Module de correction APIC/ Secure Firewall 3.0

Dernière modification : 2025-11-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

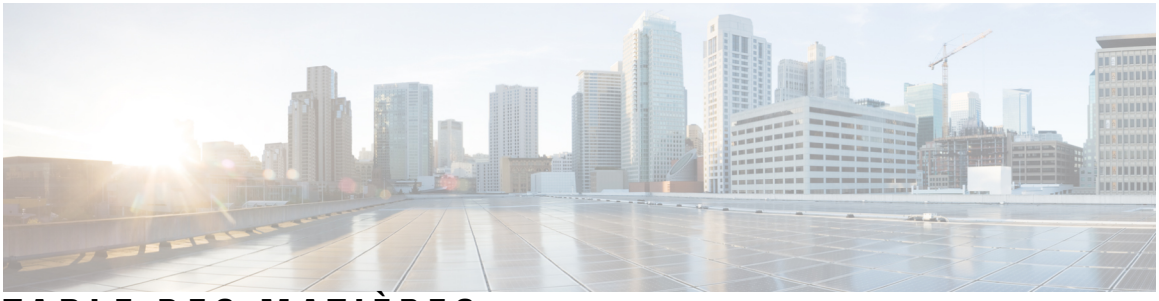


TABLE DES MATIÈRES

Full Cisco Trademarks with Software License ?

CHAPITRE 1 **À propos du module de correction** 1

À propos du module de correction 1

Fonctionnalités prises en charge 4

CHAPITRE 2 **Télécharger et installer le APIC/Cisco Secure Firewall Remediation Module** 5

Télécharger et installer le APIC/Cisco Secure Firewall Remediation Module 5

CHAPITRE 3 **Correction et mise en quarantaine** 7

Processus de correction et de mise en quarantaine 7

Comment corriger et mettre en quarantaine 7

Créer un contrat de gestion facultatif et un contrat GPT 9

Conditions préalables à la création d'un contrat de gestion facultatif et d'un contrat GPT 9

Création facultative d'un contrat de gestion et d'un contrat GPT 11

Créer une instance et un type de module de correction 12

Configurer une règle de contrôle d'accès pour la correction 15

Configurer une règle de corrélation pour la correction 17

Associer la règle de corrélation à l'instance du module de correction 18

Vérifiez la correction dans le Firewall Management Center 18

Vérifier la mise en quarantaine dans l'APIC 19

CHAPITRE 4 **Mettre manuellement en quarantaine une adresse IP** 21

Survol de la mise en quarantaine manuelle d'une adresse IP 21

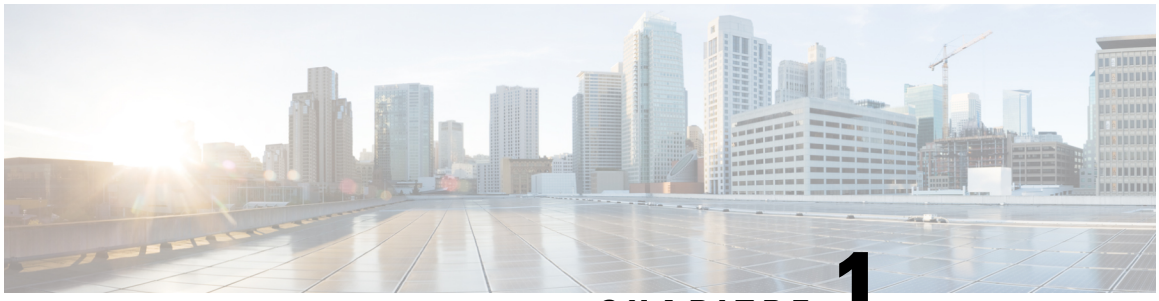
Rechercher une adresse IP à mettre en quarantaine 21

Créer un attribut GPT uSeg 22

Vérifier la mise en quarantaine manuelle de l'adresse IP 23

CHAPITRE 5 **Documentation associée** 25

Documentation associée 25



CHAPITRE 1

À propos du module de correction

- À propos du module de correction, à la page 1
- Fonctionnalités prises en charge, à la page 4

À propos du module de correction

Avec le APIC/Cisco Secure Firewall Remediation Module, lorsqu'une attaque sur votre réseau est détectée par le Firewall Management Center, le terminal incriminé peut être complètement mis en quarantaine dans le contrôleur d'infrastructure de politique d'application (APIC), afin qu'aucun autre trafic ne soit autorisé à entrer ou à sortir de ce terminal. La figure suivante montre la relation entre le Firewall Management Center et l'APIC lorsque le module de correction est installé.

Compatibilité

Le tableau suivant montre la compatibilité entre le APIC/Cisco Secure Firewall Remediation Module, le Firewall Management Center et l'APIC.

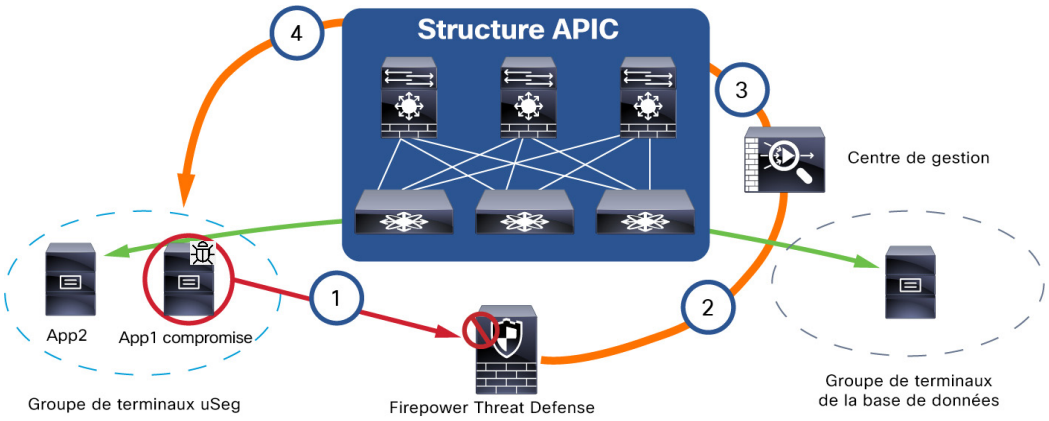
Tableau 1 : Compatibilité avec le module de correction, Firewall Management Center et l'APIC

Version du module de correction compatible avec...	version Firewall Management Center	version de l'APIC
3.0	version 7.0 ou ultérieure	5.1(1h)

Terminal compromis

La figure suivante montre comment le APIC/Cisco Secure Firewall Remediation Module réagit lorsqu'un terminal compromis est détecté.

À propos du module de correction



Le processus est le suivant :

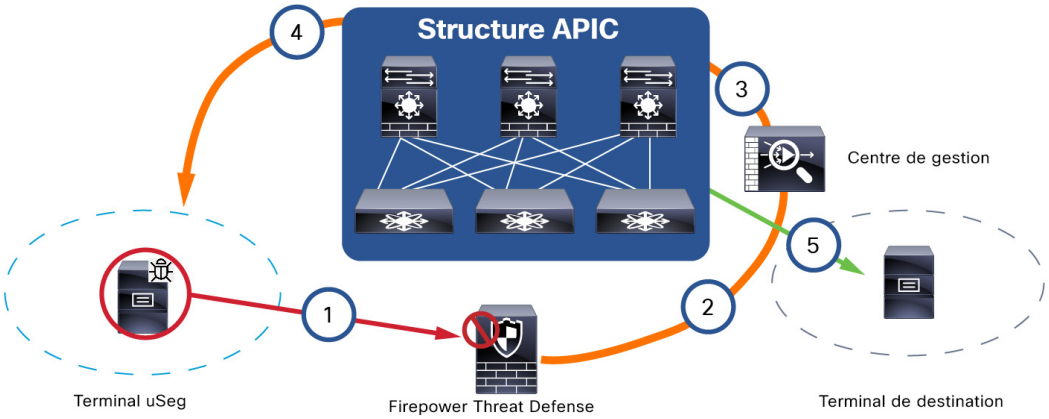
1. Un terminal avec une application compromise dans un groupe de terminaux (groupe de terminaux à gauche) lance une attaque sur un autre terminal dans la base de données GPT. L'attaque est bloquée en ligne par un périphérique géré (comme un périphérique physique ou virtuel exécutant Firepower Threat Defense).
2. Un événement d'attaque est généré et envoyé au Firewall Management Center. L'événement d'attaque comprend des informations sur le terminal compromis.
3. L'événement d'attaque déclenche le module de correction pour l'APIC, qui a utilisé l'API de routage nord (NB) de l'APIC pour contenir le terminal compromis dans la structure ACI.
4. L'APIC contient ou met rapidement la charge de travail de l'application compromise en quarantaine dans un GPT de microsegment isolé (uSeg).

   Étant donné que App2 n'est pas compromise, elle peut toujours communiquer sur le réseau.

