

Configuración de la política de identidad en el Secure Firewall Management Center (FMC)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

Introducción

Este documento describe el proceso de configuración e implementación de una política de identidad para un tráfico FTD seguro a través de FMC seguro.

Prerequisites

1. Rango ya configurado en FMC.
2. Origen de identidad ya configurado: ISE, ISE-PIC.



Nota: las instrucciones de configuración de ISE y de rango no están incluidas en este documento.

Requirements

Cisco recomienda tener conocimiento de estos temas:

- Centro de gestión de firewall seguro (FMC)
 - Firewall seguro Thread Defense (FTD)
 - Cisco Identity Services Engine (ISE)
 - Servidores LDAP/AD
 - Métodos de autenticación
1. Autenticación pasiva: uso de una fuente de usuario de identidad externa, como ISE
 2. Autenticación activa: uso del dispositivo administrado como fuente de autenticación (portal cautivo o acceso VPN remoto)

3. Sin autenticación

Componentes Utilizados

- Secure Firewall Management Center para VMWare v7.2.5
- Cisco Secure Firewall Threat Defence para VMWare v7.2.4
- Servidor de directorio activo
- Cisco Identity Services Engine (ISE) v3.2, parche 4
- Método de autenticación pasiva

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

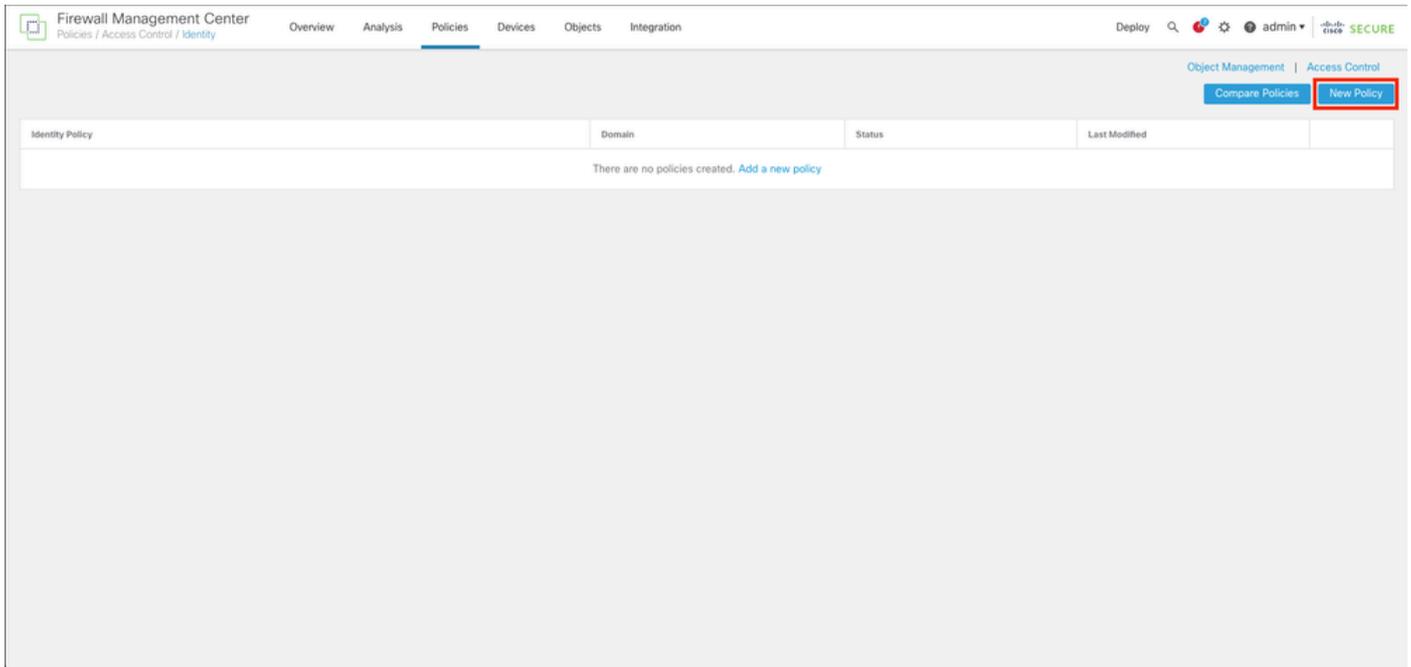
Configurar

Configuraciones

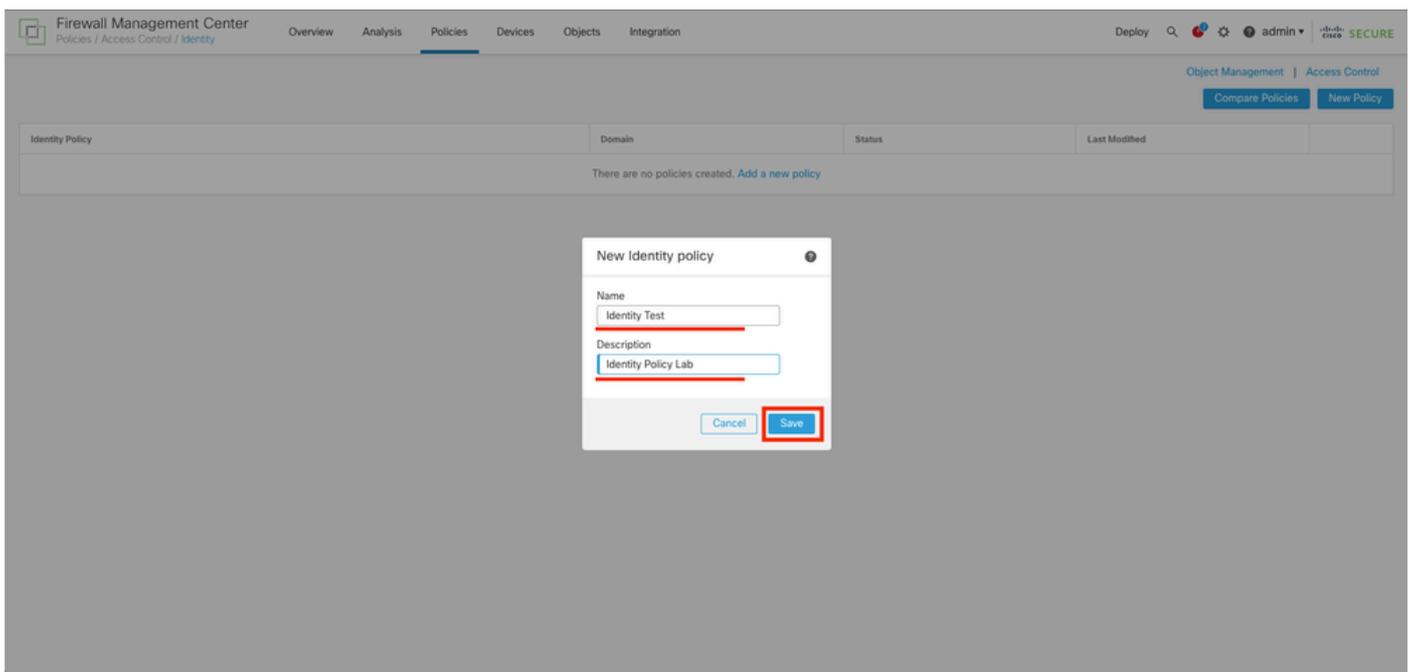
Paso 1. En la GUI de FMC, vaya a Políticas > Control de acceso > Identidad

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 for 'Access Control', 'Network Discovery', 'Actions', 'Access Control', 'Application Detectors', 'Alerts', 'Intrusion', 'Correlation', 'Scanners', 'Malware & File', 'DNS', 'Groups', 'Modules', 'Identity', 'Instances', 'SSL', and 'Prefilter'. The 'Identity' sub-menu is highlighted with a red box. The main dashboard area contains several widgets: 'Summary Dashboard' with tabs for 'Network', 'Threats', 'Intrusion Events', 'Status', and 'Geolocation'; 'Unique Applications over Time' with a line graph; 'Traffic by Application Risk' with a bar chart; 'Traffic by Business Relevance' with a bar chart; 'Top Client Applications Seen' with a bar chart; 'Top Server Applications Seen' showing 'No Data'; and 'Top Operating Systems Seen' showing 'No Data'. The interface also includes a 'Reporting' section with a 'Show the Last' dropdown set to '1 hour' and an 'Add Widgets' button.

Paso 2. Haga clic en Nueva directiva.

