Pour commencer

Les rubriques suivantes expliquent comment commencer la configuration de Cisco Firepower Threat Defense (FTD) .

Ce guide est-il pour vous?

Ce guide explique comment configurer Cisco Firepower Threat Defense à l'aide de l'interface de configuration Web Cisco Firepower Device Manager (FDM) incluse sur les appareils Cisco Firepower Threat Defense.

Le FDM vous permet de configurer les fonctionnalités de base du logiciel, les plus couramment utilisées pour les réseaux de petite ou moyenne taille. Il est spécialement conçu pour les réseaux qui comprennent un seul dispositif ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire de dispositifs multiples de grande puissance qui permet de contrôler un grand réseau contenant de nombreux dispositifs Cisco Firepower Threat Defense.

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet Cisco Firepower Threat Defense, utilisez Cisco Firepower Management Center (FMC) pour configurer vos périphériques au lieu du FDM intégré.

Vous pouvez utiliser FDM sur les périphériques suivants.

Tableau 1 : Modèles compatibles FDM

Modèle du périphérique	Version minimale du logiciel FTD
Firepower 1010, 1120, 1140	6.4
Firepower 1150	6.5
Firepower 2110, 2120, 2130, 2140	6.2.1
Cisco Secure Firewall 3110, 3120, 3130, 3140	7.1
Firepower 4110, 4120, 4140, 4150	6.5

Modèle du périphérique	Version minimale du logiciel FTD
Firepower 4112	6.6
Firepower 9300	6.5
FTDv (FTDv) pour VMware	6.2.2
FTDv pour la machine virtuelle basée sur le noyau (KVM)	6.2.3
FTDv pour le nuage Microsoft Azure	6.5
FTDv pour le nuage Amazon Web Services (AWS)	6.6
ASA 5508-X, 5516-X **Remarque** La prise en charge de ces modèles se termine avec la version 7.0, qui est la dernière version autorisée. Vous ne pouvez pas installer la version 7.1 ou une version ultérieure sur ces modèles.	6.1
ISA 3000 (Cisco 3000 Series Industrial Security Appliances)	6.2.3

Nouvelles fonctionnalités dans FDM/FTD version 7.1.0

Date de sortie : 1er décembre 2021

Le tableau suivant répertorie les nouvelles fonctions disponibles dans Cisco Firepower Threat Defense 7.1.0 lorsqu'elles sont configurées à l'aide de FDM.

Fonctionnalités	Description
Caractéristiques de la plateforme	
Secure Firewall 3100	Nous avons présenté les Cisco Secure Firewall 3110, 3120, 3130 et 3140. Vous pouvez échanger à chaud un module de réseau du même type lorsque le pare-feu est sous tension sans avoir à redémarrer; apporter d'autres modifications au module nécessite un redémarrage. Les interfaces de Cisco Secure Firewall 3100 25 Gbit/s prennent en charge la correction d'erreurs sans voie de retour ainsi que la détection de la vitesse en fonction du SFP installé. Les disques SSD sont des disques à chiffrement automatique (SED), et si vous avez deux disques SSD, ils forment un RAID logiciel. Notez que le gestionnaire de périphériques de la version 7.1 ne comprend pas d'aide en ligne pour ces périphériques. Consultez la documentation publiée sur Cisco.com. Écrans nouveaux ou modifiés : **Device (périphérique)** > **Interfaces** Commandes Cisco Firepower Threat Defense nouvelles ou modifiées : **configure network speed, configure raid, show raid, show ssd**

Fonctionnalités	Description
FTDv pour les instances AWS.	FTDv pour AWS ajoute la prise en charge de ces instances : • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv pour les instances Azure.	FTDv pour Azure ajoute la prise en charge de ces instances : • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

Fonctionnalités	Description
Fin de la prise en charge pour ASA 5508-X et 5516-X. La dernière version prise en charge est Cisco Firepower Threat Defense 7.0.	Vous ne pouvez pas installer Cisco Firepower Threat DefenseCisco Firepower Threat Defense 7.1 sur un ASA 5508-X ou 5516-X. La dernière version prise en charge pour ces modèles est Cisco Firepower Threat Defense 7.0.
Fonctionnalités de pare-feu et IPS	
Configuration de la politique d'analyse de réseau (NAP) pour Snort 3.	Vous pouvez utiliser FDM pour configurer la politique d'analyse de réseau (NAP) lors de l'exécution de Snort 3. Les politiques d'analyse de réseau contrôlent l'inspection prétraitement du trafic. Les inspecteurs préparent le trafic à une inspection plus approfondie en le normalisant et en relevant les anomalies de protocole. Vous pouvez sélectionner la NAP à utiliser pour tout le trafic et personnaliser les paramètres afin qu'ils fonctionnent de manière optimale avec le trafic de votre réseau. Vous ne pouvez pas configurer la NAP lorsque vous exécutez Snort 2. Nous avons ajouté la politique d'analyse de réseau à la boîte de dialogue des paramètres **Policies (politiques)** > **Intrusion**, avec un éditeur JSON intégré pour permettre les modifications directes, et d'autres fonctionnalités pour vous permettre de charger les remplacements ou de télécharger ceux que vous créez.
Prise en charge de la NAT manuelle pour les objets de nom de domaine complet (FQDN) en tant que destination de la traduction.	Vous pouvez utiliser un objet de réseau FQDN, par exemple spécifiant www.exemple.com, comme adresse de destination traduite dans les règles NAT manuelles. Le système configure la règle en fonction de l'adresse IP renvoyée par le serveur DNS.
Amélioration de l'authentification active pour les règles d'identité.	Vous pouvez configurer l'authentification active pour que les règles de politique d'identité redirigent l'authentification de l'utilisateur vers un nom de domaine complet (FQDN) plutôt que l'adresse IP de l'interface par laquelle la connexion de l'utilisateur entre dans le périphérique. Le nom de domaine complet doit mener à l'adresse IP de l'une des interfaces du périphérique. En utilisant un nom de domaine complet, vous pouvez attribuer un certificat pour l'authentification active que le client reconnaîtra, évitant ainsi que les utilisateurs reçoivent un avertissement de certificat non fiable lorsqu'ils sont redirigés vers une adresse IP. Le certificat peut préciser un nom de domaine complet, un nom de domaine complet générique ou plusieurs noms de domaine complets sous les autres noms de l'objet (SAN) du certificat. Nous avons ajouté l'option **Redirect to Host Name (rediriger vers le nom d'hôte)** dans les paramètres de politique d'identité.
Fonctionnalités du VPN	

Fonctionnalités	Description
Homologue de secours distants pour le VPN de site à site.	Vous pouvez configurer une connexion VPN de site à site pour inclure des homologues de secours distants. Si l'homologue distant principal n'est pas disponible, le système tentera de rétablir la connexion VPN en utilisant l'un des homologues de secours. Vous pouvez configurer des clés ou des certificats prépartagés distincts pour chaque homologue de secours. Les homologues de secours ne sont pris en charge que pour les connexions basées sur des politiques et ne sont pas disponibles pour les connexions basées sur le routage (interface de tunnel virtuel). Nous avons mis à jour l'assistant VPN de site à site pour inclure la configuration des homologues de secours.
Gestion des mots de passe pour le VPN d'accès à distance (MSCHAPv2).	Vous pouvez activer la gestion des mots de passe pour le VPN d'accès à distance. Cela permet à AnyConnect d'inviter l'utilisateur à modifier un mot de passe expiré. Sans la gestion des mots de passe, les utilisateurs doivent modifier les mots de passe expirés directement avec le serveur AAA, et AnyConnect n'invite pas l'utilisateur à changer de mot de passe. Pour les serveurs LDAP, vous pouvez également définir une période d'avertissement pour informer les utilisateurs de la prochaine expiration du mot de passe. Nous avons ajouté l'option Enable Password Management (activer la gestion des mots de passe) aux paramètres d'authentification pour les profils de connexion VPN d'accès à distance.
Navigateur externe AnyConnect SAML VPN	Lorsque vous utilisez SAML comme méthode d'authentification principale pour un profil de connexion VPN d'accès à distance, vous pouvez choisir que le client AnyConnect utilise le navigateur local du client au lieu du navigateur intégré à l'AnyConnect pour effectuer l'authentification Web. Cette option active la connexion unique (SSO) entre votre authentification VPN et d'autres connexions d'entreprise. Choisissez également cette option si vous souhaitez prendre en charge des méthodes d'authentification web, telles que l'authentification biométrique, qui ne peuvent pas être exécutées dans le navigateur intégré. Nous avons mis à jour l'assistant de profil de connexion VPN d'accès à distance pour vous permettre de configurer l'**expérience de connexion SAML**.
Fonctions d'administration et de dépannage	

Fonctionnalités	Description
Prise en charge du système de nom de domaine dynamique (DDNS) pour la mise à jour du nom de domaine complet (FQDN) aux mappages d'adresses IP pour les interfaces du système.	Vous pouvez configurer le DDNS pour les interfaces du système afin d'envoyer des mises à jour dynamiques aux serveurs DNS. Cela permet de garantir que les FQDN définis pour les interfaces sont résolus vers la bonne adresse, ce qui facilite l'accès des utilisateurs au système à l'aide d'un nom d'hôte plutôt que d'une adresse IP. Cela est particulièrement utile pour les interfaces qui obtiennent leurs adresses en utilisant DHCP, mais c'est également utile pour les interfaces à adresse statique. Après la mise à niveau, si vous avez utilisé FlexConfig pour configurer DDNS, vous devez refaire votre configuration à l'aide de FDM ou de l'API Cisco Firepower Threat Defense et supprimer l'objet DDNS FlexConfig de la politique FlexConfig avant de pouvoir déployer de nouveau les modifications. Si vous configurez DDNS à l'aide de FDM, puis passez à la gestion par FMC, la configuration DDNS est conservée pour que FMC puisse trouver le système en utilisant le nom DNS. Dans FDM, nous avons ajouté la page **System Settings (paramètres système)** > **DDNS Service (service DDNS)**. Dans l'API Cisco Firepower Threat Defense, nous avons ajouté les ressources DDNSService et DDNSInterfaceSettings.
La commande **dig** remplace la commande **nslookup** dans l'interface de ligne de commande du périphérique.	Pour rechercher l'adresse IP d'un nom de domaine complet (FQDN) dans l'interface de ligne de commande du périphérique, utilisez la commande **dig**. La commande **nslookup** a été supprimée.
Configuration du relais DHCP à l'aide de FDM.	Vous pouvez utiliser FDM pour configurer le relais DHCP. L'utilisation du relais DHCP sur une interface vous permet de diriger les requêtes DHCP vers un serveur DHCP accessible par l'autre interface. Vous pouvez configurer le relais DHCP sur les interfaces physiques, les sous-interfaces, les interfaces VLAN et les canaux EtherChannels. Vous ne pouvez pas configurer le relais DHCP si vous configurez un serveur DHCP sur n'importe quelle interface. Nous avons ajouté la page **System Settings (paramètres systèmes)** > **DHCP** > **DHCP Relay (relais DHCP)** et déplacé DHCP Server (serveur DHCP) sous la nouvelle en-tête DHCP.
Type et taille de clé pour les certificats autosignés dans FDM.	Vous pouvez préciser le type et la taille de clé lors de la génération de nouveaux certificats CA internes et internes autosignés dans FDM. Les types de clés comprennent RSA, ECDSAA et EDDSA. Les tailles autorisées varient selon le type de clé. Nous vous avertissons désormais si vous chargez un certificat dont la taille de clé est inférieure à la longueur minimale conseillée. Il existe également un filtre de recherche prédéfini pour les clés faibles afin de vous aider à trouver les certificats faibles, que vous devriez remplacer si possible.

Fonctionnalités	Description
Restrictions de validation d'utilisation pour les certificats CA de confiance.	Vous pouvez spécifier si un certificat CA de confiance peut être utilisé pour valider certains types de connexions. Vous pouvez autoriser ou empêcher la validation du serveur SSL (utilisé par le DNS dynamique), du client SSL (utilisé par le VPN d'accès à distance), du client IPsec (utilisé par le VPN de site à site) ou d'autres fonctionnalités qui ne sont pas gérées par la plateforme d'inspection Snort, comme LDAPS. L'objectif principal de ces options est de vous empêcher d'établir des connexions VPN, car elles peuvent être validées par rapport à un certificat particulier. Nous avons ajouté **Validation Usage (utilisation de la validation)** comme propriété pour les certificats CA de confiance.
Génération du mot de passe **admin** dans FDM.	Lors de la configuration initiale du système dans FDM ou lorsque vous modifiez le mot de passe **admin** par FDM, vous pouvez désormais cliquer sur un bouton pour générer un mot de passe aléatoire de 16 caractères.
Temps de démarrage et état de compilation tmatch.	La commande **show version** comprend maintenant des renseignements sur le temps nécessaire pour démarrer le système. Notez que plus la configuration est importante, plus il faut de temps pour démarrer le système. La nouvelle commande **show asp rule-engine** affiche l'état de la compilation tmatch. La compilation tmatch est utilisée pour une liste d'accès utilisée comme groupe d'accès, le tableau NAT et certains autres éléments. Il s'agit d'un processus interne qui peut consommer des ressources CPU et affecter les performances pendant son exécution si vous avez des listes de contrôle d'accès et des tableaux NAT très volumineux. Le temps de compilation dépend de la taille de la liste d'accès, du tableau NAT, etc.
Améliorations apportées à la sortie **show access-list element-count**.	La sortie de la commande **show access-list element-count** a été améliorée. Lorsqu'elle est utilisée avec la recherche de groupes d'objets activée, la sortie comprend des détails sur le nombre de groupes d'objets dans le nombre d'éléments. En outre, la sortie **show tech-support** comprend désormais la sortie de **show access-list element-count** et **show asp rule-engine**.

