Objets pour le contrôle d'accès

Les objets sont des composants réutilisables pour votre configuration. Vous pouvez les définir et les utiliser dans les configurations ASA à la place des adresses IP en ligne, des services, des noms, etc. Les objets facilitent la maintenance de vos configurations, car vous pouvez modifier un objet à un seul emplacement et répercuter cette modification dans tous les autres emplacements qui y font référence. Sans objets, vous devriez modifier les paramètres pour chaque fonctionnalité en cas de besoin, plutôt qu'une seule fois. Par exemple, si un objet réseau définit une adresse IP et un masque de sous-réseau et que vous souhaitez modifier l'adresse, vous n'avez qu'à la modifier dans la définition de l'objet, et non dans toutes les fonctionnalités qui font référence à cette adresse IP.

Lignes directrices relatives aux objets

Lignes directrices pour IPv6

Prend en charge IPv6 avec les restrictions suivantes :

- Vous pouvez combiner les entrées IPv4 et IPv6 dans un groupe d'objets réseau, mais vous ne pouvez pas utiliser un groupe d'objets mixtes pour la NAT.

Lignes directrices et limites additionnelles

- Les objets doivent avoir des noms uniques, car les objets et les groupes d'objets partagent le même espace de nom. Bien que vous puissiez créer un groupe d'objets réseau nommé « Engineering » et un groupe d'objets de service nommé « Engineering », vous devez ajouter un identifiant (ou « tag ») à la fin d'au moins un nom de groupe d'objets pour le rendre unique. Par exemple, vous pouvez utiliser les noms « Engineering_admins » et « Engineering_hosts » pour rendre les noms de groupes d'objets uniques et faciliter l'identification.
- Les noms d'objets sont limités à 64 caractères, y compris les lettres, les chiffres et les caractères suivants : .!@#$%^&()-_{}. Les noms des objets sont sensibles à la casse.

Configurer les objets.

Les sections suivantes décrivent comment configurer les objets principalement utilisés pour le contrôle d'accès.

Configurer les objets et groupes de réseau

Les objets et les groupes de réseau identifient les adresses IP ou les noms d'hôtes. Utilisez ces objets dans les listes de contrôle d'accès pour simplifier vos règles.

Configurer un objet réseau

Un objet réseau peut contenir un hôte, une adresse IP de réseau, une plage d'adresses IP, ou un nom de domaine complet (FQDN).

Vous pouvez également activer les règles NAT sur l'objet (à l'exception des objets FQDN). Pour en savoir plus sur la configuration des objets NAT, consultez Traduction d'adresses réseau (NAT).

Procédure

Étape 1 Créez ou modifiez un objet réseau en utilisant le nom de l'objet : **object network** *object_name*

Exemple :

```
hostname(config)# object network email-server
```

Étape 2 Ajoutez une adresse à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour retirer l'objet.

- **host** {*IPv4_address* | *IPv6_address*} : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
- **range** *start_address end_address* : plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.
- **fqdn** [**v4** | **v6**] *fully_qualified_domain_name* : un nom de domaine complet, c'est-à-dire le nom d'un hôte, tel que www.example.com. Précisez **v4** pour limiter l'adresse à IPv4 et **v6** pour IPv6. Si vous ne spécifiez pas de type d'adresse, IPv4 est présumé.

Exemple :

```
hostname(config-network-object)# host 10.2.2.2
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

Configurer un groupe d'objets réseau

Les groupes d'objets réseau peuvent contenir plusieurs objets réseau, ainsi que des réseaux en ligne ou des hôtes. Les groupes d'objets réseau peuvent inclure une combinaison d'adresses IPv4 et IPv6.

Cependant, vous ne pouvez pas utiliser un groupe d'objets IPv4 et IPv6 mixtes pour la NAT, ou des groupes d'objets qui comprennent des objets FQDN.

Procédure

Étape 1 Créez ou modifiez un groupe d'objets réseau en utilisant le nom de l'objet : **object-group network** *group_name*

Exemple :

```
hostname(config)# object-group network admin
```

Étape 2 Ajoutez des objets et des adresses au groupe d'objets réseau à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **network-object host** {*IPv4_address* | *IPv6_address*} : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **network-object** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} : l'adresse d'un réseau ou d'un hôte. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
- **network-object object** *object_name* : nom d'un objet réseau existant.
- **group-object** *object_group_name* : nom d'un groupe d'objets réseau existant.

Exemple :

```
hostname(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
hostname(config-network-object-group)# network-object 2001:db8:0:cd30::/60
hostname(config-network-object-group)# network-object host 10.1.1.1
hostname(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
hostname(config-network-object-group)# network-object object existing-object-1
hostname(config-network-object-group)# group-object existing-network-object-group
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

