Herança no ambiente multidomínio no FTD

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Configurar herança de política](#)
[Gerenciamento FTD em ambiente FMC multidomínio](#)
[Configuração de domínio](#)
[Visibilidade e controle de políticas em um ambiente FMC multidomínio](#)
[Adicionar usuários ao domínio](#)
[Cenário de caso de uso](#)
[Herança em um ambiente multidomínio](#)

Introduction

Este documento descreve a configuração e o funcionamento dos recursos de herança e de vários domínios. Isso também se concentra em um caso de uso real para ver como esses dois recursos funcionam juntos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Firepower Management Center (FMC) versão 6.4
- Software Firepower Threat Defense (FTD) versão 6.4

  Note: O suporte a vários domínios e recursos de herança está disponível no FMC/FTD a partir da versão 6.0.

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. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer configuração.

Informações de Apoio

Em Herança de política, as políticas de controle de acesso podem ser aninhadas onde a Política filho herda regras de uma Política básica, incluindo as configurações de ACP como Inteligência de segurança, Resposta HTTP, Configurações de registro etc. Opcionalmente, o administrador pode permitir que a política filho substitua as configurações ACP, como Security Intelligence, HTTP Response, Logging Settings ou então bloquear as configurações para que a política filho não possa substituí-las. Esse recurso é muito útil no ambiente FMC de vários domínios.

O recurso de vários domínios segmenta o acesso do usuário aos dispositivos, configurações e eventos gerenciados do FMC. Um usuário poderia alternar para/acessar outros domínios dependendo dos privilégios. Se o recurso multidomínio não estiver configurado, todos os dispositivos gerenciados, configurações e eventos pertencerão ao domínio **global**.

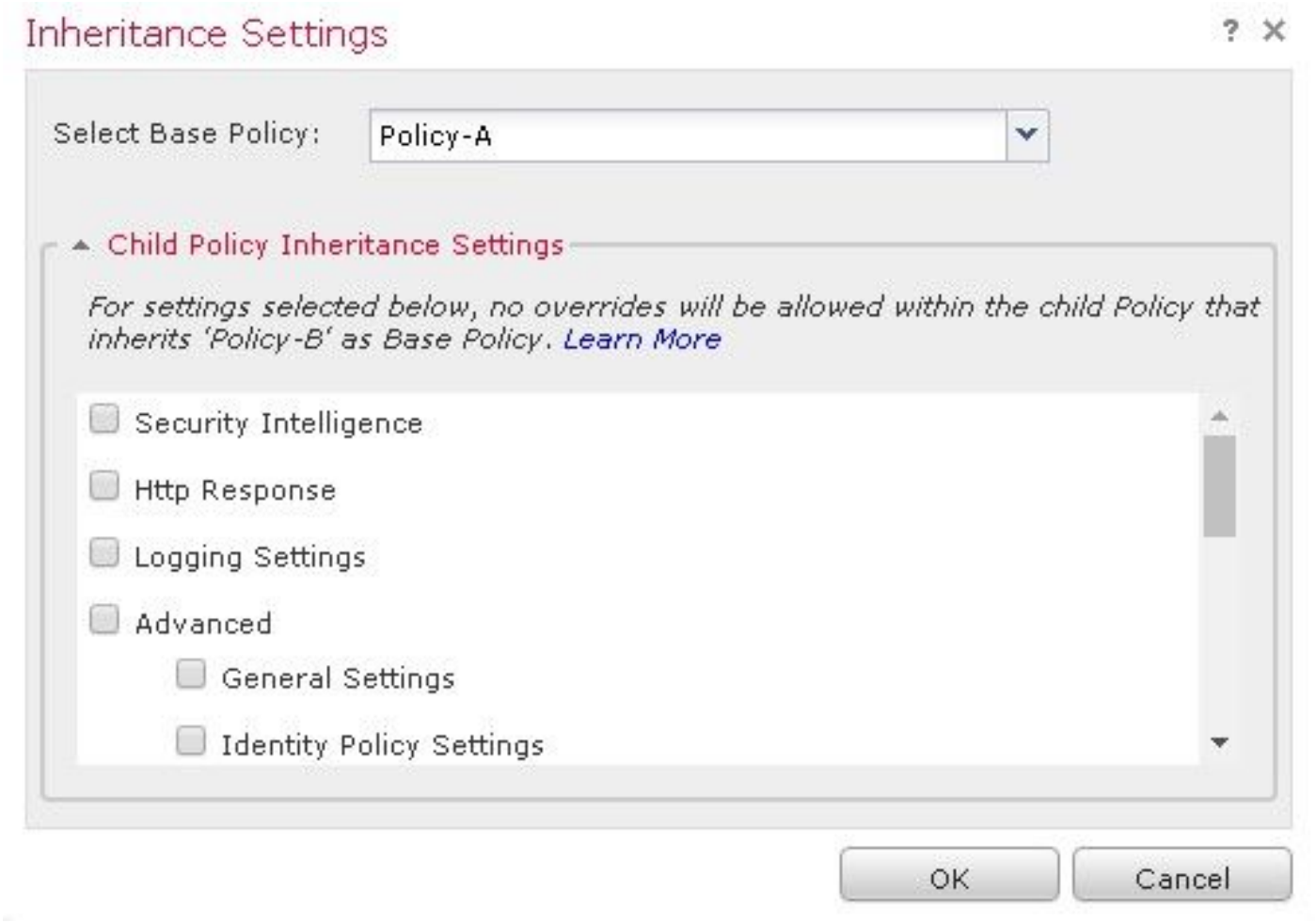
Configurar herança de política

Um domínio leaf é um domínio que não tem subdomínios adicionais. Um domínio filho é o descendente de nível seguinte do domínio em que o usuário/administrador está atualmente. O domínio pai é o ancestral direto do domínio em que o usuário/administrador está atualmente.

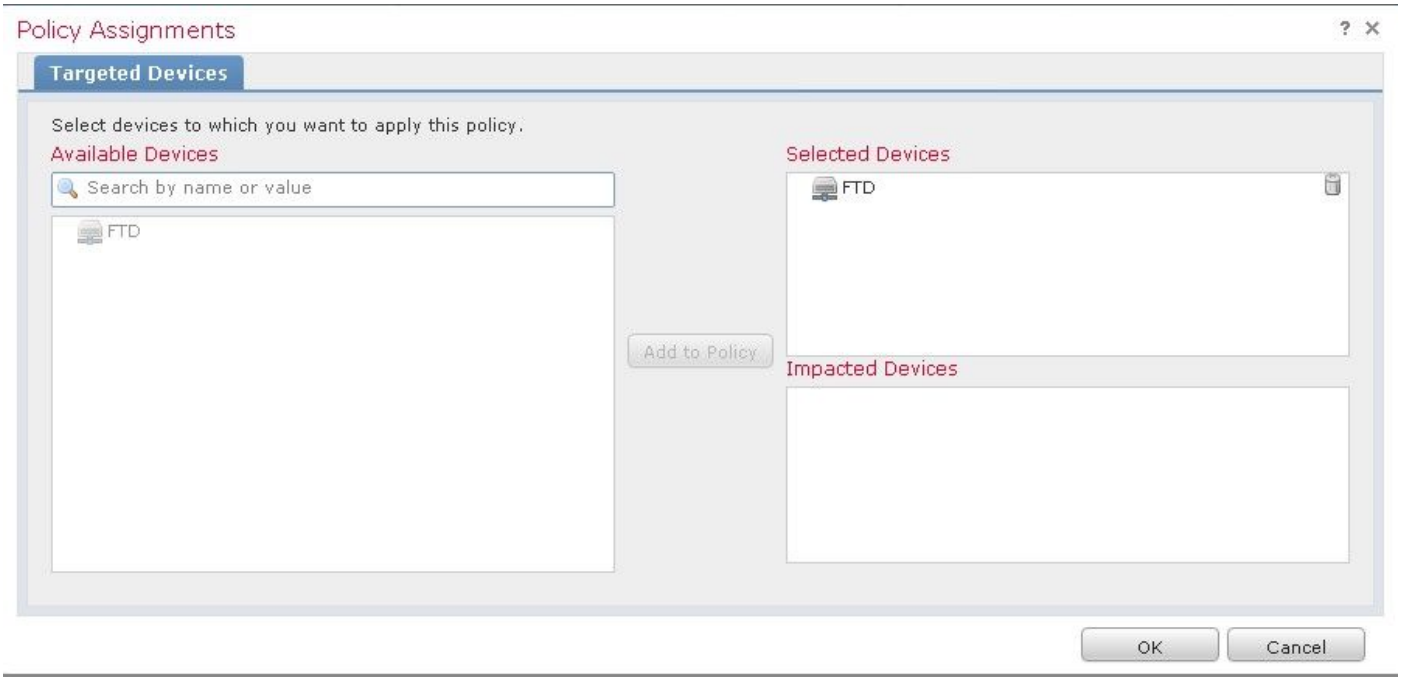
Para configurar/ativar a herança para políticas existentes:

1. Permitir que a política A seja a política básica e a política B seja a política filho (a política B herda a regra da política A)
2. **EDITE** Policy-B e clique em **Inheritance Settings** conforme mostrado na imagem.

3. Escolha Policy-A na lista suspensa **Select Base Policy** mostrada abaixo. Outras configurações de ACP, como Inteligência de segurança, Resposta HTTP, Configurações de registro, etc., podem ser herdadas para substituir as configurações da Política filho opcionalmente.

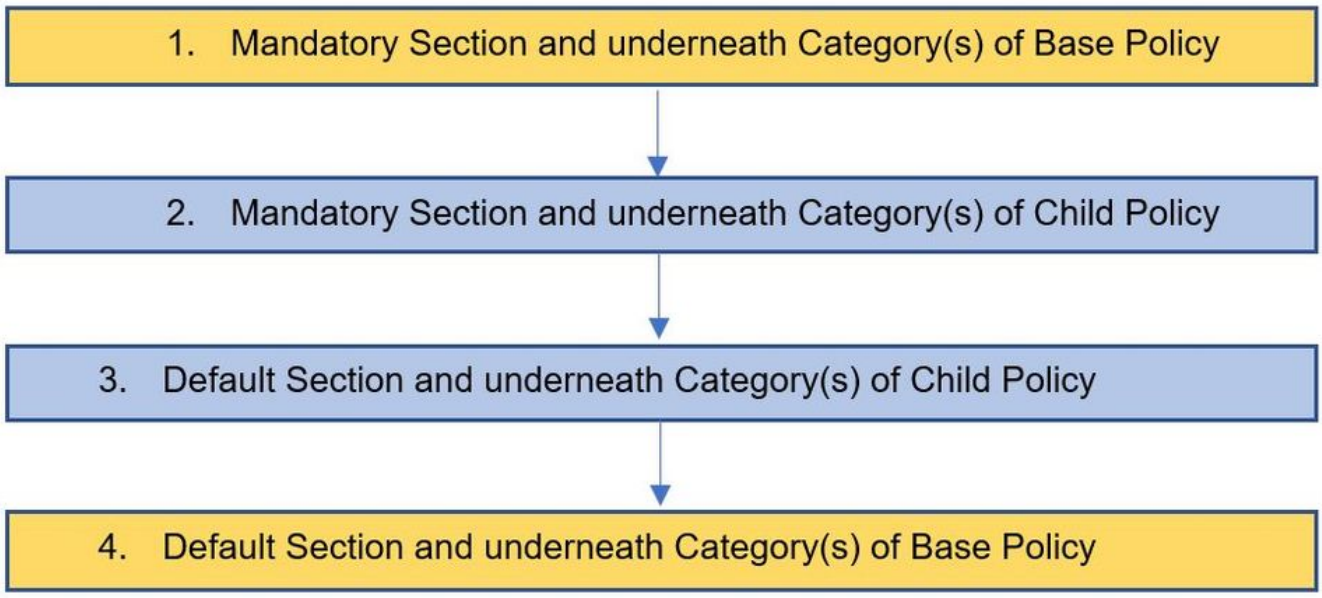


4. Execute a **atribuição de política** para a política-B filho em relação ao dispositivo FTD de destino pretendido:

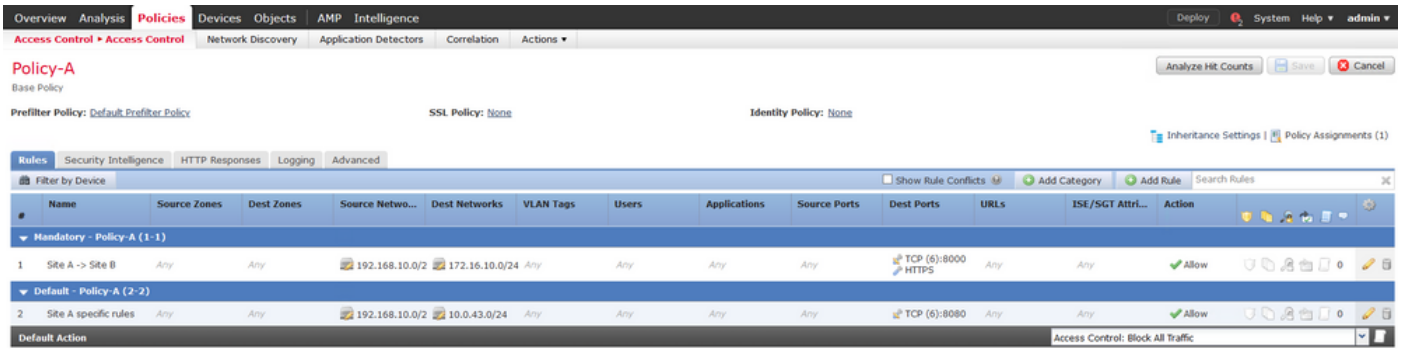


Por padrão, a **Ação Padrão** da Política Filho é herdada e definida como **Herdar da política base** como mostrado na imagem. O usuário também tem a opção de selecionar a **Ação padrão** nas Políticas fornecidas pelo sistema, conforme mostrado aqui.

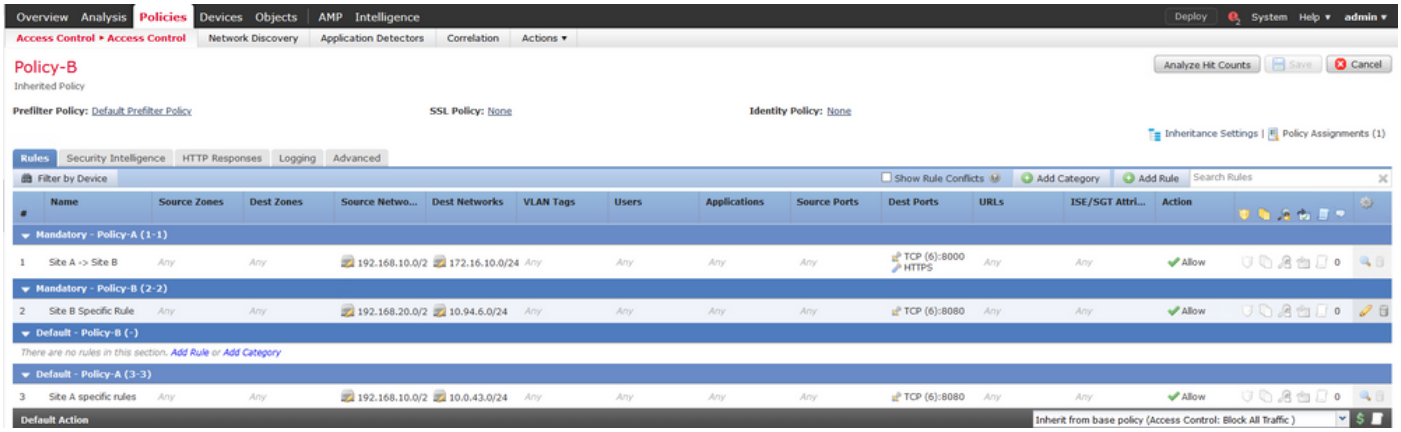
A ordem de pesquisa de tráfego sempre será de uma maneira de cima para baixo, independentemente do número de categorias adicionadas nas seções Obrigatório e Padrão. Depois de aplicar as **Configurações de Herança,** a representação ACP para a política filho B (Política filho), conforme mostrado na imagem, em linha com a **verificação da ordem de regra** mencionada anteriormente:



Esta imagem mostra como as políticas, nomeadamente a política A, que é a política de base, e a política B, que é a política da criança e que é herdada da política A, seriam mostradas no CVP.