Fonctionnalités	Description
Utilisez FDM pour configurer Cisco Firepower Threat Defense pour la gestion par un FMC.	Lorsque vous effectuez la configuration initiale à l'aide de FDM, toutes les configurations d'interface terminées dans FDM sont conservées lorsque vous passez à FMC pour la gestion, en plus des paramètres de gestion et d'accès FMC. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande Cisco Firepower Threat Defense, seuls les paramètres de gestion et d'accès FMC sont conservés (par exemple, la configuration de l'interface interne par défaut n'est pas conservée). Après être passé à FMC, vous ne pouvez plus utiliser FDM pour gérer le Cisco Firepower Threat Defense. Écrans nouveau ou modifiés : **System Settings (paramètres système)** > **Management Center (centre de gestion)**
Mettre automatiquement à jour les ensembles d'autorités de certification.	L'offre groupée de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Le système interroge désormais automatiquement Cisco pour obtenir de nouveaux certificats d'autorité de certification à une heure quotidienne définie par le système. Auparavant, vous deviez mettre à niveau le logiciel pour mettre à jour les certificats d'autorité de certification. Vous pouvez utiliser l'interface de ligne de commande pour désactiver cette fonctionnalité. **Remarque** Cette fonctionnalité n'est pas prise en charge dans les versions 7.0.0 à 7.0.4, 7.1.0 à 7.1.0.2 ou 7.2.0 à 7.2.3. Si vous effectuez une mise à niveau d'une version prise en charge vers une version non prise en charge, la fonctionnalité est temporairement désactivée et le système arrête de contacter Cisco. Commandes CLI nouvelles ou modifiées : **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall.
API REST de FTD version 6.2 (v6).	L'API REST Cisco Firepower Threat Defense pour la version logicielle 7.1 est la version 6.2. Vous pouvez utiliser la version v6 dans les URL d'API ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. Notez que l'élément de chemin de version d'URL pour la version 6.2 est le même que pour la version 6.0/1 : v6. Veuillez réévaluer tous les appels existants, car des modifications peuvent avoir été apportées aux modèles de ressources que vous utilisez. Pour ouvrir l'API Explorer et consulter les ressources, connectez-vous à FDM, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**.

Connexion au système

Il y a deux interfaces pour l'appareil Cisco Firepower Threat Defense

Interface Web FDM

Le FDM s'exécute dans votre navigateur Web. Vous utilisez cette interface pour configurer, gérer et surveiller le système.

Interface de ligne de commande (CLI, Console)

Utilisez cette interface de ligne de commande pour un dépannage avancé. Vous pouvez également l'utiliser pour la configuration initiale au lieu de FDM.

Les rubriques suivantes expliquent comment vous connecter à ces interfaces et gérer votre compte utilisateur.

Votre rôle d'utilisateur contrôle ce que vous pouvez voir et faire

Votre nom d'utilisateur est assorti d'un rôle, et votre rôle détermine ce que vous pouvez faire ou ce que vous pouvez voir dans le FDM. L'utilisateur **admin** défini localement dispose de tous les privilèges, mais si vous vous connectez à l'aide d'un compte différent, vous pourriez avoir moins de privilèges.

Le coin supérieur droit de la fenêtre FDM affiche votre nom d'utilisateur et votre niveau de privilège.

Les privilèges sont les suivants :

- **Administrateur** : vous pouvez voir et utiliser toutes les fonctionnalités.
- **Utilisateur en lecture-écriture** : vous pouvez faire tout ce qu'un utilisateur en lecture seule peut faire, ainsi que modifier et déployer la configuration. Les seules restrictions concernent les actions critiques pour le système, qui comprennent l'installation des mises à niveau, la création et la restauration de sauvegardes, l'affichage du journal d'audit et la déconnexion d'autres FDM utilisateurs.
- **Utilisateur en lecture seule** : vous pouvez afficher les tableaux de bord et la configuration, mais ne pouvez apporter aucune modification. Si vous tentez d'apporter une modification, le message d'erreur explique que cela est causé par un manque d'autorisation.

Ces privilèges ne sont pas liés à ceux disponibles pour les utilisateurs d'interface de ligne de commande.

Connectez-vous au FDM.

Utilisez l'FDM pour configurer, gérer et surveiller le système. Les fonctionnalités que vous pouvez configurer à l'aide du navigateur ne sont pas configurables à l'aide de l'interface de ligne de commande (CLI) ; vous devez utiliser l'interface Web pour mettre en œuvre vos politiques de sécurité.

Utilisez une version actuelle de Firefox, Chrome, Safari, Edge.

Remarque Si vous saisissez le mauvais mot de passe et ne parvenez pas à vous connecter lors de 3 tentatives consécutives, votre compte est verrouillé pendant 5 minutes. Vous devez attendre avant de réessayer de vous connecter.

Avant de commencer

Au départ, vous pouvez vous connecter à FDM en utilisant le nom d'utilisateur **admin** uniquement. Cependant, vous pouvez ensuite configurer l'autorisation pour les utilisateurs supplémentaires définis dans un serveur AAA externe, comme décrit dans Gestion de FDM et accès des utilisateurs FTD.

Il peut y avoir jusqu'à 5 connexions actives à la fois. Cela inclut les utilisateurs connectés au gestionnaire d'appareil et les sessions API actives, qui sont représentées par des jetons API non expirés. Si vous dépassez cette limite, la session la plus ancienne, soit la connexion au gestionnaire d'appareils ou le jeton API, expirera pour permettre la nouvelle session. Ces limites ne s'appliquent pas aux sessions SSH.

Procédure

Étape 1 À l'aide d'un navigateur, ouvrez la page d'accueil du système, par exemple, https://ftd.example.com.

Vous pouvez utiliser n'importe quelle des adresses suivantes. Vous pouvez utiliser l'adresse IPv4 ou IPv6 ou le nom DNS, si vous en avez configuré un.

- L'adresse IP de gestion.Par défaut (sur la plupart des plateformes), l'interface de gestion est un client DHCP, de sorte que l'adresse IP dépend de votre serveur DHCP.
- L'adresse d'une interface de données que vous avez ouverte pour l'accès HTTPS. Par défaut (sur la plupart des plateformes), l'interface « interne » permet l'accès HTTPS, afin que vous puissiez vous connecter à l'adresse interne par défaut 192.168.95.1. Consultez Configuration par défaut avant la configuration initiale, à la page 28 pour en savoir plus sur l'adresse IP interne de votre modèle.

  Si vous avez modifié le port de données HTTPS, vous devez inclure le port personnalisé dans l'URL. Par exemple, si vous avez changé le port en 4443 : https://ftd.example.com:4443

Astuces

Si votre navigateur n'est pas configuré pour reconnaître le certificat de serveur, vous verrez un avertissement concernant un certificat non fiable. Acceptez le certificat en tant qu'exception ou dans votre magasin de certificats racine de confiance.

Étape 2 Saisissez votre nom d'utilisateur et votre mot de passe définis pour le périphérique, puis cliquez sur **Login (Connexion)**.

Vous pouvez utiliser le nom d'utilisateur **admin**, qui est un utilisateur prédéfini. Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details** > **(Détails avancés)** > **User Data (Données utilisateur)**) lors du déploiement initial.

Votre session expirera après 30 minutes d'inactivité, et vous serez invité à vous connecter de nouveau. Vous pouvez vous déconnecter en sélectionnant **Log Out** (Déconnexion) dans le menu déroulant de l'icône utilisateur dans le coin supérieur droit de la page.

Connexion avec l'interface de ligne de commande (CLI)

Utilisez l'interface de ligne de commande (CLI) pour configurer le système et effectuer le dépannage de base du système. Vous ne pouvez pas configurer de politiques via une session d'interface de ligne de commande.

Pour vous connecter à l'interface de ligne de commande (CLI), procédez comme suit :

- Utilisez le câble de console fourni avec l'appareil pour connecter votre ordinateur à la console à l'aide d'un émulateur de terminal pour 9600 bauds, 8 bits de données, aucune parité, 1 bit d'arrêt, aucun contrôle de flux. Consultez le guide du matériel de votre appareil pour en savoir plus sur le câble de la console.

Remarque Sur les modèles de périphériques Firepower et Cisco Secure Firewall, l'interface de ligne de commande du port de console est Cisco Firepower eXtensible Operating System (FXOS). Pour certains modèles de périphérique, vous pouvez accéder à l'interface de ligne de commande Cisco Firepower Threat Defense en utilisant la commande **connect ftd**. Pour Firepower 4100/9300, consultez Se connecter à la console de l'application. Utilisez l'interface de ligne de commande de FXOS uniquement pour le dépannage au niveau du châssis. Utilisez l'interface de ligne de commande de Cisco Firepower Threat Defense pour la configuration de base, la surveillance et le dépannage normal du système. Consultez la documentation de FXOS pour obtenir des renseignements sur les commandes FXOS.

- Pour le FTDv, ouvrez la console virtuelle..
- Utilisez un client SSH pour établir une connexion à l'adresse IP de gestion. Vous pouvez également vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface aux connexions SSH (consultez Configuration de la liste d'accès de gestion). L'accès SSH aux interfaces de données est désactivé par défaut. Connectez-vous en utilisant le nom d'utilisateur **admin** ou un autre compte d'utilisateur de l'interface de ligne de commande. Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut pour le FTDv est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (détails avancés)** > **User Data (données utilisateur)**) lors du déploiement initial.

Conseils

- Après la connexion, pour des informations sur les commandes disponibles dans l'interface de ligne de commande, entrez **help** ou **?**. Pour obtenir des renseignements sur l'utilisation, consultez Référence de commande Cisco Firepower Threat Defense sur http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.
- Vous pouvez créer des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide de la commande **configure user add**. Cependant, ces utilisateurs peuvent uniquement se connecter à l'interface de ligne de commande. Ils ne peuvent pas se connecter à l'interface Web FDM.

- Vous pouvez créer des comptes utilisateur pour l'accès SSH sur un serveur externe. Pour en savoir plus sur la configuration de l'authentification externe pour l'accès SSH, consultez Configuration de l'autorisation externe (AAA) pour les utilisateurs de l'interface de commande (SSH) FTD.

Modifier votre mot de passe

Vous devez modifier périodiquement votre mot de passe. La procédure suivante explique comment modifier le mot de passe lorsque vous êtes connecté à FDM.

Remarque Si vous êtes connecté à l'interface de ligne de commande, vous pouvez modifier votre mot de passe à l'aide de la commande **configure password**. Vous pouvez modifier le mot de passe d'un autre utilisateur d'interface de ligne de commande avec la commande **configure user password** *username*.

Avant de commencer

Cette procédure s'applique uniquement aux utilisateurs locaux. Si votre compte d'utilisateur est défini sur un serveur AAA externe, vous devez modifier votre mot de passe sur ce serveur.

Procédure

Étape 1 Sélectionnez **Profile** (Profil) dans la liste déroulante de l'icône utilisateur en haut à droite du menu.

Étape 2 Cliquez sur l'onglet **Password** (Mot de passe).

Étape 3 Saisissez votre mot de passe actuel.

Étape 4 Saisissez votre nouveau mot de passe, puis confirmez-le.

Vous pouvez cliquer sur **Generate** (Générer) pour faire générer un mot de passe aléatoire de 16 caractères pour vous. Cliquez sur le bouton Show Password (Afficher le mot de passe) () pour voir les mots de passe non masqués. Ensuite, cliquez sur le lien **Copy To Clipboard** (Copier dans le presse-papiers) pour pouvoir coller le mot de passe dans le champ de confirmation.

La page comprend les exigences minimales d'un mot de passe. Vous ne pouvez pas modifier ces exigences minimales. Les mots de passe doivent :

- être composé de 8 à 128 caractères
- Avoir au moins une minuscule et une majuscule
- Avoir au moins un chiffre
- Avoir au moins un caractère spécial
- Ne pas contenir de lettre répétée

Étape 5 Cliquez sur **Change** (Modifier).

Définition des préférences de profil utilisateur

Vous pouvez définir des préférences pour l'interface utilisateur et modifier votre mot de passe.

Procédure

Étape 1 Sélectionnez **Profile** (Profil) dans la liste déroulante de l'icône utilisateur en haut à droite du menu.

Étape 2 Dans l'onglet **Profile** (Profil), configurez les éléments suivants, puis cliquez sur **Save** (Enregistrer).

- **Time Zone for Scheduling Tasks** (Fuseau horaire pour la planification des tâches) : sélectionnez le fuseau horaire que vous souhaitez utiliser pour planifier des tâches telles que les sauvegardes et les mises à jour. Le fuseau horaire du navigateur est utilisé pour les tableaux de bord et les événements, si vous définissez une zone différente.
- **Thème de couleur** : sélectionnez le thème de couleur que vous souhaitez utiliser dans l'interface utilisateur.

Étape 3 Sous l'onglet **Password** (Mot de passe), vous pouvez saisir un nouveau mot de passe et cliquer sur **Change** (Modifier).

Configuration du système

Vous devez effectuer une configuration initiale pour que le système fonctionne correctement dans votre réseau. Un déploiement réussi comprend la connexion correcte des câbles et la configuration des adresses nécessaires pour insérer l'appareil dans votre réseau et le connecter à Internet ou à un autre routeur en amont. La procédure suivante explique le processus de bout en bout.

Avant de commencer

Avant de commencer la configuration initiale, le périphérique comprend certains paramètres par défaut. Pour de plus amples renseignements, consultez la section Configuration par défaut avant la configuration initiale, à la page 28.

Procédure

Étape 1 Connecter les interfaces, à la page 14

Étape 2 Compléter la configuration initiale avec l'assistant d'installation, à la page 24

Pour en savoir plus sur la configuration résultante, consultez Configuration après la configuration initiale, à la page 31.

Connecter les interfaces

La configuration par défaut suppose que certaines interfaces sont utilisées pour les réseaux internes et externes. La configuration initiale sera plus facile à réaliser si vous connectez les câbles réseau aux interfaces en fonction de ces attentes.

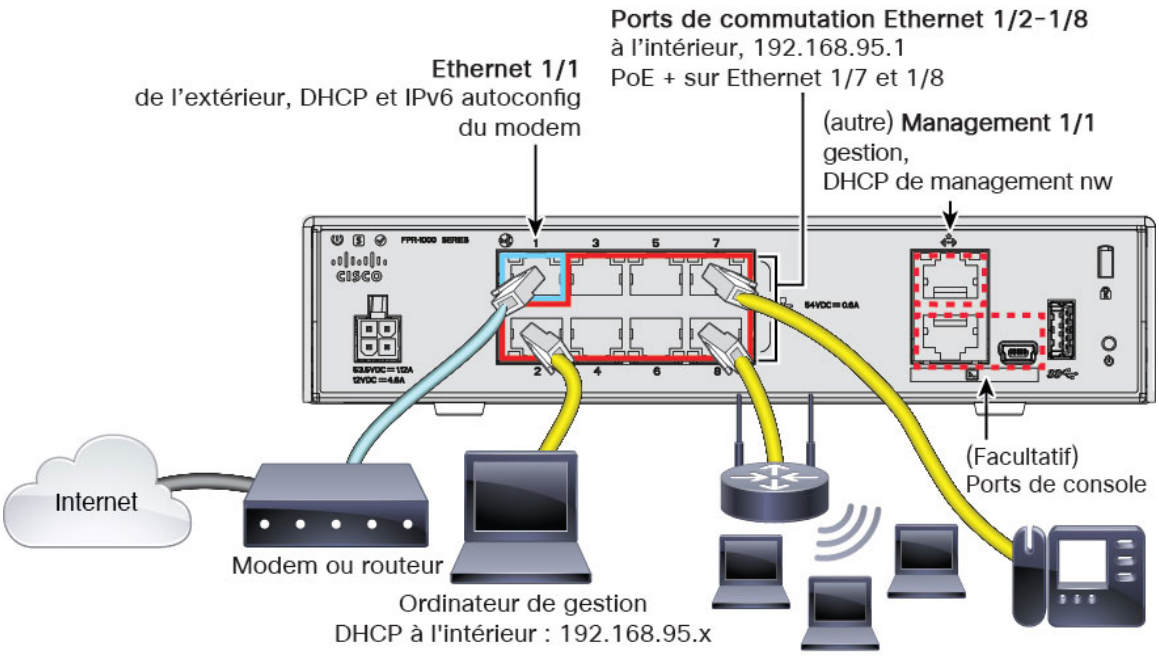
La configuration par défaut de la plupart des modèles est conçue pour vous permettre de connecter votre ordinateur de gestion à l'interface interne. Sinon, vous pouvez également connecter directement votre station de travail au port de gestion. Les interfaces sont sur des réseaux différents, alors n'essayez pas de connecter les interfaces internes et le port de gestion sur le même réseau.