   Vous pouvez mettre en quarantaine un terminal source, un terminal de destination, ou les deux, comme l'illustre la section suivante.

Mettre en quarantaine les terminaux sources et/ou de destination

Lors de la détection d'un terminal compromis, vous pouvez éventuellement mettre en quarantaine soit le terminal source, soit le terminal de destination, soit les deux, comme le montre la figure suivante.



La figure montre le processus suivant :

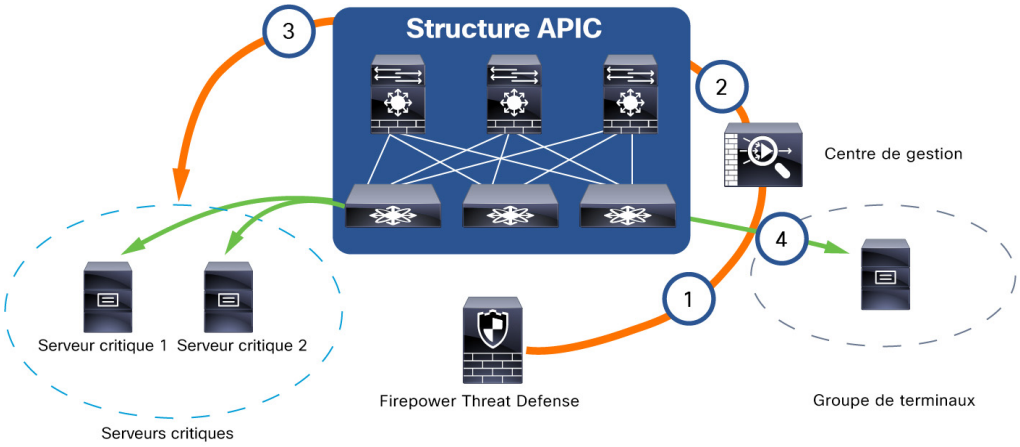
1. Un terminal avec une application compromise dans un groupe de terminaux (GPT) lance une attaque sur un autre terminal dans un autre GPT. L'attaque est bloquée en ligne par un périphérique géré (comme un périphérique physique ou virtuel exécutant Firepower Threat Defense).
2. Un événement d'attaque est généré et envoyé au Firewall Management Center. L'événement d'attaque comprend des informations sur le terminal compromis.
3. L'événement d'attaque déclenche le module de correction pour l'APIC, qui a utilisé l'API de routage nord (NB) de l'APIC pour contenir le terminal compromis dans la structure ACI.
4. L'APIC contient ou met rapidement la charge de travail de l'application compromise en quarantaine dans un GPT de microsegment isolé (uSeg).
5. Selon la configuration, le terminal source peut être mis en quarantaine, le terminal de destination peut être mis en quarantaine, ou les deux terminaux peuvent être mis en quarantaine.

   L'exemple illustré dans la figure met en quarantaine le terminal uSeg (source), mais pas le terminal de destination.

Toujours autoriser le trafic vers les serveurs critiques

Vous pouvez autoriser le trafic à destination et en provenance des serveurs critiques, même si ce trafic pourrait être jugé suspect. *Utilisez cette option avec prudence*, mais elle peut être utile lorsque vous souhaitez autoriser en tout temps ce trafic.

La figure suivante présente un exemple.



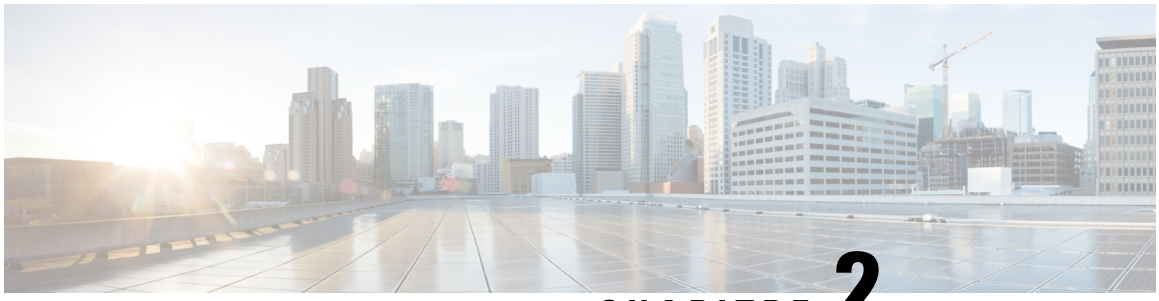
La figure montre le processus suivant :

1. Un terminal dans un `groupe de terminaux` envoie du trafic vers des serveurs désignés comme `Critical Servers` (Serveurs critiques). (Vous spécifiez ces serveurs par leur adresse IP.)
2. Le Firewall Management Center ignore ce trafic, même s'il correspond aux règles de corrélation.
3. Le trafic est toujours autorisé vers et en provenance des serveurs critiques du `groupe de terminaux` et des `serveurs critiques`, quel que soit son contenu.

Fonctionnalités prises en charge

Cette version vous permet de mettre en quarantaine les terminaux incriminés qui sont détectés par le APIC/Cisco Secure Firewall Remediation Module, à l'aide de la version 5.1(1h) de l'APIC . Pour la version 3.0 du module de correction, le comportement pris en charge lorsque les terminaux sont mis en quarantaine est décrit dans le tableau suivant :

	Le commutateur virtuel distribué (DVS) VMware	**Ordinateur sans système d'exploitation**
Vérifié en mode IPS en ligne	Oui	Oui
Mode de pont GPT	Oui	Oui
Mode routé GPT	Non	Non
Vérification de plusieurs IP en une vérification MAC	Oui	Oui
Créer uniquement un attribut uSeg de filtre d'adresse IP	Non	Non
Créer un filtre d'adresse IP et un attribut uSeg de filtre adresse MAC	Oui	Oui
Mettre en quarantaine les terminaux sources et de destination	Oui	Oui
Appliquer un contrat de gestion prédéfini aux terminaux source et de destination	Oui	Oui
Autoriser le trafic d'un terminal en quarantaine vers un groupe de terminaux L3Out	Oui	Oui
Autoriser l'audit uniquement	Oui	Oui
Toujours autoriser le trafic vers les serveurs critiques	Oui	Oui



CHAPITRE 2

Télécharger et installer le APIC/Cisco Secure Firewall Remediation Module

Téléchargez le APIC/Cisco Secure Firewall Remediation Module et installez-le dans le Cisco Secure Firewall Management Center, comme indiqué dans la section suivante.

- Télécharger et installer le APIC/Cisco Secure Firewall Remediation Module, à la page 5

Télécharger et installer le APIC/Cisco Secure Firewall Remediation Module

Avant de commencer

Assurez-vous d'utiliser des versions compatibles, comme indiqué dans le tableau suivant.

Tableau 2 : Compatibilité avec le module de correction, Firewall Management Center et l'APIC

Version du module de correction compatible avec...	version Firewall Management Center	version de l'APIC
3.0	version 7.0 ou ultérieure	5.1(1h)

Procédure

Étape 1 Téléchargez le APIC/Cisco Secure Firewall Remediation Module sur une machine sur laquelle vous vous connecterez au Firewall Management Center.

- FMC : https://software.cisco.com/download/home/278875421 Choisissez votre modèle, choisissez **Cisco Firepower Management Center Remediation Modules** (modules de correction Cisco Firepower Management Center) , puis choisissez **ACI**.
- FMC virtuel : https://software.cisco.com/download/home/286259687/type/286311510/release/Tetration Choisissez **ACI** (infrastructure axée sur les applications)

Étape 2 Connectez-vous au Firewall Management Center si vous ne l'avez pas encore fait.

Télécharger et installer le APIC/Cisco Secure Firewall Remediation Module

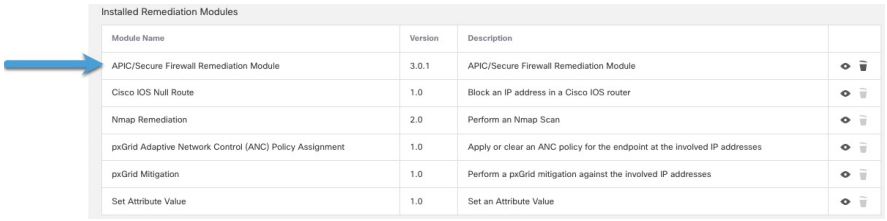
Étape 3 Cliquez sur **Policies (Politiques)** > **Actions** > **Modules**.

