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.

Overview Analysis Policies Devices Objects	AMP Intelligence		Deploy 🥵 System Help 🔻 Global 🔪 admin 🔻
Access Control + Access Control Network Discovery	Application Detectors Correlation Actions •		
Policy-B Enter Description			Analyze Hit Counts 📄 🔚 🚥 🛛 😂 Cancel
Prefilter Policy: Default Prefilter Policy	SSL Policy: None	Identity Policy: None	
			Ta Inheritance Settings M Policy Assignments (0)

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.

Inheritance Settings

select base Policy:	Policy-A	
 Child Policy Inher 	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	÷
🔲 Http Response		
🔲 Logging Setting	s	
Advanced		
🔲 General S	Settings	
T Identity P	olicy Settings	-

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

vailable Devices	Selected Devices	
Search by name or value	FTD	
	Add to Policy Impacted Devices	

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.

? X



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:

Default Action



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.

Overview Analysis Po	Devices	Objects /	AMP Intelligence									Deploy	🍳 System Help 🔻	admin v
Access Control + Access C	ontrol Networ	k Discovery	Application Detectors	Correlation	Actions •									
Policy-A Base Policy												Analyze H	it Counts 📄 🔚 Save 🛛 🕻	Cancel
Prefilter Policy: Default Prefit	er Policy			SSL Policy: None			Identity	Policy: None						
												Inheritanc	e Settings 🥂 Policy Assign	ments (1)
Rules Security Intelligen	ce HTTP Respo	nses Logging	Advanced											
Filter by Device									Show Rule Confli	cts 😣	Add Category Add Category	d Rule Sea	rch Rules	26
a Name	Source Zones	Dest Zones	Source Netwo	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLS	ISE/SGT Attri	Action	• • .a to = •	. *
👻 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	🛫 TCP (6):8000 > HTTPS	Any	Αηγ	🖋 Allow	00.840.0	/ 6
▼ Default - Policy-A (2-2)														
2 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	UD.8 to •	08
Default Action											Access Control: Block	All Traffic		~

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.

Overview Analysis Poli	cies Devices	Objects At	MP Intelligence										🍳 System Help 🔻 adı	lmin v
Access Control + Access Cor	ntrol Network	k Discovery Ap	pplication Detectors	Correlation	Actions •									
Policy-B Inherited Policy												Analyze H	it Counts 🛛 🔚 Save 🛛 😮 Ca	ancel
Prefilter Policy: Default Prefilter	Policy			SSL Policy: None			Identity	Policy: None				Tan Inheritan	ce Settings 🧮 Policy Assignmen	nts (1)
Rules Security Intelligence	 HTTP Response 	ses Logging	Advanced											
# Filter by Device									Show Rule Confli	cts 😣	Add Category	Add Rule Sea	irch Rules	×
a Name S	Source Zones	Dest Zones	Source Netwo	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLS	ISE/SGT	Attri Action	• • • • • •	
👻 Mandatory - Policy-A (1-1)													
1 Site A -> Site B A	lay	Any	2 192.168.10.0/2	2 172.16.10.0/2	4 Any	Any	Any	Any	₽ TCP (6):8000 → HTTPS	Any	Any	🖋 Allow	0.8410	۹.6
👻 Mandatory - Policy-B (2-2))													
2 Site B Specific Rule A	lay	Any	2 192.168.20.0/2	2 10.94.6.0/24	Any	Any	Any	Any	📌 TCP (6):8080	Any	Any	🖋 Allow	V D A to D o	1
👻 Default - Policy-B (-)												1		
There are no rules in this section	n. Add Rule or Add C	Category												
👻 Default - Policy-A (3-3)														
3 Site A specific rules A	lay	Any	2 192.168.10.0/2	2 10.0.43.0/24	Any	Any	Any	Any	📌 TCP (6):8080	Any	Any	🖋 Allow	0.8000	۹. 5
Default Action											Inherit from base	policy (Access Contr	ol: Block All Traffic) 👻 🕯	s 🔳

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 La (Adicionar subdomínio) sendo esmaecido no domínio de folha como mostrado na imagem.

