Quels sont le système d'exploitationet le gestionnaire d'applications pour vous?

Votre plateforme matérielle peut exécuter l'un de deux systèmes d'exploitation. Pour chaque système d'exploitation, vous avez le choix entre plusieurs gestionnaires. Ce chapitre explique les choix de systèmes d'exploitation et de .

- Systèmes d'exploitation, à la page 1
- Gestionnaires, à la page 1

Systèmes d'exploitation

Vous pouvez utiliser soit le Cisco Secure Firewall ASA ou l'application Cisco Secure Firewall Threat Defense (anciennement Cisco Firepower Threat Defense) sur votre plateforme matérielle :

- ASA : l'ASA est une solution classique de concentrateur VPN et de pare-feu dynamique avancé.

  Vous pouvez utiliser l'ASA si vous n'avez pas besoin des fonctionnalités avancées de défense contre les menaces, ou si vous avez besoin d'une fonctionnalité réservée à l'ASA qui n'est pas encore disponible sur défense contre les menaces. Cisco fournit des outils de migration de l'ASA vers défense contre les menaces pour vous aider à convertir votre ASA vers défense contre les menaces si vous commencez avec l'ASA et réimagez plus tard vers défense contre les menaces.

- Défense contre les menaces : Défense contre les menaces est un pare-feu de nouvelle génération qui combine un pare-feu dynamique avancé, un concentrateur VPN et un IPS de nouvelle génération. En d'autres termes, défense contre les menaces reprend le meilleur des fonctionnalités de l'ASA et le combine avec les meilleures fonctionnalités de pare-feu et d'IPS de nouvelle génération.

  Nous recommandons d'utiliser défense contre les menaces plutôt que l'ASA, car il contient la plupart des principales fonctionnalités de l'ASA, plus des fonctionnalités supplémentaires de pare-feu de nouvelle génération et d'IPS.

Gestionnaires

défense contre les menaces et l'ASA prennent en charge plusieurs gestionnaires.

Gestionnaires de Défense contre les menaces

Tableau 1 : Gestionnaires de Défense contre les menaces

Gestionnaire	Description
Cisco Secure Firewall Management Center (anciennement Cisco Firepower Management Center)	Le centre de gestion est un puissant gestionnaire multidispositif basé sur le Web qui fonctionne sur son propre matériel de serveur, ou comme un appareil virtuel sur un hyperviseur. Vous devriez utiliser le centre de gestion si vous voulez un gestionnaire multidispositif, et vous avez besoin de toutes les fonctionnalités sur défense contre les menaces. Le centre de gestion fournit également une analyse et une surveillance puissantes du trafic et des événements. **Remarque** Le centre de gestion n'est pas compatible avec d'autres gestionnaires, car le centre de gestion possède la configuration défense contre les menaces, et vous n'êtes pas autorisé à configurer défense contre les menaces directement, en contournant le centre de gestion. Pour commencer avec le centre de gestion, configurez d'abord le châssis conformément à Configuration initiale du châssis Firepower 4100, et puis consultez Déploiement de Défense contre les menaces avec le Centre de gestion.
Cisco Secure Firewall Device Manager (anciennement Cisco Firepower Device Manager)	Le gestionnaire d'appareil est un gestionnaire simplifié, basé sur le Web et sur l'appareil. Parce qu'il est simplifié, certaines fonctionnalités défense contre les menaces ne sont pas prises en charge à l'aide de gestionnaire d'appareil. Vous devriez utiliser le gestionnaire d'appareil si vous ne gérez qu'un petit nombre de appareils et n'avez pas besoin d'un gestionnaire multidispositifs. **Remarque** À la fois le gestionnaire d'appareil et le CDO en mode FDM peuvent découvrir la configuration sur le pare-feu, vous pouvez donc utiliser le gestionnaire d'appareil et le CDO pour gérer le même pare-feu. Le centre de gestion n'est pas compatible avec les autres gestionnaires. Pour commencer avec le gestionnaire d'appareil, configurez d'abord le châssis conformément à Configuration initiale du châssis Firepower 4100, et puis consultez Déploiement de Défense contre les menaces avec le Gestionnaire d'appareil.

