Mise à niveau Firewall Threat Defense

Ce chapitre explique comment utiliser un Version 7.2 On-Prem Firewall Management Center pour mettre à niveau Firewall Threat Defense. Si votre On-Prem Firewall Management Center exécute une version différente ou si vous utilisez Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), consultez Ce guide est-il pour vous?.

Liste de contrôle des mises à niveau pour Firewall Threat Defense

Planification et faisabilité

Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

✓	Action/Vérification	Détails
	Évaluez votre déploiement.	Comprendre où vous êtes détermine comment vous atteindrez votre objectif. En plus des informations sur la version et le modèle actuels, déterminez si votre déploiement est configuré pour une haute disponibilité/évolutivité, si vos appareils sont déployés en tant qu'IPS ou pare-feu, etc.

✓	Action/Vérification	Détails
	Planifiez votre chemin de mise à niveau.	Cela est particulièrement important pour les déploiements importants, les mises à niveau multisauts et les situations où vous devez mettre à niveau des systèmes d'exploitation ou des environnements d'hébergement. Les mises à niveau peuvent être majeures (A.x), de maintenance (A.x.y) ou de correctifs (A.x.y.z). Voir : • Chemin de mise à niveau pour On-Prem Firewall Management Center • Chemins de mise à niveau pour Firewall Threat Defense, à la page 7 • Chemins de mise à niveau pour FXOS
	Lisez les directives de mise à niveau et prévoyez les modifications de configuration.	Surtout avec les mises à niveau majeures, la mise à niveau peut entraîner ou nécessiter des modifications de configuration importantes avant ou après la mise à niveau. Commencez par celles-ci : • Directives relatives aux mises à niveau logicielles, pour les directives relatives aux mises à niveau critiques et spécifiques aux versions. • Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version, pour les fonctionnalités nouvelles et obsolètes qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions entre votre version actuelle et la version cible. • Cisco Secure Firewall Threat Defense Notes de mise à jour, dans le chapitre *Bogues ouverts et résolus*, pour les bogues qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions des notes de mise à jour entre votre version actuelle et la version cible. Si vous disposez d'un contrat d'assistance, vous pouvez utiliser l'Outil de recherche de bogues pour obtenir des listes de bogues à jour. • Notes de version Cisco Firepower 4100/9300 FXOS, pour les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300.

✓	Action/Vérification	Détails
	Décidez s'il faut utiliser l'assistant ou la page System Updates (Mises à jour du système).	Certains des éléments de la liste de contrôle font référence à l'utilisation de l'assistant de mise à niveau de Firewall Threat Defense sur la page System Updates (Mises à jour du système). L'assistant vous guide à travers les étapes de mise à niveau importantes, y compris la sélection des périphériques à mettre à niveau, la copie de l'ensemble de mises à niveau sur les périphériques, ainsi que les vérifications de la compatibilité et de l'état de préparation. Les mises à niveau effectuées avec cet assistant sont maintenant plus faciles, plus rapides, plus fiables et elles prennent moins d'espace disque. Nous vous recommandons généralement d'utiliser l'assistant pour mettre à niveau Firewall Threat Defense. Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0 cependant, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour**. Vous devez également utiliser la page System Updates (mises à jour du système) pour gérer la des paquets de mise à niveau et pour mettre à niveau les périphériques On-Prem Firewall Management Center et les périphériques plus anciens.
	Vérifiez l'accès à l'appareil.	Les périphériques peuvent arrêter de transmettre le trafic pendant la mise à niveau ou en cas d'échec de celle-ci. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique . Vous devriez également pouvoir accéder à l'interface de gestion du On-Prem Firewall Management Center sans traverser le périphérique.
	Vérifiez la bande passante.	Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Chaque fois que cela est possible, chargez les paquets de mise à niveau à l'avance. Si vous transférez un ensemble de mise à niveau vers un périphérique au moment de la mise à niveau, une bande passante insuffisante peut prolonger le délai de mise à niveau ou même entraîner son expiration. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).
	Planifiez des périodes de maintenance.	Planifiez les périodes de maintenance lorsqu'elles auront le moins d'impact, en tenant compte de tout effet sur le flux de trafic et l'inspection, et le temps que les mises à niveau sont susceptibles de prendre. Tenez compte des tâches que vous devez effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Voir : • Flux de trafic et inspection pour les mises à niveau de châssis • Tests de temps et d'espace disque

Sauvegardes

À l'exception des correctifs rapides, la mise à niveau supprime toutes les sauvegardes stockées sur le système. Nous vous recommandons *fortement* de procéder à une sauvegarde dans un emplacement distant sécurisé et de vérifier la réussite du transfert, avant et après la mise à niveau :

- Avant la mise à niveau : si une mise à niveau échoue de manière catastrophique, vous devrez peut-être effectuer une réinitialisation et une restauration. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Si vous avez une sauvegarde récente, vous pouvez revenir aux opérations normales plus rapidement.
- Après la mise à niveau : cela crée un instantané de votre déploiement nouvellement mis à niveau. Sauvegardez On-Prem Firewall Management Center après la mise à niveau de ses périphériques gérés, afin que votre nouveau fichier de sauvegarde On-Prem Firewall Management Center « sache » que ses périphériques ont été mis à niveau.

✓	Action/Vérification	Détails
	Sauvegardez Firewall Threat Defense.	Utilisez le On-Prem Firewall Management Center pour sauvegarder les configurations Firewall Threat Defense, lorsqu'elles sont prises en charge. Consultez le chapitre *Sauvegarde/restauration* dans le Guide d'administration Cisco Secure Firewall Management Center. Si vous avez un Firepower 9300 avec Firewall Threat Defense et des périphériques logiques ASA s'exécutant sur des modules distincts, utilisez ASDM ou l'interface de ligne de commande d'ASA pour sauvegarder les configurations et les autres fichiers critiques, en particulier s'il y a une migration de la configuration de l'ASA. Consultez le chapitre *Logiciels et configurations* du Guide de configuration des opérations générales de la gamme Cisco ASA.
	Sauvegardez FXOS sur le Firepower 4100/9300.	Utilisez le Firewall Chassis Manager ou l'interface de ligne de commande de FXOS pour exporter les configurations des châssis, y compris les paramètres de configuration des périphériques logiques et de la plateforme. Consultez le chapitre *Importation et exportation de la configuration* du Guide de configuration de Cisco Firepower 4100/9300 FXOS.

