



Pour commencer

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

- [Ce guide est-il pour vous?, à la page 1](#)
- [Nouvelles fonctionnalités dans la version 7.0.0 de FDM/FTD, à la page 2](#)
- [Configuration par défaut, à la page 8](#)
- [Connexion au système, à la page 15](#)
- [Configuration du système, à la page 20](#)
- [Bases de la configuration, à la page 27](#)
- [Exigences relatives aux ports de communication et à l'accès Internet, à la page 37](#)

Ce guide est-il pour vous?

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

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet 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
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	6.1
ISA 3000 (Cisco 3000 Series Industrial Security Appliances)	6.2.3

Nouvelles fonctionnalités dans la version 7.0.0 de FDM/FTD

Date de sortie : 26 mai 2021

Le tableau suivant répertorie les nouvelles fonctions disponibles dans Firepower Threat Defense 7.0.0 lorsqu'elles sont configurées à l'aide de FDM.

Fonctionnalités	Description
Caractéristiques de la plateforme	
FTDv pour HyperFlex et Nutanix.	Nous avons introduit FTDv pour Cisco HyperFlex et Nutanix Enterprise Cloud.
FTDv pour VMware vSphere/VMware ESXi 7.0.	Vous pouvez maintenant déployer FTDv sur VMware vSphere/VMware ESXi 7.0. Notez que la version 7.0 supprime également la prise en charge de VMware 6.0. Mettez à niveau l'environnement d'hébergement à une version prise en charge avant de mettre à niveau le FTD.
Nouveau mot de passe par défaut pour FTDv sur AWS.	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.

Fonctionnalités	Description
Prise en charge d'ISA 3000 pour l'arrêt.	Dans les versions 7.0.2 et ultérieures, vous pouvez éteindre l'ISA 3000; auparavant, vous pouviez uniquement redémarrer le périphérique. Dans les versions 7.0.5 et ultérieures, lorsque vous éteignez l'ISA 3000, le voyant DEL système s'éteint. Attendez au moins 10 secondes avant de couper l'alimentation du périphérique. Restrictions de version : la version 7.1 rend temporairement obsolète la prise en charge de cette fonctionnalité. Le soutien est de retour dans la version 7.2.
Fonctionnalités de pare-feu et IPS	
Nouvelle section 0 pour les règles NAT définies par le système.	Une nouvelle section 0 a été ajoutée au tableau de règles NAT. Cette section est destinée exclusivement à l'utilisation du système. Toutes les règles NAT dont le système a besoin pour le fonctionnement normal sont ajoutées à cette section, et ces règles ont priorité sur toutes les règles que vous créez. Auparavant, les règles définies par le système étaient ajoutées à la section 1, et les règles définies par l'utilisateur pouvaient interférer avec le bon fonctionnement du système. Vous ne pouvez pas ajouter, modifier ou supprimer les règles de la section 0, mais vous les verrez dans la sortie de la commande show nat detail.
Règles de prévention des intrusions personnalisées pour Snort 3.	Vous pouvez utiliser des outils hors ligne pour créer des règles de prévention des intrusions personnalisées à utiliser avec Snort 3 et les téléverser dans une politique de prévention des intrusions. Vous pouvez organiser les règles personnalisées dans vos propres groupes de règles personnalisées pour faciliter leur mise à jour au besoin. Vous pouvez également créer les règles directement dans FDM, mais les règles ont le même format que les règles téléversées. FDM ne vous guide pas dans la création des règles. Vous pouvez dupliquer des règles existantes, y compris des règles définies par le système, comme base pour une nouvelle règle de prévention des intrusions. Nous avons ajouté la prise en charge des groupes et des règles personnalisés à la page Politiques (Politiques) > Intrusion, lorsque vous modifiez une politique de prévention des intrusions.
Nouvelles fonctionnalités de Snort 3 pour les systèmes gérés par FDM.	Vous pouvez désormais configurer les fonctionnalités supplémentaires suivantes lors de l'utilisation de Snort 3 comme moteur d'inspection sur un système géré par FDM : • Règles des politiques de contrôle d'accès basées sur le temps (API FTD seulement.) • Routeurs virtuels multiples • Le déchiffrement des connexions TLS 1.1 ou version inférieure à l'aide de la politique de déchiffrement SSL. • Le déchiffrement des protocoles suivants à l'aide de la politique de déchiffrement SSL : FTPS, SMTPS, IMAPS, POP3S.

