

Héritage dans un environnement multidomaine dans FTD

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configurer l'héritage des stratégies](#)

[Gestion FTD dans un environnement FMC multidomaine](#)

[Configuration du domaine](#)

[Visibilité et contrôle des politiques dans un environnement FMC multidomaine](#)

[Ajouter des utilisateurs au domaine](#)

[Scénario d'utilisation](#)

[Héritage dans un environnement multidomaine](#)

Introduction

Ce document décrit la configuration et le fonctionnement des fonctions d'héritage et de multidomaine. Cette section porte également sur un cas d'utilisation réel pour voir comment ces deux fonctionnalités fonctionnent ensemble.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Firepower Management Center (FMC) version 6.4
- Logiciel Firepower Threat Defense (FTD) version 6.4

Note: La prise en charge des fonctionnalités multidomaine et héritage est disponible sur FMC/FTD à partir de la version 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 votre réseau

est actif, assurez-vous de bien comprendre l'impact potentiel de toute configuration.

Informations générales

Dans l'héritage de stratégie, les stratégies de contrôle d'accès peuvent être imbriquées dans lesquelles la stratégie enfant hérite des règles d'une stratégie de base, y compris les paramètres ACP tels que Security Intelligence, HTTP Response, Logging Settings, etc. L'administrateur peut éventuellement autoriser la stratégie enfant à remplacer les paramètres ACP tels que Security Intelligence, HTTP Response, Logging Settings ou à verrouiller les paramètres de sorte que la stratégie enfant ne puisse pas les remplacer. Cette fonctionnalité est très utile dans un environnement FMC multidomaine.

La fonctionnalité multidomaine segmente l'accès utilisateur aux périphériques, configurations et événements gérés de FMC. Un utilisateur peut passer à d'autres domaines ou y accéder en fonction des privilèges. Si la fonctionnalité multidomaine n'est pas configurée, tous les périphériques, configurations et événements gérés appartiennent au domaine **global**.

Configurer l'héritage des stratégies

Un domaine leaf est un domaine qui ne comporte pas d'autres sous-domaines. Un domaine enfant est le descendant de niveau suivant du domaine où se trouve actuellement l'utilisateur/l'administrateur. Le domaine parent est l'ancêtre direct du domaine où se trouve actuellement l'utilisateur/l'administrateur.

Pour configurer/activer l'héritage pour les stratégies existantes :

1. Laisser la politique A être la politique de base et la politique B être la politique enfant (la politique B hérite de la règle de la politique A)
2. **MODIFIEZ** la stratégie B et cliquez sur **Paramètres d'héritage** comme indiqué dans l'image.



3. Choisissez Policy-A dans la liste déroulante **Select Base Policy** présentée ci-dessous. D'autres paramètres ACP, tels que Security Intelligence, HTTP Response, Logging Settings, etc., peuvent être hérités pour remplacer les paramètres de la stratégie enfant (facultatif).

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. Effectuez l'**affectation de stratégie** pour la stratégie enfant Policy-B par rapport au périphérique FTD cible prévu :

