Objets

Les objets sont des conteneurs réutilisables qui définissent les critères que vous souhaitez utiliser dans les politiques ou d'autres paramètres. Par exemple, les objets réseau définissent les adresses d'hôte et de sous-réseau.

Les objets vous permettent de définir des critères afin de pouvoir réutiliser facilement les mêmes critères dans différentes politiques. Lorsque vous mettez à jour un objet, toutes les politiques qui utilisent l'objet sont automatiquement mises à jour.

- Types d'objets, à la page 1
- Gestion des objets, à la page 4

Types d'objets

Vous pouvez créer les types d'objets suivants. Dans la plupart des cas, si une politique ou un paramètre autorise un objet, vous devez utiliser un objet.

Type d'objet	Utilisation principale	Description
Profil client AnyConnect	VPN d'accès à distance.	Les profils client AnyConnect sont téléchargés sur les clients avec le logiciel client AnyConnect. Ces profils définissent de nombreuses options liées au client, telles que la connexion automatique au démarrage et la reconnexion automatique, et si l'utilisateur final peut modifier l'option à partir des client AnyConnect préférences et des paramètres avancés. Consultez Configurer et charger les profils client AnyConnect.
Filtre d'application	Règles de contrôle d'accès.	Un objet de filtre d'application définit les applications utilisées dans une connexion IP ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser les spécifications de port. Consultez Configuration des objets de filtre d'application, à la page 9.

Type d'objet	Utilisation principale	Description
Certificats	Politiques d'identité. VPN d'accès à distance. Règles de déchiffrement SSL. Serveur Web de gestion.	Les certificats numériques fournissent une identification numérique aux fins d'authentification. Les certificats sont utilisés pour les connexions SSL (Secure socket Layer), TLS (Transport Layer Security) et DTLS (Datagram TLS), comme HTTPS et LDAPS. Consultez Configuration des certificats.
Groupes DNS	Paramètres DNS pour les interfaces de gestion et de données.	Les groupes DNS définissent une liste de serveurs DNS et de certains attributs associés. Les serveurs du système de noms de domaine (DNS) résolvent les noms de domaine complets (FQDN), tels que www.exemple.com, en adresses IP. Consultez Configuration des groupes DNS.
Event List Filters (Filtres de liste d'événements)	Paramètres de journalisation système pour sélectionner les destinations de journalisation.	(Filtres du journal d'événements) et Event List Filters (Filtres de liste d'événements) créent une liste de filtres personnalisée pour les messages syslog. Vous pouvez les utiliser pour limiter les messages envoyés à un emplacement de journalisation particulier, tel qu'un serveur syslog ou le tampon de journal interne. Consultez Configurer Event List Filters (Filtres de liste d'événements).
Géolocalisation	Politiques de sécurité.	Un objet de géolocalisation définit les pays et les continents qui hébergent le périphérique qui est la source ou la destination du trafic. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser des adresses IP. Consultez Configuration des objets de géolocalisation, à la page 13.
Sources d'identité	Politiques d'identité VPN d'accès à distance Accès FDM	Les sources d'identité sont des serveurs et des bases de données qui définissent les comptes utilisateur. Vous pouvez utiliser ces informations de diverses manières, par exemple en fournissant l'identité de l'utilisateur associée à une adresse IP ou pour l'authentification des connexions VPN d'accès à distance ou de l'accès à FDM. Consultez Sources d'identité.
Politique IKE	VPN	Les objets de politique Internet Key Exchange (IKE) définissent la proposition IKE utilisée pour authentifier les homologues IPsec, négocier et distribuer les clés de chiffrement IPsec, et établir automatiquement des associations de sécurité IPsec (SA). Il existe des objets distincts pour IKEv1 et IKEv2. Consultez Configuration de la politique IKE globale.

