FTDでのマルチドメイン環境での継承

内容

概要

このドキュメントでは、継承およびマルチドメイン機能の設定と動作について説明します。また、この2つの機能がどのように連動するかを実際の使用例で説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- Firepower Management Center（FMC）
- Firepower Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Firepower Management Center(FMC)ソフトウェアバージョン6.4
- Firepower Threat Defense(FTD)ソフトウェアバージョン6.4

注：マルチドメインおよび継承機能のサポートは、6.0バージョン以降のFMC/FTDで利用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、設定が及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

ポリシーの継承では、アクセスコントロールポリシーをネストできます。子ポリシーは、Security Intelligence、HTTP Response、Logging SettingsなどのACP設定を含むベースポリシーからルールを継承します。 オプションで、管理者は子ポリシーに対して、Security Intelligence、HTTP Response、Logging SettingsなどのACP設定を上書きさせるか、子ポリシーで上書きできないように設定をロックさせます。この機能は、マルチドメインFMC環境で非常に便利です。

マルチドメイン機能は、FMCの管理対象デバイス、設定、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。ユーザは、権限に応じて他のドメインに切り替えたり、他のドメインにアクセスしたりできます。マルチドメイン機能が構成されていない場合、すべての管理対象デバイス、構成、およびイベントはグローバルドメインに属しています。

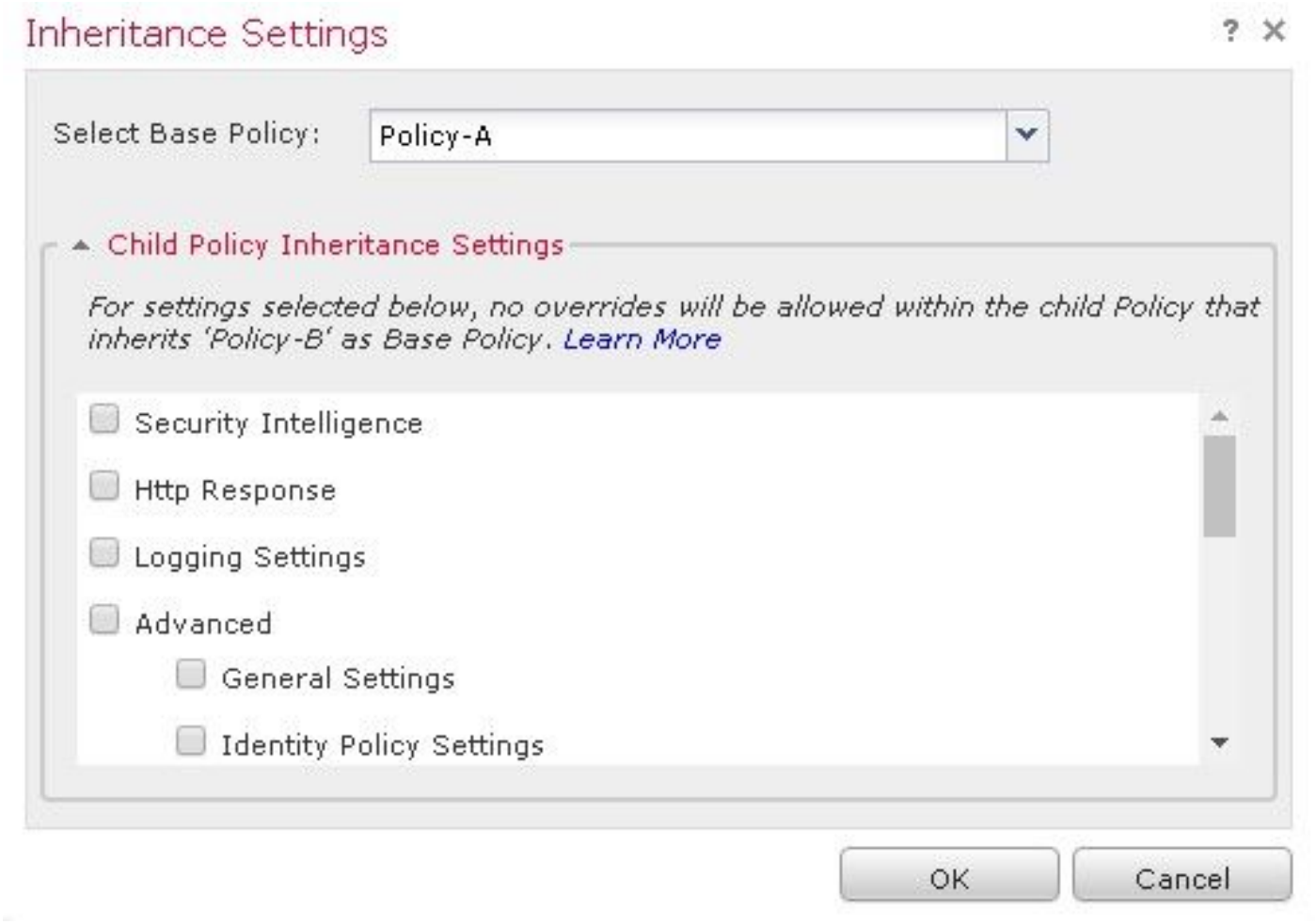
ポリシー継承の設定

リーフドメインは、それ以上サブドメインを持たないドメインです。子ドメインは、ユーザ/管理者が現在いるドメインの次レベルの子孫です。親ドメインは、ユーザ/管理者が現在いるドメインの直接の祖先です。

