

Herencia en entorno multidominio en FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar herencia de políticas](#)

[Administración de FTD en entornos FMC de varios dominios](#)

[Configuración de dominio](#)

[Visibilidad y control de políticas en un entorno FMC de varios dominios](#)

[Agregar usuarios al dominio](#)

[Caso práctico](#)

[Herencia en un entorno de varios dominios](#)

Introducción

Este documento describe la configuración y el funcionamiento de las funciones de herencia y multidominio. Esto también se centra en un caso práctico real para ver cómo funcionan juntas estas dos funciones.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

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

Nota: El soporte de la función multidominio y herencia está disponible en FMC/FTD a partir de la versión 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. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier configuración.

Antecedentes

En Herencia de políticas, las políticas de control de acceso se pueden anidar cuando la política secundaria hereda las reglas de una política base, incluida la configuración de ACP como Inteligencia de seguridad, Respuesta HTTP, Configuración de registro, etc. Opcionalmente, el administrador puede permitir que la política secundaria reemplace la configuración de ACP como Security Intelligence, HTTP Response, Logging Settings o, de lo contrario, bloquee la configuración para que la política secundaria no pueda reemplazarla. Esta función es muy útil en el entorno FMC de varios dominios.

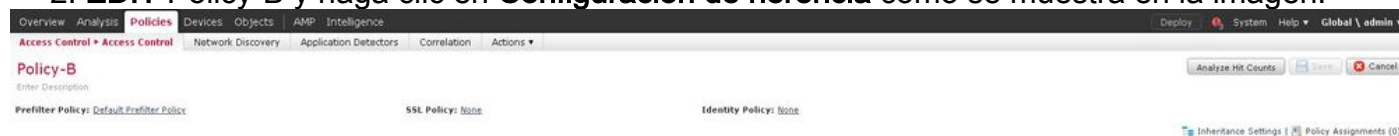
La función de varios dominios segmenta el acceso de los usuarios a los dispositivos, configuraciones y eventos administrados de FMC. Un usuario podría cambiar a otros dominios o acceder a ellos en función de los privilegios. Si la función multidominio no está configurada, todos los dispositivos, configuraciones y eventos administrados pertenecen al dominio **global**.

Configurar herencia de políticas

Un dominio de hoja es un dominio que no tiene más subdominios. Un dominio secundario es el descendiente de nivel siguiente del dominio donde el usuario/administrador está actualmente. El dominio primario es el antecesor directo del dominio donde el usuario/administrador está actualmente.

Para configurar/habilitar la herencia para las políticas que existen:

1. Deje que la política A sea la política básica y la política B la política secundaria (la política B hereda la regla de la política A)
2. **EDIT** Policy-B y haga clic en **Configuración de herencia** como se muestra en la imagen.



3. Elija Policy-A en la lista desplegable **Seleccionar política base** que se muestra a continuación. Otras opciones de configuración de ACP, como la inteligencia de seguridad, la respuesta HTTP, la configuración de registro, etc., se pueden heredar para reemplazar la configuración de la política secundaria de forma opcional.

Inheritance Settings



Select Base Policy:

▲ Child Policy Inheritance Settings

For settings selected below, no overrides will be allowed within the child Policy that inherits 'Policy-B' as Base Policy. [Learn More](#)

- Security Intelligence
- Http Response
- Logging Settings
- Advanced
 - General Settings
 - Identity Policy Settings