Ne connectez aucune des interfaces internes à un réseau doté d'un serveur DHCP actif. Cela entre en conflit avec le serveur DHCP qui fonctionne déjà sur l'interface interne Si vous souhaitez utiliser un autre serveur DHCP pour le réseau, désactivez le serveur DHCP indésirable après la configuration initiale.

Les rubriques suivantes montrent comment câbler le système pour cette topologie lorsque vous utilisez les interfaces internes pour configurer le périphérique.

Câblage du Firepower 1010

Illustration 1 : Câblage du Firepower 1010



- Connectez votre ordinateur de gestion à l'une des interfaces suivantes :
  - Ethernet 1/2 à 1/8 : Connectez votre ordinateur de gestion directement à l'un des ports de commutation internes (Ethernet 1/2 à 1/8). L'adresse IP par défaut de l'interface interne est (192.168.95.1) Cette interface exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris

l'ordinateur de gestion). Assurez-vous donc que ces paramètres n'entrent pas en conflit avec les paramètres du réseau interne.

- Management 1/1 : Connectez votre ordinateur de gestion directement au réseau de gestion. L'interface de gestion Management 1/1 obtient une adresse IP de DHCP. Assurez-vous donc que votre réseau comprend un serveur DHCP.

  Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut pour configurer une adresse IP statique, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 23.

Vous pourrez configurer ultérieurement l'accès de gestion à partir d'autres interfaces.

- Connectez le réseau externe à l'interface Ethernet 1/1.

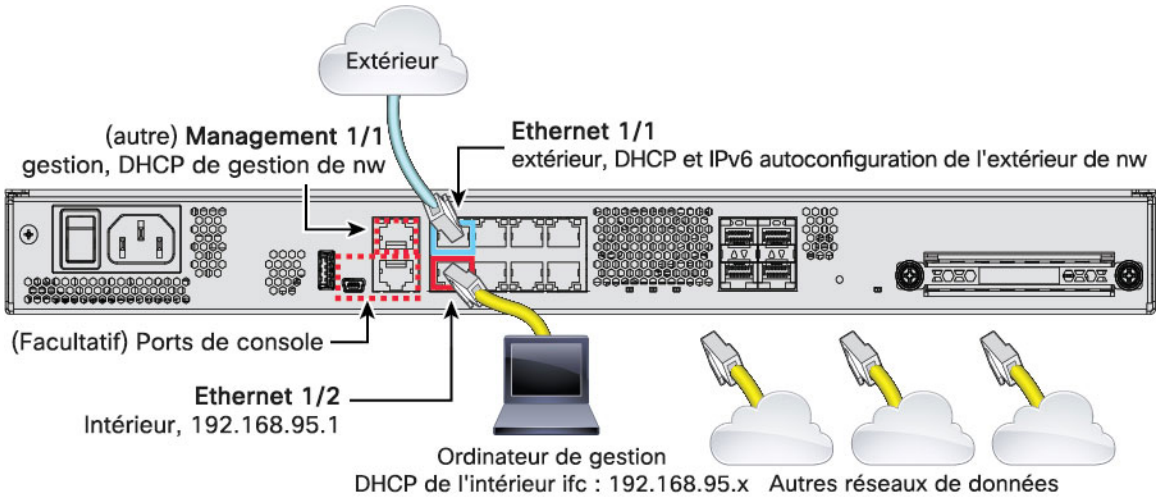
  Par défaut, l'adresse IP est obtenue à l'aide du protocole DHCP IPv4 et de la configuration automatique IPv6, mais vous pouvez définir une adresse statique lors de la configuration initiale.

- Connectez les appareils internes aux ports de commutation restants, Ethernet 1/2 à 1/8.

  Les ports Ethernet 1/7 et 1/8 sont des ports d'alimentation électrique par câble Ethernet (PoE+).

Câblage pour le Firepower 1100

Illustration 2 : Câblage pour le Firepower 1100



- Connectez votre ordinateur gestionnaire à l'une des interfaces suivantes :

  - Ethernet 1/2 : connectez votre ordinateur de gestion directement à Ethernet 1/2 pour la configuration initiale ou connectez Ethernet 1/2 à votre réseau interne. Ethernet 1/2 a une adresse IP par défaut (192.168.95.1) Cette interface exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris l'ordinateur de gestion). Assurez-vous donc que ces paramètres n'entrent pas en conflit avec les paramètres du réseau interne.

  - Management 1/1 (étiqueté MGMT)—Connectez votre ordinateur de gestion au réseau de gestion. L'interface de gestion Management 1/1 obtient une adresse IP de DHCP. Assurez-vous donc que votre réseau comprend un serveur DHCP.

Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut pour configurer une adresse IP statique, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 23.

Vous pourrez configurer ultérieurement l'accès de gestion à partir d'autres interfaces.

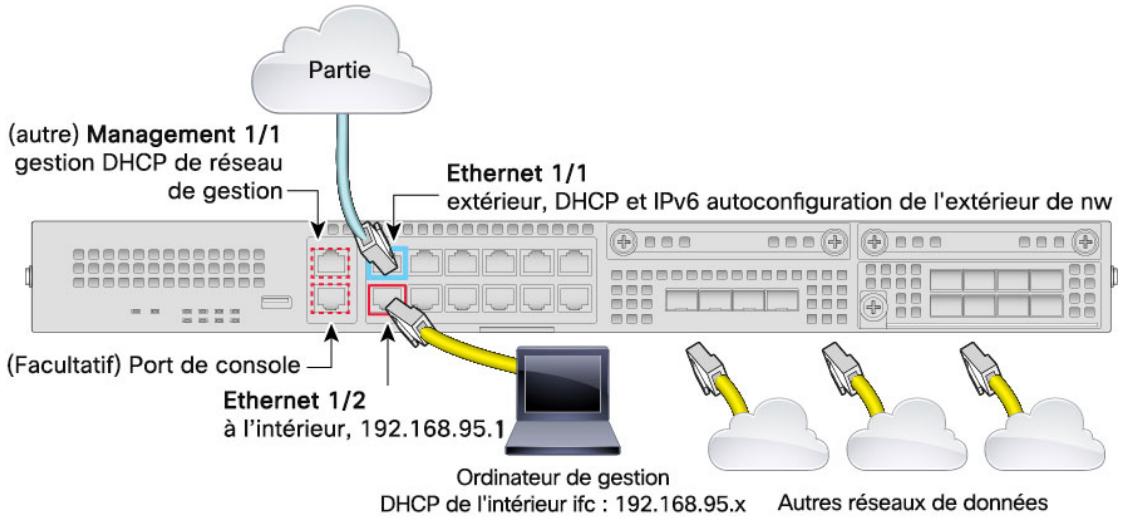
- Connectez le réseau externe à l'interface Ethernet 1/1 (WAN).

  Par défaut, l'adresse IP est obtenue à l'aide du protocole DHCP IPv4 et de la configuration automatique IPv6, mais vous pouvez définir une adresse statique lors de la configuration initiale.

- Connectez d'autres réseaux aux interfaces restantes.

Câblage du Firepower 2100

Illustration 3 : Câblage du Firepower 2100



- Connectez votre ordinateur gestionnaire à l'une des interfaces suivantes :
  - Ethernet 1/2 : connectez votre ordinateur de gestion directement à Ethernet 1/2 pour la configuration initiale ou connectez Ethernet 1/2 à votre réseau interne. Ethernet 1/2 a une adresse IP par défaut (192.168.95.1) et exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris l'ordinateur de gestion). Assurez-vous que ces paramètres n'entrent pas en conflit avec les paramètres du réseau interne existants.
  - Management 1/1 (étiqueté MGMT)—Connectez votre ordinateur de gestion au réseau de gestion. L'interface de gestion Management 1/1 obtient une adresse IP de DHCP. Assurez-vous donc que votre réseau comprend un serveur DHCP.

    Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut pour configurer une adresse IP statique, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 23.

Vous pourrez configurer ultérieurement l'accès de gestion à partir d'autres interfaces.

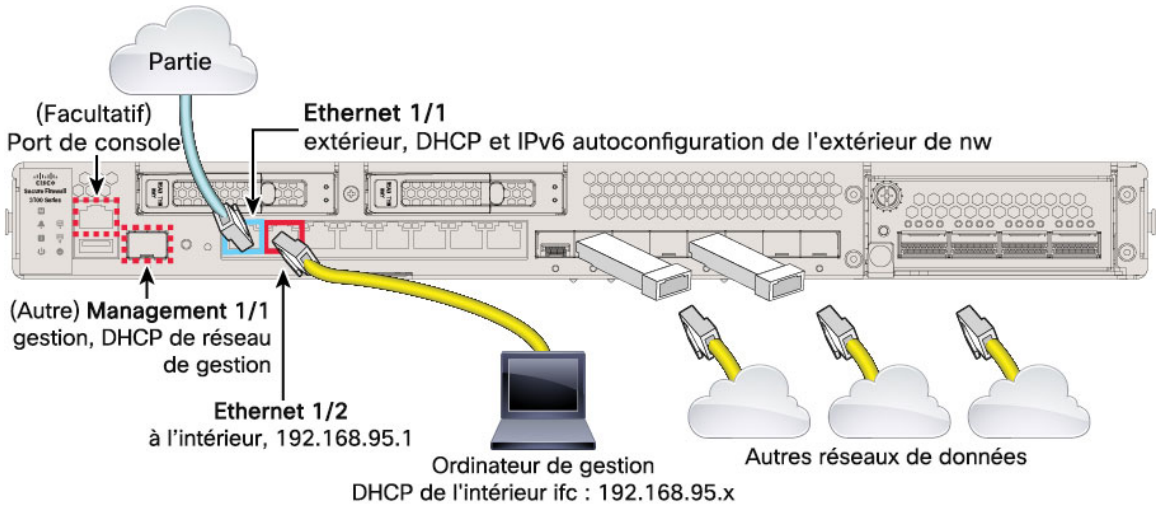
- Connectez le réseau externe à l’interface Ethernet 1/1 (WAN).

  Par défaut, l'adresse IP est obtenue à l'aide du protocole DHCP IPv4 et de la configuration automatique IPv6, mais vous pouvez définir une adresse statique lors de la configuration initiale.

- Connectez d'autres réseaux aux interfaces restantes.

Câblage du Cisco Secure Firewall 3100

Illustration 4 : Câblage du Cisco Secure Firewall 3100



Gérez le périphérique FTD sur Gestion 1/1 ou Ethernet 1/2. Selon la configuration par défaut, Ethernet 1/1 est également défini comme externe.

- Connectez votre ordinateur gestionnaire à l'une des interfaces suivantes :
  - Ethernet 1/2 : connectez votre ordinateur de gestion directement à Ethernet 1/2 pour la configuration initiale ou connectez Ethernet 1/2 à votre réseau interne. Ethernet 1/2 a une adresse IP par défaut (192.168.95.1) et exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris l’ordinateur de gestion), assurez-vous donc que ces paramètres n’entrent pas en conflit avec d’autres paramètres de réseau interne existants.
  - Gestion 1/1-Connectez la Gestion 1/1 à votre réseau de gestion, et assurez-vous que votre ordinateur de gestion est sur - ou a accès à - votre réseau de gestion. Gestion 1/1 obtient une adresse IP à partir d'un serveur DHCP sur votre réseau de gestion. Si vous utilisez cette interface, vous devez déterminer l'adresse IP attribuée au pare-feu afin de pouvoir vous connecter à l'adresse IP à partir de votre ordinateur de gestion.

    Si vous devez modifier l’adresse IP de l’interface de gestion Management 1/1 par défaut pour configurer une adresse IP statique, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l’interface de ligne de commande, à la page 23.

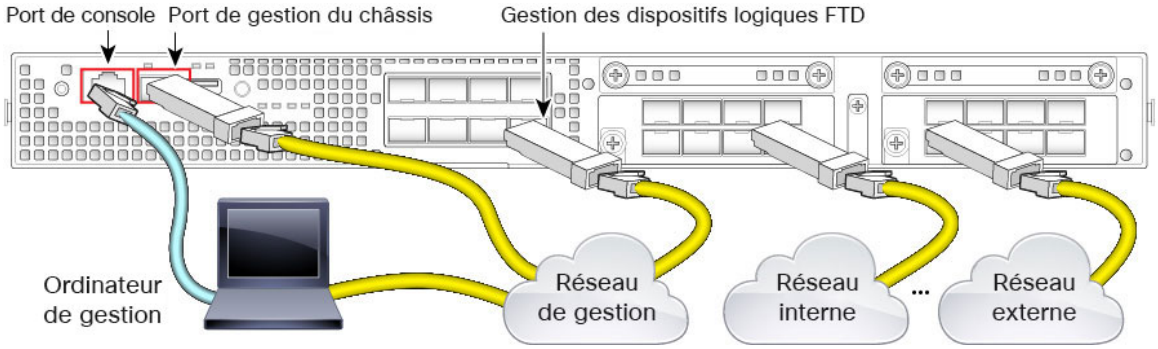
Remarque Management 1/1 est une interface à fibre optique de 10 Go qui nécessite un module SFP.

- Connectez le réseau extérieur à l'interface Ethernet1/1.

  Par défaut, l'adresse IP est obtenue à l'aide du protocole DHCP IPv4 et de la configuration automatique IPv6, mais vous pouvez définir une adresse statique lors de la configuration initiale.

