Guide d'intégration de Cisco Secure Workload et Cisco Secure Firewall Management Center

Première publication : 2021-02-25

Dernière modification : 2023-12-21

Intégration de Cisco Secure Workload avec Cisco Secure Firewall Management Center

Historique de la fonctionnalité

Tableau 1 : Historique de la fonctionnalité

Nom de la caractéristique	Version	Description de la fonctionnalité	Où trouver
Simplification du flux de travail de segmentation	3.9.1.1	Flux de travail simplifié pour le mappage de la portée aux politiques de contrôle d'accès pour l'application de Cisco Secure Firewall Management Center (FMC) et de Cisco Firepower Threat Defense (FTD). L'intégration améliorée de l'API marque le découplage des flux de travail de segmentation et d'application de correctifs virtuels.	Segmentation dans la version 3.9.1.1
Simplification du flux de travail d'application de correctifs virtuels	3.8.1.36	Flux de travail simplifié pour la charge de travail ou le filtrage des vulnérabilités et des expositions courantes (CVE, Common Vulnerability and Exposure).	Application de correctifs virtuels dans la version 3.8.1.36

À propos de cette intégration

Intégrer les possibilités de Cisco Cisco Secure Workload (anciennement Cisco Tetration) aux fonctionnalités robustes de Cisco Secure Firewall (anciennement Cisco Firepower) pour créer une solution de sécurité sans agent spécialement conçue pour :

- La segmentation des charges de travail pour lesquelles des agents logiciels ne peuvent pas être installés.

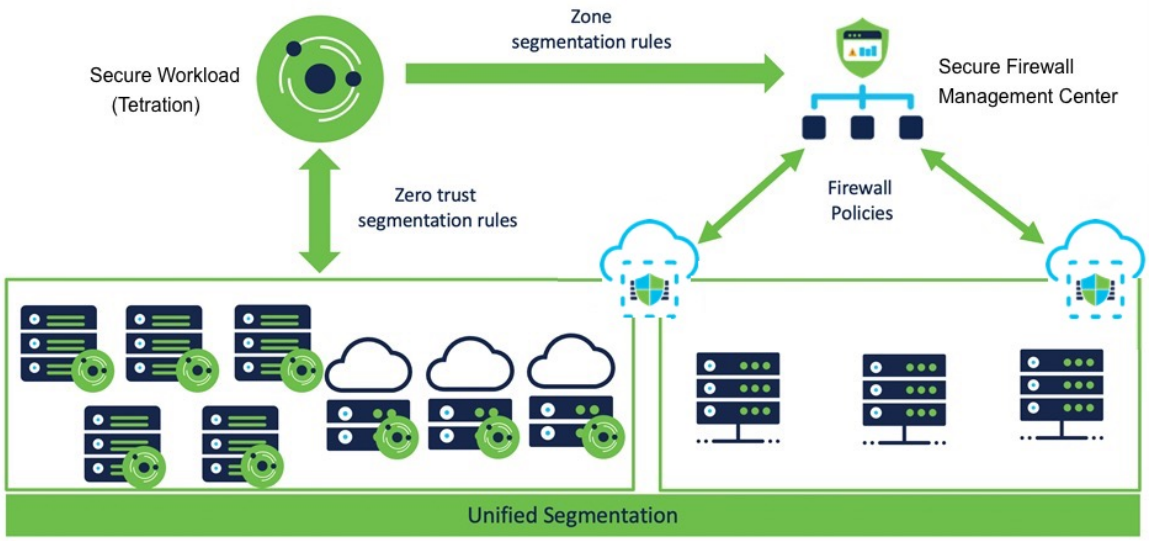
  Par exemple, utilisez cette intégration si vous n'avez pas le contrôle sur les systèmes d'exploitation des charges de travail (logiciels basés sur l'appareil) ou si les charges de travail sont exécutées sur des systèmes d'exploitation existants qui ne sont pas pris en charge par les agents.

- Segmentation du trafic pour différentes zones au niveau de votre centre de données et de votre nuage.

  Par exemple, vous pouvez appliquer facilement et à grande échelle différents ensembles de politiques au trafic entrant dans votre réseau, au trafic sortant de votre réseau et au trafic entre les charges de travail de ce dernier.

Grâce à cette intégration, Cisco Secure Workload applique et gère automatiquement les politiques de segmentation sur les pare-feu de Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense) gérés par l'instance de Cisco Secure Firewall Management Center. Les politiques sont mises à jour de manière dynamique et l'ensemble des charges de travail auxquelles elles s'appliquent est actualisé en permanence au fur et à mesure que l'environnement applicatif évolue.

Illustration 1 : Intégration de Cisco Secure Workload avec Cisco Secure Firewall Management Center



Dans les versions 3.7 et 3.6 de Cisco Secure Workload, les politiques de segmentation appliquées Cisco Secure Workload sont converties en politiques de contrôle d'accès en fonction des ensembles d'adresses IP des portées, des filtres d'inventaire et des grappes convertis en objets dynamiques dans Cisco Secure Firewall Management Center. Pour de plus amples renseignements, consultez la section Renseignements importants pour Cisco Secure Workload, versions 3.7 et 3.6, à la page 5.

Dans la version 3.5 de Tetration : Les politiques de segmentation Tetration sont converties en politiques de préfiltre dans Cisco Firepower Management Center.

Toutes versions

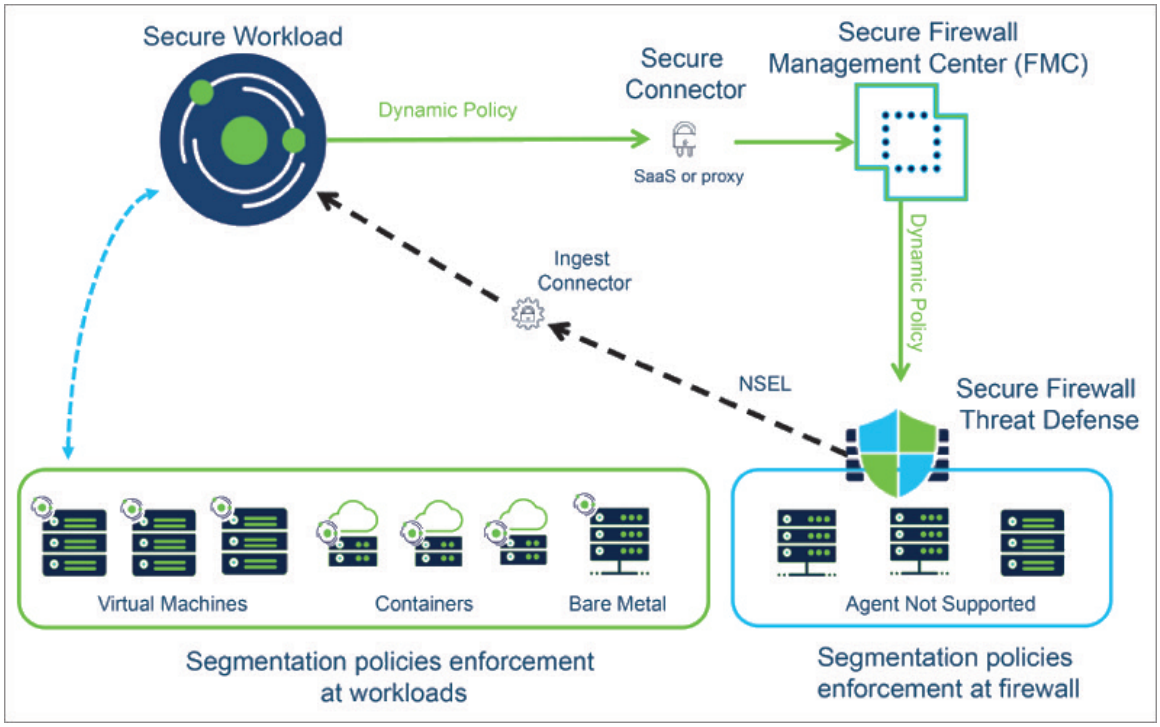
L'orchestrateur externe de Cisco Secure Firewall Management Center ne génère aucune annotation d'utilisateur.

Utilisez ce guide pour déployer la solution applicable à vos versions de produit.

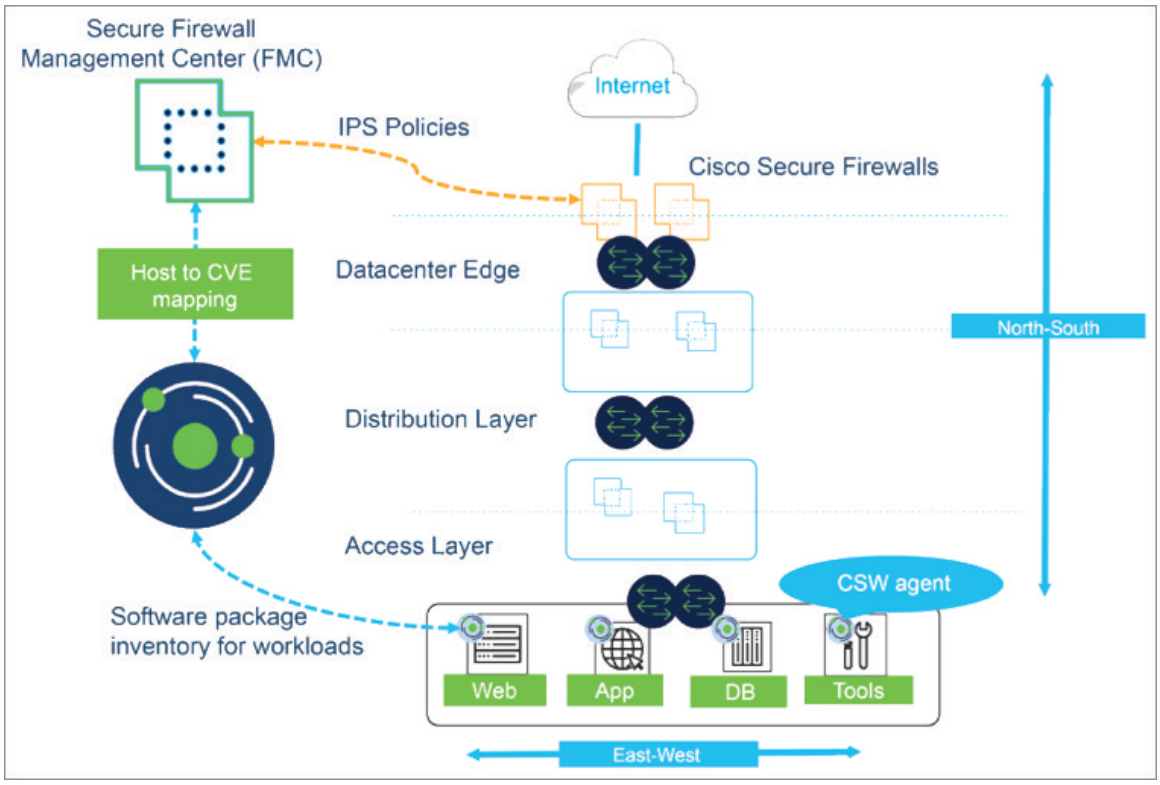
Renseignements importants pour Cisco Secure Workload version 3.8

Cette intégration offre les caractéristiques et avantages suivants :

- Visibilité et application complètes pour les charges de travail sans agent.
- Cisco Secure Workload est capable de recevoir les enregistrements NSEL de Cisco Secure Firewall Management Center et de créer automatiquement des politiques de segmentation pour les charges de travail sans agent.
- Cisco Secure Workload envoie automatiquement les politiques appliquées à Cisco Firewall Management Center.



- Cisco Secure Workload envoie les informations CVE des charges de travail basées sur des agents à Cisco Secure Firewall Management Center pour augmenter la visibilité des charges de travail vulnérables. Cela permet à FMC d'exécuter des recommandations de pare-feu afin d'ajuster les politiques de prévention des intrusions avec les signatures snort appropriées pour se protéger contre les exploits.



L'inventaire du réseau est mis à jour dynamiquement par les portées, les filtres d'inventaire et les grappes Cisco Secure Workload, sur lesquels se fondent vos politiques de segmentation; lorsque des charges de travail sont ajoutées, modifiées ou supprimées de votre réseau, Cisco Secure Workload met automatiquement à jour les objets dynamiques dans Cisco Secure Firewall Management Center sur lesquels les règles de contrôle d'accès correspondantes sont basées.

Aperçu du processus :

1. Déployez Cisco Secure Workload, Cisco Secure Firewall Management Center et les produits Cisco Secure Firewall Threat Defense.
2. Créez le connecteur FMC Cisco Secure Workload et établissez la communication avec Secure Firewall Management Center.
3. Créez des portées, des filtres d'inventaire et des grappes dans Cisco Secure Workload qui définissent les consommateurs et les fournisseurs que vous utiliserez dans vos politiques de segmentation.

   (Les « Consommateur » et « fournisseur » de Cisco Secure Workload correspondent à peu près à la « source » et à la « destination » du trafic dans Cisco Secure Firewall Management Center).
4. Détectez automatiquement les politiques à l'aide du mappage des dépendances des applications ou créez manuellement des politiques de segmentation dans l'espace de travail de l'application de Cisco Secure Workload.
5. Lorsque vous appliquez des politiques dans un espace de travail d'application, Cisco Secure Workload pousse les politiques de segmentation vers Cisco Secure Firewall Management Center en tant que règles de contrôle d'accès. Les consommateurs et les fournisseurs de ces règles sont convertis des portées, filtres d'inventaire et grappes en objets dynamiques dans Cisco Secure Firewall Management Center.

6. Les modifications sont automatiquement déployées sur les périphériques Cisco Secure Firewall Threat Defense gérés par Cisco Secure Firewall Management Center.
7. Cisco Secure Workload vérifie en permanence les modifications et envoie automatiquement les mises à jour toutes les cinq secondes.

   Les objets dynamiques, comme les portées, les filtres d'inventaire et les grappes qui constituent leur source, sont automatiquement mis à jour pour refléter les ajouts, les suppressions et les modifications apportées à l'inventaire de la charge de travail sur votre réseau. Ces modifications, et les modifications de politiques que vous appliquez dans les espaces de travail d'application, y compris l'ordre des politiques, sont automatiquement mises à jour sur les périphériques gérés par Cisco Secure Firewall Threat Defense.

Règles de politique de contrôle d'accès converties

Les types de règles de contrôle d'accès suivants sont ajoutés :

- Règles avec préfixe : *Workload_golden_*

  Ces règles, appelées règles d'or, veillent à ce que Cisco Secure Workload puisse communiquer avec tous les agents Cisco Secure Workload installés sur les charges de travail derrière les pare-feu Cisco Secure Firewall.

- Règles avec préfixe : *Workload_*

  Il s'agit des règles converties à partir des politiques de segmentation dans les espaces de travail des applications pour lesquelles l'application est activée.

- Règles avec préfixe : *Workload_ca_*

  Il s'agit des règles collectrices converties pour chaque espace de travail de l'application mise en œuvre. À partir de la version 3.7 de Cisco Secure Workload, vous pouvez utiliser les règles collectrices de Cisco Secure Workload uniquement si vous avez sélectionné l'option **Use Secure Workload Catch All** (Utiliser les règles collectrices de Cisco Secure Workload) lors de la configuration du connecteur FMC.

- Les objets dynamiques sont créés avec le préfixe : *WorkloadObj_*

L'ordre des règles correspond à l'ordre standard d'application des politiques pour les politiques et les espaces de travail Cisco Secure Workload.

Si vous supprimez ou modifiez ces règles dans FMC, vos modifications seront remplacées la prochaine fois que Cisco Secure Workload transmettra des mises à jour au FMC.

Si vous créez des règles de contrôle d'accès supplémentaires dans FMC indépendamment de cette intégration et que vous configurez l'intégration pour qu'elle fusionne les règles existantes au lieu de les remplacer, cette intégration ne modifie pas vos règles indépendantes, tant qu'elles ne sont pas nommées à l'aide de l'un des préfixes décrits ci-dessus.

Renseignements importants pour Cisco Secure Workload, versions 3.7 et 3.6

Grâce à cette intégration, vous créez des politiques de segmentation dans des espaces de travail Cisco Secure Workload et Cisco Secure Workload convertit les politiques appliquées en règles de contrôle d'accès dans Cisco Secure Firewall Management Center.

L'inventaire du réseau est géré dynamiquement par les portées, les filtres d'inventaire et les grappes Cisco Secure Workload, sur lesquels se fondent vos politiques de segmentation; lorsque des charges de travail sont ajoutées, modifiées ou supprimées de votre réseau, Cisco Secure Workload met automatiquement à jour les objets dynamiques dans Cisco Secure Firewall Management Center sur lesquels les règles de contrôle d'accès correspondantes sont basées.

Aperçu du processus :

1. Vous déployez vos produits Cisco Secure Workload, Cisco Secure Firewall Management Center et Secure Firewall Threat Defense.
2. Vous créez l'orchestrateur externe FMC dans Cisco Secure Workload et établissez la communication avec Cisco Secure Firewall Management Center.
3. Vous créez des portées, des filtres d'inventaire et des grappes dans Cisco Secure Workload qui définissent les consommateurs et les fournisseurs que vous utiliserez dans vos politiques de segmentation.

   (« Consommateur » et « Fournisseur » dans Cisco Secure Workload correspondent à peu près à la « source » et à la « destination » dans Cisco Secure Firewall Management Center).
4. Vous créez manuellement les politiques de segmentation dans les espaces de travail applicatifs dans Cisco Secure Workload.
5. Lorsque vous appliquez des politiques dans un espace de travail d'application, Cisco Secure Workload pousse les politiques de segmentation vers Cisco Secure Firewall Management Center en tant que règles de contrôle d'accès. Les consommateurs et les fournisseurs de ces règles sont convertis des portées, filtres d'inventaire et grappes en objets dynamiques dans Cisco Secure Firewall Management Center.
6. Les modifications sont automatiquement déployées sur les périphériques Cisco Secure Firewall Threat Defense gérés par Cisco Secure Firewall Management Center.
7. Cisco Secure Workload vérifie en permanence les modifications et envoie automatiquement les mises à jour toutes les cinq secondes.

   Les objets dynamiques, comme les portées, les filtres d'inventaire et les grappes qui constituent leur source, sont automatiquement mis à jour pour refléter les ajouts, les suppressions et les modifications apportées à l'inventaire de la charge de travail sur votre réseau. Ces modifications, et les modifications de politiques que vous appliquez dans les espaces de travail d'application, y compris l'ordre des politiques, sont automatiquement mises à jour sur les périphériques gérés par Cisco Secure Firewall Threat Defense.

Règles de politiques de contrôle d'accès converties : détails

- Dans Cisco Secure Workload version 3.7, les politiques de segmentation converties de Cisco Secure Workload sont ajoutées au Cisco Secure Firewall Management Center en tant que règles dans les sections respectives de la politique de contrôle d'accès. Les politiques absolues sont ajoutées dans la section des règles obligatoires et les politiques par défaut dans la section par défaut.
- Dans Cisco Secure Workload version 3.6, les politiques de segmentation converties de Cisco Secure Workload sont ajoutées en tant que règles dans la section par défaut de la politique de contrôle d'accès.

Les types de règles de contrôle d'accès suivants sont ajoutés :

- Règles avec préfixe : *Workload_golden_*

  Ces règles, appelées règles d'or, veillent à ce que Cisco Secure Workload puisse communiquer avec tous les agents Cisco Secure Workload installés sur les charges de travail derrière les pare-feu Cisco Secure Firewall.

- Règles avec préfixe : *Workload_*

  Il s'agit des règles converties à partir des politiques de segmentation dans les espaces de travail des applications pour lesquelles l'application est activée.

- Règles avec préfixe : *Workload_ca_*

  Il s'agit des règles collectrices converties pour chaque espace de travail de l'application mise en œuvre. À partir de la version 3.7 de Cisco Secure Workload, vous ne pouvez utiliser les règles collectrices de Cisco Secure Workload que si vous avez sélectionné l'option **Use Secure Workload Catch All** (Utiliser les règles collectrices de Cisco Secure Workload) lors de la configuration de l'orchestrateur externe de FMC.

L'ordre des règles correspond à l'ordre standard d'application des politiques pour les politiques et les espaces de travail Cisco Secure Workload.

Si vous supprimez ou modifiez ces règles dans FMC, vos modifications seront remplacées la prochaine fois que Cisco Secure Workload transmettra des mises à jour au FMC.