Fonctionnalités	Description
Filtrage des requêtes DNS en fonction de la catégorie d'URL et de la réputation.	Vous pouvez appliquer vos règles de catégorie et de réputation de filtrage d'URL aux demandes de consultation DNS. Si le nom de domaine complet (FQDN) dans la demande de recherche dispose d'une catégorie et d'une réputation que vous bloquez, le système bloque la réponse DNS. Étant donné que l'utilisateur ne reçoit pas de résolution DNS, l'utilisateur ne peut pas établir la connexion. Utilisez cette option pour appliquer un filtrage de catégorie et de réputation d'URL au trafic non Web. Vous devez avoir une licence de filtrage d'URL pour utiliser cette fonctionnalité. Nous avons ajouté l'option d' application de la réputation sur le trafic DNS aux paramètres de politique de contrôle d'accès.
VDB plus petite pour les périphériques à mémoire inférieure avec Snort 2.	Incidence de la mise à niveau. L'identification de l'application sur les périphériques à mémoire limitée est affectée. Pour les périphériques des versions 7.0.6 et ultérieures avec Snort 2, pour VDB 363+, le système installe maintenant une VDB de taille plus faible (également appelée <i>VDB lite</i>) sur les périphériques de mémoire limitée exécutant Snort 2. Cette plus petite VDB contient les mêmes applications, mais moins de schémas de détection. Les périphériques utilisant la plus petite VDB peuvent ne pas identifier certaines applications par rapport aux périphériques utilisant la VDB complète. Périphériques de mémoire inférieure : ASA-5508-X, ASA-5516-X Restrictions de version: la VDB de taille plus faible n'est pas prise en charge par toutes les versions. Si vous effectuez une mise à niveau à partir d'une version prise en charge vers une version non prise en charge, vous ne pouvez pas installer VDB 363+ sur les périphériques de mémoire inférieure exécutant Snort 2. Pour obtenir la liste des versions concernées, consultez CSCwd88641.
Fonctionnalités du VPN	
Paramètres de chiffrement SSL FDM pour le VPN d'accès à distance.	Vous pouvez définir les versions TLS et les chiffrements à utiliser pour les connexions de VPN d'accès à distance dans FDM. Auparavant, vous deviez utiliser l'API Firepower Threat Defense pour configurer les paramètres SSL. Nous avons ajouté les pages suivantes : Objets > Chiffrements SSL; Périphérique > Paramètres système > Paramètres SSL.
Prise en charge de Diffie-Hellman, groupe 31.	Vous pouvez désormais utiliser le groupe 31 de Diffie-Hellman (DH) dans les propositions et les politiques IKEv2.
Le nombre maximal d'interfaces de tunnel virtuel sur le périphérique est de 1024.	Le nombre maximal d'interfaces de tunnel virtuel (VTI) que vous pouvez créer est de 1024. Dans les versions précédentes, le maximum était de 100 par interface source.