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

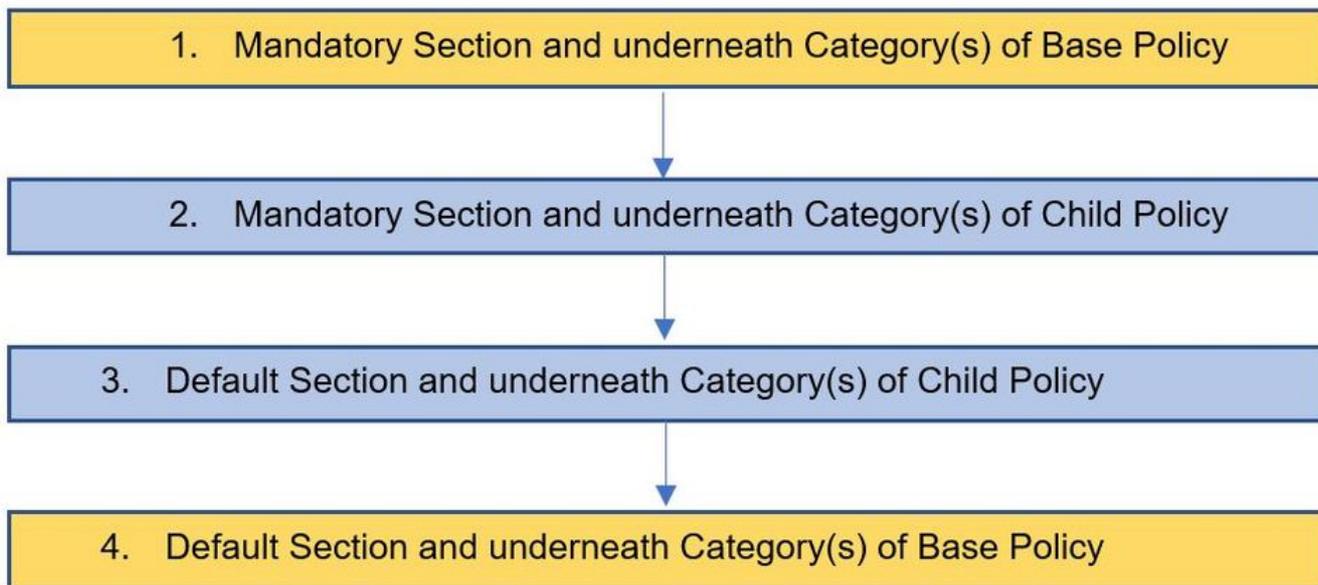
Impacted Devices

OK Cancel

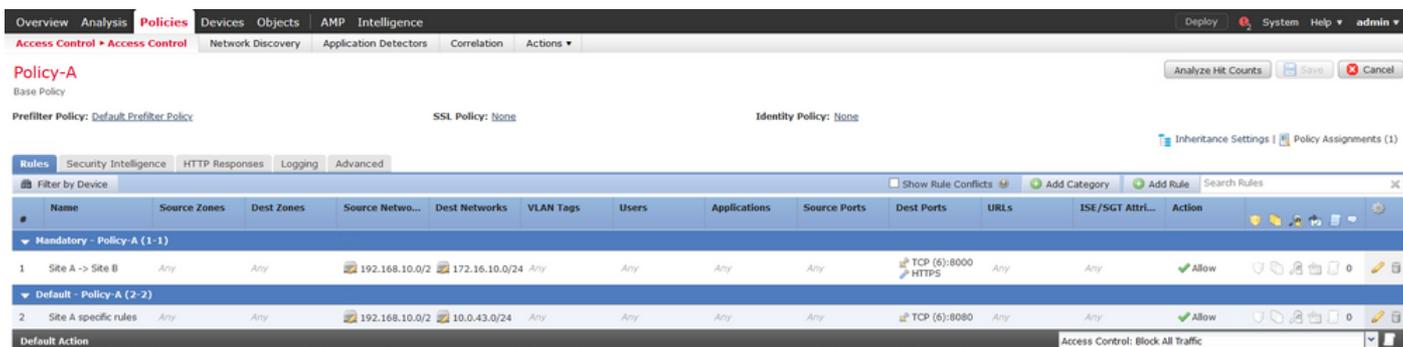
Par défaut, l'**action par défaut** de la stratégie enfant est héritée et définie sur **Hériter de la stratégie de base** comme illustré dans l'image. L'utilisateur a également la possibilité de sélectionner l'**action par défaut** dans les stratégies fournies par le système comme indiqué ici.



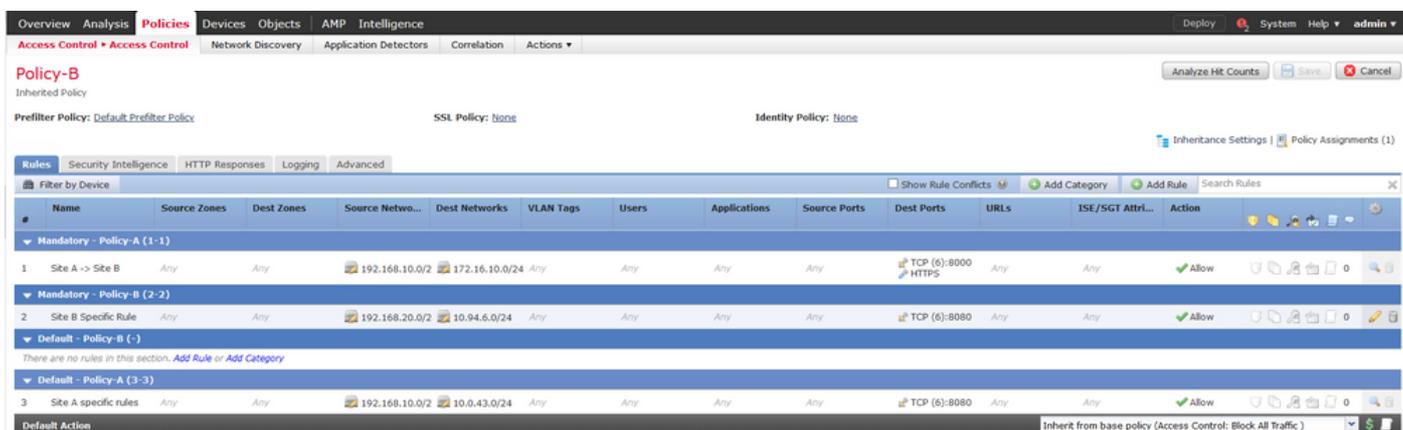
L'ordre de recherche du trafic sera toujours descendant, quel que soit le nombre de catégories ajoutées dans les sections Obligatoire et Par défaut. Après avoir appliqué les **paramètres d'héritage**, la représentation ACP pour la stratégie enfant B (Stratégie enfant) comme indiqué dans l'image, conformément à la **vérification de l'ordre des règles** mentionnée précédemment :



Cette image montre comment les deux politiques, à savoir la politique A qui est la politique de base et la politique B qui est la politique enfant et qui est héritée de la politique A, seraient affichées dans le FMC.



Cette image montre que dans Policy-B, les règles de Policy-A peuvent être vues ainsi que des règles spécifiques configurées dans Policy-B. Il convient de prendre soin de la façon dont les règles doivent être configurées en gardant à l'esprit l'ordre.



