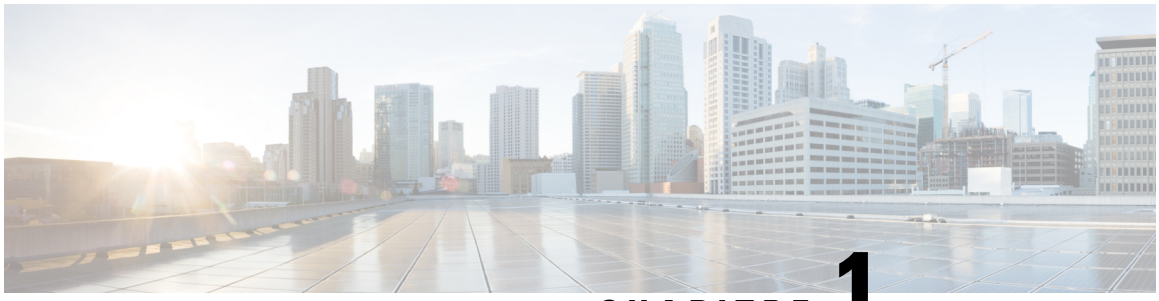
Guide de renforcement de Cisco Firepower 4100/9300 FXOS

Dernière modification : 2025-04-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPITRE 1

Introduction

Ce document fournit des informations pour vous aider à renforcer votre système d'exploitation extensible (FXOS) Cisco Firepower sur les périphériques de la plateforme 4100 et 9300, ce qui augmente la sécurité globale de votre réseau. Pour obtenir des informations sur le renforcement d'autres composants de votre déploiement Firepower, consultez les documents suivants :

- Guide Cisco pour renforcer le pare-feu ASA
- Guide de renforcement de Cisco Firepower Management Center, version 6.4
- Guide de renforcement Cisco Firepower Threat Defense, version 6.4

Les trois plans fonctionnels d'un réseau (les plans de gestion, de contrôle et de données) fournissent chacun une fonctionnalité différente qui doit être protégée.

Plan de gestion
: Le plan de gestion contient le groupe logique de tout le trafic qui prend en charge les fonctions de provisionnement, de maintenance et de surveillance pour Cisco FXOS. Le trafic dans ce groupe comprend HTTP/HTTPS, SSH, FTP, Protocole SNMP (Simple Network Management Protocol), Syslog, TACACS+, RADIUS (Remote Authentication Dial-in User Service) et DNS. Le trafic du plan de gestion est toujours destiné au Cisco FXOS local.

Plan de commande
: Le plan de commande contient le groupe logique de tous les protocoles de commutation, de signalisation, d'état de liaison et autres protocoles de contrôle utilisés pour créer et maintenir l'état du réseau et des interfaces telles que le protocole LLDP (Link Layer Discovery Protocol) et le protocole de contrôle d'agrégation de liaison. (LACP). Le trafic du plan de commande est toujours destiné au périphérique Cisco FXOS local.

Plan de données
: Le plan de données contient le groupe logique de trafic d'applications client généré par les hôtes, les clients, les serveurs et les applications qui proviennent d'autres périphériques similaires pris en charge par le réseau et en sont destinés.

Ce document est structuré en trois sections :

- Opérations réseau sécurisées
- Renforcement du plan de gestion
- Gestion des utilisateurs

Bien que la plus grande partie de ce document soit dédiée à la configuration sécurisée d'un périphérique Cisco FXOS, les configurations ne sécurisent pas complètement un réseau. Les procédures opérationnelles utilisées sur le réseau, ainsi que les personnes qui gèrent le réseau, contribuent aussi à la sécurité que la configuration des périphériques sous-jacents. Lorsque cela est possible et approprié, ce document contient des recommandations qui, mises en œuvre, permettent de sécuriser un déploiement Cisco FXOS.

• Conformité des certifications de sécurité, à la page 2

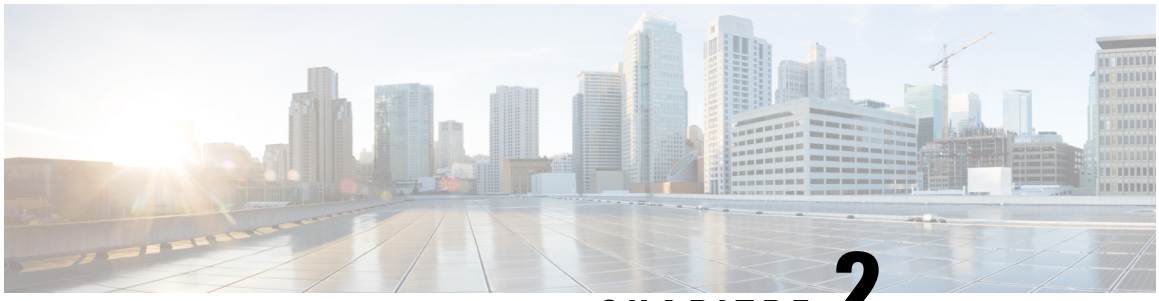
Conformité des certifications de sécurité

Prenez en note que 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.

Lorsqu'il est configuré conformément aux documents d'orientation propres à la certification, le système Firepower prend en charge la conformité 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 l'UCAPL dans la documentation du Firepower et dans l'interface Web du Firepower Management Center peuvent être interprétées comme des références à l'APL du DoDIN.
- 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.



CHAPITRE 2

Opérations réseau sécurisées

La sécurisation des opérations du réseau est un sujet important. Bien que la plus grande partie de ce document soit dédiée à la configuration sécurisée d'un périphérique Firepower 4100/9300 exécutant FXOS, les configurations à elles seules ne sécurisent pas complètement un réseau. Les procédures opérationnelles utilisées sur le réseau, ainsi que les personnes qui gèrent le réseau, contribuent aussi à la sécurité que la configuration des périphériques sous-jacents.

Les sections suivantes contiennent des recommandations opérationnelles qu'il est conseillé aux administrateurs FXOS de mettre en œuvre. Ces sections mettent en évidence des domaines critiques des opérations du réseau et ne sont pas complètes.