Overview Analysis Policies Devices Object	cts AMP Intelligence					De	eploy 🌖 🌖	System	Help 🔻 Globa	ıl∖admin v
		Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring	 Tools •
					Domain c	onfiguration is u	up to date.	🔚 Save 🕻	3 Cancel	Add Domain
Name	Description						Devices			
Global										
L1-Domain-A										778
L2-Domain-AA1							1 Device*			738
L2-Domain-AA2							1 Device*			738

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.

Overview Analysis Policies Devices Objects AMP Intelligence							Deplo	0, Sy	stem Help v	admin v
		Configuration	Users	Domains	Integration	Updates	Licenses +	Health •	Monitoring •	Tools •
					Domain con	figuration is u	up to date.	0	(dd Domain
Name	Description		Devi	ices						
Global			2 De	vices					C.	3638

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.

Add Domain

nt Domain:	L1-Domain-A		~	
evices	Advanced			
Select the d Available De	evices to which you wou wices	ld like to add to this dom	ain. Selected Devices	
Global	oy name or value afA FTD		Global	6
⊟ L1-Do	omain-A LeafB FTD	Add to Domain		

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

Name	Description	Devices	
🗉 Global			

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.

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	System Help + Global \ admin +
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions •			
						Object Management Intrusion Netwo	rk Analysis Policy ONS Import/Export
							Q New Policy
Access Control Policy			Domain		Status	Last Modified	
Base-Policy			Global		Targeting 0 devices	2020-05-27 21-43-00 Modified by "admin"	Q (5 🖉 B

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.



 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.

User Name	L1-8-admin	
Authentication	🗍 Use External Authentication Method	
Password		
Confirm Password		
Maximum 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. 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.

User Rol	e Configuration		?
Domain Default U	Global Global \L1-Domain-A Global \L1-Domain-A \L2-Domain-A Global \L1-Domain-A \L2-Domain-A Global \L1-Domain-B User Roles Jser Roles	The second secon	
		Save Cancel	

Os usuários configurados são mostrados nesta imagem:

Overview Analysis Polic	ies Devices Objects AMP Intelligence			Deploy 🧕	System	elp 🔻 Global	∖ admin ▼
		Configuration	Users Domains Integration	Updates Licenses •	Health 🔻	Monitoring 🔻	Tools •
Users User Roles	External Authentication						
						00	reate User
Username	Domains	Roles	Authentication Method	Password Lifetime	Password Lifetime		
admin	Global	Administrator	Internal	Unlimited			0
L1-A-admin	Global \ L1-Domain-A	Administrator	Internal	Unlimited			/ 1
L1-B-admin	Global	Administrator	Internal	Unlimited	Unlimited		
L2-AA-admin	Global \ L1-Domain-A \ L2-Domain-AA1	Administrator	Internal	Unlimited			/ 8
L2-AA2-admin	Global \ L1-Domain-A \ L2-Domain-AA2	Administrator	Internal	Unlimited			/ 8

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 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.

Overview Analysis Policies	Devices Objects A	MP				Deploy 0 System Hel	p 🔻 L1-Domain-A \ L1-A-admin 🔻
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions 🔻			
						Object Management Intrusion Netw	ork Analysis Policy DNS Import/Export
							O New Policy
Access Control Policy		De	omain		Status	Last Madified	
Base-Policy		Gio	ibal		Targeting 0 devices	2020-05-28 22:49:49 Modified by "admin"	BB4 6
L1-A-Policy		Glo	bal\L1-Domain-4		Targeting 0 devices	2020-05-28 23:02:14 Modified by "admin"	Q E 2 6

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.