Gestionnaire	Description
Cisco Defense Orchestrator (CDO)	CDO propose deux modes de gestion : • (7.2 et versions ultérieures) Mode de centre de gestion fourni dans le nuage avec toutes les fonctionnalités de configuration d'un centre de gestion sur site. Pour la fonctionnalité d'analyse, vous pouvez utiliser Secure Cloud Analytics dans le nuage ou un centre de gestion sur place. • (Utilisateurs existants de CDO uniquement) Mode gestionnaire de dispositifs avec une expérience utilisateur simplifiée. Ce mode n'est disponible que pour les utilisateurs qui utilisent déjà CDO pour gérer les défense contre les menaces dans le mode gestionnaire de dispositifs. Ce mode n'est pas couvert par ce guide. Comme CDO est basé sur le cloud, il n'y a pas de frais généraux liés à l'exécution de CDO sur vos propres serveurs. CDO gère également d'autres appareils de sécurité, comme les appareils ASA, de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos appareils de sécurité. Pour vous familiariser avec le provisionnement à faible intervention de CDO, consultez Défense contre les menaces Déploiement avec CDO.
Cisco Secure Firewall Threat Defense REST API	Le threat defense REST API (API REST de défense contre les menaces) vous permet d'automatiser la configuration directe de défense contre les menaces. Cette API est compatible avec l'utilisation de gestionnaire d'appareil et CDO, car elles peuvent toutes deux découvrir la configuration sur le pare-feu. Vous ne pouvez pas utiliser cette API si vous gérez défense contre les menaces à l'aide du centre de gestion. Le threat defense REST API (API REST de défense contre les menaces) n'est pas visé par ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de Cisco Secure Firewall Threat Defense REST API.
API REST du centre de gestion du Cisco Secure Firewall	L'API REST du centre de gestion vous permet d'automatiser la configuration des politiques centre de gestion qui peuvent ensuite être appliquées aux défense contre les menaces gérés. Cette API ne gère pas défense contre les menaces directement. Le management center REST API (API REST centre de gestion) n'est pas visé par ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage rapide de Cisco Secure Firewall Management Center REST API.

Gestionnaires ASA

Tableau 2 : Gestionnaires ASA

Gestionnaire	Description
Gestionnaire ASDM (Adaptive Security Device Manager)	ASDM est un gestionnaire basé sur Java qui offre une fonctionnalité ASA complète sur l'appareil. Vous devez utiliser ASDM si vous préférez une interface graphique à l'interface de ligne de commande et si vous devez seulement gérer un petit nombre d'appareils ASA. ASDM peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande, CDO ou CSM avec ASDM. Pour commencer avec ASDM, configurez d'abord le châssis en fonction de Configuration initiale du châssis Firepower 4100, puis consultez Déploiement d'ASA avec ASDM.
Interface de ligne de commande	Vous devriez utiliser l'interface de ligne de commande (CLI) de l'ASA si vous préférez ce type d'interface aux interfaces graphiques. L'interface de ligne de commande n'est toutefois pas abordée dans ce guide. Consultez les guides de configuration d'ASA pour obtenir plus d'informations.
CDO	CDO est un gestionnaire multidispositifs simplifié hébergé en nuage. Puisqu'il s'agit d'une solution simplifiée, certaines fonctionnalités ASA ne sont pas prises en charge au moyen de CDO. Vous devez utiliser CDO si vous souhaitez utiliser un gestionnaire multidispositifs offrant une expérience de gestion simplifiée. Et comme CDO est hébergé en nuage, l'exécution de CDO sur vos propres serveurs n'entraîne pas de trafic de service. Le CDO gère également d'autres appareils de sécurité, tels que les défense contre les menaces, de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos appareils de sécurité. CDO peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande ou ASDM. Le gestionnaire CDO n'est toutefois pas abordé dans ce guide. Pour commencer à utiliser CDO, consultez la page d'accueil de CDO.
Cisco Security Manager (CSM)	CSM est un puissant gestionnaire multidispositifs qui fonctionne sur son propre matériel de serveur. Vous devez utiliser CSM si vous avez besoin de gérer un grand nombre d'ASA. CSM peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande ou ASDM. Le CSM ne prend pas en charge la gestion des défense contre les menaces. Le gestionnaire CSM n'est toutefois pas abordé dans ce guide. Pour en savoir plus, consultez le guide de l'utilisateur CSM.
API REST ASA	L'API REST ASA vous permet d'automatiser la configuration d'ASA. Cependant, l'API n'inclut pas toutes les fonctionnalités de l'ASA et ne fait plus l'objet d'améliorations. L'API REST ASA n'est pas abordée dans ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage rapide de Cisco ASA REST API.

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.