Supervision des avis de sécurité Cisco

L'équipe chargée de traiter les incidents liés à la sécurité des produits Cisco (PSIRT) crée et tient à jour des publications, communément appelées « Cisco Security Advisories » (avis de sécurité Cisco), sur les problèmes de sécurité des produits Cisco. Les avis de sécurité sont disponibles sur http://www.cisco.com/go/psirt.

Pour en savoir plus sur les rapports de vulnérabilités de Cisco PSIRT, consultez la Politique sur les failles de sécurité de Cisco.

Pour maintenir un système sécurisé, les administrateurs Cisco FXOS doivent être conscients des informations communiquées dans les avis de sécurité Cisco. Une connaissance détaillée de la vulnérabilité est nécessaire avant d'évaluer la menace que la vulnérabilité peut présenter pour un réseau. Pour obtenir de l'aide sur ce processus d'évaluation, voir Triage des risques pour les annonces sur les failles de sécurité.

Passer à la dernière version de FXOS

Des mises à jour de sécurité importantes sont incluses dans chaque nouvelle version groupée de la plateforme de FXOS. Nous vous recommandons de mettre à jour votre système FXOS à la dernière version disponible dès que possible.

Pour en savoir plus sur la compatibilité et les chemins de mise à niveau pris en charge pour FXOS dans diverses configurations, consultez le guide *de compatibilité de Cisco Firepower 4100/9300 FXOS* et le *Guide de mise à niveau de Cisco Firepower 4100/9300* sur Cisco.com.

Personnaliser la bannière de pré-connexion

Vous pouvez spécifier le message que FXOS affiche aux utilisateurs avant qu'ils se connectent au Firepower Chassis Manager ou à l'interface de ligne de commande de FXOS. Du point de vue du renforcement, ce message devrait être utilisé pour dissuader tout accès non autorisé.

L'exemple d'interface de ligne de commande suivant crée une bannière de pré-connexion pour le gestionnaire de châssis FXOS et l'interface de ligne de commande FXOS :

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
 You must have explicit, authorized permission to access or configure this device.
 Unauthorized attempts and actions to access or use this system may result in civil and/or

criminal penalties.
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

Activer le mode Common Criteria ou FIPS

Si votre organisation est tenue de n'utiliser que des équipements et des logiciels conformes aux normes de sécurité établies par le ministère américain de la défense ou d'autres organismes de certification gouvernementaux, vous pouvez activer le mode Common Criteria ou FIPS pour appliquer plusieurs changements de renforcement avec un seul paramètre. Notez que si votre organisation n'est pas tenue de se conformer aux normes de conformité des certifications de sécurité, vous pouvez toujours activer les modes FIPS ou Common Criteria pour FXOS, mais sachez que cela peut entraîner des problèmes de compatibilité sur votre appareil.

Les options pour activer le mode Common Criteria ou FIPS apparaissent sous **Platform Settings (Paramètres de plateforme)** > **FIPS/Common Criteria (FMC/Critères communs)** en mode dans l'interface Web Firepower Chassis Manager.

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 Common Criteria ou FIPS 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.
- Utilisez un outil conforme aux FIPS pour l'accès aux périphériques lorsque FIPS, Common Criteria ou les deux sont activés.

Sécuriser le protocole de temps réseau (NTP)

Il est fortement recommandé d'utiliser un serveur NTP (Network Time Protocol) de confiance pour synchroniser l'heure du système sur votre Firepower 4100/9300 FXOS et ses serveurs associés.

Pour activer NTP pour FXOS, vous devez d'abord générer des ID de clé NTP et des valeurs de clé, puis ajouter le serveur NTP au châssis FXOS à l'aide du flux de travail suivant dans FXOS Chassis Manager : **Platform Settings > Set Time Source > Use NTP Server**. Pour renforcer le NTP, configurez l'authentification du serveur NTP.

Pour des instructions complètes sur la configuration d'un serveur NTP et de l'authentification par serveur NTP pour FXOS, consultez la rubrique Réglage de la date et de l'heure à l'aide de NTP du chapitre des paramètres de la plateforme du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*.

Remarque

- Lorsqu'elle est activée, la fonctionnalité d'authentification NTP est globale pour tous les serveurs configurés associés à FXOS.
- Seul SHA1 est pris en charge pour l'authentification du serveur NTP.
- Vous avez besoin de l'ID de clé et de la valeur de clé pour authentifier un serveur. L'ID de clé est utilisée pour indiquer au client et au serveur quelle valeur de clé utiliser lors du calcul du condensé du message. La valeur de clé est une valeur fixe qui est dérivée à l'aide de ip-keygen.

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.

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 bonnes pratiques de sécurité recommandées par l'industrie. Cisco propose des lignes directrices dans ce document : https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html.

Exploiter l'authentification, l'autorisation et la comptabilité

Le cadre Authentification, Autorisation et Comptabilité (AAA) est essentiel pour sécuriser l'accès interactif aux périphériques réseau. Le cadre AAA fournit un environnement hautement configurable qui peut être adapté selon les besoins du réseau.

RADIUS et TACACS+ sont tous deux pris en charge sur le système FXOS. TACACS+ chiffre l'ensemble des données utiles TCP, qui comprend le nom d'utilisateur et le mot de passe. Radius chiffre uniquement le mot de passe. De plus, TACACS+ permet l'autorisation de commande, tandis que RADIUS ne fournit que l'authentification et la traçabilité. Par conséquent, nous vous suggérons d'utiliser TACACS+ pour une sécurité d'authentification maximale.

En outre, vous pouvez utiliser LDAP pour l'authentification des utilisateurs. Pour chiffrer l'échange d'authentification LDAP, utilisez l'option CLI pour utiliser SSL.

```
Firepower/security/ldap/server # set ssl yes
```

Pour en savoir plus et pour connaître les procédures complètes sur la configuration de AAA, consultez la section « Configuration de AAA » du chapitre des paramètres de la plateforme du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*.