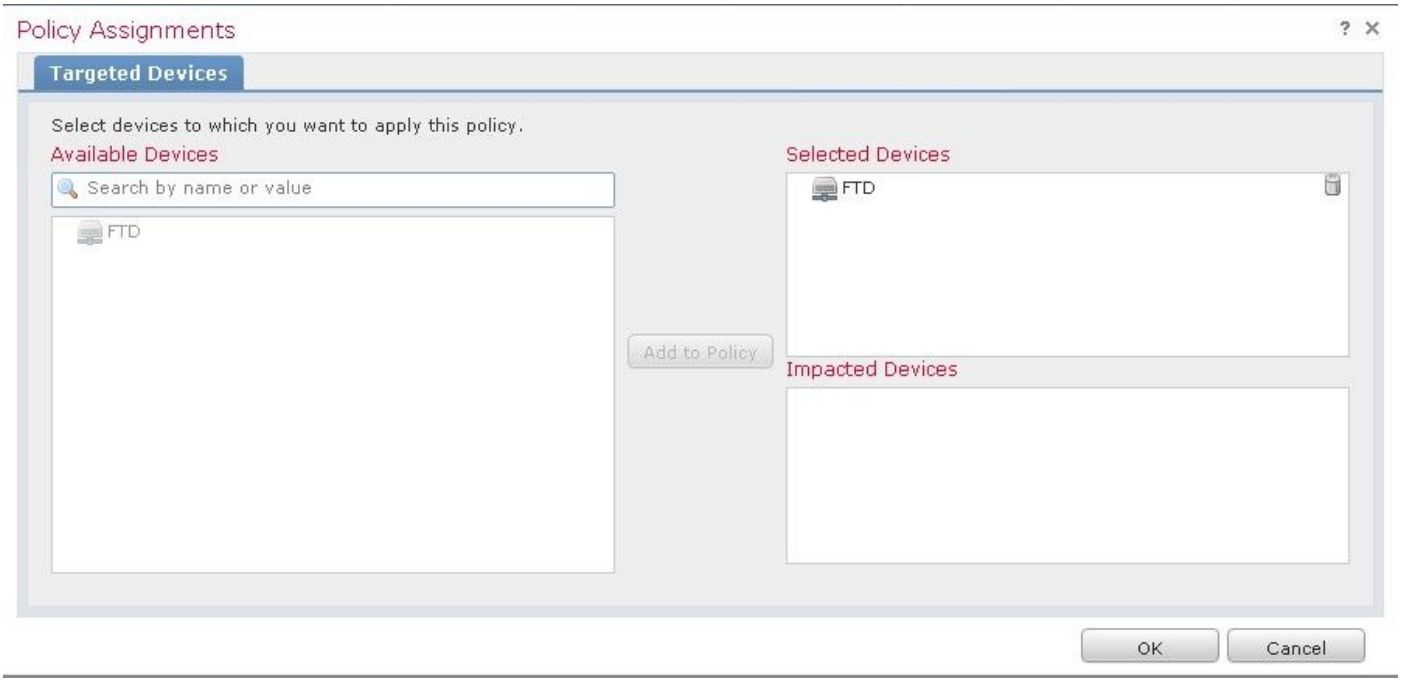
既存のポリシーの継承を設定または有効にするには、次の手順を実行します。

1. Policy-Aをベースポリシーとし、Policy-Bを子ポリシーとする（Policy-BはPolicy-Aのルールを継承する）
2. EDIT Policy-Bを選択し、図に示すようにInheritance Settingsをクリックします。

3.次に示す[Select Base Policy]ドロップダウンリストから[Policy-A]を選択します。Security Intelligence、HTTP Response、Logging Settingsなどの他のACP設定は、オプションで子ポリシーの設定を上書きするために継承できます。

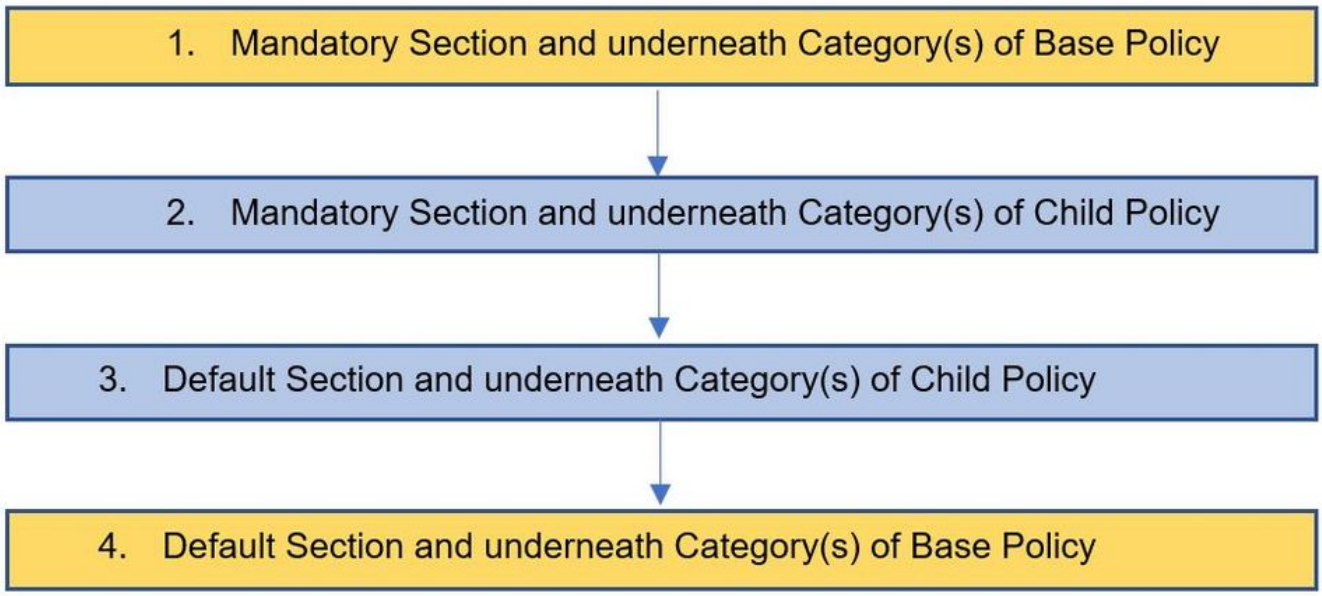


4.対象のターゲットFTDデバイスに対して子ポリシーPolicy-Bのポリシー割り当てを行います。

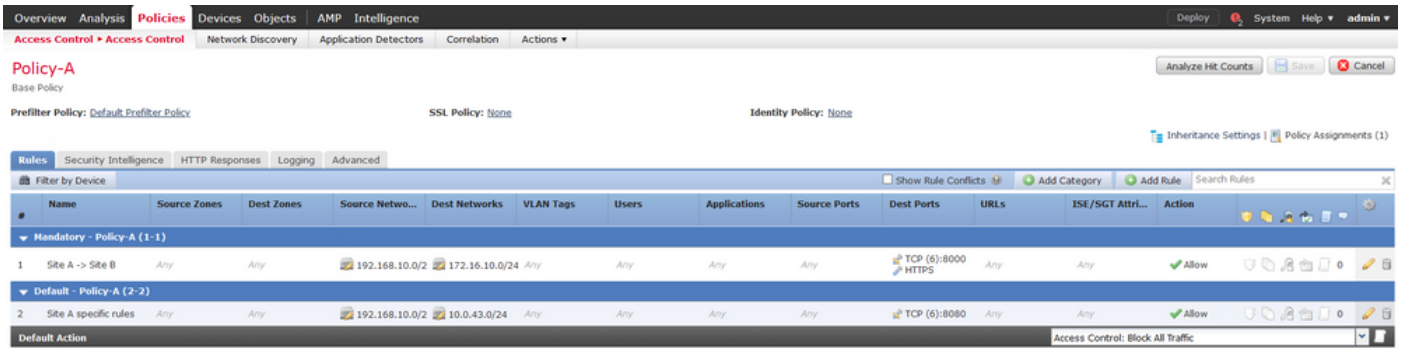


図に示すように、デフォルトでは、子ポリシーのデフォルトアクションが継承され、[基本ポリシーから継承]に設定されます。システム提供のポリシーからデフォルトアクションを選択するオプションもあります（以下を参照）。

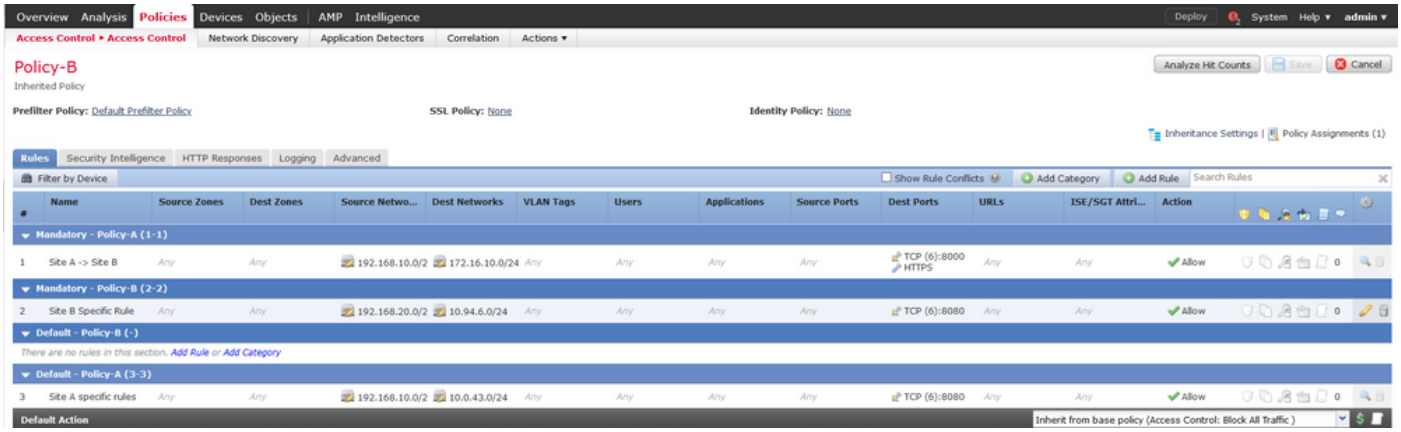
[Mandatory]セクションと[Default]セクションの両方に追加されたカテゴリの数に関係なく、トラフィックのルックアップの順序は常にトップダウン方式で行われます。継承設定を適用した後、図に示すように、子ポリシーPolicy-B (子ポリシー) のACP表現は、前述のルールチェックの順序に従って行われます。



