

Objets pour le contrôle d'accès.

Les objets sont des composants réutilisables dans 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, à la page 1
- Configurer les objets., à la page 2
- Objets de surveillance, à la page 13
- Historique pour les objets, à la page 13

Lignes directrices relatives aux objets

Directives 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.

Directives 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.
- Lorsque vous saisissez plusieurs éléments dans l'adresse source ou de destination, ou dans le service source ou de destination, dans une ACL ou une règle d'accès, ASDM crée automatiquement un groupe d'objets pour eux avec le préfixe DM_INLINE. Ces objets ne sont pas affichés dans la page des objets, mais ils sont définis sur le périphérique.

- 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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Network Object (Objet réseau)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Configurez l'adresse de l'objet en fonction des champs **Type** et **IP Version** (Version IP).

- **Hôte** : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **Réseau** : l'adresse d'un réseau. Pour IPv4, incluez le masque, par exemple, **adresse IP** = 10.0.0.0 **masque réseau** = 255.0.0.0. Pour IPv6, incluez le préfixe, tel que **adresse IP** = 2001:DB8:0:CD30:: **longueur du préfixe** = 60.
- **Plage** : une plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.
- **FQDN** : un seul nom de domaine complet, tel que www.exemple.com.

Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser cet objet réseau lorsque vous créez une règle. Si vous modifiez un objet, la modification est automatiquement héritée par toutes les règles qui utilisent l'objet.

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Network Object Group** (Groupe d'objets réseau) pour ajouter un nouvel objet. Saisissez un nom et éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des objets réseau au groupe en utilisant n'importe quelle combinaison des techniques suivantes :

- **Existing Network Objects/Groups** (Objets/groupes réseau existants) : sélectionnez un objet ou un groupe réseau déjà défini, puis cliquez sur **Add** (Ajouter) pour l'inclure dans le groupe.
- **Create New Network Object Member** (Créer un membre d'objet réseau) : saisissez les critères d'un nouvel objet réseau et cliquez sur **Add** (Ajouter).

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser cet objet réseau lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Service Object/Group (Objet/groupe de services)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Service Object (Objet de service)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Choisissez le type de service et complétez les détails au besoin :

- Protocol (Protocole) : un numéro entre 0-255, ou un nom connu, tel que **ip**, **tcp**, **udp**, **gre**, etc.
- ICMP, ICMP6 : vous pouvez laisser les champs de type de message et de code vides pour correspondre à n'importe quel message 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 (de 1 à 255). Si vous ne spécifiez pas de code, tous les codes sont utilisés.
- TCP, UDP, SCTP : vous pouvez éventuellement spécifier des ports pour la source, la destination ou les deux. Vous pouvez préciser le port par son nom ou son numéro. Vous pouvez inclure les opérateurs suivants :
  - **<** : inférieur à. Par exemple, <80.
  - **>** : supérieur à. Par exemple, >80.
  - **!=** : différent de. Par exemple, !=80.
  - **-** (trait d'union) : une plage inclusive de valeurs. Par exemple, 100-200.

Étape 4 Cliquez sur **OK**, puis sur **Apply**(appliquer).

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Service Objects/Groups (Objets/groupes de services)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Service Group (Groupe de services)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des objets de service au groupe en utilisant n'importe quelle combinaison des techniques suivantes :

- **Existing Service/Service Group** (Service/groupe de services existant) : sélectionnez un service, un objet de service ou un groupe déjà défini, puis cliquez sur **Add** (Ajouter) pour l'inclure dans le groupe.
- **Create New Member** (Créer un membre) : saisissez les critères d'un nouvel objet de service et cliquez sur **Add** (Ajouter). Si vous donnez un nom à l'objet, lorsque vous appliquez les modifications, le nouvel objet est créé et ajouté au groupe; sinon, les objets sans nom sont membres de ce groupe uniquement. Vous ne pouvez pas nommer les objets TCP-UDP; ceux-ci sont membres du groupe seulement.

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser ce groupe d'objets de service lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

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 exemple.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 de 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 4 294 967 295. 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 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**.

Étape 2 Sous **Trusted DNS Server** (Serveur DNS de confiance), configurez les options permettant de déterminer quels serveurs sont considérés comme fiables.

a) (Facultatif) Ajoutez ou supprimez des serveurs DNS de confiance configurés de manière explicite.

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau serveur, sélectionnez le type d'adresse IP (IPv4 ou IPv6), saisissez l'adresse IP du serveur et cliquez sur **OK**.
- Sélectionnez un serveur et cliquez sur **Edit** (Modifier) pour modifier l'adresse.
- Sélectionnez un serveur et cliquez sur **Delete** (Supprimer) pour le supprimer de la liste des serveurs de confiance.

b) Sélectionnez ou désélectionnez les options suivantes :

- **Any** (Tous) : faites confiance à tous les serveurs DNS, surveillez-les tous. Cette option est désactivée par défaut.
- **Configured-Servers** (Serveurs configurés) : indique si les serveurs configurés dans les groupes de serveurs DNS doivent être considérés comme fiables. Par défaut, cette option est activée.
- **DHCP-Client** (Client DHCP) : indique 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. Par défaut, cette option est activée.
- **DHCP-Pools** (Ensembles DHCP) : indique 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. Par défaut, cette option est activée.
- **DHCP-Relay** (Relais DHCP) : indique 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. Par défaut, cette option est activée.

