Guide de renforcement de Cisco Cisco Firepower Management Center, version 7.0

Dernière modification : 2024-10-25

Guide de renforcement de Cisco Firepower Management Center, version 7.0

Firepower protège les actifs et le trafic de votre réseau contre les cybermenaces, mais vous devez également configurer Firepower lui-même pour qu'il soit *renforcé*, ce qui réduit encore sa vulnérabilité aux cyberattaques. Ce guide traite du renforcement de votre déploiement Firepower, en se concentrant sur le Cisco Firepower Management Center (FMC). Pour obtenir des informations sur le renforcement d'autres composants de votre déploiement Firepower, consultez les documents suivants :

- *Guide de renforcement de Cisco Firepower Threat Defense, version 7.0*
- *Guide de renforcement de Cisco Firepower 4100/9300 FXOS*

Ce guide fait référence aux paramètres de configuration de l'interface Web FMC, mais n'est pas conçu comme un manuel détaillé de cette interface.

Les descriptions des fonctionnalités se réfèrent à la version 7.0 du système Firepower et les références croisées se réfèrent à la version 7.0 du Guide de configuration de Firepower Management Center. Les paramètres de configuration présentés dans ce manuel ne sont disponibles dans toutes les versions de Firepower. Pour en savoir plus sur les fonctionnalités nouvelles et obsolètes de chaque version, voir Cisco Firepower Management Center New Features by Release (nouvelles fonctionnalités de la plateforme de gestion Cisco FirePower Management Center par version). Pour obtenir des informations détaillées sur la configuration de votre déploiement Firepower, consultez la Documentation Firepower pour votre version.

Conformité des certifications de sécurité

Votre organisation peut être tenue de n'utiliser que des équipements et des logiciels conformes aux normes de sécurité établies par le Département de la défense des États-Unis ou d'autres organismes de certification gouvernementaux. Une fois certifié par une autorité de certification appropriée et configuré conformément aux documents d'orientation propres à la certification, Firepower est conçu pour se conformer aux normes de certification suivantes :

- Critères communs (CC) : Norme mondiale établie par l'accord international de reconnaissance des critères communs, définissant les exigences applicables aux produits de sécurité.
- Liste des produits approuvés du réseau d'information du ministère de la Défense (DoDIN APL) : Liste de produits répondant aux exigences de sécurité établies par la Defense Information Systems Agency (DISA) des États-Unis.

Remarque Le gouvernement américain a changé le nom de la liste des produits approuvés pour les capacités unifiées (UCAPL) en APL DODIN. Les références à UCAPL dans la documentation Firepower et l'interface Web Cisco Firepower Management Center peuvent être interprétées comme des références à DoDIN APL.

- Normes fédérales de traitement de l'information (FIPS) 140 : Un cahier des charges pour les modules de chiffrement.

Les documents d'orientation sur la certification sont disponibles séparément une fois que les certifications des produits sont terminées; la publication de ce guide de renforcement ne garantit pas l'achèvement des certifications de ces produits.

Les paramètres de configuration de Firepower décrits dans ce document ne garantissent pas une conformité stricte avec toutes les exigences actuelles de l'entité de certification. Pour en savoir plus sur les procédures de renforcement requises, se référer aux lignes directrices relatives à ce produit fournies par l'organisme de certification.

Ce document fournit des conseils pour renforcer la sécurité de votre FMC, mais certaines fonctions du FMC ne permettent pas d'assurer la conformité à la certification, même en utilisant les paramètres de configuration décrits dans le présent document. Pour en savoir plus, consultez « Security Certifications Compliance Recommendations » (recommandations de conformité pour les certifications de sécurité) dans le *Guide de configuration de Firepower Management Center, version 7.0*. Nous nous sommes efforcés de faire en sorte que ce guide de renforcement et le *le guide de configuration Firepower Management Center, version 7.0* n'entrent pas en conflit avec les directives propres à la certification. Si vous observez des contradictions entre la documentation de Cisco et les directives de certification, utilisez les directives de certification ou consultez le propriétaire du système.

Surveiller les avis de sécurité et les réponses de Cisco

L'équipe de réponse aux incidents de sécurité des produits Cisco (PSIRT) publie des avis PSIRT sur les problèmes de sécurité des produits Cisco. Pour les problèmes moins graves, Cisco publie également des réponses de sécurité Cisco. Les avis de sécurité et les réponses sont disponibles sur la page Cisco Security Advisories and Alerts (avis et alertes de sécurité de Cisco). De plus amples informations sur ces véhicules de communication sont disponibles dans la Politique relative aux vulnérabilités de sécurité de Cisco.

Pour maintenir un réseau sécurisé, restez au courant des avis de sécurité et des réponses de Cisco. Ils fournissent les informations dont vous avez besoin pour évaluer les menaces que les vulnérabilités font peser sur votre réseau. Reportez-vous à Risk Triage for Security Vulnerability Announcements (triage de risque pour les annonces de vulnérabilité de sécurité) pour obtenir de l'aide dans le cadre de ce processus d'évaluation.

Maintenir le système à jour

Cisco publie régulièrement des mises à jour du logiciel Firepower afin de résoudre les problèmes et d'apporter des améliorations. La mise à jour des logiciels de votre système est essentielle au maintien d'un système renforcé. Pour vous assurer que le logiciel de votre système est correctement mis à jour, utilisez les informations du chapitre « System Updates » (mises à jour du système) du *Guide de configuration de Firepower Management Center, version 7.0*, et du *Guide de mise à niveau de Firepower Management Center*.

Cisco publie également des mises à jour périodiques des bases de données utilisées par Firepower pour protéger votre réseau et vos biens. Pour assurer une protection optimale, les bases de données de géolocalisation, de règles d'intrusion et de vulnérabilités doivent être mises à jour. Avant de mettre à jour tout composant de

votre déploiement Firepower, vous *devez* lire les Notes de version de Cisco Firepower qui accompagnent la mise à jour. Elles fournissent des informations critiques et propres à la version, notamment sur la compatibilité, les conditions préalables, les nouvelles capacités, les changements de comportement et les avertissements. Certaines mises à jour peuvent être volumineuses et prendre un certain temps. Il est conseillé d'effectuer les mises à jour pendant les périodes de faible utilisation du réseau afin de réduire l'effet sur les performances du système.

Base de données de géolocalisation

La base de données de géolocalisation (GeoDB) est une base de données géographiques (telles que les coordonnées du pays et de la ville) et de données relatives à la connexion (telles que le fournisseur d'accès à Internet, le nom de domaine, le type de connexion) associées aux adresses IP routables. Lorsque Firepower détecte des informations GeoDB correspondant à une adresse IP détectée, vous pouvez afficher les informations de géolocalisation associées à cette adresse IP. Pour afficher des détails de géolocalisation autres que le pays ou le continent, vous devez installer la GeoDB sur votre système.

