Guide de renforcement de Cisco Cisco Firepower Threat Defense, version 7.0

Dernière modification : 2024-10-24

Guide de renforcement de Cisco Firepower Threat Defense, 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 Cisco Firepower Threat Defense (FTD). Pour obtenir des informations sur le renforcement d'autres composants de votre déploiement Firepower, consultez les documents suivants :

- *Guide de renforcement de Cisco Firepower Management Center, version 7.0*
- *Guide de renforcement de Cisco Firepower 4100/9300 FXOS*

Ce guide fait référence à deux méthodes différentes de configuration d'un appareil FTD, mais n'est pas conçu comme un manuel détaillé pour l'une ou l'autre des interfaces concernées.

- Certains paramètres de configuration FTD peuvent être établis par l'intermédiaire de l'interface Web FMC; les références croisées pour ce produit renvoient au *Guide de configuration de Firepower Management Center, version 7.0* .
- Certains paramètres de configuration FTD peuvent être établis à l'aide de l'interface de ligne de commande FTD. Des informations complètes sur toutes les commandes CLI référencées dans ce document sont disponibles dans la *référence des commandes Cisco Firepower Threat Defense* .

Toutes les descriptions de fonctionnalités dans ce document se réfèrent à la version Firepower 7.0. Les paramètres de configuration présentés dans ce manuel ne sont disponibles dans toutes les versions de Firepower. 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 des exigences pour les produits de sécurité.
- Liste des produits approuvés par le 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 : spécification des exigences 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 FTD, mais certaines fonctions du FTD ne permettent pas d'assurer la conformité à la certification, même en utilisant les paramètres de configuration décrits dans le présent document. Pour plus d'informations, voir « 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 « 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 sur les appareils FTD gérés par un FMC, maintenez à jour les bases de données de géolocalisation, de règles d'intrusion et de vulnérabilités sur le FMC

de gestion. 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 l'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 les règles d'intrusion sur un FMC sans accès Internet.
- Mettre à jour les règles d'intrusion sur un FMC disposant d'un accès 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, consultez « 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 plus d'informations, voir « 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 FTD. Appliquez ce paramètre via l'interface Web FMC dans la stratégie de paramétrage de la plateforme FTD, qui se trouve sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**. La modification ne prend pas effet sur le FTD tant que vous n'avez pas déployé la nouvelle configuration; consultez « Enable Security Certifications Compliance » (activer la conformité aux certifications

de sécurité) dans le *Guide de configuration Cisco Firepower Management Center, version 7.0* pour connaître tous les détails.

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.

Visibilité du trafic avec NetFlow

IOS NetFlow de Cisco vous permet de surveiller en temps réel les flux de trafic dans votre réseau. L'appareil FTD peut coordonner certaines fonctions de NetFlow, telles que l'affichage et la réinitialisation des compteurs de durée l'exécution. (Consultez les commandes CLI **show flow-export counters** et **clear flow-export counters**).

L'interface Web FMC permet de désactiver les messages syslog FTD qui sont redondants avec ceux capturés par NetFlow. Pour ce faire, créez une politique de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **Syslog** (journal système) dans le menu. À l'onglet **Syslog Settings** (paramètres du journal système), cochez la case **NetFlow Equivalent Syslogs** (journaux système équivalents à NetFlow) (Utilisez la commande CLI **show logging flow-export-syslogs** pour déterminer quels messages du journal système sont redondants).

Vous pouvez tirer parti de ces capacités si vous configurez les appareils réseau avec NetFlow. Que les informations de flux soient exportées vers un collecteur distant ou non, vous pouvez utiliser NetFlow de manière réactive si nécessaire. Consultez « Netflow Data in the Firepower System » (données NetFlow dans le système Firepower) dans le *Guide de configuration de Firepower Management Center, version 7.0* pour en savoir plus.

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.