OK Cancel

4. Haga la **Asignación de Política** para la Política Secundaria-B contra el dispositivo FTD de destino deseado:

Policy Assignments



Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

FTD

Add to Policy

Selected Devices

FTD

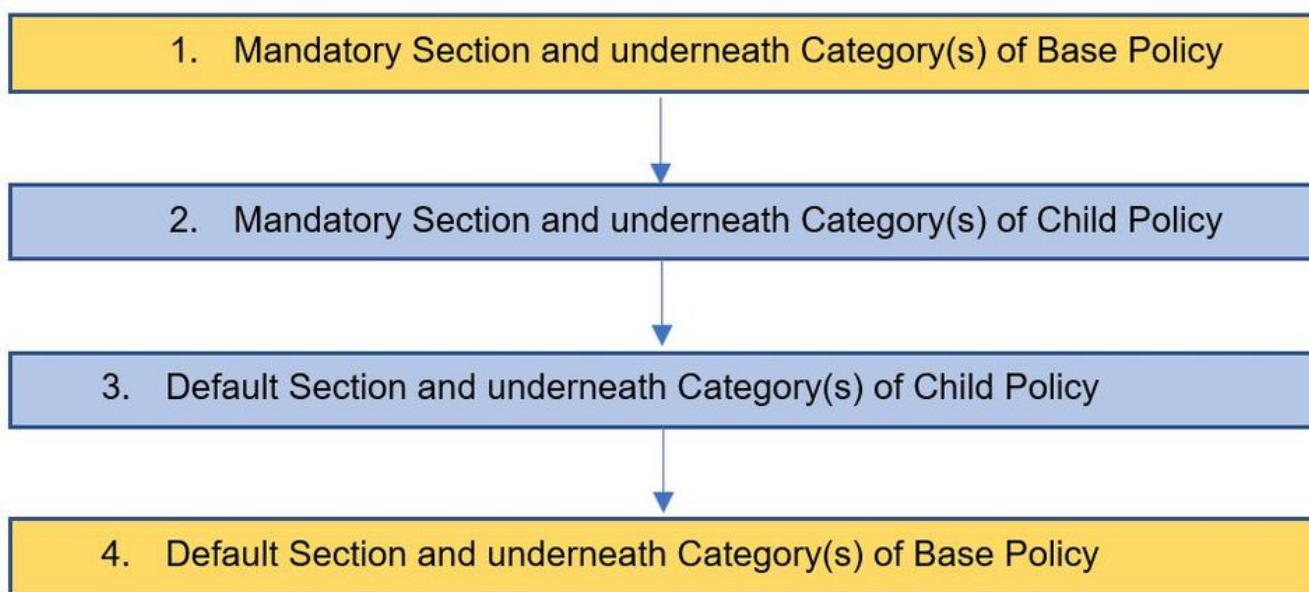
Impacted Devices

OK Cancel

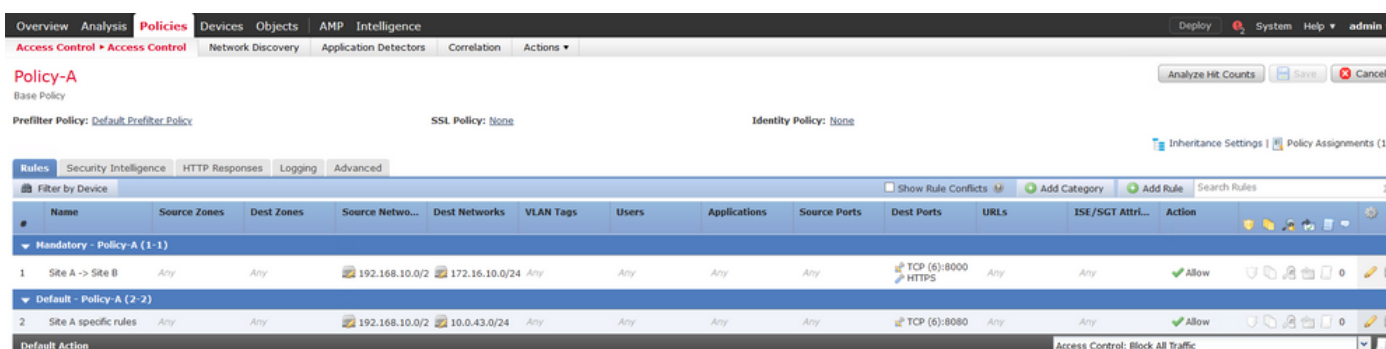
De forma predeterminada, la **Acción predeterminada** de la política secundaria se hereda y se establece en **Heredar de la política base** como se muestra en la imagen. El usuario también tiene la opción de seleccionar la **Acción predeterminada** de las Políticas proporcionadas por el sistema, como se muestra aquí.



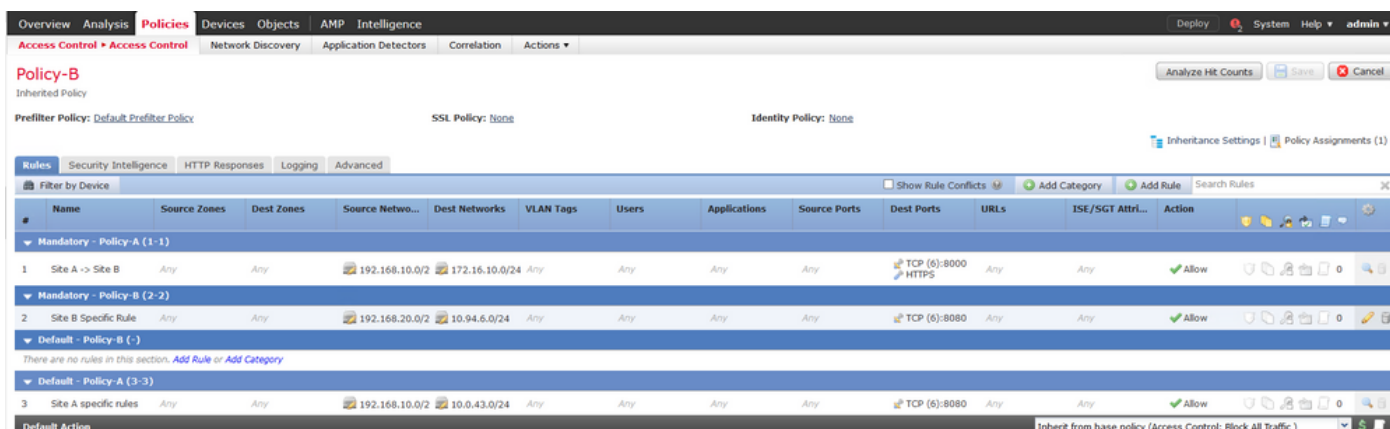
El orden de búsqueda del tráfico siempre estará de forma descendente independientemente del número de categorías agregadas en las secciones Obligatoria y Predeterminada. Después de aplicar la **configuración de herencia**, la representación ACP para la política secundaria Política-B (Política secundaria) como se muestra en la imagen, en línea con la **comprobación de orden de regla** mencionada anteriormente:



Esta imagen muestra cómo las políticas, a saber, la Política A, que es la política básica, y la Política B, que es la política secundaria y que se hereda de la Política A, se mostrarían en el FMC.




