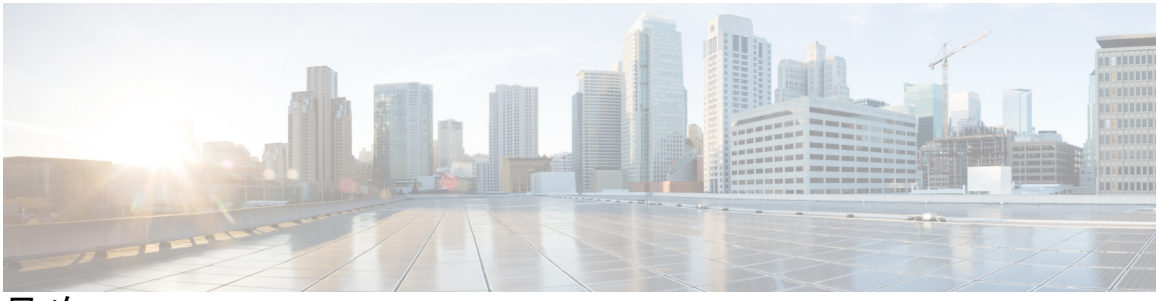
APIC/Secure Firewall 修復モジュール 3.0

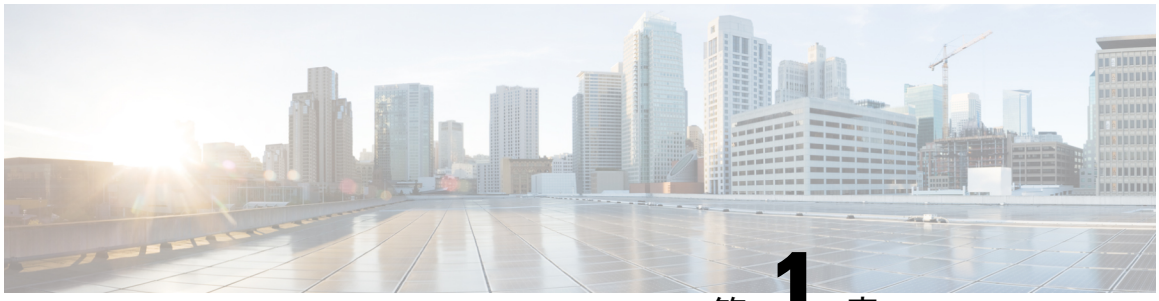
最終更新：2026 年 2 月 9 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

修復モジュールについて

修復モジュールについて

APIC/Secure Firewall Remediation Module を使用すると、ネットワークへの攻撃が Firewall Management Center によって検出された場合、問題のある端末を Application Policy Infrastructure Controller（APIC）で完全に検疫できるようになります。これにより、その端末との間でそれ以上の通信が許可されなくなります。次の図に、修復モジュールをインストールした場合の Firewall Management Center と APIC の関係を示します。

互換性

次の表に APIC/Secure Firewall Remediation Module、Firewall Management Center、および APIC 間の互換性を示します。

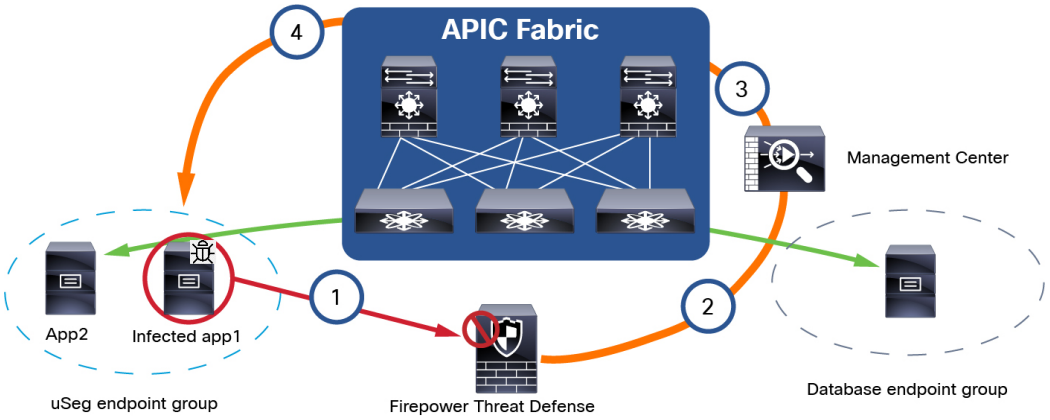
表 *1* : 修復モジュール、*Firewall Management Center*、および *APIC* との互換性

次と互換性がある修復モジュールのバージョン	Firewall Management Center バージョン	APIC のバージョン
3.0	7.0 以降	5.1(1h)

感染した端末

次の図に、感染した端末が検出されたときの APIC/Secure Firewall Remediation Moduleの対応を示します。

修復モジュールについて



そのプロセスは次のとおりです。

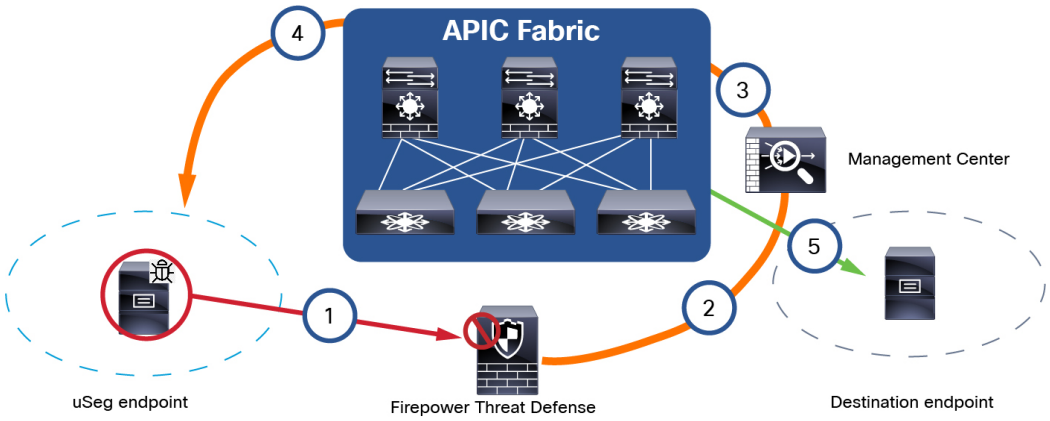
1. 端末グループ（左側の端末グループ）内のアプリケーションが感染している端末が、データベース EPG 内の別の端末に対して攻撃を開始します。攻撃は、管理対象デバイス（Firepower Threat Defense を実行している物理デバイスまたは仮想デバイスなど）によってインラインでブロックされます。
2. 攻撃イベントが生成され、Firewall Management Center に送信されます。攻撃イベントには、感染した端末に関する情報が含まれます。
3. 攻撃イベントは APIC の修復モジュールをトリガーし、APIC ノースバウンド（NB）API を使用して、ACI ファブリック内の感染した端末を封じ込めます。
4. APIC は、感染したアプリケーションワークロードを隔離されたマイクロセグメント（uSeg）EPG に迅速に封じ込めるか、検疫します。

