SCTP en mode routé et transparent, vous n'avez pas besoin de règle d'accès pour autoriser le retour, car l'ASA autorise tout le trafic de retour pour les connexions bidirectionnelles établies.

Pour les protocoles sans connexion tels que ICMP, cependant, l'ASA établit des sessions unidirectionnelles. Vous avez donc besoin de règles d'accès pour autoriser ICMP dans les deux sens (en appliquant des listes de contrôle d'accès aux interfaces de source et de destination), ou vous devez activer le moteur d'inspection ICMP. Le moteur d'inspection ICMP traite les sessions ICMP comme des connexions bidirectionnelles. Par exemple, pour contrôler ping, spécifiez **echo-reply** (**0**) (ASA to host) ou **echo** (**8**) (host to ASA).

Autoriser le trafic de diffusion et de multidiffusion

En mode de pare-feu routé, le trafic de diffusion et de multidiffusion est bloqué même si vous l'autorisez dans un critère d'accès, y compris les protocoles de routage dynamique non pris en charge et le DHCP. Vous devez configurer les protocoles de routage dynamique ou le relais DHCP pour autoriser ce trafic.

Pour les interfaces membres du même groupe de ponts en mode transparent ou de pare-feu routé, vous pouvez autoriser tout trafic IP à l'aide des règles d'accès.

Remarque Étant donné que ces types spéciaux de trafic sont sans connexion, vous devez appliquer une règle d'accès aux interfaces de trafic entrant et sortant, afin que le trafic de retour soit autorisé à passer.

Le tableau suivant répertorie les types de trafic courants que vous pouvez autoriser à l'aide de règles d'accès entre les interfaces membres du même groupe de ponts.

Tableau 1 : Trafic spécial pour les règles d'accès entre les membres d'un même groupe de ponts

Type de trafic	Protocole ou port	Notes
DHCP (protocole de configuration dynamique des hôtes)	Ports UDP 67 et 68	Si vous activez le serveur DHCP, l'ASA ne transmet pas les paquets DHCP.
EIGRP	Protocole 88	—
OSPF	Protocole 89	—
Flux de multidiffusion	Les ports UDP varient selon l'application.	Les flux de multidiffusion sont toujours destinés à une adresse de classe D (224.0.0.0 à 239.x.x.x).
RIP (v1 ou v2)	Port UDP 520	—

Règles d'accès de gestion

Vous pouvez configurer des règles d'accès qui contrôlent le trafic de gestion destiné à l'ASA. Les règles de contrôle d'accès pour le trafic de gestion vers le boîtier (défini par des commandes telles que **http**, **ssh**, ou **telnet**) ont une priorité plus élevée qu'une règle d'accès de gestion appliquée avec l'option **control-plane**. Par conséquent, ce trafic de gestion autorisé sera autorisé à entrer même s'il est explicitement refusé par la liste de contrôle d'accès vers le boîtier.

Contrairement aux règles d'accès standard, il n'y a pas de refus implicite à la fin d'un ensemble de règles de gestion pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès normales.

Vous pouvez également utiliser des règles ICMP pour contrôler le trafic ICMP vers le périphérique. Utilisez des règles d'accès étendues normales pour contrôler le trafic ICMP qui passe par le périphérique.

Règles EtherType

Cette section décrit les règles EtherType.

EtherTypes pris en charge et autres types de trafic

Une règle EtherType contrôle les éléments suivants :

- EtherType identifié par un numéro hexadécimal de 16 bits, y compris les types courants IPX et MPLS de monodiffusion ou de multidiffusion.
- Trames Ethernet V2.
- Les BPDU, qui sont autorisés par défaut. Les BPDU sont encapsulés dans le protocole SNAP et l'ASA est conçu pour gérer spécifiquement les BPDU.