この図は、ベースポリシーであるポリシーAと、ポリシーAから継承された子ポリシーであるポリシーBの両方のポリシーがFMCでどのように表示されるかを示しています。



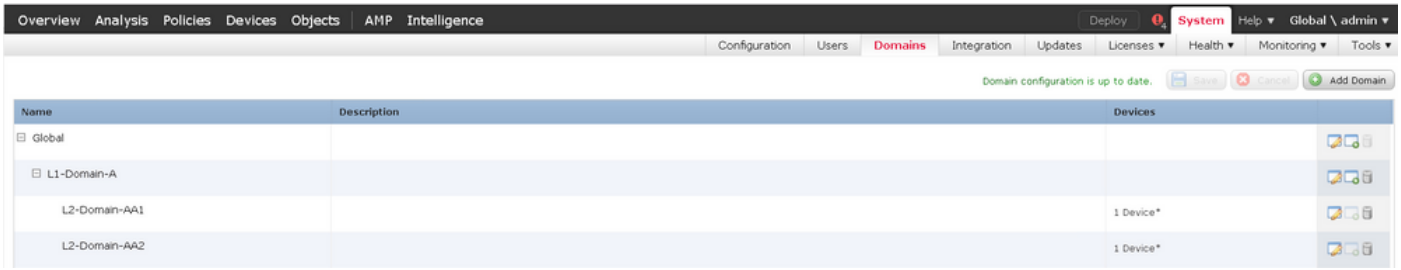
この図は、Policy-Bで、Policy-Aのルールと、Policy-B自体で設定された特定のルールを確認できることを示しています。順序に留意して、ルールの設定方法に注意する必要があります。



マルチドメインFMC環境でのFTD管理

マルチドメイン機能は、管理対象デバイス、設定、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。ユーザは、権限に応じて他のドメインに切り替えることができます。マルチドメイン機能が構成されていない場合、すべての管理対象デバイス、構成、およびイベントはグローバルドメインに属しています。

最大3レベルのドメインをグローバル・ドメインとして構成できます。すべての管理対象デバイスは、リーフ・ドメインのみに属している必要があります。これは、  （サブドメインの追加）は、図に示すように、リーフドメインでグレー表示されます。



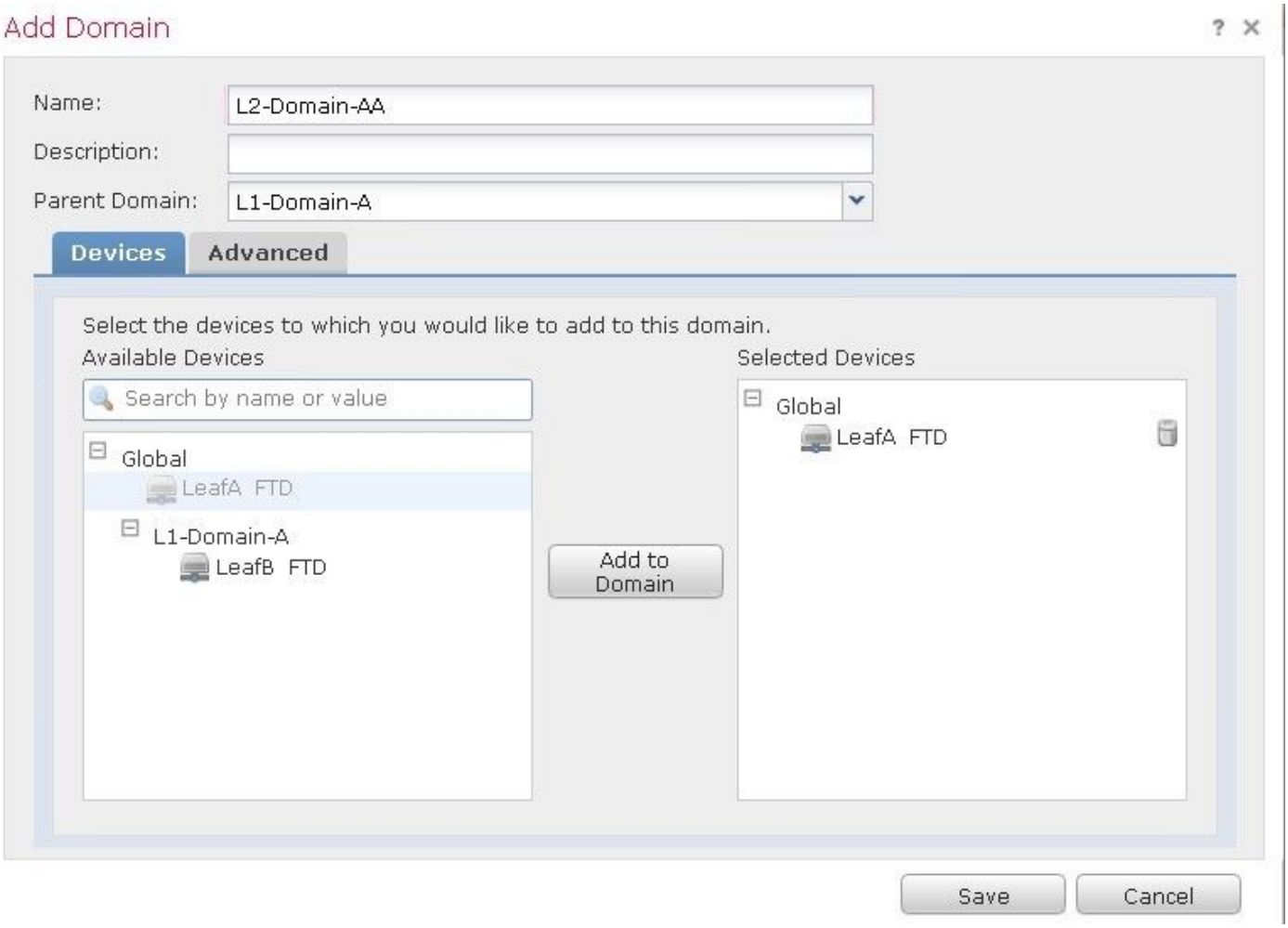
ドメインの設定

ドメインの設定は、次のように行うことができます。

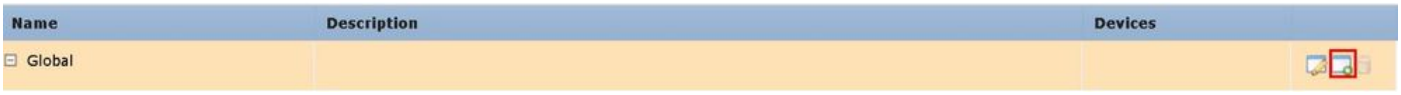
1. [システム(System)] > [ドメイン(Domains)]に移動します。デフォルトでは、グローバルドメインが存在します。

2. 図に示すように[Add Domain]をクリックします。

3. [ドメインの追加]ダイアログボックスが表示されます。ドメインの名前を入力し、ドロップダウン・リストから[親ドメイン]を選択します。これがリーフドメインである場合、図に示すように、FTDデバイスをドメインに追加する必要があります。