Configurez la synchronisation du temps NTP pour les appareils FTD à partir de l'interface Web FMC en créant une politique de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et en choisissant l'onglet **Time Synchronization** (synchronisation de l'heure) à la page de la politique. Pour en savoir plus, consultez « Configure NTP Time Synchronization for Threat Defense » (configurer la synchronisation de l'heure NTP pour Threat Defense) dans le *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 appareil FTD pour se connecter à un système de noms de domaine local afin de prendre en charge la communication sur son interface de gestion fait partie du processus de configuration initiale, décrit dans le Guide de démarrage rapide de votre modèle.

Certaines fonctions FTD qui utilisent les interfaces de données ou de diagnostic utilisent également le DNS – par exemple, NTP, les politiques de contrôle d'accès, les services VPN fournis par le FTD, un message ping ou une opération traceroute. Pour configurer le DNS pour les interfaces de données ou de diagnostic, créez une politique de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **DNS** dans la table des matières. Pour plus d'informations, voir « Configure DNS » (configurer le DNS) sous « Platform Settings for Firepower Threat Defense » (paramètres de la plateforme pour Firepower Threat Defense) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

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 et interruption SNMP sécurisées

Vous pouvez configurer un FTD pour qu'il prenne en charge l'interrogation et les pièges SNMP comme décrit dans « Configure SNMP for Threat Defense » (configurer SNMP pour Threat Defense) 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. Choisissez des options de configuration pour protéger votre système contre les menaces basées sur SNMP.

Pour configurer les fonctions SNMP pour un appareil FTD, créez une politique de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **SNMP** dans la table des matières. Pour des instructions complètes, consultez « Configure SNMP for Threat Defense » (configurer SNMP pour Threat Defense) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Utilisez les options suivantes pour durcir l'accès SNMP à l'appareil FTD :

- Lors de la création d'utilisateurs SNMP, 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.
- Créez des utilisateurs SNMPv3 avec les options suivantes :
  - Choisissez **Priv** (privé) pour le **Security Level** (Niveau de sécurité).
  - Choisissez **Encrypted** (chiffré) pour le **Encryption Password Type** (type de mot de passe de chiffrement).

Consultez « Add SNMPv3 Users » (ajouter des utilisateurs SNMPv3) dans le *Guide de configuration de Firepower Management Center, version 7.0* pour des instructions complètes.

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 plus d'informations 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*.

Sécuriser le FMC et les autres dispositifs de votre déploiement

Votre déploiement Firepower comprend le FMC et les appareils de sécurité gérés par le FMC, chacun fournissant des moyens d'accès différents. Les appareils gérés échangent des informations avec le FMC et leur sécurité est importante pour la sécurité de votre déploiement global. Analysez les appareils de votre déploiement et appliquez des configurations de renforcement si nécessaire, par exemple en sécurisant l'accès des utilisateurs et en fermant les ports de communication inutiles.

Renforcer les paramètres du protocole réseau

L'appareil FTD peut interagir avec d'autres appareils de réseau à l'aide d'un certain nombre de protocoles; choisissez les paramètres de configuration pour les communications de réseau afin de protéger l'appareil FTD, ainsi que les données qu'il envoie et reçoit.

- Par défaut, l'appareil FTD autorise jusqu'à 24 fragments par paquet IP et jusqu'à 200 fragments en attente de réassemblage. Vous devrez peut-être autoriser les fragments sur votre réseau si vous avez une application qui fragmente régulièrement les paquets, comme NFS sur UDP. Cependant, les paquets fragmentés sont souvent utilisés dans les attaques par déni de service (DoS), c'est pourquoi nous vous recommandons de ne pas autoriser les fragments.
  - Pour configurer les paramètres des fragments pour un appareil FTD, créez une stratégie de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **Fragment** dans la table des matières.
  - Pour interdire les fragments dans le trafic réseau traité par un appareil FTD, définissez l'option **Chain (Fragment)** (Chaîne [Fragment]) sur 1.