Type d'objet	Utilisation principale	Description
Proposition IPsec	VPN	Les objets Proposition IPsec configurent la proposition IPsec utilisée lors des négociations de la phase 2 d'IKE. La proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec. Il existe des objets distincts pour IKEv1 et IKEv2. Consultez Configuration des propositions IPsec.
Réseau	Politiques de sécurité et une vaste gamme de paramètres de périphérique.	Les groupes de réseaux et les objets réseau (collectivement appelés objets réseau) définissent les adresses des hôtes ou des réseaux. Consultez Configuration des objets et des groupes de réseau., à la page 5.
Port	Politiques de sécurité.	Les groupes de ports et les objets de port (collectivement appelés objets de port) définissent les protocoles, les ports ou les services ICMP pour le trafic. Consultez Configuration des objets et groupes de ports, à la page 7.
Clés secrètes	Politiques Smart CLI et FlexConfig.	Les objets de clé secrète définissent des mots de passe ou d'autres chaînes d'authentification que vous souhaitez chiffrer et masquer. Consultez Configuration des objets de clé secrète.
Zone de sécurité	Politiques de sécurité.	Une zone de sécurité est un regroupement d'interfaces. Les zones divisent le réseau en segments pour vous aider à gérer et à classer le trafic. Consultez Configuration des zones de sécurité, à la page 8.
Groupes SGT	Politiques de contrôle d'accès.	Les balises de groupe de sécurité TrustSec (SGT) définissent des balises pour le trafic, conformément à la définition utilisée dans Cisco Identity Services Engine (ISE). Vous devez configurer ISE avant de pouvoir créer ces objets. Vous pouvez ensuite utiliser les objets comme critères de correspondance source/destination dans les règles de contrôle d'accès. Consultez Configuration des groupes de balises de groupe de sécurité (SGT), à la page 15.
Moniteurs SLA	Routes statiques	Un moniteur SLA définit une adresse IP cible à utiliser pour surveiller une route statique. Si le moniteur détermine que l'adresse IP cible ne peut plus être atteinte, le système peut installer une route statique de sauvegarde. Consultez Configuration des objets du moniteur SLA.

Type d'objet	Utilisation principale	Description
Chiffrements SSL	Paramètres SSL	Un objet de chiffrement SSL définit une combinaison de niveau de sécurité, de versions de protocole TLS/DTLS et d'algorithmes de chiffrement qui peuvent être utilisés lors de l'établissement d'une connexion SSL avec FTD. Utilisez ces objets dans les paramètres système pour définir les exigences de sécurité pour les utilisateurs qui établissent des connexions TLS/SSL avec le boîtier. Consultez Configuration des paramètres de chiffrement TLS/SSL.
Serveurs journal système	Règles de contrôle d'accès Journalisation diagnostique. Politiques de renseignements sur la sécurité Règles de déchiffrement SSL. Politiques de prévention des intrusions Politique sur les fichiers et les programmes malveillants	Un objet serveur Syslog identifie un serveur qui peut recevoir des messages en mode connexion ou des messages de dépistage du journal système (syslog). Consultez Configuration des serveurs Syslog, à la page 14.
URL	Règles de contrôle d'accès Politiques de renseignements sur la sécurité	Les objets et groupes d'URL définissent les adresses URL ou IP des requêtes Web. Consultez Configuration des objets et groupes d'URL., à la page 11.
Utilisateurs	VPN d'accès à distance.	Vous pouvez créer des comptes utilisateur directement sur le périphérique pour une utilisation avec le VPN d'accès à distance. Vous pouvez utiliser les comptes d'utilisateurs locaux au lieu ou en plus d'une source d'authentification externe. Consultez Configurer les utilisateurs locaux.

Gestion des objets

Vous pouvez configurer des objets directement à partir de la page Objects (Objets) ou les configurer lors de la modification des politiques. Les deux méthodes fournissent les mêmes résultats, un objet nouveau ou mis à jour. Utilisez donc la technique qui correspond à vos besoins du moment.