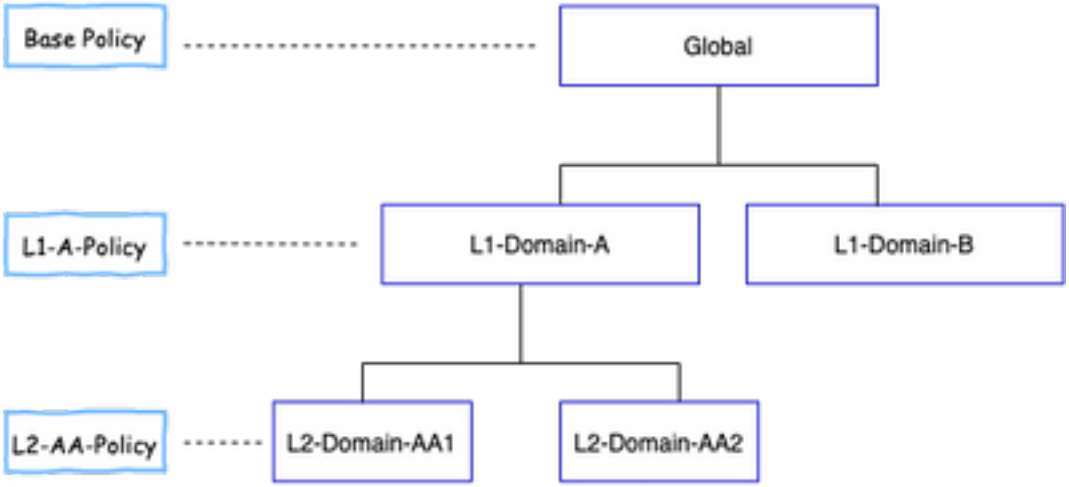


注：ドメインを追加するには、図に示すように[Add Sub Domain]**アイコンを**クリックします。ここでは、親ドメインがすでに選択されています。



マルチドメインFMC環境におけるポリシーの可視性と制御

ポリシーの可視性と制御は、グローバルドメインの管理者を除き、各ドメインユーザーに**限定されます**。この例は、次のような階層に基づいています。



可視性：この図に示すように、デフォルトのビューの[Policies]ページには、各ドメインの下で構成されたポリシー(ACP)がリストされます。

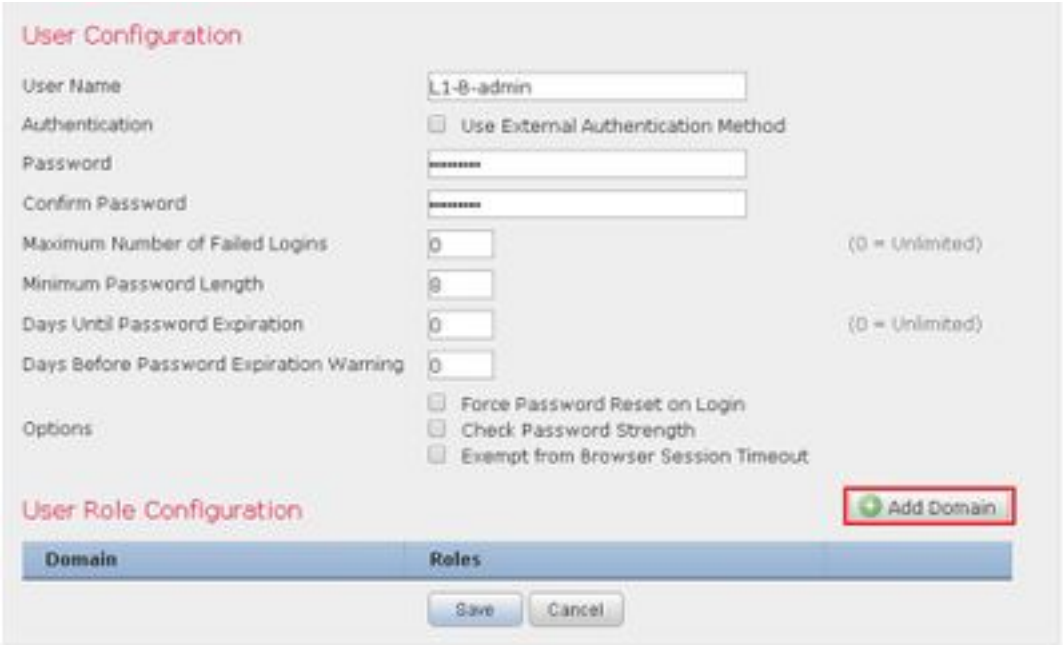
Control:各ドメインに属する管理者ユーザーは、ポリシーを編集できます。他のドメインに属するポリシー（たとえば、継承の一部）を編集するには、ドメインを現在のドメインから、ポリシーが設定されているドメインに切り替える必要があります。グローバルドメインまたはL1ドメインに属する管理者ユーザーのみ、ポリシー管理のために下位ドメインを切り替えることができます。

ドメインへのユーザの追加

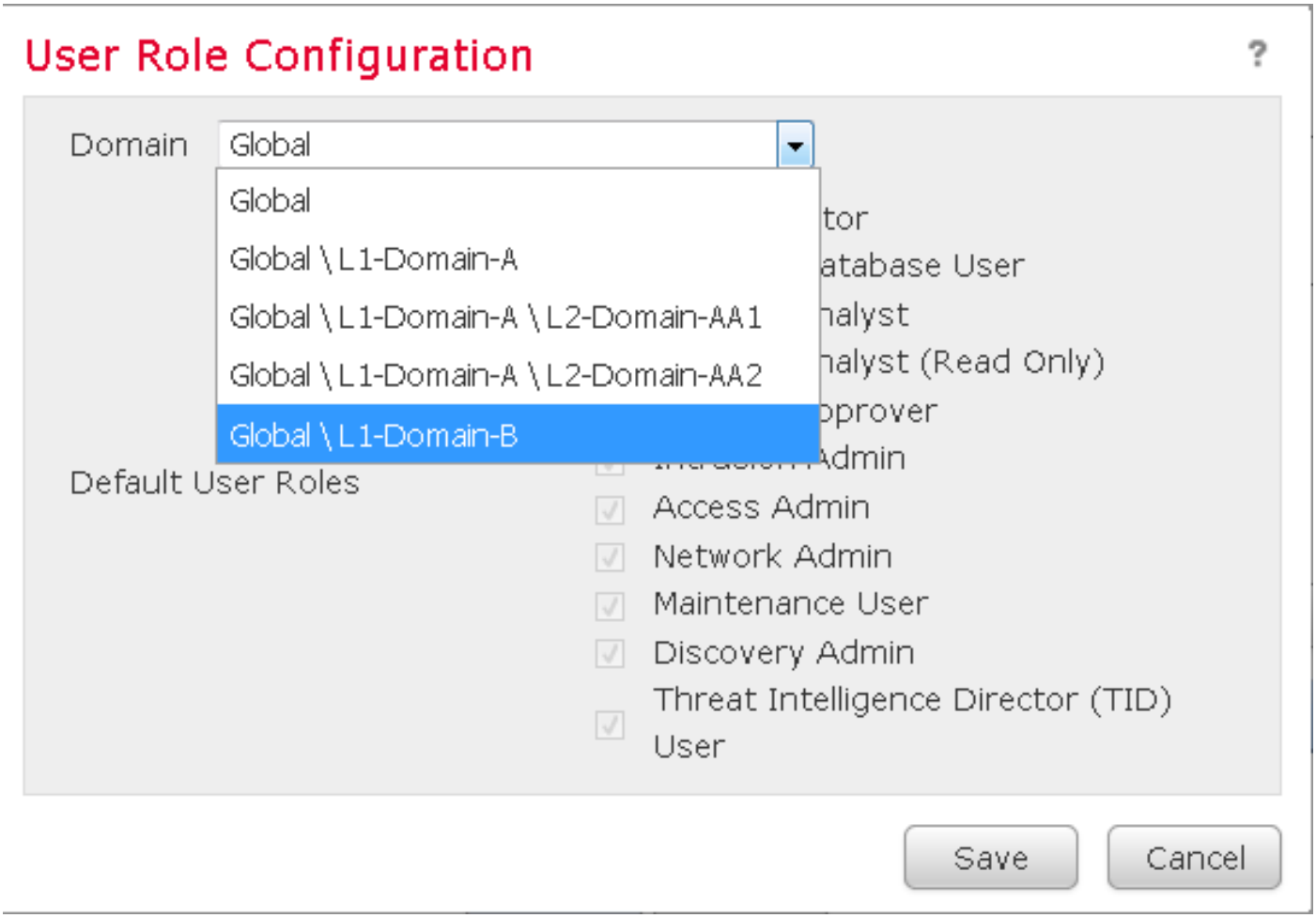
これは、特定のドメインにユーザを追加する方法を示します。この手順は、ローカルデータベースのユーザに適用されます。

