Vererbung in einer Multidomain-Umgebung in FTD

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration und Funktionsweise von Vererbungs- und Multi-Domain-Features. Der Schwerpunkt liegt dabei auch auf einem praktischen Anwendungsfall, um zu sehen, wie diese beiden Funktionen zusammenarbeiten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

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

Hinweis: Die Multi-Domain- und die Vererbungsfunktion werden ab der Version 6.0 auf FMC/FTD unterstützt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen einer Konfiguration verstehen.

Hintergrundinformationen

In der Richtlinienvererbung können Zugriffskontrollrichtlinien geschachtelt werden, in denen die untergeordnete Richtlinie Regeln von einer Basisrichtlinie erbt, einschließlich der AKP-Einstellungen wie Sicherheitsintelligenz, HTTP-Antwort, Protokollierungseinstellungen usw. Optional kann der Administrator der untergeordneten Richtlinie gestatten, die AKP-Einstellungen wie Sicherheitsintelligenz, HTTP-Antwort, Protokollierungseinstellungen zu überschreiben oder die Einstellungen zu sperren, damit die untergeordnete Richtlinie diese nicht überschreiben kann. Diese Funktion ist in einer FMC-Umgebung mit mehreren Domänen sehr nützlich.

Die Funktion für mehrere Domänen segmentiert den Benutzerzugriff auf die verwalteten Geräte, Konfigurationen und Ereignisse des FMC. Je nach Berechtigung kann ein Benutzer zu anderen Domänen wechseln bzw. auf diese zugreifen. Wenn die Multidomain-Funktion nicht konfiguriert ist, gehören alle verwalteten Geräte, Konfigurationen und Ereignisse zur **globalen** Domäne.

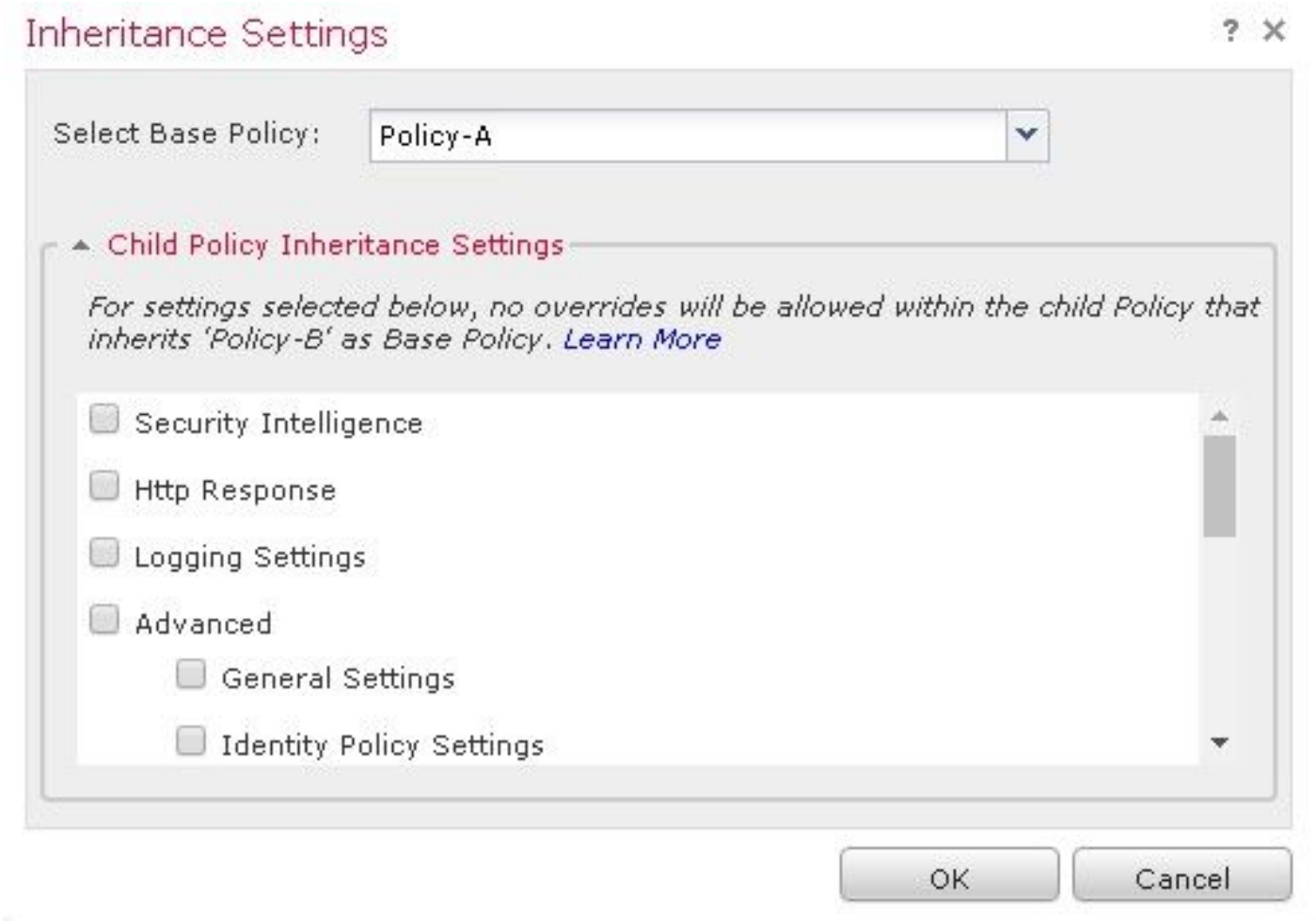
Konfigurieren der Richtlinienvererbung

Eine Leaf-Domäne ist eine Domäne, die keine weiteren Subdomänen hat. Eine untergeordnete Domäne ist der nächste Abkömmling der Domäne, in der sich der Benutzer/Administrator befindet. Die übergeordnete Domäne ist der direkte Vorfahren der Domäne, in der sich der Benutzer/Administrator befindet.

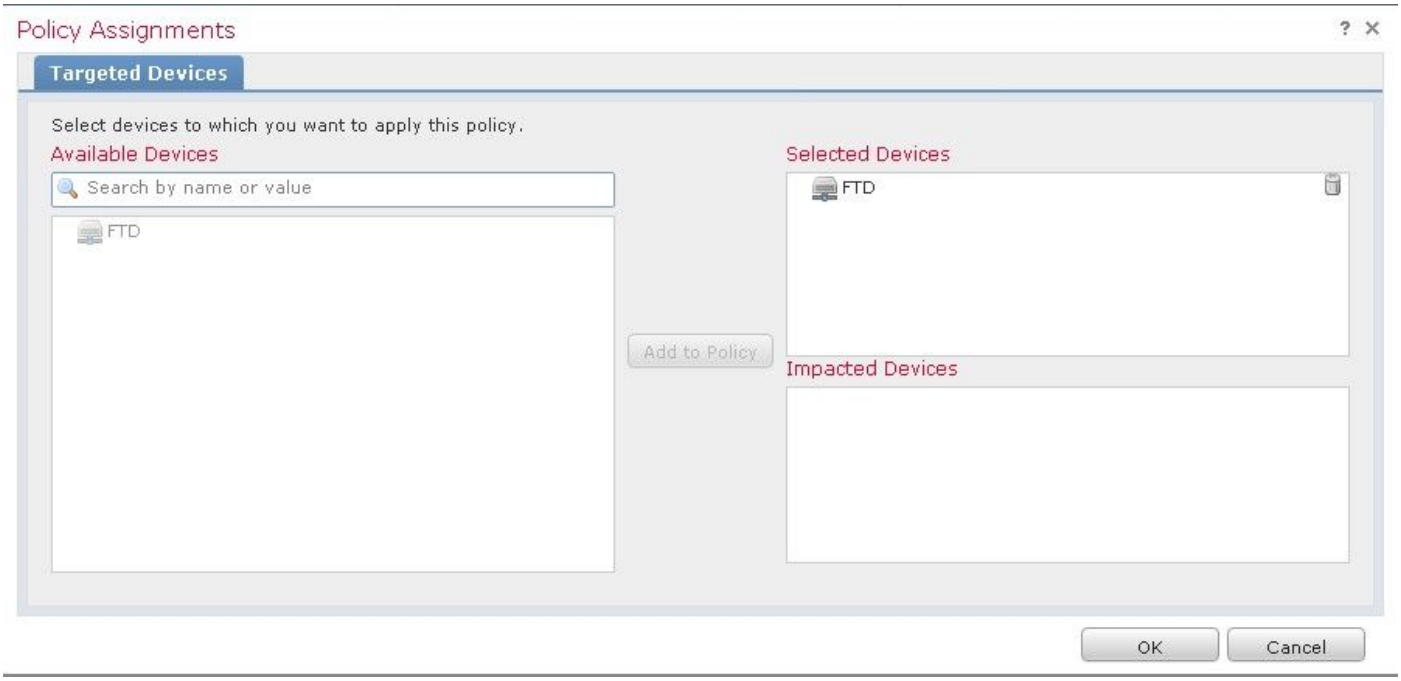
So konfigurieren/aktivieren Sie die Vererbung für vorhandene Richtlinien:

1. Policy-A soll die grundlegende Richtlinie und Policy-B die untergeordnete Richtlinie sein (Policy-B erbt die Regel von Policy-A)
2. **EDIT** Policy-B und klicken Sie auf **Vererbungseinstellungen**, wie im Bild gezeigt.

