Listes de contrôle d'accès

Les listes de contrôle d'accès (ACL) sont utilisées par de nombreuses fonctions différentes. Lorsqu'elles sont appliquées aux interfaces ou globalement en tant que règles d'accès, elles autorisent ou refusent le trafic qui passe par le périphérique. Pour les autres fonctionnalités, l'ACL sélectionne le trafic auquel la fonctionnalité s'appliquera, en effectuant un service de correspondance plutôt qu'un service de contrôle.

Les sections suivantes expliquent les bases des listes de contrôle d'accès et comment les configurer et les surveiller. Les règles d'accès, les listes de contrôle d'accès appliquées globalement ou aux interfaces, sont expliquées plus en détail dans Règles d'accès.

À propos des ACL

Les listes de contrôle d'accès (ACL) identifient les flux de trafic en fonction d'une ou de plusieurs caractéristiques, notamment l'adresse IP source et de destination, le protocole IP, les ports, EtherType et d'autres paramètres, selon le type d'ACL. Les ACL sont utilisées dans une variété de fonctionnalités. Les listes de contrôle d'accès sont composées d'une ou de plusieurs entrées de contrôle d'accès (ACE).

Types d'ACL

L'ASA utilise les types d'ACL suivants :

- ACL étendues : les listes de contrôle d'accès étendues sont le principal type que vous utiliserez. Ces listes de contrôle d'accès sont utilisées pour les critères d'accès afin d'autoriser et de refuser le trafic via le périphérique, ainsi que pour la correspondance du trafic de nombreuses fonctionnalités, notamment les politiques de service, les règles AAA, WCCP, le filtre de trafic de réseau de zombies, les stratégies de groupe VPN et les politiques DAP. Dans ASDM, bon nombre de ces fonctionnalités possèdent leurs propres pages de règles et ne peuvent pas utiliser les listes de contrôle d'accès étendues que vous définissez dans ACL Manager, bien qu'ACL Manager affiche les listes de contrôle d'accès créées sur ces pages. Consultez Configurer les ACL étendues, à la page 8.

- ACL EtherType : les listes de contrôle d'accès EtherType s'appliquent uniquement au trafic de couche 2 non IP sur les interfaces de membre de groupe de ponts. Vous pouvez utiliser ces règles pour autoriser ou abandonner le trafic en fonction de la valeur EtherType dans le paquet de couche 2. Les listes de contrôle d'accès EtherType vous permettent de contrôler le flux du trafic non IP sur le périphérique. Voir Configurer les règles EtherType.
- ACL de type Web : les listes de contrôle d'accès de type Web sont utilisées pour filtrer le trafic VPN SSL sans client. Ces listes de contrôle d'accès peuvent refuser l'accès en fonction des URL ou des adresses de destination. Consultez Configurer les ACL de type Web, à la page 13.
- ACL standard : les listes de contrôle d'accès standard identifient le trafic par adresse de destination uniquement. Il existe peu de fonctionnalités qui les utilisent : listes de routage et filtres VPN. Comme les filtres VPN permettent également des listes d'accès étendues, limitez l'utilisation de l'ACL standard aux listes de routage. Consultez Configurer les ACL standard, à la page 12.

Le tableau suivant répertorie certaines utilisations courantes des listes de contrôle d'accès et le type à utiliser.

Tableau 1 : Types d'ACL et utilisations courantes

Utilisation de l'ACL	Type d'ACL	Description
Contrôler l'accès au réseau pour le trafic IP (mode routé et transparent)	Étendu	L'ASA n'autorise aucun trafic d'une interface de sécurité inférieure vers une interface de sécurité supérieure, à moins qu'il ne soit explicitement autorisé par une liste de contrôle d'accès étendue. En mode routé, vous devez utiliser une liste de contrôle d'accès pour autoriser le trafic entre une interface membre d'un groupe de ponts et une interface située à l'extérieur du même groupe de ponts. **Remarque** Pour accéder à l'interface ASA pour l'accès de gestion, vous n'avez pas non plus besoin d'une liste de contrôle 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.
Identifier le trafic pour les règles AAA	Étendu	Les règles AAA utilisent des listes de contrôle d'accès pour identifier le trafic.
Augmenter le contrôle d'accès au réseau pour le trafic IP d'un utilisateur donné	Étendue, téléchargée à partir d'un serveur AAA pour chaque utilisateur	Vous pouvez configurer le serveur RADIUS pour télécharger une liste de contrôle d'accès dynamique à appliquer à l'utilisateur, ou le serveur peut envoyer le nom d'une liste de contrôle d'accès que vous avez déjà configurée sur l'ASA.
Accès et filtrage au VPN	Étendu Standard	Les stratégies de groupe pour l'accès à distance et les VPN de site à site utilisent des listes de contrôle d'accès standard ou étendues pour le filtrage. Les VPN d'accès à distance utilisent également des listes de contrôle d'accès étendues pour les configurations de pare-feu client et les politiques d'accès dynamique.