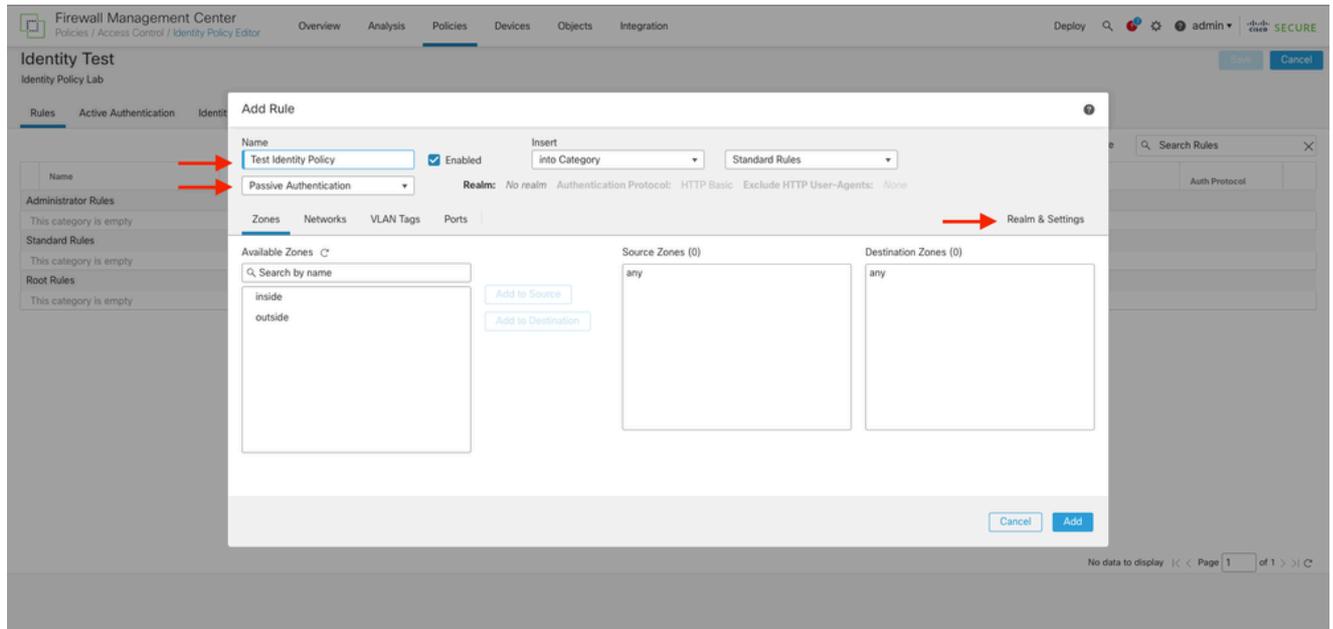


Paso 3. Asigne un nombre y una descripción a la nueva política de identidad y, a continuación, haga clic en Guardar.