3. Wählen Sie Policy-A aus der unten angezeigten Dropdown-Liste **Select Base Policy** aus. Andere AKP-Einstellungen wie Sicherheitsintelligenz, HTTP-Antwort, Protokollierungseinstellungen usw. können geerbt werden, um die Einstellungen der untergeordneten Richtlinie optional zu überschreiben.

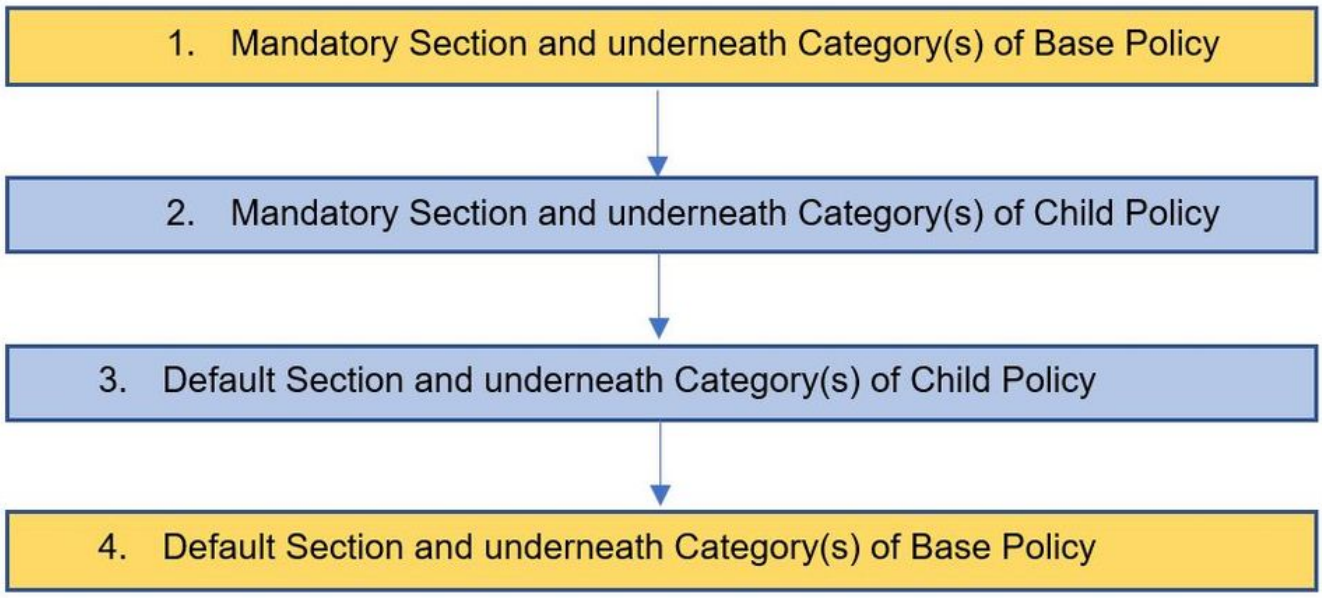


4. Führen Sie die **Richtlinienzuweisung** für die Richtlinie "Child" (Kind)-B für das beabsichtigte Ziel-FTD-Gerät aus:

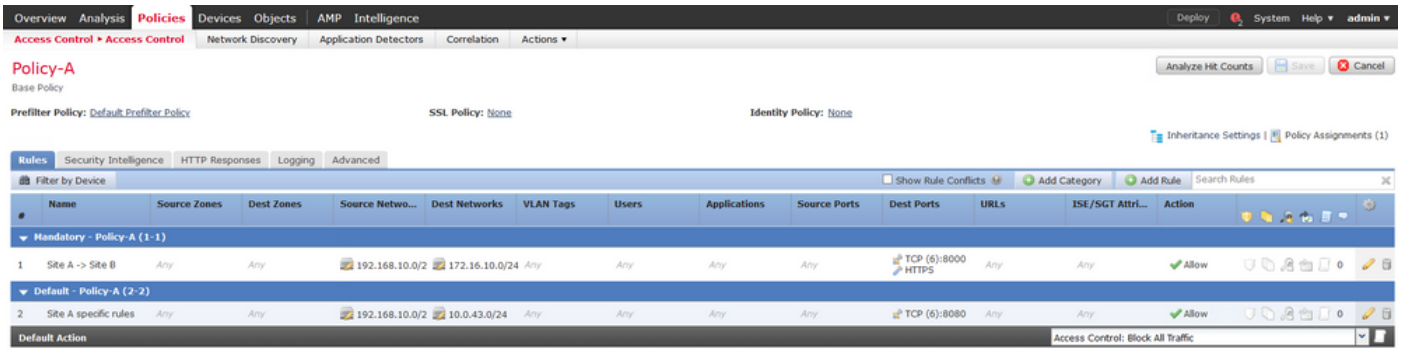


Standardmäßig wird die **Standardaktion** der Kinderrichtlinie vererbt und auf **Vererben von der Basisrichtlinie** wie im Bild gezeigt festgelegt. Der Benutzer kann auch die **Standardaktion** aus den vom System bereitgestellten Richtlinien auswählen, wie hier gezeigt.

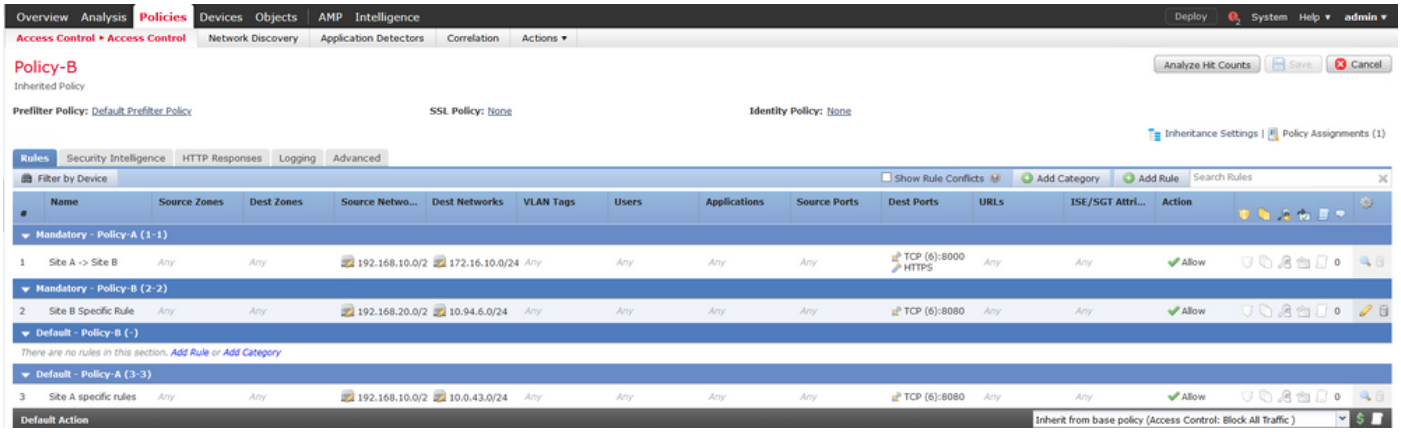
Die Reihenfolge für die Datenverkehrssuche wird immer von oben nach unten festgelegt, unabhängig von der Anzahl der Kategorien, die in den obligatorischen und den standardmäßigen Abschnitten hinzugefügt werden. Nachdem Sie die **Vererbungseinstellungen** angewendet haben**,** die AKP-Darstellung für die untergeordnete Policy-B (Child Policy), wie im Bild dargestellt, in Übereinstimmung mit der zuvor erwähnten **Regelprüfreihenfolge**:



Dieses Bild zeigt, wie im FMC sowohl die Richtlinien, nämlich "Policy-A", die Grundrichtlinie, als auch "Policy-B", d. h. die "Child Policy", die von "Policy A" übernommen wird, als auch "Policy-B" dargestellt werden.



