## 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.

Overview Analysis Policies Devices Objects	Ame incesigence		Deploy 🦄 System Help 🗸 Global Ladiain 🗸
Access Control + Access Control Network Discover	ry Application Detectors Correlation Actions •		
Policy-B Enter Description			Analyze Hit Counts
Prefilter Policy: Default Prefilter Policy	SSL Policy: None	Identity Policy: <u>None</u>	
			Ta Inheritance Settings   M Policy Assignments (0)

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:	Policy-A	× 1
<ul> <li>Child Policy Inher</li> </ul>	itance Settings	
For settings selecte inherits 'Policy-B' a	ed below, no overrides will b as Base Policy. <mark>Learn More</mark>	e allowed within the child Policy that
🔲 Security Intellig	ence	<u>^</u>
🔲 Http Response		
🔲 Logging Setting	s	
Advanced		
🔲 General S	Settings	
🔲 Identity P	olicy Settings	*

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

elect devices to which you want to apply this policy. vailable Devices	Selected Devices	
Search by name or value	FTD	ä
	Add to Policy	
		,

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.

? X



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:

Default Action



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.

Overview Analysis Policies Devices Ob	ojects AMP Intelligence				Deploy 🔍 System Help 🔻 admin 🕶
Access Control > Access Control Network Disc	covery Application Detectors Correlation	Actions •			
Policy-A Base Policy					Analyze Hit Counts 📄 Save 🛛 🔇 Cancel
Prefilter Policy: Default Prefilter Policy	SSL Policy: None		Identity Policy: None		
				T	Inheritance Settings   🥂 Policy Assignments (1)
Rules Security Intelligence HTTP Responses	Logging Advanced				
Filter by Device			Show Rule Confli	ts 😣 🔾 Add Category 📿 Add	d Rule Search Rules 30
Name Source Zones Dest	t Zones Source Netwo Dest Networks	VLAN Tags Users App	olications Source Ports Dest Ports	URLs ISE/SGT Attri	Action 💿 🏷 🖉 🗢 🔅
➡ Mandatory - Policy-A (1-1)					
1 Site A -> Site B Any Any	2 192.168.10.0/2 2 172.16.10.0/2	<b>4</b> Αογ Αογ Αογ	γ Αογ <b>€</b> TCP (6):8000 <b>∂</b> HTTPS	Απγ Απγ	🖌 Allow 🗸 🕄 🖉 🖉 🖉 🖉 🖉 🖉
▼ Default - Policy-A (2-2)					
2 Site A specific rules Any Any	192.168.10.0/2 10.0.43.0/24	Any Any Any	γ Αny 🛫 TCP (6):8080	Απγ Απγ	🖌 Allow 🔍 🗋 🖉 😭 🖉 🖉 🖉
Default Action				Access Control: Block	All Traffic

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.

Overview Analysis Pol	licies Devices	Objects At	MP Intelligence										🖉 🔍 System Help	∗ admin v
Access Control + Access Co	ontrol Network	k Discovery Ap	pplication Detectors	Correlation	Actions •									
Policy-B Inherited Policy												Analyze	Hit Counts 📄 Save	Cancel
Prefilter Policy: Default Prefilte	er Policy			SSL Policy: None			Identity	Policy: None				Talantar	nce Settings   🧮 Policy Ass	signments (1)
Rules Security Intelligence	ce HTTP Respon	ises Logging	Advanced						Show Rule Confli	cts 😡	Add Category	Add Rule Se	earch Rules	×
ø Name	Source Zones	Dest Zones	Source Netwo	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLS	ISE/SGT	Attri Action	<b>U</b> 🗞 🖉 .	
👻 Mandatory - Policy-A (1-	1)													
1 Site A -> Site B	Any	Any	2 192.168.10.0/2	2 172.16.10.0/2	4 Any	Any	Any	Any	P TCP (6):8000 HTTPS	Any	Any	🖋 Allow	00.840	0 98
👻 Mandatory - Policy-B (2-	2)													
2 Site B Specific Rule	Ααγ	Any	2 192.168.20.0/2	2 10.94.6.0/24	Any	Any	Any	Any	📌 TCP (6):8080	Any	Any	🛹 Allow	00.800	0 🥒 🗄
➡ Default - Policy-B (-)														
There are no rules in this section	on. Add Rule or Add (	Category												
👻 Default - Policy-A (3-3)														
3 Site A specific rules	Any	Any	2 192.168.10.0/2	2 10.0.43.0/24	Any	Any	Any	Any	🛫 TCP (6):8080	Any	Any	🖋 Allow	00.800	0 98
Default Action											Inherit from base	policy (Access Cont	trol: Block All Traffic )	* \$ I