Exemples

Pour créer un groupe de réseau qui comprend les adresses IP de trois administrateurs, entrez les commandes suivantes :

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
```

```
hostname (config-protocol)# network-object host 10.2.2.34
```

Créez des groupes d'objets réseau pour les utilisateurs privilégiés de différents services en entrant les commandes suivantes :

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

Vous imbriquez ensuite les trois groupes comme suit :

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

Configurer des objets de service et des groupes de services

Les objets et les groupes de service identifient les protocoles et les ports. Utilisez ces objets dans les listes de contrôle d'accès pour simplifier vos règles.

Configurer un objet de service

Un objet de service ne peut contenir qu'une seule spécification de protocole.

Procédure

Étape 1 Créez ou modifiez un objet de service en utilisant le nom de l'objet : **object service** *object_name*

Exemple :

```
hostname(config)# object service web
```

Étape 2 Ajoutez un service à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **service** *protocol* : nom ou numéro (0 à 255) d'un protocole IP. Précisez **ip** pour appliquer à tous les protocoles.
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]] : pour les messages ICMP ou ICMP version 6. Vous pouvez éventuellement spécifier le type ICMP par nom ou par numéro (0 à 255) pour limiter l'objet à

ce type de message. Si vous spécifiez un type, vous pouvez éventuellement spécifier un code ICMP pour ce type (1 à 255). Si vous ne spécifiez pas de code, tous les codes sont utilisés.

- **service** {**tcp** | **udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*] : pour TCP, UDP ou SCTP. Vous pouvez éventuellement préciser des ports pour la source, la destination ou les deux. Vous pouvez préciser le port par son nom ou son numéro. 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 100 200**.

Exemple :

```
hostname(config-service-object)# service tcp destination eq http
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

Configurer un groupe de services

Un groupe d'objets de service comprend un ensemble de protocoles, si nécessaire, y compris des ports source et de destination facultatifs pour les protocoles qui les utilisent, ainsi que le type et le code ICMP.

Avant de commencer

Vous pouvez modéliser tous les services à l'aide du groupe d'objets de service générique, qui est expliqué ici. Cependant, vous pouvez toujours configurer les types d'objets de groupe de services qui étaient disponibles avant l'ASA 8.3(1). Ces objets existants comprennent des groupes de ports TCP/UDP/TCP-UDP, des groupes de protocoles et des groupes ICMP. Le contenu de ces groupes est équivalent à la configuration associée dans le groupe d'objets de service générique, à l'exception des groupes ICMP, qui ne prennent pas en charge les codes ICMP6 ou ICMP. Si vous souhaitez toujours utiliser ces objets existants, pour obtenir des instructions détaillées, consultez la description de la commande **object-service** dans la référence de commande sur Cisco.com.

Procédure

Étape 1 Créez ou modifiez un groupe d'objets de service en utilisant le nom de l'objet : **object-group service** *object_name*

Exemple :

```
hostname(config)# object-group service general-services
```

Étape 2 Ajoutez des objets et des services au groupe d'objets de service à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **service-object** *protocol* : nom ou numéro (0 à 255) d'un protocole IP. Précisez **ip** à appliquer à tous les protocoles.
- **service-object** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]] : pour les messages ICMP ou ICMP version 6. Vous pouvez éventuellement spécifier le type ICMP par nom ou par numéro (0 à 255) pour limiter l'objet à ce type de message. Si vous spécifiez un type, vous pouvez éventuellement spécifier un code ICMP pour ce type (1 à 255). Si vous ne spécifiez pas de code, tous les codes sont utilisés.
- **service-object** {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*] : : pour TCP, UDP ou les deux, ou pour SCTP. Vous pouvez éventuellement préciser des ports pour la source, la destination ou les deux. Vous pouvez préciser le port par son nom ou son numéro. 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**.
- **service-object object** *object_name*—nom d'un objet de service existant.
- **group-object** *object_group_name*—nom d'un groupe d'objets de service existant.

Exemple :

```
hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

Exemples

L'exemple suivant montre comment ajouter des services TCP et UDP à un groupe d'objets de service :

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object tcp destination eq ftp
hostname(config-service-object-group)# service-object tcp-udp destination eq www
hostname(config-service-object-group)# service-object tcp destination eq h323
hostname(config-service-object-group)# service-object tcp destination eq https
hostname(config-service-object-group)# service-object udp destination eq ntp
```

L'exemple suivant montre comment ajouter plusieurs objets de service à un groupe d'objets de service :

```
hostname(config)# object service SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# object service HTTPS
hostname(config-service-object)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
hostname(config-service-object-group)# service-object object HTTPS
```

Configuration des objets et des groupes de service réseau

Un objet ou un groupe de service réseau définit une application. Une application peut consister en un nom de domaine DNS (comme example.com), un sous-réseau IP et, éventuellement, un protocole et un port, comme TCP/80. Ainsi, un objet ou un groupe de service réseau peut combiner le contenu d'objets de réseau et de service distincts en un seul objet.