Overview Analysis Policies	Devices Objects	АМР	D	Deploy 🧕	System Help 🔻	L1-Domain-A \ L2-Domain-AA	1 \ L2-AA-admin ▼
Access Control + Access Control	Network Discovery	Application Detectors Correlation Actions	,				
					Object Manageme	ent Intrusion Network Analysis Policy	DNS Import/Export
							New Policy
Access Control Policy		Domain	Status		Last Modifier	1	
Base-Policy		Global	Targeting 0 devices		2020-06-17 1 Modified by "a	3:48:54 dmin*	🗈 🖪 🔍 🖯
⊟ L1-A-Policy		Global \ L1-Domain-A	Targeting 0 devices		2020-06-17 1 Modified by "a	3:48:54 dmin*	🗅 🖪 🔍 🖯
L2-AA-Policy		Global \ L1-Domain-A \ L2-Domain-AA1	Targeting 1 devices Up-to-date on all targeted device	xes	2020-06-17 1 Modified by "a	3:48:54 dmin*	Pa 🖸 🥒 🖯

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.

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)	× \$ 📑

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.

Overview Analysis Policies Devices Access Control + Access Control Network Dr Base-Policy	Objects AMP Intelligence acovery Application Detectors Correlation Actions •			Dep	oloy O ₄ Syste	m Help ¥ Global \ admin ¥
Prefilter Policy: <u>Lass-Frefilter</u>	sst. Policy: t <u>sone</u> Policy Assignments Tarpeted Devices Required on Domains		Identity Policy: <u>Name</u>	7 ×	Te Inheritance S	ettings I 🕂 Policy Assignments (D)
Fiter by Device Name Source Zones Dest Zone Prindatory - Base Policy (1-1) Pule1 way way Default - Base Policy (-) There are no nules in this sector. Add Sule or Add Care Default Action	Select devices to which you want to apply this policy. Available Devices Cobbal Cobbal L1-Doman-A C2-Doman-AA C1-Doman-AA C2-Doman-BB L2-Doman-BB C2-Doman-BB C2-Doman-BB	Add to Policy	Selected Devices Global L1-Domain-B L2-Domain-BB L2-Comain-BB Larda_FTD Impacted Devices Leafa_FTD (L2-AA-Policy)	5	dd Pule Search Fu Action X Block All Traffic	e ×
		ï	OK.	Cancel		

 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

O usuário no domínio global tem visibilidade de todos os domínios configurados e pode navegar para outros domínios.

Domínio específico do usuário

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



• 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.

L2.	AA2-Policy Description												Analyze Hit (Counts 📄 Save	Cancel
Prefil	ter Policy: L1-A	-Prefilter		\$\$	L Policy: None			Ide	entity Policy: None	2					
												ī	Inheritance	Settings 🧾 Policy Assign	nents (1)
Rul	es Security	Intelligence HTTP	Responses I	Logging Advan	ced										
â	Filter by Device								C Sho	w Rule Conflicts 😣	O AI	dd Category 🛛 🕥 Add F	tule Search	Rules	×
	Name	Source Zones	Dest Zones	Source Net	Dest Netwo	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLS	ISE/SGT Att	Action	U 🔈 🖈 🗉 🔹	٢
-	Mandatory - Ba	se-Policy (1-1)													
1	Rule1	Any	Any	Any	Any	Any	Any	Any	Any	🛫 TCP (6):445 🛫 TCP (6):808	Any	Any	× Block	00.840.	۹. 6
-	Mandatory - L1	-A-Policy (2-2)													
2	SiteA->SiteB	Any	Any	2 192.168.10	0, 👳 172.16.10.0,	ng Any	Any	Any	Any	Any	Any	Any	🛹 Allow	00.2000	۹.
-	Mandatory - L2	-AA2-Policy (-)													
The	re are no rules in	n this section. Add Ruk	e or Add Category	·											
-	Default - L2-AA	2-Policy (-)													
The	re are no rules in	n this section. Add Ruk	e or Add Category	r											
-	Default - L1-A-F	Policy (-)													
The	re are no rules in	this section.													
-	Default - Base-I	Policy (-)													
The	re are no rules in	this section.									_				_
and the second second												anness Control, Black All M			

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 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).
 Regras aplicáveis ao FTD do site B (L2-Policy-B).
 FMC
 Management
 OOB Management
 Network
 INSIDE
 <

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.