Si vous créez des règles de contrôle d'accès supplémentaires dans FMC indépendamment de cette intégration et que vous configurez l'intégration pour qu'elle fusionne les règles existantes au lieu de les remplacer, cette intégration ne modifie pas vos règles indépendantes, tant qu'elles ne sont pas nommées à l'aide de l'un des préfixes décrits ci-dessus.

Objets dynamiques convertis : détails

Pour afficher les objets dynamiques, accédez à l'interface Web de FMC et sélectionnez **Objects (Objets) > Object Management (Gestion des objets) > External Attributes (Attributs externes) > Dynamic Objects (Objets dynamiques)** .

Les objets dynamiques convertis à partir de portées, de filtres d'inventaire et grappes Cisco Secure Workload, ainsi que les objets dynamiques supplémentaires requis par cette intégration, sont affichés dans la liste des objets dynamiques de FMC dans les formats suivants, selon la version de Cisco Secure Workload :

- Dans Cisco Secure Workload 3.7 :
  - Dans la colonne **Name** (Nom), les objets dynamiques sont répertoriés au format *WorkloadObj_<Secure Workload inventory filter name>*.
  - Les UUID sont affichés dans la colonne **Description** (Description). Si les UUID d'un objet sont manquants, le nom du filtre d'inventaire Cisco Secure Workload s'affiche.
- Dans Cisco Secure Workload 3.6 : les objets dynamiques sont répertoriés avec le préfixe *WorkloadObj_* .

Si vous devez modifier ces objets : modifiez les portées, les filtres d'inventaire et les grappes dans Cisco Secure Workload. Toutes les modifications que vous apportez dans FMC seront remplacées lors de la prochaine mise à jour de l'intégration par Cisco Secure Workload.

Utilisez les objets dynamiques générés par cette intégration à d'autres fins avec prudence, car leur adhésion est susceptible de changer.

Cette intégration n'a aucune incidence sur les objets dynamiques créés et gérés à l'aide d'autres mécanismes.

Facteurs à prendre en considération lors du déploiement des versions 3.7 et 3.6 de Cisco Secure Workload

Pour toutes les versions 3.7 :

Un seul orchestrateur FMC est pris en charge par Cisco Secure Firewall Management Center (anciennement Firepower Management Center).

Remarque L'orchestrateur externe Cisco Secure Workload FMC peut détecter les basculements si le FMC ne répond plus. En cas de basculement, le système efface les données en mémoire et commence la resynchronisation avec une instance FMC active. Il se peut qu'il faille trop de temps à FMC pour reproduire la configuration actuelle dans Cisco Secure Workload, ce qui entraîne l'expiration du délai de l'orchestrateur externe et une nouvelle tentative de synchronisation. Le délai d'expiration pour cette synchronisation de configuration est de 10 minutes.

FMC se protège également contre un trop grand nombre de requêtes utilisées par un seul point terminal à partir de la version 7.2 de FMC et des versions antérieures. Si FMC détecte plus de 120 requêtes en une minute, il répond par un message « Too Many Requests » (Trop de requêtes) HTTP 429 pendant une minute après avoir atteint 120 requêtes. Cette limitation est évitée dans la plupart des terminaux FMC grâce à des insertions et des lectures en bloc. Cependant, la collecte du contenu de tous les objets dynamiques entraîne une requête pour chacun d'eux.

Les limites d'une intégration se comportant correctement sont basées sur le temps nécessaire à l'orchestrateur de Cisco Secure Workload pour récupérer tous les composants de la politique (limité à 10 minutes). Chaque demande d'objet est affectée par la latence du réseau, le modèle et la charge du FMC.

Par exemple, la première minute est consacrée à recueillir des renseignements généraux sur FMC (nombre de FTD, de politiques de contrôle d'accès et de domaines), puis le reste est partagé entre 4,5 minutes à recueillir l'objet dynamique ou le filtre d'inventaire (540) et les 4,5 minutes suivantes à synchroniser les règles de politique (11 250).

Par conséquent, une charge raisonnable pour les versions actuelles des intégrations de produits serait de 10 minutes = 1 minute (pour l'installation) + (0,024 seconde * nombre de règles dans la politique du logiciel) + (0,5 seconde * nombre de filtres d'inventaire utilisés). Le dépassement de cette limite entraîne un chargement partiel qui est constaté lorsque la politique de contrôle d'accès reste dans l'état « désynchronisé » du FMC.

Pour toutes les versions 3.6 :

Un seul orchestrateur FMC est pris en charge par centre de gestion Cisco Firepower Management Center.

Si vous utilisez la version 3.6.1.36 ou ultérieure et que votre déploiement utilise des domaines :

Toutes les politiques appliquées dans tous les espaces de travail Cisco Secure Workload sont transmises à toutes les politiques de contrôle d'accès des domaines que vous spécifiez dans la configuration de l'orchestrateur FMC. (À l'exception des politiques de contrôle d'accès qui ne sont pas affectées à au moins un périphérique FTD).

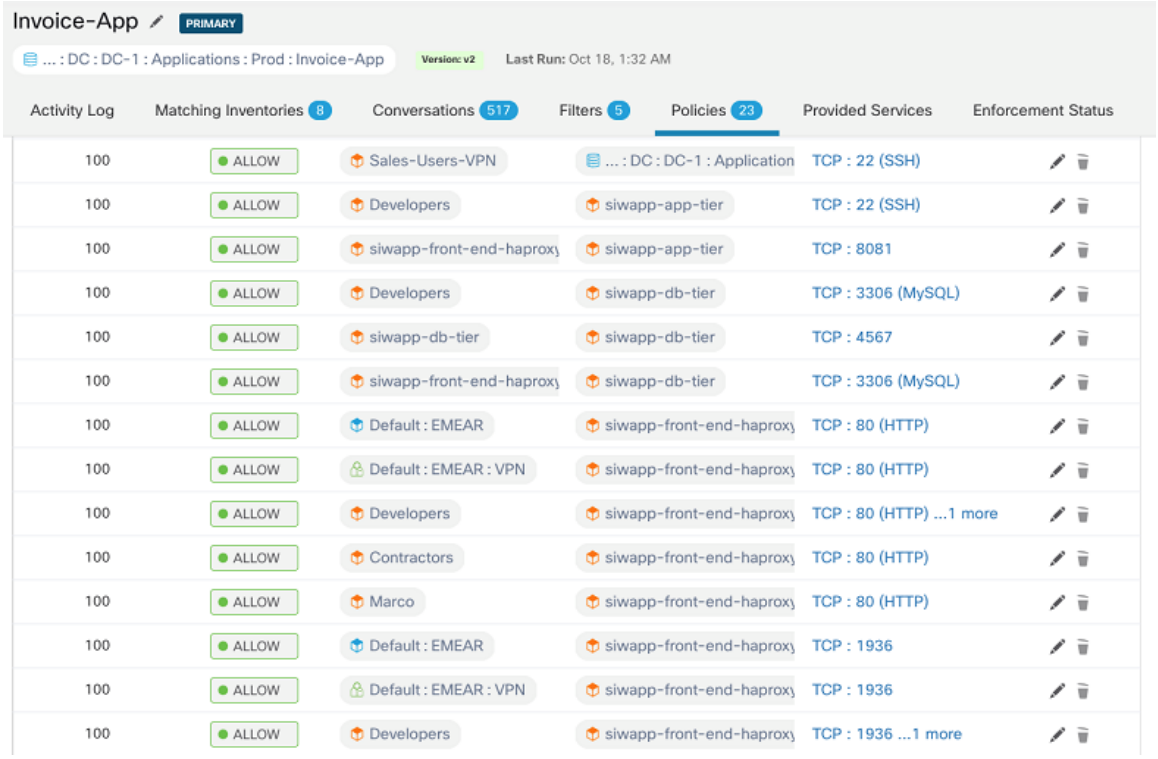
Si votre déploiement n'utilise pas de domaines OU si vous utilisez une version 3.6 antérieure à 3.6.1.36 :

Toutes les politiques appliquées dans tous les espaces de travail Cisco Secure Workload sont poussées vers toutes les politiques de contrôle d'accès qui sont affectées à un périphérique FTD.

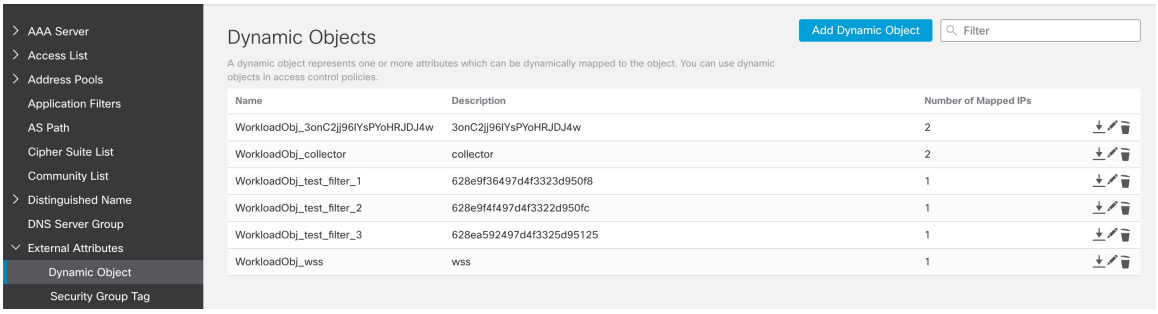
Exemple de configuration avec des objets dynamiques

Les exemples suivants illustrent l'intégration de Cisco Secure Workload version 3.7 à Cisco Secure Firewall Management Center version 7.0.1.

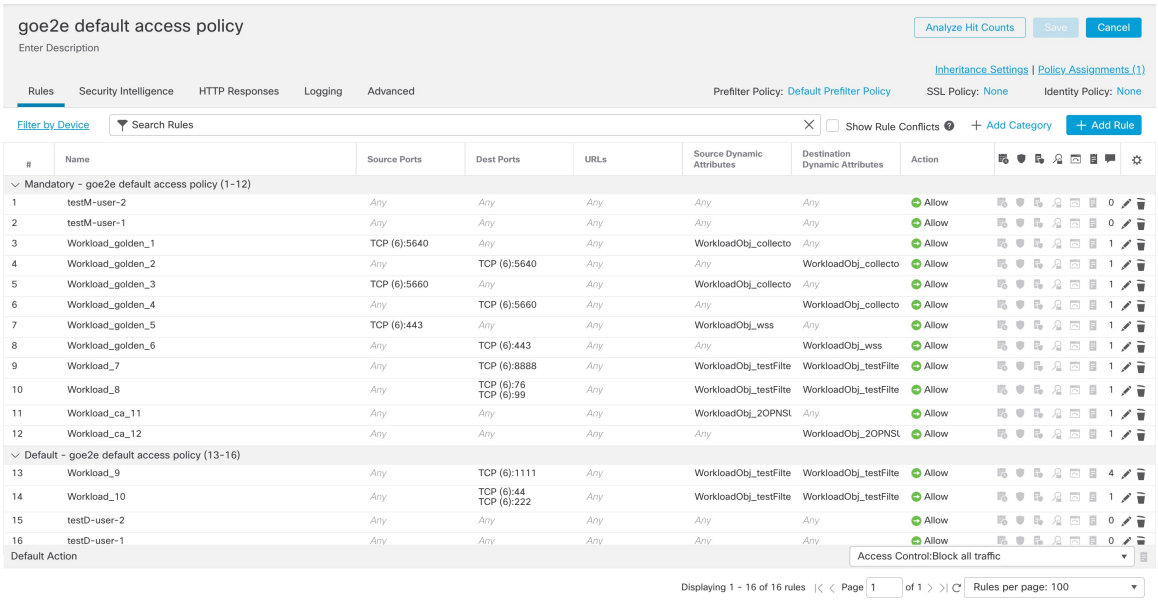
Politiques de segmentation dans Cisco Secure Workload



Objets dynamiques dans FMC

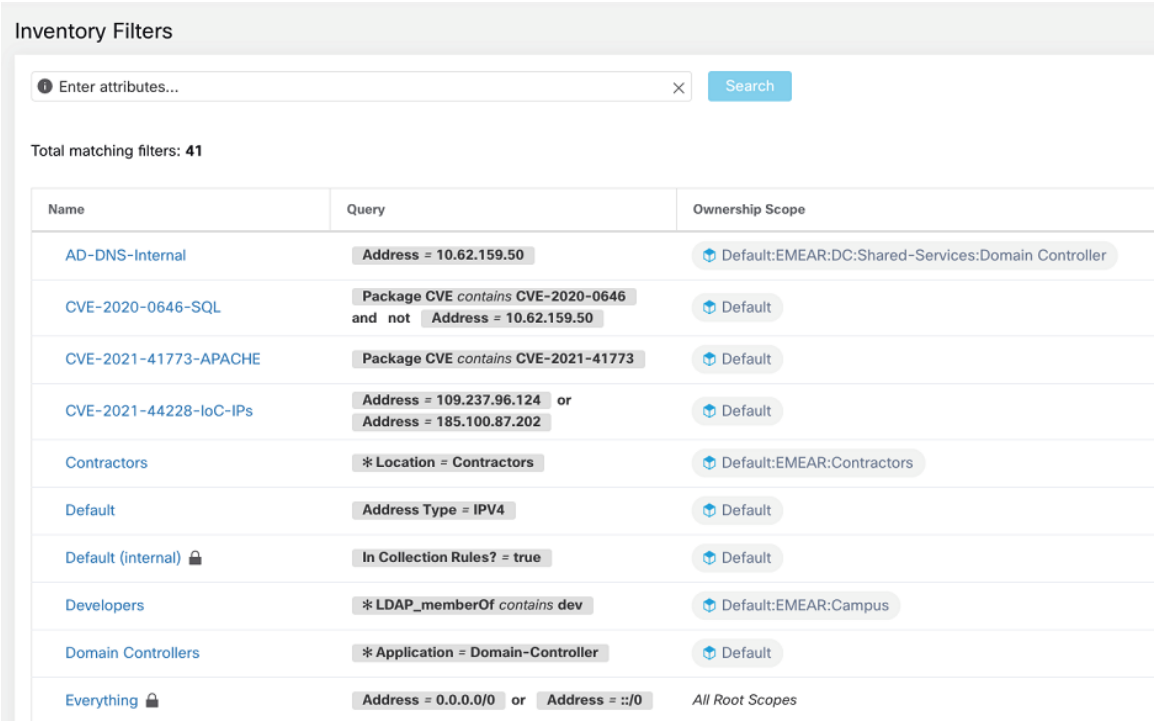


Politique de contrôle d'accès dans FMC



Portées et inventaire dans Cisco Secure Workload

Filtres dans Cisco Secure Workload



Déploiements pris en charge

Version du produit

Principales caractéristiques	Version de Cisco Secure Workload	Version de Cisco Secure Firewall Management Center et de Cisco Secure Firewall Threat Defense
Flux de travail simplifié pour le mappage de la portée aux politiques de contrôle d'accès pour l'application de Cisco Secure Firewall Management Center (FMC) et de Cisco Firepower Threat Defense (FTD).	3.9.1.1	7.2 pour la segmentation et l'application des correctifs virtuels 7.1.x pour l'application de correctifs virtuels 7.0.1 pour la segmentation

Principales caractéristiques	Version de Cisco Secure Workload	Version de Cisco Secure Firewall Management Center et de Cisco Secure Firewall Threat Defense
• Connecteur FMC pour simplifier la préparation à l'intégration FMC. • Capacité d'effectuer une application tenant compte de la topologie avec le mappage de la politique de contrôle d'accès avec la portée. • Application de correctifs virtuels pour publier des CVE à partir de charges de travail	3.8.1.1 3.8.1.36	7.2 pour la segmentation et l'application des correctifs virtuels 7.1.x pour l'application de correctifs virtuels 7.0.1 pour la segmentation
• Possibilité de modifier la priorité des politiques de segmentation de Cisco Secure Workload affichées comme des règles dans les sections Obligatoire et Par défaut de la politique de contrôle d'accès dans FMC. • Possibilité d'utiliser les règles collectrices CSW ou leur équivalent FMC, l'action par défaut de la politique de contrôle d'accès.	3.7.1.5	7.1 7.0.1
Prise en charge des domaines FMC lors de l'utilisation de politiques de contrôle d'accès avec des objets dynamiques	3.6.1.36	7.1 7.0.1
Politiques de contrôle d'accès avec des objets dynamiques **Remarque** Les politiques de préfiltre ne sont pas prises en charge à partir de Cisco Secure Workload version 3.6 et des versions ultérieures.	3.6	7.1 7.0.1

Principales caractéristiques	Version de Cisco Secure Workload	Version de Cisco Secure Firewall Management Center et de Cisco Secure Firewall Threat Defense
Règles du préfiltre	3.5	7.0 6.7 6.6

Plateformes et déploiements Cisco Secure Firewall pris en charge

- Seuls les périphériques Cisco Secure Firewall Threat Defense gérés par Cisco Secure Firewall Management Center sont pris en charge.
- La haute disponibilité du FMC est prise en charge si elle est configurée.

  Si vous incluez le nom d'hôte/l'adresse IP du FMC de secours/secondaire lors de la configuration de l'orchestrateur externe du FMC, lorsque le FMC bascule vers le nouvel appareil primaire actif, l'intégration bascule automatiquement pour utiliser le nouveau FMC actif.
- Les modes de pare-feu routé et transparent de Cisco Secure Firewall Threat Defense (FTD) sont tous deux pris en charge.

  Pour en savoir plus sur les modes de Cisco Secure Firewall Threat Defense, consultez le chapitre sur le mode de pare-feu transparent ou routé Cisco Secure Firewall Threat Defense dans le *Guide de configuration de Cisco Secure Firewall Management Center* pour votre version.

Exigences supplémentaires pour les versions 3.7 et 3.6 de Cisco Secure Workload

Nous vous recommandons d’utiliser un FMC dédié pour cette intégration.

Exigences supplémentaires dans la version 3.5 de Cisco Tetration

Les FTD doivent être affectés à un domaine dédié, utilisé uniquement pour l’intégration avec Tetration. Ainsi, les appareils FTD affectés sont les seuls vers lesquels les politiques Tetration sont transmises.

Pour plus d'informations sur la création de nouveaux domaines, la gestion des domaines et le déplacement de périphériques entre les domaines, consultez la section Gestion des domaines dans le chapitre Gestion des déploiements du Guide de configuration du Cisco Firepower Management Center pour votre version de Firepower. Par exemple :Guide de configuration du Cisco Firepower Management Center version 6.7

.

Mise en œuvre de cette intégration pour Cisco Secure Workload, version 3.9.1.1

Cette section s’applique à toutes les versions 3.9.