Utilisation de l'ACL	Type d'ACL	Description
Identifier le trafic dans une mise en correspondance des cartes de classes de trafic pour le cadre de politiques modulaires	Étendu	Les listes de contrôle d'accès peuvent être utilisées pour identifier le trafic dans une carte de trafic, utilisée par les fonctionnalités qui prennent en charge le cadre de politiques modulaires. Les fonctionnalités qui prennent en charge le cadre de politique modulaire comprennent les paramètres TCP et généraux, ainsi que l'inspection.
Pour les interfaces membres d'un groupe de ponts, contrôler l'accès au réseau pour le trafic non IP	EtherType	Vous pouvez configurer une liste de contrôle d'accès qui contrôle le trafic en fonction de son EtherType pour toute interface membre d'un groupe de ponts.
Identifier le filtrage et la redistribution des routes	Standard Étendue	Divers protocoles de routage utilisent des listes de contrôle d'accès standard pour le filtrage et la redistribution (au moyen de listes de routage) pour les adresses IPv4 et des listes de contrôle d'accès étendues pour IPv6.
Filtrage pour le VPN SSL sans client	Type Web	Vous pouvez configurer une liste de contrôle d'accès de type Web pour filtrer les URL et les destinations.

Le gestionnaire d'ACL

Le gestionnaire d'ACL apparaît sous deux formes :

- Dans la fenêtre principale, par exemple, en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **ACL Manager (Gestionnaire d'ACL)**. Dans ce cas, le gestionnaire d'ACL affiche uniquement les listes d'accès étendues. Ces listes de contrôle d'accès comprennent celles générées par les règles que vous créez dans les pages des règles d'accès, des règles de politique de service et des règles AAA. Veillez à ce que les modifications que vous apportez dans le gestionnaire d'ACL n'affectent pas négativement ces règles; les modifications que vous apportez ici seront répercutées sur ces autres pages.
- À partir d'une politique qui nécessite une ACL, en cliquant sur le bouton **Manage** (Gérer) à côté du champ. Dans ce cas, le gestionnaire d'ACL peut avoir des onglets distincts pour les listes d'ACL standard et étendues, si la politique autorise l'un ou l'autre de ces types. Sinon, l'affichage est filtré pour afficher uniquement les listes de contrôle d'accès standard, étendues ou de type Web. Le gestionnaire d'ACL n'affiche jamais les listes de contrôle d'accès EtherType.

Il existe des pages distinctes pour les listes de contrôle d'accès standard et les listes de contrôle d'accès de type Web, afin que vous puissiez les configurer dans la fenêtre principale. Ces pages sont fonctionnellement équivalentes au gestionnaire d'ACL sans le nom :

- ACL standard : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Standard ACL (ACL standard)**.
- ACL de type Web : **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Advanced (Avancé)** > **Web ACLs (ACL Web)**.

Noms d'ACL

Chaque liste de contrôle d'accès (ACL) est associée à un nom ou à un ID numérique, tel que outside_in, OUTSIDE_IN ou 101. Limitez les noms à 241 caractères ou moins. Envisagez d'utiliser toutes les lettres majuscules pour faciliter la recherche du nom lors de l'affichage d'une configuration en cours d'exécution.

Développez une convention de dénomination qui vous aidera à identifier l'objectif prévu de la liste de contrôle d'accès. Par exemple, ASDM utilise la convention *interface-name_purpose_direction*, telle que « outside_access_in », pour une liste de contrôle d'accès appliquée à l'interface « externe » dans la direction entrante.

Traditionnellement, les identifiants d'ACL étaient des numéros. Les listes de contrôle d'accès standard étaient dans la plage de 1 à 99 ou de 1 300 à 1 999. Les listes de contrôle d'accès étendues étaient dans la plage 100-199 ou 2 000-2 699. L'ASA n'applique pas ces plages, mais si vous souhaitez utiliser des chiffres, vous pouvez vous en tenir à ces conventions pour maintenir la cohérence avec les routeurs exécutant le logiciel IOS.

Ordre des entrées de contrôle d'accès

Une ACL est composée d'une ou de plusieurs ACE. Sauf si vous insérez explicitement une ACE à une ligne donnée, chaque ACE que vous saisissez pour un nom d'ACL donné est ajoutée à la fin de l'ACL.

L'ordre des ACE est important. Lorsque l'ASA décide de transférer ou d'abandonner un paquet, l'ASA teste le paquet par rapport à chaque ACE dans l'ordre dans lequel les entrées sont répertoriées. Une fois qu'une correspondance est trouvée, aucune autre Ace n'est vérifiée.

