Gestion des périphériques Cisco Secure Firewall Threat Defense avec 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 un logiciel-service (SaaS) qui gère les périphériques Secure Firewall Threat Defense et est fourni par Cisco Defense Orchestrator (CDO). Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) offre plusieurs fonctionnalités identiques à Cisco Secure Firewall Management Center sur site.

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) a la même apparence et comportement qu'un Cisco Secure Firewall Management Center sur site et utilise la même API de FMC.

En tant que produit SaaS, l'équipe des opérations Cisco Defense Orchestrator (CDO) est responsable du déploiement et de la maintenance des logiciels Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). À mesure que de nouvelles fonctionnalités sont introduites, l'équipe des opérations CDO met à jour le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) de votre détenteur CDO pour vous.

Un assistant de migration est proposé pour vous aider à migrer vos périphériques Secure Firewall Threat Defense de votre centre de gestion Secure Firewall sur site vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Les périphériques doivent être équipés du logiciel Threat Defense version 7.0.3 ou version 7.0.x ultérieure, ou version 7.2 ou ultérieure pour pouvoir être migrés. Les versions de Threat Defense 7.1 ne sont pas prises en charge.

L'intégration des périphériques Cisco Secure Firewall Threat Defense s'effectue dans CDO à l'aide de processus familiers, comme l'intégration d'un périphérique avec son numéro de série ou l'utilisation d'une commande CLI qui comprend une clé d'enregistrement. Une fois le périphérique intégré, il est visible à la fois dans CDO et dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cependant vous configurez le périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Dans CDO, vous pouvez afficher des informations spécifiques au périphérique telles que la version, l'état de configuration, la connectivité, l'intégrité et l'état du nœud. Lorsque vous cliquez sur l'état d'intégrité de CDO, vous êtes redirigé vers la page de surveillance de l'intégrité du périphérique respectif dans l'interface utilisateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

CDO fournit une prise en charge à haute disponibilité pour les périphériques de défense contre les menaces qu'il gère au moyen de l'interface de données. Cette fonctionnalité est prise en charge pour les périphériques exécutant la version logicielle 7.2 ou ultérieure.

Vous pouvez analyser les événements du journal système générés par vos périphériques de défense contre les menaces intégrés à l'aide de Security Analytics and Logging (SaaS) ou de Security Analytics and Logging (On-Premises). La version SaaS stocke les événements dans le nuage et vous affichez les événements dans CDO. La version sur site stocke les événements dans un appareil Cisco Secure Network Analytics sur site et l'analyse est effectuée dans Cisco Secure Firewall Management Center sur site. Dans les deux cas, tout comme avec un FMC sur site aujourd'hui, vous pouvez toujours envoyer les journaux à un collecteur de journaux de votre choix directement à partir des capteurs.

La licence pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est une licence gérée par périphérique et aucune licence n'est requise pour le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) lui-même. Les périphériques Cisco Secure Firewall Threat Defense existants réutilisent leurs licences Smart existantes, et les nouveaux périphériques Cisco Secure Firewall Threat Defense fournissent de nouvelles licences Smart pour chaque fonctionnalité mise en œuvre sur FTD.

Les clients existants peuvent continuer à utiliser CDO pour la gestion d'autres types de périphériques comme Cisco Secure Firewall ASA, Meraki, les périphériques Cisco IOS, Umbrella et les nuages privés virtuels AWS. Si vous utilisez CDO pour gérer un périphérique Cisco Secure Firewall Threat Defense configuré pour la gestion locale avec Firepower Device Manager, vous pouvez également continuer à les gérer avec CDO.

Pour savoir comment provisionner un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur, consultez Activer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur CDO, à la page 3.

En savoir plus sur les fonctionnalités de Cisco Firewall Management Center que nous prenons en charge dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

- Intégrer un périphérique Cisco Secure Firewall Threat Defense dans Firewall Management Center en nuage.
- Migrer un périphérique Firewall Threat Defense vers le nuage
- surveillance de l'intégrité
- Sauvegarde et restauration
- Planification
- Importer/Exporter
- Rapports et alertes
- Mode pare-feu transparent ou routé
- Haute disponibilité pour les périphériques gérés par l'interface de gestion et de données
- Interfaces
- Routage
- Objets et certificats
- Contrôle d'accès au réseau (NAT)
- Politiques de contrôle d'accès

Activer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur CDO

Si vous souhaitez gérer vos périphériques Cisco Secure Firewall Threat Defense, vous pouvez activer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur. Vous devez avoir un rôle d'utilisateur administrateur ou super administrateur pour effectuer cette tâche.