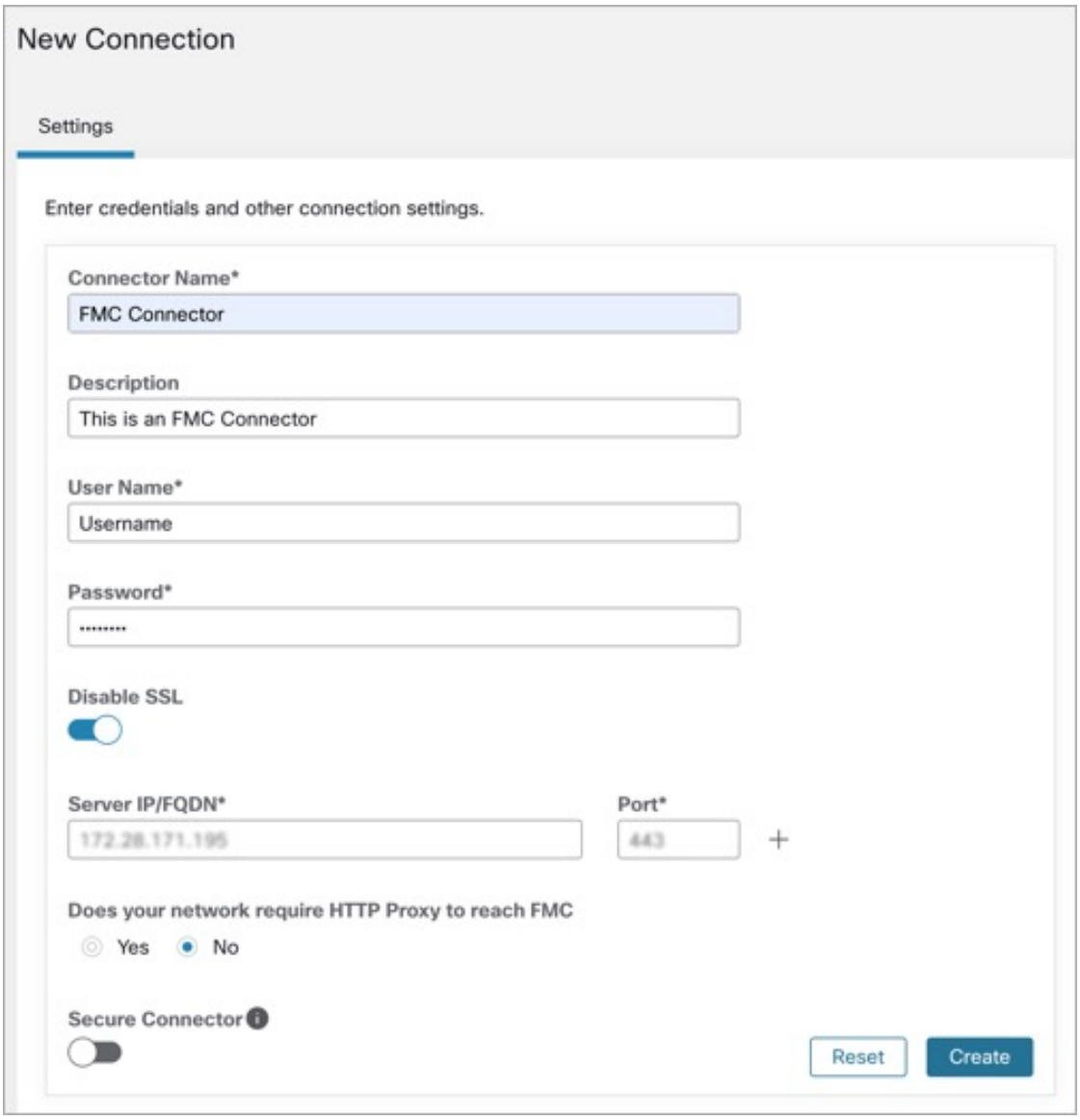
Paramètres de la version 3.9.1.1

Créez le connecteur FMC dans Cisco Secure Workload pour établir la communication avec Cisco Secure Firewall Management Center.

1. Dans le volet de navigation, choisissez **Manage (Gestion)** > **Workloads (Charges de travail)** > **Connectors (Connecteurs)**.
2. Sous **Firewall (Pare-feu)**, cliquez sur **Cisco Secure Firewall**.
3. Cliquez sur **Configure your new connector here** (Configurer votre nouveau connecteur ici).
4. À la page **New Connection** (Nouvelle connexion), saisissez les renseignements d'authentification et les autres paramètres de connexion comme suit :

Champs	Description
Nom du connecteur	Attribuez un nom unique au connecteur FMC.
Description	Saisissez une description
Nom d'utilisateur et mot de passe	Saisissez les renseignements d'authentification utilisés pour communiquer avec le FMC.
Certificat de l'autorité de certification	Pour utiliser l'authentification sécurisée, saisissez le certificat de l'autorité de certification utilisé par Cisco Secure Workload pour authentifier cet appareil FMC. Vous pouvez également cocher l'option **Disable SSL** (Désactiver SSL) lorsque le réseau est fiable et que Cisco Secure Workload ne valide pas le certificat. Vous pouvez obtenir le certificat d'autorité de certification auprès du FMC en utilisant le flux de travail de gestion des objets.
Server IP/FQDN* and Port (Adresse IP du serveur/Nom de domaine complet* et Port)	Saisissez l'adresse IP du serveur et le numéro de port du FMC associé. Le nom d'hôte doit être un nom de domaine complet ou une adresse IP du FMC.
Votre réseau nécessite-t-il un serveur mandataire (serveur mandataire) HTTP pour atteindre FMC?	Si oui, saisissez l'URL du serveur mandataire au format <hôte du serveur mandataire> :<port du serveur mandataire>
Connecteur sécurisé	Activez l'option si un connecteur sécurisé est utilisé pour tunneliser les connexions entre Cisco Secure Workload et FMC. Notez qu'avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé.

5. Cliquez sur **Create** (créer).



Segmentation dans la version 3.9.1.1

Les politiques de segmentation appliquées par Cisco Secure Workload sont converties en politiques de contrôle d'accès, à l'aide d'ensembles d'adresses IP extraits des portées, des filtres d'inventaire et des grappes. Ces ensembles sont convertis en objets dynamiques dans Cisco Secure Firewall Management Center.

Les politiques de segmentation converties de Cisco Secure Workload sont ajoutées au Cisco Secure Firewall Management Center en tant que règles dans les sections respectives de la politique de contrôle d'accès. Les politiques absolues sont ajoutées dans la section de règles obligatoires et les politiques par défaut sont ajoutées dans la section de règles par défaut.

Les types de règles de contrôle d'accès suivants sont ajoutés :

- Règles avec préfixe : *Workload_ golden_* :

Ces règles, appelées règles d'or, veillent à ce que Cisco Secure Workload puisse communiquer avec tous les agents Cisco Secure Workload installés sur les charges de travail derrière les pare-feux sécurisés.

- Règles avec préfixe : *Workload_* :

  Il s'agit des règles converties à partir des politiques de segmentation dans les espaces de travail applicatifs pour lesquelles l'application de la règle est activée.

- Règles avec préfixe : *Workload_ca_* :

  Il s'agit des règles collectrices converties pour chaque espace de travail de l'application mise en œuvre. À partir de la version de Cisco Secure Workload, vous ne pouvez utiliser les règles collectrices de Cisco Secure Workload que si vous avez sélectionné l'option Use Secure Workload Catch-All (Utiliser les règles collectrices de Cisco Secure Workload) lors de la configuration du connecteur FMC.

- Les objets dynamiques sont créés avec le préfixe : *WorkloadObj_*

Remarque

- Si vous supprimez ou modifiez ces règles dans FMC, vos modifications seront remplacées la prochaine fois que Cisco Secure Workload enverra des mises à jour sur FMC.
- Si vous créez d'autres règles de contrôle d'accès dans FMC qui sont indépendantes de cette intégration et que vous configurez l'intégration pour qu'elle fusionne plutôt que remplace les règles existantes, cette intégration ne modifie pas vos règles indépendantes, tant qu'elles ne sont pas nommées à l'aide de l'un des préfixes décrits ci-dessus.

Ajouter un mappage de politique de contrôle d'accès

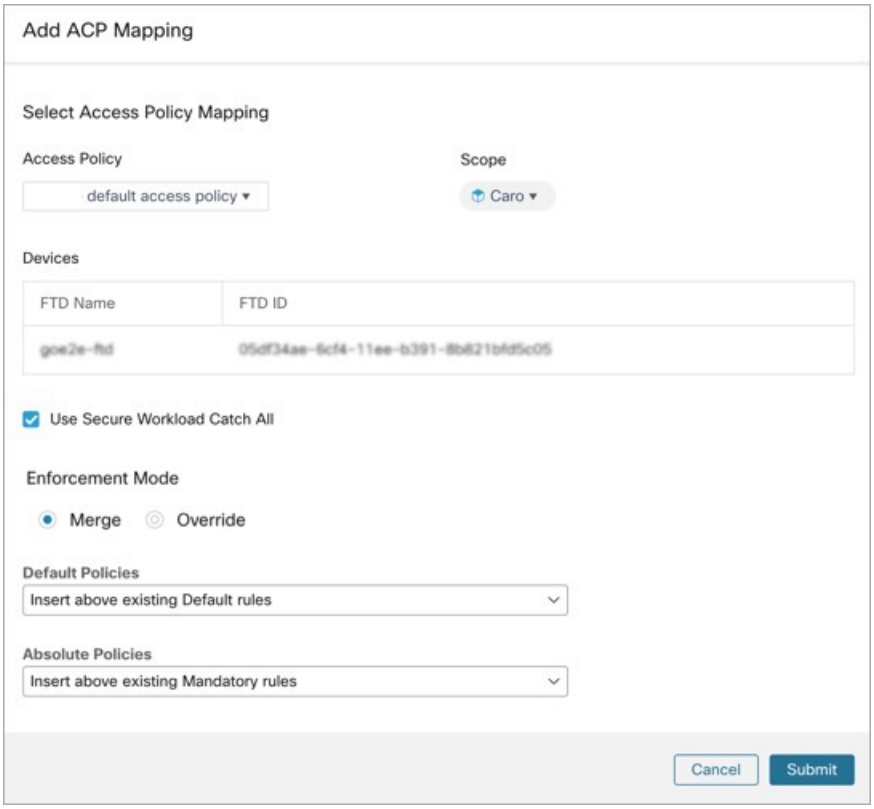
1. Dans l'onglet **Segmentation**, cliquez sur **+ Ajouter** pour associer une politique d'accès.
2. Dans la fenêtre **Add ACP Mapping** (Ajouter un mappage de la politique de contrôle d'accès), choisissez une **politique d'accès** dans la liste déroulante et associez-la à une portée. Vous ne pouvez associer une politique d'accès qu'à une seule portée.
3. Cochez la case **Use Secure Workload Catch All** (Utiliser les règles collectrices de Cisco Secure Workload) pour activer les règles collectrices de Cisco Secure Workload. Les règles collectrices de Cisco Secure Workload sont répertoriées après toutes les autres règles (les règles Cisco Secure Workload et les règles créées directement dans FMC, le cas échéant) dans la section par défaut des politiques de contrôle d'accès. Si vous décidez de désactiver les règles collectrices de Cisco Secure Workload, décochez cette option pour utiliser l'action par défaut de la politique de contrôle d'accès de FMC.
4. Sélectionnez une option de **Enforcement Mode** (Mode d'application).
   - **Fusionner** : les règles de politique Cisco Secure Workload sont ajoutées en même temps que les règles existantes créées par les utilisateurs. Vous pouvez configurer la priorité comme expliqué à l'étape suivante.
   - **Remplacer** : les règles existantes créées par les utilisateurs sont remplacées par les règles de politique Cisco Secure Workload.

Remarque La liste déroulante des priorités n'est disponible que lorsque **Merge** (Fusionner) est sélectionné comme mode d'application.

5. Dans les menus déroulants des politiques **absolue** et **par défaut**, choisissez l'option requise pour définir la priorité des politiques Cisco Secure Workload comme étant supérieure ou inférieure aux règles préexistantes dans la section respective de la politique de contrôle d'accès dans FMC.
   - Si vous choisissez l'option Insert above existing Mandatory rules (Insérer au-dessus des règles obligatoires existantes), les politiques Cisco Secure Workload ont une priorité plus élevée que les règles obligatoires.
   - Si vous choisissez l'option Insert below existing Mandatory rules (Insérer sous les règles obligatoires existantes), les politiques Cisco Secure Workload ont une priorité inférieure aux règles obligatoires.

   Par exemple, dans la liste déroulante **Politiques absolues**, si vous choisissez Insert above existing Mandatory rules (Insérer au-dessus des règles obligatoires existantes), les règles Cisco Secure Workload sont configurées au début de la section Obligatoire, suivies des règles de contrôle d'accès préexistantes dans Cisco Secure Firewall Management Center. Lorsqu'une nouvelle règle est créée, l'ordre des règles de la politique de contrôle d'accès est mis à jour en fonction de la priorité sélectionnée pour les politiques dans Cisco Secure Workload.
6. Cliquez sur **Submit** (Envoyer).

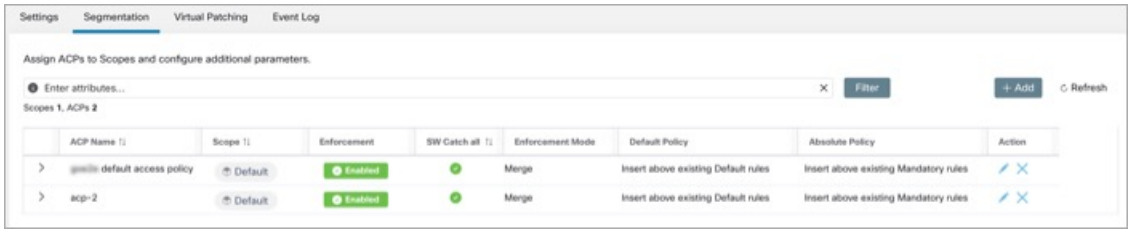
Illustration 2 : Ajouter un mappage de politique de contrôle d'accès



Modifier le mappage de la politique de contrôle d'accès

1. Sous **Action**, cliquez sur l'icône en forme de crayon pour modifier le mappage.
2. Mettez à jour les renseignements existants et cliquez sur **Submit** (Envoyer).
3. Cliquez sur **Save** (Enregistrer) pour enregistrer toutes les modifications.

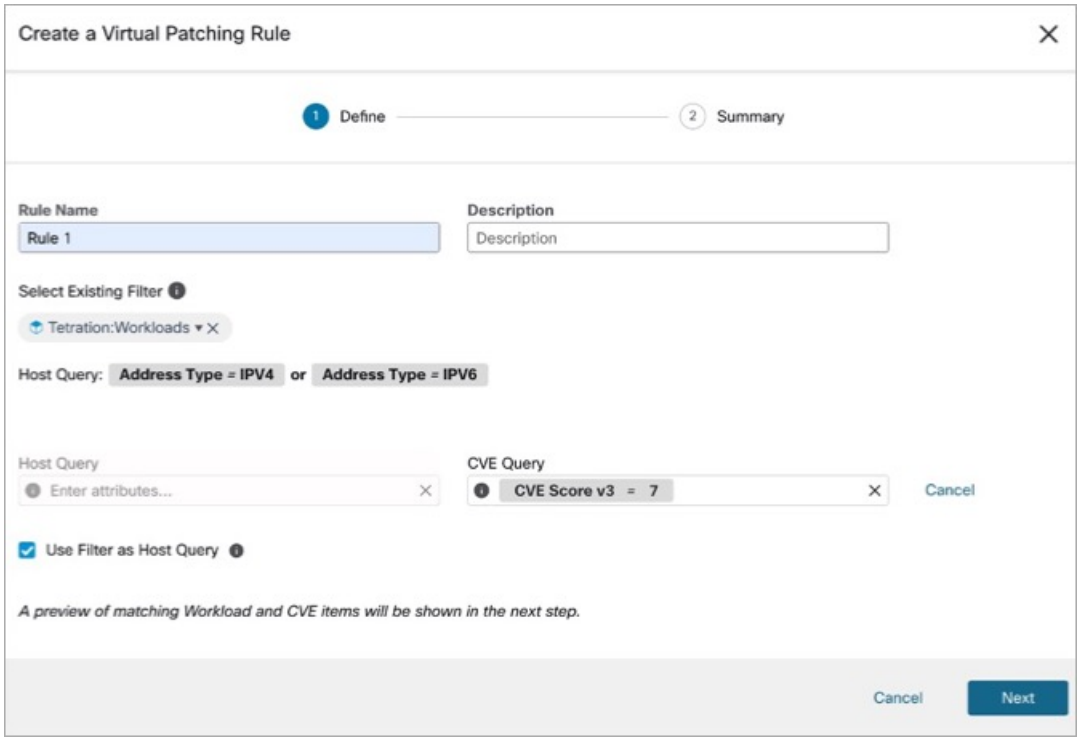
Illustration 3 : Modifier le mappage de la politique de contrôle d'accès



Application de correctifs virtuels dans la version 3.9.1.1

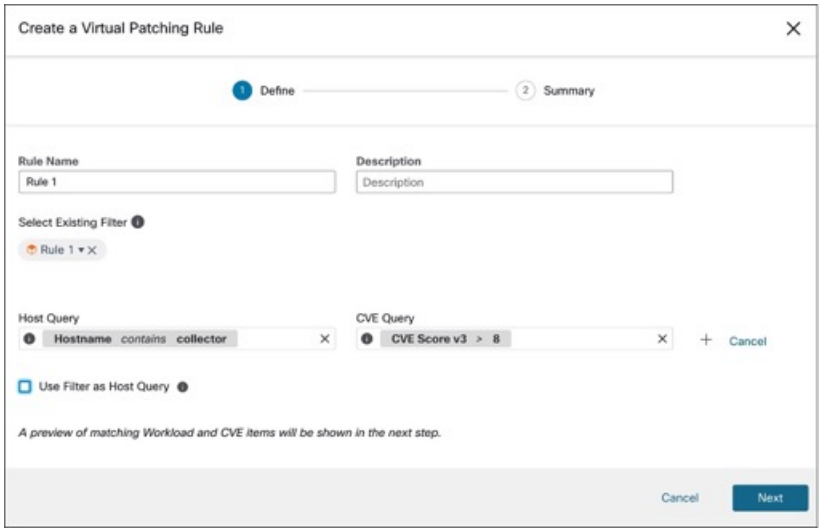
1. Dans la fenêtre **Create a Virtual Correctif Rule** (créer une règle d'application de correctifs virtuels), saisissez un **Rule Name** (Nom de règle) et une **Description** (description) pour la règle.
2. Sélectionnez un filtre existant dans la liste déroulante. Vous pouvez sélectionner une portée ou sous-portée existante pour sélectionner les hôtes à prendre en compte pour l'application de correctifs virtuels.
   - Par défaut, la case **Use Filter as Host Query** (utiliser le filtre comme requête d'hôte) est cochée. Vous pouvez continuer en saisissant simplement la requête CVE; sans créer de nouveau filtre d'application de correctifs virtuels. La requête de l'hôte comprend le contenu du filtre choisi.

Figure 4: Sans créer de nouveau filtre d'application de correctifs virtuel



- Décochez la case **Use Filter as Host Query** (Utiliser le filtre comme requête hôte) pour saisir à la fois la requête hôte et la requête CVE. Cela crée un nouveau filtre d'application de correctifs virtuels.

Figure 5: Créer un nouveau filtre d'application de correctif virtuel



3. Saisissez une requête d'hôte et de CVE. Cliquez sur l'icône + pour ajouter d'autres requêtes.

Note

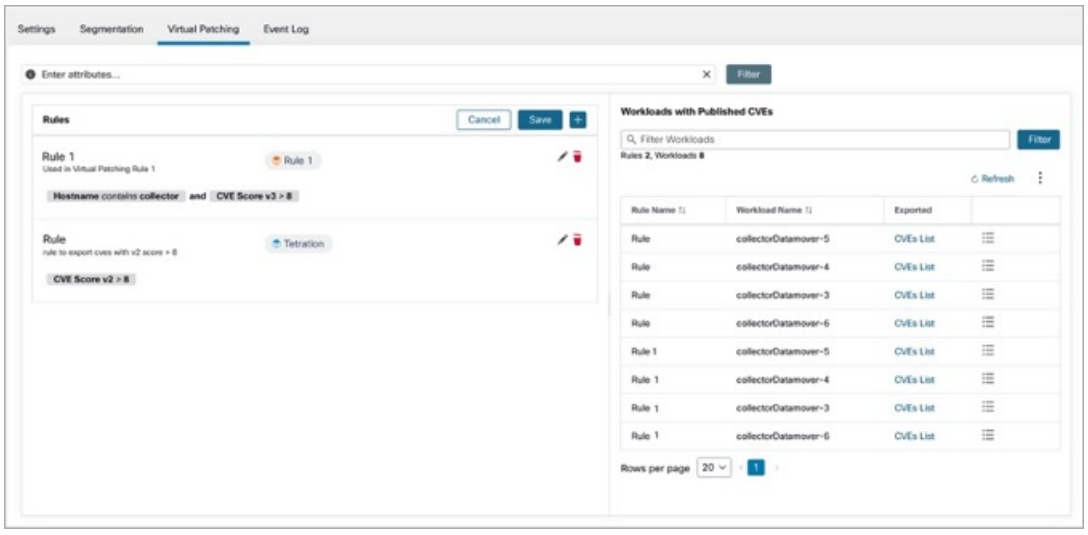
- Passez le curseur sur l'icône d'**information** pour afficher les formats de requête pris en charge.
- Par défaut, un filtre d'application de correctifs virtuels est créé en fonction de la combinaison de requêtes saisie.

