Ereditarietà in ambienti multidominio in FTD

Sommario

Introduzione

In questo documento viene descritta la configurazione e l'utilizzo delle funzionalità di ereditarietà e a più domini. Viene inoltre illustrato un caso di utilizzo reale per verificare l'interazione tra le due funzionalità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

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

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Firepower Management Center (FMC) versione 6.4
- Software Firepower Threat Defense (FTD) versione 6.4

  Nota: Il supporto di funzionalità multidominio ed ereditarietà è disponibile su FMC/FTD a partire dalla versione 6.0.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dalla configurazione.

Premesse

In Ereditarietà criterio è possibile nidificare i criteri di controllo di accesso in cui i criteri figlio ereditano le regole da un criterio di base, incluse le impostazioni del provider di servizi di audioconferenza, ad esempio Security Intelligence, HTTP Response, Logging Settings e così via. Facoltativamente, l'amministratore può consentire al criterio figlio di ignorare le impostazioni del provider di servizi di audioconferenza, ad esempio Security Intelligence, HTTP Response, Logging Settings oppure di bloccare le impostazioni in modo che il criterio figlio non possa sostituirle. Questa funzionalità è molto utile in ambienti FMC multidominio.

La funzionalità multidominio consente di segmentare l'accesso utente ai dispositivi gestiti, alle configurazioni e agli eventi di FMC. Un utente potrebbe passare ad altri domini o accedervi, a seconda dei privilegi. Se la funzionalità multidominio non è configurata, tutti i dispositivi, le configurazioni e gli eventi gestiti appartengono al dominio **globale**.

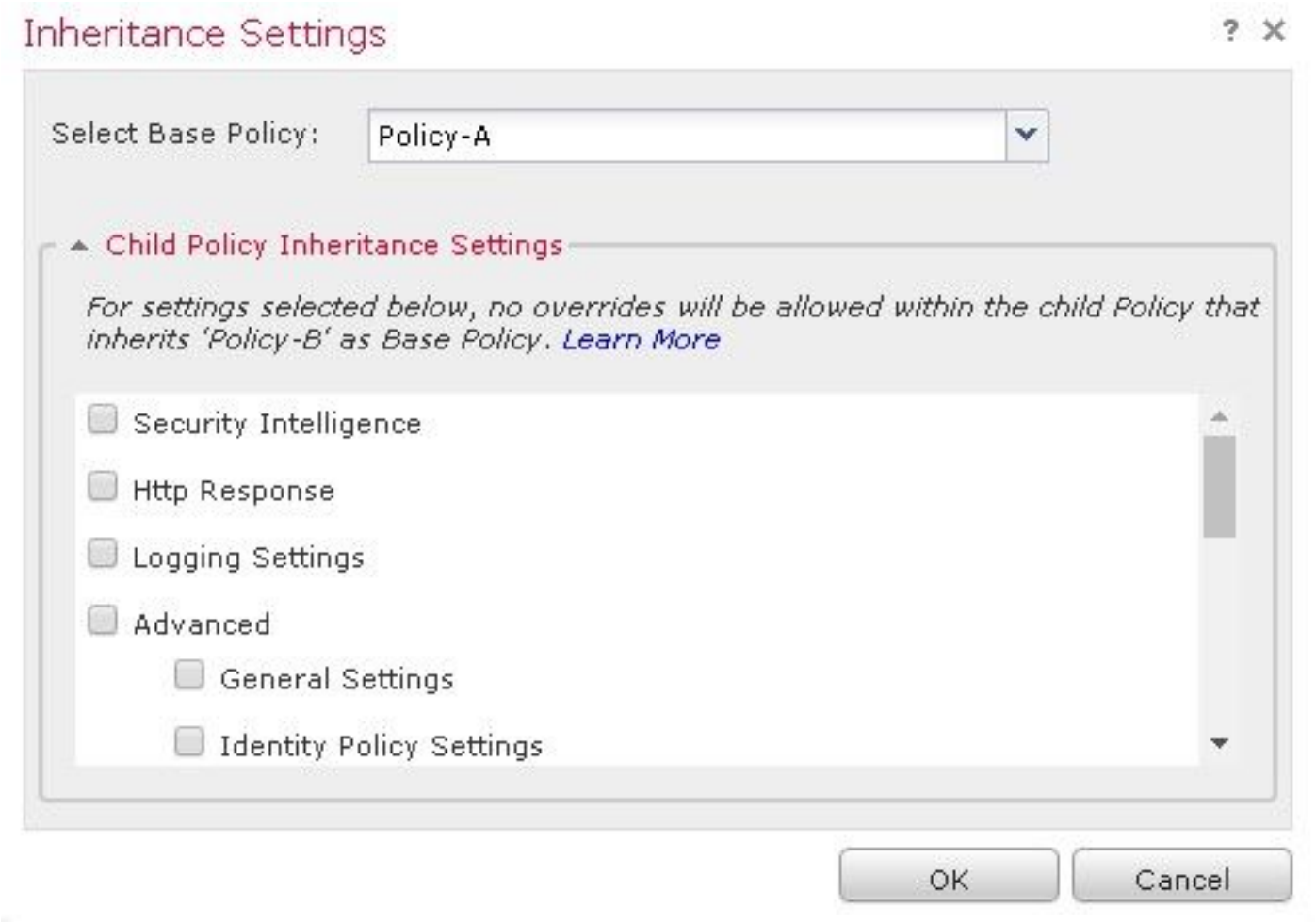
Configura ereditarietà criteri

Un dominio foglia è un dominio che non ha ulteriori sottodomini. Un dominio figlio è il discendente di livello successivo del dominio in cui si trova l'utente/amministratore. Il dominio padre è il predecessore diretto del dominio in cui si trova l'utente/amministratore.

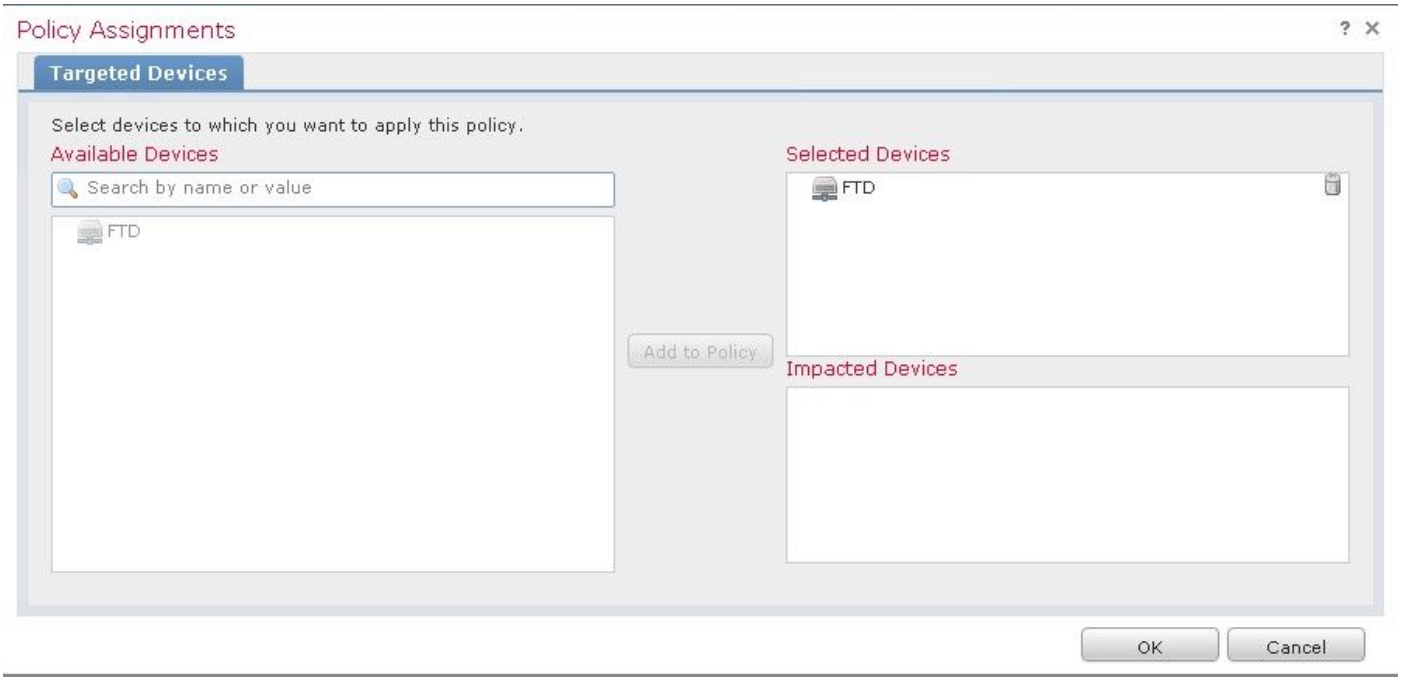
Per configurare/abilitare l'ereditarietà per i criteri esistenti:

1. Consentire a Policy-A di essere il criterio di base e Policy-B di essere il criterio figlio (Policy-B eredita la regola da Policy-A)
2. **EDIT** Policy-B e fare clic su **Inheritance Settings** come mostrato nell'immagine.

3. Scegliere Criterio-A dall'elenco a discesa **Seleziona criterio base** mostrato di seguito. Altre impostazioni del provider di servizi di audioconferenza, ad esempio Security Intelligence, HTTP Response, Logging Settings e così via, possono essere ereditate per sostituire facoltativamente le impostazioni del criterio figlio.

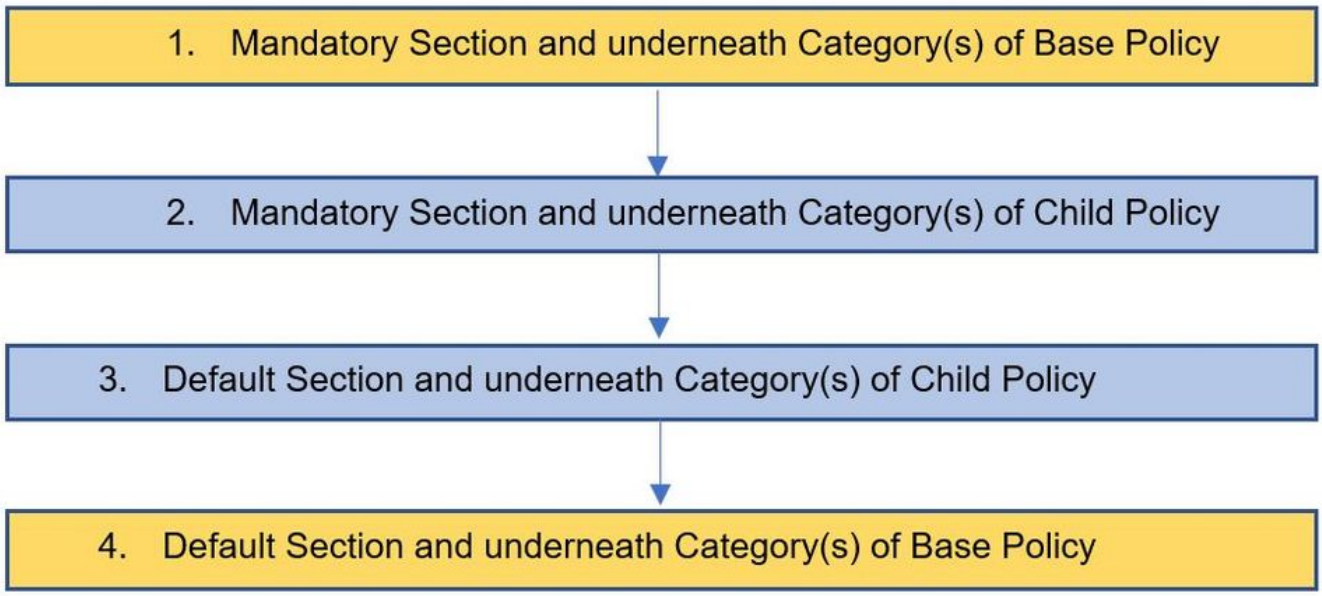


4. Eseguire l'**assegnazione dei criteri** per i criteri figlio Policy-B rispetto al dispositivo FTD di destinazione desiderato:

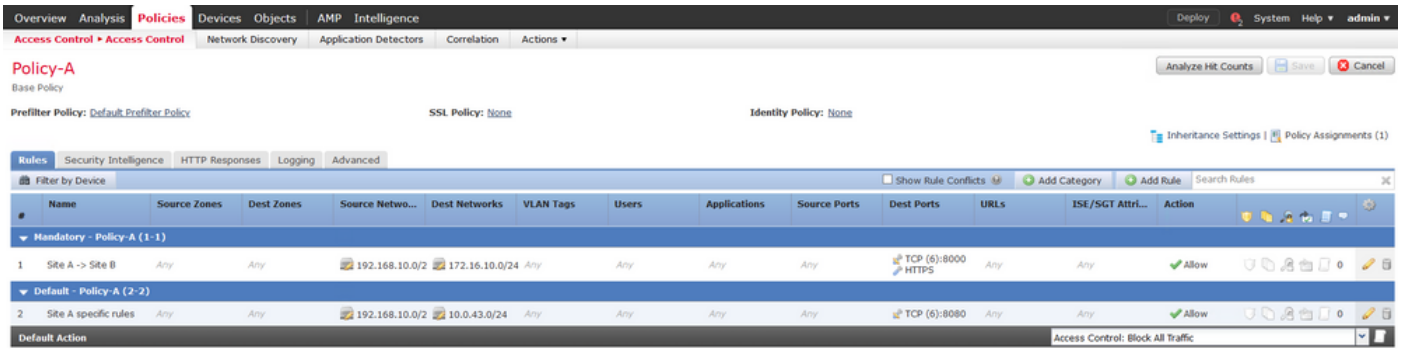


Per impostazione predefinita, l'**azione predefinita** del criterio figlio viene ereditata e impostata su **Eredita da criterio base**, come illustrato nell'immagine. L'utente ha anche la possibilità di selezionare l'**azione predefinita** dai criteri forniti dal sistema, come mostrato di seguito.

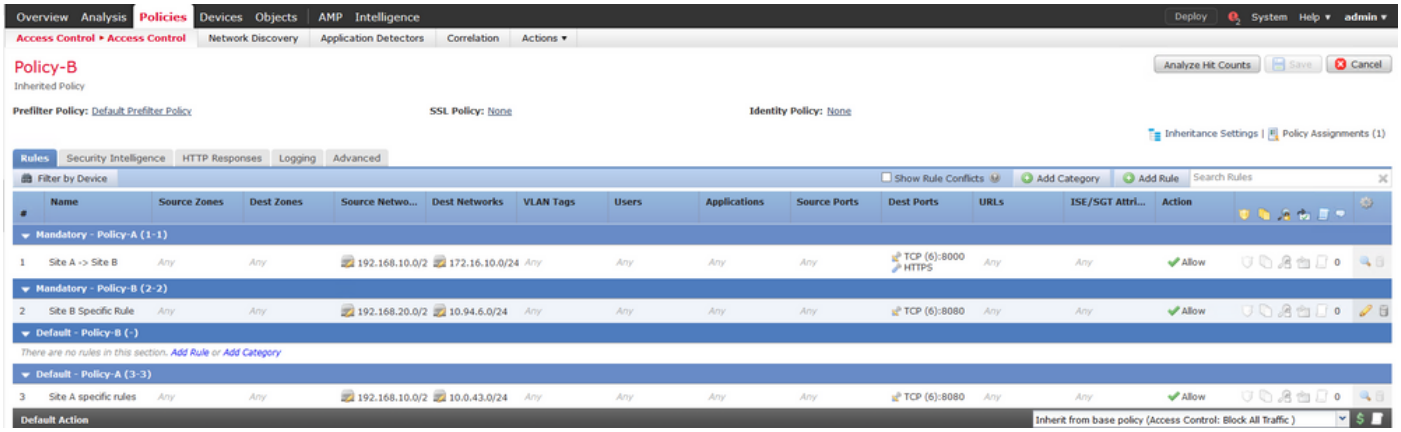
L'ordine di ricerca del traffico verrà sempre impostato in modo top-down indipendentemente dal numero di categorie aggiunte nelle sezioni Obbligatorio e Predefinito. Dopo aver applicato le **Impostazioni di ereditarietà,** la rappresentazione ACP per Criteri figlio-B (Criteri figlio) come illustrato nell'immagine, in linea con il **controllo Ordine delle regole** menzionato in precedenza:



In questa immagine viene mostrato come le politiche, ovvero la Politica A, che è la Politica di base, e la Politica B, che è la Politica figlio e che è ereditata dalla Politica A, vengono mostrate nel CCP.