Fonctionnalités	Description
Paramètres de durée de vie IPsec pour les associations de sécurité VPN de site à site.	Vous pouvez modifier les paramètres par défaut relatifs à la durée de conservation d'une association de sécurité avant de devoir être renégociée. Nous avons ajouté les options de durée de vie et d'étendue de vie à l'assistant VPN de site à site.
Fonctionnalités de routage	
Prise en charge des routeurs virtuels pour ISA 3000.	Vous pouvez configurer jusqu'à 10 routeurs virtuels sur un périphérique ISA 3000.
Routage à chemins multiples à coûts égaux (ECMP).	Vous pouvez configurer des zones de trafic ECMP pour contenir plusieurs interfaces, ce qui permet au trafic d'une connexion existante de sortir ou d'entrer dans le périphérique Firepower Threat Defense sur n'importe quelle interface de la zone. Cette fonctionnalité permet le routage à chemins multiples à coûts égaux (ECMP) sur le périphérique Firepower Threat Defense, ainsi qu'à équilibrer la charge externe du trafic vers le périphérique Firepower Threat Defense sur plusieurs interfaces. Les zones de trafic ECMP sont utilisées uniquement pour le routage. Elles ne correspondent pas aux zones de sécurité. Nous avons ajouté l'onglet ECMP Traffic Zones (Zones de trafic ECMP) aux pages de routage. Dans l'API Firepower Threat Defense, nous avons ajouté les ressources ECMPZones.
Fonctionnalités de l'interface	
Nouvelle adresse IP interne par défaut.	L'adresse IP par défaut de l'interface interne est remplacée par 192.168.95.1 au lieu de 192.168.1.1 pour éviter un conflit d'adresses IP lorsqu'une adresse sur 192.168.1.0/24 est attribuée à l'interface externe à l'aide de DHCP.
La configuration automatique IPv6 de l'adresse IP externe par défaut est maintenant activée; nouveau serveur DNS IPv6 par défaut pour la gestion.	La configuration par défaut sur l'interface externe comprend désormais la configuration automatique IPv6, en plus du client DHCP IPv4. Les serveurs DNS de gestion par défaut comprennent désormais un serveur IPv6 : 2620:119:35::35.
Prise en charge d'EtherChannel pour ISA 3000.	Vous pouvez maintenant utiliser FDM pour configurer les EtherChannels sur l'ISA 3000. Écrans nouveaux ou modifiés : Devices (Périphériques) > interfaces > EtherChannels
Caractéristiques de la licence	

Fonctionnalités	Description
Licence progressive en fonction de la performance pour FTDv.	Le FTDv prend désormais en charge les licences Smart par niveau de performance en fonction des exigences de débit et des limites de session de VPN d'accès à distance. Lorsque le FTDv est concédé avec l'une des licences de performance disponibles, deux choses se produisent. Tout d'abord, un limiteur de débit est installé qui limite le débit du périphérique à un niveau spécifié. Ensuite, le nombre de sessions VPN est plafonné au niveau spécifié par la licence.
Fonctions d'administration et de dépannage	
Configuration du relais DHCP à l'aide de l'API Firepower Threat Defense.	Incidence sur la mise à niveau. Peut empêcher le déploiement après la mise à niveau. Vous pouvez utiliser l'API Firepower Threat Defense 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. Notez que si vous avez utilisé FlexConfig dans les versions précédentes pour configurer le relais DHCP (la commande dhcprelay, vous devez refaire la configuration à l'aide de l'API et supprimer l'objet FlexConfig après la mise à niveau. Nous avons ajouté le modèle suivant à l'API Firepower Threat Defense : dhcprelayservices
Traitement de démarrage initial plus rapide et connexion anticipée à FDM.	Le processus de démarrage initial d'un système géré par FDMa été amélioré pour le rendre plus rapide. Ainsi, vous n'avez pas besoin d'attendre aussi longtemps après le démarrage du périphérique pour vous connecter à FDM. En outre, vous pouvez désormais vous connecter pendant le démarrage. Si le démarrage n'est pas terminé, vous verrez des informations d'état sur le processus afin que vous sachiez ce qui se passe sur le périphérique.
Amélioration de l'utilisation et des performances du processeur pour les connexions plusieurs à un et un à plusieurs.	Le système ne crée plus d'objets hôtes locaux et les verrouille lors de la création de connexions, sauf pour les connexions qui impliquent une NAT/PAT dynamique, l'analyse de la détection des menaces et des statistiques de l'hôte. Cela améliore les performances et l'utilisation de la CPU dans les situations où de nombreuses connexions sont dirigées vers le même serveur (comme un équilibreur de charge ou un serveur Web), ou un point terminal établit des connexions à de nombreux hôtes distants. Nous avons modifié les commandes suivantes : clear local-host (obsolète), show local-host