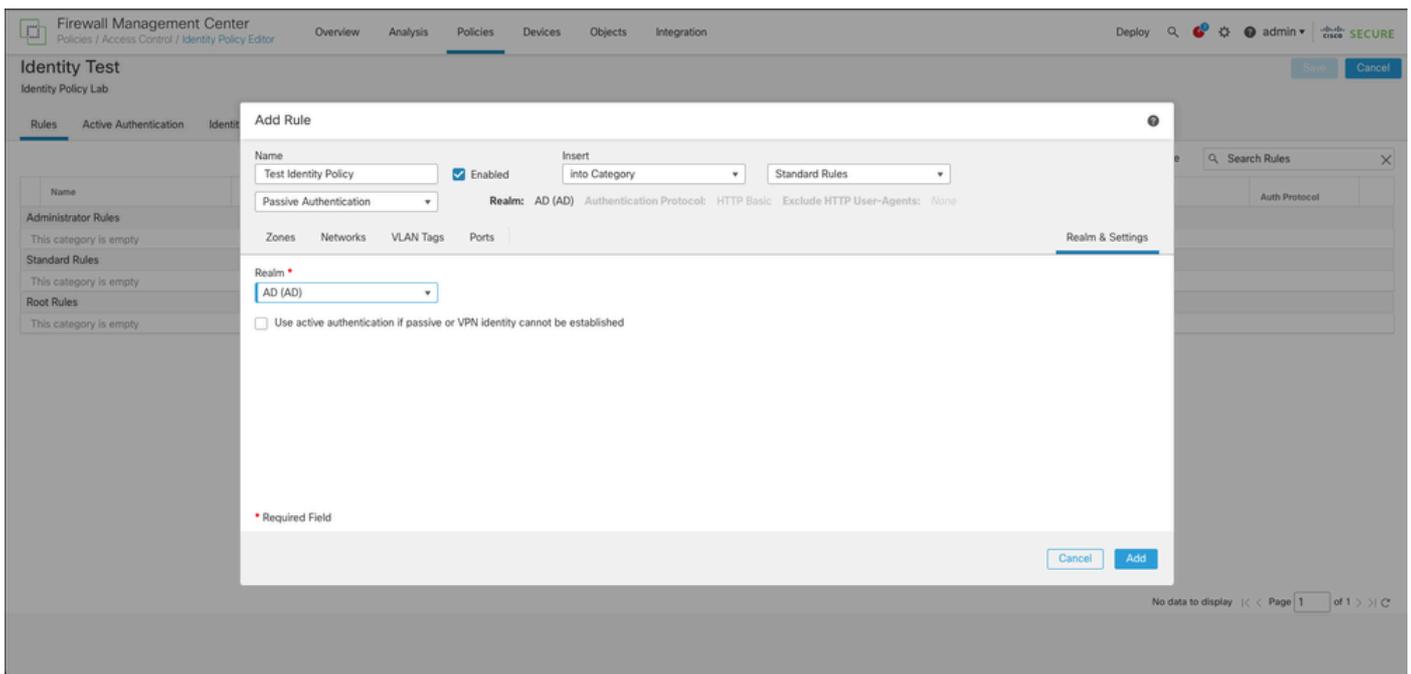


Paso 4. Haga clic en el icono + Agregar regla.

1. Asigne un nombre a la nueva regla.
2. En el campo name (nombre), elija el método de autenticación y seleccione : Passive Authentication (Autenticación pasiva).
3. A la derecha de la pantalla, seleccione Realm & Settings (Dominio y parámetros).



4. Seleccione un rango en el menú desplegable.



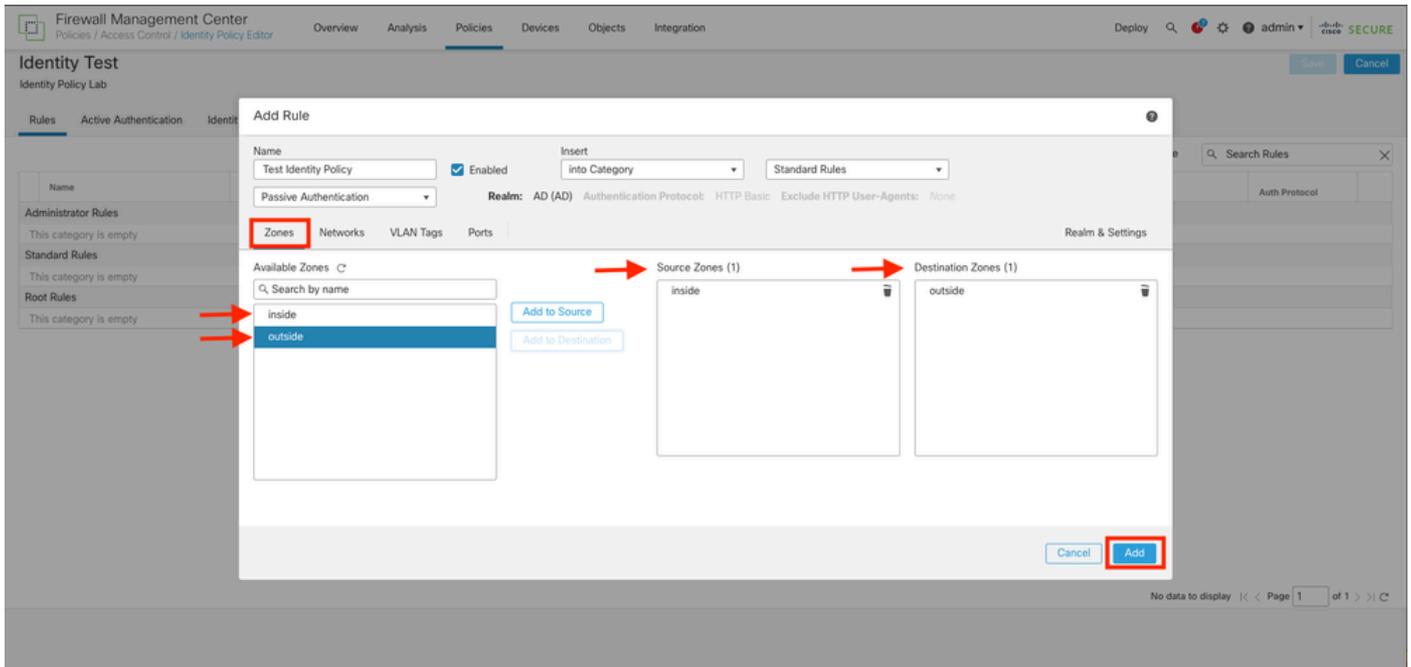
5. Haga clic en Zonas a la izquierda de la pantalla.

