# FTDでのマルチドメイン環境での継承

### 内容

概要
前提条件
要件
使用するコンポーネント
背景説明
ポリシー継承の設定
マルチドメインFMC環境でのFTD管理
ドメインの設定
マルチドメインFMC環境におけるポリシーの可視性と制御
ドメインへのユーザの追加
使用例
マルチドメイン環境での継承

### 概要

このドキュメントでは、継承およびマルチドメイン機能の設定と動作について説明します。また 、この2つの機能がどのように連動するかを実際の使用例で説明します。

### 前提条件

#### 要件

次の項目に関する基本的な知識が推奨されます。

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

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Firepower Management Center(FMC)ソフトウェアバージョン6.4
- Firepower Threat Defense(FTD)ソフトウェアバージョン6.4

**注**:マルチドメインおよび継承機能のサポートは、6.0バージョン以降のFMC/FTDで利用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。ネットワークが稼働中の場合は、設定が及ぼす潜在的な影響を十分に理解しておく必要があり ます。

## 背景説明

ポリシーの継承では、アクセスコントロールポリシーをネストできます。子ポリシーは、 Security Intelligence、HTTP Response、Logging SettingsなどのACP設定を含むベースポリシー からルールを継承します。 オプションで、管理者は子ポリシーに対して、Security Intelligence、 HTTP Response、Logging SettingsなどのACP設定を上書きさせるか、子ポリシーで上書きでき ないように設定をロックさせます。この機能は、マルチドメインFMC環境で非常に便利です。

マルチドメイン機能は、FMCの管理対象デバイス、設定、およびイベントへのユーザアクセスを セグメント化します。ユーザは、権限に応じて他のドメインに切り替えたり、他のドメインにア クセスしたりできます。マルチドメイン機能が構成されていない場合、すべての管理対象デバイ ス、構成、およびイベントはグローバルドメインに属しています。

### ポリシー継承の設定

リーフドメインは、それ以上サブドメインを持たないドメインです。子ドメインは、ユーザ/管理 者が現在いるドメインの次レベルの子孫です。親ドメインは、ユーザ/管理者が現在いるドメイン の直接の祖先です。

既存のポリシーの継承を設定または有効にするには、次の手順を実行します。

1. Policy-Aをベースポリシーとし、Policy-Bを子ポリシーとする(Policy-BはPolicy-Aのルール を継承する)

2. EDIT Policy-Bを選択し、図に示すようにInheritance Settingsをクリックします。

Access Control * Access Control	Network Discovery	Application Detectors	Correlation	Actions •				
Policy-B Enter Description							Analyze Hit Counts	Cancel
Prefilter Policy: <u>Default Prefilter Policy</u>		s	St. Policy: <u>None</u>		Edentity Policy: <u>None</u>		🍵 Inheritance Settings   📕 Polic	y Assignments (0)

3.次に示す[Select Base Policy]ドロップダ**ウンリストから**[Policy-A]を選択します。Security Intelligence、HTTP Response、Logging Settingsなどの他のACP設定は、オプションで子ポリシ ーの設定を上書きするために継承できます。 Inheritance Settings

<ul> <li>Child Policy Inheritance Settings</li> <li>For settings selected below, no overrides will be allowed within the child Polinherits 'Policy-B' as Base Policy. Learn More</li> <li>Security Intelligence</li> <li>Http Response</li> <li>Logging Settings</li> </ul>	icy that
<ul> <li>For settings selected below, no overnides will be allowed within the child Pol inherits 'Policy-B' as Base Policy. Learn More</li> <li>Security Intelligence</li> <li>Http Response</li> <li>Logging Settings</li> </ul>	
<ul> <li>Security Intelligence</li> <li>Http Response</li> <li>Logging Settings</li> </ul>	
<ul> <li>Http Response</li> <li>Logging Settings</li> </ul>	100
Logging Settings	
C Advanced	
General Settings	
Identity Policy Settings	-

### 4.対象のターゲットFTDデバイスに対して子ポリシーPolicy-Bのポリシー割り当てを行います。

cy Assignments		2
Fargeted Devices		
Select devices to which you want to apply this policy. Available Devices	Selected Devices	
🔍 Search by name or value	FTD	8
FTD .		
	Add to Policy	
	Impacted Devices	

図に示すように、デフォルト**では、子ポ**リシーのデフォルトアクションが継承され、[基本ポリシーから継承]に設定されます。システム提供のポリシーからデフォルトアクシ**ョンを選択す**るオプ ションもあります(以下を参照)。 [Mandatory]セクションと[Default]セクションの両方に追加されたカテゴリの数に関係なく、トラ フィックのルックアップの順序は常にトップダウン方式で行われます。継承設定を適用した後、 図に示すように、子ポリシーPolicy-B(子ポリシー)のACP表現は、前述のルールチェックの順 序に従って行われます。

