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. 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 ACL EtherType, à la page 20.

- 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 16.
- 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 16.

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.

Noms des 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 ACL 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.

Dans une ACL étendue, utilisez le paramètre **line** (ligne) *number* avec la commande **access-list** (liste d'accès) pour insérer les règles au bon endroit. Utilisez la commande **show access-list** *name* pour afficher les entrées d'ACL et leurs numéros de ligne afin de déterminer le bon numéro à utiliser. Pour les autres types d'ACL, vous devez recréer l'ACL (ou mieux, utiliser ASDM) pour modifier l'ordre des ACE.

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 la 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.

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 ACL 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).

```
hostname(config)# object network server1
hostname(config-network-object)# host 10.1.1.5
hostname(config-network-object)# nat (inside,outside) static 209.165.201.5

hostname(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
hostname(config)# access-group OUTSIDE in interface outside
```

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 ACL

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.

Lignes directrices 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).

- (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. Lisez la section sur les bases d'ACL pour obtenir une vue d'ensemble, puis les sections sur des types spécifiques d'ACL pour les détails.

Options de base de configuration et de gestion de l'ACL

Une ACL est composée d'une ou de plusieurs entrées de contrôle d'accès (ACE) ayant le même ID ou le même nom d'ACL. Pour créer une nouvelle ACL, vous créez simplement une ACE avec un nouveau nom d'ACL, et elle devient la première règle de la nouvelle ACL.

En utilisant une liste de contrôle d'accès, vous pouvez effectuer les opérations suivantes :

Examiner le contenu de la liste de contrôle d'accès et déterminer les numéros de ligne et le nombre de correspondances

Utilisez la commande **show access-list** *name* pour afficher le contenu de la liste de contrôle d'accès. Chaque ligne est une entrée ACE et comprend le numéro de ligne, que vous aurez besoin de connaître si vous souhaitez insérer de nouvelles entrées dans une liste de contrôle d'accès étendue. Les informations comprennent également un nombre de correspondances pour chaque ACE, qui correspond au nombre de fois que la règle a été mise en correspondance avec le trafic. Par exemple :

```
hostname# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group
LOCAL\\usergroup any any (hitcnt=0) 0xb0f5b1e1
```

Ajouter une ACE

La commande pour ajouter une ACE est **access-list** *name* [**line** *line-num*] *type parameters*. L'argument du numéro de ligne ne fonctionne que pour les listes de contrôle d'accès étendues. Si vous incluez le numéro de ligne, l'ACE est insérée à cet emplacement dans la liste de contrôle d'accès, et l'ACE qui se trouve à cet emplacement est déplacée vers le bas, ainsi que le reste des ACE (c'est-à-dire que l'insertion d'une ACE à un numéro de ligne ne remplace pas l'ancienne ACE à cette ligne). Si vous n'incluez pas de numéro de ligne, l'ACE est ajoutée à la fin de l'ACL. Les paramètres disponibles varient selon le type d'ACL; consultez les rubriques spécifiques sur chaque type d'ACL pour en savoir plus.

Ajouter des commentaires à une liste de contrôle d'accès (tous les types, sauf webtype)

Utilisez la commande **access-list** *name* [**line** *line-num*] **remark** *text* pour ajouter des remarques dans une liste de contrôle d'accès afin de faciliter l'explication de l'objectif d'une ACE. Les bonnes pratiques sont d'insérer la remarque avant l'ACE; si vous affichez la configuration dans ASDM, les remarques seront associées à l'ACE qui suit les remarques. Vous pouvez saisir plusieurs remarques avant une ACE pour inclure un commentaire détaillé. Chaque remarque est limitée à 100 caractères. Vous pouvez inclure des espaces de début pour faciliter la mise en valeur des remarques. Si vous n'incluez pas de numéro de ligne, la remarque est ajoutée à la fin de la liste de contrôle d'accès. Par exemple, vous pourriez ajouter des remarques avant d'ajouter chaque ACE :

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

Modifier ou déplacer une ACE ou une remarque

Vous ne pouvez pas modifier ou déplacer une ACE ou une remarque. Au lieu de cela, vous devez créer une nouvelle ACE ou une remarque avec les valeurs souhaitées au bon emplacement (en utilisant le numéro de ligne), puis supprimer l'ancienne ACE ou l'ancienne remarque. Comme vous ne pouvez insérer des ACE que dans les listes de contrôle d'accès étendues, vous devez recréer les listes de contrôle d'accès standard, webtype ou EtherType si vous devez modifier ou déplacer des ACE. Il est beaucoup plus facile de réorganiser une liste de contrôle d'accès longue à l'aide d'ASDM.

Supprimer une ACE ou une remarque

Utilisez la commande **no access-list** *parameters* pour supprimer une ACE ou une remarque. Utilisez la commande **show access-list** pour afficher la chaîne de paramètres que vous devez saisir : la chaîne doit correspondre exactement à une ACE ou à une remarque pour la supprimer, à l'exception de l'argument **line** *line-num*, qui est facultatif dans la commande **no access-list**.

Supprimer une liste de contrôle d'accès complète, y compris les remarques

Utilisez la commande **clear configure access-list** *name*. ATTENTION La commande ne vous demande pas de confirmation. Si vous n'incluez pas de nom, toutes les listes d'accès de l'ASA sont supprimées.