- BPDU de port de liaison (propriétaire Cisco). Les BPDU de ligne principale ont des informations VLAN dans la charge utile, de sorte que l'ASA modifie la charge utile avec le VLAN sortant si vous autorisez les BPDU.
- Intermediate System-to-Intermediate System (IS-IS)
- Le paquet de contrôle de liaison logique IEEE 802.2. Vous pouvez contrôler l'accès en fonction de l'adresse du point d'accès du service de destination.

Les types de trafic suivants ne sont pas pris en charge :

- Trames au format 802.3 : ces trames ne sont pas gérées par la règle, car elles utilisent un champ de longueur par opposition à un champ de type.

Règles EtherType pour le retour du trafic

Comme les EtherTypes sont sans connexion, vous devez appliquer la règle aux deux interfaces si vous souhaitez que le trafic passe dans les deux sens.

Autoriser MPLS

Si vous autorisez MPLS, assurez-vous que les connexions TCP du protocole de distribution d'étiquette et du protocole de distribution de balise sont établies par l'ASA en configurant les deux routeurs MPLS connectés à l'ASA pour utiliser l'adresse IP sur l'interface de l'ASA comme ID de routeur pour les sessions LDP ou TDP. (LDP et TDP permettent aux routeurs MPLS de négocier les étiquettes (adresses) utilisées pour transférer les paquets.)

Sur les routeurs Cisco IOS, saisissez la commande appropriée pour votre protocole, LDP ou TDP. L' *interface* est l'interface connectée à l'ASA.

mpls ldp router-id *interface* **force**

Ou

tag-switching tdp router-id *interface* **force**

Licences pour les règles d'accès

Les règles de contrôle d'accès ne nécessitent pas de licence spéciale.

Cependant, pour utiliser **sctp** comme protocole dans une règle, vous devez avoir une licence d'opérateur.

Lignes directrices relatives au contrôle d'accès

Lignes directrices pour IPv6

Prend en charge IPv6. Les adresses de source et de destination peuvent inclure n'importe quelle combinaison d'adresses IPv4 et IPv6.

Lignes directrices d'ACL par utilisateur

- La liste de contrôle d'accès par utilisateur utilise la valeur dans la commande **timeout uauth**, mais elle peut être remplacée par la valeur de délai d'expiration de session par utilisateur d'AAA.
- Si le trafic est refusé en raison d'une liste de contrôle d'accès par utilisateur, le message syslog 109025 est enregistré. Si le trafic est autorisé, aucun message syslog n'est généré. L'option **log** dans la liste de contrôle d'accès par utilisateur n'a aucun effet.

Lignes directrices et limites additionnelles

- Au fil du temps, votre liste de règles d'accès peut s'allonger pour inclure de nombreuses règles obsolètes. À la longue, les listes de contrôle d'accès des groupes d'accès peuvent devenir si importantes qu'elles ont une incidence sur les performances globales du système. Si vous constatez que le système rencontre des problèmes pour envoyer des messages syslog, communiquer pour la synchronisation de basculement, établir et maintenir les connexions d'accès de gestion SSH/HTTPS, etc., vous devrez peut-être élaguer vos règles d'accès. En général, vous devez maintenir activement vos listes de règles pour supprimer les règles obsolètes, les règles qui ne sont jamais touchées, les objets FQDN qui ne peuvent plus être résolus, etc. Envisagez également de mettre en œuvre la recherche de groupe d'objets.
- La recherche de groupe d'objets est activée par défaut pour les nouveaux déploiements.

  Vous pouvez réduire la mémoire requise pour la recherche des règles d'accès en activant la recherche de groupe d'objets, mais cela se fait au détriment des performances de recherche et d'une utilisation accrue du processeur. Lorsqu'elle est activée, la recherche par groupe d'objets ne développe pas les objets de réseau ou de service, mais recherche dans les critères d'accès les correspondances basées sur les définitions de ces groupes. Vous pouvez définir cette option à l'aide de la commande **object-group-search access-control**.