   App2 は感染していないため、引き続きネットワーク上での通信が可能です。

   次のセクションで示すように、送信元端末、接続先端末、またはその両方を検疫できます。

送信元端末と接続先端末、またはそのいずれかの検疫

感染した端末が検出されたら、次の図に示すように、送信元端末、接続先端末、またはその両方を任意に検疫できます。



図に次のプロセスを示します。

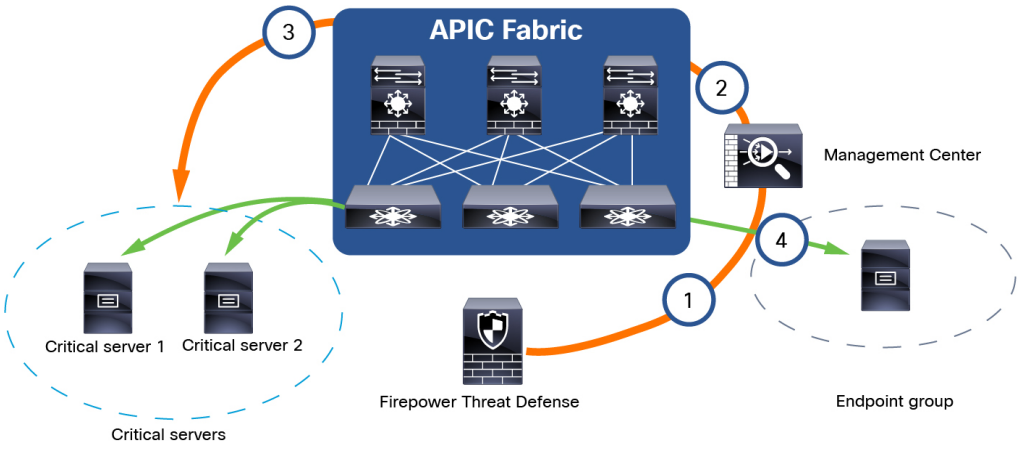
1. 端末グループ（EPG）内のアプリケーションが感染している端末が、別のEPG内の別の端末に対して攻撃を開始します。攻撃は、管理対象デバイス（Firepower Threat Defense を実行している物理デバイスまたは仮想デバイスなど）によってインラインでブロックされます。
2. 攻撃イベントが生成され、Firewall Management Center に送信されます。攻撃イベントには、感染した端末に関する情報が含まれます。
3. 攻撃イベントは APIC の修復モジュールをトリガーし、APIC ノースバウンド（NB）API を使用して、ACI ファブリック内の感染した端末を封じ込めます。
4. APICは、感染したアプリケーションワークロードを隔離されたマイクロセグメント（uSeg）EPG に迅速に封じ込めるか、検疫します。
5. 設定に応じて、送信元端末、接続先端末、または両方の端末を検疫できます。

   図に示す例では、uSeg（送信元）端末を検疫しますが、接続先端末は検疫しません。

重要なサーバーへの通信を常に許可

重要なサーバーが不審と見なされる通信を通過させている場合でも、これらのサーバーとの通信を許可できます。このオプションは注意して使用する必要がありますが、常にこの通信を許可したい場合に便利です。

次の図は例を示しています。



図に次のプロセスを示します。

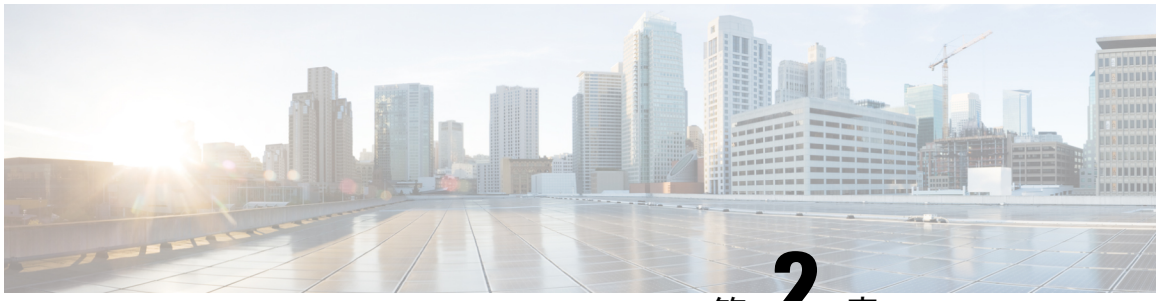
1. 端末グループ内の端末が、重要なサーバーとして指定されたサーバーに通信を転送します（これらのサーバーは IP アドレスで指定する）。
2. Firewall Management Center は、相関ルールに一致していても、この通信を無視します。
3. 通信の内容にかかわらず、端末グループ内の重要なサーバーと重要なサーバーとの間の通信は常に許可されます。

サポートされる機能

このリリースでは、APIC バージョン 5.1(1h) を使用して、APIC/Secure Firewall Remediation Moduleによって検出された問題のある端末を検疫できます。修復モジュールのバージョン 3.0 について、端末の検疫時にサポートされる動作を次の表に示します。

	VMware 分散仮想スイッチ（DVS）	**ベアメタル**
IPS インラインモードで検証済み	対応	対応
EPG ブリッジモード	対応	対応
EPG ルーテッドモード	非対応	非対応
複数の IP から 1 つの MAC のチェック	対応	対応
IP アドレスフィルタ uSeg 属性のみを作成	非対応	非対応
IP アドレスフィルタと MAC アドレスフィルタ uSeg 属性の両方の作成	対応	対応
送信元端末と接続先端末の検疫	対応	対応

	VMware 分散仮想スイッチ（DVS）	ベアメタル
送信元端末と接続先端末への事前定義された管理コントラクトの適用	対応	対応
検疫された端末から L3Out 端末グループへの通信を許可	対応	対応
監査のみを許可	対応	対応
重要なサーバーへの通信を常に許可	対応	対応



第 2 章

APIC/Secure Firewall Remediation Moduleのダウンロードとインストール

次のセクションの説明に従って APIC/Secure Firewall Remediation Moduleをダウンロードし、Secure Firewall Management Center にインストールします。

APIC/Secure Firewall Remediation Moduleのダウンロードとインストール

始める前に

次の表に示す互換性のあるバージョンを使用していることを確認します。

表 *2 :* 修復モジュール、*Firewall Management Center*、および *APIC* との互換性

次と互換性がある修復モジュールのバージョン	Firewall Management Center バージョン	APIC のバージョン
3.0	7.0 以降	5.1(1h)

手順

ステップ 1 Firewall Management Center に接続するマシンに APIC/Secure Firewall Remediation Moduleをダウンロードします。

- FMC：https://software.cisco.com/download/home/278875421。モデルを選択し、[**Firepower Management Center Remediation Modules**] を選択してから [**ACI**] を選択します。
- FMCv：https://software.cisco.com/download/home/286259687/type/286311510/release/Tetration。[**ACI**] を選択します。

APIC/Secure Firewall Remediation Moduleのダウンロードとインストール

ステップ 2 まだ Firewall Management Center にログインしていない場合は、ログインします。

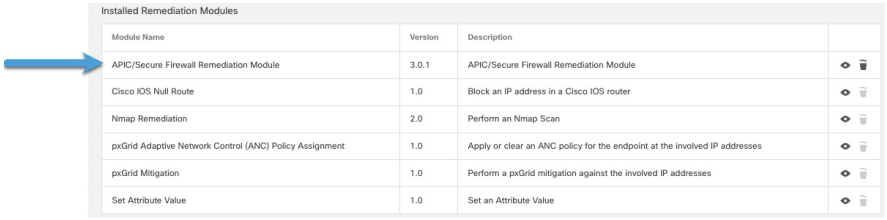
ステップ 3 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[モジュール（Modules）]** をクリックします。

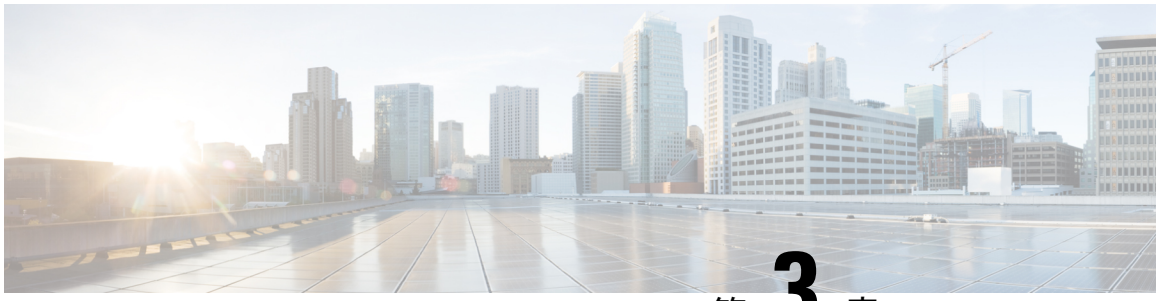
ステップ 4 [Install a New Module] セクションで [**Browse**] をクリックします。