Renommer une liste de contrôle d'accès

Utilisez la commande **access-list** *name* **rename** *new_name*.

Appliquer l'ACL à une politique

La création d'une liste de contrôle d'accès ne modifie pas à elle seule le trafic. Vous devez appliquer la liste de contrôle d'accès à une politique. Par exemple, vous pouvez utiliser la commande **access-group** pour appliquer une liste de contrôle d'accès étendue à une interface, refusant ou autorisant ainsi le trafic qui passe par l'interface.

Configurer les ACL étendues

Une ACL étendue est composée de toutes les ACE ayant le même ID ou le même nom d'ACL. Les Ajouter étendues sont le type d'ACL le plus complexe et le plus complet, et vous pouvez les utiliser pour de nombreuses fonctionnalités. L'utilisation la plus importante des ACL étendues est en tant que groupes d'accès appliqués globalement ou aux interfaces, qui déterminent le trafic qui sera refusé ou autorisé à passer par la boîte. Mais les ACL étendues sont également utilisées pour déterminer le trafic auquel d'autres services seront fournis.

Les ACL étendues étant complexes, les sections suivantes se concentrent sur la création d'ACE pour fournir des types spécifiques de correspondance de trafic. Les premières sections, sur les ACE basées sur les adresses de base et sur les ACE TCP/UDP, bâtissent les fondations pour les sections restantes.

Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets

L'ACE étendue de base fait correspondre le trafic en fonction des adresses source et de destination, y compris les adresses IPv4 et IPv6 et les noms de domaine complets (FQDN), tels que www.example.com. En fait, chaque type d'ACE étendue doit inclure des spécifications pour l'adresse source et de destination. Cette rubrique explique donc l'ACE étendue minimale.

Astuces Conseil : Si vous souhaitez mettre en correspondance le trafic en fonction d'un FQDN, vous devez créer un objet réseau pour chaque FQDN.

Pour ajouter une ACE pour la mise en correspondance des adresses IP ou des FQDN, utilisez la commande suivante :

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument source_address_argument dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

Exemple :

```
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-list ACL_IN extended permit object service-obj-http any any
```

Les options sont les suivantes :

- *access_list_name* : nom de la nouvelle ACL ou de l'ACL existante.
- Numéro de ligne : l'option **line***line_number* spécifie le numéro de ligne à laquelle insérer l'ACE; sinon, l'ACE est ajouté à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- Protocole : *protocol_argument* spécifie le protocole IP. Si vous utilisez des groupes d'objets de service réseau qui précisent le protocole et les ports, vous devez préciser **ip** dans cet argument.
  - name or *number*(nom ou numéro) : spécifie le nom ou le numéro du protocole. Précisez **ip** pour appliquer à tous les protocoles.
  - **object-group** *protocol_grp_id* : spécifie un groupe d'objets de protocole créé à l'aide de la commande **object-group protocol**.
  - **object** *service_obj_id* : spécifie un objet de service créé à l'aide de la commande **object service**. L'objet peut inclure des spécifications de port ou de type ICMP et de code, si nécessaire.
  - **object-group** *service_grp_id* : spécifie un groupe d'objets de service créé à l'aide de la commande **object-group service**.

- Adresse source, adresse de destination : *source_address_argument* spécifie l'adresse IP ou le FQDN à partir duquel le paquet est envoyé, et *dest_address_argument* spécifie l'adresse IP ou le FQDN auquel le paquet est envoyé :
  - **host** *ip_address* : spécifie une adresse d'hôte IPv4.
  - *ip_address mask* : spécifie une adresse réseau et un filtre d'adresse locale IPv4, tels que 10.100.10.0 255.255.255.0.
  - *ipv6-address/prefix-length* : spécifie un hôte IPv6 ou une adresse réseau et un préfixe.
  - **any**, **any4**, et **any6** - **any** spécifie le trafic IPv4 et IPv6 ; **any4** spécifie uniquement le trafic IPv4 ; et **any6** spécifie uniquement le trafic IPv6.
  - **interface** *interface_name* : spécifie le nom d'une interface ASA. Utilisez le nom de l'interface plutôt que l'adresse IP pour faire correspondre le trafic en fonction de l'interface qui est la source ou la destination du trafic.
  - **object** *nw_obj_id* : spécifie un objet réseau créé à l'aide de la commande **object network**.
  - **object-group** *nw_grp_id* : spécifie un groupe d'objets réseau créé à l'aide de la commande **object-group network**.
  - **object-group-network-service** *name* : spécifie le nom d'un groupe d'objets de service réseau.
- Logging (Journalisation) : les arguments **log** définissent les options de journalisation lorsqu'une ACE correspond à une connexion pour l'accès réseau (une liste de contrôle d'accès appliquée avec la commande **access-group**). Si vous saisissez l'option **log** sans arguments, vous activez le message syslog 106100 au niveau par défaut (6) et pour l'intervalle par défaut (300 secondes). Les options de journalisation sont les suivantes :
  - *level* : un niveau de gravité entre 0 et 7. La valeur par défaut est 6 (informational). Si vous modifiez ce niveau pour une ACE active, le nouveau niveau s'applique aux nouvelles connexions; les connexions existantes continuent d'être journalisées au niveau précédent.
  - **interval** *secs* : intervalle de temps en secondes entre les messages syslog, de 1 à 600. La valeur par défaut est de 300 secondes. Cette valeur est également utilisée comme valeur de délai d'expiration pour supprimer un flux inactif de la mémoire cache qui recueille les statistiques d'abandon.
  - **disable** : désactive toute la journalisation ACE.
  - **default** : active la journalisation dans le message 106023 pour les paquets refusés. Ce paramètre est identique à l'option **log** non incluse.
- Time Range (Plage temporelle) : **time-range**l'option *time_range_name* spécifie un objet de plage temporelle, qui détermine les heures du jour et les jours de la semaine pendant lesquels l'ACE est active. Si vous ne spécifiez pas de plage temporelle, l'ACE est toujours actif.
- Activation : utilisez l'option **inactive** pour désactiver l'ACE sans le supprimer. Pour la réactiver, saisissez l'ACE complète sans le mot-clé inactive.