Default Action



#### この図は、ベースポリシーであるポリシーAと、ポリシーAから継承された子ポリシーであるポリ シーBの両方のポリシーがFMCでどのように表示されるかを示しています。

Overview Analysis Policies De	ices Objects	AMP Intelligence									Deploy	🔒 System Help 🔻	admin 🔻
Access Control > Access Control	twork Discovery	Application Detectors	Correlation	Actions •									
Policy-A Base Policy											Analyze Hit Co	unts 📄 Save 🚺	Cancel
Prefiter Policy:     SSL Policy:     None     Identity Policy:     None       Rules     Security Intelligence     HTTP Responses     Logging     Advanced								ments (1)					
曲 Filter by Device								Show Rule Confli	cts 😣 🛛 🔾 Add	Category 🛛 😳 Add	Rule Search	Rules	20
Name Source Zon	s Dest Zones	Source Netwo	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLS	ISE/SGT Attri	Action		•
➡ Handatory - 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		Any	Any	🖋 Allow	00.8400	/ 8
▼ Default - Policy-A (2-2)													
2 Site A specific rules Any	Any	2 192.168.10.0/2	2 10.0.43.0/24	Αηγ	Any	Any	Any	📌 TCP (6):8080	Any	Any	🖋 Allow	00.8000	/ 8
Default Action										Access Control: Block	All Traffic		× 1

この図は、Policy-Bで、Policy-Aのルールと、Policy-B自体で設定された特定のルールを確認できることを示しています。順序に留意して、ルールの設定方法に注意する必要があります。

Overview Analysis Poli	icies Devices	Objects A	MP Intelligence									Deploy	🔒 System Help 🔻 adm	nin v
Access Control + Access Con	ntrol Network	Discovery A	Application Detectors	Correlation	Actions •									
Policy-B Inherited Policy												Analyze Hit	Counts 🛛 🔚 Save 🛛 🙆 Car	incel
Prefilter Policy: Default Prefilter	r Policy			SSL Policy: <u>None</u>			Identity	Policy: None				Ta Inheritance	2 Settings   🖳 Policy Assignment	ts (1)
Rules Security Intelligence	e HTTP Respons	ses Logging	Advanced											
B Filter by Device									Show Rule Confi	cts 😣	Add Category	Add Rule Sear	ch 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	lay 2	Any	2 192.168.10.0/2	2 172.16.10.0/2	Any	Αηγ	Any	Any		Any	Any	🖋 Allow	00.8100	4.6
👻 Mandatory - Policy-B (2-2	9													
2 Site B Specific Rule A	lay i	Any	2 192.168.20.0/2	2 10.94.6.0/24	Any	Any	Any	Any	🛫 TCP (6):8080	Any	Any	V Allow	UD.8000 4	0 8
➡ Default - Policy-B (-)														
There are no rules in this section	n. Add Rule or Add Ca	ategory												
▼ Default - Policy-A (3-3)														
3 Site A specific rules A	lay i	Any	2 192.168.10.0/2	2 10.0.43.0/24	Any	Any	Any	Any	🛫 TCP (6):8080	Any	Any	🖋 Allow	0.8100	4.6
Default Action											Inherit from base	e policy (Access Contro	l: Block All Traffic ) 🛛 👻 💲	

## マルチドメインFMC環境でのFTD管理

マルチドメイン機能は、管理対象デバイス、設定、およびイベントへのユーザアクセスをセグメ ント化します。ユーザは、権限に応じて他のドメインに切り替えることができます。マルチドメ イン機能が構成されていない場合、すべての管理対象デバイス、構成、およびイベントはグロー バルドメインに属**して**いま**す**。

最大3レベルのドメインをグローバル・ドメインとして構成できます。すべての管理対象デバイス

は、リーフ・ドメインのみに属している必要があります。これは、 🗔 (サブドメインの追加 )は、図に示すように、リーフドメインでグレー表示されます。

Overview Analysis Policies Devices Object	cts AMP Intelligence					Dep	loy 0, Syste	em Help 🔻 G	lobal \ admin 🔻
		Configuration	Users	Domains	Integration	Updates l	licenses 🔻 Hea	alth  Monito	ring ▼ Tools ▼
					Domain cor	nfiguration is up	to date. 🔚 Sav	ve 🕄 Cancel	Add Domain
Name	Description						Devices		
Global									
L1-Domain-A									
L2-Domain-AA1							1 Device*		
L2-Domain-AA2							1 Device*		

### ドメインの設定

ドメインの設定は、次のように行うことができます。

- 1. [システム(System)] > [ドメイン(Domains)]に移動します。デフォルトでは、グローバルドメ インが存在します。
- 2. 図に示すように[Add Domain]をクリックします。

Overview Analysis Policies Devices Objects AMP Intelligence							Deplo	0 By	vstem Holp v	admin <del>v</del>
		Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
					Domain cor	figuration is (	ep to date.	(	0 A	idd Domain
Name	Description		Dev	lces						
Global			2 De	vices					1	

3. [ドメインの追**加]ダイアログ**ボックスが表示されます。ドメインの名**前を入力**し、ドロップダ ウン・リストから[**親ドメイ**ン]を選択します。これがリーフドメインである場合、図に示すように 、FTDデバイスをドメインに追加する必要があります。

#### Add Domain

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

**注**:ドメインを追加するには、図に示すように[Add Sub Domain]**アイコンを**クリックしま す。ここでは、親ドメインがすでに選択されています。

Name	Description	Devices	
🗆 Global			

## マルチドメインFMC環境におけるポリシーの可視性と制御

ポリシーの可視性と制御は、グローバルドメインの管理者を除き、各ドメインユーザーに**限定さ** れま**す**。この例は、次のような階層に基づいています。



可視性:この図に示すように、デフォルトのビューの[Policies]ペー**ジには、各ドメ**インの下で構成されたポリシー(ACP)がリストされます。

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 Network Analysis Policy	DNS Import/Export
				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"	Q 15 / 6

