System Settings (paramètres système)

Les rubriques suivantes expliquent comment configurer les différents paramètres système qui sont regroupés sur la page Paramètres système. Les paramètres couvrent le fonctionnement global du système.

Configurer l'accès de gestion

L'accès de gestion fait référence à la capacité de se connecter au périphérique Cisco Firewall Threat Defense à des fins de configuration et de surveillance. Vous pouvez configurer les éléments suivants :

- AAA pour identifier la source d'identité à utiliser pour authentifier l'accès des utilisateurs. Vous pouvez utiliser la base de données d'utilisateurs locale ou un serveur AAA externe. Pour plus d'informations sur la gestion des utilisateurs administratifs, consultez Gestion de Firewall Device Manager et accès des utilisateurs Firewall Threat Defense.
- Contrôle d'accès à l'interface de gestion et aux interfaces de données. Il existe des listes d'accès distinctes pour ces interfaces. Vous pouvez décider quelles adresses IP sont autorisées pour HTTPS (utilisé pour le Firepower Device Manager) et SSH (utilisé pour l'interface de ligne de commande). Consultez Configuration de la liste d'accès de gestion, à la page 2.

- Le certificat du serveur Web de gestion, que les utilisateurs doivent accepter pour se connecter à Firepower Device Manager. En chargeant un certificat auquel vos navigateurs Web font déjà confiance, vous évitez de demander aux utilisateurs d'approuver un certificat inconnu. Consultez Configuration du certificat du serveur Web Firewall Threat Defense, à la page 4.

Configuration de la liste d'accès de gestion

Par défaut, vous pouvez atteindre les interfaces Web ou de l'interface de ligne de commande Firepower Device Manager de l'appareil sur l'adresse de gestion à partir de n'importe quelle adresse IP. L'accès au système est protégé uniquement par un nom d'utilisateur et un mot de passe. Cependant, vous pouvez configurer une liste d'accès pour autoriser les connexions à partir d'adresses IP ou de sous-réseaux spécifiques uniquement pour fournir un autre niveau de protection.

Vous pouvez également ouvrir des interfaces de données pour permettre les connexions Firepower Device Manager ou de SSH à l'interface de ligne de commande. Vous pouvez ensuite gérer l'appareil sans utiliser l'adresse de gestion. Par exemple, vous pouvez autoriser l'accès de gestion à l'interface externe, afin de pouvoir configurer le périphérique à distance. Le nom d'utilisateur et le mot de passe offre une protection contre les connexions indésirables. Par défaut, l'accès de gestion HTTPS aux interfaces de données est activé sur l'interface interne, mais désactivé sur l'interface externe. Pour le Firepower 1010 qui possède un groupe de ponts « intérieur » par défaut, cela signifie que vous pouvez effectuer les connexions de Firepower Device Manager au moyen de n'importe quelle interface de données au sein du groupe de ponts vers l'adresse IP du groupe de pont (par défaut 192.168.95.1). Vous pouvez ouvrir une connexion de gestion uniquement sur l'interface au moyen de laquelle vous accédez à l'appareil.

⚠

Mise en garde Si vous limitez l'accès à des adresses spécifiques, vous pouvez facilement vous exclure du système. Si vous supprimez l'accès pour l'adresse IP que vous utilisez actuellement et qu'il n'y a aucune entrée pour n'importe quelle adresse, vous perdrez l'accès au système lorsque vous déploierez la politique. Soyez très prudent si vous décidez de configurer la liste d'accès.

Avant de commencer

Vous ne pouvez pas configurer à la fois l'accès (accès HTTPS) Firepower Device Manager et le VPN SSL d'accès à distance AnyConnect 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 configurez les deux fonctionnalités sur la même interface, veillez à modifier le port HTTPS d'au moins l'un de ces services pour éviter un conflit.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur le lien **System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access (accès de gestion)** dans la table des matières.

Vous pouvez également configurer AAA sur cette page pour autoriser l'accès de la gestion aux utilisateurs définis dans un serveur AAA externe. Pour de plus amples renseignements, consultez la section Gestion de Firewall Device Manager et accès des utilisateurs Firewall Threat Defense.

Étape 2 Pour créer des règles pour l'adresse de gestion :

a) Sélectionnez l'onglet **Management Interface** (interface de gestion).

La liste des règles définit quelles adresses sont autorisées à accéder au port indiqué : 443 pour le Firepower Device Manager (l'interface Web HTTPS), 22 pour l'interface de ligne de commande SSH.

Les règles ne composent pas une liste ordonnée. Si une adresse IP correspond à une règle du port demandé, l'utilisateur est autorisé à tenter de se connecter au périphérique.

Remarque

Pour supprimer une règle, cliquez sur l'icône de la corbeille ( ) de la règle. Si vous supprimez toutes les règles d'un protocole, personne ne pourra accéder au périphérique sur cette interface à l'aide du protocole.

b) Cliquez sur + et complétez les options suivantes :

- **Protocol** (protocole) : Précisez si la règle est pour HTTPS (port 443) ou SSH (port 22).
- **IP Address** (adresse IP) : Sélectionnez l'objet réseau qui définit le réseau ou l'hôte IPv4 ou IPv6 qui devrait pouvoir accéder au système. Pour spécifier la sélection de « toute » adresse, sélectionnez **any-ipv4** (0.0.0.0/0) et **any-ipv6** (::/0).

c) Cliquez sur **OK**.

Étape 3 Pour créer des règles pour les interfaces de données :

a) Sélectionnez l'onglet **Data Interfaces** (interfaces de données).

La liste des règles définit quelles adresses sont autorisées à accéder au port indiqué sur l'interface : 443 pour le Firepower Device Manager (l'interface Web HTTPS), 22 pour l'interface de ligne de commande SSH.

Les règles ne composent pas une liste ordonnée. Si une adresse IP correspond à une règle du port demandé, l'utilisateur est autorisé à tenter de se connecter au périphérique.

Remarque

Pour supprimer une règle, cliquez sur l'icône de la corbeille ( ) de la règle. Si vous supprimez toutes les règles d'un protocole, personne ne pourra accéder au périphérique sur cette interface à l'aide du protocole.

b) Cliquez sur + et complétez les options suivantes :

- **Interface** : Sélectionnez l'interface sur laquelle vous souhaitez autoriser l'accès de gestion.
- **Protocols** (protocoles) : Précisez si la règle est pour HTTPS (port 443), pour SSH (port 22) ou les deux. Vous ne pouvez pas configurer les règles HTTPS pour l'interface externe si elle est utilisée dans un profil de connexion VPN d'accès distant.
- **Allowed Networks (réseaux permis)** : Sélectionnez les objets réseau qui définissent le réseau ou l'hôte IPv4 ou IPv6 qui devrait pouvoir accéder au système. Pour spécifier la sélection de « toute » adresse, sélectionnez **any-ipv4** (0.0.0.0/0) et **any-ipv6** (::/0).

c) (Facultatif) Si vous souhaitez modifier le numéro de port de données HTTPS, cliquez sur le numéro et entrez un nouveau port. Consultez Configuration du port HTTPS pour l'accès de gestion sur les interfaces de données, à la page 4

d) Cliquez sur **OK**.

Configuration du port HTTPS pour l'accès de gestion sur les interfaces de données

Par défaut, l'accès à l'appareil à des fins de gestion, que ce soit pour le Firepower Device Manager ou l'API Firewall Threat Defense, se fait au moyen du port TCP/443. Vous pouvez modifier le port d'accès de gestion pour les interfaces de données.

Si vous modifiez le port, les utilisateurs doivent inclure le port personnalisé sur l'URL pour accéder au système. Par exemple, si l'interface de données est ftd.exemple.com et que vous changez le port pour 4443, les utilisateurs doivent modifier l'URL en https://ftd.exemple.com :4443.

Toutes les interfaces de données utiliseront le même port. Vous ne pouvez pas configurer différents ports par interface.

Remarque Vous ne pouvez pas modifier le port d'accès de gestion pour l'interface de gestion. L'interface de gestion utilise toujours le port 443.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien**System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **Data Interfaces** (interfaces de données).

Étape 3 Cliquez sur le numéro de port de données HTTPS (**HTTPS Data Port**).

Étape 4 Dans la boîte de dialogue Data Interfaces Setting, remplacez le port de données HTTPS (**HTTPS Data Port**) par celui que vous souhaitez utiliser.

Vous ne pouvez pas indiquer les numéros suivants :

- Le numéro 22, car il est utilisé pour les connexions SSH.
- Le port utilisé pour le VPN d'accès distant, si vous l'avez configuré pour n'importe quelle interface que vous autorisez également pour l'accès de gestion. Le VPN d'accès à distance utilise le port 443 par défaut, mais vous pouvez configurer un port personnalisé pour ce port.
- Le port utilisé pour l'authentification active dans la politique d'identité, qui est 885 par défaut.

Étape 5 Cliquez sur **OK**.

Configuration du certificat du serveur Web Firewall Threat Defense

Lorsque vous vous connectez à l'interface Web, le système utilise un certificat numérique pour sécuriser les communications via HTTPS. Le certificat par défaut n'est pas sécurisé par votre navigateur, donc un avertissement d'autorité non fiable s'affiche et vous demande si vous souhaitez faire confiance au certificat.

Bien que les utilisateurs puissent enregistrer le certificat dans le magasin de certificats racine de confiance, vous pouvez plutôt charger un nouveau certificat que les navigateurs sont déjà configurés pour faire confiance.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien**System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **Management Web Server** (Serveur Web de gestion).

Étape 3 Dans **Web Server Certificate** (Certificat du serveur Web), sélectionnez le certificat interne à utiliser pour sécuriser les connexions HTTPS avec le Firepower Device Manager.

Si vous n'avez pas chargé ou créé le certificat, cliquez sur le lien **Create New Internal Certificate** (créer un nouveau certificat interne) au bas de la liste et créez-le maintenant.

La valeur par défaut est l'objet prédéfini DefaultWebserverCertificate.

Étape 4 Si le certificat n'est pas autosigné, ajoutez tous les certificats intermédiaires et les certificats racine de la chaîne de confiance complète à la liste **Trusted Chain** (chaîne de confiance).

Vous pouvez ajouter jusqu'à 10 certificats dans la chaîne. Cliquez sur le signe **plus (+)** pour ajouter chaque certificat intermédiaire, et finalement, le certificat racine. Lorsque vous cliquez sur **Save** (Enregistrer) (puis **Proceed** (Continuer) dans la boîte de dialogue vous avertissant que le serveur Web redémarrera, si un certificat est manquant, vous obtenez un message d'erreur avec le nom commun du certificat suivant de la chaîne qui est manquant. Vous obtiendrez également une erreur si vous ajoutez un certificat qui ne fait pas partie de la chaîne. Examinez ces messages avec soin pour identifier le certificat que vous devez ajouter ou supprimer.

Vous pouvez charger les certificats à partir d'ici en cliquant sur **Create New Trusted CA Certificate** (Créer un nouveau certificat CA de confiance) après avoir cliqué sur **+**.

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

La modification est appliquée immédiatement et le système redémarre le serveur Web. Vous n'avez pas besoin de déployer la configuration.

Attendez quelques minutes que le serveur Web redémarre, puis actualisez votre navigateur.

Configurer les paramètres de journalisation du système

Vous pouvez activer la journalisation du système (syslog) pour les périphériques Firewall Threat Defense. Les informations de journalisation peuvent vous aider à cerner et isoler les problèmes de configuration du réseau ou des périphériques. Vous pouvez activer syslog pour la journalisation des diagnostics ainsi que pour la journalisation liée aux connexions, y compris le contrôle d'accès, la prévention des intrusions et la journalisation des fichiers et des programmes malveillants.

La journalisation des diagnostics fournit des messages syslog pour les événements liés à l'intégrité des périphériques et du système, et à la configuration du réseau, qui ne sont pas liés aux connexions. Vous configurez la journalisation des connexions dans les règles de contrôle d'accès individuelles.

La journalisation des diagnostics génère des messages pour les fonctionnalités exécutées sur le plan de données, c'est-à-dire les fonctionnalités qui sont définies dans la configuration de l'interface de ligne de commande que vous pouvez afficher à l'aide de 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.

Pour en savoir plus sur ces messages, consultez la documentation *Messages syslog de Cisco Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html.

Les rubriques suivantes expliquent comment configurer la journalisation des messages de diagnostic et de fichiers/programmes malveillants vers différents emplacements de sortie.

Niveaux de gravité

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

Tableau 1 : Niveaux de gravité des messages Syslog

Numéro de niveau	Niveau de gravité	Description
0	**urgences**	Système inutilisable.
1	**alerte**	Action immédiate requise.
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 Firewall Threat Defense ne génèrent pas de messages syslog avec un niveau de gravité de zéro (urgences).

Configurer la journalisation vers un serveur Syslog distant

Vous pouvez configurer le système pour envoyer des messages de journal système à un serveur de journaux système externe. Il s'agit de la meilleure option pour la journalisation du système. En utilisant un serveur externe, vous pouvez disposer de plus d'espace pour contenir les messages et utiliser les installations du serveur pour afficher, analyser et archiver les messages.

En outre, si vous appliquez des politiques de fichiers au trafic dans les règles de contrôle d'accès, pour contrôler l'accès aux fichiers ou les programmes malveillants, ou les deux, vous pouvez configurer le système pour envoyer des messages d'événement de fichier à un serveur syslog externe. Si vous ne configurez pas de serveur syslog, les événements sont disponibles uniquement dans Event Viewer (Visionneuse d'événements) Firepower Device Manager.

La procédure suivante explique comment activer syslog pour la journalisation des diagnostics (données) et la journalisation des fichiers et des programmes malveillants. Vous pouvez également configurer la journalisation externe pour les éléments suivants :

- Les événements de connexion, en sélectionnant le serveur syslog dans les règles de contrôle d'accès individuelles, les règles de déchiffrement SSL ou les paramètres de politique Security Intelligence.
- Les incidents d'intrusion, en sélectionnant le serveur syslog dans les paramètres de la politique de prévention des intrusions.

Avant de commencer

Le paramètre syslog pour les événements liés aux fichiers ou aux programmes malveillants n'est pertinent que si vous appliquez des politiques de fichiers ou de programmes malveillants, lesquelles nécessitent les licences IPS et Malware.

En outre, vous devez vous assurer que l'option **File Events (Événements de fichiers)** > **Log Files (Fichiers journaux)** est sélectionnée dans les règles de contrôle d'accès qui appliquent ces politiques. Sinon, aucun événement n'est généré, que ce soit pour syslog ou pour Event Viewer (Visionneuse d'événements).

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur le lien **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Logging Settings** (Paramètres de journalisation) dans la table des matières.