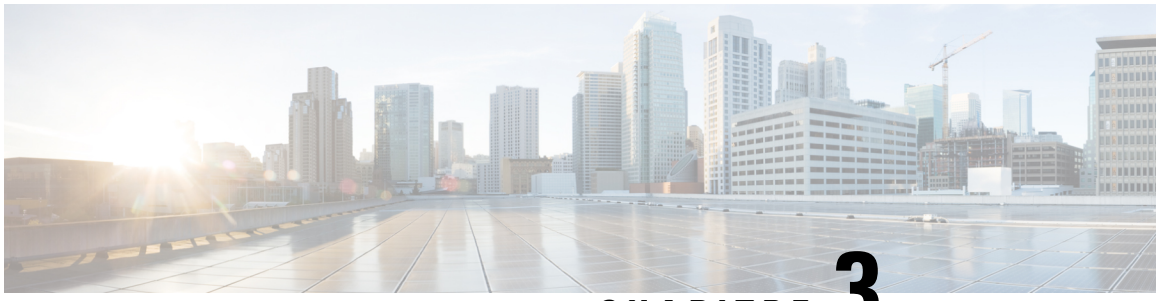
Étape 4 Dans la section Install a New Module (installer un nouveau module), cliquez sur **Browse** (parcourir).

Étape 5 Suivez les invites pour charger le module de correction.

Étape 6 Cliquez sur **Install** (Installer).

Étape 7 Une fois l'installation réussie, le APIC/Cisco Secure Firewall Remediation Module s'affiche dans la liste des modules de correction installés :





CHAPITRE 3

Correction et mise en quarantaine

Ce chapitre explique les tâches que vous devez effectuer dans l'APIC et dans le Cisco Secure Firewall Management Center pour créer des règles permettant de corriger et de mettre en quarantaine un terminal.

- Processus de correction et de mise en quarantaine, à la page 7
- Créer un contrat de gestion facultatif et un contrat GPT, à la page 9
- Créer une instance et un type de module de correction, à la page 12
- Configurer une règle de contrôle d'accès pour la correction, à la page 15
- Configurer une règle de corrélation pour la correction, à la page 17
- Associer la règle de corrélation à l'instance du module de correction, à la page 18
- Vérifiez la correction dans le Firewall Management Center, à la page 18
- Vérifier la mise en quarantaine dans l'APIC, à la page 19

Processus de correction et de mise en quarantaine

La *correction* (définir les circonstances dans lesquelles un terminal doit être mis en quarantaine) et la *mise en quarantaine* (isolement d'un terminal pour l'empêcher de communiquer sur le réseau) constituent un processus en plusieurs étapes, résumé dans la section suivante, Comment corriger et mettre en quarantaine, à la page 7.

Comment corriger et mettre en quarantaine

Les éléments suivants résument les tâches requises pour corriger et mettre en quarantaine un terminal. Vous effectuez certaines tâches dans l'APIC et dans le Firewall Management Center.

Avant de commencer

Consultez une référence comme le livre blanc d'*utilisation et de conception des groupes de terminaux (GPT)* ou le *guide de configuration de base Cisco APIC* pour comprendre les concepts liés à l'APIC.

SUMMARY STEPS

1. En option, créez un contrat de gestion et un groupe de terminaux du contrat de gestion (GPT).
2. Créez une instance et un type de module de correction.
3. Configurez une règle de contrôle d'accès qui détermine les conditions en vertu desquelles un terminal doit être mis en quarantaine.

4. Associez la règle de corrélation à la politique de correction.
5. Vérifiez la quarantaine et les mesures correctives.

DETAILED STEPS

Procédure

	Commande ou action	Objectif
Étape 1	En option, créez un contrat de gestion et un groupe de terminaux du contrat de gestion (GPT).	Effectuez cette tâche dans l'APIC. L'APIC utilise un modèle de liste autorisée, dans lequel le trafic permis est explicitement défini. Un *contrat* est un élément de politique utilisé pour définir la communication entre les GPT. Cette configuration facultative vous permet d'initier une connexion au GPT uSeg en quarantaine. Pour en savoir plus, consultez Création facultative d'un contrat de gestion et d'un contrat GPT, à la page 11.
Étape 2	Créez une instance et un type de module de correction.	Effectuez la tâche suivante dans le Firewall Management Center. Le module de correction crée, sur l'APIC, le GPT qui vous permet de visualiser et d'utiliser les terminaux en quarantaine. Le module de correction peut : • Mettre en quarantaine le terminal source, le terminal de destination ou les deux • Référencer un GPT de gestion • Auditer l'activité de correction uniquement sans déclencher la correction ou affecter le trafic de production Pour en savoir plus, consultez Créer une instance et un type de module de correction, à la page 12.
Étape 3	Configurez une règle de contrôle d'accès qui détermine les conditions en vertu desquelles un terminal doit être mis en quarantaine.	Effectuez la tâche suivante dans le Firewall Management Center. Déterminez les conditions dans lesquelles vous souhaitez qu'un terminal soit mis en quarantaine ; par exemple, transmission de trafic non sécurisé. Configurez une règle de contrôle d'accès qui déclenche à son tour la politique de correction que vous avez configurée précédemment. Pour en savoir plus, consultez Configurer une règle de contrôle d'accès pour la correction, à la page 15.
Étape 4	Associez la règle de corrélation à la politique de correction.	Effectuez la tâche suivante dans le Firewall Management Center.

	Commande ou action	Objectif
		Cela déclenche la quarantaine sur l'APIC. Pour en savoir plus, consultez Associer la règle de corrélation à l'instance du module de correction, à la page 18.
Étape 5	Vérifiez la quarantaine et les mesures correctives.	Vérifiez la *mise en quarantaine* dans l'APIC et vérifiez la *correction* dans le Firewall Management Center. Pour plus de renseignements, consultez les sections Vérifier la mise en quarantaine dans l'APIC, à la page 19 et Vérifiez la correction dans le Firewall Management Center, à la page 18.

Prochaine étape

Créer un contrat de gestion facultatif et un contrat GPT, à la page 9

Créer un contrat de gestion facultatif et un contrat GPT

Vous pouvez éventuellement prédéfinir un contrat de filtrage de trafic APIC dans le détenteur commun et un GPT de gestion dans le détenteur de gestion pour initier une connexion au GPT uSeg mis en quarantaine. Pour utiliser cette configuration facultative, vous *devez* définir un GPT de gestion dans APIC dans son détenteur **mgmt** et vous *devez* définir un contrat dans le détenteur **common**.

Pour en savoir plus, consultez le *Guide de configuration de base de Cisco APIC*.

Prochaines étapes

Conditions préalables à la création d'un contrat de gestion facultatif et d'un contrat GPT, à la page 9.

Conditions préalables à la création d'un contrat de gestion facultatif et d'un contrat GPT

Cette tâche explique comment effectuer les opérations suivantes avant de configurer un contrat de gestion facultatif et un contrat GPT :

- Créer une application ESG.
- Créez un filtre pour la mise en quarantaine que vous souhaitez effectuer ; dans cet exemple, le filtre s'applique au trafic SSH2.

Procédure

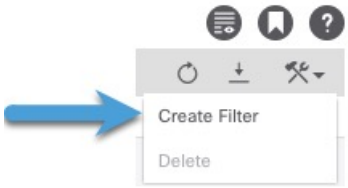
Étape 1 Connectez-vous à l'APIC.

Étape 2 Cliquez sur **Tenants (locataires)**.

Étape 3 Cliquez deux fois sur **common** (commun).

Étape 4 Dans le volet de gauche, développez **Contracts (Contrats)** > **Filters (Filtres)**.

Étape 5 Dans le volet de droite, cliquez sur **Create Filter** (Créer un filtre).



Étape 6 Attribuez au filtre un **nom** comme **SSHv2**.

Étape 7 Cliquez sur **Submit** (soumettre).

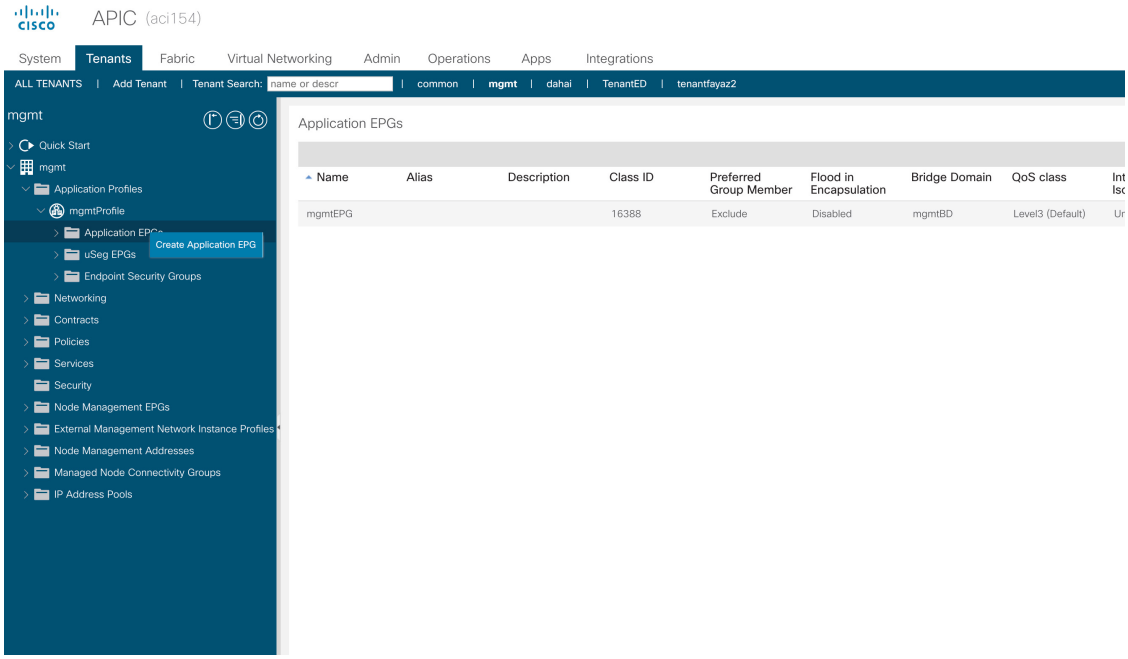
Étape 8 Dans le volet de gauche, cliquez sur **Tenants (Détenteurs)** > **ALL TENANTS (TOUS LES DÉTENTEURS)**.