Ainsi, si vous placez une règle plus spécifique après une règle plus générale, la règle la plus spécifique pourrait ne jamais être atteinte. Par exemple, si vous souhaitez autoriser le réseau 10.1.1.0/24, mais abandonner le trafic de l'hôte 10.1.1.15 sur ce sous-réseau, l'ACE qui refuse 10.1.1.15 doit venir avant celle qui autorise 10.1.1.0/24. Si l'ACE d'autorisation 10.1.1.0/24 arrive en premier, 10.1.1.15 sera autorisé et l'ACE de refus ne correspondra jamais.

Utilisez les boutons Haut et Bas pour repositionner les règles si nécessaire.

Autoriser/refuser ou mettre en correspondance/aucune correspondance

Les entrées de contrôle d'accès « autorisent » ou « refusent » le trafic qui correspond à la règle. Lorsque vous appliquez une liste de contrôle d'accès à une fonctionnalité qui détermine si le trafic est autorisé par l'ASA ou est abandonné, comme les règles d'accès globales et d'interface, « autoriser » et « refuser » signifient ce qu'elles indiquent.

Pour d'autres fonctionnalités, telles que les règles de politique de service, « autoriser » et « refuser » signifient en fait « correspondance » ou « aucune correspondance ». Dans ces cas, la liste de contrôle d'accès sélectionne le trafic qui doit recevoir les services de cette fonctionnalité, tels que l'inspection d'application ou le redirection vers un module de service. Le trafic « refusé » est simplement le trafic qui ne correspond pas à la liste de contrôle d'accès et ne recevra donc pas le service. (Dans ASDM, les règles de politique de service utilisent en fait Match/Do Not Match (Correspondance/Aucune correspondance), et les règles AAA utilisent Authenticate/Do Not Authenticate (Authentifier/Ne pas authentifier), par exemple, mais dans la CLI, il s'agit toujours de permit/deny.)

Refus implicite du contrôle d'accès

Les listes de contrôle d'accès utilisées pour les règles d'accès de transit comportent une instruction de refus implicite à la fin. Ainsi, pour les listes de contrôle d'accès de contrôle du trafic telles que celles appliquées aux interfaces, si vous n'autorisez pas explicitement un type de trafic, ce trafic est abandonné. Par exemple, si vous souhaitez autoriser tous les utilisateurs à accéder à un réseau par l'intermédiaire de l'ASA, à l'exception d'une ou de plusieurs adresses particulières, vous devez refuser ces adresses particulières, puis autoriser toutes 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 utilisées pour sélectionner le trafic pour un service, vous devez « autoriser » explicitement le trafic ; tout trafic non « autorisé » ne sera pas mis en correspondance pour le service ; le trafic « refuser » contourne le service.

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 commande EtherType ACE, le trafic IP et ARP est refusé ; seul le trafic de protocole physique, tel que la négociation automatique, est toujours autorisé.

Adresses IP utilisées pour les listes de contrôle d'accès étendues lorsque vous utilisez la NAT

Lorsque vous utilisez la NAT ou la PAT, vous traduisez des adresses ou des ports, en faisant généralement correspondre les adresses internes et externes. Si vous devez créer une liste de contrôle d'accès étendue qui s'applique à des adresses ou des ports qui ont été traduits, vous devez déterminer s'il faut utiliser les adresses ou les ports réels (non traduits) ou ceux mappés. Les exigences varient en fonction de la fonctionnalité.

L'utilisation de l'adresse et du port réels signifie que si la configuration de la NAT change, vous n'avez pas besoin de modifier les listes de contrôle d'accès.

Fonctionnalités qui utilisent des adresses IP réelles

Les commandes et fonctionnalités suivantes utilisent des adresses IP réelles dans les listes de contrôle d'accès, même si l'adresse vue sur une interface est l'adresse mappée :

- Règles d'accès (ACL étendues référencées par la commande **access-group**)
- Règles de politique de service (commande **match access-list** de Modular Policy Framework)
- Classification du trafic du filtre de trafic de zombie (commande**Dynamic-filter enable classify-list**)
- Règles AAA (commandes **aaa ... match**)
- WCCP (commande **wccp redirect-list group-list**)

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).

Fonctionnalités qui utilisent des adresses IP mappées

Les fonctionnalités suivantes utilisent des ACL, mais ces ACL utilisent les valeurs mappées comme elles sont vues sur une interface :

- ACL IPsec
- ACL de commande **capture**
- ACL par utilisateur
- ACL de protocole de routage
- Toutes les autres ACL de fonctionnalité.

ACE temporelles

Vous pouvez appliquer des objets de plage temporelle aux ACE étendues et de type Web afin que les règles soient actives pendant des périodes spécifiques uniquement. Ces types de règles vous permettent de faire la différence entre les activités acceptables à certaines heures de la journée et inacceptables à d'autres heures. Par exemple, vous pouvez appliquer des restrictions supplémentaires pendant les heures de travail et les assouplir après les heures de travail ou pendant le repas. Inversement, vous pourriez essentiellement arrêter votre réseau en dehors des heures de travail.

