Nouvelles fonctionnalités de Cisco Secure Firewall Device Manager par version

Dernière modification : 2025-11-10

Nouvelles fonctionnalités par version

Ce document décrit les nouvelles fonctionnalités et les fonctionnalités obsolètes pour chaque version.

Incidence sur la mise à niveau

Une fonctionnalité a une incidence sur la mise à niveau si sa mise à niveau et son déploiement peuvent forcer le système à traiter le trafic ou à agir différemment sans autre action de votre part. Cela arrive fréquemment avec les nouvelles capacités de détection des menaces et d'identification des applications. Une fonctionnalité peut également avoir une incidence sur la mise à niveau si celle-ci implique que vous preniez des mesures avant ou après la mise à niveau pour éviter un résultat indésirable; par exemple, si vous devez modifier une configuration.

Les descriptions des fonctionnalités comprennent, le cas échéant, l'incidence de la mise à niveau.

Fonctionnalités des versions de maintenance

Les fonctionnalités, les améliorations et les correctifs critiques inclus dans les versions de maintenance (troisième chiffre) et les correctifs (quatrième chiffre) peuvent ignorer les versions futures, selon la date de version, le type de version (court ou long terme) et d'autres facteurs. Minimisez l'incidence de la mise à niveau et autres en accédant directement à la dernière version de maintenance de la version choisie. Voir le Cisco Secure Firewall Threat Defense Notes de mise à jour.

Si vous utilisez l'interface Web dans une langue autre que l'anglais, les fonctionnalités introduites dans les versions de maintenance et les correctifs peuvent ne pas être traduites avant la prochaine version majeure.

Fonctionnalités de Snort

Snort 3 est la plateforme d'inspection par défaut pour Firewall Threat Defense avec Firepower Device Manager à partir de la version 6.7. Les fonctionnalités de Snort 3 pour les déploiements On-Prem Firewall Management Center s'appliquent également à Firepower Device Manager, même si elles ne sont pas répertoriées en tant que nouvelles fonctionnalités Firepower Device Manager. Cependant, gardez à l'esprit que On-Prem Firewall Management Center peut offrir des options plus configurables que Firepower Device Manager. Pour les améliorations de Snort par version, consultez Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version.

Important Snort 2 est obsolète dans la version 7.7 et les versions ultérieures, et empêche la mise à niveau de Firewall Threat Defense. Si vous utilisez toujours Snort 2 sur d'anciens périphériques, passez à Snort 3 pour améliorer la détection et les performances.

Règles de prévention des intrusions et mots clés

Les mises à niveau peuvent importer et activer automatiquement des règles de prévention des intrusions et de préprocesseurs nouvelles et mises à jour, les états modifiés pour les règles existantes et les paramètres de politique de prévention des intrusions par défaut modifiés. Si une nouvelle règle de prévention des intrusions utilise des mots clés qui ne sont pas pris en charge dans votre version actuelle, cette règle n'est pas importée lorsque vous mettez à jour SRU ou LSP. Après la mise à niveau et la prise en charge de ces mots clés, les nouvelles règles de prévention des inclusions sont importées et, selon la configuration IPS, peuvent être activées automatiquement et commencer à générer des événements et à affecter le flux de trafic.

Pour plus de renseignements sur les nouveaux mots clés, consultez les notes de mise à jour de Snort : https://www.snort.org/downloads.

FlexConfig

Les mises à niveau peuvent ajouter une interface Web ou la prise en charge de Smart CLI pour des fonctionnalités qui nécessitent déjà FlexConfig. Bien que vous ne puissiez pas affecter ou créer des objets FlexConfig à l'aide de commandes obsolètes, dans la plupart des cas, les FlexConfig existantes continuent de fonctionner et vous pouvez toujours les déployer. Cependant, l'utilisation de commandes obsolètes peut parfois entraîner des problèmes de déploiement. La mise à niveau ne convertit pas les FlexConfigs. Après la mise à niveau, configurez les nouvelles fonctionnalités prises en charge dans l'interface Web ou Smart CLI. Lorsque vous êtes satisfait de la nouvelle configuration, supprimez les FlexConfigs obsolètes.

Les descriptions de fonctionnalités incluent des informations sur les FlexConfigs obsolètes, le cas échéant. Pour obtenir la liste complète des FlexConfigs obsolètes, consultez votre guide de configuration.

Intégrations et journalisation

Ces intégrations et fonctions de journalisation peuvent comporter de nouvelles fonctionnalités associées aux versions de Threat Defense :

- Syslog : Messages Syslog de Cisco Secure Firewall Threat Defense
- API REST : Guide de Cisco Secure Firewall Threat Defense REST API

Version suggérée : Version 7.4.2

Pour profiter des nouvelles fonctionnalités et des problèmes résolus, nous vous recommandons de mettre à niveau tous les appareils admissibles au moins vers la version suggérée, y compris le dernier correctif. Sur le Site d'assistance et de téléchargement Cisco, la version suggérée est marquée d'une étoile d'or. Dans les versions 7.2.6 et ultérieures /7.4.1 et ultérieures, le centre de gestion vous informe lorsqu'une nouvelle version suggérée est disponible et indique les versions suggérées sur sa page de mises à niveau de produit.

Versions suggérées pour les anciens périphériques

Si un périphérique est trop ancien pour exécuter la version suggérée et que vous ne prévoyez pas d'actualiser le matériel pour le moment, choisissez une version majeure, puis utilisez le correctif dans la mesure du possible. Certaines versions majeures sont désignées *à long terme* ou *à très long terme*, alors pensez à l'une d'entre elles. Pour obtenir une explication de ces conditions, consultez Version logicielle et bulletin de soutien de la gamme de produits de pare-feu de nouvelle génération de Cisco.

Si vous êtes intéressé par une actualisation du matériel, communiquez avec votre représentant ou partenaire de Cisco.

Fonctionnalités dans la version 7.7.0 de Firewall Device Manager

Tableau 1 : Fonctionnalités dans la version 7.7.0 de Firewall Device Manager

Caractéristiques	Description
Caractéristiques de la plateforme	
Cisco Secure Firewall 1230, 1240 et 1250 (montage en rack).	Nous avons lancé le Cisco Secure Firewall CSF-1230 et CSF-1240 : • Cuivre de 8x1Gbps RJ-45 1000BASET/2,5BBASE-T • SFP+ optique 4x1 Gbps Et le pare-feu Secure Firewall CSF-1250 : • Cuivre de 8x2,5 Gbps 1000BASET/2,5BBASE-T • SFP28, 4x2,5 Gbps, optique Voir : Guide d'installation du matériel Cisco Secure Firewall CSF-1230, CSF-1240 et CSF-1250
Prise en charge de la norme IEEE 802.3bt (PoE++ et Hi-PoE) pour le Cisco Secure Firewall 1210CP.	Nous avons apporté les améliorations suivantes en matière de prise en charge d'IEEE 802.3bt : • PoE ++ et Hi-PoE, jusqu'à 90 W par port. • Périphériques alimentés à une ou plusieurs signatures. • La budgétisation de la puissance est effectuée selon le principe du premier arrivé premier servi. • Des champs de budget de puissance ont été ajoutés à **show power inline**. Écrans nouveaux ou modifiés: **Device (périphérique)** > **Interfaces** > **PoE** Commandes nouvelles ou modifiées : **show power inline**
Instances pour AWS, Azure et GCP.	Nous avons ajouté des instances pour Threat Defense Virtual dans les gammes suivantes : • AWS (Amazon Web Services) : C6i, C6a • Azure (Microsoft Azure) : Dv4, Dv5 • GCP (Google Cloud Platform) : E2, N1, N2D, C2D Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Provisionnement sans surveillance pour Firewall Threat Defense Virtual pour VMware à l'aide de l'amorçage Cloud-Init basé sur ISO.	Vous pouvez désormais déployer rapidement Firewall Threat Defense Virtual pour VMware à l'aide d'un fichier texte (day0.iso) contenant les détails de la configuration initiale tels que le nom de domaine, le mot de passe, le mode de gestion, le mode de pare-feu, les paramètres réseau et le type de déploiement. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Fonctionnalités de pare-feu et IPS	

Caractéristiques	Description
Prise en charge du contournement matériel pour les ensembles en ligne.	Si votre modèle de périphérique prend en charge le contournement matériel, vous pouvez désormais le configurer pour les ensembles en ligne contenant les interfaces prises en charge. Nous avons ajouté l'option **Bypass** (contourner) à la configuration des ensembles en ligne.
Obsolète : Snort 2.	**Incidence sur la mise à niveau. Impossible de mettre à niveau les périphériques Snort 2.** Snort 2 est obsolète. Vous ne pouvez pas mettre à niveau un périphérique Snort 2 vers la version 7.7.0 ou ultérieure. Nous avons supprimé la possibilité de passer à Snort 2, ainsi que les commandes **show snort counters** et **show snort preprocessor-memory-usage**. Avant de procéder à la mise à niveau, passez à Snort 3. Consultez le chapitre *Politiques de prévention des intrusions* dans le guide de votre version actuelle : Guide Cisco Secure Firewall Device Manager Configuration .
Fonctionnalités administratives	
Page de connexion personnalisée.	Vous pouvez personnaliser la page de connexion au gestionnaire de périphériques, notamment en y ajoutant une image et du texte. Par exemple, vous pouvez inclure des avertissements que l'utilisateur doit accepter avant de se connecter. Le texte est s'affiche également pour les séances SSH. Nous avons ajouté la page suivante : **System Settings (paramètres système)** > **Login Page (page de connexion)**.
Télémétrie de diffusion en continu personnalisée à l'aide des appels de procédure à distance Google (gRPC).	Vous pouvez configurer le périphérique pour qu'il envoie des données sur l'intégrité du système et la télémétrie à un collecteur de télémétrie externe qui utilise les appels de procédure à distance Google (gRPC) pour collecter des données. Vous pouvez ensuite utiliser votre collecteur de télémétrie pour surveiller le périphérique et l'intégrer à votre solution de télémétrie personnalisée. Utilisez l'API pour configurer cette fonctionnalité : /devicesettings/default/telemetrystreamingconfig.
Rendement	
Basculement plus rapide pour la haute disponibilitéFirewall Threat Defense	Grâce au basculement à haute disponibilité de Threat Defense, le nouveau périphérique actif génère des paquets de multidiffusion pour chaque entrée d'adresse MAC et les envoie à toutes les interfaces de groupe de pont, ce qui incite les commutateurs en amont à mettre à jour leurs tables de routage. Cette tâche s'exécute désormais de manière asynchrone dans le plan de données, privilégiant les tâches de basculement critiques dans le plan de contrôle. Cela accélère le basculement et réduit les temps d'arrêt.

Caractéristiques	Description
Le trafic d'applications chiffré à bande passante élevée contourne l'inspection d'intrusion inutile.	Le trafic d'applications chiffrées à large bande passante est désormais exempté de l'inspection des intrusions inutile, même si la connexion correspond à une règle Allow (Autoriser). Les mises à jour des règles d'intrusion (LSP) et de la base de données des vulnérabilités (VDB) peuvent modifier la liste des applications exemptées, mais celles actuellement concernées sont : AnyConnect, IPsec, iCloud Private Relay, QUIC (y compris HTTP/3) et Secure RTCP. Restrictions de version : requiert la version7.2.10 ou ultérieure /7.6.1 ou ultérieure / 7.7.0 ou ultérieure.
Configurer la récupération automatique de Firewall Threat Defense en cas d'épuisement des blocs à l'aide de FlexConfig.	Pour réduire les temps d'arrêt dus aux interruptions de services, un nouveau gestionnaire de défaillances supervise l'épuisement des blocs et, si nécessaire, recharge automatiquement les périphériques. Dans le cadre des déploiements à haute disponibilité, cela déclenche le basculement. La supervision des défaillances est automatiquement activée sur les périphériques nouveaux et mis à niveau. Pour la désactiver, utilisez FlexConfig. Commandes FlexConfig nouvelles ou modifiées : • **fault-monitor block-depletion recovery-action** {**none** | **reload**} La définition de **none** désactive le rechargement automatique, mais ne désactive pas la supervision des défaillances. Pour cela, utilisez **no fault-monitoring**. • **fault-monitor block-depletion monitor-interval** *seconds* Commandes nouvelles ou modifiées de l'interface de ligne de commande de défense contre les menaces : **show fault-monitor block-depletion** {**status** | **statistics**}
Dépannage	
L'outil de profilage de CPU comprend des statistiques d'identification des applications.	L'outil de profilage de CPU comprend désormais des statistiques d'identification des applications. Après avoir activé le profilage de CPU (**cpu profile activate**), vous pouvez désormais voir les ressources utilisées pour le traitement du trafic d'applications spécifiques. Commandes CLI nouvelles ou modifiées : **system support appid-cpu-profiling status**, **system support appid-cpu-profiling dump** Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Nouvelles statistiques sur les flux IP.	Lors de la collecte de statistiques sur les flux IP à partir d'un périphérique Firewall Threat Defense sous la direction de Centre d'assistance technique Cisco (TAC), un nouveau paramètre **all** enregistre des statistiques supplémentaires dans le fichier spécifié : port, protocole, application, latence cumulée et durée d'inspection. Commandes nouvelles ou modifiées : **system support flow-ip-profiling start flow-ip-file** *nom de fichier* **all** {**enable** | **disable**} Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Sécurité et renforcement	

Caractéristiques	Description
Limitation du privilège utilisateur Basic (de base) de l'interface de ligne de commande de Threat Defense.	La portée du privilège utilisateur Basic (de base) de l'interface de ligne de commande de Threat Defense est désormais limitée aux commandes suivantes : dig, ping, traceroute. Si vous avez créé des utilisateurs dotés du privilège Basic (de base), déterminez si vous devez leur accorder le privilège Config. Vous pouvez modifier le niveau de privilège d'un utilisateur à l'aide de la commande **configure user access**. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
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 7.0.7/7.2.10/7.6.1/ 7.7.0 (ou version ultérieure).

Fonctionnalités de Firewall Threat Defense dans la version 7.6.x

Tableau 2 : Fonctionnalités de Firewall Threat Defense dans la version 7.6.x

Caractéristiques	Description
Caractéristiques de la plateforme	
Secure Firewall 1200.	Nous avons introduit Cisco Secure Firewall 1200, qui comprend les modèles suivants : • Cisco Secure Firewall 1210CX, avec 8 ports 1000BASE-T • Cisco Secure Firewall 1210CP, avec 8 ports 1000BASE-T, où les ports 1/5-1/8 prennent en charge l'alimentation par Ethernet (PoE) • Secure Firewall 1220CX, avec 8 ports 1000BASE-T et deux ports SFP+ Voir : Guide d'installation du matériel Cisco Secure Firewall CSF-1210CE, CSF-1210CP et CSF-1220CX

Caractéristiques	Description
Désactiver le port USB-A du panneau avant sur Firepower 1000 et Secure Firewall 3100.	Vous pouvez maintenant désactiver le port USB-A du panneau avant sur Firepower 1000 et Secure Firewall 3100. Par défaut, le port est activé. Commandes CLI nouvelles ou modifiées : **system support usb show**, **system support usb port disable**, **system support usb port enable** Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Prise en charge d'IMDSv2 pour les déploiements AWS.	Threat Defense Virtual pour AWS prend désormais en charge la version 2 du service de données d'instance (IMDSv2), une amélioration de la sécurité par rapport à IMDSv1. Lorsque vous activez le service de métadonnées d'instance sur AWS, le mode IMDSv2 Optional (facultatif) correspond à l'option par défaut, mais nous vous recommandons de choisir IMDSv2 Required (requis). Nous vous recommandons également de changer vos instances mises à niveau. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Fin du soutien : Firepower 2110, 2120, 2130, 2140.	Vous ne pouvez pas exécuter la version 7.6et ultérieures sur le périphérique Firepower 2110, 2120, 2130 ou 2140.
Fonctionnalités de pare-feu et IPS	
Améliorations des performances de recherche de groupes d'objets.	La recherche de groupe d'objets est désormais plus rapide et utilise moins de ressources. Nouvelles commandes CLI : **clear asp table network-object**, **show asp table network-group** Commentaires CLI modifiés (sortie améliorée) : **debug acl logs**, **packet-tracer**, **show access-list**, **show object-group** Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Fonctions d'administration et de dépannage	
Mises à jour des exigences d'accès Internet pour le filtrage des URL.	**Incidence sur la mise à niveau. Le système se connecte à de nouvelles ressources.** Le système requiert désormais un accès à *.talos.cisco.com pour les données de filtrage d'URL. Il ne nécessite plus l'accès à regsvc.sco.cisco.com.
Mises à jour des exigences d'accès Internet pour les mises à jour des règles de prévention des intrusions.	**Incidence sur la mise à niveau. Le système se connecte à de nouvelles ressources.** Le système a maintenant besoin d'accéder aux ressources suivantes pour télécharger les règles de prévention des intrusions : • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com Il ne nécessite plus l'accès à talosintelligence.com.

Caractéristiques	Description
Traduction en français canadien pour le gestionnaire de périphériques de pare-feu.	Le gestionnaire de périphériques de pare-feu comprend une version en français canadien, en plus de l'anglais, du chinois, du japonais et du coréen. Vous devez sélectionner le français canadien comme langue du navigateur. Vous ne pouvez pas voir la version française en sélectionnant un autre type de français. Voir : Affichage des pages dans d'autres langues que l'anglais
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 7.0.7/7.2.10/7.6.1/ 7.7.0 (ou version ultérieure).
Fonctionnalités de performance	
Accélération matérielle du chiffrement DTLS 1.2 pour Cisco Secure Firewall 3100.	Cisco Secure Firewall 3100 prend désormais en charge l'accélération cryptographique et l'optimisation de sortie DTLS 1.2, ce qui améliore le débit du trafic chiffré et déchiffré DTLS. Cette fonctionnalité est automatiquement activée sur les périphériques nouveaux et mis à niveau. Pour la désactiver, utilisez FlexConfig. Commandes FlexConfig nouvelles ou modifiées : **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls** Voir : Configuration avancée

Fonctionnalités de Firewall Device Manager dans la version 7.4.x

Remarque La prise en charge des fonctionnalités de la version 7.4 de Firewall Device Manager commence à la version 7.4.1. Cela est dû au fait que la version 7.4.0 n'est disponible sur aucune plateforme prenant en charge le gestionnaire d'appareils.

Tableau 3 : Fonctionnalités de Firewall Device Manager dans la version 7.4.x

Caractéristiques	Description
Caractéristiques de la plateforme	

Caractéristiques	Description
Modules de réseau pour Cisco Secure Firewall 3130 et 3140.	Nous avons présenté ces modules de réseau pour Cisco Secure Firewall 3130 et 3140 : • Module de réseau 2 ports 100G QSFP+ (FPR3K-XNM-2X100G) Voir : Guide d'installation matérielle de Cisco Secure Firewall 3110, 3120, 3130 et 3140
Fonctionnalités de pare-feu et IPS	
Détection et masquage de données sensibles	**Incidence sur la mise à niveau. Les nouvelles règles des politiques par défaut prennent effet.** Des données sensibles telles que les numéros de sécurité sociale, les numéros de carte de crédit, les courriels, etc. peuvent être divulguées sur Internet, intentionnellement ou accidentellement. La détection des données sensibles est utilisée pour détecter et générer des événements sur d'éventuelles fuites de données sensibles et ne génère des événements que s'il y a un transfert d'une quantité importante de renseignements personnels identifiables (PII). La détection des données sensibles peut masquer les renseignements nominatifs dans la sortie des événements, en utilisant des modèles intégrés. La désactivation du masquage des données n'est pas prise en charge. Nécessite Snort 3.
Fonctionnalités du VPN	
Décharge de flux IPsec sur l'interface de boucle avec retour VTI pour Secure Firewall 3100.	**Incidence sur la mise à niveau. Les connexions admissibles commencent à être déchargées.** Sur le pare-feu Secure Firewall 3100, les connexions IPsec admissibles via l'interface de boucle avec retour VTI sont maintenant déchargées par défaut. Auparavant, cette fonctionnalité n'était prise en charge que sur les interfaces physiques. Cette fonctionnalité est automatiquement activée par la mise à niveau. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande **flow-offload-ipsec**.
Fonctionnalités de l'interface	

