

Configurare i criteri di identità in Centro gestione firewall sicuro

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazioni](#)

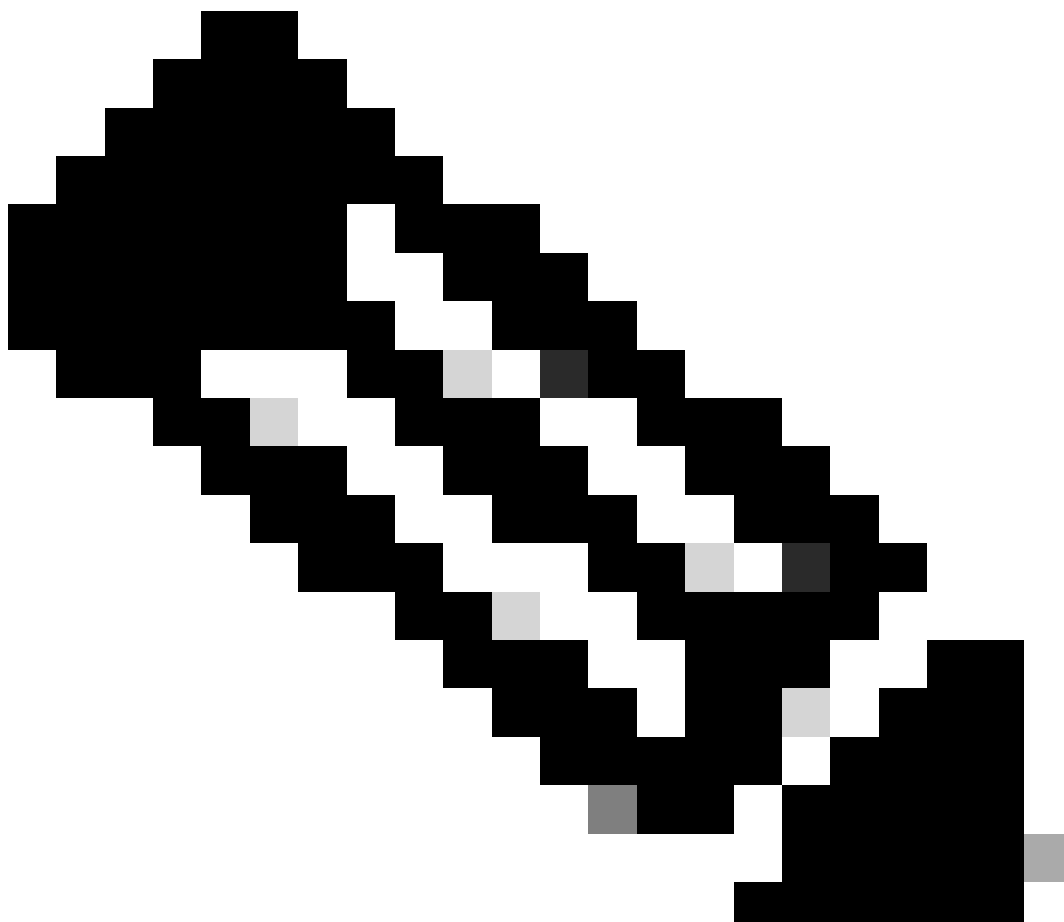
[Verifica](#)

Introduzione

In questo documento viene descritto il processo di configurazione e distribuzione di un criterio di identità per un traffico FTD sicuro tramite Secure FMC.

Prerequisiti

1. Realm già configurato in FMC.
2. Identity Source già configurato - ISE, ISE-PIC.



Nota: le istruzioni per la configurazione di ISE e Realm esulano dall'ambito di questo documento.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Centro gestione firewall protetto (FMC)
- Secure Firewall Threat Defense (FTD)
- Cisco Identity Services Engine (ISE)
- Server LDAP/AD
- Metodi di autenticazione

1. Autenticazione passiva: utilizzo di un'origine utente di identità esterna, ad esempio ISE
2. Autenticazione attiva: utilizzo del dispositivo gestito come origine di autenticazione (portale captive o accesso vpn remoto)

3. Nessuna autenticazione

Componenti usati

- Secure Firewall Management Center per VMWare v7.2.5
- Cisco Secure Firewall Threat Defense per VMWare v7.2.4
- Server Active Directory
- Patch 4 di Cisco Identity Services Engine (ISE) v3.2
- Metodo di autenticazione passiva

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 dall'uso dei comandi.