Fonctionnalités	Description
Vérification de l'état de préparation à la mise à niveau pour les périphériques gérés par FDM.	Vous pouvez exécuter une vérification de l'état de préparation à la mise à niveau sur un ensemble de mise à niveau Firepower Threat Defense téléchargé avant de tenter de l'installer. La vérification de l'état de préparation vérifie que la mise à niveau est valide pour le système et que le système répond aux autres exigences nécessaires à l'installation du paquet. L'exécution d'une vérification de l'état de préparation à la mise à niveau vous permet d'éviter les échecs d'installation. Un lien pour exécuter la vérification de l'état de préparation à la mise à niveau a été ajouté à la section System Upgrade (Mise à niveau du système) de la page Device (Périphérique) > Updates (Mises à jour).
Mettre automatiquement à jour les ensembles d'autorités de certification.	Incidence sur la mise à niveau. Le système se connecte à Cisco dans le cadre d'une nouveauté. 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. Nouvelles ressources : https://cisco.com/security/pki/ Commandes CLI nouvelles ou modifiées : configure cert-update auto-update, configure cert-update run-now, configure cert-update test, show cert-update Restrictions de version : nécessite la version 7.0.5, 7.1.0.3 ou 7.2.4. Non pris en charge avec 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. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Fonctionnalités	Description
Exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS.	Incidence sur la mise à niveau. Après la mise à niveau, lancez l'activation pour les serveurs existants. Vous pouvez désormais exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS, en vous assurant que la passerelle VPN de défense contre les menaces vérifie de manière sécurisée chaque réponse du serveur RADIUS, qu'il s'agisse d'un VPN d'accès à distance ou de l'accès au périphérique lui-même. L'option Require Message-Authenticator for all RADIUS Responses (exiger l'authentificateur Message-Authenticator pour toutes les réponses envoyées par RADIUS) est activée par défaut pour les nouveaux serveurs RADIUS. Nous vous recommandons également de l'activer pour les serveurs existants. Sa désactivation peut exposer les pare-feu à des attaques potentielles. Nouvelles commandes CLI : message-authenticator-required Restrictions de version : nécessite la version 7.0.7/ 7.7.0 (ou version ultérieure).
API REST de FTD version 6.1 (v6).	L'API REST Firepower Threat Defense pour la version logicielle 7.0 est la version 6.1. Vous pouvez utiliser la 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 6.1 est le même que pour la version 6.0 : 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.

Configuration par défaut

La configuration par défaut de votre périphérique dépend de la réussite de la configuration initiale.

Configuration par défaut avant la configuration initiale

Avant que vous ne configuriez initialement 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 21) 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.

Paramètres	Par défaut	Peut-on le modifier lors de la configuration initiale ?
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
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 BV11 n'est pas préconfigurée. BV11 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 BV11 n'est pas préconfigurée. BV11 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.

FTDpériphérique	Interface externe	Interface interne
ASA 5508-X ASA 5516-X	GigabitEthernet 1/1	GigabitEthernet 1/2
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
Firepower de la série 2100	Ethernet 1/1	Ethernet 1/2
Firepower 4100	Les interfaces de données ne sont pas préconfigurées.	Les interfaces de données ne sont pas préconfigurées.
Firepower 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 BVII.	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

Le 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 logiciel 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.
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.

Paramètres	Configuration	Configuration explicite, implicite ou par défaut
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.
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 BV11 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.	• 1010 : l'interface externe, Ethernet1/1, 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 autres interfaces de données sont désactivées. • ISA 3000 : toutes les interfaces de données sont activées et font partie du même groupe de ponts, BV11. 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 8. 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 BV11 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 <code>inside_zone</code> vers la <code>outside_zone</code>. 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 <code>inside_zone</code> à la <code>outside_zone</code>, et une règle faisant confiance à tout le trafic de la <code>outside_zone</code> à la <code>inside_zone</code>. Trafic non bloqué. Le périphérique dispose également de règles faisant confiance à tout le trafic entre les interfaces de la <code>inside_zone</code> et de la <code>outside_zone</code>. Cela permet, sans inspection, tout le trafic entre les utilisateurs de <code>inside</code> (interne) et entre les utilisateurs de <code>outside</code> (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.

