

Configuration système requise

Ce document comprend la configuration système requise pour Version 7.2.

- Plateformes On-Prem Firewall Management Center , à la page 1
- PlateformesFirewall Threat Defense , à la page 2
- Gestion du Firewall Threat Defense, à la page 4

Plateformes On-Prem Firewall Management Center

Le On-Prem Firewall Management Center fournit une console de gestion de pare-feu centralisée. Pour la compatibilité des périphériques avec le On-Prem Firewall Management Center, consultez Gestion du Firewall Threat Defense, à la page 4. Pour des informations générales sur la compatibilité, consultez le Guide de compatibilité de Cisco Secure Firewall Management Center.

Matériel On-Prem Firewall Management Center

Version 7.2 prend en charge le matériel On-Prem Firewall Management Center suivant :

- Firepower Management Center 1600
- Firepower Management Center 2600
- Firepower Management Center 4600

Vous devez également maintenir à jour le micrologiciel du contrôleur BIOS et RAID; consultez le Notes de mise à jour du correctif Cisco Secure Firewall Threat Defense/Firepower.

Firewall Management Center Virtual

Version 7.2 prend en charge les déploiements Firewall Management Center Virtual dans les nuages publics et privés.

Avec le Firewall Management Center Virtual, vous pouvez acheter une licence pour gérer 2, 10 ou 25 périphériques. Certaines plateformes prennent en charge 300 périphériques. Notez que les licences à deux appareils ne prennent pas en charge la haute disponibilité On-Prem Firewall Management Center. Pour plus de détails sur les instances prises en charge, consultez le Guide de démarrage de Cisco Secure Firewall Management Center Virtual.

Tableau 1 : Plateformes Version 7.2 Firewall Management Center Virtual

Plateforme	Appareils gérés		haute accessibilité
	2, 10, 25	300	
Nuage public			
Alibaba	OUI	—	—
Amazon Web Services (AWS)	OUI	OUI	OUI
Google Cloud Platform (GCP)	OUI	—	—
Microsoft Azure	OUI	—	—
Oracle Cloud Infrastructure (OCI)	OUI	OUI	OUI
Nuage privé			
Cisco HyperFlex	OUI	—	OUI
Machine virtuelle basée sur le noyau (KVM)	OUI	—	—
Nutanix Enterprise Cloud	OUI	—	—
OpenStack	OUI	—	—
VMware vSphere/VMware ESXi 6.5, 6.7 ou 7.0	OUI	OUI	OUI

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est fourni via Cisco Defense Orchestrator, qui unit la gestion de plusieurs solutions de sécurité Cisco. Nous nous assurons des mises à jour des fonctionnalités. Notez qu'un On-Prem Firewall Management Center déployé par le client est souvent appelé *sur site*, même pour les déploiements dans le nuage public.

Pour des informations à jour sur la compatibilité, consultez le Guide de compatibilité de Cisco Secure Firewall Management Center.

PlateformesFirewall Threat Defense

Les périphériquesThreat Defense surveillent le trafic réseau et décident s'il faut autoriser ou bloquer un trafic spécifique en fonction d'un ensemble défini de règles de sécurité. Pour en savoir plus sur les méthodes de gestion des périphériques, consultez Gestion du Firewall Threat Defense, à la page 4. Pour des informations générales sur la compatibilité, consultez Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Matériel Firewall Threat Defense

Le matériel Version 7.2Firewall Threat Defense est proposé en divers débits, capacités d'évolutivité et tailles.