Vous ne pouvez pas créer des règles basées sur le temps qui ont exactement les mêmes critères de protocole, de source, de destination et de service d'une règle qui n'inclut pas d'objet de plage temporelle. La règle non basée sur le temps remplace toujours la règle basée sur le temps en double, car elles sont redondantes.

Remarque Les utilisateurs peuvent connaître un retard d'environ 80 à 100 secondes après l'heure de fin spécifiée pour que la liste de contrôle d'accès devienne inactive. Par exemple, si l'heure de fin spécifiée est 3:50, comme l'heure de fin est inclusive, la commande est récupérée n'importe où entre 3:51:00 et 3:51:59. Une fois la commande reçue, l'ASA termine toute tâche en cours d'exécution, puis prend en charge la commande pour désactiver l'ACL.

Licences pour les listes de contrôle d'accès

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

Cependant, pour utiliser **sctp** comme protocole dans une entrée, vous devez avoir une licence Carrier.

Lignes directrices pour les ACL

Mode pare-feu

- Les listes de contrôle d'accès étendues et standard sont prises en charge dans les modes de pare-feu routé et transparent.
- Les listes de contrôle d'accès de type Web sont prises en charge en mode routé uniquement.
- Les listes de contrôle d'accès EtherType sont prises en charge pour les interfaces de membre de groupe de ponts uniquement, en modes routé et transparent.

Basculement et mise en grappe

Les sessions de configuration ne sont pas synchronisées sur les unités de basculement ou en grappe. Lorsque vous validez les modifications dans une session, elles sont appliquées normalement dans toutes les unités de basculement et de grappe.

IPv6

- Les listes de contrôle d'accès étendues et de type Web permettent une combinaison d'adresses IPv4 et IPv6.
- Les listes de contrôle d'accès standard n'autorisent pas les adresses IPv6.
- Les listes de contrôle d'accès EtherType ne contiennent pas d'adresses IP.

Directives supplémentaires

- Lorsque vous spécifiez un masque réseau, la méthode est différente de la commande **access-list** du logiciel IOS de Cisco. L'ASA utilise un masque réseau (par exemple, 255.255.255.0 pour un masque de classe C). Le masque IOS de Cisco utilise des caractères génériques (par exemple, 0.0.0.255).
- 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)**.
- (ACL étendue uniquement) Les fonctionnalités suivantes utilisent des listes de contrôle d'accès, mais ne peuvent pas accepter une liste de contrôle d'accès avec pare-feu d'identité (précisant les noms d'utilisateur ou de groupe), FQDN (noms de domaine complets) ou valeurs Cisco TrustSec :
  - commande **crypto map** du VPN
  - commande **group-policy** de VPN, sauf pour **vpn-filter**
  - WCCP
  - DAP

Configurer les ACL

Les sections suivantes expliquent comment configurer les différents types d'ACL génériques, à l'exception de ceux utilisés comme règles d'accès (y compris EtherType), règles de politique de service, règles AAA et autres utilisations pour lesquelles ASDM fournit une page à usage spécial pour ces politiques basées sur des règles.

Configurer les ACL étendues

Une ACL étendue est représentée comme un conteneur nommé d'ACE. Pour créer une nouvelle ACL, vous devez d'abord créer le conteneur. Ensuite, vous pouvez ajouter des ACE, modifier les ACE existantes et réorganiser les ACE à l'aide du tableau dans ACL Manager.

La liste de contrôle d'accès étendue peut inclure une combinaison d'adresses IPv4 et IPv6.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **ACL Manager (Gestionnaire d'ACL)**.

Étape 2 Si vous créez une nouvelle liste de contrôle d'accès, choisissez **Add (Ajouter)** > **Add ACL (Ajouter une ACL)**, saisissez un nom et cliquez sur OK (**OK**).

Le conteneur d'ACL est ajouté à la table. Vous pouvez la renommer ultérieurement en la sélectionnant et en cliquant sur **Edit** (Modifier).

Étape 3 Effectuez l'une des actions suivantes :

- Pour ajouter une ACE à la fin de la liste de contrôle d'accès, sélectionnez le nom de l'ACL ou toute ACE dans celui-ci, puis choisissez **Add> Add ACE (Ajouter> Ajouter une ACE)**.
- Pour insérer une ACE à un emplacement spécifique, sélectionnez une ACE existante et choisissez **Add> Insert (ajouter> insérer)** pour ajouter l'ACE au-dessus de la règle, ou choisissez **Add> Insert After (ajouter> insérer après)**.
- Sélectionnez une règle et cliquez sur **Edit** (Modifier).

Étape 4 Renseignez les propriétés de l'ACE. Les principales options à sélectionner sont :

- **Action : Permit/Deny (Autoriser/Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).
- **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 des ACE étendues, à la page 9.

