

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, à la page 1
- Licences pour les règles d'accès, à la page 7
- Lignes directrices relatives au contrôle d'accès, à la page 7
- Configurer le contrôle d'accès, à la page 9
- Surveillance des règles d'accès, à la page 18
- Historique des règles d'accès, à la page 19

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 :

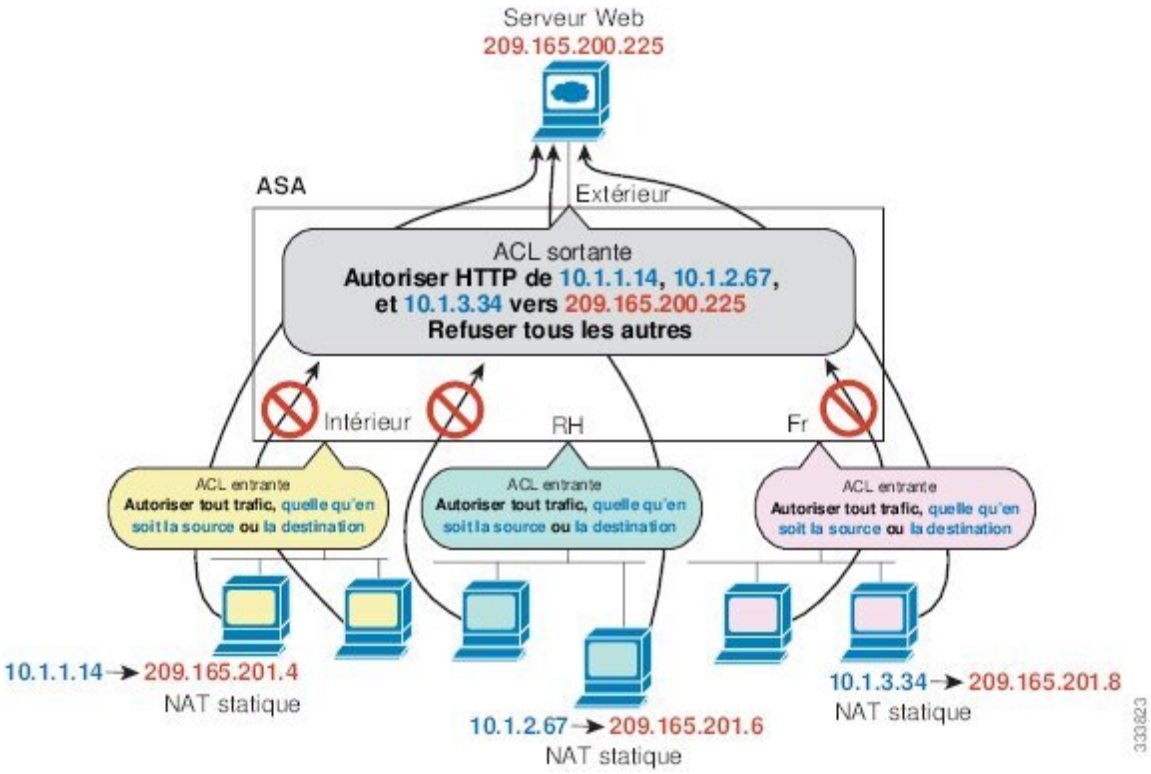
- Entrant : les règles entrantes s'appliquent au trafic lorsqu'il entre dans une interface. Les règles d'accès globales et de gestion sont toujours entrantes.
- Sortant : les règles sortantes s'appliquent au trafic lorsqu'il quitte une interface.



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



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 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 (comme les connexions HTTP, Telnet et SSH à une interface) ont une priorité plus élevée qu'une règle d'accès de gestion . 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

Directives IPv6

Prend en charge IPv6. (9.0 et versions ultérieures) Les adresses de source et de destination peuvent inclure n'importe quelle combinaison d'adresses IPv4 et IPv6. Pour les versions antérieures à la version 9.0, vous devez créer une règle d'accès IPv6 distincte.

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.

Directives 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 en cliquant sur le bouton **Advanced** (Avancé) sous le tableau des règles d'accès.

