ドメイン管理

次のトピックでは、ドメインを使用してマルチテナンシーを管理する方法について説明します。

- ドメインを使用したマルチテナンシーの概要 （1 ページ）
- ドメインの管理 （5 ページ）
- 新しいドメインの作成 （6 ページ）
- ドメイン間のデータの移動 （7 ページ）
- ドメイン間のデバイスの移動 （8 ページ）

ドメインを使用したマルチテナンシーの概要

Firepowerシステムでは、ドメインを使用したマルチテナンシーを実装できます。ドメインは、管理対象デバイス、構成、およびイベントへのユーザアクセスをセグメント化します。最上位の [グローバル（Global）] ドメインの下に、2つまたは3つのレベルで最大50個のサブドメインを作成できます。

Firepower Management Centerにログインすると、現在のドメインと呼ばれる単一ドメインにログインします。ユーザアカウントによっては、他のドメインに切り替えることができる場合があります。

ユーザ ロールによる制限に加えて、現在のドメイン レベルによってさまざまなFirepowerシステム設定の変更が制限される場合もあります。システム ソフトウェア アップデートなどのほとんどの管理タスクは、グローバル ドメインに制限されます。

その他のタスクは、サブドメインがないドメインであるリーフ ドメインに制限されます。たとえば、各管理対象デバイスをリーフ ドメインと関連付け、そのリーフ ドメインのコンテキストからデバイス管理タスクを実行する必要があります。

ヒント このガイドの各タスク トピックには、タスクを実行できるドメイン レベルを示す**サポートされるドメイン数**という値があります。

各リーフ ドメインは、そのリーフ ドメインのデバイスで集められた検出データに基づいて独自のネットワーク マップを作成します。管理対象デバイスによって報告されたイベント（接続、侵入、マルウェアなど）もデバイスのリーフ ドメインに関連付けられます。

1 ドメイン レベル：グローバル

マルチテナンシーを設定しない場合、すべてのデバイス、構成、およびイベントはグローバル ドメインに属します。グローバル ドメインは、このシナリオの場合はリーフ ドメインでもあります。ドメイン管理を除き、サブドメインを追加するまでは、ドメイン固有の構成および分析オプションは非表示になります。

2 ドメイン レベル：グローバル、セカンドレベル

2 レベルのマルチドメイン展開では、グローバル ドメインには直接の子孫ドメインのみがあります。たとえば、マネージドセキュリティ サービスプロバイダー（MSSP）は、1 つの Firepower Management Center を使用して複数の顧客のネットワーク セキュリティを管理できます。

- MSSP の管理者は、グローバル ドメインにログインして、すべての顧客の展開を管理できます。
- 各顧客の管理者は、サブドメインと呼ばれるセカンドレベルにログインして、その組織に適用されるデバイス、構成、およびイベントのみを管理できます。これらのローカル管理者は、MSSP の他の顧客の展開を表示したり、その環境に影響を与えることはできません。

3 ドメイン レベル：グローバル、セカンドレベル、サードレベル

3 レベルのマルチドメイン展開では、グローバル ドメインにはサブドメインがあり、そのうち少なくとも 1 つに独自のサブドメインがあります。前の例を拡張するには、MSSP 顧客（すでにサブドメインに制限されている）がその展開をさらにセグメント化しようとしているシナリオを考えてみます。この顧客は、2 つのクラスのデバイス（ネットワーク エッジに配置されているデバイスと内部に配置されているデバイス）を個別に管理しようとしています。

- 顧客の管理者はセカンドレベルのサブドメインにログインして、顧客の展開全体を管理できます。
- 顧客のエッジ ネットワークの管理者は、サードレベル（リーフ）ドメインにログインして、ネットワーク エッジに展開されているデバイスに適用されるデバイス、構成、およびイベントのみを管理できます。同様に、顧客の内部ネットワークの管理者は、別のサードレベル ドメインにログインして、内部のデバイス、構成、およびイベントを管理できます。エッジと内部の管理者は、互いの展開を表示できません。