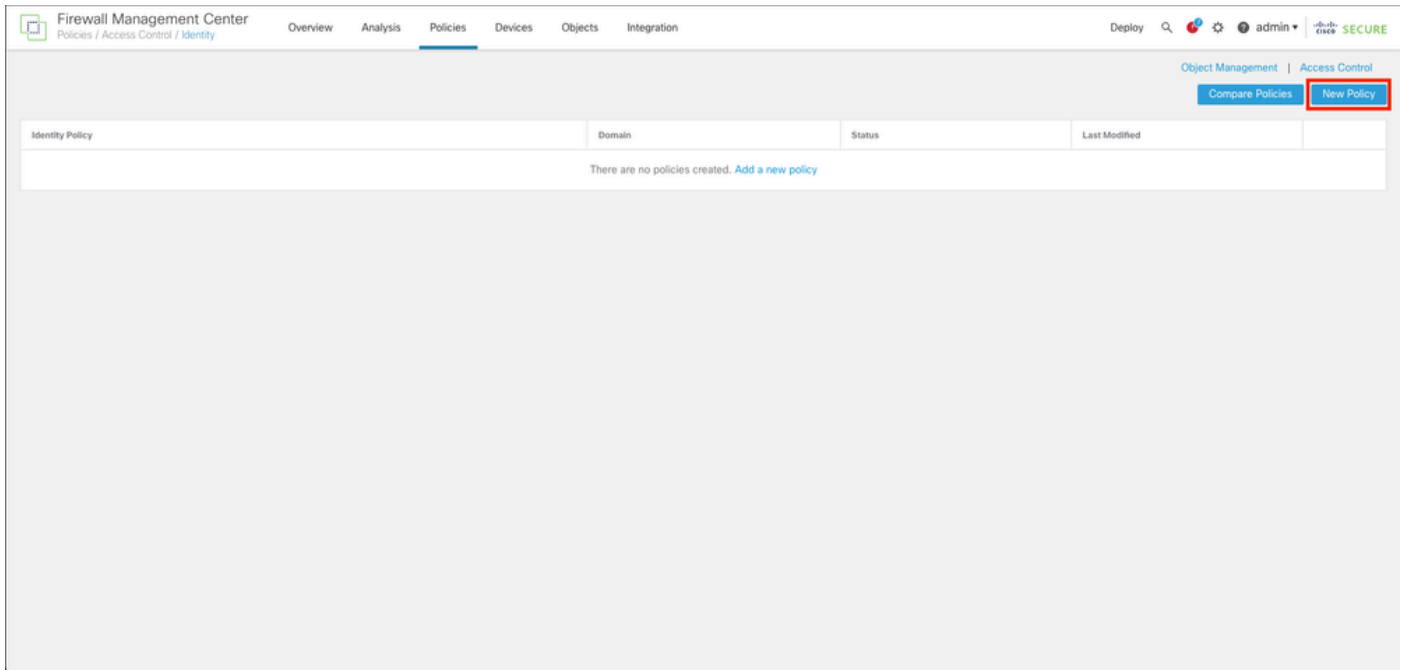
Configurazione

Configurazioni

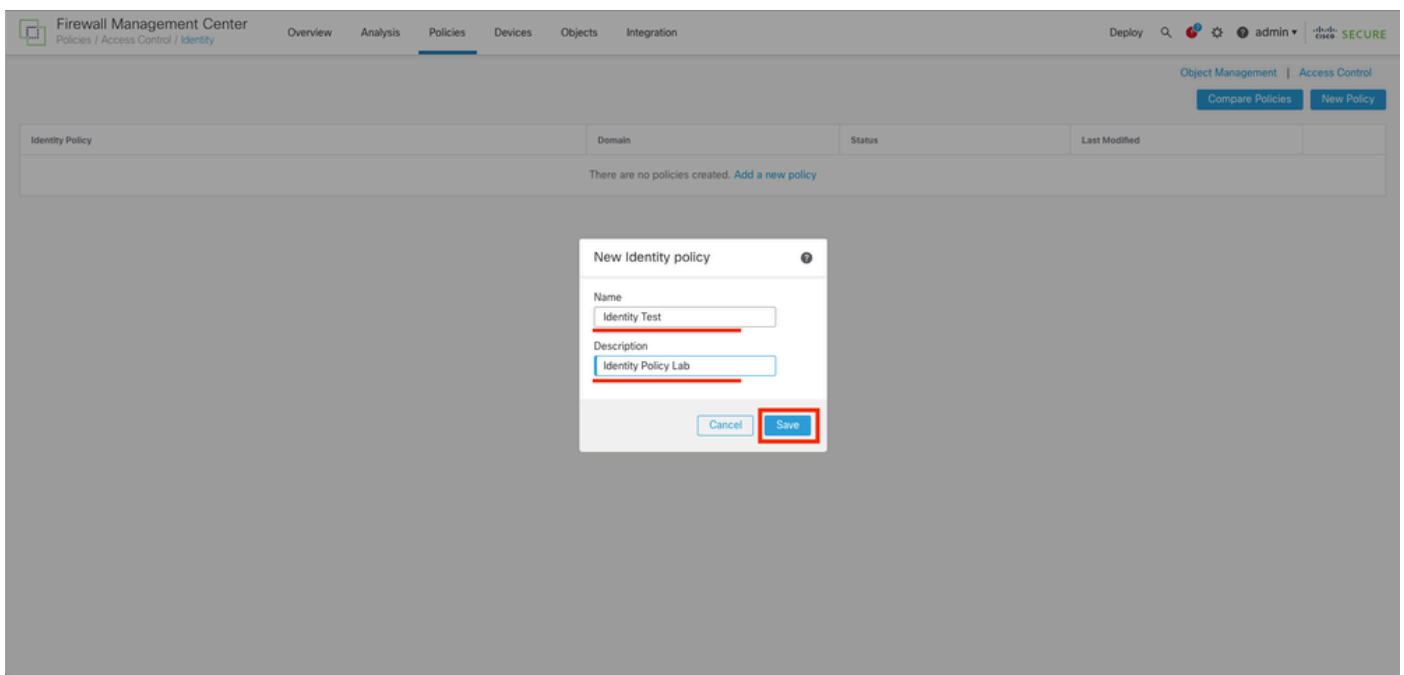
Passaggio 1. Nell'interfaccia utente di FMC, selezionare Policies > Access Control > Identity (Policy > Controllo accesso > Identità)