  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. Il 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. L'option se trouve sous **Configurations (Configurations) > Device Management (gestion des périphériques) > Advanced (Avancé) > Rule Engine (moteur de règles)**.
- 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.
- Lorsque vous saisissez plusieurs éléments dans l'adresse source ou de destination, ou dans le service source ou de destination, ASDM crée automatiquement un groupe d'objets pour eux avec le préfixe DM_INLINE. Ces objets sont automatiquement développés jusqu'à leurs composants dans la vue du tableau de règles, mais vous pouvez voir les noms des objets si vous désélectionnez la préférence **Auto-expand network and service objects with specified prefix** (Développer automatiquement les

objets réseau et de service avec le préfixe spécifié) du tableau de règles dans **Tools (Outils)** > **Preferences (Préférences)**.

- 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 les règles d'accès

Pour appliquer une règle d'accès, procédez comme suit :

Procédure

Étape 1 Choose **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**.

Les règles sont classées par interface et direction, avec un groupe distinct pour les règles globales. Si vous configurez des règles d'accès de gestion, elles sont répétées sur cette page. Ces groupes sont équivalents à la liste de contrôle d'accès étendue qui est créée et affectée à l'interface ou globalement en tant que groupe d'accès. Ces ACL apparaissent également sur la page ACL Manager (Gestionnaire d'ACL).

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez Add (Ajouter) > **Add Access Rule** (Ajouter une règle d'accès).
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter) > Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter) > Insert After (Insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont :

- **Interface** : l'interface à laquelle la règle s'applique. Sélectionnez Any (Tous) pour créer une règle globale. Pour les groupes de ponts en mode routé, vous pouvez créer des règles d'accès pour l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- **Source/Destination criteria** (Critères source/destination) : définissez la source (adresse d'origine) et la destination (adresse cible du flux de trafic). Vous configurez généralement des adresses IPv4 ou IPv6 d'hôtes ou de sous-réseaux, que vous pouvez représenter avec des groupes d'objets réseau ou des groupes d'objets de service réseau. Vous pouvez également préciser un nom d'utilisateur ou de groupe d'utilisateurs pour la source. En outre, vous pouvez utiliser le champ Service pour identifier le type spécifique de trafic si vous souhaitez cibler la règle de manière plus étroite que tout le trafic IP. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service. Si vous mettez en œuvre Cisco TrustSec, vous pouvez utiliser des groupes de sécurité pour définir la source et la destination.

Pour des informations détaillées sur les options, consultez Propriétés de la règle d'accès, à la page 10.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle d'accès dans votre configuration.

Propriétés de la règle d'accès

Lorsque vous ajoutez ou modifiez une règle d'accès, vous pouvez configurer les propriétés suivantes. Dans de nombreux champs, vous pouvez cliquer sur le bouton « ... » à droite de la zone d'édition pour sélectionner, créer ou modifier des objets disponibles pour le champ.

Interface

L'interface à laquelle la règle s'applique. Sélectionnez Any (Tous) pour créer une règle globale. Pour les groupes de ponts en mode routé, vous puvez sélectionner l'interface virtuelle de pont (BVI) ou les interfaces de membre du groupe de ponts.

Action : Autoriser/refuser

Indique si vous autorisez le trafic décrit ou si vous le refusez.

Critères de source

Les caractéristiques de l'initiateur du trafic que vous tentez de mettre en correspondance. Vous devez configurer la source, mais les autres propriétés sont facultatives.

Source

Adresse IPv4 ou IPv6 de la source. La valeur par défaut est **any**, qui correspond à toutes les adresses IPv4 ou IPv6 ; vous pouvez utiliser **any4** pour cibler IPv4 uniquement, ou **any6** pour cibler IPv6 uniquement. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0/255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::/60), le nom d'un objet réseau ou d'un groupe d'objets réseau, le nom d'un groupe d'objets de service réseau, ou le nom d'une interface.