4. Cliquez sur **Next** (suivant). Dans la fenêtre **Summary** (résumé), les listes des charges de travail et des CVE correspondants sont affichées. Les charges de travail et les CVE sont mises en correspondance de manière dynamique en fonction de la requête.
5. Cliquez sur **Create** (créer).
6. Les règles d'application de correctifs virtuels ajoutées sont affichées sous **Rules** (Règles). Saisissez les attributs et cliquez sur **Filter** (filtrer) pour affiner les résultats de la recherche.
7. Les charges de travail avec des CVE publiées sont affichées sur la droite.
   - Saisissez les attributs et cliquez sur **Filter** (filtrer) pour affiner les résultats de la recherche.
   - Cliquez sur les en-têtes de colonne pour trier les entrées.
   - Dans la colonne **Exported** (exporté), cliquez sur **CVEs List** (Liste des CVE) pour afficher une liste de tous les CVE publiés d'une charge de travail.
   - Cliquez sur le menu contextuel pour afficher le **journal d'audit** d'une charge de travail. Les journaux des 48 dernières heures sont stockés et affichés.

Modifier une règle d'application de correctifs virtuels

1. Cliquez sur **Edit** (modifier) pour ajouter d'autres règles, modifier les renseignements détaillés et/ou supprimer une règle.

   Figure 6: Modifier une règle d'application de correctifs virtuels



   - Cliquez sur l'icône + pour ajouter d'autres règles. Cliquez sur **Save** (enregistrer).

- Cliquez sur l'icône de la **corbeille** pour supprimer une règle.

2. Cliquez sur **l'icône** en forme de **crayon** pour modifier les détails d'une règle.
3. Dans la fenêtre **Edit Virtual Correctif Rule** (modifier la règle d'application de correctifs virtuels), modifiez la requête d'hôte et la requête CVE au besoin, puis enregistrez les modifications.

Le journal des événements dans la version 3.9.1.1

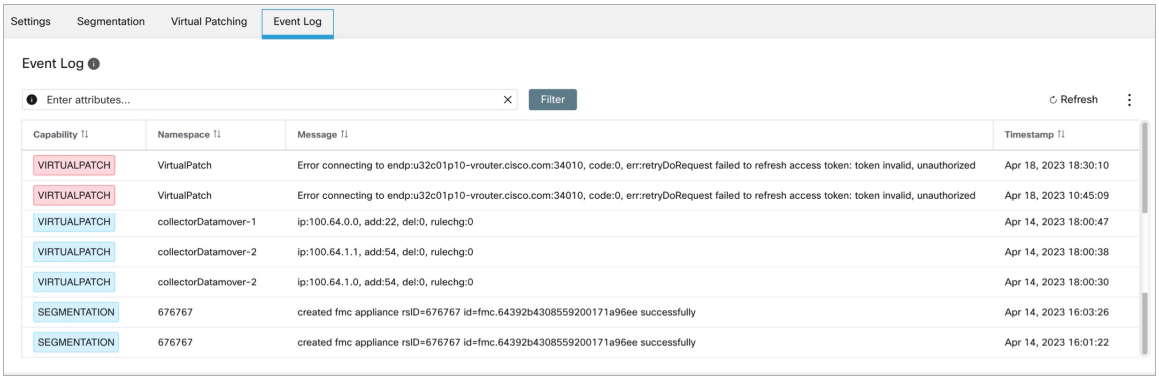
L'onglet **Event Log** (Journal des événements) répertorie les événements ou les transactions importants entre Cisco Secure Workload et Cisco Secure Firewall Management Center.

1. Saisissez les attributs pour filtrer les événements en fonction de la capacité, du niveau de l'événement, de l'espace de noms et du message.

Remarque Les codes de couleur pour le niveau de l'événement sont Information (bleu), Avertissement (orange) et Erreur (rouge).

2. Cliquez sur les en-têtes de colonne pour trier les entrées.
3. Cliquez sur l'icône du menu en trois points pour télécharger les détails au format JSON et/ou CSV.
4. Cliquez sur **Refresh** (Actualiser) pour réinitialiser tous les filtres.

Illustration 7 : Journal des événements



Mise en œuvre de cette intégration pour Cisco Secure Workload, version 3.8.1.1

Cette section s'applique à toutes les versions 3.8.

À propos des mises à niveau

Mises à niveau vers Cisco Secure Workload, version 3.8.1.1

- Mises à niveau à partir de la version 3.7.1.5

  L'orchestrateur externe FMC est migré vers Cisco Secure Firewall.

  Vos configurations préalables à la mise à niveau ne changent pas.

Après la mise à niveau vers la version 3.8.1.1, vous pouvez effectuer les opérations suivantes :

- Publiez des renseignements CVE provenant des charges de travail basées sur des agents dans Cisco Secure Firewall Management Center pour affiner les politiques IPS en exécutant les recommandations du pare-feu.
- Définissez la priorité des politiques de segmentation à répertorier dans les sections Obligatoire ou Par défaut de la politique de contrôle d'accès.
- Pour activer ou désactiver l'option d'utilisation des règles collectrices de Cisco Secure Workload, activez ou désactivez l'option **Use Secure Workload Catch All** (Utiliser les règles collectrices de Cisco Secure Workload) lors de la configuration du connecteur FMC.

Conditions préalables à l'intégration : Cisco Secure Workload, version 3.8.1.1

- Vous avez configuré un Cisco Secure Firewall Management Center (FMC) et au moins un périphérique Cisco Secure Firewall Threat Defense (FTD) pris en charge. Vous avez associé les périphériques FTD au FMC, affecté chaque FTD à une politique de contrôle d'accès et vérifié que les politiques peuvent être déployées du FMC sur les FTD et que le système traite le trafic réseau comme prévu.

  Pour obtenir des renseignements complets, consultez la documentation de Cisco Secure Firewall Management Center pour vos produits, y compris les feuilles de route relatives à la documentation de Cisco Secure Firewall Management Center.
- Votre appareil Cisco Secure Workload (sur site) ou votre compte (SaaS) est configuré et fonctionne comme prévu.
- Si vous utilisez un logiciel-service (SaaS) Cisco Secure Workload, ou si un Cisco Secure Workload local ne peut pas atteindre directement l'appareil FMC, configurez un tunnel de connecteur sécurisé pour assurer la connectivité entre les composants de la solution.

  Par défaut, Cisco Secure Workload communique avec l'API REST FMC à l'aide de HTTPS sur le port 443.

  Pour obtenir des instructions sur la configuration du connecteur sécurisé, consultez le guide de l'utilisateur Cisco Secure Workload, disponible dans l'aide en ligne de l'interface Web Cisco Secure Workload.

Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.8.1.1

Le tableau suivant présente le flux de travail de bout en bout pour configurer Cisco Secure Firewall Management Center et configurer l'intégration avec Cisco Secure Workload version 3.8.1.1.

Étape	Description	Autres renseignements
Avant de commencer	Découvrez comment fonctionne cette intégration, le processus de haut niveau pour sa mise en œuvre et toutes les considérations relatives au déploiement.	Consultez toutes les sections et tous les sujets sous Renseignements importants pour Cisco Secure Workload version 3.8, à la page 3.
Avant de commencer	Répondre aux exigences et aux conditions préalables	Consultez toutes les sections de Déploiements pris en charge, à la page 12 et Conditions préalables à l'intégration : Cisco Secure Workload, version 3.8.1.1, à la page 23.
1	Dans Cisco Secure Workload : Définissez les portées, les filtres d'inventaire, les grappes, les espaces de travail et les politiques de segmentation pour votre environnement.	Détectez automatiquement les politiques à l'aide du mappage des dépendances des applications ou créez manuellement des politiques de segmentation dans l'espace de travail de l'application de Cisco Secure Workload. Si vous avez des questions à ce sujet, consultez la section sur la segmentation du guide de l'utilisateur Cisco Secure Workload, disponible comme aide en ligne à partir de votre interface Web Cisco Secure Workload. Vous pouvez également consulter Avancé : Utiliser ADM pour générer des politiques de segmentation , à la page 54.
2	Dans FMC : Définissez l' **action par défaut** de la politique au bas de chaque politique de contrôle d'accès affectée à une protection contre les menaces Cisco Secure Firewall Threat Defense.	Cette action dépend des politiques de segmentation que vous créez. Par exemple, si vous souhaitez bloquer tout le trafic qui n'est pas explicitement autorisé par les politiques de segmentation, sélectionnez **Block all traffic** (Bloquer tout le trafic).
3	Dans FMC : Créez un compte d'utilisateur dédié à cette intégration.	Exigences pour ce compte d'utilisateur : • Le compte doit avoir le rôle Administrateur. • (Si des domaines sont configurés sur le FMC) Le compte doit avoir accès au domaine Global. Si vous avez des questions sur la création de comptes utilisateur dans FMC, consultez la rubrique « Ajouter un utilisateur interne » dans l'aide en ligne de Cisco Secure Firewall Management Center.

Étape	Description	Autres renseignements
4	Dans Cisco Secure Workload : Créez un connecteur FMC.	Créez un seul connecteur FMC par Cisco Secure Firewall Management Center. Pour créer un connecteur FMC, consultez la section Configurer le connecteur FMC en version 3.8.1.1, à la page 25.
5	Dans Cisco Secure Workload : Mettre en correspondance la politique de contrôle d'accès avec la portée	Dans Manage (Gestion) > Workloads (Charges de travail) > Connectors (Connecteurs) > Segmentation (Segmentation), créez un mappage ACP.
6	Dans Cisco Secure Workload : Créez une règle d'application de correctifs virtuels.	Dans Manage (Gestion) > Workloads (Charges de travail) > Connectors (Connecteurs) > Virtual Patching (Correctifs virtuels) , créez une règle de correctifs virtuels. Les charges de travail avec des CVE publiées sont affichées.
7	Dans Cisco Secure Workload : Appliquez les politiques sur les espaces de travail souhaités.	Dans le ou les espaces de travail, cliquez sur l'onglet **Enforcement** (Application), puis sur le bouton **Enforce Policies** (Appliquer les politiques) et suivez les instructions de l'assistant.
8	Attendez que les nouvelles règles apparaissent dans la ou les politiques de contrôle d'accès.	Cette opération est plus ou moins longue, en fonction de la quantité de données à transférer, de la vitesse des machines, de la bande passante du réseau, etc. Pour afficher les règles : Dans votre FMC, choisissez **Policies** (Politiques) > **Access Control** (Contrôle d'accès) et cliquez sur la politique à afficher.
9	Les nouvelles politiques de contrôle d'accès sont automatiquement déployées sur les périphériques gérés Cisco Secure Firewall Threat Defense associés.	Les modifications futures sont également déployées automatiquement sur les périphériques Cisco Secure Firewall Threat Defense. Si vous associez de nouveaux FTD à une politique de contrôle d'accès existante, ces derniers recevront automatiquement les règles actuelles.

Configurer le connecteur FMC en version 3.8.1.1

Avant de commencer

Suivez les étapes décrites jusqu'à présent dans la section Mise en œuvre de cette intégration pour Cisco Secure Workload version 3.8.1.1.

Paramètres

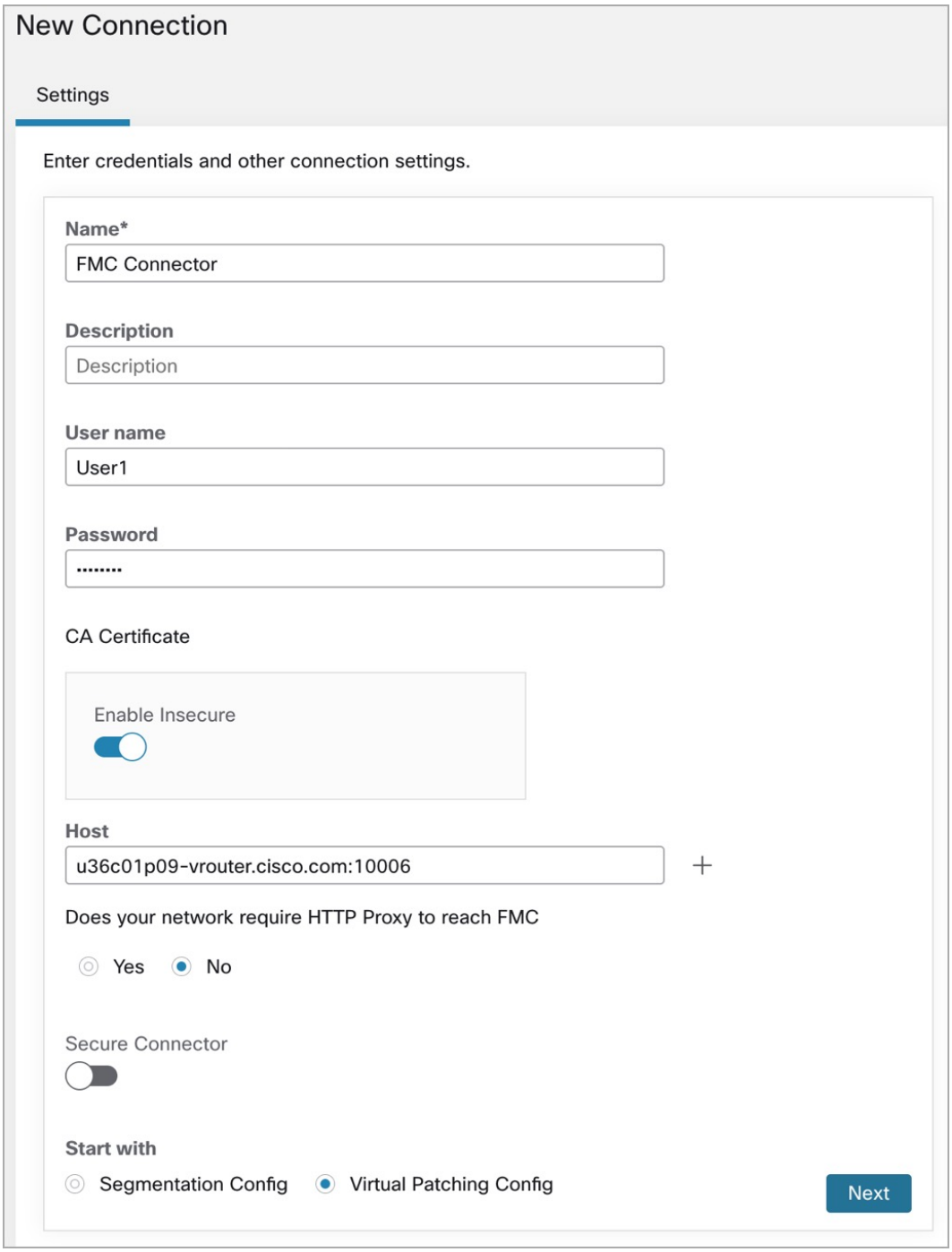
Créez le connecteur FMC dans Cisco Secure Workload pour établir la communication avec Cisco Secure Firewall Management Center.

1. Accédez à **Manage** (Gestion) > **Workloads** (Charges de travail) > **Connectors** (Connecteurs).
2. Sous **Firewall (Pare-feu)**, cliquez sur **Cisco Secure Firewall**.
3. Cliquez sur **Configure your new connector here** (Configurer votre nouveau connecteur ici).
4. Sur la page **New Connection** (Nouvelle connexion), saisissez les renseignements d'authentification et les autres paramètres de connexion comme suit :

Champs	Description
Nom	Attribuez un nom unique au connecteur FMC.
Description	Saisissez une description
Nom d'utilisateur et mot de passe	Saisissez les renseignements d'authentification utilisés pour communiquer avec le FMC.
Certificat de l'autorité de certification	Saisissez le certificat de l'autorité de certification utilisé par Cisco Secure Workload pour authentifier cet appareil FMC. Vous pouvez également cocher **Enable Insecure** (Activer l'option non sécurisée) lorsque le réseau est sécurisé et que Cisco Secure Workload ne valide pas le certificat. Vous pouvez obtenir le certificat d'autorité de certification auprès du FMC en utilisant le flux de travail de gestion des objets.
Hébergement	Saisissez le nom d'hôte et le numéro de port du FMC associé. Le format est <nom de domaine complet> : <Port> ou <IP> : <Port> Le nom d'hôte doit être un nom de domaine complet ou une adresse IP de FMC.
Votre réseau nécessite-t-il un serveur mandataire (serveur mandataire) HTTP pour atteindre FMC?	Saisissez l'URL du serveur mandataire au format <hôte du serveur mandataire> :<port du serveur mandataire>
Connecteur sécurisé	Activez l'option si un connecteur sécurisé est utilisé pour tunneliser les connexions entre Cisco Secure Workload et FMC. Avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé.

Champs	Description
Effectuez les opérations suivantes au préalable :	Choisissez la **configuration de segmentation** ou la **configuration d'application de correctifs virtuels**. a) **Configuration de la segmentation** : affectez des politiques de contrôle d'accès aux portées et configurez des paramètres supplémentaires. b) **Configuration d'application de correctifs virtuels** : configurez les règles sur les CVE à publier sur FMC.

5. Cliquez sur **Next** (suivant).



Segmentation

Les politiques de segmentation appliquées par Cisco Secure Workload sont converties en politiques de contrôle d'accès en fonction des ensembles d'adresses IP des portées, des filtres d'inventaire et des grappes convertis en objets dynamiques dans Cisco Secure Firewall Management Center.

Les politiques de segmentation converties de Cisco Secure Workload sont ajoutées au Cisco Secure Firewall Management Center en tant que règles dans les sections respectives de la politique de contrôle d'accès. Les politiques absolues sont ajoutées dans la section de règles obligatoires et les politiques par défaut sont ajoutées dans la section de règles par défaut.

Les types de règles de contrôle d'accès suivants sont ajoutés :

- Règles avec préfixe : *Workload_ golden_* :

  Ces règles, appelées règles d'or, veillent à ce que Cisco Secure Workload puisse communiquer avec tous les agents Cisco Secure Workload installés sur les charges de travail derrière les pare-feux sécurisés.

- Règles avec préfixe : *Workload_* :

  Il s'agit des règles converties à partir des politiques de segmentation dans les espaces de travail applicatifs pour lesquelles l'application de la règle est activée.

- Règles avec préfixe : *Workload_ca_* :

  Il s'agit des règles collectrices converties pour chaque espace de travail de l'application mise en œuvre. À partir de la version de Cisco Secure Workload, vous ne pouvez utiliser les règles collectrices de Cisco Secure Workload que si vous avez sélectionné l'option Use Secure Workload Catch-All (Utiliser les règles collectrices de Cisco Secure Workload) lors de la configuration du connecteur FMC.

- Les objets dynamiques sont créés avec le préfixe : *WorkloadObj_*

Remarque

- Si vous supprimez ou modifiez ces règles dans FMC, vos modifications seront remplacées la prochaine fois que Cisco Secure Workload enverra des mises à jour sur FMC.
- Si vous créez des règles de contrôle d'accès supplémentaires dans FMC indépendamment de cette intégration et que vous configurez l'intégration pour qu'elle fusionne les règles existantes au lieu de les remplacer, cette intégration ne modifie pas vos règles indépendantes, tant qu'elles ne sont pas nommées à l'aide de l'un des préfixes décrits ci-dessus.

Créer un mappage de la politique de contrôle d'accès

1. Si **Segmentation Config** (configuration de segmentation) est sélectionnée dans les paramètres, vous êtes redirigé vers la fenêtre **Create ACP Mapping** (Créer un mappage de la politique de contrôle d'accès).
2. Choisissez une **politique d'accès** dans la liste déroulante et associez-la à une **portée**. Une politique d'accès ne peut être mappée qu'à une seule portée.
3. Cochez la case **Use Secure Workload Catch All** (Utiliser les règles collectrices de Cisco Secure Workload) pour activer les règles collectrices de Cisco Secure Workload. Les règles collectrices de Cisco Secure Workload sont répertoriées après toutes les autres règles (les règles Cisco Secure Workload et les règles créées directement dans FMC, le cas échéant) dans la section par défaut des politiques de contrôle d'accès. Si vous décidez de désactiver les règles collectrices de Cisco Secure Workload, décochez cette option pour utiliser l'action par défaut de la politique de contrôle d'accès de FMC.
4. Sélectionnez une option de **Enforcement Mode** (Mode d'application).
   - **Fusionner** : les règles de politique Cisco Secure Workload sont ajoutées en même temps que les règles existantes créées par les utilisateurs. Vous pouvez configurer la priorité comme expliqué à l'étape suivante.