  Pour obtenir des instructions complètes, consultez « Configure Fragment Handling » (configurer la gestion des fragments) dans le *Guide de configuration de Firepower Management Center, version 7.0*.
- Pour les appareils FTD gérés par un Cisco Firepower Management Center, les connexions HTTPS avec le FTD ne peuvent être utilisées que pour télécharger des fichiers de capture de paquets à des fins de dépannage.

  Configurez les appareils FTD de manière à n'autoriser l'accès HTTPS que pour les adresses IP qui doivent être autorisées à télécharger des captures de paquets. Dans l'interface Web FMC, créez une politique de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **HTTP** dans la table des matières. Consultez « Configure HTTP » (configurer HTTP) dans le *Guide de configuration de Firepower Management Center, version 7.0* pour obtenir des instructions complètes.
- Par défaut, le FTD peut recevoir des paquets ICMP sur n'importe quelle interface utilisant IPv4 ou IPv6, à deux exceptions près :
  - Le FTD ne répond pas aux demandes d'écho ICMP dirigées vers une adresse de diffusion.
  - Le FTD ne répond qu'au trafic ICMP envoyé à l'interface par laquelle le trafic arrive; vous ne pouvez pas envoyer de trafic ICMP à travers une interface FTD à une interface éloignée.

  Pour protéger un appareil FTD contre les attaques basées sur ICMP, vous pouvez utiliser des règles ICMP pour limiter l'accès ICMP à des hôtes, des réseaux ou des types ICMP sélectionnés. Dans l'interface Web FMC , créez une politique de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **ICMP** dans la table des matières. Pour en savoir plus, consultez « Configure ICMP Access Rules » (configurer les règles d'accès ICMP) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

- Le FTD peut être configuré pour fournir des services DHCP et DDNS (voir« DHCP and DDNS Services for Threat Defense » (Services DHCP et DDNS pour la défense contre les menaces) dans le *Guide de configuration de Firepower Management Center, version 7.0*). De par leur nature, ces protocoles sont vulnérables aux attaques. Si vous choisissez de configurer votre appareil FTD pour DHCP ou DDNS, il est important d'appliquer les meilleures pratiques de l'industrie en matière de sécurité, d'assurer la protection physique de vos actifs réseau et de renforcer l'accès des utilisateurs à l'appareil FTD.

Services VPN sécurisés

Vous pouvez configurer le FTD pour qu'il fournisse deux types de services de réseau privé virtuel (VPN) :

- Réseau privé virtuel d'accès à distance (RA VPN) : Pour sécuriser les transmissions de messages à destination et en provenance de clients distants sur des connexions VPN RA, le FTD peut utiliser Transport Layer Security (TLS) ou IPsec_IKEv2. Avant de déployer une configuration RA VPN sur le FTD, le FMC s'assure que vous répondez aux critères décrits dans « Licences AnyConnect » (licences AnyConnect) dans le *Guide de configuration du centre de gestion Firepower, version 7.0*.

  VPN d'accès à distance sur FTD prend en charge les serveurs AD, LDAP et RADIUS AAA pour l'authentification.

  À partir de la version 7.0, le VPN RA prend en charge l'authentification locale et l'authentification multicertificat.

  - Authentification locale : Vous pouvez utiliser cette méthode d'authentification comme méthode d'authentification primaire ou secondaire, ou comme solution de repli au cas où le serveur distant configuré ne serait pas accessible. Nous vous recommandons d'utiliser un mot de passe fort pour l'authentification locale. Pour en savoir plus, consultez « Associating a Local Realm with a Remote Access VPN Policy » (Associer un domaine local à une politique VPN d'accès à distance) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