La procédure suivante explique comment créer et gérer vos objets directement à partir de la page Objects (Objets).

Remarque Lorsque vous modifiez une politique ou un paramètre, si une propriété nécessite un objet, une liste de ceux qui sont déjà définis s'affiche et vous sélectionnez l'objet approprié. Si l'objet souhaité n'existe pas encore, cliquez simplement sur le lien **Create New Object** (Créer un nouvel objet) affiché dans la liste.

Procédure

Étape 1 Sélectionnez **Objects** (Objets).

La page des objets comporte une table des matières répertoriant les types d'objets disponibles. Lorsque vous sélectionnez un type d'objet, vous voyez une liste des objets existants et vous pouvez en créer de nouveaux à partir d'ici. Vous pouvez également voir le contenu et le type de l'objet.

Étape 2 Sélectionnez le type d'objet dans la table des matières et effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**. Le contenu des objets diffère en fonction du type; consultez la rubrique de configuration pour chaque type d'objet pour obtenir des renseignements précis.
- Pour créer un objet de groupe, cliquez sur le bouton **Add Group** (Ajouter un groupe) (). Les objets de groupe comprennent plusieurs éléments.
- Pour modifier un objet, cliquez sur l'icône de modification () de l'objet. Vous ne pouvez pas modifier le contenu d'un objet prédéfini.
- Pour supprimer un objet, cliquez sur l'icône de suppression () de l'objet. Vous ne pouvez pas supprimer un objet s'il est utilisé dans une politique ou dans un autre objet, ou s'il s'agit d'un objet prédéfini.

Configuration des objets et des groupes de réseau.

Utilisez les groupes d'objets réseau et les objets réseau (désignés collectivement comme des objets réseau) pour définir les adresses des hôtes ou des réseaux. Vous pouvez ensuite utiliser les objets dans les politiques de sécurité pour définir les critères de correspondance du trafic, ou dans les paramètres pour définir les adresses des serveurs ou d'autres ressources.

Un objet réseau définit un seul hôte ou une adresse réseau, alors qu'un objet de groupe de réseau peut définir plusieurs adresses.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets réseau lors de la modification d'une propriété d'adresse en cliquant sur le lien **Create New Network** (Créer un nouveau réseau) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Network** (Réseau) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour créer un groupe, cliquez sur le bouton **Add Group** (ajouter un groupe) ().
- Pour modifier un objet ou un groupe, cliquez sur l'icône de modification () de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille () de l'objet.

Étape 3 Saisissez un nom pour l'objet et, au besoin, une description, puis définissez le contenu de l'objet.

Nous vous recommandons de ne pas utiliser une adresse IP uniquement pour le nom afin de pouvoir déterminer facilement les noms d'objets à partir du contenu d'objets ou d'adresses IP autonomes. Si vous souhaitez utiliser une adresse IP dans le nom, préfixez-la avec quelque chose de significatif, tel que host-192.168.1.2 ou network-192.168.1.0. Si vous utilisez une adresse IP comme nom, le système ajoute une barre verticale comme préfixe, par exemple, |192.168.1.2. FDM n'affiche pas de barre dans les sélecteurs d'objets, mais vous verrez cette norme de dénomination si vous examinez la configuration en cours d'utilisation à l'aide de la commande **show running-config** dans l'interface de ligne de commande.

Étape 4 Configurez le contenu de l'objet.