Pour mettre à jour la GeoDB à partir de l'interface Web FMC, utilisez **Système** > **Mises à jour** > **Mises à jour de géolocalisation**, et choisissez l'une des méthodes suivantes :

- Mettre à jour la GeoDB sur un FMC sans accès à Internet.
- Mettre à jour la GeoDB sur un FMC disposant d'un accès à Internet.
- Programmer des mises à jour automatiques récurrentes de la GeoDB sur un FMC disposant d'un accès à nternet.

Pour en savoir plus, consultez « Update the Geolocation Database » (Mettre à jour la base de données de géolocalisation) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Règles en matière d'intrusion

Au fur et à mesure que de nouvelles vulnérabilités sont connues, le groupe Cisco Talos Security Intelligence and Research Group (Talos) publie des mises à jour de règles d'intrusion (également connues sous le nom de Snort Rules Updates, ou SRU) que vous pouvez importer sur votre FMC, puis mettre en œuvre en déployant la configuration modifiée sur vos appareils gérés. Ces mises à jour ont une incidence sur les règles d'intrusion, les règles du préprocesseur et les politiques qui utilisent ces règles.

L'interface Web FMC propose trois approches pour mettre à jour des règles d'intrusion, toutes sous **Système** > **Mises à jour** > **Mises à jour des règles** :

- Mettre à jour des règles d'intrusion sur un FMC sans accès à Internet.
- Mettre à jour les règles d'intrusion sur un FMC disposant d'un accès à Internet.
- Programmer des mises à jour automatiques récurrentes des règles d'intrusion sur un FMC disposant d'un accès à Internet.

Pour en savoir plus, consultez « Update Intrusion Rules » (mise à jour des règles d'intrusion) dans le *Guide de configuration du centre de gestion Firepower, version 7.0*.

Vous pouvez également importer des règles d'intrusion locales en utilisant **Système** > **Mises à jour** > **Mises à jour des règles**. Vous pouvez créer des règles d'intrusion locales en suivant les instructions du manuel de l'utilisateur de Snort (disponible à l'adresse http://www.snort.org). Avant de les importer dans votre FMC, consultez les « Best Practices for Importing Local Intrusion Rules » (meilleures pratiques pour l'importation de règles l'intrusion locale) dans le *Guide de configuration de Firepower Management Center, version 7.0*

et assurez-vous que votre processus l'importation de règles l'intrusion locales est conforme à vos politiques de sécurité.

Base de données des vulnérabilités

La base de données des vulnérabilités (VDB) est une base de données des vulnérabilités connues auxquelles les hôtes peuvent être sensibles, ainsi que des empreintes digitales pour les systèmes d'exploitation, les clients et les applications. Le système utilise la VDB pour déterminer si un hôte particulier augmente le risque de compromission.

L'interface Web FMC propose deux approches pour mettre à jour la VDB :

- Mettre à jour manuellement la VDB (**Système** > **Mises à jour** > **Mises à jour de produits**).
- Planifier les mises à jour de la VDB (**Système** > **Outils** > **Planification**).

Pour en savoir plus, voir « Update the Vulnerability Database » (mettre à jour la base de données des vulnérabilités) dans le *Guide de configuration du centre de gestion Firepower, version 7.0*.

Listes et flux de renseignements sur la sécurité

Les listes et les flux de renseignements sur la sécurité sont des collections d'adresses IP, de noms de domaine et d'URL que vous pouvez utiliser pour filtrer rapidement le trafic correspondant à l'entrée d'une liste ou d'un flux.

Il existe des flux fournis par le système et des listes prédéfinies. Vous pouvez également utiliser des flux et des listes personnalisés. Pour afficher ces listes et ces flux, choisissez **Objects > Object Management > Security Intelligence (Objets > Gestion des objets > Security Intelligence)**. Dans le cadre des flux fournis par le système, Cisco fournit les flux suivants en tant qu'objets de renseignements sur la sécurité :

- Les flux de renseignements sur la sécurité sont régulièrement mis à jour avec les derniers renseignements sur les menaces de Talos :
  - Cisco-DNS-and-UR-Intelligence-Feed (sous DNS Lists and Flows)
  - Flux de renseignements Cisco (pour les adresses IP, sous Network Lists and Flows)

  Vous ne pouvez pas supprimer les flux fournis par le système, mais vous pouvez modifier (ou désactiver) la fréquence de leurs mises à jour. Le FMC peut maintenant mettre à jour les données de Cisco-Intelligence-Feed toutes les 5 ou 15 minutes.
- Cisco-TID-Feed (sous Network Lists and Feeds [Listes et flux de réseaux])

  Vous devez activer et configurer Threat Intelligence Director pour utiliser ce flux, qui est une collection de données observables TID.

Pour en savoir plus, consultez « Security Intelligence Lists and Feeds » (listes et flux de renseignements sur la sécurité) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Activer le mode CC ou UCAPL

Pour appliquer plusieurs changements de configuration de renforcement avec un seul paramètre, choisissez le mode CC ou UCAPL pour le FMC. Ce paramètre paraît sous **System (système)** > **Configuration** > **UCAPL/CC Compliance (conformité)** dans l'interface Web FMC.

Le choix de l'une de ces options de configuration met en œuvre les modifications répertoriées sous « Security Certification Compliance Characteristics » (caractéristiques de la conformité de la certification de sécurité) dans le *Guide de configuration de Firepower Management Center, version 7.0*. Sachez que tous les appareils de votre déploiement Firepower doivent fonctionner dans le même mode de conformité aux certifications de sécurité.

Mise en garde Une fois ce paramètre activé, vous ne pouvez plus le désactiver. Consultez « Security Certifications Compliance » (conformité des certifications de sécurité) dans le *Guide de configuration de Firepower Management Center, version 7.0* pour obtenir des informations complètes avant d'activer le mode CC ou UCAPL. Si vous devez inverser ce paramètre, contactez le Centre d'assistance technique de Cisco pour obtenir de l'aide.

Remarque L'activation de la conformité aux certifications de sécurité ne garantit pas le respect strict de toutes les exigences du mode de sécurité sélectionné. Les paramètres supplémentaires recommandés pour renforcer votre déploiement au-delà de ceux fournis par les modes CC ou UCAPL sont décrits dans ce document. Pour des informations complètes sur les procédures de renforcement requises pour une conformité totale, se référer aux lignes directrices pour ce produit fournies par l'entité de certification.

Sécuriser l'infrastructure du réseau local

Votre déploiement Firepower peut interagir avec d'autres ressources réseau pour un certain nombre de raisons. Le renforcement de ces autres services peut protéger votre système Firepower, ainsi que tous les actifs de votre réseau. Pour identifier tout ce qui doit être traité, essayez de schématiser le réseau et ses composants, les actifs, la configuration du pare-feu, la configuration des ports, les flux de données et les points de connexion.

Établir et respecter un processus de sécurité opérationnelle pour votre réseau qui prend en compte les questions de sécurité.