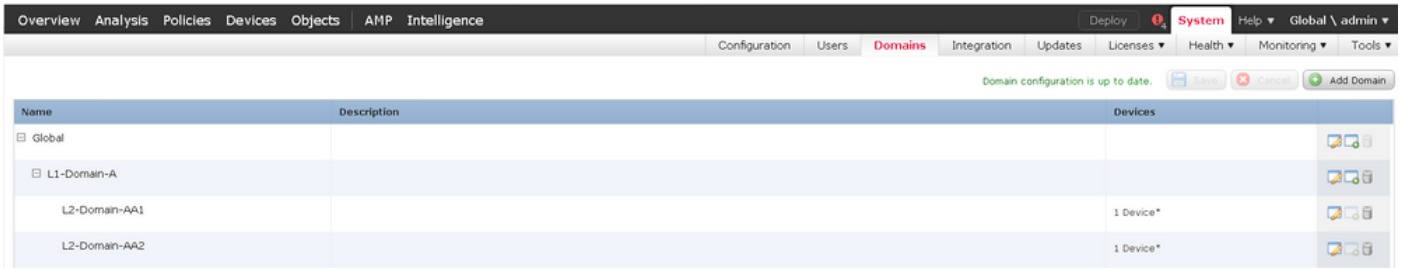
Nell'immagine viene mostrato che in Policy-B è possibile visualizzare le regole di Policy-A e le regole specifiche configurate in Policy-B. È necessario prestare attenzione alla modalità di configurazione delle regole tenendo presente l'ordine.



Gestione FTD in ambienti FMC multidominio

La funzionalità multidominio consente di segmentare l'accesso degli utenti a dispositivi, configurazioni ed eventi gestiti. Un utente potrebbe passare ad altri domini a seconda dei privilegi. Se la funzionalità multidominio non è configurata, tutti i dispositivi, le configurazioni e gli eventi gestiti appartengono al dominio **globale**.

È possibile configurare un massimo di domini a tre livelli con il dominio globale come livello uno. Tutti i dispositivi gestiti devono appartenere solo al dominio foglia. Ciò può essere confermato dal simbolo  (Aggiungi sottodominio) disattivato nel dominio foglia come mostrato nell'immagine.



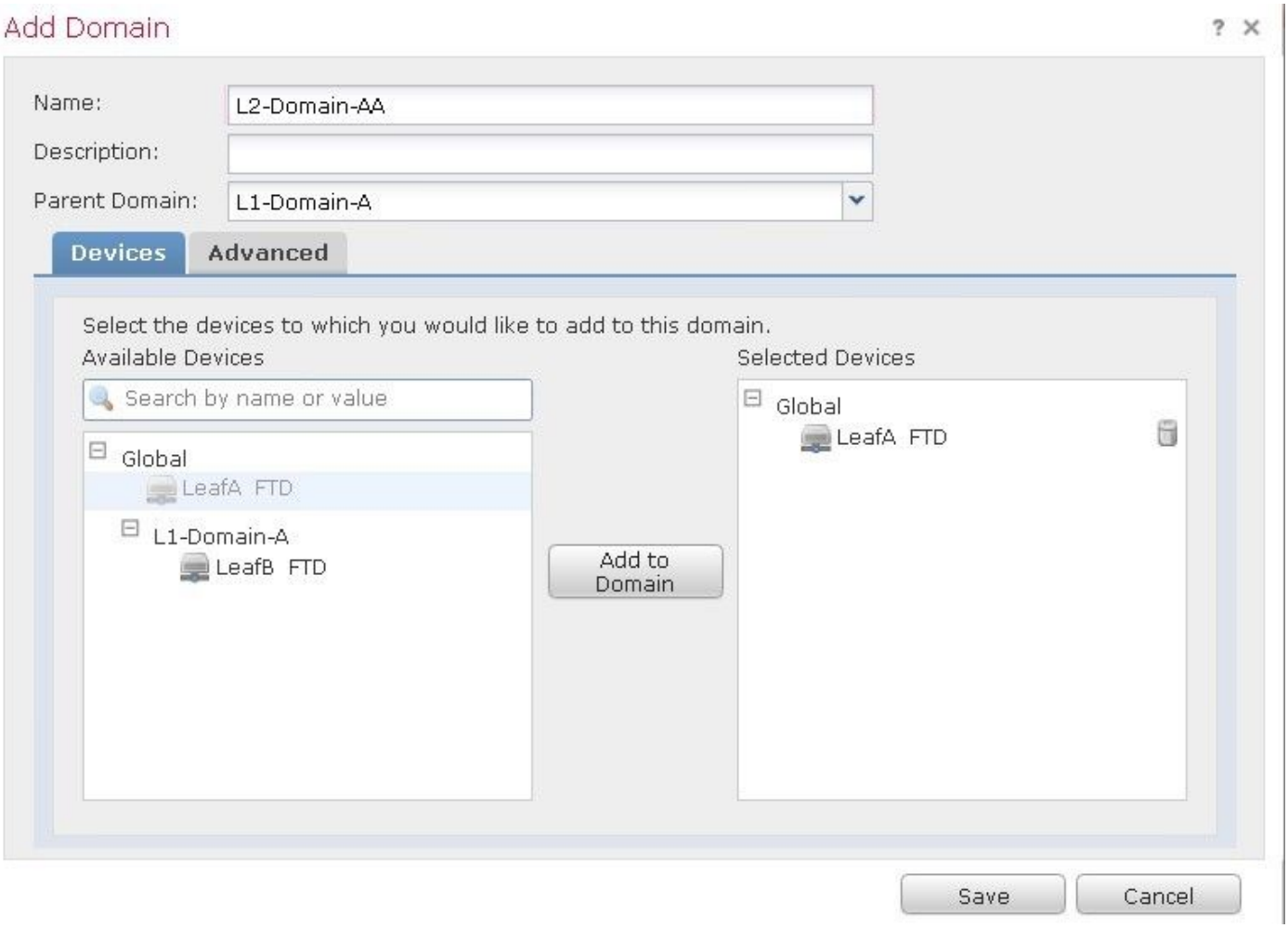
Configurazione dominio

La configurazione del dominio può essere effettuata come segue:

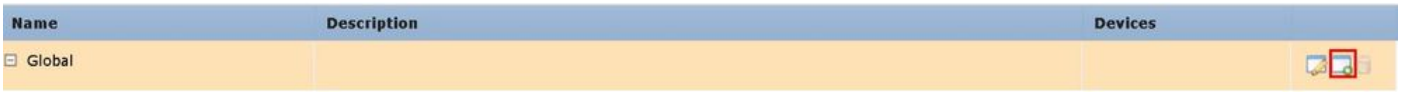
1. Passare a **Sistema > Domini**. Per impostazione predefinita, è presente il dominio **globale**.

