Paramètres de la plateforme

Les paramètres de plateforme pour les périphériques défense contre les menaces permettent de configurer une gamme de fonctionnalités indépendantes dont vous souhaitez peut-être partager les valeurs entre plusieurs périphériques. Même si vous souhaitez des paramètres différents par périphérique, vous devez créer une politique partagée et l'appliquer au périphérique souhaité.

Introduction aux paramètres de la plateforme

Une politique de paramètres de plateforme est un ensemble partagé de fonctionnalités ou de paramètres qui définissent les aspects d'un périphérique géré qui sont susceptibles d'être similaires aux autres périphériques gérés de votre déploiement, tels que les paramètres d'horloge et l'authentification externe.

Une politique partagée permet de configurer plusieurs périphériques gérés à la fois, ce qui assure la cohérence de votre déploiement et simplifie vos efforts de gestion. Toute modification apportée à une politique de paramètres de plateforme affecte tous les périphériques gérés sur lesquels vous avez appliqué la politique.

Même si vous souhaitez des paramètres différents par périphérique, vous devez créer une politique partagée et l'appliquer au périphérique souhaité.

Par exemple, les politiques de sécurité de votre entreprise peuvent exiger qu'un message « No Unauthorized Use » (Aucune utilisation non autorisée) s'affiche lorsqu'un utilisateur se connecte. Grâce aux paramètres de plateforme, vous pouvez ne définir la bannière de connexion qu'une seule fois dans une politique de paramètres de plateforme.

Vous pouvez également bénéficier de plusieurs politiques de paramètres de plateforme sur un seul centre de gestion. Par exemple, si vous avez différents hôtes de relais de messagerie que vous utilisez selon les circonstances ou si vous souhaitez tester différentes listes d'accès, vous pouvez créer plusieurs politiques de paramètres de plateforme et basculer entre elles, plutôt que de modifier une seule politique.

Exigences et conditions préalables pour les politiques de paramètres de plateforme

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur d'accès

Administrateur de réseau

Gérer les politiques de paramètres de plateforme

Utiliser la page des **paramètres de plateforme** (**Devices (appareils)** > **Platform Settings (paramètres de la plateforme)**) pour gérer les politiques des paramètres de plateforme. Cette page indique le type de périphérique pour chaque politique. La colonne **Status** (état) affiche les périphériques cibles de la politique.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Platform Settings (paramètres de la plateforme)**.

Étape 2 Pour une politique existante, vous pouvez **Copier** ( ), **Edit** ( )ou **Supprimer** ( ) la politique.

Mise en garde Vous ne devez pas supprimer la dernière politique déployée sur les machines cibles, même si elle est obsolète. Avant de supprimer complètement la politique, il est conseillé de déployer une politique différente sur ces cibles.

Étape 3 Cliquez sur **New Policy** pour créer une nouvelle politique.

a) Sélectionnez un type de périphérique dans la liste déroulante :

- **Firepower Settings** pour créer une politique partagée pour les périphériques classiques gérés.

- **Threat Defense Settings** (paramètres de défense contre les menaces) pour créer une politique partagée pour les périphériques gérés défense contre les menaces .

b) Saisissez un **nom** pour la politique et une **description** facultative.
c) Si vous le souhaitez, choisissez les **périphériques disponibles** auxquels vous souhaitez appliquer la politique, puis cliquez sur **Add** (ajouter) (ou faites glisser et déposez) pour ajouter les périphériques sélectionnés. Vous pouvez saisir une chaîne de recherche dans le champ **Search** (rechercher) pour restreindre la liste de périphériques.
d) Cliquez sur **Save** (enregistrer).

Le système crée la politique et l'ouvre pour la modifier.

Étape 4 Pour modifier les machines cibles d'une politique, cliquez sur **Edit** ( ) à côté de la politique de paramètres de plateforme que vous souhaitez modifier.

a) Cliquez sur **Policy Assignments** (Attributions de politiques)
b) Pour affecter un périphérique, une paire à haute disponibilité ou un groupe de périphériques à la politique, sélectionnez-le dans la liste **Périphériques disponibles** et cliquez sur **Add** (Ajouter). Vous pouvez également effectuer un glisser-déposer.
c) Pour supprimer une affectation de périphérique, cliquez sur **Supprimer** ( ) à côté d'un périphérique, d'une paire à haute disponibilité ou d'un groupe de périphériques dans la liste des **périphériques** sélectionnés.
d) Cliquez sur **OK**.

Prochaine étape

- Déployer les changements de configuration.

Inspection ARP

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP.

L'inspection ARP empêche les utilisateurs malveillants d'usurper l'identité d'autres hôtes ou routeurs (connue sous le nom d'usurpation d'identité ARP). L'usurpation d'identité ARP peut permettre une attaque de l'intercepteur. Par exemple, un hôte envoie une requête ARP au routeur de passerelle; le routeur de passerelle répond par l'adresse MAC du routeur de passerelle. Cependant, l'agresseur envoie une autre réponse ARP à l'hôte avec l'adresse MAC de l'agresseur au lieu de l'adresse MAC du routeur. L'agresseur peut désormais intercepter tout le trafic de l'hôte avant de le transférer au routeur.

L'inspection ARP garantit qu'un agresseur ne peut pas envoyer une réponse ARP avec l'adresse MAC de l'agresseur, tant que la bonne adresse MAC et l'adresse IP associée figurent dans le tableau ARP statique.

Lorsque vous activez l'inspection ARP, appareil de défense contre les menaces compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP, et effectue les actions suivantes :

- Si l'adresse IP, l'adresse MAC et l'interface source correspondent à une entrée ARP, le paquet est transmis.

- En cas de non-concordance entre l'adresse MAC, l'adresse IP ou l'interface, appareil de défense contre les menaces abandonne le paquet.
- Si le paquet ARP ne correspond à aucune entrée dans le tableau ARP statique, vous pouvez définir appareil de défense contre les menaces pour transférer le paquet hors de toutes les interfaces (flood) (submersion), ou pour abandonner le paquet.

Remarque L'interface dédiée Diagnostic ne submerge jamais de paquets, même si ce paramètre est réglé à flood.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Inspection ARP**.

Étape 3 Ajoutez des entrées au tableau d'inspection ARP.

a) Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée, ou cliquez sur **Edit** (Modifier) si l'entrée existe déjà.

b) Pour Advanced (Avancé), sélectionnez les options souhaitées :

- **Inspect Enabled**(inspection activée) : pour effectuer une inspection ARP sur les interfaces et les zones sélectionnées.
- **Flood Enabled** (Débordement activé) : si les demandes ARP qui ne correspondent pas aux entrées ARP statiques hors de toutes les interfaces doivent être acheminées par débordement, à l'exception de l'interface d'origine ou de l'interface de gestion dédiée. Il s'agit du comportement par défaut.

  Si vous choisissez de ne pas faire déborder les demandes ARP, seules les demandes qui correspondent exactement aux entrées ARP statiques sont autorisées.
- **Security Zones** (zones de sécurité) : ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. Les zones doivent être des zones commutées. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste de la zone de sécurité sélectionnée et l'ajouter en cliquant sur **Add**. Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 Ajoutez des entrées ARP statiques en fonction de Ajouter une entrée ARP statique.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Bannière

Vous pouvez configurer les messages à afficher aux utilisateurs lorsqu'ils se connectent à l'interface de ligne de commande (CLI) du périphérique.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Bannière**.

Étape 3 Configurer une bannière

Voici quelques conseils et exigences concernant les bannières.

- Seuls les caractères ASCII sont autorisés. Vous pouvez utiliser des retours de ligne (appuyez sur Entrée), mais vous ne pouvez pas utiliser de tabulations.
- Vous pouvez ajouter de manière dynamique le nom d'hôte ou le nom de domaine du périphérique en incluant les variables **$(hostname)** ou **$(domain)**.
- Bien qu'il n'y ait aucune restriction de longueur absolue sur les bannières, les sessions Telnet ou SSH se fermeront si la mémoire système n'est pas suffisante pour traiter les messages des bannières.
- Du point de vue de la sécurité, il est important que votre bannière dissuade les accès non autorisés. N'utilisez pas les mots « bienvenue » ou « s'il vous plaît », car ils semblent inviter des intrus à entrer. La bannière suivante donne le bon ton en cas d'accès non autorisé :

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

DNS

Les serveurs du système de noms de domaine (DNS) sont utilisés pour transformer les noms d'hôtes en adresses IP. Il existe deux paramètres de serveur DNS qui s'appliquent à différents types de trafic : le trafic de données et le trafic spécial de gestion. Le trafic de données comprend tous les services qui utilisent des noms de domaine complets pour lesquels une recherche DNS est nécessaire, comme les règles de contrôle d'accès et l'accès à distance au réseau privé virtuel. Le trafic spécial de gestion comprend le trafic provenant de l'interface de gestion, tel que les mises à jour de la configuration et de la base de données. Cette procédure ne s'applique qu'aux serveurs DNS de *données*. Pour les paramètres DNS de *gestion*, voir les commandes CLI **configure network dns servers** et **configure network dns searchdomains**.

Pour déterminer l'interface correcte pour les communications du serveur DNS, le périphérique géré utilise une recherche de routage, mais la table de routage utilisée dépend des interfaces pour lesquelles vous activez le DNS. Pour en savoir plus, reportez-vous aux paramètres de l'interface ci-dessous.

Vous pouvez éventuellement configurer plusieurs groupes de serveurs DNS et les utiliser pour résoudre différents domaines DNS. Par exemple, vous pouvez avoir un groupe par défaut "fourre-tout" qui utilise des serveurs DNS publics, pour les connexions à l'internet. Vous pouvez ensuite configurer un groupe distinct pour utiliser les serveurs DNS internes pour le trafic interne, par exemple, toute connexion à une machine du domaine exemple.com. Ainsi, les connexions à un nom de domaine complet utilisant le nom de domaine de votre organisation seront résolues à l'aide de vos serveurs DNS internes, tandis que les connexions à des serveurs publics utiliseront des serveurs DNS externes. Ces résolutions sont utilisées par toutes les fonctions qui utilisent la résolution DNS de données, telles que le NAT et les règles de contrôle d'accès.

Vous pouvez configurer des services DNS de confiance pour le snooping (surveillance) DNS à l'aide de l'onglet Serveurs DNS de confiance. Le snooping (surveillance) DNS est utilisé pour mettre en correspondance les domaines d'application et les IP afin de détecter l'application dès le premier paquet. Outre la configuration des serveurs DNS de confiance, vous pouvez inclure les serveurs déjà configurés dans le groupe DNS, le pool DHCP, le relais DHCP et le client DHCP en tant que serveurs DNS de confiance.

Remarque Pour un PBR basé sur une application, vous devez configurer des serveurs DNS de confiance. Vous devez également veiller à ce que le trafic DNS soit transmis en clair au travers de défense contre les menaces (le DNS chiffré n'est pas pris en charge) afin que les domaines puissent être résolus pour détecter les applications.

Avant de commencer

- Assurez-vous d'avoir créé ou plusieurs groupe(s) de serveurs DNS. Pour en savoir plus, consultez Création d'objets de groupe de serveurs DNS.
- Assurez-vous que vous avez créé des objets d'interface pour vous connecter aux serveurs DNS.
- Assurez-vous que le périphérique géré dispose des routes statiques ou dynamiques appropriées pour accéder aux serveurs DNS.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créer ou modifier une politique de défense contre les menaces.

Étape 2 Cliquez sur **DNS**.

Étape 3 Cliquez sur l'onglet **Paramètres DNS**.

Étape 4 Cochez **Activer la résolution de nom DNS par le périphérique**.

Étape 5 Configurer les groupes de serveurs DNS.

a) Effectuez l'une des opérations suivantes dans la liste des groupes de serveurs DNS :

- Pour ajouter un groupe à la liste, cliquez sur **Ajouter**. Vous ne pouvez pas ajouter de nouveau groupe une fois que 30 domaines de filtrage ont été configurés dans la liste existante des groupes de serveurs.
- Pour modifier les paramètres d'un groupe, cliquez sur **Edit** (✎) en regard du groupe en question.

- Pour supprimer un groupe, cliquez sur **Supprimer** ( ) à côté du groupe. La suppression d'un groupe ne supprime pas l'objet groupe de serveurs DNS, mais le supprime simplement de cette liste.

b) Lors de l'ajout ou de la modification d'un groupe, configurez les paramètres suivants, puis cliquez sur **OK** :

- **Sélectionner un groupe DNS** - Sélectionnez un objet de groupe de serveurs DNS existant ou cliquez sur **+** pour en créer un nouveau.
- **Définir par défaut**- Sélectionnez cette option pour faire de ce groupe le groupe par défaut. Toute demande de résolution DNS qui ne correspond pas aux filtres des autres groupes sera résolue en utilisant les serveurs de ce groupe.
- **Domaines de filtrage** - Pour les groupes non définis par défaut uniquement, une liste de noms de domaine séparés par des virgules, tels que exemple.com, exemple2.com. Ne pas inclure d'espaces.

  Le groupe sera utilisé pour les résolutions DNS pour ces domaines uniquement. Vous pouvez saisir un maximum de 30 domaines distincts dans tous les groupes ajoutés à cette stratégie de paramètres de plateforme DNS. Chaque nom peut comporter un maximum de 127 caractères.

  Notez que ces domaines de filtrage ne sont pas liés au nom de domaine par défaut du groupe. La liste des filtres peut être différente du domaine par défaut.

Étape 6 (Facultatif) Saisissez les valeurs du **délai d'expiration de l'entrée** et du **délai d'interrogation** en minutes.

Ces options s'appliquent uniquement aux noms de domaine complets spécifiés dans les objets réseau. Elles ne s'appliquent pas aux noms de domaine complets utilisés dans d'autres fonctions.

- La **délai d'expiration de l'entrée** spécifie la durée de vie minimale (TTL) de l'entrée DNS, en minutes. Si le délai d'expiration est plus long que la durée de vie de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la durée de vie est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée : dans ce cas, aucun délai supplémentaire n'est ajouté à la durée de vie. À l'expiration, l'entrée est supprimée de la table de consultation du DNS. La suppression d'une entrée nécessite la recompilation de la table, de sorte que des suppressions fréquentes peuvent augmenter la charge de traitement du périphérique. Comme certaines entrées DNS peuvent avoir une durée de vie très courte (jusqu'à trois secondes), vous pouvez utiliser ce paramètre pour prolonger virtuellement cette dernière. La valeur par défaut est 1 minute (c'est-à-dire que la durée de vie minimale pour toutes les résolutions est de 1 minute). La plage est comprise entre 1 et 65535 minutes.

  Notez que pour les systèmes fonctionnant sous la version 7.0 ou antérieure, le délai d'expiration est en fait ajouté à la durée de vie : il ne spécifie pas de valeur minimale.

- **Délai d'interrogation** spécifie le délai après lequel le périphérique interroge le serveur DNS pour résoudre le nom de domaine complet défini dans un objet réseau. Un nom de domaine complet est résolu périodiquement, soit à l'expiration du délai d'interrogation, soit à l'expiration de la durée de vie de l'entrée IP résolue, selon l'événement qui se produit en premier.

Étape 7 Activer les recherches DNS sur toutes les interfaces ou sur des interfaces spécifiques. Ces choix affectent également les tables de routage utilisées.

Notez que l’activation des recherches DNS sur une interface n’est pas la même chose que la spécification de l’interface source pour les recherches. Le défense contre les menaces utilise toujours une recherche de routage pour déterminer l’interface source.

- Aucune interface sélectionnée : active les recherches DNS sur toutes les interfaces, y compris les interfaces de gestion et les interfaces de gestion uniquement. Le défense contre les menaces vérifie la table de routage des données et, si aucune route n'est trouvée, il revient à la table de routage de gestion uniquement.
- Interfaces spécifiques sélectionnées mais pas l'option **Activer la recherche DNS via l'interface de diagnostic ou de gestion**, et également l'option : Active les recherches DNS sur les interfaces spécifiées. Le défense contre les menaces contrôle la table de routage des données uniquement.
- Interfaces spécifiques sélectionnées plus l'option **Activer la recherche DNS via l'interface de diagnostic ou de gestion**, et également l'option : Active les recherches DNS sur les interfaces spécifiées et l'interface du Diagnostic. Le défense contre les menaces vérifie la table de routage des données et, si aucune route n'est trouvée, revient à la table de routage de gestion uniquement.
- Seule l'option **Activer la recherche DNS via l'interface de diagnostic/** active également la recherche DNS sur Diagnostic. Le défense contre les menaces ne vérifie que la table de routage de gestion.Veillez à configurer une adresse IP pour l'interface de diagnostic sur la page **Périphériques**> **Gestion des périphériques** > **Modifier le périphérique** > **Interfaces**.

Étape 8 Pour configurer les serveurs DNS de confiance, cliquez sur l'onglet **Serveurs DNS de confiance**.