Sécuriser le serveur Network Time Protocol

La synchronisation de l'heure système sur le FMC et ses appareils gérés est essentielle au bon fonctionnement de Firepower. Il est fortement recommandé d'utiliser un serveur NTP (Network Time Protocol) sûr et fiable pour synchroniser l'heure du système sur le FMC et sur les appareils qu'il gère. À partir de l'interface Web FMC, utilisez **System (système)** > **Configuration** > **Time Synchronization (synchronisation)** et suivez les instructions de la section « Synchronize Time Using a Network NTP Server » (Synchronisation de l'heure à l'aide d'un serveur NTP de réseau) du *Guide de configuration de Firepower Management Center, version 7.0*.

Nous vous recommandons de sécuriser la communication avec les serveurs NTP en utilisant l'authentification par clé symétrique MD5, SHA-1 ou AES-128 CMAC.

Mise en garde Des conséquences inattendues peuvent se produire lorsque l'heure n'est pas synchronisée entre le FMC et les appareils gérés. Pour assurer une synchronisation correcte, configurez le FMC et tous les appareils qu'il gère pour qu'ils utilisent le même serveur NTP.

Sécuriser le système de noms de domaine (DNS)

Les ordinateurs qui communiquent entre eux dans un environnement en réseau dépendent du protocole DNS pour établir une correspondance entre les adresses IP et les noms d'hôtes. La configuration d'un FMC pour se connecter à un serveur de système de noms de domaine local fait partie du processus de configuration initiale, décrit dans le Guide de démarrage de Cisco Firepower Management Center pour votre modèle de matériel.

Le DNS peut être sensible à des types d'attaques précises conçues pour tirer parti des points faibles d'un serveur DNS qui n'est pas configuré en tenant compte de la sécurité. Assurez-vous que votre serveur DNS local est configuré conformément aux meilleures pratiques de sécurité recommandées par l'industrie; Cisco propose des lignes directrices dans ce document : http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html.

Interrogation SNMP sécurisée

Vous pouvez surveiller le FMC à l'aide de l'interrogation SNMP comme décrit dans « SNMP Polling » (interrogation SNMP) dans le Guide de configuration de Firepower Management Center, version 7.0. Si vous choisissez d'utiliser l'interrogation SNMP, vous devez savoir que la base d'informations de gestion (MIB) SNMP contient des détails sur le système qui pourrait être utilisé pour attaquer votre déploiement, tels que des informations de contact, d'administration, de localisation et de service; des informations d'adressage et de routage IP; et des statistiques d'utilisation du protocole de transmission. C'est pourquoi vous devez choisir des options de configuration pour protéger votre système contre les menaces basées sur SNMP.

Lorsque vous configurez l'interrogation SNMP (sous **System (système)** > **Configuration** > **SNMP** dans l'interface Web FMC), utilisez les options suivantes pour renforcer le SNMP dans votre déploiement Firepower :

- Choisissez SNMPv3, qui prend en charge
  - Algorithmes d'authentification tels que SHA, SHA224, SHA256 et SHA384.
  - Chiffrement avec AES256, AES192 et AES128.
  - Utilisateurs en lecture seule.
- Utilisez des mots de passe forts lorsque vous configurez le champ **Mot de passe d'authentification** pour l'accès à la gestion du réseau.

En outre, vous devez limiter votre liste d'accès SNMP aux hôtes précis qui seront utilisés pour interroger la MIB. Cette option paraît dans l'interface Web FMC sous **System (système)** > **Configuration** > **Access List (liste d'accès)**. Consultez « Configuring the Access List for Your System » (configuration de la liste d'accès pour votre système) dans le Guide de configuration de Firepower Management Center, version 7.0.

Le FMC permet également d'envoyer des alertes externes à un serveur SNMP. Pour sécuriser cette fonction, consultez Bloquer l'accès à des bases de données tierces (alerte externe sécurisée).

Important Bien que vous puissiez établir une connexion sécurisée avec un serveur SNMP à partir de Firepower, le module d'authentification n'est pas conforme à la norme FIPS.

Traduction sécurisée d'adresses de réseau (NAT)

En règle générale, les ordinateurs en réseau utilisent la traduction d'adresses de réseau (NAT) pour réaffecter les adresses IP source ou destination dans le trafic réseau. Pour protéger votre déploiement Firepower ainsi

que l'ensemble de votre infrastructure réseau contre les attaques de type NAT, configurez le service NAT dans votre réseau conformément aux meilleures pratiques de l'industrie ainsi qu'aux recommandations de votre fournisseur de NAT.

Pour en savoir plus sur la configuration de votre déploiement Firepower pour fonctionner dans un environnement NAT, voir « NAT Environments » (environnements NAT) dans le *Guide de configuration de Firepower Management Center, version 7.0*. Ces informations sont utilisées en deux temps lors de l'établissement de votre déploiement :

- Lorsque vous effectuez la configuration initiale de votre FMC comme décrit dans le Guide de démarrage de Cisco Firepower Management Center pour votre modèle de matériel.
- Lors de l'enregistrement d'un appareil géré dans le FMC comme décrit dans « Add Devices to the Firepower Management Center » (ajouter des appareils au Firepower Management Center) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Accès sécurisé aux appareils gérés

Votre déploiement Firepower comprend des appareils de sécurité gérés par le FMC, chacun fournissant différents moyens d'accès. Ces appareils échangent des informations avec le FMC et leur sécurité est importante pour la sécurité de votre déploiement global. Analysez ces appareils dans votre déploiement et appliquez des configurations de renforcement le cas échéant, comme la sécurisation de l'accès des utilisateurs et la fermeture des ports de communication inutiles.

Renforcer l'accès utilisateur FMC

Utilisateurs internes et externes

Le FMC prend en charge deux types d'utilisateurs :

- Utilisateurs internes : le système consulte une base de données locale pour l'authentification des utilisateurs.
- Utilisateurs externes – Si l'utilisateur n'est pas présent dans la base de données locale, le système interroge un serveur d'authentification LDAP ou RADIUS externe.

Vous pouvez envisager d'établir l'accès des utilisateurs par le biais d'un mécanisme d'authentification externe tel que LDAP ou RADIUS, afin d'intégrer la gestion des utilisateurs à l'infrastructure existante de votre environnement réseau, ou d'exploiter des fonctionnalités telles que l'authentification à deux facteurs. L'établissement d'une authentification externe nécessite la création d'un objet d'authentification externe dans l'interface Web FMC; les objets d'authentification externe peuvent être partagés pour authentifier les utilisateurs externes pour le FMC, ainsi que les appareils gérés.

Types d'accès utilisateur

Le FMC prend en charge deux types d'accès utilisateur :

- Une interface Web (HTTP). Cette fonction est disponible pour les comptes d'utilisateurs internes et externes.
- Accès à la ligne de commande via SSH, un numéro de série, ou une connexion clavier-écran. Cette fonction est accessible au compte **admin**, qui dispose d'un accès à l'interface de ligne de commande ou à l'interpréteur de commandes, et peut être mise à la disposition d'utilisateurs externes.