Étape 2 Sous **Remote Server** (Serveur distant), placez le curseur **Data Logging** (Journalisation des données) sur **On** (Activé) pour activer la journalisation des messages de diagnostic générés par le plan de données sur un serveur syslog externe. Configurez les options suivantes :

- **Syslog Server** (Serveur Syslog) : cliquez sur le signe **(+)** et sélectionnez un ou plusieurs objets de serveur syslog, puis cliquez sur **OK**. Si les objets n'existent pas, cliquez sur le lien **Add Syslog Server** (Ajouter un serveur Syslog) et créez-les maintenant. Pour en savoir plus, consultez Configuration des serveurs Syslog.
- **Niveau de gravité pour le filtrage des journaux système de châssis FXOS** : pour certains modèles de périphériques qui utilisent FXOS, le niveau de gravité des messages syslog générés par la plateforme FXOS de base. Cette option s'affiche uniquement si elle est pertinente pour votre périphérique. Sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés au serveur syslog.
- **Message Filtering** (Filtrage des messages) : sélectionnez l'une des options suivantes pour contrôler les messages générés pour le système d'exploitation Firewall Threat Defense.

- **Severity Level for Filtering All Events** (Niveau de gravité pour le filtrage de tous les événements) : sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés au serveur syslog.
- **Custom Logging Filter** (Filtre de journalisation personnalisé) : si vous souhaitez effectuer un filtrage supplémentaire des messages, afin de n'obtenir que les messages qui vous intéressent, sélectionnez le filtre de liste d'événements qui définit les messages que vous souhaitez générer. Si le filtre n'existe pas déjà, cliquez sur **Create New Event List Filter** (Créer un nouveau filtre de liste d'événements) et créez-le maintenant. Pour en savoir plus, consultez Configurer Event List Filters (Filtres de liste d'événements), à la page 9.

Étape 3 Placez le curseur **File/Malware** (Fichiers/Programmes malveillants) sur **On (Activé)** pour activer la journalisation vers un serveur syslog externe pour les événements liés aux fichiers et aux programmes malveillants. Configurez ensuite les options de journalisation des fichiers et des programmes malveillants :

- **Syslog Server** (Serveur Syslog) : sélectionnez l'objet serveur syslog. Si l'objet n'existe pas, cliquez sur le lien **Add Syslog Server** (Ajouter un serveur Syslog) et créez-le maintenant.
- **Log at Severity Level** (Journaliser au niveau de gravité) : sélectionnez un niveau de gravité à attribuer aux événements liés aux fichiers/aux programmes malveillants. Comme tous les événements liés aux fichiers/aux programmes malveillants sont générés au même niveau de gravité, aucun filtrage n'est effectué ; vous verrez tous les événements, peu importe le niveau choisi. Il s'agit du niveau affiché dans le champ de gravité du message (c'est-à-dire le x dans FTD-x-<message_ID>). Les événements de fichiers utilisent l'ID de message 430004, les événements de programmes malveillants sont 430005.

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

Configuration de la journalisation dans le tampon interne

Vous pouvez configurer le système pour enregistrer les messages de journal système dans un tampon de journalisation interne. Utilisez la commande **show logging** dans l'interface de ligne de commande ou la console d'interface de ligne de commande pour afficher le contenu de la mémoire tampon.

Les nouveaux messages s'ajoutent à la fin du tampon. Lorsque la mémoire tampon est remplie, le système l'efface et continue d'y ajouter des messages. Lorsque la mémoire tampon de journal est pleine, le système supprime le message le plus ancien pour faire de la place dans la mémoire tampon pour les nouveaux messages.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur le lien **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Logging Settings** (Paramètres de journalisation) dans la table des matières.

Étape 2 Réglez le curseur **Internal Buffer** (Tampon interne) sur **On** (Activé) pour activer la mémoire tampon comme destination de journalisation.

Étape 3 Configurez les options de journalisation de la mémoire tampon interne :

- **Severity Level for Filtering All Events** (Niveau de gravité pour le filtrage de tous les événements) : sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés à la mémoire tampon interne.
- **Custom Logging Filter** (Filtre de journalisation personnalisé) : (facultatif) Si vous souhaitez effectuer un filtrage supplémentaire des messages, afin de n'obtenir que les messages qui vous intéressent, sélectionnez le event list filter (filtre de liste d'événements) qui définit les messages à générer. Si le filtre n'existe pas déjà, cliquez sur **Create New Event List Filter** (Créer un nouveau filtre de liste d'événements) et créez-le maintenant. Pour en savoir plus, consultez Configurer Event List Filters (Filtres de liste d'événements), à la page 9.
- **Buffer Size (Taille du tampon)** : taille du tampon interne dans lequel les messages syslog sont enregistrés. 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 Cliquez sur **Save** (enregistrer).

Configuration de la journalisation sur la console

Vous pouvez configurer le système pour envoyer des messages à la console. Ces messages apparaissent lorsque vous vous connectez à l'interface de ligne de commande sur le port de console. Vous pouvez aussi voir ces journaux dans une session SSH sur d'autres interfaces (y compris l'adresse de gestion) en utilisant la commande **show console-output**. En outre, vous pouvez voir ces messages en temps réel dans l'interface de ligne de commande de diagnostic, entrez **system support diagnostic-cli** depuis l'interface de ligne de commande principale.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis cliquez sur le lien **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Logging Settings** (Paramètres de journalisation) dans la table des matières.

Étape 2 Réglez le curseur **Console Filter** (Filtre de console) sur **On** (Activé) pour activer la console comme destination de journalisation.

Étape 3 Sélectionnez le niveau de **gravité**. Les messages à ce niveau ou à un niveau supérieur sont envoyés à la console.

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

Configurer Event List Filters (Filtres de liste d'événements)

Un event list filter (filtre de 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 un

filtre pour affiner les messages envoyés en fonction d'une combinaison de classe d'événement, de gravité et d'identifiant de message (ID).

Vous n'utiliserez un filtre que si la limitation des messages par niveau de gravité est insuffisante pour vos besoins.

La procédure suivante explique comment créer le filtre à partir de la page **Objects** (Objets). Vous pouvez également créer un filtre lorsque vous configurez une destination de journalisation qui peut utiliser un filtre.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **Event List Filters (Filtres de liste d'événements)** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

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

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

Étape 3 Configurez les propriétés du filtre :

- **Nom** : le nom de l'objet filtre.
- **Description** : ajoutez une description facultative.
- **Gravité et classe du journal** : si vous souhaitez filtrer par classe de message, cliquez sur **+**, sélectionnez un niveau de gravité pour le filtre de classe et cliquez sur **OK**. Ensuite, cliquez sur la flèche de liste déroulante dans le niveau de gravité, sélectionnez une ou plusieurs classes à filtrer à ce niveau de gravité, puis cliquez sur **OK**.

  Le système enverra des messages de journal système pour les classes de messages spécifiées uniquement si elles sont à ce niveau de gravité ou à un niveau supérieur. Vous pouvez ajouter au maximum une ligne pour chaque niveau de gravité.

  Si vous souhaitez filtrer toutes les classes à un niveau de gravité donné, laissez la liste de gravité vide et sélectionnez plutôt le niveau de gravité global pour la destination de journalisation lorsque vous l'activez.
- **Plage de Syslog/ID de message** : si vous souhaitez filtrer par l'ID de message syslog, saisissez un ID de message unique ou une plage de numéros d'ID pour laquelle vous souhaitez générer des messages. Séparez les chiffres de début et de fin par un tiret, par exemple 100 000-200 000. Les identifiants sont des numéros à 6 chiffres. Pour des ID de message spécifiques et les messages associés, consultez *Messages Syslog de Cisco Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html.

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

Vous pouvez maintenant sélectionner cet objet dans l'option de filtrage personnalisé pour les destinations de journalisation qui l'autorisent. Accédez à **Device (Périphérique)** > **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**.

Configuration du DHCP

Un serveur DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP. Vous pouvez soit configurer des serveurs DHCP sur les interfaces pour fournir les paramètres de configuration aux clients DHCP sur le réseau associé, soit activer le relais DHCP sur les interfaces pour transférer les demandes à un serveur DHCP externe qui fonctionne sur un autre périphérique du réseau.

Ces fonctionnalités s'excluent mutuellement : vous pouvez configurer l'une ou l'autre, mais pas les deux.

Configuration du serveur DHCP

Un serveur DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP. Vous pouvez configurer un serveur DHCP sur une interface pour fournir des paramètres de configuration aux clients DHCP sur le réseau connecté.

Un client DHCP IPv4 utilise une adresse de diffusion plutôt qu'une adresse de multidiffusion pour atteindre le serveur. Le client DHCP est à l'écoute des messages sur le port UDP 68; le serveur DHCP est à l'écoute des messages sur le port UDP 67. Le serveur DHCP ne prend pas en charge les demandes BOOTP.

Remarque Ne configurez pas de serveur DHCP sur un réseau sur lequel un serveur DHCP est déjà installé. Les deux serveurs seront en conflit, ce qui engendrera des résultats imprévisibles.

Avant de commencer

Les clients DHCP doivent être sur le même réseau que l'interface sur laquelle le serveur est activé. Autrement dit, il ne peut y avoir de routeur intermédiaire entre le serveur et le client, bien qu'il puisse y avoir un commutateur.

Si vous devez prendre en charge plusieurs réseaux et que vous ne souhaitez pas configurer un serveur DHCP sur chaque interface, vous pouvez configurer le relais DHCP pour transférer les demandes DHCP d'un réseau à un serveur DHCP hébergé sur un autre réseau. Dans ce cas, le serveur DHCP doit être hébergé sur un dispositif différent du réseau : vous ne pouvez pas configurer un serveur DHCP sur une interface et un relais DHCP sur une autre interface du même dispositif. Lorsque vous utilisez le relais DHCP, assurez-vous de configurer le serveur DHCP avec des ensembles d'adresses pour chaque espace d'adressage réseau géré par le serveur DHCP.

Pour configurer le relais DHCP, voir Configuration du relais DHCP, à la page 13.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), puis sur le lien **System Settings (paramètres de système)** > **DHCP Server / Relay (serveur/relais DHCP)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **DHCP** > **DHCP Server (serveur DHCP)** dans la table des matières.

La page comporte deux onglets. Dans un premier temps, l'onglet **Configuration** affiche les paramètres globaux.

L'onglet **DHCP Servers (serveurs DHCP)** affiche les interfaces sur lesquelles vous avez configuré le serveur DHCP, indique si le serveur est activé et montre l'ensemble d'adresses pour le serveur.

Étape 2 Sous l'onglet **Configuration**, réglez la configuration automatique et les paramètres globaux.

La configuration automatique DHCP permet au serveur DHCP de fournir aux clients DHCP des informations sur le serveur DNS, le nom de domaine et le serveur WINS obtenues d'un client DHCP qui s'exécute sur l'interface précisée. Généralement, vous utiliseriez la configuration automatique si vous obtenez une adresse en utilisant DHCP sur l'interface externe, mais vous pouvez choisir n'importe quelle interface qui obtient son adresse par le biais de DHCP. Si vous ne pouvez pas utiliser la configuration automatique, vous pouvez définir manuellement les options requises.

a) Cliquez sur **Enable Auto Configuration (activer la configuration automatique)** > **On (activé)** (le curseur doit être à droite) si vous souhaitez utiliser la configuration automatique, puis sélectionnez l'interface qui obtient son adresse par le biais de DHCP sous **From Interface** (de l'interface).

Si vous configurez des routeurs virtuels, vous pouvez utiliser la configuration automatique du serveur DHCP sur une interface du routeur virtuel global uniquement. La configuration automatique n'est pas prise en charge pour les interfaces affectées à un routeur virtuel défini par l'utilisateur.

b) Si vous n'activez pas la configuration automatique ou si vous souhaitez remplacer l'un des paramètres configurés automatiquement, configurez les options globales suivantes. Ces paramètres seront envoyés aux clients DHCP sur toutes les interfaces qui hébergent le serveur DHCP.

- **Primary WINS IP Address (adresse IP WINS principale)**, **Secondary WINS IP Address (adresse IP WINS secondaire)** : Les adresses des serveurs clients WINS (Windows Internet Name Service) que les clients doivent utiliser pour la résolution de noms NetBIOS.
- **Primary DNS IP Address** (adresse IP du DNS primaire), **Secondary DNS IP Address**(adresse IP du DNS secondaire) : Les adresses des serveurs DNS (Domain Name System) que les clients doivent utiliser pour la résolution des noms de domaine. Cliquez sur **Use OpenDNS** si vous souhaitez configurer les serveurs DNS publics OpenDNS. Cliquez sur le bouton pour charger les adresses IP appropriées dans les champs.

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

Étape 3 Cliquez sur l'onglet **DHCP Servers** (serveurs DHCP) et configurez les serveurs.

a) Effectuez l'une des opérations suivantes :

- Pour configurer le serveur DHCP pour une interface qui n'est pas déjà répertoriée, cliquez sur +.
- Pour modifier un serveur DHCP existant, cliquez sur l'icône de modification ( ) du serveur.

Pour supprimer un serveur, cliquez sur l'icône de la corbeille ( ) du serveur.

b) Configurez les propriétés du serveur :

- **Enable DHCP Server (activer le serveur DHCP)** : Cette option permet d'activer le serveur. Vous pouvez configurer le serveur, mais laissez-le désactivé jusqu'à ce que vous soyez prêt à l'utiliser.
- **Interface** : Sélectionnez l'interface sur laquelle vous allez fournir les adresses DHCP aux clients. L'interface doit avoir une adresse IP statique; vous ne pouvez pas utiliser DHCP pour obtenir l'adresse de l'interface si vous souhaitez exécuter un serveur DHCP sur l'interface. Pour les groupes de ponts, vous configurez le serveur DHCP sur l'interface BVI (Bridge Virtual Interface), et non les interfaces membres, et le serveur fonctionne sur toutes les interfaces membres.

Vous ne pouvez pas configurer le serveur DHCP sur Diagnostic l'interface; configurez-le plutôt sur l'interface de gestion, dans la page **Device (dispositif)** > **System Settings (paramètres système)** > **Management Interface (dispositif de gestion)**.

- **Address Pool (ensemble d'adresses)** : La plage des adresses IP (de la plus basse à la plus élevée) que le serveur est autorisé à fournir aux clients qui demandent une adresse. Indiquez les adresses de début et de fin de l'ensemble, séparées par un tiret. Par exemple, 10.100.10.12-10.100.10.250.

  La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure : l'adresse IP de l'interface elle-même, l'adresse de diffusion ou l'adresse réseau du sous-réseau.

  La taille de l'ensemble se limite à 256 adresses par ensemble sur l'appareil Cisco Firewall Threat Defense. Si la plage d'adresses est supérieure à 253 adresses, le masque de réseau de l'interface Cisco Firewall Threat Defense ne peut pas être une adresse de classe C (par exemple, 255.255.255.0) et doit être plus grand, par exemple, 255.255.254.0.

c) Cliquez sur **OK**.