Ajoutez une ACE étendue pour la correspondance basée sur le port

Si vous spécifiez des objets de service dans une ACE, les objets de service peuvent inclure des protocoles avec des spécifications de port, comme TCP/80. Sinon, vous pouvez spécifier les ports directement dans

l'ACE. Grâce à la correspondance basée sur le port, vous pouvez cibler certains types de trafic pour les protocoles basés sur le port plutôt que tout le trafic pour le protocole.

Remarque Si vous utilisez des groupes d'objets de service réseau qui précisent le protocole et les ports, vous ne devez pas préciser les ports comme décrit dans cette rubrique. Précisez **ip** comme protocole afin que le protocole ou le port défini dans l'objet puisse correspondre.

L'ACE étendue basée sur le port est simplement l'ACE de base correspondant à l'adresse dont le protocole est **tcp**, **udp**, ou **sctp**. Pour ajouter des spécifications de port, utilisez la commande suivante :

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **sctp**} *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**] [**time-range** *time-range-name*] [**inactive**]

Exemple :

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

L'option *port_argument* spécifie le port source ou de destination. Si vous ne spécifiez pas de port, tous les ports sont mis en correspondance. Les arguments disponibles sont les suivants :

- *operator port* : le *port* peut être l'entier ou le nom d'un port. L'*operator* peut être l'une des options suivantes :
  - **lt** : inférieur à
  - **gt** : supérieur à
  - **eq** : égal à
  - **neq** : différent de
  - **plage** : une plage inclusive de valeurs. Lorsque vous utilisez cet opérateur, spécifiez deux numéros de port, par exemple, **range 100 200**.

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.

- **object-group** *service_grp_id* : spécifie un groupe d'objets de service créé à l'aide de la commande **object-group service** {**tcp** | **udp** | **tcp-udp**}. Notez que ces types d'objets ne sont plus conseillés.

  Vous ne pouvez pas spécifier les objets de service génériques recommandés, où le protocole et le port sont définis dans l'objet, comme arguments de port. Vous spécifiez ces objets dans le cadre de l'argument du protocole, comme expliqué dans Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets, à la page 9.

Pour obtenir une explication des autres mots-clés et comment utiliser les objets de service pour préciser les protocoles et les ports, consultez Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets, à la page 9.

Ajouter une ACE étendue pour la correspondance basée sur ICMP

Pour faire correspondre le trafic ICMP, utilisez l'un des mots-clés de protocole ICMP : **icmp** ou **icmp6**. Le protocole **icmp** correspond uniquement aux adresses IPv4, tandis que le protocole **icmp6** correspond uniquement aux adresses IPv6. Assurez-vous que vos adresses réseau correspondent au protocole que vous sélectionnez, sinon l'ACE ne correspondra à aucune connexion.

Si vous spécifiez des objets de service dans une ACE, les objets de service peuvent inclure des spécifications de type et de code ICMP des protocoles ICMP/ICMP6. Sinon, vous pouvez spécifier le type et le code ICMP directement dans l'ACE. Par exemple, vous pouvez cibler le trafic de demande d'écho ICMP (pings).

L'ACE étendue ICMP est simplement l'ACE de mise en correspondance d'adresses de base dont le protocole est **icmp** ou **icmp6**. Étant donné que ces protocoles ont des valeurs de type et de code, vous pouvez ajouter des spécifications de type et de code à l'ACE.

Pour ajouter une ACE pour la correspondance d'adresse IP ou de FQDN, où le protocole est ICMP ou ICMP6, utilisez la commande suivante :

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**} *source_address_argument dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

Exemple :

```
hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
hostname(config)# access-list abc extended permit icmp any any echo
```

L'option *icmp_argument* spécifie le type et le code ICMP.

- *icmp_type* [*icmp_code*] : spécifie le type ICMP par nom ou par numéro, ainsi que le code ICMP facultatif pour ce type. Si vous ne spécifiez pas de code, tous les codes sont utilisés.
- **object-group** *icmp_grp_id* : spécifie un groupe d'objets pour ICMP/ICMP6 créé à l'aide de la commande (obsolète) **object-group icmp-type**.