Étape 9 Cliquez sur **mgmt** (gestion).

Étape 10 Développez **Application Profiles (Profils d'application)** > **mgmt profile (profil de gestion)**.

Étape 11 Faites un clic droit sur **Application EPGs** (GPT d'application) et cliquez sur **Create Application EPG** (Créer un GPT d'application).

La figure suivante présente un exemple.



Étape 12 Attribuez un **nom** au GPT.

Étape 13 Dans la liste **Bridge Domain** (domaine de pont), cliquez sur WHICH BRIDGE DOMAIN (QUEL DOMAINE DE PONT).

Étape 14 Cliquez sur **Terminer**.

Prochaine étape

Création facultative d'un contrat de gestion et d'un contrat GPT, à la page 11

Création facultative d'un contrat de gestion et d'un contrat GPT

Si vous ne souhaitez pas créer de contrats, passez cette section et poursuivez avec Créer une instance et un type de module de correction, à la page 12.

Procédure

Étape 1 Connectez-vous à l'APIC.

Étape 2 Cliquez sur **ALL TENANTS** (tous les détenteurs).

Étape 3 Cliquez deux fois sur **common** (commun).

Étape 4 Développez **Contracts (Contrats)** > **Standard**.

Étape 5 Faites un clic droit sur **Standard**, puis cliquez sur **Create Contrat** (créer un contrat).

Étape 6 Dans le champ **Name** (nom), saisissez **`useg_filter_contrat`**.

Étape 7 Dans la liste **Scope** (portée), cliquez sur **Global** (globale).

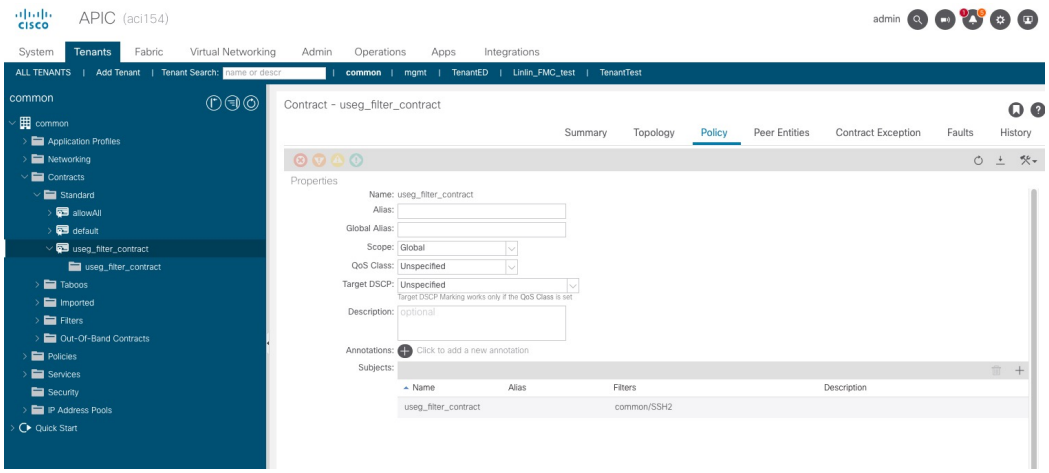
Étape 8 Faites d'autres sélections au besoin.

Étape 9 Cliquez sur **Submit** (soumettre).

Étape 10 Cliquez sur **useg_filter_contrat**.

Étape 11 Dans le volet de droite, cliquez sur l'onglet **Policy** (Politique).

La figure suivante présente un exemple.



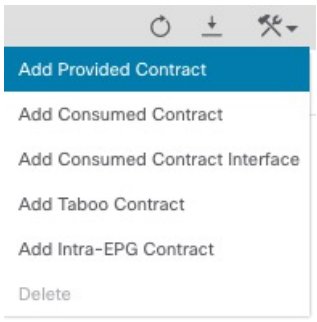
Étape 12 Cliquez sur **ALL TENANTS** (tous les détenteurs).

Étape 13 Double-cliquez sur **mgmt** (gestion).

Étape 14 Expand **mgmt (gestion)** > **Application Profiles (Profils d'application)** > **mgmtProfile (profil de gestion)** > **Application EPGs (GPT d'application)** > **mgmtEPG (GPT de gestion)** > **.**

Étape 15 Cliquez sur **Contracts** (Contrats).

Étape 16 Cliquez sur **Add Provided Contrat** (Ajouter un contrat fourni).



Étape 17 Dans la liste **Contract** (Contrat), cliquez sur **useg_filter_contract**.

Étape 18 Cliquez sur **Submit** (soumettre).

Prochaine étape

Consultez Créer une instance et un type de module de correction, à la page 12.

Créer une instance et un type de module de correction

Pour que Cisco Secure Firewall Management Center puisse détecter les menaces et informer l'APIC de les mettre en quarantaine, vous devez configurer sur Cisco Secure Firewall Management Center une instance et un type de module de correction. Pour plus d'informations sur les mesures correctives, consultez le Guide d'administration Cisco Secure Firewall Management Center. Vous pouvez éventuellement choisir de mettre en quarantaine le terminal source, le terminal de destination ou les deux.

Vous pouvez également choisir d'auditer uniquement les terminaux sans les mettre en quarantaine.

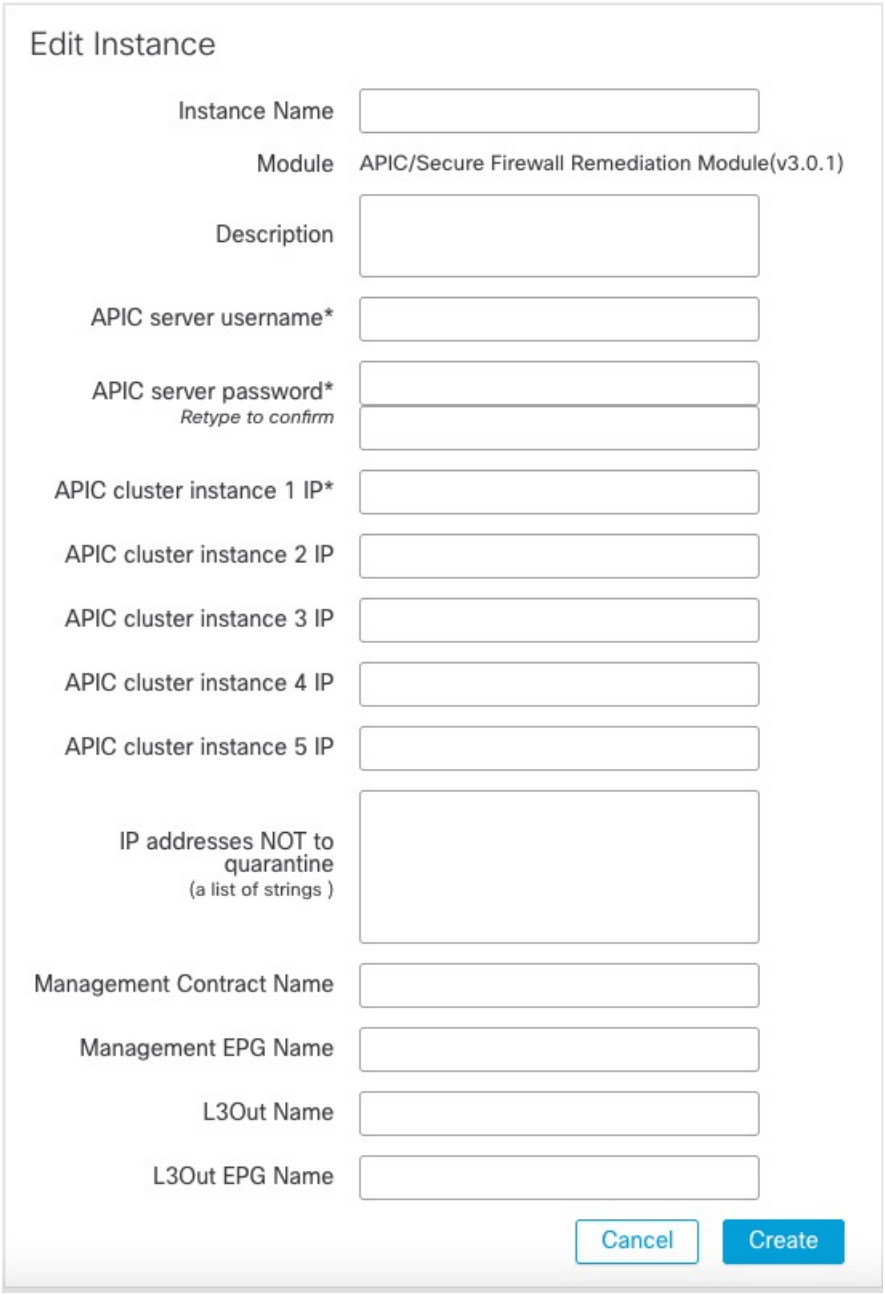
Procédure

Étape 1 Connectez-vous au Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Policies (Politiques)** > **Actions** > **Instances**.