Caractéristiques	Description
Interfaces de gestion et de dépistage fusionnées.	**Incidence sur la mise à niveau. Fusionner les interfaces après la mise à niveau.** Pour les nouveaux périphériques utilisant la version 7.4 ou ultérieure, vous ne pouvez pas utiliser l'ancienne interface de dépistage. Seule l'interface de gestion fusionnée est disponible. Si vous avez effectué la mise à niveau vers la version 7.4 ou une version ultérieure et que vous n'aviez aucune configuration pour l'interface de dépistage, les interfaces fusionneront automatiquement. Si vous avez effectué la mise à niveau vers la version 7.4 ou une version ultérieure et que vous disposez d'une configuration pour l'interface de dépistage, vous avez le choix de fusionner les interfaces manuellement ou vous pouvez continuer à utiliser l'interface de dépistage distincte. Notez que la prise en charge de l'interface de dépistage sera supprimée dans une version ultérieure. Vous devez donc planifier la fusion des interfaces dès que possible. Le mode fusionné modifie également le comportement du trafic AAA pour utiliser la table de routage des données par défaut. La table de routage destinée à la gestion uniquement ne peut désormais être utilisée que si vous spécifiez l'interface de gestion uniquement (y compris la gestion) dans la configuration. Écrans nouveaux ou modifiés : • Interface **Devices** > **(Périphériques)** > **Interfaces** > **(interfaces)** > **Management** (gestion) • (déplacé vers Interfaces) **System Settings** > **(paramètres système)** > **Management Interface** > **(interfaces de gestion)** • **Devices** > **(Périphériques)** > **Interfaces** > **(interfaces)** > **Merge Interface action needed** > **(Action de fusion de l'interface nécessaire)** > **Management Interface Merge** > **(Fusionner l'interface de gestion)** Commandes nouvelles ou modifiées : **show management-interface convergence**
Déploiement sans interface de dépistage sur la solution de défense contre les menaces virtuelles pour Azure et GCP.	Vous pouvez désormais déployer, sans l'interface de dépistage, sur Threat Defense Virtual pour Azure et GCP. Les déploiements Azure nécessitent toujours au moins deux interfaces de données, mais GCP exige que vous remplaciez l'interface de dépistage par une interface de données, pour une nouvelle exigence minimale de trois. (Auparavant, les déploiements virtuels de défense contre les menaces nécessitaient une interface de gestion, une interface de dépistage et au moins deux interfaces de données.) Restrictions : Cette fonctionnalité n'est prise en charge que pour les nouveaux déploiements. Elle n'est pas prise en charge pour les périphériques mis à niveau. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Ensembles en ligne pour Série Firepower 1000, Firepower 2100 et Secure Firewall 3100.	Vous pouvez configurer des ensembles en ligne sur les périphériques Série Firepower 1000, Firepower 2100 et Secure Firewall 3100. Nous avons ajouté l'onglet des ensembles en ligne à la page Interface.
Caractéristiques de la licence	

Caractéristiques	Description
Modifications des noms de licences et prise en charge de la licence de l'opérateur.	Les licences ont été renommées : • Threat est désormais IPS • Malware est désormais Malware Defense • Base est maintenant Essentials • AnyConnect Apex est désormais Secure Client Premier • AnyConnect Plus est désormais Secure Client Advantage • AnyConnect VPN Only est désormais Secure Client VPN Only En outre, vous pouvez désormais appliquer la licence Carrier, qui vous permet de configurer les inspections GTP/GPRS, Diameter, SCTP et M3UA. Utilisez FlexConfig pour configurer ces fonctionnalités. Voir : Obtenir les licences du système
Fonctions d'administration et de dépannage	
Serveur NTP par défaut mis à jour.	**Incidence sur la mise à niveau. Le système se connecte à de nouvelles ressources.** Les serveurs NTP par défaut sont passés de sourcefire.pool.ntp.org à time.cisco.com. Pour utiliser un autre serveur NTP, sélectionnez le **périphérique**, puis cliquez sur **Time Services** (services de temps) dans le panneau **System Settings** (Paramètres du système).
Serveurs SAML pour l'accès utilisateur de gestion HTTPS.	Vous pouvez configurer un serveur SAML pour fournir une authentification externe pour l'accès de gestion HTTPS. Vous pouvez configurer les utilisateurs externes avec les types d'autorisation d'accès suivants : administrateur, administrateur de l'audit, administrateur de la cryptographie, utilisateur en lecture-écriture, utilisateur en lecture seule. Vous pouvez utiliser la carte d'accès commun (CAC) pour vous connecter lorsque vous utilisez un serveur SAML. Nous avons mis à jour la configuration de l'objet de la source d'identité SAML et la page d'**accès à la gestion** > **des** > **paramètres système** pour les accepter.
Détecter les incompatibilités de configuration dans les paires à haute disponibilité de la défense contre les menaces.	Vous pouvez désormais utiliser l'interface de ligne de commande pour détecter les incompatibilités de configuration dans les paires à haute disponibilité de la défense contre les menaces. Commandes CLI nouvelles ou modifiées : **show failover config-sync error**, **show failover config-sync stats** Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Capturer les paquets abandonnés avec le pare-feu Secure Firewall 3100.	Les pertes de paquets résultant d'incohérences dans le tableau d'adresses MAC peuvent avoir une incidence sur vos capacités de débogage. Le pare-feu Secure Firewall 3100 peut désormais capturer ces paquets abandonnés. Commandes CLI nouvelles ou modifiées : [**drop** { **disable** | **mac-filter** }] dans la commande **capture**. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Caractéristiques	Description
Les mises à niveau de micrologiciel incluses dans les mises à niveau FXOS.	**Incidence sur la mise à niveau du châssis ou de FXOS. Les mises à niveau de micrologiciel entraînent un redémarrage supplémentaire.** Pour les périphériques Firepower 4100/9300, les mises à niveau de FXOS vers la version 2.14.1+ comprennent désormais des mises à niveau des micrologiciels. Si un composant du micrologiciel sur le périphérique est plus ancien que celui inclus dans l'offre groupée FXOS, la mise à niveau FXOS met également à jour le micrologiciel. Si le micrologiciel est mis à niveau, le périphérique redémarre deux fois, une fois pour FXOS et une autre pour le micrologiciel. Comme pour les mises à niveau de logiciels et de systèmes d'exploitation, n'apportez pas et ne déployez pas de modifications de configuration pendant la mise à niveau du micrologiciel. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau du micrologiciel. Voir : CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS
Récupération rapide après une défaillance du plan de données pour les périphériques Firepower 1000/2100 et 4100/9300.	Lorsque le processus du plan de données des périphériques Firepower 1000/2100 ou Firepower 4100/9300 plante, le système recharge le processus au lieu de redémarrer le périphérique. Le rechargement du plan de données redémarre également d'autres processus, y compris Snort. Si le plan de données tombe en panne pendant le démarrage, le périphérique suit la séquence normale de rechargement/redémarrage; cela évite une boucle de rechargement. Cette fonctionnalité est activée par défaut pour les périphériques nouveaux et mis à niveau. Pour la désactiver, utilisez FlexConfig. Commandes CLI ASA nouvelles ou modifiées : **data-plane quick-reload**, **show data-plane quick-reload status** Commandes nouvelles ou modifiées de l'interface de ligne de commande de défense contre les menaces : **show data-plane quick-reload status** Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall et Référence des commandes de la série Cisco Secure Firewall ASA.

Fonctionnalités de la version 7.3.x de Firewall Device Manager

Tableau 4 : Fonctionnalités de la version 7.3.x de Firewall Device Manager

Caractéristiques	Description
Caractéristiques de la plateforme	
Secure Firewall 3105.	Nous avons présenté le pare-feu Secure Firewall 3105. Version minimale de Threat Defense : 7.3.1

Caractéristiques	Description
Modules de réseau pour Secure Firewall 4100.	Nous avons présenté ces modules de réseau pour le périphérique Firepower 4100 : • Module réseau 100G à 2 ports (FPR4K-NM-2X100G) Plateformes prises en charge : Firepower 4112, 4115, 4125, 4145
Prise en charge des voyants DEL du système ISA 3000 pour l'arrêt.	Retour de la prise en charge de cette fonctionnalité. Lorsque vous éteignez l'ISA 3000, le voyant DEL System s'éteint. Attendez au moins 10 secondes avant de couper l'alimentation du périphérique. Cette fonctionnalité a été introduite dans la version 7.0.5, mais a été temporairement obsolète dans les versions 7.1 à 7.2.
Nouvelles formes de calcul pour la défense contre les menaces virtuelles pour OCI.	Threat Defense Virtual pour OCI prend en charge les formes de calcul suivantes : • Intel VM.DenseIO2.8 • Intel VM.StandardB1.4 • Intel VM.StandardB1.8 • Intel VM.Standard1.4 • Intel VM.Standard1.8 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Notez qu'il n'est plus possible de commander les formes de calcul VM.Standard2.4 et VM.Standard2.8 depuis février 2022. Si vous déployez la version 7.3+, nous vous recommandons une forme de calcul différente. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Fin du soutien : Firepower 4110, 4120, 4140, 4150.	Vous ne pouvez pas exécuter les versions 7.3 et ultérieures sur le périphérique Firepower 4110, 4120, 4140 ou 4150.
Fin du soutien : Firepower 9300 : modules SM-24, SM-36 et SM-44.	Vous ne pouvez pas exécuter la version 7.3+ sur le périphérique Firepower 9300 avec les modules SM-24, SM-36 ou SM-44.
Firepower 1010E ne prend pas en charge la version 7.3.	Le Firepower 1010E, qui a été introduit dans la version 7.2.3, ne prend pas pris en charge la version 7.3. L'assistance revient dans la version 7.4. Vous ne pouvez pas mettre à niveau un Firepower 1010E de la version 7.2.x vers la version 7.3 et vous ne devez pas non plus procéder à une recréation d'image. Si vous avez un périphérique Firepower 1010E exécutant la version 7.3, effectuez une nouvelle image avec une version prise en charge.
Fonctionnalités de pare-feu et IPS	

Caractéristiques	Description
Prise en charge de TLS 1.3 dans les politiques de déchiffrement SSL et comportement configurable pour les connexions non déchiffrables.	**Incidence sur la mise à niveau.** Vous pouvez configurer des règles de déchiffrement SSL pour le trafic TLS 1.3. La prise en charge de TLS 1.3 est disponible lors de l'utilisation de Snort 3 uniquement. Vous pouvez également configurer un comportement autre que celui par défaut pour les connexions non déchiffrables. Si vous utilisez Snort 3, lors de la mise à niveau, TLS 1.3 est automatiquement sélectionné pour toutes les règles qui ont toutes les versions SSL/TLS sélectionnées; sinon, TLS 1.3 n'est pas sélectionné. Le même comportement se produit si vous passez de Snort 2 à Snort 3. Nous avons ajouté TLS 1.3 comme option sous l'onglet Advanced (avancé) de la boîte de dialogue d'ajout/modification de règle. Nous avons également repensé les paramètres de politique de déchiffrement SSL pour inclure la possibilité d'activer le déchiffrement TLS 1.3 et de configurer les actions de connexion non déchiffrables. Consultez : Critères avancés pour les règles de déchiffrement SSL et Configuration des paramètres de trafic avancés et non déchiffrables
Recherche affinée par filtrage d'URL.	Vous pouvez désormais définir explicitement comment les recherches par filtrage d'URL se produisent. Vous pouvez choisir d'utiliser la base de données d'URL locale uniquement, la base de données locale et la recherche dans le nuage, ou la recherche dans le nuage uniquement. Nous avons augmenté les options de paramètres système de filtrage d'URL. Consultez : Configurer les préférences de filtrage d'URL
Fonctionnalités de l'interface	
Prise en charge d'IPv6 pour les appliances virtuelles.	Threat Defense Virtual prend désormais en charge IPv6 dans les environnements suivants : • AWS • Azure • KVM • VMware Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Client DHCPv6.	Vous pouvez maintenant obtenir une adresse IPv6 à partir de DHCPv6. Écrans nouveaux ou modifiés : **Device (périphérique)** > **Interfaces** > **Edit Interface (modifier l'interface)** > **Advanced (avancé)** Consultez : Configurer les options d'interface avancées
Fonctions d'administration et de dépannage	

Caractéristiques	Description
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
Ignorer l'autorité de certification vérifiant les certificats de confiance.	Vous pouvez ignorer la vérification si vous devez installer un certificat d'autorité de certification (CA) locale en tant que certificat d'autorité de certification de confiance. Nous avons ajouté l'option **Skip CA Certificate Check (ignorer la vérification de certificat de CA)** lors du téléversement des certificats CA de confiance.

Caractéristiques	Description
Ensemble de mise à niveau et d'installation combinées pour Cisco Secure Firewall 3100.	**Incidence de la recréation d'image.** Dans la version 7.3, nous avons combiné l'ensemble d'installation et de mise à niveau de Firewall Threat Defense pour Secure Firewall 3100, comme suit : • Paquet d'installation des versions 7.1 à 7.2 : cisco-ftd-fp3k.*version*.SPA • Paquet de mise à niveau, versions 7.1 à 7.2 : Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Ensemble combiné version 7.3+ : Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Bien que vous puissiez mettre à niveau la Firewall Threat Defense sans problème, vous ne pouvez pas restaurer l'image des anciennes versions de Firewall Threat Defense et des versions ASA directement vers la version 7.3 ou versions ultérieures de Firewall Threat Defense Cela est dû à une mise à jour de ROMMON requise par le nouveau type d'image. Pour recréer l'image de ces anciennes versions, vous devez « passer par » ASA 9.19+, qui est pris en charge avec l'ancienne ROMMON, mais aussi les mises à jour de la nouvelle ROMMON. Il n'y a pas de programme de mise à jour de ROMMON distinct. Pour accéder à la version 7.3+ de Firewall Threat Defense, vos options sont les suivantes : • Mise à niveau de la version de Firewall Threat Defense 7.1 ou 7.2 : utilisez le processus de mise à niveau normal. Consultez le guide de mise à niveau approprié. • Recréation de l'image à partir de la version 7.1 ou 7.2 de Firewall Threat Defense : en effectuant une recréation d'image vers ASA 9.19 et versions ultérieures d'abord, puis vers la version de Firewall Threat Defense 7.3 et versions ultérieures. voir *Défense contre les menaces→ASA : Firepower 1000, 2100 ; Secure Firewall 3100*, puis *ASA→Threat Defense : Firepower 1000, 2100 Mode l'appareil; Secure Firewall 3100* dans Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense. • Recréation d'image à partir d'ASA 9.17 ou 9.18 : mise à niveau vers ASA 9.19 et versions ultérieures d'abord, puis recréation d'image vers la version de Firewall Threat Defense 7.3 et versions ultérieures. Reportez-vous à Guide de mise à niveau de Cisco Secure Firewall ASA, puis à *ASA→Threat Defense : Firepower 1000, 2100 Mode l'appareil; Secure Firewall 3100* dans Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense. • Recréation d'image à partir de la Firewall Threat Defense version 7.3 et versions ultérieures : utilise le processus normal de recréation d'image. Voir *Recréer l'image du système avec une nouvelle version du logiciel* dans Guide de dépannage Cisco FXOS pour le Firepower 1000/2100 et Secure Firewall 1200/3100/4200 avec Firepower Threat Defense.

Caractéristiques	Description
API REST Firewall Threat Defense version 6.4 (v6).	L'API REST Cisco Firewall Threat Defense pour la version logicielle 7.3 est la version 6.4. Vous pouvez utiliser la version v6 dans les URL d'API ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. Notez que l'élément de chemin de version d'URL pour la version 6.4 est le même que pour toutes les versions 6.x : 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 Firepower Device Manager, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**. Voir : Guide de Cisco Secure Firewall Threat Defense REST API

Fonctionnalités Firewall Device Manager dans la version 7.2.x

Tableau 5 : Fonctionnalités Firewall Device Manager dans la version 7.2.x

Fonctionnalités	Description
Caractéristiques de la plateforme	
Firepower 1010E.	Nous avons lancé le périphérique Firepower 1010E, qui ne prend pas en charge l'alimentation par Ethernet (PoE). Version minimale de Threat Defense : 7.4.1 Voir Câblage du Firepower 1010
Threat Defense Virtual pour VMware sur VMware vSphere/VMware ESXi 8.0.	Vous pouvez maintenant déployer Threat Defense Virtual pour VMware sur VMware vSphere/VMware ESXi 8.0. Version minimale de Threat Defense : versions 7.2.9, 7.4.2 Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Threat Defense Virtual pour GCP.	Vous pouvez maintenant utiliser le gestionnaire d'appareil pour configurer Threat Defense Virtual pour GCP. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Threat Defense Virtual pour Megaport.	Vous pouvez maintenant utiliser le gestionnaire d'appareil pour configurer Threat Defense Virtual pour Megaport (Megaport Virtual Edge). La haute disponibilité est prise en charge. Défense minimale contre les menaces : 7.2.8 Autres restrictions de version : au départ, vous ne pourrez peut-être pas déployer les versions 7.3.x ou 7.4.x. Déployez plutôt les versions 7.2.8–7.2.x et effectuez la mise à niveau. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual

Fonctionnalités	Description
Modules de réseau pour Cisco Secure Firewall 3100.	Nous avons présenté ces modules de réseau pour Cisco Secure Firewall 3130 : • Module de réseau à 6 ports 1G SFP, SX (multimode) (FPR-X-NM-6X1SX-F) • Module de réseau à 6 ports 10G SFP, SR (multimode) (FPR-X-NM-6X10SR-F) • Module de réseau à 6 ports 10G SFP, LR (mode unique) (FPR-X-NM-6X10LR-F) • Module de réseau à 6 ports 25G SFP, SR (multimode) (FPR-X-NM-X25SR-F) • Module de réseau à 6 ports 25G, LR (mode unique) (FPR-X-NM-6X25LR-F) • Module de réseau à 8 ports 1G, RJ45 (cuivre) (FPR-X-NM-8X1G-F) Défense minimale contre les menaces : 7.2.1
Pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Threat Defense Virtual pour KVM.	Nous prenons désormais en charge le pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Threat Defense Virtual pour KVM. Défense minimale contre les menaces : 7.2.1 Voir : Déployer Threat Defense Virtual sur KVM
Prise en charge d'ISA 3000 pour l'arrêt.	Demande de soutien concernant l'arrêt de l'ISA 3000. Cette fonctionnalité a été introduite dans la version 7.0.2, mais a été temporairement obsolète dans la version 7.1.
Fonctionnalités de pare-feu et IPS	
La recherche de groupe d'objets est activée par défaut pour le contrôle d'accès.	La commande de configuration de la CLI **object-group-search access-control** est maintenant activée par défaut pour les nouveaux déploiements. Toutefois, si vous effectuez une mise à niveau vers la version 7.2, le paramètre reste activé ou désactivé en fonction de vos paramètres précédents. Si vous configurez la commande à l'aide de FlexConfig, vous devez évaluer si cela est toujours nécessaire. Si vous devez désactiver la fonctionnalité, utilisez FlexConfig pour mettre en œuvre la commande **no object-group-search access-control**. Voir : Référence des commandes de la série Cisco Secure Firewall ASA
Le nombre de règles persiste pendant le redémarrage.	Le redémarrage d'un périphérique ne réinitialise plus le nombre de résultats de règles de contrôle d'accès à zéro. Le nombre de résultats est réinitialisé uniquement si vous effacez activement les compteurs. En outre, les décomptes sont gérés séparément par chaque unité d'une paire ou d'une grappe à haute disponibilité. Vous pouvez utiliser la commande **show rule hits** pour afficher les compteurs cumulés pour la paire ou la grappe à haute disponibilité, ou pour voir le nombre par nœud. Nous avons modifié la commande CLI suivante : .show rule hits Voir : Examiner le nombre de résultats pour les règles
Fonctionnalités du VPN	

Fonctionnalités	Description
Décharge de flux IPsec.	Sur la Secure Firewall 3100, les flux IPsec sont déchargés par défaut. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande **flow-offload-ipsec**. Voir : Décharge de flux IPSec
Fonctionnalités de l'interface	
Prise en charge des ports d'éclatement pour Cisco Secure Firewall 3130 et 3140.	Vous pouvez maintenant configurer quatre ports d'éclatement de 10 Go pour chaque interface de 40 Go sur les Cisco Secure Firewall 3130 et 3140. Écrans nouveaux ou modifiés : **Device (périphérique)** > **Interfaces** Voir : Gérer le module de réseau pour Cisco Secure Firewall 3100
Activation ou désactivation de Cisco Trustsec sur une interface.	Vous pouvez activer ou désactiver Cisco Trustsec sur les interfaces physiques, les sous-interfaces, les interfaces EtherChannel, VLAN, les interfaces de gestion ou BVI, qu'elles soient nommées ou non. Par défaut, Cisco Trustsec est activé automatiquement lorsque vous nommez une interface. Nous avons ajouté l'attribut **Propagate Security Group Tag (propager la balise de groupe de sécurité)** aux boîtes de dialogue de configuration d'interface et l'attribut **ctsEnabled** aux différentes API d'interface. Voir : Configurer les options avancées
Caractéristiques de la licence	
Prise en charge de la réservation de licence permanente pour ISA 3000.	ISA 3000 prend désormais en charge la réservation de licences permanentes universelles pour les clients approuvés. Voir : Application des licences permanentes dans les réseaux isolés
Fonctions d'administration et de dépannage	
Capacité de forcer le déploiement complet.	Lorsque vous déployez des modifications, le système déploie normalement les modifications apportées depuis le dernier déploiement réussi. Toutefois, si vous rencontrez des problèmes, vous pouvez choisir de forcer un déploiement complet, ce qui actualise complètement la configuration sur le périphérique. Nous avons ajouté l'option **Apply Full Deployment (appliquer le déploiement complet)** à la boîte de dialogue de déploiement. Voir : Déployer vos modifications

Fonctionnalités	Description
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
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 7.0.7/7.2.10/7.6.1/ 7.7.0 (ou version ultérieure).
API REST Threat Defense, version 6.3 (v6).	L'API REST Cisco Firewall Threat Defense pour la version logicielle 7.2 est la version 6.3. Vous pouvez utiliser la version v6 dans les URL d'API ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. Notez que l'élément de chemin de version d'URL pour la version 6.3 est le même que pour les versions 6.0, 6.1 et 6.2 : 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 Firepower Device Manager, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**. Voir : Guide de Cisco Secure Firewall Threat Defense REST API

Fonctionnalités FDM dans la version 7.1.x

Tableau 6 : Fonctionnalités FDM dans la version 7.1.x

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

Fonctionnalités	Description
FTDv pour les instances AWS.	FTDv pour AWS ajoute la prise en charge de ces instances : • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv pour les instances Azure.	FTDv pour Azure ajoute la prise en charge de ces instances : • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2
Fin de la prise en charge pour ASA 5508-X et 5516-X. La dernière version prise en charge est Cisco Firewall Threat Defense 7.0.	Vous ne pouvez pas installer Cisco Firewall Threat DefenseCisco Firewall Threat Defense 7.1 sur un ASA 5508-X ou 5516-X. La dernière version prise en charge pour ces modèles est Cisco Firewall Threat Defense 7.0.