Étape 9 Par défaut, les serveurs DNS existants qui sont configurés dans le groupe (pool) DHCP, le relais DHCP, le client DHCP ou le groupe de serveurs DNS sont inclus en tant que serveurs DNS de confiance. Si vous souhaitez exclure l'un d'entre eux, décochez les cases correspondantes.

Étape 10 Pour ajouter des serveurs DNS de confiance, sous **Spécifier les serveurs DNS** cliquez sur **Modifier**.

Étape 11 Dans la boîte de dialogue **Sélectionner les serveurs DNS**, choisissez un objet hôte comme serveur DNS de confiance ou indiquez directement l'adresse IP de ce dernier :

a) Pour sélectionner des objets hôtes existants, sous **Objets hôtes disponibles**, sélectionnez l'objet hôte requis et cliquez sur **Ajouter** pour l'inclure dans **Serveurs DNS sélectionnés**. Pour plus d'informations sur l'ajout des objets hôtes, voir Création d'objets réseau.

b) Pour fournir directement l'adresse IP (IPv4 ou IPv6) du serveur DNS de confiance, entrez l'adresse dans le champ de texte indiqué et cliquez sur **Ajouter** pour l'inclure dans **Serveurs DNS sélectionnés**.

c) Cliquez sur **Save** (enregistrer). Les serveurs DNS ajoutés sont affichés dans la page **Serveurs DNS de confiance**.

Remarque Vous pouvez configurer un maximum de 12 serveurs DNS par politique.

Étape 12 (Facultatif) Pour rechercher un serveur DNS qui a été ajouté, en utilisant le nom d'hôte ou l'adresse IP, utilisez le champ de recherche sous **Spécifier les serveurs DNS**.

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

Prochaine étape

Pour utiliser les objets de type nom de domaine complet (FQDN) pour les règles de contrôle d'accès, créez un objet de type réseau FQDN qui peut ensuite être assigné à une règle de contrôle d'accès. Pour plus d'informations sur les instructions, consultez Création d'objets réseau.

Authentification extérieure

Remarque Vous devez disposer de privilèges d'administrateur pour effectuer cette tâche.

Lorsque vous activez l'authentification externe pour les utilisateurs de gestion, défense contre les menaces vérifie les informations d'authentification de l'utilisateur avec un serveur LDAP ou RADIUS, comme le précise un objet d'authentification externe.

Partage d'objets d'authentification externes

Les objets d'authentification externes peuvent être utilisés par les périphériques centre de gestion et défense contre les menaces . Vous pouvez partager le même objet entre centre de gestion et les appareils ou créer des objets distincts. Notez que défense contre les menaces prend en charge la définition des utilisateurs sur le serveur RADIUS, tandis que centre de gestion exige que vous prédéfinissiez la liste d'utilisateurs dans l'objet d'authentification extérieure. Vous pouvez choisir d'utiliser la méthode de liste prédéfinie pour défense contre les menaces , mais si vous souhaitez définir des utilisateurs sur le serveur RADIUS, vous devez créer des objets distincts pour défense contre les menaces et centre de gestion.

Remarque La plage de délai d'attente est différente pour le défense contre les menaces et le centre de gestion, donc si vous partagez un objet, assurez-vous de ne pas dépasser la plage de délai d'attente plus petite du défense contre les menaces (1-30 secondes pour LDAP, et 1-300 secondes pour RADIUS). Si vous définissez le délai d'attente à une valeur supérieure, la configuration de l'authentification externe défense contre les menaces ne fonctionnera pas.

Affectation d'objets d'authentification extérieure aux périphériques

Pour centre de gestion, activez les objets d'authentification extérieure directement sur **System (système)** > **Users (utilisateurs)** > **External Authentication (authentification extérieure)**; ce paramètre affecte uniquement l'utilisation de centre de gestion et n'a pas besoin d'être activé pour l'utilisation de périphériques gérés. Pour les appareils défense contre les menaces , vous devez activer l'objet d'authentification externe dans les paramètres de la plateforme que vous déployez sur les appareils, et vous ne pouvez activer qu'un seul objet d'authentification externe par politique. Un objet LDAP avec authentification CAC activée ne peut pas être utilisé pour l'accès au niveau de l'interface de ligne de commande.

Défense contre les menaces Champs pris en charge

Seul un sous-ensemble de champs de l'objet d'authentification extérieure est utilisé pour l'accès SSH défense contre les menaces . Si vous remplissez des champs supplémentaires, ils seront ignorés. Si vous utilisez également cet objet pour le centre de gestion, ces champs seront utilisés. Cette procédure ne couvre que les champs pris en charge pour le défense contre les menaces . Pour les autres champs, consultez *Configure External Authentication (configurer l'authentification externe) pour le Centre de gestion* dans le Guide d'administration Cisco Secure Firewall Management Center.

Noms d'utilisateur

Les noms d'utilisateur doivent être des noms d'utilisateur valides pour Linux et être en minuscules uniquement, en utilisant des caractères alphanumériques plus un point (.) ou un tiret (-). Les autres caractères spéciaux comme le signe @ et la barre oblique (/) ne sont pas pris en charge. Vous ne pouvez pas ajouter l'utilisateur **admin** pour l'authentification extérieure. Vous ne pouvez ajouter que des utilisateurs externes (dans le cadre

de l'objet d'authentification extérieure) dans centre de gestion; vous ne pouvez pas les ajouter au niveau de l'interface de ligne de commande (CLI). Notez que les utilisateurs internes ne peuvent être ajoutés qu'au niveau de la CLI, et non dans centre de gestion.

Si vous avez précédemment configuré le même nom d'utilisateur pour un utilisateur interne à l'aide de la commande **configure user add**, défense contre les menaces vérifie d'abord le mot de passe par rapport à l'utilisateur interne, et si cela échoue, il vérifie le serveur AAA. Notez que vous ne pouvez plus ajouter un utilisateur interne avec le même nom qu'un utilisateur externe; seuls les utilisateurs internes préexistants sont pris en charge. Pour les utilisateurs définis sur le serveur RADIUS, assurez-vous que le niveau de privilège est identique à celui des utilisateurs internes; sinon, vous ne pouvez pas vous connecter avec le mot de passe de l'utilisateur externe.

Niveau de privilège

Les utilisateurs LDAP ont toujours des privilèges de configuration. Les utilisateurs RADIUS peuvent être définis comme utilisateurs de configuration ou de base.

Avant de commencer

- L'accès SSH est activé par défaut sur l'interface de gestion. Pour activer l'accès SSH sur les interfaces de données, consultez Secure Shell, à la page 18. SSH n'est pas pris en charge par l'interface de diagnostic.
- Informez les utilisateurs RADIUS du comportement suivant pour définir correctement les attentes :
  - La première fois qu'un utilisateur externe se connecte, défense contre les menaces crée les structures requises, mais ne peut pas créer simultanément la session utilisateur. L'utilisateur doit simplement s'authentifier à nouveau pour démarrer la session. L'utilisateur verra un message semblable au suivant : « New external username identified. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)
  - De même, si l'autorisation de type de service de l'utilisateur a été modifiée depuis la dernière connexion, l'utilisateur devra s'authentifier de nouveau. L'utilisateur verra un message semblable au suivant : « Your authorization privilege has changed. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **External Authentication** (authentification extérieure).

Étape 3 Cliquez sur le lien **Manage External Authentication Server** (gérer le serveur d'authentification externe).

Vous pouvez également ouvrir l'écran d'authentification extérieure (External Authentication) en cliquant sur **System** > **Users** > **External Authentication.**

Étape 4 Configurez un objet d'authentification LDAP.

a) Cliquez sur **Add External Authentication Object** (ajouter un objet d'authentification externe).
b) Définir la méthode d'authentification (**Authentication Method**) sur **LDAP**
c) Saisissez un nom (**Name**) et une **Description** facultative.
d) Dans la liste déroulante, choisissez un type de serveur (**Server Type**).
e) Pour le serveur principal (**Primary Server**), entrez un nom d'hôte ou une adresse IP (**Host Name/IP Address**).

Remarque Si vous utilisez un certificat pour vous connecter via TLS ou SSL, le nom d'hôte du certificat doit correspondre au nom d'hôte utilisé dans ce champ. En outre, les adresses IPv6 ne sont pas prises en charge pour les connexions chiffrées.

f) (Facultatif) Modifier le **port** par défaut.

g) (Facultatif) Entrez les paramètres du serveur de sauvegarde **Backup Sever**.

h) Entrez les paramètres spécifiques au protocole LDAP (**LDAP-Specific Parameters**).

- **Base DN** : Saisissez le nom distinctif de base de l'annuaire LDAP auquel vous souhaitez accéder. Par exemple, pour authentifier des noms dans l'organisation de sécurité de l'entreprise de l'exemple, entrez `ou=security,dc=example,dc=com`. Vous pouvez également cliquer sur **Fetch DNs** et choisir le nom distinctif de base approprié dans la liste déroulante.
- (Facultatif) **Base Filter** (filtre de base) : Par exemple, si les objets utilisateur dans une arborescence de répertoires ont un attribut `physicalDeliveryOfficeName` et que les utilisateurs du bureau de New York ont une valeur d'attribut `NewYork` pour cet attribut, pour récupérer uniquement les utilisateurs du bureau de New York, entrez `(physicalDeliveryOfficeName=NewYork)`.
- **User Name** (nom d'utilisateur) : Saisissez un nom distinctif pour un utilisateur dont les informations d'identification sont suffisantes pour parcourir le serveur LDAP. Par exemple, si vous vous connectez à un serveur OpenLDAP où les objets utilisateur ont un attribut `uid` et que l'objet de l'administrateur de la division de sécurité de notre exemple d'entreprise a une valeur `uid` de `NetworkAdmin`, vous pouvez entrer `uid=NetworkAdmin,ou=security,dc=example,dc=com`.
- **Password** (mot de passe) et **Confirm Password** (confirmer le mot de passe) : Saisissez et confirmez le mot de passe de l'utilisateur.
- (Facultatif) **Show Advanced Options** (afficher les options avancées) : Configurez les options avancées ci-après.
  - **Encryption** (chiffrement) : Cliquez sur **None** (aucune), **TLS** ou **SSL**.

    Remarque Si vous modifiez la méthode de chiffrement après avoir précisé un port, vous réinitialiserez le port à sa valeur par défaut pour cette méthode. Pour **None** (aucune) ou **TLS**, le port est réinitialisé à la valeur par défaut de 389. Si vous choisissez le chiffrement SSL, le port sera réinitialisé à 636.

  - **SSL Certificate Upload Path** (chemin de téléchargement du certificat SSL) : Pour le chiffrement SSL ou TLS, vous devez choisir un certificat en cliquant sur **Choose File** (choisir un fichier).
  - (Non utilisé) **User Name Template** (modèle de nom d'utilisateur) : Non utilisé par défense contre les menaces .
  - **Timeout** (délai d'expiration) : Saisissez le nombre de secondes (entre 1 et 30) avant le basculement vers la connexion de secours. La valeur par défaut est 30.

    Remarque La plage de délai d'attente est différente pour le défense contre les menaces et le centre de gestion, donc si vous partagez un objet, assurez-vous de ne pas dépasser la plage de délai d'attente plus petite du défense contre les menaces (1-30 secondes). Si vous définissez le délai d'attente à une valeur supérieure, la configuration de l'authentification externe défense contre les menaces ne fonctionnera pas.

i) (Facultatif) Définissez **l'attribut d'accès à l'interface de ligne de commande** si vous souhaitez utiliser un attribut d'accès à l'interpréteur autre que le type distingué de l'utilisateur. Par exemple, sur un serveur Microsoft Active Directory, utilisez l'attribut d'accès shell `sAMAccountName` pour récupérer les utilisateurs ayant un accès shell en tapant `sAMAccountName` dans le champ **CLI Access Attribute (attribut d'accès de l'interface de ligne de commande)**.

j) Définissez le **filtre d'accès à l'interface de ligne de commande**.

À cette fin, choisissez l'une des méthodes suivantes :

- Pour utiliser le filtre que vous avez spécifié lors de la configuration des paramètres d'authentification, choisissez **Same as Base Filter** (identique au filtre de base).
- Pour récupérer des entrées d'utilisateur administratif en fonction de la valeur de l'attribut, entrez le nom de l'attribut, un opérateur de comparaison et la valeur de l'attribut à utiliser comme filtre, entre parenthèses. Par exemple, si tous les administrateurs réseau ont un attribut `manager` qui a une valeur d'attribut `shell`, vous pouvez définir un filtre de base de `(manager=shell)`.

Les noms sur le serveur LDAP doivent être des noms d'utilisateur valides pour Linux. Autrement dit, ils doivent respecter les critères suivants :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
- Tous les caractères doivent être en minuscules.
- Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

k) Cliquez sur **Save** (enregistrer).

Étape 5 Pour LDAP, si vous ajoutez ou supprimez ultérieurement des utilisateurs sur le serveur LDAP, vous devez actualiser la liste des utilisateurs et redéployer les paramètres de la plateforme.

a) Choisissez l'authentification extérieure des utilisateurs du système (**System** > **Users** > **External Authentication**).

b) Cliquez sur **Actualisation** ( ) à côté du serveur LDAP.

Si la liste des utilisateurs a changé, vous verrez un message vous invitant à déployer les modifications de configuration pour votre appareil. Les paramètres de la plateforme Firepower Theat Defense comprendront aussi le message "Out-of-Date on *x* targeted devices" indiquant sa désuétude sur certains appareils donnés.

c) Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Étape 6 Configurez un objet d'authentification RADIUS.

a) Définissez les utilisateurs sur le serveur RADIUS à l'aide de l'attribut Service-Type (type de service).

Les valeurs suivantes sont prises en charge pour l'attribut Service-Type :

- Administrateur (6) : Fournit une autorisation d'accès de configuration au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser toutes les commandes de l'interface de ligne de commande.
- NAS Prompt (7) ou tout autre niveau que 6 : Fournit une autorisation d'accès de base au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser des commandes de lecture seule, comme les commandes **show**, à des fins de surveillance et de dépannage.

Les noms doivent être des noms d'utilisateur valides pour Linux :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
- Tous les caractères doivent être en minuscules.
- Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

Vous pouvez aussi prédéfinir les utilisateurs dans l'objet d'authentification extérieure (voir l'étape 6.j, à la page 13). Pour utiliser le même serveur RADIUS pour le défense contre les menaces et centre de gestion tout en utilisant la méthode d'attribut Service-Type pour le défense contre les menaces , créez deux objets d'authentification externe qui déterminent le même serveur RADIUS : un objet inclut les utilisateurs prédéfinis du **CLI Access Filter (filtre d'accès à l'interface de ligne de commande)** (à utiliser avec le centre de gestion), et l'autre objet laisse le **CLI Access Filter (filtre d'accès à l'interface de ligne de commande)** vide (à utiliser avec les défense contre les menaces).

b) Dans centre de gestion, cliquez sur **Add External Authentication Object** (ajouter un objet d'authentification externe).
c) Définissez la méthode d'authentification (**Authentication Method**) sur **RADIUS**.
d) Saisissez un nom (**Name**) et une **Description** facultative.
e) Pour le serveur principal (**Primary Server**), entrez un nom d'hôte ou une adresse IP (**Host Name/IP Address**).

Remarque Si vous utilisez un certificat pour vous connecter via TLS ou SSL, le nom d'hôte du certificat doit correspondre au nom d'hôte utilisé dans ce champ. En outre, les adresses IPv6 ne sont pas prises en charge pour les connexions chiffrées.

f) (Facultatif) Modifier le **port** par défaut.
g) Entrez une clé secrète RADIUS (**RADIUS Secret Key**).
h) (Facultatif) Entrez les paramètres du serveur de sauvegarde **Backup Sever**.
i) Entrez les paramètres propres à RADIUS (**RADIUS Secret Key**).

- **Timeout** (délai d'expiration) : Saisissez le nombre de secondes avant le basculement vers la connexion de secours. La valeur par défaut est 30.
- **Retries** (nouvelles tentatives) : Saisissez le nombre de tentatives de connexion au serveur principal avant de passer à la connexion de secours. La valeur par défaut est de 3.

j) (Facultatif) Au lieu d'utiliser les utilisateurs définis par RADIUS, **CLI Access Filter (Filtre d'accès à l'interface de ligne de commande)**, saisissez une liste de noms d'utilisateur séparés par des virgules dans le champ **Administrator CLI Access User List (Liste des utilisateurs de l'accès à l'interface de commande administrateur)**. Par exemple, entrez `jchrichton, aerynsun, rygel`.

Vous pouvez utiliser la méthode du **CLI Access Filter (filtre d'accès à l'interface de ligne de commande)** pour défense contre les menaces pour que vous puissiez utiliser le même objet d'authentification externe avec défense contre les menaces et d'autres types de plateforme. Notez que si vous voulez utiliser des utilisateurs définis par RADIUS, vous devez laisser le filtre **CLI Access Filter (accès de l'interface de ligne de commande vide)** vide.