Progiciels de mise à niveau

Le chargement des paquets de mise à niveau vers le système avant de commencer la mise à niveau peut réduire la durée de votre fenêtre de maintenance.

✓	Action/Vérification	Détails
	Téléchargez les paquets de mise à niveau à partir de Cisco et chargez-les sur le On-Prem Firewall Management Center ou le serveur web interne.	Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco : Paquets de mise à niveau pour On-Prem Firewall Management Center et Firewall Threat Defense, à la page 13. Vous pouvez également utiliser le On-Prem Firewall Management Center pour effectuer un téléchargement direct. Chargez les paquets de mise à niveau des périphériques sur le On-Prem Firewall Management Center ou configurez les périphériques pour les obtenir à partir d'un serveur interne : • Chargez les paquets de mise à niveau Firewall Threat Defense vers le On-Prem Firewall Management Center, à la page 14 • Chargez les paquets de mise à niveau Firewall Threat Defense sur un serveur interne, à la page 15 Pour les périphériques Firepower 4100/9300, les instructions de chargement FXOS sont incluses dans les procédures de mise à niveau FXOS.
	Copiez les paquets de mise à niveau vers les périphériques.	Pour mettre à niveau Firewall Threat Defense, le paquet de mise à niveau doit se trouver sur le périphérique. L'assistant de mise à niveau de Threat Defense vous invite à copier les paquets de mise à niveau sur les périphériques qui en ont besoin. Sinon, vous pouvez utiliser la page System Updates (Mises à jour du système).

Mises à niveau associées

Étant donné que les mises à niveau de systèmes d'exploitation et d'environnements d'hébergement peuvent avoir une incidence sur le flux de trafic et l'inspection, effectuez-les pendant une période de maintenance.

✓	Action/Vérification	Détails
	Mettez à niveau l'hébergement virtuel.	Si nécessaire, mettez à niveau l'environnement d'hébergement. Si cela est nécessaire, c'est généralement parce que vous utilisez une ancienne version de VMware et effectuez une mise à niveau majeure.
	Mettez à niveau le micrologiciel sur le Firepower 4100/9300.	Nous vous recommandons d'utiliser le micrologiciel le plus récent. Consultez la section CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS.
	Mettez à niveau FXOS sur le Firepower 4100/9300.	La mise à niveau de FXOS est généralement requise pour les mises à niveau majeures, mais très rare pour les versions de maintenance et les correctifs. Pour minimiser les perturbations, mettez à niveau FXOS dans les paires à haute accessibilité Firewall Threat Defense et les grappes inter-châssis, un châssis à la fois. Consultez Mettre à niveau le châssis sur le Firepower 4100/9300.

Contrôle final

Un ensemble de vérifications finales garantit que vous êtes prêt à mettre à niveau le logiciel.

✓	Action/Vérification	Détails
	Vérifiez les configurations.	Assurez-vous d'avoir apporté les modifications de configuration requises avant la mise à niveau et d'être prêt à apporter les modifications de configuration requises après la mise à niveau.
	Vérifiez la synchronisation NTP.	Assurez-vous que tous les périphériques sont synchronisés avec le serveur NTP que vous utilisez pour donner l'heure. Bien que le moniteur d'intégrité signale si les horloges ne sont pas synchronisées de plus de 10 secondes, il convient de toujours vérifier manuellement. La désynchronisation peut entraîner l'échec de la mise à niveau. Pour vérifier l'heure : • On-Prem Firewall Management Center : Choisissez **Système** (⚙) > **Configuration** > **Time (Heure)**. • Firewall Threat Defense : Utilisez la commande **show time** de l'interface de ligne de commande.
	Déployez des configurations.	Si vous procédez au déploiement des configurations avant la mise à niveau, vous réduisez les risques d'échec. Le déploiement peut affecter le flux de trafic et l'inspection; voir Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense.
	Exécutez la vérification de l'état de préparation.	La réussite des vérifications de l'état de préparation réduit considérablement les risques d'échec de la mise à niveau. L'assistant de mise à niveau de Firewall Threat Defense vous invite à effectuer des vérifications de l'état de préparation. Sinon, vous pouvez utiliser la page System Updates (Mises à jour du système).
	Vérifiez l'espace disque.	Les vérifications de l'état de préparation comprennent une vérification de l'espace disque. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Pour vérifier l'espace disque disponible sur un périphérique, choisissez **Système** (⚙) > **Monitoring (Surveillance)** > **Statistics (Statistiques** et sélectionnez le périphérique que vous souhaitez vérifier. Sous Disk Usage (Utilisation du disque), développez les informations de By partition (Par partition).

✓	Action/Vérification	Détails
	Vérifiez les tâches en cours.	Assurez-vous que les tâches essentielles sont terminées avant de procéder à la mise à niveau. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Les mises à niveau à partir de la version 6.6.3 ou ultérieure reportent automatiquement les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. Si vous ne souhaitez pas que cela se produise (ou si vous effectuez une mise à niveau à partir d'une version antérieure), vérifiez les tâches programmées pour s'exécuter lors de la mise à niveau et annulez ou reportez-les.

Chemins de mise à niveau pour Firewall Threat Defense

Choisissez le chemin de mise à niveau qui correspond à votre déploiement.

Mettez d'abord le On-Prem Firewall Management Center à niveau. Vous ne pouvez pas mettre à niveau un périphérique au-delà du On-Prem Firewall Management Center vers une version majeure ou de maintenance plus récente. Bien qu'un périphérique corrigé (quatre chiffres) puisse être géré avec un On-Prem Firewall Management Centernon corrigé, les déploiements entièrement corrigés sont soumis à des tests avancés.