Control:**各ドメイ**ンに属する管理者ユーザーは、ポリシーを編集できます。他のドメインに属する ポリシー(たとえば、継承の一部)を編集するには、ドメインを現在のドメインから、ポリシー が設定されているドメインに切り替える必要があります。グローバルドメインまたはL1ドメイン に属する管理者ユーザーのみ、ポリシー管理のために下位ドメインを切り替えることができます 。

#### ドメインへのユーザの追加

これは、特定のドメインにユーザを追加する方法を示します。この手順は、ローカルデータベー スのユーザに適用されます。

1. [System] > [Users] に移動します。図に示すように、[Create User]をクリックします。

Overview Analysis Policies Devices Objects | AMP In Users User Roles External Authentication

2. [ユーザー構成**]ダイアログボ**ックスが表示されます。ユーザー名とパ**スワード**を入力**します** (&パスワードの確認)。 図に示すように、[Add Domain]をクリックして、指定したドメインに ユーザを追加します。

User Name	L1-8-admin	
Authentication	Use External Authentication Method	
Password		
Confirm Password		
Maximum Number of Failed Logins	0	(0 = Unlimited)
Minimum 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	
	Save Cancel	

3.ユーザを追加する[ドメイン(Domain)] ドロップダウンリストから目的のドメインを選択し、図 に示すようにロールを指定します。新しいユーザを自分のドメインまたは子ドメインに追加でき ます。

## User Role Configuration

Domain	Global		-		
	Global		tor		
	Global \ L1-Domain-A		atabase User		
	Global \ L1-Domain-A \ l	halyst			
Global \ L1-Domain-A \ L2-Domai			halyst (Read Only)		
	Global \ L1-Domain-B		pprover Idmin		
Default U	ser Roles	Access A	.dmin		
		🗸 Network	Admin		
		🗸 Maintena	nce User		
		Discovery	y Admin		
		Threat Ir	itelligence Director (TID)		
		User			
			Save Cancel		

### 設定されたユーザを次の図に示します。

Overview Analysis Polic	ies Devices Objects AMP Intelligence				Deploy 🔒	System H	elp 🔻 Globa	∖admin ▼
		Configuration	Users Domains	Integration Updat	es Licenses 🔻	Health 🔻	Monitoring •	Tools <b>v</b>
Users User Roles	External Authentication							
							0	Create User
Username	Domains	Roles	Authentication Method	1	Password Lifetime			
admin	Global	Administrator	Internal		Unlimited			0
L1-A-admin	Global \ L1-Domain-A	Administrator	Internal		Inlimited			/ 8
L1-B-admin	Global	Administrator	Internal		Unlimited			/ 1
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

FMCでのリソースアクセスは、ユーザが属するドメインに制限されます。次に示すように、ユー ザL1-A-adminがFMC UIにログインすると、アクセスはユーザが属するドメインL1-Domain-Aに制 限され、ユーザがその子ドメインに切り替わると子ドメインに制限されます。このユーザーは、 L1-Domain-Aドメインで定義されたポリシーと、ドメインが子ドメインに切り替えられたときに 子ドメインで定義されたポリシーのみを編集できます。また、次の例から、L1-A-Policyがグロー バルドメインで定義されたポリシーBase-Policyを継承して、Base-Policyを編集できます 🖉 署 名図に示すように、継承設定はBase-Policyを指定するように行われます。

Overview Analysis Policies	Devices Objects A	MP				Deploy 0 System H	elp 🔻 L1-Domain-A \ L1-A-admin 🔻
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions •			
						Object Management Intrusion Net	work Analysis Policy DNS Import/Export
							New Policy
Access Control Policy		De	main		Status	Last Madilied	
Base-Policy		Gio	bal		Targeting 0 devices	2020-05-28 22:49:49 Modified by "admin"	<b>BES</b>
L1-A-Policy		Glo	bal\L1-Domain-i	4	Targeting 0 devices	2020-05-28 23:02:14 Modified by "admin"	QE26

同様に、L2-Domain-AA1ドメインに属するユーザL2-AA-adminは、図に示すように、ドメインで 定義されたポリシーL2-AA-Policyの制御のみを持ちます。L2-AAポリシーは、L1-Domain-Aで定義 されたポリシーL1-A-Policyを継承して、次にグローバルドメインで定義されたBase-Policyを継承

?