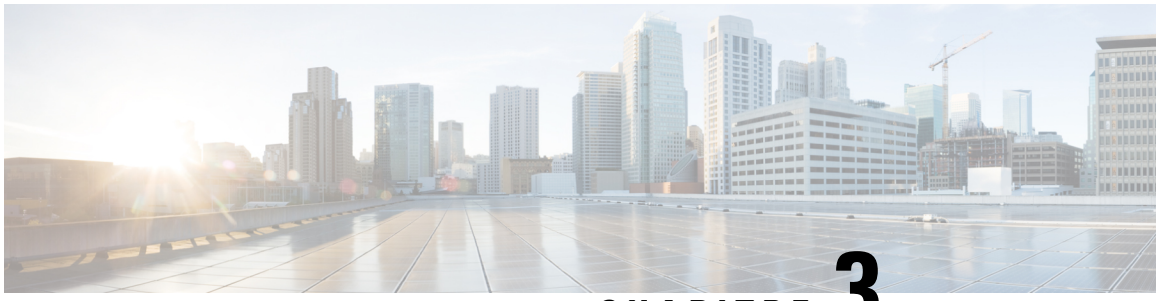
Utiliser des protocoles sécurisés

Cisco FXOS utilise de nombreux protocoles pour acheminer des données de gestion de réseau sensibles. Vous devez utiliser des protocoles sécurisés dans la mesure du possible. Un choix de protocole sécurisé comprend l'utilisation de SSH au lieu de Telnet afin que les données d'authentification et les informations de gestion soient chiffrées. En outre, vous devez utiliser des protocoles de transfert de fichiers sécurisés lorsque vous copiez des données de configuration. Par exemple, l'utilisation du protocole Secure Copy Protocol (SCP) au lieu de FTP ou TFTP. Pour en savoir plus sur l'utilisation des protocoles sécurisés, consultez la section Plan de gestion, à la page 7 de ce document.

Gestion de la configuration

La gestion de la configuration est un processus par lequel les modifications de configuration sont proposées, examinées, approuvées et déployées.

La configuration d'un appareil Cisco FXOS contient de nombreux détails sensibles, notamment les noms d'utilisateur, les mots de passe et le contenu des listes de contrôle d'accès (ACL). Le référentiel utilisé pour archiver les configurations des périphériques Cisco FXOS doit être sécurisé et l'accès doit être limité aux rôles et aux fonctions nécessitant un accès. Un accès non sécurisé à ces informations peut compromettre la sécurité de l'ensemble du réseau.



CHAPITRE 3

Plan de gestion

Le plan de gestion se compose de fonctions qui atteignent les objectifs de gestion du réseau. Ces objectifs comprennent des séances de gestion interactive à l'aide du protocole SSH ainsi que la collecte de statistiques avec le protocole SNMP. Lorsqu'on envisage la sécurité d'un appareil réseau, il est essentiel que le plan de gestion soit protégé. Si un incident de sécurité sape les fonctions du plan de gestion, la récupération ou la stabilité du réseau peut ne pas être possible.

Les sections suivantes détaillent les fonctions et les configurations de sécurité disponibles dans Cisco FXOS qui permettent de renforcer le plan de gestion :

Renforcer le plan de gestion

Le plan de gestion est utilisé pour accéder à un périphérique, le configurer et le gérer, ainsi que pour surveiller ses opérations et le réseau sur lequel il est déployé. Le plan de gestion reçoit et envoie le trafic pour les opérations de ces fonctions. Le plan de gestion et le plan de commande d'un périphérique doivent être sécurisés, car les opérations du plan de commande ont une incidence directe sur les opérations du plan de gestion. La liste suivante comprend les protocoles utilisés par le plan de gestion :

- SNMP
- Telnet
- SSH
- SFTP

- FTP
- TFTP
- HTTP / HTTPS
- Protocole Secure Copy Protocol (SCP)
- TACACS+
- RADIUS
- LDAP
- Protocole de temps réseau (NTP)
- Syslog

Les administrateurs doivent prendre des mesures pour assurer l'intégrité des plans de gestion et de commande lors des incidents de sécurité. Si l'un de ces plans est exploité avec succès, tous les plans peuvent être compromis.

Sessions de gestion du contrôle et du chiffrement

Étant donné que des renseignements peuvent être divulgués au cours d'une séance de gestion interactive, le trafic doit être chiffré afin qu'un utilisateur malveillant ne puisse pas lire les données transmises. Le chiffrement du trafic permet une connexion sécurisée d'accès à distance au périphérique. Si le trafic d'une session de gestion est envoyé sur le réseau en texte brut, un pirate pourrait obtenir des informations sensibles sur le périphérique et le réseau. Les protocoles suivants sont pris en charge sur FXOS :

- SSH
- TLS
- HTTPS
- SNMP
- LDAP
- Telnet

Remarque Telnet n'est pas un protocole sécurisé, et nous recommandons aux administrateurs de FXOS de ne pas l'utiliser.

Les sections suivantes détaillent les options de configuration de renforcement pour les protocoles de session de gestion.

Installer un certificat d'identité de confiance

Après la configuration initiale, un certificat SSL autosigné est généré pour une utilisation avec l'application Web du châssis FXOS. Comme ce certificat est autosigné, les navigateurs clients ne le font pas automatiquement confiance. La première fois qu'un nouveau navigateur client accède à l'interface Web du châssis FXOS, le navigateur lance un avertissement SSL et demande à l'utilisateur d'accepter le certificat avant d'accéder au châssis FXOS. Vous devez générer une requête de signature de certificat (CSR) à l'aide de l'interface de ligne de commande de FXOS et installer le certificat d'identité qui en découle pour l'utiliser avec le châssis FXOS. Ce certificat d'identité permet à un navigateur client de faire confiance à la connexion et d'afficher l'interface Web sans avertissement.

Pour la procédure complète d'installation d'un certificat d'identité de confiance, consultez la rubrique « Installation d'un certificat d'identité de confiance » dans le *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*.

Certificats, trousseaux de clés et points de confiance

Le protocole HTTPS utilise des composants de l'infrastructure de clé publique (PKI) pour établir des communications sécurisées entre deux appareils, comme le navigateur d'un client et le Châssis 9300 .