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

Étape 5 Cliquez sur **Apply** (Appliquer).

Propriétés des ACE étendues

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

Action : Permit/Deny (Autoriser/Refuser)

Indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).

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 les noms de votre groupe de serveurs AAA que de les saisir.

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.

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 à 65 533), 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 préciser les 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. Pour des informations détaillées sur la spécification des services, consultez Caractéristiques de service dans les ACE étendues, à la page 11.

Description

Une explication de l'objectif de l'ACE, 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 l'ACE.

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. Ces options s'appliquent uniquement aux listes de contrôle d'accès, c'est-à-dire à celles associées aux interfaces ou appliquées globalement. Les options sont ignorées pour les listes de contrôle d'accès utilisées pour d'autres fonctionnalités. 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 **« Information »** .

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.

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.

Caractéristiques de service dans les ACE étendues

Pour le service de destination dans une ACE étendue, vous pouvez spécifier l'un des critères suivants. Les options sont similaires, mais plus limitées, pour le service source, qui se limite aux critères TCP, UDP, TCP-UDP ou SCTP. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service.

Nom de l'objet

Le nom de tout type d'objet de service ou de groupe d'objets de service. Ces objets peuvent inclure bon nombre des spécifications expliquées ci-dessous, vous permettant de réutiliser facilement les définitions de service parmi les listes de contrôle d'accès. Il existe de nombreux objets prédéfinis, vous pouvez donc trouver ce dont vous avez besoin sans avoir à saisir manuellement les spécifications ou à créer vos propres objets.

Protocole

Un nombre entre 1-255, ou un nom bien connu, tel que **ip**, **tcp**, **udp**, **gre**, etc.

Ports TCP, UDP, TCP-UDP, SCTP

Vous pouvez inclure des spécifications de port dans les mots-clés **tcp**, **udp**, **tcp-udp** et **sctp**. Le mot-clé tcp-udp vous permet de définir des ports pour les deux protocoles sans avoir à les spécifier séparément. Vous pouvez utiliser les méthodes suivantes pour préciser les ports :

- Port unique : tcp/80, udp/80, tcp-udp/80, sctp/3868, ou un nom de service bien connu, tel que tcp/www, udp/snmp ou sctp/diameter.
- Plage de ports : tcp/1-100, udp/1-100, tcp-udp/1-100, sctp/1-100 correspond aux ports 1 à 100 inclus.
- Non égal à un port : ajoutez != au début de la spécification, par exemple, !=tcp/80 pour correspondre à tout trafic TCP, à l'exception du port TCP 80 (HTTP).
- Moins d'un numéro de port : ajoutez <, par exemple <tcp/150 pour faire correspondre le trafic TCP pour tout port inférieur à 150.
- Supérieur à un numéro de port : ajoutez >, par exemple, >tcp150 pour faire correspondre le trafic TCP pour tout port supérieur à 150.

Remarque DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC et Talk nécessitent chacun une définition pour TCP et une pour UDP. TACACS+ nécessite une définition pour le port 49 sur TCP.

Messages ICMP et ICMP6

Vous pouvez cibler des messages spécifiques (comme les messages de demande d'écho et de réponse ping) et même des codes de message. Il existe de nombreux objets prédéfinis qui couvrent ICMP (pour IPv4) et ICMP6 (pour IPv6), de sorte que vous n'aurez peut-être pas besoin de définir manuellement les critères. Le format est le suivant :

icmp/*icmp_message_type*[/*icmp_message_code*]

icmp6/*icmp6_message_type*[/*icmp6_message_code*]

Où le type de message est 1-255 ou un nom bien connu, et le code est 0-255. Assurez-vous que le numéro que vous sélectionnez correspond à un type ou à un code réel, sinon l'ACE ne sera jamais mise en correspondance.

Configurer les ACL standard

Une ACL standard est représentée comme un conteneur nommé d'ACE. Pour créer une nouvelle liste de contrôle d'accès, vous devez d'abord créer le conteneur. Ensuite, vous pouvez ajouter des ACE, modifier les ACE existantes et réorganiser les ACE à l'aide de la table d'ACL standard. Le tableau peut apparaître sous forme d'onglet dans ACL Manager (Gestionnaire d'ACL) lorsque vous configurez les ACL tout en configurant les politiques qui les utilisent. Si c'est le cas, les procédures sont les mêmes, à l'exception de la manière dont vous accédez à la fenêtre.

Une liste de contrôle d'accès standard utilise uniquement des adresses IPv4 et définit uniquement les adresses de destination.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Standard ACL (ACL standard)**.

Étape 2 Si vous créez une nouvelle liste de contrôle d'accès, choisissez **Add (Ajouter)** > **Add ACL (Ajouter une ACL)**, saisissez un nom et cliquez sur OK (**OK**).

Le conteneur d'ACL est ajouté à la table. Vous ne pouvez pas renommer une liste de contrôle d'accès standard.

