Gestion des objets

Ce chapitre décrit comment gérer les objets réutilisables.

Introduction aux objets

Pour une flexibilité accrue et une interface Web conviviale, le système utilise des *objets* nommés, qui sont des configurations réutilisables qui associent un nom à une valeur. Lorsque vous souhaitez utiliser cette valeur, utilisez plutôt l'objet nommé. Le système prend en charge l'utilisation d'objets à divers endroits dans l'interface Web, y compris de nombreuses politiques et règles, des recherches d'événements, des rapports, des tableaux de bord, etc. Le système fournit de nombreux objets prédéfinis qui représentent les configurations fréquemment utilisées.

Utilisez le gestionnaire d'objets pour créer et gérer des objets. De nombreuses configurations qui utilisent des objets vous permettent également de créer des objets à la volée, selon les besoins. Vous pouvez également utiliser le gestionnaire d'objets pour :

- afficher les politiques, les paramètres et les autres objets où un réseau, un port, un VLAN ou un objet d'URL est utilisé; voir Affichage des objets et de leur utilisation, à la page 8.
- regrouper des objets pour référencer plusieurs objets avec une seule configuration; voir Groupes d'objets, à la page 9.
- remplacer les valeurs d'objet pour les périphériques sélectionnés ou, dans un déploiement multidomaine, les domaines sélectionnés; voir Mises en priorité d'objets, à la page 11.

Après avoir modifié un objet utilisé dans une politique active, vous devez redéployer la configuration modifiée pour que vos modifications prennent effet. Vous ne pouvez pas supprimer un objet utilisé par une politique active.

Remarque Un objet est configuré sur un périphérique géré si, et seulement si, l'objet est utilisé dans une politique qui est affectée à ce périphérique. Si vous supprimez un objet de toutes les politiques affectées à un périphérique donné, l'objet est également supprimé de la configuration du périphérique lors du prochain déploiement, et les modifications ultérieures apportées à l'objet ne sont pas reflétées dans la configuration du périphérique.

Types d'objets

Le tableau suivant répertorie les objets que vous pouvez créer dans le système et indique si chaque type d'objet peut être regroupé ou configuré pour autoriser les remplacements.

Type d'objet	Peut-il être groupé?	Autorise-t-il les remplacements?
Réseau	oui	oui
Port	oui	oui

Type d'objet	Peut-il être groupé?	Autorise-t-il les remplacements?
Interface : • Zone de sécurité • Groupe d'interfaces	Non	Non
Zone de tunnellisation	Non	Non
Filtre d'application	Non	Non
Étiquette VLAN	oui	oui
Attribut externe : balise de groupe de sécurité (SGT) et objet dynamique	Non	Non
URL	oui	oui
Géolocalisation	Non	Non
Plage temporelle	Non	Non
Ensemble de variables	Non	Non
Renseignements sur la sécurité : réseau, DNS et listes et flux d'URL	Non	Non
Gouffre	Non	Non
Liste de fichiers	Non	Non
Liste de suite de chiffrement	Non	Non
Nom distinctif	Oui	Non
Infrastructures à clé publique (PKI) : • Autorité de certification interne et de confiance • Certificats Internes et externes	Oui	Non
Chaîne de clé	Non	oui
Groupe de serveurs DNS	Non	Non
Surveillance SLA	Non	Non
Liste des préfixes : IPv4 et IPv6	Non	oui
Carte de routage	Non	oui
Liste d'accès : standard et étendue	Non	oui
Chemin AS	Non	oui

Type d'objet	Peut-il être groupé?	Autorise-t-il les remplacements?
Liste de communautés	Non	oui
Liste des stratégies	Non	oui
FlexConfig : objets Text et FlexConfig	Non	oui

Objets et multidétention

Dans un déploiement multidomaine, vous pouvez créer des objets dans les domaines globaux et descendants, à l'exception des objets balise de groupe de sécurité (SGT), que vous ne pouvez créer que dans le domaine global. Le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ascendants, que vous ne pouvez pas modifier, à l'exception des zones de sécurité et des groupes d'interface.

Remarque Étant donné que les zones de sécurité et les groupes d'interfaces sont liés à des interfaces de périphérique, que vous configurez au niveau descendant, les administrateurs des domaines descendants peuvent afficher et modifier et les groupes de sécurité créés dans les domaines ascendants. Les utilisateurs de sous-domaine peuvent ajouter et supprimer des interfaces des zones et des groupes ascendants, mais ne peuvent pas supprimer ou renommer les zones ou les groupes.

Les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Pour les objets qui prennent en charge le regroupement, vous pouvez regrouper des objets du domaine actuel avec des objets hérités des domaines ascendants.

Les remplacements d'objets vous permettent de définir des valeurs propres au périphérique ou au domaine pour certains types d'objets, notamment le réseau, le port, la balise VLAN et l'URL. Dans un déploiement multidomaine, vous pouvez définir une valeur par défaut pour un objet dans un domaine parent et permettre aux administrateurs des domaines dépendants d'ajouter des valeurs de remplacement pour cet objet.

Le gestionnaire d'objets

Vous pouvez utiliser le gestionnaire d'objets pour créer et gérer des objets et des groupes d'objets.

Le gestionnaire d'objets affiche 20 objets ou groupes par page. Si vous avez plus de 20 objets ou groupes de n'importe quel type, utilisez les liens de navigation au bas de la page pour afficher des pages supplémentaires.

Vous pouvez également accéder à une page en particulier ou cliquer sur **Actualisation** ( ) pour actualiser l'affichage.

Accédez à la page en utilisant **Objects (objets)** > **Object Management (gestion des objets)**. Vous pouvez également accéder à la page à l'aide de **Objets** > **Autres objets FTD**.

Par défaut, la page répertorie les objets et les groupes par ordre alphabétique de nom. Vous pouvez filtrer les objets de la page par nom ou valeur.

Importation d'objets en cours

Les objets peuvent être importés à partir d'un fichier de valeurs séparées par des virgules. Jusqu'à 1 000 objets peuvent être importés en une seule tentative. Le contenu du fichier des valeurs séparées par des virgules doit suivre un format précis. Le format est différent pour chaque type d'objet. Seuls quelques types d'objets peuvent être importés. Consultez le tableau suivant pour connaître les types d'objets pris en charge et les règles correspondantes.

Type d'objet	Règles
Objet individuel	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DN • Les entrées des colonnes NAME (Nom) et DN (nom distinctif) sont obligatoires pour importer une entrée. • Vous pouvez importer des objets individuels directement dans un groupe d'objets de nom unique existant.
Objet réseau	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DESCRIPTION • TYPE • VALEUR • RECHERCHE • Les entrées des colonnes NAME (NOM) et VALUE (VALEUR) sont obligatoires pour importer une entrée de type d'hôte, de plage ou d'objet réseau. • Pour un objet de nom de domaine complet (FQDN), l'entrée de colonne TYPE doit mentionner « fqdn » et l'entrée de colonne LOOKUP (RECHERCHE) doit être définie comme « ipv4 », « ipv6 » ou « ipv4_ipv6 ». • Si aucun contenu n'est fourni dans l'entrée de la colonne LOOKUP pour l'objet FQDN, l'objet est enregistré avec la valeur de champ ipv4_ipv6.

Type d'objet	Règles
Port	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • PROTOCOLE • PORT • ICMPCODE • ICMPTYPE • L'entrée de la colonne NAME est obligatoire. • Pour les types de protocoles « tcp » et « udp », l'entrée dans la colonne PORT est obligatoire. • Pour les types de protocoles « icmp » et « icmp6 », les entrées de colonne ICMPCODE et ICMPTYPE sont obligatoires.
URL	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DESCRIPTION • URL • Les entrées des colonnes NAME et URL sont obligatoires pour importer une entrée.
Étiquette VLAN	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DESCRIPTION • TAG (BALISE) • Les entrées des colonnes NAME et TAG sont obligatoires pour importer une entrée.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez un des types d'objet suivants dans le volet gauche :

- **Distinguished Name (Nom distinctif)** > **Individual Objects (Objets individuels)** >
- **Objet réseau**
- **Port**
- **URL**
- **Étiquette VLAN**

Étape 3 Choisissez **Import Object** (importation d'objets) dans la liste déroulante **Add [Object Type]** (Ajouter un type d'objet).

Remarque Si vous avez sélectionné des **objets individuels** à l'étape précédente, cliquez sur **Importer**.

Étape 4 Cliquez sur **Parcourir**.

Étape 5 Localisez et sélectionnez le fichier séparé par des virgules sur votre système.

Étape 6 Cliquez sur **Ouvrir**

Remarque Lors de l'importation d'objets **Distinguished Name**, vous pouvez éventuellement cocher la case **Add imported Distinguished Name objects to the below object group** (Ajouter les objets de Nom distinctif importés au groupe d'objets ci-dessous) et sélectionner le nom du groupe dans la liste déroulante pour importer les objets directement dans un groupe d'objets de nom distinctif existant.

Étape 7 Cliquez sur **Import (Importer)**.

Modification d'objets

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Consultez les mises en garde relatives aux objets et aux groupes de réseau à l'adresse Réseau, à la page 48.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez un type d'objet dans la liste; voir Introduction aux objets, à la page 2.

Étape 3 Cliquez sur **Edit** (✎) à côté de l'objet que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, l'objet appartient à un domaine ancêtre ou encore, a été configuré pour ne pas autoriser les remplacements, ou encore vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Modifiez les paramètres de l'objet comme vous le souhaitez.

Étape 5 Si vous modifiez un ensemble de variables, gérez les variables de l'ensemble; voir Gestion des variables, à la page 113.

Étape 6 Pour les objets qui peuvent être configurés pour autoriser les remplacements :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13. Vous pouvez modifier ce paramètre uniquement pour les objets appartenant au domaine actuel.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 13.

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Si vous modifiez un ensemble de variables et que cet ensemble est utilisé par une politique de contrôle d'accès, cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez enregistrer vos modifications.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Affichage des objets et de leur utilisation

Vous pouvez afficher les détails d'utilisation des objets dans la page Object Management (gestion des objets). Centre de gestion fournit cette fonctionnalité pour de nombreux types d'objet. Cependant, certains types d'objets ne sont pas pris en charge.

Remarque Dans un déploiement multidomaine, vous pouvez afficher les objets de tout autre domaine. Pour afficher et modifier l'utilisation des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez un des types d'objets pris en charge suivants :

- Liste d'accès > Étendue
- Liste d'accès > Standard
- Chemin AS
- Liste de communautés
- Interface
- Réseau
- Liste des stratégies
- Port
- Liste des préfixes > Liste des préfixes IPv4
- Liste des préfixes > Liste des préfixes IPv6
- Carte de routage

- Surveillance SLA
- URL
- Étiquette VLAN

Étape 3 Cliquez sur l'icône **Rechercher une utilisation** ( ) à côté de l'objet.

La fenêtre Object Usage (utilisation des objets) affiche une liste de toutes les politiques, objets et autres paramètres dans lesquels l'objet est utilisé. Cliquez sur l'un des éléments répertoriés pour en savoir plus sur l'utilisation de l'objet. Pour les politiques et certains autres paramètres où l'objet est utilisé, vous pouvez cliquer sur les liens correspondants pour visiter les pages d'interface utilisateur respectives.

Filtrage des objets ou des groupes d'objets

Dans un déploiement multidomaine, le système affiche les objets créés dans les domaines actuel et ascendant, que vous pouvez modifier.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Saisissez vos critères de filtre dans le champ **Filter** (filtre).

La page se met à jour au fur et à mesure que vous saisissez pour afficher les éléments correspondants.

Vous pouvez utiliser les caractères génériques suivants :

- L'astérisque (*) correspond à zéro ou à plusieurs occurrences d'un caractère.
- Le signe d'insertion (^) correspond au contenu au début d'une chaîne.
- Le signe du dollar ($) correspond au contenu à la fin d'une chaîne.

Étape 3 Cochez la case **Show Unused Object** (Afficher les objets inutilisés) pour afficher les objets et les groupes d'objets qui sont inutilisés partout dans le système.

Remarque
- Si un objet fait partie d'un groupe d'objets inutilisés, l'objet est considéré comme utilisé. Cependant, le groupe d'objets inutilisés s'affiche lorsque la case **Show Unified Object** (Afficher les objets inutilisés) est cochée.
- La case à cocher **Afficher l'objet inutilisé** n'est disponible que pour les types d'objets réseau, port, URL et balise VLAN.

Groupes d'objets

Le regroupement d'objets vous permet de référencer plusieurs objets avec une seule configuration. Le système vous permet d'utiliser des objets et des groupes d'objets de manière interchangeable dans l'interface Web.

Par exemple, partout où vous utilisez un objet de port, vous pouvez également utiliser un groupe d'objets de port.

Vous pouvez regrouper des objets de réseau, de port, de balise VLAN, d'URL et de PKI. Les groupes d'objets réseau peuvent être imbriqués, c'est-à-dire que vous pouvez ajouter un groupe d'objets réseau à un autre groupe d'objets réseau sur 10 niveaux maximum.

Les objets et les groupes d'objets du même type ne peuvent pas avoir le même nom. Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Notez que le système peut identifier un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Lorsque vous modifiez un groupe d'objets utilisé dans une politique (par exemple, un groupe d'objets réseau utilisé dans une politique de contrôle d'accès), vous devez redéployer la configuration modifiée pour que vos modifications prennent effet.

La suppression d'un groupe ne supprime pas ses objets, mais uniquement leur association les uns avec les autres. En outre, vous ne pouvez pas supprimer un groupe utilisé dans une politique active. Par exemple, vous ne pouvez pas supprimer un groupe de balises VLAN que vous utilisez dans une condition VLAN dans une politique de contrôle d'accès enregistrée.

Regroupement d'objets réutilisables

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Vous pouvez regrouper des objets dans le domaine actuel avec des objets hérités des domaines ascendants.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Si le type d'objet que vous souhaitez regrouper est **Réseau**, **Port**, **URL**ou **Balise VLAN**:

a) Sélectionnez le type d'objet dans la liste des types d'objets.
b) Choisissez **Add Group** (ajouter un groupe) dans la liste déroulante **Add Object Type** (Ajouter un type d'objet).

Étape 3 Si le type d'objet que vous souhaitez regrouper est **Nom distinctif** :

a) Développez le nœud **Distinguished Name** (nom distinctif).
b) Choisissez **Object Groups** (groupes d'objets).
c) Cliquez sur **Add Distinguished Name Group** (Ajouter un groupe de noms distinctifs).

Étape 4 Si le type d'objet que vous souhaitez regrouper est **PKI**:

a) Développez le nœud **PKI** .
b) Effectuez l'une des opérations suivantes :

- **Groupes d'autorités de certification internes**
- **Groupes d'autorités de certification approuvées**
- **Groupes de certificats internes**
- **Groupes de certificats externes**

c) Cliquez sur **Add [Object Type] group** Ajouter un groupe [Type d'objet]).

Étape 5 Saisissez un **nom** unique.

Étape 6 Choisissez un ou plusieurs objets dans la liste et cliquez sur **Ajouter**.

Vous pouvez aussi :

- Utilisez le champ de filtre **Recherche** ( ) pour rechercher des objets existants à inclure. Ce champ se met à jour à mesure que vous saisissez pour afficher les éléments correspondants. Cliquez sur **Recharger** ( ) au-dessus du champ de recherche ou cliquez sur **Effacer** ( ) dans le champ de recherche pour effacer la chaîne de recherche.
- Cliquez sur **Ajouter** ( ) pour créer des objets à la volée si aucun objet existant ne répond à vos besoins.

Étape 7 Facultatif pour **le réseau**, le **port**, l'**URL**et les groupes de **balises VLAN** :

- Saisissez une **description**.
- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployez les modifications de configuration; voir Déployer les modifications de configuration.

Mises en priorité d'objets

Un remplacement d'objet vous permet de définir une valeur alternative pour un objet, que le système utilise pour les périphériques que vous spécifiez.

Vous pouvez créer un objet dont la définition convient à la plupart des périphériques, puis utiliser les dérogations pour spécifier les modifications à apporter à l'objet pour les quelques périphériques qui ont besoin de définitions différentes. Vous pouvez également créer un objet qui doit être remplacé pour tous les périphériques, mais son utilisation vous permet de créer une politique unique pour tous les périphériques. Les remplacements d'objets vous permettent de créer un ensemble plus restreint de stratégies partagées à utiliser sur l'ensemble des périphériques, sans renoncer à la possibilité de modifier les stratégies en cas de besoin pour les périphériques individuels.

Par exemple, vous pourriez vouloir refuser le trafic ICMP aux différents services de votre entreprise, chacun d'entre eux étant connecté à un réseau différent. Vous pouvez le faire au moyen d'une stratégie de contrôle d'accès avec une règle qui inclut un objet réseau appelé Réseau départemental. En autorisant les dérogations pour cet objet, vous pouvez ensuite créer des dérogations pour chaque périphérique concerné qui spécifie le réseau réel auquel ce périphérique est connecté.

Dans un déploiement multidomaine, vous pouvez définir une valeur par défaut pour un objet dans un domaine parent et permettre aux administrateurs des domaines dépendants d'ajouter des valeurs de remplacement pour cet objet. Par exemple, un fournisseur de services de sécurité gérés (MSSP) peut utiliser un seul centre de gestion pour gérer la sécurité du réseau de plusieurs clients. Les administrateurs du MSSP peuvent définir un objet dans le domaine Global pour l'utiliser dans les déploiements de tous les clients. Les administrateurs de

chaque client peuvent se connecter aux domaines descendants pour remplacer cet objet pour leur organisation. Ces administrateurs locaux ne peuvent pas voir ou affecter les valeurs prioritaires d'autres clients du MSSP.

Vous pouvez cibler un remplacement d'objet sur un domaine spécifique. Dans ce cas, le système utilise la valeur de dérogation d'objet pour tous les périphériques du domaine ciblé, à moins que vous ne la modifiiez au niveau du périphérique.

Dans le gestionnaire d'objets, vous pouvez sélectionner un objet qui peut être remplacé et définir une liste de remplacements au niveau de l'appareil ou du domaine pour cet objet.

Vous ne pouvez utiliser les remplacements d'objets qu'avec les types d'objets suivants :

- Réseau
- Port
- Balise du réseau VLAN
- URL
- Surveillance SLA
- Liste des préfixes
- Carte de routage
- Liste d'accès
- Chemin AS
- Liste de communautés
- Liste des stratégies
- Enregistrement de certificats (ICP)
- Chaîne de clé

Si vous pouvez remplacer un objet, la colonne **Dérogation** apparaît pour le type d'objet dans le gestionnaire d'objets. Les valeurs possibles pour cette colonne sont les suivantes :

- Coche verte - indique que vous pouvez créer des dérogations pour l'objet et qu'aucune dérogations n'a encore été ajoutée.
- X rouge - indique qu'il n'est pas possible de créer des dérogations pour l'objet.
- Nombre - représente le nombre de dérogations qui ont été ajoutées à cet objet (par exemple, "2" indique que deux dérogations ont été ajoutées).

Gestion des mises en priorité d'objets

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez dans la liste des types d'objets; voir Introduction aux objets, à la page 2.

Étape 3 Cliquez sur **Edit** (✎) à côté de l'objet que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, l'objet appartient à un domaine ancêtre ou encore, a été configuré pour ne pas autoriser les remplacements, ou encore vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Gérer les remplacements d'objets :

- Ajouter : ajouter des remplacements d'objets; voir Ajout de mises en priorité d'objets, à la page 13.
- Autoriser : autorisez les remplacements d'objets; voir Autoriser les mises en priorité d'objets, à la page 13.
- Supprimer : dans l'éditeur d'objets, cliquez sur **Supprimer** ( ) à côté du remplacement que vous souhaitez supprimer.
- Modifier : modifier les remplacements d'objets; voir Modification des mises en priorité d'objets, à la page 14.

Autoriser les mises en priorité d'objets

Procédure

Étape 1 Dans l'éditeur d'objets, cochez la case **Allow Overrides** (autoriser les remplacements).

Étape 2 Cliquez sur **Save** (enregistrer).

Prochaine étape

Ajouter des valeurs de mise en priorité d'objet; voyez Ajout de mises en priorité d'objets, à la page 13.

Ajout de mises en priorité d'objets

Pour les mises en garde relatives à l'utilisation d'objets ou de groupes de réseaux, voir Réseau, à la page 48.

Avant de commencer

Autorisez les mises en priorité d'objets, voir Autoriser les mises en priorité d'objets, à la page 13.

Procédure

Étape 1 Dans l'éditeur d'objets, développez la section **Override** (remplacer).

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Dans **Targets** (objectifs), choisissez les domaines ou appareils dans la liste **Available Devices and Domains** (appareils et domaines disponibles), puis cliquez sur **Add** (ajouter).

Étape 4 Dans l'onglet Remplacer, entrez un **Nom**.

Étape 5 Vous pouvez également saisir une **Description**.

Étape 6 Entrez une valeur de remplacement.

Exemple :

Pour un objet réseau, entrez une valeur réseau.

Étape 7 Cliquez sur **Add** (ajouter).

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Modification des mises en priorité d'objets

Vous pouvez modifier la description et la valeur d'un remplacement existant, mais vous ne pouvez pas modifier la liste cible existante. Au lieu de cela, vous devez ajouter un nouveau remplacement avec de nouvelles cibles, qui remplace le remplacement existant.

Pour les mises en garde relatives à l'utilisation d'objets ou de groupes de réseaux, voir Réseau, à la page 48.

Procédure

Étape 1 Dans l'éditeur d'objets, développez la section **Override** (remplacer).

Étape 2 Cliquez sur **Edit** ( ) à côté du remplacement que vous souhaitez modifier.

Étape 3 Il est également possible de modifier la **Description**.

Étape 4 Modifiez la valeur de remplacement.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer le remplacement.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer l'objet.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

serveur AAA

Ajouter des objets serveur AAA réutilisables.

Ajouter un groupe de serveurs RADIUS

Les objets de groupe de serveur RADIUS contiennent une ou plusieurs références aux serveurs RADIUS. Ces serveurs sont utilisés pour authentifier les utilisateurs qui se connectent par VPN d'accès à distance.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Avant de commencer

Remarque Vous ne pouvez pas remplacer les objets de groupe de serveurs RADIUS.

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** (Objets < Gestion des objets > Serveur AAA > Groupe de serveurs RADIUS).

Tous les objets du groupe de serveurs RADIUS actuellement configurés seront répertoriés. Utilisez le filtre pour affiner la liste.

Étape 2 Choisissez et modifiez un objet de groupe de serveurs RADIUS répertorié, ou ajoutez-en un nouveau.

Consultez Options de serveurs RADIUS, à la page 16 et Options de groupe de serveurs RADIUS, à la page 15 pour configurer cet objet.

Étape 3 Cliquez sur **Save** (Enregistrer).

Options de groupe de serveurs RADIUS

Chemin de navigation

Objets > **Gestion des objets** > **Serveur AAA** > **Groupe de serveurs RADIUS**. Choisissez et modifiez un objet de groupe de serveurs RADIUS configuré ou ajoutez-en un nouveau.

Champs

- **Name** and **Description**(nom et description) : saisissez un nom et éventuellement une description pour identifier cet objet de groupe de serveurs RADIUS.
- **Group Accountant Mode** (mode de comptabilité de groupe) : la méthode d'envoi de messages de comptabilité aux serveurs RADIUS du groupe. Choisissez **Single**(unique), les messages de gestion comptable sont envoyés à un seul serveur du groupe; il s'agit de la valeur par défaut. Ou, **Multiple**, les messages de gestion de comptes sont envoyés à tous les serveurs du groupe simultanément.
- **Retry Interval** (Intervalle entre les tentatives) : l'intervalle entre les tentatives de connexion aux serveurs RADIUS. Les valeurs sont comprises entre 1 et 10 secondes.
- **Realms** (Domaines)(facultatif) : précisez ou sélectionnez le domaine Active Directory (AD) auquel ce groupe de serveurs RADIUS est associé. Ce domaine est ensuite sélectionné dans les politiques d'identité pour accéder au groupe de serveurs RADIUS associé lors de la détermination de la source d'identité d'authentification VPN pour un flux de trafic. Ce domaine fournit efficacement un pont entre la politique d'identité et ce groupe de serveurs Radius. Si aucun domaine n'est associé à ce groupe de serveurs RADIUS, le groupe de serveurs RADIUS ne peut pas être atteint pour déterminer la source d'identité de l'authentification VPN pour un flux de trafic dans une politique d'identité.

Remarque Ce champ est obligatoire si vous utilisez le VPN d'accès à distance avec l'identité de l'utilisateur et RADIUS comme source d'identité.

- **Enable allow only** (activer autoriser seulement) : Si ce groupe de serveurs RADIUS n'est pas utilisé à des fins d'authentification, mais qu'il est utilisé à des fins d'autorisation ou de gestion de comptes, cochez ce champ pour activer le mode d'autorisation seulement pour le groupe de serveurs RADIUS.

  Le mode d'autorisation seulement élimine le besoin d'inclure le mot de passe du serveur RADIUS dans la demande d'accès. Ainsi, le mot de passe, configuré pour les serveurs RADIUS individuels, est ignoré.

- **Enable interim account update** (Activer la mise à jour intermédiaire des comptes) et **interval** (intervalle) : active la génération de messages provisoires-accounting-update RADIUS afin d'informer le serveur RADIUS des nouvelles adresses IP attribuées. Définissez la durée, en heures, de l'intervalle entre les mises à jour périodiques de la comptabilité dans le champ Intervalle. La plage valide est de 1 à 120 et la valeur par défaut est 24.

- **Enable Dynamic Authorization** and **Port** (activer l'autorisation et le port dynamiques) : active les services d'autorisation dynamique ou de changement d'autorisation (CoA) RADIUS pour ce groupe de serveurs RADIUS. Précisez le port d'écoute pour les demandes RADIUS CoA dans le champ **Port**. La plage valide est de 1 024 à 65 535 et la valeur par défaut est de 1 700. Une fois défini, le groupe de serveurs RADIUS correspondant est enregistré pour la notification CoA et écoute le port pour recevoir les mises à jour de la politique CoA à partir de Cisco Identity Services Engine (ISE).

- **Serveurs RADIUS** : consultez Options de serveurs RADIUS, à la page 16.

Sujets connexes

Ajouter un groupe de serveurs RADIUS, à la page 14

Options de serveurs RADIUS

Chemin de navigation

Objects > **Object Management** > **AAA Server** > **RADIUS Server Group** (Objets < Gestion des objets > Serveur AAA > Groupe de serveurs RADIUS). Choisissez et modifiez un objet de groupe de serveurs RADIUS répertorié ou ajoutez-en un nouveau. Ensuite, dans la boîte de dialogue RADIUS Server Group, choisissez et modifiez un serveur RADIUS répertorié ou ajoutez-en un nouveau.

Champs

- **IP Address/Hostname** (adresse IP/nom d'hôte) : l'objet réseau qui identifie le nom d'hôte ou l'adresse IP du serveur RADIUS auquel les demandes d'authentification seront envoyées. Vous ne pouvez sélectionner qu'un seul serveur pour ajouter des serveurs, ajoutez un serveur RADIUS supplémentaire à la liste du groupe de serveurs RADIUS.

Remarque Le périphérique prend désormais en charge les adresses IP IPv6 pour l'authentification RADIUS.

- **Authentication Port** (Port d'authentification) : le port sur lequel l'authentification et l'autorisation RADIUS sont effectuées. Par défaut, c'est 1812 .
- **Key** and **Confirm Key** (Clé et Confirmer la clé) : Le code secret partagé qui est utilisé pour chiffrer les données entre le périphérique géré (client) et le serveur RADIUS.

  La clé est une chaîne alphanumérique sensible à la casse comptant jusqu'à 127 caractères. Les caractères spéciaux sont autorisés.

  La clé que vous définissez dans ce champ doit correspondre à la clé du serveur RADIUS. Saisissez à nouveau la clé dans le champ Confirm (Confirmer).
- **Port de comptabilité** : le port sur lequel la gestion de comptes RADIUS est effectuée. Par défaut, c'est 1813.
- **Timeout**(délai d'expiration) : délai d'expiration de session pour l'authentification.

Remarque La valeur du délai d'expiration doit être de 60 secondes ou plus pour l'authentification à deux facteurs RADIUS. La valeur de délai d'expiration par défaut est de 10 secondes.

- **Connect Using** : Établit la connectivité du périphérique à un serveur RADIUS à l'aide d'une recherche de routage ou d'une interface spécifique.
  - Cliquez sur le bouton radio **Routing** (routage) pour utiliser la table de routage des .
  - Cliquer sur le bouton radio **Interface spécifique** et choisir une zone ou un groupe d'interfaces de sécurité ou l'interface Diagnostic (l'interface par défaut) dans la liste déroulante. .
- **Redirection ACL** : sélectionnez la liste de contrôle d'accès de redirection dans la liste ou ajoutez-en une nouvelle.

Remarque Il s'agit du nom de la liste de contrôle d'accès définie dans le périphérique pour décider du trafic à rediriger. Le nom de la liste de contrôle d'accès de redirection doit être identique au nom de la liste de contrôle d'accès de *redirection* dans le serveur ISE. Lorsque vous configurez l'objet ACL, veillez à sélectionner l'action Block (Bloquer l'action pour les serveurs ISE et DNS) et l'action Allow (autoriser) pour le reste des serveurs.

Sujets connexes

Ajouter un groupe de serveurs RADIUS, à la page 14
Options de groupe de serveurs RADIUS, à la page 15

Ajouter un serveur de connexion unique (SSO)

Avant de commencer

Obtenez les éléments suivants auprès de votre fournisseur d'identité SAML :

- URL de l'identifiant d'entité du fournisseur d'identité (IDP)
- URL de connexion
- URL de déconnexion
- Le certificat du fournisseur d'identité et l'inscription du certificat dans défense contre les menaces utilisant l'interface Web centre de gestion (**Périphériques** > **Certificats**)

Pour en savoir plus, consultez Configuration de l'authentification de la connexion unique SAML.

Procédure

Étape 1 Choisissez **Object** > **Object Management** > **AAA Server** > **Single Sign-on Server** (Objets > Gestion des objets > Serveur AAA > Serveur de connexion unique).

Étape 2 Cliquez sur **Add Single Sign-on Server** (ajouter un serveur de connexion unique) et fournissez les détails suivants :

- **Name** : nom de l'objet serveur de connexion unique SAML.
- **ID d'entité du fournisseur d'identité** : l'URL qui est définie dans le fournisseur d'identité de SAML pour identifier un fournisseur de services de manière unique.

  Il s'agit de l'URL d'une page qui sert le XML de métadonnées qui décrit comment l'émetteur SAML répondra aux demandes.
- **URL SSO** : L'URL pour la connexion au serveur du fournisseur d'identité SAML.
- **URL de déconnexion** : L'URL pour la déconnexion du serveur du fournisseur d'identité SAML.
- **URL de base** : URL qui redirige l'utilisateur vers défense contre les menaces une fois l'authentification du fournisseur d'identité terminée. Il s'agit de l'URL de l'interface d'accès configurée pour le VPN d'accès à distance défense contre les menaces .
- **Certificat du fournisseur d'identité** : certificat du fournisseur d'identité inscrit dans défense contre les menaces pour vérifier les messages signés par le fournisseur d'identité.

  Sélectionnez un certificat de fournisseur d'identification dans la liste ou cliquez sur Add (Ajouter) pour créer un nouvel objet d'inscription de certificat.

  Pour en savoir plus, consultez Gestion des certificats Défense contre les menaces.

  Vous devez inscrire tous les certificats d'autorité de certification d'applications Microsoft Azure enregistrés en tant que points de confiance sur le défense contre les menaces . Le fournisseur d'identité Microsoft Azure SAML est configuré sur défense contre les menaces pour l'application initiale. Tous les profils de connexion sont mappés au fournisseur d'identité SAML MS Azure configuré. Pour chacune des applications MS Azure (hormis l'application par défaut), vous pouvez choisir le point de confiance requis (certificat d'autorité de certification) dans la configuration du profil de connexion du VPN d'accès à distance.

  Pour de plus amples renseignements, consultez la section Configurer les paramètres AAA pour le VPN d'accès à distance.
- **Certificat de fournisseur de services** : certificat défense contre les menaces qui sera utilisé pour signer les demandes et établir un cercle de confiance avec le fournisseur d'identité.

Si vous n'avez pas inscrit de certificats défense contre les menaces internes, cliquez sur le signe plus (**+)** pour ajouter et inscrire un certificat. Pour en savoir plus, consultez Gestion des certificats Défense contre les menaces.

- **Demander une signature** : sélectionnez l'algorithme de chiffrement pour signer les demandes de connexion unique SAML.

  Les signatures sont classées de la plus faible à la plus forte : SHA1, SHA256, SHA384, SHA512. Sélectionnez Aucun pour désactiver le chiffrement.

- **Délai d'expiration de la demande** : spécifiez la durée de validité de l'assertion SAML pendant laquelle les utilisateurs doivent terminer la demande d'authentification unique. Le fournisseur d'identité de SAML a deux délais d'expiration : *NotBefore* et *NotOnOrAfter*. Le défense contre les menaces valide si son heure actuelle se trouve dans la plage temporelle de (limite inférieure) *NotBefore* et (limite supérieure) la plus faible parmi *NotBefore* plus *timeout* et *NotOnOrAfter*. Ainsi, si vous définissez un délai plus long que le délai *NotOnOrAfter* du fournisseur d'identité, le délai spécifié est ignoré et le délai *NotOnOrAfter* est sélectionné. Si la somme du délai d'expiration spécifié et du délai d'expiration *NotBefore* est inférieure au délai *NotOnOrAfter*, le délai défense contre les menaces remplace le délai d'expiration.

  La plage est comprise entre 1 et 7 200 secondes, et la valeur par défaut est de 300 secondes.

- **Activer le fournisseur d'identité uniquement accessible sur le réseau interne** : sélectionnez cette option si le fournisseur d'identité de SAML réside sur le réseau interne. Défense contre les menaces agit comme une passerelle et établit la communication entre les utilisateurs et le fournisseur d'identité à l'aide d'une session Webvpn anonyme.

- **Demande de re-authentification à la connexion** : sélectionnez cette option pour authentifier l'utilisateur à chaque connexion, même si la session précédente du fournisseur d'identité est valide.

- **Autoriser les remplacements** : cochez cette case pour autoriser les remplacements pour cet objet de serveur d'authentification unique.

Étape 3 Cliquez sur **Save** (enregistrer).

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance

Liste d'accès

Un objet de liste d'accès, également appelé liste de contrôle d'accès (ACL ou access control list), sélectionne le trafic auquel un service s'appliquera. Vous utilisez ces objets lors de la configuration de fonctionnalités particulières, telles que pour les cartes de routage des périphériques défense contre les menaces . Le trafic identifié comme autorisé par la liste de contrôle d'accès (ACL) reçoit le service, tandis que le trafic « bloqué » est exclu du service. L'exclusion du trafic d'un service ne signifie pas nécessairement son abandon.

Vous pouvez configurer les types d'ACL suivants :

- Étendu : identifie le trafic en fonction de l'adresse et des ports source et destination. Prend en charge les adresses IPv4 et IPv6, que vous pouvez combiner dans une règle donnée.
- Standard : le trafic est identifié en fonction de l'adresse de destination uniquement. Seulement IPv4 est pris en charge.

Une ACL est composée d'une ou de plusieurs entrées de contrôle d'accès (ACE), ou règles. L'ordre des ACE est important. Lors de l'évaluation de la liste de contrôle d'accès pour déterminer si un paquet correspond à une entrée ACE « autorisée », le paquet est testé 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. Par exemple, si vous souhaitez « autoriser » 10.100.10.1, mais « bloquer » le reste de 10.100.10.0/24, l'entrée allow (autoriser) doit précéder l'entrée Block (blocage). En général, placez des règles plus spécifiques en haut d'une liste de contrôle d'accès.

Les paquets qui ne correspondent pas à une entrée « autorisée » sont considérés comme bloqués.

Les rubriques suivantes expliquent comment configurer les objets ACL.

Configurer les objets ACL étendus

Utilisez des objets ACL étendus lorsque vous souhaitez faire correspondre le trafic en fonction des adresses de source et de destination, du protocole et du port, du groupe d'applications ou s'il s'agit du trafic IPv6.

Procédure

Étape 1 Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)**, puis **Liste d'accès** > **Étendue** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue) pour créer un nouvel objet.
- Cliquez sur **Edit** (✎) pour modifier un objet existant.

Étape 3 Dans la boîte de dialogue New Extended Access List Object (nouvel objet de liste d'accès étendu), saisissez un nom pour l'objet (sans espaces) et configurez les entrées de contrôle d'accès :

a) Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée.
- Cliquez sur **Edit** (✎) pour modifier une entrée existante.

b) Sélectionnez l'**action**, autoriser (correspondance) ou bloquer (non correspondance) aux critères de trafic.

Remarque Les options **Logging**, **Log Level** et **Log Interval** (Journalisation, niveau de journalisation, intervalle de journalisation) sont utilisées pour les règles d'accès uniquement (ACL connectées aux interfaces ou appliquées globalement). Comme les objets ACL ne sont pas utilisés pour les règles d'accès, conservez leurs valeurs par défaut.

c) Configurez les adresses de source et de destination dans l'onglet **Network (Réseau)** en utilisant l'une des techniques suivantes :

- Sélectionnez les objets réseau ou les groupes de votre choix dans la liste des éléments disponibles et cliquez sur **Ajouter à la source** ou **sur Ajouter à la destination**. Vous pouvez créer de nouveaux objets en cliquant sur le bouton + au-dessus de la liste. Vous pouvez combiner des adresses IPv4 et IPv6.
- Tapez une adresse dans la zone d'édition sous la liste de source ou de destination et cliquez sur **Add** (Ajouter). Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou

2001:DB8::0DB8:800:200C:417A), ou un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0 255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::60).

d) Cliquez sur l'onglet **Port** et configurez le service en utilisant l'une des techniques suivantes.

- Sélectionnez les objets de port souhaités dans la liste des objets disponibles et cliquez sur **Add to Source** (Ajouter à la source) ou **Add to Destination** (Ajouter à la destination). Vous pouvez créer de nouveaux objets en cliquant sur le bouton **+** au-dessus de la liste. L'objet peut préciser les ports TCP/UDP, les types de messages ICMP/ICMPv6 ou d'autres protocoles (y compris « any ») (tout). Cependant, le port source, que vous laisseriez généralement vide, accepte uniquement les protocoles TCP/UDP. Vous ne pouvez pas sélectionner de groupes de ports.

  Pour TCP/UDP, notez que vous devez utiliser le même protocole dans les champs source et destination, si vous spécifiez les deux. Par exemple, vous ne pouvez pas préciser un port source UDP et un port de destination TCP.