Étape 3 Dans la liste **Select a module type** (sélectionner un type de module), cliquez sur **APIC/ Secure Firewall Remediation Module (module de correction APIC/ Secure Firewall) (3.0.1)**.

Étape 4 Cliquez sur **Add** (ajouter).
La page Edit Instance (modifier l'instance) s'affiche comme suit.



Étape 5 Saisissez l'information suivante :

Article	Description
Nom de l'instance	Saisissez un nom unique pour identifier cette instance. (Les espaces ne sont pas autorisés dans le nom.)
Description	(Facultatif) Saisir une description
Nom d'utilisateur du serveur APIC	Saisissez le nom d'un utilisateur APIC disposant des privilèges d'administrateur.

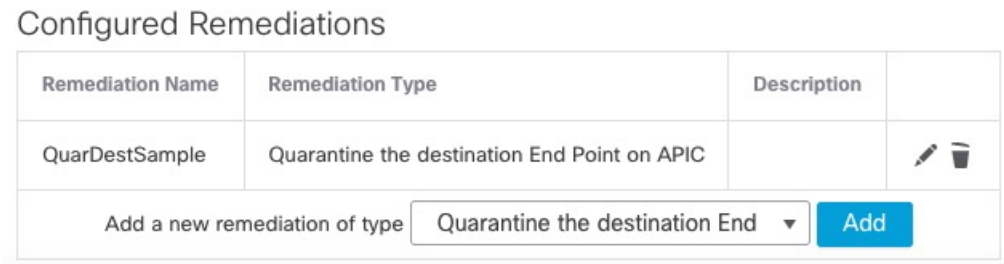
Article	Description
Mot de passe du serveur APIC	Entrer et entrer de nouveau le mot de passe de l'utilisateur
Adresse IP de l'instance 1 de la grappe APIC	Saisissez l'adresse IP du serveur APIC ou du premier serveur de la grappe.
Adresse IP de l'instance de grappe APIC	(Facultatif) Si votre grappe APIC comporte plusieurs serveurs, saisissez des adresses IP supplémentaires dans les champs prévus à cet effet.
Adresses IP à NE PAS mettre en quarantaine	(Facultatif) Saisissez une liste d'adresses IP individuelles à toujours exclure de la mise en quarantaine. Séparez les adresses IP par la fonction Enter (Entrée). Vous ne pouvez pas préciser de filtres d'adresses locales.
Nom du contrat de gestion	(Facultatif) Saisissez le nom du contrat de gestion que vous avez créé dans l'APIC. Pour en savoir plus, consultez Créer un contrat de gestion facultatif et un contrat GPT, à la page 9.
Nom du GPT de gestion	(Facultatif) Saisissez le nom du GPT auquel le contrat de gestion est associé. Pour en savoir plus, consultez Créer un contrat de gestion facultatif et un contrat GPT, à la page 9.
Nom L3Out	(Facultatif) Le nom d'une cible L3Out configurée sur l'APIC. Si vous saisissez une valeur dans **L3Out Name** (nom L3Out), vous devez également saisir une valeur dans **L3Out EPG Name** (nom GPT L3Out). Abandon du trafic entre un terminal mis en quarantaine dans une cible L3Out et le groupe de terminaux source tout en autorisant le trafic du terminal en quarantaine à des fins d'analyse d'investigation.
Nom du GPT L3out	(Facultatif) Le nom d'un groupe de terminaux L3Out (GPT) configuré sur l'APIC. Si vous saisissez une valeur dans **L3Out EPG Name** (nom GPT L3Out), vous devez également saisir une valeur dans **L3Out Name** (nom L3Out).
Audit seulement	**Off** (désactivé) (par défaut) : met en quarantaine un terminal compromis et envoie des messages d'état de corrélation à Firewall Management Center. **On** (activé) : ne met pas en quarantaine un terminal compromis ; à la place, envoie des messages d'état de corrélation à Firewall Management Center (**Analysis (Analyse)** > **Correlation (Corrélation)** > **Correlation Events (Événements de corrélation)**).

Étape 6 Dans la section Configured Remediation (correction configurée) au bas de la page, cliquez sur l'une des options suivantes, puis cliquez sur **Add** (ajouter) :

- **Mettre en quarantaine le terminal de destination sur l'APIC**
- **Mettre en quarantaine le terminal source sur l'APIC**

Le nom de la correction ne peut pas inclure d'espace.

Voici un exemple de la section Configured Remediation (correction configurée) affichant une correction.



Étape 7 Dans la page Edit Remediation (modifier la correction), saisissez les informations suivantes :

- **Remediation Name** (nom de correction) : saisissez un nom pour identifier l'instance de correction.
- (Facultatif) **Description** : saisissez une description de l'instance de correction.

Étape 8 Cliquez sur **Create** (créer).

Étape 9 Cliquez sur **Done (Terminé)**.

Étape 10 Dans la page Edit Instance (modifier l'instance), configurez au besoin une autre correction.

Prochaine étape

Consultez Configurer une règle de contrôle d'accès pour la correction, à la page 15.

Configurer une règle de contrôle d'accès pour la correction

Cet exemple montre comment créer une règle de contrôle d'accès qui bloque le protocole SSH . Après la création de cette règle, tout terminal qui tente d'établir une connexion SSH avec un autre terminal dans un GPT surveillé, voit ou les nœuds incriminés mis en quarantaine.

Procédure

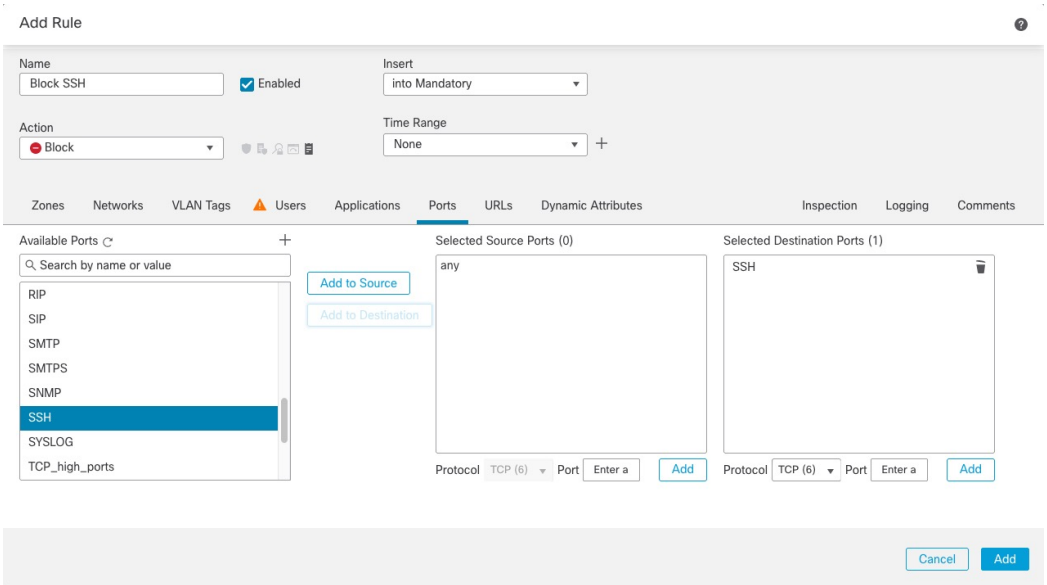
Étape 1 Connectez-vous au Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Policies (Politiques)** > **Access Control heading (En-tête Contrôle d'accès)** > **Access Control (Contrôle d'accès)**.