Configuration du relais DHCP

Vous pouvez configurer un agent de relais DHCP pour transférer les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP.

Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n'inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le dispositif Cisco Firewall Threat Defense, car il ne transfère pas le trafic de diffusion. L'agent de relais DHCP vous permet de configurer l'interface de l'appareil Cisco Firewall Threat Defense qui reçoit les diffusions pour transférer les demandes DHCP vers un serveur DHCP qui est disponible via une autre interface.

Ainsi, les clients des sous-réseaux qui n'hébergent pas de serveur DHCP peuvent tout de même obtenir des baux d'adresse IP d'un serveur DHCP qui réside sur un autre sous-réseau.

Avant de commencer

- Configurez le serveur DHCP avec des ensembles d'adresses pour chacun des sous-réseaux que vous ajoutez. Par exemple, si vous activez le client de relais DHCP sur une interface avec l'adresse 192.168.1.1/24 pour prendre en charge les clients sur le réseau 192.168.1.0/24, le serveur DHCP doit pouvoir fournir des adresses IP sur le sous-réseau 192.168.1.0/24, par exemple 192.168.1.2-192.168.1.254.
- Créez des objets de réseau hôte pour chacun des serveurs DHCP, en spécifiant l'adresse IP du serveur.
- Assurez-vous d'avoir supprimé ou désactivé tous les serveurs sur la page **DHCP** > **DHCP Servers**. Vous ne pouvez pas héberger un serveur DHCP sur une interface avec le relais DHCP activé sur une interface, même s'il s'agit d'interfaces différentes.
- Restrictions en lien avec l'interface : Une interface doit avoir un nom à utiliser pour le serveur ou l'agent. De plus :
  - L'interface ne peut pas être membre d'une zone de trafic de routage ECMP.
  - L'interface ne peut pas obtenir son adresse en utilisant DHCP.

- Vous pouvez configurer le serveur DHCP et le relais DHCP sur les interfaces physiques, les sous-interfaces, les interfaces VLAN et les canaux EtherChannels (mais pas leurs membres).
- Vous pouvez également configurer le serveur de relais DHCP sur les interfaces de tunnel virtuel (VTI).
- Aucun service ne prend en charge l'interface de gestion ou les groupes de ponts et leurs membres.

Procédure

Étape 1 Cliquez sur **Device** (appareil), puis sur le lien **System Settings** > **DHCP Server/Relay**; ensuite, cliquez sur **DHCP** > **DHCP Relay (relais DHCP)** dans la table des matières.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **DHCP** > **DHCP Relay (relais DHCP)** dans la table des matières.

Étape 2 (Facultatif) Réglez les paramètres de délai d'expiration des relais IPv4 et IPv6 (**IPv4 Relay Timeout** et **IPv6 Relay Timeout**) selon les besoins.

Ces délais définissent le délai (en nombre de secondes) autorisés pour la négociation d'adresses de relais DHCP pour la version IP donnée. La valeur par défaut est 60 secondes (une minute), mais vous pouvez définir un délai différent de 1 à 3600 secondes. Des délais plus longs peuvent être appropriés en cas de décalage important entre le sous-réseau et le serveur DHCP.

Étape 3 Configurez le serveur DHCP (**DHCP Relay Servers**).

Les serveurs de relais DHCP sont les serveurs DHCP du réseau qui doivent traiter les demandes de relais DHCP. Ces serveurs DHCP résident sur différents dispositifs du réseau à partir de l'appareil que vous configurez.

a) Cliquez sur **+**, sélectionnez un objet de réseau hôte qui possède l'adresse IP d'un serveur DHCP, puis cliquez sur **OK**.

Si l'objet n'existe pas encore, cliquez sur **Create New Network (créer un nouveau réseau)** pour le créer maintenant. Si vous ne souhaitez plus utiliser un serveur DHCP que vous avez ajouté, cliquez sur le **X** à droite de l'entrée du serveur pour le supprimer.

b) Cliquez sur l'entrée de serveur DHCP que vous avez ajoutée et sélectionnez l'interface par laquelle le serveur DHCP peut être atteint.

Étape 4 Configurez les agents de relais DHCP.

Les agents de relais DHCP s'exécutent sur les interfaces. Ils transmettent les demandes DHCP des clients de leur segment de réseau aux serveurs DHCP, puis renvoient les réponses au client.

a) Cliquez sur **+**, sélectionnez les interfaces devant exécuter l'agent de relais DHCP, puis cliquez sur **OK**.

Si vous ne souhaitez plus exécuter l'agent de relais DHCP, cliquez sur le **X** à droite de l'entrée du serveur pour le supprimer. Vous pouvez aussi désactiver tous les services de relais DHCP sans retirer l'interface de la table.

b) Cliquez sur l'entrée d'interface que vous avez ajoutée, sélectionnez les services DHCP que l'agent doit fournir, puis cliquez sur **OK**.

- **Enable IPv4** (activer IPv4) : Transfère les demandes d'adresse IPv4 au serveur DHCP. Si vous ne sélectionnez pas cette option, toute demande d'adresse IPv4 est ignorée et le client ne peut pas obtenir d'adresse IPv4.
- **Définir la route** (IPv4 uniquement) : modifiez la première adresse de routeur par défaut dans le paquet envoyé par le serveur DHCP à l'adresse de l'interface du Cisco Firewall Threat Defensedispositif qui exécute l'agent de relais DHCP. Cette action permet au client de configurer sa route par défaut pour qu'elle pointe vers le Cisco Firewall Threat Defensedispositif, même si le serveur DHCP spécifie un routeur différent. S'il n'y a pas d'option de routeur par défaut dans le paquet, l'agent de relais DHCP en ajoute une contenant l'adresse de l'interface.
- **Enable IPv6** (activer IPv6) : Transfère les demandes d'adresse IPv4 au serveur DHCP. Si vous ne sélectionnez pas cette option, toute demande d'adresse IPv6 est ignorée et le client ne peut pas obtenir d'adresse IPv6.

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

Configuration du DNS dynamique

Vous pouvez configurer le système pour utiliser la méthode de mise à jour Web afin d'envoyer les modifications du système de nom de domaine dynamique (DDNS) aux services DNS dynamiques. Ces services mettent ensuite à jour le serveur DNS pour qu'il utilise la nouvelle adresse IP associée à un nom de domaine complet (FQDN). Ainsi, lorsque les utilisateurs tentent d'accéder au système en utilisant un nom d'hôte, le DNS assure la résolution du nom pour établir une adresse IP correcte.

L'utilisation du DDNS permet de s'assurer que les noms de domaine complets définis pour les interfaces du système correspondent toujours à la bonne adresse IP. Ceci est particulièrement important si vous configurez une interface pour obtenir son adresse en utilisant DHCP. Mais il est également utile de l'utiliser pour les adresses IP statiques, afin de veiller à ce que le serveur DNS dispose des adresses correctes et à ce qu'il puisse être facilement mis à jour si vous modifiez l'adresse statique.

Vous pouvez configurer DDNS pour utiliser un groupe sélectionné de fournisseurs de services DDNS, ou utiliser l'option personnalisée pour diriger les mises à jour vers tout autre fournisseur DDNS qui prend en charge les mises à jour Web. Les noms de domaine complets que vous spécifiez pour les interfaces doivent être enregistrés auprès de ces fournisseurs de services.

Remarque Vous pouvez utiliser le Firepower Device Manager pour configurer la mise à niveau web DDNS uniquement. Vous ne pouvez pas configurer DDNS pour la méthode définie dans IETF RFC 2136.

Avant de commencer

Le système doit avoir un certificat de l'autorité de certification de confiance qui validera le certificat du fournisseur, sinon la connexion DDNS échouera. Vous pouvez télécharger les certificats sur le site du fournisseur de services. Veuillez vous assurer que le certificat approprié est téléchargé et déployé. Assurez-vous également de définir **l'utilisation de validation** pour le certificat téléchargé afin d'inclure le **serveur SSL**. Consultez Téléchargement des certificats de l'autorité de certification de confiance

Procédure

Étape 1 Cliquez sur **Device (appareil)**, puis sur le lien **System Settings (paramètres système)** > **DDNS Service (service DDNS)**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **DDNS Service** dans la table des matières.

La page comprend une liste des méthodes de mise à jour du DDNS, y compris le fournisseur de services, l'interface, le nom de domaine complet (FQDN) de l'interface et la fréquence à laquelle le serveur DNS sera mis à jour sous l'angle des modifications de l'adresse IP du FQDN. Vous pouvez cliquer sur le lien **Show Status (afficher l'état)** d'une entrée pour vérifier si elle fonctionne correctement.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une nouvelle méthode de mise à jour DNS dynamique, cliquez sur **+** ou sur le bouton **Create DDNS Service** (créer un service DDNS).
- Pour modifier une méthode de mise à jour de DNS dynamique existant, cliquez sur l'icône de modification () de la méthode.

Pour supprimer une méthode, cliquez sur l'icône de la corbeille () de la méthode.

Étape 3 Configurez les propriétés du service DNS dynamique :

- **Name** (nom) : Précisez le nom du service.
- **Mise à jour de type Web** : Sélectionnez les types d'adresses à mettre à jour en fonction de ce qui est pris en charge par votre fournisseur de service DDNS. La valeur par défaut correspond à la mise à jour de toutes les adresses IPv4 et IPv6 (**All Addresses**). Vous pouvez plutôt choisir de mettre à jour l'adresse IPv4 (**IPv4 Address**), l'adresse IPv4 et une adresse IPv6 (**IPv4 and One IPv6 Address**), l'adresse IPv6 (**One IPv6 Address**) ou toutes les adresses IPv6 (**All IPv6 Addresses**).

  Veuillez noter les points suivants pour les adresses IPv6 :

  - Seules les adresses globales sont mises à jour. L'adresse locale du lien n'est jamais mise à jour.
  - Étant donné que le Firepower Device Manager vous permet de configurer une seule adresse IPv6 par interface, en pratique, une seule adresse IPv6 sera jamais mise à niveau.

- **Service Provider (fournisseur de service)** : Sélectionnez le fournisseur de service qui recevra et traitera les mises à jour de DNS dynamique. Vous pouvez recourir aux fournisseurs de service ci-après.
  - **No-IP** : le fournisseur de service DDNS No-IP, https://www.noip.com/.
  - **Dynamic DNS** : le fournisseur de service DNS dynamique Oracle, https://account.dyn.com/.
  - **Google** : le fournisseur de service Google Domains, https://domains.google.com.
  - **Custom URL** (URL personnalisée) : tout autre fournisseur de service DDNS. Vous devrez entrer l'URL requise par le fournisseur sélectionné, y compris le nom d'utilisateur et le mot de passe, dans le champ **Web URL**. Le service DDNS doit respecter les normes décrites à l'adresse https://help.dyn.com/remote-access-api/.

- **Username** (nom d'utilisateur), **Password** (mot de passe (URL non personnalisée) : le nom d'utilisateur et le mot de passe, définis sur la plateforme du fournisseur de service, à utiliser lors de l'envoi de mises à jour de DNS dynamique.

  Remarque :

  - Le nom d'utilisateur ne peut pas inclure d'espaces, ni les caractères « @ » et « : », car ceux-ci servent de délimiteurs.
  - Le mot de passe ne peut pas inclure d'espaces ni le caractère « @ », car il sert de délimiteur. Tout caractère « : » après le premier « : » et avant « @ » est considéré comme faisant partie du mot de passe.

- **Web URL** (URL personnalisée) : si vous avez sélectionné une URL personnalisée comme fournisseur de service, entrez l'URL de votre service DNS dynamique. L'URL doit respecter le format suivant et comprendre tout au plus 511 caractères :

  http(s)://username:password@provider-domain/xyz?hostname=<h>&myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- **Interfaces et nom de domaine complet** : Sélectionnez les interfaces dont vous souhaitez mettre à jour les enregistrements DNS avec ce fournisseur de service, puis saisissez le nom de domaine complet pour chaque interface. Par exemple, interface.exemple.com. Voici les limites s'appliquant aux interfaces :
  - Vous pouvez sélectionner uniquement les sous-interfaces et les interfaces physiques nommées.
  - Vous ne pouvez pas sélectionner les types d'interface suivants : gestion (management), BVI/EtherChannel ou ses membres, réseaux VLAN, interfaces de tunnel virtuel (VTI).
  - Une interface donnée peut être sélectionnée avec une seule méthode de mise à jour du DDNS. Vous pouvez sélectionner toutes les interfaces devant utiliser un fournisseur de services dans le même objet de mise à jour de DDNS.

- **Update Interval** (intervalle de mise à jour) : fréquence d'envoi de la mise à jour de DNS dynamique. La valeur par défaut est **On Change** (à la suite d'une modification), qui envoie une mise à jour chaque fois que l'adresse IP de l'interface change. Vous pouvez également sélectionner **Hourly (horaire)**, **Daily (quotidien)** ou **Monthly (mensuel)** . Pour les options d'envoi quotidien et mensuel, configurez également l'heure de la journée de l'envoi des mises à jour. Pour l'envoi mensuel, vous devrez choisir la journée du mois.

Étape 4 Cliquez sur **OK**.

Configurer le DNS

Les serveurs du système de noms de domaine (DNS) sont utilisés pour transformer les noms d'hôtes en adresses IP. Vous configurez les serveurs DNS lors de la configuration initiale du système, et ces serveurs s'appliquent aux interfaces de données et de gestion. Vous pouvez les modifier après la configuration et utiliser des ensembles distincts de serveurs pour les interfaces de données et de gestion.

Vous devez au minimum configurer le DNS pour l'interface de gestion. Vous devez également configurer le DNS pour les interfaces de données si vous souhaitez utiliser des règles de contrôle d'accès basées sur FQDN ou si vous souhaitez utiliser les noms d'hôte dans les commandes CLI telles que **ping**.

La configuration du DNS est un processus en deux étapes : vous configurez les groupes DNS, puis vous configurez le DNS sur les interfaces.

Les rubriques suivantes expliquent plus en détail le processus.

Configuration des groupes DNS

Les groupes DNS (Domain Name System) définissent une liste de serveurs DNS et certains attributs associés. Vous pouvez configurer le DNS séparément sur les interfaces de gestion et de données. Les serveurs du système de noms de domaine (DNS) résolvent les noms de domaine complets (FQDN), tels que www.exemple.com, en adresses IP.