Vous pouvez utiliser le groupe d'objets de service réseau dans une liste de contrôle d'accès étendue à utiliser avec les listes de routage (dans le routage basé sur les politiques), les règles de contrôle d'accès et le filtre VPN. Notez que vous ne pouvez pas utiliser directement un objet de service réseau (et non un groupe) dans une liste de contrôle d'accès : vous devez d'abord placer des objets dans un objet de groupe, puis vous pouvez utiliser l'objet de groupe.

Lorsque vous utilisez des spécifications de nom de domaine, le système utilise la surveillance DNS pour obtenir les adresses IP obtenues par la demande DNS de l'utilisateur avant le début de la connexion. Cela garantit qu'une adresse IP est disponible au début d'une connexion, afin que la connexion soit gérée correctement, par des listes de routage et des règles de contrôle d'accès, à partir du premier paquet.

Lignes directrices relatives aux objets de service réseau

- L'inspection DNS est requise si vous incluez des spécifications de nom de domaine DNS dans un objet de service réseau. L'inspection DNS est activée par défaut. Ne la désactivez pas si vous utilisez des objets de service réseau.
- La surveillance de trafic DNS est effectuée uniquement sur les paquets DNS UDP et n'est pas effectuée sur les paquets DNS TCP ou HTTP. Contrairement aux objets de nom de domaine complets, les spécifications de domaine de service de réseau sont détectées immédiatement, même si vous n'utilisez pas l'objet dans une liste d'accès.
- Vous ne pouvez pas activer dnscrypt dans la liste des politiques d'inspection DNS ; il n'est pas compatible avec la surveillance DNS nécessaire pour obtenir les adresses IP des domaines utilisés dans les objets de service réseau. Tous les objets de service réseau qui comprennent des spécifications de domaine deviendront inopérants et les entrées de contrôle d'accès connexes ne correspondront pas.
- Vous pouvez définir un maximum de 1024 groupes de services réseau. Cependant, cette limite est partagée avec les groupes d'utilisateurs locaux de pare-feu d'identité. Pour chaque groupe de service de réseau défini, vous pouvez créer 2 groupes d'utilisateurs de moins.
- Les contenus des groupes de services réseau peuvent se chevaucher, mais vous ne pouvez pas créer la copie complète d'un groupe de services réseau.
- Si un objet ou un groupe de service réseau est utilisé dans une liste de contrôle d'accès, la suppression de l'objet efface simplement le contenu de l'objet. L'objet lui-même reste défini dans la configuration.

- Le mot-clé **dynamic** sur un objet ou un groupe indique que l'objet ne sera pas enregistré dans la configuration en cours d'exécution, il sera affiché uniquement dans la sortie **show object**. Ne configurez pas directement ce mot-clé. Il est principalement utilisé par les gestionnaires d'appareils externes.
- La commande **app-id** pour un objet de service réseau définit un numéro attribué par Cisco pour une application particulière, dans la plage de 1 à 4294967295. Ne configurez pas directement cette commande. Cette commande est principalement destinée à l'utilisation de gestionnaires d'appareils externes.

Configurer des serveurs DNS de confiance

Si vous configurez les noms de domaine dans les objets de service réseau, le système espionne le trafic de demande/réponse DNS pour recueillir les adresses IP des noms de domaine DNS et mettre les résultats en cache. Toute demande/réponse DNS peut être espionnée.

Les enregistrements espionnés sont A, AAAA et MX. La durée de vie (TTL) de chaque nom résolu est prise en compte dans les limites suivantes : le TTL minimal est de 2 minutes, et le maximum est de 24 heures. Cela garantit que le cache ne devient pas périmé.

Pour des raisons de sécurité, vous pouvez limiter la portée de la surveillance DNS en définissant quels serveurs DNS doivent être considérés comme de confiance. Tout trafic DNS vers des serveurs DNS non de confiance est ignoré et n'est pas utilisé pour obtenir des mappages pour les objets de service réseau. Par défaut, tous les serveurs DNS configurés et appris sont de confiance; vous ne devez modifier ce réglage que si vous souhaitez limiter la liste de confiance.