Gestion FTD dans un environnement FMC multidomaine

La fonctionnalité multidomaine segmente l'accès utilisateur aux périphériques, configurations et événements gérés. Un utilisateur peut passer à d'autres domaines en fonction des privilèges. Si la fonctionnalité multidomaine n'est pas configurée, tous les périphériques, configurations et événements gérés appartiennent au domaine **global**.

Un maximum de domaines à trois niveaux peut être configuré avec le domaine global comme niveau 1. Tous les périphériques gérés doivent appartenir au domaine Leaf uniquement. Ceci peut être confirmé à partir du symbole de  (Ajouter un sous-domaine) grisé dans le domaine feuille comme illustré dans l'image.



Configuration du domaine

La configuration du domaine peut être effectuée comme suit :

1. Accédez à **System > Domains**. Par défaut, le domaine **global** est présent.
2. Cliquez sur **Ajouter un domaine** comme indiqué dans l'image.



3. La boîte de dialogue **Ajouter un domaine** apparaît. Tapez le **nom** du domaine et sélectionnez le **domaine parent** dans la liste déroulante. S'il s'agit du domaine Leaf, le ou les périphériques FTD doivent être ajoutés au domaine comme l'indique l'image.

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

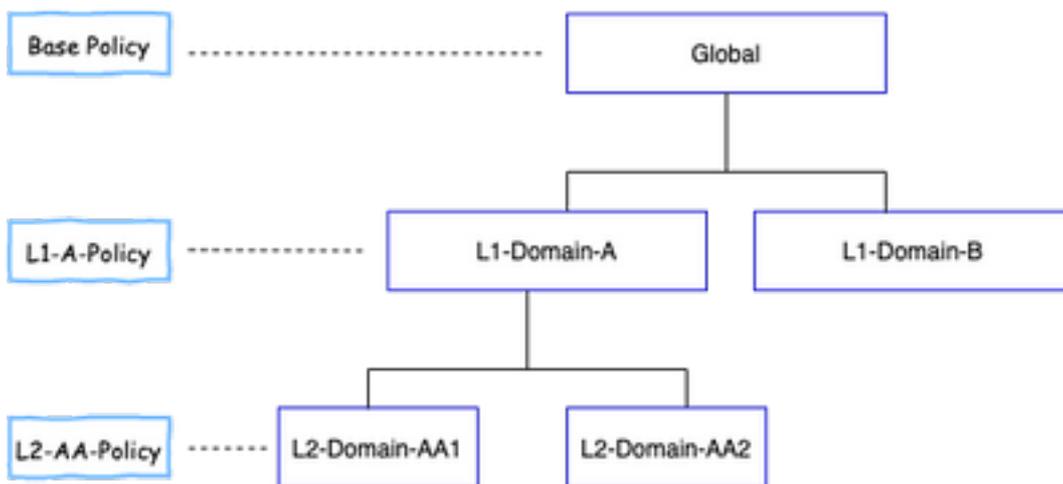
- Global
 - LeafA FTD

Note: Pour ajouter les domaines, cliquez sur l'icône **Ajouter un sous-domaine** comme indiqué dans l'image. Le domaine parent est déjà sélectionné.

Name	Description	Devices
Global		

Visibilité et contrôle des politiques dans un environnement FMC multidomaine

La visibilité et le contrôle des politiques sont limités aux utilisateurs de domaines respectifs, à l'exception d'un administrateur du domaine **global**. Cet exemple est basé sur la hiérarchie comme suit :



Visibilité : Comme l'illustre cette image, la page **Stratégies** d'affichage par défaut répertorie les stratégies (ACP) configurées sous le domaine respectif.

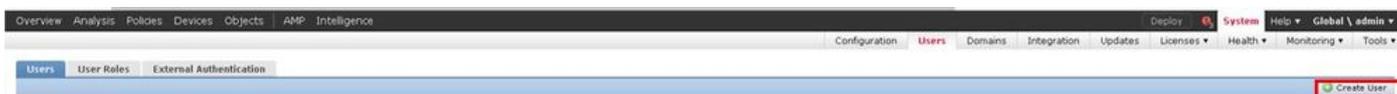
Access Control Policy	Domain	Status	Last Modified
Base-Policy	Global	Targeting 0 devices	2020-05-27 21:43:00 Modified by "admin"

Contrôle : **Les** utilisateurs **admin** qui appartiennent au domaine respectif peuvent **MODIFIER** les stratégies. Pour modifier les stratégies, qui appartiennent à d'autres domaines (par exemple dans le cadre de l'héritage), il faut basculer le domaine actuel vers un domaine sous lequel la stratégie est configurée. Seuls les utilisateurs Admin appartenant au domaine **global** ou au domaine L1 peuvent basculer autour du domaine inférieur pour la gestion des stratégies.

Ajouter des utilisateurs au domaine

Ceci montre comment ajouter des utilisateurs dans un domaine particulier. Cette procédure s'applique aux utilisateurs de la base de données locale.