Assurez-vous que ces noms d'utilisateurs correspondent à ceux du serveur RADIUS. Les noms doivent être des noms d'utilisateur valides pour Linux :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
- Tous les caractères doivent être en minuscules.
- Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

Remarque Si vous souhaitez définir uniquement des utilisateurs sur le serveur RADIUS, vous devez laisser cette section vide.

k) Cliquez sur **Save** (enregistrer).

Étape 7 Revenir à la page **Devices (périphériques)** > > **Platform Settings (paramètres de la plateforme)** > **External Authentication (authentification extérieure)**.

Étape 8 Cliquez sur **Actualisation** ( ) pour afficher les objets récemment ajoutés.

Pour LDAP, lorsque vous spécifiez le cryptage SSL ou TLS, vous devez télécharger un certificat pour la connexion; sinon, le serveur ne sera pas répertorié dans cette fenêtre.

Étape 9 Cliquez sur **Curseur activé** ( ) en regard de l'objet d'authentification extérieure que vous souhaitez utiliser. Vous ne pouvez activer qu'un seul objet.

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

Étape 11 Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Paramètres de fragmentation

Par défaut, le périphérique défense contre les menaces autorise jusqu'à 24 fragments par paquet IP et jusqu'à 200 fragments en attente d'être réassemblés. Vous devrez peut-être laisser les fragments entrer dans votre réseau si vous avez une application qui fragmente régulièrement les paquets, comme NFS sur UDP. Toutefois, si vous n'avez pas d'application qui fragmente le trafic, nous vous recommandons de ne pas autoriser les fragments en réglant l'option **Chaîne** à 1. Les paquets fragmentés sont souvent utilisés comme attaques par déni de service (DoS).

Remarque Ces paramètres établissent les valeurs par défaut des périphériques auxquels cette politique est associée. Vous pouvez remplacer ces paramètres pour des interfaces spécifiques sur un périphérique en sélectionnant **Override Default Fragment Setting** (Remplacer les paramètres de fragmentation par défaut) dans la configuration de l'interface. Lorsque vous modifiez une interface, vous pouvez trouver l'option dans **la configuration de sécurité** > **avancée**. Sélectionnez **Périphériques** > **Gestion des périphériques**, modifiez un périphérique défense contre les menaces , puis sélectionnez **Interfaces** pour modifier les propriétés de l'interface.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 PSélectionnez **Paramètres de fragmentation**

Étape 3 Configurez les options suivantes : Cliquez sur **Reset to Defaults** (réinitialisation aux valeurs par défaut) si vous souhaitez utiliser les paramètres par défaut.

- **Size (Block)** (Taille en blocs) : le nombre maximal de fragments de paquet de toutes les connexions qui peuvent être en attente de réassemblage. Par défaut, c'est 200 fragments.
- **Chaîn (fragment)** (Chaine (fragment) : le nombre maximal de paquets dans lesquels un paquet IP complet peut être fragmenté. La valeur par défaut est 24 paquets. Définissez cette option sur 1 pour interdire les fragments.
- **Timeout (sec)** (délai d'expiration, en secondes) : le nombre maximal de secondes à attendre pour l'arrivée d'un paquet fragmenté. La valeur par défaut est de 5 secondes. Si tous les fragments ne sont pas reçus dans ce délai, tous les fragments sont rejetés.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

HTTP

Vous pouvez activer le serveur HTTPS pour fournir un mécanisme de vérification de l'intégrité pour un équilibreur de charge dans le nuage, par exemple, pour défense contre les menaces virtuelles sur AWS à l'aide d'un équilibreur de charge d'application.

D'autres utilisations de HTTP sur défense contre les menaces ne sont pas prises en charge ; par exemple, le défense contre les menaces n'a pas d'interface web pour la configuration dans ce mode de gestion.

Cette configuration s'applique uniquement aux interfaces de données, y compris celles que vous avez configurées uniquement pour la gestion. Elle ne s'applique pas à l'interface de gestion dédiée. L'interface de gestion physique est partagée entre l'interface logique de diagnostic et l'interface logique de gestion; cette configuration s'applique uniquement à l'interface logique de diagnostic, s'il y a lieu, ou à d'autres interfaces de données. L'interface logique de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. Elle a une adresse IP distincte et emprunte une voie de routage statique.

Pour utiliser le protocole HTTPS, vous n'avez pas besoin d'une règle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès HTTPS conformément à cette section.

Vous ne pouvez utiliser HTTPS que vers une interface accessible; si votre hôte HTTPS est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe.

Avant de commencer

- Vous ne pouvez pas configurer HTTPS et Module AnyConnect VPN de Cisco Secure Client sur la même interface pour le même port TCP. Par exemple, si vous configurez le VPN SSL d'accès distant sur l'interface externe, vous ne pouvez pas ouvrir aussi l'interface externe pour les connexions HTTPS sur

le port 443. Si vous devez configurer les deux fonctionnalités sur la même interface, utilisez des ports différents. Par exemple, ouvrez HTTPS sur le port 4443.

- Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions HTTPS avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser tout (**any**) groupe d'objets réseau fourni par le système. Au lieu de cela, utilisez **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **HTTP**.

Étape 3 Cochez la case **Enable HTTP Server** (activer le serveur HTTP) pour activer le serveur HTTP.

Étape 4 (Facultatif) Modifiez le port HTTP. La valeur par défaut est 443.

Étape 5 Déterminez les interfaces et les adresses IP qui permettent les connexions HTTP.

Utilisez ce tableau pour limiter les interfaces qui accepteront les connexions HTTPS et définir les adresses IP des clients autorisés à établir ces connexions. Vous pouvez utiliser des adresses réseau plutôt que diverses adresses IP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.

b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet (ou groupe) de réseau qui identifie les hôtes ou les réseaux que vous autorisez à établir des connexions HTTP. Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) -Zones/interfaces disponibles) : ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions HTTP. 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 **zones de sécurité sélectionnées**/ et l'ajouter en cliquant sur **Add** (Ajouter). Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

ICMP

Par défaut, vous pouvez envoyer des paquets ICMP vers n'importe quelle interface IPv4 ou IPv6, avec les exceptions suivantes

- Le défense contre les menaces ne répond pas aux demandes ECHO ICMP dirigées vers une adresse de diffusion.
- Le défense contre les menaces répond uniquement au trafic ICMP envoyé à l'interface par laquelle le trafic entre; vous ne pouvez pas envoyer de trafic ICMP par une interface vers une interface distante.

Pour protéger le périphérique contre les attaques, vous pouvez utiliser des règles ICMP pour limiter l'accès ICMP aux interfaces à des hôtes, des réseaux ou des types ICMP particuliers. Les règles ICMP fonctionnent comme des règles d'accès, où les règles sont classées, et la première règle qui correspond à un paquet définit l'action.

Si vous configurez une règle ICMP pour une interface, une règle ICMP de refus implicite est ajoutée à la fin de la liste de règles ICMP, modifiant le comportement par défaut. Par conséquent, si vous souhaitez simplement refuser certains types de messages, vous devez inclure une règle autoriser tout à la fin de la liste de règles ICMP pour autoriser les autres types de messages.

Nous vous recommandons de toujours accorder l'autorisation pour le type de message ICMP « unreachable » (inaccessible) (type 3). Le refus des messages ICMP inaccessibles désactive la découverte de la MTU du chemin ICMP, ce qui peut interrompre le trafic IPsec et PPTP. De plus, les paquets ICMP dans IPv6 sont utilisés dans le processus de découverte de voisin IPv6.

Avant de commencer

Vérifiez que les objets nécessaires dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets. Vous avez besoin d'objets ou de groupes de réseau qui définissent les hôtes ou les réseaux souhaités, et d'objets de port qui définissent les types de messages ICMP que vous souhaitez contrôler.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **ICMP**.

Étape 3 Configurez les règles ICMP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.

b) Configurez les propriétés des règles :

- **Action** : autoriser (permettre) ou refuser (abandonner) le trafic correspondant.
- **ICMP Service** (Service ICMP) : l'objet de port qui identifie le type de message ICMP.
- **Network** (réseau) : objet ou groupe réseau qui identifie les hôtes ou les réseaux dont vous contrôlez l'accès.
- **Security Zones** (Zones de sécurité) (Interfaces de zones disponibles) : ajoutez les zones qui contiennent les interfaces que vous protégez. 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 **zones de sécurité sélectionnées**/ et l'ajouter en cliquant sur **Add** (Ajouter). Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 (Facultatif) Définir les limites de débit pour les messages ICMPv4 Unreachable (ICMPv4 Injoignable).

- **Limite du débit** : : définit la limite de débit des messages unreachable, entre 1 et 100 messages par seconde. La valeur par défaut est de 1 message par seconde.
- **Taille de la rafale** : définit le débit en rafale, entre 1 et 10. Le système envoie ce nombre de réponses, mais les réponses suivantes ne sont pas envoyées tant que la limite de débit n'est pas atteinte.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Secure Shell

Si vous avez activé l'accès sur centre de gestion à une interface de données, telle qu'externe, vous devez activer SSH sur cette interface en suivant la procédure suivante. Cette section décrit comment activer les connexions SSH à une ou plusieurs interfaces de *données* sur le défense contre les menaces . SSH n'est pas pris en charge par l'interface de diagnostic logique.

Remarque SSH est activé par défaut sur l'interface de gestion; cependant, cet écran n'affecte pas l'accès SSH de gestion.

L'interface de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. SSH pour les interfaces de données partage la liste d'utilisateurs interne et externe avec SSH pour l'interface de gestion. Les autres paramètres sont configurés séparément : pour les interfaces de données, activez SSH et accédez aux listes à l'aide de cet écran; le trafic SSH pour les interfaces de données utilise la configuration de routage normale, et non les voies de routage statiques configurées lors de l'installation ou au niveau de la CLI.

Pour l'interface de gestion, afin de configurer une liste d'accès SSH, consultez la commande **configure ssh-access-list** dans la Référence des commandes de défense contre les menaces de Cisco Secure Firewall. Pour configurer une voie de routage statique, voir la commande **configure network static-routes**. Par défaut, vous configurez la voie de routage par défaut via l'interface de gestion, lors de la configuration initiale.

Pour utiliser le protocole SSH, vous n'avez pas non plus besoin d'une règle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.

Vous ne pouvez utiliser SSH que vers une interface accessible; , si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe.

SSH prend en charge les chiffrements et les échanges de clés suivants :

- Chiffrement : aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr

- Intégrité : hmac-sha2-256
- Échange de clés : dh-group14-sha256

Remarque Après trois tentatives infructueuses consécutives de connexion à la CLI à l'aide de SSH, l'appareil met fin à la connexion SSH.

Avant de commencer

- Vous pouvez configurer les utilisateurs SSH internes au niveau de l'interface de ligne de commande (CLI) à l'aide de la commande **configure user add**; voir Ajouter un utilisateur interne au niveau de l'interface de ligne de commande. Par défaut, il existe un utilisateur administrateur (**admin**) pour lequel vous avez configuré le mot de passe lors de la configuration initiale. Vous pouvez également configurer des utilisateurs externes sur LDAP ou RADIUS en configurant l'authentification externe (**External Authentication**) dans les paramètres de la plateforme. Voir Authentification extérieure, à la page 9.
- Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions SSH avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser tout (**any**) groupe d'objets réseau fourni par le système. Au lieu de cela, utilisez **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Secure Shell** (Shell sécurisé) (Accès SSH)

Étape 3 Déterminez les interfaces et les adresses IP qui permettent les connexions SSH.

Utilisez ce tableau pour limiter les interfaces qui accepteront les connexions SSH et définir les adresses IP des clients autorisés à établir ces connexions. Vous pouvez utiliser des adresses réseau plutôt que diverses adresses IP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.
b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet (ou groupe) de réseau qui établit les hôtes ou les réseaux que vous autorisez à établir des connexions SSH. Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) -Zones/interfaces disponibles) : Ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. 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 **zones de**

sécurité sélectionnées/ et l'ajouter en cliquant sur **Add** (Ajouter). Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

SMTP Server

Vous devez identifier un serveur SMTP si vous configurez les alertes par courriel dans les paramètres Syslog. L'adresse courriel source que vous configurez pour Syslog doit être un compte valide sur les serveurs SMTP.

Avant de commencer

Assurez-vous que les objets réseau qui définissent l'adresse d'hôte des serveurs SMTP principal et secondaire existent. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets. Vous pouvez également créer les objets lors de la modification de la politique.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **Serveur SMTP**.

Étape 3 Sélectionnez les objets réseau qui déterminent l'**adresse IP du serveur principal** et, le cas échéant, l'**adresse IP du serveur secondaire**.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

SNMP

Le protocole SNMP (Simple Network Management Protocol) définit une méthode standard permettant aux stations de gestion de réseau fonctionnant sur des ordinateurs ou des postes de travail de surveiller l'intégrité et l'état de nombreux types de périphériques, notamment les commutateurs, les routeurs et les périphériques de sécurité. Vous pouvez utiliser la page SNMP pour configurer un périphérique de pare-feu pour la surveillance par les stations de gestion SNMP.

Le protocole SNMP (Simple Network Management Protocol) permet de surveiller les périphériques du réseau à partir d'un emplacement central. les périphériques de sécurité Cisco prennent en charge la surveillance du

réseau à l'aide des versions 1, 2c et 3 de SNMP, ainsi que les déroutements et l'accès en lecture SNMP; L'accès en écriture SNMP n'est pas pris en charge.

SNMPv3 prend en charge les utilisateurs en lecture seule et le chiffrement avec DES (obsolète), 3DES, AES256, AES192 et AES128.

Remarque L'option DES est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant le chiffrement DES qui ont été créés à l'aide d'une version antérieure à 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les défense contre les menaces exécutant les versions 6.6 et précédentes. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver le chiffrement DES, ou créer de nouveaux utilisateurs avec le chiffrement DES. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise le chiffrement DES sur ces défense contre les menaces échouera.

Remarque La configuration SNMP prend uniquement en charge les interfaces de routage et de dépistage.

Remarque Pour créer une alerte vers un serveur SNMP externe, accédez aux **alertes** > **d'action** > **politiques**

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **SNMP**.

Étape 3 Activez SNMP et configurez les options de base.

- **Enable SNMP Servers**(activer les serveurs SNMP) : s'il faut fournir des informations SNMP aux hôtes SNMP configurés. Vous pouvez désélectionner cette option pour désactiver la surveillance SNMP tout en conservant les informations de configuration.
- **Read Community String**, **Confirm** (Lire la chaîne de la communauté > Confirmer) : saisissez le mot de passe utilisé par une station de gestion SNMP lors de l'envoi de requêtes au périphérique défense contre les menaces . L'identifiant de communauté SNMP est un secret partagé entre les stations de gestion SNMP et les nœuds de réseau gérés. Le périphérique de sécurité utilise le mot de passe pour déterminer si la requête SNMP entrante est valide. Le mot de passe est une chaîne alphanumérique sensible à la casse comptant jusqu'à 32 caractères; les espaces et les caractères spéciaux ne sont pas autorisés.
- **System Administrator Name**(nom de l'administrateur système) : Saisissez le nom de l'administrateur du périphérique ou d'une autre personne-ressource. Cette chaîne est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.
- **Location** (Emplacement) : saisissez l'emplacement de ce périphérique de sécurité (par exemple, bâtiment 42, secteur 54). Cette chaîne est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.
- **Port** : saisissez le port UDP sur lequel les demandes entrantes seront acceptées. La valeur par défaut est 161.

Étape 4 (SNMPv3 uniquement.) Ajouter des utilisateurs SNMPv3, à la page 28.

Étape 5 Ajouter des hôtes SNMP, à la page 30.

Étape 6 Configurer les déroutements SNMP, à la page 32.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

À propos de SNMP

SNMP est un protocole de couche d'application qui facilite l'échange d'informations de gestion entre les périphériques réseau. Il fait partie de la suite de protocoles TCP/IP. Défense contre les menaces prend en charge la surveillance du réseau à l'aide des versions 1, 2c et 3 de SNMP et prend en charge l'utilisation des trois versions simultanément. L'agent SNMP qui s'exécute sur l'interface défense contre les menaces vous permet de surveiller les périphériques réseau à l'aide de systèmes de gestion par réseau (Network Management Systems ou NMS), comme HP OpenView. Défense contre les menaces prend en charge l'accès SNMP en lecture seule par l'émission d'une requête GET. L'accès en écriture SNMP n'est pas autorisé, vous ne pouvez donc pas effectuer de modifications avec SNMP. En outre, la requête SNMP SET n'est pas prise en charge.

Vous pouvez configurer la défense contre les menaces pour envoyer des déroutements, qui sont des messages non sollicités du périphérique géré vers le poste de gestion pour certains événements (notifications d'événement) à un système de gestion de réseau, ou vous pouvez utiliser le système de gestion de réseau pour parcourir les bases d'information de gestion (MIB) sur le périphériques de sécurité. Les MIB sont un ensemble de définitions, et les défense contre les menaces gèrent une base de données de valeurs pour chaque définition. Parcourir une MIB signifie émettre une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du système NMS pour déterminer les valeurs.