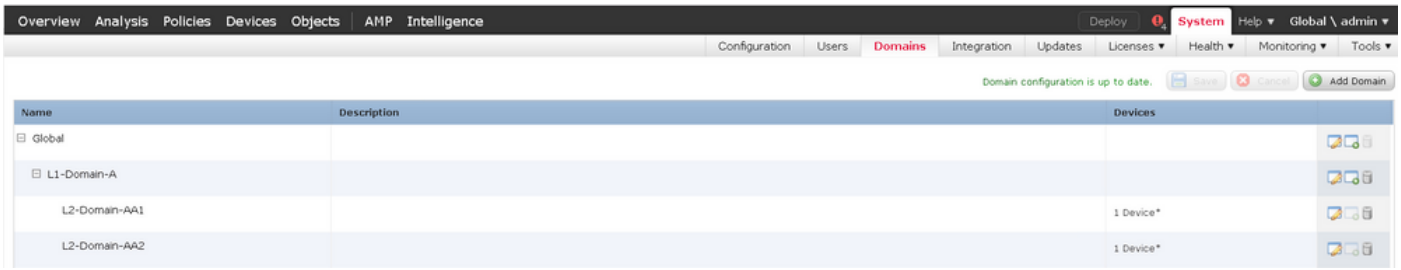
Essa imagem mostra que na Política B, as regras da Política A podem ser vistas, bem como as regras específicas configuradas na própria Política B. Deve-se ter cuidado sobre como as regras devem ser configuradas tendo em mente o pedido.



Gerenciamento FTD em ambiente FMC multidomínio

O recurso multidomínio segmenta o acesso do usuário a dispositivos gerenciados, configurações e eventos. Um usuário poderia mudar para outros domínios dependendo dos privilégios. Se o recurso multidomínio não estiver configurado, todos os dispositivos gerenciados, configurações e eventos pertencerão ao domínio **global**.

Um máximo de domínios de três níveis pode ser configurado com o domínio global como nível um. Todos os dispositivos gerenciados devem pertencer somente ao domínio leaf. Isso pode ser confirmado pelo símbolo da  (Adicionar subdomínio) sendo esmaecido no domínio de folha como mostrado na imagem.



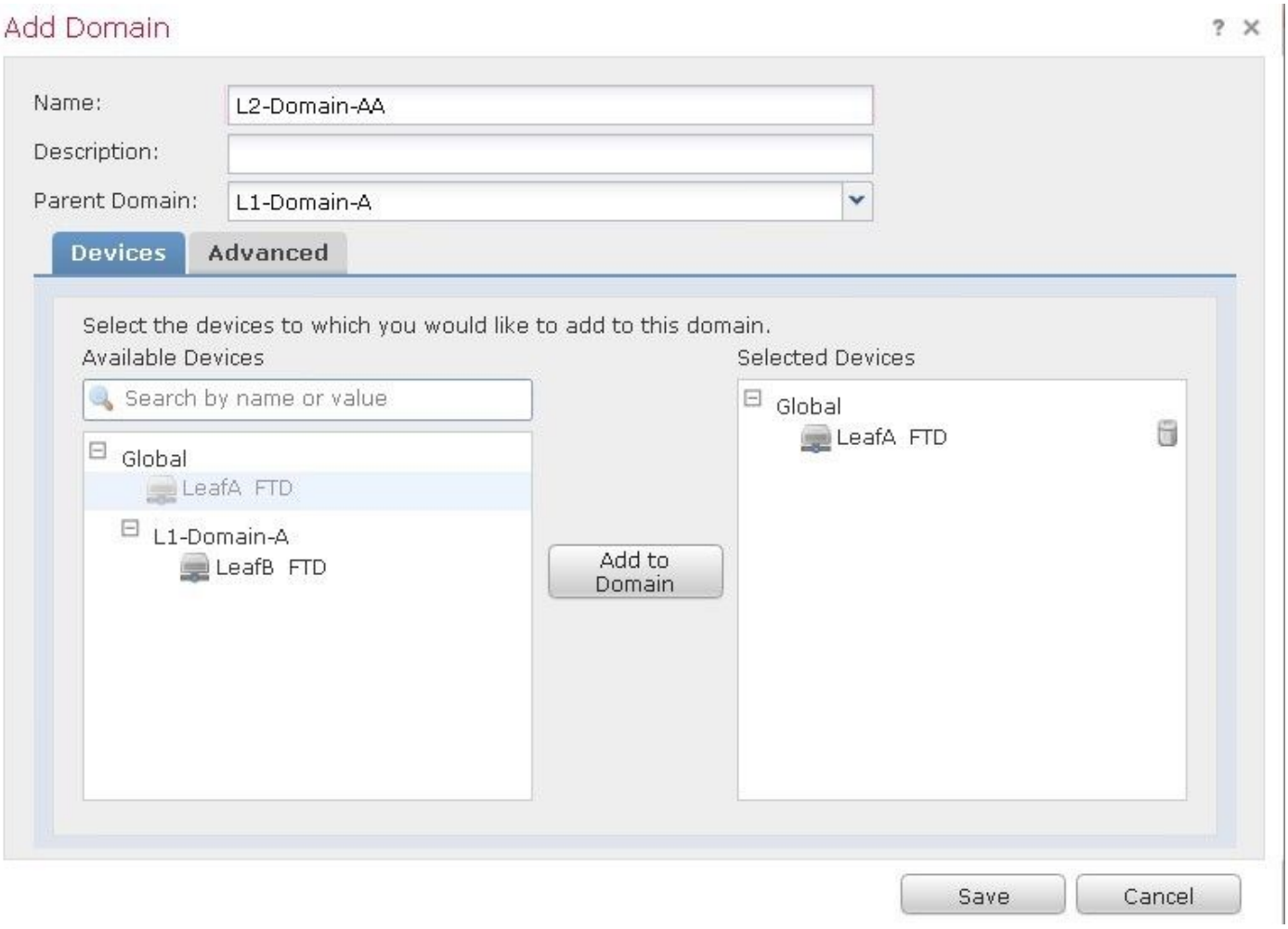
Configuração de domínio

A configuração do domínio pode ser feita da seguinte maneira:

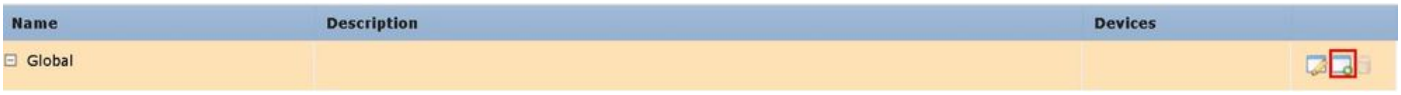
1. Navegue até **Sistema > Domínios**. Por padrão, o domínio **global** está presente.