Objets de réseau

Sélectionnez le **Type** d'objet et configurez le contenu :

- **Network** (Réseau) : saisissez une adresse réseau dans l'un des formats suivants :
  - Réseau IPv4, masque de sous-réseau inclus, par exemple : 10.100.10.0/24 ou 10.100.10.0/255.255.255.0.
  - Réseau IPv6, préfixe inclus, par exemple : 2001:DB8:0:CD30::/60.
- **Host (**Hôte) : saisissez une adresse IP d'hôte dans l'un des formats suivants :
  - Adresse d'hôte IPv4, par exemple : 10.100.10.10.
  - Adresse d'hôte IPv6, par exemple : 2001:DB8::0DB8:800:200C:417A ou 2001:DB8:0:0:0DB8:800:200C:417A.
- **Range** (Plage) : une plage d'adresses, dont l'adresse de début et l'adresse de fin sont séparées par un trait d'union. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe. Par exemple, 192.168.1.10-192.168.1.250 ou 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100.
- **FQDN** : saisissez un seul nom de domaine complet, tel que www.exemple.com. Vous ne pouvez pas utiliser de caractères génériques. Sélectionnez aussi **DNS Resolution** (Résolution DNS) afin de déterminer si vous souhaitez associer au FQDN des adresses IPv4, IPv6, ou à la fois IPv4 et IPv6. La valeur par défaut est à la fois IPv4 et IPv6. Vous pouvez utiliser ces objets dans les règles de contrôle d'accès seulement. Les règles correspondent à l'adresse IP obtenue pour le FQDN par une recherche DNS.

Groupes de réseaux

Cliquez sur le bouton **+** pour sélectionner les objets ou les groupes réseau à ajouter au groupe. Vous pouvez également créer de nouveaux objets.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets et groupes de ports

Utilisez des objets de groupe et de port (collectivement appelés objets de port) pour définir les protocoles, les ports ou les services ICMP pour le trafic. Vous pouvez utiliser les objets et les groupes dans les politiques de sécurité pour définir les critères de correspondance du trafic réseau, par exemple pour utiliser des règles d'accès pour autoriser le trafic vers des ports TCP spécifiques.

Un objet de port définit un protocole unique, un port TCP/UDP ou une plage de ports ou un service ICMP, alors qu'un objet de groupe de ports peut définir plusieurs services.

Le système comprend plusieurs objets prédéfinis pour les services communs. Vous pouvez utiliser ces objets dans vos politiques. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

Remarque Lors de la création d'objets de groupe de ports, vérifiez que la combinaison des objets a du sens. Par exemple, vous ne pouvez pas avoir un mélange de protocoles dans un objet si vous l'utilisez pour spécifier les ports source et de destination dans une règle d'accès. Faites preuve de prudence lorsque vous modifiez un objet qui est déjà utilisé, sinon vous pourriez invalider (et désactiver) les politiques qui utilisent l'objet.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de port lorsque vous modifiez une propriété de service en cliquant sur le lien **Create New Port** (Créer un nouveau port) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Ports** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour créer un groupe, cliquez sur le bouton **Add Group** (ajouter un groupe) ( ).
- Pour modifier un objet ou un groupe, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Saisissez un nom pour l'objet et, éventuellement, une description, et définissez le contenu de l'objet.

Objets de port

Sélectionnez le **protocole**, puis configurez-le comme suit :

- **TCP**, **UDP** : saisissez le numéro de port unique ou de plage de ports, par exemple, 80 (pour HTTP) ou 1-65535 (pour couvrir tous les ports).
- **ICMP**, **IPv6-ICMP** : sélectionnez le **type ICMP** et éventuellement, le **code**. Sélectionnez **Any** (Tous) pour le type à appliquer à tous les messages ICMP. Pour en apprendre davantage sur les types et les codes, consultez les pages suivantes :
  - ICMP—http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6—http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **Other** (Autre) : sélectionnez le protocole souhaité.

Groupes de ports

Cliquez sur le bouton + pour sélectionner les objets de port à ajouter au groupe. Vous pouvez également créer de nouveaux objets.

Étape 4 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des zones de sécurité

Une zone de sécurité est un regroupement d'interfaces. Les zones divisent le réseau en segments pour vous aider à gérer et à classer le trafic. Vous pouvez définir plusieurs zones, mais une interface donnée ne peut se trouver que dans une seule zone.