Chemin de mise à niveau pour Firewall Threat Defense sans FXOS

Ce tableau fournit le chemin de mise à niveau pour Firewall Threat Defense lorsque vous n'avez pas besoin de mettre à niveau le système d'exploitation. Cela comprend Cisco Secure Firewall 3100 en mode périphérique, les séries Firepower 1000/2100, la série ASA-5500-X et l'ISA 3000.

Notez que si votre version actuelle Firewall Threat Defense/On-Prem Firewall Management Center est publiée après une date postérieure à celle de votre version cible, vous ne pourrez peut-être pas mettre à niveau comme prévu. Dans ces cas, la mise à niveau échoue rapidement et affiche une erreur expliquant qu'il existe des incompatibilités de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Remarque En raison des modifications de l'interface requises pour prendre en charge l'évolutivité automatique, les mises à niveau de Threat Defense Virtual pour GCP ne peuvent pas dépasser la version 7.2.0. C'est-à-dire que vous ne pouvez pas mettre à niveau vers la version 7.2.0+ à partir de la version 7.1.x ou des versions antérieures. Vous devez déployer une nouvelle instance et refaire toutes les configurations propres au périphérique.

Tableau 1 : Mises à niveau directes de Firewall Threat Defense

Version actuelle	Version cible
7.4	→ Toute version ultérieure à 7.4.x

Version actuelle	Version cible
7.3	Une des versions suivantes : → 7.4.x → Toute version ultérieure à 7.3.x
7.2	Une des versions suivantes : → 7.4.x → 7.3.x → Toute version ultérieure à 7.2.x **Remarque** Le Firepower 1010E, introduit dans la version 7.2.3, n'est pas pris en charge dans la version 7.3. L'assistance revient dans la version 7.4.1.
7.1	Une des versions suivantes : → 7.4.x → 7.3.x → 7.2.x → Toute version ultérieure à 7.1.x
7.0 Dernière prise en charge pour ASA 5508-X et 5516-X.	Une des versions suivantes : → 7.4.x → 7.3.x → 7.2.x → 7.1.x → Toute version ultérieure à 7.0.x **Remarque** En raison d'incompatibilités avec le magasin de données, vous ne pouvez pas mettre à niveau de la version 7.0.4+ à la version 7.1.0. Nous vous recommandons de mettre à niveau directement vers la version 7.2+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer Firewall Threat Defense les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.

Version actuelle	Version cible
6.7	Une des versions suivantes : → 7.2.x → 7.1.x → 7.0.x → Toute version ultérieure à 6.7.x
6.6 Dernière prise en charge pour ASA 5525-X, 5545-X et 5555-X.	Une des versions suivantes : → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Toute version ultérieure à 6.6.x
6.5	Une des versions suivantes : → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Dernière prise en charge pour ASA 5515-X.	Une des versions suivantes : → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Une des versions suivantes : → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 Dernière prise en charge pour la série ASA 5506-X.	Une des versions suivantes : → 6.6.x → 6.5 → 6.4 → 6.3

Chemin de mise à niveau pour Firewall Threat Defense avec FXOS

Ce tableau fournit le chemin de mise à niveau pour Firewall Threat Defense sur le Firepower 4100/9300.

Notez que si votre version actuelle Firewall Threat Defense/On-Prem Firewall Management Center est publiée après une date postérieure à celle de votre version cible, vous ne pourrez peut-être pas mettre à niveau comme prévu. Dans ces cas, la mise à niveau échoue rapidement et affiche une erreur expliquant qu'il existe des incompatibilités de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Ce tableau répertorie nos combinaisons de versions spécialement qualifiées. Comme vous devez d'abord mettre à niveau FXOS, vous exécuterez brièvement une combinaison prise en charge, mais non recommandée, dans laquelle le système d'exploitation est « en avance » sur le logiciel du périphérique. Assurez-vous que la mise à niveau de FXOS ne vous rend pas compatible avec des périphériques logiques ou des instances d'applications. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Tableau 2 : Firewall Threat Defense Mises à niveau directes sur Firepower 4100/9300

Versions actuelles	Versions cibles
FXOS 2.13 avec Firewall Threat Defense7.3	→ FXOS 2.13 avec toute version ultérieure de Firewall Threat Defense 7.3.x
FXOS 2.12 avec Firewall Threat Defense 7.2 Dernière prise en charge de Firepower 4110, 4120, 4140, 4150. Dernière prise en charge de l'appareil Firepower 9300 avec les modules SM-24, SM-36 ou SM-44.	Une des versions suivantes : → FXOS 2.13 avec Firewall Threat Defense 7.3.x → FXOS 2.12 avec toute version ultérieure de Firewall Threat Defense 7.2.x
FXOS 2.11.1 avec Firewall Threat Defense 7.1	Une des versions suivantes : → FXOS 2.13 avec Firewall Threat Defense 7.3.x → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec toute version ultérieure de Firewall Threat Defense 7.1.x

Versions actuelles	Versions cibles
FXOS 2.10.1 avec Firewall Threat Defense 7.0	Une des versions suivantes : → FXOS 2.13 avec Firewall Threat Defense 7.3.x → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec toute version ultérieure de Firewall Threat Defense 7.0.x **Remarque** En raison d'incompatibilités avec le magasin de données, vous ne pouvez pas mettre à niveau de la version 7.0.4+ à la version 7.1.0. Nous vous recommandons de mettre à niveau directement vers la version 7.2+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer Firewall Threat Defense les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.
FXOS 2.9.1 avec Firewall Threat Defense 6.7	Une des versions suivantes : → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec toute version ultérieure de Firewall Threat Defense 6.7.x
FXOS 2.8.1 avec Firewall Threat Defense 6.6	Une des versions suivantes : → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec toute version ultérieure de Firewall Threat Defense 6.6.x

Versions actuelles	Versions cibles
FXOS 2.7.1 avec Firewall Threat Defense 6.5	Une des versions suivantes : → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x
FXOS 2.6.1 avec Firewall Threat Defense 6.4	Une des versions suivantes : → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5
FXOS 2.4.1 avec Firewall Threat Defense 6.3	Une des versions suivantes : → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5 → FXOS 2.6.1 avec Firewall Threat Defense 6.4
FXOS 2.3.1 avec Firewall Threat Defense 6.2.3	Une des versions suivantes : → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5 → FXOS 2.6.1 avec Firewall Threat Defense 6.4 → FXOS 2.4.1 avec Firewall Threat Defense 6.3

Ordre de mise à niveau pour Firewall Threat Defense haute disponibilité/évolutivité avec FXOS

Même dans les déploiements à disponibilité et à évolutivité élevées, vous pouvez mettre à niveau FXOS sur chaque châssis indépendamment. Pour réduire au minimum les perturbations, mettez à niveau FXOS un châssis à la fois. Pour les mises à niveau Firewall Threat Defense, le système met automatiquement à niveau un périphérique groupé à la fois.