します。また、ポリシーL2-AA-Policyを編集して、 ✓署名ユーザL2-AA-adminは、その親ドメインであるL1-Domain-Aまたは祖先ドメインであるグローバルドメインに切り替えることはできません。

Overview Analysis Policies	Devices Objects	AMP		(	Deploy	0, System Help ▼	L1-Domain-A \ L2-Domain-AA	1 \ L2-AA-admin ▼
Access Control  Access Control	Network Discovery	Application Detectors Correlation	Actions 🔻					
						Object 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*	Pa 🖪 🔍 🖯
⊟ L1-A-Policy		Global \ L1-Domain-A		Targeting 0 devices		2020-06-17 Modified by "a	13:48:54 idmin*	Pa 🖪 🔍 🖯
L2-AA-Policy		Global \ L1-Domain-A \ L2-Domain-A	A1	Targeting 1 devices Up-to-date on all targeted de	levices	2020-06-17 : Modified by "e	13:48:54 idmin*	Pa 🖸 🥒 🖯

また、L1-Domain-Aに属するユーザL1-A-adminは、L2-Domain-AA1に切り替え、L2-AA-Policyを



Overview Analys	s Policies	Devices Obj	jects AMP					(	Deploy 🧕 🧕	System He	lp ▼ L1-Dom	ain-A \ L2-	Domain-AA1 \ L2-AA	-admin <del>v</del>
Access Control • Ac	cess Control	Network Disc	covery Appl	ication Detecto	rs Correlati	on Actions	•							
L2-AA-Policy											ĺ	Analyze Hit C	ounts 🔚 Save 🚺	Cancel
Prefilter Policy: L1-A-P	refilter			SSL Policy: Non	12			Identity Pol	licy: None					
											Te Co	Inheritance :	Gettings   🧾 Policy Assign	ments (1)
Rules Security In	itelligence H	TTP Responses	Logging	Advanced										
B Filter by Device								🖾 Show Rul	e Conflicts 😣	Add Categor	ny 🔹 💿 Add Ri	ule Search P	ules	×
Name #	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT A	Action	• •	
👻 Mandatory - Base	-Policy (1-1)													
1 Rule1	Any	Any	Any	Απγ	Any	Any	Any	Any	☆ TCP (6): 445☆ TCP (6): 8080	Any	Any	🗙 Block	UD.210	۹.0
👻 Mandatory - L1-A	-Policy (2-2)													
2 SiteA->SiteB	Any	Any	2 192.168.10	2 172.16.10.0	Any	Any	Any	Any	Any	Any	Any	🛹 Allow	002100	۹.
👻 Mandatory - L2-A	A-Policy (3-3)													
3 SiteB-specific	Any	Any	2 172.16.10.0	2 172.16.20.0	Αηγ	Any	Any	Any	Any	Any	Any	🛹 Allow	00.840.0	2 🛙
👻 Default - L2-AA-P	olicy (-)													
There are no rules in th	his section. Add R	ule or Add Catego	pry											
Default - L1-A-Po	licy (-)													
Default - Base-Po										_				
Default Action										Inherit from b	ase policy (Acces:	s Control: Blo	k All Traffic )	<b>\$</b>

重要な注意点:

•非大域ドメインを削除すると、ドメインに属するユーザーは自動的にグローバルドメインに 移動されます。

FTD/sは常にリーフドメインで定義されます。この場合、リーフドメインはL2-Domain(L2-Domain-AAおよびL2-Domain-BB)です。L2ドメインに属するFTDは、L1ドメイン内または グローバルドメイン内のポリシーに割り当てることができます。この図では、グローバルド メイン内のACPは、L3ドメイン内で定義されたFTDをグローバルドメイン内で定義されたポ リシーに割り当てています。

Overview Analysis Policies Devices Access Control + Access Control Base-Policy	Objects AMP Intelligence iscovery Application Detectors Correlation Actions	•		Der	ploy 🛛 🍕 System	m Help ¥ Global \ admin ¥
Prefilter Policy: <u>base-Prefiter</u>	sst. Policy: Same Policy Assignments		Identity Policy: <u>Name</u>	? ×	The Interitance Se	ettings I 🖉 Policy Assignments (0)
Arme Source Zones Dest Zone     Mandatory - Base -Policy (1-1)     Rule1	Select devices to which you want to apply this policy. Available Devices Cobal Cobal L1-Domain-A Ca-Domain-A Ca-Domain-A L2-Domain-B L2-Domain-B Ca-Domain-B Ca-Domain-B Ca-Domain-B Ca-Domain-B	Add to Policy	Selected Devices Global L2-Domain-B Lafb_TD Impacted Devices LeafA_FTD ( L2-AA-Policy )	5	dg pule Search Rul Action X Block All Traffic	
			CK.	Cancel		

グローバルドメイン内のユーザは他のユーザ固有のドメインに移動できますが、特定のドメイン内のユーザは、自分のドメインとその子ドメイン内でのみ可視性を持ちます。次の表に示すように、グローバルドメインまたはその他の上位ドメインに移動することはできません。

グローバルドメイン

グローバルドメインのユーザは、設定されているすべ てのドメインを表示でき、他のドメインに移動できま す。

ユーザ固有のドメイン L1-Domain-Aのユーザーは、L2-Domain-AAという 分自身とその子ドメインにのみ表示され、L2-Do AAに移動できます。上位レベルのドメイン(グロ ルなど)アクセスは許可されません。