Étape 3 Effectuez l'une des actions suivantes :

- Pour ajouter une ACE à la fin de la liste de contrôle d'accès, sélectionnez le nom de l'ACL ou toute ACE dans celui-ci, puis choisissez **Add> Add ACE (Ajouter> Ajouter une ACE)**.
- Pour insérer une ACE à un emplacement spécifique, sélectionnez une ACE existante et choisissez **Add> Insert (ajouter> insérer)** pour ajouter l'ACE au-dessus de la règle, ou choisissez **Add> Insert After (ajouter> insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 4 Renseignez les propriétés de l'ACE. Les options sont les suivantes :

- **Action : Permit/Deny (Autoriser/Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).
- **Address** (Adresse) : une définition de la destination ou de l'adresse cible du flux de trafic. Vous pouvez spécifier une adresse d'hôte telle que 10.100.1.1, un réseau (au format 10.100.1.0/24 ou 10.100.1.0/255.255.255.0), ou vous pouvez sélectionner un objet réseau (qui charge simplement le contenu de l'objet dans le champ d'adresse).
- **Description : une explication de l'objectif de l'ACE, 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 l'ACE.

  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.

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

Étape 5 Cliquez sur **Apply** (Appliquer).

Configurer les ACL de type Web

Les listes de contrôle d'accès de type Web sont utilisées pour filtrer le trafic VPN SSL sans client, ce qui restreint l'accès des utilisateurs à des réseaux, des sous-réseaux, des hôtes et des serveurs Web spécifiques. Si vous ne définissez pas de filtre, toutes les connexions sont autorisées. Une liste de contrôle d'accès de type Web est représentée comme un conteneur nommé d'ACE. Pour créer une nouvelle liste de contrôle d'accès, vous devez d'abord créer le conteneur. Vous pouvez ensuite ajouter des ACE, modifier les ACE existantes et réorganiser les ACE à l'aide de la table d'ACL Web. La table apparaît en tant que gestionnaire d'ACL lorsque vous configurez les listes de contrôle d'accès de type Web tout en configurant les politiques qui les utilisent. Si c'est le cas, les procédures sont les mêmes, à l'exception de la manière dont vous accédez à la fenêtre.

L'ACL de type Web peut inclure une combinaison d'adresses IPv4 et IPv6 en plus des spécifications d'URL.

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Web** > **ACLs** > **(Configuration** > **VPN d'accès à distance** > **Accès VPN SSL sans client** > **Avancé** > **ACL Web)**.

Étape 2 Si vous créez une nouvelle liste de contrôle d'accès, choisissez **Add** > **Add ACL** (Ajouter > Ajouter une ACL), saisissez un nom et cliquez sur OK (**OK**).

Le conteneur d'ACL est ajouté à la table. Vous pouvez la renommer ultérieurement en la sélectionnant et en cliquant sur **Edit** (Modifier).

Étape 3 Effectuez l'une des actions suivantes :

- Pour ajouter une ACE à la fin de la liste de contrôle d'accès, sélectionnez le nom de l'ACL ou une ACE qu'elle contient, puis choisissez **Add > Add ACE** (Ajouter > Ajouter une ACE).
- Pour insérer une ACE à un emplacement précis, sélectionnez une ACE existante et choisissez **Add > Insert** (Ajouter > Insérer) pour ajouter l'ACE au-dessus de la règle, ou **Add > Insert After** (Ajouter > Insérer après).
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 4 Renseignez les propriétés de l'ACE. Les principales options à sélectionner sont :

- **Action : Permit (Autoriser)/Deny (Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant; il ne correspond alors pas).
- **Filter** (Filtre) : critères de correspondance du trafic en fonction de la destination. Vous pouvez soit spécifier une URL en sélectionnant le protocole et en saisissant le nom du serveur et, éventuellement, le chemin d'accès et le nom du fichier, ou vous pouvez spécifier une adresse de destination IPv4 ou IPv6 et un service TCP.

Pour des informations détaillées sur les options, consultez Propriétés des ACE Webtype, à la page 14.

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

Étape 5 Cliquez sur **Apply** (Appliquer).

Propriétés des ACE Webtype

Lorsque vous ajoutez ou modifiez une ACE dans une liste de contrôle d'accès de type Web, 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.

Pour une ACE donnée, vous pouvez filtrer par URL ou adresse, mais pas les deux.