## 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.

Overview Analysis Policies Devices	bjects AMP Intelligence					De	eploy 🔍	System	Help 🔻 Globa	l∖admin <del>v</del>
		Configuration	Users	Domains	Integration	Updates	Licenses <b>v</b>	Health 🔻	Monitoring	Tools •
					Domain o	configuration is u	up to date. [	Save 🤇	Cancel	Add Domain
Name	Description						Devices			
Global										
E L1-Domain-A										728
L2-Domain-AA1							1 Device*			700
L2-Domain-AA2							1 Device*			738

#### 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.

Overview Analysis Policies Devices Objects AMP Intelligence						Deplo	y 0 By	istem Help v	admin <del>v</del>
	Config	uration User	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
				Domain cor	figuration is a	ep to date.	1 (and ) (0	0.4	idd Domain
Name	Description	0	evices						
Global		2	Devices					C.	

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

nt Domain:	L1-Domain-A		~	
evices	Advanced			
Select the c Available De	devices to which you wou evices	Id like to add to this dom	ain. Selected Devices	
Search	by name or value eafA FTD		Global	6
E L1-D	omain-A LeafB FTD	Add to Domain		

**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	1
🗉 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.

Overview Analysis Policies Devices Of	jects AMP Intelligence			Deploy 🥵 System Help •	Global \ admin +
Access Control + Access Control Network Di	covery Application Detectors Correlation	Actions •			
				Object Management Intrusion Network Analysis Policy	ONS Import/Export
				6	O New Policy
Access Control Policy	Domain		Status	Last Modified	
Base-Policy	Global		Targeting 0 devices	2020-05-27 21:43:00 Modified by "admin"	Q15 / 6

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 Name	L1-8-admin	
Authentication	🗍 Use External Authentication Method	
Password		
Confirm Password		
Naximum Number of Failed Logins	0	(0 = Unlimited)
Ninimum Password Length	9	
Days Until Password Expiration	0	(0 = Unlimited)
Days Before Password Expiration Warning	0	
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 Rol	e Configuration	?
Domain Default U	Global   Global   Global \ L1-Domain-A   Global \ L1-Domain-A \ L2-Domain-AA1   Global \ L1-Domain-A \ L2-Domain-AA2   Global \ L1-Domain-A \ L2-Domain-AA2   Global \ L1-Domain-B   Jser Roles   Image: Series   <	
	Save Cance	:

Los usuarios configurados se muestran en esta imagen:

Overview Analysis Polic	ies Devices Objects AMP Intelligence						Depioy 🛛 💘	System	Help V Globa	I∖admin ▼
		Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring	Tools •
Users User Roles	External Authentication									
									0	Create User
Username	Domains	Roles	Authentic	ation Method	l.	Pass	word Lifetime			
admin	Global	Administrator	Internal			Unlin	nited			0
L1-A-admin	Global \ L1-Domain-A	Administrator	Internal			Unlin	nited			2 🗄
L1-B-admin	Global	Administrator	Internal			Unlin	nited			J 🕄
L2-AA-admin	Global \ L1-Domain-A \ L2-Domain-AA1	Administrator	Internal			Unlin	nited			2 🗄
L2-AA2-admin	Global \ L1-Domain-A \ L2-Domain-AA2	Administrator	Internal			Unlin	nited			/ 8

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.

Overview Analysis Policies	Devices Objects	AMP					🍳 System Help 🔻	L1-Domain-A \ L1-A-admin 🔻
Access Control + Access Control	Network Discovery	Application Detectors	Correlation A	tions 🔻				
						Object Manager	nent Intrusion Network	Analysis Policy DNS Import/Export
								New Policy
Access Control Policy		De	omain		Status	Last Madified		
Base-Policy		Gio	obal		Targeting 0 devices	2020-05-28 22:49:4 Modified by "admin"	9	<b>BB4</b> 6
L1-A-Policy		Glo	ibal \ L1-Domain-A		Targeting 0 devices	2020-05-28 23:02:1- Modified by "admin"	<u>*</u>	Q E 2 6

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.