Cette discussion sur la gestion des utilisateurs se réfère aux fonctions disponibles dans la version 7.0de Firepower; toutes les fonctions de configuration des comptes d'utilisateurs abordées dans cette section ne s'appliquent pas à toutes les versions de Firepower. Pour obtenir des informations propres à votre système, consultez le Guide de configuration de Firepower Management Center pour votre version.

Restreindre les privilèges d'administration

Le FMC prend en charge deux comptes **admin** :

- Un compte **admin** pour accéder au FMC via l'interface Web (HTTP).
- Un compte **admin** pour l'accès à l'interface de ligne de commande ou à l'interpréteur de commandes par SSH, un numéro de série ou une connexion clavier et écran. Dans la configuration par défaut, ce compte a un accès direct à l'interpréteur de commandes de Linux. Vous pouvez configurer ce compte pour qu'il accède à l'auxiliaire CLI FMC plutôt qu'à l'interpréteur de commandes Linux (voir Restreindre l'accès à Shell, à la page 8). À partir de l'interface CLI du FMC, ce compte peut accéder directement à l'interpréteur de commandes de Linux à l'aide de la commande **expert** de l'interface CLI (à moins que vous ne désactiviez la commande **expert**; là encore, voir Restreindre l'accès à Shell, à la page 8).

Remarque Dans la FMC configuration initiale, les mots de passe de ces deux comptes **admin** sont les mêmes, mais il ne s'agit pas des mêmes comptes, et le système valide ces mots de passe par rapport à des bases de données différentes.

Les comptes **admin** ont des droits de configuration supérieurs à ceux des autres utilisateurs, y compris le droit de créer des comptes supplémentaires avec les mêmes privilèges. Choisissez avec soin les utilisateurs auxquels vous accordez l'accès à un compte doté de privilèges d'administration.

Pour en savoir plus, consultez « User Accounts for Management Access » (comptes d'utilisateurs pour l'accès à des fins de gestion) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Restreindre l'accès à Shell

Par défaut, les utilisateurs disposant d'un accès à la ligne de commande obtiennent un accès direct à l'interpréteur de commandes de Linux lorsqu'ils se connectent.CLI ou de l'interpréteur de commandes doivent franchir l'étape supplémentaire consistant à entrer la commande **expert** de la CLI pour accéder à l'interpréteur de commandes de Linux.

Remarque Sur tous les appareils, le système met fin à la connexion SSH après trois tentatives infructueuses consécutives d'un utilisateur pour se connecter à la CLI ou à l'interpréteur de commandes via SSH.

⚠

Mise en garde Sur tous les appareils, les utilisateurs ayant un accès à l'interface de ligne de commande ou à l'interpréteur de commandes peuvent obtenir des privilèges racine dans l'interpréteur de commandes, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous recommandons fortement :

- Si vous établissez une authentification externe, veillez à restreindre de manière appropriée la liste des utilisateurs ayant accès à l'interface de ligne de commande ou à l'interpréteur de commandes.
- N'ajoutez pas d'utilisateurs directement dans l'interpréteur de commandes; créez des comptes en utilisant uniquement les procédures décrites dans le Guide de configuration de Firepower Management Center pour votre version.
- Sauf indication contraire du Centre d'assistance technique Cisco, n'accédez pas au FMC en utilisant le mode **expert** de l'interpréteur de commandes ou l'interface de ligne de commande.

Pour en savoir plus sur les types d'accès FMC, voir « Web Interface and CLI Access » (accès par interface Web et interface de ligne de commande) dans le *Guide de configuration du centre de gestion Firepower, version 7.0*.

La mesure de renforcement la plus sûre que vous puissiez prendre en ce qui concerne l'accès à l'interpréteur de commandes de Linux pour le FMC est de bloquer tout accès à l'interpréteur de commandes :

- Connectez-vous au FMC à l'aide d'une connexion SSH, d'un numéro de série, ou d'un clavier et d'un moniteur (voir le Guide de démarrage pour votre modèle FMC).
- Entrez la commande **system lockdown**. (Consultez l'annexe B du *Guide de configuration du centre de gestion Firepower, version 7.0*).

Une fois le verrouillage du système terminé, tout utilisateur qui se connecte au FMC avec des identifiants de ligne de commande n'aura accès qu'aux commandes CLI du FMC. Il peut s'agir d'une mesure de renforcement importante, mais il convient de l'utiliser avec précaution, car elle ne peut être annulée qu'à l'aide d'un correctif fourni par le Centre d'assistance technique Cisco.

Pour obtenir des informations complètes sur l'interface de ligne de commande FMC, consultez l'annexe B du *Guide de configuration de Firepower Management Center, version 7.0*.

Utiliser les multidétenteurs pour segmenter l'accès des utilisateurs aux appareils, configurations et événements gérés

Les administrateurs peuvent regrouper les appareils, configurations et événements gérés dans un déploiement Firepower en *domaines*, et accorder aux utilisateurs FMC l'accès aux domaines sélectionnés en fonction de leurs besoins. Les utilisateurs respectent les restrictions d'accès imposées par leur domaine, en plus de celles imposées par leur(s) rôle(s) d'utilisateur. Vous pouvez, par exemple, accorder à un compte sélectionné un accès d'administrateur complet dans un domaine, un accès d'analyste de sécurité dans un autre domaine et aucun accès dans un troisième domaine.

Créez et gérez des domaines à partir de l'interface Web FMC en utilisant l'option de menu **System (système)** > **Domains (domaines)**. Des informations complètes sur la mise en œuvre des multidétenteurs sont disponibles dans le *Guide de configuration de Firepower Management Center, version 7.0* sous la rubrique « Domain Management » (gestion de domaine).

Attribuez des droits aux utilisateurs dans les domaines à partir de l'interface Web FMC à l'aide de **Utilisateurs** > **système** > **Utilisateurs** Pour plus de détails, voir « Add an Internal User » (ajouter un utilisateur interne au niveau de l'interface Web) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Renforcer les comptes d'utilisateurs internes

Les utilisateurs internes n'ont accès au FMC que par l'intermédiaire de l'interface Web. Les administrateurs peuvent utiliser les paramètres suivants sous **Utilisateurs** > **système** > **Utilisateurs** pour renforcer le système contre les attaques par les mécanismes de connexion à l'interface Web :

- Limiter le nombre maximal d'échecs de connexion à l'interface Web avant qu'un compte ne soit bloqué et ne doive être réactivé par un administrateur.
- Appliquer une longueur de mot de passe minimale
- Définir le nombre de jours de validité des mots de passe
- Exiger des mots de passe forts
- Ne pas exempter les utilisateurs du délai de session de l'interface Web
- Attribuer des rôles d'utilisateur correspondant uniquement au type d'accès requis par le compte.
- Attribuer un domaine approprié au type d'accès requis par l'utilisateur
- Obliger l'utilisateur à réinitialiser le mot de passe du compte lors de la prochaine connexion

Pour en savoir plus sur ces paramètres, voir « User Accounts for FMC » (Comptes d'utilisateurs pour) dans le *Guide de configuration du centre de gestion Firepower, version 7.0*.