Après avoir terminé l'assistant de configuration du périphérique, vous aurez l'un des groupes DNS suivants définis par le système, ou les deux :

- CiscoUmbrellaDNSServerGroup : ce groupe comprend les adresses IP des serveurs DNS disponibles avec Cisco Umbrella. Si vous avez sélectionné ces serveurs lors de la configuration initiale, il s'agit du seul groupe défini par le système. Vous ne pouvez pas modifier le nom ou la liste de serveurs dans ce groupe, mais vous pouvez modifier les autres propriétés.
- CustomDNSServerGroup : si vous ne sélectionnez pas les serveurs Umbrella lors de la configuration du périphérique, le système crée ce groupe avec votre liste de serveurs. Vous pouvez modifier n'importe quelle propriété dans ce groupe.

Procédure

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

Étape 2 Effectuez l'une des opérations suivantes :

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

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

Étape 3 Configurez les propriétés suivantes :

- **Nom** : le nom du groupe de serveurs DNS. Le nom DefaultDNS est réservé : vous ne pouvez pas l'utiliser.
- **Adresses IP DNS** : saisissez l'adresse IP d'un serveur DNS. Cliquez sur **Add Another DNS IP Address** (Ajouter une autre adresse IP DNS) pour configurer plusieurs serveurs. Si vous souhaitez supprimer une adresse de serveur, cliquez sur l'icône de suppression ( ) en regard de l'adresse.

  La liste est en ordre de priorité : le premier serveur de la liste est toujours utilisé et les serveurs suivants ne sont utilisés que si les serveurs précédents ne répondent pas. Vous pouvez configurer jusqu'à 3 serveurs.
- Dans **Domain Search Name** (Nom de recherche du domaine), saisissez le nom de domaine de votre réseau, par exemple, exemple.com. Ce domaine est ajouté aux noms d'hôte qui ne sont pas complets, par

exemple, serverA au lieu de serverA.example.com. Le nom doit comporter moins de 63 caractères pour que le groupe puisse être utilisé pour les interfaces de données.

- **Nombre de tentatives** : le nombre de tentatives, de 0 à 10, pour réessayer la liste des serveurs DNS lorsque le système ne reçoit pas de réponse. La valeur par défaut est 2. Ce paramètre s'applique uniquement aux groupes DNS utilisés sur les interfaces de données.
- **Timeout** (Délai d'attente) : le nombre de secondes, de 1 à 30, à attendre avant d'essayer le serveur DNS suivant. La valeur par défaut est de 2 secondes. Chaque fois que le système réessaie la liste des serveurs, ce délai est doublé. Ce paramètre s'applique uniquement aux groupes DNS utilisés sur les interfaces de données.

Étape 4 Cliquez sur **OK**.

Configuration DNS pour les données et le trafic de gestion

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 le VPN d"accès à distance. Le trafic spécial de gestion comprend le trafic provenant de l'interface de gestion, tel que Smart Licensing et les mises à jour de la base de données.

Si vous utilisez l'assistant de configuration de l'interface de ligne de commande, vous configurez les serveurs DNS de gestion lors de la configuration système initiale. Vous pouvez également définir les serveurs DNS de données et de gestion dans l'assistant de configuration Firepower Device Manager. Vous pouvez modifier les valeurs par défaut des serveurs DNS en utilisant la procédure suivante.

Vous pouvez également modifier la configuration DNS de gestion dans l'interface de ligne de commande à l'aide des commandes **configure network dns servers** et **configure network dns searchdomains**. Si les interfaces de données et de gestion utilisent le même groupe DNS, le groupe est mis à jour et lors de votre prochain déploiement, les modifications sont également appliquées aux interfaces de données.

Pour déterminer l'interface correcte pour les communications du serveur DNS, le Firewall Threat Defense 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.

Si vous avez des problèmes avec la résolution DNS, consultez :

- Dépannage des problèmes généraux de DNS, à la page 21
- Dépannage du DNS pour l'interface de gestion

Avant de commencer

- Assurez-vous d'avoir créé un ou plusieurs groupe(s) de serveurs DNS. Pour plus d'informations sur les instructions, consultez Configuration des groupes DNS, à la page 18
- Assurez-vous que le périphérique Firewall Threat Defense dispose des routes statiques ou dynamiques appropriées pour accéder aux serveurs DNS.

Procédure

Étape 1 Cliquez sur **Device** (Dispositif), puis sur le lien **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.

Si vous êtes déjà sur la page **System Settings** (Paramètres système), cliquez sur **DNS Server** (Serveur DNS) dans la table des matières.

Étape 2 Configurez le DNS pour l'**interface de données**.

a) 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 périphérique 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 périphérique 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 sélectionnées, mais pas l'interface Diagnostic ou une interface de gestion uniquement : active les recherches DNS sur les interfaces spécifiées. Le périphérique contrôle la table de routage des données uniquement.
- Interfaces sélectionnées plus l'interface Diagnostic ou une interface de gestion uniquement : active les recherches DNS sur les interfaces spécifiées. Le périphérique vérifie la table de routage des données et, si aucune route n'est trouvée, revient à la table de routage de gestion uniquement.
- Uniquement l'interface Diagnostic ou une interface réservée à la gestion sélectionnée : active les recherches DNS sur Diagnostic ou sur une interface réservée à la gestion uniquement. Le périphérique ne vérifie que la table de routage de gestion.

b) Sélectionnez le **groupe DNS** qui définit les serveurs à utiliser sur les interfaces de données. Si le groupe dont vous avez besoin n'est pas encore défini, cliquez sur **Create New DNS Group (Créer un nouveau groupe DNS)** et créez-le maintenant. Sélectionnez **None** (Aucun) si vous souhaitez empêcher les recherches sur les interfaces de données.

c) (Facultatif) Configurez les **paramètres DNS FQDN** si vous utilisez des objets réseau FQDN dans les règles de contrôle d'accès.

Ces options sont utilisées uniquement lors de la résolution d'objets FQDN et sont ignorées pour tout autre type de résolution DNS.

- **Temps d'interrogation** : durée, en minutes, du cycle d'interrogation utilisé pour résoudre les objets réseau FQDN en adresses IP. Les objets FQDN sont résolus uniquement s'ils sont utilisés dans la politique de contrôle d'accès. La minuterie détermine le délai maximal entre les résolutions ; la valeur de durée de vie (TTL) de l'entrée DNS est également utilisée pour déterminer quand mettre à jour la résolution d'adresse IP, de sorte que les FQDN individuels peuvent être résolus plus fréquemment que le cycle d'interrogation. La valeur par défaut est 240 (quatre heures). La plage est comprise entre 1 et 65535 minutes.
- **Expiration** : nombre de minutes après l'expiration d'une entrée DNS (c'est-à-dire après la fin du TTL envoyé par le serveur DNS) durant lesquelles l'entrée demeure dans la table de consultation

DNS avant d'être supprimée. 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 de 1 minute (c'est-à-dire que l'entrée est supprimée une minute après la fin de la TTL). La plage est comprise entre 1 et 65535 minutes.

d) Cliquez sur **Save** (enregistrer). Vous devez également déployer la configuration pour appliquer les modifications au périphérique.

Étape 3 Configurer DNS pour l'**interface de gestion**.

a) Sélectionnez le **groupe DNS** qui définit les serveurs à utiliser sur l'interface de gestion. Si le groupe dont vous avez besoin n'est pas encore défini, cliquez sur **Create New DNS Group** (Créer un nouveau groupe DNS) et créez-le maintenant.

b) Cliquez sur **Save** (enregistrer). Vous devez déployer des modifications pour mettre à jour les serveurs DNS de gestion.

Dépannage des problèmes généraux de DNS

Vous devez configurer séparément les serveurs DNS pour les interfaces de gestion et de données. Certaines fonctionnalités permettent la résolution de noms à l'aide de l'un ou l'autre type d'interface, mais pas des deux. Parfois, une fonctionnalité donnée utilise différentes méthodes de résolution en fonction de votre utilisation.

Par exemple, les commandes **ping** *hostname* et **ping interface** *interface_name hostname* utilisent les serveurs DNS de l'interface de données pour résoudre le nom, alors que la commande **ping system** *hostname* utilise les serveurs DNS de l'interface de gestion. Cela vous permet de tester la connectivité via des interfaces spécifiques et la table de routage.

Gardez cela à l'esprit lorsque vous rencontrez des problèmes de recherche de nom d'hôte.

Pour le dépannage de DNS pour l'interface de gestion, consultez également Dépannage du DNS pour l'interface de gestion.

Lorsque vous n'obtenez aucune résolution de nom

Voici quelques conseils de dépannage si vous n'obtenez tout simplement aucune résolution de nom.

- Vérifiez que vous avez configuré des serveurs DNS pour les interfaces de gestion et de données. Pour les interfaces de données, utilisez « Any » pour l'interface. Spécifiez les interfaces explicitement uniquement si vous ne souhaitez pas autoriser le DNS sur certaines interfaces.
- Si vous utilisez l'interface de diagnostic pour les recherches sur les interfaces de données, vérifiez que vous avez configuré une adresse IP sur l'interface. Les recherches nécessitent que l'interface dispose d'une adresse IP.
- Vous ne pouvez pas atteindre le serveur DNS par Diagnostic l'interface ou par une interface de gestion uniquement, car la recherche de voie de routage trouve une correspondance dans la table de routage de données, de sorte qu'il n'y a pas de retour à la table de routage de gestion uniquement. Si vous souhaitez utiliser l'interface Diagnostic, assurez-vous qu'il s'agit de la seule interface sélectionnée.
- Envoyez un message ping à l'adresse IP de chaque serveur DNS pour vérifier qu'elle est accessible. Utilisez les mots-clés **system** et **interface** pour tester des interfaces spécifiques. Si l'envoi du message

ping échoue, vérifiez vos voies de routage statique et vos passerelles. Vous devrez peut-être ajouter des voies de routage statique pour les serveurs.

- Si l'envoi du message réussit, mais que la résolution de nom échoue, vérifiez vos règles de contrôle d'accès. Vérifiez que vous autorisez le trafic DNS (UDP/53) pour les interfaces par lesquelles les serveurs sont accessibles. Il est également possible que ce trafic soit bloqué par un périphérique qui se trouve entre votre système et le serveur DNS. Vous devrez peut-être utiliser différents serveurs DNS.
- Si l'envoi du message réussit, que les voies de routage sont adéquates et que les règles de contrôle d'accès ne posent pas le problème, considérez que le serveur DNS ne peut peut-être pas être mis en correspondance avec le nom de domaine complet. Vous devrez peut-être faire appel à différents serveurs.

Lorsque vous obtenez une mauvaise résolution de nom

Si vous obtenez une résolution de nom, mais que l'adresse IP d'un nom n'est pas exacte, il y a peut-être un problème de mise en mémoire cache. Ce problème toucherait uniquement aux fonctionnalités basées sur l'interface de données, telles que les objets réseau du nom de domaine complet utilisés dans les règles de contrôle d'accès.

Le système dispose d'une mémoire cache locale d'informations DNS obtenues lors de précédentes recherches. Lorsqu'une nouvelle recherche est requise, le système fait d'abord des recherches dans la mémoire cache locale. Si la mémoire cache locale contient les informations, l'adresse IP qui en résulte est renvoyée. Si la mémoire cache locale ne peut pas résoudre la demande, une requête DNS est envoyée aux serveurs DNS. Si un serveur DNS externe résout la demande, l'adresse IP qui en résulte est stockée dans la mémoire cache locale avec son nom d'hôte correspondant.

Chaque recherche a une durée de vie définie par le serveur DNS et expire automatiquement de la mémoire de cache. En outre, le système actualise périodiquement la valeur des noms de domaine complets qui sont utilisés dans les règles de contrôle d'accès. Au minimum, cette actualisation a lieu à l'intervalle du délai d'interrogation (par défaut, toutes les 4 heures), mais elle peut être plus fréquente en fonction de la durée de vie de l'entrée.

Utilisez les commandes **show dns-hosts** et **show dns** pour consulter la mémoire cache locale. Si les adresses IP d'un nom de domaine complet sont incorrectes, vous pouvez utiliser la commande **dns update** [**host** *hostname*] pour forcer le système à actualiser les informations. Si vous utilisez la commande sans spécifier d'hôte, tous les noms d'hôte sont actualisés.

Vous pouvez supprimer les informations mises en cache en utilisant les commandes **clear dns** [**host** *fqdn*] et **clear dns-hosts cache**.

Configuration de l'interface de gestion

L'interface de gestion est une interface virtuelle reliée au port de gestion physique. Notez que l'interface physique comprend également l'interface virtuelle de diagnostic, que vous pouvez configurer sur la page **Interfaces** avec d'autres interfaces physiques. Reportez-vous àInterface de gestion/dépistage pour obtenir plus de renseignements sur l'interface de diagnostic.

L'interface de gestion a deux utilisations :

- Vous pouvez ouvrir des connexions Web et SSH à l'adresse IP et configurer l'appareil au moyen de l'interface.
- Le système obtient les licences intelligentes et les mises à niveau de la base de données grâce à cette adresse IP.

Si vous utilisez l'assistant de configuration de l'interface de ligne de commande, vous configurez l'adresse de gestion et la passerelle du périphérique lors de la configuration système initiale. Si vous utilisez l'assistant de configuration Firepower Device Manager, l'adresse de gestion et la passerelle restent les valeurs par défaut.

Si nécessaire, vous pouvez modifier ces adresses au moyen de Firepower Device Manager. Vous pouvez également modifier l'adresse de gestion et la passerelle dans l'interface de ligne de commande à l'aide des commandes **configure network ipv4 manual** et **configure network ipv6 manual**. Pour restaurer les paramètres par défaut de l'interface de gestion, utilisez la commande **configure network** {**ipv4** | **ipv6**} **dhcp-dp-route**.

Vous pouvez définir des adresses statiques ou obtenir une adresse au moyen de DHCP si un autre périphérique du réseau de gestion agit en tant que serveur DHCP. Pour la plupart des plateformes, l'interface de gestion obtient une adresse IP de DHCP par défaut.

Mise en garde Si vous modifiez l'adresse à laquelle vous êtes actuellement connecté, vous perdrez l'accès à Firepower Device Manager (ou à l'interface de ligne de commande) lorsque vous enregistrerez les modifications, car elles s'appliqueront immédiatement. Vous devrez vous reconnecter à l'appareil. Assurez-vous que la nouvelle adresse est valide et disponible sur le réseau de gestion.

Procédure

Étape 1 Cliquer sur **l'appareil**, puis cliquez sur **Systems Settings (paramètres systèmes) du lien de** > **l'interface de gestion**.

Si vous êtes déjà sur la page **System Settings** cliquez sur **interface de gestion** dans la table des matières

Étape 2 Choisissez la façon dont vous souhaitez définir la passerelle de gestion.