- Connectez d'autres réseaux aux interfaces restantes.

Câblage du Firepower 4100



Effectuez la configuration initiale sur l'interface de gestion du dispositif logique Cisco Firepower Threat Defense. Vous pourrez activer ultérieurement la gestion à partir de n'importe quelle interface de données. Le dispositif Cisco Firepower Threat Defense nécessite un accès Internet pour les licences et les mises à jour, et le comportement par défaut consiste à acheminer le trafic de gestion vers l'adresse IP de la passerelle que vous avez spécifiée lors du déploiement du dispositif. Si vous souhaitez plutôt acheminer le trafic de gestion sur le plan dorsal vers les interfaces de données, vous pouvez configurer ce paramètre dans l'option FDM ultérieurement.

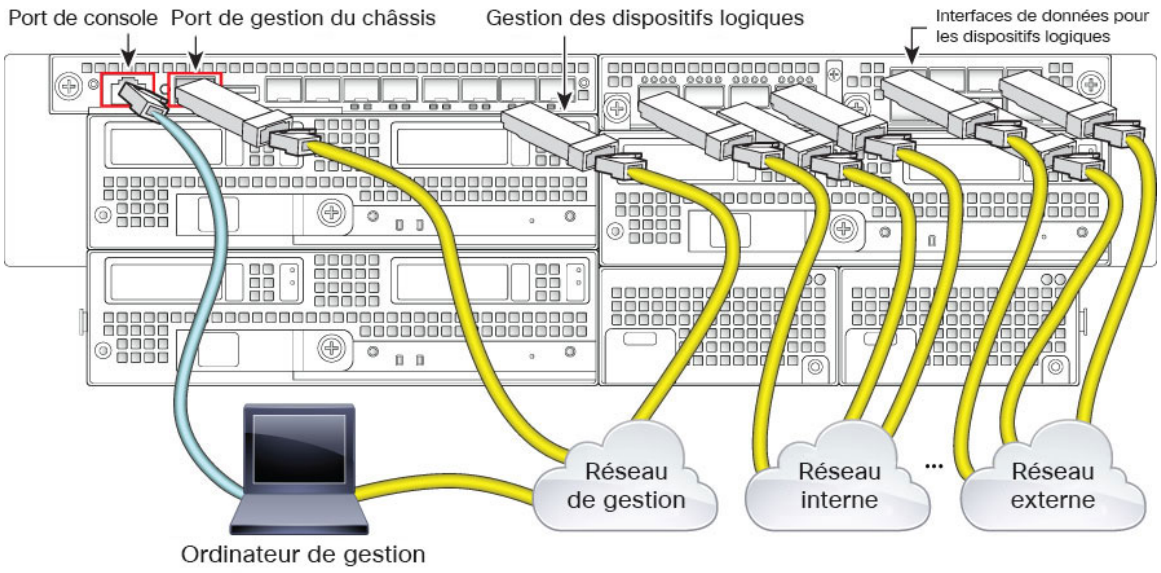
Câblez les interfaces suivantes pour la configuration initiale du châssis, la surveillance continue et l'utilisation de dispositifs logiques.

- Console port (Port de console : connectez votre ordinateur de gestion au port de console pour effectuer la configuration initiale du châssis. Le Firepower 4100 comprend un câble de console de série RS-232 à RJ-45. Vous devrez peut-être utiliser un câble série tiers vers USB pour établir la connexion.
- Chassis Management port (Port de gestion du châssis) : connectez le port de gestion du châssis à votre réseau de gestion pour la configuration et la gestion continue du châssis.
- FTD Logical device Management interface (Interface de gestion du dispositif logique) : vous pouvez choisir n'importe quelle interface du châssis à cette fin, à l'exception du port de gestion du châssis, réservé à la gestion FXOS.
- Data interfaces (Interfaces de données) : connectez les interfaces de données aux réseaux de données de votre dispositif logique. Vous pouvez configurer des interfaces physiques, des EtherChannels et des ports de dérivation (breakout) pour répartir les interfaces à haute capacité.

  Pour la haute disponibilité, utilisez une interface de données pour le lien de basculement/d'état.

Remarque Toutes les interfaces, à l'exception du port de console, nécessitent des émetteurs-récepteurs SFP, SFP+ et QSFP. Consultez le hardware installation guide (guide d'installation du matériel) pour connaître les émetteurs-récepteurs pris en charge.

Câblage du Firepower 9300



Effectuez la configuration initiale de Cisco Firepower Threat Defense sur l'interface de gestion du dispositif logique. Vous pourrez activer ultérieurement la gestion à partir de n'importe quelle interface de données. Le périphérique Cisco Firepower Threat Defense nécessite un accès Internet pour les licences et les mises à jour, et le comportement par défaut consiste à acheminer le trafic de gestion vers l'adresse IP de passerelle que vous avez spécifiée lors du déploiement du périphérique. Si vous souhaitez plutôt acheminer le trafic de gestion sur le fond de panier vers les interfaces de données, vous pouvez configurer ce paramètre dans l'option FDM ultérieurement.

Câblez les interfaces suivantes pour la configuration initiale du châssis, la surveillance continue et l'utilisation de dispositifs logiques.

- Console port (Port de console : connectez votre ordinateur de gestion au port de console pour effectuer la configuration initiale du châssis. Le Firepower 9300 comprend un câble de console de série RS-232 à RJ-45. Vous devrez peut-être utiliser un câble série tiers vers USB pour établir la connexion.
- Chassis Management port (Port de gestion du châssis) : connectez le port de gestion du châssis à votre réseau de gestion pour la configuration et la gestion continue du châssis.
- Logical device Management interface (Interface de gestion des dispositifs logiques) : utilisez une ou plusieurs interfaces pour gérer les dispositifs logiques. Vous pouvez choisir n'importe quelle interface sur le châssis à cette fin, sauf le port de gestion du châssis, qui est réservé à la gestion FXOS. Les interfaces de gestion peuvent être partagées entre les dispositifs logiques, ou vous pouvez utiliser une interface distincte par dispositif logique. En règle générale, vous partagez une interface de gestion avec tous les dispositifs logiques, ou si vous utilisez des interfaces distinctes, vous pouvez les placer sur un seul réseau de gestion. Mais vos exigences précises en matière de réseau peuvent varier.
- Data interfaces (Interfaces de données) : connectez les interfaces de données aux réseaux de données de votre dispositif logique. Vous pouvez configurer des interfaces physiques, des EtherChannels et des ports de séparation pour diviser les interfaces à haute capacité. Vous pouvez câbler plusieurs dispositifs logiques aux mêmes réseaux ou à des réseaux différents, selon les besoins de votre réseau. Tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre dispositif logique.

Pour la haute disponibilité, utilisez une interface de données pour le lien de basculement/état.

Remarque Toutes les interfaces, à l'exception du port de console, nécessitent des émetteurs-récepteurs SFP, SFP+ et QSFP. Consultez le hardware installation guide (guide d'installation du matériel) pour connaître les émetteurs-récepteurs pris en charge.

Câblage virtuel pour le FTDv

Pour installer FTDv, consultez le guide de démarrage rapide de votre plateforme virtuelle à l'adresse http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html. Le FDM est pris en charge sur les plateformes virtuelles suivantes : VMware, KVM, Microsoft Azure, Amazon Web Services (AWS).

La configuration par défaut FTDv place l'interface de gestion et l'interface interne sur le même sous-réseau. Vous devez avoir une connectivité Internet sur l'interface de gestion pour utiliser les licences Smart et obtenir des mises à jour des bases de données du système.

Ainsi, la configuration par défaut est conçue pour que vous puissiez connecter les interfaces Gestion 0-0 et le GigabitEthernet 0-1 (interne) au même réseau sur le commutateur virtuel. L'adresse de gestion par défaut utilise l'adresse IP interne comme passerelle. Ainsi, l'interface de gestion passe par l'interface interne, puis par l'interface externe, pour accéder à Internet.

Vous avez également la possibilité d'associer Gestion 0-0 à un sous-réseau différent de celui utilisé pour l'interface interne, tant que vous utilisez un réseau qui a accès à Internet. Assurez-vous que vous configurez l'adresse IP de l'interface de gestion et la passerelle de façon appropriée pour le réseau.

Notez que la configuration IP de l'interface de gestion est définie dans **Device (Périphérique)** > **System Settings (Paramètres du système)** > **Management Interface (Interface de gestion)**. Il ne s'agit pas de la même adresse IP que celle de l'interface Management0/0 (diagnostic) indiquée dans **Device (Périphérique** > **Interfaces** > **View Configuration (Afficher la configuration)**.

Comment les adaptateurs réseau et les interfaces VMware correspondent aux interfaces physiques FTD

Vous pouvez configurer jusqu'à 10 interfaces pour un périphérique VMware FTDv. Vous devez configurer au moins 4 interfaces.

Assurez-vous que le réseau source Management0-0 est associé à un réseau de VM qui peut accéder à Internet. Cela est nécessaire pour que le système puisse communiquer avec Cisco Smart Software Manager et télécharger les mises à jour de la base de données du système.

Vous affectez les réseaux lorsque vous installez l'OVF. Tant que vous configurez une interface, vous pouvez modifier ultérieurement le réseau virtuel par l'intermédiaire du client VMware. Toutefois, si vous devez ajouter une nouvelle interface, veillez à l'ajouter à la fin de la liste; si vous ajoutez ou supprimez une interface ailleurs, l'hyperviseur renumérotera vos interfaces, ce qui entraînera un mauvais alignement des ID d'interface dans votre configuration.

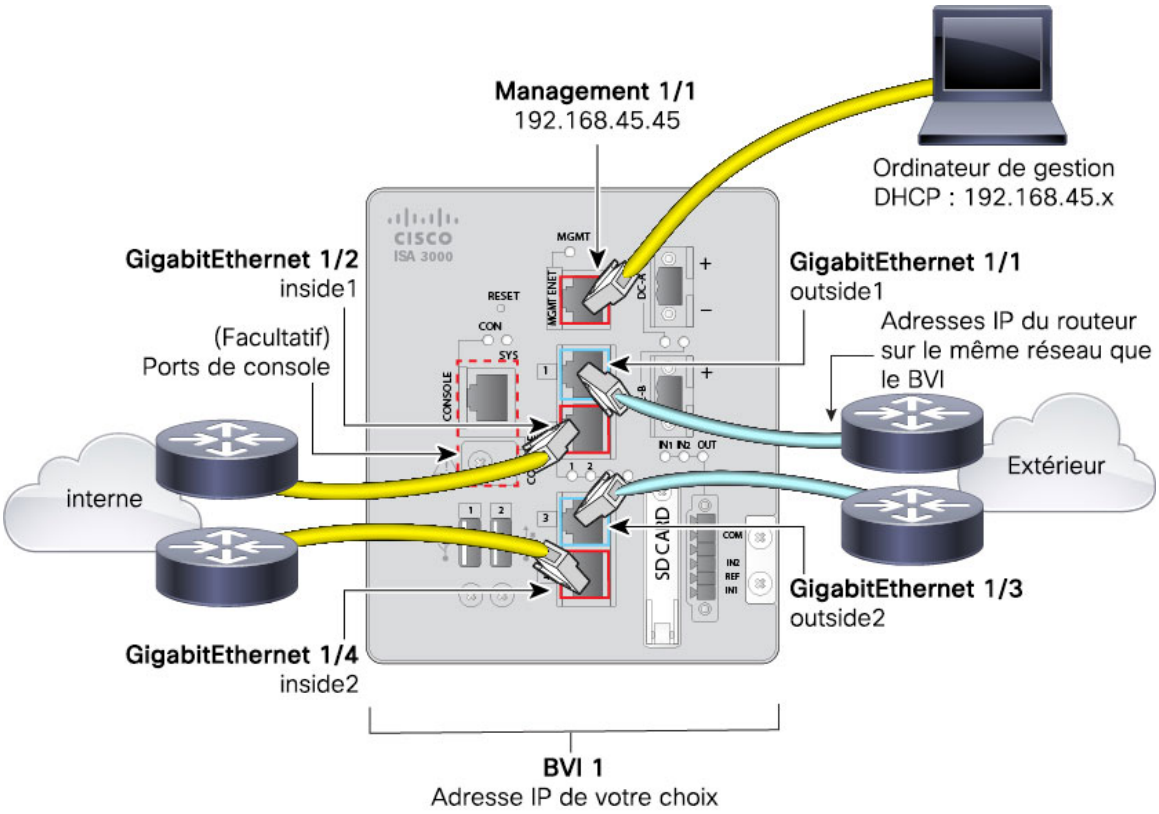
Le tableau suivant explique comment l'adaptateur réseau VMware et l'interface source correspondent aux noms d'interface physique FTDv. Pour les interfaces supplémentaires, la dénomination suit le même modèle en augmentant les numéros pertinents de une unité. Toutes les interfaces supplémentaires sont des interfaces de données. Pour plus d'informations sur l'affectation de réseaux virtuels aux machines virtuelles, consultez l'aide en ligne de VMware.

Tableau 2 : Mappage du réseau source au réseau de destination

Adaptateur réseau	Réseau source	Réseau de destination (nom de l'interface physique)	Fonction
Adaptateur réseau 1	Gestion 0-0	Management0/0	Gestion
Adaptateur réseau 2	Diagnostic 0-0	Diagnostic 0/0	Diagnostic
Adaptateur réseau 3	GigabitEthernet 0-0	GigabitEthernet 0/0	Données externes
Adaptateur réseau 4	GigabitEthernet 0-1	GigabitEthernet 0/1	Données internes
Adaptateur réseau 5	GigabitEthernet0-2	GigabitEthernet 0/2	Trafic de données
Adaptateur réseau 6	GigabitEthernet 0-3	GigabitEthernet 0/3	Trafic de données
Adaptateur réseau 7	GigabitEthernet 0-4	GigabitEthernet 0/4	Trafic de données
Adaptateur réseau 8	GigabitEthernet 0-5	GigabitEthernet 0/5	Trafic de données
Adaptateur réseau 9	GigabitEthernet 0-6	GigabitEthernet 0/6	Trafic de données
Adaptateur réseau 10	GigabitEthernet 0-7	GigabitEthernet 0/7	Trafic de données

Câblage pour ISA 3000

Illustration 5 : ISA 3000



- Connectez GigabitEthernet 1/1 à un routeur externe et GigabitEthernet 1/2 à un routeur interne.

  Ces interfaces forment une paire de contournement matériel.

- Connectez GigabitEthernet 1/3 à un routeur externe redondant, et GigabitEthernet 1/4 à un routeur interne redondant.