Étape 3 Cliquez sur **Apply** (Appliquer).

Configurer les objets de service 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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Services Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter)** > **Network Services Objects (Objets de services réseau)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.

- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 (Non recommandé). Ajoutez l'ID de l'application dans le champ **App-ID**.

Il s'agit d'un numéro unique attribué par Cisco pour une application particulière, dans la plage de 1 à 4 294 967 295. Cette option est principalement destinée à l'utilisation de gestionnaires de périphérique externes. Vous ne devez pas configurer cette valeur.

Étape 4 Ajoutez un ou plusieurs membres à l'objet :

a) Sélectionnez l'une des options suivantes dans **Create New Member** (Créer un nouveau membre), puis remplissez les informations d'adresse appropriées :

- **domain** (domaine) : nom du 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** (sous-réseau) : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez l'adresse et le masque réseau, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe, par exemple 2001:DB8:0:CD30::/60. Saisissez les valeurs appropriées dans les champs suivants :

b) Sélectionnez l'une des options suivantes dans Type de service, puis remplissez les champs appropriés :

- **protocol (protocole)** : le protocole utilisé dans la connexion, tel que tcp, udp, ip, etc. Pour rendre l'objet indépendant du service, saisissez simplement **ip**.
- **tcp** ou **udp** : saisissez le numéro de port, 1 à 65 535 ou un mnémonique, tel que www. Pour un port unique, saisissez simplement le numéro de port. Pour plusieurs ports, vous pouvez inclure le nombre après les opérateurs suivants :
  - < signifie tout port inférieur au numéro de ports spécifiés.
  - > désigne tout port supérieur au numéro de ports spécifiés.
  - **range** désigne tout port entre les deux ports spécifiés. Le premier numéro de port doit être inférieur au deuxième numéro de port.

c) Cliquez sur **Add** (ajouter) pour ajouter l'entrée à l'objet. Pour supprimer un service, sélectionnez-le et cliquez sur **Delete** (Supprimer).

d) Répétez le processus jusqu'à ce que l'objet contienne toutes les spécifications dont vous avez besoin.

Étape 5 Cliquez sur **OK**.

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Services Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter)** > **Network Services Objects (Objets de services réseau)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un groupe existant et cliquez sur **Edit** (Modifier).

Étape 3 Pour ajouter un objet de service réseau existant au groupe :

a) Sélectionnez **Existing Network-Services Objects** (Objets de services réseau existants).
b) Cliquez sur **Add** (Ajouter) pour ajouter l'objet au groupe. Pour supprimer un objet, sélectionnez-le et cliquez sur **Delete** (Supprimer).
c) Répétez le processus jusqu'à ce que le groupe contienne tous les objets dont vous avez besoin.

Étape 4 Pour définir un ou plusieurs membres directement dans le groupe :

a) Sélectionnez **Create New Network-Services Object Member** (Créer un membre d'objet de services réseau).
b) Sélectionnez l'une des options suivantes, puis complétez les informations d'adresse appropriées :

- **domain** (domaine) : nom du 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** (sous-réseau) : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez l'adresse et le masque réseau, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe, par exemple 2001:DB8:0:CD30::/60. Saisissez les valeurs appropriées dans les champs suivants :

c) Sélectionnez l'une des options suivantes dans Type de service, puis remplissez les champs appropriés :

- **protocol (protocole)** : le protocole utilisé dans la connexion, tel que tcp, udp, ip, etc. Pour rendre l'objet indépendant du service, saisissez simplement **ip**.
- **tcp** ou **udp** : saisissez le numéro de port, 1 à 65 535 ou un mnémonique, tel que www. Pour un port unique, saisissez simplement le numéro de port. Pour plusieurs ports, vous pouvez inclure le nombre après les opérateurs suivants :
  - < signifie tout port inférieur au numéro de ports spécifiés.
  - > désigne tout port supérieur au numéro de ports spécifiés.

- **range** désigne tout port entre les deux ports spécifiés. Le premier numéro de port doit être inférieur au deuxième numéro de port.

d) Cliquez sur **Add** pour ajouter le service réseau au groupe. Pour supprimer un service, sélectionnez-le et cliquez sur **Delete** (Supprimer).
e) Répétez le processus jusqu'à ce que le groupe contienne toutes les spécifications dont vous avez besoin.

Étape 5 Cliquez sur **OK**.