La passerelle détermine comment le système peut accéder à Internet pour obtenir des licences intelligentes, des mises à niveau de bases de données (telles que VDB, règle, géolocalisation, URL) et pour atteindre les serveurs DNS et NTP de gestion. Choisissez à partir de ces options :

Options IP statiques :

- **Utiliser les interfaces de données comme passerelle :** sélectionnez cette option si vous n'avez pas de réseau de gestion distinct connecté à l'interface de gestion. Le trafic est acheminé vers Internet en fonction de la table de routage, en passant généralement par l'interface externe. Cette option n'est pas prise en charge sur les appareils Firewall Threat Defense Virtual.
- **Utiliser des passerelles uniques pour l'interface de gestion :** spécifier des passerelles uniques (ci-dessous) pour IPv4 et IPv6 si vous disposez d'un réseau de gestion distinct connecté à l'interface de gestion.

Options IP de DHCP :

- **Utiliser des passerelles uniques pour l'interface de gestion avec des interfaces de secours vers les données : si le serveur DHCP fournit une passerelle, le système achemine le trafic de gestion vers la passerelle via l'interface de gestion.** Si le serveur DHCP ne fournit pas de passerelle, le système achemine le trafic de gestion en fonction de la table de tourage de l'interface de données, envoyant généralement le trafic au moyen de l'interface externe. Cette option n'est pas prise en charge sur les appareils Firewall Threat Defense Virtual.

- **Utiliser des passerelles uniques pour l'interface de gestion (pas de secours) : le système achemine le trafic de gestion via l'interface de gestion vers la passerelle fournie par le serveur DHCP.** Si le serveur DHCP ne fournit pas de passerelle, le système ne pourra atteindre que les hôtes locaux sur l'interface de gestion. Pour acheminer au moyen des interfaces de données, choisir l'option de secours.

Étape 3 Configurez l'adresse de gestion, le masque de sous-réseau ou le préfixe IPv6 et la passerelle (si nécessaire) pour IPv4, IPv6 ou les deux.

Vous devez configurer au moins un ensemble de propriétés. Laissez un ensemble vide pour désactiver cette méthode d'adressage.

Sélectionnez le type **de** > **DHCP**pour obtenir l'adresse et la passerelle au moyen de la configuration automatique DHCP ou IPv6.

Étape 4 (Facultatif) Si vous configurez une adresse IPv4 statique, configurez un serveur DHCP sur l'interface.

Si vous configurez un serveur DHCP sur l'interface de gestion, les clients du réseau de gestion peuvent obtenir leur adresse à partir du pool DHCP. Cette option n'est pas prise en charge sur les appareils Firewall Threat Defense Virtual.

a) Cliquez **Enable DHCP Server (activer le serveur DHCP)** > **sur**.
b) Entrer **le pool d'adresses** pour le serveur.

Le pool d'adresses est la plage d'adresses IP, de la plus basse à la plus haute, que le serveur est autorisé à fournir aux clients qui demandent une adresse. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'adresse de gestion et ne peut pas inclure : l'adresse IP de l'interface elle-même, l'adresse de diffusion ou l'adresse réseau du sous-réseau. Indiquez les adresses de début et de fin de l'ensemble, séparées par un tiret. Par exemple, 192.168.45.46-192.168.45.254.

Étape 5 Cliquez sur **Save (Enregistrer)**, lisez l'avertissement, puis cliquez sur **OK**.

Configurez le nom d'hôte du périphérique.

Vous pouvez modifier le nom d'hôte du périphérique.

Vous pouvez également modifier le nom d'hôte dans l'interface de ligne de commande à l'aide de la commande **configure network hostname**.

⚠

Mise en garde Si vous modifiez le nom d'hôte lorsque vous êtes connecté au système en utilisant ce nom, vous perdrez l'accès à Firepower Device Manager lorsque vous enregistrerez les modifications, car elles s'appliquent immédiatement. Vous devrez vous reconnecter à l'appareil.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur le lien **System Settings (Paramètres du système)** > **Hostname (Nom d'hôte)**.

Si vous êtes déjà sur la page des paramètres système, cliquez simplement sur **Hostname** (Nom d'hôte) dans la table des matières.

Étape 2 Entrez un nouveau nom d'hôte.

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

La modification du nom d'hôte est immédiatement appliquée à certains processus système. Cependant, vous devez déployer les modifications pour terminer la mise à jour afin que le même nom soit utilisé par tous les processus du système.

Protocole de temps réseau (NTP)

Vous devez configurer les serveurs Network Time Protocol (NTP) pour définir l'heure sur le système. Vous configurez les serveurs NTP lors de la configuration initiale du système, mais vous pouvez les modifier à l'aide de la procédure suivante. Si vous avez des problèmes avec la connexion NTP, consultez Dépannage du protocole NTP.

Le périphérique Firewall Threat Defense prend en charge NTPv4.

Remarque Pour le Firepower 4100/9300, vous ne définissez pas le NTP par l'intermédiaire de Firepower Device Manager. Configurez le NTP dans FXOS.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **Time Services (Services de temps)**.

Si vous êtes déjà sur la page System Settings (Paramètres système), cliquez simplement sur **Time Services (Services de temps)** dans la table des matières.

Étape 2 Dans **NTP Time Server** (Serveur de temps NTP), sélectionnez si vous souhaitez utiliser vos propres serveurs de temps ou ceux de Cisco.

- **Default NTP Servers (Serveurs NTP par défaut)**—Si vous sélectionnez cette option, la liste des serveurs affiche les noms des serveurs utilisés pour le NTP.
- **User-Defined NTP Servers (Serveurs NTP définis par l'utilisateur)**—Si vous sélectionnez cette option, saisissez le nom de domaine complet ou l'adresse IPv4 ou IPv6 du serveur NTP que vous souhaitez utiliser. Par exemple, ntp1.exemple.com ou 10.100.10.10. Vous pouvez ajouter jusqu'à 3 serveurs NTP.

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

Configuration du protocole Precision Time Protocol (PTP) (ISA 3000)

Le protocole PTP (Precision Time Protocol) est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques au sein d'un réseau par paquets. Ces horloges sont généralement de précision et de stabilité variables. Le protocole est spécialement conçu pour les systèmes de mesure et de contrôle industriels en réseau. Il est idéal pour une utilisation dans les systèmes distribués, car il nécessite une bande passante et un surdébit de traitement minimaux.

Un système PTP est un système en réseau distribué, composé d'une combinaison de périphériques PTP et non-PTP. Les périphériques PTP comprennent les horloges normales, les horloges périphériques et les horloges transparentes. Les périphériques non PTP comprennent les commutateurs réseau, les routeurs et les autres périphériques de l'infrastructure.

Vous pouvez configurer le périphérique Firewall Threat Defense pour qu'il soit une horloge transparente. Le périphérique Firewall Threat Defense ne synchronise pas son horloge avec les horloges PTP. Le périphérique Firewall Threat Defense utilisera le profil PTP par défaut, comme défini sur les horloges PTP.

Lorsque vous configurez les périphériques PTP, vous définissez un numéro de domaine pour les périphériques destinés à fonctionner ensemble. Ainsi, vous pouvez configurer plusieurs domaines PTP, puis configurer chaque périphérique non PTP pour utiliser les horloges PTP d'un domaine spécifique.

Avant de commencer

Déterminez le numéro de domaine configuré sur les horloges PTP que le périphérique doit utiliser. Déterminez également les interfaces par lesquelles le système peut atteindre les horloges PTP du domaine.

Voici des consignes pour la configuration du PTP :

- Cette fonctionnalité est uniquement disponible sur le périphérique Cisco ISA 3000.
- Cisco PTP prend uniquement en charge les messages PTP en multidiffusion.
- Le PTP est disponible uniquement pour les réseaux IPv4, et non pour les réseaux IPv6.
- La configuration PTP est prise en charge sur les interfaces de données Ethernet physiques, qu'elles soient autonomes ou membres d'un groupe de ponts. Elle n'est pas prise en charge sur l'interface de gestion, les sous-interfaces, les EtherChannels, les interfaces virtuelles de pont (BVI) ou toute autre interface virtuelle.
- Les flux PTP sur les sous-interfaces VLAN sont pris en charge, en supposant que la configuration PTP appropriée est présente sur l'interface parente.
- Vous devez vous assurer que les paquets PTP sont autorisés à circuler dans le périphérique. Le trafic PTP est identifié par les ports de destination UDP 319 et 320 et par l'adresse IP de destination 224.0.1.129, donc toute règle de contrôle d'accès qui autorise ce trafic devrait fonctionner.
- Lorsque les paquets PTP circulent entre des interfaces routées, vous devez activer le routage de multidiffusion et chaque interface doit rejoindre le groupe de multidiffusion IGMP 224.0.1.129. Lorsque les paquets PTP circulent entre des interfaces du même groupe de ponts, vous n'avez pas besoin d'activer le routage de multidiffusion ni de configurer le groupe IGMP.

Procédure

Étape 1 Vérifiez la configuration des interfaces orientées horloge PTP.

La configuration par défaut place toutes les interfaces dans le même groupe de ponts, mais vous pouvez retirer des interfaces du groupe de ponts. Il est important de déterminer si les interfaces sont routées ou membres de groupes de ponts, car vous devez les configurer différemment par rapport aux groupes IGMP de multidiffusion.

La procédure suivante explique comment déterminer quelles interfaces font partie du groupe de ponts. Vérifiez si les interfaces que vous configurez pour le PTP sont membres de groupes de ponts.

a) Cliquez sur **View All Interfaces** (Afficher toutes les interfaces) dans **Device (Périphérique)** > **Interfaces**.
b) Recherchez les interfaces dans la liste et vérifiez la colonne Mode. BridgeGroupMember signifie qu'il fait partie d'un groupe de ponts, sinon il doit être routé.

Étape 2 Cliquez sur **Device (Périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **Time Services (Services de temps)**.

Si vous êtes déjà sur la page **System Settings** (Paramètres du système, cliquez simplement sur **Time Services** (Services de temps) dans la table des matières.

Étape 3 Configurez les paramètres PTP :

- **Domain Number** (Numéro de domaine) : numéro de domaine configuré sur les périphériques PTP de votre réseau, de 0 à 255. Les paquets reçus dans un domaine différent sont traités comme des paquets de multidiffusion ordinaires et ne subissent aucun traitement PTP.
- **Clock Mode** (Mode horloge) : sélectionnez **EndToEndTransparent**. Vous ne pouvez utiliser le périphérique que comme horloge transparente PTP.

  Vous pouvez également sélectionner **Forward**, mais cela revient essentiellement à ne pas configurer PTP. Le numéro de domaine est ignoré. Les paquets PTP passent par le périphérique en fonction de la table de routage du trafic de multidiffusion. Il s'agit de la configuration PTP par défaut.
- **Interfaces** : sélectionnez toutes les interfaces par lesquelles le système peut se connecter à l'horloge PTP dans votre réseau. Le protocole PTP est activé uniquement sur ces interfaces.

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

Étape 5 Si certaines des interfaces que vous avez sélectionnées sont des interfaces routées, c'est-à-dire qu'elles ne sont pas membres d'un groupe de ponts, vous devez utiliser FlexConfig (FlexConfig) pour activer le routage de multidiffusion et joindre les interfaces routées au groupe IGMP approprié.

N'effectuez pas cette étape si toutes les interfaces sélectionnées sont membres d'un groupe de ponts. Vous obtiendrez un échec de déploiement si vous tentez de configurer IGMP sur un membre d'un groupe de ponts.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.
b) Cliquez sur **FlexConfig** > **FlexConfig Objects** (Objets FlexConfig) dans la table des matières de Advanced Configuration (Configuration avancée).
c) Créez l'objet nécessaire pour activer le routage de multidiffusion et configurer la jonction IGMP pour les interfaces routées.

   Voici le modèle de base pour l'objet. Dans cet exemple, GigabitEthernet1/2 est la seule interface routée sur laquelle vous activez le protocole PTP. Modifiez le nom matériel de l'interface, au besoin, et si vous

avez plusieurs interfaces routées, répétez les commandes **interface** et **igmp** pour chaque interface supplémentaire.

La commande **igmp** rejoint le groupe IGMP 224.0.1.129. Il s'agit de l'adresse IP correcte pour toutes les interfaces, quelle que soit l'adresse réseau.

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

Le modèle de négation ressemblerait à ce qui suit :

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières, ajoutez cet objet à la politique FlexConfig, puis cliquez sur **Save** (Enregistrer).

Vérifiez que l'aperçu affiche les commandes attendues provenant de votre objet.

Prochaine étape

Après avoir déployé les modifications, vous pouvez vérifier les paramètres PTP. Depuis la console d'interface de ligne de commande Firepower Device Manager, ou à partir d'une session SSH ou Console, exécutez les différentes commandes **show ptp**. Par exemple, si vous avez configuré le protocole PTP pour le domaine 10 uniquement sur GigabitEthernet1/2, la sortie peut ressembler à ce qui suit :