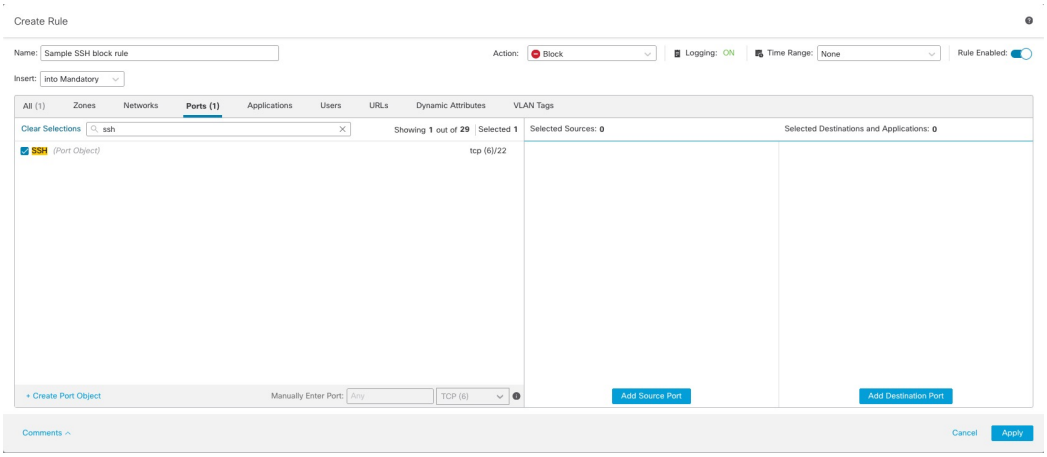
Étape 3 Créez une nouvelle politique de contrôle d'accès ou modifiez une politique existante.**Modifier** (✎)

Étape 4 Si vous modifiez une politique existante, cliquez sur **Add Rule** (ajouter une règle) pour ajouter une règle.

Saisissez les informations suivantes (Firewall Management Center version 7.2 ou antérieure).



Saisissez les informations suivantes (Firewall Management Center version 7.3 ou ultérieure).



Article	Description
Champ **Nom**	Saisissez un nom unique pour identifier cette règle. *Notez* le nom, car vous en aurez besoin plus tard.
Liste des **actions**	Cliquez sur **Block** (Bloquer).b
Page de l'onglet **Ports**	Dans la liste **Available Ports** (ports disponibles), faites défiler jusqu'à SSH et cliquez sur **Add to Destination** (ajouter à la destination).
Page de l'ongletLogging (journalisation)	Cochez la case **Log at Beginning of Connection** (journaliser au début de la connexion).

Pour plus d'informations sur les règles de contrôle d'accès, consultez Guide de configuration Cisco Secure Firewall Management Center Device.

Étape 5 Cliquez sur **Add** (ajouter).

Étape 6 En haut de la page, cliquez sur **Save**(Enregistrer) .

Prochaine étape

Consultez Configurer une règle de corrélation pour la correction, à la page 17.

Configurer une règle de corrélation pour la correction

Une règle de corrélation fournit des conditions dans lesquelles le système répond aux menaces. La tâche suivante explique comment configurer une règle de corrélation qui est déclenchée à tout point de la connexion lorsque les conditions de votre règle de contrôle d'accès sont remplies. En particulier, l'exemple de politique et de règle de contrôle d'accès sont déclenchés lorsque le trafic SSH est transmis entre les terminaux source et de destination.

Pour plus d'informations sur les politiques de corrélation, consultez Guide d'administration Cisco Secure Firewall Management Center.

Procédure

Étape 1 Connectez-vous au Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Policies (Politiques)** > **Correlation (Corrélation)**.

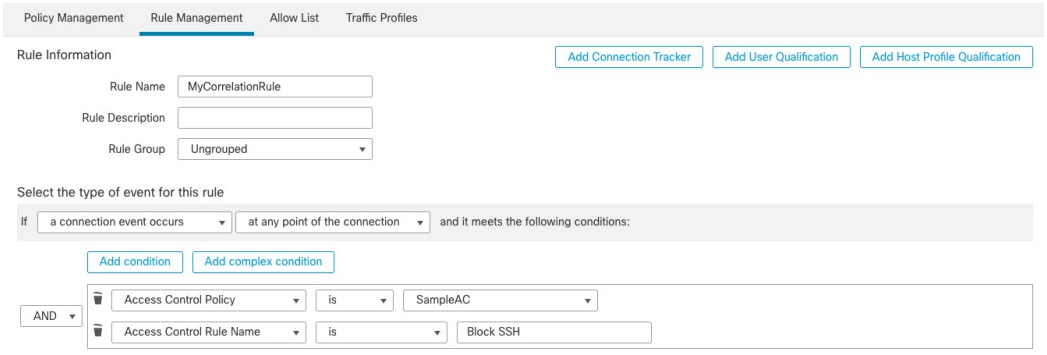
Étape 3 Cliquez sur l'onglet **Rule Management** (gestion des règles).

Étape 4 Cliquez sur **Create Rule** (créer une règle).

Étape 5 Saisissez un nom pour identifier la règle et une description facultative.

Étape 6 Dans la section Select the type of event for this rule (sélectionner le type d'événement pour cette règle), cliquez sur **a connection event occurs** (un événement de connexion se produit) et **at any point of the connection** (à tout point de la connexion).

Étape 7 Configurez le reste de la règle comme le montre la figure suivante.



Remplacez le nom de votre politique de contrôle d'accès et le nom de votre règle par ceux indiqués dans la figure précédente.

Étape 8 Définissez les autres options selon vos besoins et cliquez sur **Save** (Enregistrer).

Prochaine étape

Consultez Associer la règle de corrélation à l'instance du module de correction, à la page 18.

Associer la règle de corrélation à l'instance du module de correction

La dernière étape de la configuration de Firewall Management Center pour la correction et la quarantaine consiste à associer votre règle de corrélation à votre politique de correction. Après avoir fait cela, lorsque Firewall Management Center détecte une menace, les terminaux incriminés sont mis en quarantaine dans l'APIC.

Procédure

Étape 1 Connectez-vous au Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Policies (Politiques)** > **Correlation (Corrélation)**.

Étape 3 Cliquez sur l'onglet **Policy Management** (gestion de la politique).

Étape 4 Cliquez sur **Créer une politique**.

Étape 5 Saisissez le nom de la politique et une description facultative de la politique.

Étape 6 Ne modidiez pas la **priorité par défaut**

Étape 7 Cliquez sur **Add Rules** (ajouter des règles).

Étape 8 Cochez la case à côté du nom de la règle de corrélation que vous avez créée précédemment.

Étape 9 Cliquez sur **Add** (ajouter).

Étape 10 Cliquez sur **Réponses** ( ).

Étape 11 Dans la liste **Unassigned Responses** (réponses non attribuées), cliquez deux fois sur le nom de votre politique de correction pour la déplacer vers **Assigned Responses** (réponses attribuées).

Si le nom de votre politique de correction ne s'affiche pas, revenez à la règle de corrélation et assurez-vous que les noms de la politique de contrôle d'accès et de la règle de contrôle d'accès sont corrects.

Étape 12 Cliquez sur **Update** (mettre à jour).

Étape 13 En haut de la page, cliquez sur **Save**(Enregistrer) .

Étape 14 Déplacez le curseur de la politique de correction sur **Curseur activé** ( ).

Vérifiez la correction dans le Firewall Management Center

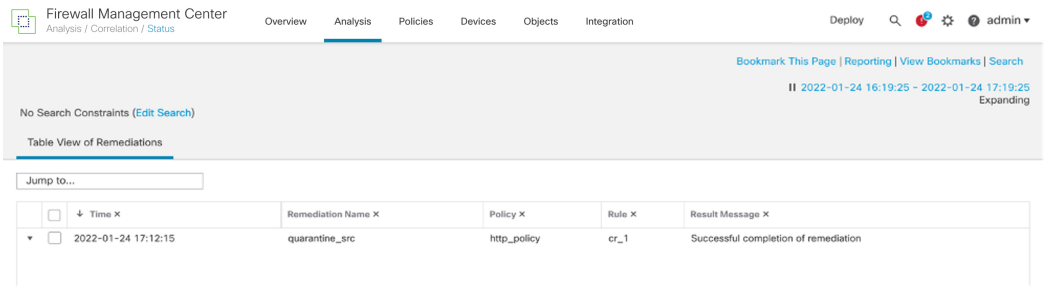
Étant donné que les corrections peuvent échouer pour diverses raisons, effectuez les étapes suivantes pour vérifier qu'aucun message d'erreur n'est répertorié pour l'état de correction sur le Firewall Management Center.

Procédure

Étape 1 Connectez-vous au Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Analysis (Analyse)** > **Correlation (Corrélation)** > **Status (État)**.

Étape 3 Dans le tableau d'état de correction, recherchez la ligne de votre politique et affichez le message de résultat. La figure suivante présente un exemple



Étape 4 La correction a réussi, consultez Vérifier la mise en quarantaine dans l'APIC, à la page 19.

Étape 5 Si une erreur s'affiche, le terminal peut toujours être mis en quarantaine si les événements de correction suivants sont réussis.