2. Fare clic su **Add Domain** (Aggiungi dominio) come mostrato nell'immagine.

3. Viene visualizzata la finestra di dialogo **Aggiungi dominio**. Digitare il **Nome** del dominio e selezionare il **Dominio padre** dall'elenco a discesa. Se questo è il dominio foglia, i dispositivi FTD devono essere aggiunti al dominio come mostrato nell'immagine.

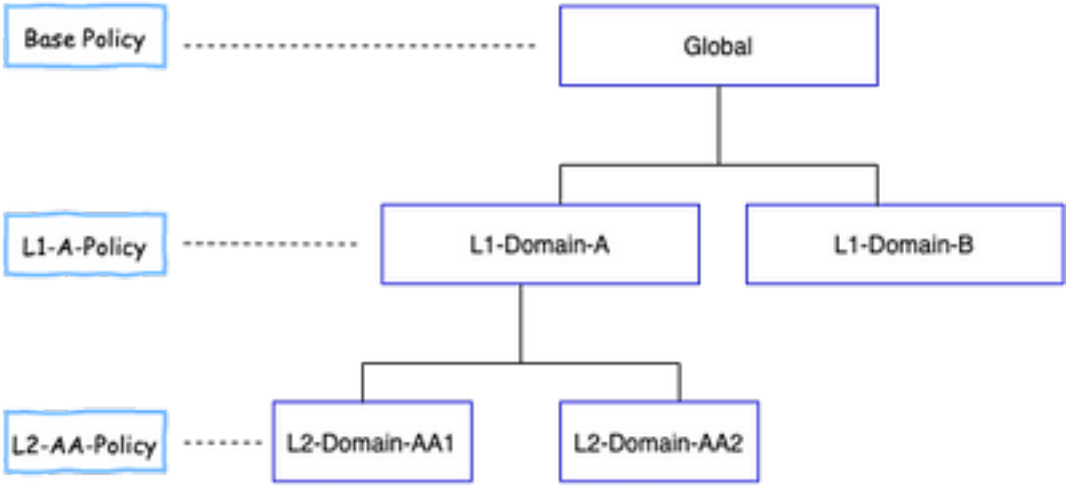


Nota: Per aggiungere i domini, fare clic sull'icona **Add Sub Domain** (Aggiungi sottodominio) come mostrato nell'immagine. Il dominio padre è già selezionato.



Visibilità e controllo delle policy in un ambiente FMC multidominio

La visibilità e il controllo dei criteri sono limitati ai rispettivi utenti del dominio, ad eccezione di un amministratore del dominio **globale**. Questo esempio si basa sulla gerarchia come segue:



Visibilità: Come mostrato in questa immagine, la pagina predefinita Visualizza **criteri** elenca i criteri configurati nel rispettivo dominio.

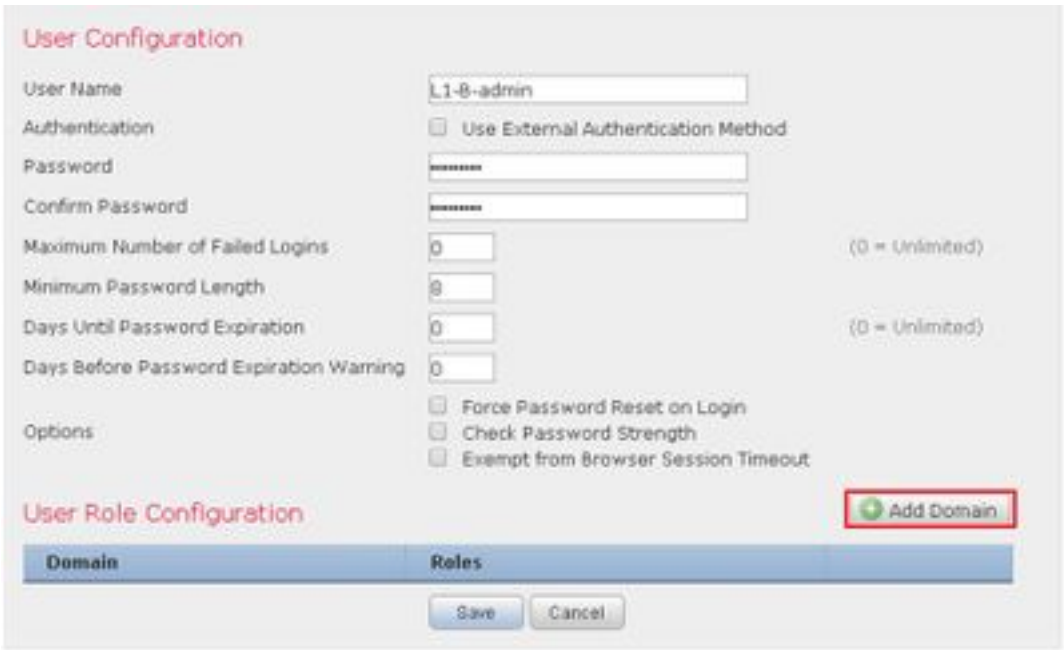
Controllo: Gli utenti **amministratori** che appartengono al rispettivo dominio possono MODIFICARE i criteri. Per modificare i criteri, che appartengono ad altri domini (ad esempio come parte dell'ereditarietà), è necessario passare dal dominio corrente a quello in cui è configurato il criterio. Solo gli utenti amministratori appartenenti al dominio **globale** o al dominio L1 possono passare al dominio inferiore per la gestione dei criteri.

Aggiungi utenti al dominio

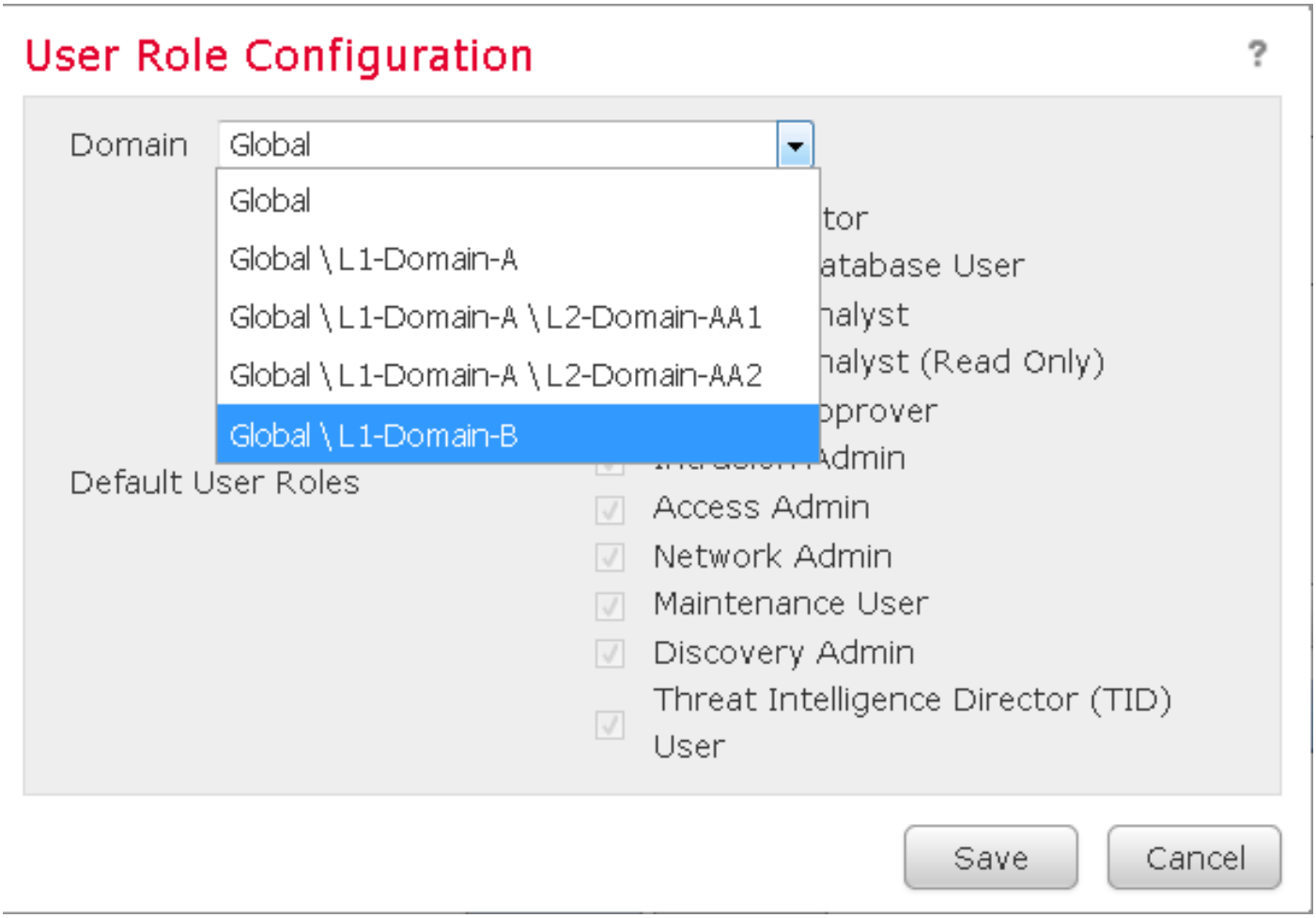
In questo esempio viene illustrato come aggiungere utenti in un dominio specifico. Questa procedura è applicabile agli utenti del database locale.