Fonctionnalités	Description
Fonctionnalités de pare-feu et IPS	
Configuration de la politique d'analyse de réseau (NAP) pour Snort 3.	Vous pouvez utiliser Firepower Device Manager pour configurer la politique d'analyse de réseau (NAP) lors de l'exécution de Snort 3. Les politiques d'analyse de réseau contrôlent l'inspection prétraitement du trafic. Les inspecteurs préparent le trafic à une inspection plus approfondie en le normalisant et en relevant les anomalies de protocole. Vous pouvez sélectionner la NAP à utiliser pour tout le trafic et personnaliser les paramètres afin qu'ils fonctionnent de manière optimale avec le trafic de votre réseau. Vous ne pouvez pas configurer la NAP lorsque vous exécutez Snort 2. Nous avons ajouté la politique d'analyse de réseau à la boîte de dialogue des paramètres **Policies (politiques)** > **Intrusion**, avec un éditeur JSON intégré pour permettre les modifications directes, et d'autres fonctionnalités pour vous permettre de charger les remplacements ou de télécharger ceux que vous créez.
Prise en charge de la NAT manuelle pour les objets de nom de domaine complet (FQDN) en tant que destination de la traduction.	Vous pouvez utiliser un objet de réseau FQDN, par exemple spécifiant www.exemple.com, comme adresse de destination traduite dans les règles NAT manuelles. Le système configure la règle en fonction de l'adresse IP renvoyée par le serveur DNS.
Amélioration de l'authentification active pour les règles d'identité.	Vous pouvez configurer l'authentification active pour que les règles de politique d'identité redirigent l'authentification de l'utilisateur vers un nom de domaine complet (FQDN) plutôt que l'adresse IP de l'interface par laquelle la connexion de l'utilisateur entre dans le périphérique. Le nom de domaine complet doit mener à l'adresse IP de l'une des interfaces du périphérique. En utilisant un nom de domaine complet, vous pouvez attribuer un certificat pour l'authentification active que le client reconnaîtra, évitant ainsi que les utilisateurs reçoivent un avertissement de certificat non fiable lorsqu'ils sont redirigés vers une adresse IP. Le certificat peut préciser un nom de domaine complet, un nom de domaine complet générique ou plusieurs noms de domaine complets sous les autres noms de l'objet (SAN) du certificat. Nous avons ajouté l'option **Redirect to Host Name (rediriger vers le nom d'hôte)** dans les paramètres de politique d'identité.
Fonctionnalités du VPN	
Homologue de secours distants pour le VPN de site à site.	Vous pouvez configurer une connexion VPN de site à site pour inclure des homologues de secours distants. Si l'homologue distant principal n'est pas disponible, le système tentera de rétablir la connexion VPN en utilisant l'un des homologues de secours. Vous pouvez configurer des clés ou des certificats prépartagés distincts pour chaque homologue de secours. Les homologues de secours ne sont pris en charge que pour les connexions basées sur des politiques et ne sont pas disponibles pour les connexions basées sur le routage (interface de tunnel virtuel). Nous avons mis à jour l'assistant VPN de site à site pour inclure la configuration des homologues de secours.

Fonctionnalités	Description
Gestion des mots de passe pour le VPN d'accès à distance (MSCHAPv2).	Vous pouvez activer la gestion des mot de passe pour le VPN d'accès à distance. Cela permet à AnyConnect d'inviter l'utilisateur à modifier un mot de passe expiré. Sans la gestion des mot de passe, les utilisateurs doivent modifier les mots de passe expirés directement avec le serveur AAA, et AnyConnect n'invite pas l'utilisateur à changer de mot de passe. Pour les serveurs LDAP, vous pouvez également définir une période d'avertissement pour informer les utilisateurs de la prochaine expiration du mot de passe. Nous avons ajouté l'option Enable Password Management (activer la gestion des mots de passe) aux paramètres d'authentification pour les profils de connexion VPN d'accès à distance.
Navigateur externe AnyConnect VPN SAML.	Lorsque vous utilisez SAML comme méthode d'authentification principale pour un profil de connexion VPN d'accès à distance, vous pouvez choisir que le client AnyConnect utilise le navigateur local du client au lieu du navigateur intégré à l'AnyConnect pour effectuer l'authentification Web. Cette option active la connexion unique (SSO) entre votre authentification VPN et d'autres connexions d'entreprise. Choisissez également cette option si vous souhaitez prendre en charge des méthodes d'authentification web, telles que l'authentification biométrique, qui ne peuvent pas être exécutées dans le navigateur intégré. Nous avons mis à jour l'assistant de profil de connexion VPN d'accès à distance pour vous permettre de configurer l'**expérience de connexion SAML**.
Fonctions d'administration et de dépannage	
Prise en charge du système de nom de domaine dynamique (DDNS) pour la mise à jour du nom de domaine complet (FQDN) aux mappages d'adresses IP pour les interfaces du système.	**Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau.** Vous pouvez configurer le DDNS pour les interfaces du système afin d'envoyer des mises à jour dynamiques aux serveurs DNS. Cela permet de garantir que les FQDN définis pour les interfaces sont résolus vers la bonne adresse, ce qui facilite l'accès des utilisateurs au système à l'aide d'un nom d'hôte plutôt que d'une adresse IP. Cela est particulièrement utile pour les interfaces qui obtiennent leurs adresses en utilisant DHCP, mais c'est également utile pour les interfaces à adresse statique. Après la mise à niveau, si vous avez utilisé FlexConfig pour configurer DDNS, vous devez refaire votre configuration à l'aide de Firepower Device Manager ou de l'API Cisco Firewall Threat Defense et supprimer l'objet DDNS FlexConfig de la politique FlexConfig avant de pouvoir déployer de nouveau les modifications. Si vous configurez DDNS à l'aide de Firepower Device Manager, puis passez à la gestion par Firewall Management Center, la configuration DDNS est conservée pour que Firewall Management Center puisse trouver le système en utilisant le nom DNS. Dans Firepower Device Manager, nous avons ajouté la page **System Settings (paramètres système)** > **DDNS Service (sevice DDNS)**. Dans l'API Cisco Firewall Threat Defense, nous avons ajouté les ressources DDNSService et DDNSInterfaceSettings.
La commande **dig** remplace la commande **nslookup** dans l'interface de ligne de commande du périphérique.	Pour rechercher l'adresse IP d'un nom de domaine complet (FQDN) dans l'interface de ligne de commande du périphérique, utilisez la commande **dig**. La commande **nslookup** a été supprimée.

Fonctionnalités	Description
Configuration du relais DHCP à l'aide de Firepower Device Manager.	Vous pouvez utiliser Firepower Device Manager pour configurer le relais DHCP. L'utilisation du relais DHCP sur une interface vous permet de diriger les requêtes DHCP vers un serveur DHCP accessible par l'autre interface. Vous pouvez configurer le relais DHCP sur les interfaces physiques, les sous-interfaces, les interfaces VLAN et les canaux EtherChannels. Vous ne pouvez pas configurer le relais DHCP si vous configurez un serveur DHCP sur n'importe quelle interface. Nous avons ajouté la page **System Settings (paramètres systèmes)** > **DHCP** > **DHCP Relay (relais DHCP)** et déplacé DHCP Server (serveur DHCP) sous la nouvelle en-tête DHCP.
Type et taille de clé pour les certificats autosignés dans Firepower Device Manager.	Vous pouvez préciser le type et la taille de clé lors de la génération de nouveaux certificats CA internes et internes autosignés dans Firepower Device Manager. Les types de clés comprennent RSA, ECDSAA et EDDSA. Les tailles autorisées varient selon le type de clé. Nous vous avertissons désormais si vous chargez un certificat dont la taille de clé est inférieure à la longueur minimale conseillée. Il existe également un filtre de recherche prédéfini pour les clés faibles afin de vous aider à trouver les certificats faibles, que vous devriez remplacer si possible.
Restrictions de validation d'utilisation pour les certificats CA de confiance.	Vous pouvez spécifier si un certificat CA de confiance peut être utilisé pour valider certains types de connexions. Vous pouvez autoriser ou empêcher la validation du serveur SSL (utilisé par le DNS dynamique), du client SSL (utilisé par le VPN d'accès à distance), du client IPsec (utilisé par le VPN de site à site) ou d'autres fonctionnalités qui ne sont pas gérées par la plateforme d'inspection Snort, comme LDAPS. L'objectif principal de ces options est de vous empêcher d'établir des connexions VPN, car elles peuvent être validées par rapport à un certificat particulier. Nous avons ajouté **Validation Usage (utilisation de la validation)** comme propriété pour les certificats CA de confiance.
Génération du mot de passe **admin** dans Firepower Device Manager.	Lors de la configuration initiale du système dans Firepower Device Manager ou lorsque vous modifiez le mot de passe **admin** par Firepower Device Manager, vous pouvez désormais cliquer sur un bouton pour générer un mot de passe aléatoire de 16 caractères.
Temps de démarrage et état de compilation tmatch.	La commande **show version** comprend maintenant des renseignements sur le temps nécessaire pour démarrer le système. Notez que plus la configuration est importante, plus il faut de temps pour démarrer le système. La nouvelle commande **show asp rule-engine** affiche l'état de la compilation tmatch. La compilation tmatch est utilisée pour une liste d'accès utilisée comme groupe d'accès, le tableau NAT et certains autres éléments. Il s'agit d'un processus interne qui peut consommer des ressources CPU et affecter les performances pendant son exécution si vous avez des listes de contrôle d'accès et des tableaux NAT très volumineux. Le temps de compilation dépend de la taille de la liste d'accès, du tableau NAT, etc.
Améliorations apportées à la sortie **show access-list element-count**.	La sortie de la commande **show access-list element-count** a été améliorée. Lorsqu'elle est utilisée avec la recherche de groupes d'objets activée, la sortie comprend des détails sur le nombre de groupes d'objets dans le nombre d'éléments. En outre, la sortie **show tech-support** comprend désormais la sortie de **show access-list element-count** et **show asp rule-engine**.

Fonctionnalités	Description
Utilisez Firepower Device Manager pour configurer Cisco Firewall Threat Defense pour la gestion par un Firewall Management Center.	Lorsque vous effectuez la configuration initiale à l'aide de Firepower Device Manager, toutes les configurations d'interface terminées dans Firepower Device Manager sont conservées lorsque vous passez à Firewall Management Center pour la gestion, en plus des paramètres de gestion et d'accès Firewall Management Center. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande Cisco Firewall Threat Defense, seuls les paramètres de gestion et d'accès Firewall Management Center sont conservés (par exemple, la configuration de l'interface interne par défaut n'est pas conservée). Après être passé à Firewall Management Center, vous ne pouvez plus utiliser Firepower Device Managerpour gérer le Cisco Firewall Threat Defense. Écrans nouveau ou modifiés : **System Settings (paramètres système)** > **Management Center (centre de gestion)**
Mettre automatiquement à jour les ensembles d'autorités de certification.	**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
API REST de FTD version 6.2 (v6).	L'API REST Cisco Firewall Threat Defense pour la version logicielle 7.1 est la version 6.2. Vous pouvez utiliser la version v6 dans les URL d'API ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. Notez que l'élément de chemin de version d'URL pour la version 6.2 est le même que pour la version 6.0/1 : v6. Veuillez réévaluer tous les appels existants, car des modifications peuvent avoir été apportées aux modèles de ressources que vous utilisez. Pour ouvrir l'API Explorer et consulter les ressources, connectez-vous à Firepower Device Manager, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**.

Fonctionnalités FDM dans la version 7.0.x

Tableau 7 : Fonctionnalités FDM dans la version 7.0.x

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 Firewall Threat Defense Virtual sur AWS.	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.
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**.

Fonctionnalités	Description
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 Firepower Device Manager, mais les règles ont le même format que les règles téléversées. Firepower Device Manager 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 **Policies (Politiques)** > **Intrusion**, lorsque vous modifiez une politique de prévention des intrusions.
Nouvelles fonctionnalités de Snort 3 pour les systèmes gérés par Firepower Device Manager.	Vous pouvez désormais configurer les fonctionnalités supplémentaires suivantes lors de l'utilisation de Snort 3 comme moteur d'inspection sur un système géré par Firepower Device Manager : • Règles des politiques de contrôle d'accès basées sur le temps (API Firewall Threat Defense 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.
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.

Fonctionnalités	Description
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 *VDB lite*) 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 Firepower Device Manager 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 Firepower Device Manager. Auparavant, vous deviez utiliser l'API Cisco Firewall 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.
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.

Fonctionnalités	Description
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 Cisco Firewall 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 Cisco Firewall Threat Defense, ainsi qu'à équilibrer la charge externe du trafic vers le périphérique Cisco Firewall 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 Cisco Firewall 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 Firepower Device Manager pour configurer les EtherChannels sur l'ISA 3000. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **interfaces** > **EtherChannels**
Caractéristiques de la licence	
Licence progressive en fonction de la performance pour Firewall Threat Defense Virtual.	Le Firewall Threat Defense Virtual 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 Firewall Threat Defense Virtual 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	

Fonctionnalités	Description
Configuration du relais DHCP à l'aide de l'API Cisco Firewall Threat Defense.	**Incidence sur la mise à niveau. Peut empêcher le déploiement après la mise à niveau.** Vous pouvez utiliser l'API Cisco Firewall 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 Cisco Firewall Threat Defense : dhcprelayservices
Traitement de démarrage initial plus rapide et connexion anticipée à Firepower Device Manager.	Le processus de démarrage initial d'un système géré par Firepower Device Managera été amélioré pour le rendre plus rapide. Ainsi, vous n'avez pas besoin d'attenter aussi longtemps après le démarrage du périphérique pour vous connecter à Firepower Device Manager. 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**
Vérification de l'état de préparation à la mise à niveau pour les périphériques gérés par Firepower Device Manager.	Vous pouvez exécuter une vérification de l'état de préparation à la mise à niveau sur un ensemble de mise à niveau Cisco Firewall 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)**.

Fonctionnalités	Description
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
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 7.0.7/7.2.10/7.6.1/ 7.7.0 (ou version ultérieure).
API REST de FTD version 6.1 (v6).	L'API REST Cisco Firewall 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 Firepower Device Manager, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**.

Fonctionnalités FDM dans la version 6.7.x

Tableau 8 : Fonctionnalités FDM dans la version 6.7.x

Caractéristiques	Description
Caractéristiques de la plateforme	
Fin du soutien pour les ASA 5525-X, 5545-X et 5555-X. La dernière version prise en charge est Cisco Firewall Threat Defense 6.6.	Vous ne pouvez pas installer Cisco Firewall Threat Defense 6.7 sur un ASA 5525-X, 5545-X ou 5555-X. La dernière version prise en charge pour ces modèles est Cisco Firewall Threat Defense 6.6.
Fonctionnalités de pare-feu et IPS	
Découverte d'identité du serveur TLS pour la mise en correspondance des règles de contrôle d'accès.	Les certificats TLS sont chiffrés. Pour que le trafic chiffré avec TLS 1.3 corresponde aux règles d'accès qui utilisent le filtrage d'applications ou d'URL, le système doit déchiffrer le certificat TLS 1.3. Nous vous recommandons d'activer la **découverte d'identité de serveur TLS** pour vous assurer que les connexions chiffrées sont associées à la règle de contrôle d'accès appropriée. Le paramètre décrypte uniquement le certificat; la connexion reste chiffrée. Nous avons ajouté le bouton et la boîte de dialogue **Paramètres de contrôle d'accès** (⚙) à la page **Politique** > **Contrôle d'accès**.
Groupe de certificat externe de l'autorité de certification	Vous pouvez maintenant personnaliser la liste des certificats d'autorités de certification de confiance utilisées par la politique de déchiffrement SSL. Par défaut, la politique utilise tous les certificats d'autorité de certification de confiance définis par le système, mais vous pouvez créer un groupe personnalisé pour ajouter d'autres certificats ou remplacer le groupe par défaut par le vôtre, plus limité. Nous avons ajouté des groupes de certificats à la page **Objets** > **Certificats** et modifié les paramètres de la politique de déchiffrement SSL pour permettre la sélection de groupes de certificats.
Séquences de domaine Active Directory pour les règles d'identité passives.	Vous pouvez créer une séquence de domaine, qui est une liste ordonnée de serveurs Active Directory (AD) et de leurs domaines, et les utiliser dans une règle d'identité d'authentification passive. Les séquences de domaine sont utiles si vous prenez en charge plusieurs domaines AD et que vous souhaitez effectuer un contrôle d'accès basé sur l'utilisateur. Au lieu d'écrire des règles distinctes pour chaque domaine AD, vous pouvez écrire une seule règle qui couvre tous vos domaines. L'ordre des domaines AD dans la séquence est utilisé pour résoudre les conflits d'identité éventuels. Nous avons ajouté l'objet de séquence de domaine AD sur la page **Objects (Objets)** > **Identity Sources (Sources d'identité)** et la possibilité de sélectionner l'objet en tant que domaine dans une règle d'identité d'authentification passive. Dans l'API Cisco Firewall Threat Defense, nous avons ajouté la ressource **RealmSequence** et dans la ressource **IdentityRule**, nous avons ajouté la possibilité de sélectionner un objet de séquence de domaine comme domaine pour une règle qui utilise l'authentification passive comme action.

Caractéristiques	Description
Prise en charge de FDM pour les objets de groupe Trustsec security group balise (SGT) et leur utilisation dans les règles de contrôle d'accès.	Dans Cisco Firewall Threat Defense 6.5, la prise en charge de l'API Cisco Firewall Threat Defense a été ajoutée pour configurer les objets de groupe SGT et les utiliser comme critères de correspondance dans les règles de contrôle d'accès. En outre, vous pourriez modifier l'objet d'identité ISE pour être à l'écoute de la rubrique SXP publiée par ISE. Vous pouvez désormais configurer ces fonctionnalités directement dans FDM. Nous avons ajouté un nouvel objet, les groupes SGT, et mis à jour la politique de contrôle d'accès pour permettre leur sélection et leur affichage. Nous avons également modifié l'objet ISE pour inclure la sélection explicite de rubriques auxquelles s'abonner.
Prise en charge de Snort 3.0.	Pour les nouveaux systèmes, Snort 3.0 est le moteur d'inspection par défaut. Si vous effectuez une mise à niveau vers la version 6.7 à partir d'une version antérieure, Snort 2.0 reste le moteur d'inspection actif, mais vous pouvez passer à Snort 3.0. Dans cette version, Snort 3.0 ne prend pas en charge les routeurs virtuels, les règles de contrôle d'accès basées sur le temps ni le déchiffrement des connexions TLS 1.1 ou inférieur. Activez Snort 3.0 uniquement si vous n'avez pas besoin de ces fonctionnalités. Vous pouvez facilement basculer entre Snort 2.0 et 3.0 pour annuler vos modifications si nécessaire. Le trafic sera interrompu chaque fois que vous changez de version. Nous avons ajouté la possibilité de changer de version Snort à la page **Device (Périphériques)** > **Updates (Mises à jour)**, dans le groupe **Intrusion Rules (Règles de prévention des intrusions)**. Dans l'API Cisco Firewall Threat Defense, nous avons ajouté la ressource IntrusionPlicy resource action/toggleinspectionengine. De plus, il y a un nouvel événement d'audit, l'événement de mise à jour des règles, qui indique quelles règles de prévention des intrusions ont été ajoutées, supprimées ou modifiées dans une mise à jour de l'ensemble de règles Snort 3.
Politiques de prévention des intrusions personnalisées pour Snort 3.	Vous pouvez créer des politiques de prévention des intrusions personnalisées lorsque vous utilisez Snort 3 comme moteur d'inspection. En comparaison, vous ne pouvez utiliser les politiques prédéfinies que si vous utilisez Snort 2. Avec les politiques de prévention des intrusions personnalisées, vous pouvez ajouter ou supprimer des groupes de règles et modifier le niveau de sécurité au niveau du groupe pour modifier efficacement l'action par défaut (désactiver, alerte ou supprimer) des règles du groupe. Les politiques de prévention des intrusions Snort 3 vous donnent plus de contrôle sur le comportement de votre système IPS/IDS sans avoir à modifier les politiques de base fournies par Cisco Talos. Nous avons modifié la page **Politiques** > **Intrusion** afin de répertorier les politiques de prévention des intrusions. Vous pouvez en créer de nouveaux et afficher ou modifier les politiques existantes, notamment en ajoutant ou en supprimant des groupes, en affectant des niveaux de sécurité et en modifiant l'action pour les règles. Vous pouvez également sélectionner plusieurs règles et modifier leurs actions. En outre, vous pouvez sélectionner des politiques de prévention des intrusions personnalisées dans les règles de contrôle d'accès.
Plusieurs serveurs syslog pour les incidents d'intrusion	Vous pouvez configurer plusieurs serveurs Syslog pour les politiques de prévention des intrusions. Les incidents d'intrusion sont envoyés à chaque serveur syslog. Nous avons ajouté la possibilité de sélectionner plusieurs objets de serveur Syslog dans la boîte de dialogue des paramètres de politique de prévention des intrusions.