2. Clique em **Adicionar domínio** conforme mostrado na imagem.

3. A caixa de diálogo **Adicionar domínio** é exibida. Digite o **Nome** do domínio e selecione o **Domínio pai** na lista suspensa. Se este for o domínio leaf, os dispositivos FTD precisam ser adicionados ao domínio como mostrado na imagem.

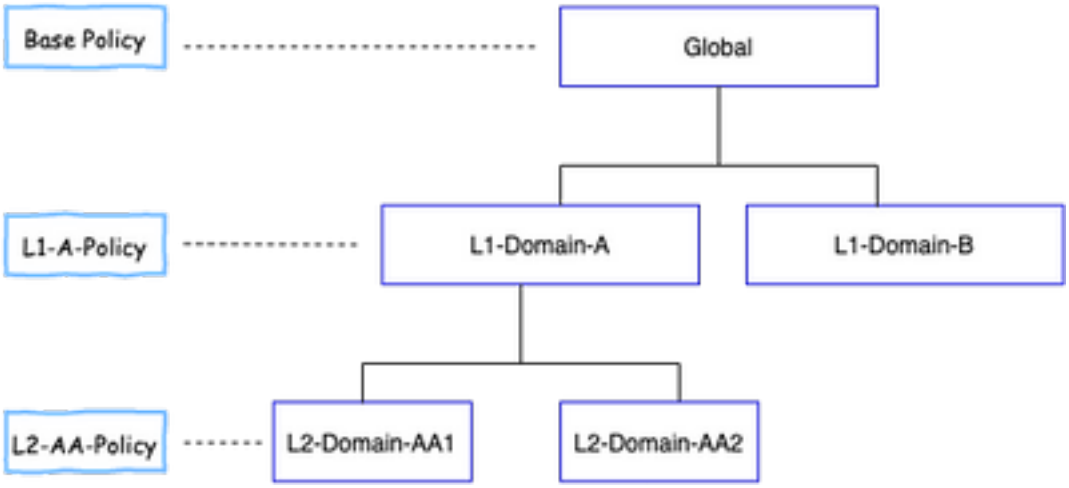


Note: Para adicionar os domínios, clique no ícone **Adicionar subdomínio** conforme mostrado na imagem. Aqui o domínio pai já está selecionado.



Visibilidade e controle de políticas em um ambiente FMC multidomínio

A visibilidade e o controle da política são limitados aos respectivos usuários de domínio, exceto por um Administrador do domínio **global**. Este exemplo é baseado na hierarquia da seguinte maneira:



Visibilidade: Como mostrado nesta imagem, a página **Políticas de** exibição padrão lista políticas (ACP) configuradas no respectivo domínio.

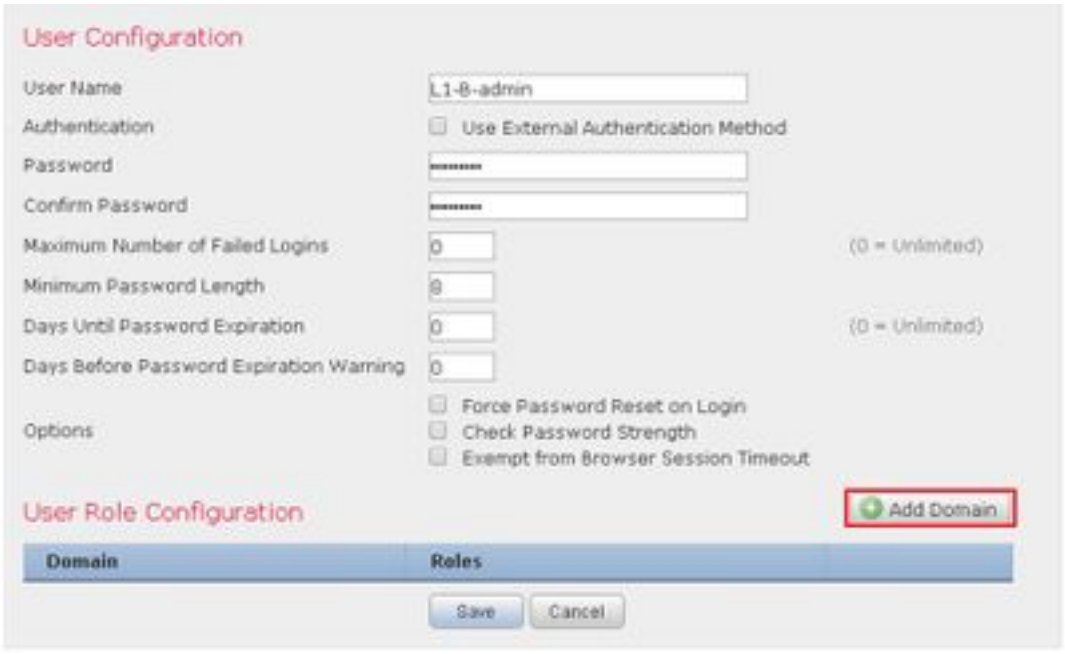
Controle: **Os** usuários **administrativos** pertencentes ao respectivo domínio podem EDITAR as políticas. Para editar as políticas, que pertencem a outros domínios (como parte da Herança), é necessário alternar o domínio de atual para um domínio no qual a Política está configurada. Somente usuários Admin pertencentes ao domínio **global** ou domínio L1 podem alternar entre o domínio inferior para o gerenciamento de políticas.

Adicionar usuários ao domínio

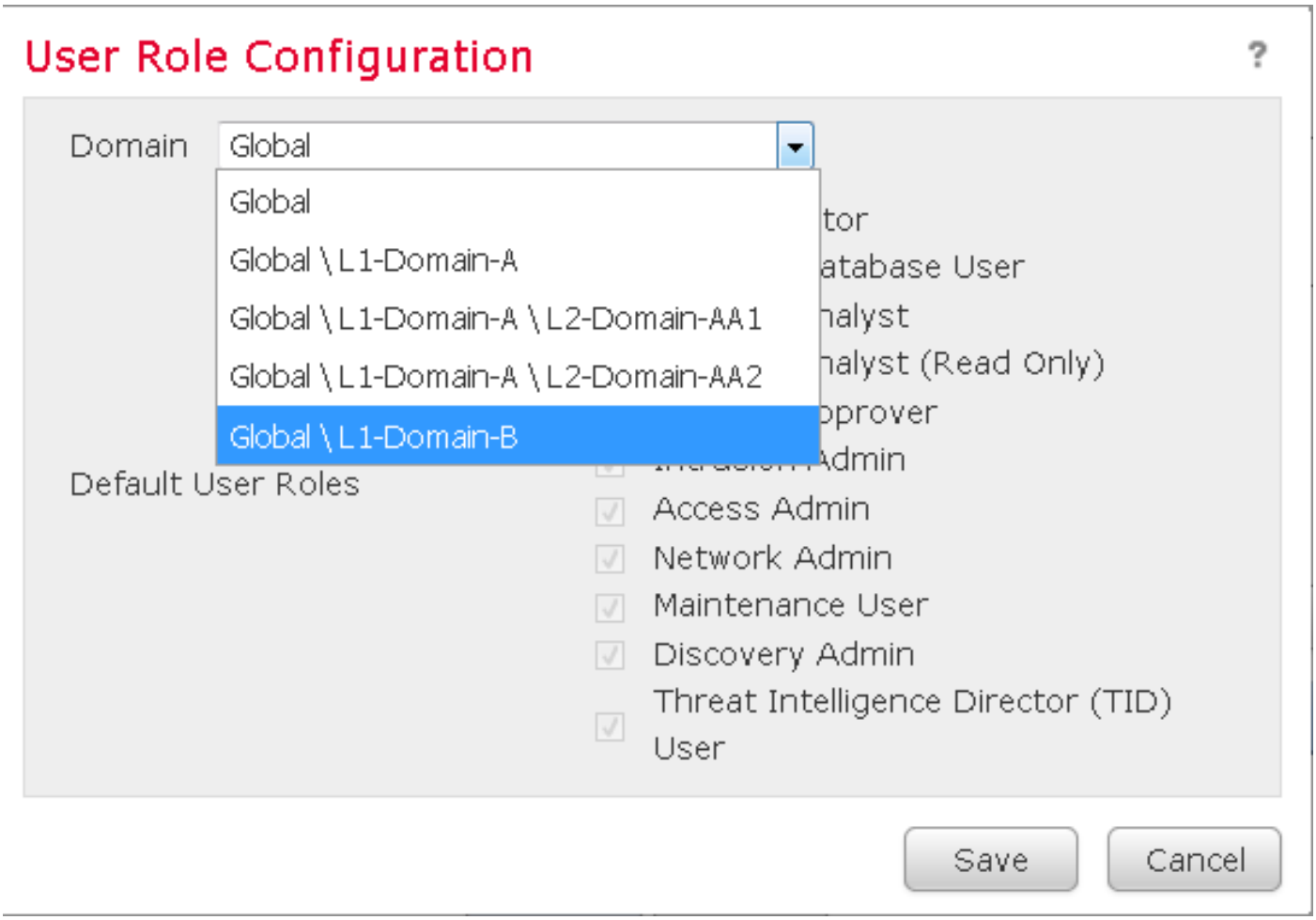
Mostra como adicionar usuários em um domínio específico. Este procedimento é aplicável aos usuários no banco de dados local.