1. Passare a **Sistema > Utenti**. Fare clic su **Create User** (Crea utente) come mostrato nell'immagine.

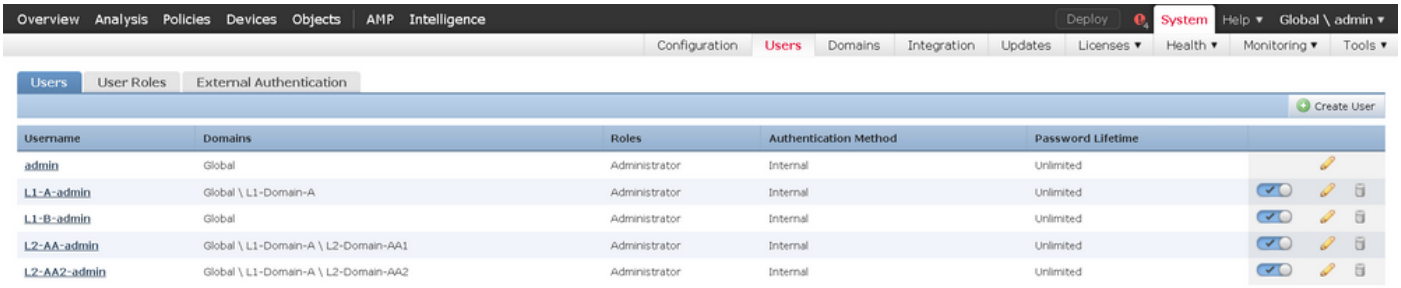
2. Viene visualizzata la finestra di dialogo **Configurazione utente**. Immettere il **nome utente** e la **password (& Conferma password)**. Fare clic su **Add Domain** (Aggiungi dominio) per aggiungere l'utente al dominio specificato, come mostrato nell'immagine.



3. Scegliere il dominio desiderato dall'elenco a discesa **Dominio** in cui si desidera aggiungere l'utente e specificare il ruolo come mostrato nell'immagine. È possibile aggiungere un nuovo utente al proprio dominio o ai domini figlio.



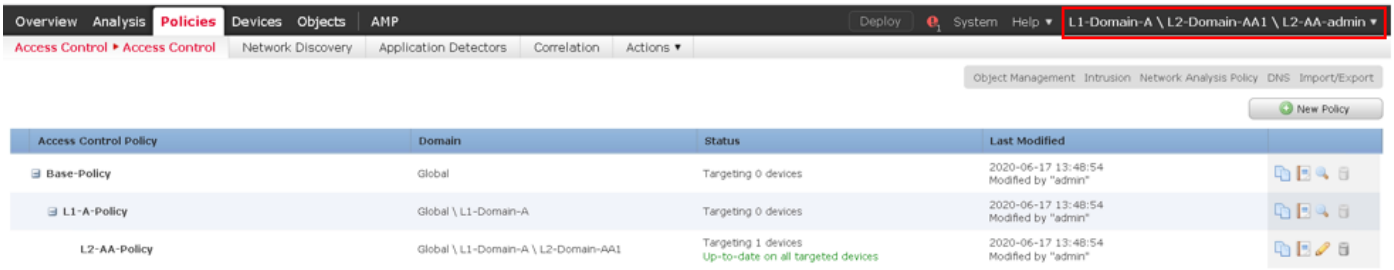
Gli utenti configurati sono mostrati in questa immagine:



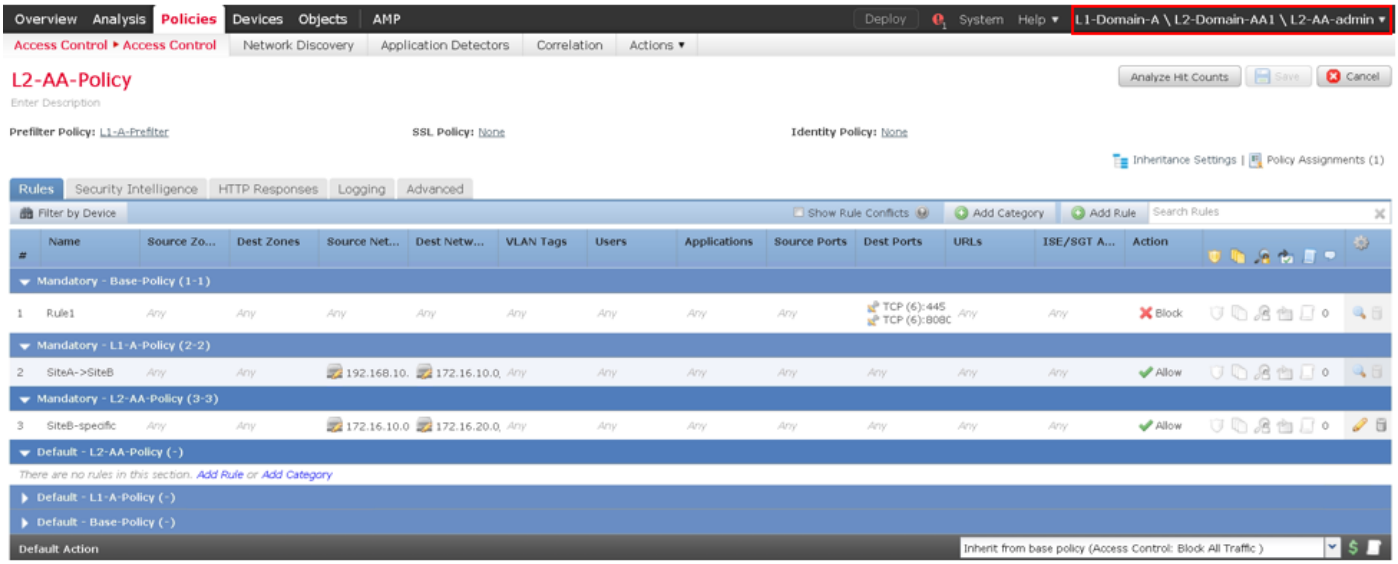
L'accesso alle risorse in FMC sarebbe limitato al dominio a cui appartiene l'utente. Come illustrato di seguito, quando l'utente **L1-A-admin** accede all'interfaccia utente di FMC, l'accesso è limitato al dominio **L1-Domain-A di** cui l'utente fa parte e al dominio figlio una volta che l'utente passa a tale dominio figlio. Questo utente può modificare solo il criterio definito nel dominio **L1-Domain-A** e il criterio definito nel dominio figlio quando il dominio viene passato al relativo dominio figlio. Inoltre, dall'esempio riportato di seguito si può vedere che **L1-A-Policy** eredita il criterio definito nel dominio globale, ovvero **Base-Policy,** e può essere modificato, come si può vedere dal firma. Le impostazioni di ereditarietà sono impostate in modo da puntare a **Base-Policy**, come mostrato nell'immagine.