- Saisissez ou sélectionnez un port ou un protocole dans la zone de modification sous la liste de source ou de destination et cliquez sur **Add** (Ajouter).

Remarque Pour obtenir une entrée qui s'applique à tout le trafic IP, sélectionnez un objet de port de destination qui précise « tous » les protocoles.

e) Cliquez sur l'onglet **Application** et choisissez les applications à regrouper pour la politique d'accès Internet direct.

Important
- Vous ne pouvez pas configurer d'applications pour les périphériques de la grappe. Par conséquent, cet onglet ne s'applique pas aux périphériques de la grappe.
- Utilisez la liste de contrôle d'accès étendue avec les applications uniquement dans le routage basé sur les politiques. Ne l'utilisez pas dans d'autres politiques, car son comportement est inconnu et non pris en charge.

Remarque
- La liste des **applications disponibles** affiche un ensemble fixe d'applications prédéfinies. Cette liste est un sous-ensemble des applications qui sont disponibles dans la politique de contrôle d'accès, car elles seules peuvent être détectées par leur premier paquet (points terminaux de nom de domaine complet résolus en adresses IP et en ports). Les définitions d'application sont mises à jour par le biais des mises à jour de la VDB et sont poussées vers défense contre les menaces lors des déploiements suivants.
- Les applications ou groupes d'applications personnalisés définis par l'utilisateur ne sont pas pris en charge.
- Actuellement, centre de gestion ne prend pas en charge les applications ou les groupes d'applications personnalisés définis par l'utilisateur et ne vous permet pas de modifier la liste des applications prédéfinies.
- Vous pouvez utiliser les options de filtre fournies sous les **filtres d'application** pour affiner cette liste.

f) Sélectionnez l'application requise et cliquez sur **Add to Rule** (Ajouter à la règle).

Remarque
- Ne configurez pas les réseaux de destination et les applications dans l'objet ACL étendu.
- Les applications sélectionnées (objets de service réseau) dans chacune des entrées de contrôle d'accès forment un groupe de services réseau (NSG). Ce groupe est déployé sur défense contre les menaces . Le NSG est utilisé dans l'accès Internet direct pour classer le trafic en fonction de la correspondance avec le groupe d'applications sélectionné.

g) Cliquez sur **Add** (ajouter) pour ajouter l'entrée à l'objet.
h) Si nécessaire, cliquez sur l'entrée et faites-la glisser pour la déplacer vers le haut ou le bas dans l'ordre des règles jusqu'à l'emplacement souhaité.

Répétez le processus pour créer ou modifier des entrées supplémentaires dans l'objet.

Étape 4 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 5 Cliquez sur **Save** (enregistrer).

Configurer les objets ACL standard

Utilisez les objets ACL standard lorsque vous souhaitez mettre en correspondance le trafic en fonction de l'adresse IPv4 de destination uniquement. Sinon, utilisez des listes de contrôle d'accès étendues.

Procédure

Étape 1 Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)**, puis **Liste d'accès** > **Standard** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :
- Cliquez sur **Add Standard Access List** (Ajouter une liste d'accès standard) pour créer un nouvel objet.
- Cliquez sur **Edit** (✎) pour modifier un objet existant.

Étape 3 Dans la boîte de dialogue Nouvel objet de liste d'accès standard, saisissez un nom pour l'objet (sans espaces) et configurez les entrées de contrôle d'accès :

a) Effectuez l'une des opérations suivantes :
- Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée.
- Cliquez sur **Edit** (✎) pour modifier une entrée existante.

b) Pour chaque entrée de contrôle d'accès, configurez les propriétés suivantes :
- **Action** : permet de déterminer si l'on souhaite autoriser (correspondance) ou bloquer (pas de correspondance) les critères de trafic.
- **Network** (réseau) : ajoutez les objets ou groupes réseau IPv4 qui identifient la destination du trafic.

c) Cliquez sur **Add** (ajouter) pour ajouter l'entrée à l'objet.

d) Si nécessaire, cliquez sur l'entrée et faites-la glisser pour la déplacer vers le haut ou le bas dans l'ordre des règles jusqu'à l'emplacement souhaité.

Répétez le processus pour créer ou modifier des entrées supplémentaires dans l'objet.

Étape 4 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 5 Cliquez sur **Save** (enregistrer).

Réserves d'adresses

Vous pouvez configurer des regroupements d'adresses IP pour IPv4 et IPv6 qui peuvent être utilisés pour l'interface de dépistage avec mise en grappe ou pour les profils d'accès à distance VPN.

Procédure

Étape 1 sélectionnez **Objets** > **Gestion des objets** > **Ensemble des adresses**.

Étape 2 Cliquez sur **IPv4 Pools** (Ensemble IPv4), puis sur **Add IPv4 Pools** (Ajouter des ensembles IPv4), et configurez les champs suivants.

- **Nom** : saisissez le nom de l'ensemble d'adresses IP. Il peut comporter jusqu'à 64 caractères
- **Description** : ajoutez une description facultative à cet ensemble d'adresses.
- **IP Address** (adresse IP) : saisissez une plage d'adresses disponibles dans l'ensemble d'adresses. Utilisez une notation décimale à point et un tiret entre le début et l'adresse de fin, par exemple : 10.10.147.100-10.10.147.176.
- **Mask** (masque) : identifie le sous-réseau sur lequel cet ensemble d'adresses IP se trouve.
- **Allow Overrides**(autoriser les remplacements) : cochez cette case pour activer les remplacements d'objets. Cliquez sur la flèche de développement pour afficher le tableau **Overrides** (Remplacements). Vous pouvez ajouter un nouveau remplacement en cliquant sur **Add**. Consultez Mises en priorité d'objets, à la page 11 pour obtenir de plus amples renseignements.

Étape 3 Cliquez sur **Save** (enregistrer).

Étape 4 Cliquez sur **IPv6 Pools** (Ensemble IPv6), puis sur **Add IPv6 Pools** (Ajouter des ensembles IPv6), et configurez les champs suivants.

- **Nom** : saisissez le nom de l'ensemble d'adresses IP. Il peut comporter jusqu'à 64 caractères
- **Description** : ajoutez une description facultative à cet ensemble d'adresses.
- **IPv6 Address** (adresse IPv6) : saisissez la première adresse IP disponible dans l'ensemble configuré et la longueur du préfixe en bits. Par exemple : 2001:DB8::1/64.
- **Number of Addresses**(nombre d'adresses) : Détermine le nombre d'adresses IPv6, en commençant par l'adresse IP de départ, qui se trouvent dans l'ensemble.
- **Allow Overrides**(autoriser les remplacements) : cochez cette case pour activer les remplacements. Cliquez sur la flèche de développement pour afficher le tableau **Overrides** (Remplacements). Vous

pouvez ajouter un nouveau remplacement en cliquant sur **Add**. Consultez Mises en priorité d'objets, à la page 11 pour obtenir de plus amples renseignements.

Étape 5 Cliquez sur **Save** (enregistrer).

Filtres d'application

Les filtres d'applications fournis par le système vous aident à effectuer le contrôle des applications en organisant les applications en fonction de caractéristiques de base: type, risque, pertinence commerciale, catégorie et balises. Dans le gestionnaire d'objets, vous pouvez créer et gérer des filtres d'application définis par l'utilisateur réutilisables en fonction de combinaisons de filtres fournis par le système ou de combinaisons personnalisées d'applications. Pour de plus amples renseignements, voir Conditions des règles d'application.

Chemin AS

Un chemin d'accès AS est un attribut obligatoire pour configurer le BGP. Il s'agit d'une séquence de numéros de système autonome par laquelle il est possible d'accéder à un réseau. Le chemin d'AS est une séquence de numéros d'AS entre les routeurs source et de destination qui forment une route dirigée pour les paquets. Les systèmes autonomes voisins (AS) utilisent BGP pour échanger et mettre à jour des messages sur la façon d'atteindre différents préfixes de systèmes autonomes. Une fois que chaque routeur a pris une nouvelle décision locale sur la meilleure route à suivre pour atteindre une destination, il envoie cette route, ou information sur le chemin, ainsi que les mesures de distance et les attributs de chemin correspondants, à chacun de ses homologues. Au fur et à mesure que ces informations transitent dans le réseau, chaque routeur le long du chemin ajoute son numéro de système autonome unique à une liste d'AS dans le message de BGP. Cette liste est l'AS-PATH de la route. Un AS-PATH associé à un préfixe AS fournissent un identifiant spécifique pour une route de transit unidirectionnelle dans le réseau. Utiliser la page Configure AS Path (Configurer le chemin AS) pour créer, copier et modifier les objets de politique de chemin du système autonome. Vous pouvez créer des objets de liste de préfixes pour IPv6 à utiliser lorsque vous configurez des cartes de routage, des cartes de politiques, le filtrage OSPF ou le filtrage de voisin BGP Un filtre de chemin AS vous permet de filtrer le message de mise à jour du routage à l'aide d'expressions régulières.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets),** puis choisissez **AS Path** dans la table des matières.

Étape 2 Cliquez sur **Add AS Path** (Ajouter un chemin d'accès de système autonome).

Étape 3 Saisissez un nom pour l'objet AS Path dans le champ **Name** (Nom). Les valeurs valides sont comprises entre 1 et 500.

Étape 4 Cliquez sur **Add** (Ajouter) dans la fenêtre **New AS Path Object** (Nouvel objet AS-Path).

a) Sélectionnez les options Allow (autoriser) ou Block (blocage) dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

b) Précisez l'expression régulière qui définit le filtre de chemin AS dans le champ **Regular Expression** (expression régulière).

c) Cliquez sur **Add** (ajouter).

Étape 5 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 6 Cliquez sur **Save** (enregistrer).

Modèle BFD

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une interface unique. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à sauts multiples. Le mode Echo est désactivé par défaut. Vous pouvez activer le mode Echo sur un seul saut uniquement.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management** > **(gestion des objets)** BFD Template (Modèle BFD)

Étape 2 Cliquez sur **Add BFD modèle** (ajouter un modèle BFD) ou **Edit**(modifier).

Remarque Si vous modifiez un modèle, vous ne pouvez pas modifier son nom et son type.

Étape 3 Dans l'onglet **Template** (modèle), configurez les éléments suivants :

- **Template Name (**nom du modèle) : nom de ce modèle BFD. Vous devez attribuer un nom afin de configurer le reste des paramètres dans le modèle. Le nom du modèle ne peut pas contenir d'espaces et ne peut pas contenir que des chiffres.
- **Type** : cliquez sur le bouton radio à **saut unique** ou à **sauts multiples**.
- **Enable Echo**(activer Echo) : (facultatif) Active Echo pour le modèle à saut unique.

Si la fonction Echo n'est pas négociée, les paquets de contrôle BFD sont envoyés à un débit élevé pour respecter le temps de détection. Si la fonction Echo est négociée, les paquets de contrôle BFD sont envoyés à un débit négocié plus lent et les paquets d'écho autodirigés sont envoyés à un débit élevé. Nous vous recommandons d'utiliser le mode Echo, si possible.

Étape 4 Dans l'onglet **Interval** (intervalle), configurez les éléments suivants :

a) Dans la liste déroulante **Interval Type** (type d'intervalle), sélectionnez **Microseconds** ou **Milliseconds** (Microsecondes ou millisecondes).

b) Dans le champ **Multiplier** (Multiplicateur), saisissez la valeur à utiliser pour calculer le temps de maintien. Cette valeur indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50. La valeur par défaut est de 3.

c) Dans le champ **Minimum Transmit** (transmission minimale), saisissez l'intervalle de transmission minimal. La plage se situe entre 50 et 999 millisecondes ou entre 50 000 et 999 000 microsecondes.

d) Dans le champ **Minimum Receive** (réception minimale), saisissez l'intervalle minimal de réception. La plage se situe entre 50 et 999 millisecondes ou entre 50 000 et 999 000 microsecondes.

Étape 5 Sous l'onglet **Authentication** (authentification), configurez les éléments suivants :

- **Authentication Type** (type d'authentification) : sélectionnez **NONE**, **md5**, **meticulous-sha-1**, **metics-md5**ou **sha-1** dans la liste déroulante.
- **Encrypted Password**(mot de passe chiffré) : (facultatif) active le chiffrement du mot de passe d'authentification.
- **Password**(mot de passe) : le mot de passe d'authentification qui doit être envoyé et reçu dans les paquets utilisant le protocole de routage en cours d'authentification. La valeur valide est une chaîne contenant de 1 à 29 caractères alphanumériques majuscules et minuscules, sauf que le premier caractère NE PEUT PAS être un chiffre ou un chiffre suivi d'un espace. Par exemple, « 1password » ou « 0 password » n'est pas valide.
- **Key ID** : ID de clé partagée qui correspond à la valeur de clé. La valeur doit être comprise entre 0 et 255.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration du modèle BFD.

Liste de suite de chiffrement

Une liste de suites de chiffrement est un objet composé de plusieurs suites de chiffrement. Chaque valeur de suite de chiffrement prédéfinie représente une suite de chiffrement utilisée pour négocier une session chiffrée SSL ou TLS. Vous pouvez utiliser des suites de chiffrement et des listes de suites de chiffrement dans les règles SSL pour contrôler le trafic chiffré en fonction du fait que le client et le serveur ont négocié la session SSL à l'aide de cette suite de chiffrement. Si vous ajoutez une liste de suite de chiffrement à une règle SSL, les sessions SSL négociées avec l'une des suites de chiffrement dans la liste correspondent à la règle.

Remarque Bien que vous puissiez utiliser les suites de chiffrement dans l'interface Web aux mêmes endroits que les listes de suites de chiffrement, vous ne pouvez pas ajouter, modifier ou supprimer de suites de chiffrement.

Création de listes de suites de chiffrement

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Cipher Suite List** (Liste de suite de chiffrement) dans la liste des types d'objets.

Étape 3 Cliquez sur **Ajouter des suites de chiffrement**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Choisissez une ou plusieurs suites de chiffrement dans la liste **Availability Ciphers** (chiffrements disponibles).

Étape 6 Cliquez sur **Add** (ajouter).

Étape 7 Vous pouvez également cliquer sur **Supprimer** ( ) à côté des suites de chiffrement dans la liste des **chiffrements sélectionnés** que vous souhaitez supprimer.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Liste de communautés

Une communauté est un attribut de BGP transitif facultatif. Une communauté étendue est un groupe plus vaste de destinations partageant un attribut commun. Il est utilisé pour le balisage de route. L'attribut de communauté BGP est une valeur numérique qui peut être affectée à un préfixe spécifique et annoncée à d'autres voisins. Les communautés peuvent être utilisées pour marquer un ensemble de préfixes qui partagent un attribut commun. Les fournisseurs en amont peuvent utiliser ces marqueurs pour appliquer une politique de routage commune, comme le filtrage ou l'attribution d'une préférence locale précise ou la modification d'autres attributs. Utilisez la page Configurer les listes de communauté pour créer, copier et modifier des objets de politique de listes de communauté. Vous pouvez créer des objets de liste de communauté à utiliser lors de la configuration de cartes de routage ou de cartes de politiques. Vous pouvez utiliser les listes de communautés pour créer des groupes de communautés à utiliser dans une clause de correspondance d'une feuille de route. La liste de communauté est une liste ordonnée de déclarations correspondantes. Les destinations sont comparées aux règles jusqu'à ce qu'une correspondance soit trouvée.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objets** > **Gestion des objets** et choisissez **Liste des communautés** dans la table des matières.

Étape 2 Cliquez sur **Add Extended Community List** (Ajouter une liste de communautés étendues).

Étape 3 Dans le champ **Name**, spécifiez un nom pour l'objet de liste de communauté.

Étape 4 Cliquez sur **Add** (Ajouter) dans la fenêtre **New Community List Object** (nouvel objet de liste de communauté).

Étape 5 Sélectionner le bouton radio **Standard** pour indiquer le type de règle de communauté.

Les listes de communautés standard sont utilisées pour spécifier des communautés et des numéros de communauté.

Remarque Vous ne pouvez pas avoir des entrées utilisant les types de règles de communauté Standard et Étendu dans le même objet de liste de communauté.

a) Sélectionnez les options Allow (autoriser) ou Block (blocage) dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

b) Dans le champ **Communautés**, spécifiez un numéro de communauté. Les valeurs valides peuvent être de 1 à 4294967295 ou de 0:1 à 65534:65535.

c) Sélectionner le **type de routage** approprié .

- **Internet** : sélectionnez cette option pour spécifier la communauté Internet bien connue. Les routages de cette communauté sont annoncés à tous les homologues (internes et externes).
- **Pas d'annonce** : sélectionnez cette option pour spécifier la communauté bien connue sans publicité. Les routages de cette communauté ne sont annoncés à aucun homologue (interne ou externe).
- **Pas d'exportation** : sélectionnez cette option pour spécifier la communauté bien connue sans exportation. Les routes avec cette communauté sont annoncées uniquement aux homologues dans le même système autonome ou uniquement aux autres systèmes sous-autonomes d'une confédération. Ces routes ne sont pas annoncées aux homologues externes.

Étape 6 Sélectionner le bouton radio **Développé** pour indiquer le type de règle de communauté.

Les listes de communautés étendues sont utilisées pour filtrer les communautés à l'aide d'une expression régulière. Les expressions régulières sont utilisées pour spécifier des modèles correspondant aux attributs de la communauté.

a) Sélectionnez les options Allow (autoriser) ou Block (blocage) dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.
b) Précisez l'expression régulière dans le champ **Expressions**.

Étape 7 Cliquez sur **Add** (ajouter).

Étape 8 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 9 Cliquez sur **Save** (enregistrer).

Communauté étendue

Une communauté étendue est un groupe plus vaste de destinations partageant un attribut commun. La liste de communauté étendue BGP possède des attributs qui peuvent être utilisés pour marquer un ensemble de préfixes qui partagent un attribut commun. Ces marqueurs sont utilisés dans la clause de correspondance d'une carte de routage pour filtrer les routes et mettre en œuvre les fuites de route entre les routeurs virtuels. Vous pouvez également définir des objets de liste de politiques avec la liste de communauté étendue pour le filtrage. La liste de communauté est une liste ordonnée de déclarations correspondantes. Les routes sont mises en correspondance avec les règles jusqu'à ce qu'une correspondance soit trouvée avec la cible de routage (cas standard) ou l'expression régulière (étendu). Utilisez la page Extended Community (communauté étendue) pour créer et modifier des objets de politique de liste de communauté étendue.

Remarque Les listes de communautés étendues s'appliquent uniquement à la configuration de l'importation ou de l'exportation de routages.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management** (Objets > Gestion des objets) et choisissez **Community List** > **Extended Community** (Liste des communautés > Communautés étendues) dans la table des matières.

Étape 2 Cliquez sur **Add Extended Community List** (Ajouter une liste de communautés étendues).

Étape 3 Dans le champ **Name** (nom), spécifiez un nom pour l'objet de liste de communauté étendue. La longueur du nom ne peut pas dépasser 80 caractères.

Étape 4 Sélectionner le type de règle de communauté étendue :

- Cliquez sur le bouton radio **Standard** pour spécifier une ou plusieurs cibles de routage.
- Cliquez sur le bouton radio **Expanded** (Développé) pour spécifier des expressions régulières.

Remarque Vous ne pouvez pas avoir d'entrées utilisant les types de règle de communauté étendue Standard et Développé dans le même objet de liste de communauté étendue.

Étape 5 Cliquez sur **Add** (ajouter).

Étape 6 Si vous avez sélectionné **Standard** comme type de règle de communauté étendue, spécifiez les éléments suivants :

a) Dans le champ **Sequence No** (Numéro de séquence), saisissez l'ordre dans lequel vous souhaitez que la règle soit exécutée.

Le numéro de séquence doit être unique dans la liste.

b) Dans la liste déroulante **Action**, si vous souhaitez autoriser des routes dont la cible de routage est spécifiée ici, sélectionnez **Allow**(autoriser); si vous souhaitez refuser les routages ayant une cible de routage spécifiée ici, sélectionnez **Block** (Bloquer).

c) Dans le champ **Route Target** (objectif de routage), précisez une cible de routage.

- Vous pouvez ajouter une seule cible de routage ou un ensemble de cibles de routage séparées par des virgules dans une seule entrée. Par exemple, *1:2,1:4,1:6*.
- Les valeurs valides sont comprises entre 1:1 et 65534:65535.
- Vous pouvez avoir un maximum de 8 objectifs de routage dans une entrée.
- Une cible de routage redondante ne peut pas être définie sur plusieurs entrées. Par exemple, disons que vous souhaitiez configurer *seq1* avec des cibles de routage *1:200,100:100,1:300* et *seq2* avec des cibles de routage *1:300,100:100,1:200*. Cela entraîne un ensemble de cibles de routage redondant et ne peut pas être déployé.

Étape 7 Si vous avez sélectionné **Développé** comme type de règle de communauté étendue, spécifiez les éléments suivants :

a) Dans le champ **Sequence No** (Numéro de séquence), saisissez l'ordre dans lequel vous souhaitez que la règle soit exécutée.

Le numéro de séquence doit être unique dans la liste.

b) Dans la liste déroulante **Action**, si vous souhaitez autoriser les routages ayant une expression régulière correspondante qui est spécifiée ici, sélectionnez **Allow**(autorisation); si vous souhaitez refuser les routages ayant une expression régulière correspondante qui est spécifiée ici, sélectionnez **Block** (Bloquer).

c) Précisez l'expression régulière dans le champ **Expressions**.

- Vous pouvez ajouter une cible de routage unique ou un ensemble de cibles de routage séparées par un espace dans une seule entrée. Par exemple, *^((16) | (18)):(.)$*.
- Vous pouvez ajouter un maximum de 16 expressions régulières à une entrée.
- Une expression régulière redondante ne peut pas être définie sur plusieurs entrées. Par exemple, disons que vous souhaitiez configurer *seq1* avec *^((16) | (18)):(.)$ ^4_[0-9]*$* comme routes cibles

et *seq2* avec *^4_[0-9]*$ ^((16) | (18)) :(.)$* routes cibles. Il en résulte un ensemble d'expressions régulières redondant qui ne peut pas être déployé.

Pour en savoir plus sur les expressions régulières BGP, consultez les renseignements ici.

Étape 8 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 9 Cliquez sur **Save** (enregistrer).

La liste de communauté étendue peut être référencée dans la clause de correspondance de l'objet de carte de routage ou de la liste des politiques :

- Dans l'objet de carte de routage, le nom de la liste de communauté étendue est affiché dans la boîte de dialogue **Add Route Map Entry** > **Match Clause** > **BGP** > **Community List** > **Add Extended Community List** (Ajouter une entrée de carte de routage > Clause de correspondance > Liste des communautés > Ajouter une liste des communautés étendues). Pour plus de détails sur la configuration des paramètres de BGP dans une carte de routage, consultez Carte de routage, à la page 76.
- Dans l'objet Liste de politiques, le nom de la liste de communauté étendue s'affiche dans la boîte de dialogue **Add Policy List** > **Community Rule** > **Add Extended Community List** (Ajouter une liste de politiques > Règle de communauté > Ajouter une liste de communautés étendues). Pour plus de détails sur la configuration des paramètres de BGP dans une liste de politiques, consultez Liste des stratégies, à la page 71.

Regroupement IPv6 du DHCP

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6), vous pouvez configurer les défense contre les menaces pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces, en définissant un ensemble DHCP IPv6 et en l'affectant au serveur DHCPv6. Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que défense contre les menaces a reçu à l'aide de la délégation de préfixe.

Pour ajouter un ensemble, consultez Créer un ensemble d'adresses IPv6 du DHCP.

Nom distinctif

Chaque objet de nom distinctif représente le nom distinctif répertorié pour le sujet ou l'émetteur d'un certificat de clé publique. Vous pouvez utiliser des groupes d'objets à nom distinctif dans les règles TLS/SSLpour contrôler le trafic chiffré selon que le client et le serveur ont négocié la session TLS/SSL en utilisant un certificat de serveur avec le nom unique comme sujet ou émetteur.

(Un *groupe de noms distinctifs* est un ensemble nommé d'objets de nom unique existants.)

Le nom distinctif peut consister en un code de pays, un nom usuel, l'organisation et l'unité organisationnelle, mais consiste généralement en un nom usuel uniquement. Par exemple, le nom usuel dans le certificat pour `https://www.cisco.com` est `cisco.com`. (Cependant, ce n'est pas toujours aussi simple; Conditions de règles de noms distinctifs (DN) montre comment trouver des noms communs.) Le certificat peut contenir plusieurs noms de domaine alternatif (Subject Alternative Names ou SAN) que vous pouvez utiliser comme DN dans une condition de règle. Pour en savoir plus sur les SAN, consultez RFC 5280, section 4.2.1.6.

Le format d'un objet de nom distinctif qui fait référence à un nom commun est `CN=name`. Si vous ajoutez une condition de règle de DN sans `CN=`, le système ajoute `CN=` avant d'enregistrer l'objet.

Comme nous le verrons plus loin dans la section Conditions de règles de noms distinctifs (DN), le système utilise l'indication du nom du serveur (SNI) pour faire correspondre le nom distinctif dans la règle TLS/SSL dès que possible.

Vous pouvez également ajouter un nom distinctif avec un de chacun des attributs répertoriés dans le tableau suivant, séparé par des virgules.

Tableau 1 : Attributs de noms distinctifs

Attribut	Description	Valeurs autorisées
C	Code de pays	deux caractères alphabétiques
NC	Nom usuel	jusqu'à 64 caractères alphanumériques, barres obliques inverses (/), tirets (-), guillemets (") ou astérisques (*) ou espaces
O	Organisation	jusqu'à 64 caractères alphanumériques, barres obliques inverses (/), tirets (-), guillemets (") ou astérisques (*) ou espaces
OU	Unité organisationnelle	jusqu'à 64 caractères alphanumériques, barres obliques inverses (/), tirets (-), guillemets (") ou astérisques (*) ou espaces

Remarques importantes sur les conditions de règle de nom distinctif

- La première fois que le système détecte une session chiffrée sur un nouveau serveur, les données de nom distinctif ne sont pas disponibles pour le traitement de ClientHello, ce qui *peut* entraîner le déchiffrement d'une première session.

  Si le serveur demande TLS 1.3, le paramètre de découverte d'identité du serveur TLS peut aider en s'assurant que le certificat du serveur est connu avant de prendre des décisions relatives à politique de déchiffrement. Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès.

- Vous *ne pouvez pas* configurer une condition de nom distinctif si vous choisissez également l'action **Déchiffrer - Clé connue**. Comme cette action vous oblige à choisir un certificat de serveur pour déchiffrer le trafic, le certificat correspond déjà au trafic.

Exemples de caractères génériques

Vous pouvez définir un ou plusieurs astérisques (*) comme caractères génériques dans un attribut. Dans un attribut de nom commun, vous pouvez définir un ou plusieurs astérisques par étiquette de nom de domaine.

les caractères génériques ne correspondent que dans cette étiquette, mais vous pouvez définir plusieurs étiquettes avec des caractères génériques. Consultez le tableau suivant pour voir des exemples.

Tableau 2 : Exemples de caractères génériques d'attribut de nom commun

Attribut	Correspondances	Ne correspond pas
NC=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

Remarque L'objet DN `CN=amp.cisco.com` ne correspond *pas* à un nom commun comme `CN=auth.amp.cisco.com`, c'est pourquoi nous vous recommandons d'utiliser les caractères génériques dans ce cas.

Pour en savoir plus et consulter des exemples, consultez Conditions de règles de noms distinctifs (DN).

Sujets connexes

Conditions de règles de noms distinctifs (DN)

Création des objets de nom distinctif

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Distinguished Name** (nom distinctif), puis choisissez **Individual Objects** (objets individuels).

Étape 3 Cliquez sur **Ajouter un nom distinctif**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Dans le champ **DN**, saisissez une valeur pour le nom distinctif ou le nom commun. Vous avez les options suivantes :

- Si vous ajoutez un nom distinctif, vous pouvez en inclure un pour chaque attribut répertorié dans Nom distinctif, à la page 30, en le séparant par des virgules.
- Si vous ajoutez un nom commun, vous pouvez inclure plusieurs étiquettes et caractères génériques.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Groupe de serveurs DNS

Les serveurs du système de noms de domaine (DNS) résolvent les noms de domaine complets (FQDN), tels que www.exemple.com, en adresses IP.

Création d'objets de groupe de serveurs DNS

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

Étape 2 Cliquez sur **Groupe de serveurs DNS** dans la liste des objets réseau.

Étape 3 Cliquez sur **Ajouter un groupe de serveurs DNS**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 De manière facultative, saisissez le **domaine par défaut** qui sera utilisé pour ajouter aux noms d'hôtes qui ne sont pas complets.

Ce paramètre n'est utilisé que pour le groupe de serveurs par défaut.

Étape 6 Les valeurs par défaut du **délai d'attente** et des **tentatives** sont pré-remplies. Modifiez ces valeurs si nécessaire.

- Tentatives - Nombre de tentatives, de 0 à 10, pour retenter d'accéder à la liste des serveurs DNS lorsque le système ne reçoit pas de réponse. La valeur par défaut est 2.
- Délai d'attente - Nombre de secondes, de 1 à 30, à attendre avant d'essayer le serveur DNS suivant. La valeur par défaut est de 2 secondes. Chaque fois que le système réessaie la liste des serveurs, ce délai est doublé.

Étape 7 Saisissez les **serveurs DNS** qui feront partie de ce groupe, au format IPv4 ou IPv6, sous forme d'entrées séparées par des virgules.

Six serveurs DNS au maximum peuvent appartenir à un groupe.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

Les serveurs DNS configurés dans le groupe de serveurs DNS doivent être affectés à des objets d'interface dans les paramètres de la plateforme DNS. Pour en savoir plus, consultez DNS.

Attributs externes

À propos des objets dynamiques créés par l'API

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

Les différences entre les objets dynamiques et les objets réseau sont les suivantes :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.
- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Sujets connexes

Ajouter ou modifier un objet dynamique créé par l'API, à la page 34

Ajouter ou modifier un objet dynamique créé par l'API

Cette procédure explique comment ajouter ou modifier un *objet dynamique*, c'est-à-dire un groupe d'adresses IP utilisant l'API, avec ou sans routage inter-domaine (*CIDR*) sans classe, qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.

Remarque Cette procédure n'est pas nécessaire si vous utilisez Connecteur d'attributs dynamiques Cisco Secure, car elle crée automatiquement des objets dynamiques pour vous.

Avant de commencer

Consultez le *guide de démarrage rapide de l'API REST de Cisco Firepower Management Center* pour obtenir des renseignements sur l'utilisation de l'API REST des services d'objet pour remplir l'objet IP avec une adresse. Les objets dynamiques ne nécessitent pas de déploiement.

Procédure

Étape 1 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **Attributs externes** > **Objets dynamiques**.

Étape 3 Cliquez sur **Add Dynamic Object** (ajouter un objet dynamique) ou sur **Edit** ( ).

Étape 4 Entrez un nom pour l'objet (sous **Name**) et, facultativement, une **description**.

Étape 5 Dans la liste **Type**, cliquez sur **IP**.

Prochaine étape

Si nécessaire, mettez à jour l'objet dynamique à l'aide de l'API. Le déploiement n'est pas nécessaire.

Objets dynamiques

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Remarque Contrairement à la plupart des autres objets, les objets dynamiques n'ont pas à être déployés sur les périphériques gérés pour prendre effet. Ajoutez simplement des objets dynamiques à la page à onglet **Dyamic Attributes** de votre règle de contrôle d'accès. les valeurs des objets sont automatiquement mises à jour sur le périphérique géré dès que possible après avoir été poussées par Connecteur d'attributs dynamiques Cisco Secure.

Il existe les types d'objets dynamiques suivants :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.
- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Pour en savoir plus sur les objets dynamiques créés par API, consultez À propos des objets dynamiques créés par l'API, à la page 34.

Utilisation d'objets dynamiques

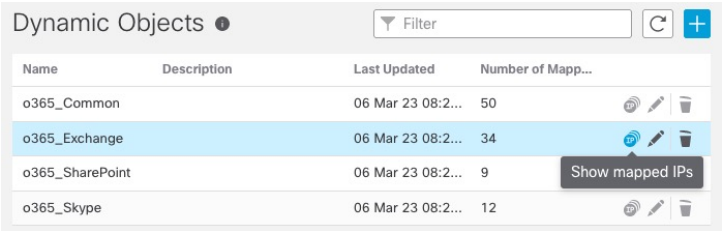
La page accessible à l'adresse **Objets** > **Gestion des objets** > **Attributs externes** > **Objet dynamique** s'affiche comme suit si vous avez déjà configuré certains objets dynamiques.

Cette page affiche des informations sur chaque objet dynamique et vous permet d'afficher ou de télécharger les adresses IP associées à cet objet. Pour en savoir plus, consultez Mappages d'objets dynamiques, à la page 36.

Mappages d'objets dynamiques

Si vous avez configuré les objets dynamiques à l'aide de l'API ou de connecteur d'attributs dynamiques, vos connecteurs envoient les adresses IP correspondant aux filtres d'attributs dynamiques à centre de gestion à des intervalles réguliers.

Pour afficher ou télécharger une liste actuelle de ces adresses IP, cliquez sur **Show Mapped IDs** (afficher les ID mappés), comme le montre la figure suivante.



Les adresses IP sont ajoutées dynamiquement au fil du temps. Vous devez donc envisager de le faire régulièrement, en particulier si vos règles de contrôle d'accès ne se comportent pas comme prévu.

Thèmes connexes

- À propos des objets dynamiques créés par l'API, à la page 34
- À propos du connecteur d'attributs dynamiques Cisco Secure

À propos des objets dynamiques créés par l'API

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

Les différences entre les objets dynamiques et les objets réseau sont les suivantes :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.

- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Sujets connexes

Ajouter ou modifier un objet dynamique créé par l'API, à la page 34

Ajouter ou modifier un objet dynamique créé par l'API

Cette procédure explique comment ajouter ou modifier un *objet dynamique,* c'est-à-dire un groupe d'adresses IP utilisant l'API, avec ou sans routage inter-domaine (*CIDR*) sans classe, qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.

Remarque Cette procédure n'est pas nécessaire si vous utilisez Connecteur d'attributs dynamiques Cisco Secure, car elle crée automatiquement des objets dynamiques pour vous.

Avant de commencer

Consultez le *guide de démarrage rapide de l'API REST de Cisco Firepower Management Center* pour obtenir des renseignements sur l'utilisation de l'API REST des services d'objet pour remplir l'objet IP avec une adresse. Les objets dynamiques ne nécessitent pas de déploiement.

Procédure

Étape 1 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **Attributs externes** > **Objets dynamiques**.

Étape 3 Cliquez sur **Add Dynamic Object** (ajouter un objet dynamique) ou sur **Edit** ( ).

Étape 4 Entrez un nom pour l'objet (sous **Name**) et, facultativement, une **description**.

Étape 5 Dans la liste **Type**, cliquez sur **IP**.

Prochaine étape

Si nécessaire, mettez à jour l'objet dynamique à l'aide de l'API. Le déploiement n'est pas nécessaire.

Balise du groupe de sécurité

Un objet Security Group Tag (SGT; balise de groupe de sécurité) spécifie une seule valeur SGT. Vous pouvez utiliser des objets SGT dans les règles pour contrôler le trafic avec des attributs SGT qui n'ont **pas** été affectés par Cisco ISE. Vous ne pouvez pas grouper ou remplacer des objets SGT.

Sujets connexes

Transition automatique des règles SGT personnalisées aux règles ISE SGT
Conditions SGT personnalisées
Conditions de règle ISE SGT ou règle SGT personnalisée

Création d'objets de balise de groupe de sécurité

Vous pouvez créer ces objets uniquement dans le domaine global. Pour utiliser l'objet sur les périphériques classiques, vous devez avoir la licence de contrôle. Pour les périphériques sous licence Smart, n'importe quelle licence suffit.

Avant de commencer

- Désactivez les connexions ISE/ISE-PIC. Vous ne pouvez pas créer d'objets SGT personnalisés si vous utilisez ISE/ISE-PIC comme source d'identité.

Procédure

Étape 1 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.
Étape 2 Cliquez sur **Attributs externes** > **Balise du groupe de sécurité**.
Étape 3 Cliquez sur **Ajouter une balise de groupe de sécurité**.
Étape 4 Saisissez un **Nom**.
Étape 5 Vous pouvez également saisir une **Description**.
Étape 6 Dans le champ **Balise**, saisissez une balise SGT unique.
Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Liste de fichiers

Si vous utilisez Défense contre les programmes malveillants et que l'info nuage AMP identifie incorrectement la disposition d'un fichier, vous pouvez ajouter le fichier à une *liste de fichiers* pour mieux détecter le fichier à l'avenir. Ces fichiers sont spécifiés à l'aide de valeurs de hachage SHA-256. Chaque liste de fichiers peut contenir jusqu'à 10 000 valeurs SHA-256 uniques.

Il existe deux catégories prédéfinies de listes de fichiers :

Liste sûre

Si vous ajoutez un fichier à cette liste, le système le traite comme si le nuage AMP avait affecté une disposition sûre.

Liste de détection personnalisée

Si vous ajoutez un fichier à cette liste, le système le traite comme si le nuage AMP avait affecté une disposition relative aux programmes malveillants.

Dans un déploiement multidomaine, une liste sûre et une liste de détection personnalisée sont présentes pour chaque domaine. Dans les domaines de niveau inférieur, vous pouvez afficher, mais pas modifier, les listes des antécédents.

Comme vous devez spécifier manuellement le comportement de blocage pour les fichiers inclus dans ces listes, le système n'interroge pas le nuage AMP sur les dispositions de ces derniers. Vous devez configurer une règle dans la politique de fichiers avec une action **Recherche de programmes malveillants dans le nuage** ou **Bloquer les programmes malveillants** et un type de fichier correspondant pour calculer la valeur SHA d'un fichier.

Mise en garde N'incluez **pas** de logiciel malveillant dans la liste sûre. La liste sûre prévaut à la fois sur le nuage AMP et sur la liste de détection personnalisée.

Fichiers sources pour les listes de fichiers

Vous pouvez ajouter plusieurs valeurs SHA-256 à une liste de fichiers en chargeant un fichier source de valeurs séparées par des virgules (CSV) contenant une liste de valeurs SHA-256 et de descriptions. centre de gestion valide le contenu et remplit la liste de fichiers avec des valeurs SHA-256 valides.

Le fichier source doit être un simple fichier texte avec une extension de nom de fichier .csv. Tout en-tête doit commencer par un signe dièse (`#`); elles sont traitées comme un commentaire et non téléversées. Chaque entrée doit contenir une seule valeur SHA-256 suivie d'une description et se terminer par le caractère `LF` ou `CR+LF` Newline. Le système ignore toute information supplémentaire dans l'entrée.