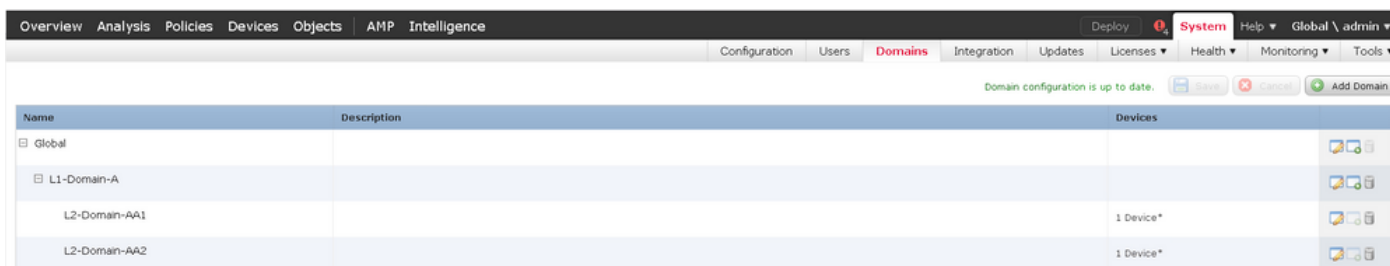
Esta imagen muestra que en la Política-B, las reglas de la Política-A se pueden ver así como las reglas específicas configuradas en la Política-B misma. Se debe tener cuidado de cómo se deben configurar las reglas teniendo en cuenta el orden.



Administración de FTD en entornos FMC de varios dominios

La función de varios dominios segmenta el acceso de los usuarios a dispositivos, configuraciones y eventos administrados. Un usuario podría cambiar a otros dominios en función de los privilegios. Si no se configura la función multidominio, todos los dispositivos, configuraciones y eventos administrados pertenecen al dominio **global**.

Se puede configurar un máximo de dominios de tres niveles con Global Domain como nivel uno. Todos los dispositivos administrados deben pertenecer únicamente al dominio de hoja. Esto se puede confirmar desde el símbolo del  (Agregar subdominio) atenuado en el dominio de hoja, como se muestra en la imagen.



Configuración de dominio

La configuración del dominio se puede realizar de la siguiente manera:

1. Vaya a **System > Domains**. De forma predeterminada, el dominio **global** está presente.
2. Haga clic en **Agregar dominio** como se muestra en la imagen.



3. Aparece el cuadro de diálogo **Agregar dominio**. Escriba el **nombre** del dominio y seleccione el **dominio principal** en la lista desplegable. Si este es el dominio de hoja, los dispositivos FTD deben agregarse al dominio como se muestra en la imagen.

Add Domain



Name:

Description:

Parent Domain:

Devices **Advanced**

Select the devices to which you would like to add to this domain.

Available Devices

- Global
 - LeafA FTD
- L1-Domain-A
 - LeafB FTD

Selected Devices

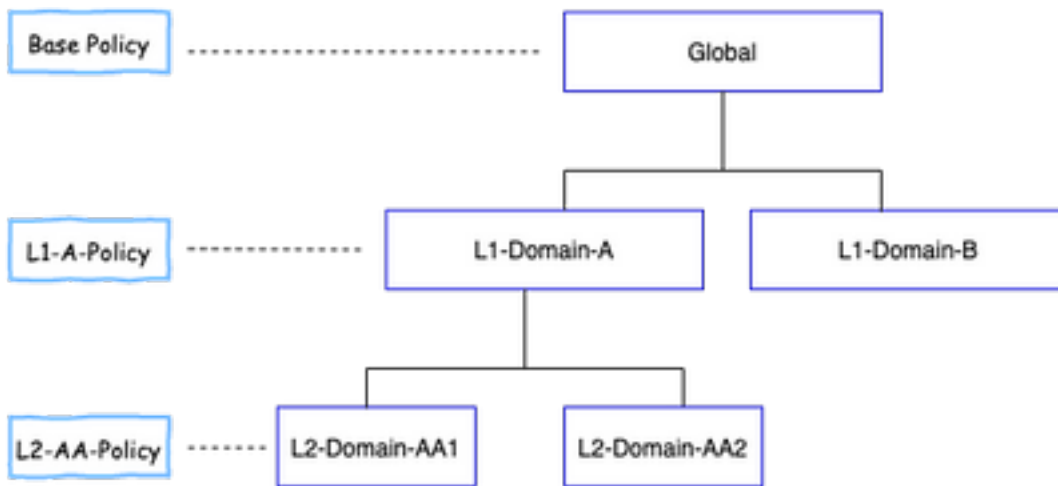
- Global
 - LeafA FTD

Nota: Para agregar los dominios, haga clic en el icono **Add Sub Domain** como se muestra en la imagen. Aquí el dominio primario ya está seleccionado.

Name	Description	Devices
Global		

Visibilidad y control de políticas en un entorno FMC de varios dominios

La visibilidad y el control de políticas se limitan a los usuarios de dominio respectivos, excepto para un administrador de dominio **global**. Este ejemplo se basa en la jerarquía de la siguiente manera:



Visibilidad: Como se muestra en esta imagen, la página de **Políticas de vista** predeterminada enumera las políticas (ACP) configuradas bajo el dominio respectivo.

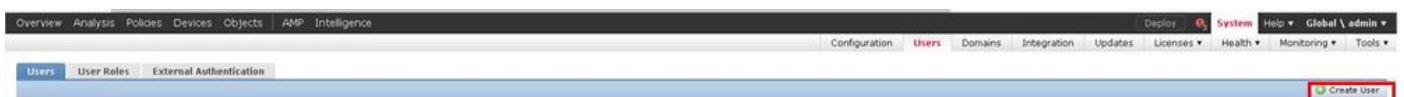


Control: Los usuarios **administrativos** que pertenecen al dominio respectivo pueden **EDITAR** las políticas. Para editar las políticas, que pertenecen a otros dominios (por ejemplo, como parte de la herencia), hay que cambiar el dominio de actual a un dominio en el que se configura la política. Sólo los usuarios administradores que pertenecen al dominio **global** o al dominio L1 pueden cambiar alrededor del dominio inferior para la administración de políticas.