Caractéristiques	Description
La correspondance de réputation d'URL peut inclure des sites dont la réputation est inconnue.	Lorsque vous configurez les critères de correspondance de trafic de catégorie d'URL et que vous sélectionnez une plage de réputation, vous pouvez inclure les URL de réputation inconnue dans la correspondance de réputation. Nous avons ajouté la case à cocher **Inclure les sites de réputation inconnue** aux critères de réputation d'URL dans les règles de contrôle d'accès et de déchiffrement SSL.
Fonctionnalités du VPN	
Virtual Tunnel Interface (VTI) et VPN de site à site basé sur le routage.	Vous pouvez désormais créer des VPN de site à site basés sur le routage en utilisant une interface de tunnel virtuel comme interface locale pour le profil de connexion VPN. Avec le VPN de site à site basé sur le routage, vous gérez les réseaux protégés dans une connexion VPN donnée en modifiant simplement la table de routage, sans modifier le profil de la connexion VPN. Vous n'avez pas besoin de suivre les réseaux distants et de mettre à jour le profil de connexion VPN pour prendre en compte ces modifications. Cela simplifie la gestion du VPN pour les fournisseurs de services infonuagiques et les grandes entreprises. Nous avons ajouté l'onglet **Virtual Tunnel Interfaces** à la page de liste des interfaces et mis à jour l'assistant VPN de site à site afin que vous puissiez utiliser un VTI comme interface locale.
Prise en charge de l'API Firewall Threat Defense pour Hostscan et Dynamic Access Policy (DAP) pour les connexions VPN d'accès à distance.	Vous pouvez télécharger les paquets Hostscan et le fichier XML de règles de politique d'accès dynamique (DAP) et configurer des règles DAP pour créer le fichier XML et contrôler la façon dont les politiques de groupe sont affectées aux utilisateurs distants en fonction des attributs liés à l'état du point terminal se connectant. Vous pouvez utiliser ces fonctionnalités pour effectuer une modification d'autorisation si vous ne disposez pas de Cisco Identity Services Engine (ISE). Vous pouvez télécharger HostScan et configurer DAP à l'aide de l'API Cisco Firewall Threat Defense uniquement; vous ne pouvez pas les configurer à l'aide de FDM. Consultez la documentation d'AnyConnect pour obtenir des renseignements sur l'utilisation de Hostscan et de DAP. Nous avons ajouté ou modifié les modèles d'objets d'API suivants Cisco Firewall Threat Defense : dapxml, hostscanpackagefiles, hostscanxmlconfigs, ravpns.
L'activation de la vérification de la révocation de certificat pour les certificats d'autorité de certification externes.	Vous pouvez utiliser l'API Cisco Firewall Threat Defense pour activer la vérification de la révocation de certificat sur un certificat d'autorité de certification externe particulier. La vérification de la révocation est particulièrement utile pour les certificats utilisés dans les VPN d'accès à distance. Vous ne pouvez pas configurer la vérification de la révocation sur un certificat à l'aide de FDM, vous devez utiliser l'API Cisco Firewall Threat Defense. Nous avons ajouté les attributs suivants à la ressource ExternalCACertificate : revocationCheck, crlCacheTime, oscpDisableNonce.

Caractéristiques	Description
Suppression de la prise en charge des groupes Diffie-Hellman moins sécurisés, et des algorithmes de chiffrement et de hachage.	**Incidence sur la mise à niveau. Peut empêcher le déploiement après la mise à niveau.** Les fonctionnalités suivantes sont obsolètes dans la version 6.6 et ont maintenant été supprimées. Si vous les utilisez toujours dans des propositions IKE ou des politiques IPsec, vous devez les remplacer après la mise à niveau avant de pouvoir déployer des modifications de configuration. Nous vous recommandons de modifier la configuration de votre VPN avant la mise à niveau pour utiliser des algorithmes de DHCP et de chiffrement pris en charge pour vous assurer que le VPN fonctionne correctement. • Groupes Diffie-Hellman : 2, 5 et 24. • Algorithmes de chiffrement pour les utilisateurs qui satisfont les exigences des contrôles à l'exportation en matière de chiffrement : DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continue d'être pris en charge (et c'est la seule option) pour les utilisateurs qui ne satisfont pas les contrôles à l'exportation. • Algorithmes de hachage : MD5.
Port personnalisé pour le VPN d'accès à distance.	Vous pouvez configurer le port utilisé pour les connexions VPN d'accès à distance (de VPN d'accès à distance). Si vous devez vous connecter à FDM sur la même interface utilisée pour de VPN d'accès à distance, vous pouvez modifier le numéro de port pour les connexions de VPN d'accès à distance. FDM utilise le port 443, qui est également le port par défaut du VPN de RA. Nous avons mis à jour l'étape des paramètres globaux de l'assistant de VPN d'accès à distance pour inclure la configuration des ports.
Prise en charge du serveur SAML pour l'authentification de l'accès distant VPN.	Vous pouvez configurer un serveur SAML 2.0 comme source d'authentification pour un VPN d'accès à distance. Voici les serveurs SAML pris en charge : Duo. Nous avons ajouté le serveur SAML comme source d'identité sur la page des **Objects (Objets)** > **Identity Sources (Sources d'identité)** et avons mis à jour les profils de connexion VPN d'accès à distance pour permettre son utilisation.
Firewall Threat Defense Prise en charge de l'API pour les profils de module AnyConnect.	Vous pouvez utiliser l'API Cisco Firewall Threat Defense pour télécharger les profils de module utilisés avec AnyConnect, comme AMP Enabler, ISE Posture ou Umbrella. Vous devez créer ces profils à l'aide des éditeurs de profils hors ligne que vous pouvez installer à partir du paquet de l'éditeur de profil AnyConnect. Nous avons ajouté l'attribut anyConnectModuleType au modèle AnyConnectClientProfile. Bien que vous puissiez initialement créer des objets de profil de client AnyConnect qui utilisent des profils de module, vous devrez toujours utiliser l'API pour modifier les objets créés dans FDM afin de préciser le type de module approprié.
Fonctionnalités de routage	

Caractéristiques	Description
Prise en charge du protocole EIGRP à l'aide de Smart CLI.	**Incidence sur la mise à niveau. Peut empêcher le déploiement après la mise à niveau.** Dans les versions précédentes, vous configuriez le protocole EIGRP dans les pages de configuration avancée à l'aide de FlexConfig. Maintenant, vous configurez EIGRP à l'aide de Smart CLI directement sur la page Routing (routage). Si vous avez configuré le protocole EIGRP à l'aide de FlexConfig, lors de la mise à niveau vers la version 6.7, vous devez supprimer l'objet FlexConfig de la politique FlexConfig, puis recréer votre configuration dans l'objet Smart CLI. Vous pouvez conserver votre objet FlexConfig de EIGRP comme référence jusqu'à ce que vous ayez terminé les mises à jour de Smart CLI. Votre configuration n'est pas convertie automatiquement. Nous avons ajouté l'objet Smart CLI EIGRP aux pages de routage.
Fonctionnalités de l'interface	
Persistance du contournement matériel pour ISA 3000.	Vous pouvez maintenant activer le contournement matériel pour les paires d'interfaces ISA 3000 avec l'option de persistance : après la restauration de l'alimentation, le contournement matériel reste activé jusqu'à ce que vous le désactiviez manuellement. Si vous activez le contournement matériel sans persistance, le contournement matériel est automatiquement désactivé après le rétablissement de l'alimentation. Il peut y avoir une brève interruption du trafic lorsque le contournement matériel est désactivé. L'option de persistance vous permet de contrôler le moment de la brève interruption du trafic. Écran Nouveau ou modifié : **Périphérique** > **Interfaces** > **Contournement matériel** > **Configuration du contournement matériel**
Synchronisation entre l'état du lien opérationnel de Cisco Firewall Threat Defense et l'état du lien physique du Firepower 4100/9300.	Le châssis Firepower 4100/9300 peut maintenant synchroniser l'état de la liaison opérationnelle Cisco Firewall Threat Defense avec l'état de la liaison physique pour les interfaces de données. Actuellement, les interfaces sont dans un état opérationnel tant que l'état de l'administrateur FXOS et que l'état du lien physique sont actifs. L'état administratif de l'interface de l'application Cisco Firewall Threat Defense n'est pas pris en compte. Sans synchronisation à partir de Cisco Firewall Threat Defense, les interfaces de données peuvent être physiquement opérationnelles avant que l'application Cisco Firewall Threat Defense ne soit complètement en ligne, par exemple, ou peuvent rester actives pendant un certain temps après que vous ayez lancé un arrêt Cisco Firewall Threat Defense. Cette fonctionnalité est désactivée par défaut et peut être activée par périphérique logique dans FXOS. **Remarque** Cette fonctionnalité n'est pas prise en charge pour un Cisco Firewall Threat Defense avec un décorateurRadware vDP. Écrans nouveaux ou modifiés Cisco Firewall chassis manager : **Périphériques logiques > Activer l'état des liens** Commandes FXOS nouvelles ou modifiées : **set link-state-sync enabled**, **show interface expand detail** Plateformes prises en charge : Firepower 4100/9300

Caractéristiques	Description
Les interfaces SFP Firepower 1100 et 2100 prennent désormais en charge la désactivation de la négociation automatique.	Vous pouvez maintenant configurer une interface SFP Firepower 1100 et 2100 pour désactiver la négociation automatique. Pour les interfaces de 10 Go, vous pouvez configurer la vitesse à 1 Go sans négociation automatique; vous ne pouvez pas désactiver la négociation automatique pour une interface dont la vitesse est réglée à 10 Go. Écran Nouveau/modifié : **Périphérique > Interfaces > Modifier l'interface > Options avancées > Vitesse** Plateformes prises en charge : Firepower 1100 et 2100
Fonctions d'administration et de dépannage	
Possibilité d'annuler une mise à niveau logicielle de Cisco Firewall Threat Defense ayant échoué et de revenir à la version précédente.	Si une mise à niveau logicielle majeure Cisco Firewall Threat Defense échoue ou ne fonctionne pas correctement, vous pouvez rétablir l'état du périphérique tel qu'il était lorsque vous avez installé la mise à niveau. Nous avons ajouté la possibilité de rétablir la mise à niveau au panneau de mise à niveau du système dans FDM. Lors d'une mise à niveau, l'écran de connexion FDM affiche l'état de la mise à niveau et vous donne la possibilité de l'annuler ou de revenir en arrière en cas d'échec de la mise à niveau. Dans l'API Cisco Firewall Threat Defense, nous avons ajouté les ressourcesCanCal Upgrade, RevertUPgrade, RetryUPgrade et UpgradeRevertInfo. Dans l'interface de ligne de commande Cisco Firewall Threat Defense, nous avons ajouté les commandes suivantes : **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.
Port HTTPS personnalisé pour l'accès FDM/API Cisco Firewall Threat Defense sur les interfaces de données.	Vous pouvez modifier le port HTTPS utilisé pour l'accès FDM ou l'API Cisco Firewall Threat Defense sur les interfaces de données. En modifiant le port à partir de la valeur 443 par défaut, vous pouvez éviter les conflits entre l'accès de gestion et d'autres fonctionnalités, telles que l'accès VPN à distance, configurées sur la même interface de données. Notez que vous ne pouvez pas modifier le port HTTPS d'accès à la gestion sur l'interface de gestion. Nous avons ajouté la possibilité de modifier le port sur la page **Device** > **System Settings** > **Management Access** > **Data Interfaces** (Périphérique > Paramètres système > Accès de gestion > Interfaces de données).

Caractéristiques	Description
Provisionnement à faible intervention pour Cisco Defense Orchestrator sur les périphériques des périphériques Firepower 1000 et 2100.	Si vous prévoyez de gérer un nouveau périphérique Cisco Firewall Threat Defense à l'aide de Cisco Defense Orchestrator (CDO), vous pouvez désormais ajouter le périphérique sans avoir à exécuter l'assistant de configuration de périphérique ni même à vous connecter à FDM. Les nouveaux périphériques Firepower des séries 1000 et 2100 sont initialement enregistrés dans le nuage de Cisco, où vous pouvez facilement les réclamer dans CDO. Une fois dans CDO, vous pouvez immédiatement gérer les périphériques à partir de CDO. Ce provisionnement à faible intervention réduit les interactions directes requises avec le périphérique physique. C'est idéal pour les bureaux à distance ou les autres emplacements où vos employés sont moins habitués à travailler avec des périphériques réseau. Nous avons modifié le provisionnement initial des périphériques Firepower des séries 1000 et 2100. Nous avons également ajouté l'inscription automatique à la page **Paramètres système** > **Services en nuage**, afin que vous puissiez lancer manuellement le processus pour les périphériques mis à niveau ou d'autres périphériques que vous avez déjà gérés à l'aide de FDM.
Prise en charge de l'API Firewall Threat Defense pour la configuration de SNMP.	**Incidence sur la mise à niveau. Peut empêcher le déploiement après la mise à niveau.** Vous pouvez utiliser l'API Cisco Firewall Threat Defense pour configurer SNMP version 2c ou 3 sur un périphérique Cisco Firewall Threat Defense géré par FDM ou CDO. Nous avons ajouté les ressources d'API suivantes : SNMPAuthentication, SNMPHost, SNMPSecurityConfiguration, SNMPServer, SNMPUser, SNMPUserGroup, SNMPv2cSecurityConfiguration, SNMPv3SecurityConfiguration. **Remarque** Si vous avez utilisé FlexConfig pour configurer SNMP, vous devez refaire la configuration à l'aide des ressources de l'API Cisco Firewall Threat Defense SNMP. Les commandes de configuration de SNMP ne sont plus autorisées dans FlexConfig. La suppression de la simple suppression de l'objet FlexConfig SNMP de la politique FlexConfig vous permettra de déployer les modifications. vous pouvez ensuite utiliser l'objet comme référence pendant que vous utilisez l'API pour reconfigurer la fonctionnalité.
Le nombre maximal de fichiers de sauvegarde conservés sur le système est réduit de 10 à 3.	Le système conservera un maximum de 3 fichiers de sauvegarde sur le système au lieu de 10. Lorsque de nouvelles sauvegardes sont créées, le fichier de sauvegarde le plus ancien est supprimé. Assurez-vous de télécharger les fichiers de sauvegarde sur un autre système afin d'avoir les versions nécessaires pour récupérer le système au cas où vous en auriez besoin.
La prise en charge de Microsoft Internet Explorer a pris fin.	Nous ne testons plus les interfaces Web Firepower à l'aide de Microsoft Internet Explorer. Nous vous recommandons de migrer vers Google Chrome, Mozilla Firefox ou Microsoft Edge.

Caractéristiques	Description
Rétrocompatibilité de la version de l'API Firewall Threat Defense	À partir de la version Cisco Firewall Threat Defense 6.7, si un modèle de ressource d'API pour une fonctionnalité ne change pas entre les versions, l'API Cisco Firewall Threat Defense peut accepter les appels basés sur l'ancienne version d'API. Même si le modèle de fonctionnalité a changé, s'il existe un moyen logique de convertir l'ancien modèle au nouveau modèle, l'ancien modèle peut fonctionner. Par exemple, un appel v4 peut être accepté sur un système v5. Si vous utilisez « latest » comme numéro de version dans vos appels, ces appels « anciens » sont interprétés comme un appel v5 dans ce scénario. Par conséquent, votre utilisation de la compatibilité ascendante dépend de la façon dont vous structurez vos appels d'API.
API REST Firewall Threat Defense version 6 (v6).	L'API REST Cisco Firewall Threat Defense pour la version logicielle 6.7 est la version 6. Vous pouvez utiliser la version v6 dans les URL d'API ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. Veuillez réévaluer tous les appels existants, car des modifications peuvent avoir été apportées aux modèles de ressources que vous utilisez. Pour ouvrir l'explorateur API et consulter les ressources, connectez-vous à FDM, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**.

Fonctionnalités FDM dans la version 6.6.x

Tableau 9 : Fonctionnalités FDM dans la version 6.6.x

Caractéristiques	Description
Caractéristiques de la plateforme	
Prise en charge de Firepower Device Manager pour Firewall Threat Defense Virtual pour le service infonuagique Amazon Web Services (AWS).	Vous pouvez configurer Cisco Firewall Threat Defense sur Firewall Threat Defense Virtual pour le Service infonuagique AWS à l'aide de Firepower Device Manager.
Firepower Device Manager pour le Firepower 4112.	Nous avons lancé Cisco Firewall Threat Defense pour le Firepower 4112. **Remarque** FXOS 2.8.1 est nécessaire.
Interfaces e1000 sur FTDv pour VMware.	**Empêche la mise à niveau.** La version 6.6 met fin à la prise en charge des interfaces e1000 sur FTDv pour VMware. Vous ne pouvez pas procéder à la mise à niveau tant que vous n'avez pas basculé vers les interfaces vmxnet3 ou ixgbe. Vous pouvez cependant déployer un nouveau périphérique. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Fonctionnalités de pare-feu et IPS	

Caractéristiques	Description
Capacité d'activation de règles de prévention des intrusions qui sont désactivées par défaut.	Chaque politique de prévention des intrusions définie par le système comporte un certain nombre de règles qui sont désactivées par défaut. Auparavant, vous ne pouviez pas modifier l'action pour ces règles d'alerte ou d'abandon. Vous pouvez maintenant modifier l'action pour les règles désactivées par défaut. Nous avons modifié la page Politique de prévention des intrusions pour afficher toutes les règles, même celles qui sont désactivées par défaut, et vous permettre de modifier l'action pour ces règles.
Le mode Système de détection d'intrusion (IDS) pour la politique de prévention des intrusions.	Vous pouvez maintenant configurer la politique de prévention des intrusions pour qu'elle fonctionne dans le mode de Système de détection d'intrusion (IDS). En mode IDS, les règles de prévention des intrusions actives émettent des alertes uniquement, même si l'action de la règle est Abandon. Ainsi, vous pouvez superviser ou tester le fonctionnement d'une politique de prévention des intrusions avant d'en faire une politique de prévention active dans le réseau. Dans Firepower Device Manager, nous avons ajouté une indication du mode d'inspection à chaque politique de prévention des intrusions sur la page des **politiques de prévention des intrusions** et un lien de **modification** pour que vous puissiez modifier le mode. Dans l'API Cisco Firewall Threat Defense, nous avons ajouté l'attribut inspectionMode à la ressource IntrusionPlicy.
Prise en charge du téléchargement manuel des paquets de mise à jour de la base de données de vulnérabilités (VDB), de la base de données de géolocalisation et des règles de prévention des intrusions.	Vous pouvez désormais récupérer manuellement les paquets de mise à jour pour la VDB, la base de données de géolocalisation et les règles de prévention des intrusions, puis les charger de votre ordinateur sur le périphérique Cisco Firewall Threat Defense à l'aide de Firepower Device Manager. Par exemple, si vous avez un réseau isolé, où Firepower Device Manager ne peut pas récupérer les mises à jour de Cisco Cloud, vous pouvez désormais obtenir les paquets de mises à jour dont vous avez besoin. Nous avons mis à jour la page **Device** > **Updates** > **(mises à jour des périphériques)** pour vous permettre de sélectionner et de téléverser un fichier à partir de votre ordinateur.
Prise en charge de l'API Cisco Firewall Threat Defense pour les règles de contrôle d'accès limitées dans le temps.	À l'aide de l'API Cisco Firewall Threat Defense, vous pouvez créer des objets de plage temporelle, qui précisent des plages temporelles uniques ou récurrentes, et appliquer ces objets aux règles de contrôle d'accès. En utilisant des plages de temps, vous pouvez appliquer une règle de contrôle d'accès au trafic à certaines heures de la journée ou à certaines périodes, pour offrir une flexibilité dans l'utilisation du réseau. Vous ne pouvez pas utiliser Firepower Device Manager pour créer ou appliquer des plages de temps, et Firepower Device Manager ne vous indique pas si une règle de contrôle d'accès est appliquée à une plage de temps. Les ressources TimeRangeObject, Recurrence, TimeZoneObject, DayLightSenregistrementDateRange et DayLightSenregistrementDayRecurrence ont été ajoutées à l'API Cisco Firewall Threat Defense. L'attribut timeRangeObjects a été ajouté à la ressource accessrules pour appliquer une plage de temps à la règle de contrôle d'accès. En outre, des modifications ont été apportées aux ressources GlobalTimeZone et TimeZone.