ステップ 5 プロンプトに従って修復モジュールをアップロードします。

ステップ 6 [Install（インストール）] をクリックします。

ステップ 7 インストールが成功すると、インストールされている修復モジュールの一覧にAPIC/Secure Firewall Remediation Moduleが表示されます。





第 3 章

修復と検疫

この章では、端末を修復および検疫するルールを作成するために、APIC および Secure Firewall Management Center で実行する必要があるタスクについて説明します。

修復および検疫プロセス

修復（端末を検疫する必要がある状況を定義）と検疫（ネットワーク上で通信できないように端末を隔離）は、次のセクション、「修復と検疫の方法 （9 ページ）」で概説する複数のステップからなるプロセスです。

修復と検疫の方法

以下に、端末を修復して検疫するために必要なタスクの概要を示します。APIC で、また Firewall Management Center でいくつかのタスクを実行します。

始める前に

APIC 関連の概念を理解するには、『*Endpoint Groups (EPG) Usage and Design*』ホワイトペーパーや『*Cisco APIC Basic Configuration Guide*』などの参考資料を参照してください。

手順の概要

1. オプションで、管理コントラクトおよび管理コントラクト端末グループ（EPG）を作成します。

2. 修復モジュールのインスタンスとタイプを作成します。
3. 端末を検疫する条件を決定するアクセス制御ルールを設定します。
4. 相関ルールを修復ポリシーに関連付けます。
5. 検疫と修復を確認します。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	オプションで、管理コントラクトおよび管理コントラクト端末グループ（EPG）を作成します。	APIC でこのタスクを実行します。 APIC では、許可する通信を明示的に定義する許可リストモデルが使用されます。コントラクトは、EPG 間の通信を定義するために使用するポリシー構造です。 このオプション設定により、検疫済みの uSeg EPG への接続を開始できます。詳細については、「オプションでの管理コントラクトおよびコントラクト EPG の作成 （13 ページ）」を参照してください。
ステップ 2	修復モジュールのインスタンスとタイプを作成します。	Firewall Management Center でこのタスクを実行します。 修復モジュールによって、検疫済みの端末を表示して操作できる EPG が APIC で作成されます。修復モジュールでは次のことができます。 • 送信元端末、接続先端末、またはその両方の検疫 • 管理 EPG の参照 • 修復をトリガーしたり、実稼働通信に影響を与えたりすることのない、修復アクティビティのみの監査 詳細については、「修復モジュールのインスタンスとタイプの作成 （14 ページ）」を参照してください。
ステップ 3	端末を検疫する条件を決定するアクセス制御ルールを設定します。	Firewall Management Center でこのタスクを実行します。 セキュアでない通信の通過など、端末を検疫する条件を決定します。以前に設定した修復ポリシーをトリガーするアクセス制御ルールを設定します。

	コマンドまたはアクション	目的
		詳細については、「修復のためのアクセス制御ルールの設定 （17 ページ）」を参照してください。
ステップ 4	相関ルールを修復ポリシーに関連付けます。	Firewall Management Center でこのタスクを実行します。 これにより、APIC で検疫がトリガーされます。詳細については、「相関ルールと修復モジュールインスタンスとの関連付け （20 ページ）」を参照してください。
ステップ 5	検疫と修復を確認します。	APIC で検疫を確認し、Firewall Management Center で修復を確認します。 詳細については、「APIC での検疫の確認 （21 ページ）」および「Firewall Management Center での修復の確認 （20 ページ）」を参照してください。

次のタスク

オプションの管理コントラクトおよびコントラクト EPG の作成 （11 ページ）

オプションの管理コントラクトおよびコントラクト EPG の作成

オプションで、共通テナントで APIC 通信フィルタリングコントラクトを、mgmt テナントで管理 EPG を事前定義して、検疫された uSeg EPG への接続を開始できます。このオプション設定を使用するには、**mgmt** テナントで APIC の管理 EPG を定義し、**common** テナントでコントラクトを定義する必要があります。

詳細については、『*Cisco APIC Basic Configuration Guide*』を参照してください。

次の作業

オプションの管理コントラクトとコントラクト EPG を作成するための前提条件 （11 ページ）。

オプションの管理コントラクトとコントラクト EPG を作成するための前提条件

このタスクでは、オプションの管理コントラクトおよびコントラクト EPG を設定する前に次の手順を実行する方法について説明します。

- アプリケーション ESG を作成します。
- 実行する検疫のフィルタを作成します。この例では、フィルタは SSH2 通信用です。

手順

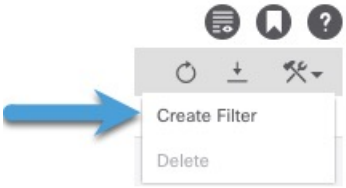
ステップ 1 APIC にログインします。

ステップ 2 **Tenants** をクリックします。

ステップ 3 [**common**] をダブルクリックします。

ステップ 4 左ペインで **[Contracts** > **Filters]** を展開します。

ステップ 5 右ペインで [**Create Filter**] をクリックします。



ステップ 6 フィルタに、[**Name**] として [**SSHv2**] を指定します。

ステップ 7 **[送信（Submit）]** をクリックします。

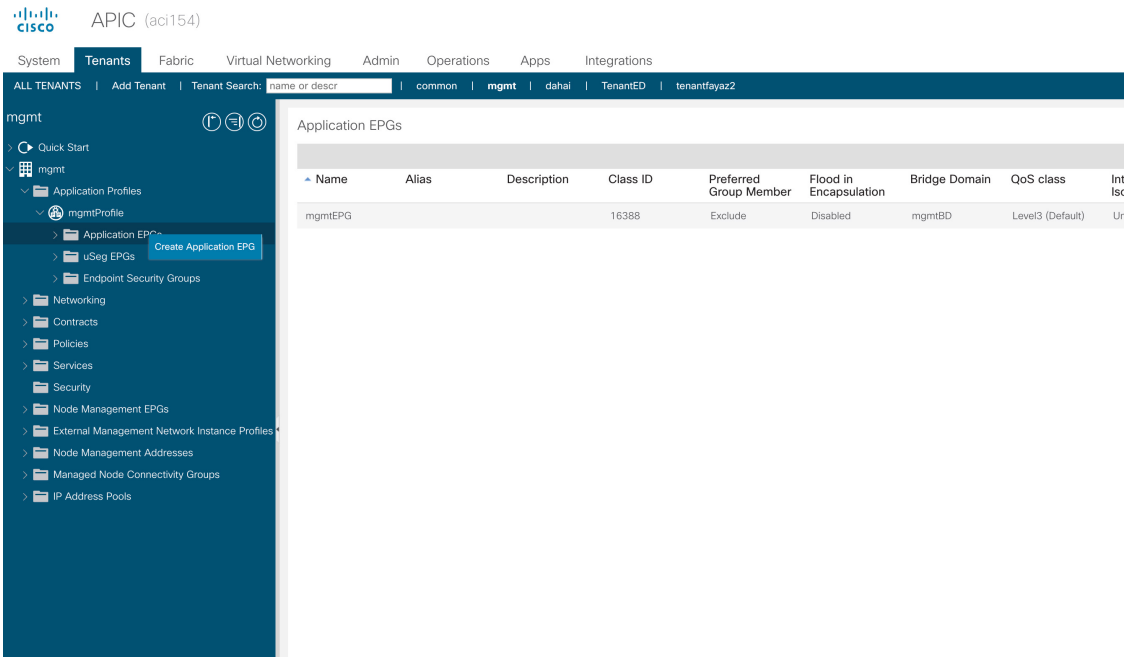
ステップ 8 左ペインで **[Tenants** > **ALL TENANTS]** をクリックします。