1. Navegue até **Sistema >Usuários**. Clique em **Criar usuário** conforme mostrado na imagem.

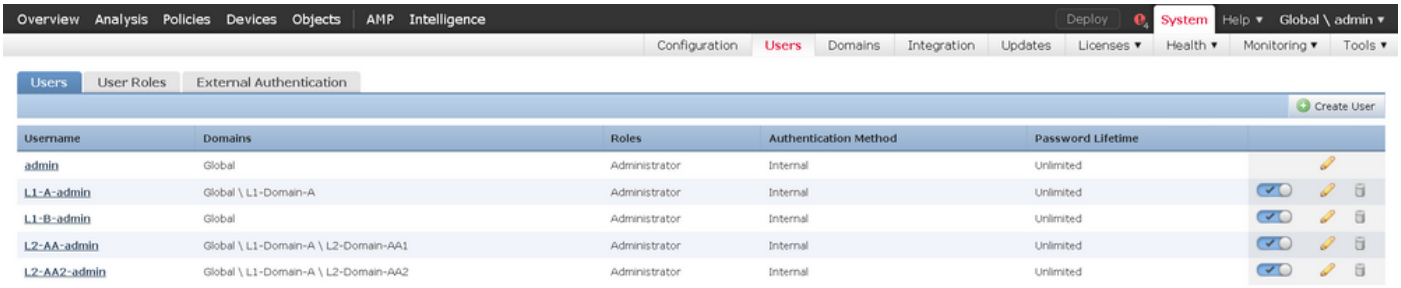
2. A caixa de diálogo **Configuração do usuário** é exibida. Preencha o **Nome de usuário** e a **Senha (& Confirmar senha)**. Clique em **Adicionar domínio** para adicionar o usuário ao domínio especificado como mostrado na imagem.



3. Escolha o domínio pretendido na lista suspensa **Domínio** em que deseja adicionar o usuário e especifique a função conforme mostrado na imagem. Um novo usuário pode ser adicionado ao próprio domínio ou aos domínios filho.

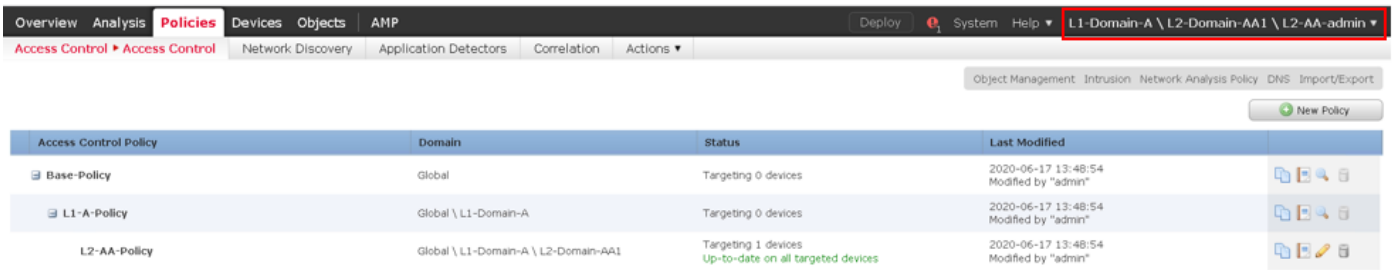


Os usuários configurados são mostrados nesta imagem:

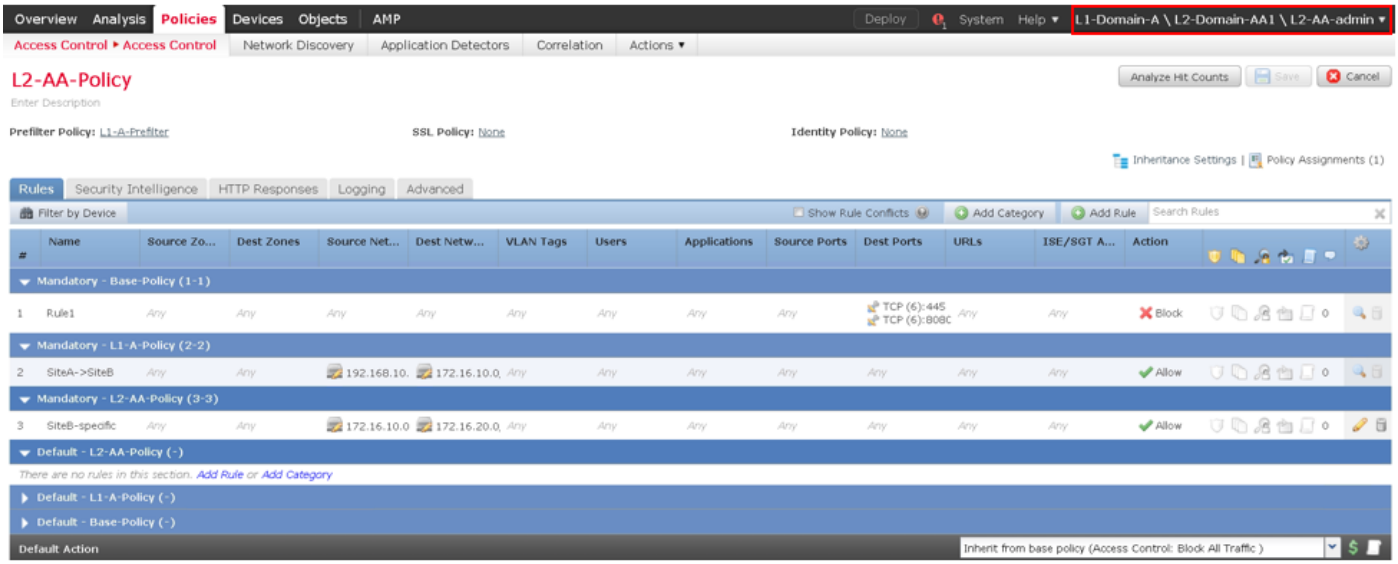


O acesso aos recursos no FMC seria limitado ao domínio ao qual o usuário pertence. Como mostrado abaixo, quando o usuário **L1-A-admin** faz login na IU do FMC, o acesso é limitado ao domínio **L1-Domain-A** do qual o usuário faz parte e ao domínio filho depois que o usuário muda para esse domínio filho. Este usuário pode editar somente a política definida no domínio **L1-Domain-A** e a política definida no domínio filho quando o domínio é comutado para seu domínio filho. Além disso, pode ser visto no exemplo abaixo que a **L1-A-Policy** herda a política definida no domínio global, ou seja, **Base-Policy**, bem como pode ser editada, que pode ser vista do  sinal. As configurações de herança são feitas para apontar para **Base-Policy**, como mostrado na imagem.