Tableau 2 : Matériel Version 7.2 Firewall Threat Defense

Plateforme	Compatibilité On-Prem Firewall Management Center		Compatibilité Firewall Device Manager		Notes
	Déployé par le client	Envoyé par nuage	Firewall Device Manager uniquement	Firewall Device Manager + CDO	
Firepower 1010E, 1010, 1120, 1140, 1150	OUI	OUI	OUI	OUI	Firepower 1010E nécessite la version 7.2.3 ou ultérieures. N'utilisez pas une version 7.2.3 ou 7.3.0 d'un On-Prem Firewall Management Center pour gérer le périphérique Firepower 1010E. Au lieu de cela, utilisez un On-Prem Firewall Management Center de version7.2.3.1 et ultérieures ou 7.3.1.1 et ultérieures.
Firepower 2110, 2120, 2130, 2140	OUI	OUI	OUI	OUI	—
Secure Firewall3110, 3120, 3130, 3140	OUI	OUI	OUI	OUI	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300 : modules SM-24, SM-36 et SM-44 Firepower 9300 : modules SM-40, SM-48 et SM-56	OUI	OUI	OUI	OUI	nécessite la version FXOS 2.12.0.31 ou ultérieure. 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.
ISA 3000	OUI	OUI	OUI	OUI	Peut nécessiter une mise à jour de ROMMON. Consultez la section Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense.

Firewall Threat Defense Virtual

Les implémentations de Version 7.2 Firewall Threat Defense Virtual prennent en charge le Smart Software Licensing à plusieurs niveaux de performance, en fonction des exigences de débit et des limites des sessions VPN d'accès à distance. Les options vont de FTDv5 (100 Mbit/s/50 sessions) à FTDv100 (16 Gbit/s/10 000 sessions). Pour en savoir plus sur les instances prises en charge, les débits et les autres exigences d'hébergement, consultez le *guide de démarrage* approprié.

Tableau 3 : Plateformes Version 7.2 Firewall Threat Defense Virtual

Plateforme du périphérique	Compatibilité On-Prem Firewall Management Center		Compatibilité Firewall Device Manager	
	Déployé par le client	Envoyé par nuage	Firewall Device Manager uniquement	Firewall Device Manager + CDO
Nuage public				
Amazon Web Services (AWS)	OUI	OUI	OUI	OUI
Microsoft Azure	OUI	OUI	OUI	OUI
Google Cloud Platform (GCP)	OUI	OUI	OUI	OUI
Oracle Cloud Infrastructure (OCI)	OUI	OUI	—	—
Nuage privé				
Cisco Hyperflex	OUI	OUI	OUI	OUI
Machine virtuelle basée sur le noyau (KVM)	OUI	OUI	OUI	OUI
Nutanix Enterprise Cloud	OUI	OUI	OUI	OUI
OpenStack	OUI	OUI	—	—
VMware vSphere/VMware ESXi 6.5, 6.7 ou 7.0	OUI	OUI	OUI	OUI

Gestion du Firewall Threat Defense

Selon le modèle et la version du périphérique, nous prenons en charge les méthodes de gestion suivantes.

On-Prem Firewall Management Center Sur place

Tous les périphériques prennent en charge la gestion à distance avec un On-Prem Firewall Management Centerdéployé par le client (*sur site*).

Les versions sont majeures (a.x), maintenance (a.x.y) ou correctif (a.x.y.z). Le On-Prem Firewall Management Center doit exécuter la même version ou une version plus récente que ses périphériques. Les nouvelles fonctionnalités et les correctifs exigent souvent la dernière version tant sur le On-Prem Firewall Management Center que sur ses périphériques. Mettez d'abord le On-Prem Firewall Management Center à niveau : vous pourrez toujours gérer les anciens périphériques, généralement quelques versions majeures.

Remarque 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.

Notez que dans la plupart des cas, vous pouvez mettre à niveau un périphérique plus ancien directement à la version majeure ou de maintenance de On-Prem Firewall Management Center. Cependant, il est parfois possible de gérer un périphérique plus ancien que vous ne pouvez pas mettre à niveau directement, même si la version cible est prise en charge sur le périphérique. Dans de rares cas, des problèmes surviennent avec des combinaisons On-Prem Firewall Management Center-périphérique spécifiques. Pour connaître les exigences propres à la version, consultez les notes de mise à jour.

Tableau 4 : Compatibilité du périphérique On-Prem Firewall Management Centersur site

Version On-Prem Firewall Management Center	Plus ancienne version de périphérique que vous pouvez gérer
7.7	7.2
7.6	7.1
7.4 Dernier soutien pour la gestion des périphériques NGIPS.	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.4	6.1
6.2.3	6.1

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Pour la compatibilité de Firewall Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.