6. En el menú Zonas disponibles, asigne una zona de origen y de destino basada en la ruta de tráfico necesaria para detectar usuarios. Para agregar una zona, haga clic en el nombre de la zona y, a continuación, seleccione en función del caso Add to Source o Add to Destination.

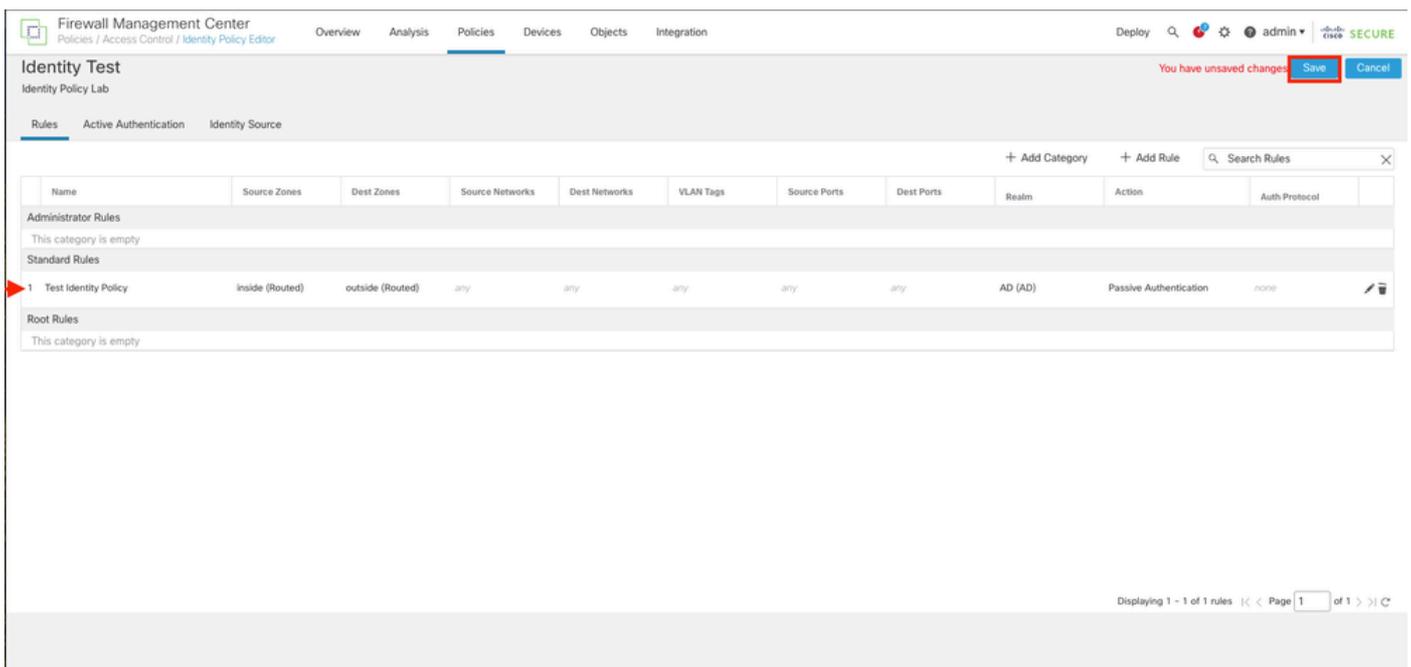


Nota: En esta documentación, la detección de usuarios se aplicará solo para el tráfico que proviene de la zona interna y se reenvía a la zona externa.