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Local User Groups (Groupes d'utilisateurs locaux)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter un nouvel objet. Saisissez un nom et éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des utilisateurs ou des groupes à l'objet à l'aide de l'une des méthodes suivantes :

- **Sélectionner les utilisateurs ou les groupes existants** : sélectionnez le domaine qui contient l'utilisateur ou le groupe, puis choisissez le nom de l'utilisateur ou du groupe dans les listes et cliquez sur **Add** (Ajouter). Pour les listes longues, utilisez la zone Find (Rechercher) pour aider à localiser l'utilisateur. Les noms sont extraits du serveur pour le domaine sélectionné.

- **Saisir manuellement les noms d'utilisateur** : vous pouvez simplement saisir les noms d'utilisateur ou de groupe dans la zone d'édition du bas et cliquer sur **Add** (Ajouter). Lorsque vous utilisez cette méthode, le nom de domaine sélectionné est ignoré et le domaine par défaut est utilisé si vous n'en spécifiez pas. Pour les utilisateurs, le format est *domain_name**username* ; pour les groupes, une double barre oblique inverse est utilisée : *domain_name**group_name*.

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser ce groupe d'objets utilisateur lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

Configurer les groupes d'objets de groupe 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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Security Group Object Groups (Groupes d'objets de groupe de sécurité)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.

- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des groupes de sécurité à l'objet à l'aide de l'une des méthodes suivantes :

- **Select existing local security group object groups** (Sélectionner des groupes d'objets de groupe de sécurité locaux existants) : choisissez dans la liste des objets déjà définis et cliquez sur **Add** (Ajouter). Pour les listes longues, utilisez la zone Rechercher pour aider à localiser l'objet.
- **Select security groups discovered from ISE** (Sélectionner des groupes de sécurité découverts à partir de l'ISE) : choisissez des groupes dans la liste des groupes existants et cliquez sur **Add** (Ajouter).
- **Manually add security tags or names** (Ajouter manuellement des balises ou des noms de sécurité) : vous pouvez simplement saisir le numéro de balise ou le nom du groupe de sécurité dans la zone de modification du bas et cliquer sur **Add** (Ajouter). 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.

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser ce groupe d'objets de groupe de sécurité lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Time Ranges (Plages de temps)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter une nouvelle plage temporelle. Saisissez un nom et éventuellement, une description.
- Choisissez une plage temporelle existante et cliquez sur **Edit** (Modifier).

Étape 3 Choisissez les heures globales de début et de fin.

La valeur par défaut est de commencer maintenant et de ne jamais terminer, mais vous pouvez définir des dates et des heures spécifiques. La plage temporelle comprend les heures que vous saisissez.

Étape 4 (Facultatif) Configurez les périodes récurrentes dans la durée active globale, telles que les jours de la semaine ou l'intervalle hebdomadaire récurrent pendant lequel la plage temporelle sera active.

a) Cliquez sur **Add** (Ajouter), ou sélectionnez une période existante et cliquez sur **Edit** (Modifier).

b) Effectuez l'une des opérations suivantes :

- Cliquez **sur Specify days of the week and times on which this recurring range will be active** (Préciser les jours de la semaine et les heures auxquelles cette plage récurrente sera active), et choisissez les jours et les heures dans les listes.
- Cliquez sur **Specify a weekly interval when this recurring range will be active** (Préciser un intervalle hebdomadaire pendant lequel cette plage récurrente sera active), et choisissez les jours et les heures dans les listes.

c) Cliquez sur **OK**.

Étape 5 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Objets de surveillance

Pour les objets de réseau, de service et de groupes de sécurité, vous pouvez analyser l'utilisation d'un objet individuel. À partir de leur page dans le dossier **Configuration > Firewall > Objects** (Configuration > Pare-feu > Objets), cliquez sur le bouton **Where Used** (Où utilisé).

Pour les objets réseau, vous pouvez également cliquer sur le bouton Not Used (Non utilisé) pour rechercher les objets qui ne sont utilisés dans aucune règle ni aucun autre objet. Cet affichage vous donne un raccourci pour supprimer ces objets inutilisés.

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.
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**.

Nom de la caractéristique	Observations Versions	Description
Objets	8.3(1)	La prise en charge des objets a été introduite.
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.
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.
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.
Amélioration étendue de l'ACL et des objets pour filtrer le trafic ICMP par code ICMP	9.0(1)	Le trafic ICMP peut maintenant être autorisé ou refusé en fonction du code ICMP. Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Objects (Objets) > Service Objects/Groups (Objets/groupes de service), Configuration (Configuration) > Firewall (Pare-feu) > Access Rule (Règle d'accès)
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 boîtes de dialogue d'ajout/modification des objets et groupes de service sur la page **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Service Objects/Groups (Objets/groupes de service)**.

Nom de la caractéristique	Observations Versions	Description
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 écrans suivants. • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Route Maps (Cartes de routage)**, boîtes de dialogue Add/Edit (Ajouter/modifier). • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, boîtes de dialogue Add/Edit (Ajouter/modifier). • **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Services Objects/Groups (Objets/groupes de services réseau)**. • **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**.
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.