Tableau 3 : Ordre de mise à niveau FXOS-Threat Defense pour Firepower 4100/9300

Firewall Threat DefenseDéploiement	Commande de mise à niveau
Autonomes	**1.** Mettez à niveau FXOS. **2.** Mettez à niveau Firewall Threat Defense.

Firewall Threat DefenseDéploiement	Commande de mise à niveau
Haute disponibilité	Mettez à niveau FXOS sur les deux châssis avant de mettre à niveau Firewall Threat Defense. Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. **1.** Mettez à niveau FXOS sur le châssis avec le serveur de secours. **2.** Changez de rôle. **3.** Mettez à niveau FXOS sur le châssis avec le nouveau serveur de secours. **4.** Mettez à niveau Firewall Threat Defense.
Grappe intra-châssis (unités sur le même châssis)	**1.** Mettez à niveau FXOS. **2.** Mettez à niveau Firewall Threat Defense.
Grappe inter-châssis (unités sur des châssis différents)	Mettez à niveau FXOS sur tous les châssis avant de mettre à niveau Firewall Threat Defense. Pour réduire au minimum les perturbations, mettez toujours à niveau un châssis d'unités de données. **1.** Mettez à niveau FXOS sur un châssis de l'unité de données. **2.** Basculez le module de contrôle sur le châssis que vous venez de mettre à niveau. **3.** Mettez à niveau FXOS sur les châssis restants. **4.** Mettez à niveau Firewall Threat Defense.

Paquets de mise à niveau pour On-Prem Firewall Management Center et Firewall Threat Defense

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco : https://www.cisco.com/go/ftd-software.

Vous utilisez le même ensemble de mises à niveau pour tous les modèles d'une famille ou d'une série. Pour trouver le bon modèle, sélectionnez ou recherchez votre modèle sur le Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Notez que les paquets de mise à niveau à sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Tableau 4 : Paquets de mise à niveau logicielle

Plateforme	Paquet de mise à niveau
Série Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar
Série Firepower 2100	Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar
Cisco Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Cisco Secure Firewall 4200 series	Cisco_Secure_FW_TD_4200_Upgrade-7.2-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Firewall Threat Defense Virtual	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar
ISA 3000 avec FTD	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar

Astuces Sélectionnez les paquets de mise à niveau disponibles pour le téléchargement direct quelque temps après que la version puisse être téléchargée manuellement. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs. SI le On-Prem Firewall Management Center dispose d'un accès Internet, cliquez sur **Download Updates** (Télécharger les mises à jour)**Système** (⚙) > **Mises à jour** pour télécharger immédiatement la dernière VDB, la dernière version de maintenance et les derniers correctifs critiques pour le On-Prem Firewall Management Center et tous les périphériques gérés.

Chargez les paquets de mise à niveau Firewall Threat Defense vers le On-Prem Firewall Management Center

sont des archives TAR signées (.tar). Après avoir téléchargé un paquet signé, la page System Updates peut prendre plus de temps à se téléverser pendant la vérification du paquet. Pour accélérer l'affichage, supprimez les ensembles de mises à niveau inutiles. Ne pas décompresser les paquets signés.

Procédure

Étape 1 Dans On-Prem Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

Étape 2 Cliquez sur **Charger la mise à jour**.

Étape 3 Pour l'**Action**, cliquez sur le bouton radio **Upload local software update package** (Charger le paquet de mise à jour du logiciel local).

Étape 4 Cliquez sur **Choisir le fichier**.

Étape 5 Accédez au paquet et cliquez sur **Charger**.

Étape 6 (Facultatif) Copiez les paquets de mise à niveau vers les périphériques gérés.

Si vous n'avez pas besoin d'activer la restauration et que vous prévoyez donc d'utiliser l'assistant de mise à niveau Firewall Threat Defense, l'assistant vous demandera de copier le paquet. Si vous utilisez la page System Updates (Mises à jour de système) pour effectuer la mise à niveau parce que vous souhaitez activer le rétablissement, nous vous recommandons de copier les paquets de mise à niveau sur les périphériques maintenant, comme suit :

a) Cliquez sur l'icône **Push or Stage Update** (Pousser la mise à jour ou lui affecter une étape) à côté du paquet de mise à niveau que vous souhaitez copier.
b) Choisissez les périphériques de destination.

   Vous pouvez copier le paquet sur tous les périphériques admissibles maintenant, ou vous pouvez le copier dans un sous-ensemble, puis utiliser l'interface de ligne de commande Firewall Threat Defense pour copier le paquet de mise à niveau entre les périphériques; voir Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques, à la page 16.

   Si les périphériques dans lesquels vous souhaitez pousser le paquet de mise à niveau ne sont pas répertoriés, vous avez choisi le mauvais paquet de mise à niveau.

c) Cliquez sur **Push** (Pousser).

Chargez les paquets de mise à niveau Firewall Threat Defense sur un serveur interne

Utilisez cette procédure pour configurer les périphériques Firewall Threat Defense afin d'obtenir les paquets de mise à niveau à partir d'un serveur web interne, plutôt qu'à partir du On-Prem Firewall Management Center. Cela est particulièrement utile si la bande passante entre le On-Prem Firewall Management Center et ses périphériques est limitée. Cela permet également de gagner de la place sur le On-Prem Firewall Management Center.