Tenez compte des points suivants :

- La suppression d'un fichier source de la liste de fichiers supprime également tous les hachages SHA-256 associés de la liste de fichiers.
- Vous ne pouvez pas téléverser plusieurs fichiers dans une liste de fichiers si, après avoir réussi le chargement du fichier source, la liste des fichiers contient plus de 10 000 valeurs SHA-256 distinctes.
- Le système tronque les descriptions dépassant 256 caractères pour les 256 premiers caractères lors du téléchargement. Si la description contient des virgules, vous devez utiliser un caractère d'échappement (`\,`). Si aucune description n'est incluse, le nom du fichier source est utilisé à la place.
- Toutes les valeurs SHA-256 non en double sont ajoutées à la liste de fichiers. Si une liste de fichiers contient une valeur SHA-256 et que vous téléversez un fichier source contenant cette valeur, la nouvelle valeur chargée ne modifie pas la valeur SHA-256 existante. Lors de l'affichage des fichiers capturés, des événements de fichiers ou des événements malveillants liés à la valeur SHA-256, tout nom ou description de menace est dérivé de la valeur SHA-256 individuelle.
- Le système ne téléverse pas les valeurs SHA-256 non valides dans un fichier source.
- Si plusieurs fichiers source téléversés contiennent une entrée pour la même valeur SHA-256, le système utilise la valeur la plus récente.
- Si un fichier source contient plusieurs entrées pour la même valeur SHA-256, le système utilise la dernière.

- Vous ne pouvez pas modifier directement un fichier source dans le gestionnaire d'objets. Pour apporter des changements, vous devez d'abord modifier directement votre fichier source, supprimer la copie sur le système, puis téléverser le fichier source modifié.
- Le nombre d'entrées associées à un fichier source fait référence au nombre de valeurs SHA-256 distinctes. Si vous supprimez un fichier source d'une liste de fichiers, le nombre total d'entrées SHA-256 que contient la liste de fichiers diminue le nombre d'entrées valides dans le fichier source.

Ajout de valeurs SHA-256 individuelles aux listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Vous pouvez soumettre la valeur SHA-256 d'un fichier pour l'ajouter à une liste de fichiers. Vous ne pouvez pas ajouter de valeurs SHA-256 en double.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Avant de commencer

- Faites un clic droit sur un événement lié à un fichier ou à un programme malveillant dans la vue des événements, choisissez **Show Full Text** (afficher le texte intégral) dans le menu contextuel et copiez la valeur SHA-256 complète pour la coller dans la liste de fichiers.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **File List** (Liste de fichiers) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** ( ) à côté de la liste de nettoyage ou de la liste de détection personnalisée où vous souhaitez ajouter un fichier.

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Choisissez `Enter SHA Value` (Saisissez la valeur SHA) dans la liste déroulante **Add by** (ajouter par).

Étape 5 Saisissez une description du fichier source dans le champ **Description**.

Étape 6 Saisissez ou collez la valeur totale du fichier dans le champ **SHA-256**. Le système ne prend pas en charge les valeurs partielles de correspondance.

Étape 7 Cliquez sur **Add** (ajouter).

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Une fois les modifications de configuration déployées, le système n'interroge plus le nuage AMP pour connaître les fichiers de la liste.

Téléversement de fichiers individuels vers des listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Si vous avez une copie du fichier que vous souhaitez ajouter à une liste de fichiers, vous pouvez la téléverser dans Cisco Secure Firewall Management Center pour analyse. le système calcule la valeur SHA-256 du fichier et ajoute le fichier à la liste. Le système n'applique pas de limite à la taille des fichiers pour le calcul de SHA-256.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **File List** (Liste de fichiers) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** ( ) à côté de la liste de nettoyage ou de la liste de détection personnalisée où vous souhaitez ajouter un fichier.

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Dans la liste déroulante **Add by** (Ajouter par), choisissez **Calculate SHA** (Calculer SHA).

Étape 5 De manière facultative, dans le champ **Description**, saisissez une description du fichier. Si vous n'saisissez pas de description, le nom du fichier est utilisé pour la description lors du téléversement.

Étape 6 Cliquez sur **Browse** (Parcourir) et choisissez un fichier à téléverser.

Étape 7 Cliquez sur **Calculate and Add SHA** (Calculer et ajouter des SHA)

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Après avoir déployé les modifications de configuration, le système n'interroge plus le nuage AMP pour les fichiers de la liste.

Téléversement de fichiers source vers les listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **File List** (Liste des fichiers).

Étape 3 Cliquez sur **Edit** (✎) à côté de la liste des fichiers auxquels vous souhaitez ajouter des valeurs à partir d'un fichier source.

Si **Afficher** (👁) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Dans la liste déroulante **Add by** (ajouter par), choisissez `List of SHAs` (liste des SHA).

Étape 5 De manière facultative, dans le champ **Description**, saisissez une description du fichier. Si vous n'saisissez pas de description, le système utilise le nom de fichier.

Étape 6 Cliquez sur **Browse** (Parcourir) pour rechercher le fichier source, puis cliquez sur **Upload and Add List** (Téléverser et ajouter une liste).

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Après le déploiement des politiques, le système n'interroge plus le nuage AMP pour connaître les fichiers de la liste.

Modification des valeurs SHA-256 dans les listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Vous pouvez modifier ou supprimer les valeurs SHA-256 individuelles dans une liste de fichiers. Notez que vous ne pouvez pas modifier directement un fichier source dans le gestionnaire d'objets. Pour apporter des changements, vous devez d'abord modifier directement votre fichier source, supprimer la copie sur le système, puis téléverser le fichier source modifié.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **File List** (Liste des fichiers).

Étape 3 Cliquez sur **Edit** ( ) à côté de la liste de nettoyage ou de la liste de détection personnalisée dans laquelle vous souhaitez modifier un fichier.

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Vous pouvez réaliser les actions suivantes :

- Cliquez sur **Edit** ( ) à côté de la valeur SHA-256 que vous souhaitez modifier et modifiez les valeurs **SHA-256** ou la **description** comme vous le souhaitez.
- Cliquez sur **Supprimer** ( ) à côté de la valeur SHA-256 que vous souhaitez supprimer.

Étape 5 Cliquez sur **Save** (Enregistrer) pour mettre à jour l'entrée de fichier dans la liste.

Étape 6 Cliquez sur **Save** pour enregistrer la liste des fichiers.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Une fois les modifications de configuration déployées, le système n'interroge plus le nuage AMP pour connaître les fichiers de la liste.

Téléchargement de fichiers source à partir de listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **File List** (Liste de fichiers) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** ( ) à côté de la liste blanche ou de la liste de détection personnalisée dans laquelle vous souhaitez télécharger un fichier source.

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 À côté du fichier source que vous souhaitez télécharger , cliquez sur **Afficher** ( ).

Étape 5 Cliquez sur **download SHA List** (télécharger la liste SHA) et suivez les instructions pour enregistrer le fichier source.

Étape 6 Cliquez sur **Close** (Fermer).

FlexConfig

Utilisez des objets de politique FlexConfig dans les politiques FlexConfig pour fournir une configuration personnalisée des fonctionnalités sur les périphériques défense contre les menaces que vous ne pouvez pas configurer autrement avec Cisco Secure Firewall Management Center. Pour en savoir plus sur les politiques FlexConfig, consultez Présentation de la politique FlexConfig.

Vous pouvez configurer les types d'objets suivants pour FlexConfig.

Objets texte

Les objets texte définissent des chaînes de texte de forme libre que vous utilisez comme variables dans un objet FlexConfig. Ces objets peuvent avoir des valeurs uniques ou être une liste de plusieurs valeurs.

Plusieurs objets texte prédéfinis sont utilisés dans les objets FlexConfig prédéfinis. Si vous utilisez l'objet FlexConfig associé, il vous suffit de modifier le contenu de l'objet texte pour personnaliser la façon dont l'objet FlexConfig configure un périphérique donné. Lors de la modification d'un objet prédéfini, il est généralement préférable de créer des remplacements de périphérique pour chaque périphérique que vous configurez, plutôt que de modifier directement les valeurs par défaut de ces objets. Cela permet d'éviter des conséquences imprévues si un autre utilisateur souhaite utiliser le même objet FlexConfig pour un ensemble différent de périphériques.

Pour en savoir plus sur la configuration des objets texte, consultez Configurer les objets texte FlexConfig.

Objets FlexConfig

L'objet FlexConfig comprend des commandes de configuration d'appareil, des variables et des instructions de langages pour l'écriture de script. Lors du déploiement de la configuration, ces instructions sont traitées pour créer une séquence de commandes de configuration avec des paramètres personnalisés pour configurer des fonctionnalités spécifiques sur les machines cibles.

Ces instructions sont configurées soit avant (en préambule) la configuration par le système des fonctionnalités définies dans les politiques et paramètres habituels centre de gestion, soit après (en annexe). Tout FlexConfig qui dépend d'objets configurés Cisco Secure Firewall Management Center(par exemple, un objet réseau) doit être ajouté à la liste de déploiement de configuration, sinon les objets nécessaires ne seront pas configurés avant que FlexConfig ne fasse référence aux objets.

Pour en savoir plus sur la configuration des objets FlexConfig, consultez Configurer les objets FlexConfig.

Géolocalisation

La géolocalisation représente un ou plusieurs pays ou continents que le système a identifiés comme étant la source ou la destination du trafic sur votre réseau surveillé. Vous pouvez utiliser des objets de géolocalisation à différents endroits de l'interface web du système, notamment dans les politiques de contrôle d'accès, les politiques SSL et les recherches d'événements. Par exemple, vous pouvez écrire une règle de contrôle d'accès qui bloque un site Web spécifique.

Pour vous assurer que vous utilisez des données de géolocalisation à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Création d'objets de géolocalisation

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Géolocalisation** dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Geolocation** (Ajouter une géolocalisation).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Cochez les cases des pays et des continents que vous souhaitez inclure dans votre objet géolocalisation. La sélection d'un continent sélectionne tous les pays de ce continent, ainsi que les pays que les mises à jour de GeoDB pourraient ajouter à ce continent ultérieurement. La désactivation d'un pays sous un continent désélectionne le continent. Vous pouvez choisir n'importe quelle combinaison de pays et de continents.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Interface

Chaque interface doit être affectée à une *zone de sécurité* ou à un *groupe d'interfaces*. Vous appliquez ensuite votre politique de sécurité sur la base de zones ou de groupes. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe à la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur, par exemple. Certaines politiques ne prennent en charge que les zones de sécurité, tandis que d'autres prennent en charge les zones et les groupes.

Pour plus d'informations sur les objets d'interface, consultez Zones de sécurité et groupes d'interfaces.

Pour ajouter des objets d'interface, consultez Créer des objets de zone de sécurité et de groupe d'interface.

Chaîne de clé

Pour améliorer la sécurité et la protection des données des périphériques, des clés changeantes pour l'authentification des homologues IGP qui ont une durée de 180 jours ou moins sont introduites. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La

modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Les clés pivotantes ne s'appliquent qu'au protocole OSPFv2. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Remarque Seul l'algorithme cryptographique MD5 est utilisé pour l'authentification.

Durée de vie d'une clé

Pour maintenir des communications stables, chaque appareil stocke des clés d'authentification de chaîne de clés et utilise plusieurs clés pour une fonctionnalité à la fois. Basée sur les durées de vie d'envoi et d'acceptation d'une clé, la gestion de la chaîne de clés fournit un mécanisme sécurisé pour gérer le roulement de clé. L'appareil utilise la durée de vie des clés pour déterminer quelles clés d'une chaîne de clés sont actives.

Chaque clé d'une chaîne de clés a deux durées de vie :

- Acceptation de la durée de vie : l'intervalle de temps pendant lequel le périphérique accepte la clé lors de l'échange de clé avec un autre périphérique.
- Durée de vie de l'envoi : intervalle de temps pendant lequel le périphérique envoie la clé lors de l'échange de clé avec un autre périphérique.

Pendant la durée de vie de l'envoi de clé, le périphérique envoie des paquets de mise à jour de routage avec la clé. Le périphérique n'accepte pas les communications d'autres périphériques lorsque la clé envoyée ne fait pas partie de la durée de vie acceptée de la clé sur le périphérique.

Si les durées de vie ne sont pas configurées, cela équivaut à configurer une clé d'authentification MD5 sans échéance.

Sélection de la clé

- Lorsque la chaîne de clés comporte plusieurs clés valides, OSPF sélectionne la clé qui a la durée de vie maximale.
- Une clé ayant une durée de vie infinie est préférée.
- Si les clés ont la même durée de vie, une clé avec l'ID de clé le plus élevé est préférée.

Création d'objets de chaîne de clé

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Key Chain** (Chaîne de clé) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Keychain** (ajouter une chaîne de clés).

Étape 4 Dans la boîte de dialogue Add Key Chaîne Object (ajouter un objet de chaîne de clés), saisissez un nom pour la chaîne de clés dans le champ **Name** (nom).

Le nom du fichier doit commencer par des caractères alphanumériques ou un trait de soulignement (_), suivis de caractères alphanumériques ou spéciaux (-, _, +, .).

Étape 5 Pour ajouter une clé à la chaîne de clés, cliquez sur **Add** (Ajouter).

Étape 6 Précisez l'identifiant de clé dans le champ **Key ID**.

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Étape 7 Les champs **Algorithm** (algorithme) et **Crypto Encryption Type** (type de chiffrement) affichent l'algorithme pris en charge et le type de chiffrement, à savoir respectivement MD5 et Texte brut.

Étape 8 Saisissez le mot de passe dans le champ **Crypto Key String** puis saisissez-le à nouveau dans le champ **Confirm Crypto Key String**.

- La longueur maximale du mot de passe peut être de 80 caractères.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Étape 9 Pour définir l'intervalle de temps pendant lequel un périphérique accepte ou envoie la clé lors de l'échange de clé avec un autre périphérique, fournissez les valeurs de durée de vie dans les champs **Accept Lifetime** et **Send Lifetime** :

Remarque Les valeurs de date et d'heure par défaut sont les fuseaux horaires UTC.

L'heure de fin peut correspondre à la durée absolue à laquelle la durée de vie de l'acceptation/envoi se termine ou n'expire jamais. L'heure de fin par défaut est DateTime.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie respective.

Étape 10 Cliquez sur **Add** (ajouter).

Répétez les étapes 5 à 10 pour créer des clés. Créez un minimum de deux clés pour une chaîne de clés dont les durées de vie se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active.

Étape 11 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 13.

Étape 12 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Réseau

Un objet réseau représente une ou plusieurs adresses IP. Vous pouvez utiliser des objets et des groupes réseau à différents endroits, notamment dans les politiques de contrôle d'accès, les variables réseau, les règles d'identité, les règles de découverte du réseau, les recherches d'événements, les rapports, les politiques d'identité, etc.

Lorsque vous configurez une option qui nécessite un objet réseau, la liste est automatiquement filtrée pour n'afficher que les objets valides pour l'option. Par exemple, certaines options nécessitent des objets hôtes, tandis que d'autres options nécessitent des sous-réseaux.

Un objet réseau peut être de l'un des types suivants :

Hébergement

Une adresse IP unique.

Exemple IPv4 :

```
209.165.200.225
```

Exemple IPv6 :

`2001:DB8::0DB8:800:200C:417A` **ou** `2001:DB8:0:0:0DB8:800:200C:417A`

Plage

Une plage d'adresses IP.

Exemple IPv4 :

```
209.165.200.225-209.165.200.250
```

Exemple IPv6 :

```
2001:db8:0:cd30::1-2001:db8:0:cd30::1000
```

Réseau

Un bloc d'adresses, également appelé sous-réseau.

Exemple IPv4 :

```
209.165.200.224/27
```

Exemple IPv6 :

```
2001:DB8:0:CD30::/60
```

Remarque Security Intelligence ignore les blocs d'adresses IP utilisant un masque de réseau `/0`.

Nom de domaine complet (FQDN)

Un seul nom de domaine complet (FQDN). Vous pouvez limiter la résolution FQDN aux adresses IPv4 uniquement, aux adresses IPv6 uniquement ou aux adresses IPv4 et IPv6. Les FQDN doivent commencer

et se terminer par un chiffre ou une lettre. Seuls les lettres, les chiffres et les traits d'union sont autorisés comme caractères internes dans un FQDN.

Par exemple :

```
www.exemple.com
```

Remarque Vous ne pouvez utiliser les objets FQDN que dans les règles de contrôle d'accès et les règles de préfiltrage, ou les règles NAT manuelles. Les règles correspondent à l'adresse IP obtenue pour le FQDN par une recherche DNS. Pour utiliser un objet réseau FQDN, assurez-vous d'avoir configuré les paramètres du serveur DNS dans Groupe de serveurs DNS, à la page 33 et les paramètres de la plate-forme DNS dans DNS.

vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Groupe

Un groupe d'objets réseau ou d'autres groupes d'objets réseau. Vous pouvez créer des groupes imbriqués en ajoutant un groupe d'objets réseau à un autre groupe d'objets réseau. Vous pouvez imbriquer jusqu'à 10 niveaux de groupes.

Si vous utilisez Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Lorsque vous créez un objet ou un groupe de réseau, l'objet est répliqué à la page **Objets > Objets réseau FTD** dans Cisco Defense Orchestrator et vice-versa.

Vous pouvez utiliser les objets de la page **Objets > Objets réseau FTD** pour spécifier des réseaux lors de la configuration d'autres produits gérés CDO, tels que ASA ou FDM.

Les modifications apportées aux objets ou aux groupes réseau dans l'une ou l'autre des listes sont répercutées dans l'instance de l'objet ou du groupe dans les deux listes. La suppression d'un objet ou d'un groupe dans l'une des listes entraîne également la suppression de l'objet ou du groupe correspondant dans l'autre liste.

Exception : si un objet créé sur la liste CDO porte le même nom qu'un objet existant sur la liste Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), l'objet ne sera pas répliqué sur la liste Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Masque générique de réseau

Vous pouvez créer et gérer des objets masques à caractère générique à partir de la page Object Management (gestion des objets).

Vous pouvez créer des objets réseau avec une adresse IP de sous-réseau étendue. L'objet réseau existant est étendu pour prendre en charge le réseau et les objets à caractère générique de réseau. L'objet réseau qui utilise le masque de caractère générique est répertorié comme **générique de réseau** dans la colonne **Type** de la page de liste des objets de réseau.

Un masque de caractère générique est une adresse IP qui est un masque discontinu de bits. Vous pouvez utiliser des masques contigus pour créer des objets de réseau standard et des masques discontinus pour les objets de réseau avec caractère générique.

Exemple d'adresse IP	Caractère générique de réseau?	Type d'objet
192.0.0.0/8	Non	Réseau

Exemple d’adresse IP	Caractère générique de réseau?	Type d’objet
10.10.0.0/255.255.0.0	Non	Réseau
10.10.0.10/255.255.0.255	Oui	Caractère générique de réseau
72.0.240.10/255.255.240.255	Oui	Caractère générique de réseau

Remarque L’objet de réseau générique et le groupe d’objets, qui contient des objets de réseau de caractère générique, sont autorisés uniquement lors de la configuration des politiques suivantes :

- Politique de préfiltre
- Politique de contrôle d’accès
- Politique NAT

Lignes directrices et limites relatives à la licence

- Pour créer des objets de réseau génériques, dans l’interface utilisateur centre de gestion, choisissez **Objects** > **Object Management** > **Network** (Objets > gestion des objets > Réseau) et cliquez sur **Add Network** (ajouter un réseau), puis sur **Add Object** (ajouter un objet). Sélectionnez l’option **Network** (réseau) et saisissez la valeur comme masque de sous-réseau développé. Exemple : 10.0.10.10/255.255.0.255.
- Le remplacement d’objet, la prise en charge d’objet de groupe, le remplacement d’objet de groupe, les littéraux avec caractère générique et l’importation d’objet avec caractère générique sont pris en charge.
- L’objet de caractère générique de réseau n’est pris en charge que pour les adresses IPv4.
- L’objet de caractère générique de réseau est pris en charge à partir de centre de gestion et Défense contre les menaces versions 7.1.
- Les objets de réseau génériques ne sont pris en charge que pour Snort-3.

Création d'objets réseau

Procédure

Étape 1 Si vous accédez à des objets réseau à partir de CDO, sélectionnez **Objets > Autres objets FTD**.

Étape 2 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 3 Sélectionnez **Réseau** dans la liste des types d'objets.

Étape 4 Sélectionnez **Ajouter un objet** dans le menu déroulant **Ajouter un réseau**.

Étape 5 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d’objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d’un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 6 Vous pouvez également saisir une **Description**.

Étape 7 Dans le champ **Réseau**, sélectionnez l'option requise et saisissez une valeur appropriée; voir Réseau, à la page 48.

Étape 8 (Objets de type FQDN uniquement) Sélectionnez la résolution DNS dans le menu déroulant **Rechercher** pour déterminer si vous souhaitez que les adresses IPv4, IPv6 ou à la fois IPv4 et IPv6 soient associées au FQDN.

Étape 9 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 13.

Étape 10 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Importer des objets réseau

Pour en savoir plus sur l'importation d'objets réseau, consultez Importation d'objets en cours, à la page 5.

Modification et suppression d'objets et de groupes de réseau

Mise en garde Lorsque vous modifiez ou supprimez un objet ou un groupe réseau de la page Object Management (gestion d'objets) dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cette modification modifie ou supprime également l'objet réseau ou le groupe correspondant répliqué dans la page Objets de Cisco Defense Orchestrator. De même, les modifications que vous apportez à ces objets dans la page des objets CDO sont reflétées pour les objets correspondants dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

ICP

Objets PKI pour application SSL

Les objets PKI représentent les certificats de clé publique et les clés privées jumelées nécessaires pour prendre en charge votre déploiement. Les objets d'autorité de certification internes et de confiance sont constitués de certificats d'autorité de certification (CA); Les objets d'autorité de certification internes contiennent également la clé privée associée au certificat. Les objets de certificat internes et externes comprennent des certificats de serveur. les objets de certificat internes contiennent également la clé privée associée au certificat.

Si vous utilisez des objets d'autorité de certification de confiance et des objets de certificat internes pour configurer une connexion à ISE/ISE-PIC, vous pouvez utiliser ISE/ISE-PIC comme source d'identité.

Si vous utilisez des objets de certificat internes pour configurer le portail captif, le système peut authentifier l'identité de votre périphérique de portail captif lors de la connexion aux navigateurs Web des utilisateurs.

Si vous utilisez des objets autorité de certification de confiance pour configurer les domaines, vous pouvez configurer des connexions sécurisées aux serveurs LDAP ou AD.

Si vous utilisez des objets PKI dans les règles SSL, vous pouvez mettre en correspondance le trafic chiffré avec :

- le certificat dans un objet de certificat externe
- un certificat signé par l'autorité de certification dans un objet d'autorité de certification de confiance ou dans la chaîne de confiance de l'autorité de certification

Si vous utilisez des objets PKI dans les règles SSL, vous pouvez déchiffrer :

- trafic sortant en signant de nouveau le certificat du serveur avec un objet d'autorité de certification interne
- le trafic entrant utilisant la clé privée connue dans un objet de certificat interne

Vous pouvez saisir manuellement les informations sur le certificat et la clé, téléverser un fichier contenant ces informations ou, dans certains cas, générer un nouveau certificat d'autorité de certification et une nouvelle clé privée.

Lorsque vous affichez une liste des objets PKI dans le gestionnaire d'objets, le système affiche le nom distinctif du sujet du certificat comme valeur d'objet. Passez votre pointeur sur la valeur pour afficher le nom distinctif du sujet du certificat. Pour afficher d'autres détails de certificats, modifiez l'objet PKI.

Remarque Le centre de gestion et les périphériques gérés chiffrent toutes les clés privées stockées dans les objets d'autorité de certification internes et les objets de certificats internes à l'aide d'une clé générée aléatoirement avant de les enregistrer. Si vous chargez des clés privées protégées par un mot de passe, le périphérique déchiffre la clé à l'aide du mot de passe fourni par l'utilisateur, puis la rechiffre avec la clé générée aléatoirement avant de l'enregistrer.

Objets PKI d'Inscription du certificat

Un Objets d'Inscription du certificat contient les informations sur le serveur de l'Autorité de certification (CA) et les paramètres d'inscription nécessaires pour créer des demandes de signature de certificat (CSR ou Certificate Signing Requests) et obtenir des certificats d'identité de l'Autorité de certification (CA) spécifiée. Ces activités se déroulent dans votre infrastructure à clé privée (PKI ou Private Key Infrastructure).

Le Objets d'Inscription du certificat peut également inclure des informations sur la révocation de certificat. Pour en savoir plus sur l'infrastructure à clé publique, les certificats numériques et l'inscription de certificats, consultez Infrastructure de l'infrastructure PKI et certificats numériques.

Objets Autorité de certification interne

Chaque objet d'autorité de certification (AC) interne que vous configurez représente le certificat de clé publique d'une AC contrôlée par votre organisation. L'objet comprend le nom de l'objet, le certificat de l'autorité de certification et la clé privée jumelée. Vous pouvez utiliser des objets de CA interne dans les règles SSL pour déchiffrer le trafic sortant chiffré en signant à nouveau le certificat de serveur avec la CA interne.

Remarque Si vous faites référence à un objet autorité de certification interne dans une règle SSL **Decrypt - Resign** (Déchiffrer - Resigner) et que la règle correspond à une session chiffrée, le navigateur de l'utilisateur peut avertir que le certificat n'est pas fiable lors de la négociation de l'établissement de liaison SSL. Pour éviter cela, ajoutez le certificat objet d'autorité de certification interne à la liste du client ou du domaine des certificats racine de confiance.

Vous pouvez créer un objet d'autorité de certification interne des manières suivantes :

- importer un certificat d'autorité de certification existant basé sur RSA ou sur une courbe elliptique et une clé privée
- générer un nouveau certificat d'autorité de certification basé sur RSA autosigné et une clé privée
- générer un certificat d'autorité de certification RSA non signé et une clé privée. Vous devez soumettre une requête de signature de certificat (CSR) à une autre autorité de certification pour signer le certificat avant d'utiliser l'objet d'autorité de certification interne.

Après avoir créé un objet d'autorité de certification interne contenant un certificat signé, vous pouvez télécharger le certificat d'autorité de certification et la clé privée. Le système chiffre les certificats téléchargés et les clés privées à l'aide du mot de passe fourni par l'utilisateur.

Qu'il soit généré par le système ou créé par l'utilisateur, vous pouvez modifier le nom interne de l'objet CA, mais vous ne pouvez pas modifier les autres propriétés de l'objet.

Vous ne pouvez pas supprimer un objet d'autorité de certification interne qui est en cours d'utilisation. En outre, après avoir modifié un objet d'autorité de certification interne utilisé dans une politique SSL, la politique de contrôle d'accès associée devient obsolète. Vous devez redéployer la politique de contrôle d'accès pour que vos modifications prennent effet.

Importation de certificats de l'autorité de certification et de clés privées

Vous pouvez configurer un objet d'autorité de certification interne en important un certificat d'autorité de certification X.509 v3 et une clé privée. Vous pouvez téléverser des fichiers codés dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Si le fichier de clé privée est protégé par un mot de passe, vous pouvez fournir le mot de passe de déchiffrement. Si le certificat et la clé sont codés au format PEM, vous pouvez également copier et coller les informations.

Vous pouvez téléverser uniquement des fichiers qui contiennent des informations de certificat ou de clé appropriées et qui sont jumelés. Le système valide la paire avant d'enregistrer l'objet.

Remarque Si vous configurez une règle avec l'action **Déchiffrer - Resigner**, la règle correspond au trafic en fonction du type d'algorithme de signature du certificat interne de l'autorité de certification référencé, en plus des conditions de la règle configurée. Vous devez télécharger un certificat d'autorité de certification basé sur une courbe elliptique pour déchiffrer le trafic sortant chiffré avec un algorithme basé sur une courbe elliptique, par exemple.

Importation d'un certificat d'autorité de certification et d'une clé privée

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Import CA** (Importer AC).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Au-dessus du champ **Certificate Data** (données de certificat), cliquez sur **Browse** (Parcourir) pour télécharger un fichier de certificat d'autorité de certification X.509 v3 codé DER ou PEM.

Étape 6 Au-dessus du champ **Key** (clé), cliquez sur **Parcourir** pour téléverser un fichier de clé privée jumelée codée en DER ou PEM.

Étape 7 Si le fichier téléversé est protégé par un mot de passe, cochez la case **Encrypted, and the password is:** (Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Génération d'un nouveau certificat d'autorité de certification et d'une nouvelle clé privée

Vous pouvez configurer un objet d'autorité de certification interne en fournissant des informations d'identification pour générer un certificat d'autorité de certification RSA autosigné et une clé privée.

Le certificat d'autorité de certification généré est valide pendant dix ans. La date de début de validité est une semaine avant la génération.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Generate CA** (Générer un certificat d'autorité de certification).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Saisissez les attributs d'identification.

Étape 6 Cliquez sur **Générer un CA autosigné**.

Nouveaux certificats signés

Vous pouvez configurer un objet d'autorité de certification interne en obtenant un certificat signé d'une autorité de certification. Cette procédure comporte deux étapes :

- Fournissez les renseignements d'identification pour configurer l'objet autorité de certification interne. Cela génère un certificat non signé et une clé privée jumelée, et crée une requête de signature de certificat (CSR) pour une autorité de certification que vous spécifiez.
- Une fois que l'autorité de certification a émis le certificat signé, chargez-le dans l'objet autorité de certification interne en remplaçant le certificat non signé.

Vous pouvez faire référence à un objet d'autorité de certification interne dans une règle SSL uniquement s'il contient un certificat signé.

Création d'un certificat d'autorité de certification non signé et d'une CSR

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Generate CA** (Générer un certificat d'autorité de certification).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Saisissez les attributs d'identification.

Étape 6 Cliquez sur **Générer une CSR**.

Étape 7 Copiez la requête de signature de certificat (CSR) à soumettre à une autorité de certification.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- Vous devez téléverser un certificat signé émis par une autorité de certification, comme décrit dans la section Téléversement d'un certificat signé émis en réponse à une requête de signature de certificat (CSR), à la page 56

Téléversement d'un certificat signé émis en réponse à une requête de signature de certificat (CSR)

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Une fois téléchargé, le certificat signé peut être référencé dans les règles SSL.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Edit** (✎) à côté de l'objet autorité de certification contenant le certificat non signé en attente de requête de signature de certificat (CSR).

Étape 4 Cliquez sur **Install Certificate** (Installer le certificat).

Étape 5 Cliquez sur **Browse** (Parcourir) pour téléverser un fichier de certificat d'autorité de certification X.509 v3 codé DER ou PEM.

Étape 6 Si le fichier téléchargé est protégé par un mot de passe, cochez la case **Encrypted, and the password is:** (Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 7 Cliquez sur **Save** (Enregistrer) pour téléverser un certificat signé vers l'objet autorité de certification.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Téléchargements de certificats d'autorité de certification et de clés privées

Vous pouvez sauvegarder ou transférer un certificat d'autorité de certification et une clé privée jumelée en téléchargeant un fichier contenant le certificat et les informations de clé à partir d'un objet d'autorité de certification interne.

⚠

Mise en garde Stockez toujours les informations de clé téléchargées dans un emplacement sécurisé.

Le système chiffre la clé privée stockée dans un objet autorité de certification interne avec une clé générée aléatoirement avant de l'enregistrer sur le disque. Si vous téléchargez un certificat et une clé privée à partir d'un objet d'autorité de certification interne, le système déchiffre d'abord les informations avant de créer un fichier contenant les informations sur le certificat et la clé privée. Vous devez ensuite fournir un mot de passe que le système utilise pour chiffrer le fichier téléchargé.

Mise en garde Les clés privées téléchargées dans le cadre d'une sauvegarde du système sont déchiffrées, puis stockées dans le fichier de sauvegarde non chiffré.

Téléchargement d'un certificat d'autorité de certification et d'une clé privée

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Vous pouvez télécharger des certificats d'autorité de certification pour le domaine actuel et les domaines ascendants.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 À proximité de l'objet d'autorité de certification interne dont vous souhaitez télécharger le certificat et la clé privée, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, cliquez sur **Afficher** ( ) pour télécharger le certificat et la clé privée pour un objet dans un domaine ascendant.

Étape 4 Cliquez sur **Télécharger**.

Étape 5 Saisissez un mot de passe de chiffrement dans les champs **Mot de passe** et **Confirmer le mot de passe**.

Étape 6 Cliquez sur **OK**.

Objets autorité de certification approuvée

L'objet Autorité de certification de confiance représente un certificat de clé publique CA appartenant à une CA de confiance. L'objet comprend le nom de l'objet et le certificat de clé publique de l'autorité de certification. Vous pouvez utiliser des objets et des groupes d'autorités de certification externes dans :

- votre politique SSL pour contrôler le trafic chiffré à l'aide d'un certificat signé par l'autorité de certification de confiance ou par toute autorité de certification de la chaîne de confiance.
- vos configurations de domaine pour établir des connexions sécurisées aux serveurs LDAP ou AD.
- votre connexion ISE/ISE-PIC. Sélectionnez des objets Autorité de certification de confiance pour les champs **autorité de certification du serveur pxGrid** et **autorité de certification du serveur MNT**.

Après avoir créé l'objet d'autorité de certification de confiance, vous pouvez modifier le nom et ajouter des listes de révocation de certificats (CRL), mais pas les autres propriétés d'objet. Il n'y a aucune limite au nombre de listes de révocation de certificats que vous pouvez ajouter à un objet. Si vous souhaitez modifier une liste de révocation de certificats que vous avez téléversée vers un objet, vous devez supprimer l'objet et le recréer.

Remarque L'ajout d'une liste de révocation de certificats à un objet n'a aucun effet lorsque l'objet est utilisé dans votre configuration d'intégration ISE/ISE-PIC.

Vous ne pouvez pas supprimer un objet d'autorité de certification de confiance qui est en cours d'utilisation. En outre, après avoir modifié un objet d'autorité de certification de confiance en cours d'utilisation, la politique de contrôle d'accès associée devient obsolète. Vous devez redéployer la politique de contrôle d'accès pour que vos modifications prennent effet.

Objet autorité de certification de confiance

Vous pouvez configurer un objet d'autorité de certification externe en téléchargeant un certificat d'autorité de certification X.509 v3. Vous pouvez téléverser un fichier codé dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Si le fichier est protégé par un mot de passe, vous devez fournir le mot de passe de déchiffrement. Si le certificat est encodé au format PEM, vous pouvez également copier et coller les informations.

Vous pouvez télécharger un certificat d'autorité de certification uniquement si le fichier contient les informations appropriées sur le certificat; le système valide le certificat avant d'enregistrer l'objet.

Ajout d'un objet autorité de certification de confiance

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Trusted CAs** (Autorités de certification de confiance).

Étape 3 Cliquez sur **Add Trusted CAs** (Ajouter des autorités de certification de confiance).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Cliquez sur **Browse** (Parcourir) pour téléverser un fichier de certificat d'autorité de certification X.509 v3 codé DER ou PEM.

Étape 6 Si le fichier est protégé par un mot de passe, cochez la case **Encrypted, and the password is:**(Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Listes de révocation de certificats des objets d'autorité de certification de confiance

Vous pouvez téléverser des listes de révocation de certificats (CRL) vers un objet d'autorité de certification de confiance. Si vous faites référence à cet objet d'autorité de certification de confiance dans une politique SSL, vous pouvez contrôler le trafic chiffré en fonction du fait que l'autorité de certification qui a émis le certificat de chiffrement de session a révoqué le certificat par la suite. Vous pouvez téléverser des fichiers codés dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Après avoir ajouté la liste de révocation de certificats, vous pouvez afficher la liste des certificats révoqués. Si vous souhaitez modifier une liste de révocation de certificats que vous avez téléversée vers un objet, vous devez supprimer l'objet et le recréer.

Vous pouvez téléverser uniquement des fichiers qui contiennent une liste de révocation de certificats appropriée. Il n'y a aucune limite au nombre de listes de révocation de certificats que vous pouvez ajouter à un objet d'autorité de certification de confiance. Cependant, vous devez enregistrer l'objet chaque fois que vous téléversez une liste de révocation de certificats avant d'ajouter une autre liste de révocation de certificats.

Remarque L'ajout d'une liste de révocation de certificats à un objet n'a aucun effet lorsque l'objet est utilisé dans votre configuration d'intégration ISE/ISE-PIC.

Ajout d'une liste de révocation de certificats à un objet d'autorité de certification de confiance

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Remarque L'ajout d'une liste de révocation de certificats à un objet n'a aucun effet lorsque l'objet est utilisé dans votre configuration d'intégration ISE/ISE-PIC.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Trusted CAs** (Autorités de certification de confiance).

Étape 3 Cliquez sur **Edit** (✎) à côté d'un objet autorité de certification de confiance.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Add CRL** (ajouter une CRL) pour téléverser un fichier CRL codé en DER ou PEM.

Étape 5 Cliquez sur **OK**.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Objets de certificat externe

L'objet de certificat externe représente un certificat de clé publique de serveur qui n'appartient pas à votre organisation. L'objet comprend le nom de l'objet et le certificat. Vous pouvez utiliser des objets de certificat externes dans les règles SSL pour contrôler le trafic chiffré avec le certificat du serveur. Par exemple, vous pouvez téléverser un certificat de serveur autosigné en qui vous avez confiance, mais que vous ne pouvez pas vérifier par un certificat d'autorité de certification de confiance.

Vous pouvez configurer un objet de certificat externe en téléversant un certificat de serveur X.509 v3. Vous pouvez téléverser un fichier dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Vous pouvez téléverser uniquement des fichiers qui contiennent des informations correctes sur le certificat de serveur. le système valide le fichier avant d'enregistrer l'objet. Si le certificat est encodé au format PEM, vous pouvez également copier et coller les informations.

Ajout d'objets de certificat externes

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **External Certs** (Certificats externes).

Étape 3 Cliquez sur **Add External Certs** (Ajouter des certificats externes).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Au-dessus du champ **Certificate Data** (données de certificat), cliquez sur **Browse** (parcourir) pour téléverser un fichier de certificat de serveur X.509 v3 codé en DER ou PEM.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Objets de certificat interne

Chaque objet de certificat interne que vous configurez représente un certificat de clé publique de serveur appartenant à votre organisation. L'objet comprend le nom de l'objet, le certificat de clé publique et une clé privée jumelée. Vous pouvez utiliser des objets et des groupes de certificats internes dans :

- vos règles SSL pour déchiffrer le trafic entrant dans l'un des serveurs de votre organisation à l'aide de la clé privée connue.
- votre connexion ISE/ISE-PIC. Sélectionnez un objet de certificat interne pour le champ **MC Server Certificate** (Certificat du serveur MC).
- votre configuration de portail captif pour authentifier l'identité de votre périphérique de portail captif lors de la connexion aux navigateurs Web des utilisateurs. Sélectionnez un objet de certificat interne pour le champ **Server Certificate** (certificat de serveur).