Utilisateur

Si vous activez le pare-feu d'identité, vous pouvez spécifier un utilisateur ou un groupe d'utilisateurs comme source du trafic. L'adresse IP que l'utilisateur utilise actuellement correspondra à la règle. Vous pouvez spécifier un nom d'utilisateur (DOMAIN\user), un groupe d'utilisateurs (DOMAIN\group, notez que le double \ indique un nom de groupe) ou un groupe d'objets utilisateur. Pour ce champ, il est beaucoup plus facile de cliquer sur «**...**» pour sélectionner des noms à partir de votre groupe de serveurs AAA que de les taper.

Groupe sécurité

Si vous activez Cisco Trustsec, vous pouvez spécifier un nom ou une balise de groupe de sécurité (1 à 65 533), ou un objet de groupe de sécurité.

More Options (Plus d'options) > Source Service (Service source)

Notez que si vous définissez le service source, le protocole du service de destination doit lui correspondre (par exemple, TCP, avec ou sans définition de port). En règle générale, vous définissez le service de destination uniquement et non le service source.

Critères de destination

Les caractéristiques de la cible du trafic que vous tentez de mettre en correspondance. Vous devez configurer la destination, mais les autres propriétés sont facultatives.

Destination

L'adresse IPv4 ou IPv6 de destination. La valeur par défaut est **any**, qui correspond à toutes les adresses IPv4 ou IPv6 ; vous pouvez utiliser **any4** pour cibler IPv4 uniquement, ou **any6** pour cibler IPv6 uniquement. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0/255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::/60), le nom d'un objet réseau ou d'un groupe d'objets réseau, le nom d'un groupe d'objets de service réseau, ou le nom d'une interface.

Groupe sécurité

Si vous activez Cisco Trustsec, vous pouvez spécifier un nom ou une balise de groupe de sécurité (1-65533), ou un objet de groupe de sécurité.

Service

Le protocole du trafic, par exemple IP, TCP, UDP, et éventuellement les ports pour TCP, UDP ou SCTP. La valeur par défaut est IP, mais vous pouvez sélectionner un protocole plus précis pour cibler le trafic avec plus de granularité. En règle générale, vous sélectionnez un type d'objet de service. Pour TCP, UDP, et SCTP, vous pouvez spécifier des ports, par exemple, tcp/80, tcp/http, tcp/10-20 (pour une plage de ports), tcp-udp/80 (correspond à tout trafic TCP ou UDP sur le port 80), sctp/diameter, etc. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service.

Description

Une explication de l'objectif de la règle, jusqu'à 100 caractères par ligne. Vous pouvez saisir plusieurs lignes; chaque ligne est ajoutée en tant que remarque dans l'interface de ligne de commande, et les remarques sont placées avant la règle.



Remarque Si vous ajoutez des remarques avec des caractères non anglais sur une plateforme (comme Windows), puis essayez de les supprimer d'une autre plateforme (comme Linux), vous ne pourrez peut-être pas les modifier ou les supprimer, car les caractères d'origine peuvent ne pas être correctement reconnus. Cette limitation est due à une dépendance de plateforme sous-jacente qui code différents caractères linguistiques de différentes manières.

Enable Logging (Activer la journalisation) ; Logging Level (Niveau de journalisation) ; More Options (Plus d'options) > Logging Interval (Intervalle de journalisation)

Les options de journalisation définissent la façon dont les messages syslog seront générés pour les règles. Vous pouvez implémenter les options de journalisation suivantes :

Désélectionnez Enable Logging (Activer la journalisation)

Cela désactivera la journalisation pour la règle. Aucun message de journal système d'aucun type ne sera émis pour les connexions qui correspondent à cette règle.

Sélectionnez Enable Logging (Activer la journalisation) avec Logging Level (Niveau de journalisation) = Default (Par défaut)

Il fournit la journalisation par défaut pour les règles. Le message de journal système 106023 est émis pour chaque connexion refusée. Si le périphérique est soumis à une attaque, la fréquence d'émission de ce message peut avoir une incidence sur les services.

Sélectionnez Enable Logging (Activer la journalisation) avec Non-Default Logging Level (Niveau de journalisation autre que celui par défaut)

Cela fournit un message de journal système résumé, 106100, au lieu de 106023. Le message 106100 est émis lors du premier impact, puis à chaque intervalle configuré dans **Plus d'options > Intervalle de journalisation** (par défaut toutes les 300 secondes, vous pouvez spécifier 1-600), montrant le nombre d'impacts pendant cet intervalle. Le niveau de journalisation conseillé est **Informational** (Informations).