Pour configurer cette fonctionnalité, vous enregistrez un pointeur (URL) à l'emplacement d'un paquet de mise à niveau sur le serveur Web. Le processus de mise à niveau obtiendra ensuite le paquet de mise à niveau du serveur web au lieu du On-Prem Firewall Management Center. Vous pouvez également utiliser le On-Prem Firewall Management Center pour copier le paquet avant d'effectuer la mise à niveau.

Répétez cette procédure pour chaque paquet de mise à niveau. Vous ne pouvez configurer qu'un seul emplacement par paquet de mise à niveau.

Avant de commencer

Copiez les paquets de mise à niveau sur un serveur web interne auquel vos périphériques peuvent accéder. Pour les serveurs Web sécurisés (HTTPS), procurez-vous le certificat numérique du serveur (format PEM). Vous devriez pouvoir obtenir le certificat de l'administrateur du serveur. Vous pouvez également utiliser votre navigateur ou un outil comme OpenSSL, pour afficher les détails du certificat du serveur et exporter ou copier le certificat.

Procédure

Étape 1 Dans On-Prem Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

Étape 2 Cliquez sur **Charger la mise à jour**.

Choisissez cette option même si vous ne chargez rien. La page suivante vous demandera de fournir une URL.

Étape 3 Pour l'**action**, cliquez sur le bouton radio **Préciser la source des mises à jour logicielles**.

Étape 4 Saisissez une **URL source** pour le paquet de mise à niveau.

Fournissez le protocole (HTTP/HTTPS) et le chemin complet. Par exemple :

`https://internal_web_server/upgrade_package.sh.REL.tar`

Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif rapide) ainsi que la version du logiciel à laquelle vous passez. Assurez-vous de saisir le bon nom de fichier.

Étape 5 Pour les serveurs HTTPS, fournissez un **certificat d'autorité de certification**.

Il s'agit du certificat numérique du serveur que vous avez obtenu plus tôt. Copiez et collez le bloc de texte entier, y compris les lignes BEGIN CERTIFICATE et END CERTIFICATE.

Étape 6 Cliquez sur **Save** (enregistrer).
L'emplacement est enregistré. Les paquets de mise à niveau chargés et les URL des paquets de mise à niveau sont listés ensemble, mais étiquetés distinctement.

Étape 7 (Facultatif) Copiez les paquets de mise à niveau vers les périphériques gérés.

Si vous n'avez pas besoin d'activer la restauration et que vous prévoyez donc d'utiliser l'assistant de mise à niveau Firewall Threat Defense, l'assistant vous demandera de copier le paquet. Si vous utilisez la page System Updates (Mises à jour de système) pour effectuer la mise à niveau parce que vous souhaitez activer le rétablissement, nous vous recommandons de copier les paquets de mise à niveau sur les périphériques maintenant, comme suit :

a) Cliquez sur l'icône **Push or Stage Update** (Pousser la mise à jour ou lui affecter une étape) à côté du paquet de mise à niveau que vous souhaitez copier.
b) Choisissez les périphériques de destination.

Vous pouvez copier le paquet sur tous les périphériques admissibles maintenant, ou vous pouvez le copier dans un sous-ensemble, puis utiliser l'interface de ligne de commande Firewall Threat Defense pour copier le paquet de mise à niveau entre les périphériques; voir Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques, à la page 16.

Si les périphériques dans lesquels vous souhaitez pousser le paquet de mise à niveau ne sont pas répertoriés, vous avez choisi le mauvais paquet de mise à niveau.

c) Cliquez sur **Push** (Pousser).

Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques

Au lieu de copier les paquets de mise à niveau sur chaque périphérique à partir de On-Prem Firewall Management Center ou du serveur Web interne, vous pouvez utiliser l'interface de ligne de commande Firewall Threat Defense pour copier les paquets de mise à niveau entre les périphériques (« synchronisation homologue à homologue »). Ce partage de ressources sécurisé et fiable passe par le réseau de gestion, mais ne repose pas sur On-Prem Firewall Management Center. Chaque périphérique peut accueillir 5 transferts simultanés de paquets.

Cette fonctionnalité est prise en charge pour les périphériques autonomes de la version 7.2.x–7.4.x gérés par le même On-Prem Firewall Management Center de la version autonome 7.2.x–7.4.x. Elle n'est pas prise en charge pour :

- Instances de conteneur.
- Paires et grappes de périphériques à haute disponibilité. Ces périphériques reçoivent le paquet les uns des autres dans le cadre de leur processus de synchronisation normal. La copie de l'ensemble de mises à niveau sur un membre du groupe la synchronise automatiquement avec tous les membres du groupe.
- Périphériques gérés par des On-Prem Firewall Management Centerà haute disponibilité.
- Périphériques dans différents domaines, ou périphériques séparés par une passerelle NAT.
- Périphériques mis à niveau à partir de la version 7.1 ou d'une version antérieure, quelle que soit la version de On-Prem Firewall Management Center.
- Périphériques exécutant la version 7.6+.

Répétez la procédure suivante pour tous les périphériques qui ont besoin de l'ensemble de mise à niveau.

Avant de commencer

- Chargez le paquet de mise à niveau de Firewall Threat Defense sur le On-Prem Firewall Management Center ou sur un serveur interne.
- Copier le paquet de mise à niveau sur le périphérique.

Procédure

Étape 1 En tant `qu'administrateur`, accédez à SSH sur tout périphérique qui a besoin du paquet.

Étape 2 Activez la fonction .

configure p2psync enable

Étape 3 Si vous ne le savez pas déjà, déterminez où vous pouvez obtenir le paquet de mise à niveau dont vous avez besoin.

show peers : répertorie les autres périphériques admissibles sur lesquels cette fonctionnalité est également activée.

show peer details *ip_address* : pour le périphérique à l'adresse IP que vous spécifiez, répertoriez les paquets de mise à niveau disponibles et leurs chemins.