Les administrateurs peuvent également configurer les paramètres suivants de manière globale pour tous les utilisateurs de l'interface Web interne sous **System (système)** > **Configuration** > **User Configuration (configuration de l'utilisateur)** :

- Limiter la réutilisation des mots de passe
- Suivi des connexions réussies
- Bloquer temporairement l'accès à l'interface Web pour les utilisateurs qui échouent à un certain nombre de tentatives de connexion.

Pour en savoir plus sur ces paramètres, voir « Global User Configuration Settings » (paramètres de configuration globale des utilisateurs) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Renforcer les comptes d'utilisateurs externes

Le FMC authentifie les comptes d'utilisateurs externes par rapport à une base de données d'utilisateurs stockée sur un serveur externe (LDAP ou RADIUS).

Remarque Si vous choisissez d'utiliser l'authentification externe, consultez les informations dans Connexions sécurisées aux serveurs prenant en charge les connexions, la connaissance et le contrôle des utilisateurs du réseau faisant autorité, à la page 17.

Remarque Pour utiliser l'authentification externe, le FMC doit utiliser le DNS. La configuration d'un FMC pour utiliser le DNS est généralement effectuée au cours du processus de configuration initiale. Assurez-vous que votre DNS local est configuré conformément aux meilleures pratiques de sécurité recommandées par l'industrie; consultez Sécuriser le système de noms de domaine (DNS), à la page 6.

Important Bien que vous puissiez établir une connexion sécurisée avec des serveurs LDAP ou RADIUS à partir de Firepower, le module d'authentification n'est pas conforme à la norme FIPS.

Pour configurer un serveur externe pour l'authentification des utilisateurs FMC, vous devez créer un objet d'authentification externe sous **Utilisateurs** > **système** > **Authentification extérieure**. Utilisez les options suivantes dans votre objet d'authentification externe pour protéger votre FMC contre d'éventuelles attaques par des comptes d'utilisateurs authentifiés de l'extérieur :

- Limitez soigneusement l'accès des utilisateurs aux comptes disposant d'un accès à l'interpréteur de commandes. Les utilisateurs de à l'interpréteur de commandes peuvent obtenir les privilèges de l'administrateur, ce qui présente un risque pour la sécurité.
- N'accordez pas aux comptes plus d'accès qu'ils n'en ont besoin :
  - Si vous utilisez LDAP, associez les rôles d'utilisateur Firepower appropriés aux utilisateurs ou groupes d'utilisateurs LDAP.
  - Si vous utilisez RADIUS, associez les rôles d'utilisateur Firepower appropriés aux attributs RADIUS.
- Si vous utilisez LDAP, sous **Advanced Options** (options avancées) lors de la configuration d'un objet d'authentification externe, configurez le chiffrement TLS ou SSL.

Pour en savoir plus, consultez « Configure External Authentication » (configurer l'authentification externe) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Établir des délais d'attente pour les sessions

En limitant la durée des sessions de connexion au compte, on réduit la possibilité pour les utilisateurs non autorisés d'exploiter les sessions non surveillées.

Pour définir les délais de session sur le FMC, utilisez **System > Configuration > Session Timeout (Système > Configuration > Délai de session)** . À partir de là, vous pouvez configurer les valeurs suivantes du délai d'attente de l'interface en minutes :

- **Expiration de la session du navigateur** : FMC temps d'attente de la session de l'interface Web.
- **Délais d'expiration de la CLI** : Délai d'accès de l'interface de ligne de commande.

Ces paramètres s'appliquent aux comptes internes et externes, quel que soit leur(s) rôle(s) d'accès. Consultez « Session Timeouts » (délais d'expiration de session) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Désactiver l'accès à l'API REST

L'API REST Firepower fournit une interface allégée permettant aux applications tierces d'afficher et de gérer la configuration de l'appareil à l'aide d'un client REST et de méthodes HTTP standard. Pour en savoir plus sur l'API REST Firepower, consultez le Guide de démarrage rapide de l'API REST de Firepower Management Center pour votre version.

Par défaut, le FMC autorise les demandes provenant d'applications utilisant l'API REST. Pour renforcer le FMC, vous devez désactiver cet accès; dans l'interface Web FMC, sélectionnez **System (système)** > **Configuration** > **REST API Preferences (préférences REST API)** et décochez la case **Enable REST API**

(activer l'API REST). Pour obtenir des informations complètes, consultez « REST API Preferences » (préférences de l'API REST) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Restreindre l'accès à distance

Sur le FMC, vous pouvez utiliser des listes d'accès pour limiter l'accès au système par adresse IP et par port. Par défaut, les ports suivants sont activés pour toute adresse IP :

- 443 (HTTPS) – Utilisé pour l'accès à l'interface Web
- 22 (SSH) – Utilisé pour l'accès à l'interface de ligne de commande ou à l'interpréteur de commandes

Vous pouvez également ajouter l'accès à l'interrogation des informations SNMP sur le port 161.

Important Bien que vous puissiez établir une connexion sécurisée avec un serveur SNMP à partir de Firepower, le module d'authentification n'est pas conforme à la norme FIPS.

Pour opérer dans un environnement plus sûr, configurez votre FMC pour autoriser ces formes d'accès qu'à des adresses IP précises, et désactivez les règles par défaut qui autorisent l'accès HTTPS ou SSH à n'importe quelle adresse IP. Ces options paraissent sous **System > Configuration > Access List** (système > Configuration > Liste d'accès) dans l'interface Web FMC. Pour en savoir plus, consultez « Access List » (liste d'accès) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Ne pas utiliser de mesures correctives

Une correction est un programme que Firepower lance en réponse à une violation de la politique de corrélation. Vous pouvez configurer plusieurs types de corrections sur le FMC, mais elles exigent toutes que le FMC communique avec des entités extérieures au Firepower de manière non sécurisée. Pour cette raison, nous recommandons de ne pas configurer un système Firepower renforcé pour utiliser des corrections. Pour en savoir plus, consultez « Remediations » (correction) dans le *Guide de configuration de Firepower Management Center, version 7.0* .

Communications sécurisées entre le FMC et le navigateur Web

Sécurisez les informations transmises entre le FMC et votre ordinateur local en utilisant des certificats HTTPS client et serveur pour sécuriser la connexion entre le FMC et le navigateur qui exécute l'interface Web. Le FMC utilise un certificat auto-signé par défaut, mais nous recommandons de le remplacer par un certificat généré par une autorité de certification mondialement connue et fiable.