  Vous ne pouvez pas spécifier les objets de service génériques recommandés, où le protocole et le type sont définis dans l'objet, comme l'argument ICMP. Vous spécifiez ces objets dans le cadre de l'argument du protocole, comme expliqué dans Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets, à la page 9.

Pour obtenir une explication des autres mots-clés, consultez Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets, à la page 9.

Ajouter une ACE étendue pour la correspondance basée sur l'utilisateur (pare-feu d'identité)

L'ACE étendue basée sur l'utilisateur est simplement l'ACE de base pour la mise en correspondance d'adresses, dans laquelle vous incluez un nom d'utilisateur ou un groupe d'utilisateurs dans les critères de correspondance de la source. En créant des règles en fonction de l'identité de l'utilisateur, vous pouvez éviter d'associer des règles à des adresses d'hôte ou de réseau statiques. Par exemple, si vous définissez une règle pour user1 et que la fonctionnalité de pare-feu d'identité associe cet utilisateur à un hôte affecté à 10.100.10.3 un jour, mais à 192.168.1.5 le jour suivant, la règle basée sur l'utilisateur s'applique toujours.

Comme vous devez toujours fournir des adresses de source et de destination, élargissez l'adresse source pour inclure les adresses probablement attribuées à l'utilisateur (généralement par DHCP). Par exemple, l'utilisateur « LOCAL\user1 any » correspondra à l'utilisateur LOCAL\user1, quelle que soit l'adresse attribuée, alors

que « LOCAL\user1 10.100.1.0 255.255.255.0 » correspond à l'utilisateur uniquement si l'adresse se trouve sur le réseau 10.100.1.0/24.

En utilisant les noms de groupe, vous pouvez définir des règles pour des catégories entières d'utilisateurs, tels que les étudiants, les enseignants, les gestionnaires, les ingénieurs, etc.

Pour ajouter une ACE pour la mise en correspondance d'utilisateurs ou de groupes, utilisez la commande suivante :

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

Exemple :

```
hostname(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

L'option *user_argument* spécifie l'utilisateur ou le groupe pour lequel mettre en correspondance le trafic en plus de l'adresse source. Les arguments disponibles sont les suivants :

- **object-group-user** *user_obj_grp_id* : spécifie un groupe d'objets utilisateur créé à l'aide de la commande **object-group user**.
- **user** {[*domain_nickname*\]*name* | **any** | **none**} : spécifie un nom d'utilisateur. Précisez **any** pour correspondre à tous les utilisateurs avec des informations d'authentification d'utilisateur, ou **none** pour faire correspondre les adresses qui ne sont pas mappées aux noms d'utilisateurs. Ces options sont particulièrement utiles pour combiner les politiques de **correspondance access-group et aaa authentication**.
- **user-group** [*domain_nickname*\]*user_group_name* : spécifie le nom d'un groupe d'utilisateurs. Notez la double barre oblique inverse (\\) qui sépare le domaine et le nom de groupe.

Pour obtenir une explication des autres mots-clés, consultez Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets, à la page 9.

Astuces Vous pouvez inclure à la fois des utilisateurs et des groupes de sécurité Cisco Trustsec dans une ACE donnée.

Ajouter une ACE étendue pour la correspondance basée sur un groupe de sécurité (Cisco TrustSec)

L'ACE étendue de groupe de sécurité (Cisco TrustSec) est simplement l'ACE de mise en correspondance d'adresses de base où vous incluez des groupes de sécurité ou des balises aux critères de correspondance de source ou de destination. En créant des règles en fonction de groupes de sécurité, vous pouvez éviter d'associer des règles à des adresses d'hôte ou de réseau statiques. Comme vous devez toujours fournir des adresses source et de destination, élargissez les adresses pour inclure les adresses qui seront probablement attribuées aux utilisateurs (généralement par DHCP).

Astuces Avant d'ajouter ce type d'ACE, configurez Cisco TrustSec.

Pour ajouter une ACE pour la correspondance de groupe de sécurité, utilisez la commande suivante :

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

Exemple :

```
hostname(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

L'option *security_group_argument* spécifie le groupe de sécurité pour lequel mettre en correspondance le trafic en plus de l'adresse source ou de destination. Les arguments disponibles sont les suivants :

- **object-group-security** *security_obj_grp_id* : spécifie un groupe d'objets de sécurité créé à l'aide de la commande **object-group security**.
- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*} : spécifie un nom ou une balise de groupe de sécurité.

Pour obtenir une explication des autres mots-clés, consultez Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets, à la page 9.

Astuces Vous pouvez inclure à la fois des utilisateurs et des groupes de sécurité Cisco Trustsec dans une ACE donnée.

