FTD中多域环境的继承

目录

简介

本文档介绍继承和多域功能的配置和工作方式。此外，本文档还重点介绍一个真实的使用案例，以了解这两个功能如何协同工作。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- Firepower管理中心(FMC)
- Firepower威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件版本：

- Firepower管理中心(FMC)软件版本6.4
- Firepower威胁防御(FTD)软件版本6.4

注意：从6.0版开始，FMC/FTD上提供多域和继承功能支持。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何配置的潜在影响。

背景信息

在策略继承中，访问控制策略可以嵌套，其中子策略从基本策略继承规则，包括安全情报、HTTP响应、日志记录设置等ACP设置。 或者，管理员可以允许子策略覆盖ACP设置，如安全情报、HTTP响应、日志记录设置，或者锁定设置，以便子策略无法覆盖它们。此功能在多域FMC环境中非常有用。

多域功能将用户对FMC受管设备、配置和事件的访问分段。用户可以根据权限切换到/访问其他域。如果未配置多域功能，则所有受管设备、配置和事件都属于**全局**域。

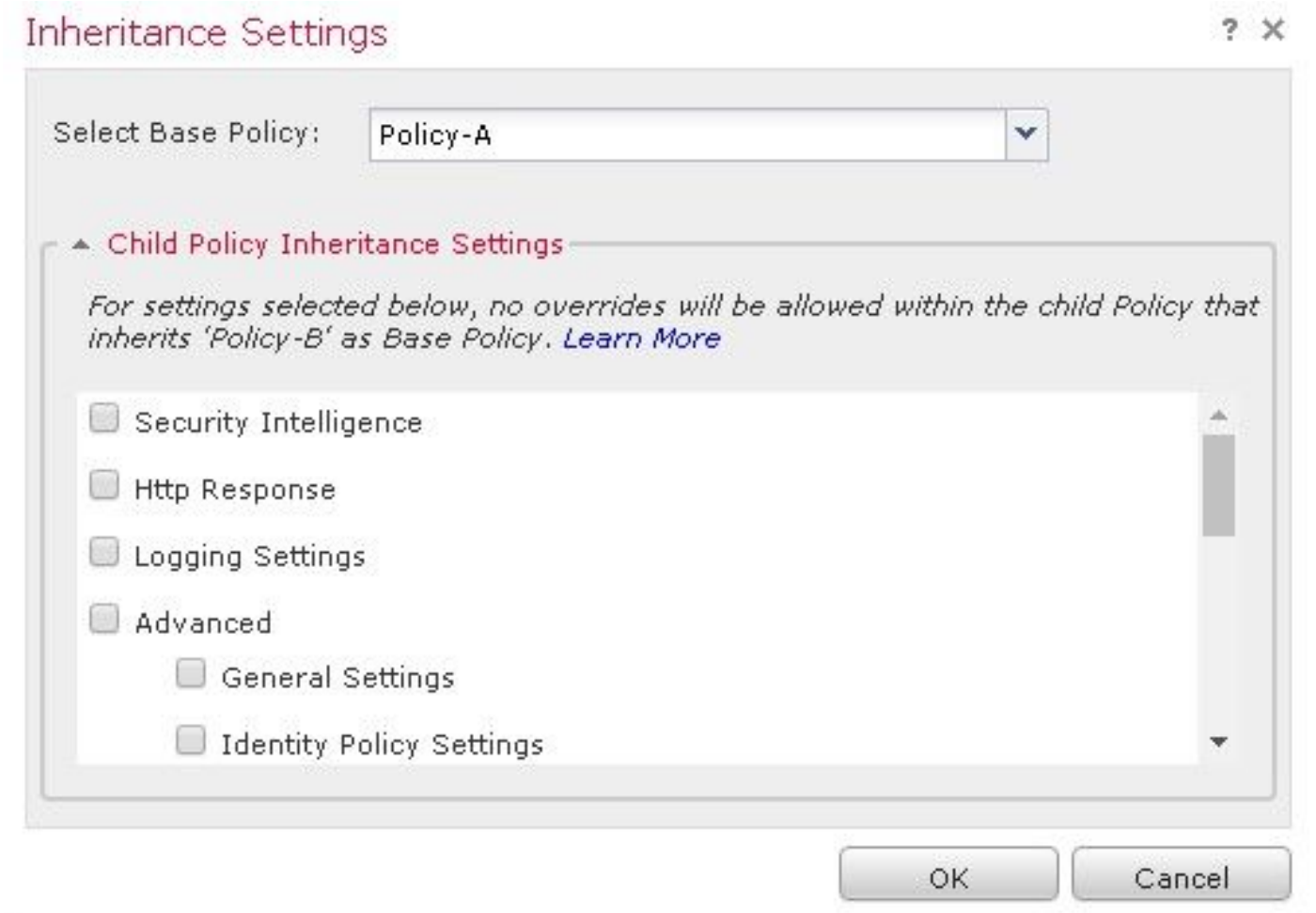
配置策略继承

枝叶域是没有其他子域的域。子域是用户/管理员当前所在域的下一级后代。父域是用户/管理员当前所在域的直接祖先。

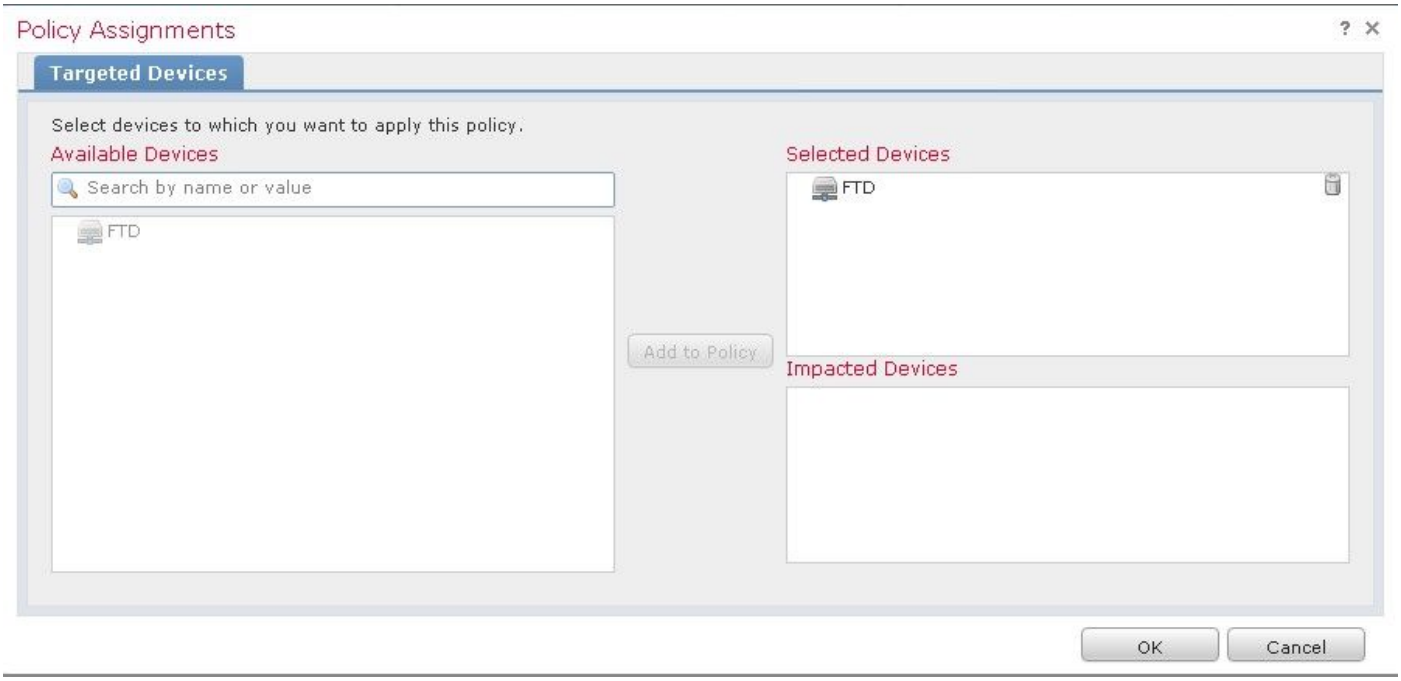
要配置/启用现有策略的继承，请执行以下操作：

1. 让策略A作为基本策略，策略B作为子策略（策略B继承策略A的规则）
2. **编辑**Policy-B，然后单击**Inheritance Settings**，如图所示。