Agregar usuarios al dominio

Muestra cómo agregar usuarios en un dominio determinado. Este procedimiento se aplica a los usuarios de la base de datos local.

1. Navegue hasta **Sistema > Usuarios**. Haga clic en **Crear usuario** como se muestra en la imagen.



2. Aparecerá el cuadro de diálogo **Configuración de usuario**. Rellene los campos **User Name** y **Password (& Confirm Password)**. Haga clic en **Agregar dominio** para agregar el usuario al dominio especificado como se muestra en la imagen.

User Configuration

User Name:

Authentication: Use External Authentication Method

Password:

Confirm Password:

Maximum Number of Failed Logins: (0 = Unlimited)

Minimum Password Length:

Days Until Password Expiration: (0 = Unlimited)

Days Before Password Expiration Warning:

Options: Force Password Reset on Login
 Check Password Strength
 Exempt from Browser Session Timeout

User Role Configuration + Add Domain

Domain	Roles

3. Elija el dominio deseado de la lista desplegable **Dominio** en la que desea agregar el usuario y especifique el rol como se muestra en la imagen. Se puede agregar un nuevo usuario al propio dominio o a los dominios secundarios.

User Role Configuration ?

Domain: ▼

Global

Global \ L1-Domain-A

Global \ L1-Domain-A \ L2-Domain-AA1

Global \ L1-Domain-A \ L2-Domain-AA2

Global \ L1-Domain-B

Default User Roles:

- Threat Intelligence Director Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin
- Threat Intelligence Director (TID) User

Los usuarios configurados se muestran en esta imagen:

Username	Domains	Roles	Authentication Method	Password Lifetime	
admin	Global	Administrator	Internal	Unlimited	
L1-A-admin	Global \ L1-Domain-A	Administrator	Internal	Unlimited	
L1-B-admin	Global	Administrator	Internal	Unlimited	
L2-AA-admin	Global \ L1-Domain-A \ L2-Domain-AA1	Administrator	Internal	Unlimited	
L2-AA2-admin	Global \ L1-Domain-A \ L2-Domain-AA2	Administrator	Internal	Unlimited	

El acceso a recursos en FMC se limitaría al dominio al que pertenece el usuario. Como se muestra a continuación, cuando el usuario **L1-A-admin** inicia sesión en la interfaz de usuario de FMC, el acceso se limita al dominio **L1-dominio A** del que forma parte el usuario y al dominio secundario una vez que el usuario cambia a ese dominio secundario. Este usuario puede editar solamente la política definida en el dominio **L1-Dominio-A** y la política definida en el dominio secundario cuando el dominio se conmuta a su dominio secundario. Además, se puede ver en el siguiente ejemplo que **L1-A-Policy** hereda la política definida en el dominio global, a saber **Base-Policy**, así como que se puede editar que se puede ver desde el signo. La configuración de herencia se realiza para señalar a la **Base-Policy** como se muestra en la imagen.

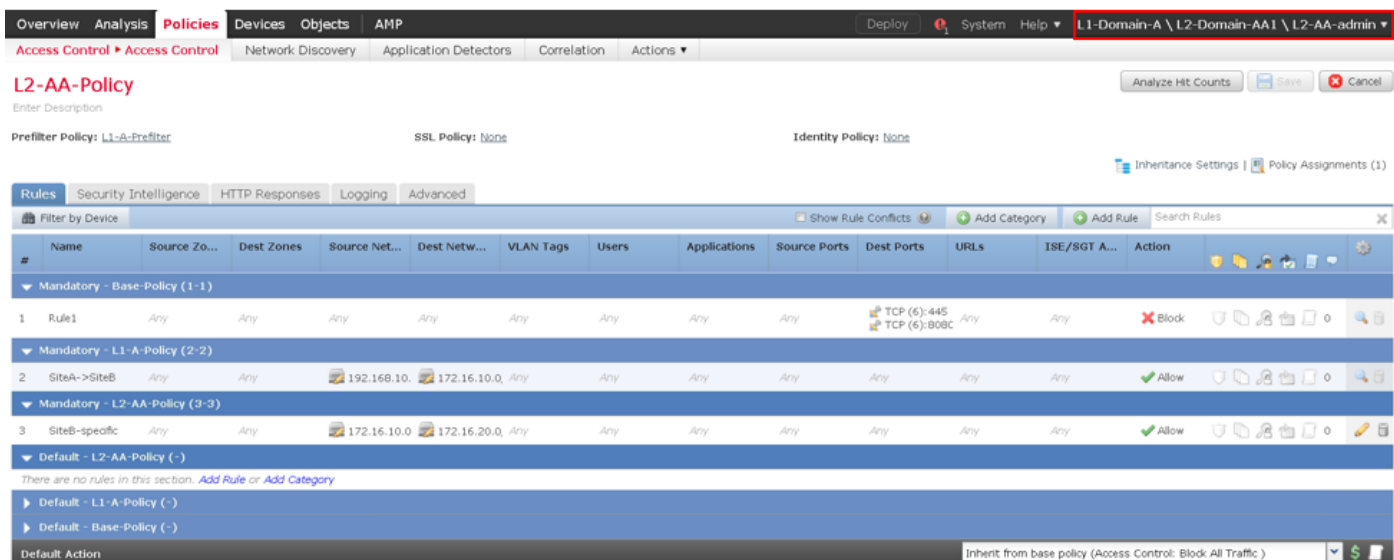
Access Control Policy	Domain	Status	Last Modified	
Base-Policy	Global	Targeting 0 devices	2020-05-28 22:49:49 Modified by "admin"	
L1-A-Policy	Global \ L1-Domain-A	Targeting 0 devices	2020-05-28 23:02:14 Modified by "admin"	

De manera similar, un usuario **L2-AA-admin** que pertenece al **dominio L2-AA1** sólo tiene control de la política **L2-AA-Policy** definida en el dominio como se muestra en la imagen. La política **L2-AA** hereda la política **L1-A-Policy** definida en **L1-Domain-A** que a su vez hereda su **política base** definida en el dominio global. Además, la política **L2-AA-Policy** se puede editar y se puede ver desde el signo. El usuario L2-AA-admin nunca puede cambiar a su dominio primario, a saber, L1-Domain-A, ni a su dominio anterior, a saber, el dominio global.