Dieses Bild zeigt, dass in Policy-B die Regeln aus Policy-A sowie die in Policy-B selbst konfigurierten spezifischen Regeln angezeigt werden. Es sollte darauf geachtet werden, wie die Regeln unter Berücksichtigung der Reihenfolge konfiguriert werden.

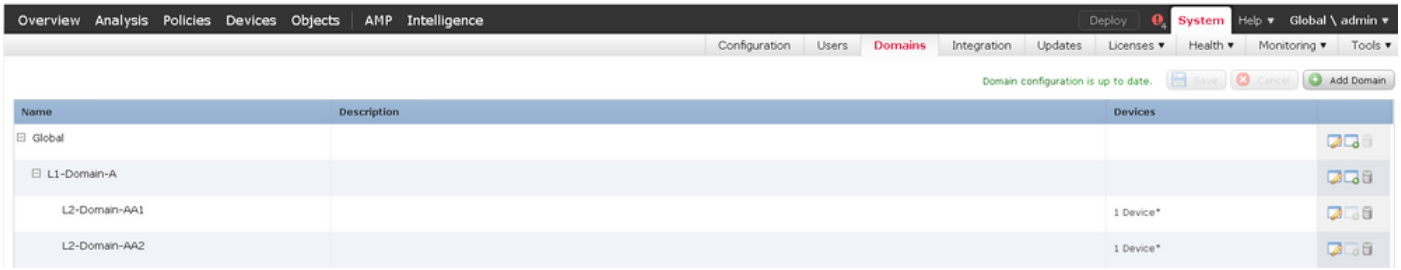


FTD-Management in Multi-Domain FMC-Umgebung

Die Funktion für mehrere Domänen segmentiert den Benutzerzugriff auf verwaltete Geräte, Konfigurationen und Ereignisse. Je nach Berechtigung kann ein Benutzer zu anderen Domänen wechseln. Wenn die Multidomain-Funktion nicht konfiguriert ist, gehören alle verwalteten Geräte, Konfigurationen und Ereignisse zur **globalen** Domäne.

Es können maximal dreistufige Domänen mit Global Domain als Level 1 konfiguriert werden. Alle verwalteten Geräte müssen nur zur Leaf-Domäne gehören. Dies kann durch das Symbol des

(Unterdomäne hinzufügen), die in der Leaf-Domäne wie im Bild gezeigt ausgegraut ist.



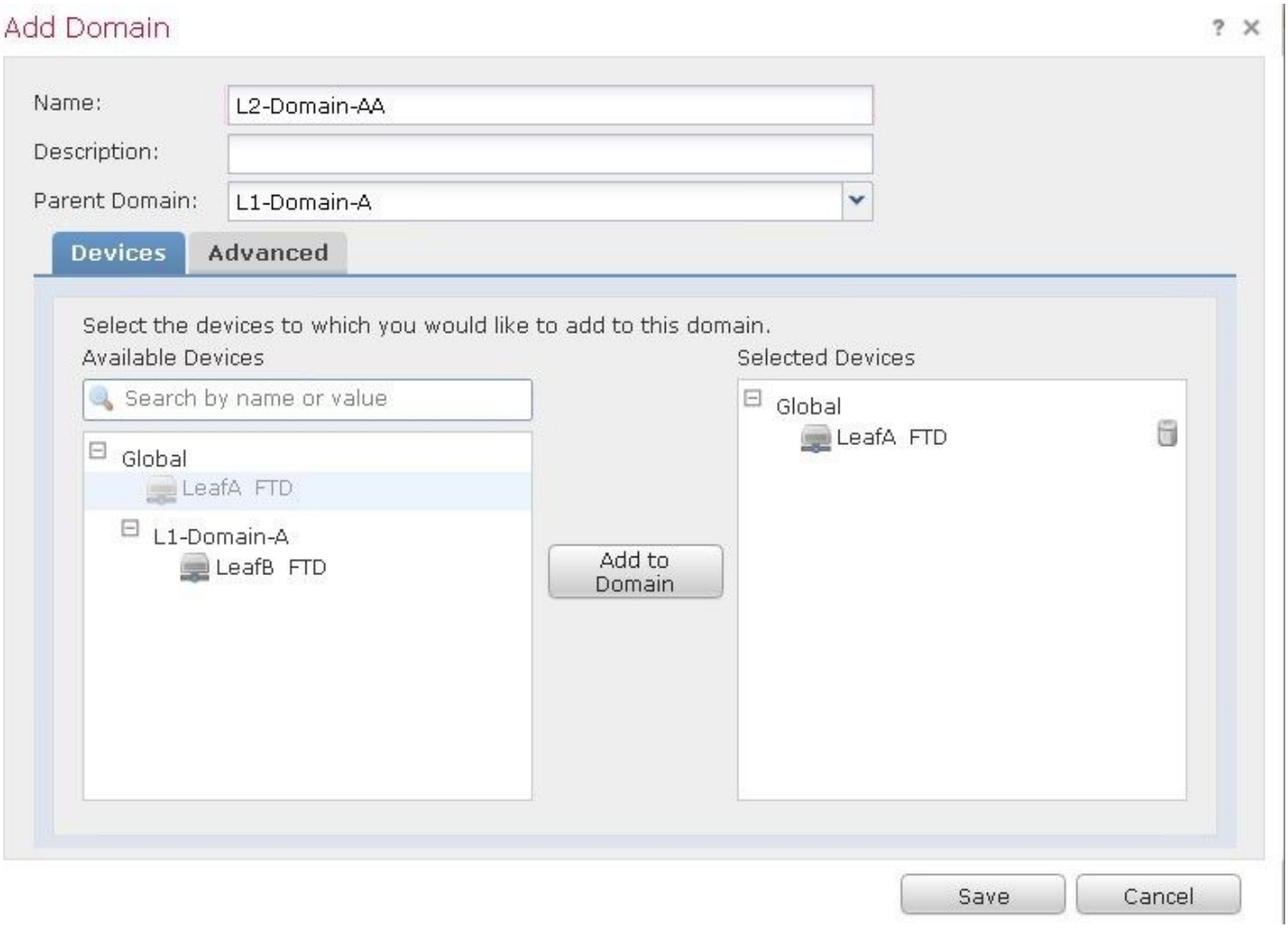
Domänenkonfiguration

Die Domänenkonfiguration kann wie folgt durchgeführt werden:

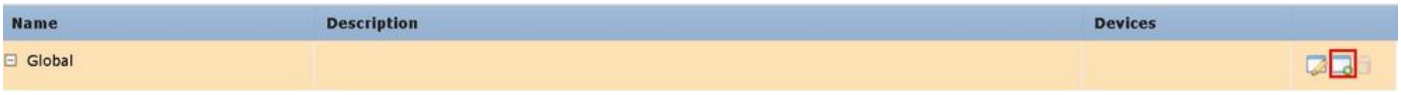
1. Navigieren Sie zu **System > Domänen**. Standardmäßig ist die **globale** Domäne vorhanden.

2. Klicken Sie auf **Domäne hinzufügen**, wie im Bild gezeigt.

3. Das Dialogfeld **Domäne hinzufügen** wird angezeigt. Geben Sie den **Namen** der Domäne ein, und wählen Sie die **Übergeordnete Domäne** aus der Dropdown-Liste aus. Wenn es sich um die Leaf-Domäne handelt, müssen die FTD-Geräte, wie im Bild gezeigt, der Domäne hinzugefügt werden.