Vous pouvez configurer un objet de certificat interne en téléchargeant un certificat de serveur X.509 v3 basé sur RSA ou sur la courbe elliptique et une clé privée appariée. Vous pouvez téléverser un fichier dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Si le fichier est protégé par un mot de passe, vous devez fournir le mot de passe de déchiffrement. Si le certificat et la clé sont codés au format PEM, vous pouvez également copier et coller les informations.

Vous pouvez téléverser uniquement des fichiers qui contiennent des informations de certificat ou de clé appropriées et qui sont jumelés. Le système valide la paire avant d'enregistrer l'objet.

Après avoir créé l'objet de certificat interne, vous pouvez modifier le nom, mais pas les autres propriétés de l'objet.

Vous ne pouvez pas supprimer un objet de certificat interne qui est en cours d'utilisation. En outre, après avoir modifié un objet de certificat interne qui est en cours d'utilisation, la politique de contrôle d'accès associée devient obsolète. Vous devez redéployer la politique de contrôle d'accès pour que vos modifications prennent effet.

Ajout d'objets de certificat externes

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal Certs** (Certificats internes).

Étape 3 Cliquez sur **Add Internal Certs** (Ajouter des certificats internes).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Au-dessus du champ **Certificate Data** (données de certificat), cliquez sur **Browse** (parcourir) pour téléverser un fichier de certificat de serveur X.509 v3 codé en DER ou PEM.

Étape 6 Au-dessus du champ **Key** (clé), ou cliquez sur **Parcourir** pour téléverser un fichier de clé privée jumelée codé en DER ou PEM.

Étape 7 Si le fichier de clé privée téléversé est protégé par un mot de passe, cochez la case **Encrypted, and the password is:** (Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 8 Cliquez sur **Save** (enregistrer).

Objets d'Inscription du certificat

Les points de confiance vous permettent de gérer et de suivre les autorités de certification et les certificats. Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de configuration spécifiques à l'autorité de certification et une association avec un certificat d'identité inscrit.

Un Objets d'Inscription du certificat contient les informations sur le serveur de l'Autorité de certification (CA) et les paramètres d'inscription nécessaires pour créer des demandes de signature de certificat (CSR ou Certificate Signing Requests) et obtenir des certificats d'identité de l'Autorité de certification (CA) spécifiée. Ces activités se déroulent dans votre infrastructure à clé privée (PKI ou Private Key Infrastructure).

Le Objets d'Inscription du certificat peut également inclure des informations sur la révocation de certificat. Pour en savoir plus sur l'infrastructure à clé publique, les certificats numériques et l'inscription de certificats, consultez Infrastructure de l'infrastructure PKI et certificats numériques.

Comment utiliser les Objets d'Inscription du certificat

Objets d'Inscription du certificatLes commandes servent à inscrire vos périphériques gérés dans votre infrastructure à clé publique et à créer des points de confiance (objets d'autorité de certification) sur les périphériques qui prennent en charge les connexions VPN en procédant comme suit :

1. Définir les paramètres pour l'authentification et l'inscription d'une autorité de certification dans une Objets d'Inscription du certificat. Précisez les paramètres partagés et utilisez la fonction de remplacement pour spécifier un paramètre d'objet unique pour différents périphériques.
2. Associez et installez cet objet sur chaque périphérique géré nécessitant le certificat d'identité. Sur le périphérique, il devient un *point de confiance*.

   Lorsqu'un Objets d'Inscription du certificat est associé à un périphérique, puis installé sur celui-ci, le processus d'inscription de certificat démarre immédiatement. Le processus est automatique pour les types d'inscription de fichiers autosignés, SCEP, EST et PKCS12, ce qui signifie qu'il ne nécessite aucune action supplémentaire de l'administrateur. L'inscription manuelle de certificats nécessite une action supplémentaire de l'administrateur.
3. Précisez le point de confiance créé dans votre configuration VPN.

Gestion des Objets d'Inscription du certificat

Pour gérer des Objets d'Inscription du certificat, accédez à **Objects > Object Management** (gestion des objets), puis dans le volet de navigation, sélectionnez **PKI > Cert Enrollment** (Inscription des certificats). Les informations suivantes sont affichées :

- Les Objets d'Inscription du certificatexistants sont répertoriés dans la colonne **Name** (nom).

  Utilisez le champ de recherche (la loupe) pour filtrer la liste.

- Le type d'inscription de chaque objet est affiché dans la colonne **Type**. Les méthodes d'inscription suivantes peuvent être utilisées :
  - **Autosigné** : le périphérique géré génère son propre certificat racine autosigné.
  - **EST** : l'inscription sur le transport sécurisé est utilisée par le périphérique pour obtenir un certificat d'identité de l'autorité de certification.
  - **SCEP** : (par défaut) le protocole Simple Certificate Enrollment Protocol est utilisé par le périphérique pour obtenir un certificat d'identité de l'autorité de certification.
  - **Manuel** : l'inscription est effectuée manuellement par l'administrateur.
  - **Fichier PKCS12** : importez un fichier PKCS12 sur un périphérique géré par Firepower Threat Defense qui prend en charge la connectivité VPN. Un fichier PKCS#12, PFX ou P12 contient le certificat du serveur, tous les certificats intermédiaires et la clé privée dans un seul fichier chiffré. Saisissez la valeur de la **phrase secrète** pour le déchiffrement.
- La colonne **Override** (Remplacement) indique si l'objet autorise les remplacements (coche verte) ou non (X rouge). Si un nombre s'affiche, il s'agit du nombre de remplacements en place.

  Utilisez l'option Override (Remplacer) pour personnaliser les paramètres d'objet pour chaque périphérique qui fait partie de la configuration VPN. Le remplacement rend les détails des points de confiance de chaque périphérique uniques. En règle générale, le nom ou l'objet commun est remplacé pour chaque périphérique dans la configuration VPN.

  Consultez Mises en priorité d'objets, à la page 11 pour obtenir plus de détails et de procédures sur le remplacement d'objets de tout type.
- **Modifiez** un Objets d'Inscription du certificat déjà créé en cliquant sur l'icône de modification (un crayon). La modification ne peut être effectuée que si l'objet d'inscription n'est associé à aucun appareil géré. Consultez les instructions d'ajout pour modifier un Objets d'Inscription du certificat. Les objets d'inscription ayant échoué peuvent être modifiés.
- **Supprimez** un Objets d'Inscription du certificat créé précédemment en cliquant sur l'icône de suppression (une corbeille). Vous ne pouvez pas supprimer un Objets d'Inscription du certificat s'il est associé à un périphérique géré.

Appuyez sur **(+) Add Cert Enrollment** (Ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** pour configurer un Objets d'Inscription du certificat, voir Ajout d'objets d'Inscription du certificat, à la page 63. Installez ensuite le certificat sur chaque périphérique de tête de réseau géré.

Sujets connexes

Installation d'un certificat à l'aide de l'inscription autosignée
Installation d'un certificat à l'aide de l'inscription EST
Installation d'un certificat à l'aide de l'inscription SCEP
Installation d'un certificat à l'aide de l'inscription manuelle
Installation d'un certificat à l'aide d'un fichier PKCS12

Ajout d'objets d'Inscription du certificat

Vous pouvez utiliser ces objets avec des périphériques défense contre les menaces . Vous devez avoir des privilèges d'administrateur ou d'administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Ouvrez la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de Cert) :

- Directement à partir de la gestion des objets : dans l'écran **Objects > Object Management** (gestion des objets), choisissez **PKI > Cert Enrollment** (PKI > Inscription des certificats) dans le volet de navigation et appuyez sur **Add Cert Enrollment**(ajouter une inscription de certificat).
- Lors de la configuration d'un périphérique géré : dans l'écran **Devices (périphériques) > Certificates (certificats)**, choisissez **Add > Add New Certificate** (ajouter un nouveau certificat), puis cliquez sur **(+)** dans le champ **Certificate Enrollment** (inscription de certificat).

Étape 2 Saisissez le **Nom** et éventuellement une **description** de cet objet d'inscription.

Une fois l'inscription terminée, ce nom est le nom du point de confiance sur les périphériques gérés auxquels il est associé.

Étape 3 Ouvrez l'onglet **CA Information** (renseignements de l'autorité de certification) et sélectionnez **Enrollment Type** (Type d'inscription).

- **Self-signed Certificate** (Certificat autosigné) : le périphérique géré, agissant en tant qu'autorité de certification, génère son propre certificat racine autosigné. Aucune autre information n'est nécessaire dans ce volet.

  Remarque Lors de l'inscription d'un certificat autosigné, vous devez préciser le Common Name (CN) dans les paramètres de certificat.

- **EST** : inscription sur le protocole de transport sécurisé. Précisez les informations EST. Consultez Options EST Objets d'Inscription du certificat, à la page 65.
- **SCEP** : (valeur par défaut) Protocole d'inscription de certificat simple Précisez les informations SCEP. Consultez Options SCEP Objets d'Inscription du certificat, à la page 66.
- **Manuel**
  - **CA Only** : cochez cette case pour créer uniquement le certificat de l'autorité de certification de l'autorité de certification sélectionnée. Un certificat d'identité ne sera pas créé pour ce certificat.

    Si vous ne cochez pas cette case, un certificat d'autorité de certification n'est pas obligatoire. Vous pouvez générer la requête de signature de certificat (CSR) sans avoir de certificat d'autorité de certification et obtenir le certificat d'identité.

  - **CA Certificate**(certificat de l'autorité de certification) : collez les informations sur le certificat de l'autorité de certification dans la zone. Vous pouvez également obtenir un certificat d'autorité de certification en le copiant à partir d'un autre périphérique.

    Vous pouvez laisser cette case vide si vous choisissez de générer une requête de signature de certificat (CSR) sans le certificat de l'autorité de certification.

- **Fichier PKCS12** : importez un fichier PKCS12 sur un périphérique géré défense contre les menaces qui prend en charge la connectivité VPN. Un fichier PKCS#12, ou PFX, contient un certificat de serveur, des certificats intermédiaires et une clé privée dans un seul fichier chiffré. Saisissez la valeur de la **phrase secrète** pour le déchiffrement.
- **Skip Check for CA flag in basic constraints of the CA Certificate** (Ignorer la vérification de l'indicateur de l'autorité de certification dans les contraintes de base du certificat de l'autorité de certification) : cochez cette case si vous souhaitez ignorer la vérification de l'extension des contraintes de base et de l'indicateur de l'autorité de certification dans un certificat de point de confiance.

- **Validation Usage** : choisissez parmi les options pour valider le certificat lors d'une connexion VPN.
  - **IPsec Client** : validez le certificat de la connexion VPN entrante IPsec site vers site.
  - **SSL Client** : validez un certificat client SSL lors d'une tentative de connexion VPN d'accès à distance.
  - **SSL Server** : sélectionnez cette option pour valider un certificat de serveur SSL, par exemple en tant que certificat de serveur Cisco Umbrella.

Étape 4 (Facultatif) Ouvrez l'onglet **Certificate Settings** (paramètres de certificat) et spécifiez le contenu du certificat. Consultez Paramètres de certificat Objets d'Inscription du certificat, à la page 67.

Ces informations sont placées dans le certificat et sont lisibles par tout tiers qui reçoit le certificat du routeur.

Étape 5 (Facultatif) Ouvrez l'onglet **Key** (clé) et spécifiez les informations de clé. Consultez Options de la clé Objets d'Inscription du certificat, à la page 68.

Étape 6 (Facultatif) Cliquez sur l'onglet **Revocation** (révocation) et spécifiez les options de révocation : Voir Options de révocation Objets d'Inscription du certificat, à la page 70.

Étape 7 **Autorisez les remplacements** de cet objet si vous le souhaitez. Consultez Mises en priorité d'objets, à la page 11 pour obtenir une description complète des remplacements d'objets.

Prochaine étape

Associez et installez l'objet d'inscription sur un appareil pour créer un point de confiance sur cet appareil.

Sujets connexes

Installation d'un certificat à l'aide de l'inscription autosignée
Installation d'un certificat à l'aide de l'inscription EST
Installation d'un certificat à l'aide de l'inscription SCEP
Installation d'un certificat à l'aide de l'inscription manuelle
Installation d'un certificat à l'aide d'un fichier PKCS12

Options EST Objets d'Inscription du certificat

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objets) > **Object Management**(gestion des objets), puis dans le volet de navigation sélectionnez **PKI** > **Cert Enrollment** (Inscription du certificat). Cliquez sur **(+) Add Cert Enrollment** (Ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat), puis sélectionnez l'onglet **CA Information** (Information de l'autorité de certification).

Champs

Enrollment Type (type d'inscription) : défini sur **EST**.

Remarque

- Le type d'inscription EST ne prend pas en charge la clé EdDSA.
- La capacité d'EST à inscrire automatiquement un périphérique à l'expiration de son certificat n'est pas prise en charge.

URL d'inscription : l'URL du serveur d'autorité de certification auquel les périphériques doivent tenter de s'inscrire.

Utilisez une URL HTTPS sous la forme **https://nom_CA:port**, où *nom_CA* est le nom DNS de l'hôte ou l'adresse IP du serveur de l'autorité de certification. Le numéro de *port* est obligatoire.

Username : nom d'utilisateur pour accéder au serveur de l'autorité de certification.

Password/Confirm Password (mot de passe/confirmation du mot de passe) : le mot de passe pour accéder au serveur de l'autorité de certification.

Fingerprint (Empreinte) : lors de la récupération du certificat de l'autorité de certification à l'aide d'EST, vous pouvez saisir l'empreinte pour le serveur d'autorité de certification. L'utilisation de l'empreinte pour vérifier l'authenticité du certificat du serveur d'autorité de certification permet d'éviter qu'un tiers non autorisé ne le remplace par un faux certificat. Saisissez l'**empreinte** pour le serveur d'autorité de certification au format hexadécimal. Si la valeur que vous saisissez ne correspond pas à l'empreinte sur le certificat, le certificat est rejeté. Obtenez l'empreinte de l'autorité de certification en contactant directement le serveur.

Interface source : l'interface qui interagit avec le serveur de l'autorité de certification. Par défaut, l'interface de dépistage s'affiche. Pour configurer une interface de données comme interface source, choisissez la zone de sécurité ou l'objet de groupe d'interfaces respectif.

Ignore EST Server Certificate Validations (Ignorer les validations du certificat du serveur EST) : la validation du certificat du serveur EST est effectuée par défaut. Cochez la case si vous voulez ignorer la validation par FTD du certificat du serveur EST.

Options SCEP Objets d'Inscription du certificat

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Cliquez sur **(+) Add Cert Enrollment** (Ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat), puis sélectionnez l'onglet **CA Information** (Information de l'autorité de certification).

Champs

Enrollment Type (type d'inscription) : défini sur **SCEP**.

URL d'inscription : l'URL du serveur d'autorité de certification auquel les périphériques doivent tenter de s'inscrire.

Utilisez une URL HTTP sous la forme **`http://nom_CA:port,`** où nom_CA est le nom DNS de l'hôte ou l'adresse IP du serveur de l'autorité de certification. Le numéro de port est obligatoire.

Remarque Si le serveur SCEP est référencé avec le nom d'hôte/Nom de domaine complet FQDN, configurez le serveur DNS à l'aide de l'objet FlexConfig.

Si l'emplacement du script cgi-bin de l'autorité de certification n'est pas celui par défaut (/cgi-bin/pkiclient.exe), vous devez également inclure l'emplacement du script non standard dans l'URL, sous la forme http://CA_name:port/script_location, où script_location est le chemin d'accès complet aux scripts de l'autorité de certification.

Mettre en doute le mot de passe/Confirmer le mot de passe : le mot de passe utilisé par le serveur d'autorité de certification pour valider l'identité du périphérique. Vous pouvez obtenir le mot de passe en contactant directement le serveur d'autorité de certification ou en saisissant l'adresse suivante dans un navigateur Web : **`http://URLHostName/certsRV/mscep/mscept.dll`**. Le mot de passe est valide pendant 60 minutes à partir du moment où vous l'obtenez du serveur d'autorité de certification. Par conséquent, il est important que vous déployiez le mot de passe dès que possible après sa création.

Période de nouvelle tentative : intervalle entre les tentatives de demande de certificat, en minutes. La valeur peut être comprise entre 1 et 60 minutes. La valeur par défaut est de 1 minute .

Nombre de tentatives : le nombre de tentatives à effectuer si aucun certificat n'est émis lors de la première demande. La valeur peut être comprise entre 1 et 100. La valeur par défaut est 10.

Source du certificat de l'autorité de certification : précisez comment le certificat de l'autorité de certification sera obtenu.

- **Récupérer à l'aide de SCEP** (option par défaut et seule option prise en charge) : récupérez le certificat du serveur de l'autorité de certification à l'aide du processus Simple Certificate Enrollment Process (SCEP). L'utilisation de SCEP nécessite une connexion entre votre périphérique et le serveur de l'autorité de certification. Assurez-vous qu'il existe une voie de routage entre votre appareil et le serveur de l'autorité de certification avant de commencer le processus d'inscription.

Empreinte : lors de la récupération du certificat de l'autorité de certification à l'aide de SCEP, vous pouvez saisir l'empreinte pour le serveur d'autorité de certification. L'utilisation de l'empreinte pour vérifier l'authenticité du certificat du serveur d'autorité de certification permet d'éviter qu'un tiers non autorisé ne le remplace par un faux certificat. Saisissez l'**empreinte** pour le serveur d'autorité de certification au format hexadécimal. Si la valeur que vous saisissez ne correspond pas à l'empreinte sur le certificat, le certificat est rejeté. Obtenez l'empreinte de l'autorité de certification en contactant directement le serveur ou en saisissant l'adresse suivante dans un navigateur Web : **`http://<URLHostName>/certsrv/mscep/mscep.dll`**.

Paramètres de certificat Objets d'Inscription du certificat

Préciser les informations supplémentaires dans les demandes de certificat envoyées au serveur de l'autorité de certification. Ces renseignements sont placés dans le certificat et peuvent être consultés par toute partie qui reçoit le certificat du routeur.

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Appuyez sur **(+) Add Cert Enrollment** (ajouter une inscription de Certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de Certificat), puis sélectionnez l'onglet **Certificate Settings** (paramètres du certificat).

Champs

Saisissez toutes les informations au format LDAP standard X.500.

- **Inclure FQDN** : Indique si l'on doit inclure le nom de domaine complet (FQDN) du périphérique dans la demande de certificat. Les options sont:
  - **Utiliser le nom d'hôte du périphérique comme nom de domaine complet**
  - **Ne pas utiliser le nom de domaine complet dans le certificat**
  - **Nom de domaine complet FQDN personnalisé** : sélectionnez cette option, puis spécifiez-la dans le champ **FQDN personnalisé** qui s'affiche.
- **Inclure l'adresse IP du périphérique** : l'interface dont l'adresse IP est incluse dans la demande de certificat.
- **Common Name (CN)** : nom commun X.500 à inclure dans le certificat.

Remarque Lors de l'inscription d'un certificat autosigné, vous devez préciser le Common Name (CN) dans les paramètres de certificat.

- **Unité organisationnelle (OU)** : nom de l'unité organisationnelle (par exemple, le nom d'un service) à inclure dans le certificat.
- **Organization (O)** : nom de l'organisation ou de l'entreprise à inclure dans le certificat.
- **Localité (L)** : la localité à inclure dans le certificat.
- **État (ST)** : État ou province à inclure dans le certificat.
- **Code pays(C)** : le pays à inclure dans le certificat. Ces codes sont conformes aux abréviations de pays ISO 3166, par exemple « US » pour les États-Unis d'Amérique.
- **Adresse courriel (E)** : l'adresse courriel à inclure dans le certificat.
- **Inclure le numéro de série du périphérique** : indique si oui ou non inclure le numéro de série du périphérique dans le certificat. L'autorité de certification utilise le numéro de série pour authentifier les certificats ou pour associer ultérieurement un certificat à un périphérique particulier. En cas de doute, incluez le numéro de série, car il est utile à des fins de débogage.

Options de la clé Objets d'Inscription du certificat

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Appuyez sur **(+) Add Cert Enrollment** (ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de Certificat), puis sélectionnez l'onglet **Key** (clé).

Champs

- **Type de clé** : RSA, ECDSA, EdDSA.

Remarque

- Pour le type d'inscription EST, ne sélectionnez pas la clé EdDSA, car elle n'est pas prise en charge.
- EdDSA est prise en charge uniquement dans les topologies VPN de site à site.
- EdDSA n'est pas prise en charge en tant que certificat d'identité pour le VPN d'accès à distance.

- **Key Name** (nom de clé) : si la paire de clés que vous souhaitez associer au certificat existe déjà, ce champ spécifie le nom de cette paire de clés. Si la paire de clés n'existe pas, ce champ spécifie le nom à attribuer à la paire de clés qui sera générée lors de l'inscription. Si vous ne spécifiez aucun nom, la paire de clés du nom de domaine complet (FQDN) est utilisée à la place.
- **Key Size** (taille de clé) : si la paire de clés n'existe pas, définit la taille de clé souhaitée (module), en bits. La taille recommandée est de 2048 bits. Plus la taille du module est grande, plus la clé est sécurisée. Cependant, les clés avec des tailles de module plus grandes prennent plus de temps à être générées (une minute ou plus lorsqu'elles sont supérieures à 512 bits) et plus de temps à traiter lorsqu'elles sont échangées.

Important

- Dans les versions 7.0 et ultérieures de centre de gestion et défense contre les menaces , vous ne pouvez pas inscrire de certificats avec des tailles de clé RSA inférieures à 2 048 bits et des clés SHA-1 avec l'algorithme de chiffrement RSA. Cependant, vous pouvez utiliser l'Inscription des certificats par l'infrastructure de clé publique de (PKI) avec chiffrement faible pour autoriser les certificats qui utilisent SHA-1 avec l'algorithme de chiffrement RSA et une taille de clé inférieure.
- Vous ne pouvez pas générer de clés RSA avec des tailles inférieures à 2 048 bits pour défense contre les menaces 7.0, même lorsque vous activez l'option de chiffrement faible.

- **Paramètres avancés** : sélectionnez **Ignorer l'utilisation de la clé IPsec** si vous ne souhaitez pas valider les valeurs des extensions d'utilisation de la clé et d'utilisation de la clé étendue des certificats de clients distants IPsec. Vous pouvez supprimer la vérification de l'utilisation des clés sur les certificats clients IPsec. Par défaut, cette option n'est pas activée.

Remarque Pour les connexions VPN de site à site, si vous utilisez une autorité de certification (CA) Windows, l'extension des politiques d'application par défaut est **intermédiaire IKE de sécurité IP**. Si vous utilisez ce paramètre par défaut, vous devez sélectionner l'option **Ignore IPsec Key Usage** (Ignorer l'utilisation de la clé IPsec) pour l'objet que vous sélectionnez. Sinon, les points terminaux ne peuvent pas établir la connexion VPN de site à site.

Inscription des certificats par l'infrastructure de clé publique de (PKI) avec chiffrement faible

L'algorithme de signature de hachage SHA-1 et les tailles de clé RSA inférieures à 2048 bits pour la certification ne sont pas prises en charge par les versions 7.0 et ultérieures de centre de gestion et défense contre les menaces . Vous ne pouvez pas inscrire de certificats dont la taille de clé RSA est inférieure à 2048 bits.

Pour remplacer ces restrictions sur les versions antérieures à 7.0 de défense contre les menaces centre de gestion7.0 , vous pouvez utiliser l'option Enablelow-crypto sur défense contre les menaces . Nous vous déconseillons d'autoriser les clés au chiffrement faible, car ces clés ne sont pas aussi sécurisées que celles dont la taille est plus élevée.

Remarque La version 7.0 ou ultérieure de Défense contre les menaces ne prend pas en charge la génération de clés RSA avec des tailles inférieures à 2048 bits, même lorsque vous autorisez le chiffrement faible.

Pour activer le chiffrement faible sur le périphérique, accédez à la page **Périphériques > Certificats**. Cliquez sur le bouton **Enable Weak-Crypto** ( ) (Autoriser le chiffrement faible) pour le périphérique défense contre les menaces . Lorsque l'option chiffrement faible est activée, le bouton se change en . Par défaut, cette option est désactivée.

Remarque Lorsqu'une inscription de certificat échoue en raison d'un chiffrement faible, centre de gestion affiche un message d'avertissement vous invitant à activer l'option chiffrement faible. De même, lorsque vous activez le bouton d'activation du chiffrement faible, centre de gestion affiche un message d'avertissement avant d'activer la configuration du chiffrement faible sur le périphérique.

Mise à niveau de versions antérieures à Défense contre les menaces 7.0

Lorsque vous effectuez une mise à niveau vers défense contre les menaces 7.0, les configurations de certificat existantes sont conservées. Cependant, si ces certificats ont des clés RSA inférieures à 2048 bits et utilisent l'algorithme de chiffrement SHA-1, ils ne peuvent pas être utilisés pour établir des connexions VPN. Vous devez soit vous procurer un certificat avec des tailles de clé RSA supérieures à 2048 bits, soit activer l'option allow faible-crypto (autoriser le chiffrement faible) pour les connexions VPN.

Options de révocation Objets d'Inscription du certificat

Précisez s'il faut vérifier l'état de révocation d'un certificat en sélectionnant et en configurant la méthode. La vérification de la révocation est désactivée par défaut, et aucune des méthodes (CRL ou OCSP) n'est vérifiée.

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Appuyez sur **(+) Add Cert Enrollment** (ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat), puis sélectionnez l'onglet **Revocation** (Révocation).

Champs

- **Enable Certificate Revocation Lists** (Activer les listes de révocation de certificats (CRL)) : cochez cette case pour activer la vérification des CRL.

- **Use CRL distribution point from the certificate** (utiliser le point de distribution des CRL du certificat) : cochez cette case pour obtenir l'URL de distribution des listes de révocation à partir du certificat.
- **Use static URL configured** (Utiliser une URL statique configurée) : cochez cette case pour ajouter une URL de distribution statique et prédéfinie pour les listes de révocation. Ajoutez ensuite les URL.

  CRL Server URLs (URL du serveur de CRL) : L'URL du serveur LDAP à partir duquel les CRL peuvent être téléchargées.

  Ces URL doivent commencer par **`http://`**. Incluez un numéro de port dans l'URL.

- **Enable Online Certificate Status Protocol (OCSP)** (Activer le protocole d'état des certificats en ligne (OCSP)) : cochez cette case pour activer la vérification OCSP.

  OCSP Server URL : URL du serveur OCSP qui vérifie la révocation si vous avez besoin de vérifications OCSP.

  Ces URL doivent commencer par **`http://`**.

- **Considérer le certificat comme valide si les informations de révocation ne sont pas accessibles** : cochée par défaut. Décochez la case si vous ne souhaitez pas autoriser cela.

Remarque La case à cocher **Considérer le certificat comme valide si les informations de révocation ne sont pas accessibles** n'a aucun effet sur les périphériques défense contre les menaces exécutant la version 6.5 ou ultérieure.

Liste des stratégies

Utilisez la page Configure Policy List (Configurer la liste des politiques) pour créer, copier et modifier des objets de politique de liste de politiques. Vous pouvez créer des objets de liste de politiques à utiliser lorsque vous configurez des cartes de routage. Lorsqu'une liste de stratégie est référencée dans une carte de routage, toutes les déclarations de correspondance dans la liste de stratégie sont évaluées et traitées. Deux listes de politiques ou plus peuvent être configurées avec une carte de routage. Une liste de politiques peut également coexister avec d'autres instructions de mise en correspondance et d'ensemble préexistantes configurées dans la même carte de routage, mais en dehors de la liste de politiques. Lorsque plusieurs listes de politiques effectuent la mise en correspondance dans une entrée de carte de routage, toutes les listes de politiques correspondent uniquement à l'attribut entrant.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets),** puis **Policy List** (liste de politiques) dans la table des matières.

Étape 2 Cliquez sur **Add Policy List** (ajouter une liste des politiques).

Étape 3 Saisissez un nom pour l'objet de liste de politiques dans le champ **Name** (Nom). Les noms des objets sont sensibles à la casse.

Étape 4 Sélectionnez si vous souhaitez autoriser ou bloquer l'accès aux conditions de correspondance dans la liste déroulante **Action**.

Étape 5 Cliquez sur l'onglet **Interface** pour distribuer les routages qui ont leur prochain saut hors de l'une des interfaces spécifiées.

Dans la liste **Zones/Interfaces**, ajoutez les zones qui contiennent les interfaces par lesquelles le périphérique communique avec le poste de gestion. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste des **Selected Zones/Interface**(Zones d'interface sélectionnées) et l'ajouter en cliquant sur **Add** (Ajouter). L'hôte ne sera configuré sur un périphérique que si ce dernier comprend les interfaces ou les zones sélectionnées.

Étape 6 Cliquez sur l'onglet **Address** pour redistribuer toutes les routes dont l'adresse de destination est autorisée par une liste d'accès ou une liste de préfixes standard.

Choisissez si vous souhaitez utiliser une **liste d'accès** ou une **liste de préfixes** pour la mise en correspondance, puis saisissez les objets ou sélectionnez les objets de liste d'accès standard ou de préfixe que vous souhaitez utiliser pour la mise en correspondance.

Étape 7 Cliquez sur l'onglet **Next Hop** (saut suivant) pour redistribuer toutes les routes pour lesquelles une adresse de routeur de saut suivant a été transmise par l'une des listes d'accès ou des listes de préfixes spécifiées.

Choisissez si vous souhaitez utiliser une **liste d'accès** ou une **liste de préfixes** pour la mise en correspondance, puis saisissez les objets ou sélectionnez les objets de liste d'accès standard ou de préfixe que vous souhaitez utiliser pour la mise en correspondance.

Étape 8 Cliquez sur l'onglet **Route Source** pour redistribuer les routages qui ont été annoncés par les routeurs et les serveurs d'accès à l'adresse spécifiée par les listes d'accès ou la liste de préfixes.

Choisissez si vous souhaitez utiliser une **liste d'accès** ou une **liste de préfixes** pour la mise en correspondance, puis saisissez les objets ou sélectionnez les objets de liste d'accès standard ou de préfixe que vous souhaitez utiliser pour la mise en correspondance.

Étape 9 Cliquez sur l'onglet **AS Path** pour faire correspondre un chemin de système autonome de BGP. Si vous spécifiez plus d'un chemin AS, la voie de routage peut correspondre à l'un ou l'autre des chemins AS.

Étape 10 Cliquez sur l'onglet **Community Rule** (Règle de communauté) pour activer la mise en correspondance de la communauté de BGP ou de la communauté étendue avec les objets de liste de communauté ou les objets de liste de communauté étendue spécifiés, respectivement. Si vous spécifiez plusieurs règles, les routages sont vérifiés par rapport aux règles jusqu'à ce qu'une autorisation ou un refus correspondant soit obtenu.

a) Pour spécifier une liste de communauté pour la règle, cliquez sur **Edit** (✎) dans le champ **Selected Community List** (liste de communauté sélectionnée). Les listes de communautés s'affichent sous **available Community List** (liste de communautés disponibles). Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**.

Pour permettre la mise en correspondance de la communauté BGP exactement avec la communauté spécifiée, cochez la case **Faire correspondre exactement la communauté spécifiée**.

b) Pour ajouter la liste de communauté étendue, cliquez sur **Edit** (✎) dans le champ **Selected Extended Community List** (liste de communautés étendues sélectionnées). Les listes de communautés étendues s'affichent sous la **liste de communautés étendues disponibles**. Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**.

Remarque Les listes de communautés étendues s'appliquent uniquement à la configuration de l'importation ou de l'exportation de routages.

Étape 11 Cliquez sur l'onglet **Métriques et balises** pour mettre en correspondance la métrique et la balise de groupe de sécurité d'une route.

a) Saisissez les valeurs de la métrique à utiliser pour la mise en correspondance dans le champ **Metric** (métrique). Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une métrique spécifiée. Les valeurs des mesures peuvent être comprises entre 0 et 4294967295.

b) Saisissez les valeurs de balise à utiliser pour la mise en correspondance dans le champ **Tag** (Balise). Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une balise de groupe de sécurité précisée. Les valeurs de balise peuvent être comprises entre 0 et 4294967295.

Étape 12 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 13 Cliquez sur **Save** (enregistrer).

Port

Les objets de port représentent différents protocoles de différentes manières :

TCP et UDP

Un objet port représente le protocole de la couche de transport, avec le numéro de protocole entre parenthèses, plus un port ou une plage de ports associés facultatifs. Par exemple : `TCP(6)/22`.

ICMP et ICMPv6 (IPv6-ICMP)

Un objet de port représente le protocole de la couche Internet ainsi qu'un type et un code facultatifs. Par exemple : `ICMP(1):3:3`.

Vous pouvez restreindre un objet de port ICMP ou IPV6-ICMP par type et, le cas échéant, code. Pour en savoir plus sur les types et les codes ICMP, consultez :

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

Autre

Un objet de port peut représenter d'autres protocoles qui n'utilisent pas de ports.

Le système fournit des objets de port par défaut pour les ports connus. Vous ne pouvez pas modifier ni supprimer ces objets par défaut. Vous pouvez créer des objets de port personnalisés en plus des objets par défaut.

Vous pouvez utiliser des objets et des groupes de ports à divers endroits de l'interface des systèmes Web, notamment pour les politiques de contrôle d'accès, les règles d'identité, les règles de découverte du réseau, les variables de port et les recherches d'événements. Par exemple, si votre entreprise utilise un client personnalisé qui utilise une plage spécifique de ports et entraîne la génération d'un nombre excessif d'événements par le système, vous pouvez configurer votre politique de découverte de réseau pour exclure la surveillance de ces ports.

Lorsque vous utilisez des objets de port, respectez les consignes suivantes :

- Vous ne pouvez pas ajouter de protocole autre que TCP ou UDP pour les conditions de port source dans les règles de contrôle d'accès. En outre, vous ne pouvez pas combiner des protocoles de transport lors de la définition de conditions de port de source et de destination dans une règle.
- Si vous ajoutez un protocole non pris en charge à un groupe d'objets de port utilisé dans une condition de port source, la règle selon laquelle il est utilisé ne prend pas effet sur le périphérique géré lorsque la configuration est déployée.
- Si vous créez un objet de port contenant des ports TCP et UDP et que vous l'ajoutez comme condition de port source dans une règle, vous ne pouvez pas ajouter de port de destination, et inversement.

Création d'objets port

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **PortL** dans la liste des types d'objets.

Étape 3 Sélectionnez **Add Object** (Ajouter un objet)dans la liste déroulante **Add Port** (Ajouter un port).

Étape 4 Saisissez un **Nom**.

Étape 5 Choisissez un **protocole**.

Étape 6 Selon le protocole que vous avez choisi, limitez par **port** ou choisissez un **type** et un **code** ICMP .

Vous pouvez saisir les ports de `1` à `65535`. Utilisez un tiret pour spécifier une plage de ports. Vous devez restreindre l'objet par port si vous avez choisi de mettre en correspondance **tous** les protocoles, en utilisant la liste déroulante **Autre**.

Étape 7 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 13.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Importation d'objets de port

Pour en savoir plus sur l'importation d'objets de port, consultez Importation d'objets en cours, à la page 5.

Liste des préfixes

Vous pouvez créer des objets de liste de préfixes pour IPv6 à utiliser lorsque vous configurez des cartes de routage, des listes de politiques, le filtrage OSPF ou le filtrage de voisin BGP

Configurer la liste des préfixes IPv6

Utilisez la page de liste Configure IPv6 Prefix (configuration du préfixe IPv6) pour créer, copier et modifier des objets de liste de préfixes. Vous pouvez créer des objets de liste de préfixes à utiliser lorsque vous configurez des cartes de routage, des cartes de politiques, le filtrage OSPF ou le filtrage de voisin BGP

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets),** puis choisissez **Prefix Lists (Liste de préfixes)** > **IPv6 Prefix List (Liste de préfixe IPv6)** dans la table des matières.

Étape 2 Cliquez sur **Add Prefix List** (Ajouter une liste de préfixe).

Étape 3 Saisissez un nom pour l'objet liste de préfixes dans le champ **Name** de la fenêtre **New Prefix List Object** (nouvel objet de liste de préfixes).

Étape 4 Cliquez sur **Add** (Ajouter) dans la fenêtre **New Prefix List Object** (nouvel objet de liste de préfixes).

Étape 5 Sélectionnez l'action appropriée Autoriser ou Bloquer dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

Étape 6 Saisissez un numéro unique qui indique la position d'une nouvelle entrée de liste de préfixes dans la liste des entrées de liste de préfixes déjà configurées pour cet objet, dans le champ **Sequence No** (N° de séquence). Si ce champ est laissé vide, le numéro de séquence sera par défaut cinq de plus que le plus grand numéro de séquence actuellement utilisé.

Étape 7 Spécifiez l'adresse IPv6 au format adresse IP/longueur de masque dans le champ **IP address** (Adresse IP).. La longueur du masque doit être une valeur valide comprise entre 1 et 128.

Étape 8 Saisissez la longueur minimale de préfixe dans le champ **Minimum Prefix Longueur** (longueur de préfixe minimale). La valeur doit être supérieure à la longueur du masque et inférieure ou égale à la longueur maximale de préfixe, si elle est spécifiée.

Étape 9 Saisissez la longueur maximale de préfixe dans le champ **Maximum Prefix Longueur** (longueur de préfixe maximale). La valeur doit être supérieure ou égale à la longueur minimale du préfixe, le cas échéant, ou supérieure à la longueur du masque si la longueur minimale du préfixe n'est pas précisée.

Étape 10 Cliquez sur **Add** (ajouter).

Étape 11 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 12 Cliquez sur **Save** (enregistrer).

Configurer la liste des préfixes IPv4

Utilisez la page de liste Configure IPv4 Prefix (configuration du préfixe IPv4) pour créer, copier et modifier des objets de liste de préfixes. Vous pouvez créer des objets de liste de préfixes à utiliser lorsque vous configurez des cartes de routage, des cartes de politiques, le filtrage OSPF ou le filtrage de voisin BGP

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management (gestion des objets),** puis **Prefix Lists** > **IPv4 Prefix List** (liste de préfixes IPv4) dans la table des matières.

Étape 2 Cliquez sur **Add Prefix List** (Ajouter une liste de préfixe).

Étape 3 Saisissez un nom pour l'objet liste de préfixes dans le champ **Name** de la fenêtre **New Prefix List Object** (nouvel objet de liste de préfixes).

Étape 4 Cliquez sur **Add** (ajouter).