3.从如下所示的“选择基**本策略”下**拉列表中选择策略A。其他ACP设置（如安全情报、HTTP响应、日志记录设置等）可以继承，以可选地覆盖子策略的设置。

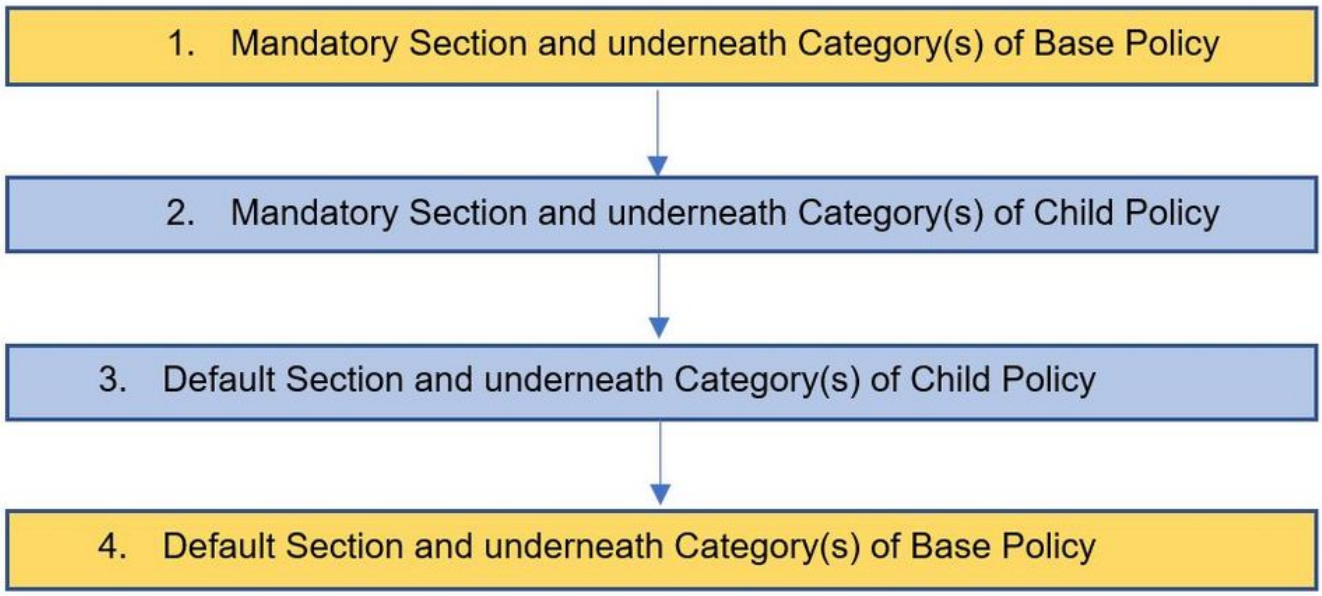


4.针对目标**FTD设**备对子策略Policy-B执行策略分配：

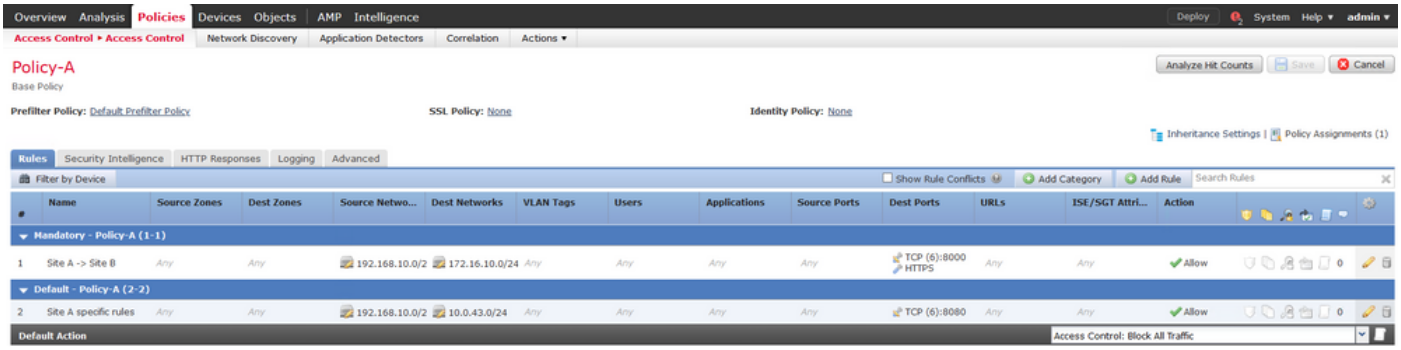


默认情况下，子**策略的**默认操作会继承并设置为**从基本策略**继承，如图所示。用户还可以选择从系统提供的策略**中选**择默认操作，如下所示。

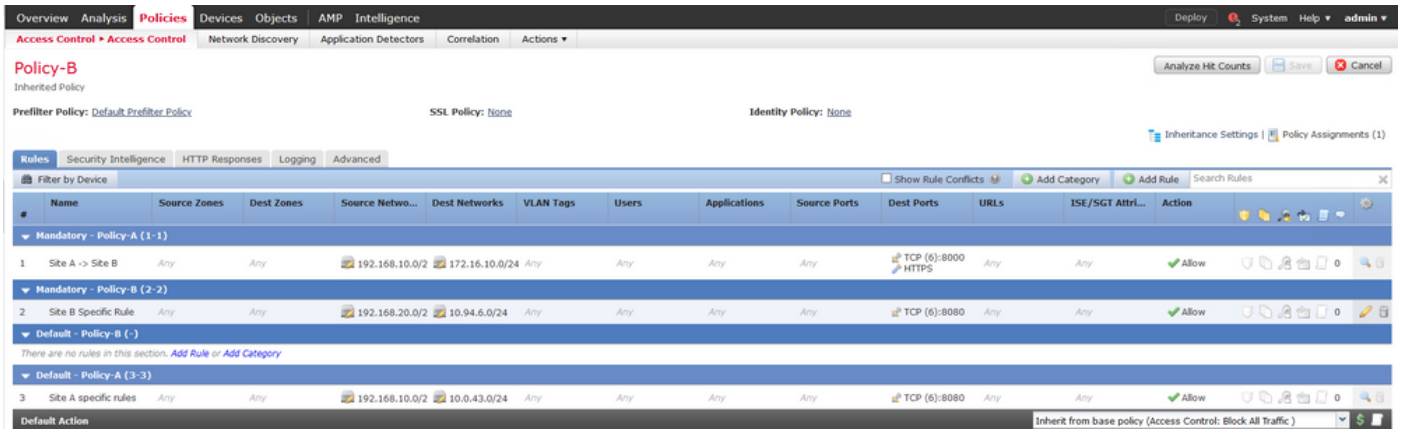
无论在Mandatory和Default部分中添加的类别数量如何，流量的查找顺序始终采用自上而下的方式。应用继承设**置后，**子策略Policy-B（子策略）的ACP表示形式如图所示，与前面提到的规则**检查顺**序一致：



此图显示策略A（基本策略）和Policy-B（子策略）（从策略A继承）如何在FMC中显示。



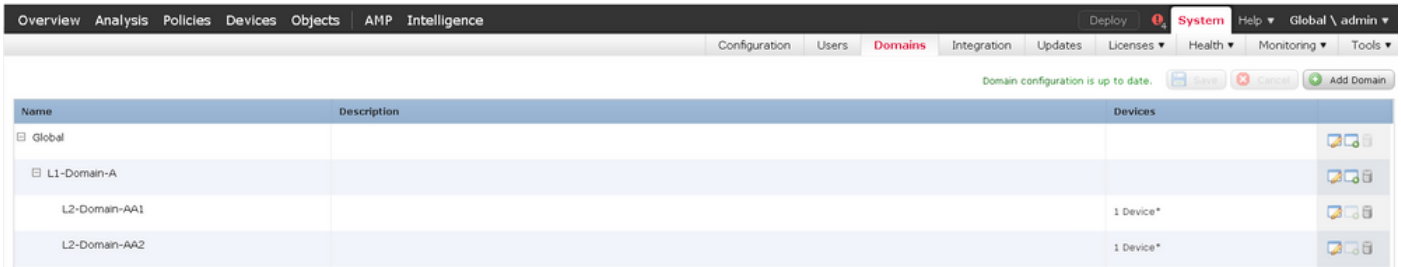
此图显示，在Policy-B中，可以看到Policy-A的规则以及Policy-B本身配置的特定规则。应注意如何配置规则，以保持顺序。