ドメインの用語

このマニュアルでは、ドメインおよびマルチドメイン展開を説明する際に次の用語を使用します。

グローバル ドメイン

マルチドメイン展開でのトップレベル ドメイン。マルチテナンシーを設定しない場合、すべてのデバイス、設定、およびイベントはグローバル ドメインに属します。グローバル ドメインの Administrators は、Firepower システム全体の導入を管理できます。

サブドメイン

第 2 または第 3 レベルのドメイン。

第 2 レベル ドメイン

グローバル ドメインの子。第 2 レベル ドメインは、リーフ ドメインにするか、サブドメインを持つことができます。

第 3 レベル ドメイン

第 2 レベル ドメインの子。第 3 レベル ドメインは常にリーフ ドメインです。

リーフ ドメイン

サブドメインを持たないドメイン。各デバイスはリーフ ドメインに属している必要があります。

子孫ドメイン

階層の現在のドメインから下のドメイン。

子ドメイン

ドメインの直接子孫。

先祖ドメイン

現在のドメインより上にある同じ系統のドメイン。

親ドメイン

ドメインの直接先祖。

兄弟ドメイン

同じ親を持つドメイン。

現在のドメイン

現在ログインしているドメイン。システムでは、Webインターフェイスの右上のユーザ名の前に現在のドメイン名が表示されます。ユーザ ロールが制限されている場合を除き、現在のドメインの設定を編集できます。

ドメインのプロパティ

ドメインのプロパティを変更するには、そのドメインの親ドメインのAdministratorアクセス権が必要です。

名前（Name）と説明（Description）

各ドメインには、その階層内に一意の名前が必要です。説明は任意です。

親ドメイン（Parent Domain）

第2および第3レベルのドメインには親ドメインがあります。ドメインを作成した後にドメインの親を変更することはできません。

デバイス

リーフ ドメインにのみデバイスを含めることができます。つまり、1つのドメインにはサブドメインまたはデバイスを含めることができますが、両方を含めることはできません。非リーフ ドメインが直接デバイスを制御している展開を保存することはできません。

ドメイン エディタで、ドメイン階層の現在の場所に応じて、Web インターフェイスに使用可能な選択されたデバイスが表示されます。

ホスト制限（Host Limit）

Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。マルチドメイン展開では、リーフ ドメインは使用可能なモニタされたホストのプールを共有しますが、個別のネットワーク マップを持っています。

各リーフ ドメインがネットワーク マップに値を入力できるように、ホスト制限を各サブドメイン レベルで設定できます。ドメインのホスト制限を **0** に設定すると、ドメインは一般的なプールで共有します。

ホスト制限を設定すると、各ドメイン レベルで異なる効果があります。

- リーフ：リーフ ドメインの場合、ホスト制限は単に、リーフ ドメインがモニタできるホスト数の制限です。
- 第2レベル：第3レベルのリーフ ドメインを管理する第2レベルのドメインの場合、ホスト制限は、リーフ ドメインがモニタできるホストの総数を表します。リーフ ドメインは、使用可能なホストのプールを共有します。
- グローバル：グローバル ドメインの場合、ホスト制限は、Firepower Management Center がモニタできるホストの総数に等しくなります。変更することはできません。

サブドメインのホスト制限の合計を、親ドメインのホスト制限より多くすることができます。たとえば、グローバル ドメインのホスト制限が 150,000 の場合、複数のサブドメインを設定して、それぞれのホスト制限を 100,000 にすることができます。これらのドメインのいずれか（すべてではない）が 100,000 のホストをモニタできます。

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または長期間非アクティブになっているホストを置換することができます。各リーフ ドメインには独自のネットワーク検出ポリシーがあるため、各リーフ ドメインは、システムが新しいホストを検出すると、独自の動作を制御します。

ドメインのホスト制限を軽減した場合に、そのネットワークマップに新しい制限より多くのホストが含まれている場合、システムは最も長い間非アクティブになっているホストを削除します。