Étape 5 Sélectionnez l'action appropriée Autoriser ou Bloquer dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

Étape 6 Saisissez un numéro unique qui indique la position d'une nouvelle entrée de liste de préfixes dans la liste des entrées de liste de préfixes déjà configurées pour cet objet, dans le champ **Sequence No** (N° de séquence). Si ce champ est laissé vide, le numéro de séquence sera par défaut cinq de plus que le plus grand numéro de séquence actuellement utilisé.

Étape 7 Précisez l'adresse IPv4 dans le format adresse IP/longueur de masque dans le champ **IP address** (adresse IP). La longueur du masque doit être une valeur valide comprise entre 1 et 32.

Étape 8 Saisissez la longueur minimale de préfixe dans le champ **Minimum Prefix Longueur** (longueur de préfixe minimale). La valeur doit être supérieure à la longueur du masque et inférieure ou égale à la longueur maximale de préfixe, si elle est spécifiée.

Étape 9 Saisissez la longueur maximale de préfixe dans le champ **Maximum Prefix Longueur** (longueur de préfixe maximale). La valeur doit être supérieure ou égale à la longueur minimale du préfixe, le cas échéant, ou supérieure à la longueur du masque si la longueur minimale du préfixe n'est pas précisée.

Étape 10 Cliquez sur **Add** (ajouter).

Étape 11 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 12 Cliquez sur **Save** (enregistrer).

Carte de routage

Les cartes de routage sont utilisées lors de la redistribution des routes dans n'importe quel processus de routage. Elles sont également utilisées lors de la génération d'une route par défaut dans un processus de routage. Une carte de routage définit les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible. Configurez une carte de routage, pour créer une nouvelle entrée de carte de routage pour un objet de carte de routage ou pour modifier une entrée existante.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Avant de commencer

Une carte de routage peut utiliser un ou plusieurs de ces objets; il n'est pas obligatoire d'ajouter tous ces objets. Créez et utilisez l'un de ces objets au besoin pour configurer votre carte de routage.

- Ajouter des listes de contrôle d'accès.
- Ajouter une entrée à la liste de préfixes.
- Ajouter un chemin AS.
- Ajouter une liste de communautés.
- Ajouter des listes de communauté étendues

Remarque Les listes de communautés étendues s'appliquent uniquement à la configuration de l'importation ou de l'exportation de routages.

- Ajouter des listes de politiques

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management (Objets > Gestion des objets),** puis **Route Map** (Carte de routage) dans la table des matières.

Étape 2 Cliquez sur **Add Route Map (ajouter une carte de routage)**.

Étape 3 Cliquez sur **Add** (ajouter) dans la fenêtre **New Route Map Object** (Nouvel objet de carte de routage).

Étape 4 Dans le champ **Sequence No.**, saisissez un nombre, de 0 à 65535, qui indique la position d'une nouvelle entrée de carte de routage dans la liste des entrées de carte de routage déjà configurées pour cet objet de carte de routage.

Remarque Nous vous recommandons de numériser les clauses par intervalles d'au moins 10 pour réserver un espace de numérotation au cas où vous souhaiteriez insérer des clauses ultérieurement.

Étape 5 Sélectionnez l'action appropriée Autoriser ou Bloquer dans la liste déroulante **Redistribution** pour indiquer l'accès à la redistribution.

Étape 6 Cliquez sur l'onglet **Clauses de correspondance** pour mettre en correspondance (routes/trafic) en fonction des critères suivants, que vous sélectionnez dans la table des matières :

- **Zones de sécurité** : mettre en correspondance le trafic en fonction des interfaces (entrée/sortie). Vous pouvez sélectionner des zones et les ajouter, ou taper des noms d'interface et les ajouter.
- : c**IPv4** : correspondance avec IPv4 (routes/trafic) en fonction des critères suivants; Sélectionnez l'onglet pour définir les critères.
  1. Cliquez sur l'onglet **Address** (adresse) pour faire correspondre les routages en fonction de l'adresse de routage. Pour les adresses IPv4, choisissez si vous souhaitez utiliser une liste d'accès ou une liste de préfixes pour la mise en correspondance dans la liste déroulante, puis saisissez ou sélectionnez les objets de liste ACL ou les objets de préfixe que vous souhaitez utiliser pour la mise en correspondance.
  2. Cliquez sur l'onglet **Next Hop** (saut suivant) pour faire correspondre les routages en fonction de l'adresse de saut suivant d'une route. Pour les adresses IPv4, choisissez si vous souhaitez utiliser

une liste d'accès ou une liste de préfixes pour la mise en correspondance dans la liste déroulante, puis saisissez ou sélectionnez les objets ACL ou la liste de préfixes que vous souhaitez utiliser pour la mise en correspondance.

3. Cliquez sur l'onglet **Route Source** (source de routage) pour faire correspondre les routages en fonction de l'adresse de la source de publicité de la route. Pour les adresses IPv4, choisissez si vous souhaitez utiliser une liste d'accès ou une liste de préfixes pour la mise en correspondance dans la liste déroulante, puis saisissez ou sélectionnez les objets ACL ou la liste de préfixes que vous souhaitez utiliser pour la mise en correspondance.

- **IPv6** : correspondance avec IPv6 (routes/trafic) en fonction de l'adresse de routage, de l'adresse du saut suivant ou de l'adresse de la source de publicité de la route.
- **BGP** : correspondance avec BGP (routes/trafic) en fonction des critères suivants : Sélectionnez l'onglet pour définir les critères.

1. Cliquez sur l'onglet **AS Path** (Chemin AS) pour permettre la mise en correspondance de la liste d'accès du système autonome BGP avec la liste d'accès au chemin spécifiée. Si vous spécifiez plusieurs listes d'accès de chemin d'accès, la voie de routage peut correspondre à l'une ou l'autre des listes d'accès de chemin d'accès.
2. Cliquez sur l'onglet **Community List** (liste de communauté) pour activer la mise en correspondance de la communauté de BGP ou de la communauté étendue avec les objets de liste de communauté ou les objets de liste de communauté étendue spécifiés, respectivement.
   - Pour spécifier une liste de communauté pour la règle, cliquez sur **Edit** (✎) dans le champ **Selected Community List** (liste de communauté sélectionnée). Les listes de communautés s'affichent sous **available Community List** (Liste des communautés disponibles). Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**. Pour en savoir plus sur la création d'objets de liste de communauté, consultez Liste de communautés, à la page 27
   - Pour ajouter la liste de communauté étendue, cliquez sur **Edit** (✎) dans le champ **Selected Extended Community List** (liste de communautés étendues sélectionnées). Les listes de communautés étendues s'affichent dans la **liste de communautés étendues disponibles**. Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**. Pour en savoir plus sur la création d'objets de liste de communautés étendues, consultez Communauté étendue, à la page 28.

   Pour permettre la mise en correspondance de la communauté de BGP exactement avec les objets de liste de communautés spécifiés, cochez la case **Correspond exactement la communauté spécifiée**. Cette option ne s'applique pas à la liste de communautés étendues.

   Remarque Si vous spécifiez plusieurs règles, les routages sont vérifiés par rapport aux règles jusqu'à ce qu'une condition d'autorisation ou de refus correspondante soit remplie. Tout routage qui ne correspond pas à au moins une communauté de correspondance ne sera pas annoncée pour les cartes de routage sortantes.

3. Cliquez sur l'onglet **Policy List** (Liste des politiques) pour configurer une carte de routage afin d'évaluer et de traiter une politique de BGP. Lorsque plusieurs listes de politiques effectuent la mise en correspondance dans une entrée de carte de routage, toutes les listes de politiques correspondent uniquement à l'attribut entrant.

- **Autres** : correspondance des routes ou du trafic en fonction des critères suivants.

1. Saisissez les valeurs de métrique à utiliser pour la mise en correspondance dans le champ **Metric Route Value** (Valeur de la route métrique) pour permettre la mise en correspondance de la métrique d'une voie de routage. Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une métrique spécifiée. Les valeurs des mesures peuvent être comprises entre 0 et 4294967295.
2. Saisissez les valeurs de balise à utiliser pour la mise en correspondance dans le champ **Valeurs de balise**. Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une balise de groupe de sécurité précisée. Les valeurs de balise peuvent être comprises entre 0 et 4294967295.
3. Cochez l'option **Route Type** (Type de routage) appropriée pour activer la correspondance du type de routage. Les types de routage valides sont External1, External2, Internal, Local, NSSA-External1 et NSSA-External2. Vous pouvez choisir plusieurs types de routage dans la liste.

Étape 7 Cliquez sur l'onglet **Set Clauses** (Définir les clauses) pour définir les routes ou le trafic en fonction des critères suivants, que vous sélectionnez dans la table des matières :

- **Valeurs des métriques** : définissez la bande passante, toutes les valeurs ou aucune des valeurs.
  1. Saisissez une valeur de mesure ou une bande passante en Kbits par seconde dans le champ **Bande passante**. Les valeurs valides sont des entiers compris entre 0 et 4294967295.
  2. Sélectionnez cette option pour préciser le type de mesure pour le protocole de routage de destination dans la liste déroulante **Metric Type** (Type de mesure). Les valeurs valides sont : internal, type-1 ou type-2.
- **Clauses BGP** : définissez les routes BGP en fonction des critères suivants; sélectionnez l'onglet pour définir les critères.
  1. Cliquez sur l'onglet **AS Path** pour modifier un chemin de système autonome pour les routes BGP.
     1. Saisissez un numéro de chemin de système autonome dans le champ **Prepend AS Path** pour ajouter une chaîne de chemin d'accès du système autonome quelconque aux routes de BGP. Habituellement, le numéro du système autonome local est ajouté plusieurs fois, ce qui augmente la longueur du chemin du système autonome. Si vous spécifiez plusieurs numéros de chemin de système autonome, la route peut précéder l'un ou l'autre de ces numéros de système.
     2. Saisissez un numéro de chemin de système autonome dans le champ **Ajouter le dernier numéro de système autonome au chemin AS** pour ajouter le dernier numéro de système autonome au chemin. Saisissez une valeur pour le numéro de système autonome comprise entre 1 et 10.
     3. Cochez la case **Convert route tag into AS path** pour convertir la balise d'une route en chemin de système autonome.
  2. Cliquez sur l'onglet **Community List** (Liste des communautés) pour définir les attributs de la communauté :

     Sous **Specific Community** (Communauté spécifique) :

     1. Cliquez sur le bouton radio **Aucun** pour supprimer l'attribut de communauté des préfixes qui transmettent la carte de routage.
     2. Cliquez sur le bouton radio **Communauté spécifique** pour saisir un numéro de communauté, le cas échéant. Les valeurs valides sont comprises entre 0 et 4294967295.

3. Cochez la case **Add to existing communities** (ajouter aux communautés existantes) pour ajouter la communauté aux communautés déjà existantes.
4. Cochez les cases **Internet**, **No-Advertise** ou **No-Export** pour utiliser l'une de ces communautés bien connues.

Sous **Specific Extended Community**(communauté étendue spécifique), dans le champ **Route Target** (Cible de la route), saisissez le numéro de la cible de la route au format *ASN:nn* :

- Vous pouvez entrer des valeurs comprises entre 1:1 et 65534:65535.

  Vous pouvez ajouter une seule cible de routage ou un ensemble de cibles de routage séparées par des virgules dans une seule entrée. Par exemple, *1:2,1:4,1:6*.

- Vous pouvez avoir un maximum de 8 objectifs de routage dans une entrée.
- Vous ne pouvez pas avoir des entrées cibles de routage redondantes dans les cartes de routage.

3. Cliquez sur l'onglet **Autres** pour définir des attributs supplémentaires.
   1. Cochez la case **Set Automatic Tag** pour calculer automatiquement la valeur de la balise.
   2. Saisissez une valeur de préférence pour le chemin d'accès au système autonome dans le champ **Set Local Preference**. Saisissez une valeur comprise entre 0 et 4294967295.
   3. Saisissez une pondération de BGP pour la table de routage dans le champ **Définir la pondération**. Saisissez une valeur entre 0 et 65 535.
   4. Sélectionnez cette option pour spécifier le code d'origine BGP. Les valeurs valides sont **IGP local,** et **Incomplet**.
   5. Dans la section IPv4 Settings (Paramètres IPv4), spécifiez une adresse IPv4 de saut suivant pour le prochain saut vers lequel les paquets sont sortis. Il n'est pas nécessaire qu'il s'agisse d'un routeur adjacent. Si vous spécifiez plusieurs adresses IPv4, les paquets peuvent être sortis à l'une ou l'autre des adresses IP.

      Sélectionnez cette option pour spécifier une liste de préfixes IPv4 dans la liste déroulante **Prefix List**.
   6. Dans la section IPv6 Settings, spécifiez une adresse IPv6 de saut suivant pour le prochain saut vers lequel les paquets sont sortis. Il n'est pas nécessaire qu'il s'agisse d'un routeur adjacent. Si vous spécifiez plusieurs adresses IPv6, les paquets peuvent être sortis à n'importe quelle des adresses IP.

      Sélectionnez cette option pour spécifier un préfixe IPv6 dans la liste déroulante **Prefix List**.

Étape 8 Cliquez sur **Add** (ajouter).

Étape 9 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.

Étape 10 Cliquez sur **Save** (enregistrer).

Renseignements de sécurité

La fonctionnalité Security Intelligence nécessite la licence IPS (pour les périphériques défense contre les menaces) ou la licence de protection (pour tous les autres types de périphériques).

Les *listes* et les *flux* de Security Intelligence sont des ensembles d'adresses IP, de noms de domaine et d'URL que vous pouvez utiliser pour filtrer rapidement le trafic qui correspond à une entrée d'une liste ou d'un flux.

- Une liste est un ensemble statique que vous gérez manuellement.
- Un flux est un ensemble dynamique qui se met à jour à intervalles réguliers sur HTTP ou HTTPS.

Les listes et les flux de renseignements sur la sécurité sont regroupés comme suit :

- DNS (noms de domaine)
- Réseau (adresses IP)
- Adresses URL

Flux de renseignements fournis par le système

Cisco fournit les flux suivants en tant qu'objets de renseignement sur la sécurité :

- Flux de renseignements sur la sécurité mis à jour régulièrement avec les dernières informations sur les menaces provenant de Talos :
  - Cisco-DNS-and-UR-Intelligence-Feed (sous DNS Lists and Flows)
  - Flux de renseignements Cisco (pour les adresses IP, sous Network Lists and Flows)

  Vous ne pouvez pas supprimer les flux fournis par le système, mais vous pouvez modifier (ou désactiver) la fréquence de leurs mises à jour.
- Cisco-TID-Feed (sous Network Lists and Flows)

  Ce flux n'est pas utilisé dans l'onglet Security Intelligence de la politique de contrôle d'accès.

  Au lieu de cela, vous devez activer et configurer Directeur de Cisco Secure Firewall threat intelligence pour utiliser ce flux, qui est un ensemble de données observables TID.

  Utilisez cet objet pour définir la fréquence de publication de ces données dans les éléments TID.

Listes prédéfinies : listes de blocage globales et listes Ne pas bloquer globales

Le système est livré avec des listes de blocage et des listes Ne pas bloquer globales pour les domaines (DNS), les adresses IP (réseaux) et les URL.

Ces listes sont vides tant que vous ne les remplissez pas. Pour créer ces listes, consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 83.

Par défaut, les politiques de contrôle d'accès et DNS utilisent ces listes dans le cadre de la Security Intelligence.

Flux personnalisés

Vous pouvez faire appel à des flux tiers ou à un flux interne personnalisé pour gérer facilement une liste de blocage à l'échelle de l'entreprise dans le cadre d'un déploiement à grande échelle comprenant plusieurs Cisco Secure Firewall Management Center.

Consultez Flux de renseignements sur la sécurité personnalisés, à la page 89.

Listes personnalisées

Les listes personnalisées peuvent alimenter et affiner les flux et les listes globales.

Consultez Listes de renseignements sur la sécurité personnalisés, à la page 91.

Emplacement d'utilisation des listes et des flux de renseignements sur la sécurité

- Adresses IP et blocages d'adresses : utilisez les listes de blocage et Ne pas bloquer dans les politiques de contrôle d'accès, dans le cadre des renseignements sur la sécurité.
- Domain Names (noms de domaine) : utilisez les listes de blocage et ne pas bloquer dans les politiques DNS, dans le cadre de Security Intelligence (Renseignements sur la sécurité).
- URL : utilisez les listes de blocage et Ne pas bloquer dans les politiques de contrôle d'accès, dans le cadre des renseignements sur la sécurité. Vous pouvez également utiliser des listes d'URL dans les règles de contrôle d'accès et de QoS pour lesquelles les phases d'analyse et de gestion du trafic ont lieu après les renseignements sur la sécurité.

Modifier les objets de renseignements sur la sécurité

Pour ajouter ou supprimer des entrées dans une liste de blocage, une liste Ne pas bloquer, un flux ou un objet gouffre :

Type d'objet	Modifier les capacités	Nécessite un redéploiement après modification?
Listes personnalisées Bloquer et Ne pas bloquer	Téléversez de nouvelles listes et des listes de remplacement à l'aide du gestionnaire d'objets.	Non
Listes de blocage et listes Ne pas bloquer par défaut (mais remplies de façon personnalisée) : globales, descendantes et propres au domaine	Ajoutez des entrées à l'aide du menu contextuel ou supprimez des entrées à l'aide du gestionnaire d'objets.	Non
Flux de renseignements fournis par le système	Désactivez ou modifiez la fréquence des mises à jour à l'aide du gestionnaire d'objets.	Non
Flux personnalisés	Modification complète à l'aide du gestionnaire d'objets.	Non
Gouffre	Modification complète à l'aide du gestionnaire d'objets.	Oui

Listes des renseignements sur la sécurité globale et de domaine

Cisco Firepower Management Center est livré avec des listes globales de blocage et Ne pas bloquer vides auxquelles vous pouvez ajouter des URL, des domaines et des adresses IP à partir d'événements sur votre réseau, à tout moment. Ces listes vous permettent d'utiliser les services Security Intelligence pour toujours bloquer des connexions particulières ou pour exempter des connexions particulières du blocage par Security Intelligence, afin qu'elles soient évaluées par d'autres processus de détection de menaces que vous avez configurés.

Par exemple, si vous remarquez un ensemble d'adresses IP routables dans les incidents d'intrusion associés aux tentatives d'exploit, vous pouvez bloquer immédiatement ces adresses IP. Bien que la propagation de vos modifications puisse prendre quelques minutes, vous n'avez pas besoin de redéployer.

Par défaut, les politiques de contrôle d'accès et DNS utilisent ces listes globales, qui s'appliquent à toutes les zones de sécurité. Vous pouvez choisir de ne pas utiliser ces listes politique par politique.

Remarque Ces options s'appliquent uniquement aux renseignements sur la sécurité. Security Intelligence ne peut pas bloquer le trafic qui a déjà fait l'objet d'un chemin d'accès rapide fastpath. De même, l'ajout d'un élément à une liste Security Intelligence Ne pas bloquer ne fait pas automatiquement confiance au trafic de correspondance de chemin d'accès rapide. Pour en savoir plus, consultez À propos des renseignements sur la sécurité.

Dans un déploiement multidomaine, vous pouvez choisir les domaines du système Firepower où vous souhaitez appliquer le blocage, ou exempter du blocage Security Intelligence, en ajoutant des éléments aux listes de domaines ainsi qu'aux listes globales; voir Listes d'informations de sécurité et multilocalisation de détention, à la page 83.

Listes d'informations de sécurité et multilocalisation de détention

Dans un déploiement multidomaine, le domaine global est propriétaire des listes de blocage globales et des listes Ne pas bloquer. Seuls les administrateurs globaux peuvent ajouter ou supprimer des éléments dans les listes globales. Les utilisateurs de sous-domaines peuvent ainsi ajouter des réseaux, des noms de domaine et des URL aux listes de blocage et de non-blocage :

- Listes de domaines : listes Bloquer ou Ne pas bloquer dont le contenu s'applique uniquement à un sous-domaine particulier. Les listes globales sont des listes de domaine pour le domaine global.
- Listes de domaines descendants : listes Bloquer ou Ne pas bloquer qui agrègent les listes de domaines des descendants du domaine actuel.

Liste de domaines

En plus de pouvoir accéder aux listes globales (mais pas les modifier), chaque sous-domaine a ses propres listes nommées, dont le contenu s'applique uniquement à ce sous-domaine. Par exemple, un sous-domaine nommé Entreprise A possède :

- Liste de blocage des domaines : Entreprise A et Liste des domaines non bloqués - Entreprise A
- Liste de blocage des domaines pour le DNS : Entreprise A, liste des domaines à ne pas bloquer pour le DNS – Entreprise A
- Liste de blocage des domaines pour le l'URL : Entreprise A, liste des domaines à ne pas bloquer pour l'URL – Entreprise A

Tout administrateur du domaine actuel ou d'un domaine supérieur peut alimenter ces listes. Vous pouvez utiliser le menu contextuel pour ajouter un élément à la liste Bloquer ou Ne pas bloquer dans le domaine actuel et dans tous les domaines descendants. Cependant, seul un administrateur du domaine associé peut supprimer un élément d'une liste de domaines.

Par exemple, un administrateur global pourrait choisir d'ajouter la même adresse IP à la liste de blocage dans le domaine global et le domaine de l'entreprise A, mais pas de l'ajouter à la liste de blocage dans le domaine de l'entreprise B. Cette action ajouterait la même adresse IP à :

- Liste de blocage globale (où elle ne peut être supprimée que par les administrateurs globaux)
- Liste de blocage de domaine - Entreprise A (où elle ne peut être supprimée que par les administrateurs de l'entreprise A)

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Listes de domaines descendants

Une liste de domaines descendants est une liste de blocage ou une liste Ne pas bloquer qui regroupe les listes de domaines des descendants du domaine actuel. Les domaines enfants n'ont pas de listes de domaines descendants.

Les listes de domaines descendants sont utiles, car un administrateur de domaine de niveau supérieur peut appliquer les paramètres généraux de Security Intelligence, tout en permettant aux utilisateurs de sous-domaine d'ajouter des éléments à une liste de blocage ou Ne pas bloquer dans leur propre déploiement.

Par exemple, le domaine global comporte les listes de domaines descendants suivantes :

- Listes bloquées des descendants - listes globales, Ne pas bloquer des descendants - globale
- Listes de blocage descendantes pour DNS - globale, Listes de non-blocage descendantes pour DNS - globale
- Listes de blocage descendantes pour URL- globale, Listes de non-blocage descendantes pour URL - globale

Remarque Les listes de domaines descendants ne s'affichent pas dans le gestionnaire d'objets, car ce sont des agrégations symboliques et non des listes remplies manuellement. Elles s'affichent là où vous pouvez les utiliser : dans les politiques de contrôle d'accès et DNS.

Ajouter des entrées aux listes globales de renseignements sur la sécurité

Lors de l'examen des événements et des tableaux de bord, vous pouvez bloquer instantanément le trafic futur impliquant des adresses IP, des domaines et des URL qui apparaissent dans ces événements en les ajoutant à une liste de blocage prédéfinie.

De même, si Security Intelligence bloque le trafic que vous souhaitez voir évalué par les processus de détection des menaces après le blocage de Security Intelligence, vous pouvez ajouter les adresses IP, les domaines et les URL des événements à une liste prédéfinie Do Not Block (Ne pas bloquer).

Le trafic est évalué par rapport aux entrées de ces listes pendant la phase de renseignement sur la sécurité de la détection des menaces.

Pour en savoir plus sur ces listes, consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 83.

Avant de commencer

Comme l'ajout d'une entrée à une liste de renseignements sur la sécurité affecte le contrôle d'accès, vous devez avoir l'un des rôles d'utilisateur suivants :

- Administrateur
- une combinaison de rôles : administrateur de réseau ou administrateur d'accès, plus analyste de sécurité et approbateur de sécurité
- un rôle personnalisé avec les autorisations Modifier la politique de contrôle d'accès et Déployer la configuration sur les périphériques

Le cas échéant, vérifiez que ces listes sont utilisées dans les politiques où vous vous attendez qu'elles soient utilisées.

Procédure

Étape 1 Accédez à un événement qui comprend une adresse IP, un domaine ou une URL que vous souhaitez toujours bloquer à l'aide de Security Intelligence, ou exempter du blocage Security Intelligence.

Étape 2 Effectuez un clic droit sur l'adresse IP, le domaine ou l'URL et choisissez l'option appropriée :

Type d'article	Option de menu contextuel
Adresse IP	Ajouter une adresse IP à la liste de blocage Ajouter une adresse IP à la liste d'autorisation Ces options ajoutent l'adresse IP aux listes respectives des réseaux.
URL	Ajouter une URL à la liste de blocage globale pour les URL Ajouter une URL à la liste globale d'autorisation pour les URL
Domaine d'une URL dans le champ URL	Ajouter un domaine à la liste de blocage globale pour les URL Ajouter un domaine à la liste d'autorisation globale pour les URL
Domaine dans le champ de requête DNS	Ajouter un domaine à la liste de blocage globale pour DNS Ajouter un domaine à la liste globale d'autorisation pour DNS

Prochaine étape

Vous n'avez PAS besoin d'effectuer de redéploiement pour que ces modifications prennent effet.

Si vous souhaitez supprimer un élément d'une liste, consultez Supprimer des entrées des listes globales de renseignements sur la sécurité, à la page 86.

Supprimer des entrées des listes globales de renseignements sur la sécurité

Remarque

- Dans les déploiements dans plusieurs domaines, le nom de ces listes peut ne pas être « global ». Pour en savoir plus, consultez Listes d'informations de sécurité et multilocalisation de détention, à la page 83.
- Pour ajouter des entrées à ces listes, consultez Ajouter des entrées aux listes globales de renseignements sur la sécurité, à la page 84.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **Security Intelligence** (Renseignements sur la sécurité)

Étape 3 Cliquez sur l'option appropriée :

- **Network Lists and Feeds** (Listes et flux de réseau) (pour les adresses IP)
- **DNS Lists and Feeds** (Listes et flux DNS) (pour les noms de domaine)
- **Listes et flux d'URL**

Étape 4 Cliquez sur le crayon à côté de la liste Blocage global ou de la liste globale Ne pas bloquer.

Étape 5 Cliquez sur le bouton de la corbeille à côté de l'entrée à supprimer.

Mises à jour de listes et de flux pour les renseignements sur la sécurité

Les mises à jour de liste et de flux remplacent le fichier de liste ou de flux existant par le contenu du nouveau fichier. Le contenu des fichiers existants et des nouveaux fichiers n'est pas fusionné.

Si le système télécharge un flux corrompu ou un flux sans entrée reconnaissable, le système continue d'utiliser les anciennes données du flux (sauf s'il s'agit du premier téléchargement). Cependant, si le système peut reconnaître une seule entrée du flux, il utilise les entrées qu'il peut reconnaître.

Par défaut, chaque flux met à jour le centre de gestion toutes les deux heures; vous pouvez modifier cette fréquence. Toutes les mises à jour reçues par le centre de gestion sont transmises immédiatement aux périphériques gérés. En outre, les périphériques gérés interrogent le FMC toutes les 30 minutes pour vérifier les changements. Vous ne pouvez pas modifier cette fréquence.

Dans un déploiement multidomaine, les flux fournis par le système appartiennent au domaine global et ne peuvent être modifiés que par un administrateur de ce domaine. Vous pouvez modifier la fréquence de mise à jour des flux personnalisés appartenant à votre domaine.

Pour modifier les intervalles de mise à jour du flux, consultez Modification de la fréquence de mise à jour des flux de renseignements sur la sécurité, à la page 87.

Modification de la fréquence de mise à jour des flux de renseignements sur la sécurité

Vous pouvez spécifier les intervalles auxquels le centre de gestion Cisco Firepower Management Center (FMC) met à jour les flux de renseignements sur la sécurité.

Pour en savoir plus sur les mises à jour de flux, consultez Mises à jour de listes et de flux pour les renseignements sur la sécurité, à la page 86.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez le type de flux dont vous souhaitez modifier la fréquence.

Le flux d'URL fourni par le système est combiné avec le flux de domaine sous **DNS Lists and Flows**.

Étape 3 À côté du flux que vous souhaitez mettre à jour, cliquez sur **Edit** ( ).

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Modifiez la **fréquence de mise à jour**.

Étape 5 Cliquez sur **Save** (enregistrer).

Listes et flux de renseignements sur la sécurité personnalisés

Listes et flux personnalisés : exigences

Mise en forme des listes et des flux

Chaque liste ou flux doit être un simple fichier texte ne dépassant pas 500 Mo. Les fichiers de liste doivent avoir l'extension .txt. Incluez une entrée ou un commentaire par ligne : une adresse IP, une URL et un nom de domaine.

Astuces Le nombre d'entrées que vous pouvez inclure est limité par la taille maximale du fichier. Par exemple, une liste d'URL sans commentaire et une longueur d'URL moyenne de 100 caractères (y compris les représentations Punycode ou pourcentage Unicode et les retours à la ligne) peut contenir plus de 5,24 millions d'entrées.

Dans une entrée de liste DNS, vous pouvez spécifier un caractère générique (`*`) pour une étiquette de domaine. Toutes les étiquettes correspondent au caractère générique. Par exemple, l'entrée `www.exemple.*` correspond à la fois à `www.exemple.com` et à `www.exemple.co`.

Si vous ajoutez des lignes de commentaires dans le fichier source, elles doivent commencer par le caractère dièse (`#`). Si vous téléversez un fichier source avec des commentaires, le système supprime vos commentaires pendant le téléchargement. Les fichiers sources que vous téléchargez contiennent toutes vos entrées sans vos commentaires.

Exigences du flux

Lorsque vous configurez un flux, vous spécifiez son emplacement à l'aide d'une URL. l'URL ne peut pas être codée en Punycode.

Pour des intervalles de mise à jour de flux de 30 minutes ou moins, vous devez spécifier une URL MD5. Cela empêche les téléchargements fréquents de flux inchangés. Si votre serveur de flux ne fournit pas d'URL MD5, vous devez utiliser un intervalle de téléchargement d'au moins 30 minutes.

Si vous utilisez une somme de contrôle MD5, elle doit être stockée dans un fichier texte simple avec uniquement la somme de contrôle. Les commentaires ne sont pas pris en charge.

Listes et flux d'URL : syntaxe d'URL et critères de correspondance

Les listes d'URL et les flux Security Intelligence, y compris les listes et les flux personnalisés et les entrées de la liste de blocage globale et de la liste Ne pas bloquer, peuvent inclure les éléments suivants, qui ont le comportement de correspondance décrit ci-dessous :

- Noms d'hôtes

  Par exemple, **`www.exemple.com`**.

- Adresses URL

  `exemple.com` correspond à **`exemple.com`** et à tous les sous-domaines, y compris **`www.exemple.com`**, **`eu.exemple.com`**, **`exemple.com/abc`**et **`www.exemple.com/def`**, mais PAS **`exemple.co.UK`** ou **`exemplexyz. com`** ou **`exemple.com.malicious-site.com`**

  Vous pouvez également inclure un chemin d'accès complet à l'URL, par exemple **`https://www.cisco.com/c/en/us/products/security/firewalls/index.html`**

Remarque Vous pouvez créer une URL, un réseau et un flux DNS personnalisés, dans lesquels vous pouvez ajouter le nom d'utilisateur et le mot de passe à l'intérieur de l'URL elle-même, par exemple : **`https://admin:password@server.domain.com/list.txt`**

Cependant, si votre mot de passe contient des caractères spéciaux comme des deux-points (:) ou l'arobase @, la transmission échouera. Vérifiez que votre mot de passe ne comporte aucun caractère spécial. Sinon, vous pouvez utiliser un mot de passe codé dans l'URL.

- Une barre oblique à la fin d'une URL pour spécifier une correspondance exacte

  `exemple.com/` correspond UNIQUEMENT à **`exemple.com`**; elle ne correspond PAS à **`www.exemple.com`** ni à aucune autre URL.

- Un caractère générique (*) pour représenter un domaine dans une URL

  Un astérisque peut représenter une chaîne de domaine complète séparée par des points, mais pas une chaîne de domaine partielle, ni n'importe quelle partie de l'URL après la première barre oblique.

  Exemples valides :

  - **`*.exemple.com`**
  - **`www.*.com`**

- **exemple.***

  (Par exemple, cela correspondra à **exemple.com** et **exemple.org** et **exemple.de**, mais PAS à **exemple.co.UK**)

- ***.exemple.***
- **exemple.*/**

Exemples non valides :

- **exemple*.com**
- **exemple.com/***

- Adresses IP (IPv4)

  Pour les adresses IPv6, ou pour utiliser des plages ou la notation CIDR, utilisez l'objet de réseau Security Intelligence.

  Vous pouvez inclure un ou plusieurs caractères génériques représentant un octet, par exemple 10.10.10.* ou 10.10.*.*.

Consultez aussi Listes de renseignements sur la sécurité personnalisés, à la page 91.

Flux de renseignements sur la sécurité personnalisés

Les flux de renseignements sur la sécurité personnalisés ou tiers vous permettent de compléter les flux de renseignements fournis par le système avec d'autres listes de blocage et de non-blocage réputées et régulièrement mises à jour sur Internet. Vous pouvez également configurer un flux interne, ce qui est utile si vous souhaitez mettre à jour plusieurs appareils Cisco Secure Firewall Management Center de votre déploiement à l'aide d'une liste de sources.

Remarque Vous ne pouvez pas ajouter de blocs d'adresses aux listes de blocage ou de ne pas bloquer en utilisant un masque réseau `/0` dans un flux de Security Intelligence. Si vous souhaitez surveiller ou bloquer tout le trafic ciblé par une politique, utilisez une règle de contrôle d'accès avec l'action de règle **Surveiller** ou **Bloquer**, respectivement, et comme valeur par défaut (`any`) (toute) pour les **réseaux source** et les réseaux de **destination**.

Vous pouvez également configurer le système pour utiliser une somme de contrôle MD5 afin de déterminer s'il faut télécharger un flux mis à jour. Si la somme de contrôle n'a pas changé depuis le dernier téléchargement du flux par le système, le système n'a pas besoin de le télécharger à nouveau. Vous pouvez utiliser des sommes de contrôle MD5 pour les flux internes, en particulier s'ils sont volumineux.

Remarque Le système n'effectue **pas** de vérification des certificats SSL homologues lors du téléchargement de flux personnalisés et ne prend pas en charge l'utilisation de groupes de certificats ou de certificats autosignés pour vérifier l'homologue distant.

Si vous souhaitez contrôler strictement quand le système met à jour un flux à partir d'Internet, vous pouvez désactiver les mises à jour automatiques pour ce flux. Cependant, les mises à jour automatiques assurent l'obtention des données pertinentes les plus à jour.

La mise à jour manuelle des flux de renseignements sur la sécurité entraîne la mise à jour de tous les flux, y compris les flux de renseignements.

Voir les exigences complètes à l'adresse suivante Listes et flux personnalisés : exigences, à la page 87.

Création de flux de renseignements sur la sécurité

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de flux que vous souhaitez ajouter.

Étape 3 Cliquez sur l'option appropriée pour le type de flux que vous avez choisi ci-dessus :

- **Add Network Lists and Feeds** (Ajouter des listes et flux de réseau) (pour les adresses IP)
- **Add DNS Lists and Feeds** (Ajouter des listes et des flux DNS)
- **Add URL Lists and Feeds** (Ajouter des listes et des flux d'URL)

Étape 4 Saisissez un **nom** pour le flux.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Choisissez **Flux** dans la liste déroulante **Type**.

Étape 6 Saisissez une **URL de flux**.

Étape 7 Saisissez une **URL MD5**.

Utilisé pour déterminer si le contenu du flux a changé depuis la dernière mise à jour, afin que le système ne télécharge pas les flux inchangés.

Une URL MD5 est requise pour les intervalles de mise à jour inférieurs à 30 minutes.

Si votre serveur de flux ne fournit pas d'URL MD5, vous devez choisir un intervalle d'au moins 30 minutes.

Étape 8 Choisissez une **Fréquence des mises à jour**

Étape 9 Cliquez sur **Save** (enregistrer).
Sauf si vous avez désactivé les mises à jour de flux, le système tente de télécharger et de vérifier le flux.

Mise à jour manuelle des flux de renseignements sur la sécurité

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Avant de commencer

Au moins un périphérique doit déjà être ajouté au centre de gestion.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de flux.

Étape 3 Cliquez sur **Mettre à jour les flux**, puis confirmez.

Étape 4 Cliquez sur **OK**.

Après avoir téléchargé et vérifié les mises à jour de flux, Cisco Secure Firewall Management Center communique les modifications à ses périphériques gérés. Votre déploiement commence à filtrer le trafic à l'aide des flux mis à jour.

Listes de renseignements sur la sécurité personnalisés

Les listes Security Intelligence sont de simples listes statiques d'adresses IP, de blocs d'adresses, d'URL ou de noms de domaine que vous téléversez manuellement dans le système. Les listes personnalisées sont utiles si vous souhaitez augmenter et affiner les flux ou l'une des listes globales, pour les périphériques gérés par Cisco Secure Firewall Management Center.

Par exemple, si un flux réputé bloque de manière incorrecte votre accès à des ressources essentielles, mais est dans l'ensemble utile pour votre organisation, vous pouvez créer une liste personnalisée ne pas bloquer qui contient uniquement les adresses IP mal classées, plutôt que de supprimer l'objet de flux d'adresses IP du Liste de blocage de la politique de contrôle d'accès.

Remarque Vous ne pouvez pas ajouter des blocs d'adresses à une liste de blocage ou de ne pas bloquer à l'aide d'un masque réseau `/0` dans une liste Security Intelligence. Si vous souhaitez surveiller ou bloquer tout le trafic ciblé par une politique, utilisez une règle de contrôle d'accès avec l'action de règle **Surveiller** ou **Bloquer**, respectivement, et comme valeur par défaut (`any`) (toute) pour les **réseaux source** et les réseaux de **destination**.

En ce qui concerne le formatage des entrées de liste, tenez compte des éléments suivants :

- Les masques réseau pour les blocs d'adresses peuvent être des nombres entiers de `0` à `32` ou de `0` à `128`, pour IPv4 et IPv6, respectivement.
- L'Unicode dans les noms de domaine doit être encodé au format Punycode et est insensible à la casse.
- Les caractères des noms de domaine sont insensibles à la casse.
- Les caractères Unicode dans les URL doivent être encodés au format de pourcentage.
- Les caractères des sous-répertoires d'URL sont sensibles à la casse.
- Les entrées de liste qui commencent par le signe dièse (`#`) sont traitées comme des commentaires.
- Consultez les exigences de format supplémentaires à l'adresse Listes et flux personnalisés : exigences, à la page 87.

En ce qui concerne la mise en correspondance des entrées de liste, tenez compte des éléments suivants :

- Le système fait correspondre les domaines de sous-niveau si un domaine de niveau supérieur existe dans une liste d'URL ou de DNS. Par exemple, si vous ajoutez `exemple.com` à une liste DNS, le système correspond à `www.exemple.com` et `test.exemple.com`.