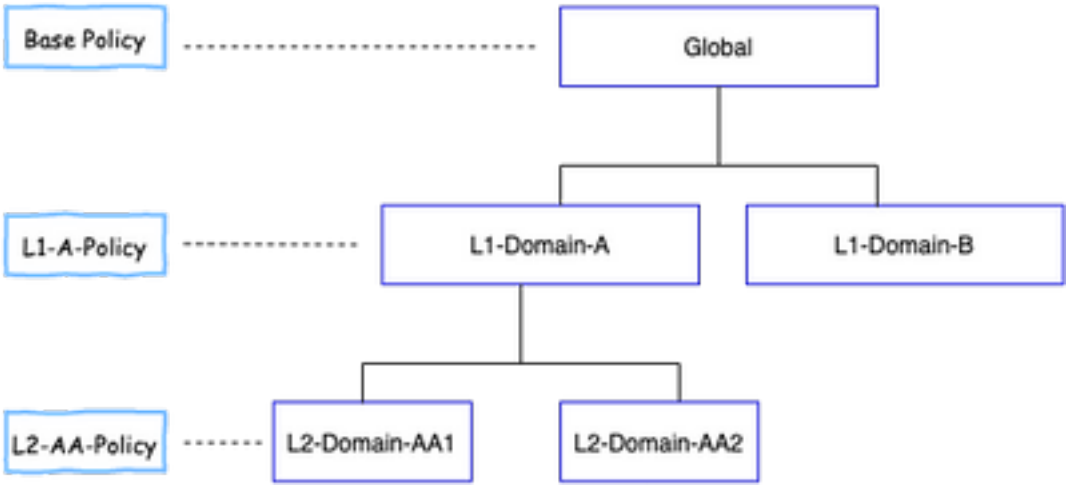


Hinweis: Um die Domänen hinzuzufügen, klicken Sie auf das Symbol **Unterdomäne hinzufügen**, wie im Bild gezeigt. Hier ist die übergeordnete Domäne bereits ausgewählt.



Richtlinientransparenz und -kontrolle in einer FMC-Umgebung mit mehreren Domänen

Die Richtlinientransparenz und -kontrolle ist auf die jeweiligen Domänenbenutzer beschränkt, mit Ausnahme eines Administrators einer **globalen** Domäne. Dieses Beispiel basiert auf der folgenden Hierarchie:



Transparenz: Wie in diesem Bild gezeigt, werden auf der Seite **Richtlinien** in der Standardansicht Richtlinien (ACP, Policies) aufgeführt, die unter der jeweiligen Domäne konfiguriert wurden.

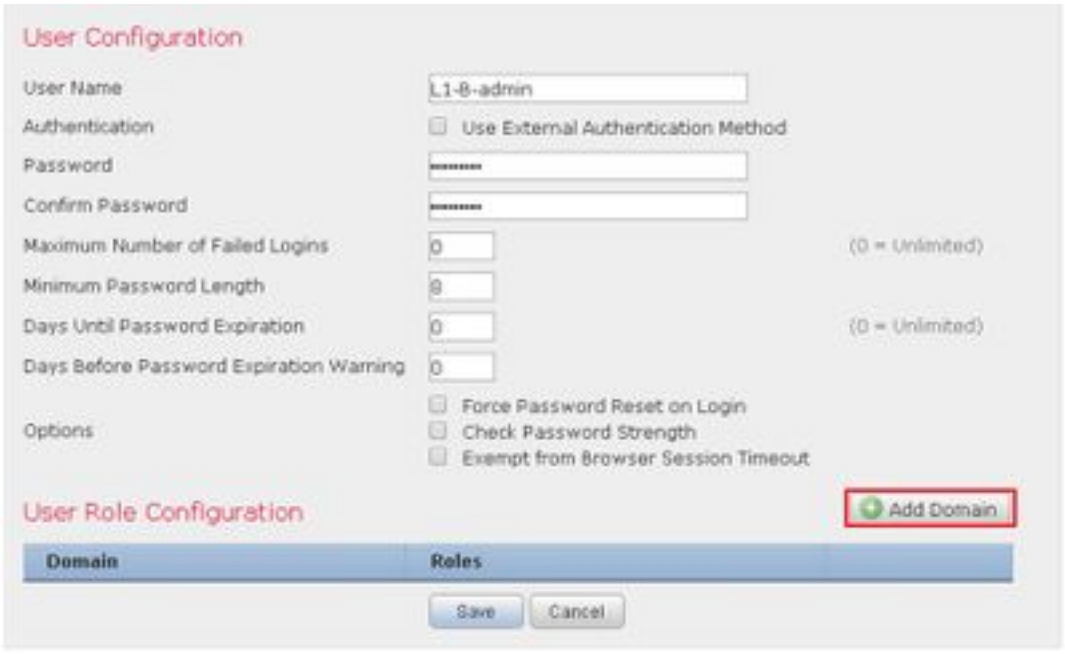
Kontrolle: **Admin-**Benutzer, die der jeweiligen Domäne angehören, können die Richtlinien BEARBEITEN. Um die Richtlinien zu bearbeiten, die zu anderen Domänen gehören (z. B. als Teil der Vererbung), muss die Domäne von der aktuellen auf eine Domäne umgestellt werden, in der die Richtlinie unter konfiguriert ist. Nur Admin-Benutzer, die der **globalen** Domäne oder der L1-Domäne angehören, können zur Richtlinienverwaltung um die untere Domäne wechseln.

Benutzer zur Domäne hinzufügen

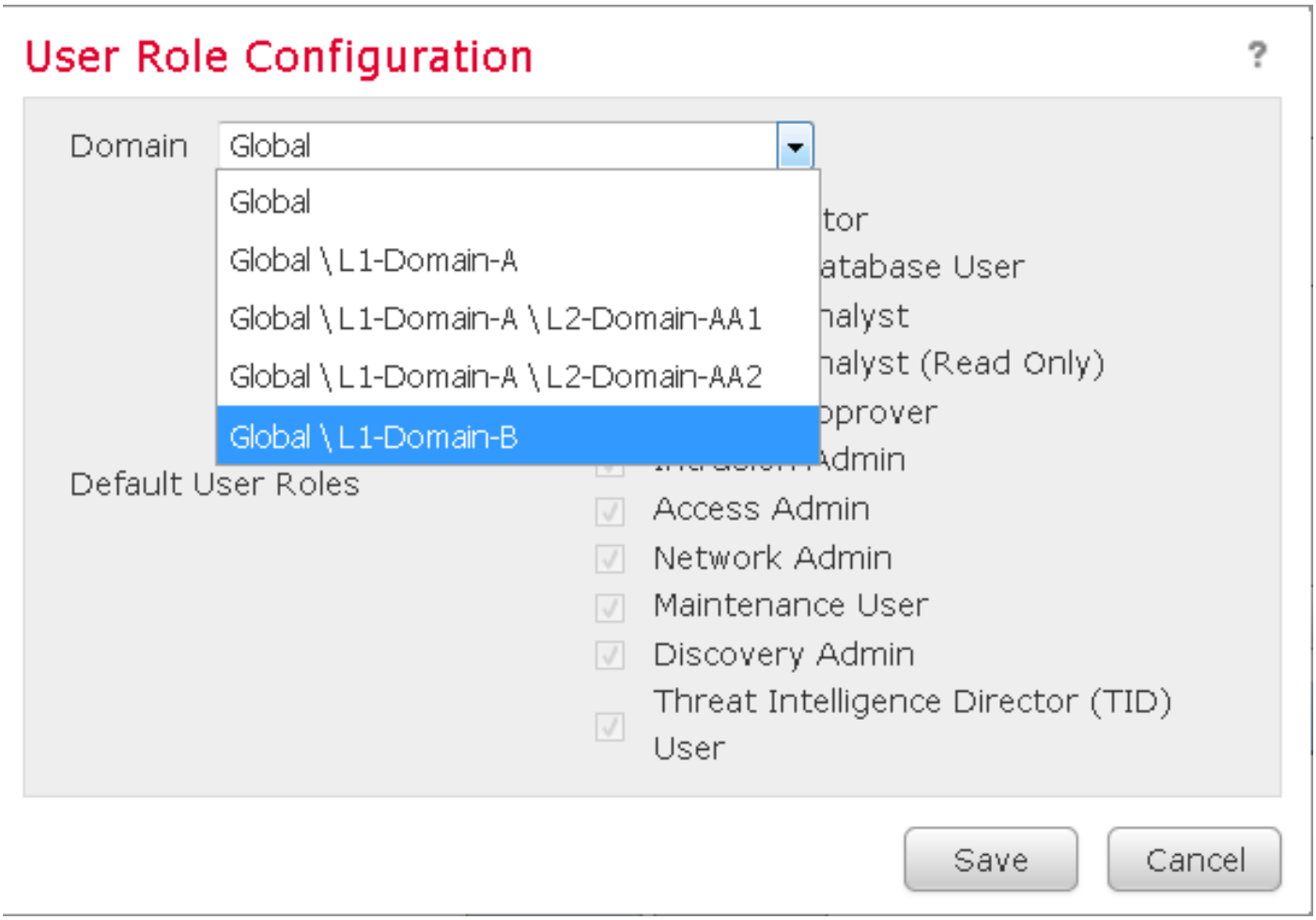
Dieses Beispiel zeigt, wie Benutzer einer bestimmten Domäne hinzugefügt werden. Dieses Verfahren gilt für Benutzer in der lokalen Datenbank.