Exemples d'ACL étendues

La liste de contrôle d'accès suivante permet à tous les hôtes (sur l'interface à laquelle vous appliquez la liste de contrôle d'accès) de passer par l'ASA :

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

La liste de contrôle d'accès suivante empêche les hôtes de l'adresse 192.168.1.0/24 d'accéder au réseau 209.165.201.0/27 pour le trafic basé sur TCP. Toutes les autres adresses sont autorisées.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

Si vous souhaitez restreindre l'accès aux hôtes sélectionnés uniquement, saisissez une autorisation ACE limitée. Par défaut, tout autre trafic est refusé, sauf autorisation explicite.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

La liste de contrôle d'accès suivante restreint tous les hôtes (sur l'interface à laquelle vous appliquez la liste de contrôle d'accès) d'accéder à un site Web à l'adresse 209.165.201.29. Tout autre trafic est autorisé.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

La liste de contrôle d'accès suivante, qui utilise des groupes d'objets, empêche plusieurs hôtes du réseau interne d'accéder à plusieurs serveurs Web. Tout autre trafic est autorisé.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

L'exemple suivant désactive temporairement une liste de contrôle d'accès qui autorise le trafic d'un groupe d'objets réseau (A) vers un autre groupe d'objets réseau (B) :

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

Pour mettre en œuvre une ACE basée sur le temps, utilisez la commande **time-range** pour définir des heures spécifiques du jour et de la semaine. Utilisez ensuite la commande **access-list extended** pour lier la plage temporelle à une ACE. L'exemple suivant associe une ACE dans la liste de contrôle d'accès « Sales » à une plage temporelle nommée « New_York_Minute ».

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

L'exemple suivant montre une liste de contrôle d'accès mixte IPv4/IPv6 :

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

Exemple de conversion d'adresses en objets pour les ACL étendues

La liste de contrôle d'accès normale suivante qui n'utilise pas de groupes d'objets empêche plusieurs hôtes du réseau interne d'accéder à plusieurs serveurs Web. Tout autre trafic est autorisé.

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

Si vous créez deux groupes d'objets réseau, un pour les hôtes internes et un pour les serveurs Web, la configuration peut être simplifiée et peut être facilement modifiée pour ajouter d'autres hôtes :

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config)# access-list ACL_IN extended deny tcp object-group denied object-group
web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

Configurer les ACL standard

Une liste de contrôle d'accès standard est composée de toutes les ACE ayant le même ID ou le même nom d'ACL. Les listes de contrôle d'accès standard sont utilisées pour un nombre limité de fonctionnalités, telles que les listes de routage ou les filtres VPN. Une liste de contrôle d'accès standard utilise uniquement des adresses IPv4 et définit uniquement les adresses de destination.

Pour ajouter une entrée de liste d'accès standard, utilisez la commande suivante :

access-list *access_list_name* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address mask*}

Exemple :

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

Les options sont les suivantes :

- Nom : l'argument *access_list_name* spécifie le nom ou le numéro d'une ACL. Les numéros traditionnels pour les listes de contrôle d'accès standard sont de 1 à 99 ou de 1 300 à 1 999, mais vous pouvez utiliser n'importe quel nom ou numéro. Vous créez une nouvelle liste de contrôle d'accès si elle n'existe pas déjà, sinon, vous ajoutez l'entrée à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- Adresse de destination : le mot-clé **any4** correspond à toutes les adresses IPv4. L'argument **host** *ip_address* correspond à une adresse IPv4 d'hôte. L'argument *ip_address ip_mask* correspond à un sous-réseau IPv4, par exemple, 10.1.1.0 255.255.255.0.

Configurer les ACL de type Web

Les ACL 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 ACL de type Web est composée de toutes les ACE ayant le même ID ou le même nom d'ACL.

Les ACL de type Web vous permettent de faire correspondre le trafic en fonction des URL ou des adresses de destination. Une seule ACE ne peut pas combiner ces spécifications. Les sections suivantes expliquent chaque type d'ACE.

Ajouter une ACE de type Web pour la correspondance d'URL

Pour faire correspondre le trafic en fonction de l'URL à laquelle l'utilisateur tente d'accéder, utilisez la commande suivante ;

access-list *access_list_name* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *time_range_name*] [**inactive**]

Exemple :

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

Les options sont les suivantes :

- *access_list_name* : nom de la liste de contrôle d'accès nouvelle ou existante. Si l'ACL existe déjà, vous ajoutez l'ACE à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- URL : le mot-clé **url** spécifie l'URL à mettre en correspondance. Utilisez **url any** pour faire correspondre tout le trafic basé sur des URL. Sinon, saisissez une chaîne d'URL, qui peut inclure des caractères génériques. Voici quelques conseils et limites sur la spécification des URL :
  - Précisez **any** pour qu'il corresponde à 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 « permit url any », 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]/**.

- Journalisation : les arguments **log** définissent les options de journalisation lorsqu'une ACE correspond à un paquet. Si vous saisissez l'option **log** sans arguments, vous activez le message syslog 106102 au niveau par défaut (6) et pour l'intervalle par défaut (300 secondes). Les options de journalisation sont les suivantes :
  - *level* : un niveau de gravité entre 0 et 7. La valeur par défaut est 6.
  - **interval** *secs* : intervalle de temps en secondes entre les messages syslog, de 1 à 600. La valeur par défaut est de 300 secondes.
  - **disable** : désactive toute la journalisation des ACL.
  - **default** : active la journalisation vers le message 106103. Ce paramètre est identique à ne pas inclure l'option **log**.
- Option de plage de temps – l'option **time-range** *time_range_name* spécifie un objet de plage temporelle, qui détermine les heures du jour et les jours de la semaine pendant lesquels l'ACE est actif. Si vous ne spécifiez pas de plage temporelle, l'ACE est toujours actif.
- Activation – utilisez l'option **inactive** pour désactiver l'ACE sans le supprimer. Pour la réactiver, saisissez l'ACE complète sans le mot-clé inactive.