7. Seleccione Agregar y Guardar.

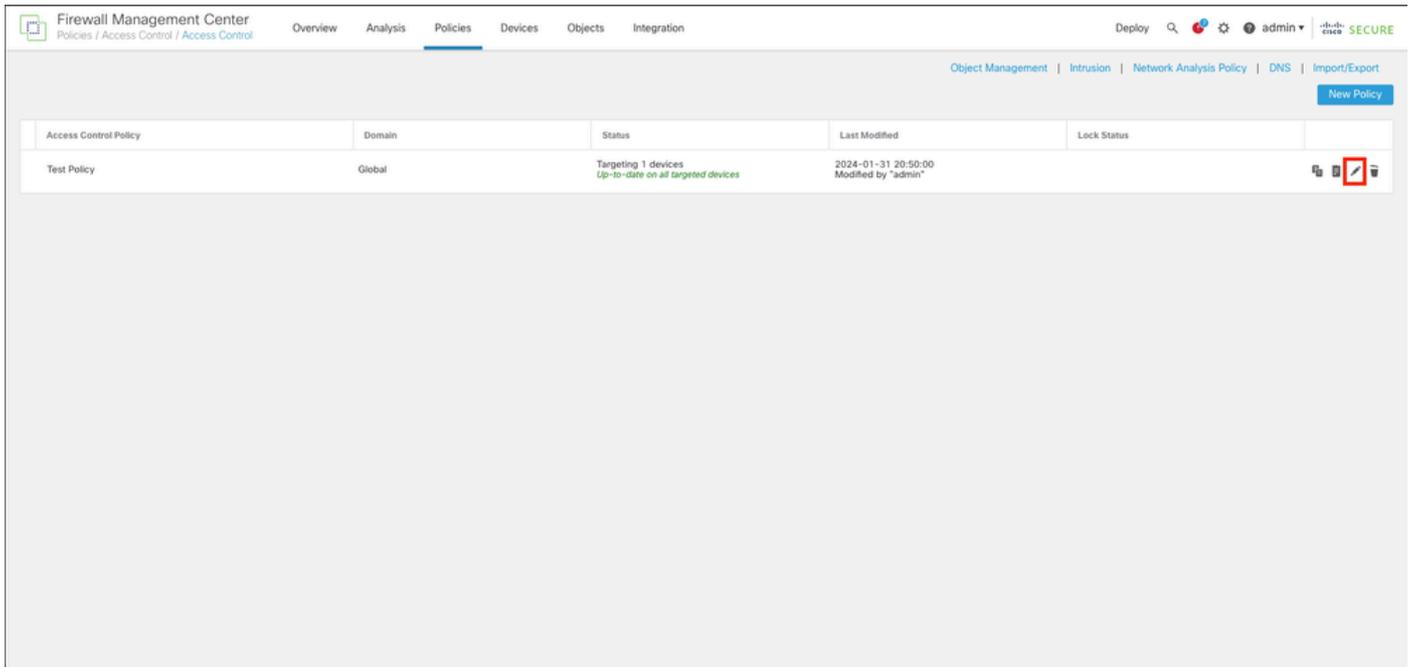


Paso 5. Valide que la nueva regla está en la política de identidad y haga clic en Guardar.