Da mesma forma, um usuário **L2-AA-admin** pertencente ao domínio **L2-Domain-AA1** tem controle somente da política **L2-AA-Policy** definida no domínio como mostrado na imagem. A **L2-AA-Policy** herda a política **L1-A-Policy** definida em **L1-Domain-A** que, por sua vez, herda a **Base-Policy** definida no domínio Global. Além disso, a política **L2-AA-Policy** pode ser editada, que pode ser vista no  sinal. O usuário L2-AA-admin nunca pode mudar para seu domínio pai, ou seja, L1-Domain-A, nem seu domínio ancestral, ou seja, o domínio global.



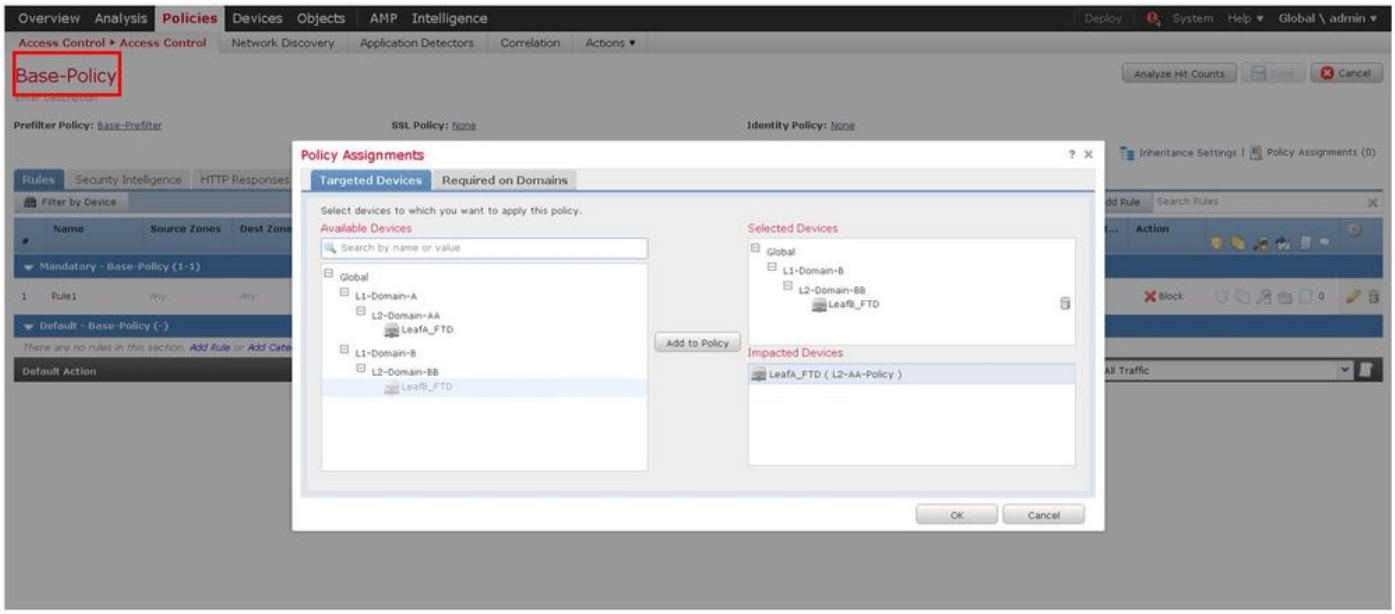
Além disso, um usuário **L1-A-admin** pertencente ao L1-Domain-A pode alternar para L2-Domain-AA1 e editar a política **L2-AA-Policy** que é vista do  conforme mostrado na imagem. Isso é aplicável até mesmo a um usuário que pertence ao domínio global e que está alternando para os domínios filho e editando as políticas definidas no domínio filho específico.



Pontos importantes a observar:

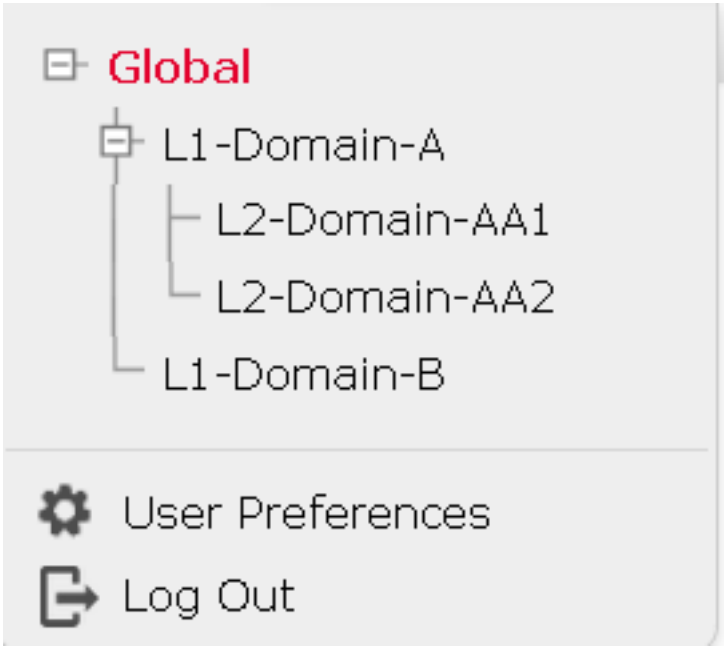
- Ao excluir os domínios não globais, os usuários pertencentes aos domínios são movidos automaticamente para o domínio **global**.

  O(s) FTD(s) é(são) sempre definido(s) no domínio leaf. Nesse caso, o domínio leaf é o **L2-Domain** (ou seja, L2-Domain-AA e L2-Domain-BB). O FTD pertencente ao **domínio L2** pode ser atribuído à política no **domínio L1** ou no domínio **global**. Nesta imagem, o ACP no domínio Global atribuiu o FTD definido no domínio L3 à política definida no domínio Global.

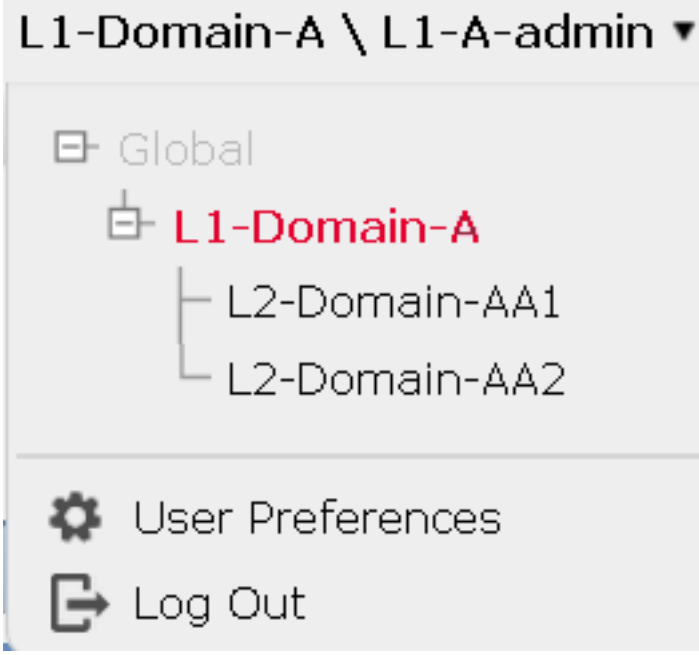


- Os usuários no domínio global podem navegar para outros domínios específicos do usuário, mas os usuários de um domínio específico só têm visibilidade em seu próprio domínio e em seus domínios filho. Eles não podem navegar para o domínio global ou qualquer outro domínio superior, como mostrado nesta tabela:

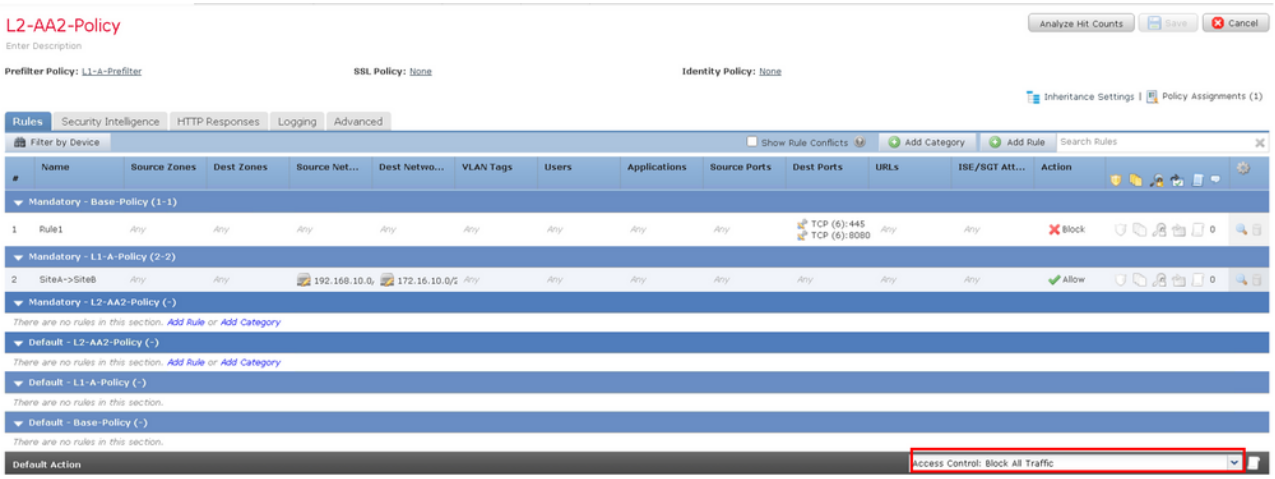
Domínio global	Domínio específico do usuário
O usuário no domínio global tem visibilidade de todos os domínios configurados e pode navegar para outros domínios.	O usuário no **L1-Domain-A** terá visibilidade some para si e seu domínio filho, ou seja, **L2-Domain-A** poderá navegar para **L2-Domain-AA**. Acesso de



domínio de nível superior (como **global**) não perm



- A ação padrão da política filho não pode ser bloqueada pela política pai e o usuário não precisa herdar a ação padrão da política pai como nesta imagem.



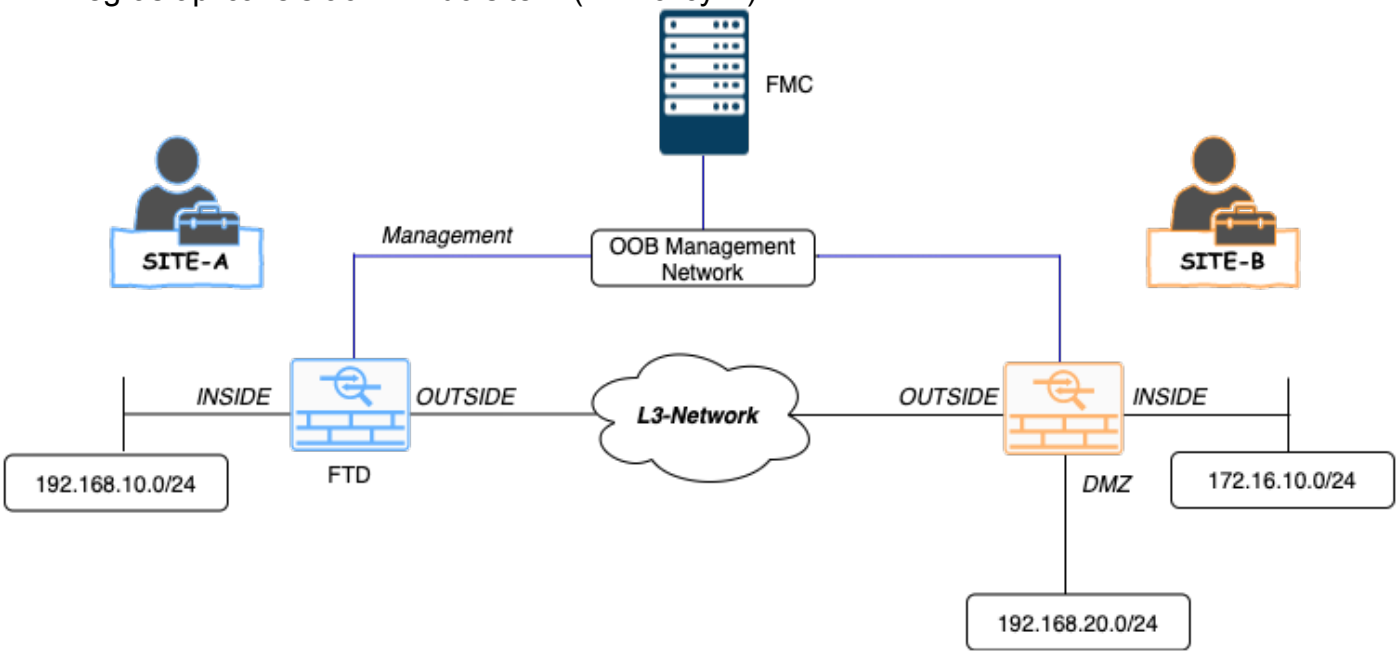
Nesta imagem, pode-se ver que o usuário não atribuiu a ação padrão como a do pai, o que pode ser evidente nas palavras **Herdar da política base:** não sendo visto na ação padrão.

Note: Deve-se ter em mente que um usuário não pode visualizar ambas as políticas de domínio L1/L2 ao mesmo tempo. O usuário precisa mudar para o domínio desejado para exibir e editar as políticas. Por exemplo: se o usuário **admin** presente no domínio global desejar exibir quais políticas estão configuradas no L1-Domain-A e no L2-Domain-AA, o usuário poderá fazer isso alterando para L1-A-Domain para exibir e editar a política configurada nesse domínio e, em seguida, alternar para L2-Domain-AA para exibir e editar a política correspondente, mas não poderá exibir ambas ao mesmo tempo. Além disso, o usuário no L1-Domain-A não pode editar ou excluir a política definida no domínio global, ou seja, a política de base que é a política pai da política L1-A e o usuário no L2-Domain-A não pode editar ou excluir as políticas, ou seja, a política de base e a política L2-A definida nos domínios global e L2-Domain-A, respectivamente.