多域FMC环境下的FTD管理

多域功能将用户对受管设备、配置和事件的访问分段。用户可以根据权限切换到其他域。如果未配置多域功能，则所有受管设备、配置和事件都属于**全局**域。

最多可以将全局域配置为第1级。所有受管设备必须仅属于叶域。这可以从  （添加子域）在枝叶域中灰显，如图所示。



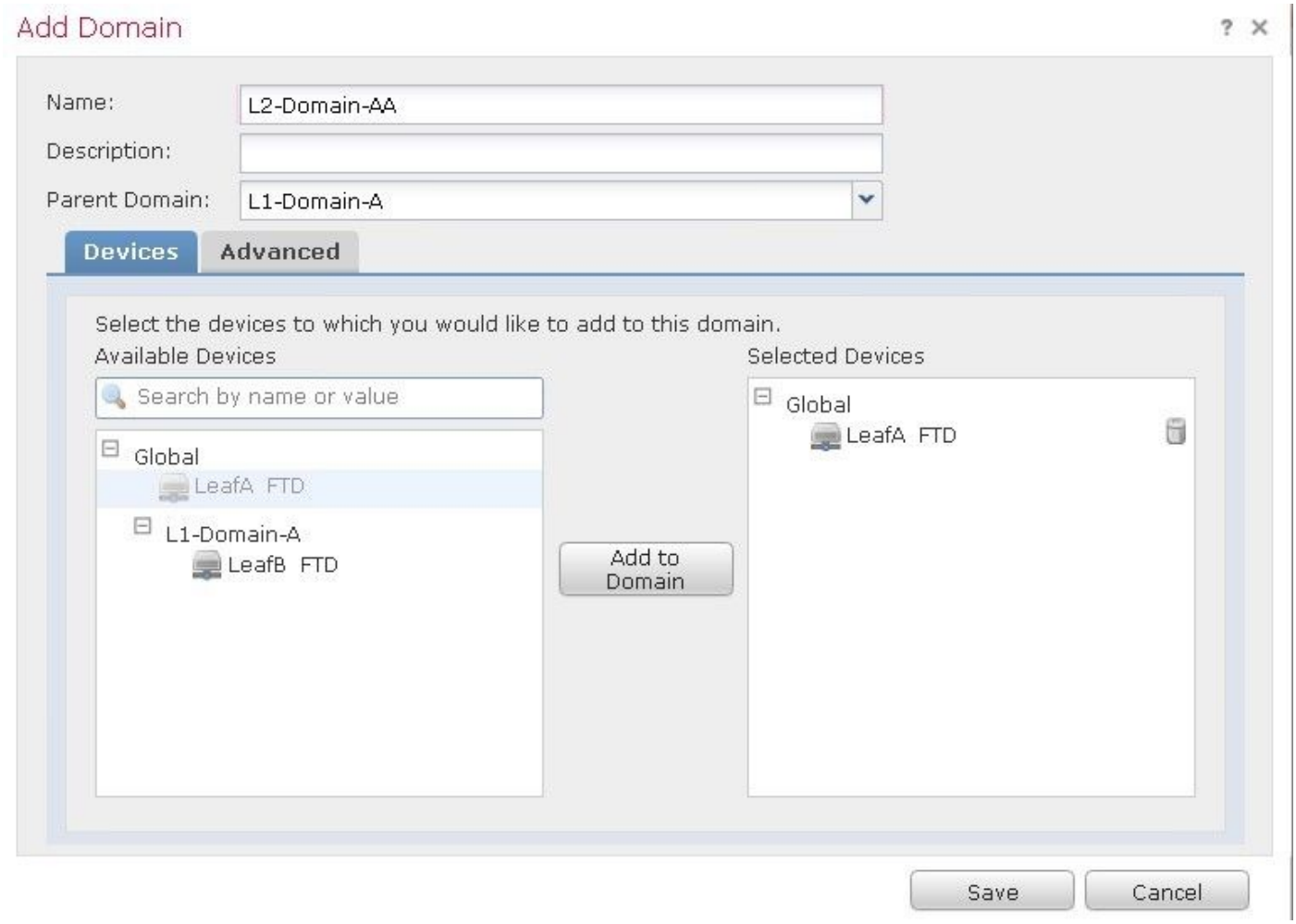
域配置

域配置可以如下执行：

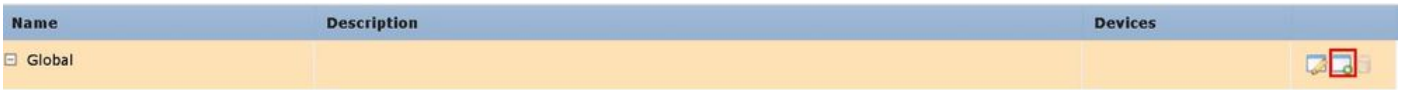
1. 导航至**系统>域**。默认情况下，**全局**域存在。

2. 单击“**添加域**”，如图所示。

3.出现“**添加域**”对话框。键入域**的名**称并从下拉列表中选择**父域**。如果这是枝叶域，则需要将FTD设备添加到域，如图所示。

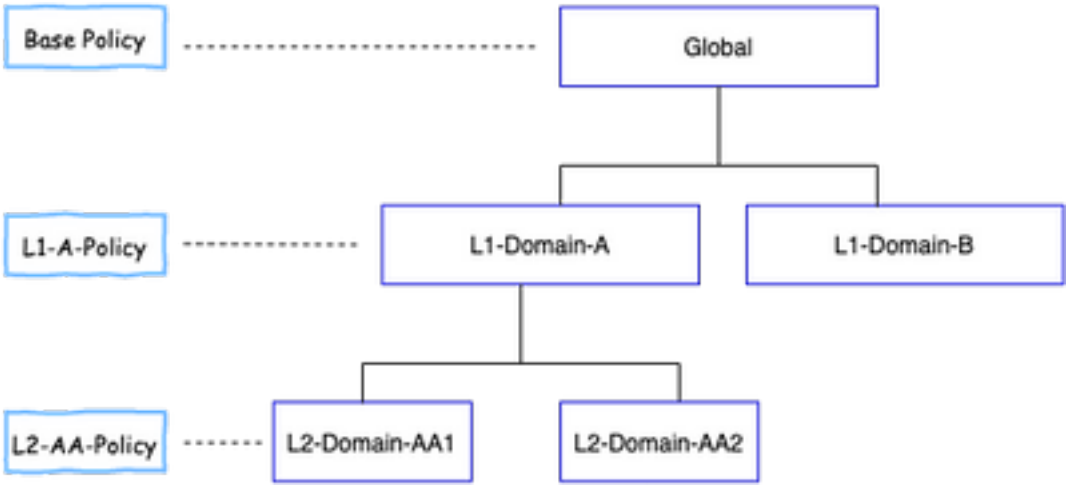


注意：要添加域，请单击添加子域**图标(如**图所示)。此处已选择父域。



多域FMC环境中的策略可视性与可控性

策略可视性与可控性仅限于各个域用户，全局域的管理**员除**外。此示例基于以下层次结构：



可视性：如此图像所示，默认视图“策**略**”页面列出在相应域下配置的策略(ACP)。

控制：**属**于相应域的管理员用户可以编辑策略。要编辑属于其他域（例如作为继承的一部分）的策略，必须将域从当前域切换到在其下配置策略的域。只有属于全局域或L1域**的管**理员用户可以在较低域周围切换以进行策略管理。