Caractéristiques	Description
Recherche de groupe d'objets pour les stratégies de contrôle d'accès.	Pendant son fonctionnement, le périphérique Cisco Firewall Threat Defense étend les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu de tout objet de réseau utilisé dans la règle d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets réseau, mais recherche dans les critères d'accès les correspondances basées sur les définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos règles d'accès sont définies ou sur la façon dont elles s'affichent dans Firepower Device Manager. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès. La recherche de groupe d'objets est désactivée par défaut. Dans Firepower Device Manager, vous devez utiliser FlexConfig pour activer la commande **object-group-search access-control**.
Fonctionnalités du VPN	
Homologue de sauvegarde pour le VPN de site à site. (API Cisco Firewall Threat Defense seulement.)	Vous pouvez utiliser l'API Cisco Firewall Threat Defense pour ajouter un homologue de sauvegarde à une connexion VPN de site à site. Par exemple, si vous avez deux fournisseurs de services Internet, vous pouvez configurer la connexion VPN pour le basculement vers le fournisseur de services Internet de secours si la connexion au premier fournisseur de services Internet n'est plus disponible. Une autre utilisation principale d'un homologue de secours est lorsque vous avez deux périphériques différents à l'autre extrémité du tunnel, comme un concentrateur principal et un concentrateur de secours. Le système doit normalement établir le tunnel vers le concentrateur principal. Si la connexion VPN échoue, le système peut automatiquement rétablir la connexion avec le concentrateur de secours. Nous avons mis à jour l'API Cisco Firewall Threat Defense afin que vous puissiez spécifier plusieurs interfaces pour outsideInterface dans la ressource SToSConnectionProfile. Nous avons également ajouté la ressource BackupPeer et l'attribut remotebackuppeers à la ressource SToSConnectionProfile. Vous ne pouvez pas configurer un homologue de secours à l'aide de Firepower Device Manager, et l'existence d'un homologue de secours ne sera pas visible dans Firepower Device Manager.
Prise en charge de la sécurité de couche de transport datagramme (DTLS) 1.2 dans un VPN d'accès à distance.	Vous pouvez maintenant utiliser DTLS 1.2 dans un VPN d'accès à distance. Cela peut être configuré uniquement à l'aide de l'API Cisco Firewall Threat Defense, vous ne pouvez pas le configurer à l'aide de Firepower Device Manager. Cependant, DTLS 1.2 fait désormais partie du groupe de chiffrement SSL par défaut, et vous pouvez activer l'utilisation générale de DTLS à l'aide de Firepower Device Manager dans les attributs AnyConnect de la politique de groupe. Notez que DTLS 1.2 n'est pas pris en charge sur les modèles ASA 5508-X ou 5516-X. Nous avons mis à jour l'attribut protocolVersion de la ressource sslcipher pour accepter DTLSV1_2 comme valeur d'énumération.

Caractéristiques	Description
Obsolète : prise en charge des groupes Diffie-Hellman moins sécurisés, et algorithmes de chiffrement et de hachage.	Les fonctionnalités suivantes sont obsolètes et seront supprimées dans une version ultérieure. Vous devez éviter de configurer ces fonctionnalités dans les propositions IKE ou les politiques IPSec pour une utilisation dans les VPN. Veuillez abandonner progressivement ces fonctionnalités et utiliser des options renforcées dès que possible. • Groupes Diffie-Hellman : 2, 5 et 24. • Algorithmes de chiffrement pour les utilisateurs qui satisfont les exigences des contrôles à l'exportation en matière de chiffrement : DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continue d'être pris en charge (et c'est la seule option) pour les utilisateurs qui ne satisfont pas les contrôles à l'exportation. • Algorithmes de hachage : MD5.
Fonctionnalités de routage	
Routeurs virtuels et Routage et transfert virtuel (VRF) Lite	Vous pouvez créer plusieurs routeurs virtuels afin de gérer des tables de routage distinctes pour des groupes d'interfaces. Étant donné que chaque routeur virtuel possède sa propre table de routage, vous pouvez assurer une séparation nette du trafic circulant à travers le périphérique. Les routeurs virtuels mettent en œuvre la version « allégée » du routage et transfert virtuel, ou VRF-Lite, qui ne prend pas en charge Multiprotocol Extensions for BGP (MBGP). Nous avons modifié la page de **routage** pour que vous puissiez activer les routeurs virtuels. Lorsque cette option est activée, la page de **routage** affiche une liste de routeurs virtuels. Vous pouvez configurer des routes statiques et des processus de routage distincts pour chaque routeur virtuel. Nous avons aussi ajouté le mot clé [**vrf** *name* | **all**] aux commandes CLI suivantes et modifié la sortie pour indiquer les informations sur le routeur virtuel, le cas échéant : **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters** Nous avons ajouté la commande suivante : **show vrf**.
Les configurations OSPF et BGP ont été déplacées dans les pages de routage.	Dans les versions précédentes, vous configuriez les protocoles OSPF et BGP dans les pages de configuration avancée à l'aide de Smart CLI. Bien que vous configuriez toujours ces processus de routage à l'aide de Smart CLI, les objets sont désormais disponibles directement sur les pages de routage. Cela vous facilitera la configuration des processus par routeur virtuel. Les objets OSPF et BGP Smart CLI ne sont plus disponibles sur la page de configuration avancée. Si vous avez configuré ces objets avant la mise à niveau vers la version 6.6, vous pouvez les trouver sur la page de routage après la mise à niveau.
Fonctionnalités de haute disponibilité	

Caractéristiques	Description
La restriction pour les utilisateurs authentifiés à l'extérieur se connectant à l'unité de secours d'une paire à haute disponibilité a été supprimée.	Auparavant, un utilisateur authentifié à l'extérieur ne pouvait pas se connecter directement à l'unité de secours d'une paire à haute disponibilité. L'utilisateur devait d'abord se connecter à l'unité active, puis déployer la configuration, avant que la connexion à l'unité en veille soit possible. Cette restriction a été supprimée. Les utilisateurs authentifiés à l'extérieur peuvent se connecter à l'unité de secours même s'ils ne se sont jamais connectés à l'unité active, à condition de fournir un nom d'utilisateur et un mot de passe valides.
Modification de la façon dont les interfaces sont gérées par la ressource BreakHAStatus dans l'API Cisco Firewall Threat Defense.	Auparavant, vous pouviez inclure le paramètre de requête **clearIntfs** pour contrôler l'état opérationnel des interfaces sur le périphérique où vous rompez la configuration à haute disponibilité (HA). À partir de la version 6.6, il y a un nouvel attribut, **interfaceOption**, que vous devez utiliser à la place du paramètre de requête clearInfs. Cet attribut est facultatif lorsqu'il est utilisé sur le nœud actif, mais obligatoire lorsqu'il est utilisé sur un nœud non actif. Vous pouvez choisir l'une des deux options suivantes : • DISABLE_INTERFACES (par défaut) : toutes les interfaces de données sur le périphérique en veille (ou sur ce périphérique) sont désactivées. • ENABLE_WITH_STANDBY_IP : si vous avez configuré une adresse IP de veille pour une interface, l'interface du périphérique en veille (ou de ce périphérique) est reconfigurée pour utiliser l'adresse en veille. Toute interface qui n'a pas d'adresse en veille est désactivée. Si vous utilisez la fonction de rupture de la haute disponibilité sur le nœud actif lorsque les périphériques sont dans un état actif/de veille intègre, cet attribut s'applique aux interfaces du nœud de secours. Dans tout autre état, par exemple actif/actif ou suspendu, l'attribut s'applique au nœud sur lequel vous lancez la rupture. Si vous utilisez le paramètre de requête clearIntfs, clearIntfs=true agira comme interfaceOption = DISABLE_INTERFACES. Cela signifie que la rupture d'une paire active/en veille avec clearIntfs=true ne désactivera plus les deux périphériques; seul le périphérique en veille sera désactivé. Lorsque vous rompez la haute disponibilité à l'aide de Firepower Device Manager, l'option d'interface est toujours définie sur DISABLE_Interfaces. Vous ne pouvez pas activer les interfaces avec l'adresse IP en veille. Utilisez l'appel d'API de l'explorateur d'interface de protocole d'application si vous souhaitez un résultat différent.
La dernière raison d'échec des problèmes de haute disponibilité est maintenant affichée sur la page de haute disponibilité.	Si la haute disponibilité (HA) échoue pour une raison quelconque, comme le périphérique actif devient indisponible et bascule vers le périphérique de secours, la dernière raison de l'échec est désormais indiquée sous les informations d'état des périphériques principal et secondaire. Les informations comprennent l'heure UTC de l'événement.
Fonctionnalités de l'interface	

Caractéristiques	Description
Prise en charge du PPPoE.	Vous pouvez maintenant configurer PPPoE pour les interfaces routées. PPPoE n'est pas pris en charge sur les unités à haute disponibilité. Écrans nouveaux ou modifiés : **Device (périphérique)** > **Interfaces** > **Edit (modifier)** > **IPv4 Address (adresses IPv4)** > **Type** > **PPPoE** Commandes nouvelles ou modifiées : **show vpdn group, show vpdn username, show vpdn session pppoe state**
L'interface de gestion agit comme client DHCP par défaut.	L'interface de gestion obtient désormais par défaut une adresse IP de DHCP au lieu d'utiliser l'adresse IP 192.168.45.45. Ce changement vous permet de facilement déployer un Cisco Firewall Threat Defense sur votre réseau existant. Cette fonctionnalité s'applique à toutes les plateformes, à l'exception de Firepower 4100/9300 (où vous définissez l'adresse IP lorsque vous déployez le périphérique logique), et de Firewall Threat Defense Virtual et ISA 3000 (qui utilisent toujours l'adresse IP 192.168.45.45). Le serveur DHCP sur l'interface de gestion n'est également plus activé. Vous pouvez toujours vous connecter à l'adresse IP interne par défaut (192.168.1.1).
Prise en charge du proxy HTTP pour les connexions de gestion Firepower Device Manager.	Vous pouvez maintenant configurer un proxy HTTP pour l'interface de gestion à utiliser avec les connexions Firepower Device Manager. Toutes les connexions de gestion, y compris les mises à jour manuelles et planifiées de base de données, passent par le proxy. Nous avons ajouté la page **System Settings (paramètres système)** > **HTTP Proxy (proxy HTTP)** pour configurer les paramètres. En outre, nous avons ajouté la ressource HTTPProxy à l'API Cisco Firewall Threat Defense.
Définissez la MTU pour l'interface de gestion.	Vous pouvez maintenant définir la MTU pour l'interface de gestion jusqu'à 1500 octets. Par défaut, la MTU est de 1500 octets. Commandes nouvelles ou modifiées : **configure network mtu, configure network management-interface mtu-management-canal** Aucun écran modifié.
Caractéristiques de la licence	
L'inscription des licences Smart et des services en nuage est désormais distincte, et vous pouvez gérer vos inscriptions séparément.	Vous pouvez désormais vous inscrire aux services en nuage en utilisant votre compte de sécurité plutôt que votre compte de licences Smart. L'inscription à l'aide du compte de sécurité est l'approche recommandée si vous avez l'intention de gérer le périphérique à l'aide de Cisco Defense Orchestrator. Vous pouvez également vous désinscrire des services en nuage sans vous désinscrire des licences Smart. Nous avons modifié le comportement de la page **System Settings (paramètres système)** > **Cloud Services (services infonuagiques)** et ajouté la possibilité de vous désinscrire des services infonuagiques. En outre, la fonctionnalité Web Analytics (analyse Web) a été supprimée de la page et vous pouvez maintenant la trouver dans **System Settings (paramètres système)** > **Web Analytics (analyses Web)**. Dans l'API Cisco Firewall Threat Defense, les ressources de CloudServices ont été modifiées pour refléter le nouveau comportement.

Caractéristiques	Description
Prise en charge de la réservation de licence permanente.	Si vous avez un réseau en isolement, où il n'y a pas de chemin d'accès à Internet, vous ne pouvez pas vous inscrire directement auprès de Cisco Smart Software Manager (CSSM) pour l'octroi de licences Smart. Dans cette situation, vous pouvez désormais obtenir l'autorisation d'utiliser le mode de réservation de licence permanente universelle (Universal PLR), dans lequel vous pouvez appliquer une licence qui n'a pas besoin de communication directe avec le CSSM. Si vous avez un réseau en isolement, communiquez avec votre représentant de compte et demandez l'autorisation d'utiliser le mode Universal PLR dans votre compte CSSM et d'obtenir les licences nécessaires. ISA 3000 ne prend pas en charge le mode Universal PLR. Nous avons ajouté la possibilité de passer en mode PLR et d'annuler et d'annuler l'enregistrement d'une licence Universal PLR sur la page **Device** > **Smart License**. Dans l'API Cisco Firewall Threat Defense, il y a de nouvelles ressources pour PLRAuthorization Code, PLR Code, PLRRelease Code, PLRRequest Code et des actions pour PLRRequestCode, InstallPLRCode et CancelReservation.
Fonctions d'administration et de dépannage	
Prise en charge direct de Firepower Device Manager de la configuration PTP (Precision Time Protocol) pour les périphériques ISA 3000.	Vous pouvez utiliser Firepower Device Manager pour configurer le protocole PTP (Precision Time Protocol) sur les périphériques ISA 3000. PTP est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques dans un réseau par paquets. Le protocole est conçu spécifiquement pour les systèmes de mesure et de contrôle industriels en réseau. Dans les versions précédentes, vous deviez utiliser FlexConfig pour configurer le PTP. Nous avons regroupé PTP avec NTP sur la même page de paramètres système et renommé la page **System Settings** > **NTP** > **(paramètres système NTP)** à **Time Services (services de temps)**. Nous avons également ajouté la ressource PTP à l'API Cisco Firewall Threat Defense.
Validation de la chaîne de confiance pour le certificat de serveur Web de gestion Firepower Device Manager.	Lorsque vous configurez un certificat non autosigné pour le serveur Web Firepower Device Manager, vous devez désormais inclure tous les certificats intermédiaires, ainsi que le certificat racine dans la chaîne d'approbation. Le système valide l'ensemble de la chaîne. Nous avons ajouté la possibilité de sélectionner les certificats de la chaîne sous l'onglet **Management Web Server (serveur Web de gestion)** sur la page **Device (appareil)** > **System Settings (paramètres système)** > **Management Access (accès à la gestion)**.
Prise en charge du chiffrement des fichiers de sauvegarde.	Vous pouvez maintenant chiffrer des fichiers de sauvegarde à l'aide d'un mot de passe. Pour restaurer une sauvegarde chiffrée, vous devez fournir le bon mot de passe. Nous avons ajouté la possibilité de choisir de chiffrer les fichiers de sauvegarde pour les tâches récurrentes, planifiées et manuelles, et de fournir le mot de passe lors de la restauration, à la page **Device (périphérique)** > **Backup and Restore (sauvegarde et restauration)**. Nous avons également ajouté les attributs encryptArchive et encryptedKey aux ressources BackupImmediate et BackupSannexe, et encryptedKey à la ressource RestoreImmediate dans l'API Cisco Firewall Threat Defense.

Caractéristiques	Description
Prise en charge de la sélection des événements à envoyer au nuage Cisco pour une utilisation par les services en nuage.	Lorsque vous configurez le périphérique pour envoyer des événements au nuage Cisco, vous pouvez désormais sélectionner les types d'événements à envoyer : intrusion, fichier/programme malveillant et connexion. Pour les événements de connexion, vous pouvez envoyer tous les événements ou uniquement les événements hautement prioritaires, c'est-à-dire ceux liés aux connexions qui déclenchent des événements d'intrusion, de fichier ou de programme malveillant, ou qui correspondent aux politiques de blocage des informations de sécurité. Nous avons modifié le fonctionnement du bouton Send Events to Cisco Cloud Enable (Activer l'envoi des événements vers le nuage Cisco). La fonctionnalité se trouve sur la page **System Settings (paramètres système(** > **Cloud Services (services en nuage)**.
API REST Cisco Firewall Threat Defense version 5 (v5).	L'API REST Cisco Firewall Threat Defense de la version logicielle 6.6 a été incrémentée à la version 5. Vous devez remplacer les versions v1/v2/v3/v4 dans les URL API par v5, ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. L'API v5 comprend de nombreuses nouvelles ressources qui couvrent toutes les fonctionnalités ajoutées dans la version du logiciel 6.6. 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 Firepower Device Manager, cliquez sur le bouton Plus d'options (⋮) et choisissez **API Explorer**.

Fonctionnalités FDM dans la version 6.4.x

Tableau 10 : Fonctionnalités FDM dans la version 6.4.x

Caractéristiques	Description
Configuration du périphérique Série Firepower 1000.	Vous pouvez configurer Cisco Firewall Threat Defense sur les appareils Série Firepower 1000 à l'aide de Firepower Device Manager. Notez que vous pouvez configurer et utiliser les ports d'alimentation par Ethernet (PoE) en tant que ports Ethernet standard, mais vous ne pouvez pas activer ou configurer les propriétés liées à la PoE.
Contournement matériel pour ISA 3000.	Vous pouvez maintenant configurer le contournement matériel pour ISA 3000 sur la page **Device** > **Interfaces (interfaces de** > **périphérique)** . Dans la version 6.3, vous deviez configurer le contournement matériel à l'aide de FlexConfig. Si vous utilisez FlexConfig, refaites la configuration sur la page Interfaces et supprimez les commandes de contournement matériel de FlexConfig. Cependant, la partie de FlexConfig dédiée à la désactivation de la répartition aléatoire des numéros de séquence TCP est toujours recommandée.

Caractéristiques	Description
Possibilité de redémarrer et d'éteindre le système à partir de la console d'interface en ligne de commande Firepower Device Manager.	Vous pouvez maintenant exécuter les commandes **reboot** et **shutdown** par l'intermédiaire de la console d'interface en ligne de commande dans Firepower Device Manager. Auparavant, vous deviez ouvrir une session SSH distincte avec le périphérique pour redémarrer ou éteindre le système. Vous devez disposer de privilèges d'administrateur pour utiliser ces commandes.
Authentification et autorisation extérieures à l'aide de RADIUS pour les utilisateurs de l'interface en ligne de commande Cisco Firewall Threat Defense.	Vous pouvez utiliser un serveur RADIUS externe pour authentifier et autoriser les utilisateurs se connectant à l'interface en ligne de commande Cisco Firewall Threat Defense. Vous pouvez donner un accès de configuration (administrateur) ou de base (lecture seule) aux utilisateurs externes. Nous avons ajouté la configuration SSH à l'onglet **AAA Configuration (configuration AAA)** sur la page **Device (périphérique)** > **System Settings (paramètres système** > **Management Access (accès de gestion)**.
Prise en charge des objets de plage de réseau et des objets de groupe de réseau imbriqué.	Vous pouvez désormais créer des objets réseau qui précisent une plage d'adresses IPv4 ou IPv6 et des objets de groupe de réseau qui incluent d'autres groupes de réseaux (c'est-à-dire des groupes imbriqués). Nous avons modifié les boîtes de dialogue pour l'ajout/la modification des objets réseau et des objets de groupe réseau afin d'inclure ces fonctionnalités, et nous avons modifié les différentes politiques de sécurité afin d'autoriser l'utilisation de ces objets, en fonction de la pertinence des spécifications d'adresse de ce type dans le contexte de la politique.
Options de recherche en texte intégral pour les objets et les règles.	Vous pouvez effectuer une recherche en texte intégral dans les objets et les règles. En recherchant une politique ou une liste d'objets qui comporte un grand nombre d'éléments, vous pouvez trouver tous les éléments qui incluent votre chaîne de recherche n'importe où dans la règle ou l'objet. Nous avons ajouté une zone de recherche à toutes les politiques qui ont des règles et à toutes les pages de la liste **Objects (objets)**. En outre, vous pouvez utiliser l'option **filter=fts~***search-string* sur les appels GET pour les objets pris en charge dans l'API afin de récupérer des éléments en fonction d'une recherche en texte intégral.
Obtention d'une liste des versions d'API prises en charge pour un périphérique Cisco Firewall Threat Defense géré par Firepower Device Manager.	Vous pouvez utiliser la méthode GET /api/versions (ApiVersions) pour obtenir la liste des versions de l'API prises en charge sur un périphérique. Vous pouvez utiliser votre client API pour communiquer et configurer le périphérique à l'aide de commandes et de syntaxes valides pour toutes les versions prises en charge.
Nombre de résultats pour les règles de contrôle d'accès.	Vous pouvez désormais afficher le nombre de résultats pour les règles de contrôle d'accès. Le nombre de résultats indique le nombre de connexions correspondant à la règle. Nous avons mis à jour la politique de contrôle d'accès pour inclure les informations sur le nombre d'accès. Dans l'API Cisco Firewall Threat Defense, nous avons ajouté la ressource HitCounts et les options **includeHitCounts** et **filter=fetchZeroHitCounts** à la ressource des règles de politique d'accès GET.

Caractéristiques	Description
Améliorations du VPN de site à site pour l'adressage dynamique et l'authentification par certificat.	Vous pouvez désormais configurer des connexions VPN de site à site afin d'utiliser des certificats au lieu de clés prépartagées pour authentifier les homologues. Vous pouvez également configurer des connexions lorsque l'homologue distant a une adresse IP inconnue (dynamique). Nous avons ajouté des options à l'assistant VPN de site à site et à l'objet de politique IKEv1.
Prise en charge des serveurs RADIUS et du changement d'autorisation dans le VPN d'accès à distance.	Vous pouvez désormais utiliser des serveurs RADIUS pour l'authentification, l'autorisation et la comptabilisation des utilisateurs du VPN d'accès à distance (RA VPN). Vous pouvez également configurer la modification d'authentification (CoA), également appelée autorisation dynamique, pour modifier l'autorisation d'un utilisateur après authentification, lorsque vous utilisez un serveur Cisco ISE RADIUS. Nous avons ajouté des attributs au serveur RADIUS et aux objets de groupe de serveurs, et rendu possible la sélection d'un groupe de serveurs RADIUS dans un profil de connexion VPN d'accès à distance.
Plusieurs profils de connexion et politiques de groupe pour le VPN d'accès à distance.	Vous pouvez configurer plusieurs profils de connexion et créer des politiques de groupe à utiliser avec les profils. Nous avons modifié la page **Device (périphérique)** > **Remote Access VPN (VPN d'accès à distance du périphérique)** pour qu'elle ait des pages distinctes pour les profils de connexion et les politiques de groupe, et nous avons mis à jour l'assistant de connexion VPN d'accès à distance pour permettre la sélection des politiques de groupe. Certains éléments qui étaient configurés précédemment dans l'assistant sont maintenant configurés dans la politique de groupe.
Prise en charge de l'authentification par certificat, de la deuxième source d'authentification et de l'authentification à deux facteurs dans le VPN d'accès à distance.	Vous pouvez utiliser des certificats pour l'authentification des utilisateurs et configurer des sources d'authentification secondaires de sorte que les utilisateurs doivent s'authentifier deux fois avant d'établir une connexion. Vous pouvez également configurer l'authentification à deux facteurs en utilisant des jetons RSA ou des codes d'accès Duo comme deuxième facteur. Nous avons mis à jour l'assistant de connexion VPN d'accès à distance pour prendre en charge la configuration de ces options supplémentaires.
Prise en charge des ensembles d'adresses IP avec plusieurs plages d'adresses et des ensembles d'adresses DHCP pour le VPN d'accès à distance.	Vous pouvez désormais configurer des ensembles d'adresses qui ont plus d'une plage d'adresses en sélectionnant plusieurs objets réseau qui précisent les sous-réseaux. En outre, vous pouvez configurer des ensembles d'adresses dans un serveur DHCP et utiliser le serveur pour fournir des adresses aux clients VPN d'accès à distance. Si vous utilisez RADIUS pour l'autorisation, vous pouvez également configurer les ensembles d'adresses dans le serveur RADIUS. Nous avons mis à jour l'assistant de connexion VPN d'accès à distance pour prendre en charge la configuration de ces options supplémentaires. Vous pouvez éventuellement configurer l'ensemble d'adresses dans la politique de groupe au lieu du profil de connexion.