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
```

```
PTP version: 2
Port state: Disabled
```

Configuration du serveur mandataire HTTP pour les connexions de gestion

S'il n'y a pas de connexion directe entre le système et Internet, vous pouvez configurer un serveur mandataire HTTP pour l'interface de gestion. Le système utilisera ensuite le serveur mandataire pour toutes les connexions de gestion, y compris les connexions à Firepower Device Manager et du système à Cisco pour le téléchargement des mises à jour de la base de données.

Vous pouvez également configurer un serveur mandataire HTTP dans l'interface de ligne de commande Firewall Threat Defense à l'aide de la commande **configure network http-proxy**.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien **System Settings (Paramètres système)** > **HTTP Proxy**.

Si vous êtes déjà sur la page **System Settings** (Paramètres système), cliquez simplement sur **HTTP Proxy** dans la table des matières.

Étape 2 Cliquez sur la bascule pour activer le serveur mandataire, puis configurez les paramètres du serveur mandataire :

- **HTTP Proxy** : adresse IP du serveur mandataire.
- **Port** : numéro de port auquel le serveur mandataire est configuré pour surveiller les connexions HTTP.
- **Utiliser l'authentification du serveur mandataire** : sélectionnez cette option si le serveur est configuré pour exiger l'authentification pour les connexions par serveur mandataire. Si vous sélectionnez cette option, saisissez également le **nom d'utilisateur** et **le mot de passe** d'un compte qui peut se connecter au serveur mandataire.

Étape 3 Cliquez sur **Save** (Enregistrer), puis confirmez que vous souhaitez apporter la modification.

Vos modifications sont appliquées immédiatement. Une tâche de déploiement n'est pas nécessaire.

Comme vous modifiez la façon dont le système effectue les connexions de gestion, vous perdrez votre connexion à Firepower Device Manager. Attendez quelques minutes que la modification soit terminée, puis actualisez la fenêtre de votre navigateur et connectez-vous de nouveau.

Configuration de Cisco Cloud Services

Vous pouvez vous inscrire aux services en nuage pour pouvoir utiliser diverses applications en nuage, comme CDO, Cisco Threat Response et le Cisco Success Network.

Une fois enregistré dans le nuage, la page affiche l'état de l'enregistrement et le type de location, ainsi que le nom du compte sous lequel l'appareil est enregistré.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page **System Settings (paramètres système)**, cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Si votre appareil n'est pas enregistré, cette page affiche les méthodes d'enregistrement pour l'enregistrement dans le nuage de Cisco. Après votre inscription au nuage, vous serez en mesure d'activer ou de désactiver les services en nuage individuels.

Étape 2 Pour vous inscrire au nuage de Cisco (en mode d'évaluation ou après vous être désinscrit de Cisco Cloud services), sélectionnez l'une des options suivantes :

- **Sécurité/**CDO**Compte** : vous pouvez utiliser l'une des méthodes suivantes :
  - **Inscription automatique auprès de la location de CDO** (Firepower 1000, 2100, Secure Firewall 3100 uniquement). Vous pouvez utiliser l'inscription automatique au lieu d'obtenir une clé d'inscription. Tout d'abord, allez à CDO et ajoutez l'appareil à l'aide du numéro de série de l'appareil. Ensuite, dans le Firepower Device Manager, activez cette case à cocher et lancez l'inscription. Obtenez le numéro de série sur le châssis de l'appareil ou sur le bon de livraison. Pour FXOS, vous pouvez aller dans l'interface de ligne de commande FXOS et utiliser la commande **show chassis detail** pour récupérer le numéro de série correct, étiqueté Serial (SN). Notez que la commande Firewall Threat Defense **show serial-number** fournit un numéro de série différent, ce qui n'est pas recommandé pour l'enregistrement CDO. Cette méthode fonctionne pour le le mode en nuage On-Prem Firewall Management Center dans CDO, ainsi que l'ancien mode de gestionnaire d'appareil dans CDO.

    Remarque
    L'ancien mode gestionnaire de dispositifs n'est disponible que pour les utilisateurs existants qui gèrent déjà les appareils Firewall Threat Defense dans ce mode.

  - Connectez-vous à votre compte CDO ou à un autre compte de sécuritéet générez une clé d'enregistrement. Revenez ensuite à cette page, sélectionnez votre**Cisco Cloud Services Region (région de Cisco Cloud Services)**, et collez votre **Registration Key (clé d'enregistrement)**. Cette méthode ne fonctionne qu'avec l'ancien mode de gestionnaire d'appareils dans CDO. Pour le centre de gestion en nuage dans CDO, consultez Passer du gestionnaire d'appareils au centre de gestion ou CDO.

    Remarque
    Le mode gestionnaire de dispositifs n'est disponible que pour les utilisateurs existants qui gèrent déjà les appareils Firewall Threat Defense dans ce mode.

    Vous pouvez également activer **Cisco Defense Orchestrator** et **Cisco Success Network** à ce stade. Ceux-ci sont activés par défaut.

- **Licence Smart** : (uniquement si vous ne l'utilisez pas.)CDO Cliquez sur le lien pour accéder à la page de licences Smart et vous inscrire auprès de CSSM. L'enregistrement auprès du CSSM enregistre également l'appareil auprès de Cloud Services .

  Remarque

Si vous vous êtes désinscrit de Cloud Services, alors l'approche Smart License de l'inscription comporte quelques étapes supplémentaires. Dans ce cas, sélectionnez **Cloud Services Region (région Cisco Cloud Services)**, puis cliquez sur **Register (inscription)**. Lisez la divulgation et cliquez sur **Accept (accepter)**.

Étape 3 Une fois que vous vous êtes inscrit aux services en nuage, vous pouvez activer ou désactiver des fonctionnalités selon vos besoins. Consultez les rubriques suivantes:

- Activation ou désactivation CDO (Mode gestionnaire d'appareil existant)
- Connexion à Cisco Success Network, à la page 32
- Envoi d'événements à Cisco Cloud, à la page 33
- Se désinscrire de Cisco Cloud services, à la page 34

Activation ou désactivation CDO (Legacy Device Manager Mode (mode de gestionnaire d'appareil existant))

Remarque Cette section s'applique uniquement à l'ancien mode de gestionnaire d'appareils dans CDO, et non au centre de gestion en nuage.

Si vous vous êtes inscrit aux services en nuage à l'aide d'une clé d'enregistrement de CDO, comme recommandé dans Configuration de Cisco Cloud Services, à la page 29, l'appareil est déjà enregistré avec CDO. Ensuite, vous pouvez désactiver ou réactiver la connexion comme vous le souhaitez.

Si l'appareil est enregistré auprès de Cisco Cloud Services à l'aide de licences intelligentes, vous aurez des problèmes si vous activez CDO : l'appareil n'apparaîtra pas dans l'inventaire CDO. Nous vous recommandons fortement de désinscrire d'abord l'appareil de Cisco Cloud services; sélectionnez **Unregister Cloud Services (annuler l'enregistrement de Cisco Cloud services)** dans la liste déroulante de l'équipement ( ). Après vous être désinscrit, obtenez un jeton d'enregistrement auprès de CDO et réinscrivez-vous à l'aide du jeton et de votre compte de sécurité, comme expliqué dans Configuration de Cisco Cloud Services, à la page 29.

pour obtenir plus de renseignements sur le fonctionnement de la gestion du cloud, consultez le portailCDO (http://www.cisco.com/go/cdo) ou demandez au revendeur ou au partenaire avec lequel vous travaillez.

Avant de commencer

Si vous avez l'intention de configurer la haute disponibilité, vous devez enregistrer les deux périphériques que vous utiliserez dans le groupe de haute disponibilité.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Cliquez sur le bouton **Enable**/**Disable** (activer/Désactiver) pour que la fonctionnalité CDO modifie le paramètre en conséquence.

Connexion à Cisco Success Network

Lorsque vous enregistrez l'appareil, vous décidez si vous souhaitez activer la connexion à Cisco Success Network. Consultez Enregistrement de l'appareil.

En activant le Cisco Success Network, vous fournissez à Cisco des informations et des statistiques d'utilisation qui sont essentielles pour que Cisco puisse vous fournir une assistance technique. Ces informations permettent également à Cisco d'améliorer le produit et de vous informer des fonctionnalités disponibles inutilisées afin de maximiser la valeur du produit sur votre réseau.

Lorsque vous activez la connectivité, votre appareil établit une connexion sécurisée avec Cisco Cloud afin que votre appareil puisse participer à des offres de services supplémentaires de Cisco, tels que les Services d'assistance technique de Cisco, la gestion du cloud et les services de surveillance. Votre appareil établira et maintiendra cette connectivité sécurisée à tout moment. pour obtenir plus de renseignements sur la déconnexion complète du nuage, consultez Se désinscrire de Cisco Cloud services, à la page 34.

Une fois que vous avez enregistré le périphérique, vous pouvez modifier le paramètre du Cisco Success Network.

Remarque Lorsque le système envoie des données à Cisco, la liste des tâches affiche une tâche de télémétrie.

Avant de commencer

Pour activer le Cisco Success Network, l'appareil doit être inscrit dans le nuage. Pour inscrire l'appareil, enregistrez l'appareil avec Cisco Smart Software Manager (sur la page de licence Smart), en sélectionnant l'option Cisco Success Network lors de l'inscription, ou inscrivez-vous avec CDO en entrant une clé d'inscription (mode gestionnaire d'appareils hérité dans CDO uniquement).CDO

Remarque Si vous activez le Cisco Success Network sur l'unité active dans un groupe à haute disponibilité, vous activez également la connexion sur l'unité en veille.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Cliquez sur le contrôle **Enable (activer)**/**Disable (désactiver)** de la fonctionnalité Cisco Success Network pour modifier le paramètre en conséquence.

Vous pouvez cliquer sur le lien de **sample data (l'exemple de données)** pour voir le type d'informations envoyées à Cisco.

Lorsque vous activez la connexion, lisez la divulgation et cliquez sur **Accep (accepter)**.

Envoi d'événements à Cisco Cloud

Vous pouvez envoyer des événements au serveur Cisco Cloud. À partir de là, divers services de Cisco Cloud peuvent accéder aux événements. Vous pouvez ensuite utiliser ces applications en nuage pour analyser les événements et évaluer les menaces que l'appareil pourrait avoir rencontrées.

Les outils en nuage déterminent si les événements que vous envoyez sont utilisés. Consultez la documentation de l'outil ou examinez les données d'événements pour vous assurer que vous n'envoyez pas d'événements inutilisés vers Cisco Cloud, ce qui gaspillerait votre bande passante et votre espace de stockage. Gardez à l'esprit que les outils tirent les événements de la même source, de sorte que votre sélection doit refléter tous les outils que vous utilisez, pas seulement l'outil le plus restrictif. Par exemple :

- L'outil Security Analytics and Logging (analyse et journalisation de la sécurité) dans CDO peut utiliser tous les événements de connexion.
- Threat Response utilise uniquement des événements de connexion de haute priorité, il n'est donc pas nécessaire d'envoyer tous les événements de connexion au nuage. En outre, il utilisera uniquement les événements hautement prioritaires des informations de sécurité.

Avant de commencer

Vous devez inscrire l'appareil à Cisco Cloud avant de pouvoir activer ce service.

Vous pouvez vous connecter à https://visibility.amp.cisco.com/ dans la région des États-Unis , https://visibility.eu.amp.cisco.com dans la région de l'UE et https://visibility.apjc.amp.cisco.com dans la région de l'APJC. Vous pouvez regarder des vidéos sur l'utilisation et les avantages de l'application sur YouTube à http://cs.co/CTRvideos. Pour en savoir plus, consultez le *Guide d'intégration Cisco Secure Firewall Threat Defense et SecureX*, que vous pouvez trouver à https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Cliquez sur le contrôle **Enable (activer)**/**Disable (désactiver)** pour l'option **Send Events to the Cisco Cloud (Envoyer les événements vers Cisco Cloud)** afin de modifier le paramètre en conséquence.

Étape 3 Lorsque vous activez le service, vous êtes invité à sélectionner les événements à envoyer au nuage. Vous pouvez modifier ces sélections ultérieurement en cliquant sur **Edit (Modifier)** en regard de la liste des événements sélectionnés. Sélectionnez les types d'événements à envoyer et cliquez sur **OK**.

- **Programme malveillant** : pour toutes les politiques de fichier que vous avez appliquées dans n'importe quelle règle de contrôle d'accès.
- **Intrusion** : pour toutes les politiques d'intrusion que vous avez appliquées dans n'importe quelle règle de contrôle d'accès.
- **Connexion** : pour les règles de contrôle d'accès lorsque vous avez activé la journalisation. Lorsque vous sélectionnez cette option, vous pouvez également choisir d'envoyer tous les événements de connexion ou d'envoyer uniquement les événements de connexion de haute priorité. Les événements de connexion hautement prioritaires sont ceux liés aux connexions qui déclenchent des événements d'intrusion, de fichier ou de programme malveillant, ou qui correspondent aux politiques de blocage des informations de sécurité.

Se désinscrire de Cisco Cloud services

Si vous ne souhaitez plus utiliser les services en nuage, vous pouvez désinscrire l'appareil du nuage. Vous souhaiterez peut-être annuler l'enregistrement lorsque vous retirez le périphérique du service ou que vous l'éliminez de quelque manière que ce soit. Si vous devez modifier la région de vos services en nuage, vous devez vous désinscrire, puis sélectionner la nouvelle région lors de votre réinscription.

La désinscription du nuage à l'aide de cette procédure n'a aucune incidence sur l'inscription de la licence Smart.

Procédure

Étape 1 Cliquez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Cisco Cloud Services**.

Si vous êtes déjà sur la page System Settings (paramètres système), cliquez simplement sur **Cisco Cloud Services** dans la table des matières.

Étape 2 Sélectionnez **Unregister Cloud Services (annuler l'enregistrement de Cisco Cloud services)** dans la liste déroulante de l'icône en forme d'engrenage ( ).

Étape 3 Lisez l'avertissement et cliquez sur **Unregister (annuler l'inscription)**.

Tous les services en nuage que vous avez activés seront automatiquement désactivés et votre capacité à les réactiver sera supprimée. Cependant, vous verrez maintenant les commandes d'enregistrement dans le nuage et vous pourrez vous inscrire à nouveau.

Activation ou désactivation de l'analyse Web

L'activation de l'analyse Web fournit à Cisco des informations anonymes sur l'utilisation du produit en fonction des pages visitées. Ces renseignements comprennent les pages consultées, le temps passé sur une page, les versions des navigateurs, la version du produit, le nom d'hôte de l'appareil, etc. Ces renseignements peuvent aider Cisco à déterminer les modèles d'utilisation des fonctionnalités et à aider Cisco à améliorer le produit. Toutes les données d'utilisation sont anonymes, et aucune donnée sensible n'est transmise.

L'analyse Web est activée par défaut.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **Web Analytics (Analyse Web)**.

Si vous êtes déjà dans la page System Settings (Paramètres système), cliquez simplement sur **Web Analytics (Analyse Web)** dans la table des matières.

Étape 2 Cliquez sur le contrôle **Enable**/**Disable** (Activer/Désactiver) de la fonctionnalité **Web Analytics** (Analyse Web) pour modifier le paramètre, au besoin.

Configuration des préférences de filtrage Cloud

Le système obtient la base de données de catégorie URL et de réputation auprès de Cisco Renseignements collectifs sur la sécurité (CSI) (Cisco Talos Intelligence Group (Talos)). Ces préférences contrôlent les mises à jour de la base de données et la façon dont le système gère les URL de catégorie ou de réputation inconnue. Vous devez activer la licence de filtrage d'URL pour définir ces préférences.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur le lien **System Settings (Paramètres système)** > **URL Filtering Preferences (Préférences de filtrage d'URL)**.

Si vous êtes déjà sur la page System Settings (Paramètres système), cliquez simplement sur **URL Filtering Preferences (Préférences de filtrage d'URL)** dans la table des matières.

Étape 2 Configurez les options suivantes :

- **Enable Automatic Updates (Activer les mises à jour automatiques)** : permet au système de vérifier et de télécharger automatiquement les données d'URL mises à jour, qui comprennent les informations de catégorie et de réputation. Le système recherche les mises à jour toutes les 30 minutes, bien que les données soient généralement mises à jour une fois par jour. La valeur par défaut est d'activer les mises à jour. Si vous désélectionnez cette option et que vous utilisez le filtrage de catégorie et de réputation, activez-le périodiquement pour obtenir de nouvelles données URL.