Analogamente, un utente **L2-AA-admin** appartenente al dominio **L2-Domain-AA1** ha solo il

controllo del criterio **L2-AA-Policy** definito nel dominio, come mostrato nell'immagine. Il criterio **L2-A** eredita il criterio **L1-A-Policy** definito in **L1-Domain-A** che a sua volta eredita il criterio **base** definito nel dominio globale. Inoltre, il criterio **L2-AA-Policy** può essere modificato, come mostrato nella firma. L'utente L2-AA-admin non può mai passare al dominio padre, ovvero L1-Domain-A, né al dominio predecessore, ovvero il dominio globale.



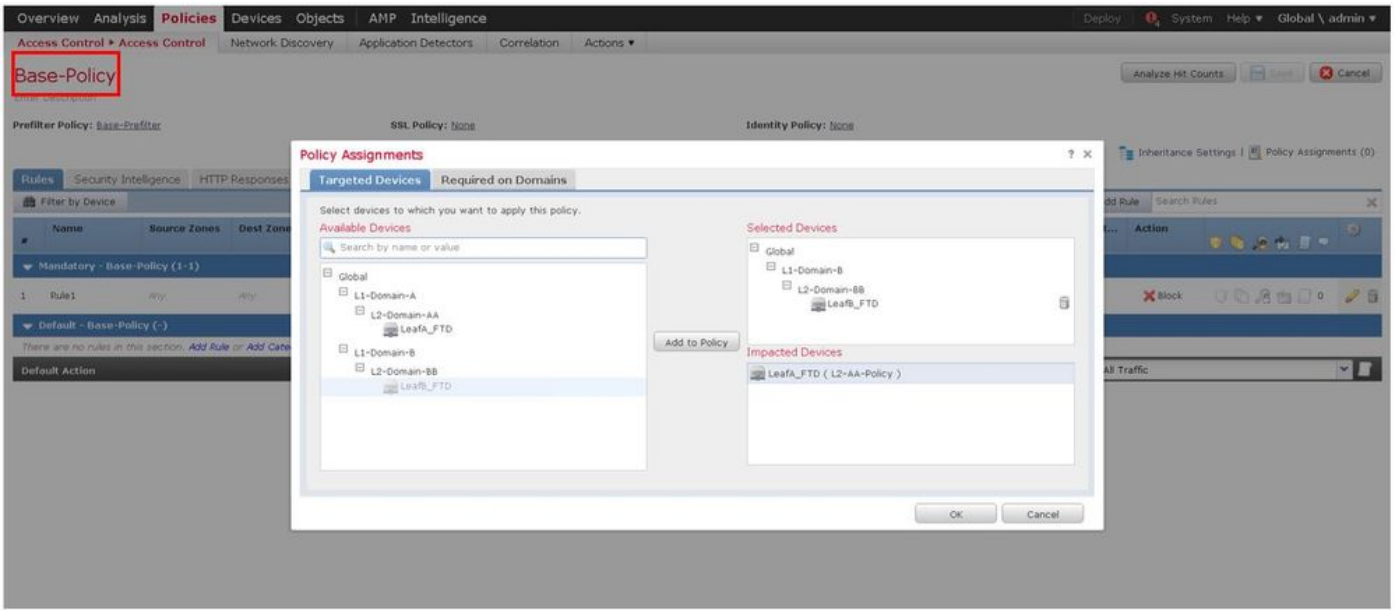
Inoltre, un utente **L1-A-admin** appartenente a L1-Domain-A può passare a L2-Domain-A1 e modificare il criterio **L2-A-Policy** che è visibile da come mostrato nell'immagine. Ciò è valido anche per un utente appartenente al dominio globale che passa ai domini figlio e modifica i criteri definiti nel dominio figlio specifico.



Punti importanti da notare:

- Quando si eliminano i domini non globali, gli utenti appartenenti ai domini vengono automaticamente spostati nel dominio **globale**.

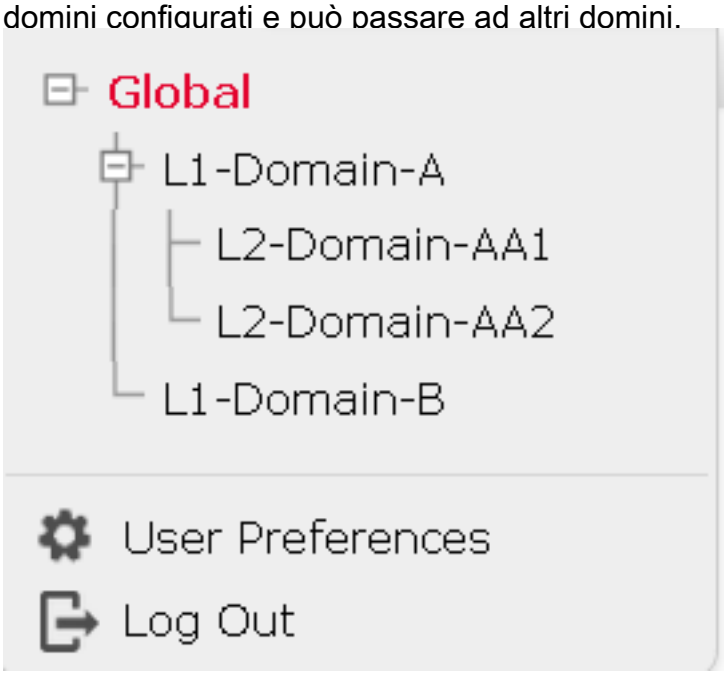
  Gli FTD sono sempre definiti nel dominio foglia. In questo caso, il dominio foglia è il dominio **L2**(cioè L2-Domain-AA e L2-Domain-BB). L'FTD appartenente al **dominio L2** può essere assegnato al criterio nel **dominio L1** o nel dominio **globale**. In questa immagine, il provider di servizi di audioconferenza nel dominio globale ha assegnato l'FTD definito nel dominio L3 al criterio definito nel dominio globale.



- Gli utenti del dominio globale possono passare ad altri domini specifici dell'utente, ma gli utenti di un dominio specifico hanno visibilità solo nel proprio dominio e nei relativi domini figlio. Non possono passare al dominio globale o a domini di livello superiore, come mostrato nella tabella seguente:

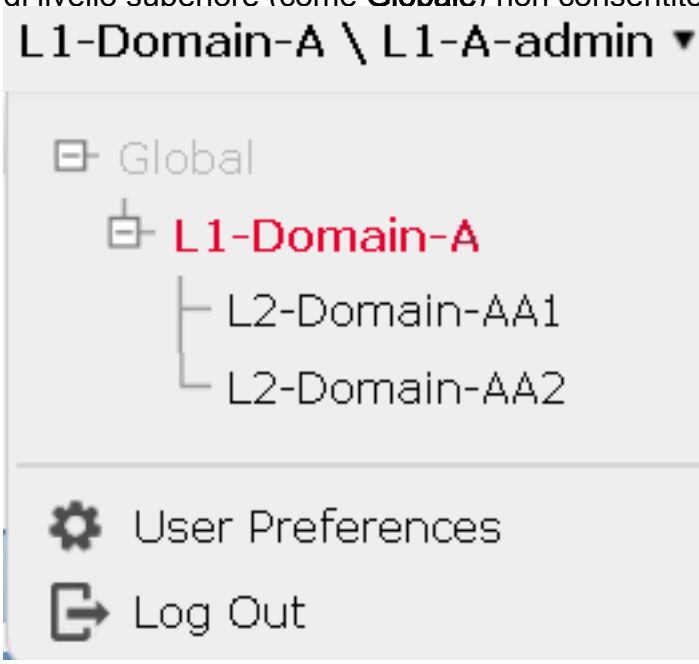
Dominio globale

L'utente nel dominio globale ha visibilità su tutti i domini configurati e può passare ad altri domini.