Procedure

Étape 1 Dans le menu CDO, cliquer sur **Tools and Services** > **Firewall Management Center** >  > **FMC** > **Enable Cloud-Delivered FMC** (Outils et services > Firewall Management Center > FMC > Activer le FMC en nuage).

Étape 2 CDO commence le provisionnement d'une instance Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) en arrière-plan; cela prend généralement entre 15 et 30 minutes. Vous pouvez suivre la progression du provisionnement dans la colonne **Status** (état) du **FMC en nuage**.

Une fois le provisionnement terminé, l'état passe à **Actif**. En outre, vous recevez une notification « **Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est prêt** » dans le panneau de notifications CDO et dans les applications sur lesquelles vous avez configuré les webhooks entrants. Consultez la section Paramètres de notification pour en savoir plus.

Note Après avoir reçu la notification **Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est prêt**, assurez-vous de vous déconnecter et de vous reconnecter une fois à votre détenteur pour voir les options du volet droit de **FMC en nuage**, telles que **Actions**, **Management** et **System**.

Vous pouvez ensuite intégrer vos périphériques défense contre les menaces au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et les gérer.

Assistance matérielle et logicielle

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend en charge ces versions de logiciel Cisco Secure Firewall Threat Defense lorsqu'elles sont installées sur un matériel ou un périphérique virtuel pris en charge :

- Version 7.0.3 ou versions ultérieures 7.0.x.
- Version 7.2 et versions ultérieures.

Remarque La version du logiciel 7.1 n'est pas prise en charge.

Consultez les caractéristiques de prise en charge de Firepower Threat Defense pour en savoir plus.

Calendrier de maintenance de la plateforme CDO

Calendrier de maintenance de CDO

CDO met à jour sa plateforme chaque semaine avec de nouvelles fonctionnalités et des améliorations de la qualité. Les mises à jour peuvent être effectuées pendant une période de 3 heures selon ce calendrier.

Tableau 1 : Calendrier de maintenance de CDO

Jour de la semaine	Heure (Heure sur 24 heures)
Jeudi	9 h UTC à 12 h UTC

Pendant cette période de maintenance, vous pouvez toujours accéder à votre client et si vous avez un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vous pouvez également accéder à cette plateforme. En outre, les périphériques que vous avez intégrés à CDO continuent d'appliquer leurs politiques de sécurité.

Remarque Nous vous déconseillons d'utiliser CDO pour déployer des modifications de configuration sur les périphériques gérés pendant les périodes de maintenance.

Si une défaillance empêche CDO ou Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) de communiquer, cette défaillance est résolue sur tous les détenteurs concernés le plus rapidement possible, même si la maintenance survient en dehors de la fenêtre de maintenance.

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

Les clients qui ont déployé un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur leur détenteur sont informés environ une semaine avant la mise à jour par CDO de l'environnement Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Les utilisateurs super-administrateurs et administrateurs du détenteur sont avisés par courriel. CDO affiche également une bannière sur sa page d'accueil pour informer tous les utilisateurs des mises à jour à venir.

La mise à jour de votre service client peut prendre jusqu'à une heure et se produit dans la période de maintenance de 3 heures le jour de maintenance attribué à la région de votre service client. Pendant la mise à jour de votre environnement hébergé, vous ne pourrez pas accéder à l'environnement Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), mais vous pourrez toujours accéder au reste de CDO.

Tableau 2 : Calendrier de maintenance de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Jour de la semaine	Heure (Heure sur 24 heures)	Région
Mercredi	04:00 UTC à 07:00 UTC	Europe, Moyen-Orient ou Afrique (EMEA)
Mercredi	17:00 UTC à 20:00 UTC	Asie-Pacifique-Japon (APJ)
Jeudi	9 h UTC à 12 h UTC	Amérique

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.