Caractéristiques	Description
Améliorations au domaines Active Directory.	Vous pouvez désormais inclure jusqu'à 10 serveurs Active Directory (AD) redondants dans un seul domaine. Vous pouvez également créer plusieurs domaines et supprimer des domaines dont vous n'avez plus besoin. En outre, la limite de téléchargement des utilisateurs dans un domaine est augmentée à 50 000 par rapport à la limite de 2 000 dans les versions précédentes. Nous avons mis à jour la page **Objects (objets)** > **Identity Sources (sources d'identité)** pour prendre en charge plusieurs domaines et serveurs. Vous pouvez sélectionner le domaine dans les critères utilisateur des règles de contrôle d'accès et de déchiffrement SSL pour appliquer la règle à tous les utilisateurs du domaine. Vous pouvez également sélectionner le domaine dans les règles d'identité et les profils de connexion VPN d'accès à distance.
Prise en charge de la redondance pour les serveurs ISE.	Lorsque vous configurez le moteur de services de vérification des identités de Cisco (ISE) en tant que source d'identité pour l'authentification passive, vous pouvez désormais configurer un serveur ISE secondaire si vous avez une configuration ISE à haute disponibilité. Nous avons ajouté un attribut pour le serveur secondaire à l'objet d'identité ISE.
Événements de fichiers/programmes malveillants envoyés aux serveurs de journal système externes.	Vous pouvez maintenant configurer un serveur syslog externe pour recevoir les événements de fichiers/programmes malveillants qui sont générés par les politiques de fichiers configurées sur les règles de contrôle d'accès. Les événements de fichiers utilisent l'ID de message 430004, les événements de programmes malveillants sont 430005. Nous avons ajouté les options de serveur syslog de fichiers/programmes malveillants à la page **Device (périphérique)** > **System Settings (paramètres système)** > **Logging Settings (paramètres de journalisation)**.
Journalisation dans le tampon interne et prise en charge des filtres de journalisation des événements personnalisés.	Vous pouvez maintenant configurer la tampon interne comme destination pour la journalisation du système. En outre, vous pouvez créer des filtres de journalisation des événements pour personnaliser les messages générés pour le serveur syslog et les destinations de journalisation du tampon interne. Nous avons ajouté l'objet Event Log Filter (filtre de journalisation des événements) à la page **Objects (objets)** et la possibilité d'utiliser l'objet sur la page **Device (périphérique)** > **System Settings (paramètres système)** > **Logging Settings (paramètres de journalisation)**. Les options de tampon interne ont également été ajoutées à la page **Logging Settings (paramètres de journalisation)**.
Certificat pour le serveur web Firepower Device Manager.	Vous pouvez maintenant configurer le certificat utilisé pour les connexions HTTPS sur l'interface de configuration Firepower Device Manager. En téléversant un certificat auquel vos navigateurs font déjà confiance, vous pouvez éviter le message d'autorité non fiable que vous obtenez lorsque vous utilisez le certificat interne par défaut. Nous avons ajouté la page **Device (périphérique)** > **System Settings (paramètres système)** > **Management Access (accès de gestion)** > **Management Web Server (serveur web de gestion)**.

Caractéristiques	Description
Assistance Cisco Threat Response.	Vous pouvez configurer le système pour envoyer des incidents d'intrusion à l'application en nuage Cisco Threat Response. Vous pouvez utiliser Cisco Threat Response pour analyser les intrusions. Nous avons ajouté Cisco Threat Response à la page **Device (périphérique)** > **System Settings (paramètres système)** > **Cloud Services (services infonuagiques)**.
Chargement manuel des mises à jour de VDB, GeoDB et SRU.	Vous pouvez désormais récupérer manuellement les paquets de mise à jour pour la VDB, la base de données de géolocalisation et les règles de prévention des intrusions, puis les charger de votre ordinateur sur le périphérique FTD à l'aide de FDM. Par exemple, si vous avez un réseau isolé, où FDM ne peut pas récupérer les mises à jour de Cisco Cloud, vous pouvez désormais obtenir les paquets de mises à jour dont vous avez besoin. Nous avons mis à jour la page **Device (périphériques) > Updates (mises à jour)** pour vous permettre de sélectionner et de téléverser un fichier à partir de votre ordinateur. Cisco FTD minimal : 6.4.0.10. Restrictions de version : cette fonctionnalité n'est pas disponible dans la version 6.5. L'assistance revient dans la version 6.6.
VDB de taille plus restreinte pour les périphériques à faible mémoire.	Pour VDB 363 et versions ultérieures, le système installe désormais une VDB de plus petite taille (également appelée *VDB lite*) sur les périphériques à mémoire limitée. 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. Cisco FTD minimal : 6.4.0.17 Périphériques de mémoire inférieure : ASA-5508-X, ASA-5515-X, ASA-5516-X, ASA-5525-X, ASA-5545-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. Pour obtenir la liste des versions concernées, consultez CSCwd88641.

Caractéristiques	Description
Mode Réservation de licence permanente (PLR) universelle.	Si vous avez un réseau en isolement, où il n'y a pas de chemin d'accès à Internet, vous ne pouvez pas vous inscrire directement auprès de Cisco Smart Software Manager (CSSM) pour l'octroi de licences Smart. Dans cette situation, vous pouvez désormais obtenir l'autorisation d'utiliser le mode de réservation de licence permanente universelle (Universal PLR), dans lequel vous pouvez appliquer une licence qui n'a pas besoin de communication directe avec le CSSM. Si vous avez un réseau en isolement, communiquez avec votre représentant de compte et demandez l'autorisation d'utiliser le mode Universal PLR dans votre compte CSSM et d'obtenir les licences nécessaires. Nous avons ajouté la possibilité de passer en mode PLR et d'annuler l'enregistrement d'une licence PLR universelle sur la page **Device (périphérique) > Smart License (licence Smart)**. Dans l'API Cisco FTD, il y a de nouvelles ressources pour PLRAuthorization Code, PLR Code, PLRRelease Code, PLRRequest Code et des actions pour PLRRequestCode, InstallPLRCode et CancelReservation. Cisco FTD minimal : 6.4.0.10. Cette fonctionnalité est temporairement retirée de la version 6.5, mais elle est rétablie dans la version 6.6. Si vous utilisez la version 6.4.0.10 ou un correctif ultérieur, nous vous recommandons de la mettre à niveau directement vers la version 6.6 ou vers une version ultérieure.
Certificats de serveur HTTPS par défaut.	**Incidence sur la mise à niveau.** L'application des correctifs peut renouveler le certificat de serveur HTTPS *par défaut* actuel du périphérique. Selon la date à laquelle il est créé, votre certificat expire comme suit : • 6.5.0.5 ou ultérieure : 800 jours • 6.5.0 à 6.5.0.4 : 3 ans • 6.4.0.9 et correctifs ultérieurs : 800 jours • 6.4.0 à 6.4.0.8 : 3 ans • 6.3.0 et tous les correctifs : 3 ans • 6.2.3 : 20 ans
Nouveaux champs syslog.	Ces nouveaux champs syslog identifient collectivement un événement de connexion unique : • UUID du capteur • Heure du premier paquet • ID de l'instance de connexion • Compteur de connexions Ces champs apparaissent également dans les journaux système (syslogs) pour les événements d'intrusion, de fichiers et de programmes malveillants, ce qui permet d'associer les événements de connexion à ces événements. Version Cisco FTD minimale : 6.4.0.4

Caractéristiques	Description
API REST Firewall Threat Defense version 3 (v3).	L'API REST Cisco Firewall Threat Defense de la version logicielle 6.4 a été incrémentée à la version 3. Vous devez remplacer v1/v2 dans les URL de l'API par v3. L'API v3 comprend de nombreuses nouvelles ressources qui couvrent toutes les fonctionnalités ajoutées dans la version du logiciel 6.4. Veuillez réévaluer tous les appels existants, car des modifications peuvent avoir été apportées aux modèles de ressources que vous utilisez. Pour ouvrir l'explorateur d'interface de protocole d'application, où vous pouvez afficher les ressources, remplacez la fin de l'URL Firepower Device Manager par **/#/api-explorer** après vous être connecté.

Fonctionnalités FDM dans la version 6.3.x

Tableau 11 : Fonctionnalités FDM dans la version 6.3.x

Fonctionnalité	Description
Configuration à haute disponibilité.	Vous pouvez configurer deux périphériques en tant que paire à haute disponibilité active/en veille. Une configuration à haute disponibilité ou de basculement joint deux périphériques de sorte que si le périphérique principal tombe en panne, le périphérique secondaire peut prendre le relais. Cela vous aide à garder votre réseau opérationnel en cas de défaillance d'un périphérique. Les périphériques doivent être du même modèle, avec le même nombre et le même type d'interfaces, et doivent exécuter la même version de logiciel. Vous pouvez configurer la haute disponibilité à partir de la page **Device (périphérique)**.
Prise en charge de l'acquisition passive de l'identité de l'utilisateur.	Vous pouvez configurer des politiques d'identité pour utiliser l'authentification passive. L'authentification passive recueille l'identité de l'utilisateur sans lui demander son nom d'utilisateur et son mot de passe. Le système obtient les mappages à partir des sources d'identité que vous spécifiez, qui peuvent être le moteur de services de vérification des identités de Cisco (ISE) ou le Passive Identity Connector du moteur de services de vérification des identités de Cisco (ISE PIC), ou les connexions des utilisateurs VPN d'accès à distance. Les modifications comprennent la prise en charge des règles d'authentification passive dans **Policies (politiques)** > **Identity (identité)**, et la configuration ISE dans **Objects (objets)** > **Identity Sources (sources d'identité)**.
Prise en charge des utilisateurs locaux pour le VPN d'accès à distance et l'identité de l'utilisateur.	Vous pouvez maintenant créer des utilisateurs directement par l'intermédiaire de Firepower Device Manager. Vous pouvez ensuite utiliser ces comptes d'utilisateurs locaux pour authentifier les connexions auprès d'un VPN d'accès à distance. Vous pouvez utiliser la base de données locale des utilisateurs comme source d'authentification principale ou de secours. En outre, vous pouvez configurer des règles d'authentification passive dans la politique d'identité afin que les noms d'utilisateurs locaux soient reflétés dans les tableaux de bord et qu'ils soient disponibles pour le trafic correspondant dans les politiques. Nous avons ajouté la page **Objects (objets)** > **Users (utilisateurs)** et mis à jour l'assistant d'accès VPN à distance pour inclure une option de secours.

Fonctionnalité	Description
Modification du comportement par défaut pour la gestion du trafic VPN dans la politique de contrôle d'accès (**sysopt connection permit-vpn**).	Le comportement par défaut concernant la gestion du trafic VPN par la politique de contrôle d'accès a été modifié. À partir de la version 6.3, par défaut, tout le trafic VPN sera traité par la politique de contrôle d'accès. Cela vous permet d'appliquer des inspections avancées, y compris le filtrage d'URL, la protection contre les intrusions et les politiques de fichiers, au trafic VPN. Vous devez configurer des règles de contrôle d'accès pour autoriser le trafic VPN. Vous pouvez également utiliser FlexConfig pour configurer la commande **sysopt connection permit-vpn**, qui demande au système de contourner la politique de contrôle d'accès (et toute inspection avancée) pour le trafic de terminaison VPN.
Prise en charge des objets réseau basés sur le nom de domaine complet et prise en charge de l'interface de données pour la recherche DNS.	Vous pouvez désormais créer des objets réseau (et des groupes) qui spécifient un hôte par nom de domaine complet (FQDN) plutôt que par une adresse IP statique. Le système recherche périodiquement le mappage du FQDN à l'adresse IP pour tout objet de FQDN utilisé dans une règle de contrôle d'accès. Vous pouvez utiliser ces objets dans les règles de contrôle d'accès seulement. Nous avons ajouté l'objet DNS Group (groupe DNS) à la page des objets et modifié la page **System Settings (paramètres système)** > **DNS Server (serveur DNS)** pour autoriser l'affectation de groupes aux interfaces de données, et la règle de contrôle d'accès pour autoriser la sélection d'objets réseau FQDN. En outre, la configuration DNS pour l'interface de gestion utilise désormais des groupes DNS au lieu d'une liste fixe d'adresses de serveur DNS.
Prise en charge du syslog TCP et possibilité d'envoyer des messages de diagnostic syslog par l'interface de gestion.	Dans les versions précédentes, les messages de diagnostic syslog (par opposition aux messages de connexion et de prévention des intrusions) utilisaient toujours une interface de données. Vous pouvez maintenant configurer le journal système de sorte que tous les messages utilisent l'interface de gestion. L'adresse IP source finale dépend de si vous utilisez les interfaces de données comme passerelle pour l'interface de gestion, auquel cas l'adresse IP sera celle de l'interface de données. Vous pouvez également configurer le journal système pour utiliser le TCP au lieu d'UDP comme protocole. Nous avons apporté des modifications à la boîte de dialogue Add/Edit (ajouter/modifier) pour les serveurs syslog à partir de **Objects (objets)** > **Syslog Servers (serveurs syslog)**.
Authentification extérieure et autorisation à l'aide de RADIUS pour les utilisateurs Firepower Device Manager.	Vous pouvez utiliser un serveur RADIUS externe pour authentifier et autoriser les utilisateurs qui se connectent à Firepower Device Manager. Vous pouvez donner aux utilisateurs externes un accès administratif, en lecture-écriture ou en lecture seule. Firepower Device Manager peut prendre en charge cinq connexions simultanées; la sixième session déconnecte automatiquement la session la plus ancienne. Vous pouvez forcer la fin d'une session d'utilisateur Firepower Device Manager si nécessaire. Nous avons ajouté des objets de serveur RADIUS et de groupe de serveurs RADIUS à la page **Objects (objets)** > **Identity Sources (sources d'identité)** pour la configuration des objets. Nous avons ajouté l'onglet **AAA Configuration (configuration AAA)** à **Device (périphérique)** > **System Settings (paramètres système)** > **Management Access (accès de gestion)** pour permettre l'utilisation des groupes de serveurs. En outre, la page **Monitoring (supervision)** > **Sessions** répertorie les utilisateurs actifs et permet à un utilisateur administratif de mettre fin à une session.

Fonctionnalité	Description
Améliorations de l'affichage et du déploiement des modifications en attente.	La fenêtre de déploiement a été modifiée pour offrir un affichage plus clair des modifications en attente qui seront déployées. En outre, vous avez désormais la possibilité d'annuler les modifications, de copier les modifications dans le presse-papiers et de télécharger les modifications dans un fichier au format YAML. Vous pouvez également nommer les tâches de déploiement pour qu'elles soient plus faciles à trouver dans le journal d'audit.
Journal d'audit.	Vous pouvez afficher un journal d'audit qui enregistre les événements comme les déploiements, les tâches système, les modifications de configuration , ainsi que la connexion et la déconnexion administratives des utilisateurs. Nous avons ajouté la page **Device (périphérique)** > **Device Administration (administration du périphérique)** > **Audit Log (journal d'audit)**.
Capacité d'exporter la configuration.	Vous pouvez télécharger une copie de la configuration du périphérique à des fins de conservation de dossiers. Cependant, vous ne pouvez pas importer cette configuration dans un périphérique. Cette fonctionnalité ne remplace pas la sauvegarde/restauration. Nous avons ajouté la page **Device (périphérique)** > **Device Administration (administration du périphérique)** > **Download Configuration (télécharger la configuration)**.
Améliorations apportées au filtrage d'URL pour les URL inconnues.	Si vous effectuez un filtrage d'URL selon la catégorie dans les règles de contrôle d'accès, les utilisateurs peuvent accéder à des URL dont la catégorie et la réputation ne sont pas définies dans la base de données d'URL. Auparavant, vous deviez activer manuellement l'option pour rechercher la catégorie et la réputation de ces URL auprès de Cisco Collective Security Intelligence (CSI). Cette option est maintenant activée par défaut. En outre, vous pouvez désormais définir la durée de vie (TTL) des résultats de la recherche, afin que le système puisse actualiser la catégorie ou la réputation pour chaque URL inconnue. Nous avons mis à jour la page **Device (périphérique)** > **System Settings (paramètres système)** > **URL Filtering Preferences (préférences de filtrage des URL)**.
La journalisation des renseignements de sécurité est maintenant activée par défaut.	La politique de renseignements de sécurité a été introduite dans la version 6.2.3, avec la journalisation désactivée par défaut. À partir de la version 6.3.0, la journalisation est activée par défaut. Si vous effectuez une mise à niveau à partir de la version 6.2.3, vos paramètres de journalisation sont conservés, qu'ils soient activés ou désactivés. Activez la journalisation si vous souhaitez voir les résultats de la mise en œuvre des politiques.
Interfaces en mode passif.	Vous pouvez configurer une interface en mode passif. Lorsqu'elle agit de manière passive, l'interface surveille simplement le trafic provenant des ports source dans le cadre d'une session de surveillance configurée sur le commutateur lui-même (pour les périphériques matériels) ou sur le réseau VLAN en mode promiscuité (pour Firewall Threat Defense Virtual). Vous pouvez utiliser le mode passif pour évaluer le comportement du périphérique Firewall Threat Defense Virtual si vous le déployez en tant que pare-feu actif. Vous pouvez également utiliser des interfaces passives dans un réseau de production si vous avez besoin de services IDS (système de détection d'intrusion), où vous souhaitez connaître les menaces, mais vous ne souhaitez pas que le périphérique empêche activement les menaces. Vous pouvez sélectionner le mode passif lors de la modification des interfaces physiques et lors de la création de zones de sécurité.

Fonctionnalité	Description
Améliorations de Smart CLI pour le protocole Open Shortest Path First (OSPF) et prise en charge du protocole BGP.	La configuration de OSPF de Smart CLI a été améliorée, y compris de nouveaux types d'objets Smart CLI pour les ACL standard et étendues, les cartes de routage, les objets du chemin AS, les listes de préfixes IPv4 et IPv6, les listes de politiques et les listes de communauté standard et étendues. En outre, vous pouvez désormais utiliser Smart CLI pour configurer le routage BGP. Vous trouverez ces fonctionnalités sur la page **Device (périphérique)** > **Advanced Configuration (configuration avancée)**
Commandes FlexConfig obsolètes.	Nous avons supprimé les commandes FlexConfig suivantes : • **access-list** : vous pouvez maintenant créer des listes d'accès **extended** et **standard** à l'aide des objets Liste d'accès étendues ou Liste d'accès standard de Smart CLI. Vous pouvez ensuite les utiliser sur les commandes prises en charge par FlexConfig qui font référence à la liste de contrôle d'accès par nom d'objet, comme **match access-list** avec une liste de contrôle d'accès étendue pour les classes de trafic des politiques de service. • **as-path** : vous pouvez maintenant créer des objets de chemin AS pour Smart CLI et les utiliser dans un objet BGP Smart CLI pour configurer un filtre de chemin AS. • **community-list** : vous pouvez maintenant créer des objets de liste de communauté étendue ou de liste de communauté standard Smart CLI et les utiliser dans un objet BGP d'interface Smart CLI pour configurer un filtre de liste de communauté. • **dns-group** : vous pouvez maintenant configurer des groupes DNS à l'aide de **Objects (objets)** > **DNS Groups (groupes DNS)** et affecter les groupes à l'aide de **Device (périphérique)** > **System Settings (paramètres système)** > **DNS Server (serveur DNS)**. • **policy-list** : vous pouvez maintenant créer des objets de liste de politiques Smart CLI et les utiliser dans un objet BGP Smart CLI pour configurer une liste de politiques. • **prefix-list** : vous pouvez maintenant créer des objets de liste de préfixes IPv4 Smart CLI et les utiliser dans un objet Smart CLI OSPF ou BGP pour configurer le filtrage de liste de préfixes pour IPv4. • **route-map** : vous pouvez maintenant créer des objets de carte de routage Smart CLI et les utiliser dans un objet Smart CLI OSPF ou BGP pour configurer des cartes de routage. • **router bgp** : vous pouvez maintenant utiliser les modèles Smart CLI pour le protocole BGP.
Améliorations pour les périphériques ISA 3000.	Vous pouvez maintenant configurer les fonctionnalités suivantes pour ISA 3000 : alarmes, contournement matériel, sauvegarde et restauration à l'aide de la carte SD. Vous utilisez FlexConfig pour configurer les alarmes et le contournement matériel. Pour la carte SD, nous avons mis à jour les pages de sauvegarde et restauration dans Firepower Device Manager.