Clés de chiffrement et trousseaux de clés

Chaque périphérique PKI contient une paire de clés de chiffrement Rivest-Shamir-Adleman (RSA) asymétriques, une conservée privée et une rendue publique, stockée dans un trousseau de clés interne. Un message chiffré avec l'une ou l'autre des clés peut être déchiffré avec l'autre clé. Pour envoyer un message chiffré, l'expéditeur chiffre le message avec la clé publique du destinataire et le destinataire déchiffre le message à l'aide de sa propre clé privée. Un expéditeur peut également prouver qu'il est propriétaire d'une clé publique en chiffrement (également appelé « signature ») d'un message connu avec sa propre clé privée. Si un destinataire peut déchiffrer le message avec succès en utilisant la clé publique en question, la possession de la clé privée correspondante par l'expéditeur est attestée. Les clés de chiffrement peuvent varier en longueur, avec des longueurs typiques de 512 bits à 2048 bits. En général, une clé longue est plus sécurisée qu'une clé plus courte. FXOS fournit un trousseau de clés par défaut avec une paire de clés initiale de 2048 bits et vous permet de créer des trousseaux de clés supplémentaires.

Le certificat de trousse de clés par défaut doit être régénéré manuellement si le nom de la grappe change ou si le certificat expire.

Certificats

Pour préparer des communications sécurisées, deux appareils échangent d'abord leurs certificats numériques. Un certificat est un fichier contenant la clé publique d'un périphérique ainsi que des informations signées sur l'identité de ce dernier. Pour prendre en charge les communications chiffrées, un appareil peut générer sa propre paire de clés et son propre certificat autosigné. Lorsqu'un utilisateur distant se connecte à un périphérique qui présente un certificat autosigné, l'utilisateur n'a pas de méthode facile pour vérifier l'identité du périphérique, et le navigateur de l'utilisateur affiche d'abord un avertissement d'authentification. Par défaut, FXOS contient un certificat autosigné intégré contenant la clé publique du trousseau de clés par défaut.

Points de confiance

Pour fournir une authentification renforcée pour FXOS, vous pouvez obtenir et installer un certificat tiers à partir d'une source ou d'un point de confiance qui confirme l'identité de votre périphérique. Le certificat tiers est signé par le point de confiance d'émetteur, qui peut être une autorité de certification racine (CA) ou une CA intermédiaire ou une ancre d'approbation faisant partie d'une chaîne d'approbation qui mène à une CA racine. Pour obtenir un nouveau certificat, vous devez générer une demande de certificat par l'intermédiaire de FXOS et soumettre la demande à un point de confiance.

Important Le certificat doit être au format X.509 codé en Base64 (CER).

Configurer le protocole HTTPS

Utilisez le flux de travail suivant pour configurer et renforcer le protocole HTTPS sur votre châssis FXOS :

1. Créez un trousseau de clés (consultez la rubrique « Création d'un trousseau de clés » du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*).
2. Créez une demande de certificat pour un trousseau de clés (consultez la rubrique « Création d'une demande de certificat pour un trousseau de clés avec des options avancées » du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*).
3. Créez un point de confiance (consultez la rubrique « Création d'un point de confiance » du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*).
4. Importez le certificat dans le trousseau de clés (consultez la rubrique « Importation d'un certificat dans un trousseau de clés » du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*).

Utilisez les options supplémentaires suivantes pour renforcer le HTTPS :

- Précisez le niveau de sécurité de la suite de chiffrement utilisé par le domaine (**set https cipher-suite-mode**). Nous recommandons une valeur **fort** ou **personnalisé**. Si vous choisissez personnalisé, vous devez préciser un niveau personnalisé de sécurité de la suite de chiffrement pour le domaine (**set https cipher-suite** *cipher-suite-spec-chaîne*).
- Activez la vérification de la liste de révocation de certificat.

Configurer SSH

Nous vous recommandons d'utiliser SSHv2, qui est activé par défaut en utilisant le port TCP 22. Notez les options de configuration de renforcement SSH suivantes qui peuvent être activées sur le serveur et le client :

Force de clé RSA (set ssh-server host-key rsa/set ssh-client host-key rsa)

La valeur du module (en bits) est un multiple de 8 de 1024 à 2048. Plus la taille du module de clé que vous spécifiez est grande, plus il faut de temps pour générer une paire de clés RSA. Nous recommandons une valeur de 2048.

Algorithmes de chiffrement (set ssh-server encrypt-algorithm/set ssh-client encrypt-algorithm)

Les algorithmes de chiffrement suivants sont pris en charge sur FXOS :

```
3des-cbc    3DES  CBC
aes128-cbc  AES128 CBC
aes128-ctr  AES128 CTR
aes192-cbc  AES192 CBC
aes192-ctr  AES192 CTR
aes256-cbc  AES256 CBC
aes256-ctr  AES256 CTR
```

Remarque 3des-cbc n'est pas conforme aux critères communs.

Algorithme d'échange de clé Diffie-Hellman (set ssh-server kex-algorithm/set ssh-client kex-algorithm)

L'échange de clés DH fournit un secret partagé qui ne peut être déterminé par aucune des parties à elles seules. L'échange de clé est combiné à une signature et à la clé de l'hôte pour authentifier l'hôte. Cette méthode d'échange de clés fournit une authentification explicite du serveur. Pour en savoir plus sur l'utilisation des méthodes d'échange de clés DH, consultez la RFC 4253.

Les algorithmes DH suivants sont pris en charge sur FXOS :

```
diffie-hellman-group14-sha1  Diffie-Hellman Group14 SHA1
```

Algorithmes MAC des serveurs et des clients (set ssh-server mac-algorithm/set ssh-client mac-algorithm)

Les algorithmes MAC suivants sont pris en charge sur FXOS :

```
hmac-sha1      Hmac SHA1
hmac-sha2-256  HMAC SHA2 256
hmac-sha2-512  HMAC SHA2 512
```

Limite de renouvellement du volume (set ssh-server rekey-limit volume/set ssh-client rekey-limit volume)

Détermine la quantité de trafic en Ko autorisée sur la connexion avant que FXOS ne se déconnecte de la session.