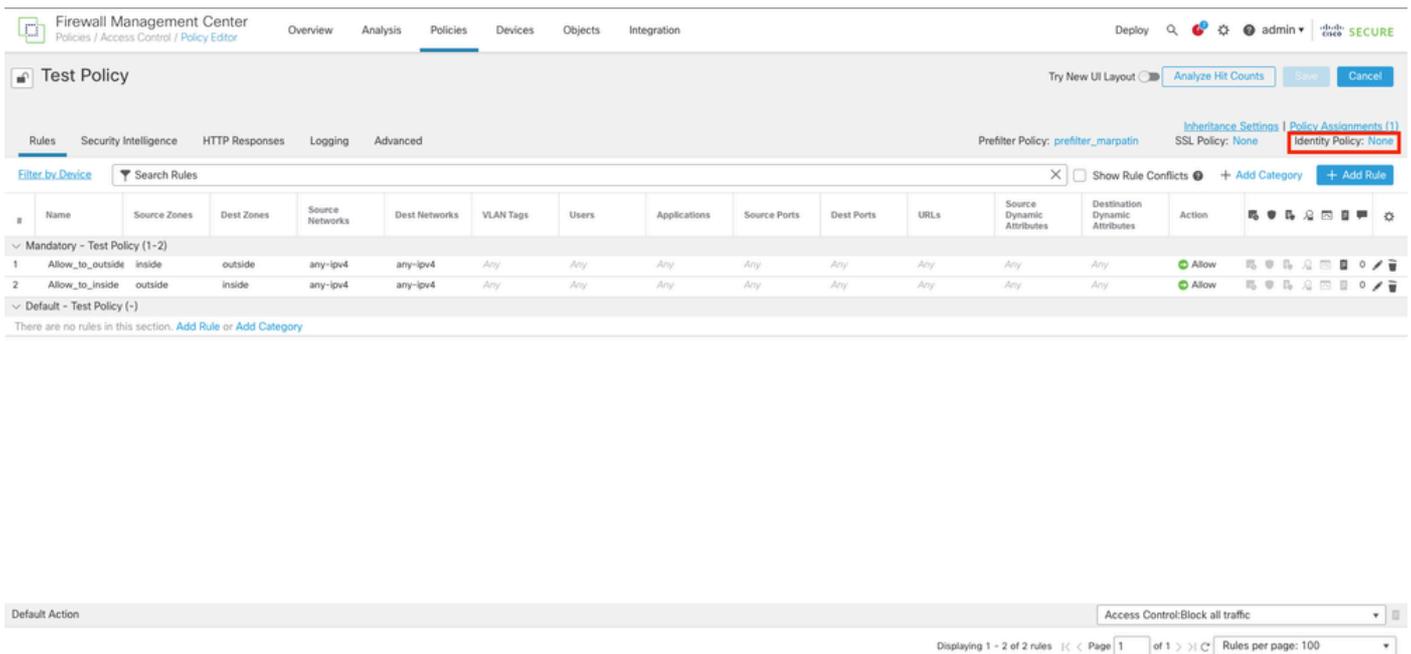


Paso 6. Vaya a Políticas > Control de acceso

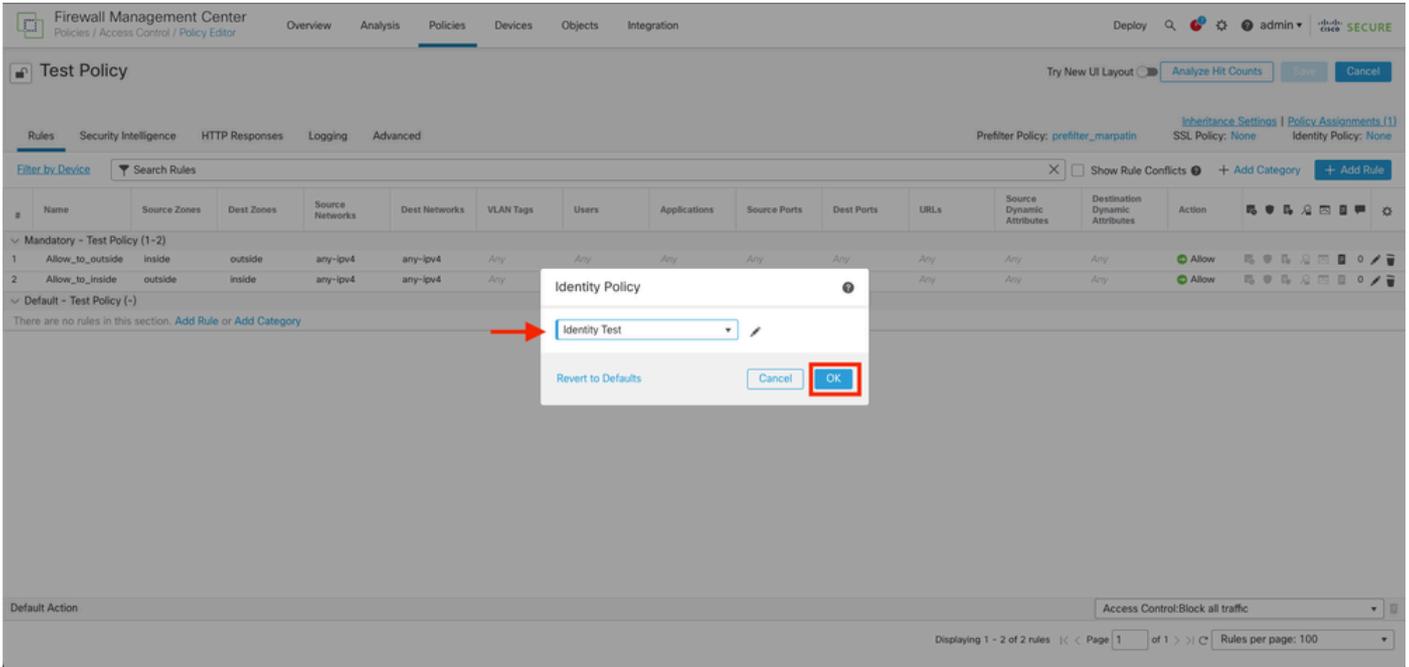
Paso 7. Identifique la política de control de acceso que se va a implementar en el firewall que administra el tráfico de usuarios y haga clic sobre el icono del lápiz para editar la política.