関連トピック

Firepower システムのホスト制限
ネットワーク検出のデータ ストレージ設定

ドメインの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ドメインのプロパティを変更するには、そのドメインの親ドメインへの管理者アクセス権が必要です。

手順

ステップ 1 **[システム（System）] > [ドメイン（Domains）]**を選択します。

ステップ 2 次のようにドメインを管理します。

- 追加：[ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] アイコンをクリックします（新しいドメインの作成 （6 ページ） を参照）。
- 編集：変更するドメインの横にある編集アイコン（  ）をクリックします（ドメインのプロパティ （3 ページ） を参照）。
- 削除：削除する空のドメインの横にある削除アイコン（  ）をクリックして、選択内容を確認します。宛先ドメインを編集することによって、削除するドメインからデバイスを移動します。

ステップ 3 ドメイン構造への変更を行い、すべてのデバイスをリーフ ドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 4 プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します（ドメイン間のデータの移動 （7 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンまたはインターフェイス グループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （8 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。設定変更の展開を参照してください。

新しいドメインの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルおよびセカンドレベル	Admin

最上位の [グローバル（Global）] ドメインの下に、2 つまたは 3 つのレベルで最大 50 個のサブドメインを作成できます。

ドメイン設定を実装する前に、リーフ ドメインにすべてのデバイスを割り当てる必要があります。リーフ ドメインにサブドメインを追加すると、ドメインはリーフ ドメインではなくなるので、デバイスを再度割り当てる必要があります。

手順

ステップ 1 グローバルまたはセカンドレベル ドメインで、**[システム（System）]** > **[ドメイン（Domains）]** を選択します。

ステップ 2 [ドメインの追加（Add Domain）] をクリックするか、または親ドメインの横にある [サブドメインの追加（Add Subdomain）] アイコンをクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] に入力します。

ステップ 4 [親ドメイン（Parent Domain）] を選択します。

ステップ 5 [デバイス（Devices）] タブで、ドメインに追加する [使用可能なデバイス（Available Devices）] を選択し、[ドメインに追加（Add to Domain）] をクリックするか、または [選択されたデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。

ステップ 6 必要に応じて、[詳細設定（Advanced）] タブをクリックして、新しいドメインがモニタできるホスト数を制限します（ドメインのプロパティ （3 ページ） を参照）。

ステップ 7 [保存（Save）] をクリックして、ドメイン管理ページに戻ります。
デバイスが非リーフ ドメインに割り当てられている場合は、システムによって警告が表示されます。これらのデバイスに新しいドメインを作成するには、[新しいドメインの作成（Create New Domain）] をクリックします。デバイスを既存のドメインに移動する予定がある場合は、[未割り当てのままにする（Keep Unassigned）] をクリックします。

ステップ 8 ドメイン構造への変更を行い、すべてのデバイスをリーフ ドメインに関連付けたら、[保存（Save）] をクリックして変更を実行します。

ステップ 9 プロンプトが表示されたら、追加の変更を行います。

- リーフ ドメインを親ドメインに変更した場合は、古いネットワーク マップを移動または削除します（ドメイン間のデータの移動 （7 ページ） を参照）。
- ドメイン間でデバイスを移動し、新しいポリシーおよびセキュリティ ゾーンまたはインターフェイス グループを割り当てる必要がある場合は、ドメイン間のデバイスの移動 （8 ページ） を参照してください。

次のタスク

- 新しいドメインのユーザ ロールとポリシー（アクセス制御、ネットワーク検出など）を設定します。必要に応じてデバイスのプロパティを更新します。
- 設定変更を展開します。設定変更の展開を参照してください。

ドメイン間のデータの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

イベントおよびネットワーク マップがリーフ ドメインに関連付けられているため、リーフ ドメインを親ドメインに変更する場合は、2 つの選択肢があります。

- ネットワーク マップおよび関連付けられているイベントを新しいリーフ ドメインに移動します。
- ネットワーク マップは削除しますが、イベントは保持します。この場合、システムが必要に応じてまたは設定されているようにイベントをプルーニングするまで、イベントは親ドメインに関連付けられたままとなります。または、古いイベントを手動で削除できます。