ステップ 9 [**mgmt**] をクリックします。

ステップ 10 **[Application Profiles** > **mgmt profile]** を展開します。

ステップ 11 **Application EPGs** を右クリックし、**Create Application EPG** をクリックします。

次の図は例を示しています。



ステップ 12 EPG の [**Name**] を指定します。

ステップ 13 [**Bridge Domain**] リストで [WHICH BRIDGE DOMAIN] をクリックします。

ステップ 14 [終了（Finish）] をクリックします。

次のタスク

オプションでの管理コントラクトおよびコントラクト EPG の作成 （13 ページ）

オプションでの管理コントラクトおよびコントラクト EPG の作成

コントラクトを作成しない場合は、このセクションをスキップして「修復モジュールのインスタンスとタイプの作成 （14 ページ）」に進みます。

手順

ステップ 1 APIC にログインします。

ステップ 2 [**ALL TENANTS**] をクリックします。

ステップ 3 [**common**] をダブルクリックします。

ステップ 4 **[Contracts > Standard]** を展開します。

ステップ 5 [**Standard**] を右クリックし、[**Create Contract**] をクリックします。

ステップ 6 [**Name**] フィールドに「**`useg_filter_contract`**」と入力します。

ステップ 7 [**Scope**] リストの [**Global**] をクリックします。

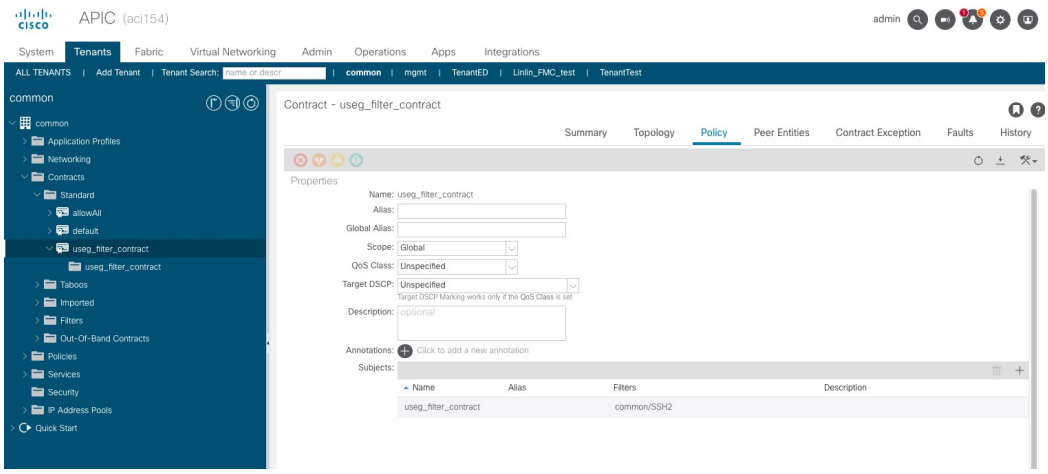
ステップ 8 必要に応じてその他の選択を行います。

ステップ 9 **[送信（Submit）]** をクリックします。

ステップ 10 [**useg_filter_contract**] をクリックします。

ステップ 11 右ペインで [**Policy**] タブをクリックします。

次の図は例を示しています。



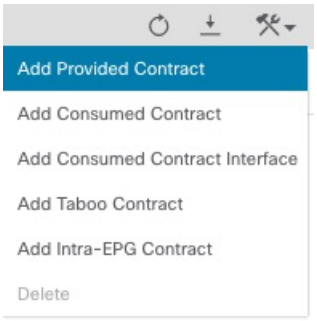
ステップ 12 [**ALL TENANTS**] をクリックします。

ステップ 13 [**mgmt**] をダブルクリックします。

ステップ 14 [**mgmt** > **Application Profiles** > **mgmtProfile** > **Application EPGs** > **mgmtEPG**] > を展開します。

ステップ 15 [コントラクト（Contracts）] をクリックします。

ステップ 16 [**Add Provided Contract**] をクリックします。



ステップ 17 [**Contract**] リストの [**useg_filter_contract**] をクリックします。

ステップ 18 **[送信（Submit）]** をクリックします。

次のタスク

修復モジュールのインスタンスとタイプの作成 （14 ページ） を参照してください。

修復モジュールのインスタンスとタイプの作成

Secure Firewall Management Center で脅威を検出し、APIC に通知して脅威を検疫できるようにするには、Secure Firewall Management Center で修復モジュールのインスタンスとタイプを設定する必要があります。修復の詳細については、『Cisco Secure Firewall Management Center アドミニストレーションガイド』を参照してください。オプションで、送信元端末、接続先端末、またはその両方を検疫することを選択できます。

端末を検疫せずに端末の監査のみを行うことも選択できます。

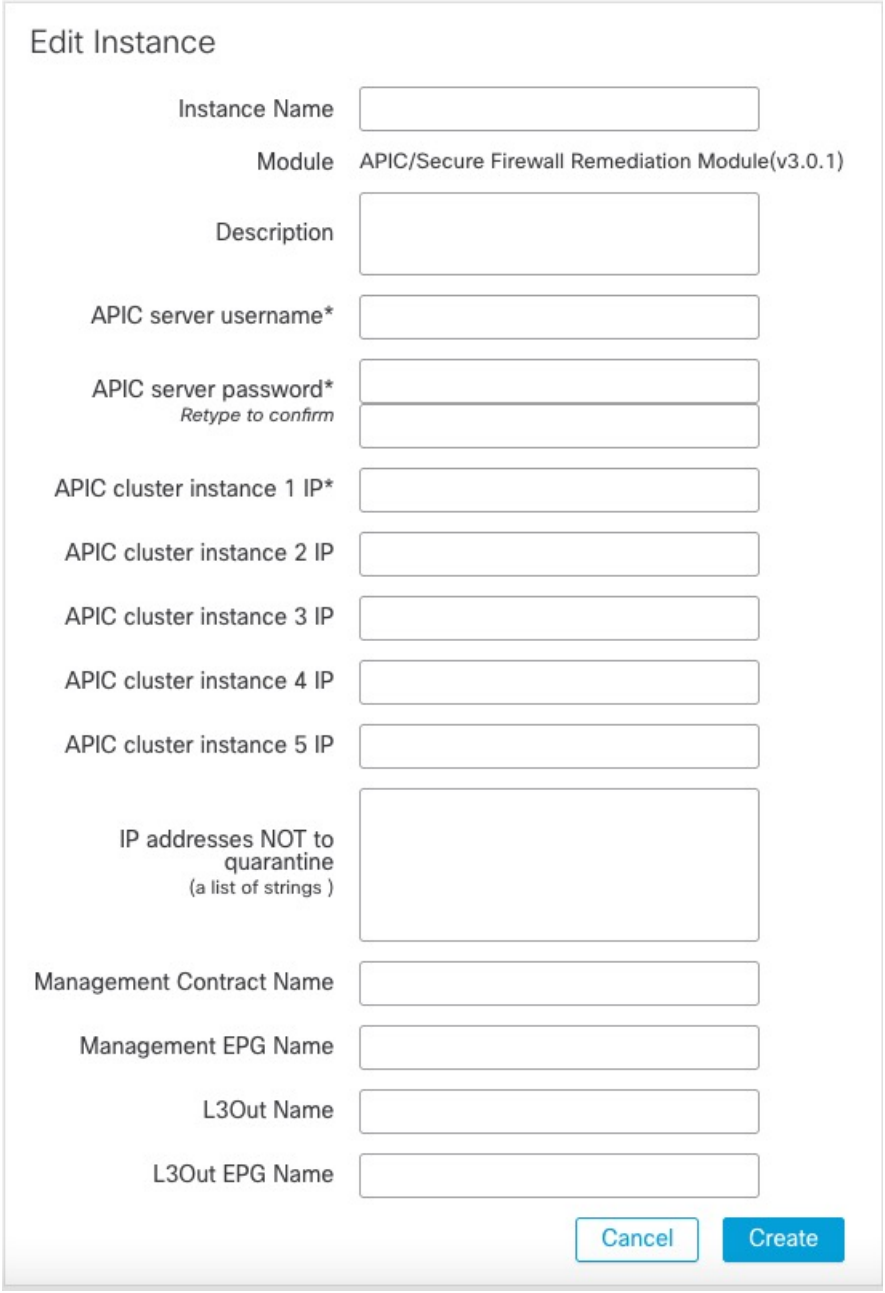
手順

ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]** をクリックします。

ステップ 3 [**Select a module type**] リストで [**APIC/Cisco Secure Firewall Remediation Module (3.0.1)**] をクリックします。