  - Authentification multicertificat : Nous vous recommandons de valider le certificat de la machine ou de l'appareil pour vous assurer qu'il s'agit bien d'un appareil émis par l'entreprise et d'authentifier le certificat d'identité de l'utilisateur pour autoriser l'accès VPN. Utiliser le client AnyConnect pour l'accès VPN pendant la phase SSL ou IKEv2 EAP. Pour en savoir plus, consultez « Configuring Multiple Certificate Authentication » (Configuration de l'authentification par certificats multiples) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

- Réseau privé virtuel site à site – Pour sécuriser les transmissions de messages à destination et en provenance de réseaux distants sur des connexions VPN site à site, le FTD peut utiliser IPSEC_IKEv1 ou IPSEC_IKEv2. En fonction de la licence de votre appareil, vous pouvez appliquer un chiffrement fort aux transmissions VPN de site à site. Le VPN site à site avec chiffrement fort nécessite une licence spéciale; consultez « Licensing for Export-Controlled Functionality » (octroi de licences pour les fonctions contrôlées par l'exportation) dans le *Guide de configuration du centre de gestion Firepower, version 7.0*.

  Il existe deux types de VPN de site à site : basé sur une politique (Crypto Map) et basé sur une route (Virtual Tunnel Interface [VTI]). Nous vous recommandons d'utiliser le VPN VTI basé sur les routes pour une sécurité accrue. Pour en savoir plus, consultez « Site-to-Site VPNs for Firepower Threat Defense » (VPN de site à site Firepower Threat Defense) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

  Lorsque vous configurez les options FTD VPN IKE et IPsec (**Appareils > VPN > Site To Site > Add**, et que vous cliquez sur les onglets **IKE** ou **IPsec**), nous vous recommandons ce qui suit :

  - Choisissez IKEv2.

- Utilisez une clé forte pour la clé manuelle prépartagée.
- Utiliser la politique IKEv2 par défaut. Par exemple, AES-GCM-NULL-SHA-LATEST.
- Cochez la case **Enable Security Association (SA) Strength Enforcement** (activer l'application de la force dans les associations de sécurité [SA]).

  Cette option garantit que l'algorithme de chiffrement utilisé par la SA IPsec enfant n'est pas plus puissant que celui de la SA IKE mère.
- Cochez la case **Enable Perfect Forward Secrecy** (activer la confidentialité de transmission parfaite).

  Cette option génère et utilise une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange contre tout déchiffrement ultérieur. Si vous sélectionnez cette option, sélectionnez l'algorithme de dérivation de clé Diffie-Hellman à utiliser lors de la génération de la clé de session PFS dans la liste déroulante **Modulus Group** (groupe de modules).

Pour en savoir plus sur les options FTD VPN IKE ci-dessus, voir « Configuring Firepower Threat Defense Site-to-site VPNs » (configuration des VPN de site à site Firepower Threat Defense) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Pour configurer ces services, consultez « Firepower Threat Defense VPN » (VPN Firepower Threat Defense) dans le *Guide de configuration de Firepower Management Center, version 7.0*. Firepower prend en charge un large éventail d'algorithmes de chiffrement et de hachage, ainsi que des groupes Diffie-Hellman. Le choix d'un chiffrement fort peut nuire aux performances du système. Vous devez donc trouver un équilibre entre sécurité et performances qui assure une protection suffisante sans compromettre l'efficacité. Pour une discussion sur les options disponibles et les facteurs à prendre en compte, consultez « How Secure Should a VPN Connection Be? » (Dans quelle mesure une connexion VPN doit-elle être sécurisée?) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Renforcer l'accès utilisateur FTD

Le FTD prend en charge deux types d'utilisateurs :

- Utilisateurs internes : l'appareil 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 pour le FTD.

Sachez que l'utilisation de l'authentification externe nécessite la configuration d'un serveur de noms de domaine pour votre déploiement. Veillez à suivre les recommandations de renforcement pour votre DNS. (Consultez Sécuriser le système de noms de domaine (DNS) (Sécuriser le système de noms de domaine [DNS])

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 la documentation Firepower pour votre version.