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Policies' menu is expanded, showing sub-menus: 'Access Control', 'Network Discovery', 'Actions', 'Access Control', 'Application Detectors', 'Alerts', 'Intrusion', 'Correlation', 'Scanners', 'Malware & File', 'Groups', 'DNS', 'Modules', 'Identity', 'Instances', 'SSL', and 'Prefilter'. The main dashboard area shows a 'Summary Dashboard' with various widgets: 'Unique Applications over Time' (line graph), 'Traffic by Application Risk' (horizontal bar chart), 'Traffic by Business Relevance' (horizontal bar chart), 'Top Client Applications Seen' (horizontal bar chart), and 'Top Server Applications Seen' (No Data). The 'Top Client Applications Seen' widget shows data for Cisco Secure Endpoint (63.33 KB), Kerberos (6.46 KB), DCE/RPC (5.02 KB), and Emap (1.20 KB).

Passaggio 2. Fare clic su Nuovo criterio.

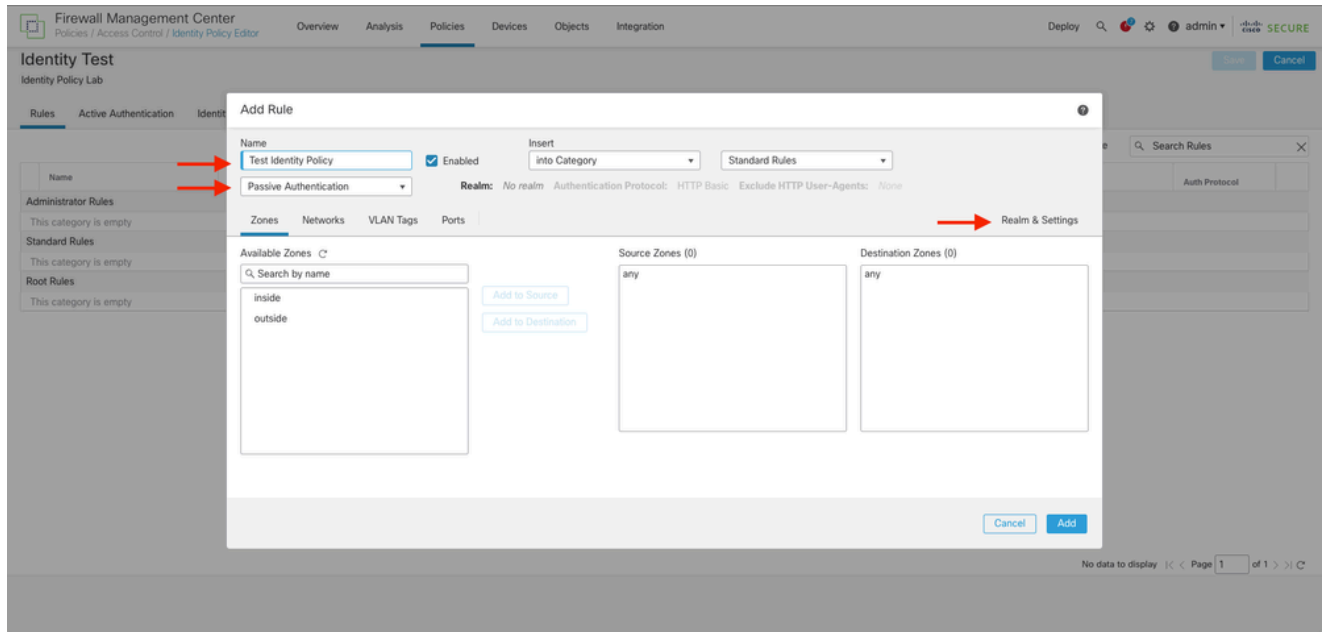


Passaggio 3. Assegnare un nome e una descrizione al nuovo criterio di identità, quindi fare clic su Salva.

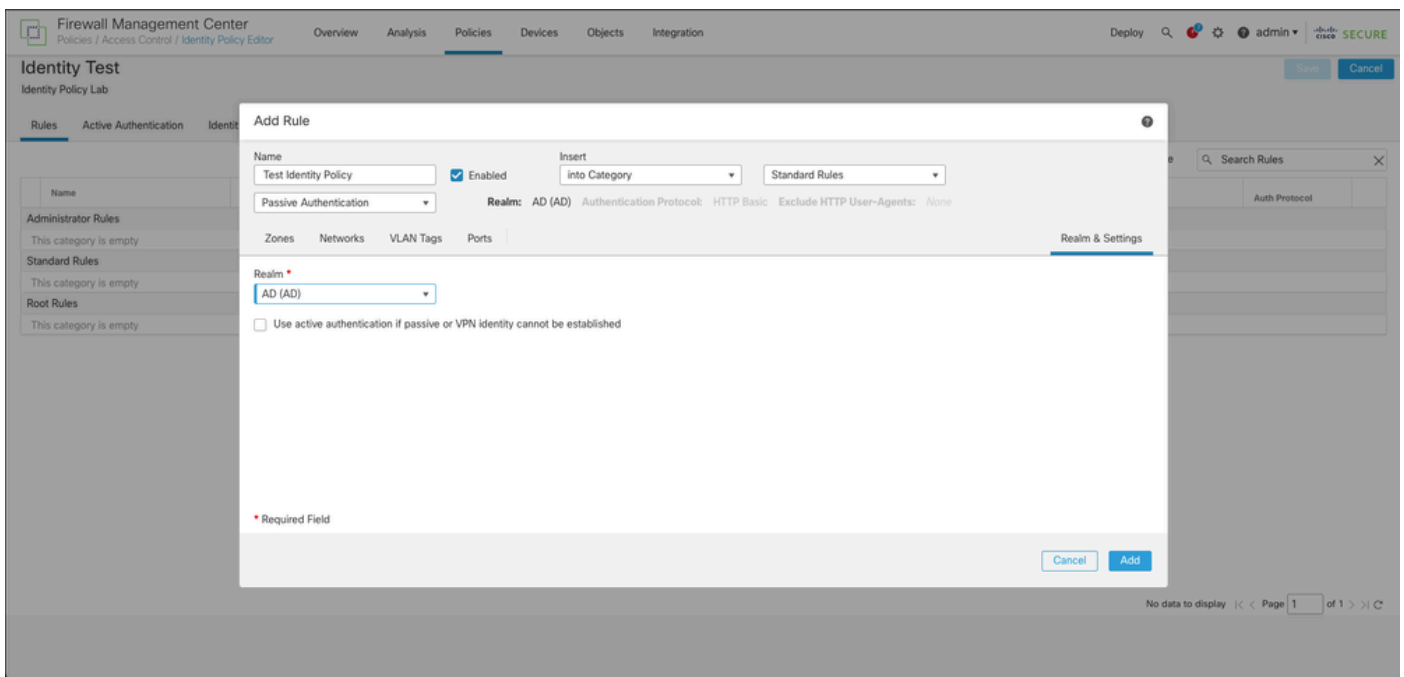


Passaggio 4. Fare clic su + Aggiungi icona regola.

1. Assegnare un nome alla nuova regola.
2. Sotto il campo del nome, scegliere il metodo di autenticazione, selezionare: Autenticazione passiva.
3. Nella parte destra dello schermo, selezionare Realm & Settings.