Le système crée les zones suivantes lors de la configuration initiale. Vous pouvez modifier ces zones pour ajouter ou supprimer des interfaces, ou vous pouvez supprimer les zones si vous ne les utilisez plus.

- **inside_zone** : Comprend l'interface interne. Si l'interface interne est un groupe de ponts, cette zone comprend toutes les interfaces membres du groupe de ponts au lieu de l'interface virtuelle de pont (BVI) interne. Cette zone est destinée à représenter les réseaux internes.
- **outside_zone** : Comprend l'interface externe. Cette zone est destinée à représenter les réseaux en dehors de votre contrôle, comme Internet.

Généralement, vous regrouperiez les interfaces selon le rôle qu'elles jouent dans votre réseau. Par exemple, vous placeriez l'interface qui se connecte à Internet dans la zone de sécurité **outside_zone** et toutes les interfaces pour vos réseaux internes dans la zone de sécurité **inside_zone**. Ensuite, vous pouvez appliquer des règles de contrôle d'accès au trafic en provenance de la zone extérieure et à destination de la zone intérieure.

Avant de créer des zones, tenez compte des règles d'accès et des autres politiques que vous souhaitez appliquer à vos réseaux. Par exemple, vous n'avez pas besoin de mettre toutes les interfaces internes dans la même zone. Si vous avez quatre réseaux internes et que vous souhaitez en traiter un différemment des trois autres, vous pouvez créer deux zones plutôt qu'une. Si vous avez une interface qui devrait permettre un accès externe à un serveur Web public, vous pouvez utiliser une zone distincte pour l'interface.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des zones de sécurité lorsque vous modifiez une propriété de zone de sécurité en cliquant sur le lien **Create New Security Zone** (créer une nouvelle zone de sécurité) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Sélectionnez le **Mode** de la zone.

Cela est directement lié au mode d'interface. La zone peut contenir un seul type d'interface.

- **Routées** : les interfaces routées sont les interfaces normales pour le trafic traversant qui peuvent appliquer des politiques de sécurité.
- **Passives** : les interfaces passives n'affectent pas le trafic qui traverse le périphérique.

Étape 5 Dans la liste des **Interfaces**, cliquez sur **+** et sélectionnez les interfaces à ajouter à la zone.

La liste affiche toutes les interfaces nommées qui ne sont pas actuellement dans une zone. Vous devez configurer une interface et lui donner un nom avant de pouvoir l'ajouter à une zone.

Si toutes les interfaces nommées sont déjà dans des zones, la liste est vide. Si vous essayez de déplacer une interface vers une autre zone, vous devez d'abord la retirer de sa zone actuelle.

Remarque
Vous ne pouvez pas ajouter une interface de groupe de ponts (BVI) à une zone. Au lieu de cela, ajoutez les interfaces de membres. Vous pouvez placer les membres dans différentes zones.

Étape 6 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets de filtre d'application

Un objet de filtre d'application définit les applications utilisées dans une connexion IP ou un filtre qui définit les applications par type, catégorie, balise, risque ou pertinence commerciale. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser les spécifications de port.

Bien que vous puissiez préciser des applications individuelles dans la règle, les filtres d'applications simplifient la création et l'administration des politiques. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

Vous pouvez sélectionner des applications et des filtres d'application directement dans une politique sans utiliser d'objets de filtre d'application. Cependant, un objet est pratique si vous souhaitez créer plusieurs politiques pour le même groupe d'applications ou de filtres. Le système comprend plusieurs filtres d'application prédéfinis, que vous ne pouvez ni modifier ni supprimer.

Remarque Cisco procède fréquemment à la mise à jour ou à l'ajout de détecteurs d'applications supplémentaires au moyen des mises à jour du système et de la base de données sur les vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de filtre d'application lors de la modification d'une règle de contrôle d'accès en cliquant sur le lien **Save As Filter** (Enregistrer en tant que filtre) après avoir ajouté des critères d'application sous l'onglet Applications.

