Inheritance in Multidomain Environment in FTD

Contents

Introduction

This document describes the configuration and working of inheritance and multi-domain features. This also focuses on a real-world use case to see how these two features work together.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

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

Components Used

The information in this document is based on these software versions:

- Firepower Management Center (FMC) software version 6.4
- Firepower Threat Defense (FTD) software version 6.4

> **Note**: The multi-domain and Inheritance feature support is available on FMC/FTD from 6.0 version onwards.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any configuration.

Background Information

In Policy Inheritance, Access control policies can be nested wherein the Child Policy inherits rules from a Base Policy including the ACP settings such as Security Intelligence, HTTP Response, Logging Settings etc. Optionally the admin can allow the child policy to override the ACP settings such as Security Intelligence, HTTP Response, Logging Settings or else lock the settings so that the child policy cannot override them. This feature is very useful in multi-domain FMC environment.

The multi-domain feature segments user access to FMC's managed devices, configurations and events. A user would be able to switch to/access other domains depending on the privileges. If the multidomain feature is not configured, all managed devices, configurations and events belong to the **Global** domain.

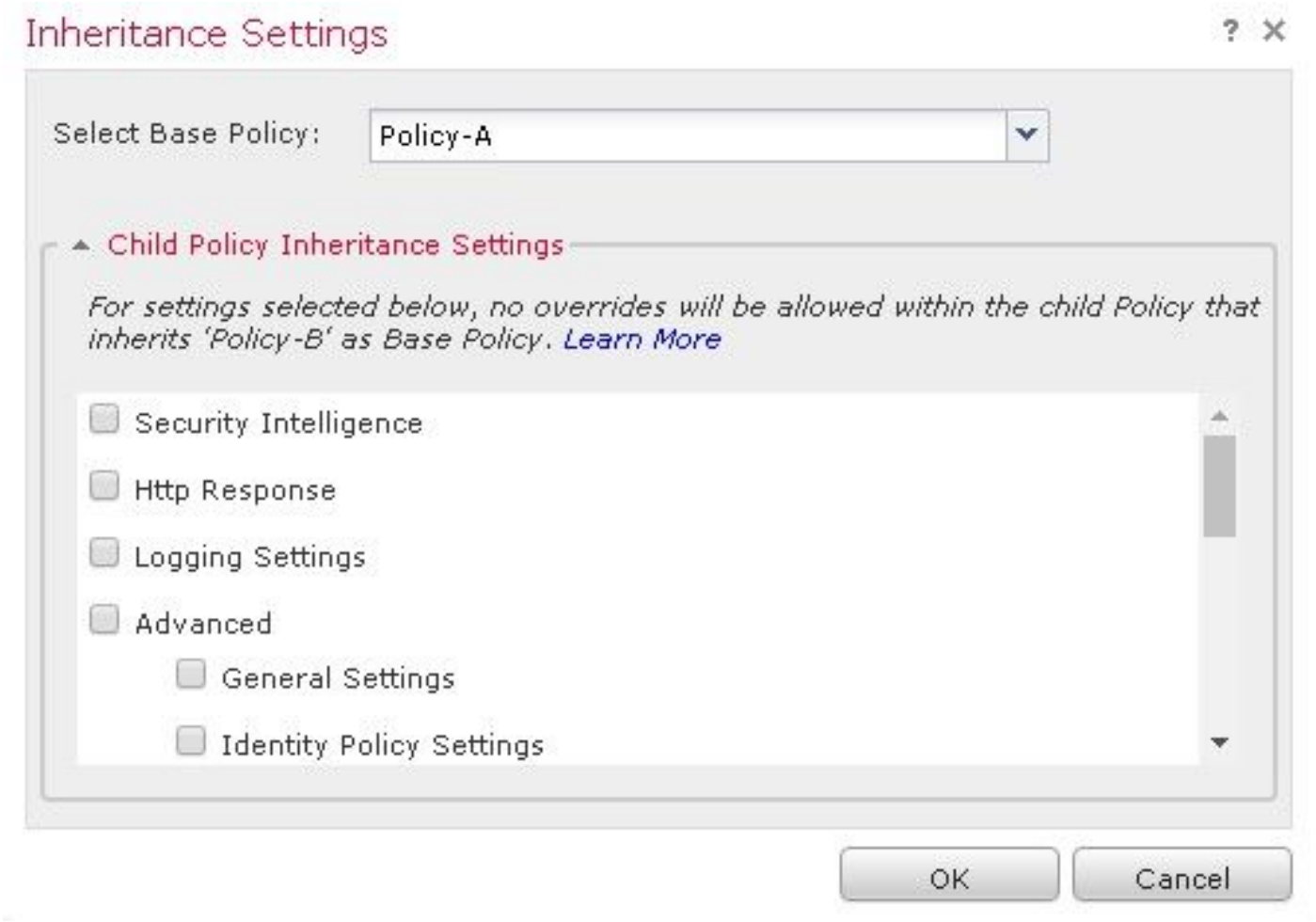
Configure Policy Inheritance

A leaf domain is a domain that does not have further subdomains. A child domain is the next-level descendent of the domain where the user/admin is currently. The parent domain is the direct ancestor of the domain where the user/admin is currently.

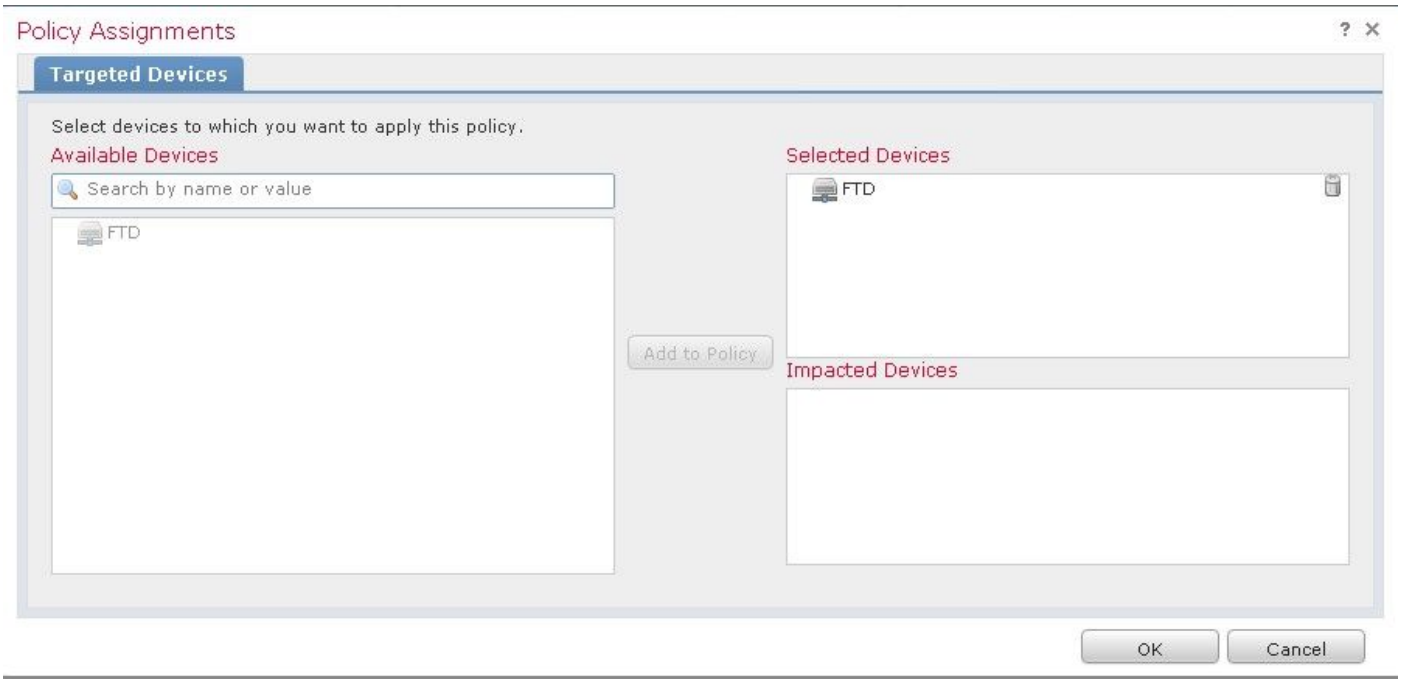
To configure/enable inheritance for policies that exist:

1. Let Policy-A be the Base Policy and Policy-B be the Child Policy (Policy-B inherits the rule from Policy-A)
2. **EDIT** Policy-B and click on **Inheritance Settings** as shown in the image.