Étape 4 Copiez le paquet à partir de n'importe quel périphérique disposant du paquet dont vous avez besoin, en spécifiant l'adresse IP et le chemin que vous venez de découvrir.

sync-from-peer *ip_address package_path*

Après avoir confirmé que vous souhaitez copier le lot, le système affiche un UUID de l'état de synchronisation que vous pouvez utiliser pour surveiller ce transfert.

Étape 5 Surveiller l'état de transfert à partir de l'interface de ligne de commande.

show p2p-sync-status : affiche l'état de la synchronisation des cinq derniers transferts vers cet appareil, y compris les transferts terminés et ayant échoué.

show p2p-sync-status *sync_status_UUID* : affiche l'état de la synchronisation d'un transfert en particulier vers ce périphérique.

Mettre à niveau Firewall Threat Defense à l'aide de l'assistant (désactiver la restauration)

Utilisez cette procédure pour mettre à niveau Firewall Threat Defense à l'aide d'un assistant.

Au fur et à mesure que vous continuez, l'assistant affiche des informations de base sur les périphériques sélectionnés, ainsi que l'état actuel de la mise à niveau. Cela inclut toutes les raisons pour lesquelles vous ne pouvez pas mettre à niveau. Si un périphérique ne « réussit » pas une étape dans l'assistant, il ne s'affiche pas à l'étape suivante.

Si vous quittez l'assistant, votre progression est conservée et les autres utilisateurs ne peuvent pas démarrer de nouveau flux de travail de mise à niveau. (Exception : si vous êtes connecté avec un CAC, votre progression est effacée 24 heures après votre déconnexion.) Si vous devez réinitialiser le flux de travail de quelqu'un d'autre, vous devez avoir un accès administrateur. Vous pouvez supprimer ou désactiver l'utilisateur, ou mettre à jour son rôle d'utilisateur afin qu'il n'ait plus l'autorisation d'utiliser **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

Notez que ni votre flux de travail ni vos mises à niveau de défense contre les menaces ne sont synchronisés entre les On-Prem Firewall Management Center haute disponibilité. En cas de basculement, vous devez recréer votre flux de travail sur le nouveau On-Prem Firewall Management Center, ce qui comprend le chargement des paquets de mise à niveau sur On-Prem Firewall Management Center et l'exécution de vérifications de l'état de préparation. (Les paquets de mise à niveau déjà copiés sur les périphériques ne sont pas supprimés, mais le On-Prem Firewall Management Center doit toujours avoir le paquet ou un pointeur vers son emplacement.)

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes lors de la désinstallation, y compris une désinstallation échouée ou un appareil ne répondant plus, consultez Mises à niveau qui ne répondent pas.

Historique de Threat Defense :

- 7.2 : Copier les paquets de mise à niveau entre les périphériques

Avant de commencer

- Décidez si vous souhaitez utiliser cette procédure.

  Nous vous recommandons généralement d'utiliser l'assistant pour mettre à niveau Firewall Threat Defense. Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0 cependant, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour**. Vous devez également utiliser la page System Updates (mises à jour du système) pour gérer la des paquets de mise à niveau et pour mettre à niveau les périphériques On-Prem Firewall Management Center et les périphériques plus anciens.

- Terminez la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Commencez le flux de travail.

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Sélectionnez les périphériques à mettre à niveau et copiez les paquets de mise à niveau.

Étape 2 Vérifiez votre sélection de périphérique.

Pour sélectionner d'autres périphériques, revenez à la page de gestion des périphériques — votre progression ne sera pas perdue. Vous pouvez ajouter et supprimer des périphériques à votre sélection, ou cliquer sur **Reset** (Réinitialiser) pour effacer votre sélection de périphériques et recommencer.

Étape 3 Sélectionnez les périphériques que vous souhaitez mettre à niveau.

Vous pouvez mettre à niveau plusieurs périphériques à la fois. Vous devez mettre à niveau les membres des grappes de périphériques et les paires à haute disponibilité en même temps.

Important
Pour des raisons de performances, si vous mettez à niveau un périphérique *à la* version 6.6.x ou une version antérieure, nous vous recommandons *fortement* de ne pas mettre à niveau plus de cinq périphériques simultanément.

Étape 4 Dans le menu **Select Action** (Sélectionner une action) ou **Select Bulk Action** (sélectionner une action en bloc) sélectionnez **Upgrade Firepower Software** (Mettre à niveau le logiciel Firepower).

L'assistant de mise à niveau des périphériques apparaît, indiquant le nombre de périphériques que vous avez sélectionnés et vous invitant à sélectionner une version cible. La page comporte deux volets : la sélection du périphérique à gauche et les détails du périphérique à droite. Cliquez sur le lien d'un périphérique dans le volet de sélection de périphériques (par exemple, « `4 périphériques` ») pour afficher les détails du périphérique correspondant.

Notez que si un flux de travail de mise à niveau est déjà en cours, vous devez d'abord soit **fusionner les périphériques** (ajouter les nouveaux périphériques sélectionnés aux périphériques sélectionnés précédemment et continuer), soit **Réinitialiser** (éliminer les sélections précédentes et utiliser uniquement les nouveaux périphériques sélectionnés).

Étape 5 Vérifiez votre sélection de périphérique.

Pour sélectionner d'autres périphériques, revenez à la page de gestion des périphériques — votre progression ne sera pas perdue. Vous pouvez ajouter et supprimer des périphériques à votre sélection, ou cliquer sur **Reset** (Réinitialiser) pour effacer votre sélection de périphériques et recommencer.

Étape 6 Dans le menu **Upgrade to** (mettre à niveau vers), sélectionnez une version cible.

Le système détermine lesquels de vos périphériques sélectionnés peuvent être mis à niveau vers cette version. Si des périphériques ne sont pas admissibles, vous pouvez cliquer sur le lien du périphérique pour en comprendre la raison. Vous n'êtes pas tenu de retirer les périphériques non admissibles; ils sont automatiquement exclus de la mise à niveau.