1. Accédez à **Système >Utilisateurs**. Cliquez sur **Créer un utilisateur** comme indiqué dans l'image.



2. La boîte de dialogue **Configuration utilisateur** s'affiche. Complétez le **nom d'utilisateur** et le **mot de passe (& Confirm Password)**. Cliquez sur **Ajouter un domaine** pour ajouter l'utilisateur au domaine spécifié comme indiqué dans l'image.

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. Choisissez le domaine prévu dans la liste déroulante **Domaine** dans laquelle vous souhaitez ajouter l'utilisateur sous et spécifiez le rôle comme indiqué dans l'image. Un nouvel utilisateur peut être ajouté à son propre domaine ou aux domaines enfants.

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

Les utilisateurs configurés sont affichés dans cette image :

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	

L'accès aux ressources sur FMC serait limité au domaine auquel appartient l'utilisateur. Comme indiqué ci-dessous, lorsque l'utilisateur **L1-A-admin** se connecte à l'interface FMC, l'accès est limité au domaine **L1-Domain-A** auquel l'utilisateur fait partie et au domaine enfant une fois que l'utilisateur passe à ce domaine enfant. Cet utilisateur ne peut modifier que la stratégie définie dans le domaine **L1-Domain-A** et la stratégie définie dans le domaine enfant lorsque le domaine est commuté vers son domaine enfant. En outre, l'exemple ci-dessous montre que **L1-A-Policy** hérite de la stratégie définie dans le domaine global, à savoir **Base-Policy**, ainsi que peut être modifiée, qui peut être vue à partir de signe. Les paramètres d'héritage pointent vers la **stratégie de base** comme indiqué dans l'image.

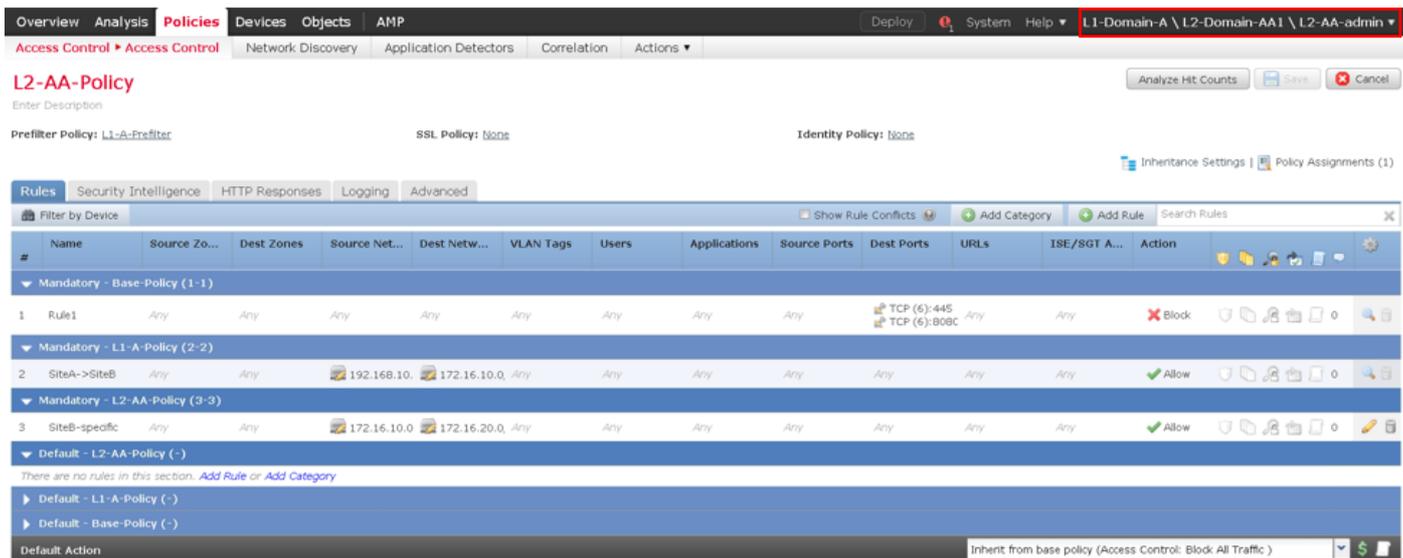
Access Control Policy	Domain	Status	Last Modified	
Base-Policy	Global	Targeting 0 devices	2020-05-28 22:49:49 Modified by "admin"	
L1-A-Policy	Global \ L1-Domain-A	Targeting 0 devices	2020-05-28 23:02:14 Modified by "admin"	

De même, un utilisateur **L2-AA-admin** appartenant au domaine **L2-Domain-AA1** n'a le contrôle que de la stratégie **L2-AA-Policy** définie dans le domaine comme indiqué dans l'image. La **stratégie L2-AA** hérite de la stratégie **L1-A-Policy** définie dans **L1-Domain-A** qui, à son tour, hérite de la **stratégie de base** définie dans le domaine global. En outre, la stratégie **L2-AA-Policy** peut être modifiée, comme vous pouvez le voir à partir de signe. L'utilisateur L2-AA-admin ne peut jamais basculer vers son domaine parent, à savoir L1-Domain-A, ni vers son domaine ancêtre, à savoir le domaine 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"	