  Ces interfaces forment une paire de contournement matériel si votre modèle comporte des ports en cuivre ; la fibre optique ne prend pas en charge le contournement matériel. Ces interfaces fournissent un chemin réseau redondant en cas d'échec de l'autre paire. Ces 4 interfaces de données se trouvent sur le même réseau de votre choix. Vous devrez configurer l'adresse IP de la BVI 1 pour qu'elle se trouve sur le même réseau que les routeurs interne et externe.

- Connectez Management 1/1 à votre ordinateur de gestion (ou au réseau de gestion).

  Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 23.

(Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande

Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut, vous pouvez vous connecter au port de console et effectuer la configuration initiale au niveau de l'interface de ligne de commande, y compris la définition de l'adresse IP de gestion, de la passerelle et d'autres paramètres réseau de base. Vous ne pouvez configurer que les paramètres de l'interface de gestion; vous ne pouvez pas configurer d'interfaces internes ou externes, que vous pouvez configurer ultérieurement dans l'interface graphique.

Remarque Vous n'avez pas besoin d'utiliser cette procédure pour Firepower 4100/9300, car vous définissez l'adresse IP manuellement lors du déploiement.

Remarque Vous ne pouvez pas relancer le script de configuration de l'interface de ligne de commande à moins d'effacer la configuration; par exemple, en recréant l'image. Cependant, tous ces paramètres peuvent être modifiés ultérieurement au niveau de l'interface de ligne de commande à l'aide des commandes **configure network**. Consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Procédure

Étape 1 Connexion au port de la console FTD. Consultez Connexion avec l'interface de ligne de commande (CLI), à la page 11 pour de plus amples renseignements.

Étape 2 Connectez-vous avec le nom d'utilisateur **admin**.

Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut pour le FTDv est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (détails avancés)** > **User Data (données utilisateur)**) lors du déploiement initial.

Étape 3 La première fois que vous vous connectez à FTD , vous êtes invité à accepter le contrat de licence de l'utilisateur final (cLUF) et à changer le mot de passe de l'administrateur. Vous verrez ensuite le script de configuration de l'interface de ligne de commande.

Les valeurs par défaut ou les valeurs saisies précédemment apparaissent entre parenthèses. Pour accepter les valeurs saisies précédemment, appuyez sur la touche **Entrée**.

Consultez les consignes suivantes :

- **Enter the IPv4 default gateway for the management interface** (saisissez la passerelle IPv4 par défaut pour l'interface de gestion). Si vous définissez une adresse IP manuelle, saisissez les interfaces de données (**data-interfaces**) ou l'adresse IP du routeur de passerelle. Le paramètre **data-interfaces** envoie le trafic de gestion sortant sur le fond de panier pour quitter une interface de données. Ce paramètre est utile si vous ne disposez pas d'un réseau de gestion distinct pouvant accéder à Internet. Le trafic provenant de l'interface de gestion comprend l'enregistrement des licences et les mises à jour de base de données qui nécessitent un accès Internet. Si vous utilisez des **data-interfaces (interfaces de données)**, vous pouvez toujours utiliser le FDM (ou SSH) sur l'interface de gestion si vous êtes directement connecté au réseau de gestion, mais pour la gestion à distance de réseaux ou d'hôtes particuliers, vous devez ajouter une

route statique à l'aide de la commande **configure network static-routes**. Notez que la gestion de FDM sur les interfaces de données n'est pas touchée par ce paramètre. Si vous utilisez DHCP, le système utilise la passerelle fournie par DHCP et utilise les interfaces de données (**data-interfaces**) comme méthode de secours si DHCP ne fournit pas de passerelle.

- **If your networking information has changed, you will need to reconnect** (si vos informations réseau ont changé, vous devrez vous reconnecter) : Si vous êtes connecté avec SSH à l'adresse IP par défaut, mais que vous avez changé l'adresse IP au moment de la configuration initiale, vous serez déconnecté. Reconnectez-vous avec la nouvelle adresse IP et le nouveau mot de passe. Les connexions à la console ne sont pas touchées.
- **Gérer l'appareil localement?** : saisissez **oui** pour utiliser FDM. Une réponse **non** signifie que vous avez l'intention d'utiliser le système FMC pour gérer le dispositif.

Exemple :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Étape 4 Connectez-vous à FDM sur la nouvelle adresse IP de gestion.

Compléter la configuration initiale avec l'assistant d'installation

Lorsque vous vous connectez pour la première fois à FDM, vous êtes guidé au moyen de l'assistant d'installation de l'appareil pour compléter la configuration initiale du système.

Si vous envisagez d'utiliser l'appareil selon une configuration à haute disponibilité, veuillez lire Préparer les deux unités pour la haute disponibilité.

Remarque Firepower 4100/9300 et ISA 3000 ne prennent pas en charge l'assistant de configuration. Cette procédure ne s'applique donc pas à ces modèles. Pour Firepower 4100/9300, toute la configuration initiale est définie lorsque vous déployez le périphérique logique à partir du châssis. Pour l'ISA 3000, une configuration spéciale par défaut est appliquée avant l'expédition.

Avant de commencer

Assurez-vous de relier une interface de données avec votre périphérique de passerelle, par exemple un modem câble ou un routeur. Pour les déploiements en périphérie, il s'agit de votre passerelle Internet. Pour les déploiements de centres de données, il s'agirait d'un routeur principal. Utilisez l'interface « externe » par défaut pour votre modèle (voir Connecter les interfaces, à la page 14et Configuration par défaut avant la configuration initiale, à la page 28).

Ensuite, reliez votre ordinateur de gestion à l'interface « interne » de votre modèle de matériel. Sinon, vous pouvez vous connecter à l'interface de gestion. Pour le FTDv, assurez-vous simplement que vous avez une connexion à l'adresse IP de gestion.

(Sauf pour le FTDv, ce qui nécessite une connectivité à Internet à partir de l'adresse IP du gestionnaire.) Une connexion entre l'interface de gestion et le réseau n'est pas nécessaire. Par défaut, le système obtient les licences système, les mises à jour de base de données et les autres mises à jour par le biais des interfaces de données (généralement l'interface externe) qui se connectent à Internet. Si vous souhaitez plutôt utiliser un réseau de gestion distinct, vous pouvez relier l'interface de gestion à un réseau et configurer une passerelle de gestion distincte une fois la configuration initiale terminée.

Pour modifier les paramètres réseau de l'interface de gestion si vous ne pouvez pas accéder à l'adresse IP par défaut, consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 23.

Procédure

Étape 1 Connectez-vous à FDM.

a) En supposant que vous n'êtes pas passé par la configuration initiale dans l'interface de ligne de commande, ouvrez le FDM à **https://***l'adresse IP*, où l'adresse est l'une des suivantes.

- Pour une connexion avec l'interface interne : **https://192.168.95.1**.
- (rle FTDv) Si vous êtes connecté à l'interface de gestion :**https://192.168.45.45**.
- (Tous les autres modèles) Pour une connexion avec l'interface de gestion : **https://***dhcp_client_ip*.

b) Connectez-vous avec le nom d'utilisateur **admin**. Pour admin, le mot de passe par défaut est Admin123. Sur AWS, le mot de passe administrateur par défaut pour le FTDv est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details (détails avancés)** > **User Data (données utilisateur)**) lors du déploiement initial.

Étape 2 S'il s'agit de la première connexion au système et que vous n'avez pas utilisé l'assistant de configuration au niveau de l'interface de ligne de commande, vous devrez lire et accepter le contrat de licence d'utilisateur final et modifier le mot de passe de l'administrateur.

Vous devez suivre ces étapes pour continuer.

Étape 3 Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

Mise en garde
Vos paramètres sont déployés sur l'appareil lorsque vous cliquez sur **Next** (suivant). L'interface sera désignée comme « externe » et sera ajoutée à la zone de sécurité « outside_zone ». Vérifiez que vos paramètres sont corrects.

Interface externe

- **Configure IPv4** (configuration de l'adresse IPv4) : l'adresse IPv4 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv4. Ne configurez pas l'adresse IP sur le même sous-réseau que l'adresse interne par défaut (voir Configuration par défaut avant la configuration initiale, à la page 28), que ce soit de manière statique ou par le biais du protocole DHCP. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE une fois que l'installation de l'assistant est terminée. Consultez Configurer une interface physique.
- **Configure IPv6** (configuration de l'adresse IPv6) : l'adresse IPv6 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv6.

Interface de gestion

- **DNS Servers** (serveurs DNS) : le serveur DNS pour l'adresse de gestion du système. Entrez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. Par défaut, les serveurs DNS publics OpenDNS ou les serveurs DNS que vous obtenez du serveur DHCP sont sélectionnés. Si vous modifiez les champs et souhaitez revenir à la valeur par défaut, cliquez sur **Use OpenDNS** (utiliser OpenDNS) pour recharger les adresses IP appropriées dans les champs. Votre fournisseur de services Internet peut exiger que vous utilisiez des serveurs DNS spécifiques. Si, après avoir terminé l'installation avec l'assistant, vous trouvez que la résolution DNS ne fonctionne pas, consultez Dépannage du DNS pour l'interface de gestion.
- **Firewall Hostname** (nom d'hôte du pare-feu) : le nom d'hôte de l'adresse de gestion du système.

Étape 4 Configurez les paramètres d'heure du système et cliquez sur **Next** (suivant).

- **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
- **NTP Time Server** (serveur horaire NTP) : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou pour saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

Étape 5 Configurez les licences Smart pour le système.

Vous devez avoir un compte de licence Smart pour obtenir et appliquer les licences requises par le système. Au départ, vous pouvez utiliser la licence d'évaluation de 90 jours, puis configurer les licences Smart ultérieurement.

Pour enregistrer le périphérique dès maintenant, sélectionnez l'option pour enregistrer le périphérique, cliquez sur le lien pour vous connecter à votre compte Smart Software Manager, générez un nouveau jeton et copiez le jeton dans la zone d'édition. Vous devez également sélectionner votre région de services et décider d'envoyer

ou non les données d'utilisation au Réseau de succès Cisco (Cisco Success Network). Le texte à l'écran explique ces paramètres plus en détail.

Si vous ne souhaitez pas encore enregistrer l'appareil, sélectionnez l'option du mode d'évaluation (evaluation mode). La période d'évaluation dure jusqu'à 90 jours. Pour enregistrer ultérieurement l'appareil et obtenir des licences intelligentes, cliquez sur **Device (périphérique)**, puis cliquez sur le lien dans le groupe des licences Smart (**Smart Licenses**).

Étape 6 Cliquez sur **Finish** (Terminer).

Prochaine étape

- Si vous souhaitez utiliser les fonctionnalités couvertes par les licences facultatives, comme le filtrage d'URL par catégorie, l'inspection des intrusions ou la prévention des logiciels malveillants, activez les licences requises. Consultez Activation ou désactivation des licences facultatives.
- Connectez les autres interfaces de données à des réseaux distincts et configurez les interfaces. Pour en savoir plus sur la configuration des interfaces, consultez Comment ajouter un sous-réseau et Interfaces.
- Si vous gérez le périphérique via l'interface interne et que vous souhaitez ouvrir des sessions d'interface de ligne de commande via l'interface interne, ouvrez l'interface interne aux connexions SSH. Consultez Configuration de la liste d'accès de gestion.
- Parcourez les scénarios d'utilisation pour apprendre comment utiliser le produit. Consultez Meilleures pratiques : scénarios d'utilisation pour FTD.

Que faire si vous n'obtenez pas d'adresse IP pour l'interface externe

La configuration par défaut du périphérique comprend une adresse IPv4 statique pour l'interface interne. Vous ne pouvez pas modifier cette adresse au moyen de l'assistant de configuration initiale du périphérique, bien que vous puissiez la modifier par la suite.

L'adresse IP interne par défaut peut entrer en conflit avec d'autres réseaux connectés au périphérique. Cela est particulièrement vrai si vous utilisez DHCP sur l'interface externe pour obtenir une adresse de votre fournisseur de services Internet. Certains fournisseurs de services Internet utilisent le même sous-réseau que le réseau interne comme ensemble d'adresses. Comme vous ne pouvez pas avoir deux interfaces de données avec des adresses sur le même sous-réseau, les adresses en conflit du fournisseur de services Internet ne peuvent pas être configurées sur l'interface externe.

En cas de conflit entre l'adresse IP statique interne et l'adresse fournie par DHCP sur l'interface externe, le diagramme de connexion doit afficher l'interface externe comme étant administrativement opérationnelle, mais sans adresse IPv4.

L'assistant de configuration terminera avec succès dans ce cas, et toutes les politiques et paramètres de NAT, d'accès et d'autres politiques et paramètres par défaut seront configurés. Suivez simplement la procédure ci-dessous pour éliminer le conflit.

Avant de commencer

Vérifiez que vous avez une bonne connexion avec le fournisseur de services Internet. Bien qu'un conflit de sous-réseau vous empêche d'obtenir une adresse sur l'interface externe, vous ne parviendrez pas à en obtenir une si vous n'avez tout simplement pas de lien avec le fournisseur de services Internet.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien dans le résumé des **Interfaces**.

Étape 2 Passez la souris sur la colonne **Actions** pour l'interface interne et cliquez sur l'icône de modification ( ).

Étape 3 Dans l'onglet **IPv4 Address**, entrez une adresse statique sur un sous-réseau unique, par exemple 192.168.2.1/24 ou 192.168.46.1/24. Notez que l'adresse de gestion par défaut est 192.168.45.45/24. Par conséquent, n'utilisez pas ce sous-réseau.

Vous avez également la possibilité d'utiliser DHCP pour obtenir une adresse si vous avez déjà un serveur DHCP sur le réseau interne. Cependant, vous devez d'abord cliquer sur **Delete** (Supprimer) dans le groupe **DHCP SERVER IS DEFINED FOR THIS INTERFACE** (LE SERVEUR DHCP EST DÉFINI POUR CETTE INTERFACE) afin de supprimer le serveur DHCP de l'interface.

Étape 4 Dans la zone **DHCP SERVER IS DEFINED FOR THIS INTERFACE** (LE SERVEUR DHCP EST DÉFINI POUR CETTE INTERFACE), cliquez sur **Edit** (Modifier) et modifiez le regroupement DHCP en une plage sur le nouveau sous-réseau, par exemple, 192.168.2.5-192.168.2.254.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications apportées à l'interface.

Étape 6 Cliquez sur le bouton **Deploy** (déployer) dans le menu pour déployer vos modifications.

Étape 7 Cliquez sur **Deploy Now** (déployer maintenant).

