Directives relatives aux mises à niveau logicielles

Pour plus de commodité, ce document duplique les directives relatives aux mises à niveau logicielles critiques et spécifiques aux versions publiées dans les notes de mise à jour Firewall Threat Defense. Pour connaître les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300, consultez Directives de mise à niveau pour le châssis Firepower 4100/9300.

Important Vous devez quand même lire les notes de mise à jour, qui peuvent contenir des informations supplémentaires essentielles et spécifiques à la version. Par exemple, les fonctionnalités nouvelles et obsolètes peuvent nécessiter des modifications de configuration avant ou après la mise à niveau, ou même empêcher la mise à niveau. Des problèmes connus (bogues ouverts) peuvent influer sur la mise à niveau.

Version minimale pour la mise à niveau

Version minimale pour la mise à niveau

Vous pouvez effectuer une mise à niveau directement vers Version 7.2, y compris les versions de maintenance, comme suit.

Tableau 1 : Version minimale pour la mise à niveau vers Version 7.2

Plateforme	Version minimale
On-Prem Firewall Management Center	6.6

Plateforme	Version minimale
Firewall Threat Defense (sauf Threat Defense Virtual avec GCP)	6.6 FXOS 2.12.0.31 est requis pour les périphériques Firepower 4100/9300. Dans la plupart des cas, nous vous recommandons d'utiliser la dernière version de FXOS dans chaque version principale. Pour vous aider à prendre une décision, consultez Notes de mise à jour de Cisco Firepower 4100/9300 FXOS, 2.12.
Threat Defense Virtual avec GCP	7.2 Vous ne pouvez pas mettre à niveau à la version 7.2+ à partir de la version 7.1 ou antérieure; vous devez déployer une nouvelle instance. La version minimale pour la mise à niveau vers une version de maintenance 7.2.x est la version 7.2.0.

Version minimale pour les correctifs.

Les correctifs modifient *uniquement* le quatrième chiffre . Vous ne pouvez pas effectuer de mise à niveau directement vers un correctif à partir d'une version majeure ou d'une version de maintenance précédente.

Directives de mise à niveau pour Version 7.2

Ces listes de contrôle fournissent des directives de mise à niveau nouvelles et/ou déjà publiées qui peuvent vous concerner.

Tableau 2 : Directives de mise à niveau pour Firewall Threat Defense avec On-Prem Firewall Management Center Version 7.2

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
TOUJOURS VÉRIFIER				
	Version minimale pour la mise à niveau, à la page 1	N'importe lequel	N'importe lequel	N'importe lequel
	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.	N'importe lequel	N'importe lequel	N'importe lequel

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
	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.	N'importe lequel	N'importe lequel	N'importe lequel
	Directives de mise à niveau pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 5	Firewall Threat Defense	N'importe lequel	N'importe lequel
	Directives de mise à niveau pour le châssis Firepower 4100/9300	Firepower 4100/9300	N'importe lequel	N'importe lequel
DIRECTIVES SUPPLÉMENTAIRES POUR LES DÉPLOIEMENTS SPÉCIFIQUES				
	Déploiement étendu après la mise à niveau, vers la version 7.2.4 à 7.2.5, pour les configurations de taille importante, à la page 3	On-Prem Firewall Management Center	6.6.0 et les versions ultérieures	7.2.4 à 7.2.5
	Reconnecter avec Cisco Cisco Secure Malware Analytics pour les On-Prem Firewall Management Center à haute disponibilité, à la page 4	On-Prem Firewall Management Center	De la version 6.4.0 à la version 6.7.x	7.0+
	Échec de la mise à niveau : ports de commutation du Firepower 1010 avec des identifiants VLAN non valides, à la page 5	Firepower 1010	De la version 6.4.0 à la version 6.6.x	6.7+

Déploiement étendu après la mise à niveau, vers la version 7.2.4 à 7.2.5, pour les configurations de taille importante

Déploiement : On-Prem Firewall Management Center

Mise à niveau à partir de : tout déploiement pour lequel l'optimisation des objets est désactivée.

Directement à : version 7.2.4 à 7.2.5

L'optimisation des objets de contrôle d'accès améliore les performances et consomme moins de ressources de périphérique lorsque vous avez des règles de contrôle d'accès avec des réseaux qui se chevauchent. Les optimisations ont lieu sur le *périphérique géré* lors du premier déploiement, après l'activation de la fonctionnalité sur On-Prem Firewall Management Center (y compris s'il est activé par une mise à niveau). Si vous avez un grand nombre de règles, le système peut prendre de quelques minutes à une heure pour évaluer vos politiques et effectuer l'optimisation des objets. Pendant ce temps, vous pourriez également constater une utilisation plus élevée du processeur sur vos périphériques. Une situation similaire se produit lors du premier

déploiement après la désactivation de la fonctionnalité (y compris si elle est désactivée par la mise à niveau). Une fois cette fonctionnalité activée ou désactivée, nous vous recommandons de la déployer au moment où elle aura le moins d'incidence, comme une fenêtre de maintenance ou une période de faible trafic.