•子ポリシーのデフォルトアクションは親ポリシーによってロックできず、この図に示す ように、ユーザは親ポリシーのデフォルトアクションを継承する必要はありません。

L2	-AA2-Polic	у										(	Analyze Hit C	counts 🔚 Save 😫	Cancel
Pref	ilter Policy: L1-A-P	refilter		SSI.	Policy: None			Ide	stity Policy: <u>None</u>	1			Inheritance	Settings   🖳 Policy Assignm	ients (1)
Ri	Iles Security In	teligence HTTP	Responses	Logging Advance	d				Char	u Dela Canflinta 🔒	0.	fd Catagony	Saarch I	2 dar	~
	Name	Source Zones	Dest Zones	Source Net	Dest Netwo	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Att	Action		0
-	Mandatory - Base	Policy (1-1)												U (0 )4 % U V	
1	Rule1	Any	Any	Any	Any	Any	Any	Any	Any	🛫 TCP (6):445 🛫 TCP (6):8080	Any	Any	× Block	00.840.	۹.8
-	Mandatory - L1-A	-Policy (2-2)													
2	SiteA->SiteB	Any	Any	192.168.10.0,	2 172.16.10.0/2	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	0 🗅 🖉 🖄 🖉 0	۹.
-	Mandatory - L2-A	A2-Policy (-)													
Th	ere are no rules in t	this section. Add Ruk	e or Add Category	r -											
-	Default - L2-AA2-	Policy (-)													
Th	ere are no rules in t	this section. Add Ruk	e or Add Category	r i i i i i i i i i i i i i i i i i i i											
-	Default - L1-A-Po	ilicy (-)													
Th	ere are no rules in t	this section.													
-	Default - Base-Po	alicy (-)													
7h	ere are no rules in t	this section.									_				_
De	fault Action											Access Control: Block All T	raffic		× 1

この図では、デフォルトのアクションが親のデフォルトのアクションとして割り当てら れていない場合が分かりま**す。「Inherit from base policy: not be seen in default action」** という単語から分かります。

注:ユーザがL1/L2ドメインポリシーを同時に表示できないことに注意してください。ポリ シーを表示および編集するには、ユーザーが目的のドメインに切り替える必要があります。 例:グローバルドメインに存在するユーザadminが、L1-Domain-AおよびL2-Domain-AAで 設定されているポリシーを表示および編集するには、L1-A-Domainに切り替え、対応するポ リシーを表示および編集します。また、L1-Domain-Aのユーザはグローバルドメインで定義 されたポリシーを編集または削除できません。つまり、L1-A-Policyの親ポリシーである Base Policy、L2-Domain-AAのユーザは、それぞれグローバルおよびL2-Domain-Aドメイン ドメインで定義のポリシーをを編集または削除できません。

### 使用例

図に示すシナリオでは、SITE-A(SiteA-FTD)のFTDとSITE-B(SiteB-FTD)が、異なるドメイン(マ ルチドメイン)を介して1つのFMCで管理され、制御されたアクセスを提供します。ポリシーの 観点からは、組織レベルでのポリシーに関する考慮事項を次に示します。

- SITEまたはDOMAINに属さない(ベースポリシー)すべてのFTDに適用されるサービス固有のBLOCKルール。
- ・サイトAからサイトBへのアクセス(L1-Policy-A)およびサイトBからサイトAへのアクセス(L1-Policy-B)を満たす要件を満たすルール。
- Site-B FTD(L2-Policy-B)に適用されるルール。



### マルチドメイン環境での継承

上記の使用例では、次のドメイン/ポリシー階層を考慮してください。SiteA-FTDおよびSiteB-FTDは、リーフドメインL1-Domain-AおよびL2-Domain-Bの一部です。



ドメイン階層の構造は次のとおりです。

- ・グローバルドメインはL1-Domain-AおよびL1-Domain-Bの親です。
- ・グローバル・ドメインはL2-Domain-Bの祖先です。
- ・L2-Domain-BはL1-Domain-Bの子
- L2-Domain-Bは子ドメインがないため、リーフドメインです。

図は、FMCから見たドメイン階層を示しています。

Overview Analysis Policies Devices Object	s AMP Intelligence		Deploy 🔮 System Help 🔻 Global \ admin 🔻
	Config	ration Users Domains Integration Updates	Licenses • Health • Monitoring • Tools •
		Domain configuration	n is up to date. 📔 Save 😢 Cancel 🙆 Add Domain
Name	Description		Devices
🗆 Global			
L1-Domain-A			1 Device"
🗄 L1-Domain-B			
L2-Domain-B			1 Device"