Une fois le déploiement terminé, le graphique de connexion devrait afficher que l'interface externe dispose maintenant d'une adresse IP. Utilisez un client sur le réseau interne pour vérifier que vous avez une connectivité à Internet ou à un autre réseau en amont.

Configuration par défaut avant la configuration initiale

Avant que vous ne configuriez initialement Cisco Firepower Threat Defense l'appareil à l'aide du gestionnaire local (FDM), l'appareil comprend la configuration par défaut suivante.

Pour de nombreux modèles, cette configuration suppose que vous ouvrez le gestionnaire d'appareils au moyen de l'interface interne, généralement en branchant votre ordinateur directement sur l'interface, et que vous utilisez le serveur DHCP défini sur l'interface interne pour fournir une adresse IP à votre ordinateur. Sinon, vous pouvez relier votre ordinateur à l'interface de gestion et utiliser DHCP pour obtenir une adresse. Cependant, certains modèles ont des configurations et des exigences de gestion par défaut différentes. Reportez-vous au tableau ci-dessous pour en savoir plus.

Remarque Vous pouvez préconfigurer un grand nombre de ces paramètres à l'aide de la configuration de l'interface de ligne de commande ((Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 23) avant d'effectuer la configuration à l'aide de l'assistant.

Paramètres de configuration par défaut

Paramètres	Par défaut	Peut-on le modifier lors de la configuration initiale ?
Mot de passe de l'utilisateur admin.	Admin123 Firepower 4100/9300 : Définissez le mot de passe lorsque vous déployez le périphérique logique. AWS : La valeur par défaut est l'ID d'instance AWS, à moins que vous ne définissiez un mot de passe par défaut avec les données utilisateur (**Advanced Details** > **User Data**) lors du déploiement initial.	Oui. Vous devez changer le mot de passe par défaut.
Adresse IP de gestion.	Obtenue par DHCP. FTDv192.168.45.45 Firepower 4100/9300 : Définissez l'adresse IP de gestion lorsque vous déployez le périphérique logique.	Non. Pour Firepower 4100/9300 : Oui.
Passerelle de gestion.	Les interfaces de données sur l'appareil. Généralement, l'interface externe devient la voie vers Internet. Cette passerelle fonctionne uniquement pour le trafic depuis l'appareil. Si le périphérique reçoit une passerelle par défaut du serveur DHCP, cette passerelle est utilisée. Firepower 4100/9300 : Définissez l'adresse IP de passerelle lorsque vous déployez le périphérique logique. ISA 3000 : 192.168.45.1. FTDv : 192.168.45.1	Non. Pour Firepower 4100/9300 : Oui.
Serveurs DNS pour l'interface de gestion.	Les serveurs DNS publics OpenDNS, IPv4 : 208.67.220.220 et 208.67.222.222; IPv6 : 2620:119:35::35. Les serveurs DNS obtenus à partir du protocole DHCP ne sont jamais utilisés. Firepower 4100/9300 : Définissez les serveurs DNS lorsque vous déployez le périphérique logique.	Oui

Paramètres	Par défaut	Peut-on le modifier lors de la configuration initiale ?
Adresse IP de l'interface interne.	192.168.95.1/24 Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : l'adresse IP BVI1 n'est pas préconfigurée. BVI1 comprend toutes les interfaces internes et externes. FTDv : 192.168.45.1/24	Non.
Serveur DHCP pour les clients internes.	Fonctionne sur l'interface interne avec l'ensemble d'adresses 192.168.95.5 à 192.168.95.254. Firepower 4100/9300 : Aucun serveur DHCP activé. ISA 3000 : Aucun serveur DHCP activé. FTDv : L'ensemble d'adresses sur l'interface interne est 192.168.45.46 à 192.168.45.254.	Non.
Configuration automatique DHCP pour les clients internes. (La configuration automatique fournit aux clients des adresses pour les serveurs WINS et DNS.)	Activé sur l'interface externe.	Oui, mais indirectement. Si vous configurez une adresse IPv4 statique pour l'interface externe, la configuration automatique du serveur DHCP est désactivée.
Adresse IP de l'interface externe.	IPv4 : Obtenu par DHCP auprès d'un fournisseur de services Internet (ISP) ou d'un routeur en amont. IPv6 : Configuration automatique. Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : l'adresse IP BVI1 n'est pas préconfigurée. BVI1 comprend toutes les interfaces internes et externes.	Oui.

Interfaces par défaut par modèle de périphérique

Vous ne pouvez pas sélectionner différentes interfaces internes et externes lors de la configuration initiale. Pour modifier les affectations d'interface après la configuration, modifiez les paramètres d'interface et de DHCP. Vous devez supprimer une interface du groupe de ponts avant de pouvoir la configurer en tant qu'interface non commutée.

FTD périphérique	Interface externe	Interface interne
Firepower 1010	Ethernet 1/1	VLAN1, qui comprend tous les autres ports de commutation, à l'exception de l'interface externe, qui est une interface physique de pare-feu.
Firepower 1120, 1140, 1150	Ethernet 1/1	Ethernet 1/2
Série Firepower 2100	Ethernet 1/1	Ethernet 1/2
Cisco Secure Firewall 3100 series	Ethernet 1/1	Ethernet 1/2
Firepower 4100	Les interfaces de données ne sont pas préconfigurées.	Les interfaces de données ne sont pas préconfigurées.
Appareils Cisco Firepower de série 9300	Les interfaces de données ne sont pas préconfigurées.	Les interfaces de données ne sont pas préconfigurées.
FTDv	GigabitEthernet 0/0	GigabitEthernet 0/1
ISA 3000	GigabitEthernet 1/1 et GigabitEthernet 1/3 GigabitEthernet 1/1 (externe1) et 1/2 (interne1) et GigabitEthernet 1/3 (externe2) et 1/4 (interne2) (modèles sans fibre uniquement) sont configurés comme paires de contournement matériel. Toutes les interfaces internes et externes font partie de BVI1.	GigabitEthernet 1/2 et GigabitEthernet 1/4

Configuration après la configuration initiale

Après avoir terminé l'assistant de configuration, la configuration du périphérique inclura les paramètres suivants. Le tableau indique si un paramètre particulier est quelque chose que vous avez choisi explicitement ou s'il a été défini pour vous en fonction de vos autres sélections. Validez toutes les configurations « impliquées » et modifiez-les si elles ne répondent pas à vos besoins.

Remarque L'Firepower 4100/9300 et ISA 3000 ne prennent pas en charge l'assistant de configuration. Pour Firepower 4100/9300, toute la configuration initiale est définie lorsque vous déployez le périphérique logique à partir du châssis. Pour l'ISA 3000, une configuration spéciale par défaut est appliquée avant l'expédition.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Mot de passe de l'utilisateur admin.	Quoi que vous ayez saisi.	Explicite.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Adresse IP de gestion.	Obtenue par DHCP. FTDv: 192.168.45.45 Firepower 4100/9300: vous avez défini l'adresse IP de gestion lorsque vous avez déployé le dispositif logique.	Situations de défaillance.
Passerelle de gestion.	Les interfaces de données sur l'appareil. Généralement, l'interface externe devient la voie vers Internet. Cette passerelle fonctionne uniquement pour le trafic provenant du périphérique. Si le périphérique reçoit une passerelle par défaut du serveur DHCP, cette passerelle est utilisée. Firepower 4100/9300: l'adresse IP de passerelle que vous avez définie lorsque vous avez déployé le périphérique logique. ISA 3000: 192.168.45.1 FTDv : 192.168.45.1	Situations de défaillance.
Serveurs DNS pour l'interface de gestion.	Les serveurs DNS publics OpenDNS, IPv4 : 208.67.220.220, 208.67.222.222; IPv6 : 2620:119:35::35, ou tout ce que vous avez saisi. Les serveurs DNS obtenus à partir du protocole DHCP ne sont jamais utilisés. Firepower 4100/9300 : les serveurs DNS que vous avez définis lors du déploiement du périphérique logique.	Explicite.
Nom d'hôte de gestion.	**Firepower** ou tout ce que vous avez saisi. Firepower 4100/9300 : le nom d'hôte que vous avez défini lors du déploiement du périphérique logique.	Explicite.
Accès à la gestion par le biais des interfaces de données.	Une règle de liste d'accès de gestion de l'interface de données permet l'accès HTTPS par le biais de l'interface interne. Les connexions SSH ne sont pas autorisées. Les connexions IPv4 et IPv6 sont autorisées. Firepower 4100/9300 : aucune interface de données n'a de règles d'accès de gestion par défaut. ISA 3000 : aucune interface de données n'a de règles d'accès de gestion par défaut. FTDv : aucune interface de données n'a de règles d'accès de gestion par défaut.	Impliqué.
Heure système.	Le fuseau horaire et les serveurs NTP que vous avez sélectionnés. Firepower 4100/9300 : l'heure système est transmise par le châssis. ISA 3000 : serveurs NTP de Cisco : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org.	Explicite.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Licence Smart.	Soit enregistré avec une licence de base, soit période d'évaluation activée, selon votre sélection. Les licences d'abonnement ne sont pas activées. Accédez à la page des licences Smart pour les activer.	Explicite.
Adresse IP de l'interface interne.	192.168.95.1/24 Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : aucune. Vous devez définir l'adresse IP BVI1 manuellement. FTDv : 192.168.45.1/24	Situations de défaillance.
Serveur DHCP pour les clients internes.	Fonctionne sur l'interface interne avec l'ensemble d'adresses 192.168.95.5 à 192.168.95.254. Firepower 4100/9300 : Aucun serveur DHCP activé. ISA 3000 : Aucun serveur DHCP activé. FTDv : L'ensemble d'adresses sur l'interface interne est 192.168.45.46 à 192.168.45.254.	Situations de défaillance.
Configuration automatique DHCP pour les clients internes. (La configuration automatique fournit aux clients des adresses pour les serveurs WINS et DNS.)	Activé sur l'interface externe si vous utilisez DHCP pour obtenir l'adresse IPv4 de l'interface externe. Si vous utilisez l'adressage statique, la configuration automatique DHCP est désactivée.	Explicit, mais indirect.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Configuration de l'interface de données.	• Firepower 1010 : l'interface externe, Ethernet 1/1, est une interface de pare-feu physique. Toutes les autres interfaces sont des ports de commutation qui sont activés et font partie de VLAN1, l'interface interne. Vous pouvez brancher des points terminaux ou des commutateurs dans ces ports et obtenir des adresses du serveur DHCP pour l'interface interne. • Firepower 4100/9300: Toutes les interfaces de données sont désactivées. • ISA 3000 : toutes les interfaces de données sont activées et font partie du même groupe de ponts, BVI1. GigabitEthernet1/1 et 1/3 sont des interfaces externes, et GigabitEthernet1/2 et 1/4 sont des interfaces internes. GigabitEthernet 1/1 (externe1) et 1/2 (interne1) et GigabitEthernet 1/3 (externe2) et 1/4 (interne2) (modèles sans fibre uniquement) sont configurés comme paires de contournement matériel. • Tous les autres modèles : les interfaces externe et interne sont les seules configurées et activées. Toutes les autres interfaces de données sont désactivées.	Situations de défaillance.
Adresse IP de l'interface externe.	Il s'agit du port externe par défaut en fonction du modèle de périphérique. Consultez Configuration par défaut avant la configuration initiale, à la page 28. L'adresse IP est obtenue par autoconfiguration DHCP et IPv6, ou il s'agit d'une adresse statique telle qu'elle est saisie (IPv4, IPv6 ou les deux). Firepower 4100/9300 : Les interfaces de données ne sont pas préconfigurées. ISA 3000 : aucune. Vous devez définir l'adresse IP BVI1 manuellement.	L'interface est par défaut. L'adressage est explicite.
Routes statiques.	Si vous configurez une adresse IPv4 ou IPv6 statique pour l'interface externe, une route par défaut statique est configurée pour IPv4/IPv6, le cas échéant, pointant vers la passerelle que vous avez définie pour ce type d'adresse. Si vous sélectionnez DHCP, la voie de routage par défaut est obtenue à partir du serveur DHCP. Des objets réseau sont également créés pour la passerelle et l'adresse « any » (toute), c'est-à-dire 0.0.0.0/0 pour IPv4, ::/0 pour IPv6.	Impliqué.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
Zones de sécurité.	**inside_zone**, comprenant les interfaces internes. Pour le Firepower 4100/9300, vous devez ajouter des interfaces manuellement à ce périmètre de sécurité. **outside_zone**, contenant les interfaces externes. Pour le Firepower 4100/9300, vous devez ajouter des interfaces manuellement à cette zone. (Vous pouvez modifier ces zones pour ajouter d'autres interfaces ou créer vos propres zones.)	Impliqué.
Politique de contrôle d'accès.	Une règle faisant confiance à tout le trafic de la inside_zone vers la outside_zone. Cela permet sans inspection à tout le trafic des utilisateurs de votre réseau de sortir et à tout le trafic de retour pour ces connexions. L'action par défaut pour tout autre trafic est de le bloquer. Cela empêche tout trafic initié de l'extérieur d'entrer dans votre réseau. Firepower 4100/9300 : il n'y a pas de règles d'accès préconfigurées. ISA 3000 : une règle faisant confiance à tout le trafic de la inside_zone à la outside_zone, et une règle faisant confiance à tout le trafic de la outside_zone à la inside_zone. Trafic non bloqué. Le périphérique dispose également de règles faisant confiance à tout le trafic entre les interfaces de la inside_zone et de la outside_zone. Cela permet, sans inspection, tout le trafic entre les utilisateurs de inside (interne) et entre les utilisateurs de outside (externe).	Impliqué.
NAT	Une règle de PAT dynamique d'interface traduit l'adresse source de tout trafic IPv4 destiné à l'interface externe en un port unique sur l'adresse IP de l'interface externe. Il existe d'autres règles PAT masquées pour activer l'accès HTTPS par le biais des interfaces internes et le routage par les interfaces de données pour l'adresse de gestion. Celles-ci ne s'affichent pas dans le tableau NAT, mais vous les verrez si vous utilisez la commande **show nat** dans l'interface de ligne de commande. Firepower 4100/9300 : la NAT n'est pas préconfigurée. ISA 3000 : la NAT n'est pas préconfigurée.	Impliqué.

Bases de la configuration

Les rubriques suivantes expliquent les méthodes de base pour la configuration du périphérique.

Configurer le périphérique

Lorsque vous vous connectez pour la première fois à FDM, vous êtes guidé dans un assistant de configuration pour vous aider à configurer les paramètres de base. Une fois que vous avez terminé l'assistant, utilisez la méthode suivante pour configurer les autres fonctionnalités et gérer la configuration du périphérique.