Notez que les choix dans le menu **Upgrade to** correspondent aux ensembles de mise à niveau de périphériques disponibles pour le système. Si votre version cible ne figure pas dans cette liste, accédez à **Système** (⚙) > **Mises à jour** et chargez ou spécifiez l'emplacement du bon paquet de mise à niveau. Si vous mettez à niveau différents modèles de périphériques et que, par conséquent, vous avez besoin de plusieurs ensembles de mise à niveau, faites de même pour tous les ensembles de mise à niveau nécessaires avant de passer à l'étape suivante.

Étape 7 Pour tous les périphériques qui ont encore besoin d'un ensemble de mise à niveau, cliquez sur **Copier le paquet de mise à niveau**, puis confirmez votre choix.

Pour mettre à niveau Firewall Threat Defense, le paquet de mise à niveau doit se trouver sur le périphérique. La copie du paquet de mise à niveau avant la mise à niveau réduit la durée de votre fenêtre de maintenance de mise à niveau.

Astuces
Vous pouvez également utiliser l'interface de ligne de commande Firewall Threat Defense pour copier les paquets de mise à niveau d'un appareil à l'autre. Pour en savoir plus, y compris les conditions d'admissibilité, consultez Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques, à la page 16.

Étape 8 Cliquez sur **Next** (suivant).

Effectuer les vérifications finales de compatibilité et d'état de préparation, ainsi que d'autres vérifications..

Étape 9 Pour tous les périphériques qui doivent réussir la vérification de l'état de préparation, cliquez sur **Exécuter la vérification de l'état de préparation**, puis confirmez votre choix.

Bien que vous puissiez ignorer les vérifications en désactivant l'option **Exiger la réussite des contrôles de compatibilité et de préparation**, nous vous déconseillons de le faire. La réussite de tous les contrôles réduit considérablement les risques d'échec de la mise à niveau. Ne déployez *pas* de modifications, ne redémarrez pas ou n'éteignez pas manuellement un périphérique pendant l'exécution des vérifications de l'état de préparation. Si un dispositif échoue au contrôle de l'état de préparation, corrigez les problèmes et relancez ce dernier. Si le contrôle de l'état de préparation révèle des problèmes que vous ne pouvez pas résoudre, ne démarrez pas la mise à niveau. Communiquez plutôt avec Centre d'assistance technique Cisco (TAC).

Notez que les vérifications de compatibilité sont automatiques. Par exemple, le système vous alerte immédiatement si vous devez mettre à niveau FXOS ou si vous devez effectuer le déploiement sur des périphériques gérés.

Étape 10 effectuer les dernières vérifications préalables à la mise à niveau.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales.

Étape 11 Si nécessaire, retournez à **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

Étape 12 Cliquez sur **Next** (suivant).

Mettre à niveau les périphériques.

Étape 13 Vérifiez la sélection de votre périphérique et la version cible.

Étape 14 (Facultatif) Modifiez l'ordre de mise à niveau des périphériques en grappe.

Affichez les détails du périphérique pour la grappe et cliquez sur **Modifier l'ordre de mise à niveau**. L'unité de contrôle est toujours mise à niveau en dernier; vous ne pouvez pas changer cela.

Étape 15 Choisissez les options de mise à niveau.

Pour les mises à niveau majeures et de maintenance , vous pouvez :

- **Annuler automatiquement la mise à niveau en cas d'échec et restaurer la version précédente** : le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.
- **Mise à niveau de Snort 2 vers Snort 3** : après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations.

  Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une

détection et une amélioration améliorées. Pour obtenir de l'aide lors de la migration, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour votre version.

Ces options ne sont pas prises en charge pour les correctifs.

Étape 16 Cliquez sur **Start Upgrade**(commencer la mise à niveau), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Vous pouvez surveiller la progression globale de la mise à niveau dans le centre de messages. Pour une progression détaillée, utilisez la fenêtre contextuelle Upgrade Status (état de la mise à niveau), accessible à partir de l'onglet Upgrade (Mise à niveau) sur la page Device Management (gestion des périphériques) et à partir du centre de messages. Pour en savoir plus sur le traitement du trafic pendant la mise à niveau, consultez Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense.

Les périphériques peuvent redémarrer deux fois pendant la mise à niveau. Il s'agit du comportement attendu.

Confirmation de la réussite et achèvement des tâches postérieures à la mise à niveau.

Étape 17 Vérifiez la réussite.

Une fois la mise à niveau terminée, choisissez **Devices (appareils)** > **Device Management (gestion des appareils)** et confirmez que les périphériques que vous avez mis à niveau disposent de la bonne version de logiciel.

Étape 18 (Facultatif) Dans les déploiements à haute disponibilité ou en grappe, examinez les rôles des périphériques.

Le processus de mise à niveau modifie les rôles de chaque périphérique de manière à ce qu'il mette toujours à niveau une unité ou un nœud de données en attente. Il ne ramène pas les périphériques aux rôles qu'ils avaient avant la mise à niveau. Si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Étape 19 Mettez à jour les règles de prévention des intrusions et la base de données des vulnérabilités.

Bien que la mise à niveau mette souvent à jour ces composants, des nouveaux peuvent être disponibles. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 20 Apportez toutes les modifications de configuration requises après la mise à niveau.

Étape 21 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.

Snort redémarre généralement lors du premier déploiement après la mise à niveau. Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur tous les périphériques, y compris ceux qui sont configurés pour la haute disponibilité ou la mise en grappe. Pour obtenir plus de renseignements, consultez Flux de trafic et inspection lors du déploiement de configurations.

Avant de déployer, vous souhaiterez peut-être passer en revue les modifications apportées par la mise à niveau (ainsi que toutes les modifications que vous avez apportées depuis la mise à niveau) : Choisissez **Deploy** > **Advanced Deploy** (Déployer > Déploiement avancé), sélectionnez les périphériques que vous venez de mettre à niveau, puis cliquez sur **Pending Changes Reports** (Rapports de modifications en attente). Une fois les rapports générés, vous pouvez les télécharger à partir de l'onglet Tâches dans le centre de messages.