Connexion au système

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

Interface Web FDM

Le Gestionnaire de périphériques de pare-feu 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 Gestionnaire de périphériques de pare-feu.

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 Gestionnaire de périphériques de pare-feu. 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 Gestionnaire de périphériques de pare-feu affiche votre nom d'utilisateur et votre niveau de privilège.

admin
Administrator 

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 Gestionnaire de périphériques de pare-feu 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 Gestionnaire de périphériques de pare-feu.

Utilisez le Gestionnaire de périphériques de pare-feu 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 Gestionnaire de périphériques de pare-feu 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 du Gestionnaire de périphériques de pare-feu et accès des utilisateurs Firewall Threat Defense](#).

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 8](#) 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, l'interface de ligne de commande du port de console est Secure Firewall eXtensible Operating System (FXOS). Pour certains modèles de périphérique, vous pouvez accéder à l'interface de ligne de commande 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 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 Firewall Threat Defense Virtual 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](http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) 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 Gestionnaire de périphériques de pare-feu.
- 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 \(SSH\) Firewall Threat Defense](#).

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 Gestionnaire de périphériques de pare-feu.



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.

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).

Affichage des pages dans d'autres langues que l'anglais

Vous pouvez afficher l'interface graphique et l'aide en ligne dans les langages suivants.

- Chinois
- Anglais (par défaut)
- Japonais
- Coréen

Pour utiliser ces langues, vous devez sélectionner cette langue dans les paramètres de votre navigateur. Il n'y a pas de paramètre de langue dans le produit lui-même.

Si votre navigateur ne prend pas en charge une langue particulière, le produit ne s'affichera pas dans cette langue. Par exemple, la version française ne s'affiche que si vous configurez le navigateur pour utiliser le Français canadien. La sélection d'un autre type de Français permet de laisser le produit en anglais.

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 8](#).

Procédure

Étape 1 [Connecter les interfaces, à la page 21](#)

Étape 2 [Compléter la configuration initiale avec l'assistant d'installation, à la page 23](#)

Pour en savoir plus sur la configuration résultante, consultez [Configuration après la configuration initiale, à la page 11](#).

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.

Consultez le [guide de démarrage](#) de votre modèle pour obtenir les schémas de câblage.

(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 Firewall Threat Defense. Consultez [Connexion avec l'interface de ligne de commande \(CLI\)](#), à la page 18 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 Firewall Threat Defense Virtual 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 Firewall Threat Defense, 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 Gestionnaire de périphériques de pare-feu (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 du Gestionnaire de périphériques de pare-feu 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 Gestionnaire de périphériques de pare-feu. Une réponse **non** signifie que vous avez l'intention d'utiliser le système Centre de gestion Firepower (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 Gestionnaire de périphériques de pare-feu 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 Gestionnaire de périphériques de pare-feu, 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 21](#) et [Configuration par défaut avant la configuration initiale, à la page 8](#)).

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 Firewall Threat Defense Virtual, assurez-vous simplement que vous avez une connexion à l'adresse IP de gestion.

(Sauf pour le Firewall Threat Defense Virtual, 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 21](#).

Procédure

Étape 1 Connectez-vous à Gestionnaire de périphériques de pare-feu.

- a) En supposant que vous n'êtes pas passé par la configuration initiale dans l'interface de ligne de commande, ouvrez le Gestionnaire de périphériques de pare-feu 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 Firewall Threat Defense Virtual) 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 Firewall Threat Defense Virtual 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 8](#)), 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 Firewall Threat Defense](#).

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.
-

Bases de la configuration

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

Configuration du périphérique

Lorsque vous vous connectez pour la première fois à Gestionnaire de périphériques de pare-feu, 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 33](#).

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 Gestionnaire de périphériques de pare-feu. 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 30](#).

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 **Politiques** (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 30.

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 Firewall Threat Defense 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 32.

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 d'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

Firewall Threat Defense 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 Gestionnaire de périphériques de pare-feu 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 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), 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 Gestionnaire de périphériques de pare-feu, 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 **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 Gestionnaire de périphériques de pare-feu 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 Gestionnaire de périphériques de pare-feu 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 Firepower Threat Defense. En fait, le Gestionnaire de périphériques de pare-feu 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 Gestionnaire de périphériques de pare-feu. 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 Gestionnaire de périphériques de pare-feu.