Fonctionnalité	Description
Prise en charge des appareils ASA 5506-X, 5506W-X, 5506H-X et 5512-X supprimée à partir de Cisco Firewall Threat Defense 6.3.	Vous ne pouvez pas installer Cisco Firewall Threat Defense 6.3 ou les versions ultérieures sur les appareils ASA 5506-X, 5506W-X, 5506H-X et 5512-X. La dernière version de Cisco Firewall Threat Defense prise en charge pour ces plateformes est 6.2.3.
Prise en charge de VMware vSphere/VMware ESXi 5.5 supprimée.	La version 6.3 met fin à la prise en charge de FTDv sur VMware vSphere/VMware ESXi 6.0. Mettez à niveau l'environnement d'hébergement à une version prise en charge avant de mettre à niveau FTD.
Analyses Web pour fournir à Cisco des renseignements sur l'utilisation des produits.	Vous pouvez activer l'analyse Web, qui fournit à Cisco des informations anonymes sur l'utilisation du produit en fonction des pages visitées. Ces renseignements peuvent aider Cisco à déterminer les modèles d'utilisation des fonctionnalités et à aider Cisco à améliorer le produit. Toutes les données d'utilisation sont anonymes, et aucune donnée sensible n'est transmise. L'analyse Web est activée par défaut. Nous avons ajouté l'analyse Web à la page **Device (périphérique)** > **System Settings (paramètres système)** > **Cloud Services (services infonuagiques)**.
L'installation d'une mise à jour de base de données sur les vulnérabilités (VDB) ne redémarre plus Snort.	Lorsque vous installez une mise à jour de VDB, l'installation elle-même ne redémarre plus Snort. Cependant, Snort continue de redémarrer lors du prochain déploiement de configuration.
Le déploiement d'une mise à jour de base de données de règles de prévention des intrusions (SRU) ne redémarre plus Snort.	Après avoir installé une mise à jour de règles de prévention des intrusions (SRU), vous devez déployer la configuration pour activer les nouvelles règles. Le déploiement de la mise à jour de la SRU ne provoque plus de redémarrage Snort .
Prise en charge de l'extension SME.	**Incidence sur la mise à niveau.** La version 6.3.0 interrompt temporairement la prise en charge de l'extension SME, introduite dans les versions 6.2.3.8/6.2.3.9. Dès lors, les actions **Decrypt-Resign** (déchiffrer-resigner) et **Decrypt-Known Key** (déchiffrer-clé connue) ne prennent temporairement pas en charge l'extension SME lors de la négociation ClientHello, qui permet des communications plus sécurisées. L'extension du service SME est définie par la RFC 7627. L'assistance revient dans la version 6.3.0.1.
API REST Cisco Firewall Threat Defense version 2 (v2).	L'API REST Cisco Firewall Threat Defense de la version logicielle 6.3 a été incrémentée à la version 2. Vous devez remplacer v1 dans les URL de l'API par v2. L'API v2 comprend de nombreuses nouvelles ressources qui couvrent toutes les fonctionnalités ajoutées dans la version du logiciel 6.3. Veuillez réévaluer tous les appels existants, car des modifications peuvent avoir été apportées aux modèles de ressources que vous utilisez. Pour ouvrir l'explorateur d'interface de protocole d'application, où vous pouvez afficher les ressources, remplacez la fin de l'URL Firepower Device Manager par **/#/api-explorer** après vous être connecté.

Fonctionnalités FDM dans la version 6.2.3

Tableau 12 : Fonctionnalités FDM dans la version 6.2.3

Caractéristiques	Description
Déchiffrement SSL/TLS	Vous pouvez déchiffrer les connexions SSL/TLS afin de pouvoir inspecter le contenu de la connexion. Sans déchiffrement, les connexions chiffrées ne peuvent pas être inspectées efficacement pour identifier les menaces d'intrusion et de programme malveillant, ou pour faire respecter vos politiques d'utilisation des URL et des applications. Nous avons ajouté la page **Policies (politiques)** > **SSL Decryption (déchiffrement SSL)** et le tableau de bord **Monitoring (supervision)** > **SSL Decryption (déchiffrement SSL)**. **Attention** Les politiques d'identité qui mettent en œuvre l'authentification active génèrent automatiquement des règles de déchiffrement SSL. Si vous effectuez une mise à niveau à partir d'une version qui ne prend pas en charge le déchiffrement SSL, la politique de déchiffrement SSL est automatiquement activée si vous avez ce type de règle. Cependant, vous devez spécifier le certificat à utiliser pour les règles Déchiffrer-Resigner après avoir terminé la mise à niveau. Modifiez les paramètres de déchiffrement SSL immédiatement après la mise à niveau.
Blocage des renseignements de sécurité.	À partir de la nouvelle page **Policies (politiques)** > **Security Intelligence (renseignements de sécurité)**, vous pouvez configurer une politique de renseignements de sécurité, que vous pouvez utiliser pour abandonner le trafic indésirable en fonction de l'adresse IP source/de destination ou de l'URL de destination. Les connexions autorisées seront toujours évaluées par les politiques de contrôle d'accès et pourraient être interrompues. Vous devez activer la licence Threat pour utiliser les renseignements de sécurité. Nous avons également renommé le tableau de bord **Policies (politiques)** en **Access And SI Rules (règles d'accès et de renseignements de sécurité)**, et le tableau de bord comprend désormais les équivalents de règles de renseignements de sécurité ainsi que les règles d'accès.
Réglage des règles de prévention des intrusions.	Vous pouvez modifier l'action pour les règles de prévention des intrusions dans les politiques de prévention des intrusions prédéfinies que vous appliquez avec vos règles de contrôle d'accès. Vous pouvez configurer chaque règle pour supprimer ou générer des événements (alertes) correspondant au trafic, ou désactiver la règle. Vous pouvez modifier l'action pour les règles activées uniquement (celles étant définies sur abandon ou alerte); vous ne pouvez pas activer une règle qui est désactivée par défaut. Pour définir les règles de prévention des intrusions, choisissez **Policies (politiques)** > **Intrusion**.

Caractéristiques	Description
Affectation automatique de la politique d'analyse de réseau (NAP) en fonction de la politique de prévention des intrusions.	Dans les versions précédentes, la Politiques d'analyse de sécurité et de connectivité équilibrées était toujours utilisée pour les paramètres de préprocesseur, peu importe la politique de prévention des intrusions attribuée à une zone de sécurité source/de destination et à une combinaison d'objets réseau spécifiques. Désormais, le système génère automatiquement des règles NAP pour affecter les politiques NAP et de prévention des intrusions du même nom au trafic en fonction de ces critères. Notez que si vous utilisez des critères de couche 4 ou 7 pour affecter différentes politiques de prévention des intrusions au trafic qui correspond autrement à la même zone de sécurité source/de destination et au même objet réseau, vous n'obtiendrez pas des politiques NAP et de prévention des intrusions parfaitement correspondantes. Vous ne pouvez pas créer de politiques d'analyse du réseau personnalisées.
Rapports détaillés pour les tableaux de bord des menaces, des agresseurs et des cibles.	Vous pouvez désormais cliquer sur les tableaux de bord des menaces, des agresseurs et des cibles pour afficher plus de détails sur les éléments signalés. Ces tableaux de bord sont disponibles sur la page Monitoring (supervision). En raison de ces nouveaux rapports, vous perdrez les données de rapport pour ces tableaux de bord lors de la mise à niveau à partir d'une version antérieure à la version 6.2.3.
Tableau de bord des applications Web.	Le nouveau tableau de bord des applications Web affiche les principales applications Web, comme Google, utilisées dans le réseau. Ce tableau de bord complète le tableau de bord Applications, qui fournit des informations relatives aux protocoles, comme l'utilisation de HTTP.
Le nouveau tableau de bord Zones remplace les tableaux de bord des zones d'entrée et des zones de sortie.	Le nouveau tableau de bord Zones affiche les principales paires de zones de sécurité pour le trafic entrant et sortant du périphérique. Ce tableau de bord remplace les tableaux de bord distincts pour les zones d'entrée et de sortie.
Nouveau tableau de bord Malware (programmes malveillants).	Le nouveau tableau de bord des programmes malveillants affiche les principales combinaisons d'actions et de disposition des programmes malveillants. Vous pouvez faire un zoom avant pour afficher les renseignements sur les types de fichiers associés. Vous devez configurer des politiques de fichiers sur les règles d'accès pour afficher ces informations.
Certificats internes autosignés et certificats internes CA.	Vous pouvez désormais générer des certificats d'identité interne autosignés. Vous pouvez également téléverser ou générer des certificats CA internes autosignés à utiliser avec les politiques de déchiffrement SSL. Configurez ces fonctionnalités sur la page **Objects (objets)** > **Certificates (certificats)**.
Possibilité de modifier les paramètres du serveur DHCP lors de la modification des propriétés de l'interface.	Vous pouvez maintenant modifier les paramètres d'un serveur DHCP configuré sur une interface en même temps que vous modifiez les propriétés de l'interface. Cela facilite la redéfinition de l'ensemble d'adresses DHCP si vous devez remplacer l'adresse IP de l'interface par un sous-réseau différent.

Caractéristiques	Description
Cisco Success Network envoie des données d'utilisation et des statistiques à Cisco pour améliorer le produit et fournir une assistance technique efficace.	Vous pouvez vous connecter à Cisco Success Network pour envoyer des données à Cisco. En activant Cisco Success Network, vous fournissez à Cisco des informations et des statistiques d'utilisation qui sont essentielles pour que Cisco puisse vous fournir une assistance technique. Ces informations permettent également à Cisco d'améliorer le produit et de vous informer des fonctionnalités disponibles inutilisées afin de maximiser la valeur du produit sur votre réseau. Vous pouvez activer la connexion lorsque vous enregistrez le périphérique avec Cisco Smart Software Manager, ou une version ultérieure à votre choix. Vous pouvez désactiver la connexion à tout moment. Cisco Success Network est un service en nuage. La page **Device (périphérique)** > **System Settings (paramètres système)** > **Cloud Management (gestion du nuage)** est renommée **Cloud Services (services infonuagiques)**. Vous pouvez configurer Cisco Defense Orchestrator à partir de la même page.
Firewall Threat Defense Virtual pour la configuration du périphérique hyperviseur de machine virtuelle basée sur le noyau (KVM).	Vous pouvez configurer Cisco Firewall Threat Defense sur Firewall Threat Defense Virtual pour les périphériques KVM à l'aide de Firepower Device Manager. Auparavant, seulement VMware était pris en charge. **Remarque** Vous devez installer une nouvelle image 6.2.3 pour obtenir la prise en charge de Firepower Device Manager. Vous ne pouvez pas mettre à niveau une machine virtuelle existante à partir d'une version antérieure puis passer à Firepower Device Manager.
Prise en charge de VMware ESXi 6.5.	Vous pouvez maintenant déployer FTDv sur VMware vSphere/VMware ESXi 6.5.
Configuration des périphériques ISA 3000 (appareils de sécurité industrielle de la série Cisco 3000).	Vous pouvez configurer Cisco Firewall Threat Defense sur les périphériques ISA 3000 à l'aide de Firepower Device Manager. Notez que ISA 3000 prend uniquement en charge la licence relative aux menaces. Il ne prend pas en charge les licences relatives au filtrage d'URL ou aux programmes malveillants. Par conséquent, vous ne pouvez pas configurer les fonctionnalités qui nécessitent les licences de filtrage d'URL ou de programmes malveillants sur ISA 3000.
Déploiement facultatif sur la mise à jour de la base de données de règles ou de la VDB.	Lorsque vous mettez à jour la base de données de règles de prévention des intrusions ou la VDB ou configurez une planification de mise à jour, vous pouvez empêcher le déploiement immédiat de la mise à jour. Étant donné que la mise à jour redémarre les plateformes d'inspection, il y a une perte de trafic momentanée pendant le déploiement. En ne déployant pas automatiquement, vous pouvez choisir de lancer le déploiement à un moment où les pertes de trafic seront le moins perturbatrices. **Remarque** Un téléchargement de VDB peut également provoquer le redémarrage de Snort, puis provoquer à nouveau un redémarrage lors du déploiement. Vous ne pouvez pas arrêter le redémarrage dû au téléchargement.

Caractéristiques	Description
Messages améliorés qui indiquent si un déploiement redémarre Snort. De plus, il est moins nécessaire de redémarrer Snort lors du déploiement.	Avant de commencer un déploiement, Firepower Device Manager indique si les mises à jour de configuration nécessitent un redémarrage de Snort. Les redémarrages de Snort entraînent une perte momentanée du trafic. Ainsi, vous savez désormais si un déploiement n'aura pas d'incidence sur le trafic et peut être effectué immédiatement, ou s'il aura une incidence sur le trafic, afin de pouvoir le déployer à un moment moins perturbateur. En outre, dans les versions précédentes, Snort redémarrait lors de chaque déploiement. Maintenant, Snort redémarre pour les raisons suivantes uniquement : • vous activez ou désactivez les politiques de déchiffrement SSL; • une base de données de règles mise à jour ou une VDB a été téléchargée; • vous avez modifié la MTU sur au moins une interface physique (mais pas la sous-interface).
Console d'interface en ligne de commande dans Firepower Device Manager.	Vous pouvez maintenant ouvrir une console d'interface en ligne de commande à partir de Firepower Device Manager. La console d'interface en ligne de commande imite une session SSH ou une session de console, mais autorise uniquement un sous-ensemble de commande : **show**, **ping**, **traceroute** et **packet-tracer**. Utilisation de la console d'interface en ligne de commande pour le dépannage et la supervision des périphériques.
Prise en charge du blocage de l'accès à l'adresse de gestion.	Vous pouvez désormais supprimer toutes les entrées de la liste d'accès de gestion pour un protocole afin d'empêcher l'accès à l'adresse IP de gestion. Auparavant, si vous supprimiez toutes les entrées, le système autorisait l'accès de toutes les adresses IP clients par défaut. Lors de la mise à niveau vers la version 6.2.3, si vous aviez précédemment une liste d'accès de gestion vide pour un protocole (HTTPS ou SSH), le système crée la règle d'autorisation par défaut pour toutes les adresses IP. Vous pouvez ensuite supprimer ces règles selon vos besoins. En outre, Firepower Device Manager reconnaîtra les modifications que vous apportez à la liste d'accès de gestion à partir de l'interface de ligne de commande, y compris si vous désactivez l'accès SSH ou HTTPS. Assurez-vous d'activer l'accès HTTPS pour au moins une interface, sinon vous ne pourrez pas configurer et gérer le périphérique.
Prise en charge de l'extension SME.	Les actions **Decrypt-Resign** (déchiffrer-resigner) et **Decrypt-Known Key** (déchiffrer-clé connue) prennent désormais en charge l'extension SME lors de la négociation ClientHello, permettant des communications plus sécurisées. L'extension du service SME est définie par la RFC 7627. **Remarque** La version 6.2.3.8 a été supprimée de Site d'assistance et de téléchargement Cisco le 7 janvier 2019. La mise à niveau vers la version 6.2.3.9 active également la prise en charge de l'extension SME. La version 6.3.0 met fin à la prise en charge de l'extension SME. La prise en charge est réintroduite dans la version 6.3.0.1. Cisco FTD minimal : version 6.2.3.8

Caractéristiques	Description
Commande CLI de rétrogradation de TLS v1.3 pour Cisco FTD.	Une nouvelle commande CLI vous permet de préciser quand rétrograder les connexions TLS v1.3 vers TLS v1.2. De nombreux navigateurs utilisent TLS v1.3 par défaut. Si vous utilisez une politique SSL pour gérer le trafic chiffré et que les membres de votre réseau supervisé utilisent des navigateurs avec TLS v1.3 activé, les sites Web qui prennent en charge TLS v1.3 ne se chargent pas. Pour plus de renseignements, consultez les commandes **system support** dans Référence des commandes de défense contre les menaces de Cisco Secure Firewall. Nous vous recommandons d'utiliser ces commandes uniquement après avoir consulté Centre d'assistance technique Cisco (TAC). Cisco FTD minimal : version 6.2.3.7
Smart CLI et FlexConfig pour la configuration des fonctionnalités à l'aide de la CLI du périphérique.	Smart CLI et FlexConfig vous permettent de configurer des fonctionnalités qui ne sont pas encore prises en charge directement par les politiques et les paramètres Firepower Device Manager. Firewall Threat Defense utilise les commandes de configuration ASA pour mettre en œuvre certaines fonctionnalités. Si vous êtes un utilisateur expérimenté et expert des commandes de configuration ASA, vous pouvez configurer ces fonctionnalités sur le périphérique à l'aide des méthodes suivantes : • Smart CLI – (méthode préférée) Un modèle Smart CLI est un modèle prédéfini pour une fonctionnalité particulière. Toutes les commandes nécessaires à la fonctionnalité sont fournies, et vous devez simplement sélectionner les valeurs des variables. Le système valide votre sélection, ce qui vous permet de configurer plus facilement une fonctionnalité correctement. S'il existe un modèle Smart CLI pour la fonctionnalité souhaitée, vous devez utiliser cette méthode. Dans cette version, vous pouvez configurer le protocole OSPFv2 à l'aide de Smart CLI. • FlexConfig : la politique FlexConfig est un ensemble d'objets FlexConfig. Les objets FlexConfig sont de forme plus libre que les modèles Smart CLI et le système n'effectue aucune validation de CLI, de variable ou de données. Vous devez connaître les commandes de configuration ASA et suivre les guides de configuration ASA pour créer une séquence valide de commandes. **Mise en garde** Cisco recommande fortement d'utiliser les Smart CLI et FlexConfig uniquement si vous êtes un utilisateur avancé avec de solides connaissances en ASA, et ce, à vos propres risques. Vous pouvez configurer toutes les commandes qui ne figurent pas sur la liste noire. L'activation de fonctionnalités par le biais de Smart CLI ou FlexConfig peut entraîner des résultats imprévus avec d'autres fonctionnalités configurées.
API REST Firewall Threat Defense et un explorateur d'interface de protocole d'application.	Vous pouvez utiliser une API REST pour interagir de manière programmée avec un périphérique Cisco Firewall Threat Defense que vous gérez localement par l'intermédiaire de Firepower Device Manager. Il existe un explorateur d'interface de protocole d'application que vous pouvez utiliser pour afficher les modèles d'objet et tester les différents appels que vous pouvez effectuer à partir d'un programme client. Pour ouvrir l'explorateur d'interface de protocole d'application, connectez-vous à Firepower Device Manager, puis modifiez le chemin sur l'URL en /#/api-Explorer, par exemple, https:FTd.example.com/#/api-Explorer.

Fonctionnalités FDM de la version 6.2.2

Tableau 13 : Fonctionnalités FDM de la version 6.2.2

Fonctionnalités	Description
Configuration du VPN d'accès à distance pour les périphériques de la gamme ASA 5500-X.	Vous pouvez configurer le SSL VPN d'accès à distance pour le client AnyConnect sur les périphériques de la gamme ASA 5500-X. Configurez le VPN d'accès à distance à partir du groupe **Device (périphérique)** > **Remote Access VPN (VPN d'accès à distance)**. Configurez les licences VPN d'accès à distance à partir du groupe **Device (périphérique)** > **Smart License (licence Smart)**.
Firewall Threat Defense Virtual pour la configuration des périphériques VMware.	Vous pouvez configurer Cisco Firewall Threat Defense sur Firewall Threat Defense Virtual pour les périphériques VMware à l'aide de Firepower Device Manager. Les autres plateformes virtuelles ne sont pas prises en charge par Firepower Device Manager. **Remarque** Vous devez installer une nouvelle image 6.2.2 pour obtenir la prise en charge de Firepower Device Manager. Vous ne pouvez pas mettre à niveau une machine virtuelle existante à partir d'une version antérieure puis passer à Firepower Device Manager.

Fonctionnalités FDM dans la version 6.2.1

Remarque Cette version s'applique uniquement à la série Firepower 2100.

Tableau 14 : Fonctionnalités FDM dans la version 6.2.1

Fonctionnalités	Description
Configuration VPN d'accès à distance	Vous pouvez configurer le SSL VPN d'accès à distance pour le client AnyConnect. Configurez le VPN d'accès à distance à partir du groupe **Device (périphérique)** > **Remote Access VPN (VPN d'accès à distance)**. Configurez les licences VPN d'accès à distance à partir du groupe **Device (périphérique)** > **Smart License (licence Smart)**.
Configuration du périphérique Série Firepower 2100.	Vous pouvez configurer Cisco Firewall Threat Defense sur les appareils Série Firepower 2100 à l'aide de Firepower Device Manager.