ステップ 4 [追加（Add）] をクリックします。
次のように [Edit Instance] ページが表示されます。



ステップ 5 次の情報を入力します。

項目	説明
インスタンス名（Instance name）	このインスタンスを識別するための名前を入力します（名前にスペースは使用できない）。
説明	（オプション）説明を入力します。
[**APIC server username**]	管理者権限を持つ APIC ユーザーのユーザー名を入力します。

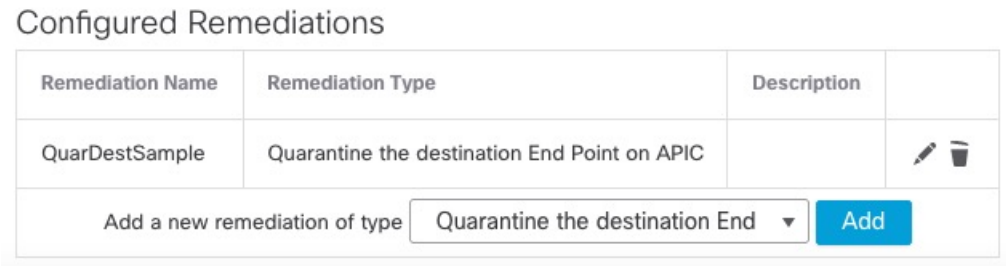
項目	説明
[**APIC server password**]	ユーザーのパスワードを 2 回入力します。
[**APIC cluster instance 1 IP**]	APIC サーバーまたはクラスター内の最初のサーバーの IP アドレスを入力します。
[**APIC cluster instance x IP**]	（オプション）APIC クラスターに複数のサーバーがある場合は、提供されたフィールドに追加の IP アドレスを入力します。
[**IP addresses NOT to quarantine**]	（オプション）検疫から常に除外する個々の IP アドレスのリストを入力します。IPアドレスは Enter で区切ります。 サブネットマスクは指定できません。
[**Management Contract Name**]	（オプション）APIC で作成した管理コントラクトの名前を入力します。 詳細については、「オプションの管理コントラクトおよびコントラクト EPG の作成 （11 ページ）」を参照してください。
[**Management EPG Name**]	（オプション）管理コントラクトが関連付けられている EPG の名前を入力します。 詳細については、「オプションの管理コントラクトおよびコントラクト EPG の作成 （11 ページ）」を参照してください。
[**L3Out Name**]	（オプション）APIC で設定された L3Out ターゲットの名前。[**L3Out Name**] に値を入力する場合は、[**L3Out EPG Name**] にも値を入力する必要があります。 L3Out ターゲットの検疫された端末と送信元端末グループ間の通信をドロップし、検疫された端末からの通信をフォレンジック分析のために許可します。
[**L3Out EPG Name**]	（オプション）APIC で設定された L3Out 端末グループ（EPG）の名前。[**L3Out EPG Name**] に値を入力する場合は、[**L3Out Name**] にも値を入力する必要があります。
[**Audit-only**]	[**Off**]（デフォルト）：感染した端末を検疫し、相関ステータスメッセージを Firewall Management Center に送信します。 [**On**]：感染した端末を検疫せずに、相関ステータスメッセージを Firewall Management Center に送信します（[**[分析（Analysis）] > [相関（Correlation）] > [相関イベント（Correlation Events）]**]）。

ステップ 6 ページの下部にある [Configured Remediation] セクションで、次のいずれかをクリックしてから [**Add**] をクリックします。

- [**Quarantine the destination End Point on APIC**]
- [**Quarantine the source End Point on APIC**]

修復名にスペースを含めることはできません。

次に、修復を示す [Configured Remediation] セクションの例を示します。



ステップ 7 [Edit Remediation] ページに以下の情報を入力します。

- [**Remediation Name**]：修復インスタンスを識別するための名前を入力します。
- （オプション）[**Description**]：修復インスタンスの説明を入力します。

ステップ 8 [作成（Create）] をクリックします。

ステップ 9 [完了（Done）] をクリックします。

ステップ 10 [Edit Instance] ページで、オプションで別の修復を設定します。

次のタスク

修復のためのアクセス制御ルールの設定 （17 ページ） を参照してください。

修復のためのアクセス制御ルールの設定

この例では、SSHプロトコルをブロックするアクセス制御ルールを作成する方法を示します。このルールを作成した後、モニター対象の EPG 内の別の端末に SSH を試みるすべての端末、つまり問題のあるノードまたはノードが検疫されます。

手順

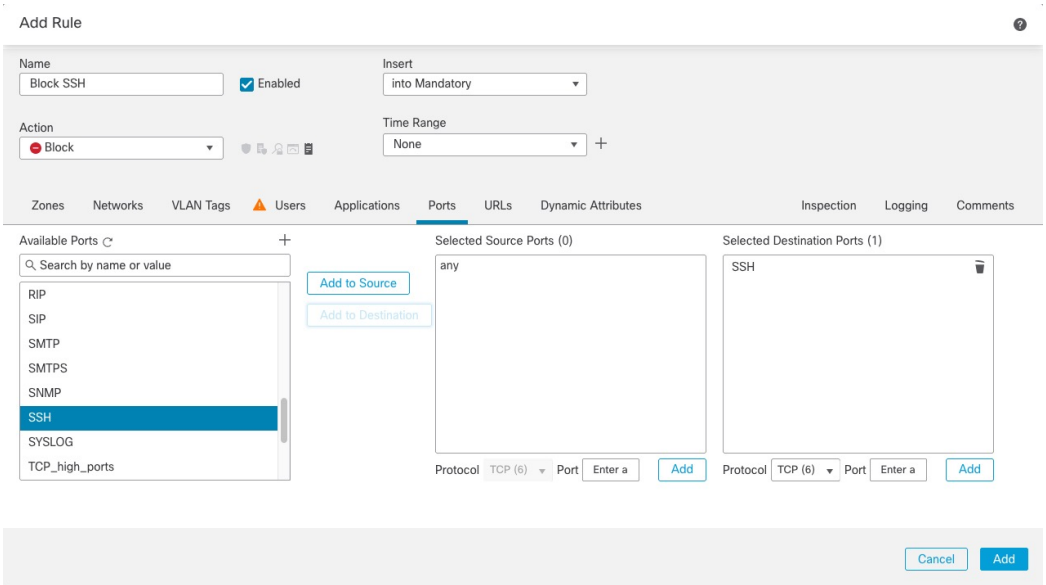
ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** をクリックします。