Paso 6. Haga clic en None en el campo Identity Policy.



Paso 7. En el menú desplegable, seleccione la política creada anteriormente en el paso 3 y, a continuación, haga clic en Aceptar para finalizar la configuración.



Paso 8. Guardar e implementar la configuración en el FTD.

Verificación

1. En la GUI de FMC, navegue hasta Análisis > Usuarios: Sesiones activas

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@jorgeju.local	users (jorgeju)		LDAP	frepower

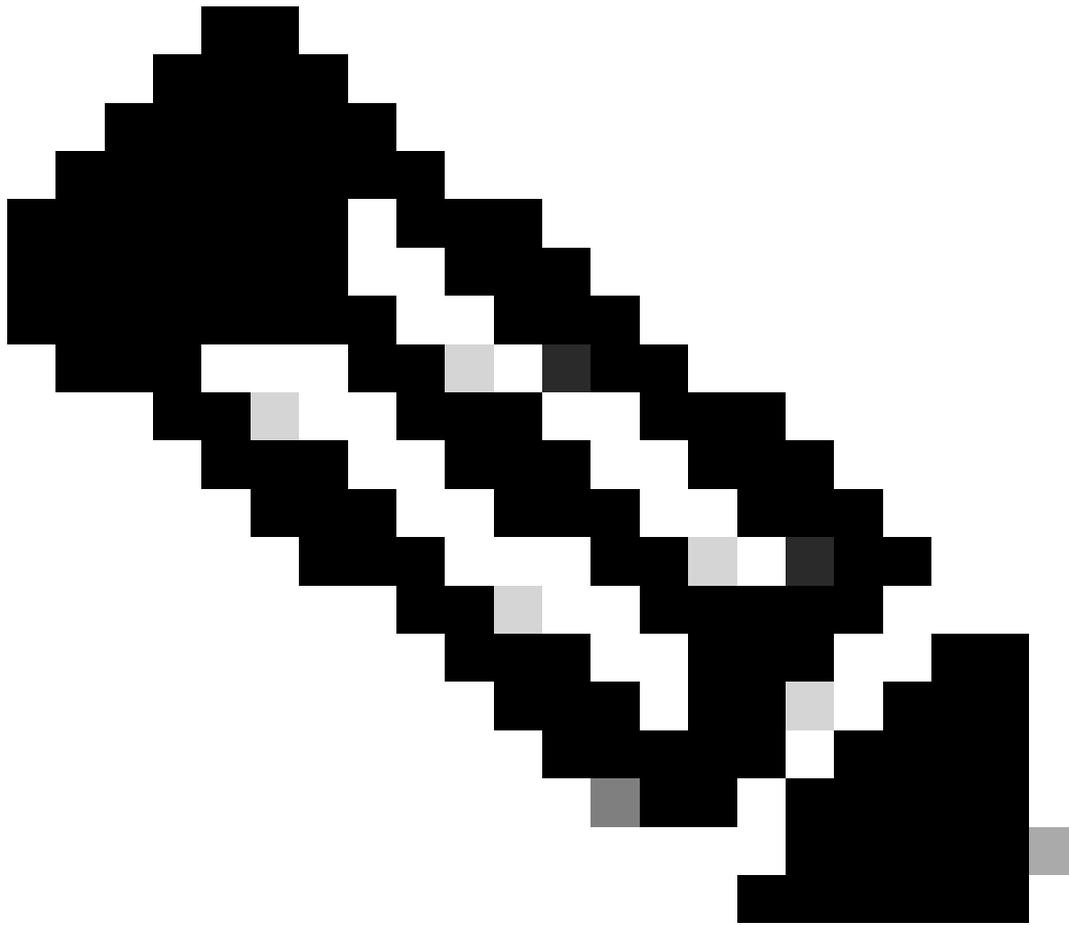
3. Validación de Análisis > Conexión > Eventos: Vista de tabla de los eventos de Conexiones

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 Category x	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: Los usuarios que coinciden con los criterios de tráfico de la política de identidad y la política de control de acceso muestran su nombre de usuario en el campo Usuario.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).