Time ReKey Limit (définir l'heure de reconnexion du serveur ssh-server/définir l'heure de rekey-limit ssh-client)

Détermine le nombre de minutes pendant lesquelles une session SSH peut être inactive avant que FXOS ne déconnecte la session.

Définir la vérification de clé d'hôte stricte (définir ssh-client stricthostkeycheck)

Contrôle la clé d'hôte SSH en vérifiant :

- **enable** (activer) - La connexion est rejetée si la clé de l'hôte n'est pas déjà dans le fichier des hôtes connus de FXOS. Vous devez ajouter manuellement des hôtes à l'aide de la commande CLI FXOS **enter ssh-host** dans l'étendue système/services.
- **prompt** (invite) - Vous êtes invité à accepter ou à rejeter la clé d'hôte si elle n'est pas déjà stockée sur le châssis.
- **disable** (désactiver) : (valeur par défaut) le châssis accepte automatiquement la clé d'hôte si elle n'a pas été stockée auparavant.

Pour connaître les procédures complètes de configuration de SSH sur votre châssis FXOS, consultez le chapitre des paramètres de la plateforme dans le *Guide de configuration de Cisco Firepower 4100/9300 FXOS Chassis Manager* et dans le *Guide de configuration de Cisco Firepower 4100/9300 FXOS CLI*.

SNMP sécurisé

Il est essentiel que votre protocole de gestion de réseau simple (SNMP) soit correctement sécurisé afin de protéger la confidentialité, l'intégrité et la disponibilité des données du réseau et des appareils réseau par lesquels ces données transitent. Le protocole SNMP fournit une kyrielle d'informations sur l'état des périphériques réseau. Ces renseignements doivent être protégés contre les utilisateurs malintentionnés qui souhaitent utiliser ces données afin d'effectuer des attaques contre le réseau.

SNMPv3 prend en charge les modèles et les niveaux de sécurité. Un modèle de sécurité est une méthode d'authentification configurée pour un utilisateur et le rôle dans lequel l'utilisateur réside. Un niveau de sécurité est le niveau de sécurité autorisé dans un modèle de sécurité. Une combinaison d'un modèle de sécurité et d'un niveau de sécurité détermine quel mécanisme de sécurité est utilisé lors du traitement d'un paquet SNMP.

Les identifiants de communauté SNMP sont des mots de passe appliqués au châssis FXOS pour restreindre l'accès en lecture seule et en lecture-écriture aux données SNMP de l'appareil. Ces identifiants de communauté, comme tous les mots de passe, doivent être sélectionnés avec soin pour éviter qu'ils ne soient pas triviaux. Les identifiants de communauté doivent être modifiés à des intervalles réguliers et conformément aux politiques de sécurité du réseau. Par exemple, les identifiants doivent être modifiés lorsqu'un administrateur réseau change de rôles ou quitte l'entreprise.

Pour en savoir plus sur les niveaux et les modèles de sécurité SNMP pris en charge, consultez la section « Configuration SNMP » du chapitre Paramètres de la plateforme du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*.

Journal système sécurisé

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

L'envoi d'informations de journalisation à un serveur syslog distant permet de corréler et d'auditer plus efficacement les événements de réseau et de sécurité sur les périphériques réseau. Notez que les messages du journal système sont transmis en texte clair. Pour cette raison, toutes les protections qu'un réseau offre au trafic de gestion (par exemple, le chiffrement ou l'accès hors bande) doivent être étendues pour inclure le trafic syslog. Pour vous assurer que le trafic journal système n'est jamais envoyé en texte clair sur des réseaux non fiables, vous pouvez configurer le canal sécurisé IPSec. IPSec fournit un service de chiffrement et d'authentification de bout en bout sur les paquets de données qui empruntent le réseau public.

Pour en savoir plus sur la configuration de syslog sur votre châssis FXOS, consultez la section Configuration de Syslog du chapitre des paramètres de la plateforme du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*. Pour en savoir plus sur la configuration d'IPSec, consultez la rubrique Configurer le canal sécurisé IPSec du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*.

Configuration de la liste d'accès IP

Par défaut, le châssis FXOS refuse tout accès au serveur Web local. Vous devez configurer votre liste d'accès IP avec les adresses IP des hôtes ou des sous-réseaux autorisés pour chaque protocole.

La liste d'accès IP prend en charge les protocoles suivants :

- HTTPS
- SSH
- SNMP

Pour chaque liste d'adresses IP (v4 ou v6), jusqu'à 100 sous-réseaux différents peuvent être configurés pour chaque service. Un sous-réseau de 0 et un préfixe de 0 permettent un accès sans restriction à un service.

Pour plus d'informations et des procédures complètes sur la configuration des listes d'accès IP sur votre châssis FXOS, consultez la rubrique « Configuration de la liste d'accès IP » dans le chapitre Paramètres de la plateforme du *Guide de configuration de Cisco Firepower 4100/9300 FXOS Chassis Manager* et de *Cisco Firepower 4100/ 9300 Guide de configuration de l'interface de ligne de commande FXOS*.

Configurer le canal sécurisé IPSec

Configurez IPSec sur votre châssis Firepower 4100/9300 pour fournir un service de chiffrement et d'authentification de bout en bout sur les paquets de données passant par le réseau public.

Remarque Si vous utilisez un canal sécurisé IPSec en mode FIPS, l'homologue IPSec doit prendre en charge la RFC 7427.

Pour des instructions complètes sur la configuration d'un canal sécurisé IPSec pour votre châssis FXOS, consultez la rubrique « Configuration du canal sécurisé IPSec » dans le chapitre Conformité des certifications de sécurité du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*.

À propos de la vérification des listes de révocations de certificat

Vous pouvez configurer votre mode de vérification de liste de révocation de certificat (CRL) pour qu'il soit strict ou décompressé dans les connexions IPSec, HTTPS et LDAP sécurisées.