  Vous pouvez utiliser la commande **object-group-search threshold** pour activer un seuil afin d'éviter la dégradation des performances. Lorsqu'elle fonctionne avec un seuil, pour chaque connexion, les adresses IP source et de destination sont comparées aux objets réseau. Si le nombre d'objets correspondant à l'adresse source multiplié par le nombre correspondant à l'adresse de destination dépasse 10 000, la connexion est abandonnée. Configurez vos règles pour éviter un nombre excessif de correspondances.

Remarque La recherche de groupe d'objets fonctionne uniquement avec les objets de réseau et de service. Elle ne fonctionne pas avec des groupes de sécurité ou des objets utilisateur. N'activez pas cette fonctionnalité si les listes de contrôle d'accès comprennent des groupes de sécurité. Le résultat peut être des listes de contrôle d'accès inactives ou un autre comportement inattendu.

- Vous pouvez améliorer les performances et la fiabilité du système en utilisant le modèle de validation transactionnelle pour les groupes d'accès. Cependant, la validation transactionnelle n'est pas recommandée si vous utilisez des objets FQDN pour des noms d'hôte dont la résolution peut changer fréquemment, car la compilation du groupe d'accès pourrait ne jamais aboutir complètement. Pour plus d'informations, consultez le chapitre sur les paramètres de base dans le guide de configuration des opérations générales. Utilisez la commande **asp rule-engine transactional-commit access-group**.
- Dans ASDM, les descriptions de règles sont basées sur les remarques de liste d'accès qui précèdent la règle dans l'ACL ; pour les nouvelles règles que vous créez dans ASDM, toutes les descriptions sont également configurées en tant que remarques avant la règle associée. Cependant, le traceur de paquets

dans ASDM correspond à la remarque configurée après la règle de correspondance dans l'interface de ligne de commande.

- Pour utiliser des objets réseau de nom de domaine complet (FQDN) comme critères de source ou de destination, vous devez également configurer DNS pour les interfaces de données.

  Notez que le contrôle de l'accès par nom de domaine complet (FQDN) est un mécanisme du meilleur effort. Prenez en compte les points suivants:

  - Étant donné que les réponses DNS peuvent être contrefaites, utilisez uniquement des serveurs DNS internes entièrement fiables.
  - Certains noms de domaine complets, en particulier pour les serveurs très populaires, peuvent avoir des centaines, sinon des milliers d'adresses IP, et celles-ci peuvent changer fréquemment. Comme le système utilise les résultats de recherche DNS en cache, les utilisateurs peuvent obtenir des adresses qui ne sont pas encore dans le cache et leurs connexions ne correspondent pas à la règle FQDN. Les règles qui utilisent des objets réseau FQDN ne fonctionnent efficacement que pour les noms qui se résolvent en moins de 100 adresses.

    Nous vous recommandons de ne pas créer de règles d'objet réseau pour un nom de domaine complet qui se résout à plus de 100 adresses, car la probabilité que l'adresse d'une connexion en soit une qui a été résolue et disponible dans le cache DNS du périphérique est faible.
  - Pour les noms de domaine complets populaires, différents serveurs DNS peuvent renvoyer un ensemble d'adresses IP différent. Ainsi, si vos utilisateurs utilisent un serveur DNS différent de celui que vous configurez, les règles de contrôle d'accès basé sur le nom de domaine complet (FQDN) pourraient ne pas s'appliquer à toutes les adresses IP du site qui sont utilisées par vos clients, et vous n'obtiendrez pas les résultats escomptés pour vos règles .
  - Certaines entrées de nom de domaine complet (FQDN) ont des valeurs de durée de vie très courte (TTL). Cela peut entraîner des recompilations fréquentes de la table de recherche, ce qui peut avoir une incidence sur les performances globales du système.

Configurer le contrôle d'accès

Les rubriques suivantes expliquent comment configurer le contrôle d'accès.

Configurer un groupe d'accès

Avant de pouvoir créer un groupe d'accès, créez la liste de contrôle d'accès.