#### 次のスナップショットは、ルールが上記のシナリオに対してL1-Policy-AおよびL2-Policy-B w.r.tで どのように定義されるかを示しています。

Overview Analys	tis Policies	Devices Obje	cts AMP	on Detectors	Correlation	Actions V					Deploy 🖣	System He	slp ¥ L1-Domain-A \	admin 🔻
L1-Policy-A					contractor	Piccono -					(	Analyze Hit I	Counts Save	Cancel
Desfiltes Dellers Defeu	h Deefline Deller			Delley Need				dentile Dellers III						
Prehiter Policy: Defau	It Prefiter Policy		55	L Policy: None			1	dentity Policy: N	008				_	
											Te 1	Inheritance Se	ettings   🧾 Policy Assignm	ients (1)
Rules Security Ir	ntelligence HTT	TP Responses L	ogging Advan	iced										
Filter by Device								Show F	tule Conflicts 😣	Add Cate	gory 🕓 Add Rule	Search Ru	les	×
# Name	Source Zones	Dest Zones	Source Net	Dest Netwo	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT At A	Action	• • • • •	۲
	e Policy (1-1)													
1 Rule 1	Any	Any	Any	Any	Any	Any	Any	Any	TCP (6):445 TCP (6):8080	Any	Any	X Block	00210	۵.
👻 Mandatory - L1-P	Policy-A (2-2)													
2 Site A -> Site B	di INSIDE	A OUTSIDE	2 192.168.10.0	2 172.16.10.0/	: Any	Any	Any	Any	Any	Any	Any	Allow	00.8000	1 3
🔻 Default - L1-Polic	cy-A (-)													
There are no rules in t	his section. Add Rul	e or Add Category												
👻 Default - Base Po	olicy (-)													
There are no rules in t	his section.													
Default Action										Inherit from	n base policy (Access (	Control: Block	All Traffic )	\$ 📑
Overview Analy:	sis Policies	Devices Obje	ects AMP							Deploy (	System Help 🔻	L1-Dom	ain-B\L2-Domain-B	\ admin *
														/ aanna .
Access Control + A	Access Control	Network Disco	very Applicat	tion Detectors	Correlation	Actions •					1			( ddmin v
Access Control > A	Access Control	Network Disco	very Applicat	tion Detectors	Correlation	Actions <b>v</b>					3 -7	Analyze Hit	Counts Gauge	Cancel
Access Control • A L2-Policy-B	Access Control	Network Disco	very Applicat	tion Detectors	Correlation	Actions •					3	Analyze Hit	Counts	S Cancel
Access Control • A L2-Policy-B	Access Control	Network Disco	very Applicat	tion Detectors	Correlation	Actions <b>v</b>					3	Analyze Hit	Counts	Cancel
Access Control > A L2-Policy-B	Access Control	Network Disco	very Applicat	tion Detectors	Correlation	Actions •		Identity Policy:	None		3	Analyze Hit	Counts Save	2 Cancel
Access Control > A L2-Policy-B Prefilter Policy: <u>Defau</u>	Access Control	Network Disco	very Applicat	tion Detectors	Correlation	Actions •		Identity Policy:	None			Analyze Hit	e Settings   📕 Policy Assis	Cancel
Access Control > A L2-Policy-B Prefilter Policy: Defau Rules Security I	Access Control	Network Discor	very Applicat se Logging Advan	tion Detectors	Correlation	Actions •		Identity Policy: ]	None		3	Analyze Hit	e Settings   📕 Policy Assi	Cancel
Access Control + A L2-Policy-B Prefilter Policy: <u>Defau</u> Rules Security I # Filter by Device	Intelligence HT	Network Disco	very Applicat St	st. Policy: <u>None</u>	Correlation	Actions •		Identity Policy:   Sho	Nane w Rule Conflicts 🔮	Add 🕥	a Category 💽 Add I	Analyze Hit	Counts	Cancel gnments (1)
Access Control + A L2-Policy-B Prefilter Policy: <u>Defay</u> Rules <u>Security I</u> Britar by Device Name	at Prefilter Policy Intelligence HT Source Zones	Network Disco TP Responses Dest Zones	very Applicat St Logging Advan Source Net	SL Policy: None	Correlation VLAN Tags	Actions ¥	Applications	Identity Policy:   Sho Source Ports	None Weile Conflicts	Add ( URLs	Category O Add I ISE/SGT At	Analyze Hit Inheritanc Rule Search Action	Counts	Cancel gnments (1)
Access Control + A L2-Policy-B Prefilter Policy: Defau Rules Security I Pitter by Device	Access Control	Network Disco TP Responses Dest Zones	Very Applicat St Logging Advan	ion Detectors St. Policy: <u>None</u> nced Dest Netwo	Correlation VLAN Tags	Actions ¥	Applications	Identity Policy:   Sho Source Ports	None www.Rule.Conflicts	Add O URLs	Category 💽 Add I	Analyze Hit	Counts Save ( e Settings   Policy Assis h Rules	Cancel gnments (1)
Access Control + A L2-Policy-B Prefilter Policy: <u>Defau</u> Rules <u>Security 1</u> Rules <u>Security 1</u> Rules <u>Name</u> Mandatory - Bas	Access Control alt Prefilter Policy intelligence HT Source Zones e Policy (1-1)	Network Disco TP Responses Dest Zones	Very Applicat St Logging Advast Source Net	tion Detectors	Correlation	Actions ¥	Applications	Identity Policy:   Show the second se	None w Rule Conflicts & Dest Ports	Add ( URLs	Category O Add	Analyze Hit Inheritanc Rule Search Action	e Settings I 💽 Policy Assist In Rules	Cancel gnments (1)