Si vous configurez un paramètre de fonctionnalité disponible dans l'API REST, mais pas dans Gestionnaire de périphériques de pare-feu, puis apportez une modification à la fonctionnalité globale (comme le VPN d'accès à distance) à l'aide de Gestionnaire de périphériques de pare-feu, 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 Gestionnaire de périphériques de pare-feu sont conservées par le biais des modifications Gestionnaire de périphériques de pare-feu. Pour une fonctionnalité donnée, vous devez vérifier si vos modifications sont conservées.

En général, vous devez éviter d'utiliser simultanément Gestionnaire de périphériques de pare-feu 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).

Exigences relatives aux ports de communication et à l'accès Internet

Les rubriques suivantes décrivent les ports qui doivent être ouverts sur le périphérique et les sites Internet auxquels l'accès est requis pour utiliser toutes les fonctionnalités disponibles sur le périphérique. Si vous

fonctionnez de manière limitée ou isolée, certains ou tous ces ports et sites Internet peuvent être bloqués pour répondre à vos besoins. Sinon, assurez-vous que ces ports et ces sites sont ouverts et accessibles.

Ports de communication utilisés par le périphérique

Les tableaux suivants répertorient les ports qui doivent être ouverts pour divers services. Utilisez des règles de contrôle d'accès pour vous assurer que l'accès à ces ports est ouvert sur les interfaces qui font face aux services ou qui font face aux utilisateurs qui devraient pouvoir accéder au périphérique à l'aide du protocole associé. Si vous n'utilisez pas de fonctionnalité, vous pouvez laisser ces ports fermés.

Tableau 2 : Ports entrants

Port entrant	Protocole/Fonctionnalité	Détails
TCP 22	SSH	Sécuriser les connexions distantes à l'interface de ligne de commande de l'appareil. Remarque Si vous utilisez la commande copy ou une autre commande qui effectue une communication externe, vous devez ouvrir ce port sortant. Par exemple, TCP/20, 21 si vous avez l'intention d'utiliser le protocole FTP.
UDP 161	SNMP	Autorisez l'accès aux MIB par interrogation SNMP.
TCP/443	HTTPS	Utilisé pour les services suivants : • Connexions de gestion à FDM. • API REST Cisco Firepower Threat Defense. • Connexions VPN SSL d'accès à distance. Si vous configurez un port personnalisé pour le VPN d'accès à distance, ouvrez ce port.
TCP/885	Portail captif	Communiquez avec une source d'identité de portail captif. Ceci est le port par défaut. Si vous configurez un autre port, ouvrez votre port personnalisé. Pour obtenir plus de renseignements, consultez Configurer les paramètres de la politique d'identité .
TCP/8989	Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Accepte les demandes autorisées. Initie également les connexions sur ce port.

Tableau 3 : Ports sortants :

Port sortant :	Protocole/Fonctionnalité	Détails
UDP/53 (Si utilisé.) TCP/53	DNS	DNS. Normalement, UDP/53 est utilisé pour DNS. Mais si vous utilisez DNS sur TCP, ouvrez également TCP/53.
UDP/67 UDP/68	DHCP (protocole de configuration dynamique des hôtes)	DHCP.

Port sortant :	Protocole/Fonctionnalité	Détails
UDP/123	NTP;	Synchronisez l'heure.
UDP/162	SNMP	Envoyez des alertes SNMP à un serveur de dé routement distant.
TCP/389 TCP/636	LDAP, LDAPS	Communiquez avec un serveur LDAP pour l'authentification externe. Si vous configurez des ports personnalisés, ouvrez ces ports. Consultez Configuration des domaines d'identité AD .
TCP/443	HTTPS	Envoyer et recevoir des données d'Internet, par exemple pour télécharger des mises à jour de bases de données.
UDP/514	Syslog	Envoyez des messages de journal système à un serveur syslog distant.
UDP/1812 UDP/1813	RADIUS	Communiquez avec un serveur RADIUS pour l'authentification externe et la gestion comptable. Si vous configurez des ports personnalisés, ouvrez-les. Consultez Configurer les serveurs RADIUS .
UDP/8514	Cisco Secure Network Analytics Manager	Envoyez des messages de journalisation du système vers le nuage.
TCP/8989	Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Transmet des informations et des statistiques d'utilisation. Accepte également les connexions sur ce port.

