

Configurar a política de identidade no Centro de gerenciamento de firewall seguro (FMC)

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

Introdução

Este documento descreve o processo de como configurar e implantar uma política de identidade para um tráfego FTD seguro através do FMC seguro.

Pré-requisitos

1. Território já configurado no FMC.
2. Origem da Identidade já Configurada - ISE, ISE-PIC.



Observação: as instruções de configuração do ISE e do Realm estão fora do escopo deste documento.

Requisitos

A Cisco recomenda ter conhecimento destes tópicos:

- Centro de gerenciamento seguro de firewall (FMC)
 - Defesa Segura por Thread de Firewall (FTD)
 - Cisco Identity Services Engine (ISE)
 - Servidores LDAP/AD
 - Métodos de autenticação
1. Autenticação Passiva : uso de origem de usuário de identidade externa, como ISE
 2. Autenticação ativa : uso do dispositivo gerenciado como fonte de Autenticação (acesso ao portal cativo ou à vpn remota)

3. Sem Autenticação

Componentes Utilizados

- Secure Firewall Management Center para VMWare v7.2.5
- Cisco Secure Firewall Threat Defense para VMWare v7.2.4
- Servidor do Active Directory
- Cisco Identity Services Engine (ISE) v3.2 patch 4
- Método de autenticação passiva