Le résumé des messages de refus peut réduire l'impact des attaques et éventuellement faciliter l'analyse des messages. Si vous subissez une attaque par déni de service, vous pourriez voir le message 106101, qui indique que le nombre de flux de refus en cache utilisés pour produire le nombre de correspondances pour le message 106100 a dépassé le maximum pour un intervalle. À ce stade, le périphérique arrête de collecter des statistiques jusqu'au prochain intervalle pour maîtriser l'attaque.

Indique si la règle s'applique à la direction In (Entrée) ou Out (Sortie).

Si la règle s'applique à la direction **In** ou **Out**. **In** est la valeur par défaut et il s'agit de la seule option pour les règles d'accès globales et de gestion.

More Options (Plus d'options) > Enable Rule (Activer la règle)

Si la règle est active sur le périphérique. Les règles désactivées s'affichent avec du texte barré dans le tableau de règles. La désactivation d'une règle vous permet d'arrêter son application au trafic sans la supprimer, de sorte que vous pouvez la réactiver ultérieurement si vous décidez que vous en avez besoin.

More Options (Plus d'options) > Time Range (Plage de temps)

Le nom de l'objet de plage temporelle qui définit les heures du jour et les jours de la semaine où la règle doit être active. Si vous ne spécifiez pas de plage temporelle, la règle est toujours active.

Configurer les options avancées pour les règles d'accès

Les options de règles d'accès avancées vous permettent de personnaliser certains aspects du comportement des règles, mais ces options ont des valeurs par défaut appropriées dans la plupart des cas.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)** .

Étape 2 Cliquez sur le bouton **Advanced** (Avancé) sous le tableau de règles.

Étape 3 Configurez les options suivantes :

- **Advanced Logging Settings** (Paramètres de journalisation avancée) : si vous configurez une journalisation différente des valeurs par défaut, le système met en cache les flux refusés afin d'établir des statistiques pour le message 106100, comme expliqué dans Évaluation des messages Syslog pour les règles d'accès, à la page 18. Pour éviter une consommation illimitée des ressources mémoire et processeur, l'ASA limite le nombre de flux *refusés* simultanés, car ceux-ci peuvent indiquer une attaque. Le message 106101 est généré lorsque cette limite est atteinte. Vous pouvez contrôler les paramètres suivants relatifs au message 106101.
  - Nombre maximal de flux refusés : nombre maximal de flux refusés autorisés avant que l'ASA cesse de les mettre en cache, entre 1 et 4 096. La valeur par défaut est 4 096.
  - Intervalle d'alerte : la durée (de 1 à 3 600 secondes) entre l'émission du message de journal système 106101, qui indique que le nombre maximal de flux de refus a été atteint. La valeur par défaut est de 300 secondes.

- **Per User Override (tableau de remplacement d'utilisateur)** : s'il faut autoriser une liste de contrôle d'accès d'utilisateur dynamique téléchargée pour l'autorisation de l'utilisateur à partir d'un serveur RADIUS de remplacer l'ACL attribuée à l'interface. Par exemple, si l'ACL de l'interface refuse tout le trafic provenant de 10.0.0.0, mais que l'ACL dynamique autorise tout le trafic provenant de 10.0.0.0, l'ACL dynamique remplace l'ACL de l'interface pour cet utilisateur. Cochez la case **Per User Override** (Remplacement par utilisateur) pour chaque interface qui doit autoriser les remplacements par l'utilisateur (direction entrante uniquement). Si la fonctionnalité de remplacement par utilisateur est désactivée, la règle d'accès fournie par le serveur RADIUS est combinée avec la règle d'accès configurée sur cette interface.