Pour lier une liste de contrôle d'accès à une interface ou pour l'appliquer globalement, utilisez la commande suivante :

access-group *access_list* { {**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**] | **global**}

Pour un groupe d'accès spécifique à l'interface :

- Précisez le nom de l'ACL étendue ou EtherType. Vous pouvez configurer une commande **access-group** par type d'ACL, interface et direction, ainsi qu'une ACL de plan de contrôle. L'ACL de plan de contrôle doit être une ACL étendue. Les ACL EtherType sont autorisées sur les interfaces de membres de groupe de ponts uniquement. Pour les groupes de ponts en mode routé, vous pouvez spécifier des listes de

contrôle d'accès étendues pour chaque direction sur l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.

- Le mot-clé **in** applique l'ACL au trafic entrant. Le mot-clé **out** applique l'ACL au trafic sortant.
- Précisez le nom **de l'interface**.
- Le mot-clé per-user-override (pour les ACL étendues entrantes uniquement) permet aux ACL d'utilisateur dynamiques qui sont téléchargées pour l'autorisation de l'utilisateur de remplacer l'ACL attribuée à l'interface. Par exemple, si l'ACL de l'interface refuse tout le trafic de 10.0.0.0, mais que l'ACL dynamique autorise tout le trafic de 10.0.0.0, l'ACL dynamique remplace l'ACL de l'interface pour cet utilisateur.

  Par défaut, le trafic d'accès à distance du VPN ne correspond pas aux listes de contrôle d'accès d'interface. Toutefois, si vous utilisez la commande no **sysopt connection permit-vpn** pour désactiver ce contournement, le comportement dépend de l'application d'un **vpn-filter** dans la stratégie de groupe et de la définition de l'option **per-user-override** :

  - Aucun **per-user-override**, aucun **vpn-filter** : le trafic est comparé à l'ACL de l'interface.
  - Aucun **per-user-override**, **vpn-filter** : le trafic est d'abord comparé à l'ACL de l'interface, puis au filtre VPN.
  - **per-user-override**, **vpn-filter** : le trafic est comparé au filtre VPN uniquement.
- Le mot-clé **control-plane** spécifie si l'ACL étendue est destinée au trafic vers le boîtier.

  Contrairement aux règles d'accès standard, il n'y a pas de refus implicite à la fin d'un ensemble de règles de gestion (plan de contrôle) pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès normales.

Pour un groupe d'accès global, spécifiez le mot-clé **global** pour appliquer l'ACL étendue à la direction entrante de toutes les interfaces.

Exemple

L'exemple suivant montre comment utiliser la commande **access-group** :