始める前に

- 以前のリーフ ドメインが現在の親ドメインになるドメイン設定を実行します（ドメインの管理 （5 ページ） を参照）。

手順

ステップ 1 現在親ドメインである以前のリーフ ドメインそれぞれに対し、2 つの選択肢があります。

- **親ドメイン**のイベントおよびネットワーク マップを継承するには、新しい**リーフ ドメイン**を選択します。

- 親ドメインのネットワーク マップを削除するが、古いイベントは保持する場合は、[なし（None）] を選択します。

ステップ 2 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

ドメイン間のデバイスの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルおよびセカンドレベル	Admin

ドメイン間でデバイスを移動すると、デバイスに適用された設定とポリシーに影響する可能性があります。システムは実行できる内容を自動的に保持および更新し、実行できない内容を削除します。

リモート アクセス VPN ポリシーをデバイスに割り当てるときは、ターゲット ドメインがリモート アクセス VPN の設定されているドメインの子孫である場合のみ、ドメイン間でデバイスを移動できます。

デバイスは、デバイス上の登録済み証明書を削除することなく子ドメインに移動できます。

具体的には次のとおりです。

- 移動したデバイスに割り当てられた正常性ポリシーが新しいドメインでアクセス不能の場合、新しい正常性ポリシーを選択できます。
- 移動したデバイスに割り当てられたアクセス コントロール ポリシーが有効でない場合、または新しいドメインでアクセスできない場合は、新しいポリシーを選択します。すべてのデバイスに、割り当てられたアクセス コントロール ポリシーが必要です。
- 移動したデバイス上のインターフェイスが、新しいドメインでアクセスできないセキュリティ ゾーンに属している場合は、新しいゾーンを選択できます。
- インターフェイスは、以下から削除されます。
  - 新しいドメインでアクセス不能で、アクセス コントロール ポリシーで使用されていないセキュリティ ゾーン。
  - すべてのインターフェイス グループ。

デバイスでポリシーの更新が必要だが、ゾーン間でインターフェイスを移動する必要がない場合は、ゾーン設定が最新であることを示すメッセージが表示されます。たとえば、デバイスのインターフェイスが共通の先祖ドメインに設定されているセキュリティゾーンに属している場合は、サブドメインからサブドメインにデバイスを移動する場合はゾーン設定を更新する必要はありません。

始める前に

- デバイスをドメインからドメインに移動し、次に新しいポリシーとセキュリティゾーンを割り当てる必要があるドメイン構成を実装します（ドメインの管理 （5 ページ） を参照）。

手順

ステップ 1 [デバイスの移動（Move Devices）] ダイアログボックスの [設定するデバイスの選択（Select Device(s) to Configure）] の下で、設定するデバイスをオンにします。

同じ正常性ポリシーとアクセス コントロール ポリシーを割り当てるには、複数のデバイスをオンにします。

ステップ 2 デバイスに適用する [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、または新しいポリシーを作成するには [新しいポリシー（New Policy）] を選択します。

ステップ 3 デバイスに適用する [正常性ポリシー（Health Policy）] を選択するか、またはデバイスに正常性ポリシーを適用しないままにするには [なし（None）] を選択します。

ステップ 4 インターフェイスを新しいゾーンに割り当てるようにプロンプトが表示された場合は、リストされている各インターフェイスに [新しいセキュリティ ゾーン（New Security Zone）] を選択するか、または後で割り当てるには [なし（None）] を選択します。

ステップ 5 すべての影響を受けるデバイスを設定した後、[保存（Save）] をクリックしてポリシーとゾーンの割り当てを保存します。

ステップ 6 [保存（Save）] をクリックして、ドメイン構成を実装します。

次のタスク

- 移動の影響を受けた移動済みデバイスでその他の設定を更新します。
- 設定変更を展開します。設定変更の展開を参照してください。