- **URL Query Source** (Source de requête d'URL) : quelle source interroger pour obtenir la catégorie et la réputation d'une URL.
  - **Local Database Only** (Base de données locale uniquement) : recherchez la catégorie et la réputation dans la base de données de filtrage d'URL locale uniquement. S'il n'y a aucune correspondance, l'URL ne sera pas classée et n'aura aucune réputation. Cette méthode peut être limitée, en particulier sur les systèmes bas de gamme qui ont un stockage limité et donc une base de données de filtrage d'URL plus petite.
  - **Local Database and Cisco Cloud** (Base de données locale et nuage Cisco) : si aucune correspondance n'est trouvée dans la base de données locale, le nuage Cisco est consulté pour obtenir des informations mises à jour sur la catégorie ou la réputation. Si une réponse est reçue en temps utile, elle est utilisée à des fins de correspondance. Sinon, s'il n'y a pas de correspondance, l'URL ne sera pas classée et n'aura aucune réputation.
  - **Cisco Cloud Only (Cisco Cloud uniquement)** : interrogez toujours le Cisco Cloud pour obtenir des informations de catégorie et de réputation. N'utilisez pas la base de données d'URL locale.
- **URL Time to Live** (Durée de vie de l'URL) (disponible si vous sélectionnez **Query Cisco CSI for Unknown URLs (Interroger Cisco CSI pour les URL inconnues)**) : durée de mise en cache des valeurs de recherche de catégorie et de réputation pour une URL donnée. À l'expiration de la durée de vie, la prochaine tentative d'accès de l'URL entraîne une nouvelle recherche de catégorie ou de réputation. Un délai plus court permet un filtrage d'URL plus précis, un délai long améliore les performances pour les URL inconnues. Vous pouvez définir le TTL à 2, 4, 8, 12, 24 ou 48 heures, une semaine ou Jamais (par défaut).

Étape 3 Au besoin, vous pouvez **Check the Category (Vérifier la catégorie)** pour une URL.

Vous pouvez vérifier la catégorie et la réputation d'une URL particulière. Saisissez l'URL dans le champ **URL to Check** (URL à vérifier), puis cliquez sur **Go** (Lancer). Vous serez redirigé vers un site Web externe pour consulter les résultats. Si vous êtes en désaccord avec une catégorisation, cliquez sur le lien **Submit a URL Category** Dispute (Soumettre une contestation de catégorie d'URL) et faites-le-nous savoir.

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

Passer de Firewall Device Manager à On-Prem Firewall Management Center ou CDO

Vous pouvez configurer le périphérique Firewall Threat Defense de manière à ce qu'il se connecte au On-Prem Firewall Management Center ou au CDO pour la gestion si vous souhaitez changer de Firepower Device Manager.

Remarque CDO peut gérer des périphériques Firewall Threat Defense à l'aide du centre de gestion en nuage. La fonctionnalité simplifiée de gestionnaire de périphériques de CDO n'est disponible que pour les utilisateurs existants qui gèrent déjà Firewall Threat Defense dans ce mode. Cette procédure s'applique uniquement au centre de gestion en nuage.

Lorsque vous effectuez la configuration du On-Prem Firewall Management Center/CDO à l'aide du Firepower Device Manager, *toute* la configuration de l'interface effectuée dans Firepower Device Manager est conservée lorsque vous passez au On-Prem Firewall Management Center/CDO pour la gestion, en plus de l'interface de gestion et des paramètres d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande Firewall Threat Defense pour la configuration initiale de On-Prem Firewall Management Center/CDO, seuls l'interface de gestion et les paramètres d'accès du gestionnaire sont conservés (par exemple, la configuration par défaut de l'interface interne n'est pas conservée).

Après avoir basculé vers le On-Prem Firewall Management Center/CDO, vous ne pouvez plus utiliser le Firepower Device Manager pour gérer le périphérique Firewall Threat Defense.

Avant de commencer

Si le pare-feu est configuré pour la haute disponibilité, vous devez d'abord interrompre la configuration à haute disponibilité à l'aide de Firepower Device Manager (si possible) ou de la commande **configure high-availability disable**. Idéalement, cassez la haute disponibilité de l'unité active.

Procédure

Étape 1 Si vous avez enregistré le pare-feu dans Cisco Smart Software Manager, vous devez vous désinscrire avant de changer de gestionnaire. Consultez Désinscrire le périphérique.

La désinscription du pare-feu libère la licence de base et toutes les licences de fonctionnalités. Si vous ne désinscrivez pas le pare-feu, ces licences restent affectées au pare-feu dans Cisco Smart Software Manager.

Étape 2 (Peut être requis) Configurez l'interface de gestion. Consultez Configuration de l'interface de gestion, à la page 22.

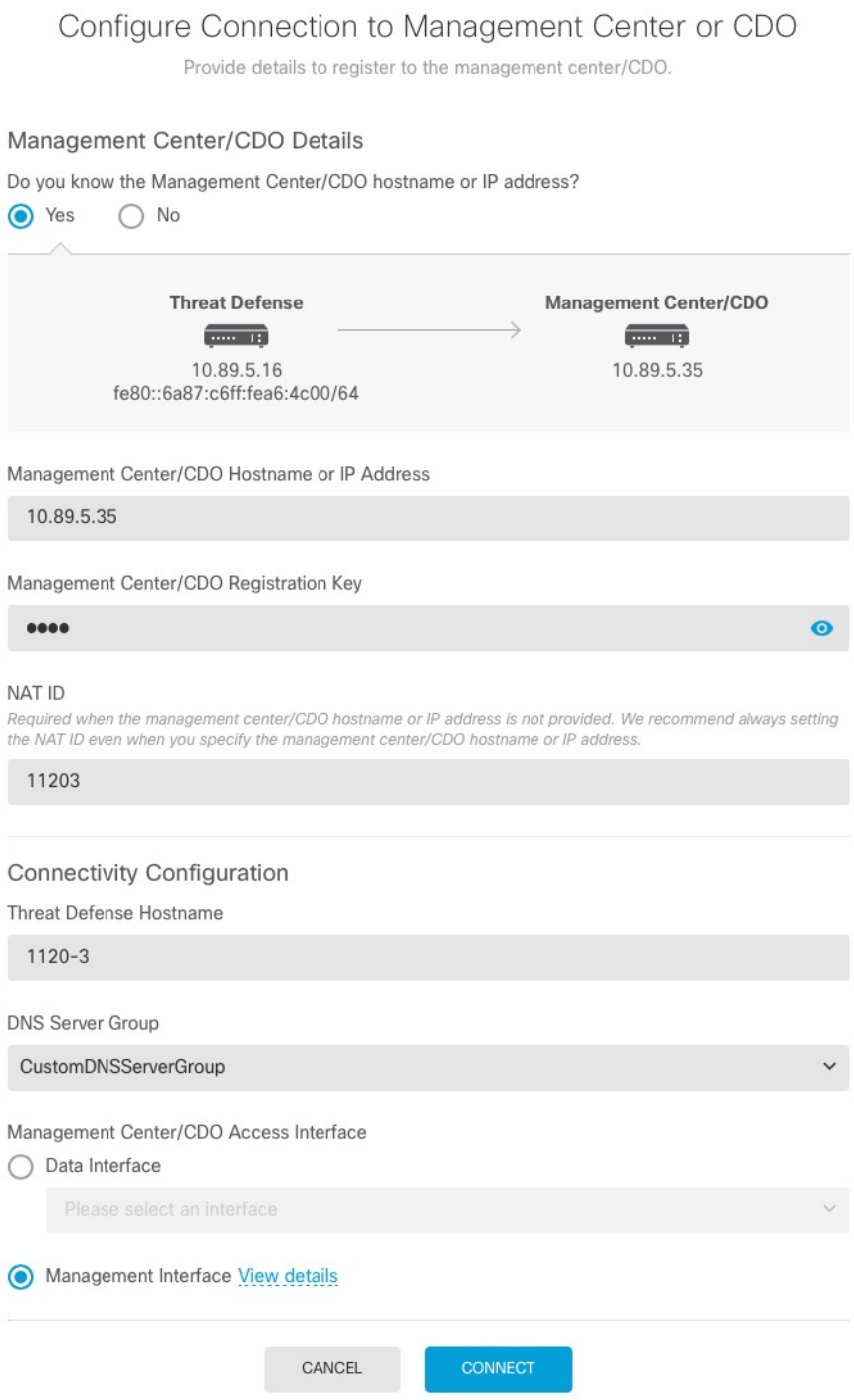
Vous devrez peut-être modifier la configuration de l'interface de gestion, même si vous avez l'intention d'utiliser une interface de données pour l'accès du gestionnaire. Vous devrez vous reconnecter au Firepower Device Manager si vous utilisiez l'interface de gestion pour la connexionFirepower Device Manager.

- Interface de données pour l'accès du gestionnaire : l'interface de gestion doit avoir la passerelle définie sur les interfaces de données. Par défaut, l'interface de gestion reçoit une adresse IP et une passerelle de DHCP. Si vous ne recevez pas de passerelle de DHCP (par exemple, vous n'avez pas connecté cette interface à un réseau), la passerelle utilisera par défaut les interfaces de données et vous n'aurez rien à configurer. Si vous avez reçu une passerelle de DHCP, vous devez plutôt configurer cette interface avec une adresse IP statique et définir la passerelle sur les interfaces de données.
- Interface de gestion pour l'accès du gestionnaire : si vous souhaitez configurer une adresse IP statique, assurez-vous également de définir la passerelle par défaut pour qu'elle soit une passerelle unique au lieu des interfaces de données. Si vous utilisez DHCP, vous n'avez pas besoin de configurer quoi que ce soit en supposant que vous ayez réussi à obtenir la passerelle à partir de DHCP.

Étape 3 Sélectionnez **Device (appareil)** > **System Settings (paramètres système)** > **Central Management (gestion centrale)**, et cliquez sur **Proceed (exécuter)** pour mettre en place la gestion du On-Prem Firewall Management Center/CDO.

Étape 4 Configurer le **Centre de gestion// Détails**/.

Illustration 1 : Détails du centre de gestion/CDO



a) Pour **Connaissez-vous le nom de domaine ou l'adresse IP du centre de gestion/CDO?** Cliquez sur **Oui** si vous pouvez atteindre le On-Prem Firewall Management Center/CDO à l'aide d'une adresse IP ou d'un nom de domaine, ou sur **Non** si le On-Prem Firewall Management CenterCDO est derrière un NAT ou n'a pas d'adresse IP ou de nom de domaine public.

Au moins l'un des appareils, soit le On-Prem Firewall Management Center/CDO ou le Firewall Threat Defense , doit avoir une adresse IP accessible pour établir le canal de communication bidirectionnel et chiffré par SSL entre les deux appareils.

b) Si vous avez choisi **Oui**, entrez le nom de domaine **ou l'adresse IP du Nom de domaine/adresse IP**

c) Indiquez la clé d'enregistrement du **centre de gestion/**.

Cette clé est une clé d'enregistrement à usage unique de votre choix que vous indiquerez également sur On-Prem Firewall Management Center/CDOlors de l'enregistrement de l'appareil Firewall Threat Defense. La clé d'enregistrement doit comporter entre 2 et 36 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet ID peut être utilisé pour plusieurs appareils s'enregistrant auprès de On-Prem Firewall Management Center/CDO.

a) Précisez un **ID NAT**.

Cet ID est une chaîne de caractères unique de votre choix que vous spécifierez également sur le site Web de On-Prem Firewall Management Center/CDO. L'identifiant de NAT doit comporter entre 2 et 36 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet ID *ne peut pas* être utilisé pour tout autre appareil s'enregistrant auprès de On-Prem Firewall Management Center/CDO. L'ID NAT est utilisé en combinaison avec l'adresse IP pour vérifier que la connexion provient du bon dispositif; Ce n'est qu'après l'authentification de l'adresse IP/de l'ID NAT que la clé d'enregistrement sera vérifiée. Nous vous recommandons de toujours utiliser l'ID NAT, même lorsqu'il est facultatif, mais il est obligatoire si :

- Vous définissez l'adresse IP On-Prem Firewall Management Center sur **DONTRESOLVE**.
- Lors de l'ajout du périphérique sur le On-Prem Firewall Management Center, vous ne spécifiez pas d'adresse IP ou de nom de domaine de périphérique accessible.
- Vous utilisez l'interface de données pour la gestion, même si vous définissez des adresses IP des deux côtés.
- Le On-Prem Firewall Management Center utilise plusieurs interfaces de gestion.

Étape 5 Configurez la **configuration de la connectivité.**

a) Précisez le **nom d'hôte FTD**.

Si vous utilisez une interface de données pour l'accès au **centre de gestion/à l'interface d'accès** , ce nom de domaine complet (FQDN) sera utilisé pour cette interface.

b) Précisez le **groupe de serveurs DNS**.

Choisissez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNServerGroup**, qui comprend les serveurs OpenDNS.

Si vous avez l'intention de choisir une interface de données pour **l'interface d'accès du centre de gestion/, l'interface**d'accès FMC, ce paramètre définit le serveur DNS de l'interface de *données*. Le serveur DNS de gestion que vous avez défini avec l'assistant de configuration est utilisé pour le trafic de gestion. Le serveur de données DNS est utilisé pour DDNS (si configuré) ou pour les politiques de sécurité s'appliquant à cette interface. Vous êtes susceptible de choisir le même groupe de serveurs DNS que celui que vous avez utilisé pour la gestion, car le trafic de gestion et de données atteint le serveur DNS par l'interface externe.

Sur le On-Prem Firewall Management Center/CDO, les serveurs DNS de l'interface de données sont configurés dans la politique de paramètres de plateforme que vous attribuez à ce dispositif Firewall Threat Defense. Quand vous ajoutez l'appareil Firewall Threat Defense au On-Prem Firewall Management

Center/CDO, le paramètre local est maintenu, et les serveurs DNS ne sont *pas* ajoutés à une politique de paramètres de plateforme. Toutefois, si vous attribuez ultérieurement à l'appareil Firewall Threat Defense une politique de paramètres de plateforme qui inclut une configuration DNS, cette configuration remplacera le paramètre local. Nous vous suggérons de configurer activement les paramètres de la plateforme DNS pour qu'ils correspondent à ce paramètre afin d'amener le On-Prem Firewall Management Center/CDO et l'appareil Firewall Threat Defense en synchronisation.

De plus, les serveurs DNS locaux ne sont conservés par le On-Prem Firewall Management Center/CDO si les serveurs DNS ont été découverts lors de l'enregistrement initial.

Si vous avez l'intention de choisir l'interface de gestion pour le **centre de gestion/ d'accèsCDO**, alors ce paramètre configure le serveur DNS de gestion.

c) Pour le **centre de gestion/ d'accès SCC/CDOl'interface**, choisissez n'importe quelle interface configurée.

Vous pouvez changer l'interface du gestionnaire après avoir enregistré l'appareil Firewall Threat Defense sur le On-Prem Firewall Management Center/CDO, pour l'interface de gestion ou une autre interface de données.

Étape 6 (Facultatif) Si vous avez choisi une interface de données et qu'il ne s'agit pas de l'interface externe, ajoutez une route par défaut.

Vous verrez un message vous demandant de vérifier que vous avez une route par défaut dans l'interface. Si vous avez choisi l'extérieur, vous avez déjà configuré cette route dans le cadre de l'assistant de configuration. Si vous avez choisi une autre interface, vous devez configurer manuellement une route par défaut avant de vous connecter au On-Prem Firewall Management Center/CDO.Reportez-vous à Configuration des routes statiquespour obtenir plus de renseignements sur la configuration des routes statiques.

Si vous avez choisi l'interface de gestion, vous devez configurer la passerelle pour qu'elle soit une passerelle unique avant de pouvoir continuer sur cet écran. Consultez Configuration de l'interface de gestion, à la page 22.

Étape 7 (Facultatif) Si vous avez choisi une interface de données, cliquez sur **Add a Dynamic DNS (DDNS) method (ajouter une méthode DNS dynamique (DDNS))**.

DDNS garantit que le On-Prem Firewall Management Center/CDO peut atteindre le périphérique Firewall Threat Defense à son nom de domaine complet (FQDN) si l'adresse IP change. Consultez **Device (appareil)** > **System Settings (paramètres système)** > **DDNS Service (service DDNS)** pour configurer le service DDNS.

Si vous configurez le DDNS avant d'ajouter le périphérique Firewall Threat Defense au On-Prem Firewall Management CenterCDO, le périphérique Firewall Threat Defense ajoute automatiquement des certificats pour toutes les principales autorités de certification de l'offre groupée d'autorités de certification racine de confiance Cisco afin que le périphérique Firewall Threat Defense puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Firewall Threat Defense prend en charge tout serveur DDNS qui utilise la spécification DynDNS Remote API (https://help.dyn.com/remote-access-api/).

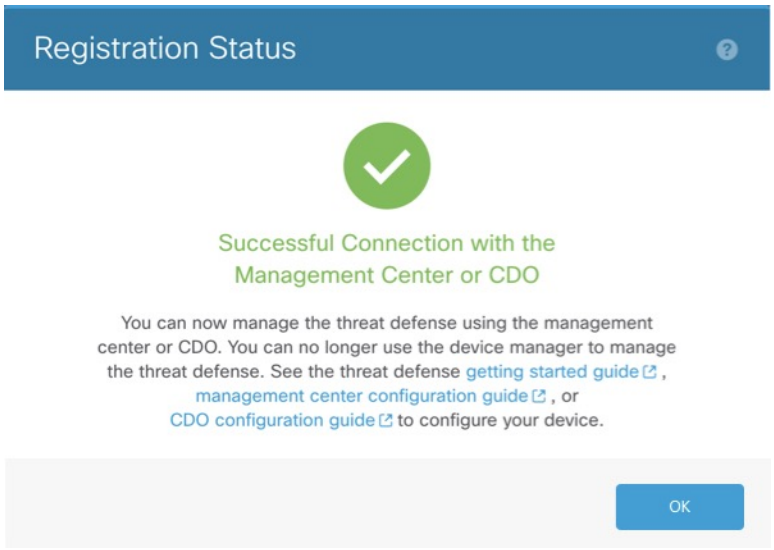
DDNS n'est pas pris en charge lors de l'utilisation de l'interface de gestion pour l'accès du gestionnaire.

Étape 8 Cliquez sur **Connect (connexion)**. La boîte de dialogue **Registration Status (état de l'enregistrement)** affiche l'état actuel du commutateur sur On-Prem Firewall Management Center/CDO. Après l'étape **d'enregistrement du centre de gestion/enregistrement des**enregistrement des paramètres d'enregistrement du FMC, accédez à On-Prem Firewall Management Center/CDO, et ajoutez le pare-feu.

Si vous souhaitez annuler le basculement vers le On-Prem Firewall Management Center/CDO, cliquez sur **Cancel Registration (annuler l'enregistrement)**. Sinon, ne fermez pas la fenêtre du navigateur Firepower Device Manager avant la fin de **l'étape d'enregistrement des paramètresd'enregistrement du centre de gestion/CDO**. Si vous le faites, le processus sera suspendu et ne reprendra que lorsque vous vous reconnecterez au.Firepower Device Manager

Si vous restez connecté à Firepower Device Manager après l'étape d'enregistrement des paramètres **d'enregistrement du CDO**vous verrez finalement la boîte de dialogue **Connexion réussie Centre de gestion** Succès de la connexion avec FMC, après quoi vous serez déconnecté du Firepower Device Manager.

Illustration 2 : Connexion réussie



Passez de l'option On-Prem Firewall Management Center ou CDO à l'option Firewall Device Manager

Vous pouvez configurer le périphérique Firewall Threat Defense actuellement géré par le On-Prem Firewall Management Center sur site ou dans le nuage pour qu'il utilise Firepower Device Manager à la place.

Vous pouvez passer de On-Prem Firewall Management Center à Firepower Device Manager sans réinstaller le logiciel. Avant de passer de On-Prem Firewall Management Center à Firepower Device Manager, vérifiez que Firepower Device Manager répond à toutes vos exigences de configuration. Si vous souhaitez passer de Firepower Device Manager à On-Prem Firewall Management Center, consultez Passer de Firewall Device Manager à On-Prem Firewall Management Center ou CDO, à la page 36.

⚠

Mise en garde Le passage à Firepower Device Manager efface la configuration du périphérique et ramène le système à la configuration par défaut. Cependant, l'adresse IP de gestion et le nom d'hôte sont conservés.

Procédure

Étape 1 Dans le On-Prem Firewall Management Center , ,supprimez le pare-feu de la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.

Étape 2 Connectez-vous à l'interface de ligne de commande Firewall Threat Defense, à partir du port de console ou à l'aide de SSH. Pour SSH, ouvrez une connexion à l'**adresse IP de gestion** et connectez-vous à la CLI Firewall Threat Defense avec le nom d'utilisateur d'**administrateur** (ou tout autre utilisateur disposant de privilèges d'administrateur).

Le port de console se connecte par défaut à l'interface de ligne de commande de FXOS. Connectez-vous à l'interface de ligne de commande Firewall Threat Defense à l'aide de la commande **connect ftd**. La session SSH se connecte directement à l'interface de ligne de commande Firewall Threat Defense.

Si vous ne pouvez pas vous connecter à l'adresse IP de gestion, effectuez l'une des opérations suivantes :

- Vérifiez que le port physique de gestion est câblé à un réseau fonctionnel.
- Assurez-vous que l'adresse IP de gestion et la passerelle sont configurées pour le réseau de gestion. Utilisez la commande **configure network ipv4/ipv6 manual**.

Étape 3 Vérifiez que vous êtes actuellement en mode de gestion à distance.

show managers

Exemple :