1. Navigieren Sie zu **System >Benutzer**. Klicken Sie auf **Benutzer erstellen**, wie im Bild gezeigt.

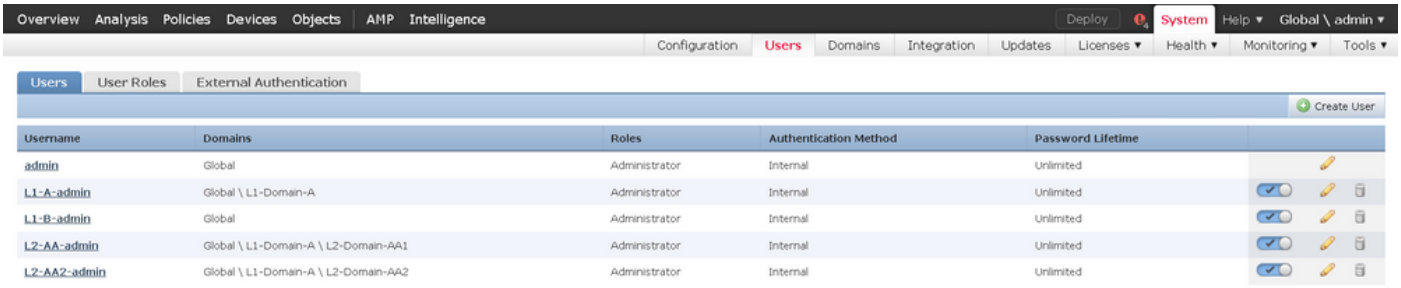
2. Das Dialogfeld **Benutzerkonfiguration** wird angezeigt. Geben Sie den **Benutzernamen** und das **Kennwort (& Confirm Password)** ein. Klicken Sie auf **Domäne hinzufügen**, um den Benutzer der angegebenen Domäne hinzuzufügen, wie im Bild gezeigt.



3. Wählen Sie die gewünschte Domäne aus der Dropdown-Liste **Domain (Domäne) aus**, unter der Sie den Benutzer hinzufügen möchten, und geben Sie die Rolle wie im Bild dargestellt an. Ein neuer Benutzer kann der eigenen Domäne oder den untergeordneten Domänen hinzugefügt werden.

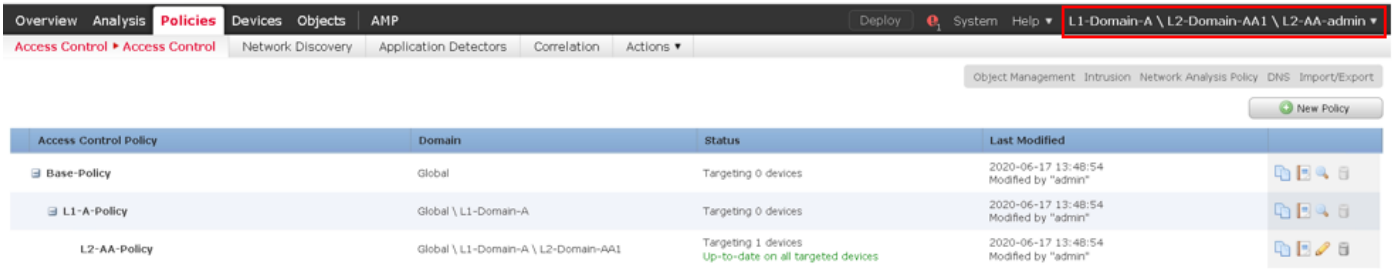


Die konfigurierten Benutzer werden in diesem Bild angezeigt:

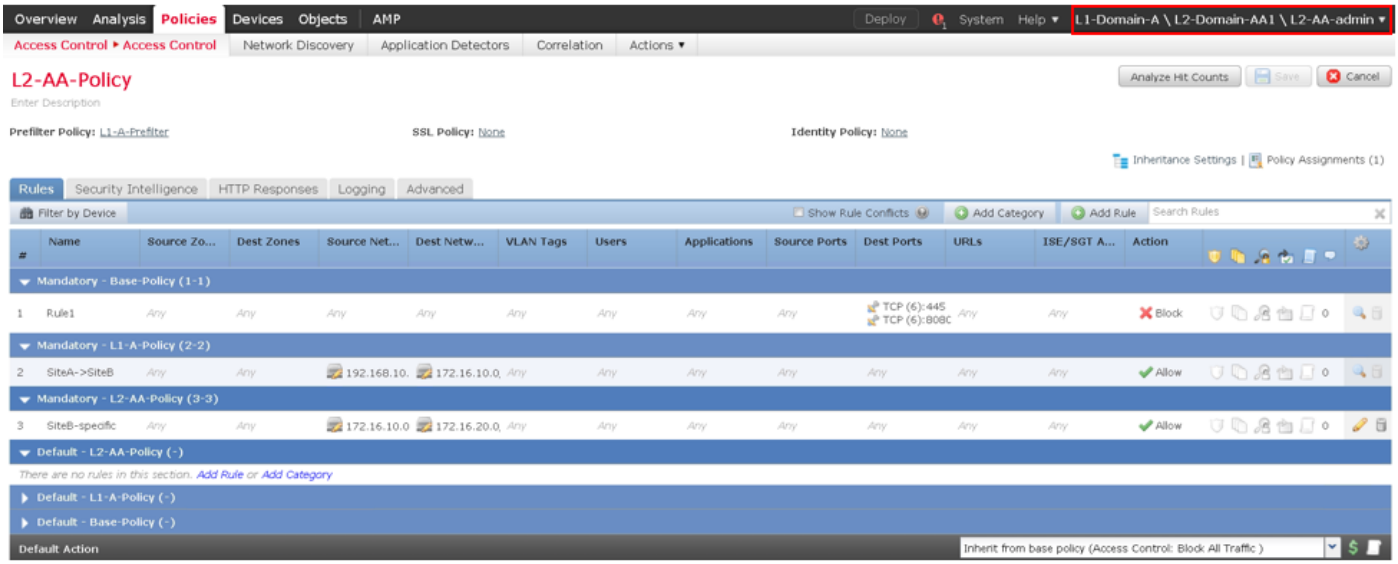


Der Ressourcenzugriff auf FMC würde auf die Domäne beschränkt, der der Benutzer angehört. Wie unten gezeigt, ist der Zugriff bei der Anmeldung des Benutzers **L1-A-admin** bei der FMC-Benutzeroberfläche auf Domänen- **L1-Domänen-A** beschränkt, zu denen der Benutzer gehört, und auf die untergeordnete Domäne, sobald der Benutzer zu dieser untergeordneten Domäne wechselt. Dieser Benutzer kann nur die in der **L1-Domäne-A-**Domäne definierte Richtlinie und die in der untergeordneten Domäne definierte Richtlinie bearbeiten, wenn die Domäne auf die untergeordnete Domäne umgeschaltet wird. Das folgende Beispiel zeigt, dass **L1-A-Policy** die in der globalen Domäne definierte Richtlinie erbt, d. h. **Base-Policy**, und bearbeitet werden kann, die aus dem  Zeichen. Die Vererbungseinstellungen werden so festgelegt, dass sie auf die **Basisrichtlinie** verweisen, wie im Bild gezeigt.