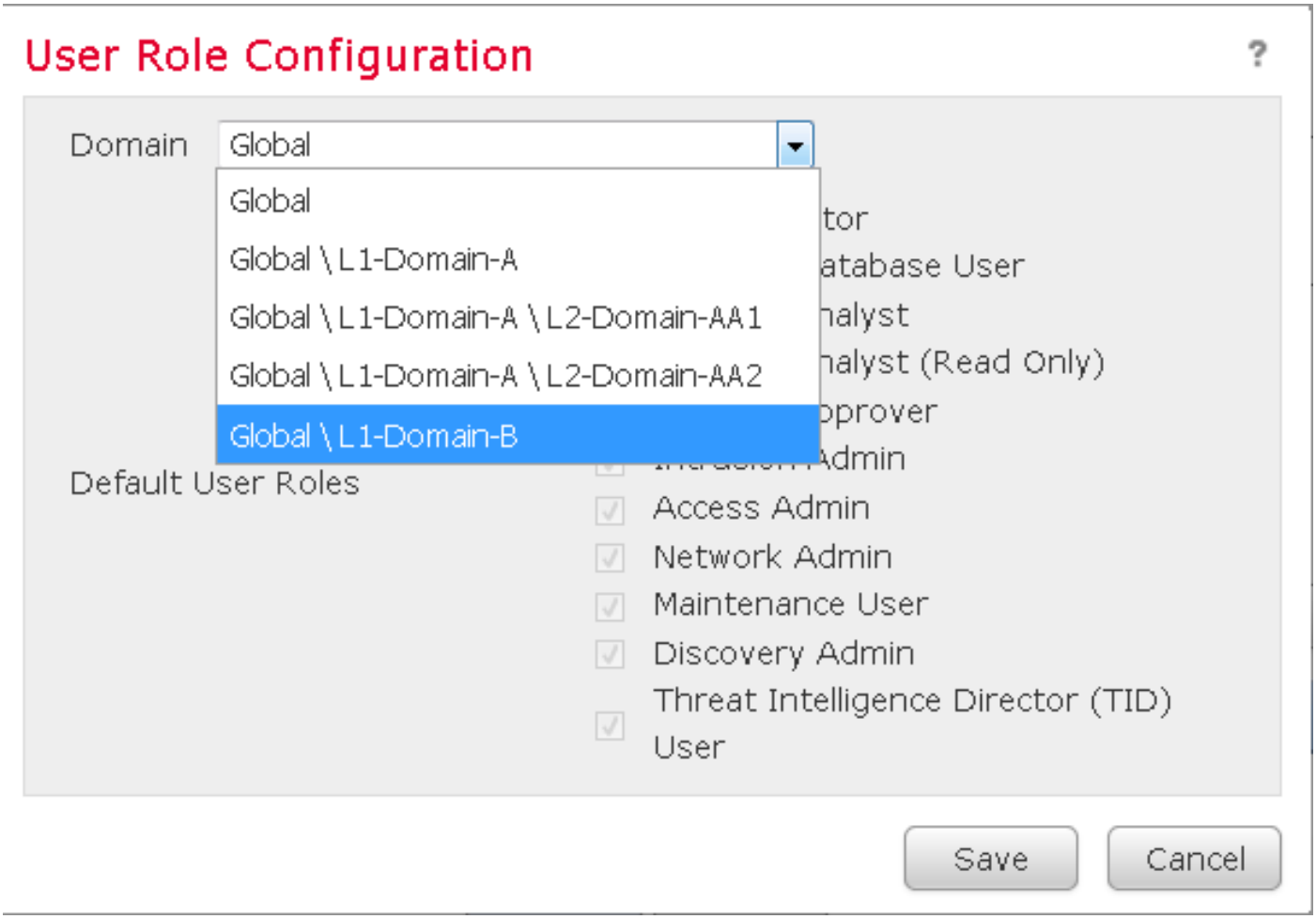
将用户添加到域

这显示如何在特定域中添加用户。此过程适用于本地数据库中的用户。

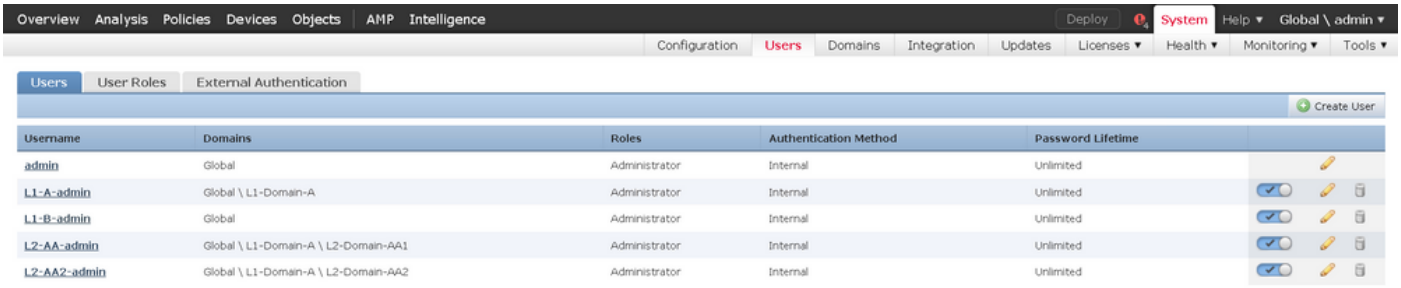
1. 导航至**System > Users**。单击“**创建用**户”，如图所示。

2.出现“**用户配置**”对话框。填写“用**户名**”和“**密码**”（**&确认密码**）。 单击**Add Domain**将用户添加到指定域，如图所示。

3.从“域”下拉列表中**选择**要在其下添加用户的目标域，并指定角色，如图所示。新用户可以添加到自己的域或子域。

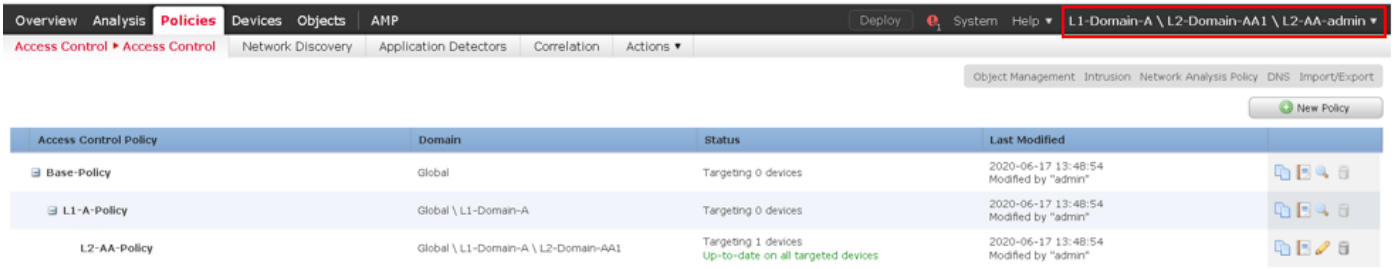


配置的用户显示在下图中：

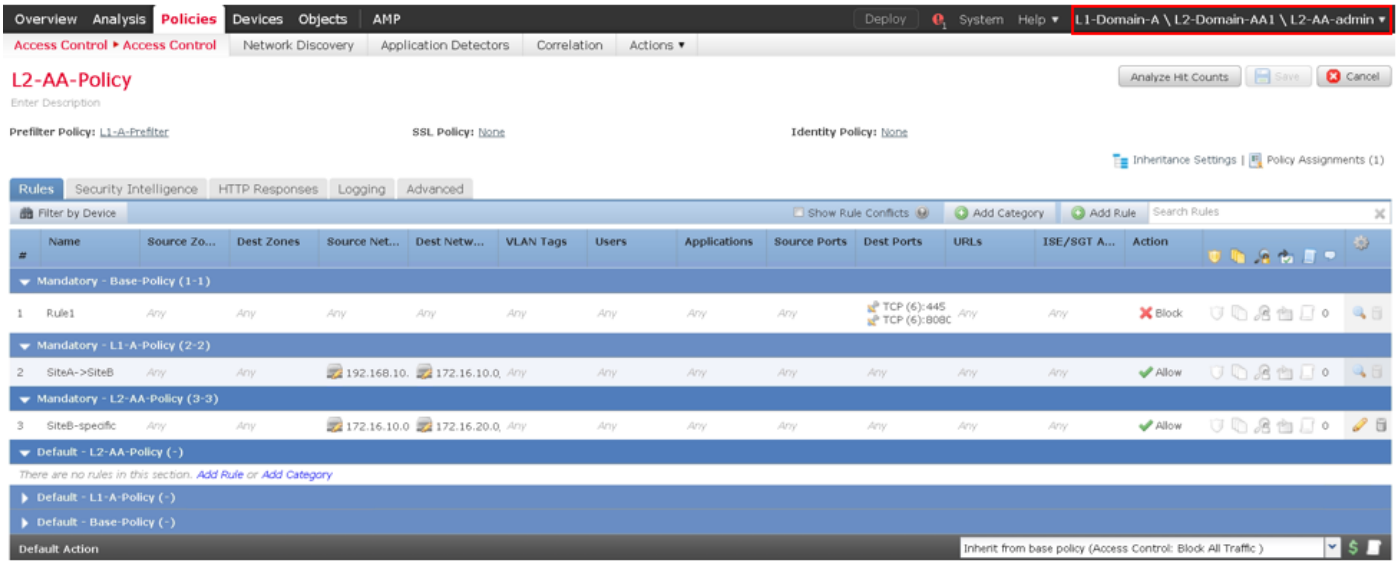


FMC上的资源访问将限于用户所属的域。如下所示，当**user-L1-A-admin**登录FMC UI时，访问仅限于用户所属的域**-L1-Domain-A**，当用户切换到该子域时，访问仅限于子域。当域切换到其子域时，此用户只能编辑在**L1-Domain-A域**中定义的策略和在子域中定义的策略。此外，从以下示例可以看到**L1-A-**Policy继承了全局域(即**Base-Policy)中定义的策略**，也可以编辑，从  签名。继承设置将指向基本策**略，如**图所示。

同样，**属于L2-Domain-AA1**域的用户**L2-AA-admin**仅对域中定义的策略**L2-AA-Policy**具有控制权，如图所示。**L2-AA-Policy**继承**L1-Domain-A**中定义的策略**L1-A-Policy**，该策略继承在全局域中定义的**Base-Policy**。此外，可以**编辑策略L2-AA-**Policy，该策略可从  签名。用户L2-AA-admin永远无法切换到其父域L1-Domain-A或其祖先域（即全局域）。