Cenário de caso de uso

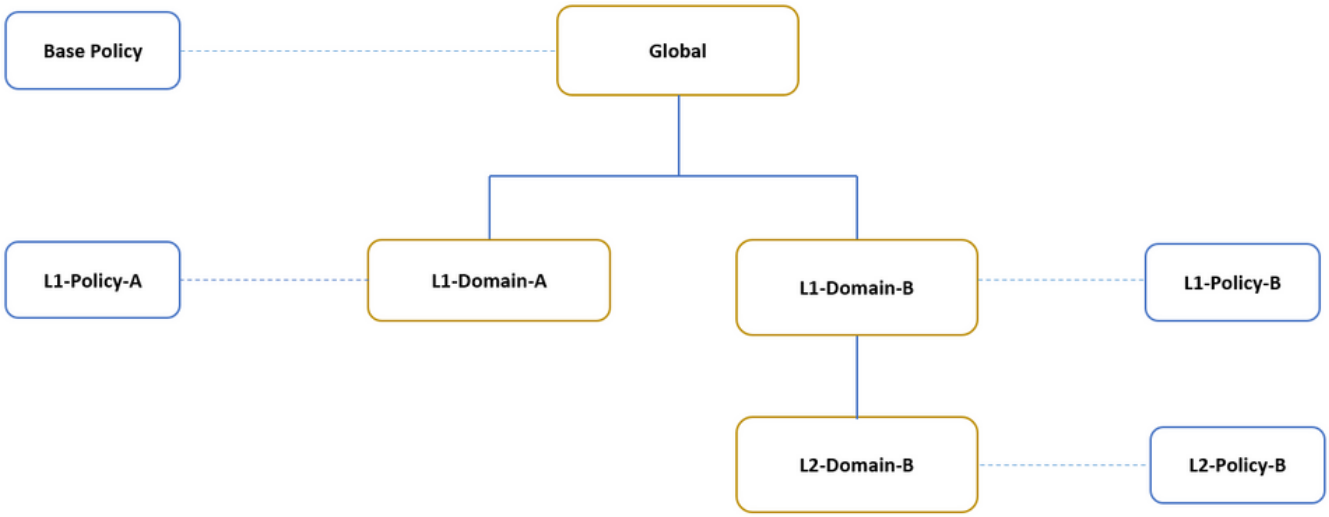
Considere o cenário descrito na imagem, os FTDs do SITE-A (SiteA-FTD) e do SITE-B (SiteB-FTD) são gerenciados por um único FMC através de diferentes domínios (multi-domínios) para fornecer acesso controlado. Do ponto de vista da política, essas são as considerações de política no nível da organização:

- As regras de BLOCO específicas do serviço aplicáveis a TODOS os FTDs independentes de SITE ou DOMÍNIO pertencem a (política básica).
- Regras que atendem aos requisitos para atender ao acesso do Site A ao Site B (L1-Policy-A) e do Site B ao acesso do Site A (L1-Policy-B).
- Regras aplicáveis ao FTD do site B (L2-Policy-B).



Herança em um ambiente multidomínio

Para o caso de uso mencionado acima, considere a seguinte hierarquia de Domínio/Política. SiteA-FTD e SiteB-FTD fazem parte dos domínios de folha L1-Domain-A e L2-Domain-B, respectivamente.

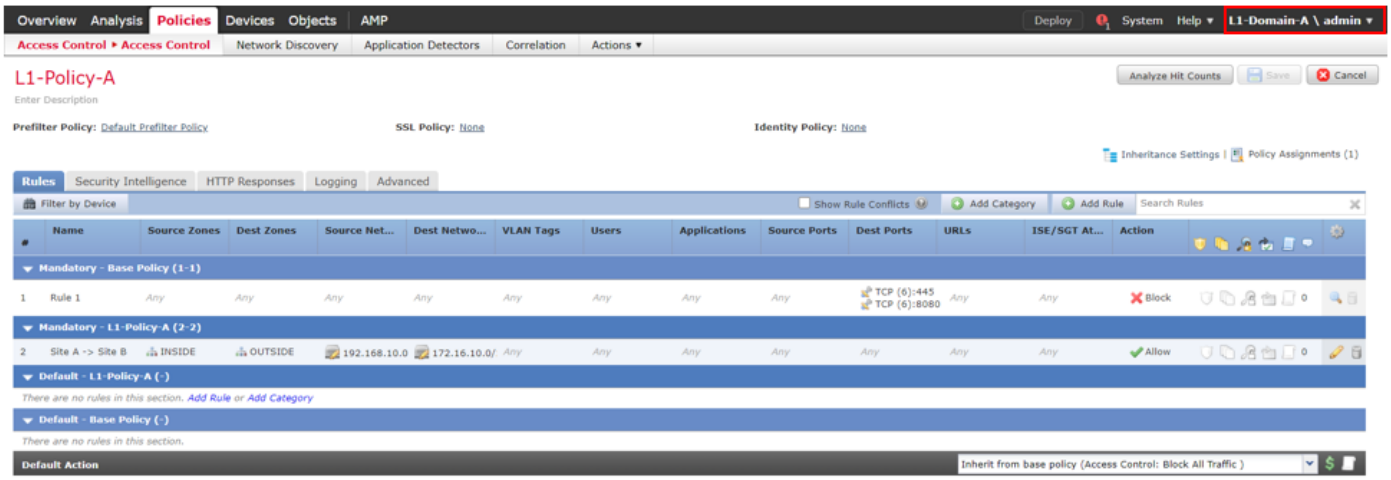


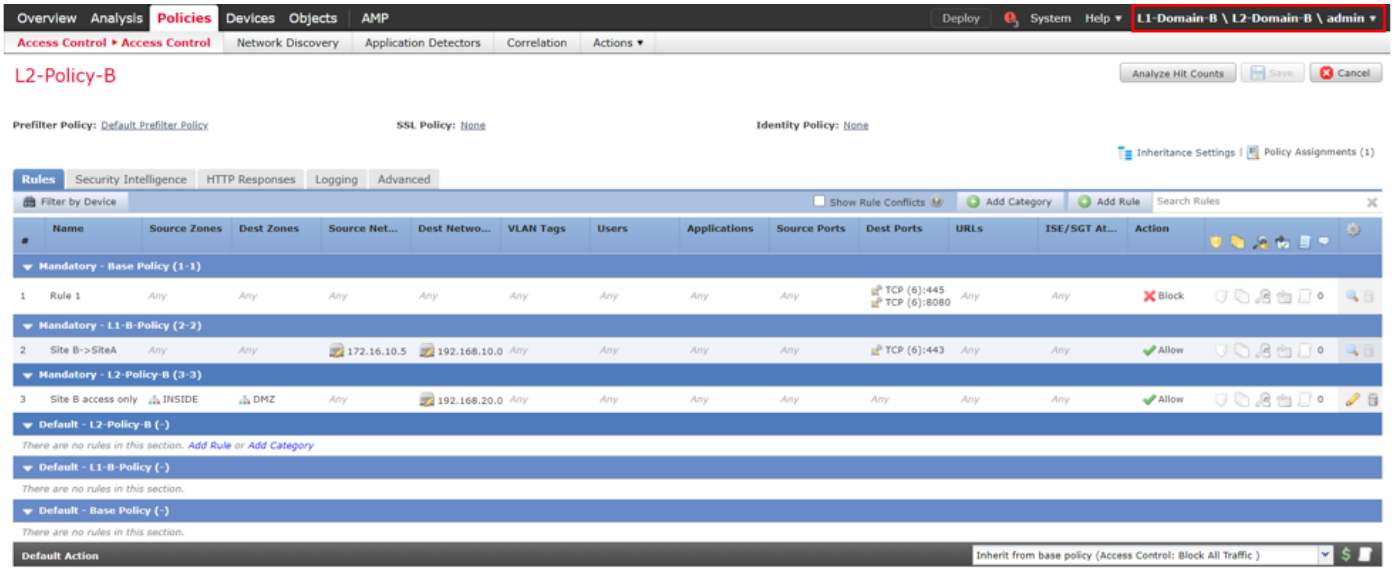
A estrutura da hierarquia de domínio é a seguinte:

- **O** domínio **global** é **pai** do **L1-Domain-A** e **L1-Domain-B**.
- **O** domínio **global** é **ancestral** do **L2-Domain-B**.
- **L2-Domain-B** é filho de **L1-Domain-B**
- **L2-Domain-B** é domínio de folha porque não tem domínios filho.

A imagem mostra a hierarquia de domínio como vista do FMC.

O snapshot abaixo mostra como as regras são definidas em **L1-Policy-A** e **L2-Policy-B** w.r.t para o cenário acima.





Você deve sempre considerar as regras e sua herança em mente ao configurar vários domínios para evitar bloquear tráfego legítimo ou permitir tráfego indesejado.