

Guide de compatibilité de l'outil de migration Cisco Secure Firewall

Première publication : 2020-10-29

Dernière modification : 2023-02-02

Guide de compatibilité de l'outil de migration de pare-feu sécurisé

Ce guide présente la compatibilité du matériel et du logiciel Cisco Secure Firewall, y compris les exigences relatives au système d'exploitation et à l'environnement d'hébergement.

Plateformes prises en charge pour la migration

Les périphériques ASA, ASA avec FPS, gérés par FDM et les plateformes de protection contre les menaces suivantes sont pris en charge pour la migration avec l'outil de migration Cisco Secure Firewall :

Plateformes ASA source prises en charge

Vous pouvez utiliser l'outil de migration de Cisco Secure Firewall pour migrer la configuration à partir des plateformes ASA à contexte unique ou à contexte multiple suivantes :



Remarque L'outil de migration de Cisco Secure Firewall prend en charge la migration des périphériques ASA autonomes vers un périphérique Défense contre les menaces autonome uniquement.

- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- ASA 5580
- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X

- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA 5585-X avec ASA uniquement (l'outil de migration de Cisco Secure Firewall ne fait pas migrer la configuration à partir de Module ASA FirePOWER)
- Firepower de série 1000
- Série Firepower 2100
- Pare-feu de série 3100
- Firepower de série 4100
- Série Firepower 9300
 - SM-24
 - SM-36
 - SM-40
 - SM-44
 - SM-48
 - SM-56
- ASA virtuel sur VMware, déployé à l'aide de VMware ESXi, du client Web VMware vSphere ou du client autonome vSphere

Modèles ASA source pris en charge pour ASA avec migration FPS :

Le module Cisco ASA FirePOWER est déployé sur les périphériques suivants :



Remarque

L'outil de migration de Cisco Secure Firewall prend en charge la migration des périphériques ASA autonomes avec FPS vers un périphérique Défense contre les menaces autonome uniquement.

- ASA5506-X
- ASA5506H-X
- ASA5506W-X
- ASA5508-X
- ASA 5512-X
- ASA 5515-X
- ASA5516-X
- ASA5525-X

- ASA5545-X
- ASA 5555-X
- ASA5585-X-SSP-10
- ASA5585-X-SSP-20
- ASA5585-X-SSP-40
- ASA5585-X-SSP-60

Plateformes de périphériques sources gérées par FDM

Vous pouvez utiliser l'outil de migration de Cisco Secure Firewall pour migrer la configuration à partir des plateformes de périphériques gérées par FDM suivantes :

- Firepower de Série 1000
- Firepower Série 2100
- Pare-feu de série 3100
- Firepower de série 4100
- Firepower de série 9300
- FDM virtuel sur VMware, AWS, Azure et KVM

Plateformes Défense contre les menaces cibles prises en charge

Vous pouvez utiliser l'outil de migration de Cisco Secure Firewall pour migrer une configuration ASA source, ASA avec FPS, Check Point, PAN et Fortinet vers l'instance autonome ou de conteneur des plateformes Défense contre les menaces suivantes :

- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- Firepower de Série 1000
- Série Firepower 2100
- Pare-feu de série 3100

- Firepower de série 4100
- Série Firepower 9300 qui comprend :
 - SM-24
 - SM-36
 - SM-40
 - SM-44
 - SM-48
 - SM-56
- Le défense virtuelle contre les menaces sur VMware, déployé à l'aide de VMware ESXi, VMware vSphere Web Client ou client autonome vSphere

Versions logicielles prises en charge pour la migration

Les versions suivantes sont ASA, ASA avec FPS, Check Point, PAN, Fortinet et Défense contre les menaces pour la migration :

Versions de pare-feu ASA prises en charge

L'outil de migration Cisco Secure Firewall prend en charge la migration à partir d'un périphérique qui exécute le logiciel ASA version 8.4 ou plus récente.

ASA pris en charge avec les versions de pare-feu FPS

L'outil de migration Cisco Secure Firewall prend en charge la migration à partir d'un périphérique qui exécute ASA avec le logiciel FPS version 9.2.2 et ultérieure.

Pour plus de détails, consultez la section [Compatibilité du module ASA FirePOWER](#) dans le guide de compatibilité Cisco ASA.

Versions du gestionnaire de périphériques prises en charge

L'outil de migration Cisco Secure Firewall prend en charge la migration à partir d'un gestionnaire d'appareil qui exécute la version 7.2 ou plus récente.

Versions de pare-feu de Check Point prises en charge

L'outil de migration Cisco Secure Firewall prend désormais en charge la migration vers Défense contre les menaces le système d'exploitation Check Point versions r75 à r77.30 et r80 à r80.40. Sélectionnez la version de Check Point appropriée dans la page **Select Source (Sélectionner la source)**.