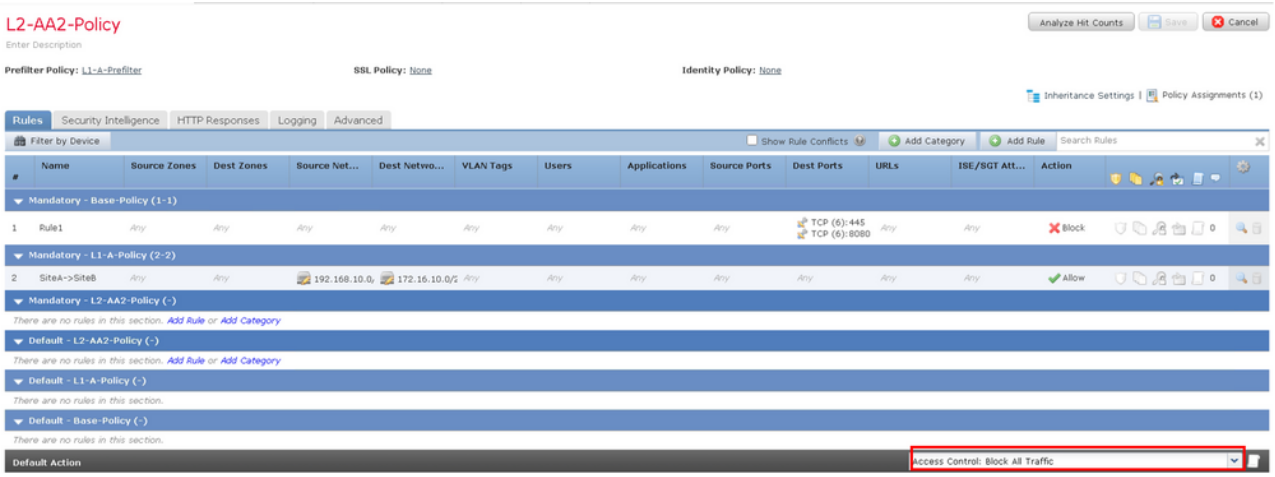


Dominio specifico dell'utente

L'utente in **L1-Domain-A** avrà visibilità solo su se stesso e sul relativo dominio figlio, ovvero **L2-Dor A** e potrà passare a **L2-Domain-A**. Accesso al do di livello superiore (come **Globale**) non consentito



- L'azione predefinita del criterio figlio non può essere bloccata dal criterio padre e l'utente non deve ereditare l'azione predefinita del criterio padre come in questa immagine.



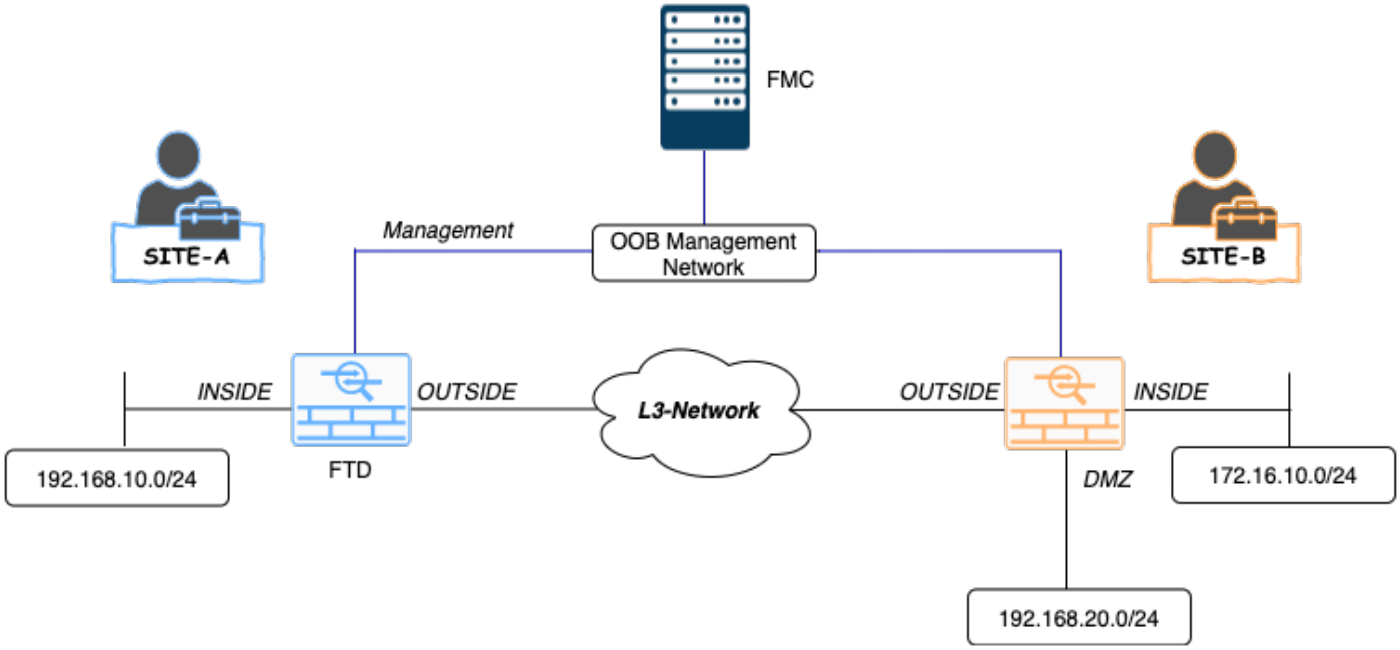
In questa immagine è possibile vedere che l'utente non ha assegnato l'azione predefinita come quella del padre, come si evince dalle parole **Eredita da criterio di base:** non visualizzato nell'azione predefinita.

Nota: È necessario tenere presente che un utente non può visualizzare contemporaneamente entrambi i criteri di dominio L1/L2. L'utente deve passare al dominio desiderato per visualizzare e modificare i criteri. Ad esempio: se l'utente **admin** presente nel dominio globale desidera visualizzare i criteri configurati in L1-Domain-A e L2-Domain-A, l'utente può farlo passando a L1-A-Domain per visualizzare e modificare i criteri configurati in tale dominio e quindi passando a L2-Domain-A per visualizzare e modificare i criteri corrispondenti, ma non può visualizzare entrambi contemporaneamente. Inoltre, l'utente in L1-Domain-A non può modificare o eliminare i criteri definiti nel dominio globale, ad esempio i criteri di base, che sono i criteri padre di L1-A-Policy, e l'utente in L2-Domain-A non può modificare o eliminare i criteri, ovvero i criteri di base e L2-A-Policy, definiti rispettivamente nei domini globali e L2-Domain-A.