FXOS récupère les informations de CRL dynamiques (non statiques) à partir des informations CDP d'un certificat X.509, ce qui indique les informations de CRL dynamiques. L'administration du système télécharge manuellement les informations sur les CRL statiques, ce qui indique les informations sur les CRL locales dans le système FXOS. FXOS traite les informations de CRL dynamiques en fonction du certificat de traitement actuel dans la chaîne de certificats. La liste de révocation de certificats statique est appliquée à l'ensemble de la chaîne de certificats homologues.

Pour les étapes à suivre pour activer ou désactiver les contrôles de révocation de certificat pour vos connexions sécurisées IPSec, LDAP et HTTPS, consultez Configuration du canal sécurisé IPSec, Création d'un fournisseur LDAP et configuration du protocole HTTPS.

Remarque

- Si le mode de vérification de révocation de certificat est défini sur Strict, la CRL statique ne s'applique que lorsque la chaîne de certificats homologues a un niveau de 1 ou plus. (Par exemple, lorsque la chaîne de certificats homologues ne contient que le certificat de l'autorité de certification racine et le certificat homologue signé par l'autorité de certification racine.)
- Lors de la configuration de la CRL statique pour IPSec, le champ Authority Key Identifier (authkey) doit être présent dans le fichier CRL importé. Dans le cas contraire, IPSec la considère comme non valide.
- La CRL statique a priorité sur la CRL dynamique du même émetteur. Lorsque FXOS valide le certificat homologue, si une CRL statique valide (déterminée) du même émetteur existe, FXOS ignore le CDP dans le certificat homologue.
- La vérification stricte des CRL est activée par défaut dans les scénarios suivants :
  - Connexions fournisseur LDAP sécurisées, connexions IPSec ou entrées de certificat client nouvellement créées
  - Gestionnaires de châssis FXOS nouvellement déployés (déployés avec une version initiale de démarrage de FXOS 2.3.1.x ou une version ultérieure)

Les tableaux suivants décrivent les résultats de la connexion, en fonction de vos paramètres de vérification de liste de révocation de certificat et de la validation de certificat.

Tableau 1 : Mode de vérification de révocation de certificat défini sur Strict sans CRL statique locale

Sans CRL statique locale	Connexion LDAP	Connexion IPSec	Authentification par certificat client
Vérification de la chaîne de certificats des pairs	Une chaîne de certificats complète est requise	Une chaîne de certificats complète est requise	Une chaîne de certificats complète est requise
Vérification du protocole de découverte Cisco (CDP) dans la chaîne de certificats de pair	Une chaîne de certificats complète est requise	Une chaîne de certificats complète est requise	Une chaîne de certificats complète est requise
Le protocole de découverte Cisco (CDP) vérifie le certificat de l'autorité de certification racine de la chaîne de certificats homologues	Oui	Sans objet	Oui
Tout échec de validation de certificat dans la chaîne de certificats homologues	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système
Tout certificat révoqué dans la chaîne de certificats de pair	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système

Sans CRL statique locale	Connexion LDAP	Connexion IPSec	Authentification par certificat client
Un CDP manquant dans la chaîne de certificats de pair	La connexion échoue avec le message de journalisation système	Certificat de pair : échec de la connexion avec le message syslog Autorités de certification intermédiaires : échecs de connexion	La connexion échoue avec le message de journalisation système
Une CRL de CDP est vide dans la chaîne de certificats de pair avec une signature valide	Connexion établie avec succès	Connexion établie avec succès	La connexion échoue avec le message de journalisation système
Aucun CDP de la chaîne de certificats homologues ne peut être téléchargé	La connexion échoue avec le message de journalisation système	Certificat de pair : échec de la connexion avec le message syslog Autorités de certification intermédiaires : échecs de connexion	La connexion échoue avec le message de journalisation système
Le certificat a CDP, mais le serveur CDP est en panne	La connexion échoue avec le message de journalisation système	Certificat de pair : échec de la connexion avec le message syslog Autorités de certification intermédiaires : échecs de connexion	La connexion échoue avec le message de journalisation système
Le certificat a un CDP, le serveur est opérationnel et la CRL est sur le CDP, mais la CRL a une signature non valide	La connexion échoue avec le message de journalisation système	Certificat de pair : échec de la connexion avec le message syslog Autorités de certification intermédiaires : échecs de connexion	La connexion échoue avec le message de journalisation système

Tableau 2 : Mode de vérification de révocation de certificat défini sur Strict avec une CRL statique locale

Avec CRL statique locale	Connexion LDAP	Connexion IPSec
Vérification de la chaîne de certificats des pairs	Une chaîne de certificats complète est requise	Une chaîne de certificats complète est requise
Vérification du CDP dans la chaîne de certificats de pair	Une chaîne de certificats complète est requise	Une chaîne de certificats complète est requise
CDP vérifie le certificat de l'autorité de certification racine de la chaîne de certificats homologues	Oui	Sans objet

Avec CRL statique locale	Connexion LDAP	Connexion IPSec
Tout échec de validation de certificat dans la chaîne de certificats homologues	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système
Tout certificat révoqué dans la chaîne de certificats de pair	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système
Un CDP manquant dans la chaîne de certificats homologue (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Une CRL de CDP est vide dans la chaîne de certificats des homologues (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Aucun CDP de la chaîne de certificats homologues ne peut pas être téléchargé (le niveau de chaîne de certificats est de 1)	Connexion établie avec succès	Connexion établie avec succès
Le certificat a un CDP, mais le serveur CDP est en panne (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Le certificat a un CDP, le serveur est opérationnel et la CRL est sur le CDP, mais la CRL a une signature non valide (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Le niveau de la chaîne de certificats du pair est supérieur à 1	La connexion échoue avec le message de journalisation système	Combiné avec le CDP, la connexion réussit S'il n'y a pas de CDP, la connexion échoue avec le message de journal système

Tableau 3 : Mode de vérification de révocation de certificat défini sur Développé sans CRL statique locale

Sans CRL statique locale	Connexion LDAP	Connexion IPSec	Authentification par certificat client
Vérification de la chaîne de certificats des pairs	Chaîne de certificats complète	Chaîne de certificats complète	Chaîne de certificats complète
Vérification du CDP dans la chaîne de certificats de pair	Chaîne de certificats complète	Chaîne de certificats complète	Chaîne de certificats complète