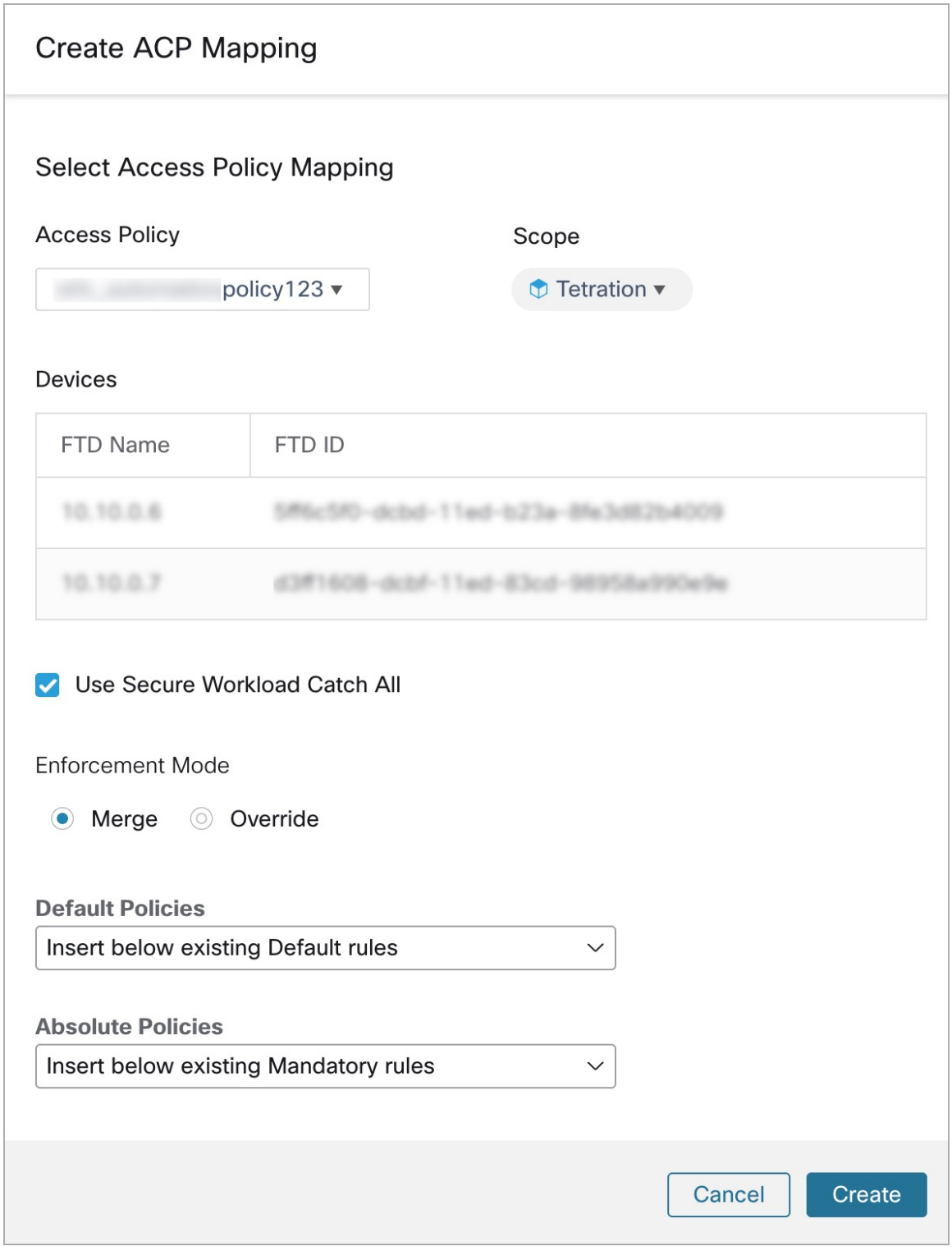
- **Remplacer** : les règles existantes créées par les utilisateurs sont remplacées par les règles de politique Cisco Secure Workload.

Remarque Les options du menu déroulant de priorité ne sont disponibles que lorsque **Merge** (Fusionner) est sélectionné comme mode d'application.

5. Dans les menus déroulants des politiques **absolue** et **par défaut**, choisissez l'option requise pour définir la priorité des politiques Cisco Secure Workload comme étant supérieure ou inférieure aux règles préexistantes dans la section respective de la politique de contrôle d'accès dans FMC.
   - Si vous choisissez l'option Insert above existing Mandatory rules (Insérer au-dessus des règles obligatoires existantes), les politiques Cisco Secure Workload ont une priorité plus élevée que les règles obligatoires.
   - Si vous choisissez l'option Insert below existing Mandatory rules (Insérer sous les règles obligatoires existantes), les politiques Cisco Secure Workload ont une priorité inférieure aux règles obligatoires.

   Par exemple, dans le menu déroulant **Absolute Policies** (Politiques absolues), si vous choisissez Insérer au-dessus des règles obligatoires existantes, les règles Cisco Secure Workload sont configurées au début de la section Obligatoire, suivies de toutes les règles de contrôle d'accès préexistantes dans Cisco Secure Firewall Management Center. Lorsqu'une nouvelle règle est créée, l'ordre des règles de la politique de contrôle d'accès est mis à jour en fonction de la priorité sélectionnée pour les politiques dans Cisco Secure Workload.

Illustration 8 : Créer un mappage de la politique de contrôle d'accès



6. Cliquez sur **Create** (créer).

Modifier le mappage de la politique de contrôle d'accès

1. Dans l'onglet Segmentation, cliquez sur **Edit** (Modifier).
2. Sous **Action** (Action), cliquez sur l'icône de modification.
3. Apportez les modifications nécessaires et cliquez sur **Save** (enregistrer).
4. Cliquez sur l'icône **+** pour mapper une autre politique de contrôle d'accès à une portée.
5. Cliquez sur **Save** (Enregistrer) pour enregistrer toutes les modifications.

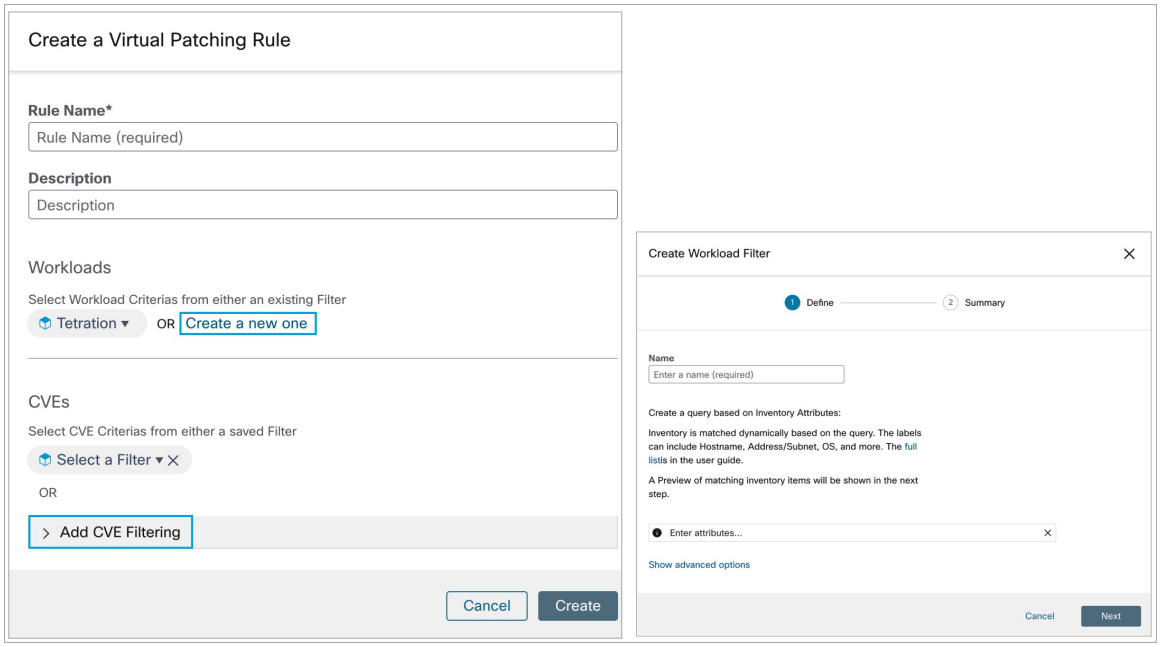
Application de correctifs virtuels

Les correctifs virtuels, également appelés correctifs externes et correctifs juste à temps, sont une technique de sécurité utilisée pour protéger les applications et les systèmes informatiques contre les vulnérabilités connues. L'application de correctifs virtuels, utilisée à l'origine par le système de prévention des intrusions (IPS), met en œuvre des correctifs temporaires ou des solutions de contournement pour corriger les vulnérabilités jusqu'à ce qu'un correctif permanent puisse être développé et appliqué.

Par exemple, les entreprises qui respectent le cycle de vie de développement logiciel prennent le temps de détecter, de corriger et de développer une nouvelle version de l'application. Le système peut être protégé par l'installation d'un pare-feu et l'ajout de règles IPS jusqu'à ce que la nouvelle version de l'application soit déployée. Cisco Secure Workload publie les CVE sur le pare-feu pour qu'ils soient pris en compte lors de la création des politiques IPS.

1. Si le paramètre **Virtual Patching Config** (Configuration d'application de correctifs virtuels) est sélectionné, vous serez redirigé vers la fenêtre **Create a Virtual Patching Rule** (créer une règle d'application de correctifs virtuels).
2. Saisissez un **Rule Name**) (Nom de règle) et une **Description** (Description).
3. Vous pouvez choisir un filtre de charge de travail existant ou en créer un nouveau.
4. Vous pouvez choisir un filtre CVE existant ou ajouter un filtre CVE en saisissant une requête CVE.
5. Cliquez sur **Create** (créer).
6. Sous l'onglet **Virtual Patching** (Correctif virtuel), sous **Rules** (Règes), cliquez sur **Add Rule** (ajouter une règle) pour ajouter une ou plusieurs règles.

Figure 9: Créer une règle d'application de correctif virtuel



7. Les règles d'application de correctifs virtuels ajoutées sont affichées sous Rules (Règles).
   - Vous pouvez rechercher par **Rule Name** (Nom de règle) et par **Description** (Description).
   - Cliquez sur l'icône de **filtre** pour choisir les colonnes à afficher.
   - Sous **Actions**, cliquez sur l'icône de **modification** pour modifier les détails d'une règle d'application de correctifs virtuels.
   - Sous **Actions**, cliquez sur l'icône de la **corbeille** pour supprimer une règle d'application de correctifs virtuels.

8. Les charges de travail avec des CVE publiées sont affichées sur la droite.
   - Vous pouvez filtrer les données en saisissant des attributs tels que le Nom de la règle, le Filtre d'inventaire, la Charge de travail et le Pire score.
   - Cliquez sur l'icône de menu pour téléverser les détails au format JSON et/ou CSV.
   - Cliquez sur les en-têtes de colonne pour trier les entrées.
   - Dans la colonne **Exported** (exporté), cliquez sur **CVEs List** (Liste des CVE) pour afficher une liste de tous les CVE publiés d'une charge de travail.
   - Cliquez sur le menu contextuel pour afficher le **journal d'audit**. Les journaux des 48 dernières heures sont stockés et affichés.

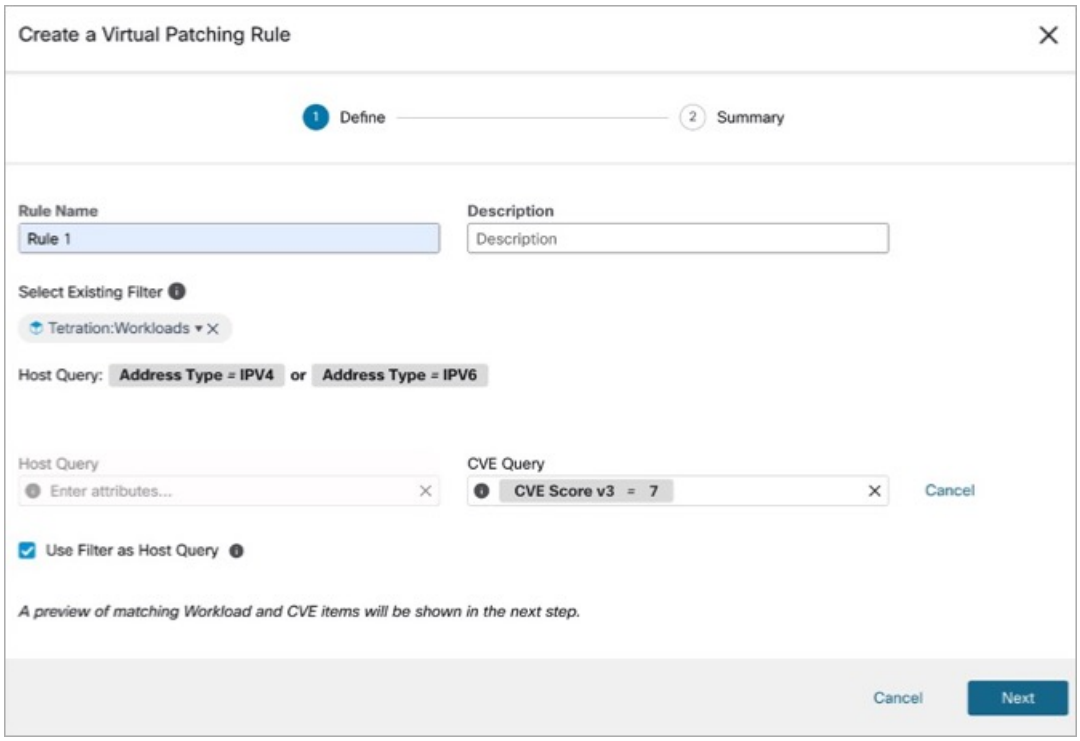
Application de correctifs virtuels dans la version 3.8.1.36

1. Dans la fenêtre **Create a Virtual Correctif Rule** (créer une règle d'application de correctifs virtuels), saisissez un **Rule Name** (Nom de règle) et une **Description** (description) pour la règle.

2. Sélectionnez un filtre existant dans la liste déroulante. Vous pouvez sélectionner une portée ou sous-portée existante pour sélectionner les hôtes à prendre en compte pour l'application de correctifs virtuels.

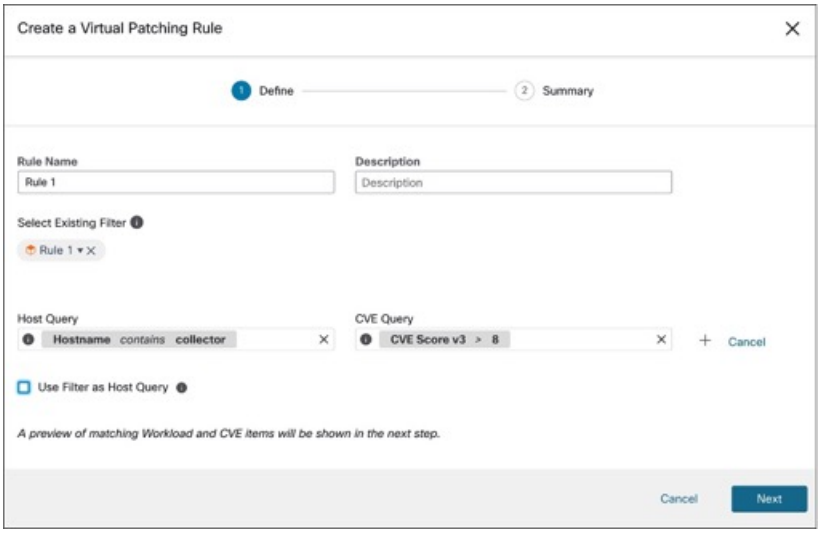
   - Par défaut, la case **Use Filter as Host Query** (utiliser le filtre comme requête d'hôte) est cochée. Vous pouvez continuer en saisissant simplement la requête CVE; sans créer de nouveau filtre d'application de correctifs virtuels. La requête de l'hôte comprend le contenu du filtre choisi.

     Figure 10: Sans créer de nouveau filtre d'application de correctifs virtuel



   - Décochez la case **Use Filter as Host Query** (Utiliser le filtre comme requête hôte) pour saisir à la fois la requête hôte et la requête CVE. Cela crée un nouveau filtre d'application de correctifs virtuels.

Figure 11: Créer un nouveau filtre d'application de correctif virtuel



3. Saisissez une requête d'hôte et de CVE. Cliquez sur l'icône + pour ajouter d'autres requêtes.

Note

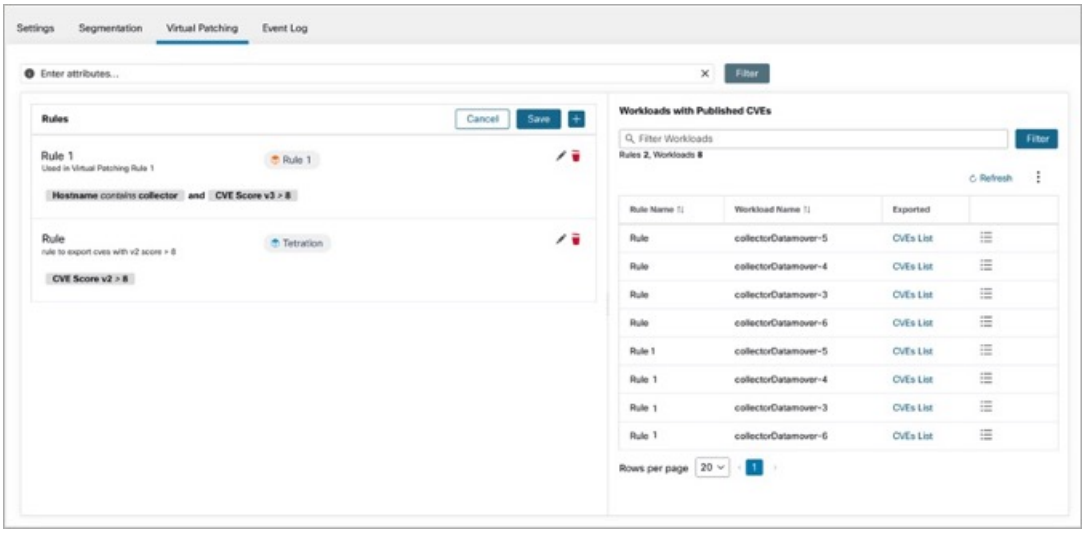
- Passez le curseur sur l'icône d'**information** pour afficher les formats de requête pris en charge.
- Par défaut, un filtre d'application de correctifs virtuels est créé en fonction de la combinaison de requêtes saisie.

4. Cliquez sur **Next** (suivant). Dans la fenêtre **Summary** (résumé), les listes des charges de travail et des CVE correspondants sont affichées. Les charges de travail et les CVE sont mises en correspondance de manière dynamique en fonction de la requête.
5. Cliquez sur **Create** (créer).
6. Les règles d'application de correctifs virtuels ajoutées sont affichées sous **Rules** (Règles). Saisissez les attributs et cliquez sur **Filter** (filtrer) pour affiner les résultats de la recherche.
7. Les charges de travail avec des CVE publiées sont affichées sur la droite.
   - Saisissez les attributs et cliquez sur **Filter** (filtrer) pour affiner les résultats de la recherche.
   - Cliquez sur les en-têtes de colonne pour trier les entrées.
   - Dans la colonne **Exported** (exporté), cliquez sur **CVEs List** (Liste des CVE) pour afficher une liste de tous les CVE publiés d'une charge de travail.
   - Cliquez sur le menu contextuel pour afficher le **journal d'audit** d'une charge de travail. Les journaux des 48 dernières heures sont stockés et affichés.

Modifier une règle d'application de correctifs virtuels

1. Cliquez sur **Edit** (modifier) pour ajouter d'autres règles, modifier les renseignements détaillés et/ou supprimer une règle.

Figure 12: Modifier une règle d'application de correctifs virtuels



- Cliquez sur l'icône + pour ajouter d'autres règles. Cliquez sur **Save** (enregistrer).
- Cliquez sur l'icône de la **corbeille** pour supprimer une règle.

2. Cliquez sur **l'icône** en forme de **crayon** pour modifier les détails d'une règle.
3. Dans la fenêtre **Edit Virtual Correctif Rule** (modifier la règle d'application de correctifs virtuels), modifiez la requête d'hôte et la requête CVE au besoin, puis enregistrez les modifications.