- **Action : Permit/Deny (Autoriser/Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).
  - **Filter on URL** (Filtrer sur l'URL) : correspondance du trafic en fonction de l'URL de destination. Sélectionnez le protocole et saisissez le nom du serveur et, éventuellement, le chemin d'accès et le

nom du fichier. Par exemple, http://www.example.com ou, pour couvrir tous les serveurs, http://*.example.com. Voici quelques conseils et limites sur la spécification des URL :

- Sélectionnez **any** pour faire correspondre toutes les URL.
- La fonction « permit url any » autorisera toutes les URL qui ont le format protocole://server-ip/path et bloquera le trafic qui ne correspond pas à ce modèle, comme le transfert de port. Il doit y avoir une commande ACE pour autoriser les connexions au port requis (port 1494 dans le cas de Citrix) afin qu'un refus implicite ne se produise pas.
- Les modules d'extension de tunnel Smart et ica ne sont pas touchés par une liste de contrôle d'accès avec « autoriser l'URL n'importe quel », car ils correspondent uniquement aux types smart-tunnel:// et ica://.
- Vous pouvez utiliser les protocoles suivants : cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel:// et smtp://. Vous pouvez également utiliser des caractères génériques dans le protocole; par exemple, htt* correspond à http et https, et un astérisque * correspond à tous les protocoles. Par exemple, ://.example.com correspond à tout trafic de type URL vers le réseau example.com.
- Si vous spécifiez une URL smart-tunnel://, vous pouvez inclure le nom du serveur uniquement. L'URL ne peut pas contenir de chemin. Par exemple, smart-tunnel://www.example.com est acceptable, mais smart-tunnel://www.example.com/index.html ne l'est pas.
- Un astérisque * correspond à zéro ou à un nombre quelconque de caractères. Pour faire correspondre une URL http, saisissez http://*/*.
- Un point d'interrogation ? correspond exactement à un caractère.
- Les crochets [] sont des opérateurs de plage, correspondant à n'importe quel caractère dans la plage. Par exemple, pour faire correspondre à la fois http://www.cisco.com:80/ et http://www.cisco.com:81/, saisissez **http://www.cisco.com:8[01]/**.

- **Filter on Address and Service** (Filtrer sur l'adresse et le service) : correspondance du trafic en fonction de l'adresse de destination et du service.
  - **Address** (Adresse) : adresse IPv4 ou IPv6 de la destination. Pour faire correspondre toutes les adresses, vous pouvez utiliser **any**, qui correspond à toutes les adresses IPv4 ou IPv6, **any4** pour correspondre à IPv4 uniquement, ou **any6** pour correspondre uniquement à IPv6. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), ou 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).
  - **Service** : une seule spécification de service TCP. La valeur par défaut est **tcp** sans port, mais vous pouvez spécifier un seul port (comme tcp/80 ou tcp/www) ou une plage de ports (comme tcp/1-100). Vous pouvez inclure des opérateurs; par exemple, !=tcp/80 exclut le port 80; <tcp/80 correspond à tous les ports inférieurs à 80; >tcp/80 correspond à tous les ports supérieurs à 80.

- **Enable Logging (Activer la journalisation)** ; **Logging Level (Niveau de journalisation)** ; **More Options (Autres options) > Logging Interval** (Intervalle de journalisation) : les options de journalisation définissent la façon dont les messages syslog seront générés pour les règles qui refusent réellement le trafic. Vous pouvez implémenter les options de journalisation suivantes :

- **Désélectionnez Enable Logging** (Activer la journalisation) : cela désactive la journalisation pour la règle. Aucun message de journal système d'aucun type ne sera émis pour le trafic refusé par cette règle.
- **Sélectionnez Enable Logging (Activer la journalisation) avec Logging Level (Niveau de journalisation) = Default** (Par défaut) : cela fournit la journalisation par défaut pour les règles. Le message de journal système 106103 est émis pour chaque paquet refusé. 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 syslog résumé, 106102, au lieu de 106103. Le message 106102 est émis lors de la première occurrence, puis à nouveau à chaque intervalle configuré dans **More Options (Autres options) > Logging Interval** (Intervalle de journalisation) (la valeur par défaut est toutes les 300 secondes, vous pouvez spécifier 1–600), en affichant le nombre d'occurrences pendant cet intervalle. Le niveau de journalisation recommandé est **Informational** (Informationnel).

- **More Options (Autres options) > Time Range (Plage de temps)** : 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.

Exemples d'ACL de type Web

Voici quelques exemples de règles basées sur URL pour les listes de contrôle d'accès de type Web.

	Filtre	Incidence
Refuser	url http://*.yahoo.com/	Refuse l'accès à l'ensemble de Yahoo!
Refuser	url cifs://fileserver/share/directory	Refuse l'accès à tous les fichiers de l'emplacement spécifié.
Refuser	url https://www.example.com/ directory/file.html	Refuse l'accès au fichier précisé.
Autoriser	url https://www.example.com/directory	Permet l'accès à l'emplacement précisé.
Refuser	url http://*:8080/	Refuse l'accès HTTP de n'importe où via le port 8080.
Refuser	url http://10.10.10.10	Refuse l'accès HTTP à 10.10.10.10.
Autoriser	url any	Permet l'accès à n'importe quelle URL. Généralement utilisé après une liste de contrôle d'accès qui refuse l'accès à l'URL.