Sans CRL statique locale	Connexion LDAP	Connexion IPSec	Authentification par certificat client
Le protocole de découverte Cisco (CDP) vérifie le certificat de l'autorité de certification racine de la chaîne de certificats homologues	Oui	Sans objet	Oui
Tout échec de validation de certificat dans la chaîne de certificats homologues	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système
Tout certificat révoqué dans la chaîne de certificats de pair	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système
Un CDP manquant dans la chaîne de certificats de pair	Connexion établie avec succès	Connexion établie avec succès	La connexion échoue avec le message de journalisation système
Une CRL de CDP est vide dans la chaîne de certificats de pair avec une signature valide	Connexion établie avec succès	Connexion établie avec succès	Connexion établie avec succès
Aucun CDP de la chaîne de certificats homologues ne peut être téléchargé	Connexion établie avec succès	Connexion établie avec succès	Connexion établie avec succès
Le certificat a CDP, mais le serveur CDP est en panne	Connexion établie avec succès	Connexion établie avec succès	Connexion établie avec succès
Le certificat a un CDP, le serveur est opérationnel et la CRL est sur le CDP, mais la CRL a une signature non valide	Connexion établie avec succès	Connexion établie avec succès	Connexion établie avec succès

Tableau 4 : Mode de vérification de révocation de certificat défini sur Développé avec une CRL statique locale

Avec CRL statique locale	Connexion LDAP	Connexion IPSec
Vérification de la chaîne de certificats des pairs	Chaîne de certificats complète	Chaîne de certificats complète
Vérification du CDP dans la chaîne de certificats de pair	Chaîne de certificats complète	Chaîne de certificats complète

Avec CRL statique locale	Connexion LDAP	Connexion IPSec
CDP vérifie le certificat de l'autorité de certification racine de la chaîne de certificats homologues	Oui	Sans objet
Tout échec de validation de certificat dans la chaîne de certificats homologues	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système
Tout certificat révoqué dans la chaîne de certificats de pair	La connexion échoue avec le message de journalisation système	La connexion échoue avec le message de journalisation système
Un CDP manquant dans la chaîne de certificats homologue (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Une CRL de CDP est vide dans la chaîne de certificats des homologues (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Aucun CDP de la chaîne de certificats homologues ne peut pas être téléchargé (le niveau de chaîne de certificats est de 1)	Connexion établie avec succès	Connexion établie avec succès
Le certificat a CDP, mais le serveur CDP est en panne (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Le certificat a un CDP, le serveur est opérationnel et la CRL est sur le CDP, mais la CRL a une signature non valide (le niveau de chaîne de certificats est 1)	Connexion établie avec succès	Connexion établie avec succès
Le niveau de la chaîne de certificats du pair est supérieur à 1	La connexion échoue avec le message de journalisation système	Combiné avec le CDP, la connexion réussit S'il n'y a pas de CDP, la connexion échoue avec le message de journal système

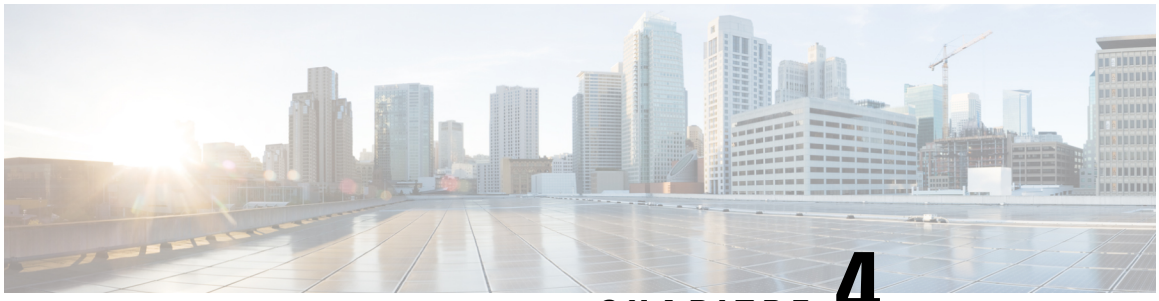
Configurer la CRL statique pour un point de confiance

Les certifications révoquées sont conservées dans la liste des révocations de certification (Certificate Revocation List ou CRL). Les applications clients utilisent la liste de révocation de certificats pour vérifier l'authentification d'un serveur. Les applications serveur utilisent la liste de révocation de certificats pour accorder ou refuser les demandes d'accès des applications clientes qui ne sont plus de confiance.

Vous pouvez configurer votre châssis Firepower 4100/9300 pour valider les certificats de pair à l'aide des informations de la liste de révocation de certification (CRL).

Une fois que vous avez configuré la validation des certificats homologues à l'aide des informations de la liste de révocation de certification, vous pouvez également configurer votre système pour télécharger périodiquement une CRL afin qu'une nouvelle CRL soit utilisée toutes les 1 à 24 heures pour valider les certificats.

Pour des instructions détaillées sur la configuration d'une liste de révocation de certification pour un point de confiance, consultez la rubrique « Configurer la CRL statique pour un point de confiance » dans le chapitre Conformité des certifications de sécurité du *Guide de configuration de l'interface de ligne de commande Cisco Firepower 4100/9300 FXOS*.



CHAPITRE 4

Contrôle d'accès basé sur les rôles sécurisé

Les rôles d'utilisateur sont assortis de privilèges qui définissent ce que peut faire l'utilisateur dans le système. Le système contient les rôles d'utilisateur suivants :

Administrateur

Accès complet en lecture et écriture à l'ensemble du système. Le compte admin par défaut se voit attribuer ce rôle par défaut et ne peut pas être modifié.

Lecture seule

Accès en lecture seule à la configuration du système sans privilège de modification de l'état du système.

Opérations

Accès en lecture-écriture à la configuration NTP, à la configuration de Smart Call Home pour les licences Smart et aux journaux du système, y compris les serveurs et les défaillances Syslog. Accès en lecture au reste du système.

Administrateur AAA

Accès en lecture-écriture aux utilisateurs, aux rôles et à la configuration AAA. Accès en lecture au reste du système.