Journal des événements

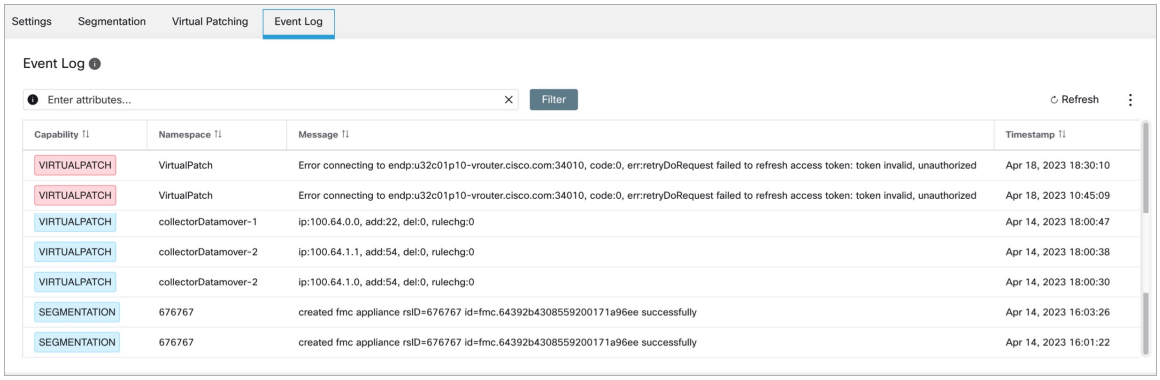
L'onglet **Event Log** (Journal des événements) répertorie les événements ou les transactions importants entre Cisco Secure Workload et Cisco Secure Firewall Management Center.

1. Saisissez les attributs pour filtrer les événements en fonction de la capacité, du niveau de l'événement, de l'espace de noms et du message.

Remarque Les codes de couleur pour le niveau de l'événement sont Information (bleu), Avertissement (orange) et Erreur (rouge).

2. Cliquez sur les en-têtes de colonne pour trier les entrées.
3. Cliquez sur l'icône du menu en trois points pour télécharger les détails au format JSON et/ou CSV.
4. Cliquez sur **Refresh** (Actualiser) pour réinitialiser tous les filtres.

Illustration 13 : Journal des événements



Mise en œuvre de cette intégration pour Cisco Secure Workload, version 3.7.1.5

Cette section s'applique à toutes les versions 3.7.

À propos des mises à niveau

Mises à niveau vers Cisco Secure Workload, version 3.7.1.5

- Mises à niveau à partir de la version 3.6.1.36 :

  Vos configurations préalables à la mise à niveau ne changent pas.

- Mises à niveau à partir des versions 3.6.x antérieures à la 3.6.1.36 :

  Si les domaines sont configurés dans votre Cisco Firepower Management Center et que l'application a été activée dans l'orchestrateur :

  Par défaut, tous les domaines sont sélectionnés pour application.

Après la mise à niveau vers la version 3.7.1.5, vous pouvez effectuer les opérations suivantes :

- Définissez la priorité des politiques de segmentation à répertorier dans les sections Obligatoire ou Par défaut de la politique de contrôle d'accès.
- Pour activer ou désactiver l'option d'utilisation des règles collectrices de Cisco Secure Workload cochez ou décochez l'option **Use Secure Workload Catch All** (Utiliser les règles collectrices de Cisco Secure Workload) lors de la configuration de l'orchestrateur externe FMC.

Conditions préalables à l'intégration : Cisco Secure Workload, version 3.7.1.5

- Vous avez configuré un Cisco Secure Firewall Management Center (FMC) et au moins un périphérique Cisco Secure Firewall Threat Defense (FTD) pris en charge. Vous avez associé les périphériques FTD au FMC, affecté chaque FTD à une politique de contrôle d'accès et vérifié que les politiques peuvent être déployées du FMC sur les FTD et que le système traite le trafic réseau comme prévu.

Pour obtenir des renseignements complets, consultez la documentation de Cisco Secure Firewall Management Center pour vos produits, y compris les feuilles de route relatives à la documentation de Cisco Secure Firewall Management Center.

- Votre appareil Cisco Secure Workload (sur site) ou votre compte (SaaS) est configuré et fonctionne comme prévu.
- Si vous utilisez un logiciel-service (SaaS) Cisco Secure Workload, ou si un Cisco Secure Workload local ne peut pas atteindre directement l'appareil FMC, configurez un tunnel de connecteur sécurisé pour assurer la connectivité entre les composants de la solution.

  Par défaut, Cisco Secure Workload communique avec l'API REST FMC à l'aide de HTTPS sur le port 443.

  Pour obtenir des instructions sur la configuration du connecteur sécurisé, consultez le guide de l'utilisateur Cisco Secure Workload, disponible dans l'aide en ligne de l'interface Web Cisco Secure Workload.

Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.7.1.5

Le tableau suivant présente le flux de travail de bout en bout pour configurer Cisco Secure Firewall Management Center et configurer l'intégration avec Cisco Secure Workload version 3.7.1.5.

Étape	Description	Autres renseignements
Avant de commencer	Découvrez comment fonctionne cette intégration, le processus de haut niveau pour sa mise en œuvre et toutes les considérations relatives au déploiement.	Consultez toutes les sections et tous les sujets sous Renseignements importants pour Cisco Secure Workload, versions 3.7 et 3.6, à la page 5.
Avant de commencer	Répondre aux exigences et aux conditions préalables	Consultez toutes les sections de Déploiements pris en charge, à la page 12 et Conditions préalables à l'intégration : Cisco Secure Workload, version 3.7.1.5, à la page 37.
1	Dans Cisco Secure Workload : Définissez les portées, les filtres d'inventaire, les grappes, les espaces de travail et les politiques de segmentation pour votre environnement.	Créez manuellement les politiques de segmentation que vous souhaitez appliquer à l'ensemble de charges de travail qui seront définies par des objets dynamiques dans Cisco Secure Firewall. Si vous avez des questions à ce sujet, consultez la section sur la segmentation du guide de l'utilisateur Cisco Secure Workload, disponible comme aide en ligne à partir de votre interface Web Cisco Secure Workload. Vous pouvez également consulter Avancé : Utiliser ADM pour générer des politiques de segmentation , à la page 54.

Étape	Description	Autres renseignements
2	Dans FMC : Définissez l' **action par défaut** de la politique au bas de chaque politique de contrôle d'accès affectée à une protection contre les menaces Cisco Secure Firewall Threat Defense.	Cette action dépend des politiques de segmentation que vous créez. Par exemple, si vous souhaitez bloquer tout le trafic qui n'est pas explicitement autorisé par les politiques de segmentation, sélectionnez **Block all traffic** (Bloquer tout le trafic).
3	Dans FMC : Créez un compte d'utilisateur dédié à cette intégration.	Exigences pour ce compte d'utilisateur : • Le compte doit avoir le rôle Administrateur. • (Si des domaines sont configurés sur le FMC) Le compte doit avoir accès au domaine Global. Si vous avez des questions sur la création de comptes utilisateur dans FMC, consultez la rubrique « Ajouter un utilisateur interne » dans l'aide en ligne de Cisco Secure Firewall Management Center.
4	Dans Cisco Secure Workload : Créer un orchestrateur FMC.	Créez un seul orchestrateur FMC par Cisco Secure Firewall Management Center. Pour créer un orchestrateur FMC à l'aide d'OpenAPI, consultez la section Configurer l'orchestrateur FMC dans la version 3.7.1.5, à la page 40 du guide de l'utilisateur sur votre portail Web Cisco Secure Workload.
5	Dans Cisco Secure Workload : Appliquez les politiques sur les espaces de travail souhaités. (Cette action est distincte de l'activation de l'application dans l'orchestrateur FMC).	Dans le ou les espaces de travail, cliquez sur l'onglet **Enforcement** (Application), puis sur le bouton **Enforce Policies** (Appliquer les politiques) et suivez les instructions de l'assistant.
6	Activez l'application de l'orchestrateur : Si vous n'avez pas encore sélectionné de domaines dans l'orchestrateur FMC, faites-le maintenant.	Modifiez l'orchestrateur FMC pour sélectionner des domaines. (Si aucun domaine n'est configuré sur votre FMC, vous devrez sélectionner le domaine **Global**). Lorsque vous cliquez sur **Update** (Mettre à jour) après avoir sélectionné des domaines, cela active l'application de l'orchestrateur et déploie vos politiques Cisco Secure Workload sur vos périphériques FTD gérés. Pour de plus amples renseignements, consultez la section Modification d'un orchestrateur FMC dans la version 3.7.1.5, à la page 44.

Étape	Description	Autres renseignements
7	Attendez que les nouvelles règles apparaissent dans la ou les politiques de contrôle d'accès.	Cette opération est plus ou moins longue, en fonction de la quantité de données à transférer, de la vitesse des machines, de la bande passante du réseau, etc. Pour afficher les règles : Dans votre FMC, choisissez **Policies** (Politiques) > **Access Control** (Contrôle d'accès) et cliquez sur la politique à afficher.
8	Les nouvelles politiques de contrôle d'accès sont automatiquement déployées sur les périphériques gérés Cisco Secure Firewall Threat Defense associés.	Les modifications futures sont également déployées automatiquement sur les périphériques Cisco Secure Firewall Threat Defense. Si vous associez de nouveaux FTD à une politique de contrôle d'accès existante, ces derniers recevront automatiquement les règles actuelles.

Configurer l'orchestrateur FMC dans la version 3.7.1.5

Avant de commencer

Suivez les étapes décrites jusqu'à présent dans le tableau de Mise en œuvre de cette intégration pour Cisco Secure Workload, version 3.7.1.5, à la page 37.

Procédure

Étape 1 Dans l'interface Web Cisco Secure Workload, sélectionnez **Manage > External Orchestrators**(Gestion > Orchestrateurs externes).

Étape 2 Cliquez sur **Create New Configuration** (Créer une nouvelle configuration)

Étape 3 Sous l'onglet **Basic Config** (configuration de base), configurez les champs suivants :

Option	Description
Type	Sélectionnez **FMC**.
Nom	Attribuez un nom unique à l'orchestrateur FMC.
Description	Saisissez une description pour l'orchestrateur.

Option	Description
Intervalles complets de l'instantané	Saisissez l'intervalle complet de l'instantané, en secondes. Le champ **Full Snapshot Interval(s)** (Intervalles complets de l'instantané) spécifie la fréquence à laquelle l'orchestrateur externe du FMC teste la connectivité FMC sur Cisco Secure Workload. Si une erreur se produit (par exemple, si le FMC n'est pas accessible en raison de problèmes de réseau ou si des informations d'authentification d'utilisateur ou de point terminal non valides ont été utilisées), l'orchestrateur FMC signale l'erreur dans le champ **Status** (État). Valeur par défaut : `3 600 secondes`
Nom d'utilisateur **Mot de passe**	Saisissez le nom d'utilisateur et le mot de passe de l'utilisateur dédié que vous avez créé dans FMC, comme indiqué précédemment dans ce document. Ces renseignements d'authentification sont utilisés pour communiquer avec le FMC.
Certificat de l'autorité de certification	Saisissez le certificat de l'autorité de certification que Cisco Secure Workload utilisera pour authentifier ce FMC. Vous pouvez obtenir ce certificat auprès de FMC en utilisant le flux de travail de gestion d'objets. Pour en savoir plus, consultez les rubriques sur les objets de l'autorité de certification interne dans le chapitre Objets réutilisables du *Guide de configuration de Cisco Firepower Management Center* pour votre version de Firepower.
Accept Self-signed Cert (Accepter le certificat autosigné)	Cochez cette case pour configurer l'orchestrateur FMC de façon à ce qu'il fasse confiance à un certificat autosigné.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Si vous utilisez Cisco Secure Workload SaaS, vous devez activer cette option. Si vous utilisez un appareil Cisco Secure Workload sur site, vous devrez peut-être activer cette option. Avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé, comme décrit dans Conditions préalables à l'intégration : Cisco Secure Workload, version 3.7.1.5, à la page 37.
Utiliser l'outil Catch All (règles collectrices) de Cisco Secure Workload	Cochez cette case pour activer les règles collectrices de Cisco Secure Workload. Les règles collectrices de Cisco Secure Workload sont répertoriées après toutes les autres règles (les règles Cisco Secure Workload et les règles créées directement dans FMC, le cas échéant) dans la section par défaut des politiques de contrôle d'accès. Si vous décidez de désactiver les règles collectrices de Cisco Secure Workload, décochez cette option pour utiliser l'action par défaut de la politique de contrôle d'accès de FMC.

Option		Description
Mode de mise en application	**Fusionner/Remplacer**	Sélectionnez **Merge** (Fusionner) ou **Override** (Remplacer) dans la liste déroulante. • Si vous sélectionnez **Override**(Remplacer), les politiques Cisco Secure Workload appliquées remplacent toutes les règles de contrôle d'accès FMC existantes. **Important** Si vous sélectionnez cette option, toutes les règles existantes de toutes les politiques de contrôle d'accès associées à un périphérique FTD (Firewall Threat Defense) (dans les domaines que vous sélectionnez, le cas échéant) seront supprimées et irrécupérables. • Si vous souhaitez conserver des règles, nous vous recommandons de les exporter avant de poursuivre cette intégration ou d'utiliser l'option **Fusionner** (décrite à la ligne suivante). **Remarque** Si **Enforcement Mode** (Mode d'application) est défini sur **Merge** (Fusionner) : • Nous vous recommandons de ne pas utiliser le préfixe `Workload_` pour les règles que vous saisissez manuellement dans FMC, car elles seront automatiquement supprimées. • Évitez d'effectuer simultanément le déploiement FTD à l'aide de l'interface utilisateur de FMC et l'application des politiques à l'aide de Cisco Secure Workload. Ces opérations asynchrones et de longue durée (environ 2 minutes) sont en concurrence les unes avec les autres et peuvent entraîner l'échec du déploiement FTD. Si le déploiement FTD échoue en raison d'applications de politiques concurrentes, vous devez le recommencer.
	Priorité de politique absolue ou par défaut	

Option		Description
		Les options du menu déroulant de priorité ne sont disponibles que lorsque **Merge** (Fusionner) est sélectionné comme mode d'application. Dans les menus déroulants des politiques absolue ou par défaut, sélectionner l'option requise pour afficher les politiques Cisco Secure Workload au-dessus ou en dessous des règles préexistantes dans la section respective de la politique de contrôle d'accès dans FMC. Par exemple, dans le menu déroulant **Absolute Policies** (Politiques absolues), si vous choisissez **Insérer au-dessus des règles obligatoires existantes**, les règles Cisco Secure Workload sont configurées au début de la section **Obligatoire**, suivies de toutes les règles de contrôle d'accès préexistantes dans Cisco Secure Firewall Management Center. Lorsqu'une nouvelle règle est créée, l'ordre des règles de la politique de contrôle d'accès est mis à jour en fonction de la priorité sélectionnée pour les politiques dans Cisco Secure Workload.

Étape 4 Cliquez sur le lien **Host Lists** (Listes d'hôtes) à gauche.

Étape 5 Saisissez le nom d'hôte et le numéro de port du FMC associé.

Le `host name` (nom d'hôte) doit être un nom de domaine complet pour FMC ou une adresse IP.

Le `port number` (numéro de port) par défaut est 443.

Si votre FMC est déployé dans une configuration prise en charge en haute disponibilité, saisissez également le nom d'hôte et le port du FMC de secours/secondaire.

Étape 6 Cliquez sur **Create** (créer).

Il se peut que vous voyiez brièvement une bannière verte pour indiquer que Cisco Secure Workload s'est connecté avec succès à Cisco Secure Firewall Management Center.

Une fois la connexion établie, Cisco Secure Workload récupère tous les domaines configurés sur votre Cisco Secure Firewall Management Center. Cette opération peut prendre quelques minutes.

(Si aucun domaine n'est configuré, Cisco Secure Workload récupère le domaine **Global** (Global).)

Une fois que les domaines ont été récupérés avec succès, vous verrez l'option de sélection des domaines s'afficher.

Étape 7 Si vous ne souhaitez pas déployer de politiques sur vos périphériques gérés Cisco Secure Firewall Threat Defense maintenant :

Lorsque l'option de sélection de domaines s'affiche, cliquez sur **Cancel** (Annuler).

Lorsque vous êtes prêt à déployer des politiques, revenez à la page **External Orchestrators** (Orchestrateurs externes), modifiez cet orchestrateur, cliquez sur **Domains** (Domaines) et sélectionnez les domaines comme décrit à l'étape suivante.

Étape 8 Sélectionnez le ou les domaines sur lesquels vous souhaitez appliquer les politiques de segmentation.

Si aucun domaine n'est configuré pour votre déploiement de Cisco Secure Firewall, sélectionnez le domaine **Global** (global).

Étape 9 Cliquez sur **Update** (mettre à jour).

Les politiques de segmentation sont appliquées aux politiques de contrôle d'accès dans les domaines que vous avez sélectionnés, et les modifications sont déployées sur les périphériques Cisco Secure Firewall Threat Defense associés.

Le temps nécessaire pour transférer les règles est généralement de quelques minutes, mais dépend du nombre de règles de politique et de la configuration des ressources des périphériques Cisco Secure Firewall Management Center et Cisco Secure Firewall Threat Defense.

Prochaine étape

Revenez au tableau de présentation des procédures dans Mise en œuvre de cette intégration pour Cisco Secure Workload, version 3.7.1.5, à la page 37 et passez aux étapes restantes.

Modification d'un orchestrateur FMC dans la version 3.7.1.5

- Vous pouvez créer l'orchestrateur FMC sans préciser les domaines sur lesquels appliquer la politique, puis modifier la configuration de l'orchestrateur ultérieurement pour préciser les domaines d'application.

  L'application se produit lorsque vous cliquez sur **Update** (Mettre à jour) après avoir sélectionné les domaines.

- Si vous modifiez un orchestrateur externe FMC, vous devez saisir à nouveau le mot de passe du compte FMC.

- Si vous modifiez un orchestrateur FMC pour lequel des domaines sont sélectionnés, Cisco Secure Workload récupère les domaines.

  Les domaines que vous avez déjà sélectionnés restent sélectionnés.

- Si vous modifiez un orchestrateur, il est possible que la page des orchestrateurs externes affiche initialement l'état de la connexion comme **Failure** (Échec) pendant que la connexion et la synchronisation se produisent, mais devient **Succeed** (Réussite) après quelques instants. Vous pouvez ensuite modifier les domaines.

Mise en œuvre de cette intégration pour Cisco Secure Workload, version 3.6

Cette section s'applique à toutes les versions 3.6.x. Les informations propres à la version sont étiquetées comme telles.

À propos des mises à niveau

Mises à niveau vers la version 3.6.1.36

Si des domaines sont configurés dans votre centre de gestion Cisco Firepower Management Center (FMC) et que leur application a été activée dans l'orchestrateur FMC avant la mise à niveau vers la version 3.6.1.36 :

Par défaut, tous les domaines sont sélectionnés pour application.

Mises à niveau dans la version 3.5 vers la version 3.6.1.5

Si vous avez configuré l'intégration FMC dans la version 3.5 et que vous souhaitez mettre à niveau vers la version 3.6.1.5, consultez les renseignements importants dans le *Guide de mise à niveau de Cisco Secure Workload*. Vous n'avez pas besoin d'utiliser la procédure décrite ci-dessous.

Conditions préalables à l'intégration : Cisco Secure Workload version 3.6

- Vous avez configuré un centre de gestion Cisco Firepower Management Center (FMC) et au moins un périphérique Firepower Threat Defense (FTD) pris en charge. Vous avez associé le ou les FTD au FMC, affecté chaque FTD à une politique de contrôle d'accès, vérifié que les politiques peuvent être déployées du FMC vers le ou les FTD et que le système traite le trafic réseau comme prévu.

  Pour obtenir des renseignements complets, consultez la documentation du Cisco Secure Firewall Management Center pour vos produits, y compris la feuille de route de la documentation du Cisco Secure Firewall.

- Votre appareil Cisco Secure Workload (sur site) ou votre compte (SaaS) est configuré et fonctionne comme prévu.

- Si vous utilisez un logiciel-service (SaaS) Cisco Secure Workload, ou si un Cisco Secure Workload local ne peut pas atteindre directement l'appareil FMC, configurez un tunnel de connecteur sécurisé pour assurer la connectivité entre les composants de la solution.

  Par défaut, Cisco Secure Workload communique avec l'API REST FMC à l'aide de HTTPS sur le port 443.