Pour planifier, utilisez le tableau suivant.

Tableau 3 : Planification des mises à niveau du On-Prem Firewall Management Center avec optimisation des objets

Version	Paramètre par défaut/de recréation d'image	Mise à niveau	Pour Activer/Désactiver
7.0.5 et versions antérieures	Non pris en charge (désactivé).	—	—
7.0.6 ou version ultérieure, versions de maint.	Disabled (Désactivé)	Respecte votre paramètre actuel.	Communiquez avec Centre d'assistance technique Cisco (TAC).
7.1.0 à 7.2.3	Non pris en charge (désactivé).	Désactive.	—
7.2.4 à 7.2.5	Activé.	Active.	Communiquez avec Centre d'assistance technique Cisco (TAC).
7.3.x	Non pris en charge (désactivé).	Désactive.	—
7.4.0	Activé.	Active.	Communiquez avec Centre d'assistance technique Cisco (TAC).

Reconnecter avec Cisco Cisco Secure Malware Analytics pour les On-Prem Firewall Management Center à haute disponibilité

Déploiements : déploiements à haute disponibilité/AMP pour les réseaux (détection de programmes malveillants) où vous soumettez des fichiers pour analyse dynamique

Mise à niveau à partir de : de la version 6.4.0 à la version 6.7.x

Directement vers : version 7.0.0 et versions ultérieures

Bogue connexe : CSClu35704

La version 7.0.0 corrige un problème de haute disponibilité qui empêchait le système de soumettre des fichiers pour analyse dynamique après un basculement. Pour que le correctif prenne effet, vous devez vous réassocier au nuage public Cisco Cisco Secure Malware Analytics.

Une fois que vous avez mis à niveau la paire à haute disponibilité, sur le On-Prem Firewall Management Center principal :

1. Choisissez **AMP** > **Connexions d'analyse dynamique**.
2. Cliquez sur **Associer** dans la ligne du tableau correspondant au nuage public.

Une fenêtre de portail s'ouvre. Vous n'avez pas besoin de vous connecter. La réassociation se produit en arrière-plan, en quelques minutes.

Échec de la mise à niveau : ports de commutation du Firepower 1010 avec des identifiants VLAN non valides

Déploiements : Firepower 1010

Mise à niveau à partir de : de la version 6.4 à la version 6.6

Directement vers : version 6.7 et versions ultérieures

Pour le Firepower 1010, les mises à niveau de Firewall Threat Defense vers la version 6.7 ou une version ultérieure échoueront si vous avez configuré des ports de commutation avec un identifiant de VLAN compris entre 3968 et 4047. Ces identifiants sont destinés à un usage interne uniquement.

Directives de mise à niveau pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Vous ne mettez pas à niveau le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Nous nous assurons des mises à jour des fonctionnalités. Pour mettre à niveau Firewall Threat Defense avec le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), consultez le Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion Firewall livré dans le nuage.

Mises à niveau qui ne répondent pas

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 pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image..

Mise à niveau ne répondant pas

Ne pas redémarrer une mise à niveau en cours. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC)

Mise à niveau Firewall Threat Defense sans réponse

Pour les mises à niveau majeures et de maintenance, vous pouvez annuler manuellement les mises à niveau en cours ou ayant échoué, et réessayer les mises à niveau qui ont échoué. Dans On-Prem Firewall Management Center, utilisez la fenêtre contextuelle Upgrade Status (état de la mise à niveau), accessible à partir de l'onglet Mise à niveau sur la page de gestion des périphériques et à partir du centre de messages. Vous pouvez également utiliser la CLI Firewall Threat Defense.

Remarque Par défaut, Firewall Threat Defense revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« auto-cancel ») (Annulation automatique). Pour pouvoir annuler manuellement ou réessayer une mise à niveau qui a échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. L'annulation automatique n'est pas prise en charge pour les correctifs. 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.

Cette fonctionnalité n'est pas prise en charge pour les correctifs ou pour les mises à niveau à partir de la version 6.6 et des versions antérieures.

Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense

Mises à niveau logicielles pour les périphériques autonomes

Les périphériques fonctionnent en mode maintenance pendant leur mise à niveau. Le passage en mode maintenance au début de la mise à niveau entraîne une interruption de 2 à 3 secondes dans l'inspection du trafic. Les configurations des interfaces déterminent la façon dont un périphérique autonome gère le trafic à ce moment-là et pendant la mise à niveau.

Tableau 4 : Flux de trafic et inspection : mises à niveau logicielles pour les périphériques autonomes

Configuration de l'interface		Comportement du trafic
Interfaces de pare-feu	Routées ou commutées, y compris EtherChannel, redondant, sous-interfaces. Les interfaces commutées sont également appelées interfaces de groupe de ponts ou interfaces transparentes.	Abandonné. Pour les interfaces de groupe de ponts sur ISA 3000 uniquement, vous pouvez utiliser une politique FlexConfig pour configurer le contournement matériel en cas de panne de courant. Cela entraîne une baisse du trafic pendant les mises à niveau logicielles, mais sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Configuration de l'interface		Comportement du trafic
Interfaces IPS uniquement	Ensemble en ligne, contournement matériel activé de force : **contournement : forcé**	Réussite sans inspection jusqu'à ce que vous désactiviez le contournement matériel ou que vous le remettiez en mode veille.
	Ensemble en ligne, contournement matériel en mode veille : **Contournement : en veille**	Abandonné lors de la mise à niveau, alors que le périphérique est en mode de maintenance. Ensuite, réussite sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.
	Ensemble en ligne, contournement matériel désactivé : **contournement : désactivé**	Abandonné.
	Ensemble en ligne, pas de module de contournement matériel.	Abandonné.
	en ligne : tap mode (mode Tap)	Sortie de paquet immédiate, copie non inspectée.
	Passif, ERSPAN passif.	sans interruption, sans inspection

Mises à niveau logicielles pour une disponibilité et une évolutivité élevées

Vous ne devriez pas subir d'interruptions dans le flux de trafic ou l'inspection lors de la mise à niveau des périphériques à haute disponibilité ou en grappe. Pour les paires à haute disponibilité, le périphérique de secours est mis à niveau en premier. Les périphériques changent de rôle, puis le nouvel appareil en attente effectue la mise à niveau.

Dans le cas des grappes, le ou les modules de sécurité des données sont mis à niveau en premier, puis le module de contrôle. Pendant la mise à niveau du module de contrôle de sécurité, bien que l'inspection et le traitement du trafic se poursuivent normalement, le système interrompt la journalisation des événements. Les événements du trafic traité pendant le temps d'arrêt de la journalisation s'affichent avec des horodatages non synchronisés une fois la mise à niveau terminée. Toutefois, si le temps d'arrêt pour la journalisation est important, le système peut supprimer les événements les plus anciens avant de pouvoir être journalisés.

Notez que les mises à niveau transparentes ne sont pas prises en charge pour les grappes à une seule unité. Les interruptions du flux de trafic et de l'inspection dépendent des configurations d'interface de l'unité active, tout comme pour les périphériques autonomes.

Restauration logicielle (versions majeures et de maintenance)

Vous devez vous attendre à des interruptions du flux de trafic et de l'inspection pendant la reprise, même dans un déploiement à disponibilité et à évolutivité élevée. En effet, la restauration fonctionne mieux lorsque toutes les unités sont restaurées simultanément. La restauration simultanée signifie que les interruptions du flux de trafic et de l'inspection dépendent des configurations des interfaces uniquement, comme si chaque périphérique était autonome.

Désinstallation logicielle (correctifs)

Pour les périphériques autonomes, les interruptions du flux de trafic et de l'inspection pendant la désinstallation du correctif sont les mêmes que pour la mise à niveau. Dans les déploiements à haute disponibilité et évolutivité,

vous devez explicitement planifier un ordre de désinstallation qui réduit les perturbations au minimum. En effet, vous désinstallez les correctifs des périphériques individuellement, même ceux que vous avez mis à niveau sous forme d'unité.

Déploiement des modifications de configuration

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 et l'évolutivité. Les configurations de l'interface déterminent si le trafic chute ou s'il passe sans inspection pendant l'interruption. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Snort redémarre généralement lors du premier déploiement, immédiatement après la mise à niveau. Il ne redémarre pas pendant d'autres déploiements, sauf si, avant le déploiement, vous modifiez des politiques ou des configurations de périphériques spécifiques.