Access Control Policy	Domain	Status	Last Modified	
Base-Policy	Global	Targeting 0 devices	2020-06-17 13:48:54 Modified by "admin"	
L1-A-Policy	Global \ L1-Domain-A	Targeting 0 devices	2020-06-17 13:48:54 Modified by "admin"	
L2-AA-Policy	Global \ L1-Domain-A \ L2-Domain-AA1	Targeting 1 devices Up-to-date on all targeted devices	2020-06-17 13:48:54 Modified by "admin"	

Además, un usuario **L1-A-admin** que pertenece a L1-Domain-A puede cambiar a L2-Domain-AA1

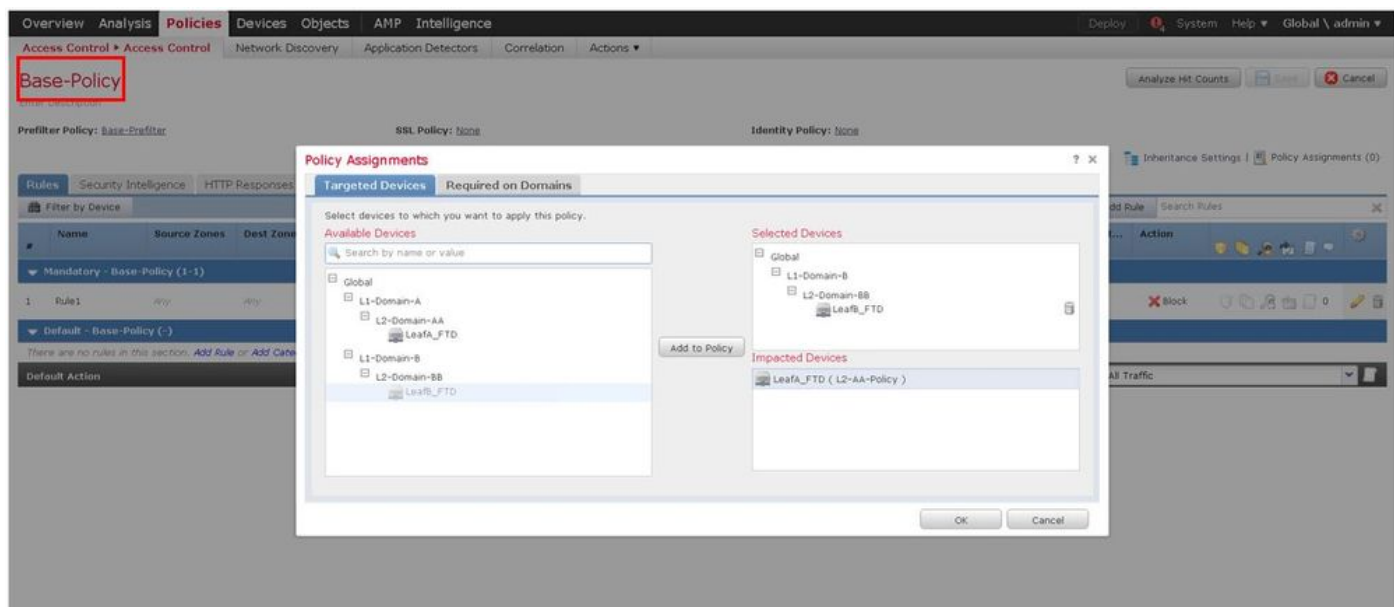
y editar la política **L2-AA-Policy** que se ve desde el como se muestra en la imagen. Esto se aplica incluso a un usuario que pertenece al dominio global y que cambia a los dominios secundarios y edita las políticas definidas en el dominio secundario en particular.



Puntos importantes a tener en cuenta:

- Al eliminar los dominios no globales, los usuarios que pertenecen a los dominios se mueven automáticamente al dominio **global**.

Los FTD se definen siempre en el dominio de hoja. En este caso, el dominio de hoja es el **L2-Domain**(es decir, L2-Domain-AA y L2-Domain-BB). El FTD que pertenece a **L2-Domain** se puede asignar a la política en **L1-Domain** o en el **Global** Domain. En esta imagen, el ACP en el dominio Global asignó el FTD definido en el dominio L3 a la política definida en el dominio Global.