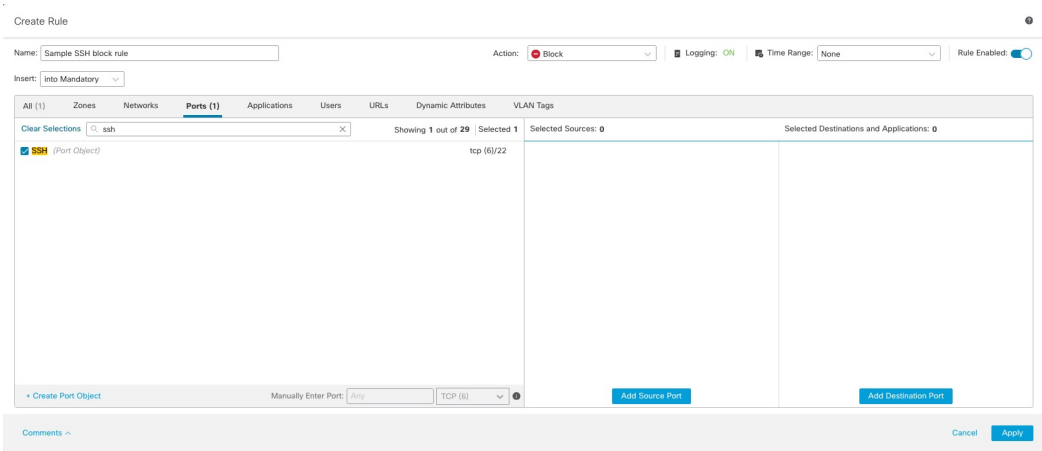
ステップ 3 新しいアクセス制御ポリシーを作成するか、[[編集（Edit）]（）] をクリックして既存のポリシーを編集します。

ステップ 4 既存のポリシーを編集している場合は、[**Add Rule**] をクリックしてルールを追加します。

次の情報を入力します（Firewall Management Center バージョン 7.2 以前）。



次の情報を入力します（Firewall Management Center バージョン 7.3 以降）。



項目	説明
[Name] フィールド	このルールを識別する名前を入力します。後で必要になるため、名前を書き留めてください。
[**Action**] リスト	[**Block**] をクリックします。
[**Ports**] タブページ	[**Available Ports**] リストから SSH までスクロールし、[**Add to Destination**] をクリックします。
[**Logging**] タブページ	[**Log at Beginning of Connection**] チェックボックスをオンにします。

アクセス制御ルールの詳細については、『Cisco Secure Firewall Management Center デバイス構成ガイド』を参照してください。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 ページの上部にある [保存（Save）] をクリックします。

次のタスク

修復のための相関ルールの設定 （19 ページ） を参照してください。

修復のための相関ルールの設定

相関ルールは、システムが脅威に応答する条件を提供します。次のタスクでは、アクセス制御ルールの条件が満たされたときに接続の任意の時点でトリガーされる相関ルールを設定する方法について説明します。特に、サンプルアクセス制御ポリシーおよびルールは、送信元端末と接続先端末間で SSH 通信が通過するときにトリガーされます。

相関ポリシーとルールの詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』を参照してください。

手順

ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [相関（Correlation）]** をクリックします。

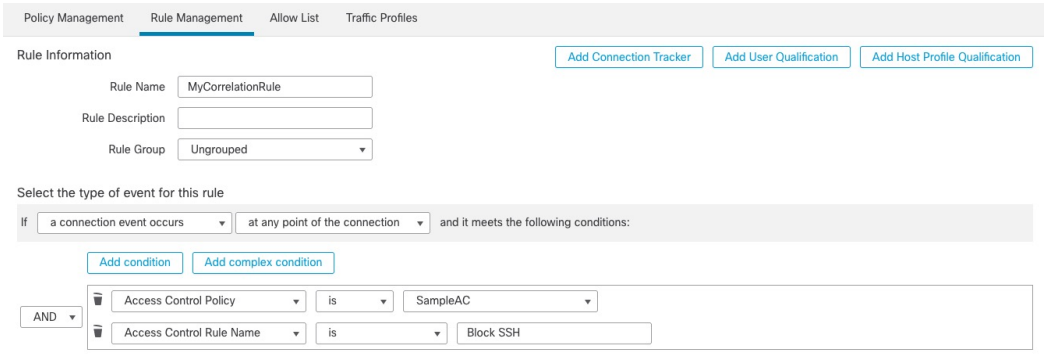
ステップ 3 [**Rule Management**] タブをクリックします。

ステップ 4 [ルールの作成（Create Rule）] をクリックします。

ステップ 5 ルールとオプションの説明を識別するための名前を入力します。

ステップ 6 [Select the type of event for this rule] セクションで [**a connection event occurs**] と [**at any point of the connection**] をクリックします。

ステップ 7 次の図に示すように、ルールの残りの部分を設定します。



前の図に示したアクセス制御ポリシーの名前とルール名を置き換えます。

ステップ 8 必要に応じてその他のオプションを設定し、[**Save**]をクリックします。

次のタスク

相関ルールと修復モジュールインスタンスとの関連付け （20 ページ） を参照してください。

相関ルールと修復モジュールインスタンスとの関連付け

修復および検疫用に Firewall Management Center を設定する最後の手順では、相関ルールを修復ポリシーと関連付けます。その後は、Firewall Management Center で脅威が検出されると、問題のある端末が APIC で検疫されます。

手順

ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。
ステップ 2 **[ポリシー（Policies）] > [相関（Correlation）]** をクリックします。
ステップ 3 [**Policy Management**] タブをクリックします。
ステップ 4 [ポリシーの作成（Create Policy）] をクリックします。
ステップ 5 ポリシー名とオプションのポリシーの説明を入力します。
ステップ 6 [**Default Priority**] は変更しないでください。
ステップ 7 [Add Rules] をクリックします。
ステップ 8 事前に作成した相関ルール名の横にあるチェックボックスをオンにします。
ステップ 9 [追加（Add）] をクリックします。
ステップ 10 [応答（Responses）]（ ） をクリックします。
ステップ 11 [**Unassigned Responses**] リストから、修復ポリシーの名前をダブルクリックして、[**Assigned Responses**] に移動します。

修復ポリシーの名前が表示されない場合は、相関ルールに戻り、アクセス制御ポリシーとアクセス制御ルールの両方の名前が正しいことを確認します。

ステップ 12 **[更新（Update）]**をクリックします。
ステップ 13 ページの上部にある [保存（Save）] をクリックします。
ステップ 14 修復ポリシーのスライダを [有効なスライダ（Slider enabled）]（ ） に移動します。

Firewall Management Center での修復の確認

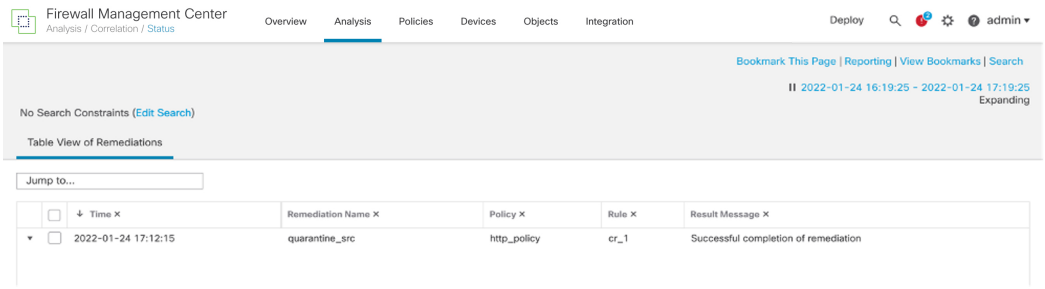
修復はさまざまな理由で失敗する可能性があるため、次の手順を実行して、Firewall Management Center の修復ステータスにエラーメッセージが表示されていないことを確認します。

手順

ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）]** をクリックします。

ステップ 3 [修復ステータス（Remediation Status）] テーブルで、ポリシーの行を見つけ、結果のメッセージを確認します。
次の図に例を示します。