  Pour obtenir des instructions sur la configuration du connecteur sécurisé, consultez le guide de l'utilisateur Cisco Secure Workload, disponible dans l'aide en ligne de l'interface Web Cisco Secure Workload.

Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.6

Le tableau suivant présente le flux de travail de bout en bout pour configurer un Cisco Firepower Management Center (FMC) et configurer l'intégration avec Cisco Secure Workload version 3.6.

Étape	Description	Autres renseignements
Avant de commencer	Découvrez comment fonctionne cette intégration, le processus de haut niveau pour sa mise en œuvre et toutes les considérations relatives au déploiement.	Consultez toutes les sections et tous les sujets sous Renseignements importants pour Cisco Secure Workload, versions 3.7 et 3.6, à la page 5.
Avant de commencer	Répondre aux exigences et aux conditions préalables	Consultez toutes les sections de Déploiements pris en charge, à la page 12 et Conditions préalables à l'intégration : Cisco Secure Workload version 3.6, à la page 45.

Étape	Description	Autres renseignements
1	Dans Cisco Secure Workload : Définissez les portées, les filtres d'inventaire, les grappes, les espaces de travail et les politiques de segmentation pour votre environnement.	Créez manuellement des politiques de segmentation que vous souhaitez appliquer à l'ensemble de charges de travail qui seront définies par des objets dynamiques dans Firepower. Si vous avez des questions à ce sujet, consultez la section sur la segmentation du guide de l'utilisateur Cisco Secure Workload, disponible comme aide en ligne à partir de votre interface Web Cisco Secure Workload. Vous pouvez également consulter Avancé : Utiliser ADM pour générer des politiques de segmentation , à la page 54.
2	Dans FMC : Au bas de chaque politique de contrôle d'accès attribuée à un FTD, définissez l' **action par défaut** pour la politique.	Cette action dépend des politiques de segmentation que vous créez. Par exemple, si vous souhaitez bloquer tout le trafic qui n'est pas explicitement autorisé par les politiques de segmentation, sélectionnez **Block all traffic** (Bloquer tout le trafic).
3	Dans FMC : Créez un compte d'utilisateur dédié à cette intégration.	Exigences pour ce compte d'utilisateur : • Le compte doit avoir le rôle Administrateur. • (Si des domaines sont configurés sur le FMC) Le compte doit avoir accès au domaine Global. Si vous avez des questions sur la création de comptes utilisateur dans FMC, consultez la rubrique « Ajouter un utilisateur interne » de l'aide en ligne du Cisco Firepower Management Center.

Étape	Description	Autres renseignements
4	Dans Cisco Secure Workload : Créer un orchestrateur FMC.	Créez un seul orchestrateur FMC par Cisco Firepower Management Center. • Pour Cisco Secure Workload version 3.6.1.36 : Voir la section Configurer l'orchestrateur FMC dans la version 3.6.1.36, à la page 48. • Pour les versions 3.6.1.5 à 3.6.1.20 de Cisco Secure Workload : Voir Configurer FMC Orchestrator dans Cisco Secure Workload versions 3.6.1.5 à 3.6.1.20, à la page 51, ci-dessous. Pour créer un orchestrateur FMC à l'aide d'OpenAPI, consultez le guide de l'utilisateur disponible dans l'aide en ligne de votre portail Web Cisco Secure Workload. Pour la version 3.6.1.36, ne négligez pas la section sur les domaines.
5	Dans Cisco Secure Workload : Appliquez les politiques sur les espaces de travail souhaités. (Cette action est distincte de l'activation de l'application dans l'orchestrateur FMC).	Dans le ou les espaces de travail, cliquez sur l'onglet **Enforcement** (Application), puis sur le bouton **Enforce Policies** (Appliquer les politiques) et suivez les instructions de l'assistant.
6	Dans Cisco Secure Workload version 3.6.1.36 : Activez l'application de l'orchestrateur : Si vous n'avez pas encore sélectionné de domaines dans l'orchestrateur FMC, faites-le maintenant.	Modifiez l'orchestrateur FMC pour sélectionner des domaines. (Si aucun domaine n'est configuré sur votre FMC, vous devrez sélectionner le domaine **Global**). Lorsque vous cliquez sur **Update** (Mettre à jour) après avoir sélectionné des domaines, cela active l'application de l'orchestrateur et déploie vos politiques Cisco Secure Workload sur vos périphériques FTD gérés. Pour de plus amples renseignements, consultez la section Modification d'un orchestrateur FMC dans la version 3.6.1.36, à la page 55.
	Dans les versions 3.6.1.5 à 3.6.1.20 de Cisco Secure Workload : Si vous n'avez pas encore activé l'application dans l'orchestrateur externe de FMC, faites-le maintenant.	Modifiez l'orchestrateur FMC que vous avez configuré ci-dessus et sélectionnez **Enable Enforcement** (Activer l'application).

Étape	Description	Autres renseignements
7	Attendez que les nouvelles règles apparaissent dans la ou les politiques de contrôle d'accès.	Cette opération est plus ou moins longue, en fonction de la quantité de données à transférer, de la vitesse des machines, de la bande passante du réseau, etc. Pour afficher les règles dans votre Cisco Firepower Management Center : Dans votre FMC, choisissez **Policies** (Politiques) > **Access Control** (Contrôle d'accès) et cliquez sur la politique à afficher.
8	Les nouvelles politiques de contrôle d'accès sont automatiquement déployées sur les FTD gérés associés.	Les modifications futures sont également déployées automatiquement sur les périphériques FTD. Si vous associez de nouveaux FTD à une politique de contrôle d'accès existante, ces derniers recevront automatiquement les règles actuelles.

Configurer l'orchestrateur FMC dans la version 3.6.1.36

Avant de commencer

Suivez les étapes décrites jusqu'à présent dans le tableau de Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.6, à la page 45.

Si vous utilisez une version 3.6 antérieure à la 3.6.1.36, n'utilisez pas cette procédure. Au lieu de cela, consultez Configurer FMC Orchestrator dans Cisco Secure Workload versions 3.6.1.5 à 3.6.1.20, à la page 51.

Procédure

Étape 1 Dans l'interface Web Cisco Secure Workload, sélectionnez **Manage > External Orchestrators**(Gestion > Orchestrateurs externes).

Étape 2 Cliquez sur **Create New Configuration** (Créer une nouvelle configuration)

Étape 3 Sous l'onglet « Basic Configs » (Configurations de base), configurez les champs suivants :

Option	Description
Type	Sélectionnez **FMC**.
Nom	Attribuez un nom unique à l'orchestrateur FMC.
Description	Saisissez une description pour l'orchestrateur.

Option	Description
Intervalles complets de l'instantané	Saisissez l'intervalle complet de l'instantané, en secondes. Le champ **Full Snapshot Interval(s)** (Intervalles complets de l'instantané) spécifie la fréquence à laquelle l'orchestrateur externe du FMC teste la connectivité FMC sur Cisco Secure Workload. Si une erreur se produit (par exemple, si le FMC n'est pas accessible en raison de problèmes de réseau ou si des informations d'authentification d'utilisateur ou de point terminal non valides ont été utilisées), l'orchestrateur FMC signale l'erreur dans le champ **Status** (État). Valeur par défaut : `3 600 secondes`
Nom d'utilisateur **Mot de passe**	Saisissez le nom d'utilisateur et le mot de passe de l'utilisateur dédié que vous avez créé dans FMC, comme indiqué précédemment dans ce document. Ces renseignements d'authentification sont utilisés pour communiquer avec le FMC.
Certificat de l'autorité de certification	Saisissez le certificat de l'autorité de certification que Cisco Secure Workload utilisera pour authentifier ce FMC. Vous pouvez obtenir ce certificat auprès de FMC en utilisant le flux de travail de gestion d'objets. Pour en savoir plus, consultez les rubriques sur les objets de l'autorité de certification interne dans le chapitre Objets réutilisables du *Guide de configuration de Cisco Firepower Management Center* pour votre version de Firepower.
Accept Self-signed Cert (Accepter le certificat autosigné)	Cochez cette case pour configurer l'orchestrateur FMC de façon à ce qu'il fasse confiance à un certificat autosigné.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Si vous utilisez Cisco Secure Workload SaaS, vous devez activer cette option. Si vous utilisez un appareil Cisco Secure Workload sur site, vous devrez peut-être activer cette option. Avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé, comme décrit dans Conditions préalables à l'intégration : Cisco Secure Workload version 3.6, à la page 45.

Option	Description
Mode de mise en application	Sélectionnez **Merge** (Fusionner) ou **Override** (Remplacer) dans la liste déroulante. • Si vous sélectionnez **Override**(Remplacer), les politiques Cisco Secure Workload appliquées remplacent toutes les règles de contrôle d'accès FMC existantes. **Important** Si vous sélectionnez cette option, toutes les règles existantes de toutes les politiques de contrôle d'accès associées à un périphérique FTD (Firewall Threat Defense) (dans les domaines que vous sélectionnez, le cas échéant) seront supprimées et irrécupérables. Si vous souhaitez conserver des règles, nous vous recommandons d'exporter les règles avant de poursuivre cette intégration ou d'utiliser l'option **Merge** (Fusionner) (décrite ci-dessous). • Si vous sélectionnez **Merge** (Fusionner), les règles de Cisco Secure Workload sont ajoutées au début de la liste des règles de contrôle d'accès. **Remarque** Si **Enforcement Mode** (Mode d'application) est défini sur **Merge** (Fusionner) : • Nous vous recommandons de ne pas utiliser le préfixe `Workload_` pour les règles que vous saisissez manuellement dans FMC, car elles seront automatiquement supprimées. • Évitez d'effectuer simultanément le déploiement FTD à l'aide de l'interface utilisateur de FMC et l'application des politiques à l'aide de Cisco Secure Workload. Ces opérations asynchrones et de longue durée (environ 2 minutes) sont en concurrence les unes avec les autres et peuvent entraîner l'échec du déploiement FTD. Si le déploiement FTD échoue en raison d'applications de politiques concurrentes, vous devez le recommencer.

Étape 4 Cliquez sur le lien **Host Lists** (Listes d'hôtes) à gauche.

Étape 5 Saisissez le nom d'hôte et le numéro de port du FMC associé.

Le `host name` (nom d'hôte) doit être un nom de domaine complet pour FMC ou une adresse IP.

Le `port number` (numéro de port) par défaut est 443.

Si votre FMC est déployé dans une configuration prise en charge en haute disponibilité, saisissez également le nom d'hôte et le port du FMC de secours/secondaire.

Étape 6 Cliquez sur **Create** (créer).

Vous pourriez voir s'afficher brièvement une bannière verte pour indiquer que Cisco Secure Workload s'est connecté avec succès à votre Cisco Firepower Management Center.

Une fois la connexion établie, Cisco Secure Workload récupère les domaines configurés sur votre Cisco Firepower Management Center. Cette opération peut prendre quelques minutes.

(Si aucun domaine n'est configuré, Cisco Secure Workload récupère le domaine **Global** (Global).)

Une fois que les domaines ont été récupérés avec succès, vous verrez l'option de sélection des domaines s'afficher.

Étape 7 Si vous ne souhaitez pas déployer de politiques sur vos périphériques FTD gérés maintenant :

Lorsque l'option de sélection de domaines s'affiche, cliquez sur **Cancel** (Annuler).

Lorsque vous êtes prêt à déployer des politiques, revenez à la page External Orchestrators (Orchestrateurs externes), modifiez cet orchestrateur, cliquez sur **Domains** (Domaines) et sélectionnez les domaines comme décrit à l'étape suivante.

Étape 8 Sélectionnez le ou les domaines sur lesquels vous souhaitez appliquer les politiques de segmentation.

Si votre déploiement Firepower n'a pas de domaines configurés, sélectionnez le domaine **Global** (domaine global).

Étape 9 Cliquez sur **Update** (mettre à jour).

Les politiques de segmentation sont transmises aux politiques de contrôle d'accès des domaines que vous avez sélectionnés et les modifications sont déployées sur les périphériques FTD associés.

Le temps nécessaire pour transmettre les règles est généralement de quelques minutes, mais dépend du nombre de règles de politique et de la configuration des ressources du FMC et des FTD.

Prochaine étape

Revenez au tableau de présentation des procédures dans Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.6, à la page 45 et passez aux étapes restantes.

Configurer FMC Orchestrator dans Cisco Secure Workload versions 3.6.1.5 à 3.6.1.20

Utilisez la procédure suivante pour créer un orchestrateur externe FMC à l'aide de l'interface Web Cisco Secure Workload.

Avant de commencer

Suivez les étapes décrites jusqu'à présent dans le tableau de Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.6, à la page 45.

Si vous utilisez la version 3.6.1.36, n'utilisez pas cette procédure. Au lieu de cela, consultez Configurer l'orchestrateur FMC dans la version 3.6.1.36, à la page 48.

Procédure

Étape 1 Accédez à **Manage (Gestion) > External Orchestrators (Orchestrateurs externes).**

Étape 2 Cliquez sur **Create New Configuration** (Créer une nouvelle configuration)

Étape 3 Sous l'onglet « Basic Configs » (Configurations de base), configurez les champs suivants :

Option	Description
Type	Sélectionnez **FMC**.
Nom	Attribuez un nom unique à l'orchestrateur FMC.
Description	Saisissez une description pour l'orchestrateur.
Intervalles complets de l'instantané	Saisissez l'intervalle complet de l'instantané, en secondes. Le champ **Full Snapshot Interval(s)** (Intervalles complets de l'instantané) spécifie la fréquence à laquelle l'orchestrateur externe du FMC teste la connectivité FMC sur Cisco Secure Workload. Si une erreur se produit (par exemple, si le FMC n'est pas accessible en raison de problèmes de réseau ou si des informations d'authentification d'utilisateur ou de point terminal non valides ont été utilisées), l'orchestrateur FMC signale l'erreur dans le champ **Status** (État). Valeur par défaut : `3 600 secondes`
Nom d'utilisateur **Mot de passe**	Saisissez le nom d'utilisateur et le mot de passe de l'utilisateur dédié que vous avez créé dans FMC, comme indiqué précédemment dans ce document. Ces renseignements d'authentification sont utilisés pour communiquer avec le FMC.
Certificat de l'autorité de certification	Saisissez le certificat de l'autorité de certification que Cisco Secure Workload utilisera pour authentifier ce FMC. Vous pouvez obtenir ce certificat auprès de FMC en utilisant le flux de travail de gestion d'objets. Pour en savoir plus, consultez les rubriques sur les objets de l'autorité de certification interne dans le chapitre Objets réutilisables du *Guide de configuration de Cisco Firepower Management Center* pour votre version de Firepower.
Accept Self-signed Cert (Accepter le certificat autosigné)	Cochez cette case pour configurer l'orchestrateur FMC de façon à ce qu'il fasse confiance à un certificat autosigné.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Si vous utilisez Cisco Secure Workload SaaS, vous devez activer cette option. Si vous utilisez un appareil Cisco Secure Workload sur site, vous devrez peut-être activer cette option. Avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé, comme décrit plus haut dans ce document. Pour en savoir plus sur la fonction de tunnelisation du connecteur sécurisé, consultez le Guide de l'utilisateur disponible à partir de votre interface Web Cisco Secure Workload.

Option	Description
Activer l'application	Cochez cette case pour envoyer les politiques vers le FMC et ses périphériques FTD gérés. Cette case est cochée par défaut. Vous pouvez sélectionner cette case même si vous n'avez pas encore appliqué les politiques pour les espaces de travail; le système transmettra automatiquement les politiques vers le FMC et ses FTD gérés lorsque vous activez l'application sur un espace de travail. Si vous décochez cette case, les politiques ne seront pas transmises vers le FMC et toutes les règles précédemment transmises vers le FMC seront effacées.
Mode de mise en application	Sélectionnez **Merge** ou **Override** (fusionner ou remplacer) dans la liste déroulante. • Si vous sélectionnez **Override**(Remplacer), les politiques Cisco Secure Workload appliquées remplacent toutes les règles de contrôle d'accès FMC existantes. **Important** Si vous sélectionnez cette option, toutes les règles existantes de toutes les politiques de contrôle d'accès associées à un périphérique FTD seront supprimées et irrécupérables. Si vous souhaitez conserver des règles, nous vous recommandons d'exporter les règles avant de poursuivre cette intégration ou d'utiliser l'option **Merge** (Fusionner) (décrite ci-dessous). • Si vous sélectionnez **Merge** (Fusionner), les règles de Cisco Secure Workload sont ajoutées au début de la liste des règles de contrôle d'accès. **Remarque** Si **Enforcement Mode** (Mode d'application) est défini sur **Merge** (Fusionner) : • Nous vous recommandons de ne pas utiliser le préfixe `Workload_` pour les règles que vous saisissez manuellement dans FMC, car elles seront automatiquement supprimées. • Évitez d'effectuer simultanément le déploiement FTD à l'aide de l'interface utilisateur de FMC et l'application des politiques à l'aide de Cisco Secure Workload. Ces opérations asynchrones et de longue durée (environ 2 minutes) sont en concurrence les unes avec les autres et peuvent entraîner l'échec du déploiement FTD. Si le déploiement FTD échoue en raison d'applications de politiques concurrentes, vous devez le recommencer.

Étape 4 Cliquez sur l'onglet **Host Lists (listes d'hôtes).**

Étape 5 Saisissez le nom d'hôte et le numéro de port du FMC associé.

Le `host name` (nom d'hôte) doit être un nom de domaine complet pour FMC ou une adresse IP.

Le `port number` (numéro de port) par défaut est 443.

Si votre FMC est déployé dans une configuration prise en charge en haute disponibilité, saisissez également le nom d'hôte et le port du FMC de secours/secondaire.

Étape 6 Cliquez sur **Create** (créer).

Le temps nécessaire pour transmettre les règles est généralement de quelques minutes, mais dépend du nombre de règles de politique et de la configuration des ressources du FMC et des FTD.

Après quelques minutes, vérifiez l'état de l'intégration :

a) Dans la page **External Orchestrators (orchestrateurs externes)**, cliquez sur la ligne correspondant à votre orchestrateur FMC nouvellement créé.
b) La boîte de dialogue Configuration Details (Détails de la configuration) s'affiche. Si la connexion est réussie, le champ **Progress Status** (État de la progression) affiche le nombre de FTD trouvés.

Prochaine étape

Revenez au tableau de présentation des procédures dans Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.6, à la page 45 et passez aux étapes restantes.

Avancé : Utiliser ADM pour générer des politiques de segmentation

Pour permettre à ADM de découvrir les politiques de segmentation au lieu de les créer manuellement :

1. Suivez les étapes décrites dans Mettre en œuvre cette intégration pour Cisco Secure Workload, version 3.6, à la page 45, mais effectuez les étapes générales suivantes au lieu de créer les politiques manuellement.
2. Au sein de Cisco Firepower Management Center :
    1. Utilisez flexconfig pour configurer le système afin d'exporter les enregistrements NSEL (données de flux).

       Pour obtenir des instructions, consultez la documentation de votre produit Firepower à l'adresse https://www.cisco.com/c/en/us/support/security/defense-center/series.html#~tab-documents.
    2. Assurez-vous que le trafic que vous souhaitez affecter avec vos politiques est généré.
3. Dans Cisco Secure Workload :
    1. Déployez un dispositif d'acquisition (appliance virtuelle) qui contiendra les données de flux.
    2. Configurez un connecteur ASA pour recueillir les données de flux de votre système Firepower.

       (Ce connecteur recueille les données de flux des périphériques FTD).
    3. Attendez un certain temps que le système recueille suffisamment de données de flux pour générer les politiques appropriées.
    4. Exécutez ADM dans tous les espaces de travail d'application concernés
    5. Analysez, validez et approuvez les politiques de segmentation suggérées avant de les appliquer

Pour en savoir plus sur les étapes Cisco Secure Workload, consultez le guide de l'utilisateur dans l'interface Web Cisco Secure Workload.

Modification d'un orchestrateur FMC dans la version 3.6.1.36

- Vous pouvez créer l'orchestrateur FMC sans préciser les domaines sur lesquels appliquer la politique, puis modifier la configuration de l'orchestrateur ultérieurement pour préciser les domaines d'application.

  L'application se produit lorsque vous cliquez sur **Update** (Mettre à jour) après avoir sélectionné les domaines.

- Si vous modifiez un orchestrateur externe FMC, vous devez saisir à nouveau le mot de passe du compte FMC.