Les appareils Cisco Firepower Threat Defense gérés par un FMC offrent un seul moyen d'accès à l'utilisateur : une interface de ligne de commande à laquelle on peut accéder en utilisant une connexion SSH, un numéro de série ou un clavier et moniteur pour les appareils physiques. Avec certains paramètres de configuration, ces utilisateurs peuvent également accéder à l'interpréteur de commandes de Linux.

Restreindre les privilèges de configuration

Par défaut, les appareils FTD fournissent un seul utilisateur **admin** avec des droits d'administrateur complets pour toutes les commandes FTD CLI. Cet utilisateur peut créer des comptes supplémentaires et leur accorder l'un des deux niveaux de privilèges d'accès avec la commande CLI **configure user access** :

- Basic : l'utilisateur peut utiliser des commandes CLI FTD qui n'ont aucune incidence sur la configuration du système.
- Config : l'utilisateur peut utiliser toutes les commandes CLI FTD, y compris celles qui permettent de configurer le système de manière importante.

Soyez prudent lorsque vous attribuez des droits d'accès à la configuration à un compte et lorsque vous choisissez les utilisateurs auxquels vous accordez l'accès à un compte avec des droits d'accès à la configuration.

Restreindre l'accès à Linux Shell

Le FTD géré par le FMC ne prend en charge que l'accès CLI via son interface de gestion, en utilisant une connexion SSH, un numéro de série, ou un clavier et un moniteur. Cette fonction est accessible au compte **admin**, aux utilisateurs internes et peut être mise à la disposition des utilisateurs externes.

Les utilisateurs ayant un accès de niveau configuration peuvent utiliser la commande CLI **expert** pour accéder à l'interpréteur de commandes de Linux.

Mise en garde Sur tous les appareils, les comptes disposant d'un accès de niveau configuration CLI ou d'un accès à l'interpréteur de commandes Linux peuvent obtenir les privilèges sudoers dans l'interpréteur de commandes de Linux, ce qui peut présenter un risque pour la sécurité. Pour renforcer la sécurité du système, nous recommandons :

- Lorsque vous donnez à des utilisateurs l'accès à des comptes authentifiés en externe sur des appareils FTD, n'oubliez pas que tous les comptes authentifiés en externe sur des appareils FTD ont un accès au niveau de configuration de la CLI.
- N'ajoutez pas de nouveaux comptes directement dans le l'interpréteur de commandes de Linux; sur les appareils FTD, créez de nouveaux comptes en utilisant uniquement la commande CLI **configure user add**.
- Utilisez la commande FTD CLI **configure ssh-access-list** pour limiter les adresses IP à partir desquelles un appareil FTD acceptera les connexions SSH sur son interface de gestion.

Les administrateurs peuvent également configurer le FTD pour bloquer tout accès à l'interpréteur de commandes de Linux à l'aide de la commande CLI **system lockdown-sensor**. Une fois le verrouillage du système terminé, tout utilisateur qui se connecte au FTD n'aura accès qu'aux commandes CLI du FTD. Il peut s'agir d'une mesure de renforcement importante, mais il convient de l'utiliser avec précaution, car elle ne peut être annulée sans un correctif du Centre d'assistance technique Cisc.

Renforcer les comptes d'utilisateurs internes

Lors de la configuration d'utilisateurs internes individuels, les utilisateurs disposant d'un accès Config peuvent utiliser les commandes CLI **configure user** FTD pour renforcer le système contre les attaques par le biais des mécanismes de connexion à l'interface Web. Les paramètres suivants sont disponibles :

- Limiter le nombre maximal d'échecs de connexion avant qu'un utilisateur ne soit bloqué et doive être réactivé par un administrateur (**configurer l'utilisateur maxfailedlogins**).
- Imposer une longueur de mot de passe minimale (**configurer l'utilisateur minpasswdlen**).
- Définir le nombre de jours de validité des mots de passe (**configurer le paramètre de vieillissement des utilisateurs**).
- Exiger des mots de passe forts (**configurer la vérification de la force de l'utilisateur**).
- Attribuez à l'utilisateur des privilèges d'accès correspondant uniquement au type d'accès dont il a besoin (**configurer l'accès de l'utilisateur**).
- Forcer l'utilisateur à réinitialiser le mot de passe du compte lors de la prochaine connexion (**configure user forcereset**).