Un agent SNMP informe les stations de gestion désignées si des événements prédéfinis nécessitent une notification, par exemple, lorsqu'une liaison du réseau monte ou tombe en panne. La notification qu'il envoie comprend un OID SNMP, qui s'identifie aux stations de gestion. L'agent répond également lorsqu'une station de gestion demande des renseignements.

Terminologie SNMP

Le tableau suivant répertorie les termes couramment utilisés avec SNMP.

Tableau 1 : Terminologie SNMP

Terme	Description
Agent	Le serveur SNMP exécuté sur Cisco Secure Firewall Threat Defense. L'agent SNMP présente les caractéristiques suivantes : • Répond aux demandes d'informations et d'actions de le poste de gestion de réseau. • Contrôle l'accès à sa base d'information de gestion, l'ensemble d'objets que le gestionnaire SNMP peut afficher ou modifier. • N'autorise pas les opérations SET.

Terme	Description
Navigation	Surveille l'intégrité d'un périphérique à partir de le poste de gestion de réseau en interrogeant les informations requises de l'agent SNMP sur le périphérique. Cette activité peut comprendre l'émission d'une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir de le poste de gestion de réseau afin de déterminer les valeurs.
Bases d'informations de gestion (MIB)	Structures de données normalisées pour la collecte d'informations sur les paquets, les connexions, les tampons, les basculements, etc. Les MIB sont définies par le produit, les protocoles et les normes matérielles utilisés par la plupart des périphériques réseau. Les stations de gestion de réseau SNMP peuvent parcourir les MIB et demander l'envoi de données ou d'événements précis au fur et à mesure qu'ils se produisent.
Postes de gestion de réseau (NSM, Network Management Station)	Les ordinateurs ou postes de travail configurés pour surveiller les événements SNMP et gérer les périphériques.
Identifiant d'objet (OID)	Le système qui identifie un appareil auprès de son système de gestion système et indique aux utilisateurs la source des renseignements surveillés et affichés.
Trap	Événements prédéfinis qui génèrent un message de l'agent SNMP au système NMS. Les événements comprennent des conditions d'alarme telles qu'un démarrage, un retrait, un démarrage à froid, un démarrage à chaud, une authentification ou des messages syslog.

MIB et déroutements

Les MIB sont standard ou spécifiques à l'entreprise. Les MIB standard sont créées par l'IETF et documentées dans diverses RFC. Un déroutement signale des événements importants se produisant sur un périphérique réseau, le plus souvent des erreurs ou des défaillances. Les déroutements SNMP sont définies dans les MIB standard ou spécifiques à l'entreprise. Les déroutements standard sont créés par l'IETF et documentés dans diverses normes RFC. Les déroutements de SNMP sont compilés dans le logiciel ASA.

Si nécessaire, vous pouvez également télécharger des RFC, des MIB standard et des déroutements standard à partir des emplacements suivants :

http://www.ietf.org/

Parcourez le navigateur d'objets SNMP pour rechercher les MIB, les déroutements et les OID de Cisco à partir de l'emplacement suivant :

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Téléchargez également les OID de Cisco par FTP à partir de l'emplacement suivant :

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

Tableaux et objets pris en charge dans les MIB

Les sections suivantes répertorient les tableaux et les objets pris en charge pour les MIB précisées.

Interrogation de VPN d'accès à distance

Tableau 2 : CISCO-REMOTE-ACCESS-MONITOR-MIB

Compteur	OID	Description
Sessions actives	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	Le nombre de sessions actuellement actives.
Utilisateurs	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	Le nombre d'utilisateurs qui ont des sessions actives.
Nombre le plus élevé de sessions	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	Le nombre de sessions d'accès à distance de pointe depuis la mise en service du système.

Interrogation du tunnel VPN site à site

Tableau 3 : CISCO-REMOTE-ACCESS-MONITOR-MIB

Compteur	OID	Description
Sessions LAN à LAN	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	Le nombre de sessions LAN à LAN actuellement actives.
Nombre le plus élevé de sessions LAN à LAN	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	Le nombre de pics de sessions simultanées de réseau à réseau local depuis que le système est opérationnel.

Interrogation de la connexion

Tableau 4 : CISCO-FIREWALL-MIB

Compteur	OID	Description
Connexions actives	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	Le nombre de connexions actuellement utilisées par l'ensemble du pare-feu.
Pic de connexions	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	Le nombre le plus élevé de connexions utilisées en même temps depuis le démarrage du système.
Nombre de connexions par seconde	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	Taux actuels de connexions par seconde sur le pare-feu.

Compteur	OID	Description
Nombre maximal de connexions par seconde	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	Le nombre le plus élevé de connexions par seconde sur le pare-feu depuis le démarrage du système.

Interrogation de traduction NAT

Tableau 5 : CISCO-NAT-EXT-MIB

Compteur	OID	Description
Traductions actives	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	Le nombre total d'entrées de traduction d'adresses actuellement disponibles dans le périphérique NAT. Ceci indique l'ensemble des entrées de traduction créées à partir des mécanismes de traduction d'adresses statiques et dynamiques.
Traductions actives en pointe	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	Le nombre maximal d'entrées de traduction d'adresses qui sont actives en même temps depuis le démarrage du système. Il s'agit du filigrane le plus élevé des entrées de traduction d'adresses actives à tout moment depuis le démarrage du système. Cet objet comprend les entrées de traduction créées à partir des mécanismes de traduction d'adresses statiques et dynamiques.

Interrogation des entrées de la table de routage

Tableau 6 : IP-FORWARD-MIB

Compteur	OID	Description
Traductions actives	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	Le nombre total d'entrées inetCidrRouteTable actuelles valides.

Interrogation de l'état du duplex de l'interface

Tableau 7 : CISCO-IF-EXTENSION-MIB

Compteur	OID	Description
État du duplex	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	Cet objet spécifie l'état configuré du duplex sur une interface donnée.
État du duplex détecté	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	Cet objet spécifie l'état du duplex détecté sur une interface donnée.

Sondage du taux d'incidents d'intrusion Snort 3

Tableau 8 : CISCO-UNIFIED-FIREWALL-MIB

Compteur	OID	Description
Taux d'incidents d'intrusion Snort 3	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	Fréquence à laquelle les incidents d'intrusion ont été enregistrés par Snort sur ce pare-feu en moyenne sur les 300 dernières secondes.

Notification de déroutement d'homologue BGP

Tableau 9 : BGP4-MIB

Compteur	OID	Description
Déroutement d'homologue BGP	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	L'événement BGPbackwardTransition est généré lorsque BGP FSM passe d'un état de numérotation supérieur à un état de numérotation inférieur.

interrogation d'utilisation de la CPU

Tableau 10 : CISCO-PROCESS-MIB

Compteur	OID	Description
Utilisation totale de la CPU	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	Utilisation totale du processeur du système au cours de la dernière minute
Utilisation de chaque cœur de CPU	Paramètres associés et valeurs de cPMCPUTotal1minRev 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	Valeurs d'utilisation de chaque cœur de CPU au cours de la dernière minute, où « n » représente le nombre de cœurs. Exemples : • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) : pourcentage d'utilisation de la CPU agrégé du système (cette valeur est identique à l'utilisation de la CPU du système de la version 3.6.1.4.1.9.9.109.1.1.1.1.7.1 en mode contexte unique). • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) : pourcentage d'utilisation moyenne du processeur Snort (valeur agrégée totale de toutes les instances Snort) • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) : pourcentage moyen de processus système (moyenne des cœurs « Sysprocess »)

Remarque Les OID de SNMP 1.3.6.1.2.1.25.3.3 et 1.3.6.1.2.1.25.3.4 se rapportant à la surveillance de la CPU (hrProcessorTable et hrNetworkTable) ont été supprimés sur la plateforme ASA FirePOWER. Vous pouvez afficher et surveiller les détails sur l'intégrité du processeur du périphérique uniquement par l'intermédiaire de son gestionnaire de périphériques.

Ajouter des utilisateurs SNMPv3

Remarque Vous créez des utilisateurs pour SNMPv3 uniquement. Ces étapes ne s'appliquent pas à SNMPv1 ou SNMPv2c.

Notez que SNMPv3 ne prend en charge que les utilisateurs en lecture seule.

Les utilisateurs SNMP doivent utiliser un nom d'utilisateur, un mot de passe d'authentification, un mot de passe de chiffrement et des algorithmes d'authentification et de chiffrement précisés.

Remarque Lorsque vous utilisez SNMPv3 avec mise en grappe ou haute disponibilité, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité à haute disponibilité, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire vers la nouvelle unité.

Les options d'algorithme d'authentification sont MD5 (obsolète, versions antérieures à 6.5 uniquement), SHA, SHA224, SHA256 et SHA384.

Remarque L'option MD5 est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant l'algorithme d'authentification MD5 qui ont été créés à l'aide d'une version antérieure à 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les FTD exécutant les versions 6.7 ou antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver l'algorithme d'authentification MD5, ou créer de nouveaux utilisateurs avec l'algorithme d'authentification MD5. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise l'algorithme d'authentification MD5 sur ces défense contre les menaces échouera.

Les options d'algorithme de chiffrement sont DES (obsolète, versions antérieures à 6.5 uniquement), 3DES, AES256, AES192 et AES128.

Remarque L'option DES est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant le chiffrement DES qui ont été créés à l'aide d'une version antérieure à la 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les défense contre les menaces exécutant les versions 6.7 et antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver le chiffrement DES, ou créer de nouveaux utilisateurs avec le chiffrement DES. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise le chiffrement DES sur ces défense contre les menaces échouera.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **SNMP** > **Utilisateurs**.

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Sélectionnez le niveau de sécurité de l'utilisateur dans la liste déroulante **Security Level** (niveau de sécurité).

- **Auth** : authentification mais pas de confidentialité, ce qui signifie que les messages sont authentifiés.
- **No Auth** : pas d'authentification ni de confidentialité, ce qui signifie qu'aucune sécurité n'est appliquée aux messages.
- **Priv** : authentification et confidentialité, ce qui signifie que les messages sont authentifiés et chiffrés.

Étape 5 Saisissez le nom de l'utilisateur SNMP dans le champ **Username**. Les noms d'utilisateur doivent comporter 32 caractères ou moins.

Étape 6 Sélectionnez le type de mot de passe que vous souhaitez utiliser dans la liste déroulante **Encryption Password Type** (type de mot de passe de chiffrement).

- **Effacer le texte** : le périphérique défense contre les menaces chiffrera toujours le mot de passe lors du déploiement sur le périphérique.
- **Chiffré** : le périphérique défense contre les menaces déploiera directement le mot de passe chiffré.

Étape 7 Dans la liste déroulante **Auth Algorithm Type** (Type d'algorithme d'authentification), sélectionnez le type d'authentification que vous souhaitez utiliser : SHA, SHA224, SHA256ou SHA384.

Remarque L'option MD5 est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant l'algorithme d'authentification MD5 qui ont été créés à l'aide d'une version antérieure à 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les FTD exécutant les versions 6.7 ou antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver l'algorithme d'authentification MD5, ou créer de nouveaux utilisateurs avec l'algorithme d'authentification MD5. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise l'algorithme d'authentification MD5 sur ces défense contre les menaces échouera.

Étape 8 Dans le champ **Authentication Password** (mot de passe d'authentification), saisissez le mot de passe à utiliser pour l'authentification. Si vous avez sélectionné Chiffré comme type de mot de passe de chiffrement, le mot de passe doit être au format xx:xx:xx..., où xx sont des valeurs hexadécimales.

Remarque La longueur du mot de passe dépend de l'algorithme d'authentification sélectionné. Pour tous les mots de passe, la longueur doit être de 256 caractères ou moins.

Si vous avez sélectionné Clear Text (effacer le texte) comme type de mot de passe de chiffrement, répétez le mot de passe dans le champ **Confirm** (Confirmer).

Étape 9 Dans la liste déroulante **Encryption Type** (Type de chiffrement), sélectionnez le type de chiffrement que vous souhaitez utiliser : AES128, AES192, AES256, 3DES.

Remarque Pour utiliser le chiffrement AES ou 3DES, la licence appropriée doit être installée sur le périphérique.

Remarque L'option DES est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant le chiffrement DES qui ont été créés à l'aide d'une version antérieure à la 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les défense contre les menaces exécutant les versions 6.7 et antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver le chiffrement DES, ou créer de nouveaux utilisateurs avec le chiffrement DES. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise le chiffrement DES sur ces défense contre les menaces échouera.

Étape 10 Saisissez le mot de passe à utiliser pour le chiffrement dans le champ **Encryption Password** (mot de passe de chiffrement). Si vous avez sélectionné Chiffré comme type de mot de passe de chiffrement, le mot de passe doit être au format xx:xx:xx..., où xx sont des valeurs hexadécimales. Pour les mots de passe chiffrés, la longueur du mot de passe dépend du type de chiffrement sélectionné. Les tailles des mots de passe sont les suivantes (où chaque xx est un octal) :

- AES 128 nécessite 16 octaux
- AES 192 nécessite 24 octaux
- AES 256 nécessite 32 octaux
- 3DES nécessite 32 octaux
- DES peut être de n'importe quelle taille

Remarque Pour tous les mots de passe, la longueur doit être de 256 caractères ou moins.

Si vous avez sélectionné Clear Text (effacer le texte) comme type de mot de passe de chiffrement, répétez le mot de passe dans le champ **Confirm** (Confirmer).

Étape 11 Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Ajouter des hôtes SNMP

Utilisez la commande Hôte pour ajouter ou modifier des entrées dans le tableau Hôtes SNMP de la page SNMP. Ces entrées représentent les stations de gestion SNMP autorisées à accéder au périphérique défense contre les menaces .

Vous pouvez ajouter jusqu'à 8 192 hôtes. Cependant, seulement 128 de ceux-cis peuvent être utilisés pour les déroutements.

Avant de commencer

Vérifiez que les objets réseau qui définissent les stations de gestion SNMP existent. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets réseaux.

Remarque Les objets réseau pris en charge comprennent les hôtes IPv6, les hôtes IPv4, la plage IPv4 et les adresses de sous-réseau IPv4.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **SNMP** > **Hosts** (Hôtes SNMP).

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Dans le champ **IP Address** (adresse IP), saisissez un hôte IPv6 ou IPv4 valide, ou sélectionnez l'objet réseau qui définit l'adresse d'hôte de le poste de gestion SNMP.

L'adresse IP peut être un hôte IPv6, un hôte IPv4, une plage IPv4 ou un sous-réseau IPv4.

Étape 5 Sélectionnez la version de SNMP appropriée dans la liste déroulante **SNMP version**.

Étape 6 (SNMPv3 uniquement.) Sélectionnez le nom d'utilisateur de l'utilisateur SNMP que vous avez configuré dans la liste déroulante **User Name** (nom d'utilisateur).

Remarque Vous pouvez associer jusqu'à 23 utilisateurs SNMP par hôte SNMP.

Étape 7 (SNMPv1, 2c uniquement.) Dans le champ **Read Community String** (Lire la chaîne de la communauté), saisissez le nom de communauté que vous avez déjà configuré pour l'accès en lecture au périphérique. Saisissez à nouveau la chaîne pour la confirmer.

Remarque Cette chaîne est obligatoire uniquement si la chaîne utilisée avec cette station SNMP est différente de celle déjà définie dans la section **Enable SNMP Server** (activer le serveur SNMP).

Étape 8 Sélectionner le type de communication entre le périphérique et le poste de gestion SNMP. Vous pouvez sélectionner les deux types.

- **Poll** (interrogation) : le poste de gestion demande régulièrement des informations au périphérique.
- **Trap** (Déroutement) : le périphérique envoie les événements de déroutement au poste de gestion au fur et à mesure qu'ils se produisent.

Remarque Lorsque l'adresse IP de l'hôte SNMP est une plage IPv4 ou un sous-réseau IPv4, vous pouvez configurer soit **interrogation**, soit **déroutement**, mais pas les deux.

Étape 9 Dans le champ **Port**, saisissez un numéro de port UDP pour l'hôte SNMP. La valeur par défaut est 162. La plage valide est de 1 à 65 535.

Étape 10 Sélectionnez le type d'interface pour la communication entre le périphérique et le poste de gestion SNMP dans les options **Accessible par**. Vous pouvez sélectionner l'interface de gestion du périphérique ou une zone de sécurité ou une interface nommée disponible.

- **Device Management Interface** (interface de gestion des périphériques) : la communication entre le périphérique et le poste de gestion SNMP s'effectue par l'interface de gestion.
  - Lorsque vous choisissez cette interface pour l'interrogation SNMPv3, tous les utilisateurs SNMPv3 configurés sont autorisés à interroger et ne sont pas limités à l'utilisateur choisi dans Étape 6, à la page 31. Ici, SNMPv1 et SNMPv2c ne sont pas autorisés à partir d'un hôte SNMPv3.

- Lorsque vous choisissez cette interface pour l'interrogation SNMPv1 et SNMPv2c, l'interrogation ne se limite pas du tout à la version sélectionnée dans Étape 5, à la page 31.