- Los usuarios del dominio global pueden navegar a otros dominios específicos de usuario, pero los usuarios de un dominio específico solo tienen visibilidad en su propio dominio y sus dominios secundarios. No pueden navegar al dominio global ni a ningún otro dominio superior, como se muestra en esta tabla:

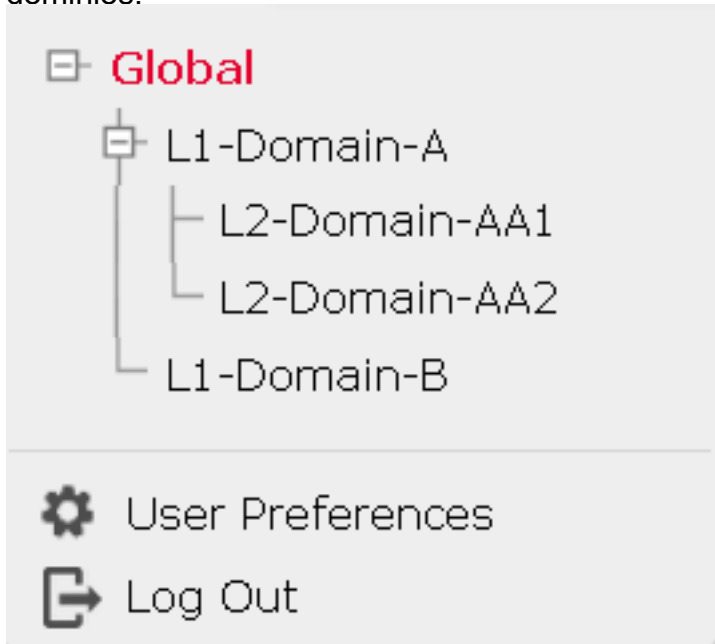
Dominio global

El usuario del dominio global tiene visibilidad de todos los dominios configurados y puede navegar a otros

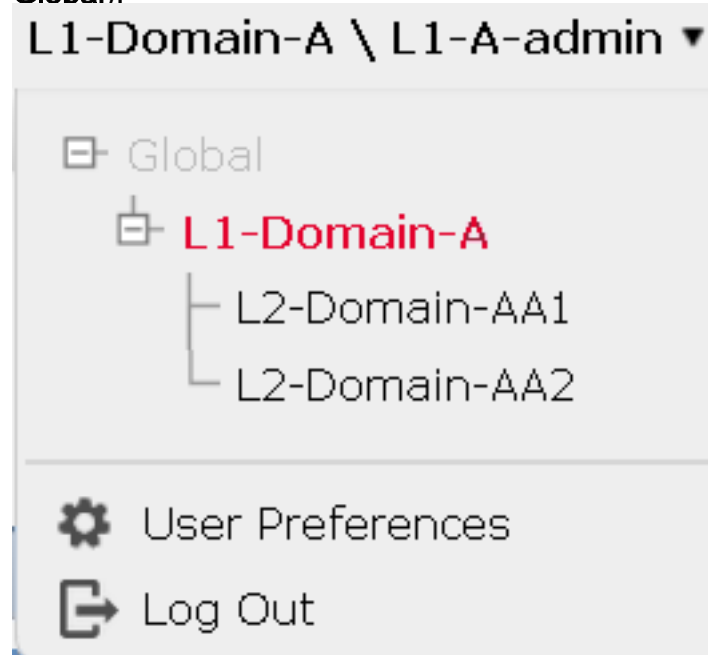
Dominio específico del usuario

El usuario en **L1-Domain-A** tendrá visibilidad sólo sí mismo y su dominio secundario, a saber, **L2-**

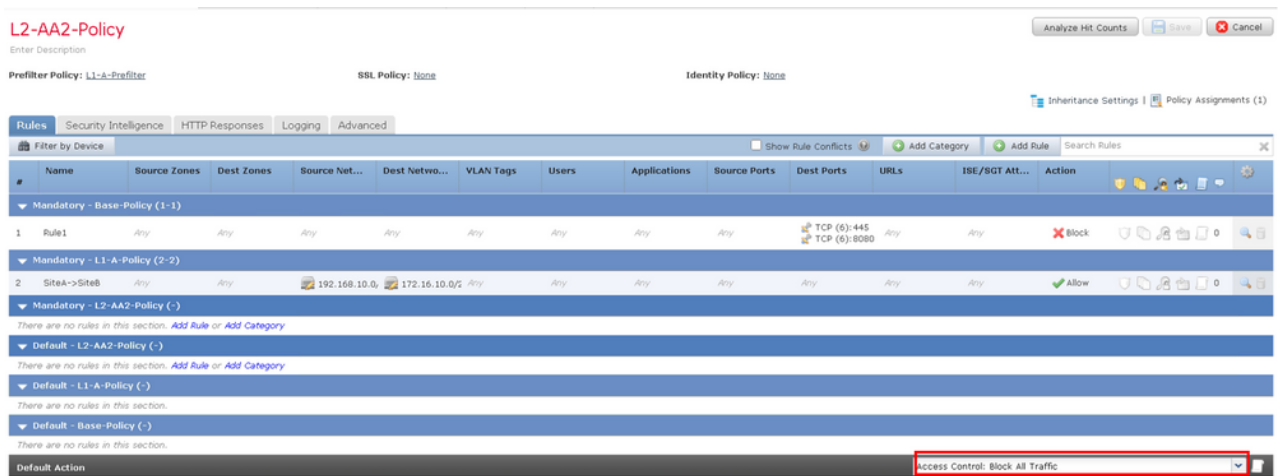
dominios.



Domain-AA y puede navegar a L2-Domain-AA. No permite el acceso a dominios de nivel superior (como Global).



- La acción predeterminada de la política secundaria no puede ser bloqueada por la política principal y el usuario no necesita heredar la acción predeterminada de la política principal como en esta imagen.



En esta imagen, se puede ver que el usuario no ha asignado la acción predeterminada como la del padre, lo que puede ser evidente a partir de las palabras **Hereder de la política base**: no ser visto en la acción predeterminada.