3. Choose Policy-A from **Select Base Policy** drop-down list shown below. Other ACP settings such as Security Intelligence, HTTP Response, Logging Settings etc. can be inherited to override settings of Child Policy optionally.

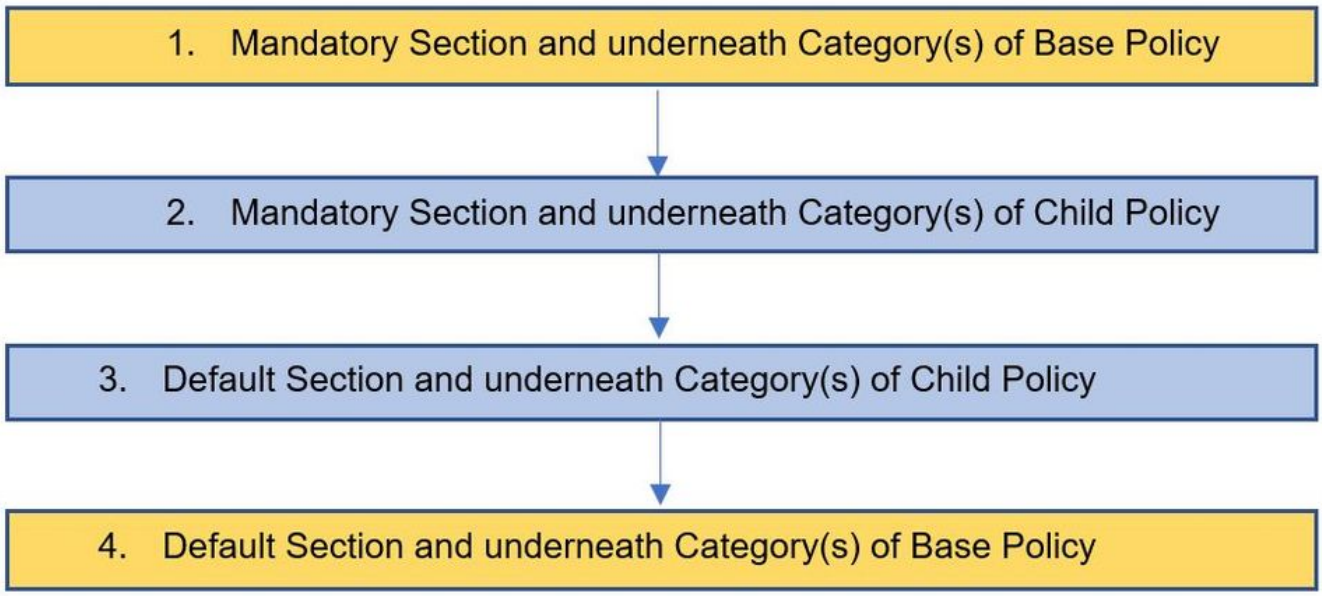


4. Do the **Policy Assignment** for the child policy Policy-B against the intended target FTD device:

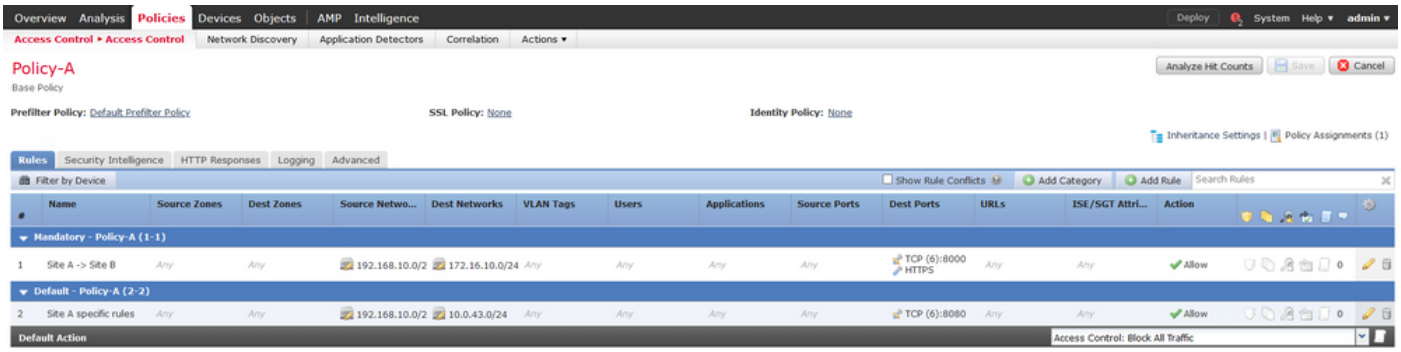


By default, the **Default Action** of Child Policy is inherited and set to **Inherit from base policy** as shown in the image. The user also has the option to select the **Default Action** from the System-Provided Policies as shown here.

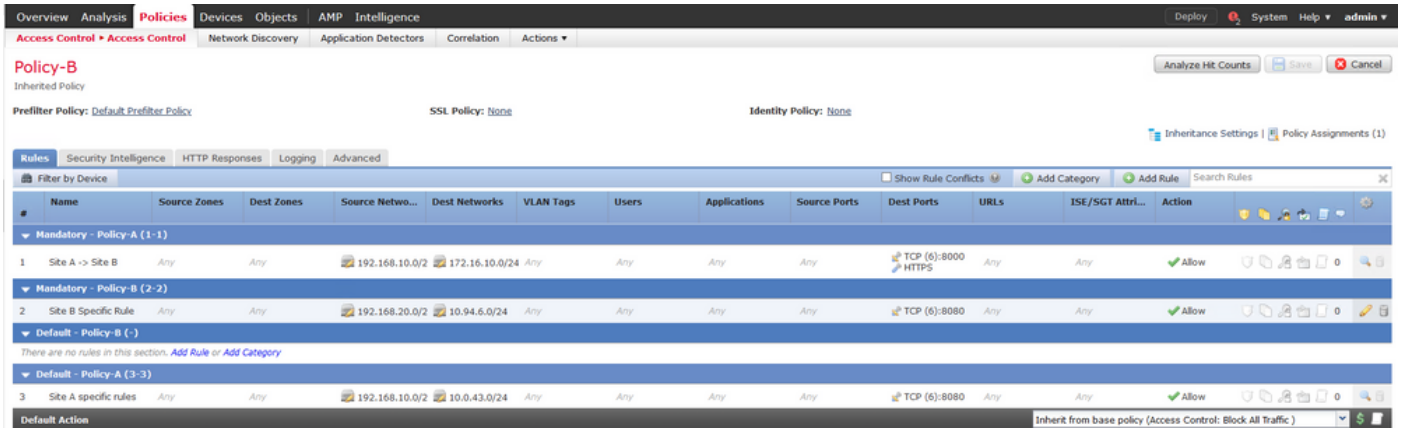
The order of lookup for traffic will always be in a top-down manner irrespective of number of categories added in both Mandatory and Default sections. After you apply the **Inheritance Settings,** the ACP representation for child policy Policy-B (Child Policy) as shown in the image, in-line with the **Order of rule check** mentioned earlier:



This image shows how both the policies namely Policy-A which is the base policy and Policy-B which is the child policy and which is inherited from Policy A would be shown in the FMC.