Remarque La clé est que vous définissez les serveurs DNS utilisés par vos clients comme serveurs de confiance.

Avant de commencer

La surveillance DNS dépend de l'inspection DNS, qui est activée par défaut. Assurez-vous de ne pas désactiver l'inspection. En outre, la surveillance DSN est incompatible avec la fonctionnalité **dnscrypt**, donc n'activez pas cette commande dans la liste des politiques d'inspection DNS.

Procédure

Étape 1 Utilisez la commande **show dns trusted-source detail** pour déterminer les serveurs de confiance actuels qui ont été téléchargés dans le chemin de données pour une utilisation avec la résolution de domaine d'objet de service réseau.

La valeur par défaut est de faire confiance à tout serveur DNS que vous configurez dans un groupe DNS ou qui est configuré par l'intermédiaire d'un client/serveur DHCP ou d'un relais. Cette commande vous affiche les paramètres actuels et les serveurs auxquels vous faites confiance.

Exemple :

```
ciscoasa# show dns trusted-source detail
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
```

```
    DNS Server Configured: 10.163.47.11: management : N/A
    DNS Server Configured: 10.37.137.85: management : N/A
    DNS Server Configured: 10.37.142.73: management : N/A
Data-Path DNS Trusted Source (count 3): <ip>/<refcnt>; Trust-any disabled
  10.37.142.73/1
  10.37.137.85/1
  10.163.47.11/1
```

Étape 2 (Facultatif) Ajoutez ou supprimez des serveurs DNS de confiance configurés de manière explicite :

dns trusted-source *liste_ip*

La *liste_ip* est une liste séparée par des espaces des adresses IP des serveurs DNS auxquels il faut faire confiance. Vous pouvez répertorier jusqu'à 12 adresses IPv4 et IPv6. Précisez **any** pour couvrir tous les serveurs DNS. Utilisez la forme **no** de la commande pour retirer un serveur.

Étape 3 (Facultatif) Indiquez si les serveurs configurés dans les groupes de serveurs DNS doivent être considérés comme fiables.

dns trusted-source configured-servers

Un serveur configuré est un serveur spécifié dans les groupes DNS ou les commandes de serveur de noms. Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Étape 4 (Facultatif) Indiquez si les serveurs DNS configurés dans les ensembles DHCP pour les clients qui obtiennent des adresses par l'intermédiaire des serveurs DHCP exécutés sur les interfaces d'appareils doivent être considérés comme fiables.

dns trusted-source dhcp-pools

Il s'agit des serveurs qui sont configurés sur la commande **dhcpd dns** et sont donc uniquement IPv4. Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Étape 5 (Facultatif) Indiquez si les serveurs identifiés par la surveillance des messages de relais DHCP entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance.

dns trusted-source dhcp-relay

Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Étape 6 (Facultatif) Indiquez si les serveurs identifiés par la surveillance des messages entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance.

dns trusted-source dhcp-client

Cette option s'applique lorsque vous configurez la commande **dhcpd auto_config** pour configurer les serveurs DHCP sur les interfaces internes en utilisant les informations obtenues à partir des interfaces de l'appareil qui utilisent le client DHCP pour obtenir une adresse IP. Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Configurer les objets de service de réseau

Un objet de service réseau définit une seule application. Il définit l'emplacement de l'application par la spécification du sous-réseau ou, plus communément, par le nom de domaine DNS. Vous pouvez également inclure le protocole et le port pour restreindre la portée de l'application.

Vous ne pouvez utiliser ces objets que dans des objets de groupe de services réseau; vous ne pouvez pas utiliser directement un objet de service réseau dans une entrée de liste de contrôle d'accès (ACE).

Procédure

Étape 1 Créez ou modifiez un objet de service réseau en utilisant le nom d'objet :

object network-service *object_name*

Le nom peut comporter jusqu'à 128 caractères. Si vous incluez des espaces, vous devez mettre le nom entre guillemets doubles.

Exemple :

```
ciscoasa(config)# object network-service webex
```

Étape 2 Ajoutez un ou plusieurs emplacements d'application et services facultatifs à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer l'emplacement. Vous pouvez entrer ces commandes plusieurs fois.

- **domain** *domain_name* [*service*] : le nom DNS, jusqu'à 253 caractères. Il peut s'agir d'un nom complet (comme www.example.com) ou partiel (comme example.com), auquel cas l'objet correspond à tous les sous-domaines, c'est-à-dire les serveurs avec le nom partiel (comme www.example.com, www1.example.com, long.server.name.example.com, etc.). Les connexions seront comparées au nom le plus long si une correspondance exacte est disponible. Le nom de domaine peut se résoudre en plusieurs adresses IP.
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.