192.168.20.0/24



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.

Overview Analysis Policies Devices	Objects AMP Intelligence		De	ploy 📀 System Help 🔻 Global \ admir	n v
		Configuration Users	Domains Integration Updates	Licenses • Health • Monitoring • Tool	s v
			Domain configuration is u	op to date. 📄 Save 🔞 Cancel 🔕 Add Domi	ain
Name	Description			Devices	
Global					Î
L1-Domain-A				1 Device"	
E L1-Domain-B					
L2-Domain-B				1 Device"	

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

Overview Analysi	s Policies	Devices Obje	cts AMP								Neploy 🔒	System H	elp 🔻 L1-Domain-A \	admin 🔻
Access Control + Ac	cess Control	Network Discov	very Applica	ion Detectors	Correlation	Actions •								
L1-Policy-A	.1-Policy-A Raalyze Hit Counts 🛛 📄 Save 🗋 😂 Cance													Cancel
Prefilter Policy: Default	Prefilter Policy		S	it. Policy: None			1	dentity Policy: 🛽	ione					
											Te 1	Inheritance S	ettings 🧾 Policy Assignm	ents (1)
Rules Security In	ales Security Intelligence HTTP Responses Logging Advanced													
B Filter by Device								Show F	Rule Conflicts 🧕	Add Category	🔕 Add Rule	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	• • <u>a</u> 🕁 🗉 •	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	00.840.	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	Απγ	Any	Any	Any	Any	Any	Allow 🐦	002000	J 🕄
👻 Default - L1-Polic	y-∧ (-)													
There are no rules in th	is section. Add Rule	e or Add Category												
👻 Default - Base Pol	icy (-)													
There are no rules in th	is section.													
Default Action										Inherit from bas	e policy (Access	Control: Block	c All Traffic) 👻	\$ 📑

Overview Analysis Policies Devices	Objects AMP						eploy 🔒 Sys	tem Help 🔻	L1-Domain	B \ L2-Domain-B \ a	dmin v
Access Control > Access Control Network	Discovery Application D	Detectors Correlation	Actions •								
L2-Policy-B									Analyze Hit Cou	ints 📄 Save 🛛 😫	Cancel
Prefilter Policy: <u>Default Prefilter Policy</u>	SSL Po	licy: <u>None</u>		Id	lentity Policy: <u>No</u>	ne		1	Inheritance Se	ttings 📕 Policy Assignm	ents (1)
Filter by Device	es Logging Mavanced				Show	Rule Conflicts 😣	Add Category	🔹 📀 Add Ru	le Search Ru	les	×
Name Source Zones Dest Zo	nes Source Net De	st Netwo VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLS I	SE/SGT At	Action	• • 4 6	٢
▼ Mandatory - Base Policy (1-1)											
1 Rule 1 Any Any	Any Anj	y Any	Any	Any	Алу	☆ TCP (6):445☆ TCP (6):8080	Any	Any	🗙 Block	00.2400	۹. ۵
▼ Mandatory - L1-B-Policy (2-2)											
2 Site B->SiteA Any Any	2 172.16.10.5 👳	192.168.10.0 Any	Any	Any	Any	📌 TCP (6):443	Any	Any	🛷 Allow	0020000	9,8
▼ 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	Allow 🗸	00.200.	/ 🛙
▼ Default - L2-Policy-B (-)											
There are no rules in this section. Add Rule or Add Ca	tegory										
➡ Default - L1-B-Policy (-)											
There are no rules in this section.											
➡ Default - Base Policy (-)											
Where are no order in this continu											

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