Overview Analysis Policies	Devices Objects	AMP			Deploy	$m{0}_1$ Syste	m Help 🔻	L1-Domain-A \ L2-Domain-AA	1 \ L2-AA-admin ▼
Access Control + Access Control	Network Discovery	Application Detectors Correlation	Actions 🔻						
						Ob	ject Managem	ent Intrusion Network Analysis Policy	DNS Import/Export
									New Policy
Access Control Policy		Domain		Status			Last Modifie	d	
Base-Policy		Global		Targeting 0 devices			2020-06-17 1 Modified by "a	13:48:54 idmin*	🗈 🖪 🔍 🖯
⊒ L1-A-Policy		Global \ L1-Domain-A		Targeting 0 devices			2020-06-17 Modified by "a	.3:48:54 idmin*	🗅 🖪 🔍 🖯
L2-AA-Policy		Global \ L1-Domain-A \ L2-Domain-AA	1	Targeting 1 devices Up-to-date on all targeted d	levices		2020-06-17 1 Modified by "a	3:48:54 dmin*	Pa 🖸 🥒 🖯

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.

Overview Analys	s Policies	Devices Ob	jects AMP							System H	elp 🔻 L1-Don	nain-A \ L2-	Domain-AA1 \ L2-A#	-admin 🔻
Access Control • Ac	cess Control	Network Dis	covery Appl	ication Detecto	rs Correlat	on Actions	•				_			
L2-AA-Policy Enter Description											(	Analyze Hit C	counts 🔚 Save	🙁 Cancel
Prefilter Policy: L1-A-P	refiter			SSL Policy: Non	2			Identity Po	licy: None					
Pulse Security In	talliganca	TTD Deeponeer	Logging	Advanced							1	Inheritance :	Settings   🥂 Policy Assig	nments (1)
Filter by Device	itelligence H	IT IP Responses	Logging	Advanced				Show Ru	le Conflicts 😡	Add Categ	ory 🙆 Add R	ule Search P	tules	×
Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT A	Action		- 45
#													😈 🐚 🔏 🏚 🧾 🖞	- ~~
👻 Mandatory - Base	-Policy (1-1)													
1 Rule1	Any	Any	Any	Any	Any	Any	Any	Any	📌 TCP (6):445 📌 TCP (6):8080	Any	Any	🗙 Block	00.2100	۹. 🗄
👻 Mandatory - L1-A	-Policy (2-2)													
2 SiteA->SiteB	Any	Any	2 192.168.10	. 👼 172.16.10.0	Any	Any	Any	Any	Any	Any	Any	🛹 Allow	002000	۹
👻 Mandatory - L2-A	A-Policy (3-3)													
3 SiteB-specific	Any	Any	2 172.16.10.0	172.16.20.0	Any	Any	Any	Any	Any	Any	Any	Allow	VDROD	0
🗢 Default - L2-AA-P	olicy (-)													
There are no rules in t	his section. <mark>Add R</mark>	ule or Add Categ	pry											
Default - L1-A-Po														
Default - Base-Po														
Default Action										Inherit from	base policy (Acces	s Control: Blo	k All Traffic )	× \$ 📑

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.

Overview Analysis Policies Devices	Objects AMP Intelligence	-		Dep	oloy   🌒 System	v Help ♥ Global \ admin ♥
Base-Policy					Analyze Hit Cou	nts
Prefilter Policy: Base-Prefiter	SSL Policy: Mane		Identity Policy: NODE			
	Policy Assignments			? X	Inheritance Se	ttings   🧾 Policy Assignments (0)
Rules Security Intelligence HTTP Responses	Targeted Devices Required on Domains Select devices to which you want to apply this policy.				dd Rule Search Rule	s X
Name         Source Zones         Dest Zone                Mandatory - Bose-Policy (1-1)                 Policy                 1 Rule 1 - May - May               May               May                 Visionalt - Base-Policy (-)                 Policy - Add Care	Available Devices  Cobal  L1-Domain-A  L2-Domain-A  L3-Domain-AA  Lata Lata Lata Lata	Add to Policy	Selected Devices	8	L., Action XBlock	00.800 · /8
Default Action	Luaff_FTD		LeafA_FTD ( L2-AA-Policy )	Cancel	All Traffic	

 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. N

• 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.