- Le système n'effectue pas de recherches DNS (directes ou inverses) sur les entrées de liste DNS ou d'URL. Par exemple, si vous ajoutez `http://192.168.0.2` à une liste d'URL et qu'elle se résout en `http://www.exemple.com`, le système ne correspond qu'à `http://192.168.0.2`, et non `http://www.exemple.com`.

Téléversement de nouvelles listes de renseignements sur la sécurité vers Cisco Secure Firewall Management Center

Pour modifier une liste de renseignements sur la sécurité, vous devez apporter vos modifications au fichier source et téléverser une nouvelle copie. Vous ne pouvez pas modifier le contenu du fichier à l'aide de l'interface Web. Si vous n'avez pas accès au fichier source, téléchargez une copie du fichier système.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de liste.

Étape 3 Cliquez sur l'option appropriée pour la liste que vous avez choisie ci-dessus :

- **Add Network Lists and Feeds** (Ajouter des listes et flux de réseau) (pour les adresses IP)
- **Add DNS Lists and Feeds** (Ajouter des listes et des flux DNS)
- **Add URL Lists and Feeds** (Ajouter des listes et des flux d'URL)

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Dans la liste déroulante **Type**, sélectionnez **List** (Liste).

Étape 6 Cliquez sur **Browse** (Parcourir) pour accéder au fichier de liste `.txt`, puis cliquez sur **Upload** (Téléverser).

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Vous n'avez pas besoin de redéployer ces modifications pour qu'elles prennent effet. Si vous souhaitez supprimer une entrée de la liste, reportez-vous à Supprimer des entrées des listes globales de renseignements sur la sécurité, à la page 86.

Mises à jour des listes de renseignements sur la sécurité

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de liste.

Étape 3 À côté de la liste que vous souhaitez mettre à jour, cliquez sur **Edit** ( ).

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Si vous avez besoin d'une copie de la liste pour la modifier, cliquez sur **Télécharger**, puis suivez les instructions de votre navigateur pour enregistrer la liste en tant que fichier texte.

Étape 5 Apportez des modifications à la liste si nécessaire.

Étape 6 Dans la fenêtre contextuelle Security Intelligence, cliquez sur **Parcourir** pour naviguer jusqu'à la liste modifiée, puis cliquez sur **Téléverser**.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Vous n'avez pas besoin de redéployer ces modifications pour qu'elles prennent effet. Si vous souhaitez supprimer une entrée de la liste, reportez-vous à Supprimer des entrées des listes globales de renseignements sur la sécurité, à la page 86.

Gouffre

Un objet gouffre (sinkhole) représente soit un serveur DNS qui fournit des adresses non routables pour tous les noms de domaine du gouffre, soit une adresse IP qui ne se résout pas en serveur. Vous pouvez faire référence à l'objet gouffre dans une règle du protocole DNS pour rediriger le trafic correspondant vers le gouffre. Vous devez affecter à l'objet une adresse IPv4 et une adresse IPv6.

Création d'objets de gouffre

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Sinkhole** (Ajouter un gouffre).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Saisissez les **adresses IPv4** et **IPv6** de votre gouffre.

Étape 6 Vous avez les options suivantes :

- Si vous souhaitez rediriger le trafic vers un serveur gouffre, choisissez **Log Connections to Sinkhole** (Journaliser les connections vers le gouffre).

- Si vous souhaitez rediriger le trafic vers une adresse IP qui ne résout pas, choisissez **Block and Log Connections to Sinkhole** (Bloquer et journaliser les connections vers le gouffre).

Étape 7 Si vous souhaitez attribuer un type d'indication de compromission (IoC) à votre gouffre, choisissez-en un dans la liste déroulante **Type**.

Étape 8 Cliquez sur **Save** (enregistrer).

Surveillance SLA

Chaque moniteur d'accord de niveau de service (SLA) du protocole Internet définit une politique de connectivité à une adresse surveillée et suit la disponibilité d'une route vers l'adresse. La disponibilité des routes est vérifiée périodiquement en envoyant des demandes d'écho ICMP et en attendant la réponse. Si les demandes n'aboutissent pas, la route est supprimée de la table de routage et remplacée par une route de secours. Les tâches de surveillance SLA démarrent immédiatement après le déploiement et continuent de s'exécuter à moins que vous ne supprimiez le moniteur SLA de la configuration de l'appareil, c'est-à-dire qu'elles ne vieillissent pas. L'objet Moniteur d'accord de niveau de service (SLA) du protocole Internet est utilisé dans le champ Suivi de la route d'une politique de route statique IPv4. Les routes IPv6 n'ont pas la possibilité d'utiliser le moniteur SLA via le suivi de route.

Vous pouvez utiliser ces objets avec des périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management** et **SLA Monitor** dans la table des matières.

Étape 2 Cliquez sur **Ajouter un moniteur SLA** .

Étape 3 Saisissez un nom pour l'objet dans le champ **Name** (Nom).

Étape 4 (Facultatif) Dans le champ **Description**, saisissez la description.

Étape 5 Saisissez la fréquence des transmissions de requêtes ECHO ICMP, en secondes, dans le champ **Fréquence**. Les valeurs valides vont de 1 à 604800 secondes (7 jours). La valeur par défaut est de 60 secondes.

Remarque La fréquence ne peut pas être inférieure à la valeur du délai d'expiration; vous devez convertir la fréquence en millisecondes pour comparer les valeurs.

Étape 6 Saisissez le numéro d'ID de l'opération SLA dans le champ **SLA Monitor ID** (ID du moniteur SLA). Les valeurs sont comprises entre 1 et 2147483647. Vous pouvez créer un maximum de 2 000 opérations SLA sur un périphérique. Chaque numéro d'ID doit être unique pour la politique et la configuration du périphérique.

Étape 7 Saisissez le délai qui doit s'exécuter après une demande ECHO ICMP avant qu'un seuil d'augmentation soit déclaré, en millisecondes, dans le champ **Threshold** (Seuil). Les valeurs valides vont de 0 à 2147483647 millisecondes. La valeur par défaut est de 5 000 millisecondes. La valeur de seuil est utilisée uniquement pour indiquer les événements qui dépassent la valeur définie. Vous pouvez utiliser ces événements pour évaluer la valeur de délai d'expiration appropriée. Il ne s'agit pas d'un indicateur direct de l'accessibilité de l'adresse surveillée.

Remarque La valeur du seuil ne doit pas dépasser la valeur du délai d'expiration

Étape 8 Saisissez le délai pendant lequel l'opération SLA attend une réponse aux demandes ECHO ICMP, en millisecondes, dans le champ **Timeout** (délai d'expiration). Les valeurs sont comprises entre 0 et 604800000 millisecondes (7 jours). La valeur par défaut est de 5 000 millisecondes. Si aucune réponse n'est reçue de

l'adresse surveillée dans le délai défini dans ce champ, la voie de routage statique est supprimée de la table de routage et remplacée par la voie de routage de secours.

Remarque La valeur du délai d'expiration ne peut pas dépasser la valeur de fréquence (ajustez la valeur de fréquence aux millisecondes pour comparer les chiffres).

Étape 9 Saisissez la taille de la charge utile du paquet de requête ICMP, en octets, dans le champ **Data Size** (taille des données). Les valeurs sont comprises entre 0 et 16 384 octets. La valeur par défaut est de 28 octets, ce qui crée un paquet ICMP de 64 octets au total. Ne définissez pas cette valeur au-delà du maximum autorisé par le protocole ou par la PMTU (path Maximum Transmission Unit). Pour des raisons d'accessibilité, vous devrez peut-être augmenter la taille des données par défaut pour détecter les modifications de PMTU entre la source et la cible. Une PMTU faible peut affecter les performances de la session et, si elle est détectée, peut indiquer que le chemin secondaire doit être utilisé.

Étape 10 Saisissez une valeur pour le type de service (ToS) défini dans l'en-tête IP du paquet de demande ICMP dans le champ **ToS** . Les valeurs sont comprises entre 0 et 255. La valeur par défaut est 0. Ce champ contient des informations comme le retard, la préséance, la fiabilité, etc. Il peut être utilisé par d'autres périphériques du réseau pour le routage des politiques et des fonctionnalités telles que le débit d'accès garanti.

Étape 11 Saisissez le nombre de paquets qui sont envoyés dans le champ **Number of Packets** (Nombre de paquets). Les valeurs sont comprises entre 1 et 100. La valeur par défaut est 1 paquet.

Remarque Augmentez le nombre de paquets par défaut si vous craignez que la perte de paquets ne fasse faussement croire au périphérique Cisco Secure Firewall Threat Defense que l'adresse surveillée ne peut pas être atteinte.

Étape 12 Dans le champ **Monitored Address** (adresse surveillée), saisissez l'adresse IP dont la disponibilité est surveillée par l'opération d'ANS.

Étape 13 La liste des **zones disponibles** affiche à la fois les zones et les groupes d'interfaces. Dans la liste **Zones/Interfaces**, ajoutez les zones ou les groupes d'interfaces qui contiennent les interfaces par lesquelles le périphérique communique avec le poste de gestion. Pour spécifier une interface unique, vous devez créer une zone ou les groupes d'interfaces pour l'interface; voir Créer des objets de zone de sécurité et de groupe d'interface. L'hôte ne sera configuré sur un périphérique que si ce dernier comprend les interfaces ou les zones sélectionnées.

Étape 14 Cliquez sur **Save** (enregistrer).

Plage temporelle

Utilisez des objets de plage temporelle pour définir les périodes que vous utiliserez pour déterminer quand les règles s'appliquent.

Remarque Les listes de contrôle d'accès basées sur le temps sont également prises en charge dans Snort 3 à partir de centre de gestion 7.0.

Création d'objets de plages temporelles

Si vous souhaitez qu'une politique s'applique uniquement pendant une plage temporelle spécifiée, créez un objet de plage temporelle, puis spécifiez cet objet dans la politique. Notez que cet objet ne fonctionne que sur les périphériques défense contre les menaces .

Vous pouvez spécifier des objets de plage temporelle uniquement dans les types de politique répertoriés au bas de cette rubrique.

Remarque Le fuseau horaire représente l'heure locale du périphérique et est utilisé UNIQUEMENT pour appliquer les plages de temps dans les règles des politiques qui prennent en charge les plages de temps. Le fuseau horaire ne modifie pas l'heure configurée du périphérique. Pour vérifier la configuration, dans l'interface de ligne de commande défense contre les menaces , utilisez les commandes **show time-range timezone** et **show time** (consultez le guide Référence des commandes de défense contre les menaces de Cisco Secure Firewall). En outre, le fuseau horaire d'un châssis prévaut sur le fuseau horaire du centre de gestion.

Avant de commencer

Les plages de temps sont appliquées en fonction du fuseau horaire associé au périphérique qui traite le trafic. Par défaut, il s'agit de l'heure UTC. Pour modifier le fuseau horaire associé à un appareil, accédez à **Périphérique > Paramètres de la plateforme**.

Procédure

Étape 1 Choisissez **Objects (objets) > Object Management (gestion des objets)**.

Étape 2 Sélectionnez **URL** dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Time Range** (Ajouter la plage temporelle).

Étape 4 Saisissez les valeurs.

Suivez les directives suivantes :

- Si vous voyez une zone d'erreur rouge autour du nom d'objet que vous avez saisi, passez le curseur sur le champ **Name** (Nom) pour voir les restrictions de dénomination.
- Toutes les heures sont en heures UTC, sauf si vous spécifiez un fuseau horaire pour le périphérique dans **Périphérique > Paramètres de la plateforme**.
- Saisir les heures au format 24 heures. Par exemple, saisissez 13:30 pour 1:30 pm.
- Pour spécifier une seule plage continue, comme les heures typiques de fin de semaine (du vendredi à 17 h au lundi à 8 h, y compris le soir et la nuit), choisissez comme type de plage **Plage**.
- Pour définir une partie de plusieurs jours, par exemple du lundi au vendredi, de 8 h à 17 h (sauf les soirs, les nuits et les premières heures du matin), choisissez comme type de plage **Intervalle quotidien**.
- Vous pouvez spécifier jusqu'à 28 périodes pour un seul objet.
- Pour spécifier plusieurs heures du jour non contiguïtés ou différentes heures pour différents jours, créez plusieurs intervalles récurrents. Par exemple, pour appliquer une politique à tout moment en dehors des heures de travail normales, créez un seul objet de plage temporelle avec les deux intervalles récurrents suivants :

- A un Intervalle quotidien du lundi au vendredi, de 17 h à 8 h, et
- Une plage d'intervalles récurrents, du vendredi à 17 h au lundi à 8 h.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurez les plages de temps pour l'un des éléments suivants :

- Règles de contrôle d'accès
- Règles du préfiltre
- Règle de tunnel
- Politique de groupe VPN

Dans un objet de politique de groupe VPN, précisez l'objet de plage temporelle à l'aide du champ **Access Hours** (Heures d'accès). Pour de plus amples renseignements, consultez Configurer les objets de politique de groupe, à la page 122 et Options avancées de la politique de groupe, à la page 129.

Fuseau horaire

Pour spécifier un fuseau horaire local pour un périphérique géré, créez un objet de fuseau horaire et spécifiez-le dans la politique des paramètres de la plateforme du périphérique qui lui est affectée.

L'heure locale du périphérique est utilisée UNIQUEMENT pour appliquer des plages de temps dans les règles des politiques qui prennent en charge les plages de temps, telles que les politiques de contrôle d'accès, de préfiltre et de groupe VPN. Si vous n'attribuez pas de fuseau horaire à un périphérique, l'heure UTC est utilisée par défaut lors de l'application des plages de temps dans ces politiques. Aucune autre fonctionnalité du système n'utilise le fuseau horaire spécifié dans un objet de fuseau horaire.

Les objets de fuseau horaire sont pris en charge uniquement pour les périphériques défense contre les menaces .

Remarque Les listes de contrôle d'accès basées sur le temps sont également prises en charge dans Snort 3 à partir de centre de gestion 7.0.

Zone de tunnellisation

Une *zone de tunnel* représente certains types de textes bruts et l'intercommunication que vous balisez explicitement pour une analyse spéciale. Une zone de tunnel n'est pas un objet d'interface, même si vous pouvez l'utiliser comme contrainte d'interface dans certaines configurations.

Pour de plus amples renseignements, voir Zones de tunnel et préfiltrage.

URL

Important Pour connaître les bonnes pratiques en matière d'utilisation de cette option et d'options similaires dans les configurations Security Intelligence et les règles d'URL dans les politiques de contrôle d'accès et de QoS, consultez Options de filtrage manuel d'URL.

Un objet URL définit une seule URL ou adresse IP, alors qu'un objet de groupe d'URL peut définir plusieurs URL ou adresses. Vous pouvez utiliser les objets et les groupes URL à divers endroits de l'interface web du système, notamment pour les politiques de contrôle d'accès et les recherches d'événements.

Lors de la création d'objets URL, gardez les points suivants à l'esprit :

- Si vous n'incluez pas de chemin (c'est-à-dire qu'il n'y a pas de caractères / dans l'URL), la correspondance est basée sur le nom d'hôte du serveur uniquement. Si vous incluez un ou plusieurs caractères /, la chaîne URL complète est utilisée pour une correspondance de sous-chaîne. Ainsi, une URL est considérée comme en correspondance si l'une des conditions suivantes est remplie :
  - La chaîne se trouve au début de l'URL.
  - La chaîne suit un point.
  - La chaîne contient un point au début.
  - La chaîne suit les caractères ://.

  Par exemple, ign.com correspond à ign.com ou www.ign.com, mais pas à versign.com.

Remarque Nous vous recommandons de ne pas utiliser le filtrage manuel d'URL pour bloquer ou autoriser des pages Web individuelles ou des parties de sites (c'est-à-dire les chaînes URL avec des caractères /), car les serveurs peuvent être réorganisés et les pages déplacées vers de nouveaux chemins.

- Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS). En d'autres termes, si vous bloquez un site Web, les trafics HTTP et HTTPS vers ce site Web sont bloqués, sauf si vous utilisez une condition d'application pour cibler un protocole spécifique. Lors de la création d'un objet URL, vous n'avez pas besoin de préciser le protocole lors de la création d'un objet. Par exemple, utilisez exemple.com plutôt que http://exemple.com.
- Si vous prévoyez utiliser un objet URL pour faire correspondre le trafic HTTPS dans une règle de contrôle d'accès, créez l'objet en utilisant le nom usuel du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic. De plus, le système ne tient pas compte des sous-domaines du nom usuel du sujet. N'incluez donc pas les informations de ce sous-domaine. Par exemple, utilisez exemple.com plutôt que www.exemple.com.

  Cependant, veuillez comprendre que le nom usuel du sujet dans le certificat peut être complètement sans rapport avec le nom de domaine d'un site Web. Par exemple, le nom usuel du sujet dans le certificat pour youtube.com est *.Google.com (bien entendu, cela peut changer à tout moment). Vous obtiendrez des résultats plus cohérents si vous utilisez la politique de déchiffrement SSL pour déchiffrer le trafic HTTPS afin que les règles de filtrage d'URL fonctionnent sur le trafic déchiffré.

Remarque Les objets URL ne correspondront pas au trafic HTTPS si le navigateur reprend une session TLS, car les informations de certificat ne sont plus disponibles. Ainsi, même si vous configurez soigneusement l'objet URL, vous pourriez obtenir des résultats incohérents pour les connexions HTTPS.

Création d'objets URL

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **URL** dans la liste des types d'objets.

Étape 3 Sélectionnez **Add Object (Ajouter un objet)** dans le menu déroulant **Add URL (Ajouter une URL)**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Vous pouvez également saisir une **Description**.

Étape 6 Saisissez **l'URL** ou l'adresse IP.

Étape 7 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 13.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Ensemble de variables

La plupart des variables représentent des valeurs couramment utilisées dans les règles de prévention des intrusions pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles, Mises à niveau des profils adaptatifs, et de règles dynamiques.

Astuces Les règles de préprocesseur peuvent déclencher des événements quels que soient les hôtes définis par les variables de réseau utilisées dans les règles de prévention des intrusions.

Vous utilisez des ensembles de variables pour gérer, personnaliser et regrouper vos variables. Vous pouvez utiliser l'ensemble de variables par défaut fourni par le système ou créer vos propres ensembles personnalisés. Dans n'importe quel ensemble, vous pouvez modifier des variables par défaut prédéfinies et ajouter et modifier des variables définies par l'utilisateur.

La plupart des règles d'objet partagé et des règles de texte standard fournies par le système utilisent des variables par défaut prédéfinies pour définir les réseaux et les numéros de port. Par exemple, la majorité des règles utilisent la variable `$HOME_NET` pour préciser le réseau protégé et la variable `$EXTERNAL_NET`pour préciser le réseau non protégé (ou externe). En outre, les règles spécialisées utilisent souvent d'autres variables prédéfinies. Par exemple, les règles qui détectent les exploits contre les serveurs Web utilisent les variables `$HTTP_SERVERS` et `$HTTP_PORTS`.

Les règles sont plus efficaces lorsque les variables reflètent avec plus de précision votre environnement réseau. Vous devez au minimum modifier les variables par défaut de l'ensemble par défaut. En s'assurant qu'une variable comme `$HOME_NET` définit correctement votre réseau et que `$HTTP_SERVERS` inclut tous les serveurs Web de ce dernier, le traitement est optimisé et tous les systèmes pertinents sont surveillés pour détecter toute activité suspecte.

Pour utiliser vos variables, vous liez des ensembles de variables aux politiques de prévention des intrusions associées aux règles de contrôle d'accès ou à l'action par défaut d'une politique de contrôle d'accès. Par défaut, l'ensemble de variables par défaut est lié à toutes les politiques de prévention des intrusions utilisées par les politiques de contrôle d'accès.

L'ajout d'une variable à un ensemble l'ajoute à tous les ensembles; c'est-à-dire que chaque ensemble de variables est un ensemble de toutes les variables actuellement configurées sur votre système. Dans n'importe quel ensemble de variables, vous pouvez ajouter des variables définies par l'utilisateur et personnaliser la valeur de n'importe quelle variable.

Au départ, le système fournit un seul ensemble de variables par défaut composé de valeurs par défaut prédéfinies. Chaque variable de l'ensemble par défaut est initialement définie à sa valeur par défaut, qui, pour une variable prédéfinie, est la valeur définie par Talos Intelligence Group et fournie dans les mises à jour de règles.

Bien que vous puissiez laisser les variables prédéfinies configurées à leurs valeurs par défaut, Cisco vous recommande de modifier un sous-ensemble de variables prédéfinies.

Vous pouvez travailler avec les variables uniquement dans l'ensemble par défaut, mais dans de nombreux cas, vous pouvez tirer profit de l'ajout d'un ou de plusieurs ensembles personnalisés, de la configuration de différentes valeurs de variables dans différents ensembles, et peut-être même de l'ajout de nouvelles variables.

Lorsque vous utilisez plusieurs ensembles, il est important de se rappeler que la *valeur actuelle* de toute variable de l'ensemble par défaut détermine la *valeur par défaut* de la variable dans tous les autres ensembles.

Lorsque vous sélectionnez **Ensembles de variables** dans la page Gestionnaire d'objets, le gestionnaire d'objets répertorie l'ensemble de variables par défaut et les ensembles personnalisés que vous avez créés.

Sur un système nouvellement installé, l'ensemble de variables par défaut est composé uniquement des variables par défaut prédéfinies par Cisco.

Chaque ensemble de variables comprend les variables par défaut fournies par le système et toutes les variables personnalisées que vous avez ajoutées à partir d'un ensemble de variables. Notez que vous pouvez modifier l'ensemble par défaut, mais que vous ne pouvez pas renommer ou supprimer l'ensemble par défaut.

Dans un déploiement multidomaine, le système génère un ensemble de variables par défaut pour chaque sous-domaine.

Mise en garde L'importation d'une politique de contrôle d'accès ou de prévention des intrusions remplace les variables par défaut existantes dans l'ensemble de variables par défaut par les variables par défaut importées. Si votre ensemble de variables par défaut existant contient une variable personnalisée qui ne figure pas dans l'ensemble de variables par défaut importé, l'unique variable est conservée.

Sujets connexes

Gestion des variables, à la page 113
Gestion des ensembles de variables, à la page 112

Ensembles de variables dans les politiques de prévention des intrusions

Par défaut, le système Firepower lie l'ensemble de variables par défaut à toutes les politiques de prévention des intrusions utilisées dans une politique de contrôle d'accès. Lorsque vous déployez une politique de contrôle d'accès qui fait appel à une politique de prévention des intrusions, les règles de prévention des intrusions que vous avez activées dans la politique de prévention des intrusions utilisent les valeurs de variables de l'ensemble de variables liées.

Lorsque vous modifiez un ensemble de variables personnalisées utilisé par une politique de prévention des intrusions dans une politique de contrôle d'accès, le système affiche l'état de cette politique comme obsolète dans la page Access Control Policy. Vous devez déployer la politique de contrôle d'accès pour mettre en œuvre les modifications dans votre ensemble de variables. Lorsque vous modifiez l'ensemble par défaut, le système reflète l'état de toutes les politiques de contrôle d'accès qui utilisent des politiques de prévention des intrusions comme obsolètes et vous devez redéployer toutes les politiques de contrôle d'accès pour implémenter vos modifications.

Variables

Les variables appartiennent à l'une des catégories suivantes :

Variables par défaut

Les variables fournies par le système Firepower Vous ne pouvez pas renommer ou supprimer une variable par défaut, et vous ne pouvez pas modifier sa valeur par défaut. Cependant, vous pouvez créer une version personnalisée d'une variable par défaut.

Variables personnalisées

les variables que vous créez. Ces variables peuvent inclure :

- *des variables personnalisées par défaut*

  Lorsque vous modifiez la valeur d'une variable par défaut, le système la déplace de la zone des variables par défaut vers la zone des variables personnalisées. Étant donné que les valeurs des variables de l'ensemble par défaut déterminent les valeurs par défaut des variables dans les ensembles personnalisés, la personnalisation d'une variable par défaut dans l'ensemble par défaut modifie la valeur par défaut de la variable dans tous les autres ensembles.

- *des variables définies par l'utilisateur*

Vous pouvez ajouter et supprimer vos propres variables, personnaliser leurs valeurs au sein de différents ensembles de variables et réinitialiser les variables personnalisées à leurs valeurs par défaut. Lorsque vous réinitialisez une variable définie par l'utilisateur, elle reste dans la zone des variables personnalisées.

Les variables définies par l'utilisateur peuvent être de l'un des types suivants :

- Les variables *de réseau* précisent les adresses IP des hôtes dans votre trafic réseau.
- Les variables de *port* précisent les ports TCP ou UDP dans le trafic réseau, y compris la valeur `any (quelconque)` des deux types.

Par exemple, si vous créez des règles de texte standard personnalisées, vous pouvez également ajouter vos propres variables définies par l'utilisateur pour refléter plus précisément votre trafic ou comme raccourcis pour simplifier le processus de création de règles. Sinon, si vous créez une règle selon laquelle vous souhaitez inspecter le trafic dans la « zone démilitarisée » (ou DMZ) uniquement, vous pouvez créer une variable nommée `$DMZ` dont la valeur répertorie les adresses IP des serveurs qui sont exposées. Vous pouvez ensuite utiliser la variable `$DMZ` dans toute règle écrite pour cette zone.

Variables avancées

Les variables fournies par le système Firepower dans des conditions précises Ces variables ont un déploiement très limité.

Variables prédéfinies par défaut

Par défaut, le système Firepower fournit un seul ensemble de variables par défaut, qui comprend des variables par défaut prédéfinies. Talos Intelligence Group utilise les mises à jour de règles pour fournir des règles de prévention des intrusions nouvelles et mises à jour et d'autres éléments de politique de prévention des intrusions, y compris les variables par défaut.

Étant donné que de nombreuses règles de prévention des intrusions fournies par le système utilisent des variables par défaut prédéfinies, vous devez définir des valeurs appropriées pour ces variables. Selon la façon dont vous utilisez les ensembles de variables pour identifier le trafic sur votre réseau, vous pouvez modifier les valeurs de ces variables par défaut dans n'importe quel ensemble de variables ou dans tous.

Mise en garde L'importation d'une politique de contrôle d'accès ou de prévention des intrusions remplace les variables par défaut existantes dans l'ensemble de variables par défaut par les variables par défaut importées. Si votre ensemble de variables par défaut existant contient une variable personnalisée qui ne figure pas dans l'ensemble de variables par défaut importé, l'unique variable est conservée.

Le tableau suivant décrit les variables fournies par le système et indique celles que vous modifiez généralement. Pour obtenir de l'aide sur la façon d'adapter les variables à votre réseau, communiquez avec les services professionnels ou le service d'assistance.

Tableau 3 : Variables fournies par le système

Nom de variable	Description	Modifier?
`$AIM_SERVERS`	Définit les serveurs AOL de messagerie instantanée connus (AIM) et est utilisé dans les règles basées sur le clavardage et les règles qui recherchent les exploits AIM.	Non exigé

Nom de variable	Description	Modifier?
`$DNS_SERVERS`	Définit les serveurs DNS (Domain Name Service). Si vous créez une règle qui affecte spécifiquement les serveurs DNS, vous pouvez utiliser la variable `$DNS_SERVERS` comme adresse IP de destination ou de source.	Non requis dans l'ensemble de règles actuel.
`$EXTERNAL_NET`	Définit le réseau que le système Firepower considère comme le réseau non protégé et est utilisé dans de nombreuses règles pour définir le réseau externe.	Oui, vous devez définir correctement `$HOME_NET`, puis exclure `$HOME_NET` comme valeur pour `$EXTERNAL_NET`.
`$FILE_DATA_PORTS`	Définit les ports non chiffrés utilisés dans les règles de prévention des intrusions qui détectent les fichiers dans un flux réseau.	Non exigé
`$FTP_PORTS`	Définit les ports des serveurs FTP de votre réseau et est utilisé pour les règles d'exploit de serveur FTP.	Oui, si vos serveurs FTP utilisent des ports autres que les ports par défaut (vous pouvez afficher les ports par défaut dans l'interface Web).
`$GTP_PORTS`	Définit les ports du canal de données où le décodeur de paquets extrait la charge utile à l'intérieur d'une PDU GTP (General Packet Radio Service [GPRS] Tunneling Protocol).	Non exigé
`$HOME_NET`	Définit le réseau que la politique de prévention des intrusions associée surveille et est utilisé dans de nombreuses règles pour définir le réseau interne.	Oui, pour inclure les adresses IP de votre réseau interne.
`$HTTP_PORTS`	Définit les ports des serveurs Web de votre réseau et est utilisé pour les règles d'exploit de serveur Web.	Oui, si vos serveurs Web utilisent des ports autres que les ports par défaut (vous pouvez afficher les ports par défaut dans l'interface Web).
`$HTTP_SERVERS`	Définit les serveurs Web de votre réseau. Utilisé dans les règles d'exploit de serveur Web.	Oui, si vous exécutez des serveurs HTTP.
`$ORACLE_PORTS`	Définit les ports du serveur de base de données Oracle sur votre réseau et est utilisé dans les règles qui analysent les attaques sur les bases de données Oracle.	Oui, si vous utilisez des serveurs Oracle.
`$SHELLCODE_PORTS`	Définit les ports sur lesquels vous souhaitez que le système analyse les exploits de code Shell et est utilisé dans les règles qui détectent les exploits qui utilisent le code Shell.	Non exigé
`$SIP_PORTS`	Définit les ports des serveurs SIP sur votre réseau et est utilisé pour les règles d'exploitation SIP.	Non exigé
`$SIP_SERVERS`	Définit les serveurs SIP sur votre réseau et est utilisé dans les règles qui traitent des exploits ciblés par SIP.	Oui, si vous exécutez des serveurs SIP, vous devez définir correctement `$HOME_NET`, puis inclure `$HOME_NET` comme valeur pour `$SIP_SERVERS`.

Nom de variable	Description	Modifier?
`$SMTP_SERVERS`	Définit les serveurs SMTP sur votre réseau et est utilisé dans les règles qui traitent des exploitations qui ciblent les serveurs de messagerie.	Oui, si vous utilisez des serveurs SMTP.
`$SNMP_SERVERS`	Définit les serveurs SNMP sur votre réseau et est utilisé dans les règles qui analysent les attaques sur les serveurs SNMP.	Oui, si vous utilisez des serveurs SNMP.
`$SNORT_BPF`	Identifie une variable avancée existante qui s'affiche uniquement sur votre système dans une version du logiciel Firepower antérieure à la version 5.3.0 que vous avez par la suite mise à niveau vers la version 5.3.0 ou une version ultérieure.	Non, vous pouvez uniquement afficher ou supprimer cette variable. Vous ne pouvez pas le modifier ou le récupérer après l'avoir supprimé.
`$SQL_SERVERS`	Définit les serveurs de base de données sur votre réseau et est utilisé dans les règles qui traitent des exploitations ciblées par la base de données.	Oui, si vous exécutez des serveurs SQL.
`$SSH_PORTS`	Définit les ports des serveurs SSH sur votre réseau et est utilisé pour les règles d'exploitation des serveurs SSH.	Oui, si vos serveurs SSH utilisent des ports autres que le port par défaut (vous pouvez afficher les ports par défaut dans l'interface Web).
`$SSH_SERVERS`	Définit les serveurs SSH sur votre réseau et est utilisé dans les règles qui traitent des exploits ciblés par SSH.	Oui, si vous exécutez des serveurs SSH, vous devez définir correctement `$HOME_NET`, puis inclure `$HOME_NET` comme valeur pour `$SSH_SERVERS`.
`$TELNET_SERVERS`	Définit les serveurs Telnet connus sur votre réseau et est utilisé dans les règles qui traitent des exploits ciblés par les serveurs Telnet.	Oui, si vous utilisez des serveurs Telnet.
`$USER_CONF`	Fournit un outil général qui vous permet de configurer une ou plusieurs fonctionnalités non disponibles autrement via l'interface Web. Les configurations `$USER_CONF` conflictuelles ou en double arrêtent le système.	Non, uniquement comme indiqué dans la description d'une fonctionnalité ou avec les conseils du service d'assistance.

Variables du réseau

Les variables de réseau représentent des adresses IP que vous pouvez utiliser dans les règles de prévention des intrusions que vous activez dans une politique de prévention des intrusions et dans les suppressions de règles de politique de prévention des intrusions, les états des règles dynamiques et Mises à niveau des profils adaptatifs. Les variables de réseau se distinguent des objets et des groupes d'objets réseau en ce que les variables de réseau sont propres aux politiques et aux règles de prévention des intrusions, tandis que vous pouvez utiliser des objets et des groupes de réseau pour représenter des adresses IP à divers endroits de l'interface Web du système, y compris les politiques de contrôle d'accès, , règles de prévention des intrusions, règles de découverte de réseau, recherches d'événements, rapports, etc.

Vous pouvez utiliser des variables de réseau dans les configurations suivantes pour préciser les adresses IP des hôtes sur votre réseau :

- règles de prévention des intrusions : les champs d'en-tête des adresses **IP source** et **IP de destination** des règles de prévention des intrusions vous permettent de restreindre l'inspection des paquets aux paquets provenant ou destinés à des adresses IP spécifiques.
- suppressions : le champ **Network** (Réseau) dans les suppressions de règles de prévention des intrusions source ou de destination vous permet de supprimer les notifications d'incidents d'intrusion lorsqu'une adresse IP ou une plage d'adresses IP spécifique déclenche une règle de prévention des intrusions ou un préprocesseur.
- états de règles dynamiques : le champ **Réseau** dans les états de règles dynamiques de source ou de destination vous permet de détecter lorsqu'un trop grand nombre de correspondances pour une règle de prévention des intrusions ou une règle de préprocesseur se produisent dans une période donnée.
- Mises à niveau des profils adaptatifs - lorsque vous activez les mises à jour de profils adaptatifs, le champ **Networks** (réseaux) des profils adaptatifs identifie les hôtes pour lesquels vous souhaitez améliorer le réassemblage des fragments de paquets et des flux TCP dans les déploiements passifs.

Lorsque vous utilisez des variables dans les champs mentionnés dans cette section, l'ensemble de variables que vous liez à une politique de prévention des intrusions détermine les valeurs des variables dans le trafic réseau gérées par une politique de contrôle d'accès qui utilise la politique de prévention des intrusions.

Vous pouvez ajouter n'importe quelle combinaison des configurations réseau suivantes à une variable :

- toute combinaison de variables de réseau, d'objets réseau et de groupes d'objets réseau que vous sélectionnez dans la liste des réseaux disponibles
- les objets de réseau individuels que vous ajoutez à partir de la page Nouvelle variable ou de la page Modifier la variable, et que vous pouvez ensuite ajouter à votre variable et à d'autres variables existantes et futures
- Adresses IP uniques, littérales ou blocs d'adresses

  Vous pouvez répertorier plusieurs adresses IP littérales et blocs d'adresses en les ajoutant individuellement. Vous pouvez répertorier les adresses IPv4 et IPv6 et les blocs d'adresses seuls ou dans n'importe quelle combinaison. Lorsque vous spécifiez des adresses IPv6, vous pouvez utiliser n'importe quelle convention d'adressage définie dans la RFC 4291.

La valeur par défaut pour les réseaux inclus dans toute variable que vous ajoutez est le mot `any`, qui indique toute adresse IPv4 ou IPv6. La valeur par défaut pour les réseaux exclus est `none`, ce qui indique l'absence de réseau. Vous pouvez également spécifier l'adresse `::` dans une valeur littérale pour indiquer toute adresse IPv6 dans la liste des réseaux inclus, ou aucune adresse IPv6 dans la liste des exclusions.

L'ajout de réseaux à la liste des exclus annule les adresses et les blocs d'adresses spécifiés. C'est-à-dire que vous pouvez mettre en correspondance n'importe quelle adresse IP, à l'exception de l'adresse IP ou des blocs d'adresses exclus.

Par exemple, en excluant l'adresse littérale `192.168.1.1`, vous spécifiez toute adresse IP autre que 192.168.1.1 et en excluant `2001:db8:ca2e::fa4c`, toute adresse IP autre que 2001:db8:ca2e::fa4c.

Vous pouvez exclure toute combinaison de réseaux à l'aide de réseaux littéraux ou disponibles. Par exemple, l'exclusion des valeurs littérales `192.168.1.1` et `192.168.1.5` *inclut* toute adresse IP autre que 192.168.1.1 ou 192.168.1.5. C'est-à-dire que le système interprète cela comme « **not** 192.168.1.1 **and not** 192.168.1.5 », ce qui correspond à toute adresse IP autre que celles indiquées entre parenthèses.

Tenez compte des points suivants lors de l'ajout ou de la modification de variables de réseau :

- Vous ne pouvez pas logiquement exclure la valeur `any` qui, si elle était exclue, indiquerait l'absence d'adresse. Par exemple, vous ne pouvez pas ajouter une variable avec la valeur « `any` » à la liste des réseaux exclus.
- Les variables de réseau identifient le trafic pour la règle de prévention des intrusions et les fonctionnalités de politique de prévention des intrusions précisées. Notez que les règles de préprocesseur peuvent déclencher des événements quels que soient les hôtes définis par les variables de réseau utilisées dans les règles de prévention des intrusions.
- Les valeurs exclues doivent correspondre à un sous-ensemble de valeurs incluses. Par exemple, vous ne pouvez pas inclure le bloc d'adresse 192.168.5.0/24 et exclure 192.168.6.0/24.

Variables du port

Les variables de port représentent les ports TCP et UDP que vous pouvez utiliser dans les champs d'en-tête du **port source** et du **port de destination** des règles de prévention des intrusions que vous activez dans une politique de prévention des intrusions. Les variables de port se différencient des objets de port et des groupes d'objets de port en ce que les variables de port sont propres aux règles de prévention des intrusions. Vous pouvez utiliser des objets et des groupes de ports à divers endroits de l'interface des systèmes Web, notamment pour les politiques de contrôle d'accès, les règles d'identité, les règles de découverte du réseau, les variables de port et les recherches d'événements.

Vous pouvez utiliser des variables de port dans les champs d'en-tête du **port source** et du **port de destination** de la règle de prévention des intrusions pour restreindre l'inspection des paquets aux paquets provenant ou destinés à des ports TCP ou UDP spécifiques.

Lorsque vous utilisez des variables dans ces champs, l'ensemble de variables que vous liez à la politique de prévention des intrusions associée à une règle ou une politique de contrôle d'accès détermine les valeurs de ces variables dans le trafic réseau où vous déployez la politique de contrôle d'accès.

Vous pouvez ajouter n'importe quelle combinaison des configurations de ports suivantes à une variable :

- toute combinaison de variables de port et d'objets de port que vous sélectionnez dans la liste des ports disponibles

  Notez que la liste des ports disponibles n'affiche pas les groupes d'objets de port et que vous ne pouvez pas les ajouter aux variables.