En outre, un utilisateur **L1-A-admin** appartenant à L1-Domain-A peut passer à L2-Domain-AA1 et

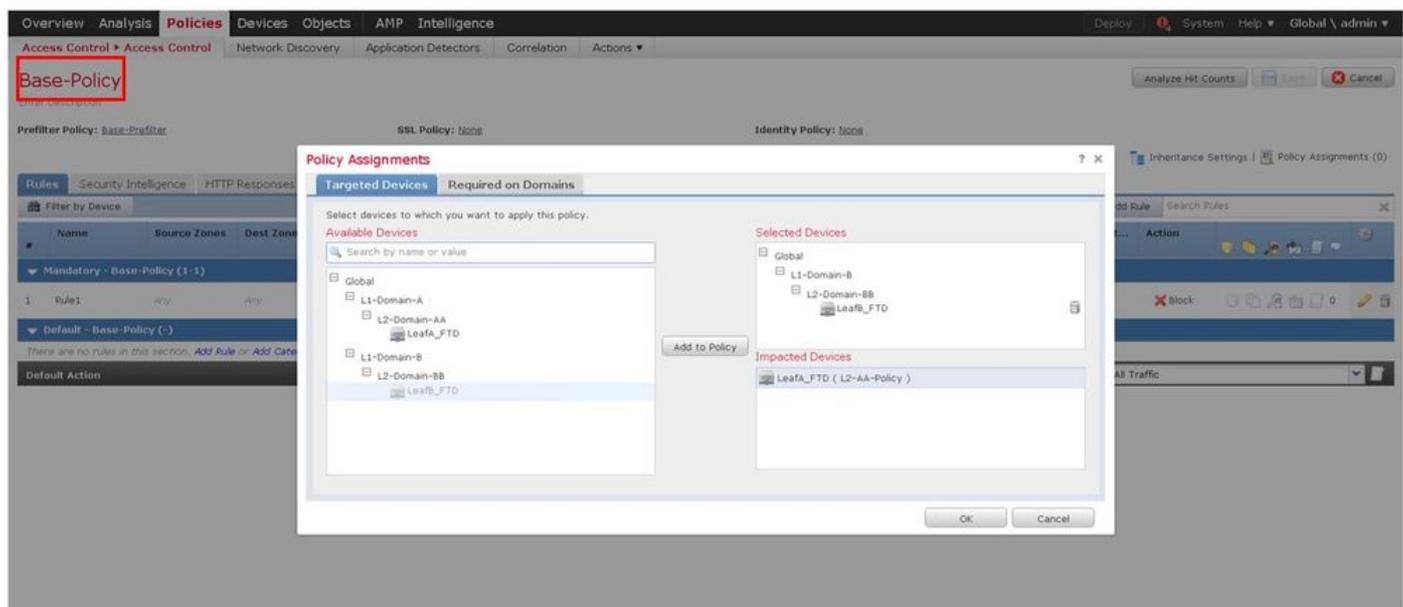
modifier la stratégie **L2-AA-Policy** qui est vue à partir de comme indiqué dans l'image. Ceci s'applique même à un utilisateur appartenant au domaine global et basculant vers les domaines enfants et modifiant les stratégies définies dans le domaine enfant particulier.



Points importants à noter :

- Lors de la suppression des domaines non globaux, les utilisateurs appartenant aux domaines sont automatiquement déplacés vers le domaine **global**.

Les FTD/s sont toujours définis dans le domaine Leaf. Dans ce cas, le domaine leaf est le domaine **L2** (c'est-à-dire L2-Domain-AA et L2-Domain-BB). Le FTD appartenant au domaine **L2** peut être affecté à la stratégie dans le domaine **L1** ou dans le domaine **global**. Dans cette image, l'ACP dans le domaine Global a attribué le FTD défini dans le domaine L3 à la stratégie définie dans le domaine Global.



- Les utilisateurs du domaine global peuvent naviguer vers d'autres domaines spécifiques à l'utilisateur, mais les utilisateurs d'un domaine spécifique n'ont de visibilité que dans leur propre domaine et leurs domaines enfants. Ils ne peuvent pas accéder au domaine global ou à tout autre domaine supérieur, comme indiqué dans ce tableau :

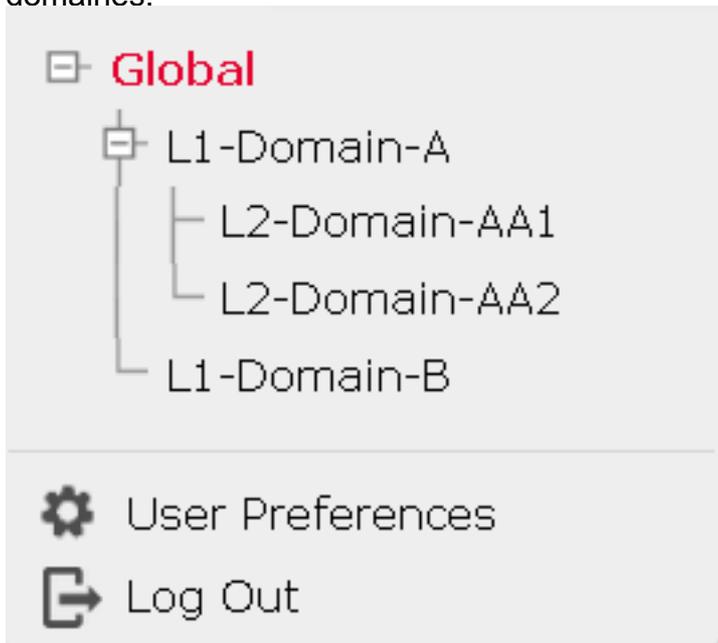
Domaine global

L'utilisateur du domaine global a une visibilité sur tous les domaines configurés et peut accéder à d'autres