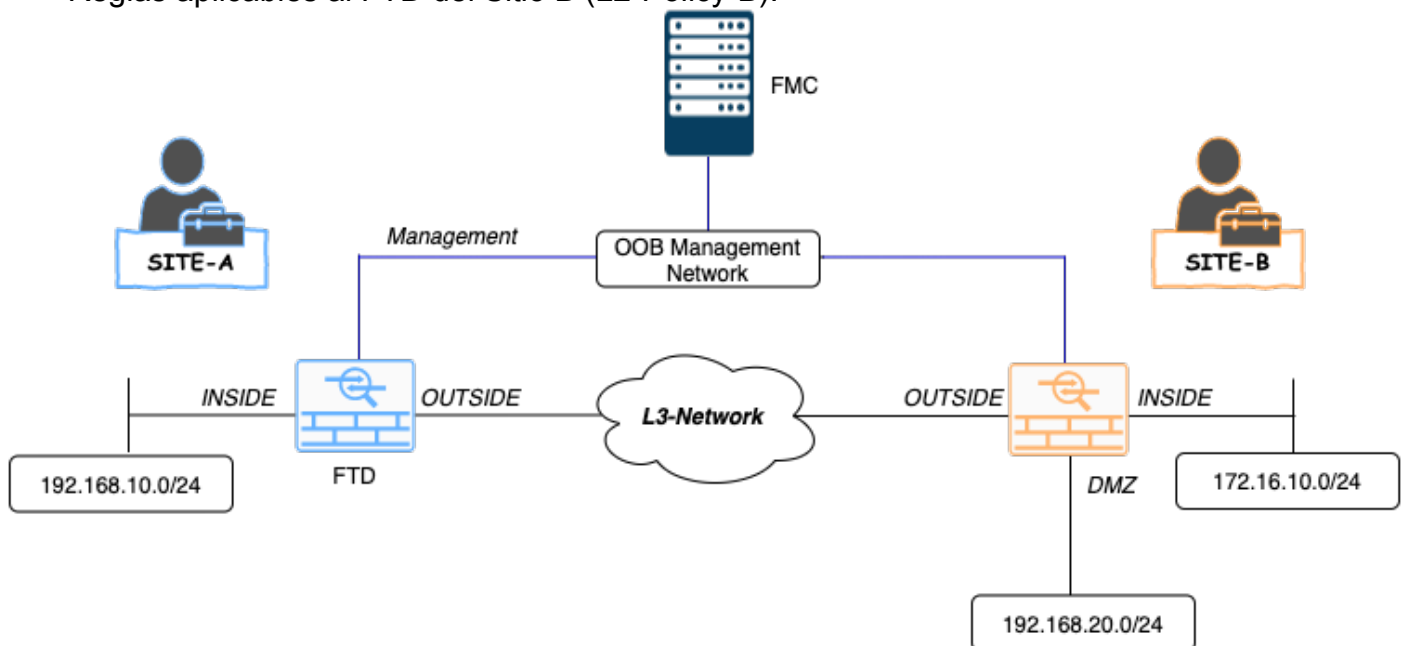
Nota: Debe tenerse en cuenta que un usuario no puede ver ambas políticas de dominio L1/L2 al mismo tiempo. El usuario debe cambiar al dominio deseado para ver y editar las políticas. Por ejemplo: si el usuario **admin** presente en el dominio global desea ver qué políticas se configuran en L1-Domain-A y L2-Domain-AA, el usuario puede hacerlo si cambia a L1-A-Domain para ver y editar la política configurada en ese dominio y luego cambia a L2-Domain-AA para ver y editar la política correspondiente, pero no puede ver ambas al mismo tiempo. Además, el usuario de L1-Domain-A no puede editar ni eliminar la política definida en el dominio global, es decir, la política base, que es la política principal de L1-A-Policy, y el usuario de L2-Domain-AA no puede editar ni eliminar las políticas, a saber, la política base y la política L2-A definida en dominios globales y L2-Domain-A

respectivamente.

Caso práctico

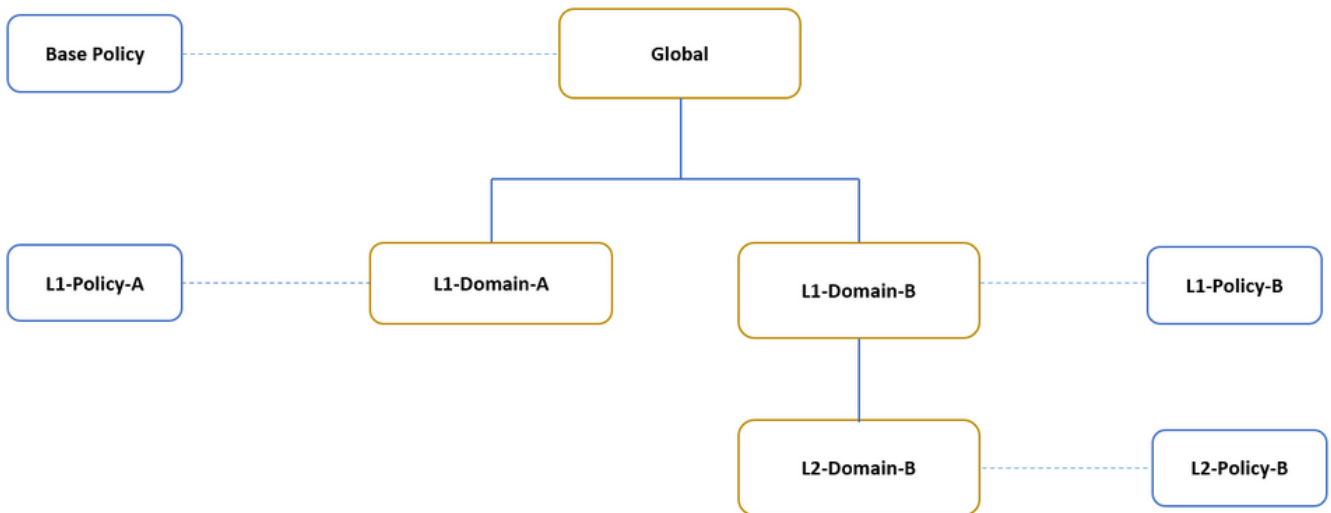
Considere el escenario representado en la imagen, los FTD del SITE-A (SiteA-FTD) y el SITE-B (SiteB-FTD) se gestionan mediante un único FMC a través de diferentes dominios (multidominio) para proporcionar acceso controlado. Desde el punto de vista de las políticas, estas son las consideraciones de política a nivel de organización:

- Las reglas de BLOQUE específicas del servicio que se aplican a TODOS los FTD independientes del SITIO o DOMINIO pertenecen a (política base).
- Reglas que cumplen los requisitos para cumplir el acceso del Sitio A al Sitio B (L1-Policy-A) y el Acceso del Sitio B al Sitio A (L1-Policy-B).
- Reglas aplicables al FTD del Sitio B (L2-Policy-B).



Herencia en un entorno de varios dominios

Para el caso de uso mencionado anteriormente, considere la siguiente jerarquía de dominio/política. SiteA-FTD y SiteB-FTD son parte de los dominios de hoja L1-Domain-A y L2-Domain-B respectivamente.



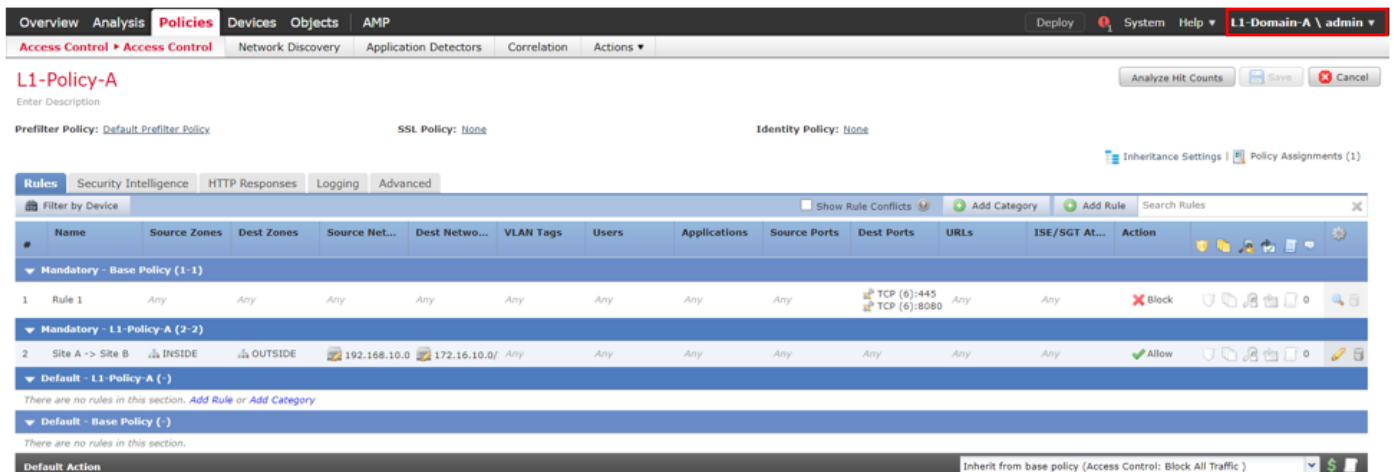
La estructura para la jerarquía de dominios es la siguiente:

- El dominio **global** es **primario** de **L1-Domain-A** y de **L1-Domain-B**.
- El dominio **global** es **ancestro** de **L2-Domain-B**.
- **L2-Domain-B** es hijo de **L1-Domain-B**
- **L2-Domain-B** es un dominio de hoja ya que no tiene dominios secundarios.

La imagen muestra la jerarquía de dominios tal como se ve desde FMC.



La siguiente instantánea muestra cómo se definen las reglas en **L1-Policy-A** y **L2-Policy-B** w.r.t al escenario anterior.



Overview Analysis **Policies** Devices Objects AMP Deploy System Help L1-Domain-B \ L2-Domain-B \ admin

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

L2-Policy-B

Analyze Hit Counts Save Cancel

Prefilter Policy: Default.Prefilter.Policy SSL Policy: None Identity Policy: None

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Net...	Dest Netwo...	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT At...	Action	
▼ Mandatory - Base Policy (1-1)														
1	Rule 1	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):445 TCP (6):8080	Any	Any	Block	
▼ Mandatory - L1-B-Policy (2-2)														
2	Site B->SiteA	Any	Any	172.16.10.5	192.168.10.0	Any	Any	Any	Any	TCP (6):443	Any	Any	Allow	
▼ Mandatory - L2-Policy-B (3-3)														
3	Site B access only	INSIDE	DNZ	Any	192.168.20.0	Any	Any	Any	Any	Any	Any	Any	Allow	
▼ Default - L2-Policy-B (-)														
There are no rules in this section. Add Rule or Add Category														
▼ Default - L1-B-Policy (-)														
There are no rules in this section.														
▼ Default - Base Policy (-)														
There are no rules in this section.														
Default Action													Inherit from base policy (Access Control: Block All Traffic)	

Siempre debe tener en cuenta las reglas y su herencia al configurar varios dominios para evitar bloquear el tráfico legítimo o permitir el tráfico no deseado.