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access in interface outside
```

La commande **access-list** permet à tout hôte d'accéder à l'adresse de l'hôte en utilisant le port 80. La commande **access-group** précise que la commande **access-list** s'applique au trafic entrant dans l'interface externe.

Configurer les règles d'accès ICMP

Par défaut, vous pouvez envoyer des paquets ICMP vers n'importe quelle interface IPv4 ou IPv6, avec les exceptions suivantes

- L'ASA ne répond pas aux demandes ECHO ICMP dirigées vers une adresse de diffusion.
- L'ASA répond uniquement au trafic ICMP envoyé à l'interface par laquelle le trafic entre; vous ne pouvez pas envoyer de trafic ICMP par une interface vers une interface distante.

Pour protéger le périphérique contre les attaques, vous pouvez utiliser des règles ICMP pour limiter l'accès ICMP aux interfaces à des hôtes, des réseaux ou des types ICMP particuliers. Les règles ICMP fonctionnent comme des règles d'accès, où les règles sont classées, et la première règle qui correspond à un paquet définit l'action.

Si vous configurez une règle ICMP pour une interface, une règle ICMP de refus implicite est ajoutée à la fin de la liste de règles ICMP, modifiant le comportement par défaut. Par conséquent, si vous souhaitez simplement refuser certains types de messages, vous devez inclure une règle autoriser tout à la fin de la liste de règles ICMP pour autoriser les autres types de messages.

Nous vous recommandons de toujours accorder l'autorisation pour le type de message ICMP « unreachable » (inaccessible) (type 3). Le refus des messages ICMP inaccessibles désactive la découverte de la MTU du chemin ICMP, ce qui peut interrompre le trafic IPsec et PPTP. De plus, les paquets ICMP dans IPv6 sont utilisés dans le processus de découverte de voisin IPv6.

Procédure

Étape 1 Créez des règles pour le trafic ICMP.

icmp {**permit** | **deny**} {**host** *ip_address* | *ip_address mask* | **any**} [*icmp_type*] *interface_name*

Si vous ne spécifiez pas de *icmp_type*, la règle s'applique à tous les types. Vous pouvez saisir le numéro ou le nom. Pour contrôler ping, spécifiez echo-reply (0) (ASA-to-host) ou echo (8) (host-to-ASA).

Pour l'adresse, vous pouvez appliquer la règle à **any** adresse, à un **hôte** unique ou à un réseau (*ip_address mask*).

Étape 2 Créez des règles pour le trafic ICMPv6 (IPv6).

ipv6 icmp {**permit** | **deny**} {**host** *ipv6_address* | *ipv6-network*/*prefix-length* | **any**} [*icmp_type*] *interface_name*

Si vous ne spécifiez pas de *icmp_type*, la règle s'applique à tous les types.

Pour l'adresse, vous pouvez appliquer la règle à **any** adresse, à un **hôte** unique ou à un réseau (*ipv6-network*/*prefix-length*).

Étape 3 (Facultatif) Définissez des limites de débit sur les messages ICMP inaccessibles afin que l'ASA apparaisse sur la sortie de la route de trace.

icmp unreachable rate-limit *rate* **burst-size** *size*

La limite de débit peut aller de 1 à 100, 1 étant la valeur par défaut. La taille de rafale peut être comprise entre 1 et 10. Le nombre de réponses de la taille de rafale est envoyé, mais les réponses suivantes ne sont pas envoyées tant que la limite de débit n'est pas atteinte.

Exemple :

Augmenter la limite de débit, ainsi qu'activer la commande **set connection decrement-ttl** dans une politique de service, est nécessaire pour permettre un traceroute à travers l'ASA qui montre l'ASA comme l'un des sauts. Par exemple, la politique suivante augmente la limite de débit et décrémente la valeur de durée de vie (TTL) pour tout le trafic via l'ASA.

```
icmp unreachable rate-limit 50 burst-size 10
class-map global-class
  match any
policy-map global_policy
  class global-class
```