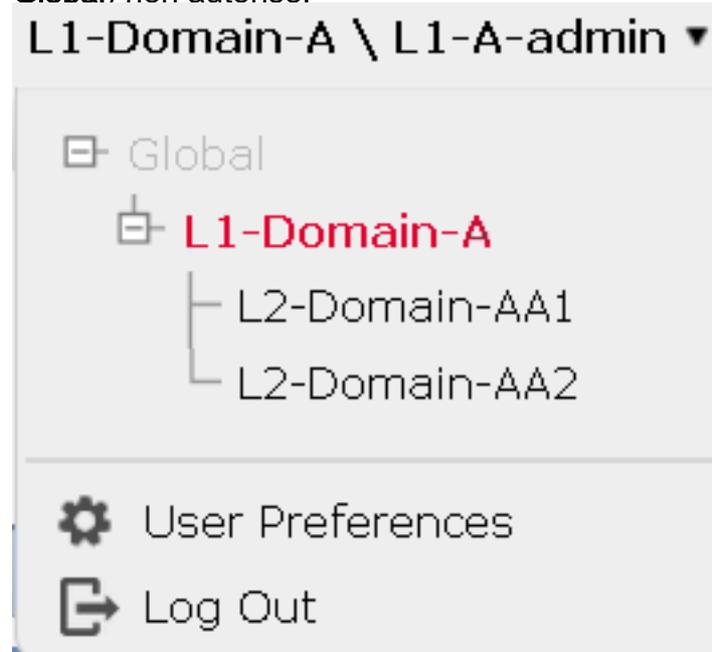
Domaine spécifique à l'utilisateur

L'utilisateur dans **L1-Domain-A** aura une visibilité uniquement sur lui-même et son domaine enfant,

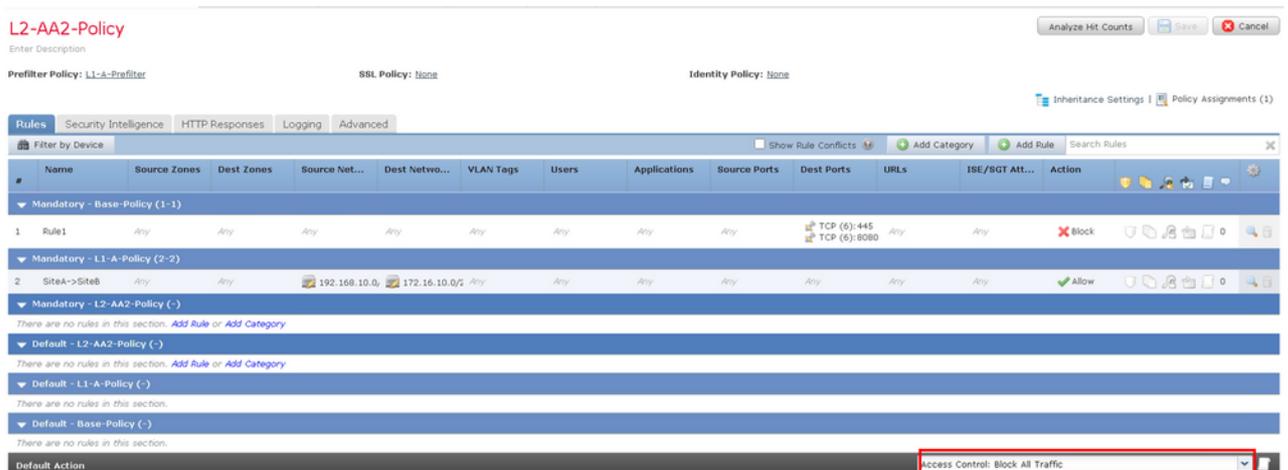
domaines.



savoir **L2-Domain-AA** et pourra accéder à **L2-Dom AA**. Accès au domaine de niveau supérieur (comme **Global**) non autorisé.



- L'action par défaut de la stratégie enfant ne peut pas être verrouillée par la stratégie parente et l'utilisateur n'a pas besoin d'hériter de l'action par défaut de la stratégie parente comme dans cette image.



Dans cette image, on peut voir que l'utilisateur n'a pas assigné l'action par défaut comme celle du parent, ce qui peut être évident à partir des mots **Hériter de la stratégie de base** : ne pas être vu dans l'action par défaut.