La spécification de service pour ces commandes est la même. Précisez le service uniquement si vous souhaitez limiter la portée des connexions correspondantes. Par défaut, toute connexion aux adresses IP résolues correspond à l'objet.

protocol [*operator port*]

où :

- *protocol* est le protocole utilisé dans la connexion, tel que tcp, udp, ip, etc. Utilisez ? pour voir la liste des protocoles.
- (TCP/UDP uniquement) *operator* est l'un des suivants :
  - **eq** est égal au numéro de port spécifié.
  - **lt** désigne tout port inférieur au numéro de port spécifié.
  - **gt** désigne tout port supérieur au numéro de port spécifié.
  - **range** désigne tout port entre les deux ports spécifiés.
- (TCP/UDP uniquement.) *port* est le numéro de port, de 1 à 65 535 ou un mnémonique, tel que www. Utilisez ? pour voir les mnémoniques. Pour les plages, vous devez spécifier deux ports, le premier port étant un nombre inférieur au deuxième.

Étape 3 (Facultatif) Ajoutez une description (jusqu'à 200 caractères) : **description** *string*

Exemples

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

Configurer les groupes d'objets de service réseau

Les groupes de services réseau peuvent contenir des objets de service réseau et des spécifications explicites de sous-réseau ou de domaine. Vous pouvez utiliser des objets de service réseau dans les entrées de liste de contrôle d'accès (ACE) pour le routage basé sur les politiques, le contrôle d'accès et le filtre VPN.

Utilisez des groupes de services réseau pour définir une catégorie d'applications qui doivent être gérées de la même manière. Par exemple, vous pouvez créer un groupe unique qui définit les applications dont le trafic doit être dirigé vers Internet plutôt que vers le tunnel VPN de site à site vers la plateforme centrale de l'entreprise.

Il n'y a aucune limite au nombre d'applications que vous incluez dans un groupe d'objets de service réseau, que ce soit explicitement ou par référence à des objets de service réseau.

Procédure

Étape 1 Créez ou modifiez un groupe d'objets de service réseau en utilisant le nom de groupe :

object-group network-service *group_name*

Le nom peut comporter jusqu'à 128 caractères et peut inclure des espaces. Si vous incluez des espaces, vous devez mettre le nom entre guillemets doubles.

Exemple :

```
ciscoasa(config)# object-group network-service SaaS_Applications
```

Étape 2 Ajoutez un ou plusieurs emplacements d'application et services facultatifs à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer l'emplacement. Vous pouvez entrer ces commandes plusieurs fois.

- **network-service-member** *object_name* : le nom d'un objet de service réseau à inclure dans le groupe. S'il y a des espaces dans le nom, mettez le nom entre guillemets doubles.
- **domain** *domain_name* [*service*] : le nom DNS, jusqu'à 253 caractères. Il peut s'agir d'un nom complet (comme www.example.com) ou partiel (comme example.com), auquel cas l'objet correspond à tous les sous-domaines, c'est-à-dire les serveurs avec le nom partiel (comme www.example.com, www1.example.com, long.server.name.example.com, etc.). Les connexions seront comparées au nom le plus long si une correspondance exacte est disponible. Le nom de domaine peut se résoudre en plusieurs adresses IP.

- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.

La spécification de service pour ces commandes est la même. Précisez le service uniquement si vous souhaitez limiter la portée des connexions correspondantes. Par défaut, toute connexion aux adresses IP résolues correspond à l'objet.

protocol [*operator port*]

où :

- *protocol* est le protocole utilisé dans la connexion, tel que tcp, udp, ip, etc. Utilisez ? pour voir la liste des protocoles.
- (TCP/UDP uniquement) *operator* est l'un des suivants :
  - **eq** est égal au numéro de port spécifié.
  - **lt** désigne tout port inférieur au numéro de port spécifié.
  - **gt** désigne tout port supérieur au numéro de port spécifié.
  - **range** désigne tout port entre les deux ports spécifiés.
- (TCP/UDP uniquement.) *port* est le numéro de port, de 1 à 65 535 ou un mnémonique, tel que www. Utilisez ? pour voir les mnémoniques. Pour les plages, vous devez spécifier deux ports, le premier port étant un nombre inférieur au deuxième.

Étape 3 (Facultatif) Ajoutez une description (jusqu'à 200 caractères) : **description** *string*

Exemples

Configurez un ensemble d'applications SaaS à l'aide d'objets de service réseau définis précédemment.