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

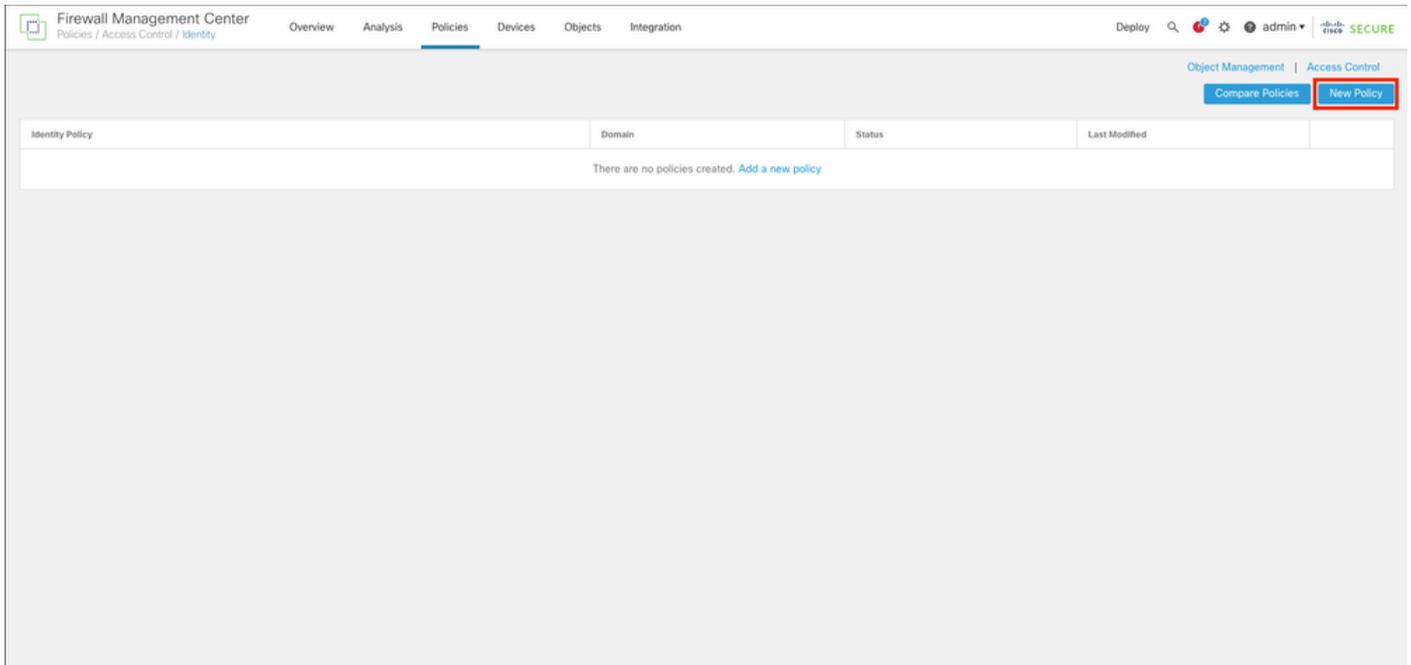
Configurar

Configurações

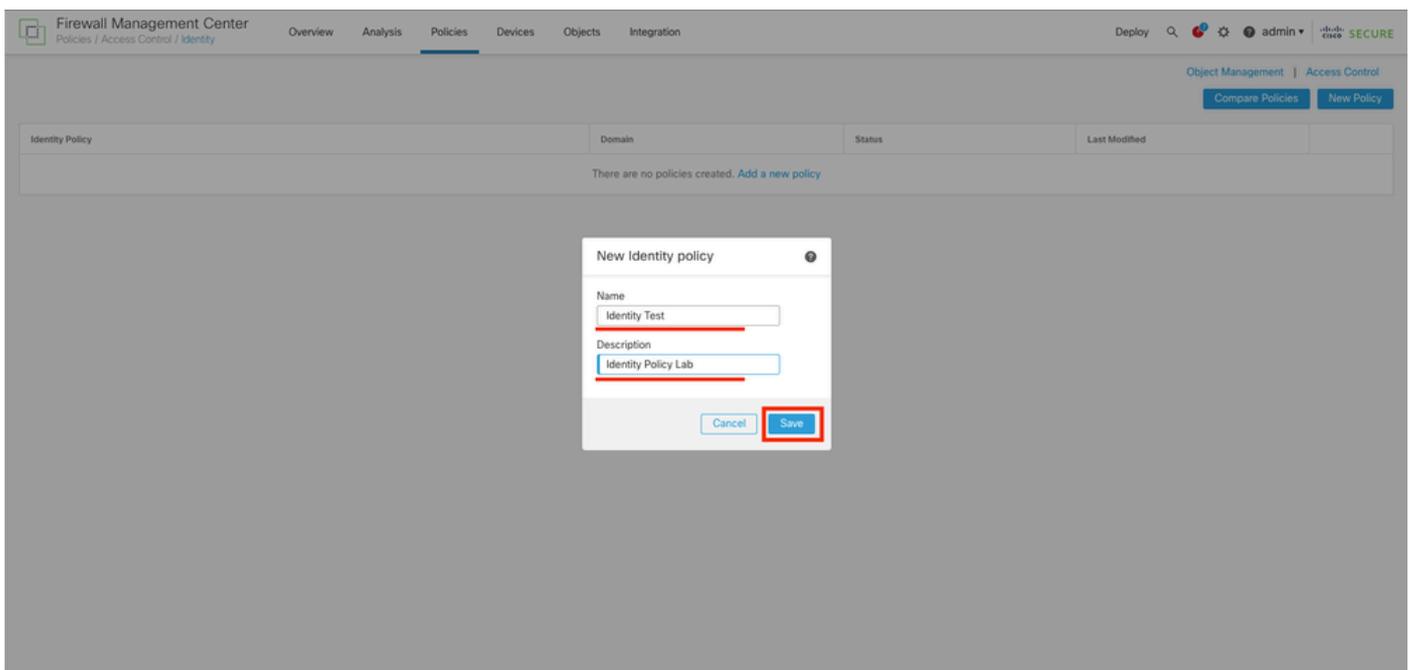
Etapa 1. Na GUI do FMC , navegue até Políticas > Access Control > Identity

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', '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' (Network, Threats, Intrusion Events, Status, Geolocation), 'Unique Applications over Time' (line graph), 'Traffic by Application Risk' (bar chart), 'Traffic by Business Relevance' (bar chart), 'Top Client Applications Seen' (bar chart), 'Top Server Applications Seen' (No Data), and 'Top Operating Systems Seen' (No Data). The 'Top Client Applications Seen' widget shows data for Cisco Secure Endpoint (83.33 KB), Kerberos (6.46 KB), DCE/RPC (5.02 KB), and Emap (1.24 KB).

Etapa 2. Clique em Nova política.