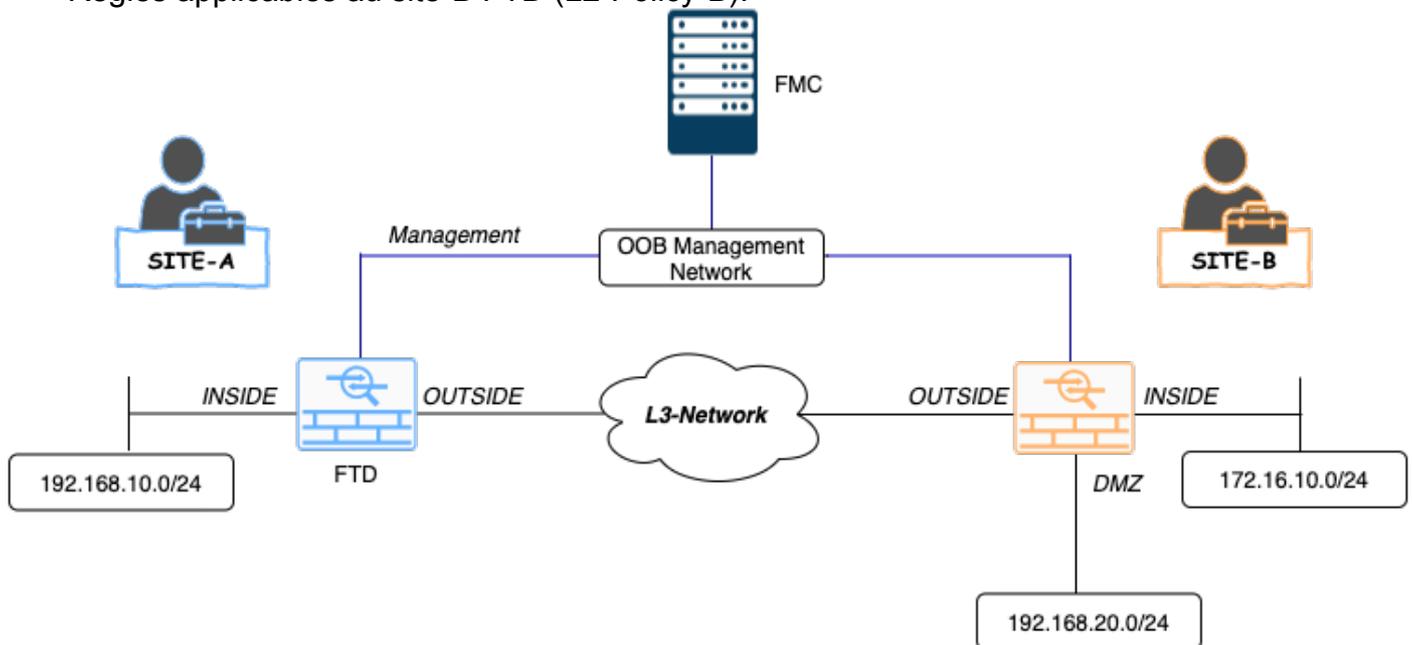
Note: N'oubliez pas qu'un utilisateur ne peut pas afficher simultanément les deux stratégies de domaine L1/L2. L'utilisateur doit passer au domaine souhaité pour afficher et modifier les stratégies. Exemple : si l'utilisateur **admin** présent dans le domaine global souhaite afficher les stratégies configurées dans L1-Domain-A et L2-Domain-AA, l'utilisateur peut le faire en basculant vers L1-A-Domain pour afficher et modifier la stratégie configurée dans ce domaine, puis en basculant vers L2-Domain-AA pour afficher et modifier la stratégie correspondante, mais ne peut pas afficher les deux en même temps. En outre, l'utilisateur de L1-Domain-A ne peut pas modifier ou supprimer la stratégie définie dans le domaine global, c'est-à-dire la stratégie de base qui est la stratégie parente de L1-A-Policy, et l'utilisateur de L2-Domain-AA ne peut pas modifier ou supprimer les stratégies, à savoir la stratégie de

base et la stratégie de couche 2-A définie dans les domaines globaux et de couche 2-Domain-A respectivement.