4. Selezionare un realm dal menu a discesa.



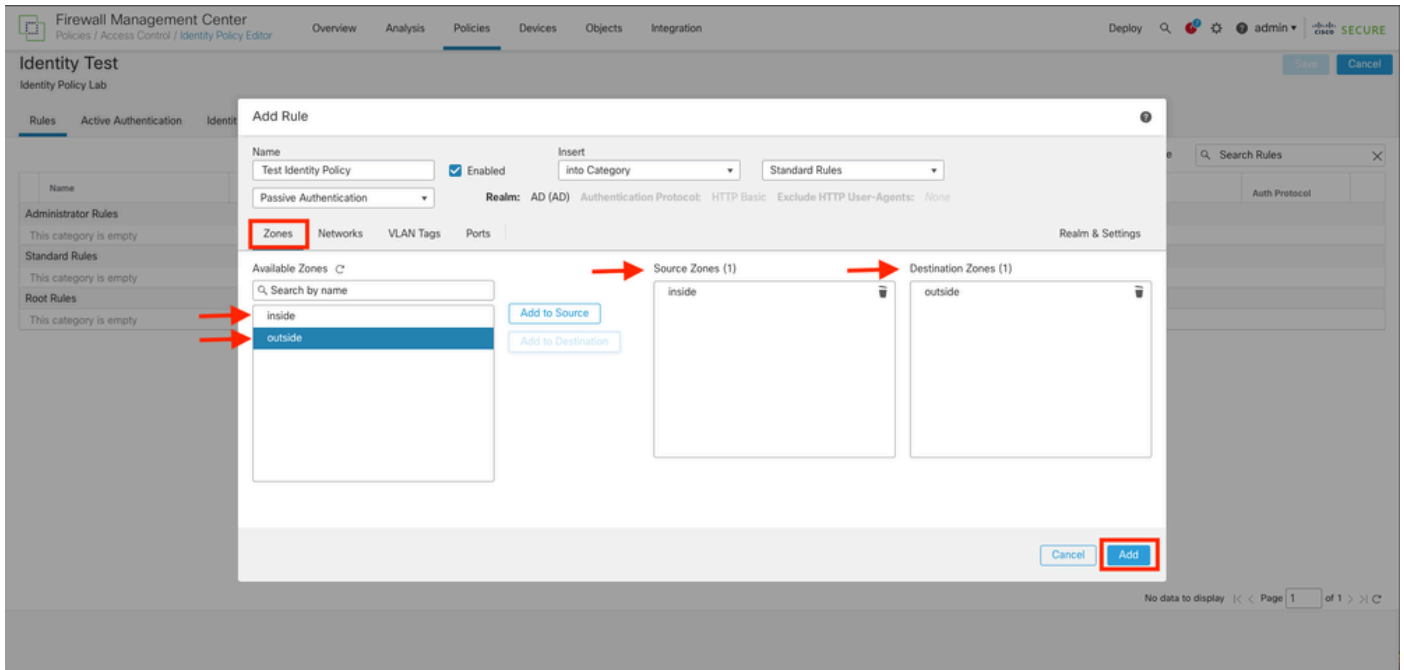
5. Fare clic su Zones a sinistra dello schermo.

6. Dal menu Zone disponibili, assegnare una zona di origine e di destinazione basata sul percorso del traffico necessario per rilevare gli utenti. Per aggiungere una zona, fare clic sul nome della zona e selezionare a seconda del caso Aggiungi a origine o Aggiungi a destinazione.