- **Security Zones ou Named Interface** (zones de sécurité ou interface nommée) : la communication entre le périphérique et le poste de gestion SNMP s'effectue par une zone ou une interface de sécurité.
  - Recherchez des zones dans le champ **Zones disponibles**.
  - Ajoutez les zones qui contiennent les interfaces par lesquelles le périphérique communique avec le poste de gestion dans le champ **Zone/interface sélectionnée** . 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 11 Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les déroutements SNMP

Utilisez les déroutements SNMP pour configurer les déroutements SNMP (notifications d'événements) pour le périphérique défense contre les menaces . Les déroutements sont différents de la navigation; il s'agit de « commentaires » non sollicités du périphérique défense contre les menaces au poste de gestion pour certains événements, comme l'établissement de liaison, la perte de liaison et l'événement généré par syslog. Un ID d'objet SNMP (OID) pour le périphérique apparaît dans les déroutements d'événements SNMP envoyés par le périphérique.

Certains déroutements ne sont pas applicables à certains modèles de matériel. Ces déroutements seront ignorés si vous appliquez la politique à l'un de ces modèles. Par exemple, tous les modèles n'ont pas d'unités remplaçables sur site, de sorte que la fonction de déroutement **d'insertion/suppression d'unité remplaçable sur site** ne sera pas configurée sur ces modèles.

Les déroutements SNMP sont définies dans les MIB standard ou spécifiques à l'entreprise. Les déroutements standard sont créés par l'IETF et documentés dans diverses normes RFC. Les déroutements SNMP sont compilés dans le logiciel défense contre les menaces .

Si nécessaire, vous pouvez télécharger les RFC, les MIB standard et les déroutements standard à partir de l'emplacement suivant :

http://www.ietf.org/

Parcourez la liste complète des MIB, des déroutements et des OID de Cisco à partir de l'emplacement suivant :

Navigateur pour les objets SNMP

Téléchargez également les OID de Cisco par FTP à partir de l'emplacement suivant :

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **SNMP** > **SNMP Traps** (Déroutements SNMP) pour configurer les déroutements de SNMP (notifications d'événements) pour le périphérique défense contre les menaces .

Étape 3 Sélectionnez les options Enable Traps (activer les déroutements) appropriées. Vous pouvez sélectionner l'une ou l'autre des options ou les deux.

a) Cochez la case **Enable All SNMP Traps** (activer tous les déroutements SNMP) pour sélectionner rapidement tous les déroutements dans les quatre sections suivantes.

b) Cochez la case **Enable All Syslog Traps** (activer tous les déroutements syslog) pour activer la transmission des messages syslog liés aux déroutements.

Remarque Les déroutements SNMP ont une priorité plus élevée que les autres messages de notification de défense contre les menaces , car ils sont supposés être en temps quasi réel. Lorsque vous activez toutes les alertes de SNMP ou de syslog, il est possible que le processus SNMP consomme les ressources excédentaires de l'agent et du réseau, ce qui entraîne le blocage du système. Si vous remarquez des retards du système, des demandes non terminées ou des échéances de délais d'expiration, vous pouvez activer de manière sélective les déroutements SNMP et syslog. Vous pouvez également limiter la fréquence à laquelle les messages syslog sont générés par niveau de gravité ou ID de message. Par exemple, tous les ID de messages syslog qui commencent par les chiffres 212 sont associés à la classe SNMP; voir Limiter le débit de génération des messages Syslog, à la page 52.

Étape 4 Les déroutements de notification d'événement de la section **Standard** sont activés par défaut pour une politique existante :

- **Authentification** : accès SNMP non autorisé. Cet échec d'authentification se produit pour les paquets avec un identifiant de communauté incorrect.
- **Link Up** (Lien disponible) : l'un des liens de communication du périphérique est devenu disponible (il a été établi), comme l'indique la notification.
- **Link Down** (Lien en panne) : l'un des liens de communication du périphérique est en panne, comme indiqué dans la notification.
- **Cold Start** Démarrage à froid) : le périphérique se réinitialise, de sorte que sa configuration ou la mise en œuvre de l'entité de protocole peut être modifiée.
- **Warm Start** (Démarrage à chaud) : le périphérique se réinitialise de sorte que sa configuration et la mise en œuvre de l'entité de protocole ne changent pas.

Étape 5 Sélectionnez les déroutements de notification d'événement souhaités dans la section **Entity MIB** (MIB d'entité) :

- **Field Replaceable Unit Insert** (Insertion d'unité remplaçable sur site) : une unité remplaçable sur site (FRU) a été insérée, comme indiqué. (Les FRU comprennent les assemblages comme les blocs d'alimentation, les ventilateurs, les modules de processeur, les modules d'interface, etc.)
- **Field Replaceable Unit Delete** (Suppression d'une unité remplaçable sur site : une unité remplaçable sur site (FRU) a été supprimée, comme indiqué dans la notification.
- **Configuration Change** (Changement de configuration : il y a eu une modification matérielle, comme indiqué dans la notification

Étape 6 Sélectionnez les déroutements de notification d'événement souhaités dans la section **Resource** :

- **Connection Limit Reached** (Limite de connexion atteinte) : ce détournement indique qu'une tentative de connexion a été rejetée car la limite de connexions configurée a été atteinte.

Étape 7 Sélectionnez les déroutements de notification d'événement souhaités dans la section **Autre** :

- **NAT Packet Discard** (élimination des paquets NAT) : cette notification est générée lorsque des paquets IP sont rejetés par la fonction NAT. Les adresses ou les ports de traduction d'adresses réseau disponibles sont inférieurs au seuil configuré.
- **CPU Rising Threshold** (Seuil en hausse de la CPU) : cette notification est générée lorsque l'augmentation de l'utilisation de la CPU dépasse un seuil prédéfini pendant une période configurée. Cochez cette option pour activer les notifications de seuil d'augmentation de la CPU :
  - **Percentage** (Pourcentage) : la valeur par défaut est 70 % pour la notification de seuil élevé; la plage se situe entre 10 et 94 %. Le seuil critique est codé en dur à 95 %.
  - **Period** (Période) : la période de surveillance par défaut est de 1 minute; la valeur doit être comprise entre 1 et 60 minutes.
- **Memory Rising Threshold** (Seuil de hausse de la mémoire) : cette notification est générée lorsque l'augmentation de l'utilisation de la mémoire dépasse un seuil prédéfini, réduisant ainsi la mémoire disponible. Cochez cette option pour activer les notifications de seuil d'augmentation de la mémoire :
  - **Percentage** (Pourcentage) : la valeur par défaut est 70 % pour la notification de seuil élevé; la plage se situe entre 50 et 95 %.
- **Failover** (Basculement) : cette notification est générée en cas de changement dans l'état de basculement, comme indiqué par CISCO-UNIFIED-FIREWALL-MIB.
- **Cluster** (Grappe) : cette notification est générée lorsqu'un changement est apporté à l'intégrité de la grappe, comme indiqué par CISCO-UNIFIED-FIREWALL-MIB.
- **Peer Flap** (Oscillation homologue) : cette notification est générée en cas d'oscillation de route BGP, une situation dans laquelle les systèmes BGP envoient un nombre excessif de messages de mise à jour pour annoncer les informations sur l'accessibilité du réseau.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

SSL

Remarque Vous devez disposer de privilèges d'administrateur et faire partie d'un domaine secondaire pour effectuer cette tâche.

Vous devez vous assurer que vous exécutez une version sous licence complète de Cisco Secure Firewall Management Center. Les paramètres SSL seront désactivés si vous exécutez Cisco Secure Firewall Management Center en mode d'évaluation. En outre, les paramètres SSL sont désactivés lorsque la version sous licence de Cisco Secure Firewall Management Center ne répond pas aux critères de conformité pour l'exportation. Si vous utilisez le VPN d'accès à distance avec SSL, les fonctionnalités de chiffrement renforcé doivent être activées sur votre compte Smart. Pour en savoir plus, consultez *Types et restrictions de licences* dans le Guide d'administration Cisco Secure Firewall Management Center.

Procédure

Étape 1 Sélectionnez **Devices (périphériques) > Platform Settings (paramètres de la plateforme)** et créez ou modifiez une politique défense contre les menaces .

Étape 2 Sélectionnez **SSL**.

Étape 3 Ajoutez des entrées au tableau **Add SSL Configuration** (Ajouter une configuration SSL).

a) Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée, ou cliquez sur **Edit** (Modifier) si l'entrée existe déjà.

b) Sélectionnez les configurations de sécurité requises dans la liste déroulante .

- **Protocol Version** (Version du protocole) : Spécifie les protocoles TLS à utiliser lors de l'établissement des sessions VPN d'accès à distance.
- **Security Level** (niveau de sécurité) : Indique le type de positionnement de sécurité que vous souhaitez configurer pour SSL.

Étape 4 Sélectionnez les **algorithmes disponibles** en fonction de la version de protocole que vous sélectionnez et cliquez sur **Add** (ajouter) pour les inclure pour le protocole sélectionné. Pour en savoir plus, consultez À propos des paramètres SSL, à la page 36.

Les algorithmes sont répertoriés en fonction de la version de protocole que vous sélectionnez. Chaque protocole de sécurité identifie un algorithme unique pour le paramétrage du niveau de sécurité.

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

Prochaine étape

Sélectionnez **Deploy (Déployer)** > **Deployment (Déploiement)** et cliquez sur **Deploy** afin de déployer la politique sur les périphériques attribués.

À propos des paramètres SSL

Le périphérique défense contre les menaces utilise le protocole SSL (Secure sockets Layer) et le protocole TLS (Transport Layer Security) pour prendre en charge la transmission sécurisée des messages pour la connexion VPN d'accès à distance à partir de clients distants. La fenêtre SSL Settings (paramètres SSL) vous permet de configurer les versions SSL et les algorithmes de chiffrement qui seront négociés et utilisés pour la transmission des messages lors de l'accès VPN à distance sur SSL.

Remarque Bien que vous configuriez centre de gestion et défense contre les menaces pour fonctionner en mode de conformité avec les certifications de sécurité (UCAPL, CC ou FIPS), centre de gestion permet la configuration de chiffrements non pris en charge. Par exemple, en mode FIPS activé, le centre de gestion permet de configurer DH groupe 5, qui n'est pas conforme à la norme FIPS. Cependant, le tunnel VPN ne négocie pas en raison d'une utilisation du chiffrement non conforme.

Configurez les paramètres SSL à l'emplacement suivant :

Devices (périphériques) Platform Settings (paramètres de la plateforme) > SSL

Champs

Minimum SSL Version as Server(Version SSL minimale en tant que serveur) : précisez la version minimale du protocole SSL/TLS que le périphérique défense contre les menaces utilise lorsqu'il agit en tant que serveur. Par exemple, lorsqu'il fonctionne comme passerelle VPN d'accès à distance.

TLS Version (Version TLS) : sélectionnez l'une des versions TLS suivantes dans la liste déroulante :

TLS V1	Accepte les messages client hello SSLv2 et négocie TLSv1 (ou version supérieure).
TLSV1.1	Accepte les messages client hello SSLv2 et négocie TLSv1.1 (ou version supérieure).
TLSV1.2	Accepte les messages client hello SSLv2 et négocie TLSv1.2 (ou version supérieure).
TLSv1.3	Accepte les hellos de clients SSLv2 et négocie TLSv1.3 (ou version ultérieure).

Remarque TLS 1.3 dans le VPN d'accès à distance nécessite Cisco Secure Client, version 5.0 ou ultérieure.

DTLS Version (Version DTLS) : sélectionnez les versions DTLS dans la liste déroulante, en fonction de la version TLS sélectionnée. Par défaut, DTLSv1 est configuré sur les périphériques défense contre les menaces . Vous pouvez choisir la version DTLS selon vos besoins.

Remarque Assurez-vous que la version du protocole TLS est supérieure ou égale à la version de protocole DTLS sélectionnée. Les versions du protocole TLS prennent en charge les versions DTLS suivantes :

TLS V1	DTLSv1
TLSV1.1	DTLSv1

TLSV1.2	DTLSv1, DTLSv1.2
TLSv1.3	DTLSv1, DTLSv1.2

Diffie-Hellman Group : choisissez un groupe dans la liste déroulante. Les options disponibles sont Group1 - module de 768 bits, Group2 - module de 1024 bits, Group5 - module de 1536 bits, Group14 - module de 2048 bits, ordre premier de 224 bits, et Group24 - module de 2048 bits, ordre premier de 256 bits. La valeur par défaut est Group1.

Elliptical Curve Diffie-Hellman Group(groupe Diffie-Hellman de courbe elliptique) : choisissez un groupe dans la liste déroulante. Les options disponibles sont Groupe19 – EC 256 bits, Groupe20 – EC 384 bits et Groupe21 – EC 521 bits. La valeur par défaut est Group19.

TLSv1.2 ajoute la prise en charge des chiffrements suivants :

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

Remarque Les chiffrements ECDSA et DHE ont la priorité la plus élevée.

TLSv1.3 ajoute la prise en charge des chiffrements suivants :

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384

Le tableau de configuration SSL peut être utilisé pour spécifier la version du protocole, le niveau de sécurité et les algorithmes de chiffrement que vous souhaitez prendre en charge sur les Cisco Secure Firewall Threat Defense.

Protocol Version (Version du protocole) : répertorie la version du protocole que le périphérique Cisco Secure Firewall Threat Defense prend en charge et utilise pour les connexions SSL. Les versions de protocole disponibles sont les suivantes :

- Par défaut
- TLSV1
- TLSV1.1
- TLSV1.2
- TLSv1.3
- DTLSv1
- DTLSv1.2

Security Level (niveau de sécurité) : dresse la liste des niveaux de sécurité de chiffrement que le périphérique défense contre les menaces prend en charge et utilise pour les connexions SSL.

Si vous possédez des périphériques défense contre les menaces avec licence d'évaluation, le niveau de sécurité est Faible par défaut. Avec la licence smart défense contre les menaces , le niveau de sécurité par défaut est Élevé. Vous pouvez choisir l'une des options suivantes pour configurer le niveau de sécurité requis :

- **Tout** comprend tous les chiffrements, y compris NULL-SHA.
- **Faible** comprend tous les chiffrements, sauf NULL-SHA.
- **Moyen** comprend tous les chiffrements, sauf NULL-SHA, DES-CBC-SHA, CR4-SHA et RC4-MD5 (il s'agit du chiffrement par défaut).
- **Fips** comprend tous les chiffrements conformes FIPS, sauf NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA, TLS_CHACHA20_POLY1305_SHA256.
- **Élevé** comprend uniquement AES-256 avec les chiffrements SHA-2 et s'applique à TLS version 1.2 et à la version *par défaut*.
- **Personnalisé** comprend un ou plusieurs chiffrements que vous spécifiez dans la zone Algorithmes de chiffrement/chaîne personnalisée. Cette option vous fournit un contrôle total de la suite de chiffrement à l'aide de chaînes de définition de chiffrement OpenSSL.

Cipher Algorithms/Custom String (Algorithmes de chiffrement/chaîne personnalisée) : répertorie les algorithmes de chiffrement que le périphérique défense contre les menaces prend en charge et utilise pour les connexions SSL. Pour plus d'informations sur les chiffrements à l'aide d'OpenSSL, consultez https://www.openssl.org/docs/apps/ciphers.html

Le périphérique défense contre les menaces spécifie l'ordre de priorité des chiffrements pris en charge comme suit :

Chiffrements pris en charge par TLSv1.2 uniquement

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384

DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

Chiffreurs non pris en charge par TLSv1.1 ou TLSv1.2

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

Syslog

Vous pouvez activer la journalisation du système (syslog) pour les périphériques défense contre les menaces . Les informations de journalisation peuvent vous aider à cerner et isoler les problèmes de configuration du réseau ou des périphériques. Vous pouvez également envoyer certains événements de sécurité à un serveur syslog. Les rubriques suivantes expliquent la journalisation et la manière de la configurer.

À propos de Syslog

La journalisation du système est une méthode de collecte de messages des périphériques vers un serveur exécutant un daemon syslog. La journalisation sur un serveur syslog central facilite l'agrégation des journaux et des alertes. Les périphériques Cisco peuvent envoyer leurs messages de journal à un service syslog de type UNIX. Un service syslog accepte les messages et les stocke dans des fichiers ou les imprimés conformément à un fichier de configuration simple. Cette forme de journalisation offre un stockage protégé à long terme pour les journaux. Les journaux sont utiles pour les dépannages de routine et pour le traitement des incidents.