1. [System] > [Users] に移動します。図に示すように、[Create User]をクリックします。

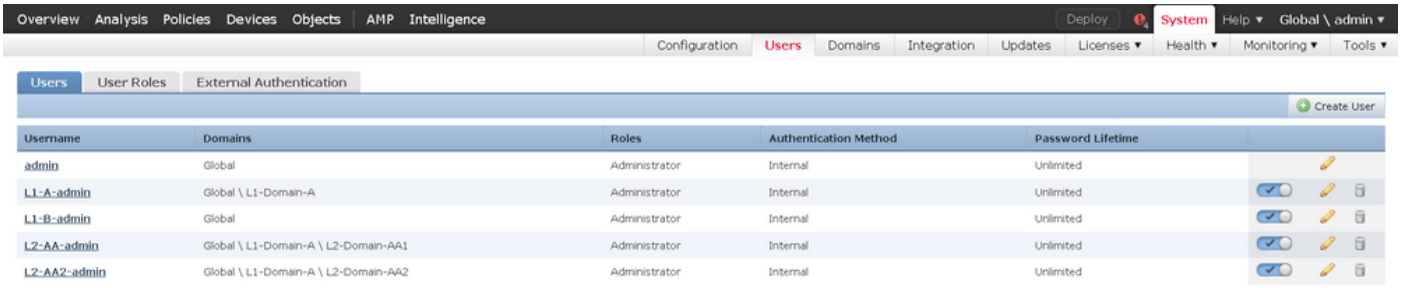
2. [ユーザー構成]ダイアログボックスが表示されます。ユーザー名とパスワードを入力します（&パスワードの確認）。 図に示すように、[Add Domain]をクリックして、指定したドメインにユーザを追加します。



3.ユーザを追加する[ドメイン(Domain)] ドロップダウンリストから目的のドメインを選択し、図に示すようにロールを指定します。新しいユーザを自分のドメインまたは子ドメインに追加できます。



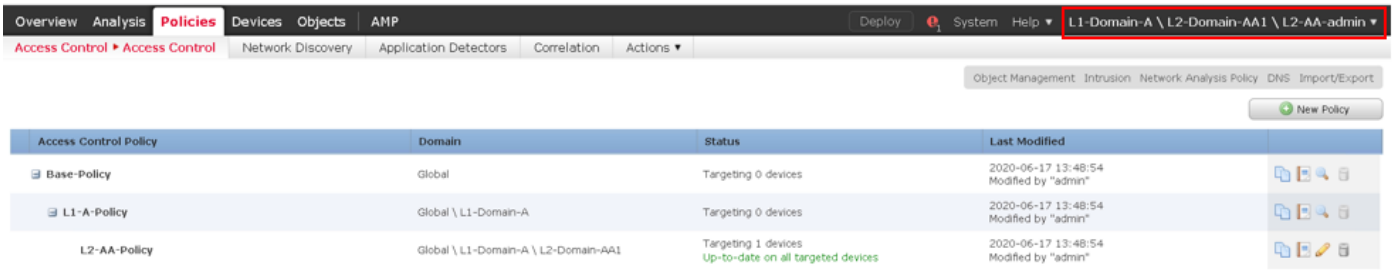
設定されたユーザを次の図に示します。



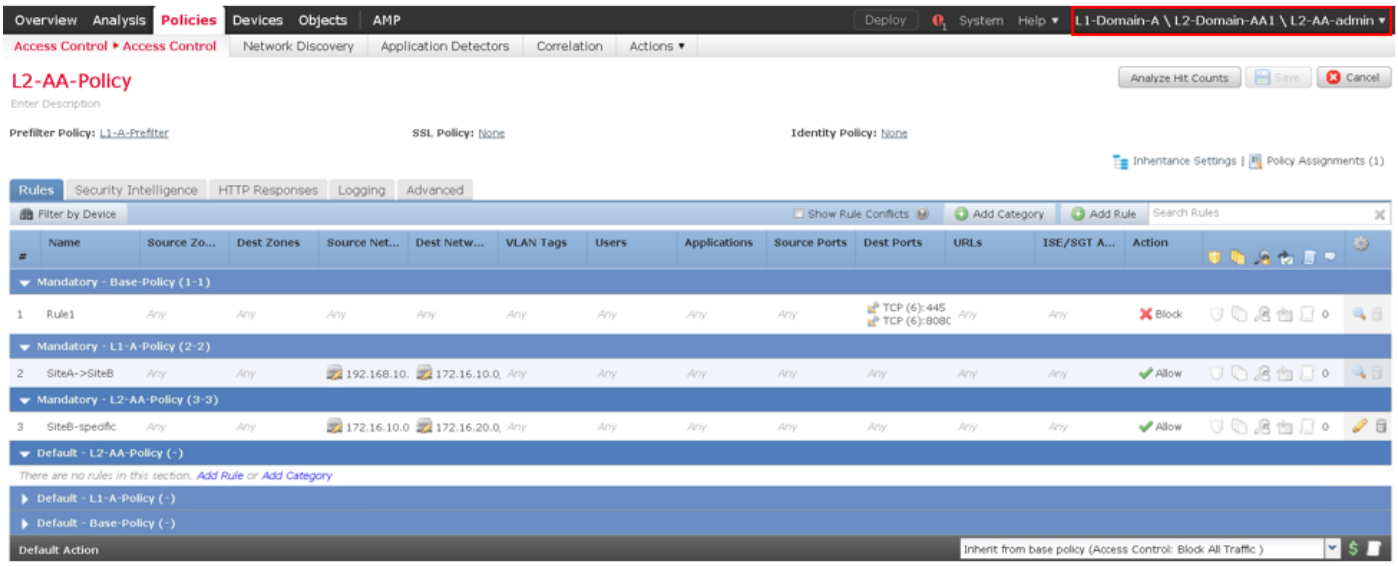
FMCでのリソースアクセスは、ユーザが属するドメインに制限されます。次に示すように、ユーザL1-A-adminがFMC UIにログインすると、アクセスはユーザが属するドメインL1-Domain-Aに制限され、ユーザがその子ドメインに切り替わると子ドメインに制限されます。このユーザーは、L1-Domain-Aドメインで定義されたポリシーと、ドメインが子ドメインに切り替えられたときに子ドメインで定義されたポリシーのみを編集できます。また、次の例から、L1-A-Policyがグローバルドメインで定義されたポリシーBase-Policyを継承して、Base-Policyを編集できます 署名図に示すように、継承設定はBase-Policyを指定するように行われます。