Étape 6 Si vous voyez une erreur, consultez Vérifier la mise en quarantaine dans l'APIC, à la page 19 pour vérifier si la mise en quarantaine a réussi ou non. Si la mise en quarantaine a réussi, vous pouvez ignorer tous ses messages d'erreur.

Prochaine étape

Consultez Vérifier la mise en quarantaine dans l'APIC, à la page 19.

Vérifier la mise en quarantaine dans l'APIC

Avant de commencer

Effectuez les tâches décrites en Vérifiez la correction dans le Firewall Management Center, à la page 18.

Procédure

Étape 1 Connectez-vous à l'APIC.

Étape 2 Cliquez sur la page **Tenants** (détenteurs).

Étape 3 Cliquez sur **ALL TENANTS** (tous les détenteurs).

Étape 4 Cliquez deux fois sur le nom du détenteur compromis.

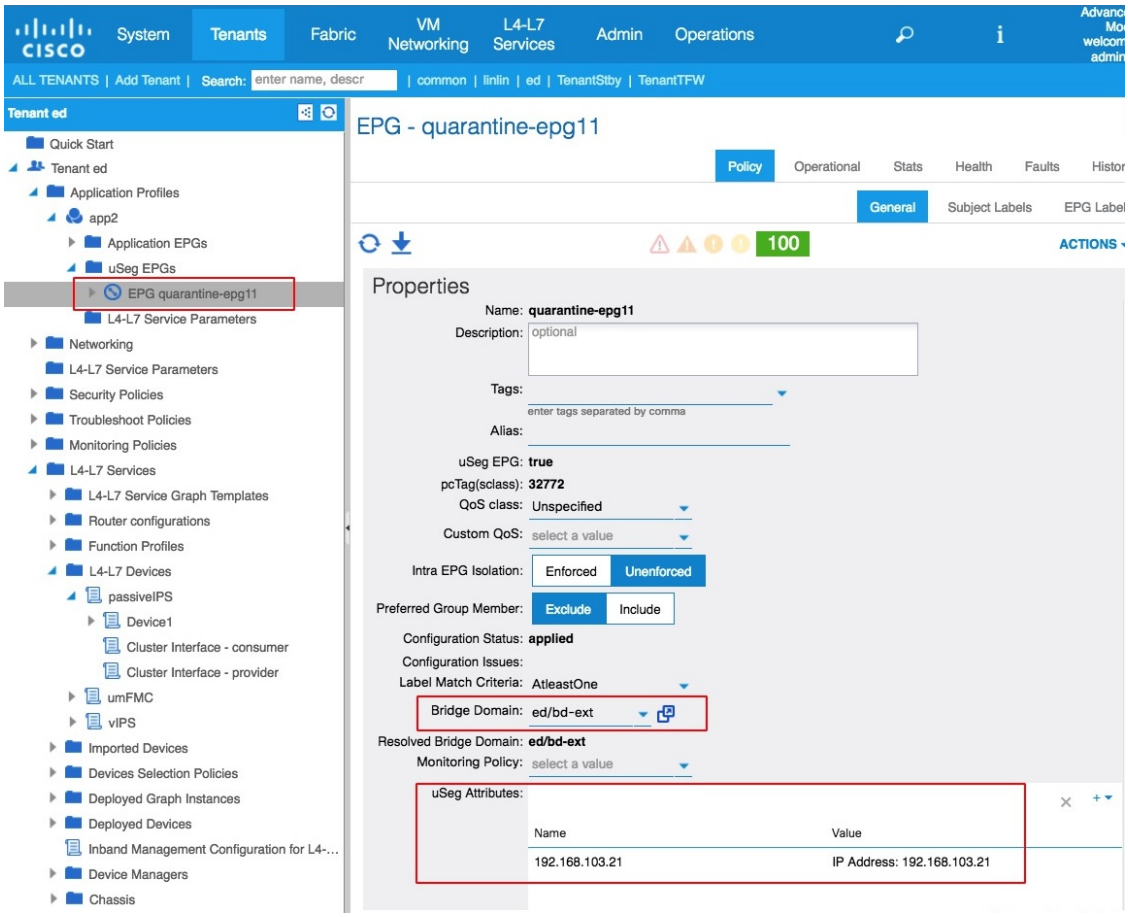
Étape 5 Développez l'application compromise dans le volet de gauche.

Étape 6 Cliquez sur **uSeg EPGs** (GPT uSeg)

Étape 7 Cliquez sur la quarantaine GPT pour le terminal en quarantaine.

Étape 8 Dans le volet de droite, cliquez sur **Policy (politique)** > **General (générale)**.

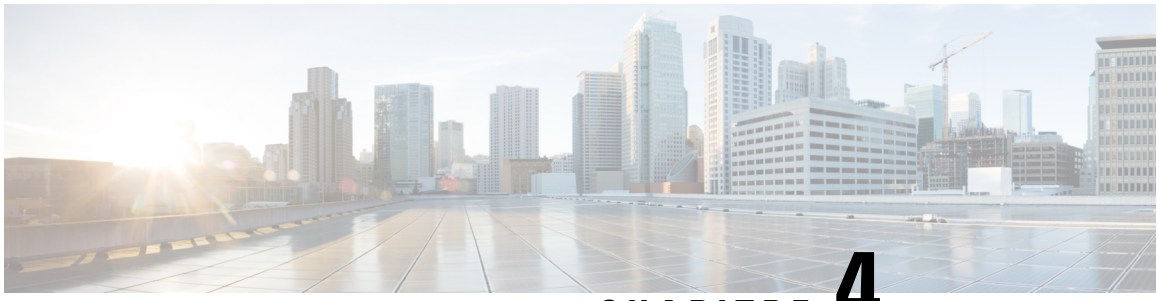
Étape 9 Vérifiez qu'un ou plusieurs attributs uSeg ont été créés sur le serveur APIC .
La figure suivante présente un exemple.



La figure montre qu'un périphérique à l'adresse IP 192.168.103.21 a été mis en quarantaine.

Remarque
Pour VMware DVS et Bare Metal (ordinateur sans système d'exploitation) (en mode pont), deux attributs (filtres) sont automatiquement créés lorsqu'un terminal est mis en quarantaine : un attribut pour l'adresse IP et un attribut pour l'adresse MAC. Par conséquent, pour supprimer la quarantaine, vous devez supprimer les deux attributs.

Étape 10 Si aucun attribut uSeg n'a été créé, mais que vous savez que les conditions définies par une règle de corrélation ont été remplies, la quarantaine a échoué. Pour mettre manuellement l'adresse IP en quarantaine , consultez Survol de la mise en quarantaine manuelle d'une adresse IP, à la page 21.



CHAPITRE 4

Mettre manuellement en quarantaine une adresse IP

En cas d'échec de votre quarantaine , vous pouvez mettre manuellement en quarantaine une ou plusieurs adresses IP, comme indiqué dans les rubriques suivantes.

- Survol de la mise en quarantaine manuelle d'une adresse IP, à la page 21
- Rechercher une adresse IP à mettre en quarantaine, à la page 21
- Créer un attribut GPT uSeg, à la page 22
- Vérifier la mise en quarantaine manuelle de l'adresse IP, à la page 23

Survol de la mise en quarantaine manuelle d'une adresse IP

Si une mise en quarantaine échoue, comme indiqué dans les sections précédentes de ce guide, vous pouvez effectuer manuellement la mise en quarantaine d'une adresse IP. Vous devez trouver l'adresse IP et l'adresse MAC à mettre en quarantaine. L'adresse IP est affichée dans le Cisco Secure Firewall Management Center et l'adresse MAC est affichée dans l'APIC.

Rechercher une adresse IP à mettre en quarantaine

Cette rubrique explique comment consulter les journaux de corrélation dans le Firewall Management Center pour trouver une adresse IP à mettre en quarantaine.

Procédure

Étape 1 Connectez-vous au Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Analysis (Analyse)** > **Correlation (Corrélation)** > **Status (État)**.

Étape 3 Recherchez l'horodatage de l'entrée pour la quarantaine infructueuse et notez l'adresse IP source.

Étape 4 Connectez-vous à l'APIC si vous ne l'avez pas encore fait.

Étape 5 Dans la page de l'onglet des opérations, cliquez sur **EP Tracker**, saisissez l'adresse IP et appuyez sur Enter (Entrée).

Étape 6 Si aucune information ne s'affiche, le terminal ne peut pas être mis en quarantaine. Si plusieurs adresses IP s'affichent, recherchez celle du détenteur incriminé.