Avant de commencer

Lors de l'édition d'un filtre, si une application sélectionnée a été supprimée par une mise à jour de VDB, « (Deprecated) » s'affiche après le nom de l'application. Vous devez supprimer ces applications du filtre, sinon les déploiements et les mises à niveau logicielles du système suivants seront bloqués.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Application Filters** (Filtres d'applications) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification () de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille () de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Dans la liste **Applications**, cliquez sur **Add + (Ajouter +)** et sélectionnez les applications et les filtres à ajouter à l'objet.

La liste initiale affiche les applications dans une liste déroulante continuellement. Cliquez sur **Advanced Filter** (Filtre avancé) pour afficher les options de filtre et faciliter la sélection des applications. Cliquez sur **Add** (Ajouter) lorsque vous avez effectué vos sélections. Vous pouvez répéter le processus pour ajouter des applications ou des filtres supplémentaires.

Remarque
Plusieurs sélections dans un seul critère de filtre ont une relation OU. Par exemple, le risque est élevé ou très élevé. La relation entre les filtres est ET, donc le risque est élevé ou très élevé, ET la pertinence commerciale est faible ou très faible. Lorsque vous sélectionnez des filtres, la liste des applications dans l'affichage est mise à jour pour n'afficher que celles qui répondent aux critères. Vous pouvez utiliser ces filtres pour vous aider à trouver les applications que vous souhaitez ajouter individuellement ou pour vérifier que vous sélectionnez les filtres souhaités à ajouter à la règle.

Risques

La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation, de très faible à très élevée.

Pertinence commerciale

La probabilité que l'application soit utilisée dans le cadre des activités professionnelles de votre entreprise, plutôt qu'à des fins récréatives, de très faible à très élevée.

Types

Le type d'application :

- **Application Protocol** (Protocole d'application) : protocoles d'application tels que HTTP et SSH, qui représentent les communications entre les hôtes.
- **Client Protocol** (Protocole client) : clients tels que les navigateurs Web et les clients de messagerie, qui représentent les logiciels s'exécutant sur l'hôte.

- **Web Application** (Application Web) : applications Web telles que MPEG video et Facebook, qui représentent le contenu ou l'URL demandée pour le trafic HTTP.

Catégories

Une classification générale de l'application qui décrit sa fonction la plus essentielle.

Étiquettes

Des informations supplémentaires sur l'application, similaires à la catégorie.

Pour le trafic chiffré, le système peut identifier et filtrer le trafic en utilisant uniquement les applications marquées **SSL Protocol** (Protocole SSL). Les applications sans cette balise ne peuvent être détectées que dans le trafic non chiffré ou déchiffré. Le système attribue la balise de **trafic déchiffré** aux applications qu'il peut détecter dans le trafic déchiffré uniquement, non chiffré ou non déchiffré.

Liste des applications (bas de l'affichage)

Cette liste est mise à jour à mesure que vous sélectionnez des filtres dans les options au-dessus de la liste, de sorte que vous pouvez voir les applications qui correspondent actuellement au filtre. Utilisez cette liste pour vérifier que votre filtre cible les applications souhaitées lorsque vous avez l'intention d'ajouter des critères de filtre à la règle. Si votre intention est d'ajouter des applications spécifiques, sélectionnez-les dans cette liste.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets et groupes d'URL.

Utiliser des objets et des groupes d'URL (collectivement appelés objets d'URL) pour définir les adresses URL ou IP des requêtes Web. Vous pouvez utiliser ces objets pour mettre en œuvre le filtrage manuel d'URL dans les politiques de contrôle d'accès, ou le blocage dans les politiques Security Intelligence.

Un objet URL définit une seule URL ou adresse IP, alors qu'un objet de groupe d'URL peut définir plusieurs URL ou adresses.