Ajouter une ACE de type Web pour la correspondance d'adresses IP

Vous pouvez mettre en correspondance le trafic en fonction de l'adresse de destination à laquelle l'utilisateur tente d'accéder. L'ACL de type Web peut inclure une combinaison d'adresses IPv4 et IPv6 en plus des spécifications d'URL.

Pour ajouter une ACE de type Web pour la mise en correspondance des adresses IP, utilisez la commande suivante :

access-list *access_list_name* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *time_range_name*]] [**inactive**]]

Exemple :

```
hostname(config)# access-list acl_company webtype permit tcp any
```

Pour obtenir une explication des mots-clés non expliqués ici, consultez Ajouter une ACE de type Web pour la correspondance d'URL, à la page 17. Les mots-clés et les arguments spécifiques à ce type d'ACE sont les suivants :

- **tcp** : le protocole TCP. Les listes de contrôle d'accès de type Web correspondent uniquement au trafic TCP.
- Adresse de destination : le *dest_address_argument* précise l'adresse IP à laquelle le paquet est envoyé :
  - **host** *ip_address* : spécifie une adresse d'hôte IPv4.
  - *dest_ip_address masque* : spécifie une adresse réseau IPv4 et un masque de sous-réseau, tel que 10.100.10.0 255.255.255.0.
  - *ipv6-address/prefix-length* : spécifie un hôte IPv6 ou une adresse réseau et un préfixe.
  - **any**, **any4**, et **any6** :**any** spécifie le trafic IPv4 et IPv6 ; **any4** spécifie uniquement le trafic IPv4 ; et **any6** spécifie uniquement le trafic IPv6.

- *operator port* : le port de destination. Si vous ne spécifiez pas de ports, tous les ports sont mis en correspondance. Le *port* peut être l'entier ou le nom d'un port TCP. L'*opérateur* peut être l'une des options suivantes :
  - **lt** : inférieur à
  - **gt** : supérieur à
  - **eq** : égal à
  - **neq** : différent de
  - **range** : une plage inclusive de valeurs. Lorsque vous utilisez cet opérateur, spécifiez deux numéros de port, par exemple, **range 100 à 200**.

Exemples d'ACL de type Web

L'exemple suivant montre comment refuser l'accès à une URL d'entreprise spécifique :

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

L'exemple suivant montre comment refuser l'accès à une page Web spécifique :

```
hostname(config)# access-list acl_file webtype deny url https://www.example.com/dir/file.html
```

L'exemple suivant montre comment refuser l'accès HTTP à toute URL sur un serveur spécifique via le port 8080 :

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

Les exemples suivants montrent comment utiliser les caractères génériques dans les listes de contrôle d'accès de type Web.

- L'exemple suivant correspond à des URL telles que http://www.example.com/layouts/1033:

  ```
  access-list VPN-Group webtype permit url http://www.example.com/*
  ```

- L'exemple suivant correspond à des URL telles que http://www.example.com/ et http://www.example.net/:

  ```
  access-list test webtype permit url http://www.example.*
  ```

- L'exemple suivant correspond à des URL telles que http://www.example.com et ftp://wwz.example.com:

  ```
  access-list test webtype permit url *://ww?.e*co*/
  ```

- L'exemple suivant correspond à des URL telles que http://www.cisco.com:80 et https://www.cisco.com:81:

  ```
  access-list test webtype permit url *://ww?.c*co*:8[01]/
  ```

L'opérateur de plage « [] » dans l'exemple précédent spécifie que les caractères **0** ou **1** peuvent se produire à cet emplacement.

- L'exemple suivant correspond à des URL telles que http://www.example.com et http://www.example.net:

```
access-list test webtype permit url http://www.[a-z]xample?*/
```

L'opérateur de plage « [] » dans l'exemple précédent spécifie que tout caractère dans la plage de **a** à **z** peut se produire.

- L'exemple suivant correspond aux URL http ou https qui comprennent « cgi » quelque part dans le nom ou le chemin d'accès du fichier.

```
access-list test webtype permit url htt*://*/*cgi?*
```

Remarque Pour faire correspondre une URL http, vous devez saisir **http://*/*** au lieu de http://*.

L'exemple suivant montre comment appliquer une liste de contrôle d'accès de type Web pour désactiver l'accès à des partages CIFS spécifiques.

Dans ce scénario, nous avons un dossier racine nommé « shares » qui contient deux sous-dossiers nommés « Marketing_Reports » et « Sales_Reports ». Nous souhaitons refuser spécifiquement l'accès au dossier « shares/Marketing_Reports ».

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

Cependant, en raison du « refuser tout » implicite à la fin de la liste de contrôle d'accès, l'ACL ci-dessus rend tous les sous-dossiers inaccessibles (« shares/Sales_Reports » et « shares/Marketing_Reports »), y compris le dossier racine (« shares »).