Tableau 11 : Journaux du système pour Cisco Secure Firewall Threat Defense

Journaux associés à	Détails	Configurer dans
Intégrité des périphériques et du système, configuration du réseau	Cette configuration syslog génère des messages pour les fonctionnalités s'exécutant sur le plan de données, c'est-à-dire les fonctionnalités définies dans la configuration de l'interface de ligne de commande que vous pouvez afficher avec la commande **show running-config**. Cela inclut des fonctionnalités telles que le routage, le VPN, les interfaces de données, le serveur DHCP, la NAT, etc. Les messages du journal système du plan de données sont numérotés et sont identiques à ceux générés par les périphériques exécutant le logiciel ASA. Cependant, Cisco Secure Firewall Threat Defense ne génère pas nécessairement tous les types de messages disponibles pour le logiciel ASA. Pour en savoir plus sur ces messages, consultez *Messages Syslog Cisco Cisco Secure Firewall Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html. Cette configuration est expliquée dans les rubriques suivantes.	**Paramètres de la plateforme**
Événements de sécurité	Cette configuration syslog génère des alertes pour les fichiers et les programmes malveillants, la connexion, les renseignements sur la sécurité et les incidents d'intrusion.	les **paramètres de la plateforme** et la **journalisation** et la politique de contrôle d'accès
(Tous les périphériques) Politiques, règles et événements	Cette configuration syslog génère des alertes pour les règles de contrôle d'accès, les règles de prévention des intrusions et d'autres services avancés, comme décrit dans la section *Configurations prenant en charge les réponses aux alertes* dans le Guide d'administration Cisco Secure Firewall Management Center. Ces messages ne sont pas numérotés. Pour des informations sur la configuration de ce type de messages syslog, consultez *Création d'une réponse à une alerte syslog* dans le Guide d'administration Cisco Secure Firewall Management Center.	Les **réponses aux alertes** et la **journalisation** dans une politique de contrôle d'accès;

Vous pouvez configurer plusieurs serveurs syslog et contrôler les messages et les événements envoyés à chaque serveur. Vous pouvez également configurer différentes destinations, telles que la console, le courriel, la mémoire tampon interne, etc.

Niveaux de gravité

Le tableau suivant répertorie les niveaux de gravité des messages du journal système.

Tableau 12 : Niveaux de gravité des messages Syslog

Numéro de niveau	Niveau de gravité	Description
0	**urgences**	Système inutilisable.
1	**alerte**	Action immédiate requise.

Numéro de niveau	Niveau de gravité	Description
2	**critique**	Conditions critiques.
3	**erreur**	Conditions d'erreur.
4	**avertissement**	Conditions de mise en garde.
5	**notification**	Condition normale, mais pouvant être grave
6	**renseignements**	Messages informatifs seulement.
7	**débogage**	Messages de débogage uniquement Ne journalisez à ce niveau que temporairement, lors du débogage des problèmes. Ce niveau de journalisation peut générer tant de messages que les performances du système peuvent en être affectées.

Remarque ASA et Défense contre les menaces ne génèrent pas de messages syslog avec un niveau de gravité de zéro (urgences).

Filtrage des messages Syslog

Vous pouvez filtrer les messages syslog générés de sorte que seuls certains messages syslog soient envoyés vers une destination de sortie particulière. Par exemple, vous pouvez configurer appareil de défense contre les menaces pour envoyer tous les messages syslog vers une destination de sortie et pour envoyer un sous-ensemble de ces messages syslog vers une autre destination de sortie.

Plus précisément, vous pouvez diriger les messages du syslog vers une destination de sortie en fonction des critères suivants :

- Numéros d'ID des messages Syslog

  (Cela ne s'applique pas aux messages syslog pour les événements de sécurité tels que les événements de connexion et les incidents d'intrusions.)

- Niveau de gravité des messages du journal système
- Classe de messages Syslog (équivalente à une zone fonctionnelle)

  (Cela ne s'applique pas aux messages syslog pour les événements de sécurité tels que les événements de connexion et les incidents d'intrusions.)

Vous personnalisez ces critères en créant une liste de messages que vous pouvez préciser lorsque vous définissez la destination de sortie. Sinon, vous pouvez configurer les appareil de défense contre les menaces pour envoyer une classe de messages particulière à chaque type de destination de sortie indépendamment de la liste de messages.

(Les listes de messages ne s'appliquent pas aux messages syslog pour les événements de sécurité tels que les événements de connexion et de prévention des intrusions.)

Classe de messages Syslog

Remarque Cette rubrique ne s'applique pas aux messages des événements de sécurité (connexion, intrusion, etc.)

Vous pouvez utiliser les classes de messages syslog de deux manières :

- Précisez un emplacement de sortie pour toute une catégorie de messages du journal système.
- Créez une liste de messages qui spécifie la classe du message.

La classe de messages syslog fournit une méthode de catégorisation des messages syslog par type, ce qui équivaut à une fonctionnalité ou à une fonction du périphérique. Par exemple, la classe rip désigne le routage RIP.

Tous les messages syslog d'une classe particulière partagent les trois mêmes chiffres initiaux dans leurs numéros d'ID de message syslog. Par exemple, tous les ID de message syslog qui commencent par les chiffres 611 sont associés à la classe vpnc (client VPN). Les messages syslog associés à la fonctionnalité de client VPN vont de 611101 à 611323.

En outre, la plupart des messages syslog ISAKMP ont un ensemble commun d'objets ajoutés au début pour aider à identifier le tunnel. Ces objets précèdent le texte descriptif d'un message syslog lorsqu'ils sont disponibles. Si l'objet est inconnu au moment de la génération du message syslog, la combinaison en-tête = valeur ne s'affiche pas.

Les objets portent le préfixe suivant :

Group = *groupname*, Username = *user*, IP = *IP_address*

Lorsque le groupe est le groupe de tunnels, le nom d'utilisateur est le nom d'utilisateur de la base de données locale ou du serveur AAA et l'adresse IP est l'adresse IP publique du client d'accès à distance ou de l'homologue de couche 2.

Le tableau suivant répertorie les classes de messages et la plage d'ID de message dans chaque classe.

Tableau 13 : Classes de messages syslog et numéros d'ID de messages associés

Class (classe)	Définition	Numéros d'ID des messages Syslog
auth	Authentification de l'utilisateur	109, 113
—	Listes d'accès	106
—	Pare-feu d'application	415
—	Filtre de trafic de réseau de zombies	338
bridge (pont)	Pare-feu transparent	110, 220
ca	Autorité de certification de l'infrastructure de clé publique (PKI)	717
citrix	Client Citrix	723
—	Mise en grappes	747

Class (classe)	Définition	Numéros d'ID des messages Syslog
—	Gestion des cartes	323
config (configurer)	Interface de commande	111, 112, 208, 308
csd	Poste de travail sécurisé	724
cts	TrustSec de Cisco	776
DAP	Politiques d'accès dynamique	734
eap, eapoudp	EAP ou EAPoUDP pour le contrôle d'admission au réseau	333, 334
eigrp	Routage EIGRP	336
e-mail	Serveur mandataire de courriel	719
—	Surveillance de l'environnement	735
ha	Basculement	101, 102, 103, 104, 105, 210, 311, 709
—	Pare-feu basé sur l'identité	746
ids	Système de détection des intrusions	400, 733
—	Boîte à outils IKEv2	750, 751, 752
ip	Pile d'adresse IP	209, 215, 313, 317, 408
ipaa	Affectation d'adresse IP	735
ips	Système de protection contre les intrusions	400, 401, 420
—	IPv6	325
—	Licence	444
mdm-proxy	Mandataire MDM	802.
nac	Contrôle d'admission au réseau (NAC)	731, 732
nacpolicy	Politique NAC	731
nacsettings	Paramètres NAC pour appliquer la politique NAC	732
—	NAT et PAT	305
—	Point d'accès réseau	713
np	Processeur de réseau	319
—	NP SSL	725
ospf	Routage OSPF	318, 409, 503, 613

Class (classe)	Définition	Numéros d'ID des messages Syslog
—	Chiffrement de mot de passe	742
—	Serveur mandataire téléphonique	337
protocole RIP	Routage RIP	107, 312
rm	Gestionnaire des ressources	321
—	Smart Call Home	120
séance de formation	Séance d'utilisateur	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212
—	ScanSafe	775
ssl	Pile SSL	725
svc	Client VPN SSL	722
sys	Système	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Détection des menaces	733
tag-switching	Commutation de balise de service	779
vm	Mise en correspondance VLAN	730
vpdn	Sessions PPTP et L2TP	213, 403, 603
vpn	IKE et IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	Client VPN	611
vpnfo	Basculement du VPN	720
vpnlb	Équilibrage de la charge VPN	718
—	VXLAN	778
webfo	Basculement WebVPN	721
webvpn	WebVPN et Secure Client (services client sécurisés)	716

Lignes directrices relatives à la journalisation

Cette section comprend des consignes et des limites que vous devez consulter avant de configurer la journalisation.

Directives IPv6

- IPv6 est pris en charge. Les journaux système peuvent être envoyés en utilisant les protocoles TCP ou UDP.
- Assurez-vous que l'interface configurée pour l'envoi des journaux système est activée, qu'elle est compatible avec IPv6, et que le serveur syslog est accessible par l'intermédiaire de l'interface désignée.
- La journalisation sécurisée sur IPv6 n'est pas prise en charge.

Directives supplémentaires

- Ne configurez pas centre de gestion en tant que serveur syslog principal. Le centre de gestion peut journaliser certains syslog. Cependant, il ne dispose pas de dispositions de stockage adéquates pour contenir une quantité d'informations provenant d'événements de connexion pour chaque capteur, en particulier lorsque plusieurs capteurs sont utilisés et que tous envoient des journaux système.
- Le serveur syslog doit exécuter un programme de serveur appelé syslogd. Windows fournit un serveur syslog dans le cadre de son système d'exploitation.
- Pour afficher les journaux générés par appareil de défense contre les menaces , vous devez spécifier une destination de sortie de journalisation. Si vous activez la journalisation sans préciser de destination de sortie de journalisation, l'appareil de défense contre les menaces génère des messages mais ne les enregistre pas à un emplacement à partir duquel vous pouvez les afficher. Vous devez spécifier chaque destination de sortie de journalisation séparément.
- 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.
- Il n'est pas possible d'affecter deux listes ou classes différentes à des serveurs syslog différents ou aux mêmes emplacements.
- Vous pouvez configurer jusqu'à seize serveurs de journaux système.
- Le serveur syslog doit être accessible au moyen de appareil de défense contre les menaces . Vous devez configurer le périphérique pour refuser les messages ICMP unreachable (ICMP injoignable) sur l'interface par laquelle le serveur syslog est accessible et pour envoyer des journaux syslog au même serveur. Assurez-vous d'avoir activé la journalisation pour tous les niveaux de gravité. Pour éviter que le serveur syslog ne se bloque, supprimez la génération des syslogs 313001, 313004 et 313005.
- Le nombre de connexions UDP pour syslog est directement lié au nombre de CPU sur la plateforme matérielle et au nombre de serveurs syslog que vous configurez. À tout moment, il peut y avoir autant de connexions syslog UDP qu'il y a de CPU multiplié par le nombre de serveurs syslog configurés. Il s'agit du comportement attendu. Notez que le délai d'inactivité de la connexion UDP globale s'applique à ces sessions et que la valeur par défaut est de 2 minutes. Vous pouvez ajuster ce paramètre si vous souhaitez fermer ces sessions plus rapidement, mais le délai d'expiration s'applique à toutes les connexions UDP, pas seulement au syslog.

- Lorsque appareil de défense contre les menaces envoie des journaux système via TCP, la connexion prend environ une minute pour s'établir après le redémarrage du service syslogd.

Configurer la journalisation syslog pour les périphériques FTD

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 47.

Pour configurer les paramètres Syslog, utilisez les étapes suivantes :

Avant de commencer

Voir les exigences dans Lignes directrices relatives à la journalisation, à la page 45.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **Syslog** dans la table des matières.

Étape 3 Cliquez sur **Logging Setup** (Configuration de la journalisation) pour activer la journalisation, préciser les paramètres du serveur FTP et préciser l'utilisation de la mémoire Flash. Pour en savoir plus, consultez Activer la journalisation et configurer les paramètres de base, à la page 47

Étape 4 Cliquez sur **Logging Destinations** pour activer la journalisation vers des destinations spécifiques et pour spécifier le filtrage sur le niveau de gravité du message, la classe d'événement ou sur une liste d'événements personnalisée. Pour en savoir plus, consultez Activer les destinations de la journalisation, à la page 49

Vous devez activer une destination de journalisation pour voir les messages à cette destination.

Étape 5 Cliquez sur **E-mail Setup** pour spécifier l'adresse de messagerie utilisée comme adresse source pour les messages syslog envoyés comme messages électroniques. Pour en savoir plus, consultez Envoyer des messages Syslog à une adresse courriel, à la page 50

Étape 6 Cliquez sur **Events List** pour définir une liste d'événements personnalisée qui comprend une classe d'événement, un niveau de gravité et un ID d'événement. Pour en savoir plus, consultez Créer une liste d'événements personnalisée, à la page 51

Étape 7 Cliquez sur **Rate Limit** pour préciser le volume de messages envoyés vers toutes les destinations configurées et définir le niveau de gravité des messages auquel vous souhaitez affecter des limites de débit. Pour en savoir plus, consultez Limiter le débit de génération des messages Syslog, à la page 52

Étape 8 Cliquez sur **Syslog Settings** pour définir la fonction de journalisation, activer l'inclusion d'un horodatage et activer d'autres paramètres pour configurer un serveur comme destination syslog. Pour en savoir plus, consultez Configurer les paramètres Syslog, à la page 53

Étape 9 Cliquez sur **Syslog Servers** pour préciser l'adresse IP, le protocole utilisé, le format et la zone de sécurité du serveur Syslog désigné comme destination de journalisation. Pour en savoir plus, consultez Configurer un serveur Syslog, à la page 55

Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité

Les « événements de sécurité » comprennent les événements de connexion, de renseignements sur la sécurité, les intrusions, les fichiers et les programmes malveillants.

Certains des paramètres du journal système sur la page **Périphériques > Paramètres de la plateforme > Paramètres de défense contre les menaces > Syslog** et ses onglets s'appliquent aux messages du journal système pour les événements de sécurité, mais la plupart ne s'appliquent qu'aux messages d'événements liés à l'intégrité du système et à la mise en réseau.

Les paramètres suivants s'appliquent aux messages syslog pour les événements de sécurité :

- Onglet **Configuration des connexions** :
  - **Envoyer les journaux systèmes en format EMBLEM**
- Onglet **Paramètres journal système** :
  - **Activer l'horodatage des messages de journal système**
  - **Format de l'horodatage**
  - **Activer l'ID de l'appareil de journal système**
- Onglet **Serveurs journal système** :
  - Toutes les options du formulaire **Add Syslog Server** (Ajouter un serveur Syslog) (et la liste des serveurs configurés).

Activer la journalisation et configurer les paramètres de base

Vous devez activer la journalisation pour que le système génère des messages syslog pour les événements du plan de données.

Vous pouvez également configurer l'archivage sur un serveur flash ou FTP comme emplacement de stockage lorsque la mémoire tampon locale est pleine. Vous pouvez manipuler les données de journalisation après leur enregistrement. Par exemple, vous pouvez préciser les actions à exécuter lorsque certains types de messages Syslog sont enregistrés, extraire les données du journal et enregistrer les enregistrements dans un autre fichier pour créer des rapports ou suivre les statistiques à l'aide d'un script spécifique au site.

La procédure suivante explique certains des paramètres de base du journal système.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et de prévention des intrusions), la plupart des paramètres de la plateforme défense contre les menaces ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 47.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Logging Setup** (configuration de la journalisation Syslog).

Étape 3 Activez la journalisation et configurez les paramètres de journalisation de base.

- **Enable Logging**(activer la journalisation) : active la journalisation du système du plan de données pour le périphérique défense contre les menaces .
- **Enable Logging on the Failover Standby Unit**(activer la journalisation sur l'unité de secours de basculement) : active la journalisation du périphérique de secours pour le périphérique défense contre les menaces , si elle est disponible.
- **Send syslog in EMBLEM format** : active la journalisation au format EMBLEM pour chaque destination de journalisation. Si vous activez EMBLEM, vous devez utiliser le protocole UDP pour publier les messages du journal système. EMBLEM n'est pas compatible avec TCP.

  Remarque Les messages syslog au format RFC5424 affichent généralement la valeur de priorité (PRI). Cependant, dans centre de gestion, si vous souhaitez afficher la valeur PRI dans les messages syslog des défense contre les menaces gérés, assurez-vous d'activer le format EMBLEM. Pour en savoir plus sur PRI, consultez RFC5424.

- **Send debug messages as syslogs** (envoyer les messages de débogage en tant que syslog) : redirige toutes les données de sortie de la trace de débogage vers le syslog. Le message du journal système ne s'affiche pas dans la console si cette option est activée. Par conséquent, pour voir les messages de débogage, vous devez activer la journalisation sur la console et la configurer comme destination pour le numéro et le niveau de journalisation du message syslog de débogage. Le numéro du message syslog utilisé est 711001. Le niveau de journalisation par défaut pour ce journal système est « debug ».
- **Taille de la mémoire du tampon interne** : spécifiez la taille de la mémoire tampon interne dans laquelle les messages du journal système sont enregistrés si la mémoire tampon de journalisation est activée. Lorsque la mémoire tampon est pleine, elle est remplacée. Par défaut, c'est de 4096 octets. La plage se situe entre 4096 et 52428800.