Scénario d'utilisation

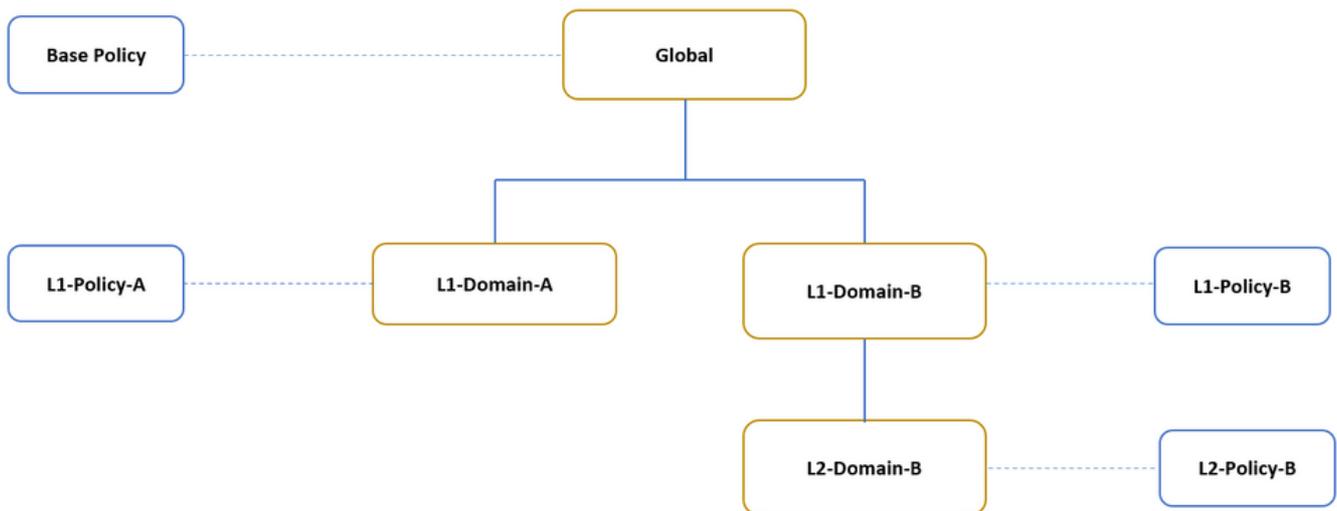
Considérez le scénario représenté dans l'image, les FTD de SITE-A (SiteA-FTD) et de SITE-B (SiteB-FTD) sont gérés par un FMC unique via différents domaines (multidomaine) pour fournir un accès contrôlé. Du point de vue de la politique, voici les considérations de politique au niveau de l'organisation :

- Les règles BLOC spécifiques au service qui sont applicables à TOUS les FTD indépendants du SITE ou du DOMAINE appartiennent à (Stratégie de base).
- Règles qui répondent aux conditions requises pour l'accès de Site-A à Site-B (L1-Policy-A) et de Site-B à Site-A (L1-Policy-B).
- Règles applicables au site-B FTD (L2-Policy-B).



Héritage dans un environnement multidomaine

Pour le cas d'utilisation mentionné ci-dessus, considérez la hiérarchie de domaine/stratégie suivante. SiteA-FTD et SiteB-FTD font partie des domaines Leaf L1-Domain-A et L2-Domain-B respectivement.



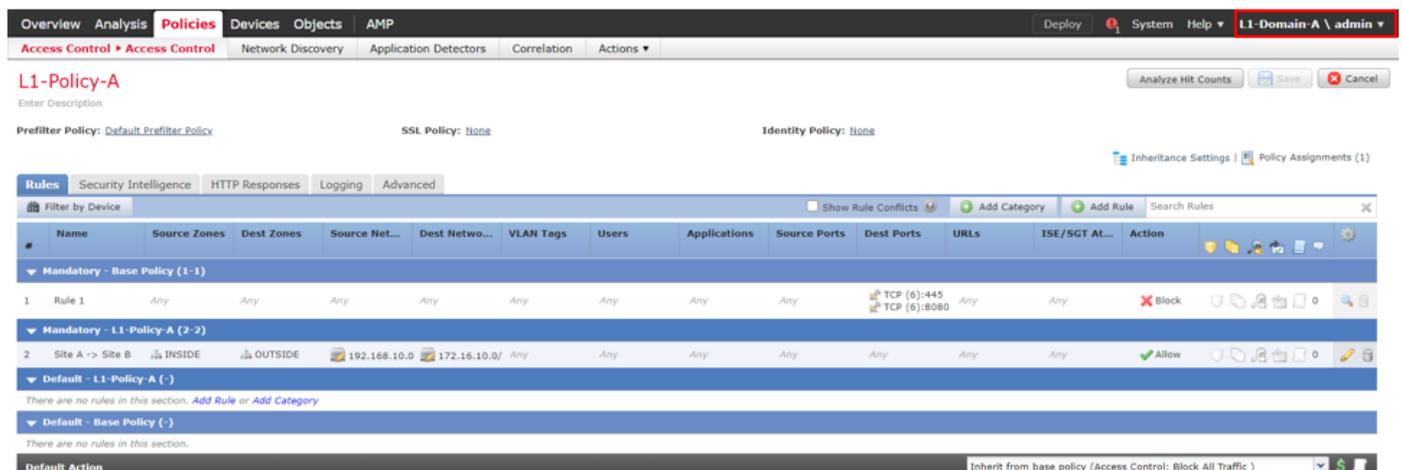
La structure de la hiérarchie de domaine est la suivante :

- Le domaine **global** est parent de **L1-Domain-A** et **L1-Domain-B**.
- Le domaine **global** est ancêtre de **L2-Domain-B**.
- **L2-Domain-B** est l'enfant de **L1-Domain-B**
- **L2-Domain-B** est un domaine leaf car il n'a pas de domaines enfants.

L'image montre la hiérarchie de domaine telle qu'elle apparaît à partir de FMC.



L'instantané ci-dessous montre comment les règles sont définies dans **L1-Policy-A** et **L2-Policy-B** avec r.t au scénario ci-dessus.



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)	

Vous devez toujours tenir compte des règles et de leur héritage lors de la configuration de plusieurs domaines pour éviter de bloquer le trafic légitime ou d'autoriser le trafic indésirable.