Access Control + A L2-Policy-B Prefilter Policy: Defau Rules Security I Filter by Device Name Mandatory: Bass 1 Rule 1	Access Control alt Prefilter Policy Intelligence HT Source Zones e Policy (1=1) Any	Network Disco TP Responses Dest Zones	Very Applicat St Logging Advas Source Net Any	SL Policy: Nane nced Dest Netwo Any	Correlation VLAN Tags Any	Actions V	Applications	Identity Policy:   Sho Source Ports Any	None We Rule Conflicts & Dest Ports * TCP (6):44	9 <b>3</b> Add ( URLs	Category O Add I ISE/SGT AL Any	Analyze Hit Inheritanc Rule Searcl Action	Counts	Cancel gnments (1)
Access Control + A L2-Policy-B Prefilter Policy: <u>Defau</u> Rules <u>Security I</u> # Filter by Device Name Mandatory - Bas 1 Rule 1 V Mandatory - L1-	Access Control alt Prefilter Policy Intelligence HT Source Zones e Policy (1-1) Any B-Policy (2-2)	Network Disco TP Responses Dest Zones	Very Applicat St Logging Advan Source Net Any	SL Policy: None nced Dest Netwo Any	Correlation VLAN Tegs Any	Actions V	Applications Any	Identity Policy: Sho Source Ports	None W Rule Conflicts & Dest Ports TCP (6):44 TCP (6):80	add ( URLs 5 80 Any	Category Q Add I ISE/SGT At Any	Analyze Hit Inheritanc Rule Searcl Action	Counts	Cancel gnments (1) X
Access Control + A L2-Policy-B Prefilter Policy: Defau Rules Security I Filter by Device Wandatory - Bas 1 Rule 1 Wandatory - L1- 2 Site B-SiteA	Access Control alt Prefilter Policy intelligence HT Source Zones re Policy (1=1) Any B: Policy (2=2) Any	Network Disco TP Responses Dest Zones Any Any	Very Applicat St Logging Advar Source Net Any 22172.16.10.5	SL Policy: None nced Dest Netwo Any 22 192.168.10	Correlation VLAN Tags Any .0 Any	Actions V Users Any Any	Applications Any Any	Identity Policy:   Shu Source Ports Any Any	Wone w Rule Conflicts & Dest Ports		Category O Add I ISE/SGT At Any Any	Analyze Hit Inheritanc Rule Searcl Action X Block	Counts	Cancel     gnments (1)     X     0     0     0     0
Access Control + A L2-Policy-B Prefilter Policy: Defas Rules Security I # Filter by Device Wandatory - Bas 1 Rule 1 Wandatory - L1= 2 Site B->SiteA Wandatory - L2=	Access Control dt Prefilter Policy Intelligence HT Source Zones e Policy (1-1) Any B-Policy (2-2) Any Policy B (3-3)	Network Disco TP Responses	Very Applicat St Logging Advast Source Net Any 2021 172.16.10.5	SL Policy: None need Dest Netwo Any 2021192.166.10	Correlation VLAN Tags Any .0 Any	Actions   Action	Applications Any Any	Identity Policy: ; Shu Source Ports Any Any	None We Rule Conflicts & Dest Ports TCP (6):44 * TCP (6):44	Add α     URLs     So Any     Any	Add I ISE/SCT At Any Any	Analyze Hit Inheritanc Rule Searcl Action X Block	Counts	Cancel gnments (1) X 0 4 8 0 4 8
Access Control + A L2-Policy-B Prefilter Policy: Defau Rules Security I Fitter by Device Name Mandatory - Bass 1 Rule 1 V Mandatory - L1: 2 Site 8->SiteA V Mandatory - L2: 3 Site 8 access on	Access Control dt Prefilter Policy Intelligence HT Source Zones e Policy (1-1) Any B-Policy (2-2) Any Any My Any Supplicy-B (3-3) Ny AISTOE	Network Disco TP Responses	Very Applicat St Logging Advant Source Net Any 2021 172.16.10.5	SL Policy: Nane nced Dest Netwo Any 2 192.166.10	Correlation VLAN Tags Any .0 Any .0 Any	Actions   Action	Applications Any Any Any	Identity Policy: Shu Source Ports Any Any Any	None We Rule Conflicts Dest Ports TCP (6):44 Any	Add α     URLs     S     Any     Any     Any	Add ISE/SGT At Any Any Any	Analyze Hit Inheritanc Rule Searci Action X Block V Allow	Counts	Cancel gnments (1) X
Access Control + A L2-Policy-B Prefilter Policy: Defau Rules Security I Fitter by Device Mandatory - Bass 1 Rule 1 V Mandatory - L1- 2 Site B ->SiteA V Mandatory - L2- 3 Site B ->SiteA	Access Control	Network Disco TP Responses Dest Zones Any Any ah DMZ	Very Applicat St Logging Advant Source Net Any 172.16.10.5	SL Policy: Nane nced Dest Netwo Any 2012102108.100 2012108.100 2012108.200	Correlation VLAN Tags Any .0 Any .0 Any	Actions ▼ Users Any Any Any	Applications Any Any Any	Identity Policy:   Source Ports Any Any Any Any	None WRUE Conflicts Dest Ports PTCP (6):44 Any	5 Add 0 URLs 50 Any 3 Any Any	Add ISE/SGT At Any Any Any	Analyze Hit Inheritanc Rule Search Action Search Action	Counts	Cancel gnments (1) X