Pour résoudre le problème, ajoutez une nouvelle liste de contrôle d'accès pour autoriser l'accès au dossier racine et aux sous-dossiers restants :

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

Configurer les ACL EtherType

Les ACL EtherType s'appliquent au trafic de couche 2 non IP sur les interfaces membres de groupes 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 ACL EtherType vous permettent de contrôler le flux du trafic non IP dans le groupe de ponts. Notez que les trames au format 802.3 ne sont pas gérées par la liste de contrôle d'accès, car elles utilisent un champ de longueur par opposition à un champ de type.

Pour ajouter une EtherType ACE, utilisez la commande suivante :

access-list *access_list_name* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} | **eii-ipx** | **ipx** | **isis** | **mpls-multicast** | **mpls-unicast** | *hex_number*}

Exemple :

```
hostname(config)# access-list ETHER ethertype deny mpls-multicast
```

Les options sont les suivantes :

- *access_list_name*—Le nom de la nouvelle ou existante ACL. Si l'ACL existe déjà, vous ajoutez l'ACE à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse un paquet si les conditions correspondent. Le mot-clé **permit** autorise un paquet si les conditions correspondent.
- Critères de correspondance du trafic : vous pouvez mettre en correspondance le trafic en utilisant les options suivantes :
  - **any** : correspond à tout le trafic de couche 2.
  - **bpdu** : unités de données de protocole de pont (dsap 0x42), qui sont autorisées par défaut. Ce mot-clé est converti en **dsap bpdu**.
  - **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} : l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2. Incluez l'adresse que vous souhaitez autoriser ou refuser en format hexadécimal, de 0x01 à 0xff. Vous pouvez également utiliser les mots-clés suivants pour créer des règles pour les valeurs communes :
    - **bpdu** pour 0x42, unités de données de protocole de pont.
    - **ipx** pour 0xe0, Internet Packet Exchange (IPX) 802.2 LLC.
    - **isis** pour 0xfe, Intermediate System to Intermediate System (IS-IS).
    - **raw-ipx** pour 0xff, format brut IPX 802.3.
  - **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**.
  - **isis** : Intermediate System to Intermediate System (IS-IS). Ce mot-clé est converti en **dsap isis**.
  - **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.

Exemples d'ACL EtherType

Les exemples suivants montrent comment configurer les listes de contrôle d'accès EtherType, y compris comment les appliquer à une interface.

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

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
```

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

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

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

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

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

Modifier les ACL dans une session de configuration isolée

Lorsque vous modifiez une liste de contrôle d'accès utilisée pour les règles d'accès ou à toute autre fin, la modification est immédiatement mise en œuvre et a une incidence sur le trafic. Avec les règles d'accès, vous pouvez activer le modèle de validation transactionnelle pour vous assurer que les nouvelles règles ne deviennent actives qu'une fois la compilation des règles terminée, mais la compilation se produit après chaque ACE que vous modifiez.

Si vous souhaitez isoler davantage l'impact de la modification des listes de contrôle d'accès, vous pouvez apporter vos modifications dans une « session de configuration », qui est un mode isolé qui vous permet de modifier plusieurs ACE et objets avant de valider explicitement vos modifications. Ainsi, vous pouvez vous assurer que toutes les modifications prévues sont terminées avant de modifier le comportement du périphérique.

Avant de commencer

- Vous pouvez modifier les listes de contrôle d'accès référencées par une commande access-group, mais vous ne pouvez pas modifier les listes de contrôle d'accès référencées par une autre commande. Vous pouvez également modifier les listes de contrôle d'accès non référencées ou en créer de nouvelles.
- Vous pouvez créer ou modifier des objets et des groupes d'objets, mais si vous en créez un dans une session, vous ne pouvez pas le modifier dans la même session. Si l'objet n'est pas défini comme vous le souhaitez, vous devez valider vos modifications, puis modifier l'objet, ou ignorer la session complète et recommencer.
- Lorsque vous modifiez une liste de contrôle d'accès référencée par une commande access-group (règles d'accès), le modèle de validation transactionnelle est utilisé lorsque vous validez la session. Ainsi, l'ACL est complètement compilée avant que la nouvelle ACL ne remplace l'ancienne version.

Procédure

Étape 1 Démarrer une session.