```
set connection decrement-ttl
```

Exemples

L'exemple suivant montre comment autoriser tous les hôtes, à l'exception de celui à 10.1.1.15, à utiliser ICMP pour l'interface interne :

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

L'exemple suivant montre comment autoriser l'hôte à 10.1.1.15 à utiliser uniquement le message ping vers l'interface interne :

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

L'exemple suivant montre comment refuser toutes les demandes ping et autoriser tous les messages packet-too-big (pour prendre en charge la découverte de MTU du chemin) sur l'interface externe :

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

L'exemple suivant montre comment autoriser l'hôte 2000:0:0:4::2 ou les hôtes du préfixe 2001::/64 à envoyer un message ping à l'interface externe :

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

Surveillance des règles d'accès

Pour surveiller l'accès au réseau, entrez les commandes suivantes :

- **clear access-list** *id* **counters**

  Efface le nombre d'accès de la liste d'accès.

- **show access-list** [*name*]

  Affiche les listes d'accès, y compris le numéro de ligne de chaque ACE et le nombre d'accès. Incluez un nom d'ACL ou vous verrez toutes les listes d'accès.

- **show running-config access-group**

  Affiche l'ACL actuelle liée aux interfaces.

Évaluation des messages Syslog pour les règles d'accès

Utilisez une visionneuse d'événements syslog, comme celle dans ASDM, pour afficher les messages liés aux règles d'accès.

Si vous utilisez la journalisation par défaut, le message syslog 106023 s'affiche pour les flux explicitement refusés uniquement. Le trafic qui correspond à l'entrée « refuser implicite » qui termine la liste de règles n'est pas journalisé.

En cas d'attaque de l'ASA, le nombre de messages de journal système pour les paquets refusés peut être très élevé. Nous vous recommandons d'activer plutôt la journalisation à l'aide du message syslog 106100, qui fournit des statistiques pour chaque règle (y compris les règles d'autorisation) et vous permet de limiter le nombre de messages syslog produits. Sinon, vous pouvez désactiver toute la journalisation pour une règle donnée.

Lorsque vous activez la journalisation pour le message 106100, si un paquet correspond à une ACE, l'ASA crée une entrée de flux pour suivre le nombre de paquets reçus dans un intervalle spécifique. L'ASA génère un message syslog au premier résultat et à la fin de chaque intervalle, identifiant le nombre total de résultats au cours de l'intervalle et l'horodatage du dernier résultat. À la fin de chaque intervalle, l'ASA réinitialise le nombre de résultats à 0. Si aucun paquet ne correspond à l'ACE pendant un intervalle, l'ASA supprime l'entrée de flux. Lorsque vous configurez la journalisation pour une règle, vous pouvez contrôler l'intervalle et même le niveau de gravité du message de journal, par règle.

Un flux est défini par les adresses IP source et de destination, les protocoles et les ports. Comme le port source peut différer pour une nouvelle connexion entre les deux mêmes hôtes, vous pourriez ne pas voir le même incrément de flux, car un nouveau flux a été créé pour la connexion.

Les paquets autorisés qui appartiennent à des connexions établies n'ont pas besoin d'être vérifiés par rapport aux listes de contrôle d'accès; seul le paquet initial est journalisé et inclus dans le nombre de résultats. Pour les protocoles sans connexion, comme ICMP, tous les paquets sont journalisés, même s'ils sont autorisés, et tous les paquets refusés sont journalisés.

Consultez le *guide des messages de journal système* pour obtenir des renseignements sur les messages de journal système.

Astuces Lorsque vous activez la journalisation pour le message 106100, si un paquet correspond à une ACE, l'ASA crée une entrée de flux pour suivre le nombre de paquets reçus dans un intervalle spécifique. L'ASA dispose d'un maximum de 32 K flux de journalisation pour les ACE. Un grand nombre de flux peuvent exister simultanément à tout moment. Pour éviter une utilisation illimitée des ressources de mémoire et de processeur, l'ASA impose une limite au nombre de flux *de refus* simultanés; la limite est placée sur les flux de refus uniquement (et non sur les flux d'autorisation), car ils peuvent indiquer une attaque. Lorsque la limite est atteinte, l'ASA ne crée pas de nouveau flux de refus pour la journalisation jusqu'à ce que les flux existants expirent et envoie le message 106101. Vous pouvez contrôler la fréquence de ce message à l'aide de la commande **access-list alert-interval** *secs* et le nombre maximal de flux de refus mis en cache à l'aide de la commande **access-list deny-flow-max** *number*.

Exemples de configuration pour autoriser ou refuser l'accès au réseau

Voici quelques exemples de configuration typiques pour autoriser ou refuser l'accès au réseau.

Exemples d'ACL étendues

L'exemple suivant ajoute un objet réseau pour le serveur interne 1, effectue une NAT statique pour le serveur et permet l'accès de l'extérieur pour le serveur interne 1.

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12

hostname(config)# access-list outside_access extended permit tcp any object inside-server1
 eq www
hostname(config)# access-group outside_access in interface outside
```