Prochaine étape

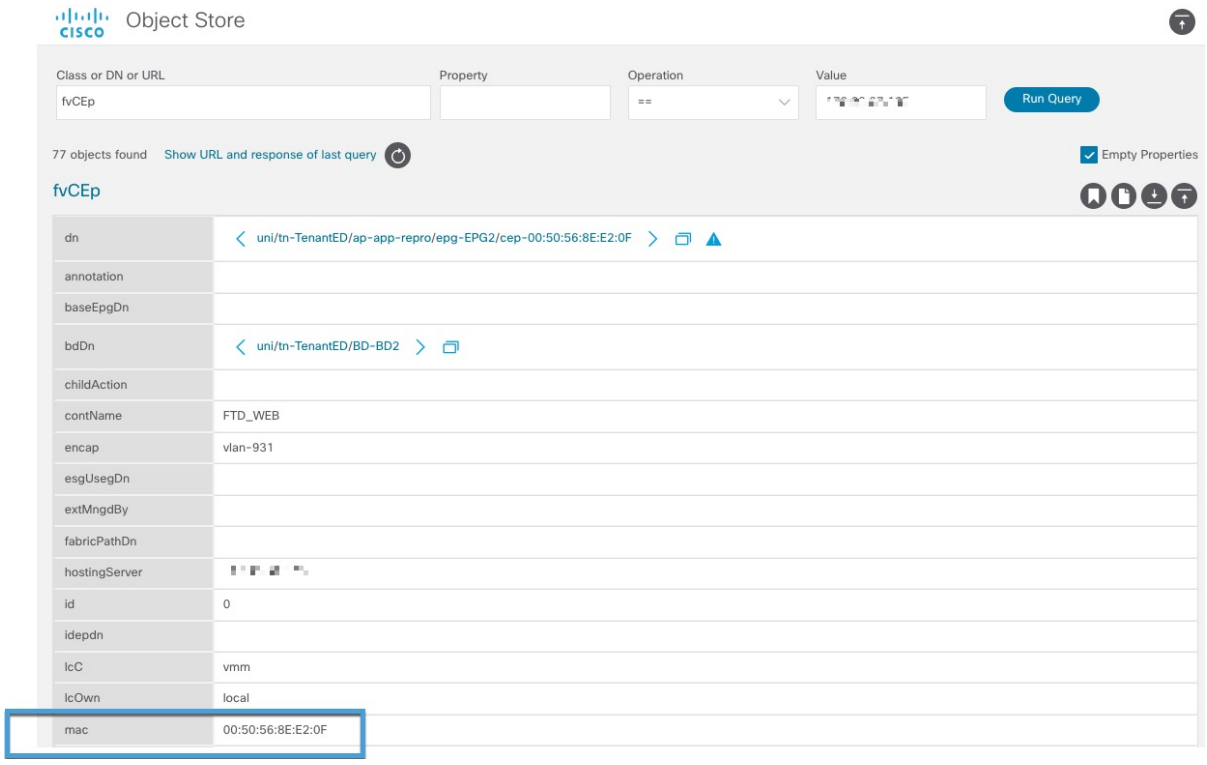
Créer un attribut GPT uSeg, à la page 22

Créer un attribut GPT uSeg

Si vous pouvez identifier le GPT du terminal que vous souhaitez mettre en quarantaine, créez un attribut uSeg GPT (GPT uSeg) correspondant à ce terminal.

Procédure

Étape 1 Pour trouver l'adresse MAC correspondant à l'adresse IP à mettre en quarantaine, accédez au navigateur du magasin d'objets de l'APIC à l'adresse https: //*apic_IP_address*/**visore.html**. Utilisez l'adresse IP du terminal pour exécuter une requête et afficher l'adresse MAC.
La figure suivante présente un exemple.



Étape 2 Ouvrez une session dans APIC si ce n'est pas déjà fait.

Étape 3 Cliquez sur **Tenants (Détenteurs)** > **ALL TENANTS (tous les détenteurs)**.

Étape 4 Cliquez deux fois sur le détenteur qui contient le terminal à mettre en quarantaine.

Étape 5 Développez **Networking (Réseautage)** > **Bridge Domains (Domaines de pont)**.

Étape 6 Relevez le domaine de pont du GPT.

Étape 7 Développez **Application Profiles (Profils d'application)** > ***profile-name (nom-du-profil)*** > **Application EPGs (GPT d'application)** > ***epg-name (nom-du-gpt)*** et relevez le nom du profil de domaine.

Étape 8 Développez **Application Profiles** (Profils d'application) et cliquez avec le bouton droit sur **uSeg EPG** (GPT uSeg).

Étape 9 Cliquez sur **Create uSeg EPG** (Créer un GPT uSeg).

Étape 10 Saisissez un nom pour le GPT uSeg, au format **uSegEPG***endpoint-name* (nom-du-terminal). (Par exemple, **uSegEPG-EPG1**.)

Étape 11 Dans la liste **Bridge Domain** (domaine de pont), cliquez sur le domaine de pont du GPT .

Étape 12 Cliquez sur **Next** (suivant).

Étape 13 Sur la page Domains (Domaines), cliquez sur **Ajouter** (+).

Étape 14 Dans la liste **Domain Profiles** (Profils de domaine), cliquez sur le profil du domaine.

Étape 15 Définissez **Deployment Immediacy** (Immédiateté de déploiement) sur **Immediate** (Immédiat).

Étape 16 Définissez **Resolution Immediacy** (Immédiateté de résolution) sur **Immediate** (Immédiat).

Étape 17 Ajoutez un attribut de filtre IP en cliquant sur **Ajouter** (+) dans le coin inférieur droit et saisissez l'adresse IP pour le nom et le filtre.

Étape 18 Cliquez sur **Update** (Mettre à jour), puis sur **Finish** (Terminer).

Si le GPT uSeg ne s'affiche pas, actualisez la page de votre navigateur.

Étape 19 Cliquez sur **uSeg Attributes** (Attributs uSeg).

Étape 20 Cliquez sur **Ajouter** (+)

Étape 21 Ajoutez des attributs pour l'adresse IP et l'adresse MAC de l'hôte en quarantaine, avec l'opérateur **Match Any** (Correspondre à n'importe lequel).

Pour le filtre IP, utilisez l'adresse IP comme nom. Pour le filtre MAC, utilisez l'adresse IP, suivie d'un trait de soulignement et des trois derniers octets de l'adresse MAC comme nom.

Étape 22 Faites un clic droit sur **Domains** (Domaines) – VMs and Bare Metals (Machines virtuelles et ordinateurs sans système d'exploitation) sous le nouveau uSeg GPT créé, puis ajoutez une association de domaine portant le même nom et le même type de domaine que le GPT d'origine.

Étape 23 Pour Bare Metal (ordinateur sans système d'exploitation), cliquez avec le bouton droit sur **Static Leafs** (feuilles statiques), puis cliquez sur **Static Link with Node** (lier statiquement à un nœud).

Étape 24 Cliquez sur **Submit** (soumettre).

Prochaine étape

Vérifier la mise en quarantaine manuelle de l'adresse IP, à la page 23

Vérifier la mise en quarantaine manuelle de l'adresse IP

Vérifiez qu'aucun trafic ne peut entrer ou sortir du terminal mis en quarantaine.

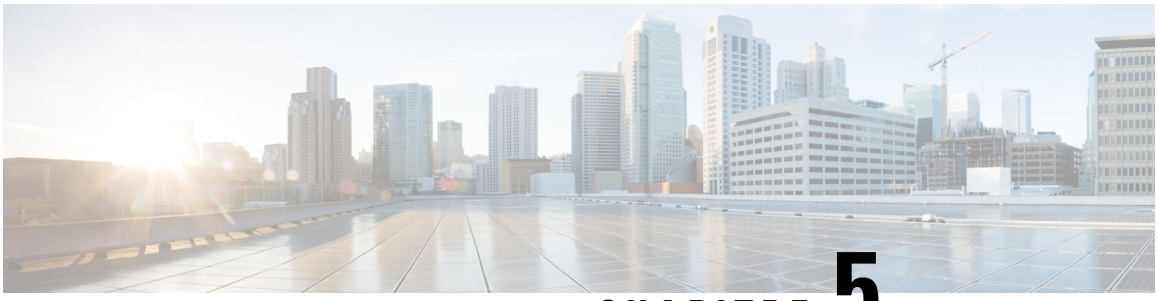
Avant de commencer

Procédure

Étape 1 Effectuez une tâche comme envoyer un message Ping à une adresse IP en quarantaine.

L'opération doit échouer.

Étape 2 Si le Ping réussit, vérifiez les adresses IP et MAC du terminal à mettre en quarantaine, puis réessayez.



CHAPITRE 5

Documentation associée

• Documentation associée, à la page 25

Documentation associée

Pour des renseignements supplémentaires sur Cisco APIC/Cisco Secure Firewall Remediation Module, consultez le guide approprié.

Pour des informations supplémentaires sur l'APIC et ACI de Cisco, consultez la documentation de l'APIC.

Pour savoir comment utiliser l'outil Cisco Bug Search Tool (BST), soumettre une demande de service et consulter la base de connaissances Support Case Manager, reportez-vous au Support Case Manager (Gestionnaire de dossiers d'assistance).

Documentation associée

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.