Scenario Use Case

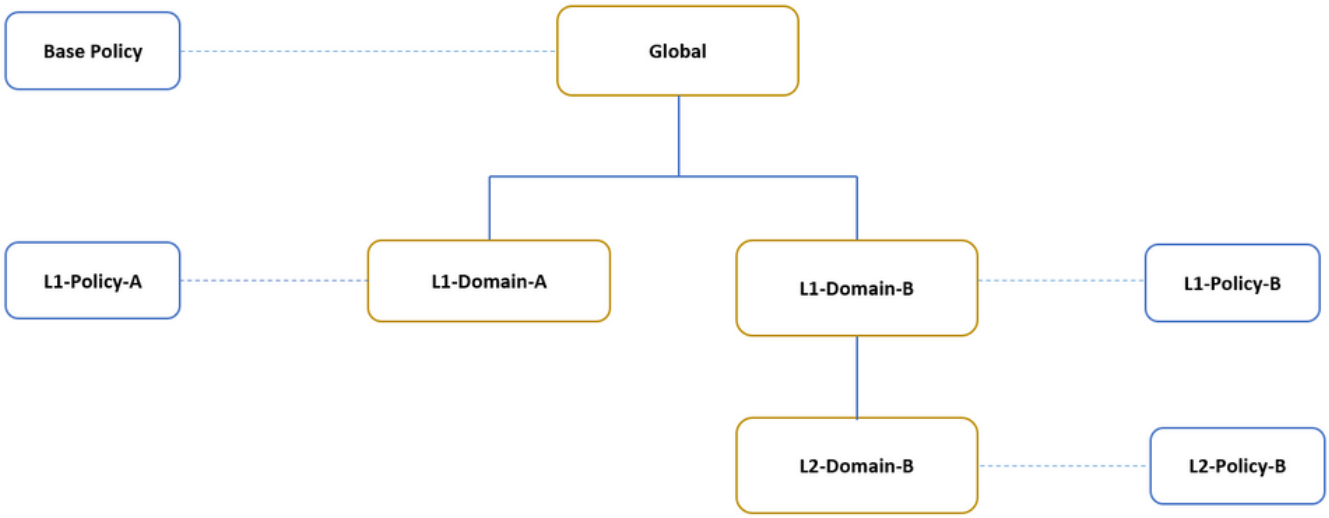
Si consideri lo scenario illustrato nell'immagine, i FTD del SITO A (sito A-FTD) e del SITO B (sito B-FTD) sono gestiti da un singolo FMC attraverso domini diversi (multidominio) per fornire accesso controllato. Dal punto di vista delle politiche, queste sono le considerazioni relative alle politiche a livello di organizzazione:

- Le regole di BLOCCO specifiche del servizio applicabili a TUTTI gli FTD indipendenti dal SITO o dal DOMINIO appartengono a (Criterio di base).
- Regole che soddisfano i requisiti per l'accesso da Sito A a Sito B (L1-Policy-A) e da Sito B a Sito A (L1-Policy-B).
- Regole applicabili all'FTD del sito B (L2-Policy-B).



Ereditarietà in un ambiente a più domini

Per il caso di utilizzo sopra indicato, considerare la seguente gerarchia di dominio/criteri. Il sito A-FTD e il sito B-FTD fanno parte rispettivamente dei domini foglia L1-Dominio-A e L2-Dominio-B.

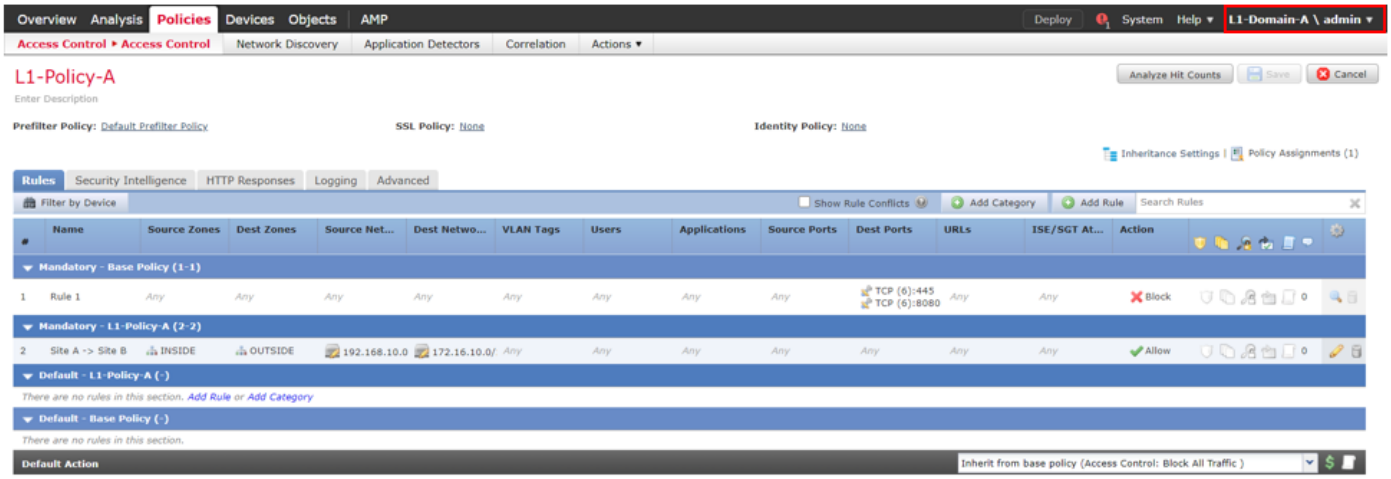


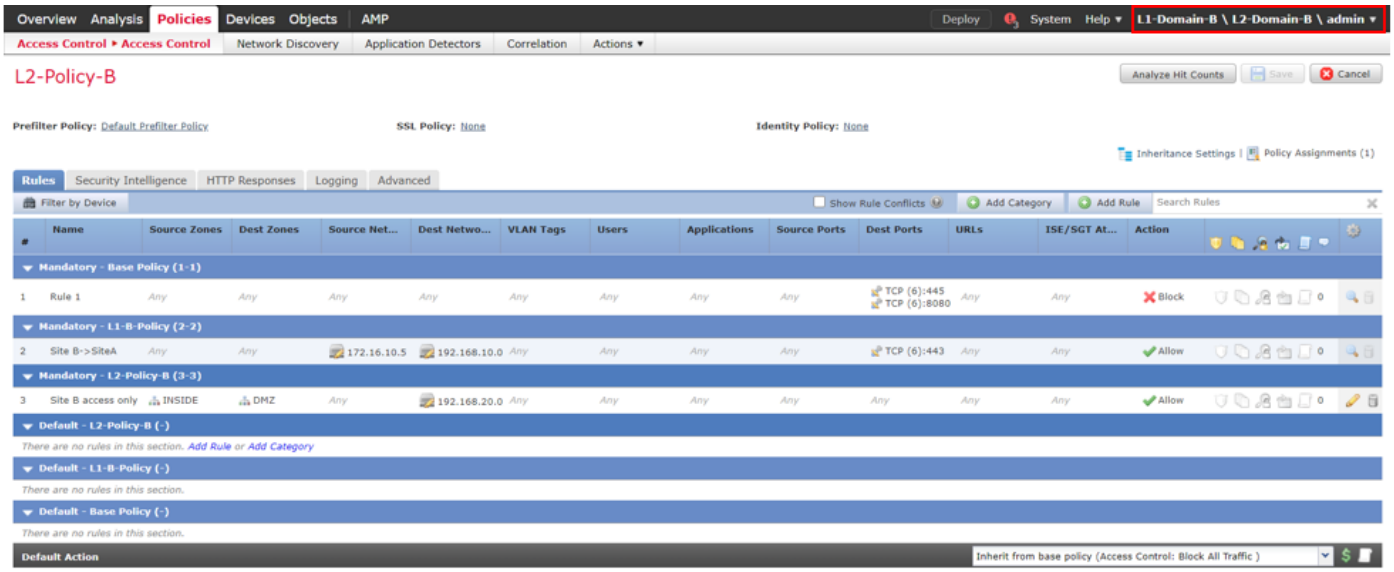
La struttura della gerarchia dei domini è la seguente:

- Il dominio **globale** è **padre** di **L1-Domain-A** e **L1-Domain-B**.
- Il dominio **globale** è **predecessore** di **L2-Domain-B**.
- **L2-Domain-B** è figlio di **L1-Domain-B**
- **L2-Domain-B** è un dominio foglia perché non ha domini figlio.

Nell'immagine è illustrata la gerarchia dei domini visualizzata da FMC.

L'istantanea seguente mostra come le regole vengono definite in **L1-Policy-A** e **L2-Policy-B** w.r.t per lo scenario precedente.





Quando si configurano più domini in modo da evitare il blocco del traffico legittimo o il traffico indesiderato, è necessario tenere sempre in considerazione le regole e la relativa ereditarietà.