Access Control + A L2-Policy-B Prefilter Policy: Defau Rules Security I Filter by Device Manae Mandatory - L1- Site Bacceso Mandatory - L1- Site Bacceso Site Bacceso Default - L2-Site	Access Control alt Prefilter Policy Intelligence HT Source Zones e Policy (1-1) Any B-Policy (2-2) Any Policy-B (3-3) Policy -B (3-3) Policy -	Network Disco TP Responses Dest Zones Any Any da DMZ	Very Applicat St Logging Advant Source Net Any 22172.16.10.5 Any	SI. Policy: Nane nced Dest Netwo Any 22 192.168.10	Correlation       VLAN Tags       Any       .0     Any       .0     Any	Actions ▼ Users Any Any Any Any	Applications Any Any Any	Identity Policy:   Source Ports Any Any Any	None Welle Conflicts	Add α     Add α     Add α     Add α     Add α	Category Add ISE/SGT At Any Any Any Any	Analyze Hit Inheritanc Rule Search Action X Block V Allow	Counts	Cancel gnments (1) X 0 4 5 0 4 5
Access Control + A L2-Policy-B Prefilter Policy: <u>Defau</u> Rules <u>Security I</u> Filter by Device Wandatory - Bas Mandatory - L1- Site B-SSiteA Mandatory - L2- Site B-SSiteA Mandatory - L2- Site B access on Default - L2-Poli There are no rules in 1 W Default - L1-B-P	Access Control alt Prefilter Policy Intelligence HT Source Zones e Policy (1-1) Any B-Policy (2-2) Any Policy-B (3-3) ny & It/SIDE icy-B (3) this section. Add Ro Bigr (1)	Network Disco TP Responses Dest Zones Any Any ab DMZ de or Add Category	Very Applicat St Logging Advan Source Net Any 172.16.10.5	SL Policy: Nane nced Dest Netwo Any 2012102100	Correlation           VLAN Tags           Any           .0         Any           .0         Any	Actions ▼ Users Any Any Any	Applications Any Any Any	Identity Policy:   Sho Any Any Any	None WRule Conflicts Dest Ports TCP (6):44 PTCP (6):44 Any	<ul> <li>Add α</li> <li>URLs</li> <li>δ<sub>0</sub> Aαγ</li> <li>3 Aαγ</li> </ul>	Add I ISE/SGT AL Any Any Any	Analyze Hit Inheritanc Rule Search Action Block Allow	Counts	Cancel genments (1) X 0 Q Q 0 Q Q 0 Q Q 0 Q Q 0 Q
Access Control + A L2-Policy-B Prefilter Policy: Dafau Rules Security I Fitter by Davice Wandatory - Bas Mandatory - Bas Name Mandatory - L1- Site B - SiteA Mandatory - L2- Site B - SiteA Mandatory - L2- Mandatory - L2-	Access Control alt Prefilter Policy intelligence HTT Source Zones a Policy (1=1) Any Policy (2=2) Any Policy-B (3=3) htyB HSIDE icy-B (3=3) this section. Add Rue olicy (-) this section.	Network Disco       TP Responses       Image: Dest Zones       Any       Any       Any       Image: Dest Zones       Image: Des	Very Applicat St Logging Advan Source Net Any 172.16.10.5	SL Policy: None	Correlation VLAN Tags Any Any Any Any Any	Actions ▼ Users Any Any Any	Applications Any Any Any	Identity Policy:   Shu Source Ports Any Any Any Any	None W Rule Conflicts & Dest Ports TCP (6):44 # TCP (6):44 Any	<ul> <li>Add d</li> <li>URLs</li> <li>San Any</li> <li>Any</li> </ul>	Add I ISE/SCT At Any Any Any	Analyze Hil Inheritanc Rule Search Action X Block Allow	Counts	Cancel gnments (1) X 0 4 3 0 4 3 0 4 3 0 4 3
Access Control + A L2-Policy-B Prefilter Policy: Defait Rules Security I Fitter by Device Wandatory - Bass 1 Rule 1 Wandatory - L1-2 2 Site B->SiteA Wandatory - L2-1 3 Site B->SiteA Wandatory - L2-1 3 Site B access on Default - L2-Poli There are no rules in I There are no rules in I There are no rules in I	Access Control	Network Disco TP Responses	very Applicat St Logging Advan Source Net Any 172.16.10.5	SL Policy: Name need Dest Netwo Any 22192.168.20	Correlation VLAN Tags Any Any Any Any	Actions ▼ Users Any Any Any	Applications Any Any Any	Identity Policy:   Shurce Ports	None We Rule Conflicts Dest Ports TCP (6):44 Any	Add α     URLs     S     Any     Any     Any	Add ISE/SGT At Any Any Any	Analyze Hit Inheritanc Rule Searci Action X Block Allow	Counts	Cancel gnments (1) X
Access Control + A L2-Policy-B Prefilter Policy: <u>Defait</u> Rules Security I Fitter by Device Mandatory = Bass Mandatory = Li-S Site B->SiteA Mandatory = L2-4 Site B->SiteA Mandatory = L2-4 Site B->SiteA Mandatory = L2-4 Site B->SiteA Mandatory = L2-4 Mandatory = L2-4	Access Control	Network Disco TP Responses	Very Applicat St Logging Advant Source Net Any 2002 172.16.10.5	SL Policy: Nane nced Dest Netwo Any 2 192.166.20	Correlation VLAN Tags Any .0 Any .0 Any	Actions ▼ Users Any Any Any Any	Applications Any Any Any	Identity Policy:   Source Ports	None W Rule Conflicts Dest Ports PTCP (6):44 Any	<ul> <li>Add d</li> <li>URLs</li> <li>URLs</li> <li>Any</li> <li>Any</li> <li>Any</li> </ul>	Add ISE/SGT At Any Any Any	Analyze Hit Inheritanc Rule Search Action Selock Allow	Counts	Cancel gnments (1) × 0 4 3 0 4 3 0 2 5

正規のトラフィックをブロックしたり、不要なトラフィックを許可したりしないように複数のド メインを設定する場合は、必ずルールとその継承を考慮する必要があります。