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

Configurer les groupes d'utilisateurs locaux

Vous pouvez créer des groupes d'utilisateurs locaux à utiliser dans les fonctionnalités qui prennent en charge le pare-feu d'identité en incluant le groupe dans une liste de contrôle d'accès étendue, qui peut à son tour être utilisée dans une règle d'accès, par exemple.

L'ASA envoie une requête LDAP au serveur Active Directory pour les groupes d'utilisateurs globalement définis dans le contrôleur de domaine Active Directory. L'ASA importe ces groupes pour les règles basées sur l'identité. Cependant, l'ASA peut avoir des ressources réseau locales qui ne sont pas définies globalement, ce qui nécessite des groupes d'utilisateurs locaux avec des politiques de sécurité locales. Les groupes

d'utilisateurs locaux peuvent contenir des groupes imbriqués et des groupes d'utilisateurs importés d'Active Directory. L'ASA consolide les groupes locaux et Active Directory.

Un utilisateur peut appartenir à des groupes d'utilisateurs locaux et à des groupes d'utilisateurs importés d'Active Directory.

Comme vous pouvez utiliser les noms d'utilisateurs et les noms de groupes d'utilisateurs directement dans une liste de contrôle d'accès, vous ne devez configurer les groupes d'utilisateurs locaux que si :

- Vous souhaitez créer un groupe d'utilisateurs défini dans la base de données LOCAL.
- Vous souhaitez créer un groupe d'utilisateurs ou de groupes d'utilisateurs qui ne sont pas capturés dans un seul groupe d'utilisateurs défini sur le serveur AD.

Procédure

Étape 1 Créez ou modifiez un groupe d'objets utilisateur en utilisant le nom de l'objet : **object-group user** *group_name*

Exemple :

```
hostname(config)# object-group user admins
```

Étape 2 Ajoutez des utilisateurs et des groupes au groupe d'objets utilisateur à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **user** [*domain_NETBIOS_name*\]*username* : un nom d'utilisateur. S'il y a un espace dans le nom de domaine ou le nom d'utilisateur, vous devez placer le nom de domaine et le nom d'utilisateur entre guillemets. Le nom de domaine peut être LOCAL (pour les utilisateurs définis dans la base de données locale) ou un nom de domaine Active Directory (AD), comme spécifié dans la commande **user-identity domain** *domain_NetBIOS_name* **aaa-server** *aaa_server_group_tag* . Lors de l'ajout d'utilisateurs définis dans un domaine AD, *user_name* doit être le sAMAccountName d'Active Directory, qui est unique, plutôt que le nom commun (cn), qui peut ne pas être unique. Si vous ne spécifiez pas de nom de domaine, le nom par défaut est utilisé, qui est LOCAL ou celui défini dans la commande **user-identity default-domain**.
- **user-group** [*domain_NETBIOS_name*\]*username* : un groupe d'utilisateurs. S'il y a un espace dans le nom de domaine ou le nom du groupe, vous devez placer le nom de domaine et le nom du groupe entre guillemets. Notez le double \\ qui sépare les noms de domaine et de groupe.
- **group-object** *object_group_name* : nom d'un groupe d'objets utilisateur existant.

Exemple :

```
hostname(config-user-object-group)# user EXAMPLE\admin
hostname(config-user-object-group)# user-group EXAMPLE\\managers
hostname(config-user-object-group)# group-object local-admins
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

Configurer les groupes d'objets de sécurité

Vous pouvez créer des groupes d'objets de groupe de sécurité pour une utilisation dans les fonctionnalités qui prennent en charge Cisco TrustSec en incluant le groupe dans une liste de contrôle d'accès étendue, qui peut à son tour être utilisée dans une règle d'accès, par exemple.

Lorsqu'il est intégré à Cisco TrustSec, l'ASA télécharge les informations de groupe de sécurité à partir d'ISE. L'ISE agit comme un référentiel d'identité en fournissant un mappage d'identité balise Cisco TrustSec à utilisateur et un mappage de ressource balise à serveur Cisco TrustSec. Vous provisionnez et gérez les listes de contrôle d'accès de groupe de sécurité de manière centralisée sur ISE.

Cependant, l'ASA peut avoir des ressources réseau locales qui ne sont pas définies globalement et qui nécessitent des groupes de sécurité locaux avec des politiques de sécurité locales. Les groupes de sécurité locaux peuvent contenir des groupes de sécurité imbriqués qui sont téléchargés à partir d'ISE. L'ASA consolide les groupes de sécurité locaux et centraux.

Pour créer des groupes de sécurité locaux sur l'ASA, vous créez un groupe d'objets de sécurité local. Un groupe d'objets de sécurité local peut contenir un ou plusieurs groupes d'objets de sécurité imbriqués ou des identifiants de sécurité ou des noms de groupes de sécurité. Vous pouvez également créer un nouvel ID de sécurité ou un nom de groupe de sécurité qui n'existe pas sur l'ASA.

Vous pouvez utiliser les groupes d'objets de sécurité que vous créez sur l'ASA pour contrôler l'accès aux ressources réseau. Vous pouvez utiliser le groupe d'objets de sécurité dans le cadre d'un groupe d'accès ou d'une politique de service.

Astuces Si vous créez un groupe avec des balises ou des noms qui ne sont pas connus de l'ASA, toutes les règles qui utilisent le groupe seront inactives jusqu'à ce que les balises ou les noms soient résolus avec ISE.

Procédure

Étape 1 Créez ou modifiez un groupe d'objets de groupe de sécurité en utilisant le nom d'objet : **object-group security** *group_name*

Exemple :