Étape 4 (Facultatif) Activez la journalisation VPN en cochant la case **Enable Logging to Secure Firewall Management Center** (Activer la journalisation vers le FMC, Activer la journalisation vers Secure Firewall Management Center). Choisissez le niveau de gravité syslog pour les messages VPN dans la liste déroulante **Niveau de journalisation**.

Les journaux système de dépannage VPN peuvent ajouter une charge excessive sur centre de gestion. Par conséquent, activez cette option avec prudence. En outre, lorsque vous configurez un périphérique avec un VPN de site à site ou d'accès à distance, celui-ci active automatiquement par défaut l'envoi des journaux système VPN au centre de gestion. Le niveau de journalisation par défaut est Error (erreur). Nous vous recommandons de limiter le niveau de journalisation à Error (erreur) et à un niveau supérieur pour restreindre le flux excessif de journaux système vers centre de gestion, en particulier dans le cas du VPN d'accès à distance, où plusieurs périphériques sont impliqués.

Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 40.

Étape 5 (Facultatif) Configurez un serveur FTP si vous souhaitez enregistrer le contenu de la mémoire tampon des journaux sur le serveur avant que la mémoire tampon ne soit remplacée. Spécifier les informations du serveur FTP

- **FTP Server Buffer Wrap** (encapsulation de la mémoire tampon du serveur FTP) : pour enregistrer le contenu de la mémoire tampon sur le serveur FTP avant qu'elle ne soit remplacée, cochez cette case et saisissez les informations de destination nécessaires dans les champs suivants. Pour supprimer la configuration FTP, désélectionnez cette option.
- **IP Address** (adresse IP) : sélectionnez l'objet de réseau hôte qui contient l'adresse IP du serveur FTP.
- **User Name** (nom d'utilisateur) : saisissez le nom d'utilisateur à utiliser lors de la connexion au serveur FTP.
- **Path** (chemin) : Saisissez le chemin, relatif à la racine du FTP, où le contenu de la mémoire tampon doit être enregistré.
- **Password/Confirm** (mot de passe/confirmation) : saisissez et confirmez le mot de passe utilisé pour authentifier le nom d'utilisateur sur le serveur FTP.

Étape 6 (Facultatif) Précisez la taille de la mémoire flash si vous souhaitez enregistrer le contenu de la mémoire tampon du journal dans la mémoire flash avant que la mémoire tampon ne soit remplacée.

- **Flash** : cochez cette case pour enregistrer le contenu de la mémoire tampon dans la mémoire flash avant qu'elle ne soit remplacée.
- **Mémoire flash maximale à utiliser par la journalisation (Ko)** : spécifiez l'espace maximal à utiliser dans la mémoire flash pour la journalisation (en Ko). La plage va de 4 à 80 44 176 kilo.
- **Espace libre minimal à conserver (Ko)** : précise l'espace libre minimal à conserver dans la mémoire flash (en Ko). La plage va de 0 à 8044176 Ko.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Activer les destinations de la journalisation

Vous devez activer une destination de journalisation pour voir les messages à cette destination. Lors de l'activation d'une destination, vous devez également préciser le filtre de messages pour la destination.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 47.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Logging Destinations** (destinations de journalisation Syslog).

Étape 3 Cliquez sur **Add** (ajouter) pour activer une destination et appliquer un filtre de journalisation, ou modifiez une destination existante.

Étape 4 Dans la boîte de dialogue **Logging Destinations** (destination de journalisation), sélectionnez une destination et configurez le filtre à utiliser pour une destination :

a) Choisissez la destination que vous activez dans la liste déroulante **Logging Destination** (Destination de journalisation). Vous pouvez créer un filtre par destination : de console, de courriel, de tampon interne, de déroutement SNMP, de sessions SSH et de serveurs Syslog.

Remarque La journalisation de la console et des sessions SSH ne fonctionne que dans l'interface de commande en ligne de dépistage. Entrez **system support diagnostic-cli**.

b) Dans **Event Class**, (Classe d'événements) choisissez le filtre qui s'appliquera à toutes les classes non répertoriées dans le tableau.

Vous pouvez configurer ces filtres :

- **Filter on severity**(filtre en fonction de la gravité) : sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés à la destination
- **Use Event List** (utiliser la liste d'événements) : sélectionnez la liste d'événements qui définit le filtre. Vous créez ces listes sur la page **Event Lists** (listes d'événements).
- **Disable Logging** (Désactiver la journalisation) : empêche l'envoi des messages à cette destination.

c) Si vous souhaitez créer des filtres par classe d'événement, cliquez sur **Add** (ajouter) pour créer un nouveau filtre ou modifiez un filtre existant et sélectionnez la classe d'événement et le niveau de gravité pour limiter les messages dans cette classe. Cliquez sur **OK** pour enregistrer le filtre.

Pour obtenir une explication des classes d'événements, consultez Classe de messages Syslog, à la page 42.

d) Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Envoyer des messages Syslog à une adresse courriel

Vous pouvez configurer une liste de destinataires des messages syslog à envoyer sous forme de courriel.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 47.

Avant de commencer

- Configurez un serveur SMTP dans la page des paramètres de la plateforme du serveur SMTP.
- Activer la journalisation et configurer les paramètres de base, à la page 47
- Activer les destinations de la journalisation

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Email Setup** (configuration de la messagerie Syslog).

Étape 3 Spécifiez l'adresse de courriel utilisée comme adresse source pour les messages syslog envoyés comme courriels.

Étape 4 Cliquez sur **Add** (ajouter) pour saisir la nouvelle adresse de courriel des messages syslog précisés.

Étape 5 Choisissez le niveau de gravité des messages syslog qui sont envoyés au destinataire dans la liste déroulante.

Le filtre de gravité des messages syslog utilisé pour l'adresse de courriel de destination entraîne l'envoi des messages du niveau de gravité spécifié et du niveau supérieur. Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 40.

Étape 6 Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Créer une liste d'événements personnalisée

Une liste d'événements est un filtre personnalisé que vous pouvez appliquer à une destination de journalisation pour contrôler les messages envoyés à la destination. Normalement, vous filtrez les messages pour une destination donnée uniquement en fonction de la gravité, mais vous pouvez utiliser une liste d'événements pour affiner les messages envoyés en fonction d'une combinaison de classe d'événement, de gravité et d'identifiant de message (ID).

La création d'une liste d'événements personnalisée est un processus en deux étapes. Vous créez une liste personnalisée dans la liste d'**événements**, puis vous utilisez cette dernière pour définir le filtre de journalisation pour les différents types de destination, dans le champ **Logging Destinations** (Destinations de la journalisation).

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 47.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Events List** (liste des événements Syslog).

Étape 3 Configurez une liste d'événements.

a) Cliquez sur **Add** pour ajouter une nouvelle liste, ou modifiez une liste existante.

b) Saisissez un nom pour la liste d'événements dans le champ **Name** (Nom). Les espaces ne sont pas autorisées

c) Pour identifier les messages en fonction de la gravité ou de la classe d'événement, sélectionnez l'onglet **Severity/Event Class** (classe de gravité/événement) et ajoutez ou modifiez des entrées.

Pour en savoir plus sur les classes disponibles, consultez Classe de messages Syslog, à la page 42.

Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 40.

Certaines classes d'événements ne sont pas applicables au périphérique en mode transparent. Si de telles options sont configurées, elles seront contournées et ne seront pas déployées.

d) Pour identifier les messages spécifiquement par l'ID du message, sélectionnez l' **ID du message** et ajoutez ou modifiez les ID.

Vous pouvez saisir une plage d'ID en utilisant un tiret, par exemple 100000-200000. Les identifiants comportent six chiffres. Pour en savoir plus sur la façon dont les trois premiers chiffres sont mappés aux entités, consultez Classe de messages Syslog, à la page 42.

Pour connaître les numéros des messages, consultez la section la Messages Syslog de Cisco ASA.

e) Cliquez sur **OK** pour enregistrer la liste d'événements.

Étape 4 Cliquez sur **Logging Destinations** (Destinations de la journalisation) et ajoutez ou modifiez la destination qui doit utiliser le filtre.

Consultez Activer les destinations de la journalisation, à la page 49.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Limiter le débit de génération des messages Syslog

Vous pouvez limiter la fréquence à laquelle les messages Syslog sont générés par niveau de gravité ou ID de message. Vous pouvez spécifier des limites individuelles pour chaque niveau de journalisation et chaque ID de message Syslog. Si les paramètres entrent en conflit, les limites d'ID de message Syslog prévalent.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 47.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Rate Limit (Limitation du débit)**.

Étape 3 Pour limiter la génération de messages par niveau de gravité, cliquez sur **Logging Level** > **Add** (ajouter un niveau de journalisation) et configurez les options suivantes :

- **Niveau de journalisation** : le niveau de gravité pour lequel vous limitez le débit. Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 40.
- S**Nombre de messages** : nombre maximal de messages du type spécifié autorisé dans la période spécifiée.
- **Intervalle** : nombre de secondes avant que le compteur de limite de débit ne soit réinitialisé.

Étape 4 Cliquez sur **OK**.

Étape 5 Pour limiter la génération de messages par ID de message Syslog, cliquez sur **Syslog Level** > **Add** (ajouter un niveau Syslog) et configurez les options suivantes :

- **Syslog ID** : L'ID du message syslog pour lequel vous êtes en train de limiter le débit. Pour connaître les numéros des messages, consultez la section la Messages Syslog de Cisco ASA.
- S**Nombre de messages** : nombre maximal de messages du type spécifié autorisé dans la période spécifiée.
- **Intervalle** : nombre de secondes avant que le compteur de limite de débit ne soit réinitialisé.

Étape 6 Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les paramètres Syslog

Vous pouvez configurer les paramètres généraux du journal système pour définir le code de fonction à inclure dans les messages syslog qui sont envoyés aux serveurs de journal système, préciser si un horodatage est inclus dans chaque message, préciser l'ID de périphérique à inclure dans les messages, afficher et modifier les niveaux de gravité pour et désactiver la génération de messages spécifiques.

Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et de prévention des intrusions), certains paramètres sur cette page ne s'appliquent pas à ces messages. Consultez la section *Paramètres de la plateforme de défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité* dans Guide d'administration Cisco Secure Firewall Management Center.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Syslog Settings** (paramètres du journal système).

Étape 3 Dans la liste déroulante **Facility** (Facilité), sélectionnez un système de journalisation pour les serveurs syslog à utiliser comme base pour classer les messages.

La valeur par défaut est LOCAL4(20), ce qui est attendu de la plupart des systèmes UNIX. Cependant, comme vos périphériques réseau partagent les installations disponibles, vous devrez peut-être modifier cette valeur pour les journaux système.

Les valeurs de Facilité ne sont généralement pas pertinentes pour les événements de sécurité.

Étape 4 Cochez la case **Enable timestamp on each syslog message** (Activer l'horodatage de chaque message syslog) pour inclure la date et l'heure auxquelles un message a été généré dans le message syslog.

Étape 5 Sélectionnez le **format d'horodatage** pour le message syslog :

- Le format existant (MMM jj aaaa HH:mm:ss) est le format par défaut des messages syslog.

  Lorsque ce format d'horodatage est sélectionné, les messages n'indiquent pas le fuseau horaire, qui est toujours l'heure UTC.

- La RFC 5424 (aaaa-MM-jjTHH:mm:ssZ) utilise le format d'horodatage ISO 8601 comme spécifié dans le format de journal système RFC 5424.

  Si vous sélectionnez le format RFC 5424, un « Z » est ajouté à la fin de chaque horodatage pour indiquer que l'horodatage utilise le fuseau horaire UTC.

Étape 6 Si vous souhaitez ajouter un identifiant d'appareil aux messages du journal système (qui est placé au début du message), cochez la case **Enable Syslog Device ID** (activer l'ID d'appareil syslog), puis sélectionnez le type d'ID.

- **Interface** : pour utiliser l'adresse IP de l'interface sélectionnée, quelle que soit l'interface par laquelle le périphérique envoie le message. Sélectionnez la zone de sécurité qui identifie l'interface. La zone doit correspondre à une seule interface.
- **ID défini par l'utilisateur** : pour utiliser une chaîne de texte (jusqu'à 16 caractères) de votre choix.
- **Nom d'hôte** : permet de sélectionner le nom d'hôte de ce périphérique.

Étape 7 Utilisez le tableau Syslog Message pour modifier les paramètres par défaut des messages syslog spécifiques. Vous devez configurer les règles dans ce tableau uniquement si vous souhaitez modifier les paramètres par défaut. Vous pouvez modifier la gravité attribuée à un message ou vous pouvez désactiver la génération d'un message.

Par défaut, Netflow est activé et les entrées sont affichées dans le tableau.

a) Pour supprimer les messages syslog redondants en raison de Netflow, sélectionnez **Netflow Equivalent Syslogs** (Syslogs équivalents à Netflow).

   Cela ajoute les messages au tableau en tant que messages supprimés.

   Remarque Si l'un de ces équivalents syslog se trouve déjà dans le tableau, vos règles existantes ne sont pas remplacées.

b) Pour ajouter une règle, cliquez sur **Add** (Ajouter).
c) Sélectionnez le numéro du message dont vous souhaitez modifier la configuration dans la liste déroulante **Syslog ID** (ID Syslog), puis sélectionnez le nouveau niveau de gravité dans la liste déroulante **Logging Level** (Niveau de journalisation), ou sélectionnez **Supprimé** pour désactiver la génération du message. En règle générale, vous ne modifiez pas le niveau de gravité et ne désactivez pas le message, mais vous pouvez apporter des modifications aux deux champs si vous le souhaitez.
d) Cliquez sur **OK** pour ajouter la règle au tableau.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Prochaine étape

- Déployer les changements de configuration.

Configurer un serveur Syslog

Pour configurer un serveur syslog afin de gérer les messages générés par votre système, procédez comme suit.

Si vous souhaitez que ce serveur de journal système reçoive les événements de sécurité tels que les événements de connexion et d'intrusions, consultez également Paramètres de plateforme Défense contre les menaces qui s’appliquent aux messages du journal des événements de sécurité, à la page 47.

Avant de commencer

- Voir les exigences dans Lignes directrices relatives à la journalisation, à la page 45.
- Vérifiez que vos périphériques peuvent atteindre votre collecteur syslog sur le réseau.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Syslog Server**(Serveur syslog).

Étape 3 Cochez la case **Allow user traffic to pass when TCP syslog server is down (Recommended) (autoriser le trafic à passer lorsque le serveur TCP syslog est en panne (recommandé))** pour autoriser le trafic si un serveur syslog qui utilise le protocole TCP est en panne.

Remarque
- Par défaut, cette option est activée. Sauf si nécessaire, nous vous recommandons d’autoriser les connexions via le périphérique de défense contre les menaces lorsque le serveur syslog TCP externe est inaccessible pour le périphérique.
- Lorsque l’option **Autoriser le trafic utilisateur à passer lorsque le serveur de syslog TCP est en panne** est désactivée dans centre de gestion version 6.2.x ou une version antérieure, son état persiste même après la mise à niveau vers la version 6.3 ou ultérieure. Assurez-vous de l’activer manuellement.
- Lorsque cette option est désactivée et que plusieurs serveurs syslog TCP sont configurés dans le périphérique, le trafic de l’utilisateur est autorisé à passer si au moins un des serveurs est accessible par le périphérique de défense contre les menaces. Par conséquent, l’option désactivé n’est appliquée que lorsqu’aucun des serveurs syslog TCP configurés dans le périphérique n’est accessible. Le périphérique génère le journal système suivant, qui décrit la cause première du trafic refusé qui passe par le périphérique :

  ```
  %FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. Les
  nouvelles connexions sont refusées en fonction de la politique de journalisation
  allow-hostdown
  ```

Étape 4 Dans le champ **Message queue size (messages)**, saisissez une taille de file d’attente pour le stockage des messages syslog sur le périphérique de sécurité lorsque le serveur syslog est occupé. Le minimum est de 1 message. La valeur par défaut est 512. Précisez 0 pour permettre la mise en file d’attente d’un nombre illimité de messages (en fonction de la mémoire de bloc disponible).

Lorsque les messages dépassent la taille de la file d’attente configurée, ils sont abandonnés et entraînent l’absence du journal système. Pour déterminer la taille idéale de file d’attente, vous devez identifier la mémoire de blocs disponible. Utilisez la commande **showblocks** pour connaître l’utilisation actuelle de la mémoire.

Pour en savoir plus sur la commande et ses attributs, consultez *le Guide de référence des commandes Cisco Secure Firewall ASA*. Pour obtenir de l'aide, communiquez avec le centre d'assistance technique de Cisco (Cisco TAC).