同様に、L2-Domain-AA1ドメインに属するユーザL2-AA-adminは、図に示すように、ドメインで定義されたポリシーL2-AA-Policyの制御のみを持ちます。L2-AAポリシーは、L1-Domain-Aで定義されたポリシーL1-A-Policyを継承して、次にグローバルドメインで定義されたBase-Policyを継承

します。また、ポリシーL2-AA-Policyを編集して、 署名ユーザL2-AA-adminは、その親ドメインであるL1-Domain-Aまたは祖先ドメインであるグローバルドメインに切り替えることはできません。



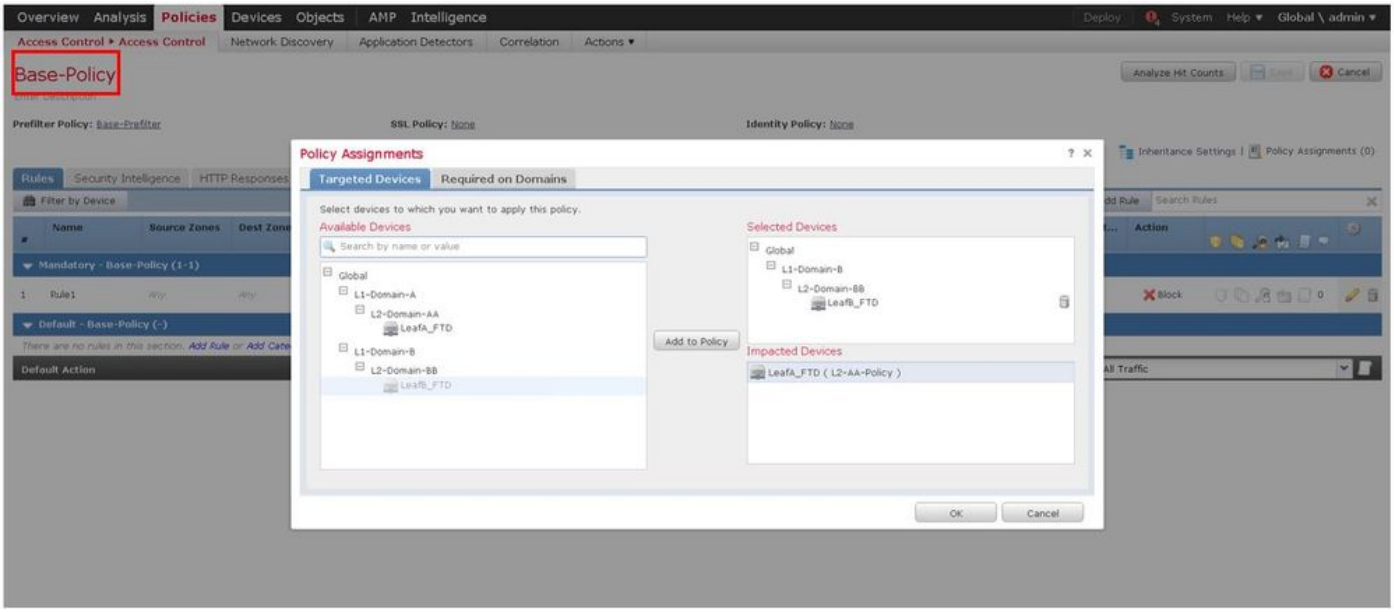
また、L1-Domain-Aに属するユーザL1-A-adminは、L2-Domain-AA1に切り替え、L2-AA-Policyを編集できます。 図に示すように署名します。これは、グローバルドメインに属し、子ドメインに切り替え、特定の子ドメインで定義されたポリシーを編集するユーザにも適用されます。



重要な注意点：

- 非大域ドメインを削除すると、ドメインに属するユーザーは自動的にグローバルドメインに移動されます。

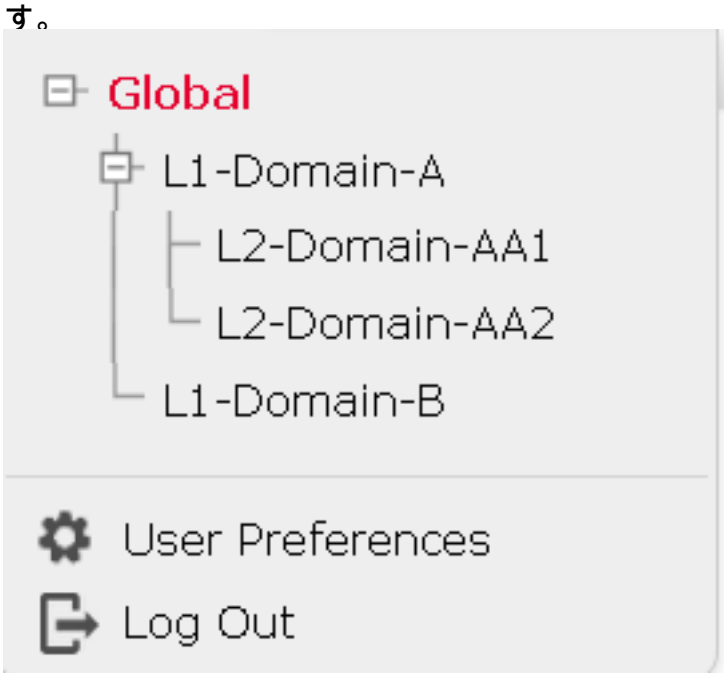
  FTD/sは常にリーフドメインで定義されます。この場合、リーフドメインはL2-Domain（L2-Domain-AAおよびL2-Domain-BB）です。 L2ドメインに属するFTDは、L1ドメイン内またはグローバルドメイン内のポリシーに割り当てることができます。この図では、グローバルドメイン内のACPは、L3ドメイン内で定義されたFTDをグローバルドメイン内で定義されたポリシーに割り当てています。



- グローバルドメイン内のユーザは他のユーザ固有のドメインに移動できますが、特定のドメイン内のユーザは、自分のドメインとその子ドメイン内でのみ可視性を持ちます。次の表に示すように、グローバルドメインまたはその他の上位ドメインに移動することはできません。