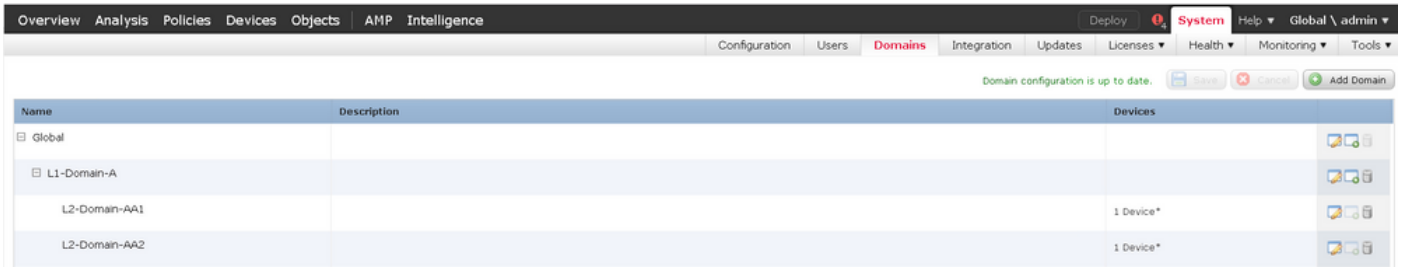
This image shows that in Policy-B, the rules from Policy-A can be seen as well as specific rules configured in Policy-B itself. Care should be taken as to how the rules should be configured keeping in mind the order.



FTD Management in Multi-Domain FMC Environment

The multidomain feature segments user access to managed devices, configurations, and events. A user would be able to switch to other domains depending on the privileges. If the multidomain feature is not configured, all the managed devices, configurations, and events belong to the **Global** domain.

A maximum of three-level domains can be configured with Global Domain as level one. All managed devices must belong to the leaf domain only. This can be confirmed from the symbol of the  (Add Sub Domain) being grayed out in the leaf domain as shown in the image.



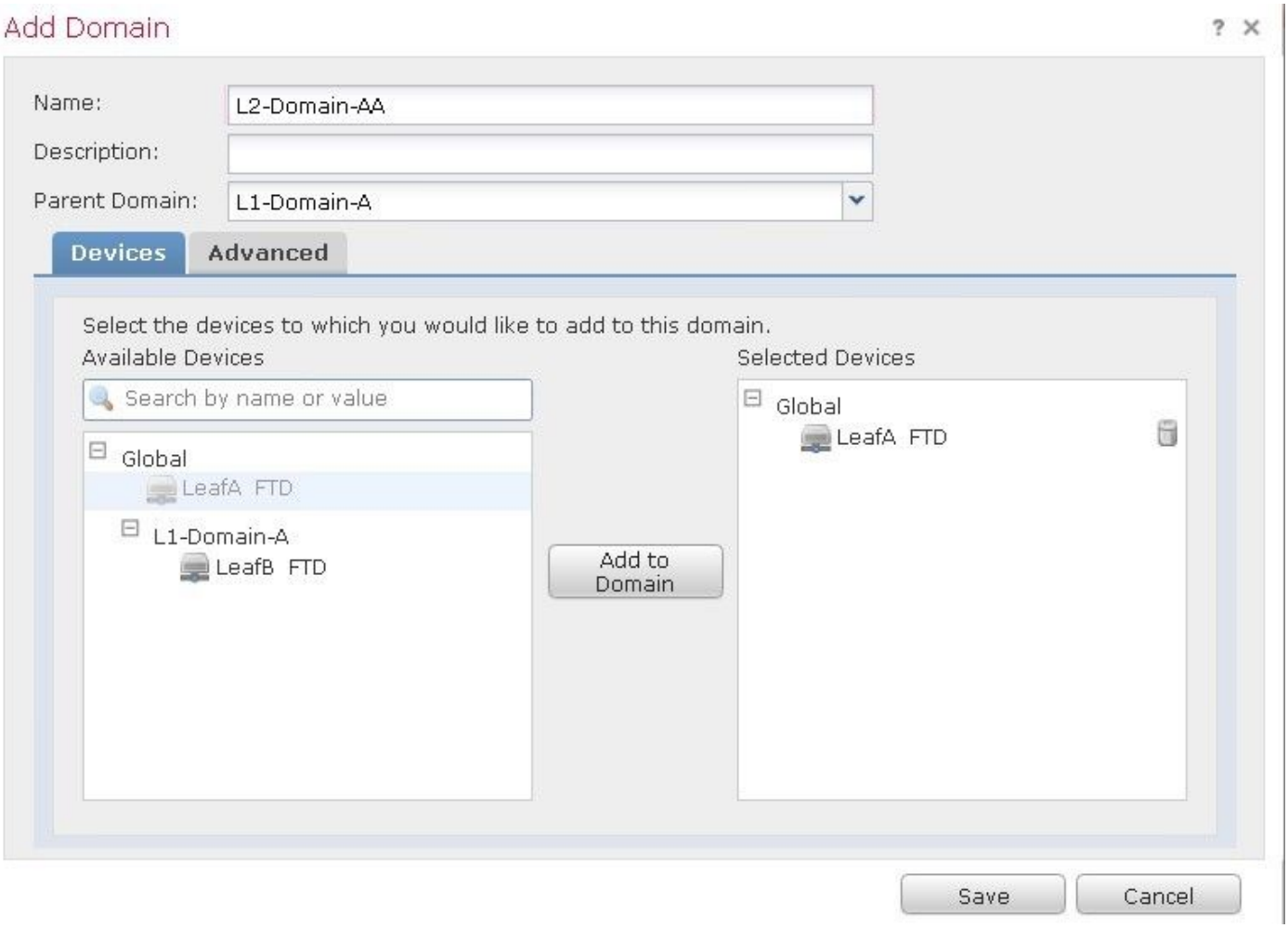
Domain Configuration

The domain configuration can be done as follows:

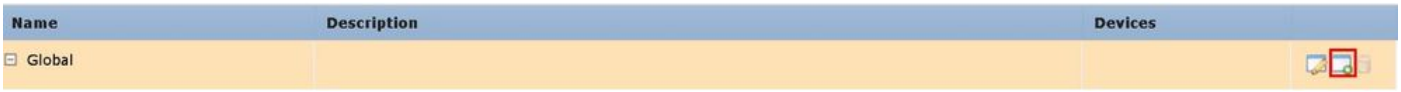
1. Navigate to **System > Domains**. By default, the **Global** domain is present.

2. Click on **Add Domain** as shown in the image.

3. The **Add Domain** dialog box appears. Type the **Name** of the domain and select the **Parent Domain** from drop-down list. If this is the leaf domain, the FTD device(s) needs to be added to the domain as shown in the image.