- objets de port individuels que vous ajoutez à partir de la page Nouvelle variable ou Modifier la variable, et que vous pouvez ensuite ajouter à votre variable et à d'autres variables existantes et futures

  Seuls les ports TCP et UDP, y compris la valeur `any` pour les deux types, sont des valeurs de variable valides. Si vous utilisez la page créer ou modifier les variables pour ajouter un objet de port valide qui n'est pas une valeur de variable valide, l'objet est ajouté au système, mais ne s'affiche pas dans la liste des objets disponibles. Lorsque vous utilisez le gestionnaire d'objets pour modifier un objet de port utilisé dans une variable, vous pouvez uniquement remplacer sa valeur par une valeur de variable valide.

- Valeurs de port littéral unique et plages de ports

  Vous devez séparer les plages de ports par un tiret (-). Les plages de ports indiquées par un deux-points (:) sont prises en charge pour la compatibilité ascendante, mais vous ne pouvez pas utiliser les deux-points dans les variables de port que vous créez.

  Vous pouvez répertorier plusieurs valeurs et plages de port littérales en les ajoutant individuellement, dans n'importe quelle combinaison.

Tenez compte des points suivants lors de l'ajout ou de la modification des variables de port :

- La valeur par défaut des ports inclus dans toute variable que vous ajoutez est le mot `any`, qui indique n'importe quel port ou plage de ports. La valeur par défaut pour les ports exclus est `none`, ce qui indique l'absence de ports.

Astuces Pour créer une variable avec la valeur `any`, nommez et enregistrez la variable sans ajouter de valeur spécifique.

- Vous ne pouvez pas logiquement exclure la valeur `any` qui, si elle était exclue, indiquerait l'absence de ports. Par exemple, vous ne pouvez pas enregistrer un ensemble de variables lorsque vous ajoutez une variable avec la valeur `any` à la liste des ports exclus.
- L'ajout de ports à la liste des exclus annule les ports et les plages de ports spécifiés. Autrement dit, vous pouvez mettre en correspondance n'importe quel port, à l'exception des ports ou des plages de ports exclus.
- Les valeurs exclues doivent correspondre à un sous-ensemble de valeurs incluses. Par exemple, vous ne pouvez pas inclure la plage de ports 10 à 50 et exclure le port 60.

Variables avancées

Les variables avancées vous permettent de configurer des fonctionnalités que vous ne pouvez pas configurer autrement via l'interface Web. Le système ne fournit actuellement qu'une seule variable avancée, la variable USER_CONF.

USER_CONF

USER_CONF fournit un outil général qui vous permet de configurer une ou plusieurs fonctionnalités non disponibles autrement via l'interface Web.

Mise en garde N'utilisez **pas** la variable avancée USER_CONF pour configurer une fonctionnalité de politique de prévention des intrusions, à moins que le service d'assistance ou ne vous le demande dans la description de la fonctionnalité. Les configurations conflictuelles ou en double arrêteront le système.

Lors de la modification de USER_CONF, vous pouvez taper jusqu'à 4096 caractères au total sur une seule ligne; la ligne retourne automatiquement à la fin. Vous pouvez inclure n'importe quel nombre d'instructions ou de lignes valides jusqu'à ce que vous atteigniez la longueur maximale de 8 192 caractères pour une variable ou une limite physique, comme l'espace disque. Utilisez la barre oblique inverse (\) après tout arguments complets dans une directive de commande.

La réinitialisation de USER_CONF le vide.

Réinitialisation de variable

Vous pouvez réinitialiser une variable à sa valeur par défaut dans la page de nouvelle définition de variable ou dans la page de modification des variables. Le tableau suivant résume les principes de base de la réinitialisation des variables.

Tableau 4 : Valeurs de réinitialisation variables

Réinitialisation de ce type de variable...	Dans cet ensemble, saisissez...	Le réinitialise à...
par défaut	par défaut	la valeur de mise à jour de la règle
Définie par l'utilisateur	par défaut	`Tous`
par défaut ou défini par l'utilisateur	personnalisé	la valeur définie par défaut actuelle (modifiée ou non)

La réinitialisation d'une variable dans un ensemble personnalisé la réinitialise simplement à la valeur actuelle pour cette variable dans l'ensemble par défaut.

À l'inverse, la réinitialisation ou la modification de la valeur d'une variable de l'ensemble par défaut met toujours à jour la valeur par défaut de cette variable dans tous les ensembles personnalisés. Lorsque l'icône de réinitialisation est grisée, ce qui indique que vous ne pouvez pas réinitialiser la variable, cela signifie que la variable n'a pas de valeur personnalisée dans cet ensemble. À moins que vous n'ayez personnalisé la valeur d'une variable dans un ensemble personnalisé, une modification apportée à la variable dans l'ensemble par défaut met à jour la valeur utilisée dans toute politique de prévention des intrusions à laquelle vous avez lié l'ensemble de variables.

Remarque Il est recommandé lorsque vous modifiez une variable dans l'ensemble par défaut pour évaluer comment la modification affecte toute politique de prévention des intrusions qui utilise la variable dans un ensemble personnalisé lié, en particulier lorsque vous n'avez pas personnalisé la valeur de la variable dans l'ensemble personnalisé.

Vous pouvez passer votre curseur sur l'**icône de réinitialisation** dans un ensemble de variables pour afficher la valeur de réinitialisation. Lorsque la valeur personnalisée et la valeur de réinitialisation sont identiques, cela indique l'un des éléments suivants :

- vous êtes dans l'ensemble personnalisé ou par défaut où vous avez ajouté la variable avec la valeur `any`
- vous vous trouvez dans l'ensemble personnalisé où vous avez ajouté la variable avec une valeur explicite et choisi d'utiliser la valeur configurée comme valeur par défaut

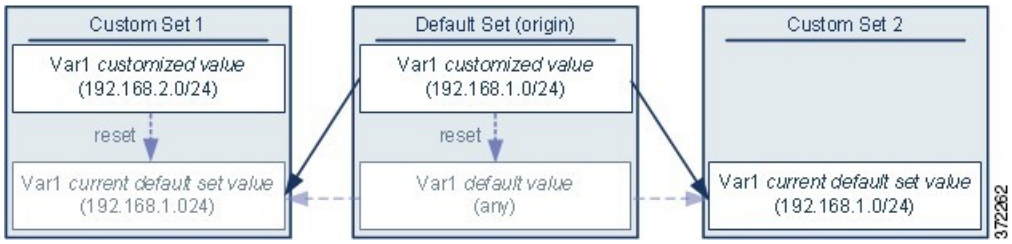
Ajout de variables aux ensembles

L'ajout d'une variable à un ensemble de variables l'ajoute à tous les autres ensembles. Lorsque vous ajoutez une variable à partir d'un ensemble personnalisé, vous devez choisir d'utiliser la valeur configurée comme valeur personnalisée dans l'ensemble par défaut :

- **Si vous utilisez la valeur configurée** (par exemple, 192.168.0.0/16), la variable est ajoutée à l'ensemble par défaut en utilisant la valeur configurée comme valeur personnalisée avec une valeur par défaut `any` (quelconque). Étant donné que la valeur actuelle de l'ensemble par défaut détermine la valeur par défaut des autres ensembles, la valeur initiale par défaut des autres ensembles personnalisés est la valeur configurée (qui dans cet exemple est 192.168.0.0/16).
- **Si vous n'utilisez pas la valeur configurée**, la variable est ajoutée à l'ensemble par défaut en utilisant uniquement la valeur par défaut `any` et, par conséquent, la valeur par défaut initiale dans les autres ensembles personnalisés est `any`.

Exemple : ajout de variables définies par l'utilisateur aux ensembles par défaut

Le diagramme suivant illustre les interactions entre ensembles lorsque vous ajoutez la variable définie par l'utilisateur `Var1` à l'ensemble par défaut avec la valeur `192.168.1.0/24`.



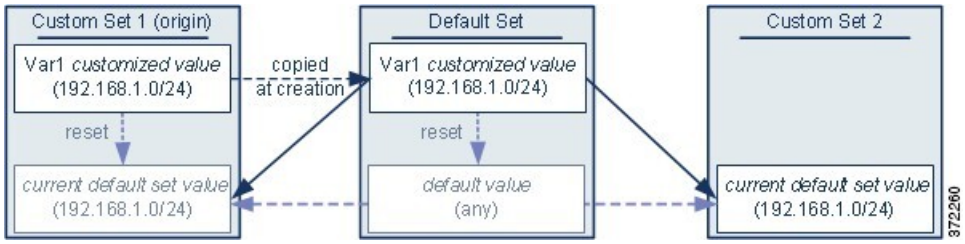
Vous pouvez personnaliser la valeur de `Var1` dans n'importe quel ensemble. Dans l'ensemble personnalisé 2 où `Var1` n'a pas été personnalisé, sa valeur est `192.168.1.0/24`. Dans l'ensemble personnalisé 1, la valeur personnalisée `192.168.2.0/24` de `Variable 1` remplace la valeur par défaut. La réinitialisation d'une variable définie par l'utilisateur dans l'ensemble par défaut réinitialise sa valeur par défaut à `any` (n'importe quel) dans tous les ensembles.

Il est important de noter que dans cet exemple, si vous ne mettez pas à jour `Var1` dans l'ensemble personnalisé 2, la personnalisation ou la réinitialisation de la valeur par défaut `Var1` dans l'ensemble personnalisé met à jour en conséquence la valeur par défaut actuelle de `Var1` dans l'ensemble personnalisé 2, ce qui a une incidence sur toute politique de prévention des intrusions liée à l'ensemble de variables.

Bien que cela ne soit pas illustré dans l'exemple, notez que les interactions entre les ensembles sont les mêmes pour les variables définies par l'utilisateur et les variables par défaut, sauf que la réinitialisation d'une variable par défaut dans l'ensemble par défaut la réinitialise à la valeur configurée par Cisco dans la mise à jour de la règle actuelle.

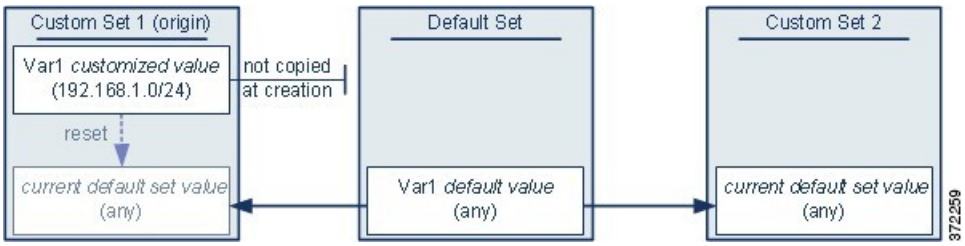
Exemple : ajout de variables définies par l'utilisateur aux ensembles personnalisés

Les deux exemples suivants illustrent les interactions entre des ensembles de variables lorsque vous ajoutez une variable définie par l'utilisateur à un ensemble personnalisé. Lorsque vous enregistrez la nouvelle variable, un message vous demande si vous souhaitez utiliser la valeur configurée comme valeur par défaut pour les autres ensembles. Dans l'exemple suivant, vous choisissez **d'utiliser** la valeur configurée.



Notez que, à l'exception de l'origine de `Var1` de l'ensemble personnalisé 1, cet exemple est identique à l'exemple ci-dessus dans lequel vous avez ajouté `Var1` à l'ensemble par défaut. L'ajout de la valeur personnalisée `192.168.1.0/24` en tant que `Var1` à l'ensemble personnalisé 1 copie la valeur dans l'ensemble par défaut en tant que valeur personnalisée avec une valeur par défaut `quelconque`. Par la suite, les valeurs de `Var1` et les interactions sont les mêmes que si vous aviez ajouté `Var1` à l'ensemble par défaut. Comme pour l'exemple précédent, gardez à l'esprit que la poursuite de la personnalisation ou de la réinitialisation de `Var1` dans l'ensemble par défaut met à jour en conséquence la valeur par défaut actuelle de `var1` dans l'ensemble personnalisé 2, ce qui a une incidence sur toute politique de prévention des intrusions liée à l'ensemble de variables.

Dans l'exemple suivant, vous ajoutez `Var1` avec la valeur de 192.168.1.0/24 à l'ensemble personnalisé 1 comme dans l'exemple précédent, mais vous choisissez **de ne pas utiliser** la valeur configurée `Var1` comme valeur par défaut dans les autres ensembles.



Cette approche ajoute `Var1` à tous les ensembles avec la valeur par défaut `any` quelconque). Après avoir ajouté `Var1` vous pouvez personnaliser sa valeur dans n'importe quel ensemble. Un avantage de cette approche est que, en ne personnalisant pas `Var1` dans l'ensemble par défaut, vous réduisez le risque de personnaliser la valeur dans l'ensemble par défaut et de modifier ainsi par inadvertance la valeur actuelle dans un ensemble comme l'ensemble personnalisé 2 où vous n'avez pas personnalisé `Var1`.

Variables imbriquées

Vous pouvez imbriquer des variables tant qu'il ne s'agit pas d'une imbrication circulaire. Les variables inversées imbriquées ne sont pas prises en charge.

Variables imbriquées valides

Dans cet exemple, SMTP_SERVERS, HTTP_SERVERS et OTHER_SERVERS sont des variables imbriquées valides.

Variable	Type	Réseaux inclus	Réseaux exclus
SMTP_SERVERS	personnalisée par défaut	10.1.1.1	—
HTTP_SERVERS	personnalisée par défaut	10.1.1.2	—
OTHER_SERVERS	Définie par l'utilisateur	10.2.2.0/24	—
HOME_NET	personnalisée par défaut	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

Variable imbriquée non valide

Dans cet exemple, HOME_NET est une variable imbriquée non valide, car l'imbrication de HOME_NET est circulaire; c'est-à-dire que la définition de OTHER_SERVERS comprend HOME_NET, de sorte que vous imbriqueriez HOME_NET en elle-même.

Variable	Type	Réseaux inclus	Réseaux exclus
SMTP_SERVERS	personnalisée par défaut	10.1.1.1	—
HTTP_SERVERS	personnalisée par défaut	10.1.1.2	—

Variable	Type	Réseaux inclus	Réseaux exclus
OTHER_SERVERS	Définie par l'utilisateur	10.2.2.0/24 HOME_NET	—
HOME_NET	personnalisée par défaut	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

Une variable imbriquée et inversée non prise en charge

Comme les variables imbriquées et inversées ne sont pas prises en charge, vous ne pouvez pas utiliser la variable NONCORE_NET comme l'illustre cet exemple pour représenter des adresses IP qui se trouvent à l'extérieur de vos réseaux protégés.

Variable	Type	Réseaux inclus	Réseaux exclus
HOME_NET	personnalisée par défaut	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	personnalisée par défaut	—	HOME_NET
DMZ_NET	Définie par l'utilisateur	10.4.0.0/16	—
NOT_DMZ_NET	Définie par l'utilisateur	—	DMZ_NET
NONCORE_NET	Définie par l'utilisateur	EXTERNAL_NET NOT_DMZ_NET	—

Option de remplacement d'une variable inversée imbriquée non prise en charge

Comme alternative à l'exemple ci-dessus, vous pouvez représenter les adresses IP qui sont en dehors de vos réseaux protégés en créant la variable NONCORE_NET comme indiqué dans cet exemple.

Variable	Type	Réseaux inclus	Réseaux exclus
HOME_NET	personnalisée par défaut	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	Définie par l'utilisateur	10.4.0.0/16	—
NONCORE_NET	Définie par l'utilisateur	—	HOME_NET DMZ_NET

Gestion des ensembles de variables

Pour utiliser des ensembles de variables, vous devez avoir la licence IPS (pour périphériques défense contre les menaces) ou la licence de protection (pour tous les autres types de périphérique).

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Gérez vos ensembles de variables :

- Ajouter : si vous souhaitez ajouter un ensemble de variables personnalisé, cliquez sur **Add Variable Set**(ajouter un ensemble de variables) ; voir Création d'ensembles de variables, à la page 112.
- Supprimer : si vous souhaitez supprimer un ensemble de variables personnalisé, cliquez sur **Supprimer** ( ) à côté de l'ensemble de variables, puis cliquez sur **Yes**(oui). Vous ne pouvez pas supprimer l'ensemble de variables par défaut ni les ensembles de variables appartenant à des domaines ascendants.

  Remarque Les variables créées dans un ensemble de variables que vous supprimez ne sont pas supprimées ni affectées dans d'autres ensembles.

- Modifier : si vous souhaitez modifier un ensemble de variables, cliquez sur **Edit** ( ) à côté de l'ensemble de variables que vous souhaitez modifier. voir Modification d'objets, à la page 7.
- Filtrer : si vous souhaitez filtrer les ensembles de variables par nom, commencez par saisir un nom; Pendant que vous tapez, la page s'actualise pour afficher les noms correspondants. Si vous souhaitez effacer le filtrage de noms, cliquez sur **Effacer** ( ) dans le champ de filtre.
- Gérer les variables : pour gérer les variables incluses dans les ensembles de variables, consultez Gestion des variables, à la page 113.

Création d'ensembles de variables

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Variable Set** (Ajouter un ensemble de variables).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Vous pouvez également saisir une **Description**.

Étape 6 Gérer les variables de l'ensemble; voir Gestion des variables, à la page 113.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Gestion des variables

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** ( ) à côté de l'ensemble de variables que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Gérez vos variables :

- Affichage : si vous souhaitez afficher la valeur complète d'une variable, passez votre pointeur sur la valeur dans la colonne **Value** (valeur) à côté de la variable.
- Add si vous souhaitez ajouter une variable, cliquez sur **Add** (ajouter); voir Ajout de variables, à la page 114.
- Supprimer : cliquez sur **Supprimer** ( ) à côté de la variable. Si vous avez enregistré l'ensemble de variables depuis l'ajout de la variable, cliquez sur **Yes** (oui) pour confirmer que vous souhaitez supprimer la variable.

  Vous *ne pouvez pas* supprimer les éléments suivants :

  - Variables par défaut
  - les variables définies par l'utilisateur qui sont utilisées par les règles de prévention des intrusions ou d'autres variables
  - variable appartenant à des domaines ascendants

- Modifier : cliquez sur **Edit** ( ) à côté de la variable que vous souhaitez modifier. Consultez Modification des variables, à la page 115

- Réinitialiser : si vous souhaitez réinitialiser une variable modifiée à sa valeur par défaut, cliquez sur **Réinitialiser** à côté de la variable modifiée. Si Réinitialisation est grisé, l'une des conditions suivantes est remplie :
  - La valeur actuelle est déjà la valeur par défaut.
  - La configuration appartient à un domaine antécédent.

Astuces Passez votre pointeur sur une réinitialisation active pour afficher la valeur par défaut.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer l'ensemble de variables. Si l'ensemble de variables est utilisé par une politique de contrôle d'accès, cliquez sur **Yes** (oui) pour confirmer que vous souhaitez enregistrer vos modifications.

Étant donné que la valeur actuelle de l'ensemble par défaut détermine la valeur par défaut de tous les autres ensembles, la modification ou la réinitialisation d'une variable dans l'ensemble par défaut change la valeur actuelle dans les autres ensembles où vous n'avez pas personnalisé la valeur par défaut.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Ajout de variables

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Procédure

Étape 1 Dans l'éditeur de jeux de variables, cliquez sur **Add** (Ajouter).

Étape 2 Saisir un **nom** unique de la variable.

Étape 3 Dans la liste déroulante **Type** (Type), choisissez **Network** (réseau) ou **Port**(port).

Étape 4 Précisez les valeurs de la variable :

- Si vous souhaitez déplacer des éléments de la liste des réseaux ou des ports disponibles vers la liste des éléments inclus ou exclus, vous pouvez choisir un ou plusieurs éléments puis les faire glisser et les déposer, ou encore cliquer sur **Inclure** ou **Exclure**.

  Astuces Si des adresses ou des ports dans les listes des inclus et des exclus d'une variable de réseau ou de port se chevauchent, les adresses ou les ports exclus prévalent.

- Saisissez une valeur littérale unique, puis cliquez sur **Add** (Ajouter). Pour les variables de réseau, vous pouvez saisir une seule adresse IP ou un seul bloc d'adresses. Pour les variables de port, vous pouvez ajouter un seul port ou plage de ports, en séparant les valeurs supérieure et inférieure par un tiret (-). Répétez cette étape autant de fois que nécessaire pour saisir plusieurs valeurs littérales.
- Si vous souhaitez supprimer un élément des listes des inclus ou des exclus, cliquez sur **Supprimer** ( ) à côté de l'élément.

Remarque La liste des éléments à inclure ou à exclure peut être composée de n'importe quelle combinaison de chaînes littérales et de variables, d'objets et de groupes d'objets réseau existants dans le cas des variables réseau.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la variable. Si vous ajoutez une nouvelle variable à partir d'un ensemble personnalisé, vous avez les options suivantes :

- Cliquez sur **Yes** (oui) pour ajouter la variable en utilisant la valeur configurée comme valeur personnalisée dans l'ensemble par défaut et, par conséquent, comme valeur par défaut dans les autres ensembles personnalisés.
- Cliquez sur **No** (non) pour ajouter la variable comme valeur par défaut `toute` dans l'ensemble par défaut et, par conséquent, dans les autres ensembles personnalisés.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer l'ensemble de variables. Vos modifications sont enregistrées et toute politique de contrôle d'accès à laquelle l'ensemble de variables est lié affiche un état obsolète.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Modification des variables

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Vous pouvez modifier les variables personnalisées et par défaut.

Vous ne pouvez pas modifier les valeurs du **nom** ou du **type** dans une variable existante.

Procédure

Étape 1 Dans l'éditeur de jeux de variables, cliquez sur **Edit** ( ) à côté de la variable que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 2 Modifiez la variable :

- Si vous souhaitez déplacer des éléments de la liste des réseaux ou des ports disponibles vers la liste des éléments inclus ou exclus, vous pouvez sélectionner un ou plusieurs éléments puis les faire glisser et les déposer, ou encore cliquer sur **Inclure** ou **Exclure**.

  Astuces Si des adresses ou des ports dans les listes des inclus et des exclus d'une variable de réseau ou de port se chevauchent, les adresses ou les ports exclus prévalent.

- Saisissez une valeur littérale unique, puis cliquez sur **Add** (Ajouter). Pour les variables de réseau, vous pouvez saisir une seule adresse IP ou un seul bloc d'adresses. Pour les variables de port, vous pouvez ajouter un seul port ou plage de ports, en séparant les valeurs supérieure et inférieure par un tiret (-). Répétez cette étape autant de fois que nécessaire pour saisir plusieurs valeurs littérales.
- Si vous souhaitez supprimer un élément des listes des inclus ou des exclus, cliquez sur **Supprimer** ( ) à côté de l'élément.

Remarque La liste des éléments à inclure ou à exclure peut être composée de n'importe quelle combinaison de chaînes littérales et de variables, d'objets et de groupes d'objets réseau existants dans le cas des variables réseau.

Étape 3 Cliquez sur **Save** (Enregistrer) pour enregistrer la variable.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer l'ensemble de variables. Si l'ensemble de variables est utilisé par une politique de contrôle d'accès, cliquez sur **Yes** (oui) pour confirmer que vous souhaitez enregistrer vos modifications. Vos modifications sont enregistrées et toute politique de contrôle d'accès à laquelle l'ensemble de variables est lié affiche un état obsolète.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Étiquette VLAN

Chaque objet de balise VLAN que vous configurez représente une balise VLAN ou une série de balises.

Vous pouvez regrouper des objets de balise VLAN. Les groupes représentent plusieurs objets; l'utilisation d'une gamme de balises VLAN dans un seul objet n'est pas considérée comme un groupe dans ce sens.

Vous pouvez utiliser des objets et des groupes de balise VLAN à divers endroits dans l'interface Web du système, y compris des règles et des recherches d'événements. Par exemple, vous pouvez écrire une règle de contrôle d'accès qui bloque un site Web spécifique.

Création d'objets de balise VLAN

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Balise VLAN** dans la liste des types d'objets.

Étape 3 Sélectionnez **Add Object (Ajouter un objet)** dans le menu déroulant **Add URL (Ajouter une URL)**.

Étape 4 Saisissez un **Nom**.

Étape 5 Saisissez une **description**.

Étape 6 Saisissez une valeur dans le champ **Balise VLAN**. Utilisez un tiret pour spécifier une plage de balises VLAN.

Étape 7 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 13.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 13.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

VPN

Vous pouvez utiliser les objets VPN suivants sur les périphériques défense contre les menaces . Pour utiliser ces objets, vous devez avoir des privilèges d'administrateur et votre compte de licences Smart doit satisfaire aux contrôles à l'exportation. Vous pouvez configurer ces objets dans les domaines descendant uniquement.

Objets carte de certificat

Les objets de carte de certificats sont un ensemble nommé de règles de correspondance de certificats. Ces objets sont utilisés pour fournir une association entre un certificat reçu et un profil de connexion VPN d'accès à distance. Les profils de connexion et les objets carte de certificat font tous deux partie d'une politique VPN d'accès à distance. Si un certificat reçu correspond aux règles contenues dans la carte de certificats, la connexion est « mappée » ou associée au profil de connexion précisé. Les règles sont dans l'ordre de priorité, elles sont mises en correspondance dans l'ordre dans lequel elles sont affichées dans l'interface utilisateur. La mise en correspondance se termine lorsque la première règle de l'objet de carte de certificats génère une correspondance.

Navigation

Objets > **Gestion des objets** > **VPN** > **Carte de certificat**

Champs

- **Nom** : identifiez cet objet pour qu'il puisse être désigné à partir d'autres configurations, telles que celle d'un accès distant à distance VPN.
- **Critère de mappage** : spécifiez le contenu du certificat à évaluer. Si le certificat satisfait à ces règles, l'utilisateur est mappé au profil de connexion contenant cet objet.
  - **Champ**) :sélectionnez le champ de la règle de correspondance en fonction du sujet ou de l'émetteur du certificat client.

    Lorsque le **champ** est défini sur *Alternative Subject* (Sujet substitut) ou *Extended Key Usage* (Usage prolongé de la clé), le composant doit être un *champ entier*
  - **Composant** : sélectionnez le composant du certificat client à utiliser pour la règle de correspondance.

Remarque **Composant SER (Serial Number)** : assurez-vous de préciser le numéro de série dans le champ Objet. Le mappage de certificat correspond uniquement à un attribut de numéro de série dans le nom du sujet.

- **Opérateur** : sélectionnez l'opérateur pour la règle de correspondance comme suit :
  - Égalité : le composant du certificat doit correspondre à la valeur saisie. S'il ne correspond pas exactement, la connexion est refusée.
  - Contient : le composant de certificat doit contenir la valeur saisie. Si le composant ne contient pas la valeur indiquée, la connexion est refusée.
  - Non égal : le composant du certificat ne peut pas être égal à la valeur saisie. Par exemple, pour un composant de certificat sélectionné de Pays et une valeur entrée de États-Unis, si la valeur du comté du client est États-Unis, la connexion est refusée.
  - Ne contient pas : le composant de certificat ne peut pas contenir la valeur saisie. Par exemple, pour un composant de certificat sélectionné de Pays et une valeur entrée de États-Unis, si la valeur du comté du client contient des États-Unis, la connexion est refusée.

- **Valeur** : la valeur de la règle de correspondance. La valeur saisie est associée au composant et à l'opérateur sélectionnés.

Sujets connexes

Configurer les cartes de certificat

Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés)

Les attributs personnalisés sont utilisés par le Secure Client (services client sécurisés) pour configurer des fonctionnalités telles que le VPN par application, l'autorisation ou le report de la mise à niveau et la tunnellisation fractionnée dynamique. Un attribut personnalisé a un type et une valeur nommée. Le type de l'attribut est défini en premier, puis une ou plusieurs valeurs nommées de ce type peuvent être définies. Vous pouvez créer les objets des attributs personnalisés Secure Client à l'aide des centre de gestion, ajouter les objets à une politique de groupe et associer la politique de groupe à un VPN d'accès à distance pour activer les fonctionnalités pour les clients VPN.

Défense contre les menaces prend en charge les fonctionnalités suivantes à l'aide des objets d'attribut personnalisé :

- **Per App VPN** : la fonctionnalité Per App VPN permet d'identifier une application et de canaliser uniquement les applications autorisées par l'administrateur défense contre les menaces sur le VPN.
- **Allow or différer upgrade** – La mise à niveau différée permet à l'utilisateur Secure Client (services client sécurisés) de retarder le téléchargement de la mise à niveau Secure Client (services client sécurisés). Lorsqu'une mise à jour de client est disponible, vous pouvez configurer les attributs pour Secure Client (services client sécurisés) afin d'ouvrir une boîte de dialogue demandant à l'utilisateur s'il souhaite effectuer la mise à jour ou de reporter la mise à niveau.

- **Dynamic Split Tunneling** – Grâce à la tunnelisation dynamique fractionnée, vous pouvez provisionner des politiques qui incluent ou excluent des adresses IP ou des réseaux du tunnel VPN. La tunnellisation dynamique fractionnée est configurée en créant un attribut personnalisé et en l'ajoutant à une politique de groupe.

Pour obtenir des instructions détaillées sur la configuration des attributs personnalisés Secure Client (services client sécurisés), consultez Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés), à la page 119 et

Pour en savoir plus sur les attributs personnalisés à configurer pour une fonctionnalité, consultez le *Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect)* pour la version Secure Client (services client sécurisés) que vous utilisez.

Sujets connexes

Options de politique de groupe Secure Client (services client sécurisés), à la page 125

Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés)

Avant de commencer

Assurez-vous d'avoir effectué les étapes suivantes avant d'ajouter un objet d'attribut personnalisé au VPN par application :

- Le VPN par application doit être correctement configuré au moyen de MDM et chaque appareil doit être inscrit sur le serveur de MDM
- Créez une chaîne codée en base64 pour chaque application à l'aide du sélecteur d'applications d'entreprise Cisco Secure Client (services client sécurisés).
  1. Téléchargez l'outil Cisco Enterprise Application Selector Secure Client (services client sécurisés) ici.
  2. Ouvrez l'outil de sélection d'applications et sélectionnez la plateforme mobile dans le menu déroulant situé dans le coin supérieur gauche.
  3. Ajoutez une règle en saisissant un nom convivial et un ID d'application. les autres champs sont facultatifs.
  4. Dans la barre de menus, cliquez sur **Policy** (politique). La règle base65 codée s'affiche dans son format codé.
  5. Sélectionnez et copiez la chaîne de politique, puis enregistrez-la pour l'utiliser ultérieurement lors de la création de l'objet d'attributs personnalisés Secure Client (services client sécurisés).

Procédure

Étape 1 Choisissez **Objets** > **Gestion des objets** > **VPN** > **Attributs personnalisés**.

Étape 2 Cliquez sur **Attribut personnalisé Secure Client**.

Étape 3 Saisissez un nom pour l'attribut (sous **Name**) et, facultativement, une **description**.

Étape 4 Sélectionnez un attribut dans la liste déroulante **Attribut Secure Client** :

- **Per App VPN** (VPN par application) : sélectionnez cette option et spécifiez la chaîne codée en base64 dans la zone **Attribute Value** (valeur d'attribut).
- **Allow Defer Update**(autoriser ou différer la mise à jour) : sélectionnez l'une des options suivantes et spécifiez les informations requises pour autoriser ou différer la mise à jour Secure Client (services client sécurisés) :
  - **Show the prompt until user takes action** (Afficher l'invite jusqu'à ce que l'utilisateur prenne action) : affichez l'invite à l'utilisateur VPN jusqu'à ce que l'utilisateur choisisse d'autoriser ou de différer la mise à jour du client VPN.
  - **Show the prompt until times out** (Afficher l'invite jusqu'à l'expiration) : choisissez cette option pour afficher l'invite pendant une durée donnée et spécifiez la durée dans la zone **Timeout** (délai d'expiration).
  - **Do not show the prompt and take automatic action** (Ne pas afficher l'invite et passer à l'action automatique) : choisissez cette option pour autoriser ou différer automatiquement la mise à jour du VPN.
  - **Default Action** (action par défaut) : sélectionnez l'action par défaut à entreprendre lorsque l'utilisateur ne répond pas ou lorsque vous souhaitez configurer une action automatique sans l'intervention de l'utilisateur. Vous pouvez choisir de mettre à jour le Secure Client (services client sécurisés) ou de reporter la mise à jour.
  - **Minimum Version** – Spécifiez la version minimale de Secure Client qui doit être présente sur le système client pour autoriser ou reporter la mise à jour.
- **Dynamic Split Tunneling** (Tunnel fractionné dynamique) : sélectionnez cette option pour inclure ou exclure des adresses IP ou des réseaux du tunnel VPN.
  - **Include domains** (Inclure les domaines) : spécifiez les noms de domaine qui seront inclus dans le tunnel VPN d'accès à distance.
  - **Exclude domains** (Exclure les domaines) : spécifiez les noms de domaines qui seront exclus du tunnel VPN d'accès à distance.

Étape 5 Cochez la case **Allow Overrides** (autoriser les remplacements) pour autoriser les remplacements d'objets.

Étape 6 Cliquez sur **Save** (enregistrer).
L'objet d'attributs personnalisés est ajouté à la liste.

Prochaine étape

Associer les attributs personnalisés à une politique de groupe. Voir Ajouter des attributs personnalisés à une politique de groupe, à la page 120 .

Ajouter des attributs personnalisés à une politique de groupe

Vous devez associer des attributs personnalisés Secure Client à une politique de groupe pour les utiliser pour les connexions VPN d'accès à distance. Vous

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Group Policy** (Politique de groupe).

Étape 2 Ajouter une nouvelle politique de groupe ou modifier une politique de groupe existante.

Étape 3 Cliquez sur **Secure Client** > **Custom Attributes**.

Étape 4 Cliquez sur **Add** (ajouter).

Étape 5 Sélectionnez l'**Secure Client** : VPN par application, Autoriser le report de la mise à jour ou Tunnel fractionné dynamique.

Étape 6 Sélectionnez un **objet d'attribut personnalisé** dans la liste.

Remarque Cliquez sur Add (+) pour créer un nouvel objet d'attribut personnalisé pour l'attribut Secure Client sélectionné. Vous pouvez également créer un objet d'attribut personnalisé dans **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Custom Attribute**(Attributs personnalisés). Consultez Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés), à la page 119.

Étape 7 Cliquez sur **Add** (ajouter) pour enregistrer les attributs dans la politique de groupe, puis cliquez sur **Save** (Enregistrer) pour enregistrer les modifications dans la politique de groupe.

Sujets connexes

Options de politique de groupe Secure Client (services client sécurisés), à la page 125

Objets politique de groupe Défense contre les menaces

Une politique de groupe est un ensemble de paires d'attributs et de valeurs, stockées dans un objet de politique de groupe, qui définissent l'expérience du VPN d'accès à distance. Par exemple, dans l'objet de politiques de groupe, vous configurez les attributs généraux tels que les adresses, les protocoles et les paramètres de connexion.

La politique de groupe appliquée à un utilisateur est déterminée lors de l'établissement du tunnel VPN. Le serveur d'autorisation RADIUS attribue la politique de groupe, ou elle est obtenue à partir du profil de connexion actuel.

Remarque Il n'y a pas d'hérédité d'attributs de politiques de groupe sur défense contre les menaces . Un objet de politiques de groupe est utilisé entièrement pour un utilisateur. L'objet de politique de groupe identifié par le serveur AAA lors de la connexion est utilisé ou, s'il n'est pas spécifié, la politique de groupe par défaut configurée pour la connexion VPN est utilisée. La politique de groupe par défaut peut être définie selon vos valeurs par défaut, mais ne sera utilisée que si elle est affectée à un profil de connexion et qu'aucune autre politique de groupe n'a été définie pour l'utilisateur.

Pour utiliser des objets de groupe, vous devez avoir l'une de ces licences Secure Client (services client sécurisés) associée à votre compte de licences Smart avec les fonctionnalités dont l'exportation contrôlée est activée :

- VPN client sécurisé uniquement

- Secure Client Advantage
- Secure Client Premier

Sujets connexes

Configurer les objets de politique de groupe, à la page 122

Configurer les objets de politique de groupe

Consultez Objets politique de groupe Défense contre les menaces, à la page 121.

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**.

Les politiques configurées précédemment sont répertoriées, y compris les valeurs par défaut du système. Selon votre niveau d'accès, vous pouvez modifier, afficher ou supprimer une politique de groupe.

Étape 2 Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier.

Étape 3 Saisissez un **nom** et, éventuellement, une **description** pour cette politique.

Le nom peut comporter jusqu'à 64 caractères. Les espaces sont autorisés. La description peut comporter jusqu'à 1 024 caractères.

Étape 4 Spécifiez les paramètres **généraux** de cette politique de groupe, comme décrit dans Options générales de politique de groupe, à la page 122.

Étape 5 Précisez les paramètres **Secure Client** pour cette politique de groupe, comme décrit dans Options de politique de groupe Secure Client (services client sécurisés), à la page 125.

Étape 6 Spécifiez les paramètres **avancés** pour cette politique de groupe, comme décrit dans Options avancées de la politique de groupe, à la page 129.

Étape 7 Cliquez sur **Save** (enregistrer).
La nouvelle politique de groupe est ajoutée à la liste.

Prochaine étape

Ajoutez l'objet de politique de groupe à un profil de connexion VPN d'accès à distance.

Options générales de politique de groupe

Chemin de navigation

Objects (Objets) > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**, Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier., puis sélectionnez l'onglet **General** (General).

Champs des protocoles VPN

Précisez les types de tunnels VPN d'accès à distance qui peuvent être utilisés lors de l'application de cette politique de groupe. **SSL** ou **IPsec IKEv2**.

Réserves d'adresses IP

Spécifie l'attribution d'adresse IPv4 qui est appliquée en fonction des ensembles d'adresses qui sont spécifiques aux groupes d'utilisateurs dans le VPN d'accès à distance. Pour le VPN d'accès à distance, vous pouvez attribuer une adresse IP à partir d'ensembles d'adresses spécifiques à des groupes d'utilisateurs identifiés en utilisant RADIUS/ISE pour l'autorisation. Vous pouvez appliquer en toute transparence des politiques pour des utilisateurs ou groupes d'utilisateurs dans des systèmes qui ne sont pas sensibles à l'identité en configurant une politique de groupe particulière comme attribut d'autorisation RADIUS (GroupPolitique/Classe) pour un groupe d'utilisateurs en particulier. Par exemple, vous devez sélectionner un ensemble d'adresses spécifique pour les sous-traitants et l'application des politiques, en utilisant ces adresses pour autoriser un accès restreint au réseau interne.