Pour configurer les certificats HTTPS pour votre FMC, utilisez **System (système)** > **Configuration** > **HTTPS Certificate (certificat HTTPS)** dans l'interface Web FMC; consultez « HTTPS Certificate » (certificat HTTPS) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Protéger les sauvegardes

Pour protéger les données du système et leur disponibilité, effectuez des sauvegardes régulières de votre FMC. La fonction de sauvegarde paraît sous **Système** > **Outils** > **Sauvegarde et restauration** dans l'interface Web FMC. Pour en savoir plus, consultez « Back up the FMC) (sauvegarde du) dans le *Guide de configuration du Firepower Management Center, version 7.0*.

Le FMC permet de stocker automatiquement les sauvegardes sur un appareil distant. L'utilisation de cette fonction n'est pas recommandée pour un système renforcé car la connexion entre le FMC et l'appareil de stockage à distance ne peut pas être sécurisée.

Exportation et importation de la configuration de protection

Le FMC permet d'exporter un certain nombre de configurations du système (telles que les stratégies, les tables personnalisées et les modèles de rapport) vers un fichier qui peut ensuite être utilisé pour importer ces mêmes configurations vers un autre FMC exécutant la même version de Firepower. Cette fonction peut faire gagner du temps aux administrateurs qui ajoutent de nouveaux appareils à un déploiement, mais elle doit être utilisée avec précaution pour éviter les failles de sécurité. Les précautions suivantes doivent être prises lors de l'utilisation de la fonction d'exportation/importation :

- Sécuriser les communications entre le FMC et le navigateur Web pour protéger les informations de configuration transférées. Voir Communications sécurisées entre le FMC et le navigateur Web, à la page 12.
- Accès sécurisé à l'ordinateur local où est stocké le fichier de configuration exporté; la protection de ce fichier est importante pour la sécurité de votre déploiement Firepower.
- Sachez que si vous exportez une configuration qui utilise des objets PKI contenant des clés privées, le système déchiffre les clés privées avant l'exportation; les clés privées exportées sont stockées en texte clair. Lors de l'importation, le système chiffre les clés à l'aide d'une clé générée de manière aléatoire.

Les fonctions d'exportation et d'importation de la configuration paraissent dans l'interface Web FMC sous **Système** > **Outils** > **Importer/Exporter**. Pour obtenir des informations complètes sur cette fonctionnalité, reportez-vous à « Configuration Import and Export » (importation et exportation de la configuration) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Protéger les rapports

Le système Firepower propose plusieurs types de rapports, qui contiennent tous des informations sensibles qu'il convient de protéger contre l'accès par du personnel non autorisé. Tous les types de rapports présentés ici peuvent être téléchargés du FMC sur votre ordinateur local sous forme non chiffrée. Avant de télécharger des rapports, sécurisez les communications entre le FMC et le navigateur Web afin de protéger les informations transférées. (Consultez Communications sécurisées entre le FMC et le navigateur Web [communications sécurisées entre le FMC et le navigateur Web]). En outre, un accès sécurisé à l'ordinateur local où sont stockés les rapports.

- Les rapports standard sont des rapports détaillés et personnalisables sur tous les aspects de votre système, disponibles aux formats HTML, CSV et PDF. Les rapports sur les risques sont des résumés au format HTML des risques trouvés dans votre organisation.

  Sur l'interface Web FMC, les rapports standard et les rapports de risque paraissent sous **Overview (aperçu)** > **Reporting (rapports)**. Pour ces rapports, Firepower propose deux options de stockage en plus du téléchargement local, chacune présentant un risque de sécurité :

  - Vous pouvez envoyer automatiquement le rapport par courrier électronique à un serveur sélectionné. Nous ne recommandons pas l'utilisation de cette fonction dans un système renforcé, car le courrier électronique ne peut pas être sécurisé.
  - Vous pouvez enregistrer automatiquement les rapports sur un appareil distant. Nous ne recommandons pas l'utilisation de cette fonction pour un système renforcé, car la connexion entre le FMC et l'appareil de stockage à distance ne peut pas être sécurisée.

Pour obtenir des informations complètes sur la conception et la génération de rapports standard et de rapports sur les risques, consultez « Working with Reports » (travailler avec des rapports) dans le *Guide de configuration de Firepower Management Center, version 7.0* .

- Les rapports de surveillance de l'état de santé pour le dépannage contiennent des informations que Centre d'assistance technique Cisco peut utiliser pour diagnostiquer les problèmes du système s'ils surviennent. Pour générer ces rapports à partir de l'interface Web FMC, utilisez **Moniteur** > **d'intégrité** > **de système**et suivez les instructions sous « Health Monitor Reports for Troubleshooting » (rapports de surveillance de l'intégrité pour le dépannage) dans le *Guide de configuration du centre de gestion Firepower, version 7.0*. Le FMC produit des fichiers de dépannage au format `.tar.gz`.
- Les rapports sur les polices sont des fichiers PDF qui fournissent des détails sur la configuration actuelle sauvegardée d'une politique. Pour générer un rapport de politique, accédez à la page de gestion de la politique pour laquelle vous souhaitez obtenir un rapport et cliquez sur l'icône de rapport (). Pour obtenir une liste complète des politiques qui prennent en charge les rapports, consultez« Generating Current Policy Report » (générer des rapports sur les politiques appliquées) dans le *Guide de configuration de Firepower Management Center, version 7.0*.
- Utilisez les rapports de comparaison pour vérifier la conformité des changements de politique avec les normes de votre organisation ou pour optimiser les performances du système. Vous pouvez examiner les différences entre deux politiques ou entre une politique sauvegardée et la configuration en cours d'exécution. Pour générer un rapport de comparaison (disponible au format PDF uniquement), accédez à la page de gestion du type de polices que vous souhaitez comparer et sélectionnez **Compare Policies** (comparer les politiques). (Consultez « Comparing Policies » (comparaison des politiques) dans le *Guide de configuration de Firepower Management Center, version 7.0*.
- Les rapports d'incidents peuvent inclure des informations sur des incidents de violations présumées de la politique de sécurité, telles que le résumé, le statut et les informations spécifiques aux événements que vous ajoutez à l'incident. Ces rapports peuvent être formatés au format HTML, PDF ou CSV. Dans l'interface Web FMC, générez ces rapports à partir de la page d'analyse des incidents à **Analysis** > **Intrusions** > **Incidents**, et utilisez les instructions sous « Generating Incident Reports » (générer des rapports d'incidents) dans le *Guide de configuration de Firepower Management Center, version 7.0*.
- Le presse-papiers des événements d'intrusion est une zone de stockage où vous pouvez copier des événements à partir de n'importe quelle vue d'événement d'intrusion, puis générer des rapports sur ces événements en formats HTML, PDF ou CSV. Dans l'interface Web FMC, vous devez d'abord ajouter des événements au presse-papiers, puis vous pouvez générer ces rapports à l'aide de **Analysis** > **Intrusions** > **Clipboard**. Consultez « The Intrusion Events Clipboard » (Le presse-papiers des événements d'intrusion) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Alerte externe sécurisée

Vous pouvez configurer le FMC pour qu'il envoit des notifications appelées *réponses d'alerte* vers des serveurs externes lorsque des événements sélectionnés se produisent. Si ces alertes peuvent être utiles pour surveiller l'activité du système, elles peuvent présenter un risque pour la sécurité si la connexion au serveur externe ne peut pas être sécurisée.