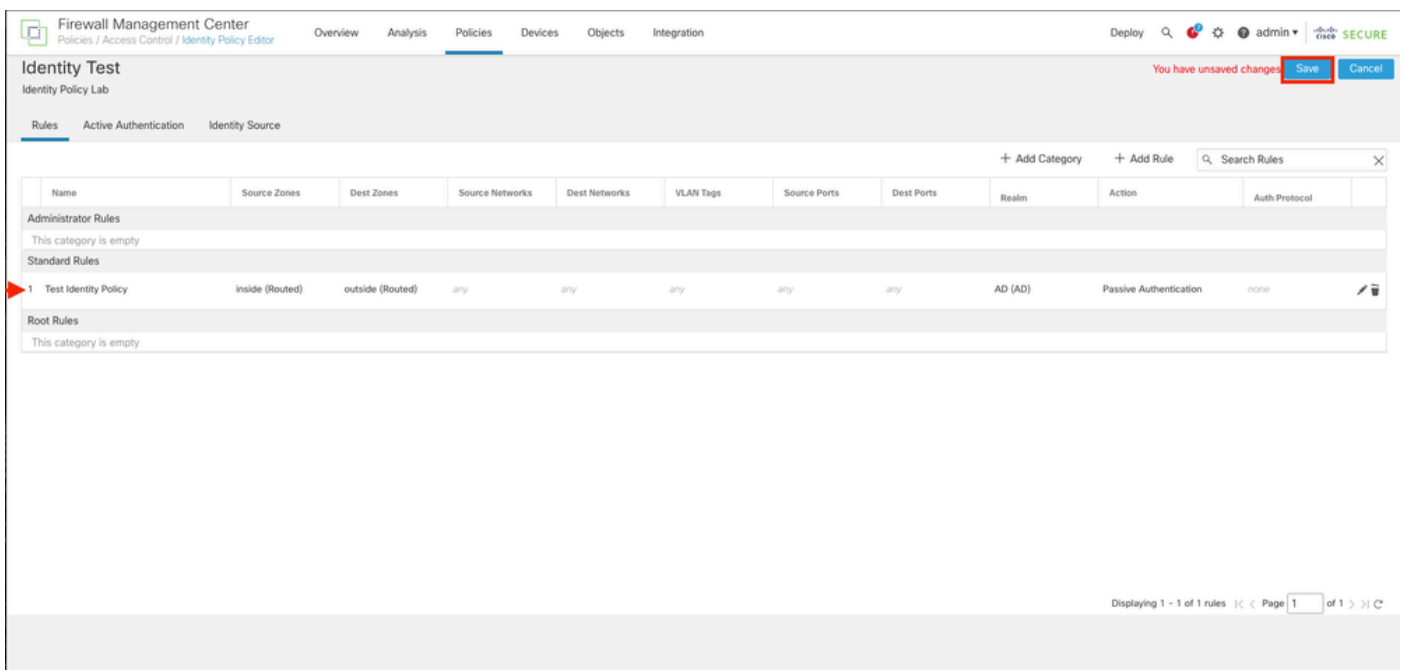


Nota: in questa documentazione il rilevamento da parte dell'utente verrà applicato solo al traffico proveniente dalla zona interna e inoltrato alla zona esterna.

7. Selezionare Aggiungi e Salva.

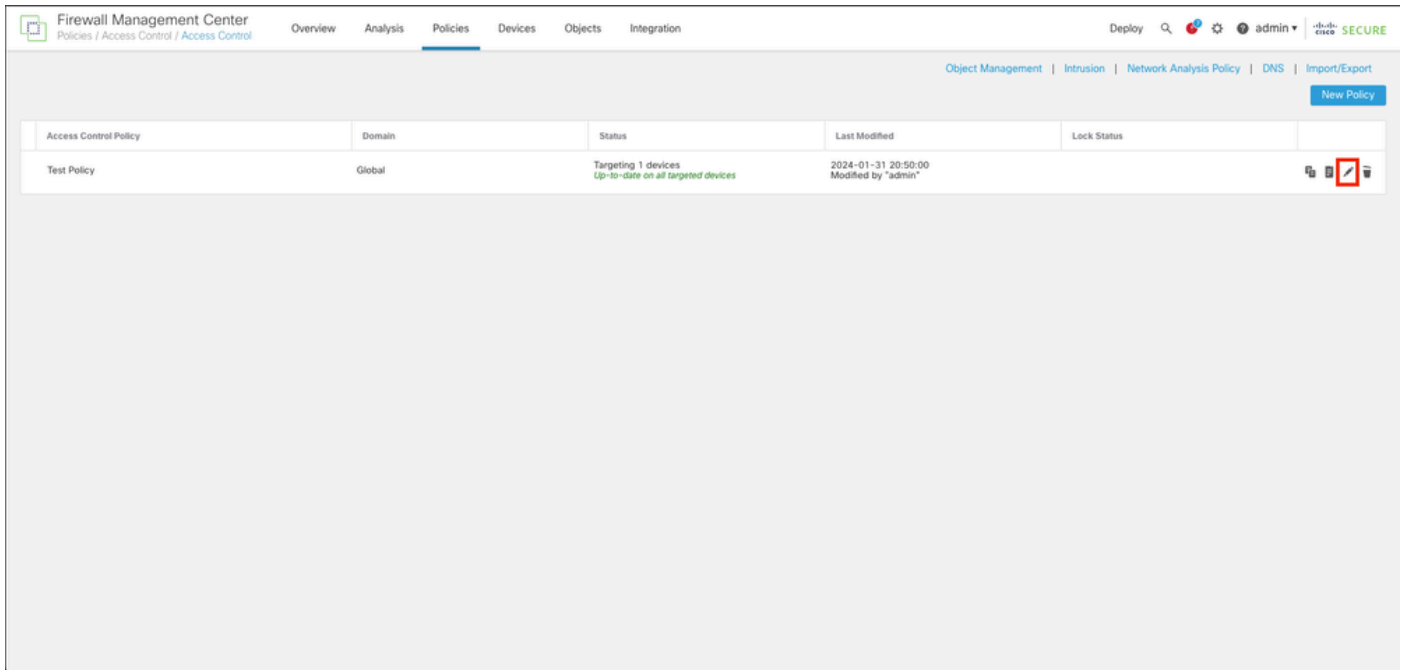


Passaggio 5. Verificare che la nuova regola sia presente nel criterio di identità e fare clic su Salva.