Ebenso hat ein Benutzer **L2-AA-admin**, der zur **L2-Domain-AA1-**Domäne gehört, nur die Kontrolle über die Richtlinie **L2-AA-Policy**, die in der Domäne definiert ist, wie im Bild gezeigt. Die **L2-AA-Richtlinie** erbt die Richtlinie **L1-A-Policy**, die in **L1-Domain-A** definiert ist, die wiederum **Base-Policy** erbt, die in der globalen Domäne definiert ist. Zusätzlich kann die Richtlinie **L2-AA-Policy** bearbeitet werden, die im Abschnitt  Zeichen. Der Benutzer L2-AA-admin kann nie zu seiner übergeordneten Domäne wechseln, nämlich zu L1-Domain-A oder seiner Vorfahren-Domäne, nämlich zur globalen Domäne.



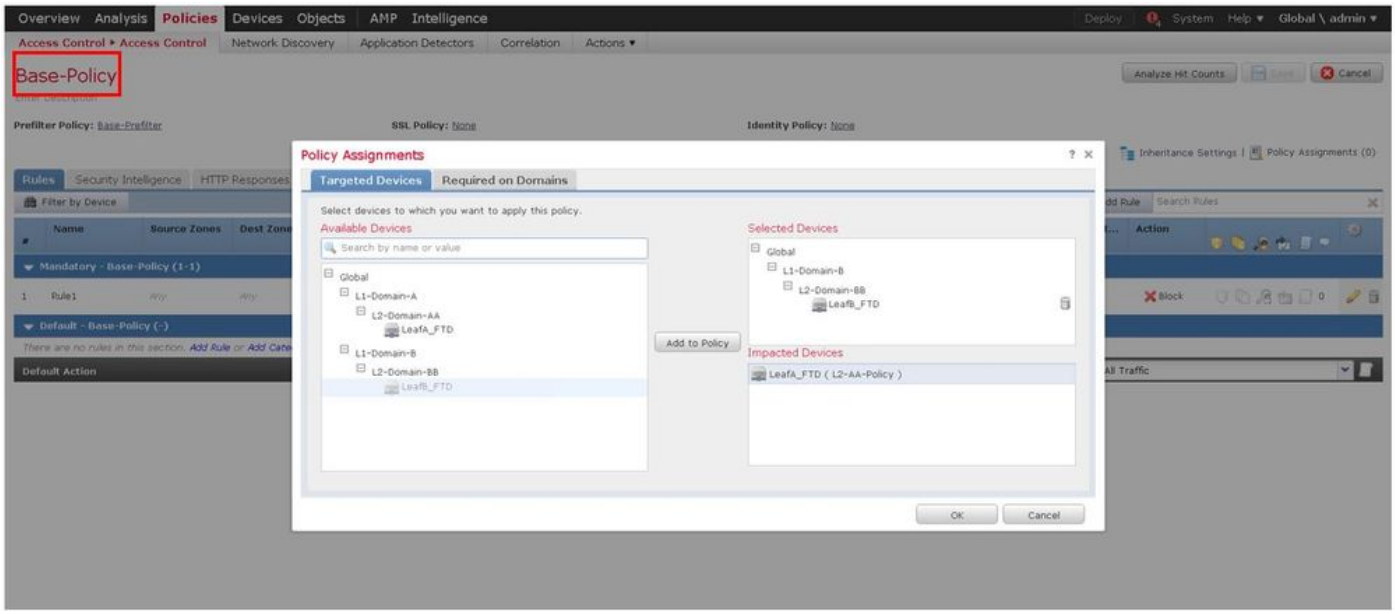
Außerdem kann ein Benutzer **L1-A-admin**, der zur L1-Domäne-A gehört, zu L2-Domain-AA1 wechseln und die Richtlinie **L2-AA-Policy** bearbeiten, die aus dem  wie im Bild gezeigt. Dies gilt auch für einen Benutzer, der der globalen Domäne angehört und zu den untergeordneten Domänen wechselt und die in der jeweiligen untergeordneten Domäne definierten Richtlinien bearbeitet.



Wichtige Punkte:

- Beim Löschen der nicht globalen Domänen werden die zu den Domänen gehörenden Benutzer automatisch in die **globale** Domäne verschoben.

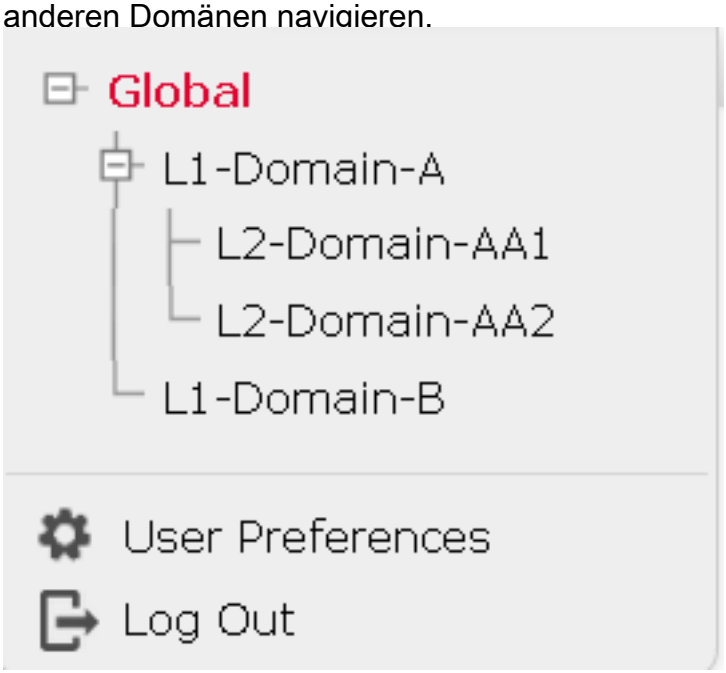
  Die FTDs sind/sind immer in der Leaf-Domäne definiert. In diesem Fall ist die Leaf-Domäne die **L2-Domäne** (d. h. L2-Domain-AA und L2-Domain-BB). Die zur **L2-Domäne** gehörende FTD kann der Richtlinie in der **L1-Domäne** oder in der **globalen** Domäne zugewiesen werden. In diesem Bild weist das ACP in der globalen Domäne die in der L3-Domäne definierte FTD der in der globalen Domäne definierten Richtlinie zu.



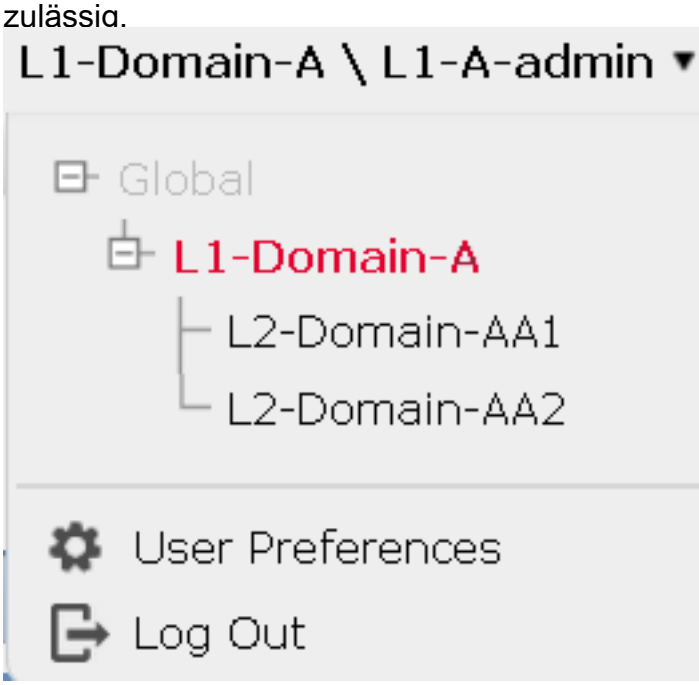
- Benutzer in der globalen Domäne können zu anderen benutzerspezifischen Domänen navigieren. Benutzer einer bestimmten Domäne haben jedoch nur Transparenz in ihrer eigenen Domäne und ihren untergeordneten Domänen. Sie können nicht zur globalen Domäne oder zu anderen höheren Domänen navigieren, wie in der folgenden Tabelle gezeigt:

Globale Domäne	**Benutzerspezifische Domäne**
Benutzer in der globalen Domäne haben Transparenz für alle konfigurierten Domänen und können zu	Benutzer in **L1-Domäne-A** haben nur Transparen sich und die untergeordnete Domäne - **L2-Domai**

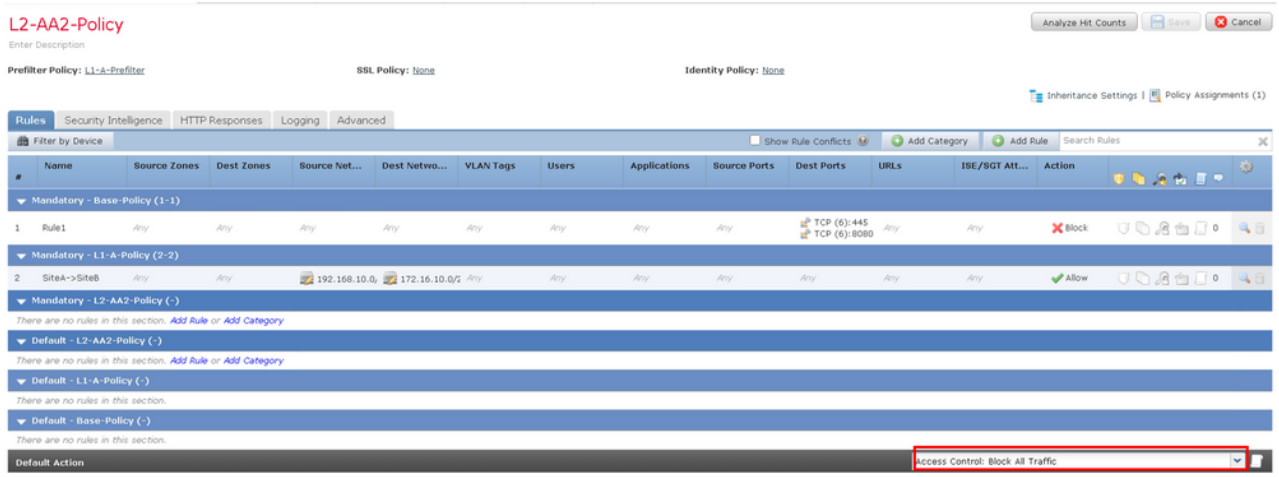
anderen Domänen navigieren.



und können zur **L2-Domäne-AA** navigieren. Der Domänen-Zugriff höherer Ebene (wie **Global**) ist nicht zulässig.



- Die Standardaktion der untergeordneten Richtlinie kann nicht durch die übergeordnete Richtlinie gesperrt werden, und der Benutzer muss die Standardaktion der übergeordneten Richtlinie nicht wie in diesem Bild erben.



In diesem Bild ist zu erkennen, dass der Benutzer nicht die Standardaktion des übergeordneten Elements zugewiesen hat, die sich aus dem Wort **Erben von Basisrichtlinie** ablesen lässt: nicht in der Standardaktion sichtbar.

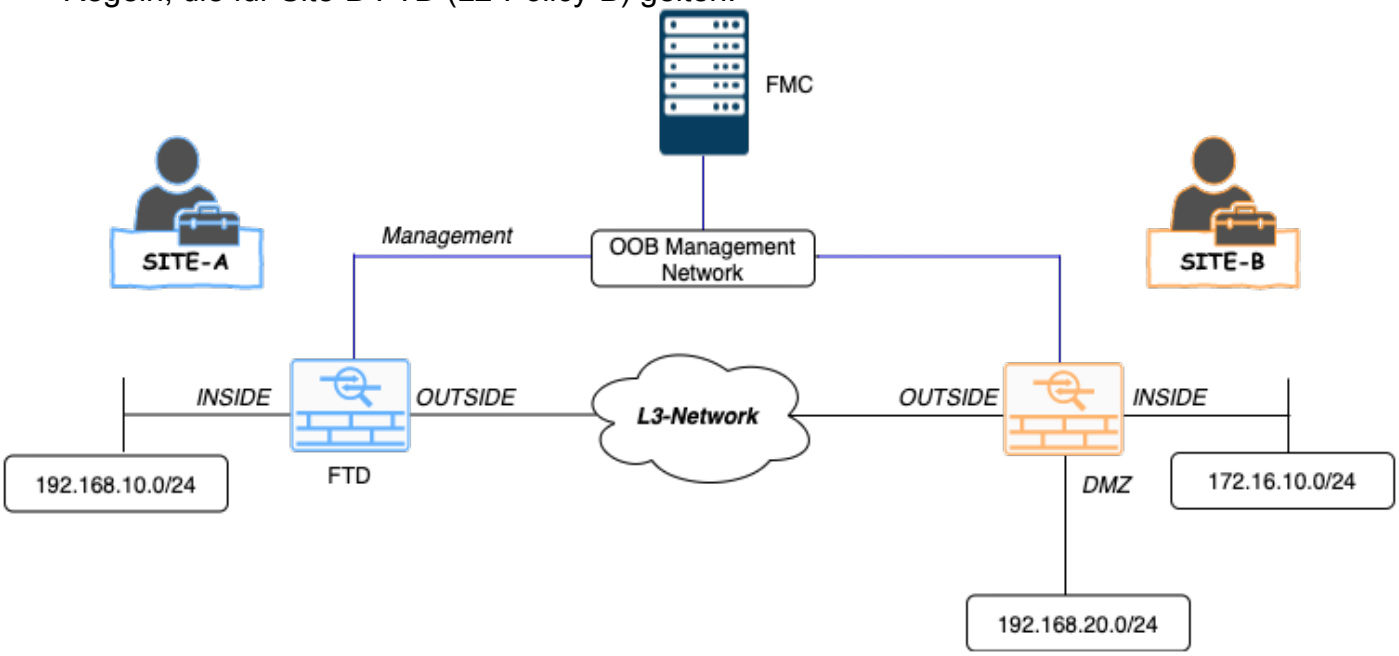
Hinweis: Es sollte beachtet werden, dass ein Benutzer nicht gleichzeitig beide L1/L2-Domänenrichtlinien anzeigen kann. Der Benutzer muss zur gewünschten Domäne wechseln, um die Richtlinien anzuzeigen und zu bearbeiten. Beispiel: Wenn der in der globalen Domäne **vorhandene** Benutzer **Admin** anzeigen möchte, welche Richtlinien in L1-Domain-A und L2-Domain-AA konfiguriert sind, kann der Benutzer dies tun, indem er zu L1-A-Domain wechselt, um die in dieser Domäne konfigurierte Richtlinie anzuzeigen und zu bearbeiten, und dann zu L2-Domain-AA wechselt, um die entsprechende Richtlinie anzuzeigen und zu bearbeiten, aber nicht beide gleichzeitig anzeigen. Außerdem kann der Benutzer in L1-Domäne-A die in der globalen Domäne definierte Richtlinie nicht bearbeiten oder löschen, d. h. die Basisrichtlinie, die die übergeordnete Richtlinie von L1-A-Richtlinie ist, und der

Benutzer in L2-Domäne-AA kann die Richtlinien Basisrichtlinie und L2-A-Richtlinie, die in der globalen bzw. der L2-Domäne-A-Domäne definiert sind, nicht bearbeiten oder löschen.