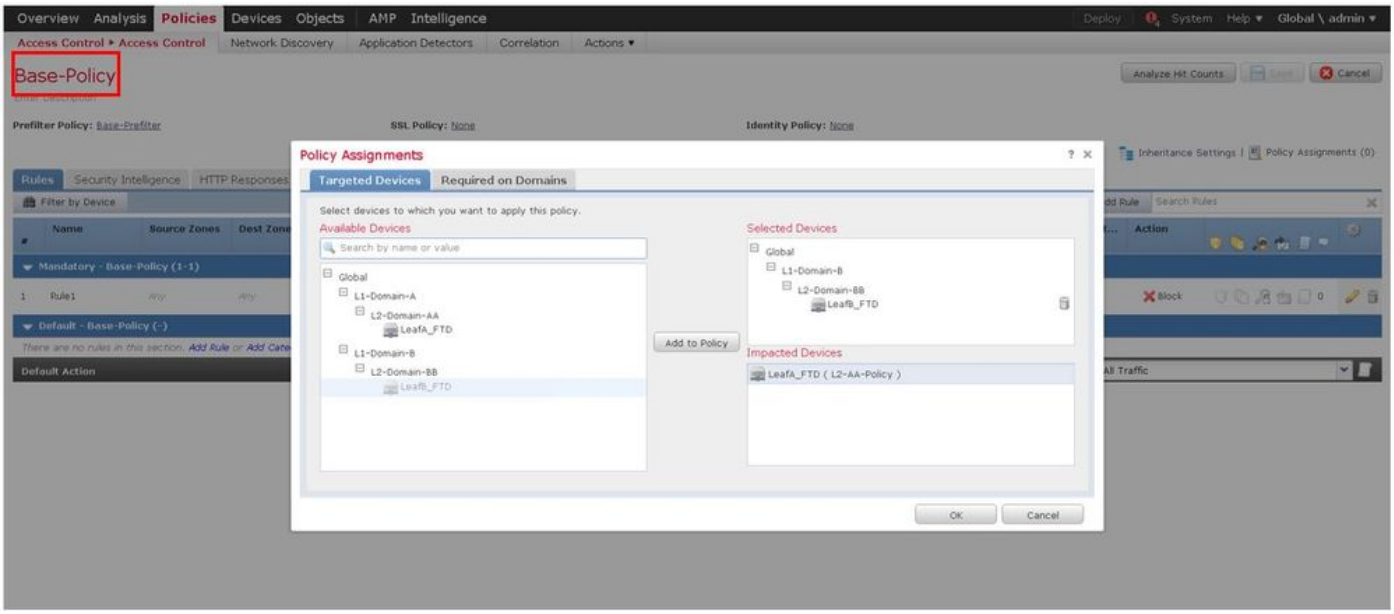
此外，**属于L1-**Domain-A的用户L1-A-admin可以切换到L2-Domain-AA1并编辑从**L2-AA-Policy中**看到的策略  如图所示。这甚至适用于属于全局域的用户，切换到子域并编辑在特定子域中定义的策略。



需要注意的要点：

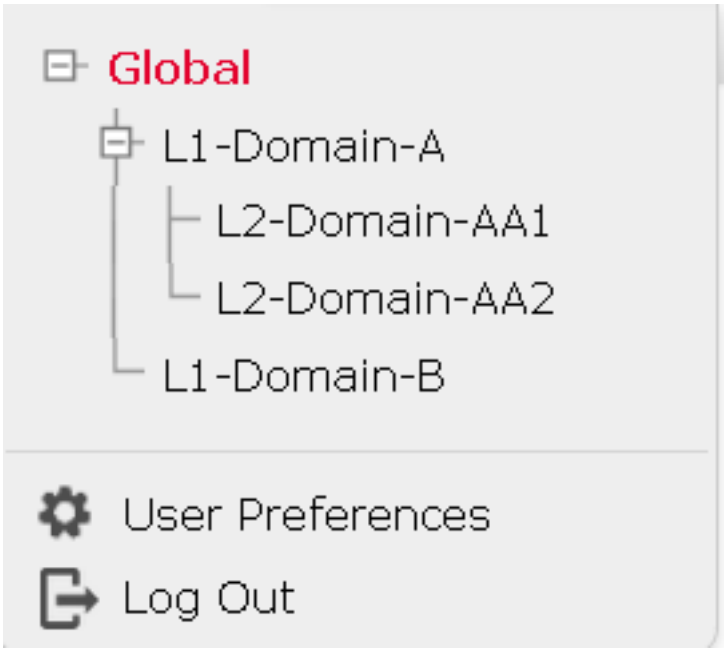
- 删除非全局域时，属于这些域的用户会自动移动到全局域中。

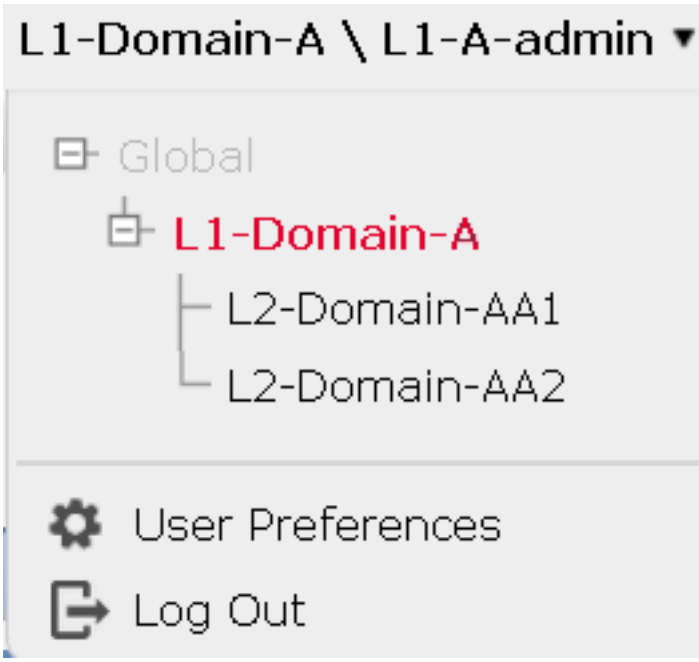
  FTD/s始终在枝叶域中定义。在本例中，枝叶域是**L2-Domain**（即L2-Domain-AA和L2-Domain-BB）。 属于L2域**的FTD可**以分配到L1域或**全局域**中的**策**略。在此映像中，全局域中的ACP将在L3域中定义的FTD分配给在全局域中定义的策略。