```
hostname(config)# object-group security mktg-sg
```

Étape 2 Ajoutez des objets au groupe d'objets du groupe de services à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **security-group** {**tag** *sgt_number* | **name** *sg_name*} : balise de groupe de sécurité (SGT) ou nom. Une balise est un nombre de 1 à 65 533 et est attribuée à un périphérique par l'authentification IEEE 802.1X, l'authentification Web ou le contournement de l'authentification MAC (MAB) par ISE. Les noms de groupes de sécurité sont créés sur l'ISE et fournissent des noms conviviaux pour les groupes de sécurité. La table des groupes de sécurité mappe les balises SGT aux noms de groupes de sécurité. Consultez votre configuration ISE pour connaître les balises et les noms valides.
- **group-object** *object_group_name* : nom d'un groupe d'objets de groupe de sécurité existant.

Exemple :

```
hostname(config-security-object-group)# security-group tag 1
hostname(config-security-object-group)# security-group name mgkt
hostname(config-security-object-group)# group-object local-sg
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

Configurer les plages de temps

Un objet de plage temporelle définit une durée spécifique composée d'une heure de début, d'une heure de fin et d'entrées récurrentes facultatives. Vous utilisez ces objets dans les règles ACL pour fournir un accès défini dans le temps à certaines fonctionnalités ou ressources. Par exemple, vous pouvez créer une règle d'accès qui autorise l'accès à un serveur particulier pendant les heures de travail uniquement.

Remarque Vous pouvez inclure plusieurs entrées périodiques dans un objet de plage temporelle. Si une plage temporelle comporte à la fois des valeurs absolues et des valeurs périodiques, les valeurs périodiques ne sont exploitées qu'une fois l'heure de début absolue atteinte et ne sont plus exploitées une fois l'heure de fin absolue atteinte.

La création d'une plage temporelle ne restreint pas l'accès au périphérique. Cette procédure définit uniquement la plage temporelle. Vous devez ensuite utiliser l'objet dans une règle de contrôle d'accès.

Procédure

Étape 1 Créez la plage de temps: **time-range** *name*

Étape 2 (Facultatif) Ajoutez une heure de début ou de fin (ou les deux) à la plage temporelle.

absolute [**start** *time date*] [**end** *time date*]

Si vous ne spécifiez pas d'heure de début, l'heure de début par défaut est maintenant.

L'*heure* est au format 24 heures *hh*:*mm*. Par exemple, 8:00 correspond à 8 h et 20:00 à 20 h.

La *date* est au format *jour mois année*; par exemple, **1 janvier 2014**.

Étape 3 (Facultatif) Ajouter des périodes récurrentes.

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

Vous pouvez spécifier les valeurs suivantes pour *days-of-the-week*. Notez que vous pouvez spécifier un deuxième jour de la semaine uniquement si vous spécifiez un seul jour pour le premier argument.

- **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, ou **Sunday**. Vous pouvez en spécifier plusieurs, séparés par des espaces, pour le premier argument *days-of-the-week*.
- **tous les jours**
- **jours de la semaine**
- **fin de semaine**

L'*heure* est au format 24 heures *hh*:*mm*. Par exemple, 8:00 correspond à 8 h et 20:00 à 20 h.

Vous pouvez répéter cette commande pour configurer plusieurs périodes récurrentes.

Exemples

Voici un exemple de plage de temps absolue commençant à 8 h le 1/01/2006. Comme aucune heure et date de fin ne sont spécifiées, la plage temporelle est en vigueur indéfiniment.

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

Voici un exemple de plage temporelle hebdomadaire de 8 h à 18 h en semaine :

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

L'exemple suivant établit une date de fin pour la plage temporelle et définit une période en semaine de 8 h à 17 h, avec des heures différentes après 17 h pour lundi, mercredi, vendredi par rapport à mardi, jeudi.