Ressources Internet consultées par le périphérique

Les fonctionnalités suivantes doivent avoir accès aux ressources Internet associées pour fonctionner correctement. Le périphérique utilise les ports TCP/80 et TCP/443 selon les besoins.

Tableau 4 : Ressources Internet consultées par le périphérique

Caractéristiques	Motif	Haute disponibilité	Ressource
Offres groupées de certificats de l'autorité de certification (CA)	Demande de nouveaux certificats d'autorité de certification (CA) à une heure quotidienne définie par le système. L'offre groupée de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Cette fonctionnalité est configurée dans l'interface de ligne de commande à l'aide de la commande configure cert-update auto-update. Disponible dans les versions 7.0(5), 7.1(0.3), 7.2(4), 7.3 et ultérieures.	Chaque homologue télécharge ses propres certificats.	cisco.com/security/pki
Défense contre les programmes malveillants 1	Recherches Cisco AMP Cloud	Les deux homologues effectuent des recherches.	Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint et le fonctionnement de Malware Analytics.
	Téléchargez les mises à jour de signatures pour la préclassification des fichiers et l'analyse des programmes malveillants locaux.	Les homologues actifs téléchargent et se synchronisent en mode veille.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Envoyer des fichiers pour analyse dynamique. Requête de résultats d'analyse dynamique.	Les deux homologues soumettent ou interrogent des rapports d'analyse dynamique.	fmc.api.threatgrid.com fmc.api.threatgrid.eu fmc.api.threatgrid.ca fmc.api.threatgrid.com.au fmc.api.threatgrid.in
Renseignements de sécurité	Télécharger les flux de renseignements sur la sécurité	Les homologues actifs téléchargent et se synchronisent en mode veille.	intelligence.sourcefire.com

Caractéristiques	Motif	Haute disponibilité	Ressource
Filtrage d'URL	Télécharger des données de catégorie d'URL et de réputation. Interroger (rechercher) manuellement les données de catégorie d'URL et de réputation. Rechercher des URL non classées.	Les homologues actifs téléchargent et se synchronisent en mode veille.	URL : • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com Blocs IPv4 : • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 Blocs IPv6 : • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Propriété Smart Software Manager	Communiquez avec le Smart Software Manager.	L'homologue actif communique.	www.cisco.com
Cisco Success Network	Transmettez des informations et des statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Accepte les demandes autorisées et transmet les renseignements et les statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989
Services en nuage généraux	—	—	api-sse.cisco.com
Intégration Cisco XDR	Configurer les périphériques pour envoyer des événements au Cisco Security Cloud.	L'homologue actif communique.	Guide d'intégration Cisco Secure Firewall Threat Defense et Cisco XDR.
Synchronisation de l'heure	Synchronisez l'heure dans votre déploiement. Non pris en charge avec un serveur mandataire.	Les deux homologues communiquent avec le serveur NTP.	Utilisateur configuré. Serveurs par défaut : • 0.sourcefire.pool.ntp.org • 1.sourcefire.pool.ntp.org • 2.sourcefire.pool.ntp.org

Caractéristiques	Motif	Haute disponibilité	Ressource
Règles d'intrusion	Télécharger les règles d'intrusion (SRU/LSP).	Les homologues actifs téléchargent et se synchronisent en mode veille.	talosintelligence.com
Base de données sur la vulnérabilité	Télécharger les mises à jour VDB.	Les homologues actifs téléchargent et se synchronisent en mode veille.	support.sourcefire.com
Base de données de géolocalisation	Télécharger les mises à jour GeoDB.	Les homologues actifs téléchargent et se synchronisent en mode veille.	support.sourcefire.com

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.

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.

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.