L'exemple suivant permet à tous les hôtes de communiquer entre les réseaux interne et RH, mais uniquement des hôtes spécifiques d'accéder au réseau externe :

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

L'exemple suivant utilise des groupes d'objets pour autoriser un trafic spécifique sur l'interface interne :

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

Exemples EtherType

Par exemple, l'exemple d'ACL suivant permet les EtherTypes courants provenant de l'interface interne :

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

L'exemple suivant autorise certains EtherTypes par l'ASA, mais il refuse tous les autres :

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

L'exemple suivant refuse le trafic avec EtherType 0x1256, mais autorise tous les autres sur les deux interfaces :

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

Historique des règles d'accès

Nom de la caractéristique	Versions de plateforme	Description
Critères d'accès de l'interface	7.0(1)	Contrôle de l'accès au réseau par l'intermédiaire de l'ASA à l'aide des ACL. Nous avons introduit la commande suivante : **access-group**.
Critères d'accès globaux	8.3(1)	Des règles d'accès globales ont été introduites. Nous avons modifié la commande suivante : **access-group.**
Prise en charge du pare-feu d'identité	8.4(2)	Vous pouvez maintenant utiliser des utilisateurs et des groupes de pare-feu d'identité pour la source et la destination. Vous pouvez utiliser une liste de contrôle d'accès de pare-feu d'identité avec des règles d'accès, des règles AAA et pour l'authentification VPN. Nous avons modifié les commandes suivantes : **access-list extended**.
Prise en charge des ACL EtherType pour le trafic IS-IS	8.4(5), 9.1(2)	En mode de pare-feu transparent, l'ASA peut désormais transmettre le trafic IS-IS à l'aide d'une liste de contrôle d'accès EtherType. Nous avons modifié la commande suivante : **access-list ethertype** {**permit** | **deny**} **isis**.
Prise en charge de TrustSec	9.0(1)	Vous pouvez maintenant utiliser les groupes de sécurité TrustSec pour la source et la destination. Vous pouvez utiliser une liste de contrôle d'accès de pare-feu d'identité avec des règles d'accès. Nous avons modifié les commandes suivantes : **access-list extended**.

Nom de la caractéristique	Versions de plateforme	Description
ACL unifiée pour IPv4 et IPv6	9.0(1)	Les ACL prennent désormais en charge les adresses IPv4 et IPv6. Vous pouvez même spécifier une combinaison d'adresses IPv4 et IPv6 pour la source et la destination. Le mot-clé **any** a été modifié pour représenter le trafic IPv4 et IPv6. Les mots-clés **any4** et **any6** ont été ajoutés pour représenter le trafic IPv4 uniquement et IPv6 uniquement, respectivement. Les ACL propres à IPv6 sont obsolètes. Les ACL IPv6 existantes sont migrées vers des ACL étendues. Pour en savoir plus, consultez les notes de mise à jour. Nous avons modifié les commandes suivantes : **access-list extended**, **access-list webtype**. Nous avons supprimé les commandes suivantes : **ipv6 access-list**, **ipv6 access-list webtype**, **ipv6-vpn-filter**
Amélioration des ACL étendues et des objets pour filtrer le trafic ICMP par code ICMP	9.0(1)	Le trafic ICMP peut maintenant être autorisé ou refusé en fonction du code ICMP. Nous avons introduit ou modifié les commandes suivantes : **access-list extended**, **service-object, service**.
Modèle de validation transactionnelle sur le moteur de règles de groupe d'accès	9.1(5)	Lorsque cette option est activée, une mise à jour de règle est appliquée une fois la compilation de la règle terminée, sans affecter les performances de correspondance de la règle. Nous avons introduit les commandes suivantes : **asp rule-engine transactional-commit**, **show running-config asp rule-engine transactional-commit**, **clear configure asp rule-engine transactional-commit**.
Session de configuration pour modifier les ACL et les objets. Référencement ultérieur des objets et desACL dans les règles d'accès.	9.3(2)	Vous pouvez maintenant modifier les ACL et les objets dans une session de configuration isolée. Vous pouvez également référencer des objets et des ACL à l'avance, c'est-à-dire configurer des règles et des groupes d'accès pour des objets ou des ACL qui n'existent pas encore. Nous avons introduit les commandes **clear config-session**, **clear session**, **configure session**, **forward-reference**, et **show config-session**.
Prise en charge des règles d'accès pour le protocole Stream Control Transmission Protocol (SCTP)	9.5(2)	Vous pouvez maintenant créer des règles d'accès à l'aide du protocole **sctp**, y compris des spécifications de port. Nous avons modifié la commande suivante : **access-list extended**.
Prise en charge de la règle Ethertype pour l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2.	9.6(2)	Vous pouvez maintenant écrire des règles de contrôle d'accès Ethertype pour l'adresse du point d'accès de service de destination du paquet de contrôle de liaison logique IEEE 802.2. En raison de cet ajout, le mot clé **bpdu** ne correspond plus au trafic prévu. Rewrite **bpdu** rules for **dsap 0x42**. Nous avons modifié les commandes suivantes : **access-list ethertype**