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

Surveillance des objets

Pour surveiller des objets et des groupes, entrez les commandes suivantes :

- **show access-list**

  Affiche les entrées de la liste d'accès. Les entrées qui comprennent des objets sont également développées en entrées individuelles en fonction du contenu de l'objet.

- **show running-config object** [**id** *object_id*]

  Affiche tous les objets actuels. Utilisez le mot-clé **id** pour afficher un seul objet par nom.

- **show running-config object** *object_type*

  Affiche les objets actuels par type, **network** ou **service**.

- **show running-config object-group** [**id** *group_id*]

  Affiche tous les groupes d'objets actuels. Utilisez le mot-clé **id** pour afficher un seul groupe d'objets par nom.

- **show running-config object-group** *grp_type*

Affiche les groupes d'objets actuels par type de groupe.

Historique pour les objets

Nom de la caractéristique	Observations Versions	Description
Groupes d'objets	7.0(1)	Les groupes d'objets simplifient la création et la maintenance des listes de contrôle d'accès. Nous avons introduit ou modifié les commandes suivantes : **object-group** *protocol*, **object-group** *network*, **object-group** *service*, **object-group** *icmp_type*.
Expressions régulières et listes des politiques	7.2(1)	Les expressions régulières et les listes des politiques ont été introduites pour être utilisées dans les listes des politiques d'inspection. Les commandes suivantes ont été introduites : **class-map type regex**, **regex**, **match regex**.
Objets	8.3(1)	La prise en charge des objets a été introduite. Nous avons introduit ou modifié les commandes suivantes : **object-network**, **object-service**, **object-group** network, **object-group** service, **network object**, **access-list extended**, **access-list webtype**, **access-list remark**.
Groupes d'objets utilisateur pour le pare-feu d'identité	8.4(2)	Les groupes d'objets utilisateur pour le pare-feu d'identité ont été introduits. Nous avons introduit les commandes suivantes : **object-network user**, **user**.
Groupes d'objets de groupe de sécurité pour Cisco TrustSec	8.4(2)	Les groupes d'objets de groupe de sécurité pour Cisco TrustSec ont été introduits. Nous avons introduit les commandes suivantes : **object-network security**, **security**.
Groupes d'objets réseau mixtes IPv4 et IPv6	9.0(1)	Auparavant, les groupes d'objets réseau ne pouvaient contenir que toutes les adresses IPv4 ou toutes les adresses IPv6. Les groupes d'objets réseau peuvent désormais prendre en charge une combinaison d'adresses IPv4 et IPv6. **Remarque** Vous ne pouvez pas utiliser un groupe d'objets mixtes pour la NAT. Nous avons modifié les commandes suivantes : **object-group network**.
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**.

Nom de la caractéristique	Observations Versions	Description
Prise en charge des objets de service pour le protocole SCTP (Stream Control Transmission Protocol)	9.5(2)	Vous pouvez maintenant créer des objets de service et des groupes qui spécifient des ports SCTP. Nous avons modifié les commandes suivantes : **service-object**, **service**.
Objets de service réseau et leur utilisation dans le routage et le contrôle d'accès basés sur des politiques	9.17(1)	Vous pouvez configurer des objets de service de réseau et les utiliser dans des listes de contrôle d'accès étendues pour les utiliser dans les cartes de routage basées sur des politiques et les groupes de contrôle d'accès. Les objets de service de réseau comprennent les spécifications de sous-réseau IP ou de nom de domaine DNS, ainsi que les spécifications de protocole et de port, qui combinent notamment des objets de réseau et de service. Cette fonctionnalité comprend également la possibilité de définir des serveurs DNS de confiance, pour s'assurer que toutes les résolutions de noms de domaine DNS acquièrent des adresses IP de sources de confiance. Nous avons ajouté ou modifié les commandes suivantes : **access-list extended**, **app-id**, **clear configure object network-service**, **clear configure object-group network-service**, **clear dns ip-cache**, **clear object**, **clear object-group**, **debug network-service**, **description**, **dns trusted-source**, **domain**, **network-service-member**, **network-service reload**, **object-group network-service**, **object network-service**, **policy-route cost**, **set adaptive-interface cost**, **show asp table classify**, **show asp table network-service**, **show dns trusted-source**, **show dns ip-cache**, **show object**, **show object-group**, **show running-config**, **subnet**.
Prise en charge des groupes de services réseau	9.19(1)	Vous pouvez désormais définir un maximum de 1 024 groupes de services réseau.

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.