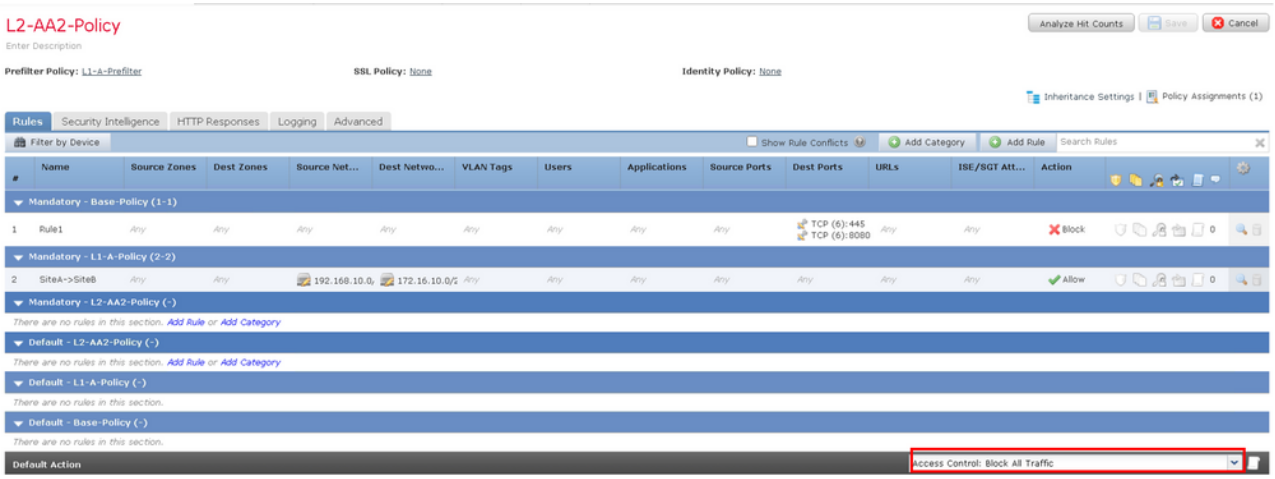
- 全局域中的用户可以导航到其他特定于用户的域，但特定域中的用户只能在其自己的域及其子域中具有可视性。它们无法导航到全局域或任何其他更高的域，如下表所示：

全局域	**用户特定域**
全局域中的用户可以查看配置的所有域，并且可以导航到其他域。	L1-**域 — A中的用户**将仅对自己及其子域(即**L2 — AA)具有可视性**，并且可以导航**到L2 — 域 — AA**。许更高级域(**如全**局)访问。





- 子策略的默认操作无法被父策略锁定，用户无需继承父策略的默认操作，如此映像中所示。



在此图像中，可以看到用户尚未将默认操作指定为父级的默认操作，从“从基本策略继承：**未在默认操作**中看到”这些字可以明显看出。

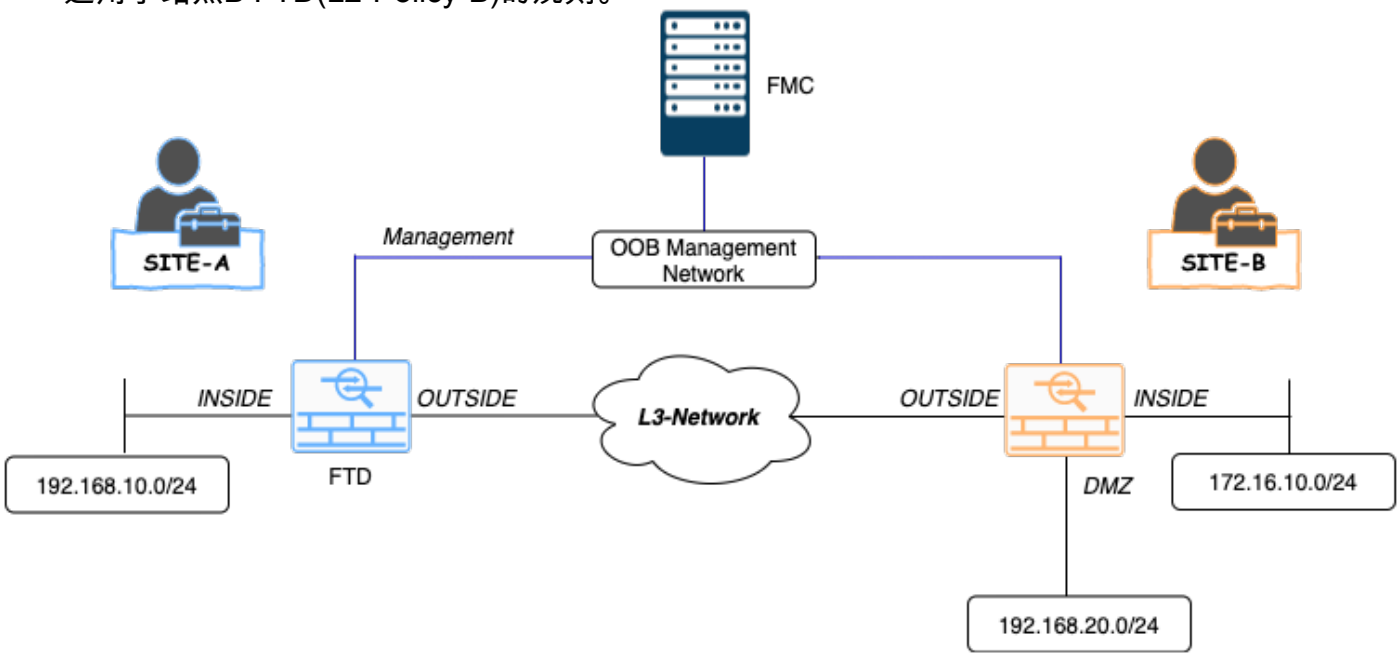
注意：应记住，用户不能同时查看L1/L2域策略。用户需要切换到所需域以查看和编辑策略。例如：如果全局域中的用户**admin**想查看L1-Domain-A和L2-Domain-AA中配置的策略，则用户可以通过切换到L1-A-Domain来查看和编辑该域中配置的策略，然后切换到L2-Domain-AA来查看和编辑相应的策略，但无法同时查看两者。此外，L1-Domain-A中的用户无法编辑或删除在全局域中定义的策略，即L1-A-Policy的父策略Base Policy，L2-Domain-AA中的用户不能分别编辑或删除在全局域和L2-Domain-A域中定义的策略Base Policy和L2-A-Policy。

使用案例配置

请考虑图中所示的场景，SITE-A(SiteA-FTD)和SITE-B(SiteB-FTD)的FTD由单个FMC通过不同域（多域）管理，以提供受控访问。从策略角度来看，以下是组织级别的策略考虑因素：