Tableau 5 : Flux de trafic et inspection : déploiement des modifications de configuration

Configuration de l'interface		Comportement du trafic
Interfaces de pare-feu	Routées ou commutées, y compris EtherChannel, redondant, sous-interfaces. Les interfaces commutées sont également appelées interfaces de groupe de ponts ou interfaces transparentes.	Abandonné.
Interfaces IPS uniquement	Ensemble en ligne : **Failsafe** (sécurité intégrée) activée ou désactivée	Réussi sans inspection Quelques paquets peuvent être perdus si l'option **Failsafe** est désactivé et si le processus Snort est occupé mais pas arrêté.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : désactivée	Abandonné.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : activés	Réussi sans inspection
	en ligne : tap mode (mode Tap)	Sortie de paquet immédiate, copie non inspectée.
	Passif, ERSPAN passif.	sans interruption, sans inspection

Flux de trafic et inspection lors du déploiement de configurations

Snort redémarre généralement lors du premier déploiement, immédiatement après la mise à niveau. Cela signifie que pour les mises à niveau On-Prem Firewall Management Center, Snort peut redémarrer sur tous les périphériques gérés. Snort ne redémarre pas après les déploiements suivants, sauf si, préalablement au déploiement, vous modifiez des politiques ou des configurations de périphériques spécifiques.

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 et l'évolutivité. Les configurations de l'interface déterminent si le trafic chute ou s'il passe sans inspection pendant l'interruption. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Tableau 6 : Flux de trafic et inspection : déploiement des modifications de configuration

Configuration de l'interface		**Comportement du trafic**
Interfaces de pare-feu	Routées ou commutées, y compris EtherChannel, redondant, sous-interfaces. Les interfaces commutées sont également appelées interfaces de groupe de ponts ou interfaces transparentes.	Abandonné.
Interfaces IPS uniquement	Ensemble en ligne : **Failsafe** (sécurité intégrée) activée ou désactivée	Réussi sans inspection Quelques paquets peuvent être perdus si l'option **Failsafe** est désactivé et si le processus Snort est occupé mais pas arrêté.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : désactivée	Abandonné.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : activés	Réussi sans inspection
	en ligne : tap mode (mode Tap)	Sortie de paquet immédiate, copie non inspectée.
	Passif, ERSPAN passif.	sans interruption, sans inspection

Temps et espace disque

Délai de mise à niveau

Nous vous recommandons de suivre et d'enregistrer vos propres délais de mise à niveau afin de pouvoir les utiliser comme références futures. Le tableau suivant répertorie certaines éléments qui peuvent influer sur le délai de mise à niveau.

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, voir Mises à niveau qui ne répondent pas, à la page 5.

Tableau 7 : Remarques concernant le délai de mise à niveau

Éléments à prendre en compte	Détails
Versions	Le délai de mise à niveau augmente généralement si votre mise à niveau ignore des versions.
Modèles	Le délai de mise à niveau augmente généralement avec les modèles inférieurs.
Appliances virtuelles	Le délai de mise à niveau dans les déploiements virtuels dépend fortement du matériel.
Haute disponibilité et mise en grappe	Dans une configuration à haute disponibilité ou en grappe, les périphériques sont mis à niveau un par un afin de préserver la continuité des opérations, chaque périphérique fonctionnant en mode maintenance pendant sa mise à niveau. Par conséquent, la mise à niveau d'une paire de périphériques ou d'une grappe complète prend plus de temps que la mise à niveau d'un périphérique autonome.
Configurations	Le délai de mise à niveau peut augmenter en fonction de la complexité de vos configurations, de la taille de vos bases de données d'événements et de l'incidence de la mise à niveau. Par exemple, si vous utilisez de nombreuses règles de contrôle d'accès et que la mise à niveau doit apporter des modifications générales à la façon dont ces règles sont stockées, la mise à niveau peut prendre plus de temps.
Composants	Vous pourriez avoir besoin de plus de temps pour effectuer des mises à niveau de systèmes d'exploitation ou d'hébergement virtuel, des transferts de paquets de mise à niveau, des vérifications de l'état de préparation, des mises à jour de la VDB et des règles de prévention des intrusions (SRU/LSP), du déploiement de la configuration et d'autres tâches connexes.

Espace disque à mettre à niveau

Pour mettre à niveau, le paquet de mise à niveau doit se trouver sur l'appliance. Pour les mises à niveau de périphérique, vous devez également disposer d'un espace suffisant sur le On-Prem Firewall Management Center (dans / Volume ou /var) pour le paquet de mise à niveau du périphérique. Sinon, vous pouvez utiliser un serveur interne pour les stocker. Les vérifications de l'état de préparation doivent indiquer si vous disposez d'un espace disque suffisant pour effectuer la mise à niveau. Sans suffisamment d'espace disque libre, la mise à niveau échoue.

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.