Si votre déploiement Firepower utilise le multidétenteur, tenez compte du domaine auquel appartient un appareil FTD lorsque vous accordez aux utilisateurs l'accès à ce périphérique.

Pour en savoir plus, consultez « Domain Management » (gestion des domaines) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Renforcer les comptes d'utilisateurs externes

Si vous choisissez d'utiliser un serveur externe pour l'authentification des utilisateurs FTD, gardez à l'esprit que les utilisateurs externes ont toujours des privilèges de configuration; les autres rôles d'utilisateur ne sont pas pris en charge. Configurez l'authentification externe pour les utilisateurs FTD à partir de l'interface Web FMC en créant une politique de paramètres de plateforme FTD sous **Devices > Platform Settings** (Appareils > Paramètres de la plateforme), et en choisissant **External Authentication** (authentification externe) dans la table des matières. La configuration de comptes d'utilisateurs externes nécessite l'établissement d'une connexion avec un serveur LDAP ou RADIUS par le biais d'un objet d'authentification externe. Pour plus d'informations, voir « Configure External Authentication for SSH » (configurer l'authentification externe pour SSH) dans le *Guide de configuration de Firepower Management Center, version 7.0*.

Important Vous pouvez établir des connexions sécurisées avec des serveurs LDAP ou RADIUS à partir de Firepower, mais le module d'authentification n'est pas conforme à la norme FIPS.

- Sachez que tous les utilisateurs externes FTD ont un accès de configuration, et à moins que vous ne bloquiez l'accès au shell Linux avec la commande **system lockdown-sensor**, ces utilisateurs peuvent accéder à l'interpréteur de commandes Linux. Les utilisateurs de l'interpréteur de commandes Linux peuvent obtenir les privilèges de l'administrateur, ce qui présente un risque pour la sécurité.
- Si vous utilisez LDAP pour effectuer l'authentification externe, sous **Advanced Options** (options avancées), configurez le chiffrement TLS ou SSL.

Établir des délais d'attente pour les sessions

La limitation de la durée des connexions à un FTD réduit la possibilité pour les utilisateurs non autorisés d'exploiter les sessions non surveillées.

Pour définir des délais de session sur un appareil FTD, créez une stratégie de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **Timeouts** (délais d'expiration) dans la table des matières. Consultez « Configure Global Timeouts » (configurer les délais d'expiration globaux) dans le *Guide de configuration de Firepower Management Center, version 7.0* pour des instructions complètes.

Considérations sur l'API REST FTD

L'API REST Cisco Firepower Threat Defense 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. L'API est décrite dans le *Cisco Firepower Threat Defense REST API Guide* (guide REST API de Cisco Firepower Threat Defense).

Important Bien que vous puissiez établir des connexions sécurisées entre le FTD et un client API REST à l'aide de TLS, le module d'authentification n'est pas conforme aux normes FIPS.

Protéger les sauvegardes

Pour protéger les données du système et leur disponibilité, effectuez des sauvegardes régulières de votre appareil FTD. La fonction de sauvegarde paraît sous **Système** > **Outils** > **Sauvegarde et restauration** dans l'interface Web FMC et est décrite dans « Backup Devices Remotely » (sauvegarde à distance des appareils) dans le *Guide de configuration de Firepower Management Center, version 7.0*. Pour restaurer une configuration FTD sauvegardée, utilisez la commande FTD **restore** de l'interface de ligne de commande.