ステップ 4 修復が成功した場合は、「APIC での検疫の確認 （21 ページ）」を参照してください。

ステップ 5 エラーが表示されても、後続の修復イベントが成功すると、端末が引き続き検疫される可能性があります。

ステップ 6 エラーが表示された場合は、「APIC での検疫の確認 （21 ページ）」を参照して、検疫が成功したかどうかを確認します。最終的に検疫に成功した場合は、すべてのエラーメッセージを無視できます。

次のタスク

APIC での検疫の確認 （21 ページ） を参照してください。

APIC での検疫の確認

始める前に

「Firewall Management Center での修復の確認 （20 ページ）」で説明されているタスクを完了します。

手順

ステップ 1 APIC にログインします。

ステップ 2 **[Tenants]** タブページをクリックします。

ステップ 3 **[ALL TENANTS]** をクリックします。

ステップ 4 感染したテナントの名前をダブルクリックします。

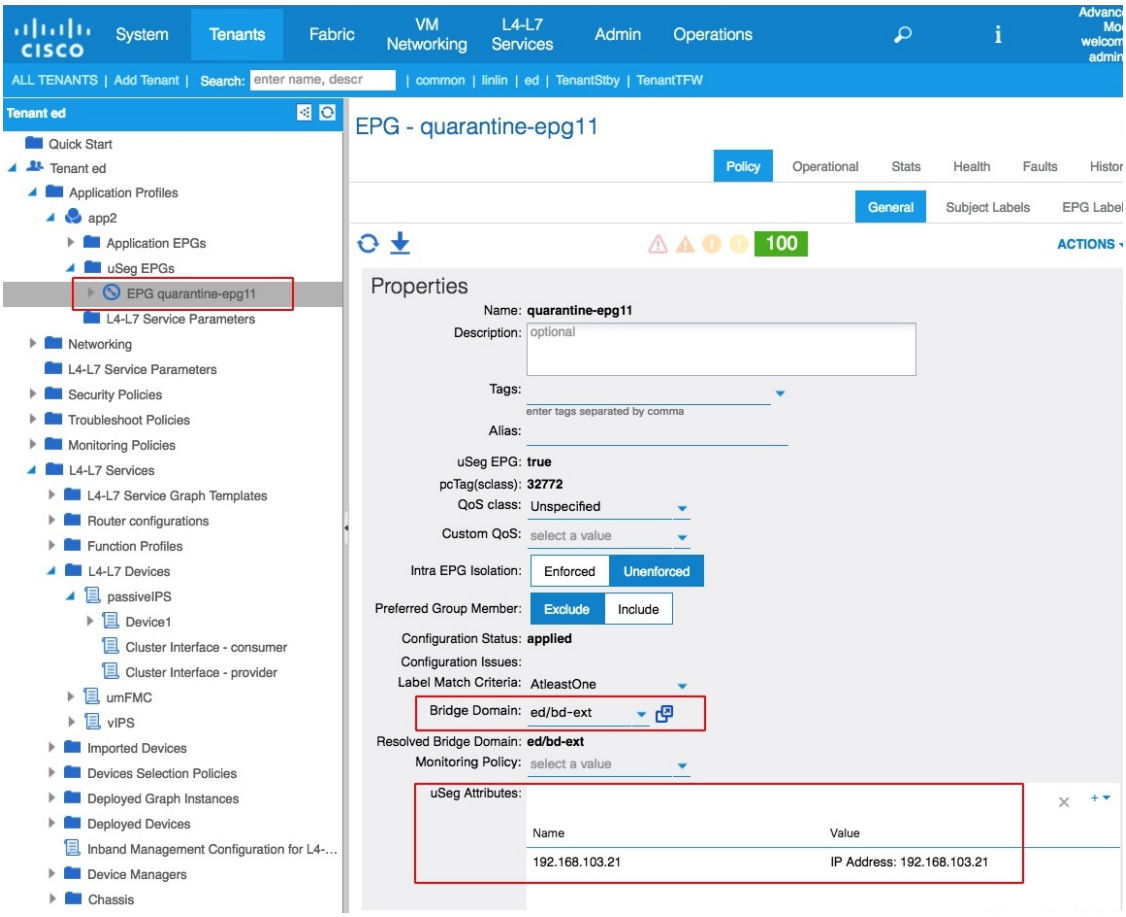
ステップ 5 左ペインで、感染したアプリケーションを展開します。

ステップ 6 [**uSeg EPGs**] をクリックします。

ステップ 7 検疫済みの端末の EPG 検疫をクリックします。

ステップ 8 右側のパネルで **[Policy** > **General]** をクリックします。

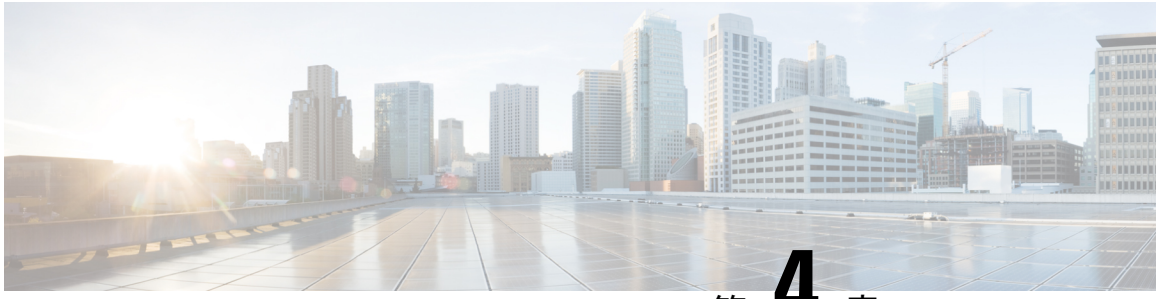
ステップ 9 APIC サーバーで 1 つ以上の uSeg 属性が作成されていることを確認します。
次の図は例を示しています。



この図に、IP アドレス 192.168.103.21 のデバイスが検疫されたことを示します。

（注）
VMware DVS およびベアメタル（ブリッジモード）の場合、端末が検疫されると、IP アドレス用の 1 つの属性と MAC アドレス用の 1 つの属性の 2 つの属性（フィルタ）が自動的に作成されます。したがって、検疫を削除するには、両方の属性を削除する必要があります。

ステップ 10 uSeg 属性が作成されていないが、相関ルールによって設定された条件が満たされていることがわかっている場合は、検疫は失敗します。IP アドレスを手動で検疫するには、「IP アドレスの手動検疫の概要（23 ページ）」を参照してください。



第 4 章

IP アドレスの手動検疫

検疫に失敗した場合は、以下のトピックの説明に従って、複数の IP アドレスを手動で検疫できます。

IP アドレスの手動検疫の概要

このガイドの前のセクションで説明したように、検疫が失敗した場合は、その IP アドレスを手動で検疫できます。検疫する IP アドレスと MAC アドレスを見つける必要があります。IP アドレスは Secure Firewall Management Center に、MAC アドレスは APIC に表示されます。

検疫する IP アドレスの検索

このトピックでは、Firewall Management Center で相関ログを確認して、検疫する IP アドレスを見つける方法について説明します。

手順

ステップ 1 まだ Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **[分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）]** をクリックします。