À l'aide de l'interface Web de FXOS Chassis Manager ou de l'interface de ligne de commande de FXOS, vous pouvez configurer les paramètres suivants pour chaque compte d'utilisateur du système :

- User Role (Rôle d'utilisateur) : le rôle qui représente les privilèges que vous souhaitez attribuer au compte d'utilisateur.

  Tous les utilisateurs se voient attribuer le rôle en lecture seule par défaut et ce rôle ne peut pas être désélectionné. Pour attribuer plusieurs rôles, maintenez **`la touche Ctrl`**enfoncée et cliquez sur les rôles souhaités.

- Date d'échéance du compte
- Account Status (État du compte) : si l'état est défini sur **Actif**, l'utilisateur peut se connecter au Firepower Chassis Manager et à l'interface de ligne de commande FXOS avec son identifiant de connexion et son mot de passe.

Pour une sécurité maximale sur les comptes authentifiés localement, configurez le protocole SSH pour les sessions chiffrées.

- Gestion des mots de passe, à la page 22
- Renforcement de la protection des comptes d'utilisateurs authentifiés localement, à la page 22

• Renforcer les comptes d'utilisateurs authentifiés à distance, à la page 22

Gestion des mots de passe

Les mots de passe contrôlent l'accès aux ressources ou aux périphériques, et les administrateurs définissent les mots de passe pour authentifier les demandes. Lorsque FXOS reçoit une demande d'accès à une ressource ou à un périphérique, la demande est contestée pour la vérification du mot de passe et de l'identité, et l'accès est accordé, refusé ou limité en fonction du résultat. Les bonnes pratiques de sécurité exigent que les mots de passe soient gérés avec un serveur d'authentification LDAP, TACACS+ ou RADIUS. Cependant, un mot de passe configuré localement pour l'accès est toujours requis en cas de défaillance des services LDAP, TACACS+ ou RADIUS. Un appareil peut également avoir d'autres renseignements de mot de passe dans sa configuration, comme une clé NTP ou une chaîne de communauté SNMP.

Renforcement de la protection des comptes d'utilisateurs authentifiés localement

Lors de la configuration des rôles individuels des utilisateurs internes, les utilisateurs du compte administrateur peuvent utiliser les paramètres suivants pour renforcer le système contre les attaques par le biais des mécanismes de connexion à l'interface Web :

- Définissez le nombre maximal de tentatives de connexion infructueuses autorisées avant qu'un utilisateur ne soit bloqué hors du châssis Firepower 4100/9300 pendant une durée déterminée (**définir max-login-attempts**)
- Définissez la durée pendant laquelle l'utilisateur doit rester verrouillé hors du système après avoir dépassé le nombre maximal de tentatives de connexion (**set user-account-unlock-time**)
- Appliquez une longueur de mot de passe minimale (**set min-password-length**)
- Précisez le nombre minimal d'heures qu'un utilisateur authentifié localement doit attendre avant de modifier un mot de passe nouvellement créé (**set no-change-interval**)
- Définissez le nombre de jours pendant lesquels les comptes des utilisateurs locaux sont valides (**définir l'expiration**)
- Exigez des mots de passe sécurisés (**set enforce-strong-password yes**)
- Attribuer à l'utilisateur des privilèges d'accès correspondant uniquement au type d'accès dont il a besoin (**créer un rôle**).

Renforcer les comptes d'utilisateurs authentifiés à distance

Un compte d'utilisateur authentifié à distance est tout compte d'utilisateur authentifié par LDAP, RADIUS ou TACACS+. L'authentification à distance permet un maximum de 16 serveurs TACACS+, de 16 serveurs RADIUS et de 16 fournisseurs LDAP pour un total de 48 fournisseurs.

AAA est un ensemble de services destinés à contrôler l'accès aux ressources informatiques, à appliquer des politiques, à évaluer l'utilisation et à fournir les renseignements nécessaires pour facturer les services. Ces processus sont considérés comme importants pour une gestion et une sécurité efficaces du réseau.

Notez que si un utilisateur gère un compte d'utilisateur local et un compte d'utilisateur distant simultanément, les rôles définis dans le compte d'utilisateur local remplacent ceux maintenus dans le compte d'utilisateur distant.

TACACS+ est un protocole d'authentification que le châssis FXOS peut utiliser pour authentifier les utilisateurs de gestion sur un serveur AAA distant. Ces utilisateurs de gestion peuvent accéder au châssis FXOS par SSH, HTTPS, Telnet ou HTTP. Nous recommandons le protocole SSH pour une sécurité maximale lors de l'accès au châssis FXOS. De nombreuses méthodes d'authentification offrent une sécurité renforcée.

L'authentification TACACS+, ou plus généralement l'authentification AAA, permet d'utiliser des comptes d'utilisateurs individuels pour chaque administrateur réseau. Lorsque vous ne dépendez pas d'un seul mot de passe partagé, la sécurité du réseau est améliorée et votre responsabilité est renforcée.

RADIUS est un protocole similaire à TACACS+; Cependant, il chiffre uniquement le mot de passe envoyé sur le réseau. En revanche, TACACS+ chiffre l'ensemble des données utiles TCP, qui comprend le nom d'utilisateur et le mot de passe. Pour cette raison, nous vous recommandons d'utiliser TACACS+ de préférence à RADIUS lorsque TACACS+ est pris en charge par le serveur AAA.

LDAP est un protocole client-serveur pour l'accès aux services d'annuaire, tels que Microsoft Active Directory. LDAP n'exige aucune sécurité entre le client et le serveur. Cependant, au moyen du protocole SSL, LDAP peut chiffrer les sessions d'utilisateur entre le client et le serveur. Ainsi, toutes les informations transférées dans les transactions LDAP sur le réseau sont sécurisées. Pour cette raison, nous vous recommandons fortement d'utiliser LDAP de préférence à TLS.

Pour en savoir plus et pour les procédures détaillées sur la configuration de RADIUS, TACAS+ et LDAP sur votre châssis FXOS, consultez la section Configuration de AAA dans le chapitre des paramètres de la plateforme du *Guide de configuration de l'interface de ligne de commande 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.