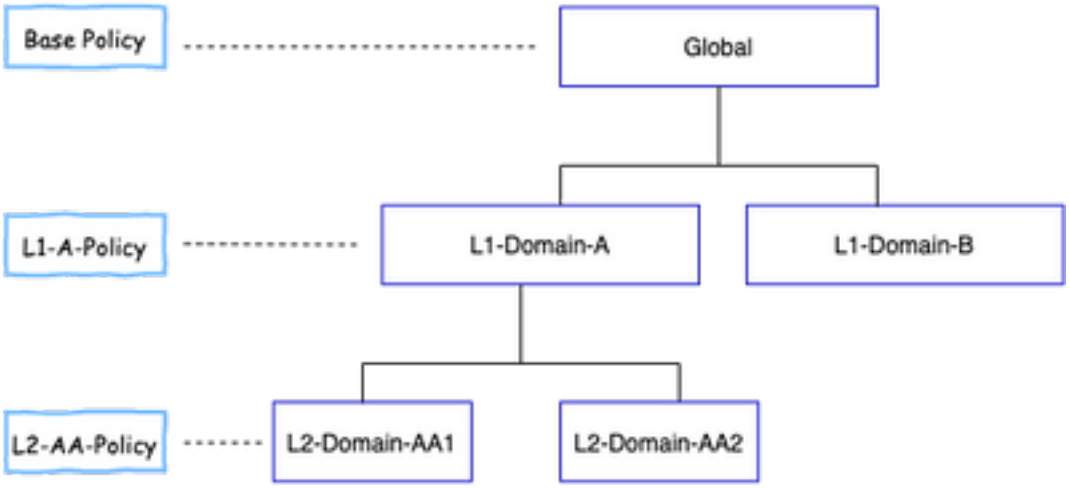


Note: In order to add the domains, click on the **Add Sub Domain** icon as shown in the image. Here the parent domain is already selected.



Policy Visibility & Control in a Multi-Domain FMC Environment

Policy visibility and control is limited to respective domain users except for an Admin of **Global** domain. This example is based on the hierarchy as follows:



Visibility: As shown in this image, the default view **Policies** page lists policies (ACP) configured under the respective domain.

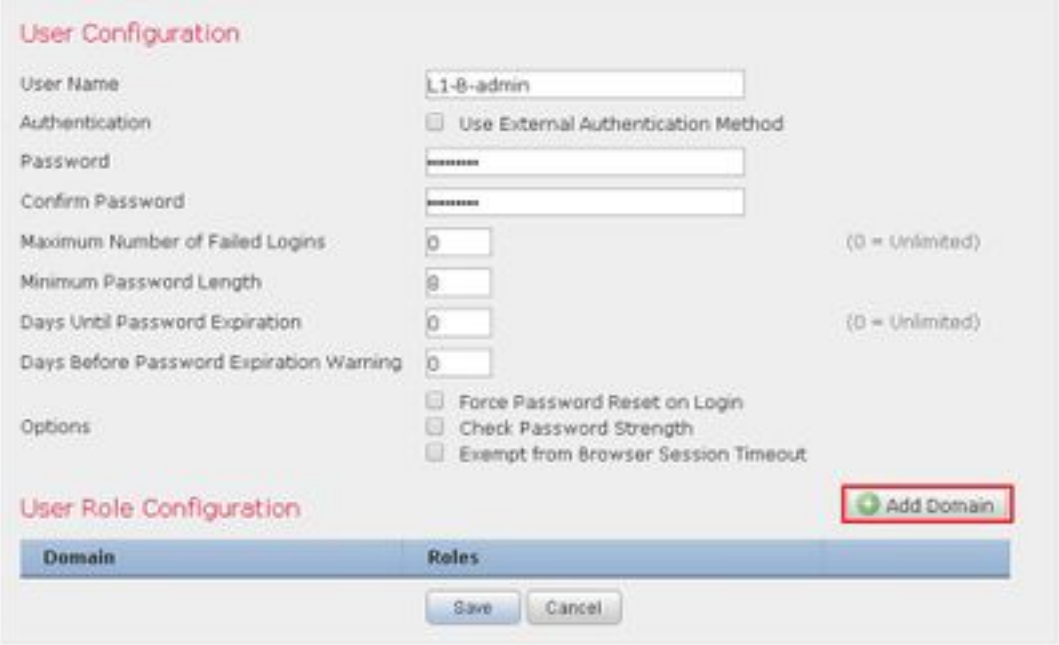
Control: **Admin** users, that belong to the respective domain can EDIT the policies. To edit the policies, which belong to other domains (say as part of Inheritance), one has to switch the domain from current to a Domain where the Policy is configured under. Only Admin user/s belonging to **Global** domain or L1 Domain can switch around the lower domain for policy management.

Add Users to Domain

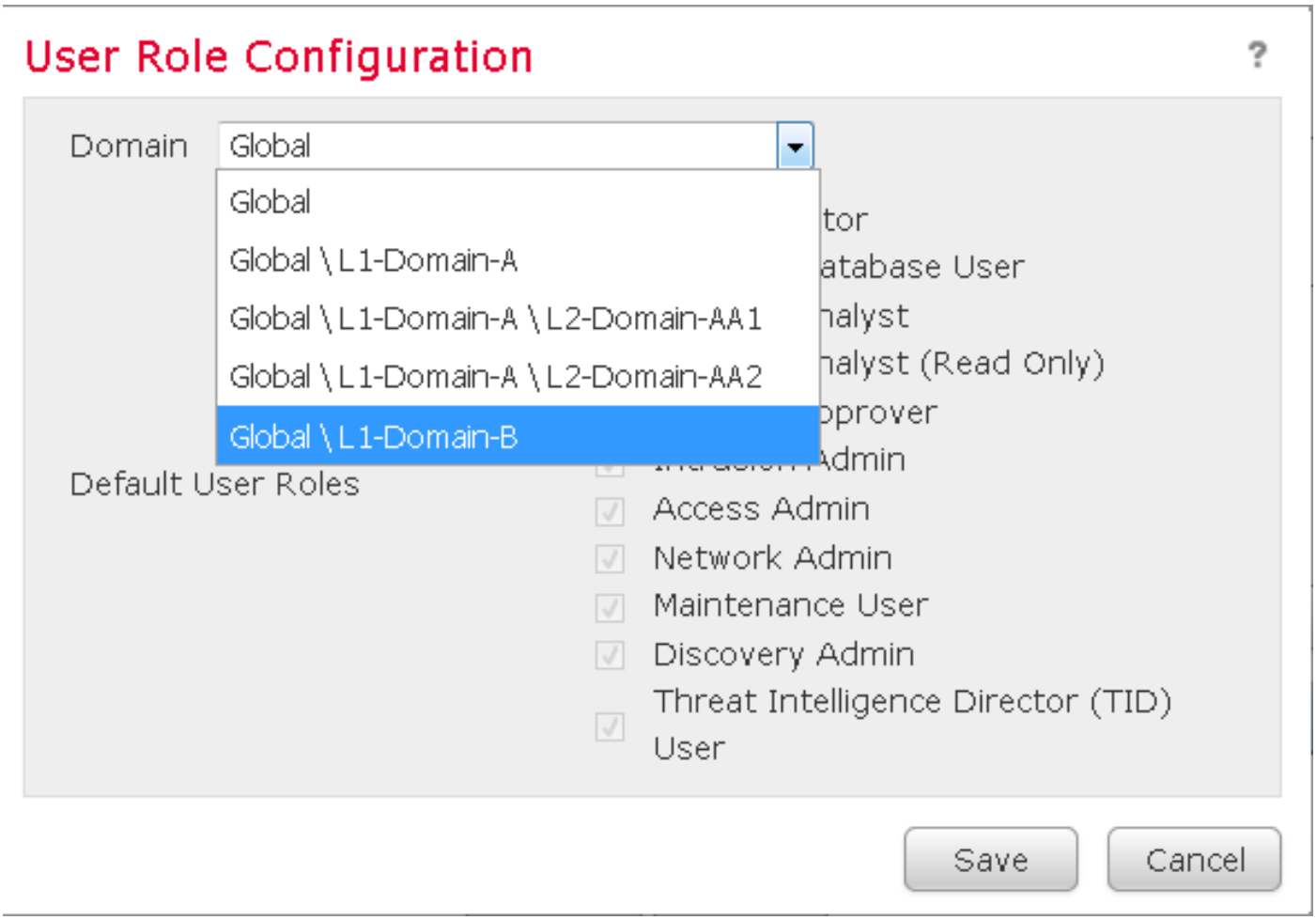
This shows how to add users in a particular domain. This procedure is applicable to users in the local database.