L'ordre de préférence par lequel le périphérique défense contre les menaces affecte les ensembles d'adresses IPv4 aux clients :

1. Attribut RADIUS pour l'ensemble d'adresses IPv4
2. Attribut RADIUS pour la politique de groupe
3. Ensemble d'adresses dans la politique de groupe mappé à un profil de connexion
4. Ensemble d'adresses IPv4 dans le profil de connexion

Certaines limites de l'utilisation des ensembles d'adresses IP dans la politique de groupe :

- L'ensemble d'adresses IPv6 n'est pas pris en charge.
- Un maximum de 6 ensembles d'adresses IPv4 peut être configuré.
- Des échecs de déploiement surviennent lorsque les ensembles d'adresses en cours d'utilisation sont modifiés. Vous devez déconnecter tous les utilisateurs avant d'apporter des modifications aux ensembles d'adresses.
- Lorsque des ensembles d'adresses sont renommés ou que des regroupements d'adresses qui se chevauchent sont configurés, le déploiement peut échouer. Vous devez déployer les modifications en supprimant l'ancien ensemble d'adresses, puis en déployant l'ensemble modifié.

  Quelques commandes de dépannage :

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

Champs de la bannière

Spécifie le texte de la bannière à présenter aux utilisateurs lors de la connexion. La longueur peut aller jusqu'à 491 caractères. Il n'y a pas de valeur par défaut. Le client VPN IPsec prend en charge le langage HTML complet pour la bannière, cependant, le Secure Client (services client sécurisés) ne prend en charge que le HTML partiel. Pour vous assurer que la bannière s'affiche correctement pour les utilisateurs distants, utilisez la balise /n pour les clients IPsec et la balise
 pour les clients SSL.

Champs DNS/WINS

Les serveurs DNS (Domain Naming System) et WINS (Windows Internet Naming System). Utilisé pour la résolution de nom Secure Client (services client sécurisés).

- **Primary DNS Server** et **Secondary DNS Server** (servers DNS primaire et secondaire) : sélectionnez ou créez un objet réseau qui définit les adresses IPv4 ou IPv6 des serveurs DNS que vous souhaitez que ce groupe utilise.
- **Serveur WINS principal** et **serveur WINS secondaire** : sélectionnez ou créez un objet réseau contenant les adresses IP des serveurs WINS que vous souhaitez que ce groupe utilise.
- **DHCP Network Scope**(portée du réseau DHCP) : sélectionnez ou créez un objet réseau contenant une adresse IPv4 routable sur le même sous-réseau que le pool souhaité, mais pas dans le pool. Le serveur DHCP détermine à quel sous-réseau cette adresse IP appartient et attribue une adresse IP de cet ensemble d'adresses. Si elle n'est pas définie correctement, le déploiement de la politique VPN échoue.

  Si vous configurez des serveurs DHCP pour l'ensemble d'adresses dans le profil de connexion, la portée de DHCP identifie les sous-réseaux à utiliser pour le regroupement pour ce groupe. Le serveur DHCP doit également avoir des adresses dans le même sous-réseau identifié par la portée. La portée vous permet de sélectionner un sous-ensemble des ensembles d'adresses définis dans le serveur DHCP à utiliser pour ce groupe précis.

  Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

  Nous vous recommandons d'utiliser l'adresse IP d'une interface chaque fois que cela est possible à des fins de routage. Par exemple, si l'ensemble d'adresses est 10.100.10.2-10.100.10.254 et que l'adresse d'interface est 10.100.10.1/24, utilisez 10.100.10.1 comme portée DHCP. N'utilisez pas le numéro de réseau. Vous ne pouvez utiliser DHCP que pour l'adressage IPv4. Si l'adresse que vous choisissez n'est pas une adresse d'interface, vous devrez peut-être créer une voie de routage statique pour l'adresse de portée.

  LINK-SELECTION (RFC 3527) et SUBNET-SELECTION (RFC 3011) ne sont actuellement pas pris en charge.
- **Default Domain**(domaine par défaut) : nom du domaine par défaut. Précisez un domaine de niveau supérieur, par exemple, example.com.

Champs de la tunnellisation fractionnée

La tunnellisation fractionnée dirige une partie du trafic réseau dans le tunnel VPN (chiffré) et le trafic réseau restant à l'extérieur du tunnel VPN (non chiffré ou « en clair »).

- **Tunnellisation fractionnée IPv4 / Tunneling fractionnée IPv6** : par défaut, la tunnellisation fractionnée n'est pas activée. Pour IPv4 et IPv6, elle est définie sur **Allow all traffic over tunnel**(autoriser tout le trafic sur le tunnel). Lorsque cette fonction est laissée telle quelle, tout le trafic du terminal passe sur la connexion VPN.

  Pour configurer la tunnellisation fractionnée, choisissez les **réseaux de tunnels spécifiés ci-dessous** ou la politique **Exclure les réseaux spécifiés ci-dessous**. Configurez ensuite une liste de contrôle d'accès pour cette politique.
- **Type de liste de réseaux de tunnels fractionnés** : choisissez le type de liste d'accès que vous utilisez. Ensuite, sélectionnez ou créez une **liste d'accès standard** ou une **liste d'accès étendue**. Consultez Liste d'accès, à la page 19 pour en savoir plus.
- **tunnelisation fractionnée des requêtes DNS** : également connu sous le nom de DNS fractionné. Configurez le comportement du DNS attendu dans votre environnement.

Par défaut, le DNS fractionné n'est pas activé et défini sur **Envoi d'une requête DNS conformément à la politique de tunnelisation fractionnée**. Choisissez **Toujours envoyer la requête DNS sur le tunnel** pour forcer l'envoi de toutes les requêtes DNS par le tunnel au réseau privé.

Pour configurer le DNS fractionné, choisissez **SEnvoyer uniquement les domaines spécifiés par tunnel** et saisissez la liste de noms de domaine dans le champ **Domain List**. Ces demandes sont résolues par le tunnel fractionné vers le réseau privé. Tous les autres noms sont résolus à l'aide du serveur DNS public. Choisissez jusqu'à dix entrées dans la liste de domaines, séparées par des virgules. La chaîne complète ne peut pas dépasser 255 caractères.

Sujets connexes

Configurer les objets de politique de groupe, à la page 122

Options de politique de groupe Secure Client (services client sécurisés)

Ces spécifications s'appliquent au fonctionnement du VPN Secure Client (services client sécurisés).

Navigation

Objects (Objets) > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**. Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier. Sélectionnez ensuite l'onglet **Secure Client**.

Champs de profil

Profil : sélectionnez ou créez un objet fichier contenant Secure Client Profile. Consultez Objets de fichier, à la page 135 pour en savoir plus sur la création d'objet.

Le Secure Client Profile est un groupe de paramètres de configuration stockés dans un fichier XML. Le logiciel Secure Client (services client sécurisés) l'utilise pour configurer les entrées de connexion qui s'affichent dans l'interface utilisateur du client. Ces paramètres (balises XML) configurent également les paramètres pour activer davantage de fonctionnalités Secure Client (services client sécurisés).

Utilisez l'outil graphique Secure Client Profile Editor, un outil de configuration indépendant, pour créer le Secure Client Profile. Consultez le chapitre *Secure Client Profile Editor* dans la version appropriée du de l'administrateur deCisco Secure Client (y compris AnyConnect) le guide de l'administrateur de Cisco Secure Client (y compris AnyConnect) pour en savoir plus.

Champs du Profil de gestion

Un tunnel VPN de gestion garantit la connectivité au réseau d'entreprise quand le terminal est sous tension, même si l'utilisateur final ne se connecte pas sur le VPN.

Profil VPN de gestion : le fichier du profil de gestion contient les paramètres permettant d'activer et d'établir le tunnel VPN de gestion sur le terminal.

L'éditeur de profil du tunnel VPN de gestion autonome peut être utilisé pour créer un nouveau fichier de profil ou modifier un fichier de profil existant. Vous pouvez télécharger l'éditeur de profil à partir du Centre de téléchargement de logiciels Cisco.

Pour plus d'informations sur l'ajout d'un fichier de profil, consultez Objets de fichier, à la page 135.

Champs des modules clients

Cisco VPN client sécurisé uniquement offre une sécurité améliorée grâce à divers modules intégrés. Ces modules fournissent des services comme la sécurité du Web, la visibilité du réseau dans les flux de terminaux et la protection en itinérance hors réseau. Chaque module client comprend un profil client qui comprend un groupe de configurations personnalisées selon vos besoins.

Les modules Secure Client (services client sécurisés) suivants sont facultatifs et vous pouvez configurer ces modules pour qu'ils soient téléchargés lorsqu'un utilisateur VPN télécharge Secure Client (services client sécurisés) :

- **AMP Enabler** (Facilitateur AMP) : déploie une protection avancée contre les programmes malveillants (AMP) pour les terminaux.
- **DART** : prend un instantané des journaux du système et d'autres informations de dépistage, qui peuvent être envoyées au Cisco TAC pour le dépannage.
- **Posture ISE** : utilise la bibliothèque OSSWAT pour effectuer des vérifications de posture afin d'évaluer la conformité d'un point terminal.
- **Gestionnaire d'accès réseau** : fournit la norme 802.1X (couche 2) et l'authentification des périphériques pour l'accès aux réseaux câblés et sans fil.
- **Visibilité du réseau** : améliore la capacité de l'administrateur de l'entreprise à effectuer la planification de la capacité et des services, l'audit, la conformité et l'analyse de sécurité.
- **Démarrer avant la connexion** : force l'utilisateur à se connecter à l'infrastructure de l'entreprise par une connexion VPN avant de se connecter à Windows en démarrant Secure Client (services client sécurisés) avant que la boîte de dialogue de connexion Windows ne s'affiche.
- **Sécurité d'itinérance Umbrella** : assure la sécurité de la couche DNS lorsqu'aucun VPN n'est actif.
- **Sécurité Web** : analyse les éléments d'une page Web, autorise le contenu acceptable et bloque le contenu malveillant ou inacceptable en fonction d'une politique de sécurité définie.

Cliquez sur **Add** (ajouter) et sélectionnez les options suivantes pour chaque module client :

- **Module client** : sélectionnez le module Secure Client (services client sécurisés) dans la liste.
- **Profil à télécharger** : sélectionnez ou créez un objet fichier contenant Secure Client Profile. Consultez Objets de fichier, à la page 135 pour en savoir plus sur la création d'objet.
- **Enable module download**(activer le téléchargement de module) : sélectionnez cette option pour permettre aux points terminaux de télécharger le module client avec le profil. Si cette option n'est pas sélectionnée, les points terminaux ne peuvent télécharger que le profil client.

Utilisez l'outil graphique Secure Client Profile Editor, un outil de configuration indépendant, pour créer un profil client pour chaque module. Téléchargez Secure Client Profile Editor depuis le centre de téléchargement de logiciels Cisco. Consultez le chapitre *Secure Client Profile Editor* dans la version appropriée du Cisco Secure Client (y compris AnyConnect) pour en savoir plus.

Champs des paramètres SSL

- **Compression SSL**: indique s'il faut activer la Compression des données et, si oui, la méthode de compression de données à utiliser, DeFlate ou LZS. La Compression SSL est désactivée par défaut.

La compression des données accélère les débits de transmission, mais augmente également les besoins en mémoire et l'utilisation du processeur pour chaque session utilisateur. Par conséquent, la diminution du débit global du périphérique de sécurité.

- **Compression DTLS** : s'il faut compresser les connexions DTLS (Datagram Transport Layer Security) pour ce groupe à l'aide de LZS ou non. La Compression DTLS est désactivée par défaut.
- **Taille MTU** : taille maximale d'unité de transmission (MTU) pour les connexions de VPN SSL établies par VPN client sécurisé uniquement . La valeur par défaut est 1 406 octets, et la plage valide est de 576 à 1 462 octets.
    - **Ignore DF Bit**(ignorer le bit DF) : s'il faut ignorer le bit Ne pas fragmenter (DF) dans les paquets qui ont besoin de fragmentation. Permet la fragmentation forcée des paquets dont le bit DF est activé, leur permettant de passer par le tunnel.

Champs des paramètres de connexion

- **Activez les messages Keepalive entre Secure Client et la passerelle VPN**. Et son intervalle. (**Intervalle**) : s'il faut échanger des messages Keepalive entre les homologues pour démontrer qu'ils sont disponibles pour envoyer et recevoir des données dans le tunnel. La valeur par défaut est activée. Les messages Keepalive sont transmis à des intervalles définis. Si elle est activée, saisissez l'intervalle de temps (en secondes) pendant lequel le client distant attend entre l'envoi de paquets IKE Keepalive. L'intervalle par défaut est de 20 secondes, et la plage valide est de 15 à 600 secondes.
- **Enable Dead Peer (DPD) Detection (Détection des homologues inactifs) sur ...**. Et leurs paramètres d' **intervalle** : La détection des homologues inactifs (DPD) garantit que la passerelle sécurisée VPN ou le client VPN détectent rapidement lorsque l'homologue ne répond plus et que la connexion échoue. La valeur par défaut est activée pour la passerelle et le client. Les messages DPD sont transmis à des intervalles définis. Si elle est activée, saisissez l'intervalle (en secondes) pendant lequel le client distant attend entre l'envoi de messages DPD. L'intervalle par défaut est de 30 secondes et la plage valide est de 5 à 3 600 secondes.
- **Enable Client Bypass Protocol** (activer le protocole de contournement du client) : vous permet de configurer la façon dont la passerelle sécurisée gère le trafic IPv4 (lorsqu'elle s'attend uniquement au trafic IPv6) ou la façon dont elle gère le trafic IPv6 (lorsqu'elle s'attend uniquement au trafic IPv4).

  Lorsque Secure Client (services client sécurisés) établit une connexion VPN avec la tête de réseau, celle-ci lui attribue une adresse IPv4, IPv6 ou aux deux une adresse IPv4 et IPv6. Si la tête de réseau affecte uniquement une adresse IPv4 ou IPv6 à la connexion Secure Client (services client sécurisés), vous pouvez configurer le protocole de contournement du client pour abandonner le trafic réseau pour lequel la tête de réseau n'a pas attribué d'adresse IP (par défaut, désactivé, non coché), ou autoriser que ce trafic contourne la tête de réseau et soit envoyé par le client non chiffré ou « en clair » (activé, coché).

  Par exemple, supposons que la passerelle sécurisée attribue uniquement une adresse IPv4 à la connexion Secure Client (services client sécurisés) et que le point terminal fonctionne à deux niveaux. Lorsque le point terminal tente d'atteindre une adresse IPv6, si le protocole de contournement des clients est désactivé, le trafic IPv6 est abandonné; cependant, si le protocole de contournement client est activé, le trafic IPv6 est envoyé par le client en clair.
- **Renouveler la connexion SSL** : permet au client de renouveler la clé de la connexion, en renégociant les clés de chiffrement et les vecteurs d'initialisation, ce qui augmente la sécurité de la connexion. Le paramètre par défaut est Désactivé. Lorsque cette option est activée, la renégociation peut être effectuée à un intervalle spécifié et renouveler le clés du tunnel existant ou créer un nouveau tunnel en définissant les champs suivants :

- **Méthode** : disponible lorsque le renouvellement de SSL est activé. Créer un **nouveau tunnel** (par défaut) ou renégocier les spécifications du **tunnel existant**.
- **Intervalle** : disponible lorsque le renouvellement SSL est activé. Définir avec une valeur par défaut de 4 minutes avec une plage de 4 à 10080 minutes (1 semaine).

- **Client Firewall Rules** (règles de pare-feu client) : utilisez les règles de pare-feu client pour configurer les paramètres de pare-feu pour la plateforme du client VPN. Les règles sont basées sur des critères tels que l'adresse source, l'adresse de destination et le protocole. Les objets bloc de création de la liste de contrôle d'accès étendue sont utilisés pour définir les critères de filtre de trafic. Sélectionnez ou créez une liste de contrôle d'accès étendue pour cette politique de groupe. Définissez une **règle de réseau privé** pour contrôler les données circulant vers le réseau privé, une **règle de réseau public** pour contrôler les données circulant « en clair » en dehors du tunnel VPN établi, ou les deux.

Remarque Assurez-vous que l'ACL contient uniquement les ports TCP/UDP/ICMP/IP et que le réseau source soit à any (n'importe quel), any-ipv4 (n'importe quel ipv4) ou any-ipv6 (n'importe quel ipv6)

Seuls les clients VPN exécutant Microsoft Windows peuvent utiliser ces paramètres de pare-feu.

Champs d'attributs personnalisés

Cette section répertorie les attributs personnalisés Secure Client qui sont utilisés par Secure Client (services client sécurisés) pour configurer des fonctionnalités telles que le VPN par application, l'autorisation ou le report de la mise à niveau et la tunnellisation fractionnée dynamique. Cliquez sur **Add** (ajouter) pour ajouter des attributs personnalisés à la politique de groupe.

1. Sélectionnez l'**Secure Client** : VPN par application, Autorisez le report de la mise à jour ou la tunnelisation fractionnée dynamique.
2. Sélectionnez un **objet d'attribut personnalisé** dans la liste.

Remarque Cliquez sur Add (+) pour créer un nouvel objet d'attribut personnalisé pour l'attribut Secure Client sélectionné. Vous pouvez également créer un objet d'attribut personnalisé dans **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Custom Attribute**(Attributs personnalisés). Consultez Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés), à la page 119.

3. Cliquez sur **Add** (ajouter) pour enregistrer les attributs dans la politique de groupe, puis cliquez sur **Save** (Enregistrer) pour enregistrer les modifications dans la politique de groupe.

Sujets connexes

Configurer les objets de politique de groupe, à la page 122

Options avancées de la politique de groupe

Chemin de navigation

Objects (Objets) > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**, Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier., puis sélectionnez l'onglet **Advanced** (Avancé).

Champs de filtres de trafic

- **Access List Filter** (filtre de liste d'accès) : les filtres sont constitués de règles qui déterminent s'il faut autoriser ou bloquer les paquets de données acheminés par tunnel passant par la connexion VPN. Les règles sont basées sur des critères tels que l'adresse source, l'adresse de destination et le protocole. Notez que le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application. Les objets bloc de création de la liste de contrôle d'accès étendue sont utilisés pour définir les critères de filtre de trafic. Sélectionnez ou créez une nouvelle ACL étendue pour cette politique de groupe.
- **Restrict VPN to VLAN** (Restreindre le VPN au VLAN) : également appelé « mappage VLAN », ce paramètre spécifie l'interface VLAN de sortie des sessions auxquelles cette politique de groupe s'applique. L'ASA transfère tout le trafic de ce groupe vers le VLAN sélectionné.

  Utilisez cet attribut pour affecter un VLAN à la politique de groupe pour simplifier le contrôle d'accès. L'affectation d'une valeur à cet attribut est une alternative à l'utilisation de listes de contrôle d'accès pour filtrer le trafic sur une session. En plus de la valeur par défaut (Unrestricted) (non restreinte), la liste déroulante affiche uniquement les VLAN configurés dans cet ASA. Les valeurs autorisées sont comprises entre 1 et 4 094.

Champs de paramètres de session

- **Heures d'accès** : sélectionnez ou créez un objet de plage temporelle. Cet objet spécifie la plage temporelle pendant laquelle cette politique de groupe est disponible pour être appliquée à un utilisateur d'accès à distance. Consultez Plage temporelle, à la page 95 pour en savoir plus.
- **Simultaneous Logins Per User (connexions simultanées par utilisateur**) : Précise le nombre maximal de connexions simultanées autorisées pour un utilisateur. La valeur par défaut est 3. La valeur minimale est 0, ce qui désactive la connexion et empêche l'accès de l'utilisateur. Autoriser plusieurs connexions simultanées peut compromettre la sécurité et affecter les performances.
- **Maximum Connection Time/Alert Interval** (Temps de connexion / Intervalle d'alerte maximum) : spécifie la durée maximale de connexion de l'utilisateur en minutes. À la fin de ce temps, le système arrête la connexion. La durée minimale est de 1 minute). L'intervalle d'alerte spécifie l'intervalle de temps qui s'écoule avant que le temps de connexion maximal ne soit atteint pour qu'un message soit affiché à l'intention de l'utilisateur.
- **Idle Timeout/Alert Interval** (Intervalle d'inactivité/d'alerte) : spécifie le délai d'inactivité de cet utilisateur en minutes. S'il n'y a aucune activité de communication sur la connexion de l'utilisateur pendant cette période, le système arrête la connexion. La durée minimale est de 1 minute. La valeur par défaut est de 30 minutes. L'intervalle d'alerte spécifie l'intervalle de temps qui s'écoule avant que le temps d'inactivité ne soit atteint pour qu'un message soit affiché à l'intention de l'utilisateur.

Sujets connexes

Configurer les objets de politique de groupe, à la page 122

Propositions IPsec Défense contre les menaces

Les propositions (ou ensembles de transformations) IPsec sont utilisées lors de la configuration des topologies VPN. Négociation de l'association de sécurité IPsec avec ISAKMP : les pairs conviennent d'utiliser une proposition particulière pour protéger un flux de données particulier. La proposition doit être la même pour les deux homologues.

Il existe des objets de proposition IPsec distincts selon la version IKE, IKEv1 ou IKEv2 :

- Lorsque vous créez un objet de proposition IKEv1 IPsec (ensemble de transformations), vous sélectionnez le mode dans lequel IPsec fonctionne et définissez les types de chiffrement et d'authentification requis. Vous pouvez sélectionner une seule option pour les algorithmes. Si vous souhaitez prendre en charge plusieurs combinaisons dans un VPN, créez plusieurs objets IKEv1 IPsec Proposition.
- Lorsque vous créez une proposition IKEv2 IPsec, vous pouvez sélectionner tous les algorithmes de chiffrement et de hachage autorisés dans un VPN. Lors des négociations IKEv2, les pairs sélectionnent les options les plus appropriées que les deux supportent.

Le protocole Encapsulating Security Protocol (ESP) est utilisé pour les propositions d'IPsec IKEv1 et IKEv2. Il fournit des services d'authentification, de chiffrement et d'antirelecture. ESP est un protocole IP de type 50.

Remarque Nous vous recommandons d'utiliser à la fois le chiffrement et l'authentification sur les tunnels IPsec.

Configurer des objets de proposition IKEv1 IPsec

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (Gestion des objets)**puis, **VPN** > **IPsec IKEv1 Proposal (Proposition IPSec IKEv1)** dans la table des matières.

Les propositions configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** ( ), **Afficher** ( )ou **Supprimer** ( ) une proposition.

Étape 2 Choisissez **Ajouter** ( )**Add IPsec IKEv1 Proposal** (Ajouter la proposition IPsec IKEv1) pour créer une nouvelle proposition.

Étape 3 Saisissez un **nom** pour cette proposition

Le nom de l'objet Politique. Un maximum de 128 caractères est permis

Étape 4 Saisissez une **description** pour cette proposition.

Une description de l'objet Politique Un maximum de 1024 caractères est permis

Étape 5 Choisissez la méthode de **chiffrement ESP**. L'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition.

Pour IKEv1, sélectionnez l'une des options. Au moment de décider quel chiffrement et quels algorithmes de hachage utiliser pour la proposition IPsec, votre choix se limite aux algorithmes pris en charge par les périphériques du VPN. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser.

Étape 6 Sélectionnez une option pour **ESP Hash** (Hachage ESP).

Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser.

Étape 7 Cliquez sur **Save** (Enregistrer).
La nouvelle proposition est ajoutée à la liste.

Configurer des objets de proposition IKEv2 IPsec

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (Gestion des objets)**puis, **VPN** > **IKEv2 IPsec Proposal (Proposition IPSec IKEv2)** dans la table des matières.

Les propositions configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** ( ), **Afficher** ( )ou **Supprimer** ( ) une proposition.

Étape 2 Choisissez **Ajouter** ( )**Add IKEv2 IPsec Proposal** (Ajouter la proposition IPSec IKEv2) pour créer une nouvelle proposition.

Étape 3 Saisissez un **nom** pour cette proposition

Le nom de l'objet Politique. Un maximum de 128 caractères est permis

Étape 4 Saisissez une **description** pour cette proposition.

Une description de l'objet Politique Un maximum de 1024 caractères est permis

Étape 5 Choisissez la méthode de **hachage ESP** ou l'algorithme de hachage ou d'intégrité à utiliser dans la proposition d'authentification.

Remarque Défense contre les menaces ne prend pas en charge les tunnels IPSec avec chiffrement NULL. Assurez-vous de ne pas choisir le chiffrement NULL pour la proposition IPSec IKEv2.

Pour IKEv2, sélectionnez toutes les options que vous souhaitez prendre en charge pour **le hachage ESP**. Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser.

Étape 6 Choisissez la méthode de **chiffrement ESP**. L'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition.

Pour IKEv2, cliquez sur Select pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner toutes les options que vous souhaitez prendre en charge. Au moment de décider quel chiffrement et quels algorithmes de hachage utiliser pour la proposition IPsec, votre choix se limite aux algorithmes pris en charge

par les périphériques du VPN. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser.

Étape 7 Cliquez sur **Save** (Enregistrer).
La nouvelle proposition est ajoutée à la liste.

Politiques IKE Défense contre les menaces

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec. La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion. Une proposition IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité utilisés pour protéger les négociations IKE ultérieures.

IKEv1 : les propositions IKE contiennent un ensemble unique d'algorithmes et un groupe de modules. Vous pouvez créer plusieurs politiques en fonction de leur ordre de priorité pour vous assurer qu'au moins une politique correspond à la politique d'un homologue distant. Contrairement à IKEv1, dans une proposition IKEv2, vous pouvez sélectionner plusieurs algorithmes et groupes de modules dans une politique. Puisque les homologues choisissent pendant la négociation de la phase 1, cela permet de créer une seule proposition IKE, mais d'envisager plusieurs propositions différentes pour donner une priorité plus élevée aux options les plus souhaitées. Pour IKEv2, l'objet de politique ne spécifie pas l'authentification, les autres politiques doivent définir les exigences d'authentification.

Une politique IKE est requise lorsque vous configurez un VPN IPsec de site à site . Pour en savoir plus, consultez VPN.

Configurer des objets de politique IKEv1

Utilisez la page Politique IKEv1 pour créer, supprimer ou modifier un objet de politique IKEv1. Ces objets de politique contiennent les paramètres requis pour les politiques IKEv1.

Procédure

Étape 1 Choisissez **Objets** > **Gestion des objets**, puis **VPN** > **Politique IKEv1** dans la table des matières.

Les politiques configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** ( ), **Afficher** ( )ou **Supprimer** ( ) une proposition.

Étape 2 (Facultatif) Choisissez **Ajouter** ( )**Add IKEv1 Policy (ajouter une politique IKEv1)** pour créer un nouvel objet de politique.

Étape 3 Entrez un **nom** pour la politique. Un maximum de 128 caractères est permis

Étape 4 (Facultatif) Saisissez une **description** pour cette proposition. Un maximum de 1,024 caractères est permis

Étape 5 Saisissez la valeur de **priorité** de la politique IKE.

La valeur de priorité détermine l'ordre de la politique IKE par rapport aux deux homologues négociateurs lors de la tentative de recherche d'une association de sécurité (SA) commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de première priorité, il essaie d'utiliser les paramètres définis dans le niveau de priorité immédiatement inférieur. Les valeurs valides sont comprises entre 1 et 65 535. Plus le numéro de priorité est faible, plus la priorité est élevée. Si vous laissez ce champ vide, le centre de gestion attribue la valeur non attribuée la plus basse en commençant par 1, puis 5, puis continue par incréments de 5.

Étape 6 Choisissez la méthode de **chiffrement**.

Au moment de décider quel chiffrement et quels algorithmes de hachage utiliser pour la politique IKEv1, votre choix se limite aux algorithmes pris en charge par les périphériques homologues. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Pour IKEv1, sélectionnez l'une des options. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser.

Étape 7 Choisissez l'algorithme de **hachage** qui crée un condensé de message, qui est utilisé pour assurer l'intégrité du message.

Lorsque vous décidez quels algorithmes de chiffrement et de hachage utiliser pour la proposition IKEv1, votre choix se limite aux algorithmes pris en charge par les périphériques gérés. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser.

Étape 8 Définissez le **Diffie-Hellman Group**.

Le groupe Diffie-Hellman à utiliser pour le chiffrement. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez le groupe que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Choix du groupe de module Diffie-Hellman à utiliser.

Étape 9 Définissez la **Durée de vie** de l'association de sécurité (SA) en secondes Vous pouvez spécifier une valeur comprise entre 120 et 2 147 483 647 secondes. La valeur par défaut est 86 400.

Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En général, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE sont sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes.

Étape 10 Définissez la **méthode d'authentification** à utiliser entre les deux homologues.

- **Clé** prépartagée : les clés prépartagées permettent de partager une clé secrète entre deux homologues et d'être utilisée par IKE pendant la phase d'authentification. Si l'un des homologues participants n'est pas configuré avec la même clé prépartagée, le SA IKE ne peut pas être établi.
- **Certificat** : lorsque vous utilisez les certificats comme méthode d'authentification pour les connexions VPN, les homologues obtiennent des certificats numériques d'un serveur d'autorité de certification de votre infrastructure PKI et les échangent pour s'authentifier mutuellement.

Remarque Dans une topologie VPN qui prend en charge IKEv1, la **méthode d'authentification** spécifiée dans l'objet de politique IKEv1 choisi devient la valeur par défaut dans le paramètre de type d'**authentification** IKEv1. Ces valeurs doivent correspondre, sinon, votre configuration produira une erreur.

Étape 11 Cliquez sur **Save** (Enregistrer).

La nouvelle politique IKEv1 est ajoutée à la liste.

Configurer des objets de politique IKEv2

Utilisez la boîte de dialogue de politique IKEv2 pour créer, supprimer et modifier un objet de politique IKEv2. Ces objets de politique contiennent les paramètres requis pour les politiques IKEv2.

Procédure

Étape 1 Choisissez **Objets** > **Gestion des objets**, puis **Politique IKEv2** > **VPN** dans la table des matières.

Les politiques configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** ( ), **Afficher** ( )ou **Supprimer** ( ) une politique.

Étape 2 Choisissez **Ajouter** ( )**Add IKEv2 Policy** (ajouter une politique IKEv2) pour créer une nouvelle politique.

Étape 3 Entrez un **nom** pour la politique.

Le nom de l'objet Politique. Un maximum de 128 caractères est permis

Étape 4 Saisissez une **description** pour la politique.

Une description de l'objet Politique Un maximum de 1024 caractères est permis

Étape 5 Saisissez la **priorité**.

Valeur de priorité de la proposition IKE. La valeur de priorité détermine l'ordre des propositions IKE par rapport aux deux homologues négociateurs lors de la tentative de recherche d'une association de sécurité commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de première priorité, il essaie d'utiliser les paramètres définis dans la politique de priorité la plus basse suivante. Cette valeur peut être comprise entre 1 et 65 535. Plus le numéro de priorité est faible, plus la priorité est élevée. Si vous laissez ce champ vide, le centre de gestion attribue la valeur non attribuée la plus basse en commençant par 1, puis 5, puis continue par incréments de 5.

Étape 6 Définissez la **Durée de vie** de l'association de sécurité (SA) en secondes Vous pouvez spécifier une valeur comprise entre 120 et 2 147 483 647 secondes. La valeur par défaut est 86 400.

Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En général, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE sont sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes.

Étape 7 Choisissez la partie **Integrity Algorithms** (algorithmes d'intégrité) de l'algorithme de hachage utilisé dans la politique IKE. L'algorithme de hachage crée un condensé de message, qui est utilisé pour assurer l'intégrité du message.

Lorsque vous décidez quels algorithmes de chiffrement et de hachage utiliser pour la proposition IKEv2, votre choix se limite aux algorithmes pris en charge par les périphériques gérés. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Sélectionnez tous les algorithmes que vous souhaitez autoriser dans le VPN.Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser.

Étape 8 Choisissez l' **algorithme de chiffrement** utilisé pour établir le SA de phase 1 en vue de protéger les négociations de la phase 2.

Lorsque vous décidez quels algorithmes de chiffrement et de hachage utiliser pour la proposition IKEv2, votre choix se limite aux algorithmes pris en charge par les périphériques gérés. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Sélectionnez tous les algorithmes que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser.

Étape 9 Choisissez **l'algorithme PRF**.

La partie fonction pseudo-aléatoire (PRF) de l'algorithme de hachage utilisée dans la politique IKE. Dans IKEv1, les algorithmes d'intégrité et de PRF ne sont pas séparés, mais dans IKEv2, vous pouvez spécifier des algorithmes différents pour ces éléments. Sélectionnez tous les algorithmes que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser.

Étape 10 Sélectionnez et **ajoutez** un **groupe DH**.

Le groupe Diffie-Hellman utilisé pour le chiffrement. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez les groupes que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Choix du groupe de module Diffie-Hellman à utiliser.

Étape 11 Cliquez sur **Save** (Enregistrer).
Si une combinaison valide de choix a été sélectionnée, la nouvelle politique IKEv2 est ajoutée à la liste. Sinon, des erreurs s'affichent et vous devez apporter les modifications en conséquence pour enregistrer cette politique avec succès.

Objets de fichier

Utilisez les boîtes de dialogue Add (ajouter) et Edit File Object (modifier un objet de fichier) pour créer et modifier des objets fichier. Les objets de fichier représentent les fichiers utilisés dans les configurations, généralement pour les stratégies VPN d'accès à distance. Ils peuvent contenir des fichiers Secure Client Profile et Secure Client Image.

Des profils sont également créés pour chaque module AnyConnect et VPN de gestion Secure Client (services client sécurisés) à l'aide d'éditeurs de profils indépendants et déployés selon les exigences de l'utilisateur final et les politiques d'authentification définies par l'administrateur sur les points terminaux dans le cadre de Secure Client, et ils mettent les profils réseau préconfigurés à la disposition des utilisateurs finaux.

Lorsque vous créez un objet fichier, centre de gestion effectue une copie du fichier dans son référentiel. Ces fichiers sont sauvegardés chaque fois que vous créez une sauvegarde de la base de données et ils sont restaurés si vous restaurez la base de données. Lors de la copie d'un fichier vers la plateforme pour l'utiliser dans un objet fichier, ne copiez pas le fichier directement dans le référentiel de fichiers.

Lorsque vous déployez des configurations qui précisent un objet fichier, le fichier associé est téléchargé sur le périphérique dans le répertoire approprié.

Vous pouvez cliquer sur l'une des options suivantes pour chaque fichier :

- **télécharger** : Cliquez ici pour télécharger le fichier Secure Client.
- **Modifier** : modifiez les détails de l'objet fichier.

- **Supprimer** :Supprimez l'objet fichier Secure Client (services client sécurisés). Lorsque vous supprimez un objet fichier, le fichier associé n'est pas supprimé du référentiel de fichiers, seul l'objet est supprimé.

Chemin de navigation

Objet > **Gestion** > **VPN** > **Fichier Secure Client**.

Champs

- **Name** (non) : saisissez le nom du fichier pour identifier l'objet fichier. vous pouvez ajouter jusqu'à 128 caractères.
- **File Name**(nom de fichier) : cliquez sur **Parcourir** pour sélectionner le fichier. Le nom et le chemin d'accès complet du fichier sont ajoutés lorsque vous sélectionnez le fichier.
- **File Type** (type de fichier) : choisissez le type de fichier correspondant au fichier que vous avez sélectionné. Les types de fichiers suivants sont disponibles :
  - **Image Secure Client** : Sélectionnez ce type lorsque vous ajoutez l'image Secure Client (services client sécurisés) que vous avez téléchargée à partir du Centre de téléchargement de logiciels Cisco.

    Vous pouvez associer toute image Secure Client (services client sécurisés) nouvelle ou supplémentaire à la politique VPN d'accès à distance. Vous pouvez également dissocier les ensembles de clients non pris en charge ou en fin de vie qui ne sont plus nécessaires.
  - **Secure Client VPN Profile** (Profil VPN AnyConnect, Profil de VPN Secure client) : Choisissez ce type pour le fichier de profil VPN Secure Client.

    Le fichier de profil est créé à l'aide de l'outil Secure Client Profile Editor basé sur GUI, un outil de configuration indépendant. Consulter le chapitre *Secure Client Profile Editor* de la version appropriée du Guide de l' Guide de l'utilisateur de Cisco Secure Client (y compris AnyConnect) pour en savoir plus.
  - **Secure Client Management VPN Profile** sélectionnez ce type lorsque vous ajoutez un fichier de profil pour le tunnel VPN de gestion Secure Client.

    Téléchargez l'**éditeur de profil autonome de tunnel de gestion VPN** Secure Client à partir du centre de téléchargement de logiciels Cisco si vous ne l'avez pas encore fait et créez un profil avec les paramètres requis pour le tunnel VPN de gestion Secure Client.
  - **Profil de service d'activateur AMP** : le profil est utilisé pour l'activateur Secure Client. L'activateur Cisco Advanced Malware Protection avec ce profil est transmis aux points terminaux à partir de défense contre les menaces lorsqu'un utilisateur de VPN d'accès à distance se connecte au VPN.
  - **Profil de commentaire** : vous pouvez ajouter un profil de commentaire sur l'expérience client et sélectionner ce type pour recevoir des informations sur les fonctionnalités et les modules que les clients ont activés et qu'ils utilisent.
  - **ISE Posture Profile** : Choisissez cette option si vous ajoutez un fichier de profil pour le module Secure Client ISE Posture.
  - **NAM Service Profile** : configurez et ajoutez le fichier de profil NAM à l'aide de l'éditeur de profil Network Access Manager.
  - **Network Visibility Service Profile** : fichier de profil pour le module Secure Client de visibilité réseau. Vous pouvez créer le profil à l'aide de l'éditeur de profils NVM.

- **Profil de sécurité Umbrella itinérante** : vous devez sélectionner ce type de fichier si vous déployez le module de sécurité Umbrella itinérante en utilisant le fichier .json créé à l'aide de l'éditeur de profils.
- **Web Security Service Profile** :Sélectionnez ce type de fichier lorsque vous ajoutez un fichier de profil pour le module de sécurité Web.
- **Secure Firewall Posture Package** : Sélectionnez ce type de fichier lorsque vous ajoutez un fichier de paquet Secure Firewall Posture. Ce fichier est utilisé lors de la configuration d'une politique d'accès dynamique (DAP) pour recueillir des informations sur le système d'exploitation, les logiciels antivirus, anti-logiciels espions et pare-feu installés sur les points d'accès.
- **Secure Client External Browser Package** : ce type de fichier permet de sélectionner un fichier de paquet de navigateur externe pour l'authentification unique Web SAML.

  Vous pouvez ajouter un le fichier de paquet quand une nouvelle version du fichier de paquet externe est disponible.

  Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance.

- **Description** : ajoutez une description facultative.

Sujets connexes

Image Cisco Secure Client
Options de politique de groupe Secure Client (services client sécurisés), à la page 125

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.