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 le dispositif de stockage à distance n'est peut-être pas sécurisée.

Exportation sécurisée des données

L'interface de ligne de commande FTD permet de télécharger certains fichiers du FTD vers un ordinateur local. Cette fonction est fournie pour que vous puissiez collecter des informations à fournir au Centre d'assistance technique Cisco lors du dépannage de votre système, et ne doit pas être utilisée de manière occasionnelle. Prenez des précautions pour protéger tous les fichiers que vous téléchargez à partir de FTD; choisissez les options les plus sûres lors du téléchargement, sécurisez l'ordinateur local où vous stockez les données et utilisez les protocoles les plus sûrs lorsque vous transmettez des fichiers à l'ATC. En particulier, soyez conscient des risques possibles lorsque vous utilisez les commandes suivantes :

- **show asp inspect-dp snort queue-exhaustion** [**snapshot** *snapshot_id*] [**export** *location*]

  L'option **export** ne prend en charge que TFTP.

- **file copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  Cette commande transfère des fichiers vers un hôte distant à l'aide d'un protocole FTP non sécurisé.

- **copy [/noverify] /noconfirm** {**/pcap capture:/**[*buffer_name*] | *src_url* | **running-config** | **startup-config**} *dest_url*

Les options suivantes pour *src_url* et *dest_url* permettent de sécuriser les données copiées :

- Mémoire flash interne
- Mémoire du système
- Clé USB externe en option
- HTTPS sécurisé avec mot de passe
- SCP sécurisé avec mot de passe, précisant l'interface cible sur le serveur SCP
- FTP sécurisé avec mot de passe
- TFTP sécurisé avec mot de passe, précisant l'interface cible sur le serveur TFTP

Nous recommandons de ne pas utiliser les options *src_url* et *dest_url* suivantes dans un système renforcé :

- SMB, serveur UNIX, système de fichiers local
- Système de fichiers de trace de grappe. (Les systèmes dont la conformité aux certifications de sécurité est activée ne prennent pas en charge les grappes).

- **cpu profile dump** *dest_url*

  Les options suivantes pour *dest_url* permettent de sécuriser le vidage des données :

  - Mémoire flash interne
  - Clé USB externe en option
  - HTTPS sécurisé avec mot de passe
  - SMB, serveur UNIX, système de fichiers local
  - SCP sécurisé avec mot de passe, précisant l'interface cible sur le serveur SCP
  - FTP sécurisé avec mot de passe
  - TFTP sécurisé avec mot de passe, précisant l'interface cible sur le serveur TFTP

  Nous déconseillons l'utilisation de systèmes de fichiers en grappe pour les options *src_url* et *dest_url* dans un système renforcé.

- **file secure-copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  Copie le(s) fichier(s) vers un hôte distant à l'aide de SCP.

Journal système sécurisé

Le FTD peut envoyer des messages de journal système à un serveur de journaux système externe; choisir des options sécurisées lors de la configuration de la fonctionnalité de journaux système :

1. Créez une politique de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **Syslog** (journal système) dans la table des matières. Lors de l'ajout d'un serveur de journaux système sous l'onglet **Serveurs syslog** (serveur de journal système), veillez à choisir le protocole TCP et à cocher la case **Enable secure syslog** (activer le journal système sécurisé). Ces options s'appliquent aux messages de journal système générés par le FTD si vous ne les remplacez pas ailleurs dans la configuration de votre appareil.

Remarque Par défaut, lorsque le journal système sécurisé est activé, si un serveur de journaux système utilisant TCP est en panne, le FTD ne transmet pas le trafic. Pour modifier ce comportement, cochez la case **Allow user traffic to pass when TCP syslog server is down** (autoriser le trafic utilisateur à passer lorsque le serveur de journaux système TCP est hors service).