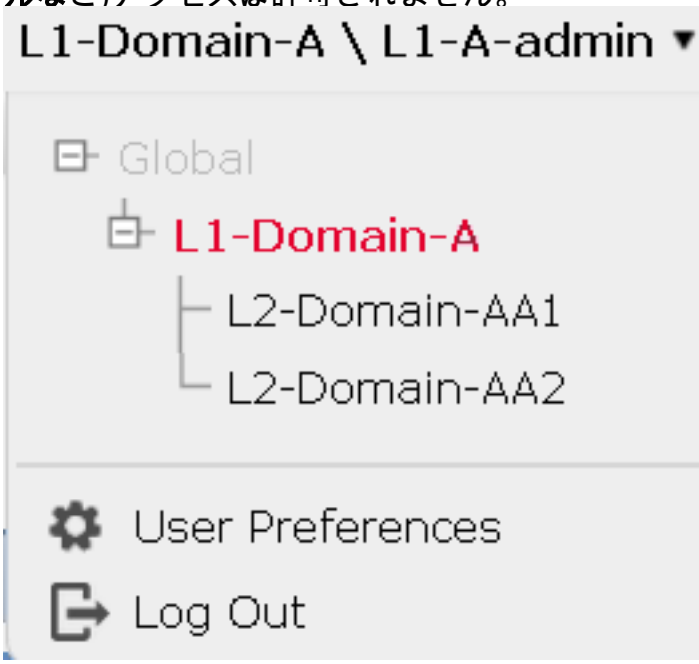
グローバルドメイン

グローバルドメインのユーザは、設定されているすべてのドメインを表示でき、他のドメインに移動できます。

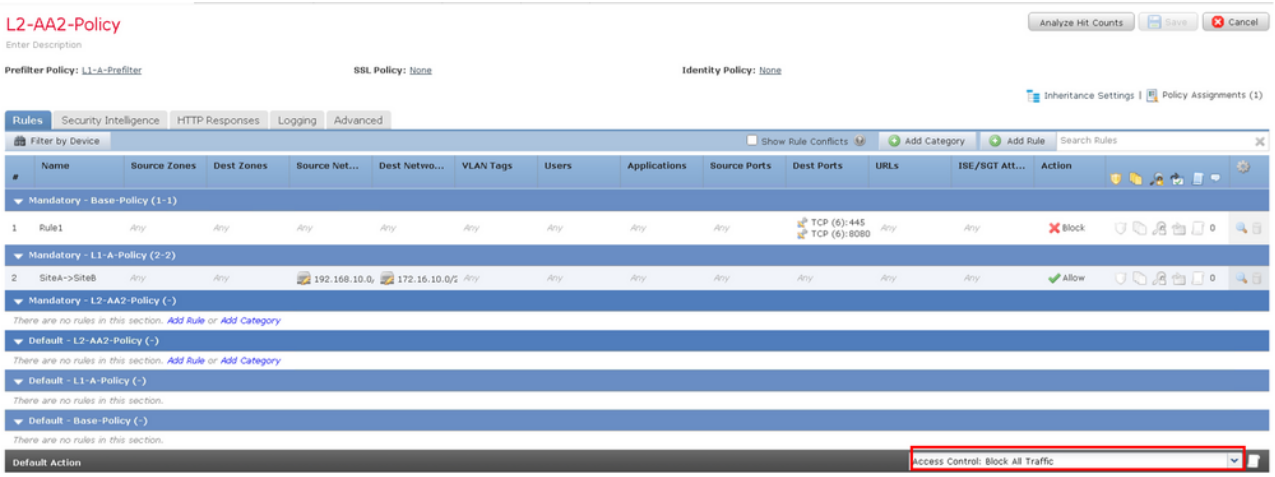


ユーザ固有のドメイン

L1-Domain-Aのユーザーは、L2-Domain-AAという自分自身とその子ドメインにのみ表示され、L2-Domain-AAに移動できます。上位レベルのドメイン(グローバルなど)アクセスは許可されません。



- 子ポリシーのデフォルトアクションは親ポリシーによってロックできず、この図に示すように、ユーザは親ポリシーのデフォルトアクションを継承する必要はありません。



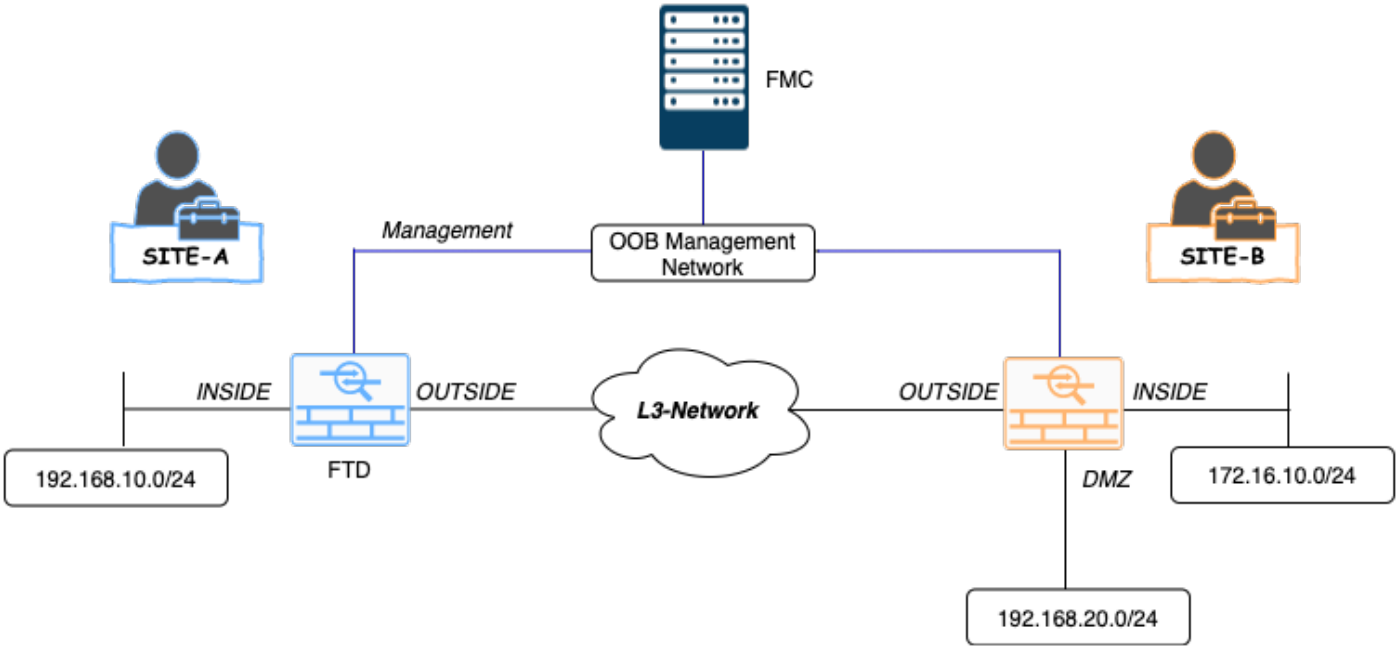
この図では、デフォルトのアクションが親のデフォルトのアクションとして割り当てられていない場合が分かります。「Inherit from base policy: not be seen in default action」という単語から分かります。

注：ユーザがL1/L2ドメインポリシーを同時に表示できないことに注意してください。ポリシーを表示および編集するには、ユーザーが目的のドメインに切り替える必要があります。例：グローバルドメインに存在するユーザ**admin**が、L1-Domain-AおよびL2-Domain-AAで設定されているポリシーを表示および編集するには、L1-A-Domainに切り替え、対応するポリシーを表示および編集します。また、L1-Domain-Aのユーザはグローバルドメインで定義されたポリシーを編集または削除できません。つまり、L1-A-Policyの親ポリシーであるBase Policy、L2-Domain-AAのユーザは、それぞれグローバルおよびL2-Domain-Aドメインドメインで定義のポリシーをを編集または削除できません。