1. Navigate to **System >Users**. Click on **Create User** as shown in the image.

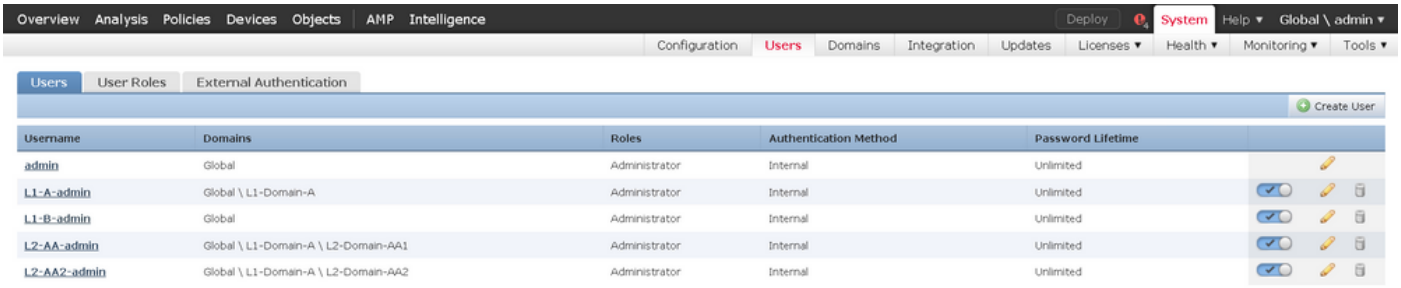
2. The **User Configuration** dialog box appears. Fill in the **User Name** and the **Password (& Confirm Password)**. Click on **Add Domain** to add the user to the specified domain as shown in the image.



3. Choose the intended domain from **Domain** drop-down list where you wish to add the user under and specify the role as shown in the image. A new user can be added to the own domain or the child domains.

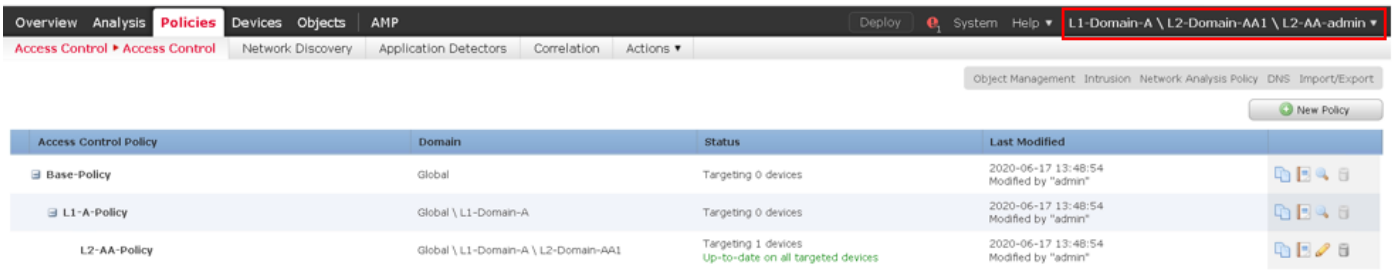


The users configured are shown in this image:

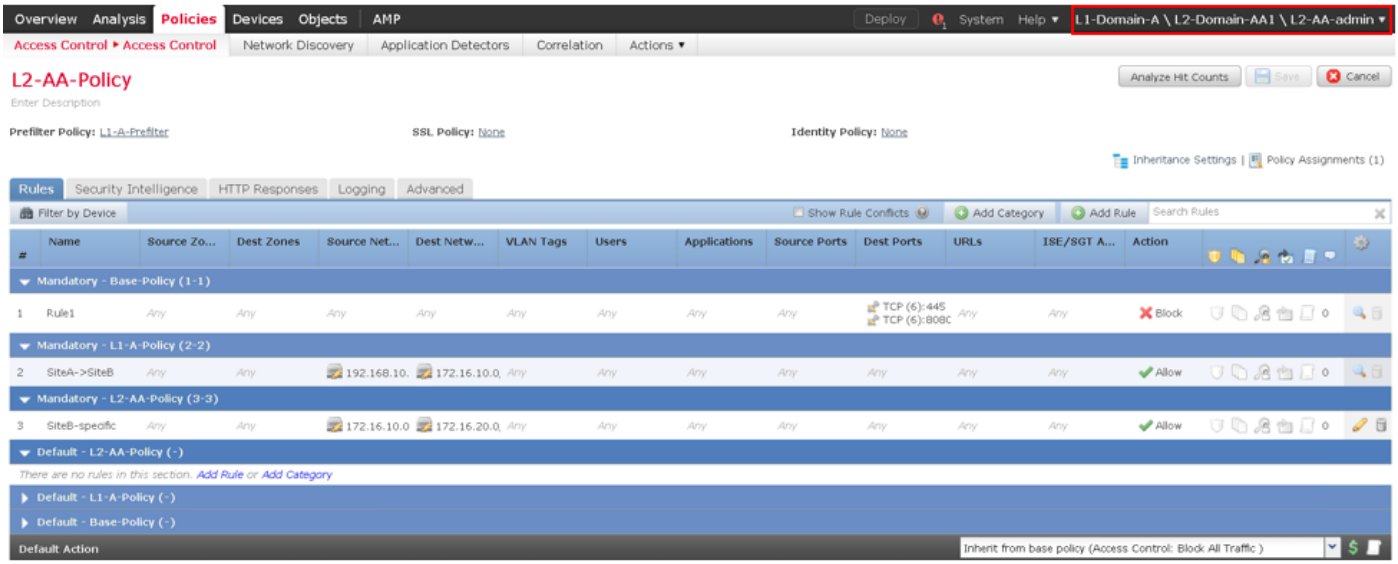


Resource access on FMC would be limited to the domain to which the user belongs to. As shown below, when user- **L1-A-admin** logs into FMC UI, access is limited to Domain- **L1-Domain-A** which the user is part of, and to the child domain once the user switches to that child domain. This user can edit only the policy defined in the **L1-Domain-A** domain and the policy defined in the child domain when the domain is switched to its child domain. Also, it can be seen from the below example that **L1-A-Policy** inherits the policy defined in the global domain namely **Base-Policy** as well as can be edited which can be seen from the  sign. The inheritance settings are made to point to the **Base-Policy** as shown in the image.

Similarly, a user **L2-AA-admin** belonging to the **L2-Domain-AA1** domain only has control of the policy **L2-AA-Policy** defined in the domain as shown in the image. The **L2-AA-Policy** inherits the policy **L1-A-Policy** defined in **L1-Domain-A** which in turn inherits **Base-Policy** defined in Global domain. Additionally, the policy **L2-AA-Policy** can be edited which can be seen from the  sign. The user L2-AA-admin can never switch to its parent domain namely L1-Domain-A nor its ancestor domain namely the global domain.