  Par défaut, le trafic VPN d'accès à distance n'est pas comparé aux ACL d'interface. Toutefois, si vous désélectionnez l'option **Enable inbound VPN sessions to bypass interface access lists (Activer les sessions VPN entrantes pour** contourner les listes d'accès d'interface) dans Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Connection Profiles (Profils de connexion) Secure Client (services client sécurisés), le comportement dépend de la présence d'un filtre VPN dans la stratégie de groupe (voir le champ Filter (Filtre) dans Configuration (Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > Add/Edit (Ajouter/Modifier) > General (Général) > More Options (Plus d'options)), ainsi que du paramètre Per User Override.
  - Aucun remplacement par utilisateur, pas de filtre VPN : le trafic est comparé à l'ACL de l'interface.

- Aucun remplacement par utilisateur, filtre VPN : le trafic est d'abord comparé à l'ACL de l'interface, puis au filtre VPN.
- Par remplacement d'utilisateur, filtre VPN : le trafic est comparé au filtre VPN uniquement.

- **Object Group Search Setting** (Paramètre de recherche des groupes d'objets) : vous pouvez réduire la mémoire requise pour rechercher les règles d'accès utilisant des groupes d'objets en sélectionnant **Enable Object Group Search Algorithm** (Activer l'algorithme de recherche des groupes d'objets), mais cela se fait au détriment des performances de recherche des règles. Lorsqu'elle est activée, la recherche par groupe d'objets ne développe pas les objets de réseau, mais recherche dans les règles d'accès les correspondances basées sur les définitions de ces groupes.

  Sélectionnez **Enable Object Group Search Threshold** (Activer le seuil de recherche des groupes d'objets) afin de définir un seuil permettant d'éviter une 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 objets de groupe de sécurité. 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.

- **Forward Reference Setting** (Paramètre de référence anticipée) **— (Versions antérieures à 7.18 uniquement.)** Normalement, vous ne pouvez pas référencer un objet ou un groupe d'objets qui n'existe pas dans une ACL ou un groupe d'objets, ni supprimer un objet actuellement référencé. Vous ne pouvez pas non plus référencer une liste de contrôle d'accès qui n'existe pas dans une commande **access-group** (pour appliquer les règles d'accès). Cependant, vous pouvez modifier ce comportement par défaut afin d'autoriser les références anticipées (« forward references ») vers des objets ou des ACL avant leur création. Jusqu'à ce que vous créiez les objets ou les listes de contrôle d'accès, toutes les règles ou tous les groupes d'accès qui les référencent sont ignorés. Sélectionnez **Enable the Forward Reference of Objects and Object-Groups** (Activer les références anticipées des objets et des groupes d'objets) pour activer cette fonctionnalité. Sachez que si vous activez le référencement vers l'avant, ASDM ne peut pas faire la différence entre une référence type à un objet existant et une référence vers l'avant.

  Remarque
  Ce paramètre est activé par défaut et n'est plus configurable à partir de l'ASA 9.18(1).

Étape 4 Cliquez sur **OK**.

Configurer les règles d'accès de gestion

Vous pouvez configurer une liste de contrôle d'accès d'interface qui contrôle le trafic de gestion jusqu'au boîtier d'un homologue spécifique (ou d'un ensemble d'homologues) vers l'ASA. Un scénario dans lequel ce type d'ACL serait utile est lorsque vous souhaitez bloquer les attaques par déni de service IKE.

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.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Règles d'accès de gestion**.

Les règles sont classées par interface. Chaque groupe équivaut à la liste de contrôle étendue qui est créée et affectée à l'interface en tant qu'ACL de plan de commande. Ces listes de contrôle d'accès apparaissent également dans les pages Access Rules (Règles d'accès) et ACL Manager (Gestionnaire d'ACL).

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez **Add (Ajouter) > Add Management Access Rule (Ajouter une règle d'accès de gestion)**.
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter) > Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter) > Insert After (Insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont :

- **Interface** : l'interface à laquelle la règle s'applique. Pour les groupes de ponts en mode routé, vous pouvez créer des règles d'accès pour l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- **Source/Destination criteria** (Critères source/destination) : définissez la source (adresse d'origine) et la destination (adresse cible du flux de trafic). Vous configurez généralement l'adresse IPv4 ou IPv6 des hôtes ou des sous-réseaux, que vous pouvez représenter avec des groupes d'objets réseau. Vous pouvez également préciser un nom d'utilisateur ou de groupe d'utilisateurs pour la source. En outre, vous pouvez utiliser le champ Service pour identifier le type spécifique de trafic si vous souhaitez cibler la règle de manière plus étroite que tout le trafic IP. Si vous mettez en œuvre Cisco TrustSec, vous pouvez utiliser des groupes de sécurité pour définir la source et la destination.