Anwendungsfall

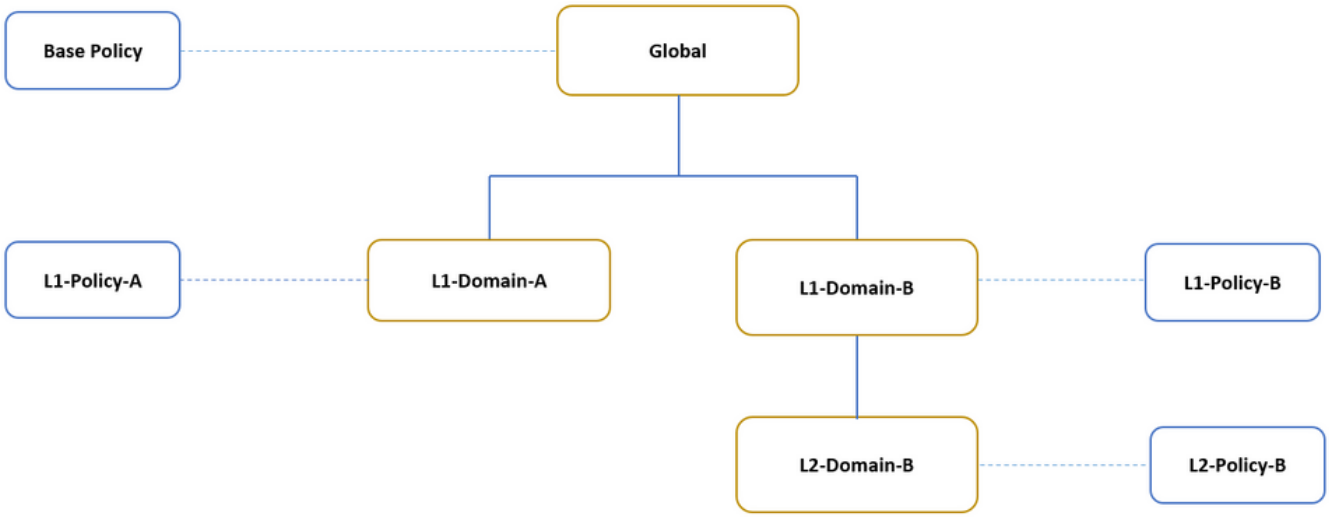
Betrachten wir das im Bild dargestellte Szenario: FTDs von SITE-A (SiteA-FTD) und SITE-B (SiteB-FTD) werden von einem einzigen FMC über verschiedene Domänen (Multi-Domain) verwaltet, um einen kontrollierten Zugriff zu ermöglichen. Aus politischer Sicht sind dies die politischen Überlegungen auf Unternehmensebene:

- Service-spezifische BLOCK-Regeln, die für ALLE FTDs gelten, die unabhängig von SITE oder DOMÄNE sind, gehören zu (Base-Policy).
- Regeln, die die Anforderungen für den Zugriff von Site-A auf Site-B (L1-Policy-A) und von Site-B auf Site-A (L1-Policy-B) erfüllen.
- Regeln, die für Site-B FTD (L2-Policy-B) gelten.



Vererbung in einer Umgebung mit mehreren Domänen

Berücksichtigen Sie für den oben genannten Anwendungsfall die folgende Domänen-/Richtlinienhierarchie. SiteA-FTD und SiteB-FTD sind jeweils Teil der Leaf-Domänen L1-Domain-A und L2-Domain-B.

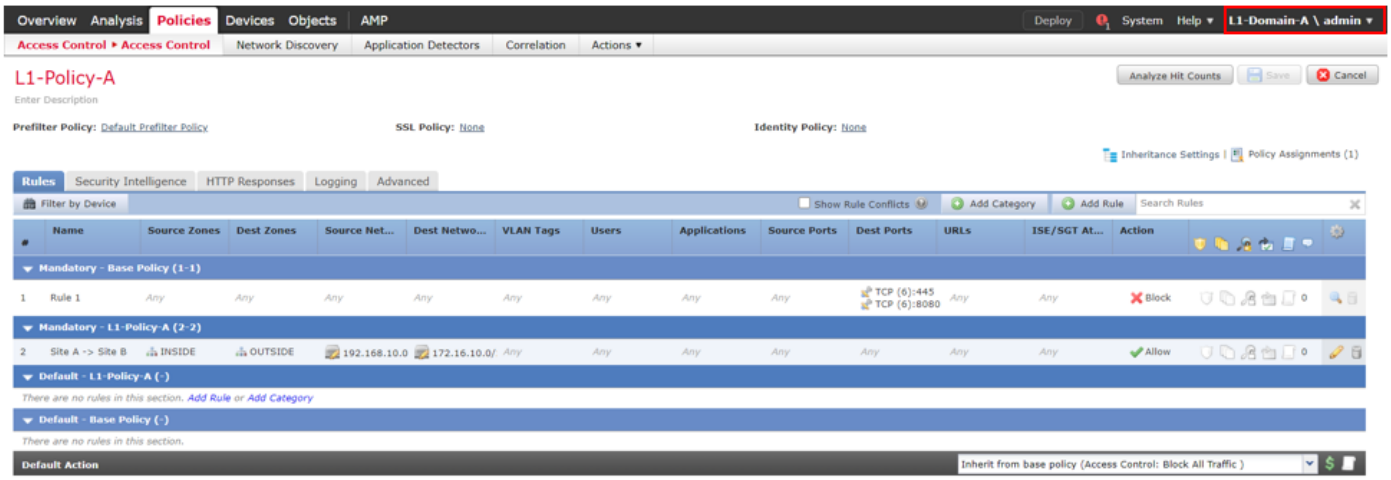


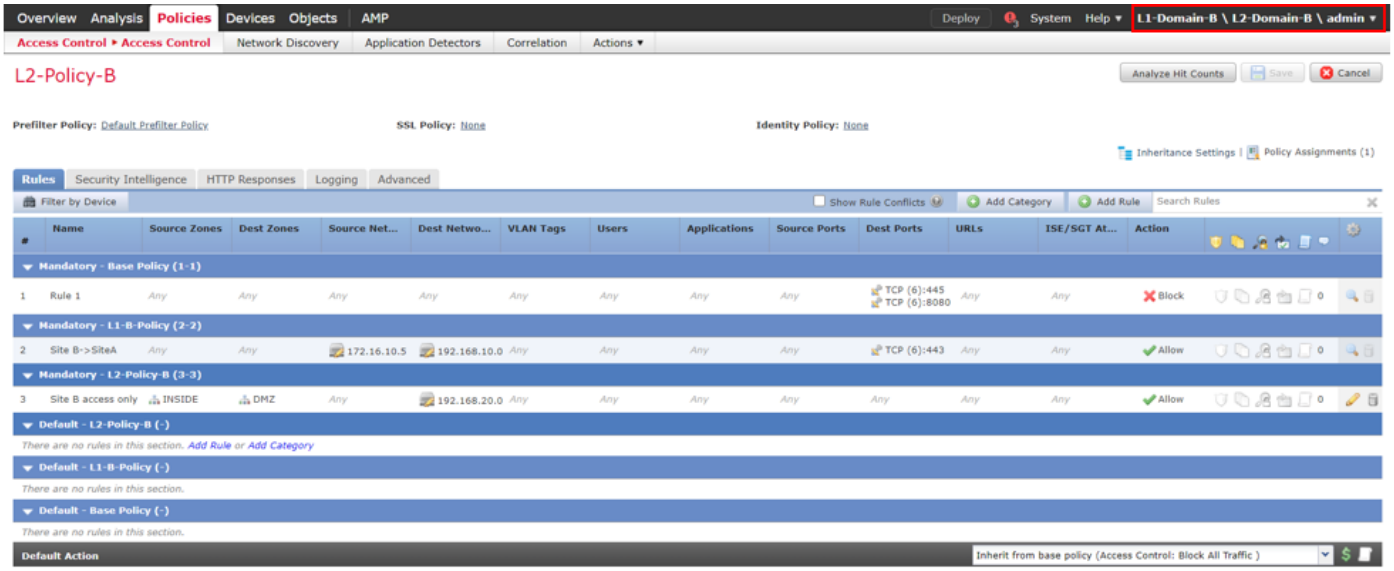
Die Struktur für die Domänenhierarchie ist wie folgt:

- **Die globale** Domäne ist **übergeordnet** von **L1-Domäne-A** und **L1-Domäne-B**.
- **Global** Domain ist **Vorfahren** von **L2-Domain-B**.
- **L2-Domain-B** ist das untergeordnete Element von **L1-Domain-B.**
- **L2-Domain-B** ist Leaf-Domäne, da sie keine untergeordneten Domänen hat.

Das Bild zeigt die Domänenhierarchie, wie im FMC dargestellt.

Der folgende Snapshot zeigt, wie die Regeln in **L1-Policy-A** und **L2-Policy-B** mit r.t für das obige Szenario definiert werden.





Bei der Konfiguration mehrerer Domänen sollten Sie immer die Regeln und deren Vererbung berücksichtigen, um zu verhindern, dass legitimer Datenverkehr blockiert oder unerwünschter Datenverkehr zugelassen wird.