ステップ 3 失敗した検疫のエントリのタイムスタンプを見つけ、送信元 IP アドレスを書き留めます。

ステップ 4 まだ APIC にログインしていない場合は、ログインします。

ステップ 5 [Operation] タブページで **[EP Tracker]** をクリックし、IP アドレスを入力して Enter を押します。

ステップ 6 情報が表示されない場合は、端末を検疫できません。複数の IP アドレスが表示される場合は、問題のあるテナントの IP アドレスを検索します。

次のタスク

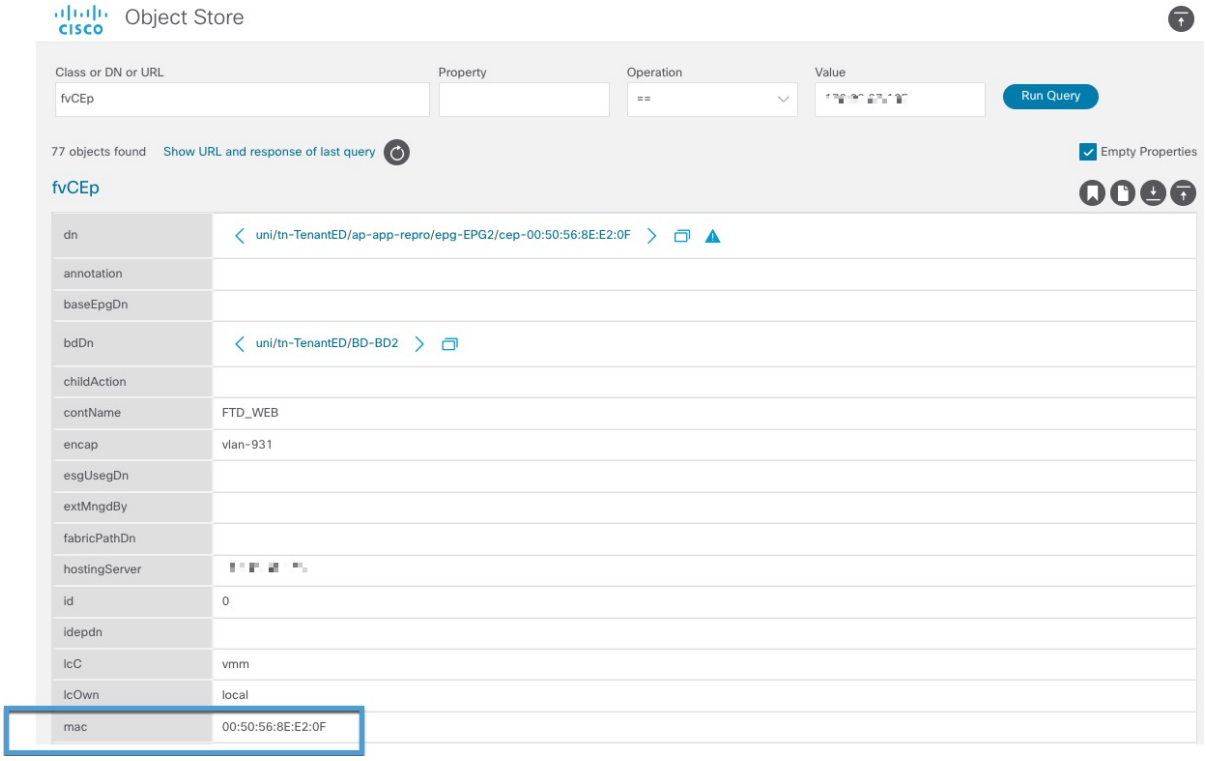
uSeg EPG 属性の作成 （24 ページ）

uSeg EPG 属性の作成

検疫する端末の EPG を識別できる場合は、この端末に対応する uSeg EPG 属性を作成します。

手順

ステップ 1 検疫する IP アドレスの MAC アドレスを検索するには、https://*apic_IP_address*/**visore.html** で APIC オブジェクトストアブラウザに移動します。端末の IP アドレスを使用してクエリを実行し、MAC アドレスを表示します。
次の図は例を示しています。



ステップ 2 まだ APIC にログインしていない場合は、ログインします。

ステップ 3 **[Tenants > ALL TENANTS]** をクリックします。

ステップ 4 検疫する端末を含むテナントをダブルクリックします。

ステップ 5 **[Networking** > **Bridge Domains]** を展開します。

ステップ 6 EPG ブリッジドメインを書き留めます。

ステップ 7 **[Application Profiles** > ***profile-name*** > **Application EPGs]** > ***epg-name***を展開し、ドメインプロファイル名を書き留めます。

ステップ 8 [**Application Profiles**] を展開し、[**uSeg EPG**] を右クリックします。

ステップ 9 [**Create uSeg EPG**] をクリックします。

ステップ 10 uSeg EPG の名前を **uSegEPG***endpoint-name* の形式で入力します（例：**uSegEPG-EPG1**）。

ステップ 11 [**Bridge Domain**] リストから EPG のブリッジドメインをクリックします。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 ドメインページで [[追加（Add）] (+)] をクリックします。

ステップ 14 [**Domain Profiles**] リストでドメインプロファイルをクリックします。

ステップ 15 [**Deployment Immediacy**] を [**Immediate**] に設定します。

ステップ 16 [**Resolution Immediacy**] を [**Immediate**] に設定します。

ステップ 17 右下の [[追加（Add）] (+)] をクリックし、名前とフィルタ用の IP アドレスを入力して、IP フィルタ属性を追加します。

ステップ 18 **Update** をクリックし、**Finish** をクリックします。

uSeg EPG が表示されない場合は、ブラウザのページを更新してください。

ステップ 19 [**uSeg Attributes**] をクリックします。

ステップ 20 クリック [追加（Add）] (+)

ステップ 21 [**Match Any**] の演算子を使用して、検疫されたホストの IP アドレスと MAC アドレスの属性を追加します。

IP フィルタの場合、名前として IP アドレスを使用します。MAC フィルタの場合、IP アドレスと下線、および MAC アドレスの最後の 3 つのオクテットを名前として使用します。

ステップ 22 新たに作成した uSeg EPG の下で [**Domains**]（VMs およびベアメタル）を右クリックし、元の EPG と同一の名前とドメインタイプでドメイン関連付けを追加します。

ステップ 23 ベアメタルの場合、[**Static Leafs**] を右クリックし、[**Statically Link With Node**] をクリックします。

ステップ 24 **[送信（Submit）]** をクリックします。

次のタスク

手動 IP アドレス検疫の確認 （25 ページ）

手動 IP アドレス検疫の確認

検疫された端末から通信が出入りできないことを確認します。

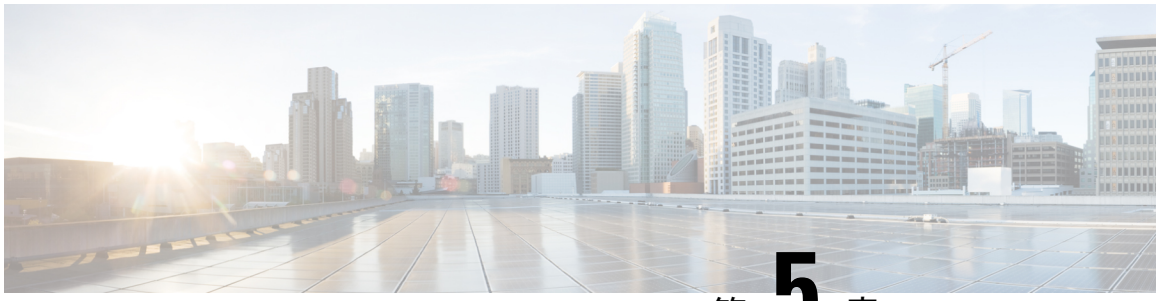
始める前に

手順

ステップ 1 検疫された IP アドレスに ping などのタスクを実行します。

操作は失敗するはずです。

ステップ 2 ping に成功した場合は、検疫する端末の IP アドレスと MAC アドレスを確認して、再試行します。



第 5 章

関連資料

関連資料

Cisco APIC/Secure Firewall Remediation Moduleの詳細については、該当するガイドを参照してください。

Cisco APIC および ACI の詳細については、『APIC Documentation』を参照してください。

バグ検索ツール（BST）の使用、サービスリクエストの送信、追加情報の収集の詳細については、「Support Case Manager」を参照してください。

関連資料

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。