2. Configurez la journalisation dans vos politiques de contrôle d'accès afin d'hériter des paramètres de journalisation de la politique des paramètres de la plateforme. (Sous **Policies** > **Access Control** <each policy> **[chaque politique] > Logging [journalisation]**, cochez la case **Use the syslog settings configured in the FTD Platform Settings policy deployed on the device** [Utiliser les paramètres du journal système configurés dans la stratégie des paramètres de la plateforme FTD déployée sur l'appareil]).

Avec ces deux paramètres de configuration en place, le journal système FTD se comporte comme suit :

- Les paramètres du journal système de la stratégie des paramètres de la plateforme s'appliquent aux messages du journal système relatifs à l'état de l'appareil et du système, ainsi qu'à la configuration du réseau.
- Les paramètres du journal système dans les paramètres de plateforme s'appliquent aux journaux système pour les événements de connexion et de renseignement de sécurité *à moins* que vous ne remplaciez le paramètre de la politique de contrôle d'accès à l'un des endroits répertoriés dans « Configuration Locations for Syslogs for Configuration and Security Intelligence Events (All Devices) » (Emplacements de configuration pour les journaux système des événements de configuration et de renseignement sur la sécurité [tous les appareil]) dans le *Guide de configuration de Firepower Management Center, version 7.0*. Ces dérogations ne fournissent pas d'option de journal système sécurisée, et nous recommandons donc de ne pas les utiliser dans un environnement sécurisé.
- Les paramètres du journal système de la politique de paramètres de plate-forme s'appliquent aux journaux système pour les événements d'intrusion *à moins* que vous ne remplaciez le paramètre de la politique de contrôle d'accès à l'un des endroits répertoriés dans « Configuration Locations for Syslogs for Intrusion Events (FTD 6.3 Devices) » (Emplacements de configuration pour les journaux système relatifs aux événements d'intrusion [appareils FTD 6.3] dans le *Guide de configuration de Firepower Management Center, version 7.0*. Ces dérogations ne fournissent pas d'option de journal système sécurisée, et nous recommandons donc de ne pas les utiliser dans un environnement sécurisé.

Personnaliser la bannière de connexion

Vous pouvez configurer l'appareil FTD pour qu'il transmette des informations essentielles aux utilisateurs lorsqu'ils se connectent à l'interface de ligne de commande. Du point de vue de la sécurité, la bannière de connexion doit décourager les accès non autorisés :

> Vous vous êtes connecté à un appareil sécurisé. Si vous n'êtes pas autorisé à accéder à cet appareil, déconnectez-vous immédiatement sous peine de poursuites pénales.

Pour configurer la bannière de connexion d'un appareil FTD, créez une stratégie de paramètres de plateforme FTD sous **Devices (appareils)** > **Platform Settings (paramètres de plateforme)**, et choisissez **Banner** (bannière) dans la table des matières. Consultez « Configure Banners » (configurer les bannières) dans le *Guide de configuration de Firepower Management Center, version 7.0* pour des instructions complètes.

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 12.

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, consultez « About User Identity Sources » (à propos des sources d'identité des utilisateurs) 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* (domaines) 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** comem 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** comem 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.

Remarque Firepower se connecte à un serveur RADIUS pour l'identité de l'utilisateur uniquement si un appareil géré FTD dans le déploiement est configuré pour fournir un accès à distance VPN, qui sera utilisé comme source d'identité de l'utilisateur. Pour plus d'informations sur la configuration et la sécurisation du VPN d'accès à distance, consultez Renforcer les paramètres du protocole réseau (renforcer les paramètres du protocole réseau).

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, consultez « 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 gérant la 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 FTD dépend d'un micrologiciel et d'un système d'exploitation sous-jacent complexe. 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 appareils FTD modèles 2100, 4100 et 9300, sécurisez le système d'exploitation Firepower eXtensible sur lequel le FTD fonctionne; voir le *guide de renforcement Cisco Firepower 4100/9300 FXOS*.

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.