```
> show managers
Type                      : Manager
Host                      : 10.89.5.35
Display name              : 10.89.5.35
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
```

Étape 4 Supprimez le gestionnaire distant et passez en mode sans gestionnaire.

configure manager delete *uuid*

Vous ne pouvez pas passer directement de la gestion à distance à la gestion locale. Si vous avez défini plusieurs gestionnaires, vous devez préciser l'identifiant (également appelé UUID; voir la commande **show managers**. Supprimez chaque entrée de gestionnaire séparément.

Exemple :

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

Étape 5 Configurez le gestionnaire local.

configure manager local

Vous pouvez maintenant utiliser un navigateur Web pour ouvrir le gestionnaire local à l'adresse **https://***management-IP-address*.

Exemple :

```
> configure manager local
Deleting task list
```

```
> show managers
Managed locally.
```

Configuration des paramètres de chiffrement TLS/SSL

Les paramètres de chiffrement SSL contrôlent les versions TLS et les suites de chiffrement autorisées pour les connexions TLS/SSL avec le périphérique.

Normalement, la suite de chiffrement que vous configurez devrait avoir plusieurs suites de chiffrement disponibles. Le système déterminera la version TLS la plus élevée prise en charge par le client et le périphérique Firewall Threat Defense, puis choisira une suite de chiffrement prise en charge par les deux et compatible avec la version TLS. Le système sélectionnera la version TLS et la suite de chiffrement les plus puissantes prises en charge par les deux points terminaux pour assurer la connexion la plus sécurisée possible parmi les chiffrements que vous autorisez.

Avant de commencer

Par défaut, le système utilise l'objet DefaultSSLCipher pour définir les suites de chiffrement autorisées. Vous pouvez plutôt choisir l'un des autres objets de chiffrement prédéfinis ou créer votre propre objet personnalisé. Idéalement, créez un seul objet qui inclut toutes les versions et uniquement les chiffrements TLS que vous souhaitez autoriser. Pour créer votre propre objet, consultez Configurer les objets de chiffrement TLS/SSL, à la page 44.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien **System Settings (Paramètres du système)** > **SSL Settings (Paramètres SSL)**.

Étape 2 Configurer les **paramètres SSL** :

Ces paramètres contrôlent les chiffrements que les clients sont autorisés à utiliser lors de l'établissement des connexions à distance au réseau privé virtuel.

- **Ciphers** (Chiffrements) : sélectionnez les objets de chiffrement SSL qui définissent les versions TLS et les algorithmes de chiffrement autorisés.

  Cliquez sur **Create New Cipher** (Créer un nouveau chiffrement) au bas de la liste si vous devez créer un objet maintenant.

- **Ephemeral Diffie-Hellman Group Groupe Diffie-Hellman éphémère)** : le groupe DH à utiliser pour les algorithmes de chiffrement éphémères. Pour obtenir une explication des groupes DH, consultez Choix du groupe de module Diffie-Hellman à utiliser. La valeur par défaut est 14.

- **Elliptical Curve DH Grou**p (Groupe DH de courbe elliptique) : le groupe DH à utiliser pour les algorithmes de chiffrement de courbe elliptique. Par défaut, c'est 19.

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

Configurer les objets de chiffrement TLS/SSL

Les objets de chiffrement SSL définissent une combinaison de niveau de sécurité, de versions de protocole TLS/DTLS et d'algorithmes de chiffrement qui peuvent être utilisés lors de l'établissement d'une connexion SSL avec un périphérique Firewall Threat Defense. Utilisez ces objets dans **Device (Périphérique)** > **System Settings (Paramètres système)** > **SSL Settings (Paramètres SSL)** pour définir les exigences de sécurité pour les utilisateurs qui établissent des connexions SSL avec le boîtier.

Les versions TLS et les chiffrements que vous pouvez sélectionner sont contrôlés par votre compte de licence Smart. Si vous respectez les exigences de conformité en matière d'exportation, vous pouvez sélectionner n'importe quelle combinaison d'options. Si votre licence n'est pas conforme à la norme d'exportation, vous êtes limité à TLSv1.0 et DES-DC-SHA, qui sont les options de sécurité les plus basses. Le mode d'évaluation est considéré comme un mode non conforme, de sorte que vos options sont limitées jusqu'à ce que vous obteniez une licence pour le système.

Le système comprend plusieurs objets prédéfinis. Vous ne devez créer de nouveaux objets que si les objets prédéfinis ne correspondent pas à vos exigences de sécurité. Les objets sont les suivants :

- DefaultSSLCipher : il s'agit d'un groupe de niveau de sécurité faible. Il s'agit du réglage par défaut utilisé dans les paramètres SSL pour s'assurer que le plus grand nombre de clients possible puisse effectuer les connexions au système. Il comprend toutes les versions de protocole et tous les chiffrements pris en charge par le système.
- CiscoRecommendedCipher : il s'agit d'un groupe de niveau de sécurité élevé, qui comprend uniquement les chiffrements les plus sécurisés et la version TLS. Ce groupe offre la sécurité la plus élevée, mais vous devez vous assurer que vos clients peuvent utiliser les chiffrements correspondants. Il est plus probable que certains clients ne soient pas en mesure d'établir les connexions en raison de problèmes de non-concordance de chiffrement.

Procédure

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

Étape 2 Effectuez l'une des opérations suivantes :

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

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

Étape 3 Entrez un nom pour l'objet (sous **Name**) et, facultativement, une description.

Étape 4 Configurez les options suivantes :

- **Security Level** (Niveau de sécurité) : le niveau de sécurité relatif de l'objet. Notez que si vous modifiez les versions de protocole ou la liste des suites de chiffrement après avoir sélectionné un niveau de sécurité, le niveau réel de sécurité fourni par l'objet peut ne pas correspondre au niveau de sécurité. Effectuez l'une des opérations suivantes :
  - **All** (Tout) : inclut tous les niveaux TLS et toutes les suites de chiffrement dans l'objet, de sécurité faible à sécurité élevée.

- **Low (Faible)** : comprend toutes les versions et chiffrements TLS, ce qui permet aux utilisateurs d'établir des connexions avec les chiffrements les moins sécurisés. Pour une licence non conforme à l'exportation, cela inclut TLSv1.0 et DES-CBC-SHA.
- **Medium** (Moyen) : comprend toutes les versions TLS, mais supprime certains chiffrements plutôt non sécurisés. Il n'y a qu'une différence minimale entre cette option et l'option Faible/Tout. Vous ne pouvez pas utiliser cette option avec les licences qui ne sont pas conformes à l'exportation.
- **High** (Élevé) : autorise uniquement les dernières versions DTLS et TLS, et les chiffrements qui fonctionnent avec ces versions. Cette option limite les connexions aux chiffrements les plus sécurisés actuellement disponibles. Vous ne pouvez pas utiliser cette option avec les licences qui ne sont pas conformes à l'exportation.
- **Custom** (Personnalisé) : sélectionnez cette option si vous souhaitez sélectionner les versions TLS et les chiffrements individuellement. Les options que vous sélectionnez détermineront si vous définissez un paramètre de chiffrement de sécurité élevée ou faible. Bien qu'il n'y ait pas de valeurs par défaut pour un objet personnalisé, si vous avez sélectionné un autre niveau avant de sélectionner personnalisé, les options affichées précédemment restent sélectionnées pour votre commodité.

- **Protocol Versions** (Versions de protocole) : versions TLS/DTLS qu'un client est autorisé à utiliser lors de l'établissement d'une connexion TLS/SSL avec le périphérique Firewall Threat Defense. Pour un objet personnalisé, sélectionnez les versions que vous souhaitez prendre en charge. Pour les autres niveaux de sécurité, il ne faut généralement pas modifier la liste, mais vous pouvez ajouter ou supprimer des versions comme vous le souhaitez.
- **Applicable Cipher Suites** (Suites de chiffrement applicables) : les algorithmes de chiffrement que le client peut utiliser. Cliquez sur **+** pour ajouter de nouvelles suites; cliquez sur **x** dans une suite pour la supprimer.

  Votre sélection de version de protocole contrôle les suites disponibles dans cette liste. Si vous modifiez les versions de protocole, toute suite sélectionnée qui ne fonctionne plus avec les versions sélectionnées est signalée : vous devez les supprimer ou rajouter la version de protocole requise.

Étape 5 Cliquez sur **OK**.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.