- Si vous modifiez un orchestrateur FMC pour lequel des domaines sont sélectionnés, Cisco Secure Workload récupère les domaines.

  Les domaines que vous avez déjà sélectionnés restent sélectionnés.

- Si vous modifiez un orchestrateur, il est possible que la page des orchestrateurs externes affiche initialement l'état de la connexion comme **Failure** (Échec) pendant que la connexion et la synchronisation se produisent, mais devient **Succeed** (Réussite) après quelques instants. Vous pouvez ensuite modifier les domaines.

Mettre en œuvre cette intégration pour Tetration version 3.5

Le tableau suivant présente le flux de travail de bout en bout pour configurer un centre de gestion Cisco Firepower Management Center et configurer son intégration à Tetration.

Étape	Description	Lien vers la procédure
1	Dans Tetration : Définissez les portées, les espaces de travail et les politiques de segmentation pour votre environnement.	Consultez la section sur la segmentation du guide de l'utilisateur Tetration : https://<cluster>/documentation/ui/adm.html
2	Si vous utilisez le logiciel-service Tetration ou si l'appareil FMC n'est pas directement accessible à partir de Tetration, configurez un tunnel de connecteur sécurisé pour assurer la connectivité.	Par défaut, Tetration communique avec l'API REST FMC à l'aide de HTTPS sur le port 443. Consulter le Guide de l'utilisateur Tetration à l'adresse https://<cluster>/documentation/ui/software_agents/secure_connector.html

Étape	Description	Lien vers la procédure
3	Configurez un FMC virtuel ou physique. Consultez le guide de démarrage associé à votre appareil.	Guide de démarrage (GD) pour Cisco Firepower Management Center Virtual : https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-intro.html Guide de démarrage (GD) pour Cisco Firepower Management Center 1000, 2500, et 4500 : https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1000-2500-4500/fmc-1000-2500-4500.html Guide de démarrage (GD) pour Cisco Firepower Management Center 1600, 2600, et 4600 : https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1600-2600-4600/fmc-1600-2600-4600.html
4	Dans FMC : Créez un domaine dédié à utiliser uniquement pour l'intégration à Tetration.	Reportez-vous à la section Création de domaines dans le chapitre sur la gestion du déploiement du Guide de configuration du Cisco Firepower Management Center pour votre version de Firepower. Par exemple :https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/domain_management.html#task_F3D21E5A48DF4F5FA0B3C1C4A86AA80D

Étape	Description	Lien vers la procédure
5	Dans FMC : Attribuez des périphériques FTD au FMC dans le domaine dédié que vous avez créé ci-dessus. **Remarque** Cela peut également être réalisé ultérieurement dans le processus, car l'intégration Tetration/FMC est en mesure de détecter les périphériques FTD nouvellement affectés.	Pour ajouter des périphériques gérés à un FMC, utilisez la page **Devices (Périphériques)Device Management (Gestion des périphériques)** dans l'interface graphique du FMC. Pour en savoir plus, consultez la rubrique Ajouter des périphériques gérés au FMC dans le Guide de démarrage correspondant à votre déploiement. Par exemple : • Guide de démarrage (GD) pour Cisco Firepower Management Center Virtual : https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-initial-admin.html • Guide de démarrage (GD) pour Cisco Firepower Management Center 1000, 2500, et 4500 : https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1000-2500-4500/fmc-1000-2500-4500.html#Cisco_Task.dita_009a8ec9-d320-4577-bcf5-9b09bfef3a2f • Guide de démarrage (GD) pour Cisco Firepower Management Center 1600, 2600, et 4600 : https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1600-2600-4600/fmc-1600-2600-4600.html#Cisco_Task.dita_009a8ec9-d320-4577-bcf5-9b09bfef3a2f
6	Dans FMC : Attribuez une politique de contrôle d'accès et de préfiltre au(x) FTD sous le domaine dédié que vous avez créé ci-dessus. La politique de préfiltre affectée au(x) FTD ne doit pas être la politique de préfiltre `par défaut` en lecture seule. Si l'orchestrateur FMC trouve un périphérique FTD auquel une `politique de préfiltre par défaut` est affectée, il ne transmettra pas les mises en application de politique à ce FTD.	Reportez-vous à la rubrique Configuration du préfiltre dans le chapitre Préfiltre et Politiques de préfiltre du Guide de configuration du Cisco Firepower Management Center pour votre version de Firepower. Par exemple : https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/prefiltering_and_prefilter_policies.html#id_17608

Étape	Description	Lien vers la procédure
7	Dans FMC : Créez un compte d'utilisateur interne personnalisé dédié à l'intégration de Tetration et de FMC. Notez que ce compte d'utilisateur interne doit être : • doté du rôle d'administrateur. • Dans le ou les mêmes domaines que les politiques d'accès et de préfiltre associées au périphérique FTD.	Reportez-vous à la rubrique Ajouter un utilisateur interne du Guide de configuration du centre de gestion Cisco Firepower Management Center pour votre version de Firepower. Par exemple :https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/user_accounts_fmc.html#task_j5n_1cr_qcb
8	Dans Tetration : Créer un orchestrateur FMC.	Configurer un orchestrateur FMC dans Cisco Tetration version 3.5, à la page 58
9	Dans Tetration : Effectuez l'application des politiques sur les espaces de travail souhaités.	Consultez la section Politiques du guide de l'utilisateur Tetration : https://<cluster>/documentation/ui/adm/policies.html
10	L'exécuteur de politique FMC déploie les politiques sur la politique de préfiltre de tous les FTD associés.	Dans Cisco Firepower Management Center, choisissez**Policies (Politiques)** > **Access Control (Contrôle d'accès)** > **Prefilter (Préfiltre).** Cliquer sur la politique associée pour afficher les règles appliquées de Tetration sur le ou les périphériques FTD. Pour en savoir plus, consultez les rubriques relatives aux Préfiltre et Politiques de préfiltre dans le chapitre sur le contrôle d'accès du Guide de configuration de Cisco Firepower Management correspondant à votre version de Firepower. Par exemple :https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/prefiltering_and_prefilter_policies.html#id_18072

Configurer un orchestrateur FMC dans Cisco Tetration version 3.5

Utilisez la procédure suivante pour créer un orchestrateur externe FMC à l'aide de l'interface Web de Tetration.

Procédure

Étape 1 Accédez à **Visibility (Visibilité) > External Orchestrators (Orchestrateurs externes)**

Étape 2 Cliquez sur **Create New Configuration** (Créer une nouvelle configuration)

Étape 3 Sous l'onglet « Basic Configs » (Configurations de base), configurez les champs suivants :

Option	Description
Type	Sélectionnez **FMC**.
Nom	Attribuez un nom unique à l'orchestrateur FMC.
Description	Saisissez une description pour l'orchestrateur.
Intervalles complets de l'instantané	Saisissez l'intervalle complet de l'instantané, en secondes. Le champ **Full Snapshot Interval(s)** (Intervalles complets de l'instantané) spécifie la fréquence à laquelle l'orchestrateur externe du FMC teste la connectivité du FMC sur Tetration. Si une erreur se produit (par exemple, si le FMC n'est pas accessible en raison de problèmes de réseau ou si des informations d'authentification d'utilisateur ou de point terminal non valides ont été utilisées), l'orchestrateur FMC signale l'erreur dans le champ **Status** (État). Valeur par défaut : `3 600 secondes`
Nom d'utilisateur **Mot de passe**	Saisissez le nom d'utilisateur et le mot de passe de l'utilisateur dédié que vous avez créé dans FMC, comme indiqué précédemment dans ce document. Ces renseignements d'authentification sont utilisés pour communiquer avec le FMC.
Certificat de l'autorité de certification	Saisissez le certificat de l'autorité de certification que Tetration utilisera pour authentifier ce FMC. Vous pouvez obtenir ce certificat auprès de FMC en utilisant le flux de travail de gestion d'objets. Pour en savoir plus, consultez les rubriques sur les objets de l'autorité de certification interne dans le chapitre Objets réutilisables du *Guide de configuration de Cisco Firepower Management Center* pour votre version de Firepower.
Accept Self-signed Cert (Accepter le certificat autosigné)	Cochez cette case pour configurer l'orchestrateur FMC de façon à ce qu'il fasse confiance à un certificat autosigné.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Si vous utilisez le logiciel-service Tetration, vous devez activer cette option. Si vous utilisez un appareil Tetration sur site, vous devrez peut-être activer cette option. Avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé, comme décrit plus haut dans ce document. Pour en savoir plus sur la fonction de tunnelisation du connecteur sécurisé, consultez le Guide de l'utilisateur disponible à partir de votre interface Web Tetration.

Option	Description
Activer l'application	Cochez cette case pour envoyer les politiques vers le FMC et ses périphériques FTD gérés. Cette case est cochée par défaut. Vous pouvez sélectionner cette case même si vous n'avez pas encore appliqué les politiques pour les espaces de travail; le système transmettra automatiquement les politiques vers le FMC et ses FTD gérés lorsque vous activez l'application sur un espace de travail. Si vous décochez cette case, les politiques ne seront pas transmises vers le FMC et toutes les règles de préfiltre précédemment transmises vers le FMC seront effacées.
Mode de mise en application	Sélectionnez **Merge** ou **Override** (fusionner ou remplacer) dans la liste déroulante. • Si vous sélectionnez **Override**(Remplacer), les politiques Tetration appliquées remplacent toutes les règles de politique de préfiltre existantes. **Important** Si vous sélectionnez cette option, toutes les règles de politique de préfiltre existantes seront supprimées et irrécupérables. Si vous souhaitez conserver des règles, nous vous recommandons d'exporter les règles avant de poursuivre cette intégration ou d'utiliser l'option **Merge** (Fusionner) (décrite ci-dessous). • Si vous sélectionnez **Merge** (Fusionner), les règles de Tetration sont ajoutées au début de la liste des règles de préfiltre. **Remarque** Si **Enforcement Mode** (Mode d'application) est défini sur **Merge** (Fusionner) : • Nous vous recommandons de ne pas utiliser le préfixe `Tetrul_` pour les règles que vous saisissez manuellement dans FMC, car elles seront automatiquement supprimées. • Évitez d'effectuer simultanément le déploiement FTD à l'aide de l'interface utilisateur de FMC et l'application des politiques à l'aide de Tetration. Ces opérations asynchrones et de longue durée (environ 2 minutes) sont en concurrence les unes avec les autres et peuvent entraîner l'échec du déploiement FTD. Si le déploiement FTD échoue en raison d'applications de politiques concurrentes, vous devez le recommencer.

Étape 4 Cliquez sur l'onglet **Host Lists (listes d'hôtes).**

Étape 5 Saisissez le nom d'hôte et le numéro de port du FMC associé.

Le `host name` (nom d'hôte) doit être un nom de domaine complet pour FMC ou une adresse IP.

Le `port number` (numéro de port) par défaut est 443.

Si votre FMC est déployé dans une configuration prise en charge en haute disponibilité, saisissez également le nom d'hôte et le port du FMC de secours/secondaire.

Étape 6 Cliquez sur **Create** (créer).

Le temps nécessaire pour transmettre les règles est généralement de quelques minutes, mais dépend du nombre de règles de politique et de la configuration des ressources du FMC et des FTD.

Après quelques minutes, vérifiez l'état de l'intégration :

a) Dans la page **External Orchestrators (orchestrateurs externes)**, cliquez sur la ligne correspondant à votre orchestrateur FMC nouvellement créé.
b) La boîte de dialogue Configuration Details (Détails de la configuration) s'affiche. Si la connexion est réussie, le champ **Progress Status** (État de la progression) affiche le nombre de FTD trouvés.

Afficher l'état d'application des domaines

Pour la version 3.6.1.36 ou ultérieure : dans la liste des orchestrateurs sur la page **Manage (Gestion) > External Orchestrators (Orchestrateurs externes)** :

- Pour la version 3.6.1.36 :

  Application affiche toujours **Disabled** (Désactivé) .

- Pour les versions3.7 :

  Si l'application est activée pour au moins un domaine, l'indicateur « **Enforcement** » (Application) indique **Enabled** (Activée).

Pour toutes les versions susmentionnées, pour voir quels domaines font l'objet d'une application :

1. Modifiez la configuration pour un orchestrateur FMC particulier.
2. Cliquez sur **Domains** (domaines).
3. L'application est activée pour tous les domaines répertoriés dans cette page Domains (Domaines).

Dépanner l'intégration de Cisco Secure Workload/Tetration avec Cisco Secure Firewall Management Center

Utilisez les procédures suivantes pour résoudre les problèmes de configuration courants d'intégration entre Cisco Secure Workload/Tetration et Cisco Secure Firewall Management Center.

Dépannage des problèmes de connexion de la migration

Utilisez la page des **orchestrateurs externes** pour identifier les problèmes courants à l'origine des échecs de connexion.

1. Accédez à la page des **orchestrateurs externes** :

   Pour Cisco Secure Workload version 3.6 : elle se trouve dans le menu **Manage** (Gestion).

   Dans le cas de Tetration 3.5 : dans le menu **Visibility** (visibilité).

2. Sur la page des orchestrateurs externes, recherchez la ligne correspondant à votre orchestrateur FMC.
3. L'état de la connexion de l'intégration s'affiche dans la colonne **Connection Status** (État de la connexion). Si cette colonne affiche `Failure` (Échec), cliquez sur la ligne pour afficher plus de détails.
4. Dans le tableau Configuration Details (détails de la configuration), recherchez la ligne **Authentication Failure Error** (erreur d'échec d'authentification).

Si le champ **Authentication Failure Error** (Erreur d'échec d'authentification) affiche `Waiting to connect` (En attente de connexion), attendez une ou deux minutes avant d'actualiser la page.

Si la ligne en **Authentication Failure Error** (Erreur d'échec d'authentification) affiche une erreur semblable à ce qui suit :

```
fmc clusterUUID=602c4264755f0263ee16e5af failed to connect to appliance 172.28.171.193:10447
```

Vérifiez les problèmes de configuration suivants :

Problème	Étapes de dépannage
Le `nom d'hôte` IP ou `le numéro de port` configuré n'est pas valide.	Assurez-vous que le `nom d'hôte` et `le numéro de port` FMC que vous avez saisis dans la configuration de l'orchestrateur externe FMC sont corrects. Vérifiez votre connectivité à l'adresse IP et au port configurés.
Le **nom d'utilisateur** ou le **mot de passe** est incorrect.	Assurez-vous que les champs **Username** (nom d'utilisateur) et **Password** (mot de passe) que vous avez saisis dans la configuration de l'orchestrateur FMC correspondent à l'utilisateur dédié que vous avez créé dans FMC et que l'utilisateur dispose des privilèges nécessaires tels que spécifiés précédemment dans ce document. **Remarque** Le nombre de fois de suite que les utilisateurs peuvent saisir des identifiants de connexion erronés à l'interface Web avant que le système ne bloque temporairement l'accès au compte pendant une période configurable, est déterminé par le paramètre **Max Number of Login Failures** (Nombre maximal d'échecs de connexion) au sein de la configuration générale de l'utilisateur de FMC. Pour plus d'informations, reportez-vous à la rubrique Paramètres de configuration générale de l'utilisateur du chapitre Paramètres de la plateforme matérielle du Guide Cisco Secure Firewall Management Center correspondant à votre version de Cisco Secure Firewall.

Problème	Étapes de dépannage
La case **Secure Connector Tunnel** (Tunnel du connecteur sécurisé) est cochée dans les configurations de base de l'orchestrateur FMC, mais le connecteur sécurisé n'est pas déployé correctement.	Vérifiez que le connecteur sécurisé est déployé correctement. Pour en apprendre davantage, consultez la section Connecteur sécurisé de votre guide de l'utilisateur :

(Cisco Secure Workload 3.6.1.36 et versions ultérieures) La liste d'état n'affiche pas l'état d'application par domaine

Consultez Afficher l'état d'application des domaines, à la page 61.

(Cisco Secure Workload version 3.6) Détecter les problèmes d'application de la politique

- Dans FMC, sélectionnez **Devices** (périphériques) > **Device Management** (gestion des périphériques) et assurez-vous qu'une politique de contrôle d'accès est attribuée aux FTD.
- Cliquez sur la politique de contrôle d'accès associée aux FTD et vérifiez que la section par défaut de la liste des règles comprend les règles attendues.
- Sinon, assurez-vous que les renseignements d'authentification de l'utilisateur dédié au FMC disposent de l'accès requis.

  Si vous ne constatez que des règles d'or, c'est que vous n'avez probablement pas mis en place de politique dans les espaces de travail des applications.

  Vérifiez que l'application de la politique est activée dans les espaces de travail.
- Dans la configuration de l'orchestrateur externe FMC :
  - Vérifiez que Cisco Secure Workload peut se connecter avec succès au FMC.
  - Selon votre version 3.6 et selon que votre déploiement FMC comporte plusieurs domaines configurés :

    Vérifiez que la case **Enable Enforcement** (activer l'application) est cochée.

    -ou-

    Vérifiez que les domaines adéquats sont sélectionnés.

Astuces Pour afficher les détails d'un orchestrateur FMC, y compris le nombre de périphériques FTD gérés qui reçoivent des mises à jour de politiques par l'intermédiaire de cet orchestrateur : accédez à **Manage (Gestion) > External Orchestrators (Orchestrateurs externes)** et cliquez sur la ligne de votre orchestrateur FMC. Le nombre de FTD s'affiche dans la ligne **Progress Status** (État d'avancement) du tableau qui s'affiche.

.

(Tetration version 3.5) Détecter les problèmes d'application des politiques

Utilisez les étapes suivantes pour vérifier que vos règles Tetration sont appliquées sur les FTD associés :

1. Dans Cisco Secure Firewall Management Center, sélectionnez **Devices** (Périphériques) > **Device Management** (Gestion des périphériques).
2. Cliquez sur le lien de politique de contrôle d'accès pour le FTD associé.
3. Si la politique de préfiltre affectée à la politique de contrôle d'accès du FTD est la valeur par défaut en lecture seule de la `politique de préfiltre par défaut`, Tetration ignore le déploiement des politiques sur le FTD. Vous devez créer une politique de préfiltre personnalisée que Tetration pourra utiliser dans son intégration avec FMC. (Voir l'étape concernée dans Mettre en œuvre cette intégration pour Tetration version 3.5, à la page 55).

Si votre règle personnalisée ne figure pas dans la liste des politiques de contrôle d'accès, vérifiez qu'elles sont appliquées :

1. Dans Cisco Secure Firewall Management Center, accédez à **Policies** (Politiques) > **Access Control** (Contrôle d'accès) > **Prefilter** (Préfiltre).
2. Cliquez sur votre politique de préfiltre personnalisée pour afficher sa liste de règles.

Si votre politique de préfiltre personnalisée apparaît dans la liste de contrôle d'accès, mais qu'aucune règle Tetration appliquée ne s'affiche :

- Vérifiez la connectivité FMC
- Vérifiez que la case **Enable Enforcement** (activer l'application) est cochée dans la configuration des **orchestrateurs externes** Tetration.
- Vérifiez que l'application de la politique a été effectuée.

Échec de la mise à jour de la politique dans le déploiement haute disponibilité de FMC

Ce basculement peut prendre jusqu'à 4 minutes; pendant ce temps, toute application de politique au FMC non actif échouera.

Les règles de Cisco Secure Workload ne s'affichent pas dans la politique de contrôle d'accès

- Les règles sont transmises uniquement aux politiques de contrôle d'accès auxquelles au moins un périphérique FTD est affecté.
- Vérifiez l'état de la connexion de l'orchestrateur FMC sur la page Orchestrateurs externes.
- Si vous utilisez Cisco Secure Workload version 3.6.1.36, assurez-vous d'avoir sélectionné les domaines attendus dans l'orchestrateur FMC.

Communiquer avec le centre d'assistance technique Cisco (TAC).

Si le problème persiste, communiquez avec l'équipe de soutien de Cisco appropriée en fonction de votre déploiement :

- Cisco Secure Workload/Tetration sur site - Communiquez avec le Cisco TAC
- Cisco Secure Workload/Tetration SaaS Ouvrez un dossier auprès de l'équipe de soutien du logiciel-service (SaaS)

Historique de l'intégration Cisco Secure Workload/FMC

Pour en savoir plus sur l'historique de l'intégration de Cisco Secure Workload et de l'intégration de FMC, ainsi que des versions de produits prises en charge, consultez Déploiements pris en charge, à la page 12.

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.