Remarque VSX n'est pas pris en charge.

L'outil de migration Cisco Secure Firewall prend désormais en charge la migration à partir de la plateforme Check Point Gaia.

Versions de pare-feu de Palo Alto Networks prises en charge

L'outil de migration Cisco Secure Firewall prend en charge la migration vers Défense contre les menaces le système d'exploitation du pare-feu PAN version 6.1.x et version plus récente.

Versions de pare-feu Fortinet prises en charge

L'outil de migration Cisco Secure Firewall prend en charge la migration vers Défense contre les menaces la version 5.0 ou ultérieure du système d'exploitation du pare-feu Fortinet et la version plus récente.

Versions Cisco Secure Firewall Management Center prises en charge pour la configuration ASA source

Pour ASA, l'outil de migration Cisco Secure Firewall prend en charge la migration vers un périphérique Défense contre les menaces géré par centre de gestion qui exécute la version 6.2.3 ou 6.2.3+.



Remarque Certaines fonctionnalités ne sont prises en charge que dans les versions récentes de centre de gestion et Défense contre les menaces.



Remarque Pour des délais de migration optimaux, nous vous recommandons d'effectuer une mise à niveau de centre de gestion à la version suggérée qui peut être téléchargée à l'adresse suivante : software.cisco.com/downloads.

Versions de Centre de gestion prises en charge pour l'ASA source avec configuration FPS

Pour ASA avec FPS, l'outil de migration Cisco Secure Firewall prend en charge la migration vers un périphérique Défense contre les menaces géré par un centre de gestion qui exécute la version 6.5+.

Versions Centre de gestion prises en charge pour la configuration des périphériques gérés par FDM source

Pour les périphériques gérés par FDM, l'outil de migration Cisco Secure Firewall prend en charge la migration vers un centre de gestion qui exécute la version 7.3+.

Versions Centre de gestion prises en charge pour la configuration de la source du pare-feu Check Point, PAN et du pare-feu Fortinet

Pour le pare-feu Check Point, PAN et le pare-feu Fortinet, l'outil de migration Cisco Secure Firewall prend en charge la migration vers un périphérique Défense contre les menaces géré par un centre de gestion qui exécute la version 6.2.3.3 ou une version récente.



Remarque Certaines fonctionnalités ne sont prises en charge que dans les versions récentes de centre de gestion et Défense contre les menaces. Par exemple, les ACL basées sur le temps dans Fortinet sont prises en charge à partir de la version centre de gestion 6.6 ou récente.



Remarque La migration vers l'appareil Défense contre les menace 6.7 n'est pas actuellement prise en charge. Par conséquent, la migration peut échouer si le périphérique est configuré avec une interface de données pour l'accès centre de gestion.

Versions Défense contre les menaces prises en charge

L'outil de migration Cisco Secure Firewall recommande la migration vers un périphérique en cours d'exécution Défense contre les menace, version 6.2.3 ou récente.

Pour obtenir des renseignements détaillés sur la compatibilité du logiciel et du matériel Cisco Secure Firewall, y compris les exigences relatives au système d'exploitation et à l'environnement d'hébergement, pour Défense contre les menace, consultez le [Guide de compatibilité de Cisco Secure Firewall](#).

Configuration requise pour l'outil de migration Cisco Secure Firewall

L'outil de migration Cisco Secure Firewall a les exigences en matière d'infrastructure et de plateforme suivantes :

- Fonctionne sur un système d'exploitation Microsoft Windows 10 64-bit ou sur une version macOS 10.13 ou une version récente
- Google Chrome comme navigateur par défaut du système
- (Windows) Comporte des paramètres de veille configurés dans la consommation et la veille pour ne jamais mettre l'ordinateur en veille, de sorte que le système ne se met pas en veille lors d'une migration importante
- (macOS) Comporte des paramètres d'économie d'énergie configurés de sorte que l'ordinateur et le disque dur ne se mettent pas en veille lors d'une migration importante

Documentation associée

Cette section récapitule la documentation relative à l'outil de migration Cisco Secure Firewall.

- [Le Guide de compatibilité Cisco Secure Firewall Threat Defense](#) : décrit la compatibilité matérielle et logicielle du pare-feu Cisco, y compris les exigences relatives au système d'exploitation et à l'environnement d'hébergement.
- [La compatibilité Cisco ASA](#) : répertorie la compatibilité et les exigences logicielles et matérielles de Cisco ASA.
- [La compatibilité Cisco Firepower 4100/9300 FXOS](#) : répertorie les renseignements sur la compatibilité matérielle et logicielle pour les appareils de sécurité FXOS, Cisco Firepower 9300 et Cisco Firepower 4100, ainsi que les périphériques logiques pris en charge.

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.