Fonctionnalités FDM dans la version 6.2.0

Tableau 15 : Fonctionnalités FDM dans la version 6.2.0

Fonctionnalités	Description
Gestion en nuage de Cisco Defense Orchestrator (CDO).	Vous pouvez gérer le périphérique à l'aide du portail en nuage Cisco Defense Orchestrator. Sélectionnez**Device** > **System Settings** > **Cloud Management** (Périphérique > Paramètres système > Gestion en nuage). Pour en savoir plus sur Cisco Defense Orchestrator, consultez http://www.cisco.com/go/cdo.
Faire glisser et déposer les règles d'accès.	Vous pouvez faire glisser et déposer des règles d'accès pour les déplacer dans le tableau de règles.
Mettre à niveau le logiciel Cisco Firewall Threat Defense au moyen de Firepower Device Manager.	Vous pouvez installer les mises à niveau logicielles au moyen de Firepower Device Manager. Sélectionnez **Périphérique** > **Mettre à jour**.
Modifications de la configuration par défaut	Pour les périphériques nouveaux ou recréés, la configuration par défaut comprend des modifications importantes, notamment : • (ASA 5506-X, 5506W-X, 5506H-X.) À l'exception de la première interface de données et de l'interface Wi-Fi des modèles ASA 5506W-X, toutes les autres interfaces de données de ces modèles d'appareil sont structurées en deux. groupe de ponts et activé. Il y a un serveur DHCP dans le groupe de ponts internes. Vous pouvez brancher des points terminaux ou des commutateurs dans n'importe quelle interface pontée, et les points terminaux obtiennent des adresses sur le réseau 192.168.1.0/24. • L'adresse IP de l'interface interne est désormais 192.168.1.1, et un serveur DHCP est défini sur l'interface avec l'ensemble d'adresses 192.168.1.5-192.168.1.254. • L'accès HTTPS est activé sur l'interface interne, vous pouvez donc ouvrir Firepower Device Manager via l'interface interne à l'adresse par défaut, 192.168.1.1. Pour les modèles ASA 5506-X, vous pouvez le faire par l'intermédiaire de n'importe quelle interface de membre de groupe de ponts. • Le port de gestion héberge un serveur DHCP pour le réseau 192.168.45.0/24. Vous pouvez brancher un poste de travail directement sur le port de gestion, obtenir une adresse IP et ouvrir Firepower Device Manager pour configurer le périphérique. • Les serveurs DNS publics OpenDNS sont désormais les serveurs DNS par défaut pour l'interface de gestion. Auparavant, il n'y avait pas de serveur DNS par défaut. Vous pouvez configurer différents serveurs DNS lors de la configuration du périphérique. • La passerelle par défaut pour l'adresse IP de gestion doit utiliser les interfaces de données pour le routage vers Internet. Ainsi, vous n'avez pas besoin de câbler l'interface physique de gestion à un réseau.

Fonctionnalités	Description
Modifications de l'interface de gestion et des accès.	Plusieurs modifications apportées au fonctionnement de l'adresse de gestion et de l'accès à Firepower Device Manager : • Vous pouvez maintenant ouvrir des interfaces de données vers les connexions HTTPS (pour Firepower Device Manager) et SSH (pour CLI). Vous n'avez pas besoin d'un réseau de gestion distinct pour connecter le port physique de gestion/dépistage au réseau interne pour gérer le périphérique. Sélectionnez **Device** > **System Settings** > **Management Access List** (Périphérique > Paramètres système Gestion de la liste des accès). • Le système peut obtenir des mises à jour de la base de données du système par la passerelle pour l'interface externe. Vous n'avez pas besoin d'avoir de voie de routage explicite entre l'interface ou le réseau de gestion et Internet. La valeur par défaut est d'utiliser les routages internes dans les interfaces de données. Cependant, vous pouvez définir une passerelle spécifique si vous préférez utiliser un réseau de gestion distinct. Sélectionnez**Device** > **System Settings** > **Management Interface** (Périphérique > Paramètres système > interface de gestion). • Vous pouvez utiliser Firepower Device Manager pour configurer l'interface de gestion afin d'obtenir son adresse IP par l'intermédiaire de DHCP. Sélectionnez**Device** > **System Settings** > **Management Interface** (Périphérique > Paramètres système > interface de gestion). • Vous pouvez configurer un serveur DHCP à l'adresse de gestion si vous configurez une adresse statique. Sélectionnez**Device** > **System Settings** > **Management Interface** (Périphérique > Paramètres système > interface de gestion).
Modifications diverses à l'interface utilisateur.	Voici les modifications notables apportées à l'interface utilisateur Firepower Device Manager. • Élément du menu principal **Périphérique**. Dans les versions précédentes, cet élément de menu était le nom d'hôte de votre périphérique. De plus, la page ouverte s'appelle Device Summary au lieu de Device Dashboard (Résumé du périphérique au lieu de Tableau de bord du périphérique). • Vous ne pouvez pas sélectionner une autre interface externe lors de la configuration initiale du périphérique. La première interface de données est l'interface externe par défaut. • **Device (Périphérique)** > **System Settings (Paramètres système)** > **Cloud Preferences (Préférences en nuage)** est désormais appelé **Device (Périphérique)** > **System Settings (Paramètres système)** > **URL Filtering Preferences (Préférences de filtrage d'URL)**. • La page **System Settings** > **DHCP Server** (paramètres système > serveur DHCP) est désormais organisée en deux onglets, le tableau des serveurs DHCP étant séparé des paramètres globaux.
Connexions de VPN de site à site.	Vous pouvez configurer des connexions de réseau privé virtuel (VPN) de site à site à l'aide de clés prépartagées. Vous pouvez configurer les connexions IKEv1 et IKEv2.

Fonctionnalités	Description
Prise en charge intégrée du routage et du pont.	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que le périphérique Cisco Firewall Threat Defense relie par des ponts au lieu de routes. Le périphérique Cisco Firewall Threat Defense n'est pas un vrai pont, car Cisco Firewall Threat Defense continue d'agir comme de pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Cette fonctionnalité vous permet de configurer des groupes de ponts et d'acheminer entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une alternative à l'utilisation d'un commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur le périphérique Cisco Firewall Threat Defense à affecter au groupe de ponts. Les BVI peuvent être une interface nommée et peuvent participer séparément des interfaces membres à certaines fonctionnalités, telles que le serveur DHCP, où vous configurez d'autres fonctionnalités sur les interfaces membres des groupes de ponts, comme la NAT et les règles de contrôle d'accès. Sélectionnez **Device** > **Interfaces** pour configurer un groupe de ponts (Périphérique > interfaces).

Fonctionnalités FDM dans la version 6.1.x

Tableau 16 : Fonctionnalités FDM dans la version 6.1.x

Fonctionnalités	Description
Périphériques pris en charge.	Vous pouvez gérer les types de périphériques suivants à l'aide de Firepower Device Manager : • ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X • ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X
Pris en charge en mode pare-feu.	Vous pouvez configurer des périphériques fonctionnant uniquement en mode routé. Le mode transparent n'est pas pris en charge.
Types et modes d'interface pris en charge.	Vous pouvez configurer uniquement les interfaces routées; vous ne pouvez pas configurer des interfaces en ligne, Tap en ligne ou passives. De plus, vous pouvez configurer uniquement des interfaces physiques et des sous-interfaces. Vous ne pouvez pas configurer EtherChannel ou des interfaces redondantes. Vous ne pouvez pas non plus configurer PPPoE.

Fonctionnalités	Description

Politiques de sécurité.	Vous pouvez configurer les types de politiques de sécurité suivants :
	• Contrôle d'accès : déterminez les connexions autorisées à traverser le périphérique. Vous pouvez effectuer les types de contrôle d'accès suivants :
	  • Filtrage par zone de sécurité, adresse IP, géolocalisation, protocole et port.
	  • Filtrage par nom d'utilisateur et groupe d'utilisateurs.
	  • Filtrage d'applications.
	  • Catégorie d'URL, réputation et filtrage d'URL individuelles.
	  • Politiques de prévention des intrusions, prévention des menaces.
	  • Politiques de fichiers, prévention des programmes malveillants.
	• Politiques d'identité : déterminent l'utilisateur associé à une adresse IP. Le système prend en charge l'authentification active uniquement, et non l'authentification passive.
	• Network address Translation (traduction d'adresses réseau) : conversion entre adresses internes et externes. La plupart des fonctionnalités de traduction d'adresses réseau sont prises en charge, à l'exception des réserves PAT.

Routage.	Vous pouvez configurer des routes statiques. Les protocoles de routage dynamique ne sont pas pris en charge.
Surveillance du système et syslog.	Firepower Device Manager comprend une visionneuse d'événements qui vous permet d'afficher les événements de connexion récents. Vous pouvez également configurer un serveur syslog externe pour recueillir les événements en vue d'une analyse à long terme. Il existe également de nombreux tableaux de bord qui fournissent des renseignements statistiques sur le système et le trafic qui passe par le système.
Configuration des interfaces de gestion.	Vous pouvez configurer l'adresse de gestion et l'interface à partir de Firepower Device Manager; vous n'avez pas besoin d'utiliser l'interface de ligne de commande. Vous pouvez configurer le nom d'hôte du système, l'adresse IP de gestion et la passerelle, les serveurs DNS, les serveurs NTP et les règles d'accès pour limiter les adresses IP qui peuvent accéder à l'interface de commande en ligne ou à Firepower Device Manager.

Fonctionnalités	Description
Planification de mises à jour.	Vous pouvez contrôler la fréquence de mise à jour des bases de données du système. • Élément du menu principal **Périphérique**. Dans les versions précédentes, cet élément de menu était le nom d'hôte de votre périphérique. De plus, la page ouverte s'appelle Device Summary au lieu de Device Dashboard (Résumé du périphérique au lieu de Tableau de bord du périphérique). • Vous ne pouvez pas sélectionner une autre interface externe lors de la configuration initiale du périphérique. La première interface de données est l'interface externe par défaut. • **Device (Périphérique)** > **System Settings (Paramètres système)** > **Cloud Preferences (Préférences en nuage)** est désormais appelé **Device (Périphérique)** > **System Settings (Paramètres système)** > **URL Filtering Preferences (Préférences de filtrage d'URL)**. • La page **System Settings** > **DHCP Server** (paramètres système > serveur DHCP) est désormais organisée en deux onglets, le tableau des serveurs DHCP étant séparé des paramètres globaux.
Sauvegarde et restauration.	Vous pouvez sauvegarder le système et le restaurer à partir de Firepower Device Manager.
Résolution de problèmes des fichiers.	Vous pouvez générer un fichier de dépannage à partir de Firepower Device Manager lorsque vous travaillez avec le service d'assistance technique de Cisco.

Dates de publication

Tableau 17 : Dates de la version 7.7

Version	Créer	Date	Plateformes
7.7.10	À déterminer	À déterminer	Tous
7.7.0	91	2025-03-14	Centre de gestion
	89	2025-03-05	Tous les appareils

Tableau 18 : Dates de la version 7.6

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
7.6.1	291	2025-06-02	Tous les types de documents	Tous les types de documents
7.6.0	113	16 septembre 2024	Tous les types de documents	Tous les types de documents
	41	2024-06-27	—	N'est plus disponible.

Tableau 19 : Dates de la version 7.4

Version	Créer	Date	Plateformes
7.4.2.3	4	2025-06-17	Tous
7.4.2.2	28	2025-03-03	Tous les types de documents
7.4.2.1	30	2024-10-09	Tous les types de documents
7.4.2	172	2024-07-31	Tous les types de documents
7.4.1.1	12	2024-04-15	Tous les types de documents
7.4.1	172	2023-12-13	Tous les types de documents
7.4.0	81	2023-09-07	Centre de gestion Cisco Secure Firewall 4200 series

Tableau 20 : Dates de la version 7.3

Version	Créer	Date	Plateformes
7.3.1.2	79	2024-05-09	Tous les types de documents
7.3.1.1	83	2023-08-24	Tous les types de documents
7.3.1	19	2023-03-14	Tous les types de documents
7.3.0	69	2022-11-29	Tous les types de documents

Tableau 21 : Dates de la version 7.2

Version	Créer	Date	Plateformes
7.2.10	210	2025-05-22	Tous les types de documents
7.2.9	44	2024-10-22	Tous les types de documents
7.2.8.1	17	2024-08-26	Tous les types de documents
7.2.8	25	2024-06-24	Tous les types de documents
7.2.7	500	2024-04-29	Tous les types de documents
7.2.6	168	2024-04-22	N’est plus disponible.
	167	2024-03-19	N’est plus disponible.
7.2.5.2	4	2024-05-06	Tous les types de documents
7.2.5.1	29	2023-11-14	Tous les types de documents
7.2.5	208	2023-07-27	Tous les types de documents

Version	Créer	Date	Plateformes
7.2.4.1	43	2023-07-27	Tous les types de documents
7.2.4	169	10-05-2023	Centre de gestion
	165	2023-05-03	Appareils
7.2.3.1	13	2023-04-18	Centre de gestion
7.2.3	77	2023-02-27	Tous les types de documents
7.2.2	54	2022-11-29	Tous les types de documents
7.2.1	40	2022-10-03	Tous les types de documents
7.2.0.1	12	2022-08-10	Tous les types de documents
7.2.0	82	2022-06-06	Tous les types de documents

Tableau 22 : Dates de la version 7.1

Version	Créer	Date	Plateformes
7.1.0.3	108	2023-03-15	Tous les types de documents
7.1.0.2	28	2022-08-03	FMC/FMCv Cisco Secure Firewall 3100 series
7.1.0.1	28	2022-02-24	FMC/FMCv Tous les périphériques, sauf Cisco Secure Firewall série 3100
7.1.0	90	2021-12-01	Tous les types de documents

Tableau 23 : Dates de la version 7.0

Version	Créer	Date	Plateformes
7.0.7	519	2025-02-14	FTD/FTDv
	518	2025-01-29	FMC/FMCv ASA FirePOWER NGIPSv
7.0.6.3	50	2024-09-10	Tous les types de documents
7.0.6.2	65	2024-04-15	Tous les types de documents
7.0.6.1	36	2023-11-13	Tous les types de documents
7.0.6	236	2023-07-18	Tous les types de documents

Version	Créer	Date	Plateformes
7.0.5.1	5	2023-04-26	NGIPSv Pour les périphériques dont la conformité aux certifications de sécurité est activée (mode CC/UCAPL). À utiliser avec un FMC version 7.0.5.
7.0.5	72	2022-11-17	Tous les types de documents
7.0.4	55	2022-08-10	Tous les types de documents
7.0.3	37	2022-06-30	Tous les types de documents
7.0.2.1	10	2022-06-27	Tous les types de documents
7.0.2	88	2022-05-05	Tous les types de documents
7.0.1.1	11	2022-02-17	Tous les types de documents
7.0.1	84	2021-10-07	Tous les types de documents
7.0.0.1	15	2021-07-15	Tous les types de documents
7.0.0	94	2021-05-26	Tous les types de documents

Tableau 24 : Dates de la version 6.7

Version	Créer	Date	Plateformes
6.7.0.3	105	2022-02-17	Tous les types de documents
6.7.0.2	24	2021-05-11	Tous les types de documents
6.7.0.1	13	2021-03-24	Tous les types de documents
6.7.0	65	2020-11-02	Tous les types de documents

Tableau 25 : Dates de la version 6.6

Version	Créer	Date	Plateformes
6.6.7.2	11	2024-04-24	Tous les types de documents
6.6.7.1	42	2023-01-26	Tous les types de documents
6.6.7	223	2022-07-14	Tous les types de documents
6.6.5.2	14	2022-03-24	Tous les types de documents
6.6.5.1	15	2021-12-06	Tous les types de documents
6.6.5	81	2021-08-03	Tous les types de documents

Version	Créer	Date	Plateformes
6.6.4	64	2021-04-29	Série Firepower 1000
	59	2021-04-26	FMC/FMCv Tous les périphériques, sauf Firepower série 1000
6.6.3	80	2021-03-11	Tous les types de documents
6.6.1	91	2020-09-20	Tous les types de documents
	90	2020-09-08	—
6.6.0.1	7	2020-07-22	Tous les types de documents
6.6.0	90	2020-05-08	Firepower 4112
		2020-04-06	FMC/FMCv Tous les périphériques, sauf Firepower série 4112

Tableau 26 : Dates de la version 6.5

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.5.0.5	95	2021-02-09	Tous les types de documents	—
6.5.0.4	57	2020-03-02	Tous les types de documents	—
6.5.0.3	30	03-02-2020	N'est plus disponible.	—
6.5.0.2	57	2019-12-19	Tous les types de documents	—
6.5.0.1	35	2019-11-20	N'est plus disponible.	—
6.5.0	123	03-02-2020	FMC/FMCv	FMC/FMCv
	120	08-10-2019	—	—
	115	2019-09-26	Tous les appareils	Tous les appareils

Tableau 27 : Dates de la version 6.4

Version	Créer	Date	Plateformes
6.4.0.18	24	2024-04-24	Tous les types de documents
6.4.0.17	26	2023-09-28	Tous les types de documents
6.4.0.16	50	2022-11-21	Tous les types de documents
6.4.0.15	26	2022-05-31	Tous les types de documents
6.4.0.14	67	2022-02-18	Tous les types de documents

Version	Créer	Date	Plateformes
6.4.0.13	57	2021-12-02	Tous les types de documents
6.4.0.12	112	2021-05-12	Tous les types de documents
6.4.0.11	11	2021-01-11	Tous les types de documents
6.4.0.10	95	2020-10-21	Tous les types de documents
6.4.0.9	62	2020-05-26	Tous les types de documents
6.4.0.8	28	2020-01-29	Tous les types de documents
6.4.0.7	53	2019-12-19	Tous les types de documents
6.4.0.6	28	2019-10-16	N’est plus disponible.
6.4.0.5	23	2019-09-18	Tous les types de documents
6.4.0.4	34	2019-08-21	Tous les types de documents
6.4.0.3	29	2019-07-17	Tous les types de documents
6.4.0.2	35	03-07-2019	FMC/FMCv FTD/FTDv, sauf série Firepower 1000
	34	2019-06-27	—
		2019-06-26	Série Firepower 7000/8000 ASA FirePOWER NGIPSv

Version	Créer	Date	Plateformes
6.4.0.1	17	2019-06-27	FMC 1600, 2600, 4600
		2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 avec modules SM-40, SM-48 et SM-56
		2019-05-15	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 avec modules SM-24, SM-36 et SM-44 ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Série Firepower 7000/8000 NGIPSv
6.4.0	113	03-03-2020	FMC/FMCv
	102	2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 avec modules SM-40, SM-48 et SM-56
		2019-06-13	Firepower 1010, 1120, 1140
		2019-04-24	Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 avec modules SM-24, SM-36 et SM-44 ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Série Firepower 7000/8000 NGIPSv

Tableau 28 : Dates de la version 6.3

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.3.0.5	35	2019-11-18	Série Firepower 7000/8000 NGIPSv	—
	34	2019-11-18	FMC/FMCv Tous les périphériques Cisco FTD ASA FirePOWER	—
6.3.0.4	44	2019-08-14	Tous les types de documents	—
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600	—
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les appareils	—
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600	—
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les appareils	—
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600	—
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les appareils	—
6.3.0	85	22-01-2019	Firepower 4100/9300	Firepower 4100/9300
	84	18-12-2018	FMC/FMCv ASA FirePOWER	—
	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	Tous les périphériques Cisco FTD, sauf Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMC virtuel Tous les périphériques, sauf Firepower 4100/9300

Tableau 29 : Dates de la version 6.2.3

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.2.3.18	50	2022-02-16	Tous les types de documents	—
6.2.3.17	30	2021-06-21	Tous les types de documents	—
6.2.3.16	59	2020-07-13	Tous les types de documents	—
6.2.3.15	39	2020-02-05	FTD/FTDv	—
	38	2019-09-18	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.14	41	03-07-2019	Tous les types de documents	—
	36	2019-06-12	Tous les types de documents	—
6.2.3.13	53	2019-05-16	Tous les types de documents	—
6.2.3.12	80	2019-04-17	Tous les types de documents	—
6.2.3.11	55	17-03-2019	Tous les types de documents	—
	53	2019-03-13	—	—
6.2.3.10	59	2019-02-07	Tous les types de documents	—
6.2.3.9	54	2019-01-10	Tous les types de documents	—
6.2.3.8	51	2019-01-02	N'est plus disponible.	—
6.2.3.7	51	2018-11-15	Tous les types de documents	—
6.2.3.6	37	2018-10-10	Tous les types de documents	—
6.2.3.5	53	06-11-2018	FTD/FTDv	—
	52	2018-09-12	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.4	42	2018-08-13	Tous les types de documents	—
6.2.3.3	76	2018-07-11	Tous les types de documents	—

Version	Créer	Date	Plateformes : mise à niveau	Plateformes : recréation d'image
6.2.3.2	46	2018-06-27	Tous les types de documents	—
	42	2018-06-06	—	—
6.2.3.1	47	2018-06-28	Tous les types de documents	—
	45	2018-06-21	—	—
	43	2018-05-02	—	—
6.2.3	113	01-06-2020	FMC/FMCv	FMC/FMCv
	111	25-11-2019	—	FTDv : AWS, Azure
	110	14-06-2019	—	—
	99	07-09-2018	—	—
	96	26-07-2018	—	—
	92	05-07-2018	—	—
	88	11-06-2018	—	—
	85	09-04-2018	—	—
	84	09-04-2018	Série Firepower 7000/8000 NGIPSv	—
	83	02-04-2018	FTD/FTDv ASA FirePOWER	FTD : Plateformes physiques FTDv : VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
	79	2018-03-29	—	—

Tableau 30 : Dates de la version 6.2.2

Version	Créer	Date	Plateformes
6.2.2.5	57	2018-11-27	Tous les types de documents

Version	Créer	Date	Plateformes
6.2.2.4	43	2018-09-21	FTD/FTDv
	34	2018-07-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018-06-15	—
6.2.2.3	69	2018-06-19	Tous les types de documents
	66	2018-04-24	—
6.2.2.2	109	2018-02-28	Tous les types de documents
6.2.2.1	80	2017-12-05	Série Firepower 2100
	78	2017-11-20	—
	73	2017-11-06	FMC/FMCv Tous les périphériques, sauf Firepower série 2100
6.2.2	81	2017-09-05	Tous les types de documents

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.