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.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets URL lorsque vous modifiez une propriété d'URL en cliquant sur le lien **Create New URL** (Créer une nouvelle URL) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects (Objets)**, puis sélectionnez **URL** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour créer un groupe, cliquez sur le bouton **Add Group** (ajouter un groupe) ( ).
- Pour modifier un objet ou un groupe, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Définissez le contenu de l'objet.

Objets de l'URL

Saisissez une URL ou une adresse IP dans la boîte **URL**. Vous ne pouvez pas utiliser de caractères génériques dans l'URL.

Groupe d'URL

Cliquez sur le bouton + pour sélectionner les objets URL à ajouter au groupe. Vous pouvez également créer de nouveaux objets.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des objets de géolocalisation

Un objet de géolocalisation définit les pays et les continents qui hébergent le périphérique qui est la source ou la destination du trafic. Vous pouvez utiliser ces objets dans les politiques pour contrôler le trafic au lieu d'utiliser des adresses IP. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

Vous pouvez généralement sélectionner des emplacements géographiques directement dans une politique sans utiliser d'objets de géolocalisation. Cependant, un objet est pratique si vous souhaitez créer plusieurs politiques pour le même groupe de pays et de continents.

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

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de géolocalisation lors de la modification d'une propriété de réseau en cliquant sur le lien **Create New Geolocation** (Créer une nouvelle géolocalisation) affiché dans la liste des objets.

Procédure

Étape 1 Sélectionnez **Objects (Objets)**, puis **Geolocation** (Géolocalisation) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Dans la liste **Continents/Countries** (Continents/Pays), cliquez sur **Add** (Ajouter) et sélectionnez les continents et les pays à ajouter à l'objet.

La sélection d'un continent sélectionne tous les pays du continent.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des serveurs Syslog

Un objet serveur Syslog identifie un serveur qui peut recevoir des messages en mode connexion ou des messages de dépistage du journal système (syslog). Si vous avez un serveur syslog configuré pour la collecte et l'analyse des journaux, créez des objets pour les définir et utilisez les objets dans les politiques connexes.

Vous pouvez envoyer les types d'événements suivants au serveur syslog :

- Événements de connexion. Configurez l'objet serveur syslog sur les types de politiques suivants : règles de contrôle d'accès et action par défaut, règles de déchiffrement SSL et action par défaut, politique sur les renseignements de sécurité.
- les incidents d'intrusion. Configurez l'objet serveur syslog dans la politique de prévention des intrusions.
- Événements de diagnostic. Voir Configurer la journalisation vers un serveur Syslog distant.
- Événements liés aux fichiers ou aux programmes malveillants. Configurez le serveur syslog dans **Device (Appareil)** > **System Settings (Paramètres du système)** > **Logging Settings (Paramètres de journalisation)**.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de serveur syslog tout en modifiant une propriété de serveur de journal système en cliquant sur le lien **Add Syslog Server** (Ajouter un serveur syslog) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Syslog Servers** (Serveurs syslog) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés du serveur :

- **IP Address** (adresse IP) : saisissez l'adresse IP du serveur syslog.
- **Protocol Type** (Type de protocole), **Port Number** (Numéro de port) : sélectionnez le protocole et saisissez le numéro de port à utiliser pour syslog. La valeur par défaut est UDP/514. Si vous sélectionnez **TCP**, le système peut reconnaître lorsque le serveur syslog n'est pas disponible et arrête d'envoyer des événements jusqu'à ce que le serveur soit de nouveau disponible. Le port UDP par défaut est 514 et le port TCP par défaut est 1470. Le port doit être compris entre 1 025 et 65 535.

  Remarque
  Si vous utilisez TCP comme protocole de transport, le système ouvre quatre connexions au serveur syslog pour s'assurer que les messages ne sont pas perdus. Si vous utilisez le serveur syslog pour collecter les

messages d'un très grand nombre de périphériques et que le surdébit de la connexion combinée est trop important pour le serveur, utilisez plutôt UDP.