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge en mode routé des règles EtherType sur les interfaces membres de groupes de ponts et des règles d'accès étendues sur les interfaces virtuelles de pont (BVI).	9.7(1)	Vous pouvez maintenant créer des ACL EtherType et les appliquer aux interfaces membres de groupes de ponts en mode routé. Vous pouvez également appliquer des règles d'accès étendues à l'interface virtuelle de pont (BVI) en plus des interfaces membres. Nous avons modifié les commandes suivantes : **access-group**, **access-list ethertype**.
Modifications de la liste de contrôle d'accès Ethertype.	9.9(1)	Les listes de contrôle d'accès EtherType prennent désormais en charge Ethernet II IPX (EII IPX). En outre, de nouveaux mots clés sont ajoutés au mot clé DSAP pour prendre en charge les valeurs DSAP courantes : BPDU (0x42), IPX (0xE0), IPX brut (0xFF) et ISIS (0xFE). Par conséquent, les entrées de contrôle d'accès EtherType existantes qui utilisent les mots-clés BPDU ou ISIS seront converties automatiquement pour utiliser la spécification DSAP, et les règles pour IPX seront converties en trois règles (DSAP IPX, DSAP brut IPX et EII IPX). De plus, la capture de paquets qui utilise IPX comme valeur EtherType est obsolète, car IPX correspond à trois EtherTypes distincts. Nous avons modifié les commandes suivantes : **access-list ethertype** a ajouté les nouveaux mots clés **eii-ipx** et **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}; **capture ethernet-type** ne prend plus en charge le mot clé **ipx**.
Le seuil de recherche du groupe d'objets est désormais désactivé par défaut.	9.12(1)	Si vous avez activé la recherche par groupe d'objets, la fonctionnalité a été soumise à un seuil pour aider à empêcher la dégradation des performances. Ce seuil est désormais désactivé par défaut. Vous pouvez l'activer en utilisant la commande **object-group-search threshold**. Nous avons ajouté la commande suivante : **object-group-search threshold**.
Le référencement direct des ACL et des objets est toujours activé. De plus, la recherche de groupes d'objets pour le contrôle d'accès est désormais activée par défaut.	9.18(1)	Vous pouvez faire référence à des ACL ou à des objets réseau qui n'existent pas encore lors de la configuration de groupes d'accès ou de critères d'accès. De plus, la recherche de groupes d'objets est désormais activée par défaut pour le contrôle d'accès pour les *nouveaux* déploiements. Cette commande restera désactivée lors de la mise à niveau des périphériques. Si vous souhaitez l'activer (conseillé), vous devez le faire manuellement. Nous avons supprimé la commande **forward-reference enable** et modifié la valeur par défaut pour **object-group-search access-control** afin de l'activer.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.