使用例

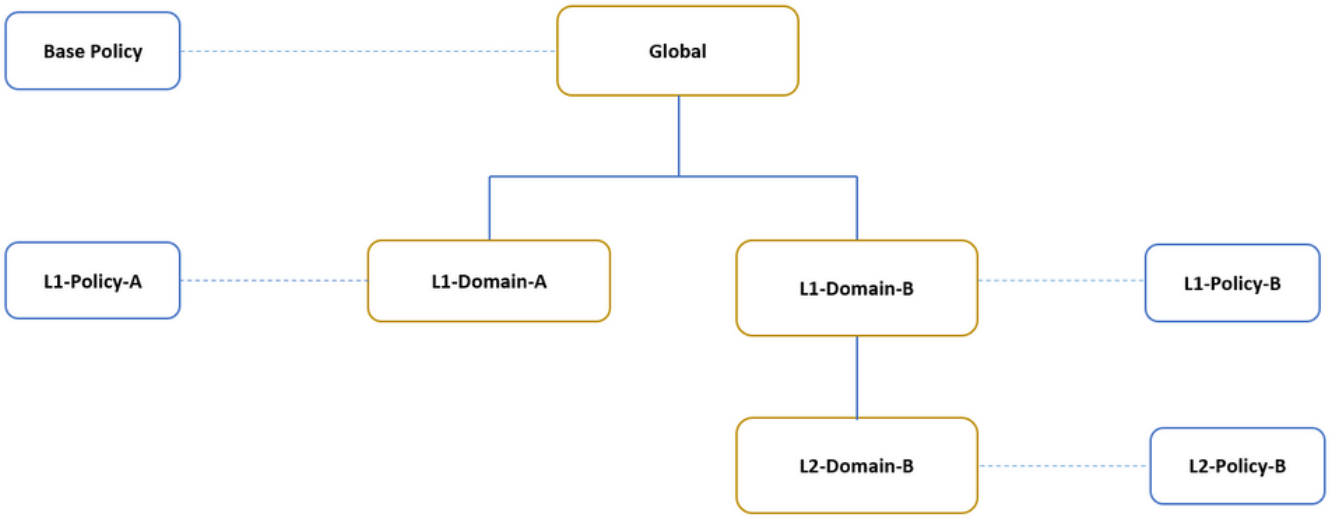
図に示すシナリオでは、SITE-A(SiteA-FTD)のFTDとSITE-B(SiteB-FTD)が、異なるドメイン（マルチドメイン）を介して1つのFMCで管理され、制御されたアクセスを提供します。ポリシーの観点からは、組織レベルでのポリシーに関する考慮事項を次に示します。

- SITEまたはDOMAINに属さない（ベースポリシー）すべてのFTDに適用されるサービス固有のBLOCKルール。
- サイトAからサイトBへのアクセス(L1-Policy-A)およびサイトBからサイトAへのアクセス(L1-Policy-B)を満たす要件を満たすルール。
- Site-B FTD(L2-Policy-B)に適用されるルール。



マルチドメイン環境での継承

上記の使用例では、次のドメイン/ポリシー階層を考慮してください。SiteA-FTDおよびSiteB-FTDは、リーフドメインL1-Domain-AおよびL2-Domain-Bの一部です。

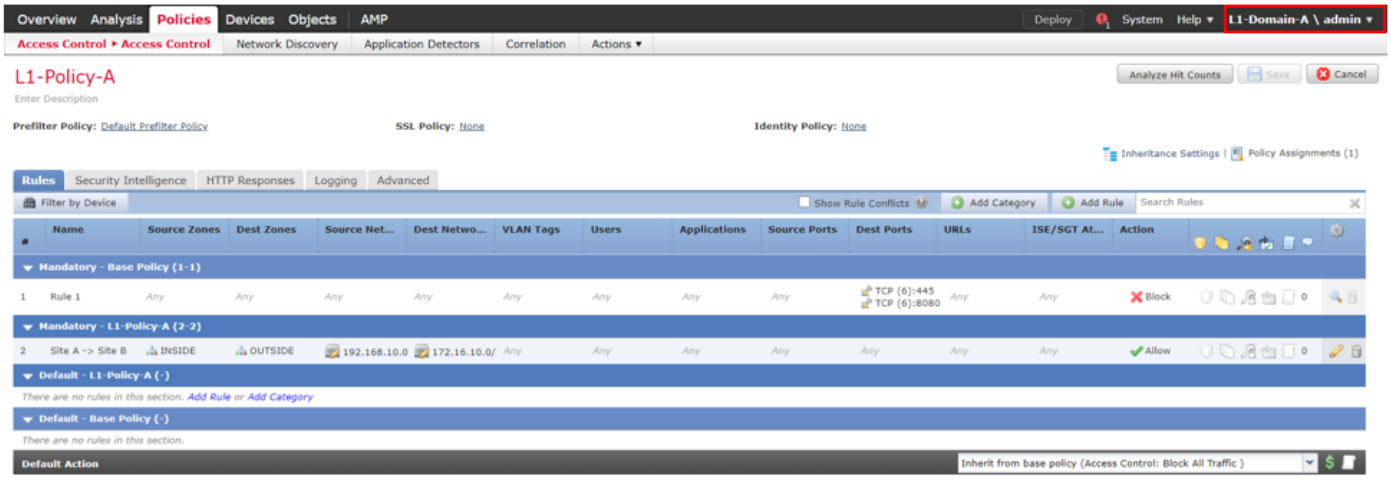


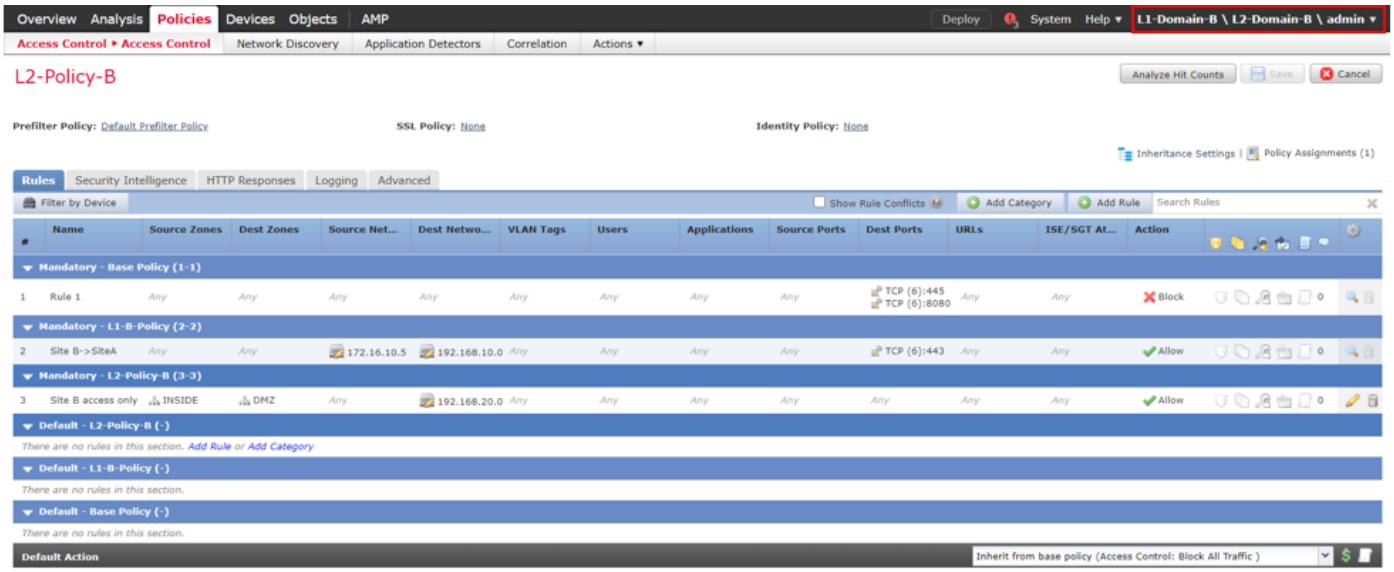
ドメイン階層の構造は次のとおりです。

- **グローバルドメインはL1-Domain-AおよびL1-Domain-Bの親です。**
- **グローバル· ドメインはL2-Domain-Bの祖先です。**
- **L2-Domain-BはL1-Domain-Bの子**
- **L2-Domain-Bは子ドメインがないため、リーフドメインです。**

図は、FMCから見たドメイン階層を示しています。

次のスナップショットは、ルールが上記のシナリオに対して**L1-Policy-A**および**L2-Policy-B** w.r.tでどのように定義されるかを示しています。





正規のトラフィックをブロックしたり、不要なトラフィックを許可したりしないように複数のドメインを設定する場合は、必ずルールとその継承を考慮する必要があります。