Pour des informations détaillées sur les options, consultez Propriétés de la règle d'accès, à la page 10.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle dans votre configuration.

Configurer les règles EtherType

Les règles EtherType s'appliquent au trafic de couche 2 non IP sur les interfaces membres de groupes de ponts (en mode de pare-feu routé ou transparent). Vous pouvez utiliser ces règles pour autoriser ou abandonner le trafic en fonction de la valeur EtherType dans le paquet de couche 2. Les règles EtherType vous permettent de contrôler le flux du trafic non IP dans l'ASA.

Vous pouvez appliquer des règles d'accès étendues et EtherType à une interface membre d'un groupe de ponts. Les règles EtherType prévalent sur les règles d'accès étendues.

Procédure

Étape 1 Choisissez **ConfigurationFirewall (Pare-feu)EtherType Rules (Règles EtherType)**

Les règles sont classées par interface et par direction. Chaque groupe équivaut à l'ACL EtherType créée et affectée à l'interface.

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez **Add (Ajouter)** > **Add EtherType Rule (Ajouter une règle EtherType)** .
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter)** > **Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter)** > **Insert After (Insérer après)** .
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont :

- **Interface** : l'interface à laquelle la règle s'applique.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- EtherType : vous pouvez mettre en correspondance le trafic en utilisant les options suivantes :
  - **any** : correspond à tout le trafic.
  - **bpdu** : unités de données de protocole de pont, qui sont autorisées par défaut. Lorsque vous appliquez la configuration, ce mot-clé est converti en **dsap bpdu** sur le périphérique.
  - **dsap** : l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2. Vous devez également inclure l'adresse que vous souhaitez autoriser ou refuser en hexadécimal, de 0x01 à 0xff, dans **DSAP Value** (Valeur DSAP). Voici les valeurs de certaines adresses courantes :
    - **0x42** : unités de données de protocole de pont (BPDU). Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap bpdu** sur le périphérique.
    - **0xe0** : Internet Packet Exchange (IPX) 802.2 LLC. Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap ipx** sur le périphérique.
    - **0xfe** : Intermediate System to Intermediate System (IS-IS). Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap isis** sur le périphérique.
    - **0xff** : format brut IPX 802.3. Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap raw-ipx** sur le périphérique.
  - **eii-ipx** : format IPX Ethernet II, EtherType 0x8137.

- **ipx** : Internet Packet Exchange (IPX). Ce mot-clé est un raccourci pour configurer trois règles distinctes, pour **dsap ipx** , **dsap raw-ipx** , et **eii-ipx** . La conversion est effectuée lorsque vous appliquez la configuration au périphérique.
- **isis** : Intermediate System to Intermediate System (IS-IS). Lorsque vous appliquez la configuration, ce mot-clé est converti en **dsap isis** sur le périphérique.
- **mpls-multicast** : multidiffusion MPLS.
- **mpls-unicast :** monodiffusion MPLS.
- *hex_number* —Tout EtherType qui peut être identifié par un nombre hexadécimal de 16 bits de 0x600 à 0xffff. Consultez la RFC 1700, « Nombres attribués », à l'adresse http://www.ietf.org/rfc/rfc1700.txt pour obtenir la liste des EtherTypes.

- **Description** : une explication de l'objectif de la règle, jusqu'à 100 caractères par ligne. Vous pouvez saisir plusieurs lignes; chaque ligne est ajoutée en tant que remarque dans l'interface de ligne de commande, et les remarques sont placées avant la règle.
- **More Options (Autres options)** > **Direction** : indique si la règle s'applique à la direction **In** (Entrée) ou **Out** (Sortie). **In (Entrée)** est le paramètre par défaut.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle dans votre configuration.