L2 Ent	2-AA2-Po er Description	olicy											Analyze Hit C	ounts 🔚 Save 😣	Cancel
Pre	filter Policy: L	1-A-Prefilter		88	L Policy: None			Ide	ntity Policy: None						
												T	Inheritance	Settings   🥂 Policy Assignm	ients (1)
R	ules Secur	rity Intelligence HTTP	Responses I	Logging Advan	ced										
đ	Filter by Devi	ice							🗌 Shor	w Rule Conflicts 😣	🔾 Add 🤇	Category 🛛 🕥 Add R	tule Search P	tules	×
	Name	Source Zones	Dest Zones	Source Net	Dest Netwo	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Att	Action		
-	Mandatory -	Base-Policy (1-1)													
1	Rule1	Any	Any	Any	Any	Any	Any	Any	Any	🛫 TCP (6):445 🛫 TCP (6):808	Any	Any	× Block	002100	۹.5
-	Mandatory -	L1-A-Policy (2-2)													
2	SiteA->Site	eB Any	Any	192.168.10.	0, 👳 172.16.10.0,	n Any	Any	Any	Any	Any	Any	Any	Allow 🐦	0 0 2 1 10	9
-	Mandatory -	L2-AA2-Policy (-)													
72	iere are no ruk	es in this section. Add Rul	e or Add Category	(											
-	Default - L2-	AA2-Policy (-)													
72	iere are no ruk	es in this section. Add Rul	le or Add Category	(											
-	Default - L1-	A-Policy (-)													
72	iere are no ruk	es in this section.													
-	Default - Ba	se-Policy (-)													
77	iere are no ruk	es in this section.													_
D	fault Action										Acc	ess Control: Block All T	raffic		× 1

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 Heredar 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).





#### 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.

								_	
Overview Analysis Policies Devices Object	s AMP Intelligence					Deploy	🔹 Syster	n Help 🔻 Glol	bal \ admin 🔻
		Configuration	Users	Domains	Integration	Updates Lic	enses 🔻 Heal	th  Monitori	ig ▼ Tools ▼
					Domain o	configuration is up to	date. 🔠 Save	Cancel	Add Domain
Name	Description					D	evices		
🗄 Global									<b>73</b> 8 Î
L1-Domain-A						1	Device*		
E L1-Domain-B									
L2-Domain-B						1	Device*		

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

Overview Analysi	is Policies	Devices Obje	cts AMP								Deploy 🔒	System H	elp 🔻 L1-Domain-A \	admin 🔻
Access Control + Ac	cess Control	Network Discov	very Applicat	ion Detectors	Correlation	Actions •								
L1-Policy-A											(	Analyze Hit	Counts Save	Cancel
Prefilter Policy: Default	Prefilter Policy		S	iL Policy: None			1	Identity Policy: 🖞	ione					
											Te	Inheritance S	iettings   🖳 Policy Assignm	ents (1)
Rules Security In	telligence HTT	P Responses L	ogging Adva	nced										
B Filter by Device								Show I	Rule Conflicts 😣	Add Category	🔇 Add Rule	e Search R	ules	ж
Name #	Source Zones	Dest Zones	Source Net	Dest Netwo	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs I	SE/SGT At	Action	• • • •	۲
👻 Mandatory - Base	Policy (1-1)													
1 Rule 1	Any	Any	Any	Any	Any	Any	Any	Any	☆ TCP (6):445☆ TCP (6):8080	Any	Any	X Block	0.2010	۹.8
👻 Mandatory - L1-P	olicy-A (2-2)													
2 Site A -> Site B	👍 INSIDE	A OUTSIDE	2 192.168.10.0	2 172.16.10.0/	Any	Any	Any	Any	Any	Any	Any	Allow 🔶	002000	6
👻 Default - L1-Polic	γ- <b>∧ (</b> -)													
There are no rules in th	is section. Add Rule	or Add Category												
👻 Default - Base Pol	licy (-)													
There are no rules in th	is section.													
Default Action										Inherit from bas	e policy (Access	Control: Bloc	k All Traffic ) 👻	\$ 📄

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
Prefilter Policy: <u>Default Prefiter Policy</u> SSL Policy: <u>Mane</u>	Identity Policy: Kana
Rules Security Intelligence In LP Responses Logging Advanced	Show Rule Conflicts W 🙆 Add Category 🙆 Add Rule Search Rules
Name Source Zones Dest Zones Source Net Dest Netwo VLAN Tags Users Applicati	tions Source Ports Dest Ports URLs ISE/SCT 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 XBlock 🗍 🖓 🖄 🗌 0 🔍 3
▼ Mandatory - L1-B-Policy (2-2)	
2 Site B->SiteA Any Any 2172.16.10.5 2192.168.10.0 Any Any Any	Any 👷 TCP (6):443 Any Any 🧳 Allow 🗍 🖒 🖉 🖄 🗍 O 🔍 🔂
▼ Mandatory - L2-Policy-B (3-3)	
3 Site B access only 🚠 INSIDE 🚠 DMZ Any 👷 192.168.20.0 Any Any Any	Any Any Any Any Any 🖌 🖓 🖓 🖓 🎜 🖉 🥖
▼ 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.	

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.