Le FMC permet d'envoyer des réponses aux alertes sous trois formes différentes :

- Les réponses aux alertes envoyées à syslog peuvent ne pas être sécurisées. (**Politiques** > **Actions** > **Alerts (alertes)** > **Create Alert (créer l'alerte)** > **Create Syslog Alert (créer une alerte syslog)** dans l'interface Web FMC); nous ne recommandons pas de configurer votre FMC pour envoyer de telles alertes dans un environnement renforcé.

- Les informations que le FMC envoie à un serveur externe par courrier électronique peuvent être sécurisées si vous configurez la connexion avec l'hôte du relais de courrier de manière à utiliser le chiffrement (TLS ou SSLv3) et à exiger un nom d'utilisateur et un mot de passe. Effectuez cette opération via l'interface Web FMC en utilisant **System** > **Configuration > Email Notification (système > Configuration > Notification par courrier électronique)**. Pour en savoir plus, consultez « Configuring a Mail Relay Host and Notification Address » (configuration d'un hôte de relais de messagerie et d'une adresse de notification) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

  Une fois que vous avez sécurisé la connexion avec l'hôte du relais de messagerie, les données transmises par le FMC sont protégées par les fonctions suivantes :

  - Réponses aux alertes par courrier électronique, décrites dans « Creating an Email Alert Response » (création d'une réponse à une alerte par courriel) dans le *Guide de configuration de Firepower Management Center, version 7.0*. (Configurer ce paramètre en utilisant **Policies (Politiques)** > **Actions** > **Alerts (alertes)** > **Create Alert (créer l'alerte)** > **Create Email Alert (créer une alerte courriel)** dans l'interface Web FMC).
  - Notifications d'élagage des données, décrites dans « Configuring Database Event Limits » (configuration des limites d'événements de la base de données) dans le *Guide de configuration de Firepower Management Center, version 7.0*. (Configurer ce paramètre sous **System (système)** > **Configuration** > **Database (base de données)** dans l'interface Web FMC).

- Les alertes envoyées à un serveur SNMP peuvent être sécurisées en utilisant les options suivantes sous **Politiques** > **Actions** > **Alerts (alertes)** > **Create Alert (créer l'alerte)** > **Create SNMP Alert (créer une alerte SNMP)** dans l'interface Web FMC :

  - Choisissez SNMP v3 pour la **Version**. Ce protocole prend en charge :
    - Algorithmes d'authentification tels que SHA, SHA224, SHA256 et SHA384.
    - Chiffrement avec AES256, AES192 et AES128.
    - Utilisateurs en lecture seule.
  - Choisissez un **protocole d'authentification** pour sécuriser la connexion (MD5 ou SHA) et fournissez un **mot de passe**.
  - Choisissez DES comme **protocole de confidentialité** et fournissez un **mot de passe**.
  - Fournir un **Engine ID** (identifiant du moteur) que le système utilisera pour coder les messages. Il est recommandé d'utiliser la version hexadécimale de l'adresse IP du FMC. Par exemple, si le FMC a une adresse IP de 10.1.1.77, utilisez 0a01014D0.

  En outre, vous devez limiter votre liste d'accès SNMP aux hôtes précis auxquels le FMC enverra des alertes SNMP. (Cette option paraît dans l'interface Web FMC sous **System (système)** > **Configuration** > **Access List (liste d'accès)**. Consultez « Configure an Access List » (configurer une liste d'accès) dans le *Guide de configuration de Firepower Management Center, version 7.0*).

  Le FMC prend également en charge l'interrogation SNMP. Pour sécuriser cette fonction, consultez Interrogation SNMP sécurisée.

Important Bien que vous puissiez configurer des connexions sécurisées à un serveur SNMP ou SMTP à partir de Firepower, le module d'authentification n'est pas conforme à la norme FIPS.

Pour obtenir des informations complètes sur les alertes externes, consultez « External Alerting with Alert Responses » (alertes externes avec réponses aux alertes) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Protéger les journaux d'audit

Le FMC conserve des journaux en lecture seule de l'activité des utilisateurs, configurés par le biais du **System (système)** > **Configuration** > **Audit Log (journalisation d'audit)**. Pour économiser les ressources mémoire du FMC, vous pouvez stocker ces journaux en externe (flux vers le Syslog ou vers un serveur HTTP). Toutefois, cela peut présenter un risque pour la sécurité, à moins que vous ne sécurisiez le canal de diffusion des journaux d'audit en activant TLS et en établissant une authentification mutuelle à l'aide de certificats TLS. Pour en savoir plus, consultez « Securely Stream Audit Logs » (diffusion sécurisée des journaux d'audit) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Sécuriser la connexion à eStreamer

L'Event Streamer (eStreamer) vous permet de transmettre plusieurs types de données d'événements d'un FMC à une application client développée sur mesure. Pour en savoir plus, consultez le Guide d'intégration Firepower eStreamer pour votre version. Si votre organisation choisit de créer et d'utiliser un client eStreamer, prenez les précautions suivantes :

- Développez votre application en utilisant les meilleures pratiques de l'industrie en matière de sécurité
- Configurez la connexion entre le FMC et le client eStreamer pour que les données soient transmises en toute sécurité. Faites-le dans l'interface Web FMC sous **Intégration** > **système** > **eStreamer** > **Créer client** en fournissant un mot de passe pour chiffrer le fichier de certificat qui sécurise la connexion avec l'hôte exécutant le client eStreamer. Pour en savoir plus, consultez « Configuring eStreamer Client Communications » (Configuration des communications avec le client eStreamer) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Bloquer l'accès à des bases de données tierces

Assurez-vous que les applications clientes tierces n'ont pas accès à la base de données FMC; dans l'interface Web FMC, sous **System (système)** > **Configuration** > **External Database Access (accès de base de données externe)**, assurez-vous que la case **Allow External Database Access** (autoriser l'accès externe à la base de données) est décochée. Pour en savoir plus, consultez « External Database Access Settings » (paramètres d'accès aux bases de données externes) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Personnaliser la bannière de connexion

La page de connexion au système est susceptible d'être vue par des personnes ayant ou non un accès autorisé au FMC. Personnalisez votre bannière de connexion de manière à ce qu'elle n'affiche que les informations appropriées à la vue de tous. Sur l'interface Web FMC, utilisez **System (système)** > **Configuration** > **Login Banner (bannière de connexion)**. Pour obtenir des informations complètes, consultez « Login Banners » (bannières de connexion) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Connexions sécurisées aux serveurs prenant en charge les connexions, la connaissance et le contrôle des utilisateurs du réseau faisant autorité

Les stratégies d'identité Firepower utilisent des sources d'identité pour authentifier les utilisateurs du réseau et collecter des données sur les utilisateurs afin de les connaître et de les contrôler. L'établissement des sources d'identité des utilisateurs nécessite une connexion entre le FMC ou un appareil géré et l'un des types de serveurs suivants :

- Microsoft Active Directory
- Linux Open LDAP
- RADIUS

Important Bien que vous puissiez établir une connexion sécurisée avec des serveurs LDAP, Microsoft AD ou RADIUS à partir de Firepower, le module d'authentification n'est pas conforme à la norme FIPS.