Si vous avez du mal à dissocier visuellement les éléments, sélectionnez un schéma de couleur différent dans le profil d'utilisateur. Sélectionnez **Profile** (Profil) dans le menu déroulant de l'icône utilisateur dans le coin supérieur droit de la page.

Procédure

Étape 1 Cliquez sur **Device (périphérique)** pour accéder au **Device Summary (Résumé du périphérique)**.

Le tableau de bord affiche un état visuel du périphérique, y compris les interfaces activées et si les paramètres de clé sont configurés (en vert) ou doivent toujours être configurés. Pour en savoir plus, consultez Affichage de l'interface et de l'état de gestion, à la page 42.

Au-dessus de l'image d'état se trouve un résumé du modèle de périphérique, de la version du logiciel, de la version VDB (système et base de données relative aux vulnérabilités) et des dernières règles de prévention des intrusions mises à jour. Cette zone affiche aussi l'état de la haute disponibilité, y compris des liens pour configurer la fonctionnalité ; voir Haute disponibilité (basculement). Elle affiche également l'état d'enregistrement dans le nuage, où vous voyez le compte auquel le périphérique est inscrit si vous utilisez la gestion en nuage ; voir Configuration de Cisco Cloud Services.

Sous l'image se trouvent des groupes pour les différentes fonctionnalités que vous pouvez configurer, avec des résumés des configurations dans chaque groupe et des actions que vous pouvez effectuer pour gérer la configuration du système.

Étape 2 Cliquez sur les liens dans chaque groupe pour configurer les paramètres ou effectuer les actions.

Voici un résumé des groupes :

- **Interface** : vous devez avoir au moins deux interfaces de données configurées en plus de l'interface de gestion. Consultez Interfaces.
- **Routing (Routage)** : la configuration du routage. Vous devez définir une route par défaut. D'autres routes peuvent être nécessaires selon votre configuration. Consultez Routage.
- **Updates** (Mises à jour) : mises à jour de géolocalisation, des règles de prévention des intrusions et de la base de données des vulnérabilités, ainsi que mises à niveau du logiciel système. Configurez un calendrier de mises à jour régulières afin de vous assurer de disposer des dernières mises à jour de base de données si vous utilisez ces fonctionnalités. Vous pouvez également accéder à cette page si vous devez télécharger une mise à jour avant l'exécution de la mise à jour planifiée. Consultez Mise à jour des bases de données système et des flux.
- **System Settings** (Paramètres système) : ce groupe comprend divers paramètres. Certains sont des paramètres de base que vous configurez lors de la configuration initiale du périphérique, puis que vous modifiez rarement. Consultez Paramètres système.

- **Smart License** (Licence Smart) : affiche l'état actuel des licences du système. Vous devez installer les licences appropriées pour utiliser le système. Certaines fonctionnalités nécessitent des licences particulières. Consultez Octroi de licence du système.
- **Backup and Restore** (Sauvegarde et restauration) : sauvegardez la configuration du système ou restaurez une sauvegarde précédente. Consultez Sauvegarde et restauration du système.
- **Troubleshoot** (Dépannage) : générez un fichier de dépannage à la demande du centre d'assistance technique de Cisco. Consultez Création d'un fichier de dépannage.
- **Site-to-Site VPN** (VPN de site à site) : connexions de réseau privé virtuel (VPN) de site à site entre ce périphérique et des périphériques distants. Consultez Gestion des VPN de site à site.
- **Remote Access VPN** (VPN d'accès à distance) : configuration de réseau privé virtuel (VPN) d'accès à distance qui permet à des clients externes de se connecter à votre réseau interne. Consultez Configuration du VPN d'accès à distance.
- **Advanced Configuration** (Configuration avancée) : utilisez FlexConfig et Smart CLI pour configurer des fonctionnalités que vous ne pouvez pas configurer autrement à l'aide de FDM. Consultez Configuration avancée.
- **Device Administration** (Administration du périphérique) : affichez le journal d'audit ou exportez une copie de la configuration. Consultez Audit et gestion du changement.

Étape 3 Cliquez sur le bouton **Deploy** (déployer) dans le menu pour déployer vos modifications.

Les modifications ne sont actives sur le périphérique que lorsque vous les déployez. Consultez Déploiement des modifications, à la page 39.

Prochaine étape

Cliquez sur **Policies** (Politiques) dans le menu principal et configurez la politique de sécurité pour le système. Vous pouvez également cliquer sur **Objects** (Objets) pour configurer les objets nécessaires dans ces politiques.

Configuration des politiques de sécurité

Utilisez les politiques de sécurité pour mettre en œuvre la politique d'utilisation acceptable de votre entreprise et pour protéger votre réseau contre les intrusions et les autres menaces.

Procédure

Étape 1 Cliquez sur **Policies** (Politiques).

La page Security Policies (Politiques de sécurité) affiche le flux général d'une connexion dans le système et l'ordre dans lequel les politiques de sécurité sont appliquées.

Étape 2 Cliquez sur le nom d'une politique et configurez-la.

Vous n'aurez peut-être pas besoin de configurer chaque type de politique, bien que vous deviez toujours avoir une politique de contrôle d'accès. Voici un résumé des politiques :

- **Déchiffrement SSL** : Si vous souhaitez inspecter les connexions chiffrées (comme HTTPS) pour détecter les intrusions, les logiciels malveillants, etc., vous devez déchiffrer les connexions. Utilisez la politique de déchiffrement SSL pour déterminer les connexions qui doivent être déchiffrées. Le système rechiffre la connexion après l'avoir inspectée. Consultez Configuration des politiques de déchiffrement SSL.
- **Identité** : Si vous souhaitez corréler l'activité du réseau à des utilisateurs individuels ou contrôler l'accès au réseau en fonction de l'utilisateur ou de l'appartenance à un groupe d'utilisateurs, utilisez la politique d'identité pour déterminer l'utilisateur associé à une adresse IP source donnée. Consultez Configuration des politiques d'identité.
- **Security Intelligence** (Renseignements sur la sécurité) : utilisez la politique sur les renseignements sur la sécurité pour supprimer rapidement les connexions en provenance des adresses IP ou des URL de la liste de blocage ou vers celles-ci. En inscrivant sur la liste de blocage les mauvais sites connus, vous n'avez pas besoin de les prendre en compte dans votre politique de contrôle d'accès. Cisco fournit des flux régulièrement mis à jour d'adresses et d'adresses URL incorrectes afin que la liste de blocage issue des renseignements sur la sécurité se mette à jour de façon dynamique. En utilisant les flux, vous n'avez pas besoin de modifier la politique pour ajouter ou supprimer des éléments dans la liste de blocage. Consultez Configurer les renseignements sur la sécurité.
- **NAT** (Network Address Translation, traduction d'adresses réseau) : utilisez la politique NAT pour convertir les adresses IP internes en adresses de routage externe. Consultez Configurer la traduction d'adresses réseau (NAT).
- **Contrôle d'accès** : Utilisez la politique de contrôle d'accès pour déterminer les connexions autorisées sur le réseau. Vous pouvez procéder au filtrage selon la zone de sécurité, l'adresse IP, le protocole, le port, l'application, l'adresse URL, l'utilisateur ou le groupe d'utilisateurs. Vous pouvez aussi appliquer également des politiques en lien avec la prévention des intrusions et avec la présence de fichiers (logiciels malveillants) en utilisant des règles de contrôle d'accès. Utilisez cette politique pour mettre en œuvre le filtrage d'URL. Consultez Configuration de la politique de contrôle d'accès.
- **Intrusion** : Utilisez les politiques de prévention des intrusions pour rechercher les menaces connues. Bien que vous appliquiez des politiques de prévention des intrusions à l'aide de règles de contrôle d'accès, vous pouvez modifier lesdites politiques pour activer ou désactiver sélectivement des règles de prévention précises en lien avec les intrusions. Consultez Stratégies de prévention des intrusions.

Étape 3 Cliquez sur le bouton **Deploy** (déployer) dans le menu pour déployer vos modifications.

Les modifications ne sont actives sur le périphérique que lorsque vous les déployez. Consultez Déploiement des modifications, à la page 39.

Recherche de règles ou d'objets

Vous pouvez utiliser la recherche en texte intégral sur des listes de règles de politique ou d'objets pour vous aider à trouver l'élément que vous souhaitez modifier. Cela est particulièrement utile lorsqu'il s'agit de politiques qui ont des centaines de règles ou de longues listes d'objets.

La méthode d'utilisation de la recherche sur les règles et les objets est la même pour tout type de politique (à l'exception de la politique de prévention des intrusions) ou d'objet : dans le champ **Search (Rechercher)**, saisissez une chaîne à trouver, puis appuyez sur Enter (Entrée).

Cette chaîne peut exister dans n'importe quelle partie de la règle ou de l'objet, et elle peut être partielle. Vous pouvez utiliser l'astérisque * comme caractère générique pour correspondre à zéro ou à plusieurs caractères. N'incluez pas les caractères suivants, ils ne sont pas pris en charge dans la chaîne de recherche : ?~!{}<>:%. Les caractères suivants sont ignorés : ;#&.

La chaîne peut apparaître dans un objet du groupe. Par exemple, vous pouvez saisir une adresse IP et rechercher les objets ou les groupes réseau qui précisent cette adresse.

Lorsque vous avez terminé, cliquez sur le **x** à droite de la zone de recherche pour effacer le filtre.

Déploiement des modifications

Lorsque vous mettez à jour une politique ou un paramètre, la modification n'est pas immédiatement appliquée au périphérique. Il existe un processus en deux étapes :

1. Apportez vos modifications.
2. Déployez vos modifications.

Ce processus vous permet d'apporter un groupe de modifications connexes sans vous obliger à exécuter un périphérique d'une manière « partiellement configurée ». Dans la plupart des cas, le déploiement inclut uniquement vos modifications. Toutefois, si nécessaire, le système réappliquera l'ensemble de la configuration, ce qui pourrait perturber votre réseau. En outre, certaines modifications nécessitent le redémarrage des moteurs d'inspection, avec une diminution du trafic lors du redémarrage. Ainsi, envisagez de déployer des modifications lorsque les perturbations potentielles auront le moins d'impact.

Remarque Si la tâche de déploiement échoue, le système doit restaurer toutes les modifications partielles de la configuration précédente. La restauration comprend l'effacement de la configuration du plan de données et le redéploiement de la version précédente. Cela perturbera le trafic jusqu'à la fin de la restauration.

Après avoir terminé les modifications que vous souhaitez apporter, utilisez la procédure suivante pour les déployer sur le périphérique.

Mise en garde Le périphérique FTD abandonne le trafic lorsque les moteurs d'inspection sont occupés en raison d'un problème de ressources logicielles ou en panne en raison d'une configuration nécessitant le redémarrage des moteurs pendant le déploiement de la configuration. Pour des informations détaillées sur les modifications nécessitant un redémarrage, consultez Changements de configuration qui redémarrent les moteurs d'inspection., à la page 41.

Procédure

Étape 1 Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

L'icône est mise en évidence avec un point lorsqu'il y a des modifications non déployées.

La fenêtre Pending Changes (modifications en attente) affiche une comparaison de la version déployée de la configuration avec les modifications en attente. Ces modifications sont codées par couleur pour indiquer les éléments supprimés, ajoutés ou modifiés. Consultez la légende dans la fenêtre pour obtenir une explication des couleurs.

Si le déploiement nécessite le redémarrage des moteurs d'inspection, la page comprend un message qui fournit des détails sur les modifications qui nécessitent un redémarrage. Si la perte de trafic momentanée à ce moment est inacceptable, fermez la boîte de dialogue et attendez un meilleur moment pour déployer les modifications.

Si l'icône n'est pas en surbrillance, vous pouvez toujours cliquer dessus pour voir la date et l'heure de la dernière tâche de déploiement réussie. Il existe également un lien pour vous afficher l'historique de déploiement, qui vous mène vers la page d'audit filtrée pour afficher uniquement les tâches de déploiement.

Étape 2 Si vous êtes satisfait des modifications, vous pouvez cliquer sur **Deploy Now** (déployer maintenant) pour lancer le travail immédiatement.

La fenêtre montrera que le déploiement est en cours. Vous pouvez fermer la fenêtre ou attendre la fin du déploiement. Si vous fermez la fenêtre alors que le déploiement est en cours, le travail ne s'arrête pas. Vous pouvez voir les résultats dans la liste des tâches ou dans le journal d'audit. Si vous laissez la fenêtre ouverte, cliquez sur le lien **Deployment History** (historique de déploiement) pour afficher les résultats.

Vous pouvez également effectuer les opérations suivantes :

- **Name the Job** (Nommer la tâche) : pour nommer la tâche de déploiement, cliquez sur la flèche déroulante sur le bouton **Deploy Now** (Déployer maintenant) et sélectionnez **Name the Deployment Job** (Nommer la tâche de déploiement). Saisissez un nom, puis cliquez sur **Deploy** (Déployer). Le nom s'affichera dans Audit et dans Deployment History (Historique des déploiements) en tant qu'élément de la tâche, ce qui pourrait vous aider à la retrouver plus facilement.

  Par exemple, si vous nommez une tâche « Configuration de l'interface DMZ », un déploiement réussi sera nommé « Déploiement terminé : Configuration de l'interface DMZ ». De plus, le nom est utilisé comme Event Name (Nom de l'événement) dans les événements Task Started (Tâche démarrée) et Task Completed (Tâche terminée) associés à la tâche de déploiement.

- **Discard Changes** (Supprimer les modifications) : pour supprimer toutes les modifications en attente, cliquez sur **More Options (Plus d'options)** > **Discard All (Supprimer tout)**. Vous êtes invité à confirmer.

- **Copy Changes** (Copier les modifications) : pour copier la liste des modifications dans le presse-papier, cliquez sur **More Options (Plus d'options)** > **Copy to Clipboard (Copier dans le presse-papiers)**. Cette option fonctionne uniquement s'il y a moins de 500 modifications.

- **Download Changes** (Télécharger les modifications) : pour télécharger la liste des modifications sous forme de fichier, cliquez sur **More Options (Plus d'options)** > **Download as Text (Télécharger en tant que texte)**. Vous êtes invité à enregistrer le fichier sur votre poste de travail. Il utilise le format YAML. Vous pouvez l'afficher dans un éditeur de texte si vous n'avez pas d'éditeur prenant spécifiquement en charge le format YAML.

Changements de configuration qui redémarrent les moteurs d'inspection.

N'importe laquelle des configurations ou actions suivantes redémarre les moteurs d'inspection lorsque vous déployez des modifications de configuration.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations nécessite le redémarrage des moteurs d'inspection, ce qui interrompt l'inspection du trafic et entraîne une perte de trafic.