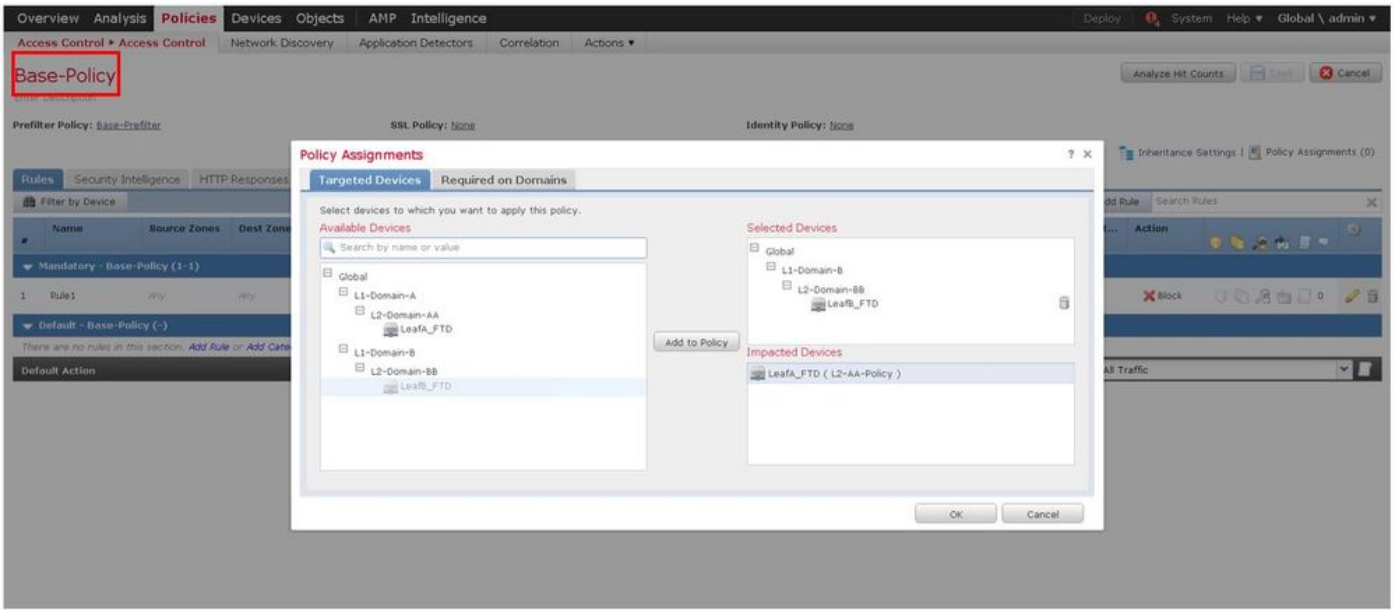
Also, a user **L1-A-admin** belonging to L1-Domain-A can switch to L2-Domain-AA1 and edit the policy **L2-AA-Policy** which is seen from the  sign as shown in the image. This is applicable even to a user belonging to the global domain and switching to the child domains and editing the policies defined in the particular child domain.



Important points to note:

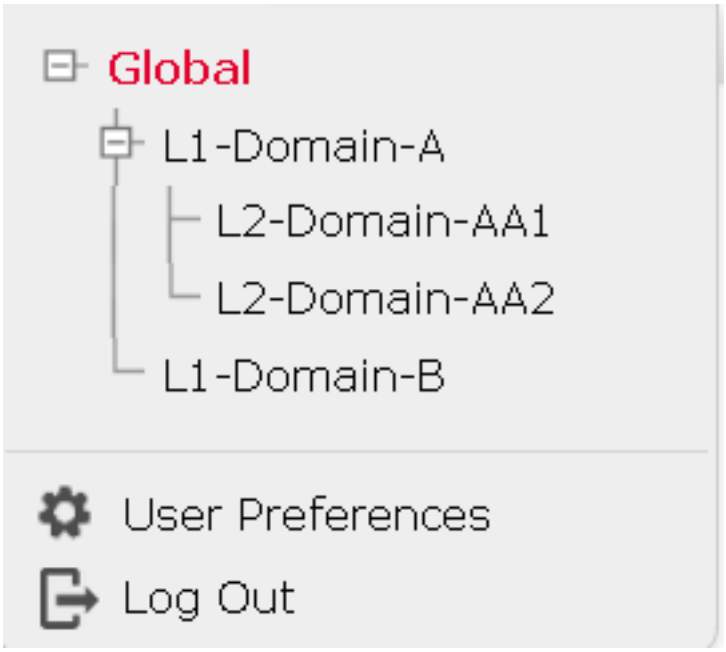
- On deleting the non-global domains, the users belonging to the domains are automatically moved to the **Global** domain.

  The FTD/s is/are always defined in the leaf domain. In this case, the leaf domain is the **L2-Domain**(i.e. L2-Domain-AA & L2-Domain-BB). The FTD belonging to **L2-Domain** can be assigned to the policy in **L1-Domain** or in the **Global** Domain. In this image, the ACP in the Global domain assigned the FTD defined in the L3 domain to the policy defined in the Global domain.

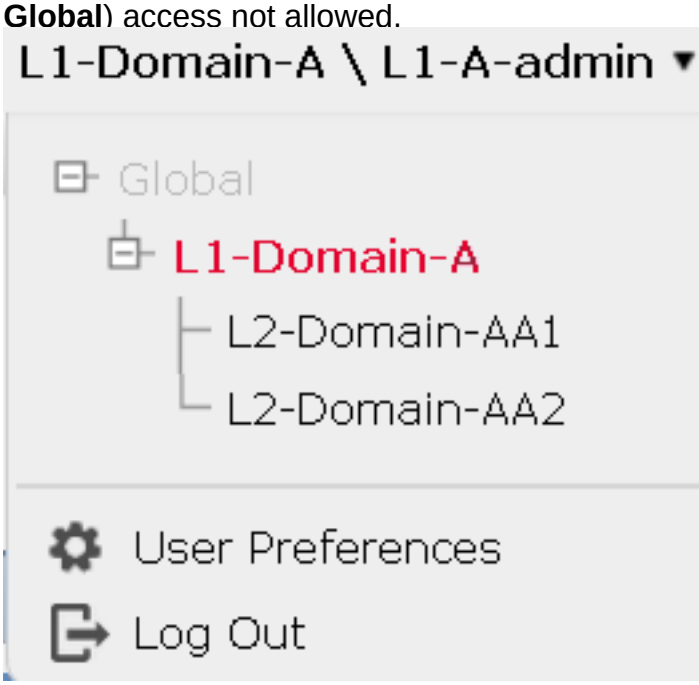


- Users in the global domain can navigate to other user-specific domains but users from a specific domain only have visibility in their own domain and their child domains. They cannot navigate to the global domain or any other higher domains, as shown in this table:

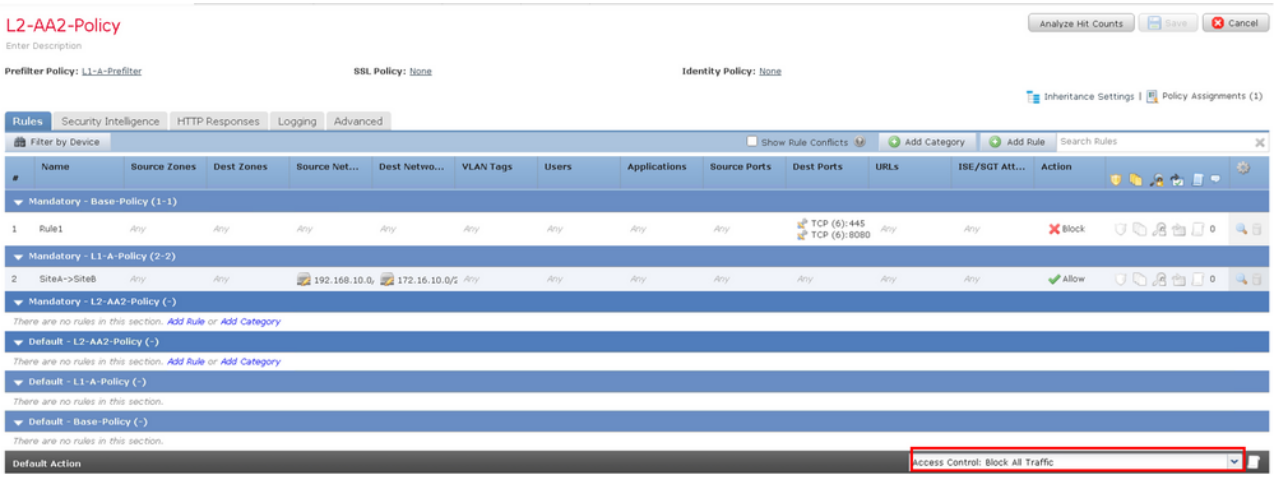
Global Domain	**User-Specific Domain**
User in the global domain has visibility to all domains configured and can navigate to other domains.	User in **L1-Domain-A** will have visibility only to se and its child domain namely- **L2-Domain-AA** and navigate to **L2-Domain-AA**. Higher-level domain



Global) access not allowed.



- The default action of the child policy cannot be locked by the parent policy and the user need not inherit the default action of the parent policy as in this image.



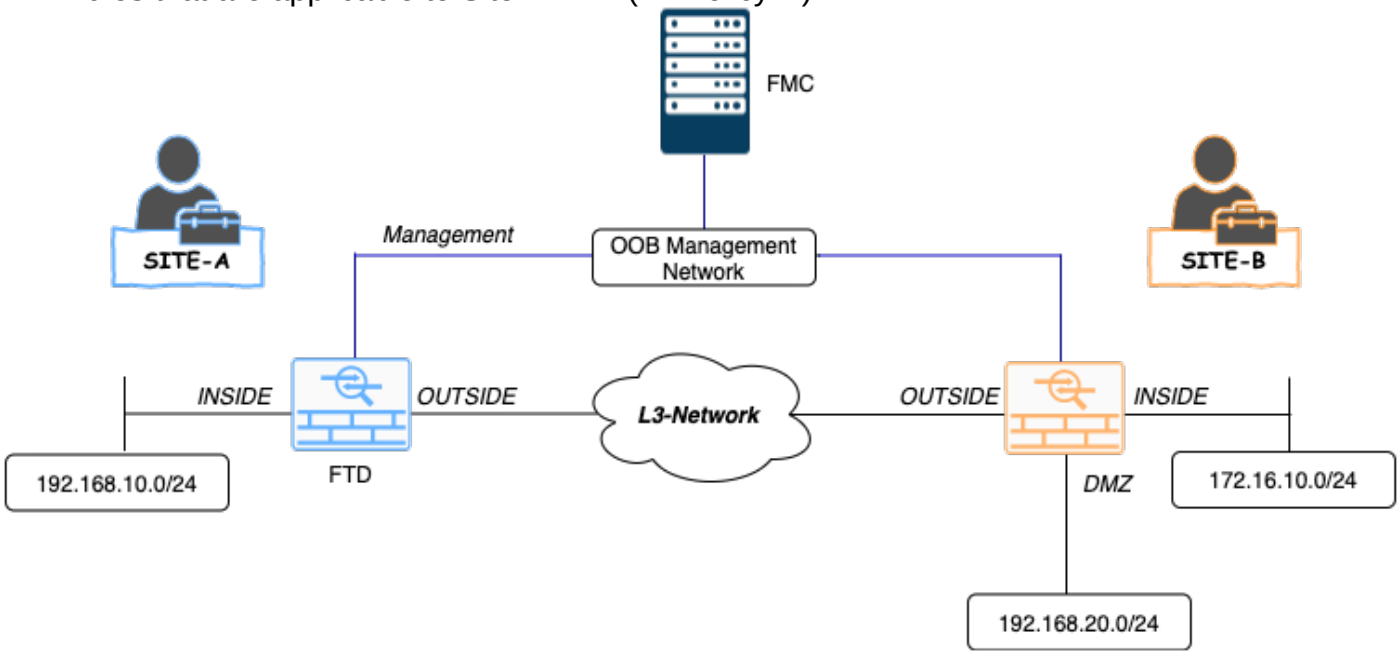
In this image, it can be seen that the user has not assigned the default action as that of the parent which can be evident from the words **Inherit from base policy:** not being seen in default action.

Note: It should be kept in mind that a user cannot view both the L1/L2 domain policies at the same time. The user needs to switch to the desired domain to view and edit the policies. For example: if user **admin** present in the global domain wants to view what policies are configured in L1-Domain-A and L2-Domain-AA, the user can do so by switching to L1-A-Domain to view and edit the policy configured in that domain and then switching to L2-Domain-AA to view and edit the corresponding policy but cannot view both at the same time. Also, user in L1-Domain-A cannot edit or delete the policy defined in the global domain i.e. Base Policy which is the parent policy of L1-A-Policy, and user in L2-Domain-AA cannot edit or delete the polices namely Base Policy and L2-A-Policy defined in global and L2-Domain-A domains respectively.

Use Case Scenario

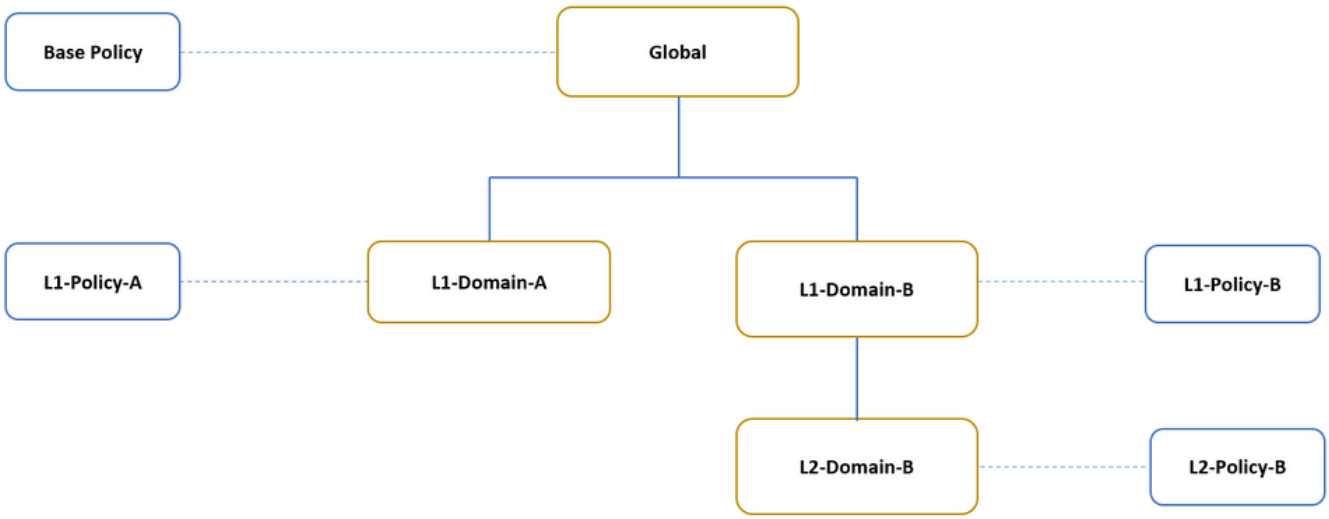
Consider the scenario depicted in the image, FTDs of SITE-A (SiteA-FTD) and SITE-B (SiteB-FTD) are managed by a single FMC via different Domains (multi-domain) to provide controlled access. From a policy standpoint these are the policy considerations at an organization level:

- Service-specific BLOCK rules that are applicable to ALL FTDs independent of SITE or DOMAIN belong to (Base-Policy).
- Rules that meet the requirements to meet Site-A to Site-B access (L1-Policy-A) and Site-B to Site-A access (L1-Policy-B).
- Rules that are applicable to Site-B FTD (L2-Policy-B).