Remarque Si vous choisissez d'utiliser LDAP ou Microsoft AD pour effectuer l'authentification externe, consultez les informations figurant dans Renforcer les comptes d'utilisateurs externes, à la page 10.

Remarque Firepower utilise chacun de ces serveurs pour prendre en charge une combinaison différente des caractéristiques possibles de l'identité de l'utilisateur. Pour en savoir plus, voir « About User Identity Sources » (à propos des sources d'identité des utilisateurs) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Remarque Firepower peut également utiliser des serveurs RADIUS pour fournir une capacité VPN à votre réseau. Pour en savoir plus, consultez « Firepower Threat Defense VPN » (VPN Firepower Threat Defense) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Sécuriser les connexions avec les serveurs Active Directory et LDAP

Les objets Firepower appelés *realms* décrivent les paramètres de connexion associés à un domaine sur un serveur Active Directory ou LDAP. Pour en savoir plus sur la configuration des domaines, voir « Create and Manage Realms » (Créer et gérer des domaines) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Lorsque vous créez un domaine (**Domaines** > **d'intégration** > **système** dans l'interface Web FMC), gardez à l'esprit les points suivants pour sécuriser les connexions avec les serveurs AD ou LDAP :

Pour les domaines associés aux serveurs Active Directory :

- Choisissez des mots de passe forts pour le **mot de passe d'AD Join** et le **mot de passe du répertoire**.
- Lors de l'ajout d'un annuaire à un domaine Active Directory :

- Sélectionnez **STARTTLS** ou **LDAPS** comme mode de **chiffrement** (ne choisissez pas **None** [aucun]).
- Précisez un **certificat SSL** à utiliser pour l'authentification auprès du contrôleur de domaine Active Directory. Nous recommandons d'utiliser un certificat généré par une autorité de certification mondialement connue et fiable.

Pour les domaines associés aux serveurs LDAP :

- Choisissez des mots de passe forts pour le **mot de passe du répertoire**.
- Lors de l'ajout d'un répertoire à un domaine LDAP :
  - Sélectionnez **STARTTLS** ou **LDAPS** comme mode de **chiffrement** (ne choisissez pas **None** [aucun]).
  - Précisez un **certificat SSL** à utiliser pour l'authentification auprès du serveur LDAP. Nous recommandons d'utiliser un certificat généré par une autorité de certification mondialement connue et fiable.

Sécuriser les connexions avec les serveurs RADIUS

Pour configurer une connexion avec un serveur RADIUS, créez un objet Groupe de serveurs RADIUS (**Objects (objets)** > **Object Management (gestion des objets)** > **RADIUS Server Group (groupe de serveurs RADIUS)** dans l'interface Web FMC) et ajoutez un serveur RADIUS au groupe. Pour sécuriser la connexion avec le serveur RADIUS, choisissez les options suivantes dans la boîte de dialogue **New RADIUS Server** (nouveau serveur RADIUS) :

- Fournissez une **clé** et une **clé de confirmation** pour chiffrer les données entre l'appareil géré et le serveur RADIUS.
- Précisez une interface pour la connexion qui peut prendre en charge la transmission sécurisée des données.

Inscription au certificat sécurisé

Vous pouvez configurer l'inscription des certificats pour FTD sur un canal sécurisé. L'appareil utilise la fonction : inscription sur le protocole de transport sécurisé, soit Enrollment over Secure Transport (EST), pour obtenir un certificat d'identité auprès de l'autorité de certification. EST utilise TLS pour assurer le transport sécurisé des messages.

Pour configurer EST, choisissez **Objects > Object Management** (Objets > Gestion des objets), puis dans le volet de navigation choisissez **PKI > Cert Enrollment** (PKI > Inscription des certificats). Cliquez sur **Add Cert Enrollment** (ajouter une inscription de certificat), puis cliquez sur l'onglet **CA Information (information de l'autorité de certification)**. Dans la liste déroulante **Enrollment Type** (type d'inscription), choisissez EST.

Si vous ne souhaitez pas que FTD valide le certificat du serveur EST, nous vous recommandons de ne pas cocher la case **Ignore EST Server Certificate Validations** (ignorer les validations du certificat du serveur EST). Par défaut, FTD valide le certificat du serveur EST. Le type d'inscription EST ne prend en charge que les clés RSA et ECDSA, et ne prend pas en charge les clés EdDSA. Pour en savoir plus, voir « Options EST de l'objet d'inscription de certificat » (options EST de l'objet d'inscription au certificat) dans *Guide de configuration de Firepower Management Center, version 7.0*.

Sur les versions 7.0 et supérieures du FMC et de FTD, vous ne pouvez pas inscrire de certificats avec des tailles de clé RSA inférieures à 2 048 bits et des clés utilisant SHA-1. Pour ignorer ces restrictions dans le FMC 7.0, qui gère FTD exécutant des versions inférieures à 7.0, l'option **Enable Weak-Crypto** (Activer le chiffrement faible) est proposée (**Devices > Certificates**[Appareils > Certificats]). Par défaut, l'option weak-crypto est désactivée. Nous vous déconseillons d'activer des clés de cryptage faibles, car ces clés ne sont pas aussi sûres que celles dont la taille est plus élevée. Pour les versions 7.0 et supérieures de FMC et FTD, vous pouvez activer le chiffrement faible pour permettre la validation des certificats d'homologues, etc. Cependant, cette configuration ne s'applique pas à l'inscription des certificats.

Renforcer les composants de soutien

Le logiciel FMC dépend d'un micrologiciel et d'un système d'exploitation sous-jacents complexes. Ces composants logiciels sous-jacents comportent leurs propres risques de sécurité qui doivent être pris en compte :

- Mettez en place un processus de sécurité opérationnelle pour votre réseau qui tienne compte des questions de sécurité.
- Pour les modèles FMC 1000, 1600, 2000, 2500, 2600, 4000, 4500 et 4600, pour renforcer les composants de l'appareil matériel qui sous-tendent le logiciel FMC, voir le *guide de renforcement Cisco UCS*.

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.