Déploiement

Certaines modifications requièrent le redémarrage des plateformes d'inspection, ce qui entraînera une perte de trafic momentanée. Voici les modifications qui requièrent le redémarrage de la plateforme d'inspection :

- La politique de déchiffrement SSL est activée ou désactivée.
- La MTU a été modifiée sur au moins une interface physique (mais pas les sous-interfaces).
- Vous ajoutez ou supprimez une politique de fichiers dans une règle de contrôle d'accès.
- La VDB a été mise à jour.
- Création ou interruption de la configuration à haute disponibilité.

En outre, certains paquets peuvent être abandonnés lors du déploiement si le processus Snort est occupé, avec une utilisation totale de l'UC dépassant 60 %. Vous pouvez vérifier l'utilisation actuelle de l'UC pour Snort à l'aide de la commande **show asp inspect-dp snort**.

Mises à jour des bases de données du système

Si vous téléchargez une mise à jour de la base de données des règles ou de la VDB, vous devez déployer la mise à jour pour qu'elle devienne active. Ce déploiement peut redémarrer les moteurs d'inspection. Lorsque vous téléchargez manuellement une mise à jour ou planifiez une mise à jour, vous pouvez indiquer si le système doit déployer automatiquement les modifications une fois le téléchargement terminé. Si le système ne déploie pas automatiquement la mise à jour, la mise à jour est appliquée lors du prochain déploiement de modifications, auquel cas les moteurs d'inspection pourraient redémarrer.

Mises à jour du système

L'installation d'une mise à jour ou d'un correctif du système qui ne redémarre pas le système et comprend une modification binaire nécessite le redémarrage des moteurs d'inspection. Les modifications binaires peuvent inclure des modifications des moteurs d'inspection, d'un préprocesseur, de la base de données relative aux vulnérabilités (VDB) ou d'une règle d'objet partagé. Notez également qu'un correctif qui n'inclut pas de modification binaire peut parfois nécessiter un redémarrage Snort.

Modifications de configuration qui forcent un déploiement complet

Dans la plupart des cas, le déploiement inclut uniquement vos modifications. Toutefois, si nécessaire, le système réappliquera l'ensemble de la configuration, ce qui pourrait perturber votre réseau. Voici quelques modifications qui forcent un déploiement complet.

- Les politiques de renseignements de sécurité ou d'identité sont initialement activées.

- Les politiques de renseignements de sécurité et d'identité sont désactivées.
- Création d'un EtherChannel lorsque vous réutilisez des données.
- Suppression d'un EtherChannel.
- Modification des associations d'interfaces membres d'un EtherChannel.
- Suppression de toute interface utilisée dans la configuration. Par exemple, suppression d'une sous-interface qui fait partie d'un périmètre de sécurité utilisé par une règle de contrôle d'accès.
- Modification d'un objet FlexConfig qui fait partie de la politique FlexConfig ou suppression d'un objet de la politique, lorsque cet objet ne comprend pas de lignes de négation. L'omission des lignes de négation force le système à un déploiement complet, car il n'y a aucun moyen spécifique de supprimer la configuration produite par l'objet FlexConfig. Vous pouvez éviter ce problème en insérant toujours les lignes de négation appropriées dans chaque objet FlexConfig.

Affichage de l'interface et de l'état de gestion

Le résumé du périphérique comprend une vue graphique de votre périphérique et la sélection des paramètres pour l'adresse de gestion. Pour ouvrir le Device Summary (Résumé du périphérique, cliquez sur **Device** (Périphérique).

Les éléments de ce graphique changent de couleur en fonction de l'état de l'élément. Le fait de passer le curseur sur des éléments fournit parfois des informations supplémentaires. Utilisez ce graphique pour surveiller les éléments suivants.

Remarque La partie interface du graphique, y compris les informations sur l'état de l'interface, est également disponible sur la page **Interfaces** et dans le tableau de bord **de surveillance** > **du système**.

État d'interface

Passez le curseur sur un port pour voir ses adresses IP et ses états d'activation et de liaison. Les adresses IP peuvent être attribuées statiquement ou obtenues à l'aide de DHCP. Le déplacement sur une interface virtuelle de pont (BVI) affiche également la liste des interfaces membres.

Les ports d'interface utilisent le code de couleur suivant :

- Vert : l'interface est configurée, activée et la liaison est activée.
- Gris : l'interface n'est pas activée.
- Orange/rouge : l'interface est configurée et activée, mais la liaison est en panne. Si l'interface est câblée, il s'agit d'une condition d'erreur qui doit être corrigée. Si l'interface n'est pas câblée, il s'agit de l'état attendu.

Connexions de réseau internes et externes

Le graphique indique quel port est connecté aux réseaux externe (ou en amont) et interne, dans les conditions suivantes.

- Réseau interne : le port du réseau interne est affiché pour l'interface nommée « inside » (interne) uniquement. S'il existe d'autres réseaux internes, ils ne sont pas affichés. Si vous ne nommez aucune interface « inside », aucun port n'est marqué comme port interne.
- Réseau externe : le port du réseau externe est affiché pour l'interface nommée « outside » (externe) uniquement. Comme pour le réseau interne, ce nom est requis, ou aucun port n'est marqué comme port externe.

État des paramètres de l'interface de gestion

Le graphique indique si la passerelle, les serveurs DNS, les serveurs NTP et les licences Smart sont configurés pour l'adresse de gestion et si ces paramètres fonctionnent correctement.

Le vert indique que la fonctionnalité est configurée et fonctionne correctement, le gris indique qu'elle n'est pas configurée ou ne fonctionne pas correctement. Par exemple, la zone DNS est grisée si les serveurs ne sont pas accessibles. Passez le curseur sur les éléments pour voir plus d'informations.

Si vous détectez des problèmes, corrigez-les comme suit :

- Port et passerelle de l'interface de gestion : sélectionnez **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)**.
- Serveurs DNS : sélectionnez **System Settings (Paramètres système)** > **DNS Server**.
- Serveurs NTP : sélectionnez **System Settings (Paramètres système)** > **NTP**. Voir aussi Dépannage du protocole NTP.
- Licence Smart : cliquez sur le lien **View Configuration** (Afficher la configuration) dans le groupe Licence Smart.

Affichage de l'état des tâches du système

Les tâches système comprennent des actions qui se produisent sans votre participation directe, telles que la récupération et l'application de diverses mises à jour de base de données. Vous pouvez afficher une liste de ces tâches et leur état pour vérifier que ces tâches système sont effectuées avec succès.

La liste des tâches affiche l'état consolidé des tâches système et des tâches de déploiement. Le journal d'audit contient des informations plus détaillées et est accessible sous **Device (Périphérique)** > **Device Administration (Administration du périphérique)** > **Audit Log (Journal d'audit).** Par exemple, le journal d'audit affiche des événements distincts pour le début et la fin de la tâche, alors que la liste des tâches fusionne ces événements en une seule entrée. En outre, l'entrée du journal d'audit d'un déploiement comprend des informations détaillées sur les modifications déployées.

Procédure

Étape 1 Cliquez sur le bouton **Task List** (Liste des tâches) dans le menu principal.

La liste des tâches s'ouvre, affichant l'état et les détails des tâches du système.

Étape 2 Évaluez l'état de la tâche.

Si vous détectez un problème persistant, vous devrez peut-être corriger la configuration du périphérique. Par exemple, un échec persistant à obtenir les mises à jour de la base de données peut indiquer qu'il n'y a pas de chemin d'accès à Internet pour l'adresse IP de gestion du périphérique. Vous devrez peut-être communiquer avec le centre d'assistance technique de Cisco (TAC) pour certains problèmes, comme indiqué dans les descriptions des tâches.

Vous pouvez effectuer les opérations suivantes avec la liste des tâches :

- Cliquez sur les boutons **Success** (Réussites) ou **Failures** (Échecs) pour filtrer la liste selon ces états.
- Cliquez sur l'icône de suppression ( ) d'une tâche afin de la supprimer de la liste.
- Cliquez sur **Remove All Completed Tasks** (Supprimer toutes les tâches terminées) pour vider la liste de toutes les tâches qui ne sont pas en cours.

Utilisation de la console d'interface de ligne de commande pour surveiller et tester la configuration

FTD Les périphériques comprennent une interface de ligne de commande (CLI) que vous pouvez utiliser pour la surveillance et le dépannage. Bien que vous puissiez ouvrir une session SSH pour obtenir l'accès à toutes les commandes du système, vous pouvez également ouvrir une console d'interface de ligne de commande dans le FDM pour utiliser des commandes en lecture seule, telles que les diverses commandes **show** et **ping**, **traceroute**, et **packet-tracer**. Si vous disposez de privilèges d'administrateur, vous pouvez également accéder aux commandes **failover**, **reboot** et **shutdown**.

Vous pouvez laisser la console d'interface de ligne de commande ouverte pendant que vous vous déplacez d'une page à l'autre, configurez et déployez les fonctionnalités. Par exemple, après avoir déployé une nouvelle route statique, vous pouvez utiliser **ping** dans la console d'interface de ligne de commande pour vérifier que le réseau cible est accessible.

La console d'interface de ligne de commande utilise l'interface de ligne de commande de base Cisco Firepower Threat Defense. Vous ne pouvez pas accéder à l'interface de ligne de commande de diagnostic, au mode expert ou à l'interface de ligne de commande de FXOS (sur les modèles qui utilisent FXOS) à l'aide de la console d'interface de ligne de commande. Utilisez SSH si vous devez passer à ces autres modes de CLI.

Pour de plus amples renseignements, voir Référence de commande Cisco Firepower Threat Defense, https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

Remarques :

- Bien que **ping** soit pris en charge dans la console CLI, la commande **ping system** n'est pas prise en charge.
- Le système peut traiter au maximum 2 commandes simultanées. Ainsi, si un autre utilisateur émet des commandes (par exemple, à l'aide de l'API REST), vous devrez peut-être attendre que d'autres commandes soient terminées avant d'entrer une commande. S'il s'agit d'un problème persistant, utilisez une session SSH au lieu de la console d'interface de ligne de commande.
- Les commandes renvoient des informations en fonction de la configuration déployée. Si vous apportez une modification de configuration dans FDM, mais que vous ne la déployez pas, vous ne verrez pas les

résultats de votre modification dans la sortie de commande. Par exemple, si vous créez une nouvelle route statique mais ne la déployez pas, cette route ne s'affichera pas dans la sortie **show route**.

Procédure

Étape 1 Cliquez sur le bouton **CLI Console** (Console CLI) dans le coin supérieur droit de la page Web.

Étape 2 Saisissez les commandes à l'invite et appuyez sur **Enter (Entrée)**.

Certaines commandes prennent plus de temps à produire une sortie que d'autres, veuillez patienter. Si vous recevez un message indiquant que l'exécution de la commande a expiré, veuillez réessayer. Vous obtiendrez également une erreur de délai d'expiration si vous entrez une commande qui nécessite des réponses interactives, comme **show perfstats**. Si le problème persiste, vous devrez peut-être utiliser un client SSH au lieu de la console d'interface de ligne de commande.

Voici quelques conseils sur la façon d'utiliser la fenêtre.

- Appuyez sur la touche **Tab** (Onglet) pour terminer automatiquement une commande après l'avoir partiellement saisie. De plus, Onglet répertorie les paramètres disponibles à ce stade de la commande. L'onglet fonctionne jusqu'à trois niveaux de mot-clé. Après trois niveaux, vous devez utiliser la référence de commande pour obtenir plus d'informations.
- Vous pouvez arrêter l'exécution de la commande en appuyant sur Ctrl+C.
- Pour déplacer la fenêtre, cliquez et maintenez n'importe où dans l'en-tête, puis faites glisser la fenêtre vers l'emplacement souhaité.
- Cliquez sur le **Expand (Développer)** () ou **Collapse (Réduire)** () pour agrandir ou réduire la fenêtre.
- Cliquez sur le bouton **Undock Into Separate Window** (Détacher dans une fenêtre séparée) () pour dissocier la fenêtre de la page Web dans la fenêtre de son propre navigateur. Pour l'ancrer de nouveau, cliquez sur le bouton **Dock to Main Window** (Ancrer à la fenêtre principale) ().
- Cliquez et faites glisser pour surligner le texte, puis appuyez sur Ctrl+C pour copier le résultat dans le presse-papiers.
- Cliquez sur le bouton **Clear CLI (Effacer la CLI)** () pour effacer toute la sortie.
- Cliquez sur le bouton **Copy Last Output (Copier la dernière sortie)** () pour copier le résultat de la dernière commande que vous avez saisie dans le presse-papiers.

Étape 3 Lorsque vous avez terminé, fermez simplement la fenêtre de la console. N'utilisez pas la commande **exit**.

Bien que les informations d'authentification que vous utilisez pour vous connecter au FDM valident votre accès à l'interface de ligne de commande, vous n'êtes jamais connecté à l'interface de ligne de commande lorsque vous utilisez la console.

Utilisation conjointe de FDM et de l'API REST

Lorsque vous configurez le périphérique en mode gestion locale, vous pouvez le configurer à l'aide de FDM et de l'API REST Cisco Firepower Threat Defense. En fait, le FDM utilise l'API REST pour configurer l'appareil.

Cependant, veuillez comprendre que l'API REST peut fournir des fonctionnalités supplémentaires que celles disponibles par l'intermédiaire du FDM. Ainsi, pour une fonctionnalité donnée, vous pourrez peut-être configurer des paramètres à l'aide de l'API REST qui ne peuvent pas s'afficher lorsque vous affichez la configuration à l'aide de FDM.

Si vous configurez un paramètre de fonctionnalité disponible dans l'API REST, mais pas dans FDM, puis apportez une modification à la fonctionnalité globale (comme le VPN d'accès à distance) à l'aide de FDM, ce paramètre peut être annulé. Le fait qu'un paramètre API uniquement soit conservé peut varier et, dans de nombreux cas, les modifications apportées par l'API aux paramètres non disponibles dans FDM sont conservées par le biais des modifications FDM. Pour une fonctionnalité donnée, vous devez vérifier si vos modifications sont conservées.

En général, vous devez éviter d'utiliser simultanément FDM et l'API REST pour une fonctionnalité donnée. Au lieu de cela, choisissez une méthode ou une autre, fonctionnalité par fonctionnalité, pour configurer le périphérique.

Vous pouvez afficher et essayer les méthodes API à l'aide de l'explorateur API. Cliquez sur le bouton des autres options (⋮) et choisissez **API Explorer** (Explorateur d'interface de protocole d'application).

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.