Étape 5 Pour ajouter un nouveau serveur syslog, cliquez sur **Add** (Ajouter).

a) Dans la liste déroulante **IP Address** (adresse IP), sélectionnez un objet hôte réseau qui contient l'adresse IP du serveur Syslog.

b) Choisissez le protocole (TCP ou UDP) et saisissez le numéro de port pour les communications entre le périphérique défense contre les menaces et le serveur Syslog.

UDP est plus rapide et utilise moins de ressources sur le périphérique que TCP.

Le port par défaut pour UDP est 514. Vous devez configurer manuellement le port 1470 pour le protocole TCP. Les valeurs de port valides autres que les valeurs par défaut sont comprises entre 1025 et 65535, pour l'un ou l'autre de ces protocoles.

c) Cochez la case **Log messages in Cisco EMBLEM format (UDP only)** (enregistrer les messages au format Cisco EMBLEM (UDP uniquement)) pour indiquer s'il faut consigner les messages au format Cisco EMBLEM (disponible uniquement si UDP est sélectionné comme protocole).

Remarque Les messages syslog au format RFC5424 affichent généralement la valeur de priorité (PRI). Cependant, dans centre de gestion, ce n'est que lorsque vous activez la journalisation au format Cisco EMBLEM, que la valeur PRI dans les messages syslog du défense contre les menaces géré s'affiche. Pour en savoir plus sur PRI, consultez RFC5424.

d) Cochez la case **Enable Secure Syslog** (activer Syslog sécurisé) pour chiffrer la connexion entre le périphérique et le serveur à l'aide de SSL/TLS sur TCP.

Remarque Vous devez sélectionner TCP comme protocole et une valeur de port comprise entre 1 025 et 65535 pour utiliser cette option. Vous devez également téléverser le certificat requis pour communiquer avec le serveur syslog sur la page **Devices (Périphériques)** > **Certificates** (Certificats). Enfin, téléversez le certificat du périphérique défense contre les menaces vers le serveur syslog pour mettre en place la relation sécurisée et lui permettre de déchiffrer le trafic. L'option **Enable Secure Syslog** (Activer Syslog sécurisé) n'est pas prise en charge sur l'interface de gestion du périphérique.

e) Sélectionnez **Interface de gestion de périphériques**, **les zones de sécurité ou interfaces nommées** pour communiquer avec le serveur Syslog.

- **Device Management Interface** (Interface de gestion de périphériques) : envoie des journaux système à partir de l'interface de gestion. Nous vous recommandons d'utiliser cette option lors de la configuration de syslog sur les événements Snort.

  Remarque L'option **Device Management Interface** (interface de gestion de périphériques) ne prend pas en charge l'option **Enable Secure Syslog** (Activer Syslog sécurisé).

- **Zones de sécurité ou interfaces nommées** : sélectionnez les interfaces dans la liste des **zones disponibles** et cliquez sur **Add** (Ajouter).

  Important Les messages syslog du plan de données défense contre les menaces (Lina) ne peuvent pas être envoyés via l'interface de dépistage. Configurez les autres interfaces ou l'interface de gestion (Br1/Management0) pour envoyer les messages syslog du plan de données.

f) Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Prochaine étape

- Déployer les changements de configuration.

Délai d'expiration

Vous pouvez définir les durées d'inactivité globales pour la connexion et les intervalles de traduction de divers protocoles. Si l'emplacement n'a pas été utilisé pendant la durée d'inactivité spécifiée, la ressource est remise dans le groupement (pool) libre.

Vous pouvez également définir un délai d'expiration pour les sessions de console avec le périphérique.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Délais d'expiration**.

Étape 3 Configurez les délais d'expiration que vous souhaitez modifier.

Pour un paramètre donné, sélectionnez **Personnalisé** pour définir votre valeur, **Par défaut** pour revenir à la valeur par défaut du système. Dans la plupart des cas, le délai d'expiration maximal est de 1193 heures.

Vous pouvez désactiver certains délais d'expiration en sélectionnant **Disable** (désactiver).

- **Console Timeout**(délai d'expiration de la console) : le temps d'inactivité avant la fermeture d'une connexion à la console. Il s'agit d'une plage ou de 5 à 1 440 minutes. La valeur par défaut est 0, ce qui signifie que la session n'expire pas. Si vous modifiez la valeur, les sessions de console existantes utilisent l'ancienne valeur de délai d'expiration. La nouvelle valeur s'applique uniquement aux nouvelles connexions.
- **Intervalle de traduction (xlate)**—le temps d'inactivité jusqu'à ce qu'un intervalle de traduction NAT soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est de 3 heures.
- **Connection (Conn)**—Le temps d'inactivité jusqu'à ce qu'un emplacement de connexion soit libéré. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 1 heure.
- **Half-Closed**—Le temps d'inactivité jusqu'à la fermeture d'une connexion TCP semi-fermée. Une connexion est considérée comme à moitié fermée si FIN et FIN-ACK ont été vus. Si seul le FIN a été vu, le délai d'expiration de connexion normal s'applique. La durée minimale est de 30 secondes. La valeur par défaut est 10 minutes.
- **UDP**—le temps d'inactivité avant la fermeture d'une connexion UDP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes.
- **ICMP**—le temps d'inactivité après lequel les états ICMP généraux sont fermés. La valeur par défaut et minimale est de 2 secondes.

- **RPC/Sun RPC**—le temps d'inactivité jusqu'à ce qu'un emplacement SunRPC soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 10 minutes.

  Dans une connexion basée sur les appels RPC Sun, lorsque la connexion parente est supprimée ou a expiré, une nouvelle connexion enfant peut ne pas être considérée comme faisant partie de la connexion parent-enfant et, par conséquent, la nouvelle connexion peut être évaluée conformément à la politique ou règles définies dans le système. Après l'expiration de la connexion parente, les connexions enfant existantes ne sont valides que jusqu'à ce que la valeur de délai d'expiration définie soit atteinte.

- **H.225**—le temps d'inactivité avant la fermeture d'une connexion de signalisation H.225. La valeur par défaut est de 1 heure. Pour fermer une connexion immédiatement après l'élimination de tous les appels, un délai d'expiration de 1 seconde (0:0:1) est recommandé.

- **H.323**—le temps d'inactivité après lequel les connexions multimédias H.245 (TCP) et H.323 (UDP) sont fermées. La valeur par défaut est et minimale est de 5 minutes. Comme le même indicateur de connexion est défini sur les connexions multimédias H.245 et H.323, la connexion H.245 (TCP) partage le délai d'inactivité avec la connexion multimédia H.323 (RTP et RTCP).

- **SIP**—le temps d'inactivité avant la fermeture d'une connexion de port de signalisation SIP. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 30 minutes.

- **SIP Media**—le temps d'inactivité avant la fermeture d'une connexion de port de support SIP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes. La minuterie de médias SIP est utilisée pour les paquets de médias SIP RTP/RTCP avec SIP UDP, plutôt que le délai d'inactivité d'UDP.

- **SIP Disconnect**—le temps d'inactivité après lequel la session SIP est supprimée si 200 OK n'est pas reçu pour un message CANCEL ou BYE, entre 0:0:1 et 0:10:0. La valeur par défaut est 2 minutes. (0:2:0)

- **SIP Invite**—le temps d'inactivité après lequel les pinholes pour les réponses PROVISOIRES et les xlates de médias seront fermés, entre 0:1:0 et 00:30:0. La valeur par défaut est de 3 minutes. (0:3:0).

- **SIP Provisional Media**—la valeur du délai d'expiration pour les connexions multimédias provisoires SIP, entre 1 et 30 minutes. La valeur par défaut est 2 minutes.

- **Floating Connection**—Lorsqu'il existe plusieurs routes vers un réseau avec différentes métriques, le système utilise celle ayant la meilleure métrique au moment de la création de la connexion. Si un meilleur routage devient disponible, ce délai d'expiration permet de fermer les connexions afin qu'une connexion puisse être rétablie pour utiliser le meilleur routage. La valeur par défaut est 0 (la connexion n'expire jamais). Pour permettre d'utiliser de meilleures routes, définissez le délai d'expiration à une valeur comprise entre 0:0:30 et 1193:0:0.

- **Xlate PAT**—Le temps d'inactivité jusqu'à ce qu'un intervalle de traduction PAT soit libéré, entre 0:0:30 et 0:5:0. La valeur par défaut est de 30 secondes. Vous pourriez souhaiter augmenter le délai d'expiration si les routeurs en amont rejettent les nouvelles connexions utilisant un port PAT libéré, car la connexion précédente pourrait toujours être ouverte sur le périphérique en amont.

- **TCP Proxy Reassembly**—le délai d'inactivité après lequel les paquets en mémoire tampon en attente de réassemblage sont abandonnés, entre 0:0:10 et 1193:0:0. La valeur par défaut est de 1 minute (0:1:0).

- **ARP Timeout** : délai d'expiration ARP, le nombre de secondes entre les recompilations de la table ARP, de 60 à 42 94967. La valeur par défaut est de 14 400 secondes (4 heures).

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Synchronisation du temps

Utilisez un serveur NTP (Network Time Protocol) pour synchroniser les paramètres de l'horloge sur vos périphériques. Nous vous recommandons de configurer tous les défense contre les menaces gérés par un centre de gestion pour utiliser le même serveur NTP que centre de gestion. Le défense contre les menaces obtient son heure directement à partir du serveur NTP configuré. Si les serveurs NTP configurés de défense contre les menaces ne sont pas accessibles pour une raison quelconque, il synchronise l'heure avec celle de centre de gestion.

Le périphérique prend en charge NTPv4.

Remarque Si vous déployez défense contre les menaces sur les châssis Firepower 4100/9300, vous devez configurer NTP sur les châssis Firepower 4100/9300 pour que les licences Smart fonctionnent correctement et pour que les horodatages soient corrects sur les enregistrements des périphériques. Vous devez utiliser le même serveur NTP pour les châssis Firepower 4100/9300 et centre de gestion.

Avant de commencer

- Si votre entreprise dispose d'un ou de plusieurs serveurs NTP que votre défense contre les menaces peut atteindre, utilisez le même serveur ou les serveurs NTP pour vos périphériques que vous avez configurés pour la synchronisation de l'heure sur la page **Système > Configuration** sur votre centre de gestion.
- Si vous avez sélectionné **Utiliser le serveur NTP authentifié uniquement** lors de la configuration du ou des serveurs NTP pour centre de gestion, utilisez uniquement le ou les serveurs NTP configurés pour s'authentifier avec centre de gestion] pour vos périphériques. (Les périphériques gérés utiliseront les mêmes serveurs NTP que centre de gestion, mais leurs connexions NTP n'utiliseront pas l'authentification.)
- Si votre périphérique ne peut pas atteindre un serveur NTP ou si votre entreprise n'en a pas, vous devez utiliser l'option **Via le NTP de Defense Center** comme indiqué dans la procédure suivante.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez la **Synchronisation de l'heure**.

Étape 3 Configurez l'une des options d'horloge suivantes :

- **Via NTP du Defense Center** : (option par défaut). Le périphérique géré obtient l'heure des serveurs NTP que vous avez configurés pour le centre de gestion (à l'exception des serveurs NTP authentifiés) et synchronise directement l'heure avec ces serveurs. Toutefois, si l'une des conditions suivantes est vraie, le périphérique géré synchronise l'heure à partir de centre de gestion :
  - Les serveurs NTP de centre de gestionne sont pas accessibles par le périphérique.

- Le centre de gestion n’a aucun serveur non authentifié.

- **Via NTP de** : si votre centre de gestion utilise des serveurs NTP sur le réseau, sélectionnez cette option et saisissez le nom DNS complet (comme ntp.exemple.com) ou l'adresse IPv4 ou IPv6 des serveurs NTP que vous avez spécifiés. Dans **Système > Configuration > Synchronisation de l’heure**. Si les serveurs NTP ne sont pas accessibles, le centre de gestion sert de serveur NTP.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Fuseau horaire

Par défaut, le système utilise le fuseau horaire UTC. Pour désigner un fuseau horaire différent pour un périphérique, utilisez cette procédure.

Le fuseau horaire que vous spécifiez sera utilisé uniquement pour l’application horaire de la politique dans les politiques qui prennent en charge cette fonctionnalité.

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.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme)** et créez ou modifiez la politique défense contre les menaces .

Vous pouvez également créer des objets de fuseau horaire à partir de la page **Objects > Object Management > Time Zone** (Objets > Gestion des objets > Fuseau horaire).

Étape 2 Créez un nouvel objet de fuseau horaire en cliquant sur le signe plus **(+)**.

Étape 3 Sélectionnez le fuseau horaire

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Créez des objets de plage temporelle, sélectionnez les plages de temps applicables dans les règles de contrôle d’accès et de préfiltre, et affectez les politiques parentes aux périphériques associés au fuseau horaire correct.

- Déployer les changements de configuration.

Conformité UCAPL/CC

Pour plus d'informations sur ce paramètre et comment l'activer pour centre de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center.

Mise en garde Après avoir activé ce paramètre, vous ne pouvez pas le désactiver. Si vous devez sortir le périphérique du mode CC ou UCAPL, vous devez effectuer une réinitialisation de l'image.

Avant de commencer

- Les périphériques Cisco Secure Firewall Threat Defense ne peuvent pas utiliser de licence d'évaluation; votre Smart Software Manager compte doit être activé pour les fonctionnalités contrôlées par l'exportation.
- Les périphériques Cisco Secure Firewall Threat Defense doivent être déployés en mode routé.
- Vous devez être un utilisateur administrateur pour effectuer cette tâche.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **UCAPL/CC Compliance** (Conformité UCAPL/CC).

Étape 3 Pour activer *en permanence* la conformité des certifications de sécurité sur le périphérique, vous avez deux choix :

- Pour activer la conformité aux certifications de sécurité en mode Common Criteria (Critère commun), choisissez **CC** dans la liste déroulante.
- Pour activer la conformité aux certifications de sécurité en mode de liste des produits approuvés pour les capacités unifiées, choisissez **UCAPL** dans la liste déroulante.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Profil de rendement

Le profil de rendement détermine l'affectation des cœurs de CPU du périphérique à deux des principaux processus du système : le plan de données (Lina) et Snort. Le plan de données gère les connexions VPN, le routage et les autres traitements de base des couches 3 et 4. Snort fournit une inspection avancée, y compris la prévention des intrusions et des programmes malveillants, le filtrage d'URL, le filtrage d'applications et d'autres fonctionnalités qui nécessitent une inspection approfondie des paquets.

Si vous utilisez un équilibre entre les fonctionnalités de base et les fonctionnalités avancées, ne modifiez pas le profil de rendement. Le système est conçu pour fournir une affectation équilibrée de cœurs à ces processus. L'affectation diffère en fonction du modèle de matériel.

Toutefois, si vous utilisez le périphérique principalement pour le VPN, ou pour l'intrusion et d'autres inspections avancées, vous pouvez fausser le profil de rendements de sorte que plus de cœurs sont affectés aux fonctionnalités les plus utilisées. Cela pourrait améliorer les performances du système.

Avant de commencer

- Ces paramètres s'appliquent uniquement aux systèmes exécutant la version 7.3+.
- Le profil de rendement est pris en charge sur les types de périphériques suivants :
  - Firepower 4100/9300
  - Cisco Secure Firewall Threat Defense Virtual
- La modification du profil de rendement n'est pas prise en charge sur les unités d'une grappe ou d'un groupe à haute disponibilité, ou sur celles configurées pour des instances multiples. Le déploiement est bloqué si vous affectez le profil à autre chose qu'à des périphériques autonomes.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Profil de rendement**.

Étape 3 Sélectionner un profil :

- **Par défaut** : Il s'agit du paramètre recommandé et de la meilleure option si vous configurez à la fois le VPN et l'inspection de prévention des intrusions.
- **VPN lourd avec chemin de préfiltre fastpath :**si vous utilisez principalement le périphérique comme point terminal ou tête de réseau VPN et que vous configurez des règles dans la politique de préfiltre pour faire passer le trafic VPN en mode accéléré, vous pouvez choisir cette option pour affecter la majorité des cœurs de CPU au plan de données. L'allocation est de 90 % de plan de données et 10 % de Snort.
- **VPN lourd avec inspection** : si vous utilisez principalement le périphérique comme point terminal VPN ou tête de ligne, mais que vous n'utilisez pas la politique de préfiltre pour accélérer le trafic VPN, vous pouvez choisir cette option pour affecter la majorité des cœurs de CPU au plan de données. Cette option suppose que vous laissez l'inspection de prévention des intrusions, le filtrage d'URL et d'autres fonctions avancées qui utilisent Snort sur un autre appareil du réseau. L'allocation est de 60 % de plan de données et 40 % de Snort.
- **IPS lourd** : si vous ne configurez pas de VPN, mais que vous utilisez le périphérique pour la prévention des intrusions, vous pouvez choisir cette option pour affecter la majorité du cœur de CPU au processus Snort. L'allocation est de 30 % de plan de données, 70 % de Snort.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Déployez la politique

Étape 6 Une fois le déploiement terminé, vous devez redémarrer chaque périphérique concerné pour que les nouvelles affectations de cœurs puissent être effectuées.

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.