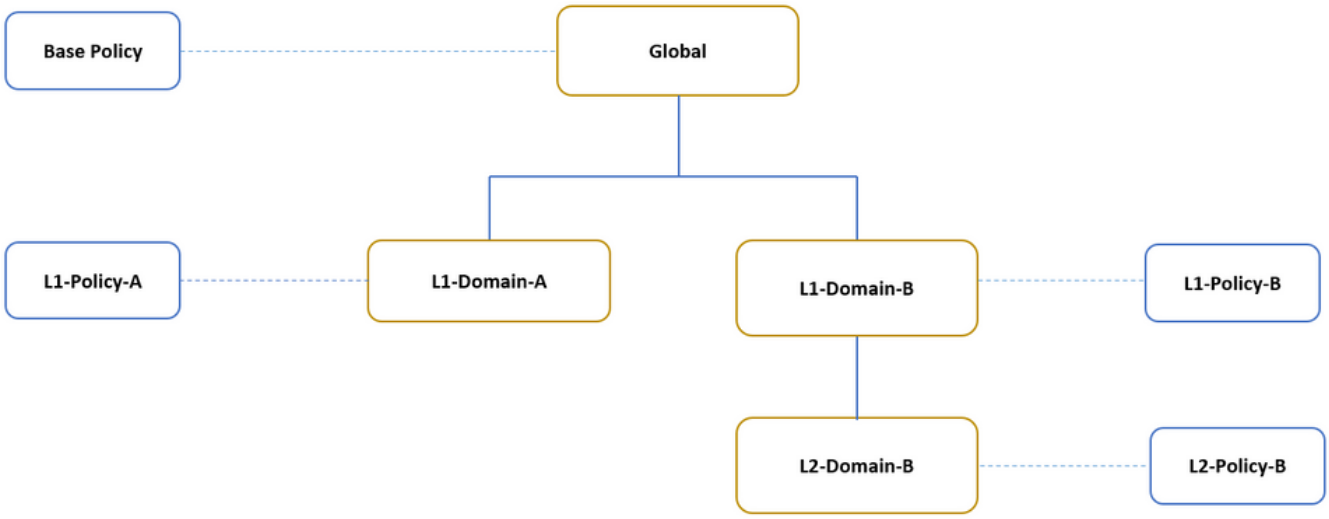
- 适用于所有FTD的服务特定BLOCK规则，独立于站点或域属于（基本策略）。
- 满足满足站点A到站点B访问(L1-Policy-A)和站点B到站点A访问(L1-Policy-B)要求的规则。

- 适用于站点B FTD(L2-Policy-B)的规则。



多域环境中的继承

对于上述使用案例，请考虑以下域/策略层次结构。SiteA-FTD和SiteB-FTD分别属于枝叶域L1-Domain-A和L2-Domain-B。

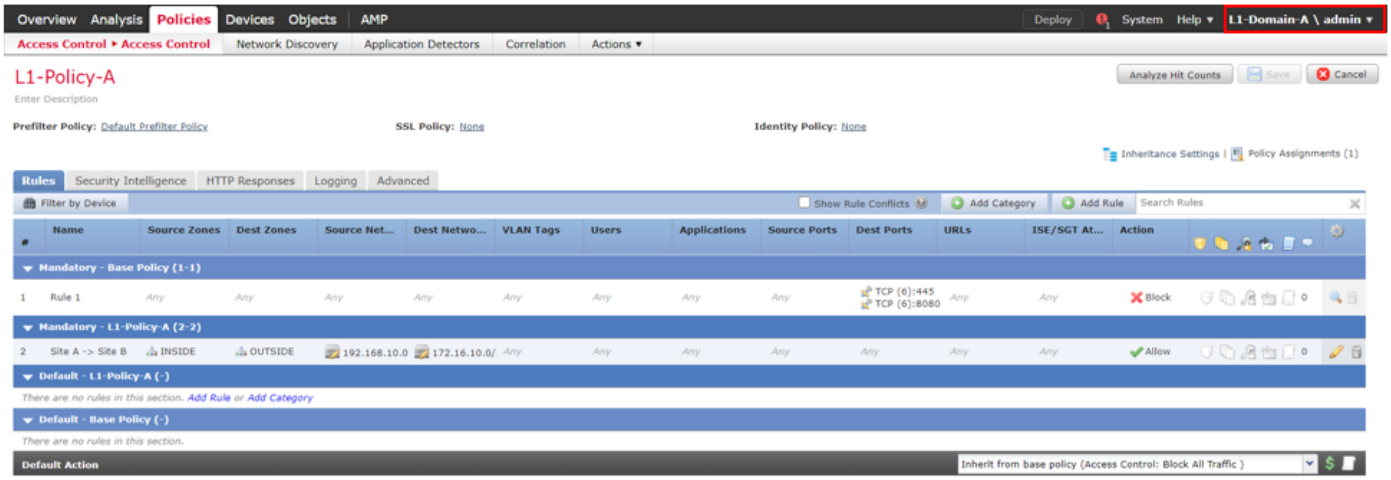


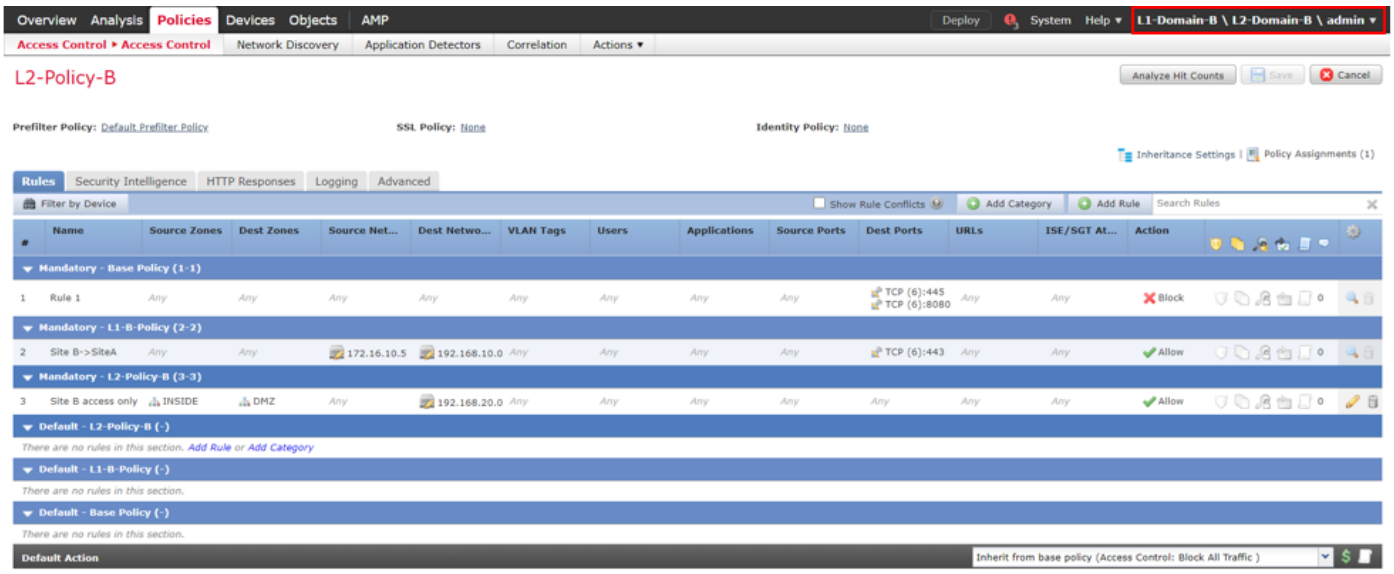
域层次结构如下：

- **全局域是**L1-**Domain-A和**L1-Domain-B的父域。
- **全局域是**L2-**Domain-B的祖先。**
- **L2-Domain-B**是L1-**Domain-B的子级**
- **L2-Domain-B是枝叶**域，因为它没有子域。

该图显示从FMC看到的域层次结构。

以下快照显示了如何在**L1-Policy-A**和**L2-Policy-B** w.r.t中定义规则到上述方案。





在配置多个域以避免阻止合法流量或允许不需要的流量时，应始终考虑规则及其继承。