```
hostname#configure session session_name
hostname(config-s)#
```

Si *session_name* existe déjà, vous ouvrez cette session. Sinon, vous créez une nouvelle session.

Utilisez la commande **show configuration session** pour afficher les sessions existantes. Vous pouvez avoir au maximum 3 sessions actives à la fois. Si vous devez supprimer une ancienne session inutilisée, utilisez la commande **clear configuration session** *session_name*.

Si vous ne pouvez pas ouvrir une session existante parce que quelqu'un d'autre la modifie, vous pouvez effacer l'indicateur qui indique que la session est en cours de modification. Effectuez cette opération uniquement si vous êtes certain que la session n'est pas modifiée. Utilisez la commande **clear session** *session_name* **access** pour réinitialiser l'indicateur.

Étape 2 (Sessions non validées uniquement.) Apportef vos modifications. Vous pouvez utiliser les commandes de base suivantes avec n'importe quel paramètre :

- **Accès-Liste**
- **objet**
- **object-group**

Étape 3 Décidez que faire de la session. Les commandes disponibles dépendent de la validation précédente de la session. Les commandes possibles sont :

- **exit** : pour quitter simplement la session sans valider ni ignorer les modifications, afin de pouvoir revenir ultérieurement.
- **commit** [**noconfirm** [**revert-save** | **config-save**]] : (sessions non validées uniquement.) Validez vos modifications. Il vous est demandé si vous souhaitez enregistrer la session. Vous pouvez enregistrer la session de rétablissement (**revert-save**), ce qui vous permet d'annuler vos modifications à l'aide de la commande **revert**, ou de la session de configuration (**config-save**), qui comprend toutes les modifications apportées dans la session (vous permettant de valider les mêmes modifications à nouveau si vous le souhaitez). Si vous enregistrez la session de restauration ou de configuration, les modifications sont validées, mais la session reste active. Vous pouvez ouvrir la session et revenir ou valider les modifications. Vous pouvez éviter l'invite en incluant l'option **noconfirm** et, éventuellement, l'option d'enregistrement souhaitée.
- **abort** : (sessions non validées uniquement.) Pour abandonner vos modifications et supprimer la session. Si vous souhaitez conserver la session, quittez la session et utilisez la commande **clear session** *session_name* **configuration**, qui vide la session sans la supprimer.
- **revert** : (sessions validées uniquement.) Pour annuler vos modifications, rétablissez la configuration à ce qu'elle était avant de valider la session, puis supprimez la session.
- **show configuration session** [*session_name*] : pour afficher les modifications apportées dans la session.

Surveiller les ACL

Pour superviser les ACLs, saisissez l'une des commandes suivantes :

- **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 ACL sont utilisées pour contrôler l'accès au réseau ou pour spécifier le trafic pour de nombreuses fonctionnalités à utiliser. 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 ACL de type Web sont utilisées dans le filtrage VPN SSL sans client. Les ACL EtherType contrôlent le trafic de couche 2 non IP. Nous avons lancé les commandes suivantes : **access-list extended, access-list standard, access-list webtype**, **access-list ethertype**.
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. Nous avons modifié les commandes suivantes : **access-list extended**.
Prise en charge des ACL EtherType pour le trafic IS-IS	8.4(5), 9.1(2)	En mode de pare-feu transparent, l'ASA peut désormais contrôler le trafic IS-IS à l'aide d'une liste de contrôle d'accès EtherType. Nous avons modifié la commande suivante : **access-list ethertype** {**permit** | **deny**} **isis**.
Prise en charge de 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. Nous avons modifié les commandes suivantes : **access-list extended**.

Nom de la caractéristique	Versions	Description
ACL unifiées étendues et de type Web pour IPv4 et IPv6	9.0(1)	Les ACL 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 ACL propres à IPv6 sont obsolètes. Les ACL IPv6 existantes sont migrées vers des ACL étendues. Pour en savoir plus, consultez les notes de mise à jour. Nous avons modifié les commandes suivantes : **access-list extended**, **access-list webtype**. Nous avons supprimé les commandes suivantes : **ipv6 access-list**, **ipv6 access-list webtype**, **ipv6-vpn-filter**.
Amélioration des ACL étendues et des objets pour filtrer le trafic ICMP par code ICMP	9.0(1)	Le trafic ICMP peut maintenant être autorisé ou refusé en fonction du code ICMP. Nous avons introduit ou modifié les commandes suivantes : **access-list extended**, **service-object**, **service**.
Session de configuration pour modifier les listes de contrôle d'accès et les objets. Référencement ultérieur des objets et desACL dans les règles d'accès.	9.3(2)	Vous pouvez maintenant modifier les ACL et les objets dans une session de configuration isolée. Vous pouvez également référencer des objets et des ACL à l'avance, c'est-à-dire configurer des règles et des groupes d'accès pour des objets ou des ACL qui n'existent pas encore. Nous avons introduit les commandes **clear configuration session**, **clear session**, **configure session**, **forward-reference** et **show configuration session**.
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 la commande suivante : **access-list extended** .
Prise en charge de la règle Ethertype pour l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2.	9.6(2)	Vous pouvez maintenant écrire des règles de contrôle d'accès Ethertype pour l'adresse du point d'accès de service de destination du paquet de contrôle de liaison logique IEEE 802.2. En raison de cet ajout, le mot clé **bpdu** ne correspond plus au trafic prévu. Rewrite **bpdu** rules for **dsap 0x42**. Nous avons modifié les commandes suivantes : **access-list ethertype**
Prise en charge en mode routé des règles EtherType sur les interfaces membres de groupes de ponts et des règles d'accès étendues sur les interfaces virtuelles de pont (BVI).	9.7(1)	Vous pouvez maintenant créer des ACL EtherType et les appliquer aux interfaces membres de groupes de ponts en mode routé. Vous pouvez également appliquer des règles d'accès étendues à l'interface virtuelle de pont (BVI) en plus des interfaces membres. Nous avons modifié les commandes suivantes : **access-group**, **access-list ethertype**.

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

À propos de la traduction

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

À propos de la traduction

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

À propos de la traduction

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