Prochaine étape

(Facultatif) Effacez l'assistant en cliquant sur **Terminer**. Jusqu'à ce que vous fassiez cela, la page continue d'afficher les détails de la mise à niveau que vous venez d'effectuer.

Mettre à niveau Firewall Threat Defense via System (Système) > Updates (Mises à jour) (Enable Revert (Activer la restauration))

Utilisez cette procédure pour mettre à niveau Firewall Threat Defense en utilisant la page de mises à jour du système.

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes lors de la désinstallation, y compris une désinstallation échouée ou un appareil ne répondant plus, consultez Mises à niveau qui ne répondent pas.

Avant de commencer

- Décidez si vous souhaitez utiliser cette procédure.

  Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour** pour mettre à niveau Firewall Threat Defense. C'est la seule façon de définir l'option **Enable revert after successful upgrade** (Activer le retour après réussite de la mise à niveau), ce qui va à l'encontre de notre recommandation habituelle d'utiliser l'assistant de mise à niveau de Firewall Threat Defense.

- Terminez la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Dans On-Prem Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

Étape 2 Sous Available Updates (Mises à jour disponibles), cliquez sur l'icône **Install** (Installer) à côté du paquet de mise à niveau.

Si les périphériques que vous souhaitez mettre à niveau ne sont pas répertoriés, vous avez choisi le mauvais paquet de mise à niveau.

Le système affiche une liste des périphériques admissibles, ainsi que leurs résultats de vérification de compatibilité préalables à la mise à niveau. Cette vérification préalable vous empêche d'effectuer la mise à niveau s'il existe des problèmes manifestes qui entraîneront l'échec de votre mise à niveau.

Étape 3 Sélectionnez les périphériques que vous souhaitez vérifier et cliquez sur **Check Readiness** (Vérifier l'état de préparation).

Les vérifications de l'état de préparation évaluent l'état de préparation pour les mises à niveau majeures et de maintenance. Le temps nécessaire pour exécuter une vérification de l'état de préparation varie en fonction du modèle. Ne redémarrez pas ou n'arrêtez pas les vérifications de l'état de préparation manuellement.

Sous Vérifications de l'état de préparation de sur cette page, vous pouvez voir l'état de vérification pour l'ensemble de votre déploiement, y compris les vérifications en cours et les vérifications ayant échoué. Vous pouvez également

utiliser cette page pour réexécuter facilement les vérifications après un échec. Ou, surveillez l'état de préparation de la mise à jour dans le centre de messages.

Si vous ne pouvez pas sélectionner un appareil autrement admissible, assurez-vous qu'il a réussi ses vérifications de compatibilité. Si un périphérique échoue aux vérifications de l'état de préparation, corrigez les problèmes avant d'effectuer la mise à niveau.

Étape 4 Choisissez les périphériques à mettre à niveau.

Vous pouvez mettre à niveau plusieurs périphériques à la fois s'ils utilisent le même paquet de mise à niveau. Vous devez mettre à niveau les membres des grappes de périphériques et les paires à haute disponibilité en même temps.

Important
Nous vous recommandons *fortement* de mettre à niveau moins de cinq périphériques simultanément à partir de la page de mise à jour du système. Vous ne pouvez pas arrêter la mise à niveau tant que tous les périphériques sélectionnés n'ont pas terminé le processus. S'il y a un problème avec la mise à niveau d'un périphérique, tous les périphériques doivent terminer la mise à niveau avant que vous puissiez résoudre le problème.

Étape 5 Choisissez les options de mise à niveau.

Pour les mises à niveau majeures et de maintenance , vous pouvez :

- **Annuler automatiquement la mise à niveau en cas d'échec et restaurer la version précédente** : le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.
- **Activer la restauration après une mise à niveau réussie** : pendant les 30 jours suivant une mise à niveau réussie, vous pouvez rétablir l'état d'avant la mise à niveau du périphérique .
- **Mise à niveau de Snort 2 vers Snort 3** : après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations.

  Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide lors de la migration, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour votre version.

Ces options ne sont pas prises en charge pour les correctifs.

Étape 6 Cliquez sur **Install** (Installer), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Vous pouvez surveiller la progression de la mise à niveau dans le centre de messagerie. Pour en savoir plus sur le traitement du trafic pendant la mise à niveau, consultez Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense.

Les périphériques peuvent redémarrer deux fois pendant la mise à niveau. Il s'agit du comportement attendu.

Étape 7 Vérifiez la réussite.

Une fois la mise à niveau terminée, choisissez **Devices (appareils)** > **Device Management (gestion des appareils)** et confirmez que les périphériques que vous avez mis à niveau disposent de la bonne version de logiciel.

Étape 8 (Facultatif) Dans les déploiements à haute disponibilité ou en grappe, examinez les rôles des périphériques.

Le processus de mise à niveau modifie les rôles de chaque périphérique de manière à ce qu'il mette toujours à niveau une unité ou un nœud de données en attente. Il ne ramène pas les périphériques aux rôles qu'ils avaient avant la mise à niveau. Si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Étape 9 Mettez à jour les règles de prévention des intrusions et la base de données des vulnérabilités.

Bien que la mise à niveau mette souvent à jour ces composants, des nouveaux peuvent être disponibles. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 10 Apportez toutes les modifications de configuration requises après la mise à niveau.

Étape 11 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.

Snort redémarre généralement lors du premier déploiement après la mise à niveau. Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur tous les périphériques, y compris ceux qui sont configurés pour la haute disponibilité ou la mise en grappe. Pour obtenir plus de renseignements, consultez Flux de trafic et inspection lors du déploiement de configurations.

Avant de déployer, vous souhaiterez peut-être passer en revue les modifications apportées par la mise à niveau (ainsi que toutes les modifications que vous avez apportées depuis la mise à niveau) : Choisissez **Deploy** > **Advanced Deploy** (Déployer > Déploiement avancé), sélectionnez les périphériques que vous venez de mettre à niveau, puis cliquez sur **Pending Changes Reports** (Rapports de modifications en attente). Une fois les rapports générés, vous pouvez les télécharger à partir de l'onglet Tâches dans le centre de messages.

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.