Inheritance in a Multi-Domain Environment

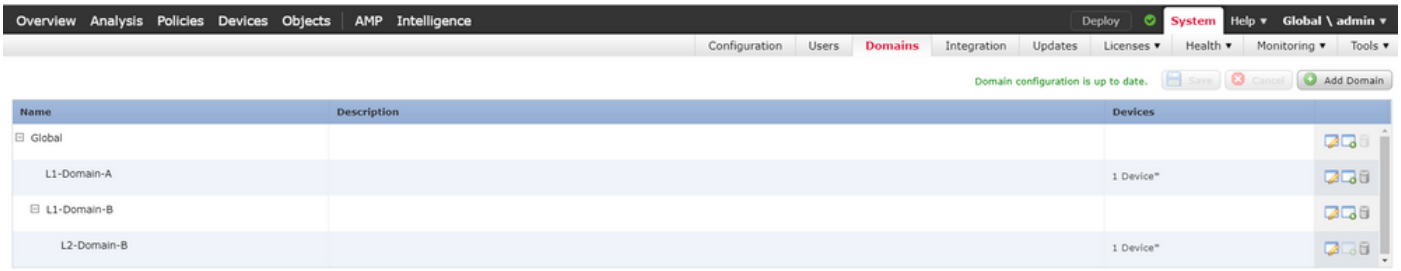
For the use case mentioned above, consider the following Domain/ Policy hierarchy. SiteA-FTD and SiteB-FTD are part of leaf-domains L1-Domain-A and L2-Domain-B respectively.



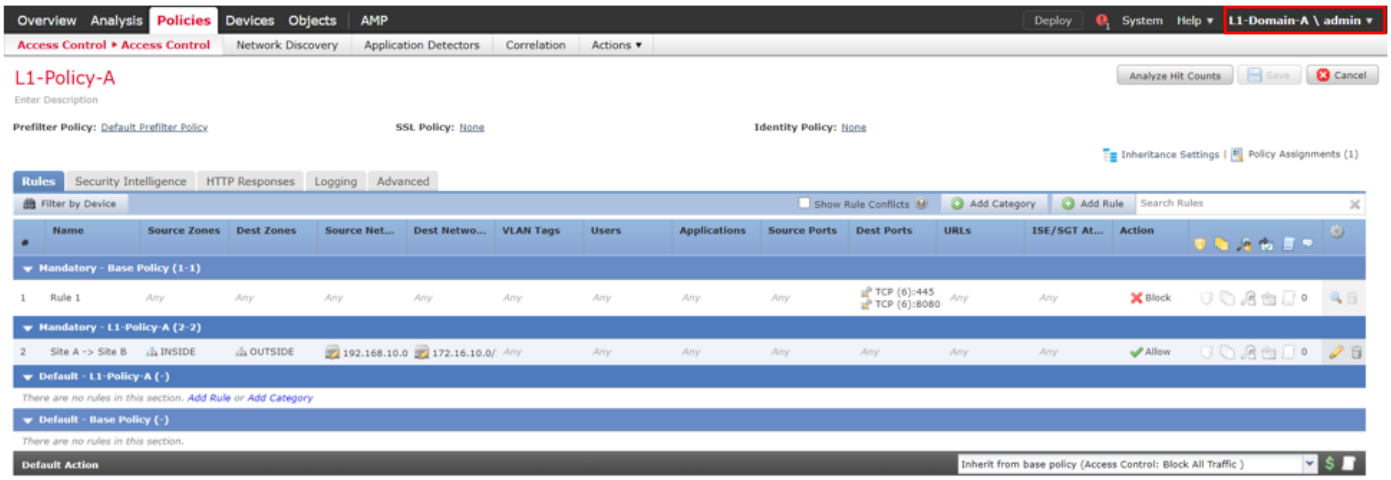
The structure for the domain hierarchy is as follows:

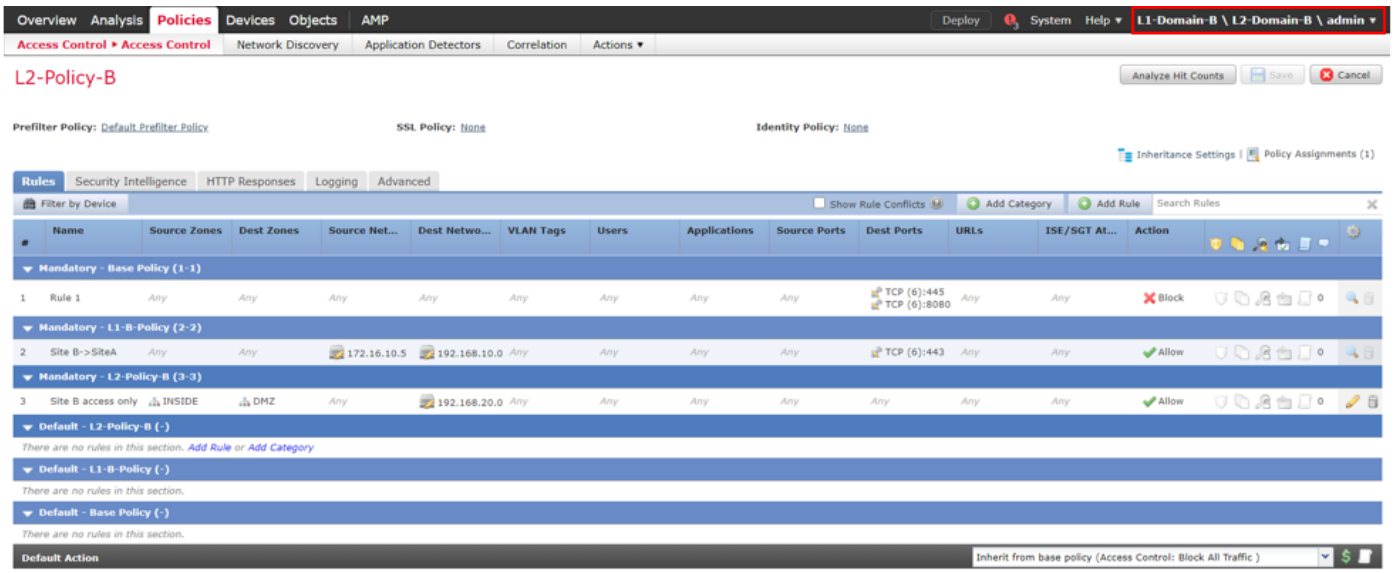
- **Global** domain is **parent** of **L1-Domain-A** and **L1-Domain-B**.
- **Global** domain is **ancestor** of **L2-Domain-B**.
- **L2-Domain-B** is child of **L1-Domain-B**
- **L2-Domain-B** is leaf domain as it does not have child domains.

The image shows the domain hierarchy as seen from FMC.



The below snapshot shows how the rules are defined in **L1-Policy-A** and **L2-Policy-B** w.r.t to the above scenario.





You should always consider the rules and their inheritance in mind when configuring multiple domains to avoid blocking legitimate traffic or allowing unwanted traffic.