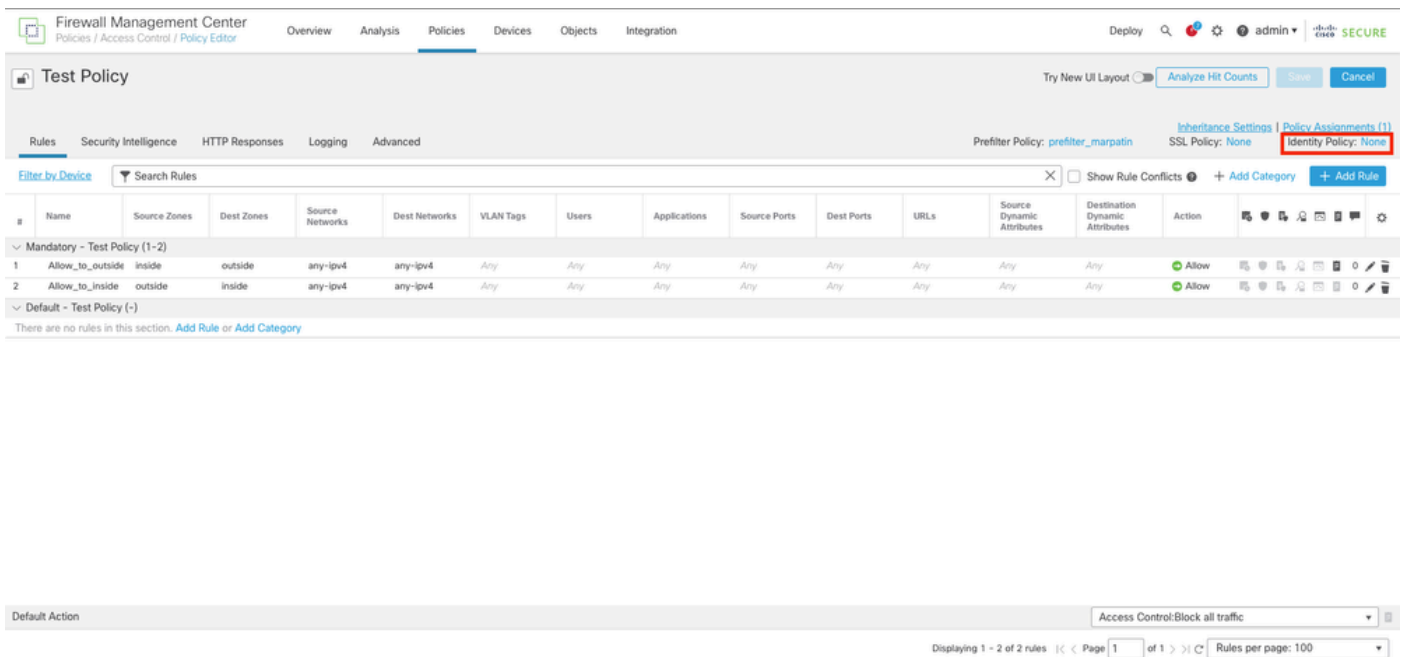


Passaggio 6. Passare a Criteri > Controllo accesso

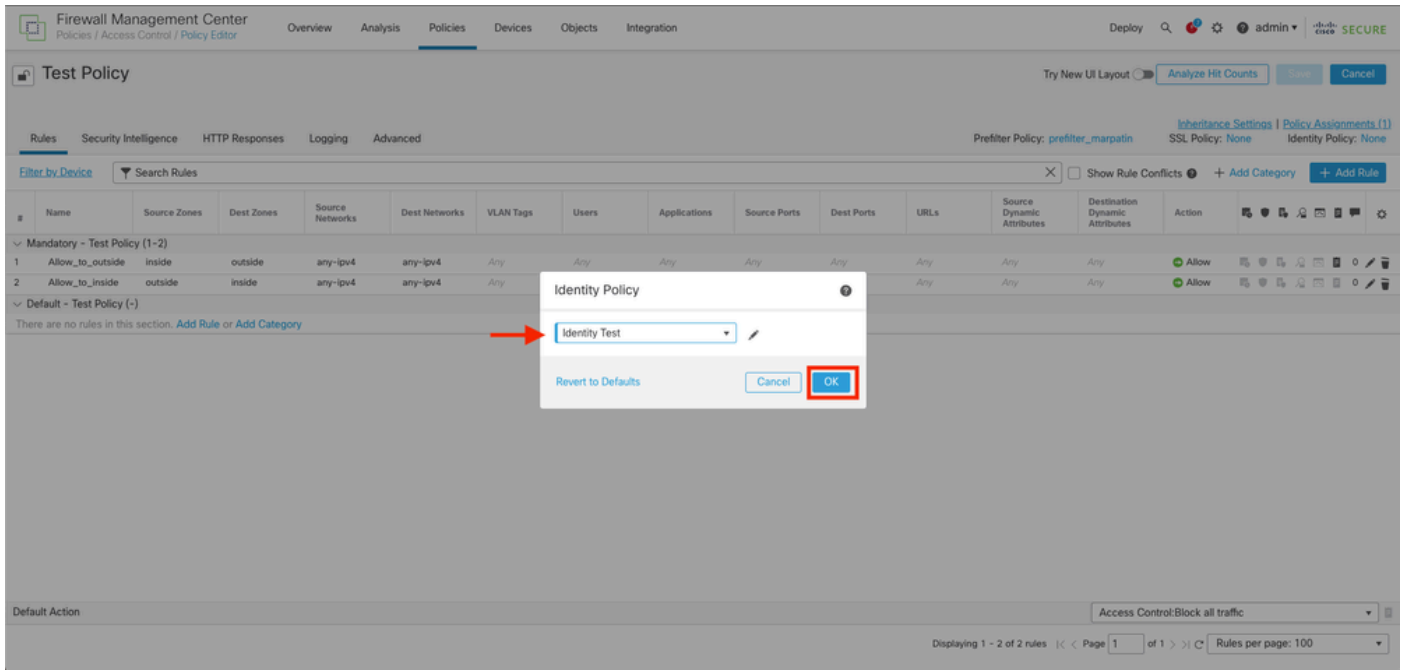
Passaggio 7. Identificare i criteri di controllo di accesso che verranno distribuiti nel firewall che gestisce il traffico degli utenti e fare clic sull'icona della matita per modificare i criteri.



Passaggio 6. Fare clic su None (Nessuno) nel campo Identity Policy (Criteri di identità).



Passaggio 7. Dal menu a discesa, selezionare il criterio creato in precedenza nel passaggio 3, quindi fare clic su OK per completare la configurazione.



Passaggio 8. Salvare e distribuire la configurazione nell'FTD.

Verifica

1. Nell'interfaccia utente di FMC, selezionare Analisi > Utenti: sessioni attive

No Search Constraints (Edit Search)

Table View of Active Sessions Active Sessions

Jump to...

	Login Time x	Last Seen x	User x	Authentication Type x	Current IP x	Realm x	Username x	First Name x	Last Name x	E-Mail x	Department x	Phone x	Discovery Application x	Device x
▼	2024-01-09 15:20:06	2024-01-31 16:21:08	sfua (LDAP:sfua, LDAP)	Passive Authentication	10.4.23.129	LDAP	sfua	sfua		sfua@orgeju.local	users (orgeju)		LDAP	frepower

3. Convalida da Analisi > Connessione > Eventi: vista tabella degli eventi di connessione

Search Constraints (Edit Search Save Search)

Connections with Application Details Table View of Connection Events

Jump to...

	First Packet x	Last Packet x	Action x	Reason x	Initiator IP x	Initiator Country x	Initiator User x	Responder IP x	Responder Country x	Security Intelligence x Category	Ingress Security Zone x	Egress Security Zone x	Source Port / ICMP Type x	Destination Port / ICMP Code x	SSL Status x	Application Protocol x	Client x	CI Ve
▼	2024-01-31 16:26:46		Allow		10.4.23.129		sfua (LDAP:sfua, LDAP)	10.6.11.5			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	
▼	2024-01-31 16:26:45		Allow		10.4.23.129		sfua (LDAP:sfua, LDAP)	10.6.11.4			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	
▼	2024-01-31 16:26:44		Allow		10.4.23.129		sfua (LDAP:sfua, LDAP)	10.6.11.3			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	
▼	2024-01-31 16:26:23		Allow		10.4.23.129		sfua (LDAP:sfua, LDAP)	10.6.11.2			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	



Nota: gli utenti che soddisfano i criteri relativi al traffico per i criteri di identità e di controllo dell'accesso vengono visualizzati con il proprio nome utente nel campo Utente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).