Surveillance des ACL

Les tableaux ACL Manager (Gestionnaire d'ACL), Standard ACL (ACL standard), Web ACL (ACL Web) et EtherType ACL (ACL EtherType) affichent une vue consolidée des listes de contrôle d'accès. Mais pour voir exactement ce qui est configuré sur le périphérique, vous pouvez utiliser les commandes suivantes. Saisissez les commandes dans **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

- **show access-list** [*name*] : affiche les listes d'accès, y compris le numéro de ligne pour chaque ACE et le nombre de résultats. Incluez un nom d'ACL ou vous verrez toutes les listes d'accès.
- **show running-config access-list** [*name*] : affiche la configuration actuelle de la liste d'accès en cours d'exécution. Incluez un nom d'ACL ou vous verrez toutes les listes d'accès.

Historique des ACL

Nom de la caractéristique	Versions	Description
ACL étendues, standard, de type Web	7.0(1)	Les listes de contrôle d'accès sont utilisées pour contrôler l'accès au réseau ou pour spécifier le trafic sur lequel de nombreuses fonctionnalités doivent agir. Une liste de contrôle d'accès étendue est utilisée pour le contrôle d'accès traversant le boîtier et plusieurs autres fonctionnalités. Les listes de contrôle d'accès standard sont utilisées dans les cartes de routage et les filtres VPN. Les listes de contrôle d'accès de type Web sont utilisées dans le filtrage VPN SSL sans client. Les listes de contrôle d'accès EtherType contrôlent le trafic de couche 2 non IP. Nous avons ajouté le gestionnaire d'ACL et d'autres pages pour configurer les listes de contrôle d'accès.
Adresses IP réelles dans les listes de contrôle d'accès étendues	8.3(1)	Lors de l'utilisation de la NAT ou de la PAT, les adresses et les ports mappés ne sont plus utilisés dans une liste de contrôle d'accès pour plusieurs fonctionnalités. Vous devez utiliser les adresses et les ports réels non traduits pour ces fonctionnalités. L'utilisation de l'adresse et du port réels signifie que si la configuration de la NAT change, vous n'avez pas besoin de modifier les listes de contrôle d'accès.
Prise en charge du pare-feu d'identité dans les listes de contrôle d'accès étendues	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 d'EtherType ACL pour le trafic IS-IS	8.4(5), 9.1(2)	En mode de pare-feu transparent, l'ASA peut désormais contrôler 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 Cisco TrustSec dans les listes de contrôle d'accès étendues	9.0(1)	Vous pouvez maintenant utiliser les groupes de sécurité Cisco 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.

Nom de la caractéristique	Versions	Description
ACL unifiées étendues et de type Web pour IPv4 et IPv6	9.0(1)	Les listes de contrôle d'accès étendues et de type Web 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 listes de contrôle d'accès propres à IPv6 sont obsolètes. Les listes de contrôle d'accès IPv6 existantes sont migrées vers des listes de contrôle d'accès étendues. Pour en savoir plus, consultez les notes de mise à jour. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Access Rules (Critères d'accès) Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au 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 services) Configuration > Firewall (Pare-feu) > Access Rules (Critères d'accès)
Session de configuration pour modifier les listes de contrôle d'accès et les objets. Référencement ultérieur des objets et des listes de contrôle d'accès dans les règles d'accès.	9.3(2)	Vous pouvez maintenant modifier les listes de contrôle d'accès 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 modifié les paramètres avancés pour les règles d'accès.
Prise en charge d'ACL pour le protocole SCTP (Stream Control Transmission Protocol)	9.5(2)	Vous pouvez maintenant créer des règles d'ACL à l'aide du protocole **sctp**, y compris les spécifications de port. Nous avons modifié les boîtes de dialogue d'ajout/modification pour les entrées de contrôle d'accès sur la page **Configuration** > **Firewall** > **Advanced** > **ACL Manager**.
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)**.

Nom de la caractéristique	Versions	Description
Prise en charge en mode routé des règles Ethertype sur les interfaces membres de groupe de ponts et des règles d'accès étendues sur les interfaces virtuelles de groupe de ponts (BVI).	9.7(1)	Vous pouvez maintenant créer des listes de contrôle d'accès Ethertype et les appliquer aux interfaces membres de groupes de ponts en mode routé. Vous pouvez également appliquer des règles d'accès étendues à la BVI (Bridge Virtual Interface) 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)**.
Prise en charge des groupes d'objets de service réseau dans les listes de contrôle d'accès étendues.	9.17(1)	Vous pouvez utiliser des objets de service réseau comme critères de source et de destination dans les listes de contrôle d'accès étendues et les règles de contrôle d'accès. Nous avons modifié l'écran suivant : Add/Edit extended ACE or access rule (Ajouter/Modifier une ACE étendue ou une règle d'accès) sur la page Firewall (Pare-feu).
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.