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 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ICMP**.

Étape 2 Configurez les règles ICMP.

a) Ajoutez une règle (**Add (Ajouter) > Rule (Règle)**, **Add (Ajouter) > IPv6 Rule (Règle IPv6)** ou **Add (Ajouter) > Insert (Insérer)**), ou sélectionnez une règle et modifiez-la.
b) Sélectionnez le type ICMP que vous souhaitez contrôler, ou **any** pour appliquer la règle à tous les types.
c) Sélectionnez l'interface à laquelle la règle s'applique. Vous devez créer des règles distinctes pour chaque interface.
d) Choisissez si vous autorisez ou refusez l'accès pour le trafic correspondant.
e) Sélectionnez **Any Address** (Toute adresse) pour appliquer la règle à tout le trafic. Sinon, saisissez l'adresse et le masque (pour IPv4) ou l'adresse et la longueur du préfixe (pour IPv6) de l'hôte ou du réseau que vous essayez de contrôler.
f) Cliquez sur **OK**.

Étape 3 (Facultatif) Pour définir les limites de messages ICMP inaccessibles, définissez les options suivantes. L'augmentation de la limite de débit, ainsi que l'activation de l'option **Decrement time to live for a connection (Décrémenter la durée de vie d'une connexion)** dans une politique de service (dans la boîte de dialogue Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Rule Actions (Actions de règle) > Connection Settings (Paramètres de connexion)), est nécessaire pour permettre un traceroute à travers l'ASA qui affiche l'ASA comme l'un des sauts.

- Limitation de débit— : définit la limite de débit des messages unreachable, entre 1 et 100 messages par seconde. La valeur par défaut est de 1 message par seconde.
- Taille de la rafale—définit le débit en rafale, entre 1 et 10. Le système envoie ce nombre de réponses, mais les réponses suivantes ne sont pas envoyées tant que la limite de débit n'est pas atteinte.

Étape 4 Cliquez sur **Apply**.

Surveillance des règles d'accès

La page Règles d'accès comprend le nombre de résultats pour chaque règle. Passez le pointeur sur le nombre d'accès pour afficher l'heure de mise à jour et l'intervalle du compteur. Pour réinitialiser le nombre d'accès, cliquez avec le bouton droit sur la règle et sélectionnez **Clear Hit Count** (Effacer le nombre d'accès), mais sachez que cela efface le compteur de toutes les règles appliquées à la même interface dans la même direction.

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 et le nombre maximal de flux de refus mis en cache dans les paramètres avancés; voir Configurer les options avancées pour les règles d'accès, à la page 13.

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 l'écran suivant : Configuration > Firewall (Pare-feu) > Access Rules (Règles d'accès).

Nom de la caractéristique	Versions de plateforme	Description
Critères d'accès globaux	8.3(1)	Des règles d'accès globales ont été introduites. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Access Rules (Règles d'accès).
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.
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 l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > EtherType Rules (Règles EtherType).
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.
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 écrans suivants : Configuration > Firewall (Pare-feu) > Access Rules (Règles d'accès) Configuration (Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > General (Général) > More Options (Autres options)
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 écrans suivants : Configuration > Firewall (Pare-feu) > Objects (Objets) > Service Objects/Groups (Objets/groupes de service) Configuration (Configuration) > Firewall (Pare-feu) > Access Rule (Règle d'accès)

Nom de la caractéristique	Versions de plateforme	Description
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 l'écran suivant : Configuration (Configuration) > Device Management (Gestion des périphériques) > Advanced (Avancé) > Rule Engine (Moteur de règles).
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.
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 les boîtes de dialogue d'ajout/modification des règles d'accès sur la page **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**.
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. Réécrivez les règles **bpdu** pour utiliser **dsap 0x42**. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**.
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 écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**, **Configuration** > **Firewall (Pare-feu)** > **Ethertype Rules (Règles 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 écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**.

Nom de la caractéristique	Versions de plateforme	Description
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 modifié l'écran suivant : **Configuration** > **Access Rules (Critères d'accès)** > **Advanced (Avancé)**.
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.