- **Interface for Device Logs** (Interface pour les journaux du périphérique) : sélectionnez l'interface à utiliser pour l'envoi de messages de dépistage syslog. Les types d'événements suivants utilisent toujours l'interface de gestion : connexion, intrusion, fichier, programme malveillant. Votre sélection d'interface détermine l'adresse IP associée aux messages syslog. Sélectionnez l'une des options suivantes :
  - **Data Interface** (interface de données) : utilisez l'interface de données que vous sélectionnez pour les messages de dépistage syslog. Si le serveur est accessible par l'intermédiaire d'une interface de membre de groupe de ponts, sélectionnez l'interface de groupe de ponts (BVI).S'il est accessible via l'interface de diagnostic (l'interface de gestion physique), nous vous recommandons de sélectionner **Management Interface** (Interface de gestion) plutôt que cette option. Vous ne pouvez pas sélectionner une interface passive.

    Pour les messages système de connexion, d'intrusion, de fichier et de programme malveillant, l'adresse IP source sera soit pour l'interface de gestion, soit pour l'interface de la passerelle si vous passez par des interfaces de données. Notez qu'il doit y avoir des routes appropriées dans la table de routage qui dirigent le trafic vers le serveur syslog via l'interface sélectionnée pour ces types d'événements.
  - **Management Interface** (Interface de gestion) : utilisez l'interface de gestion virtuelle pour tous les types de messages syslog. L'adresse IP source sera soit pour l'interface de gestion, soit pour l'interface de la passerelle si vous passez par des interfaces de données.

Étape 4 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des groupes de balises de groupe de sécurité (SGT)

Utilisez les objets de groupe de balises de sécurité (SGT) pour identifier les adresses source ou de destination en fonction d'une balise SGT attribuée par le Moteur de services d'identité (ISE). Vous pouvez ensuite utiliser les objets dans les règles de contrôle d'accès pour définir les critères de correspondance du trafic.

Vous ne pouvez pas utiliser les informations extraites d'ISE directement dans une règle de contrôle d'accès. Au lieu de cela, vous devez créer des groupes SGT, qui font référence aux informations SGT téléchargées. Vos groupes de balises SGT peuvent faire référence à plusieurs SGT, vous pouvez donc appliquer une politique basée sur les collections de balises pertinentes, le cas échéant.

Pour en savoir plus sur l'utilisation des balises SGT pour le contrôle d'accès, consultez Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec.

Avant de commencer

Avant de créer des groupes SGT, vous devez configurer la source d'identité ISE pour vous abonner aux mappages SXP et déployer les modifications. Le système récupère ensuite les informations SGT à partir du serveur ISE. Ce n'est qu'après le téléchargement des balises SGT que vous pourrez créer des groupes de SGT.

Procédure

Étape 1 Sélectionnez **Objects (Objets)**, puis sélectionnez **SGT Groups (Groupes SGT)** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification () de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille () de l'objet.

Étape 3 Entrez un **nom** pour l'objet et, facultativement, une description,

Étape 4 Sous **Tags (Balises)**, cliquez sur le signe **+** et sélectionnez les balises SGT téléchargées à inclure dans l'objet.

Pour supprimer une balise SGT, cliquez sur le **x** à droite du nom de la balise.

Si la liste est vide, le système n'a pas pu télécharger les mappages SGT. Si cela se produit :

- Assurez-vous que l'objet d'identité ISE s'abonne à la rubrique SXP. Vous devez vous abonner à SXP pour obtenir les mappages.
- Vérifiez que les mappages statiques sont définis dans ISE et qu'ISE est configuré pour publier ces mappages. S'il n'y a aucun mappage, il n'y a tout simplement rien à télécharger. Consultez Configurer les groupes de sécurité et la publication SXP dans ISE

Étape 5 Cliquez sur **OK**.

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.