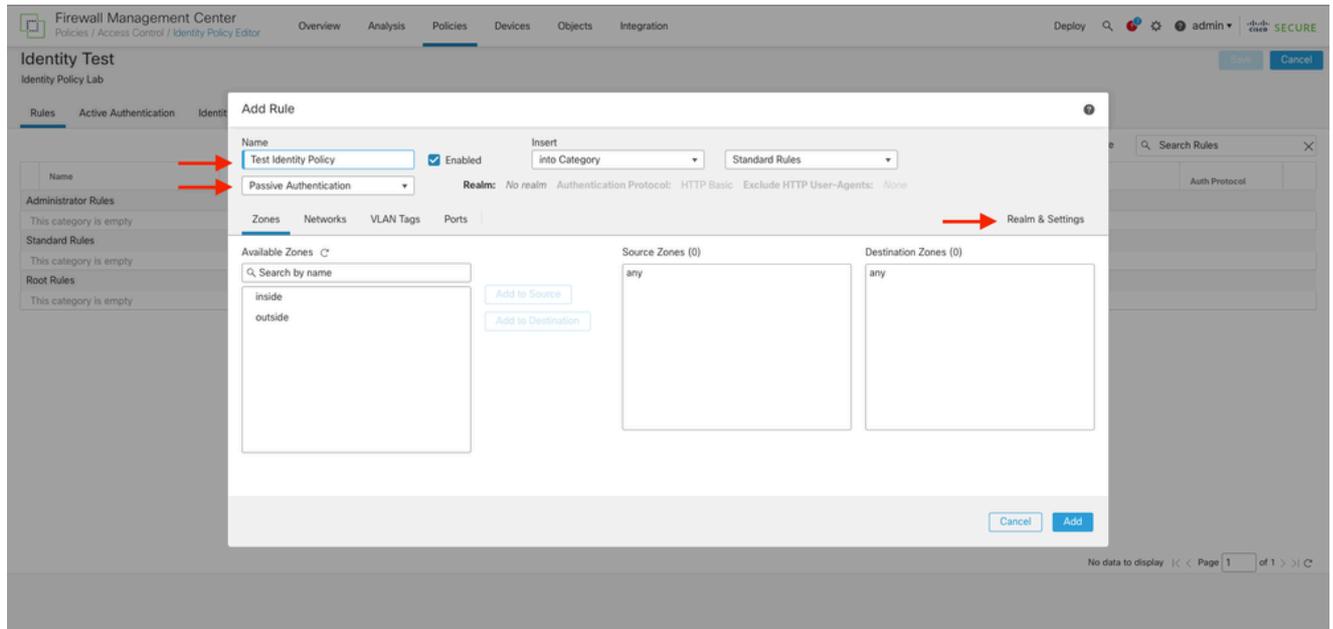


Etapa 3. Atribua um nome e uma descrição à nova política de identidade e clique em Salvar.

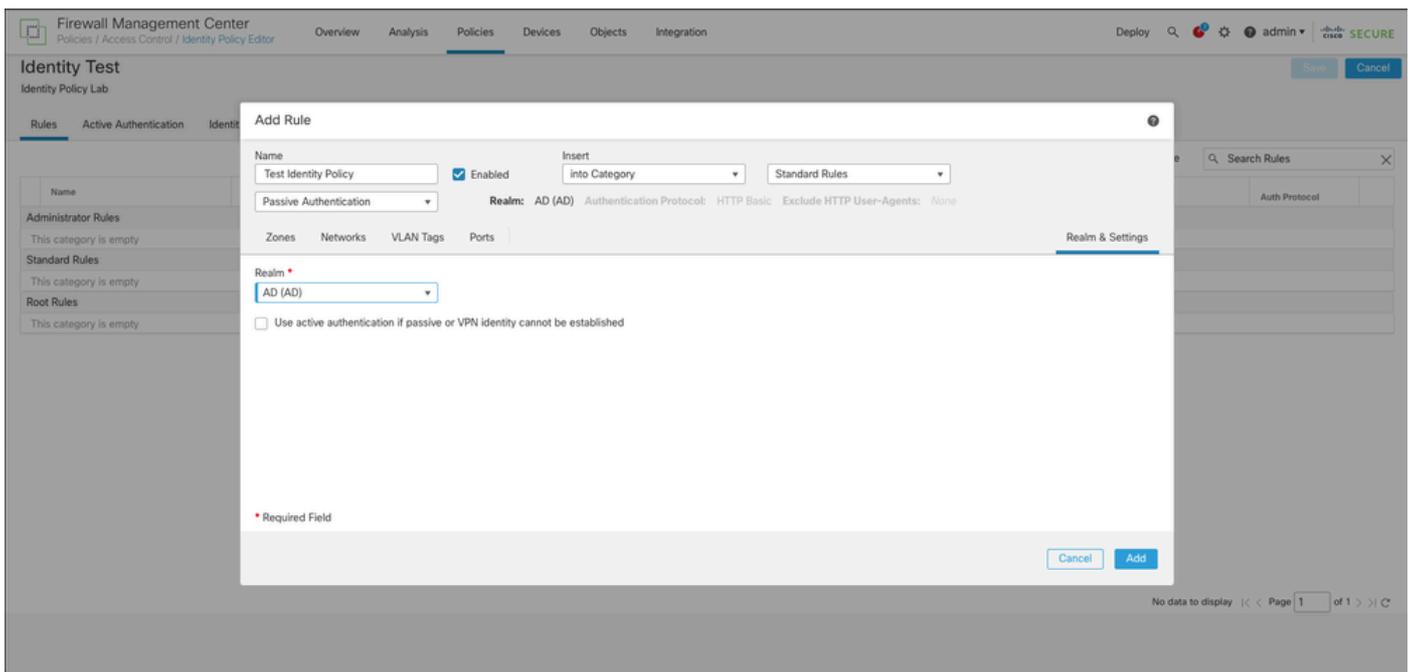


Etapa 4. Clique no ícone + Adicionar regra.

1. Atribua um nome à nova regra.
2. No campo de nome, escolha o método de autenticação e selecione : Autenticação passiva.
3. À direita da tela, selecione Realm & Settings (Realm e configurações).



4. Selecione um Realm no menu drop-down.



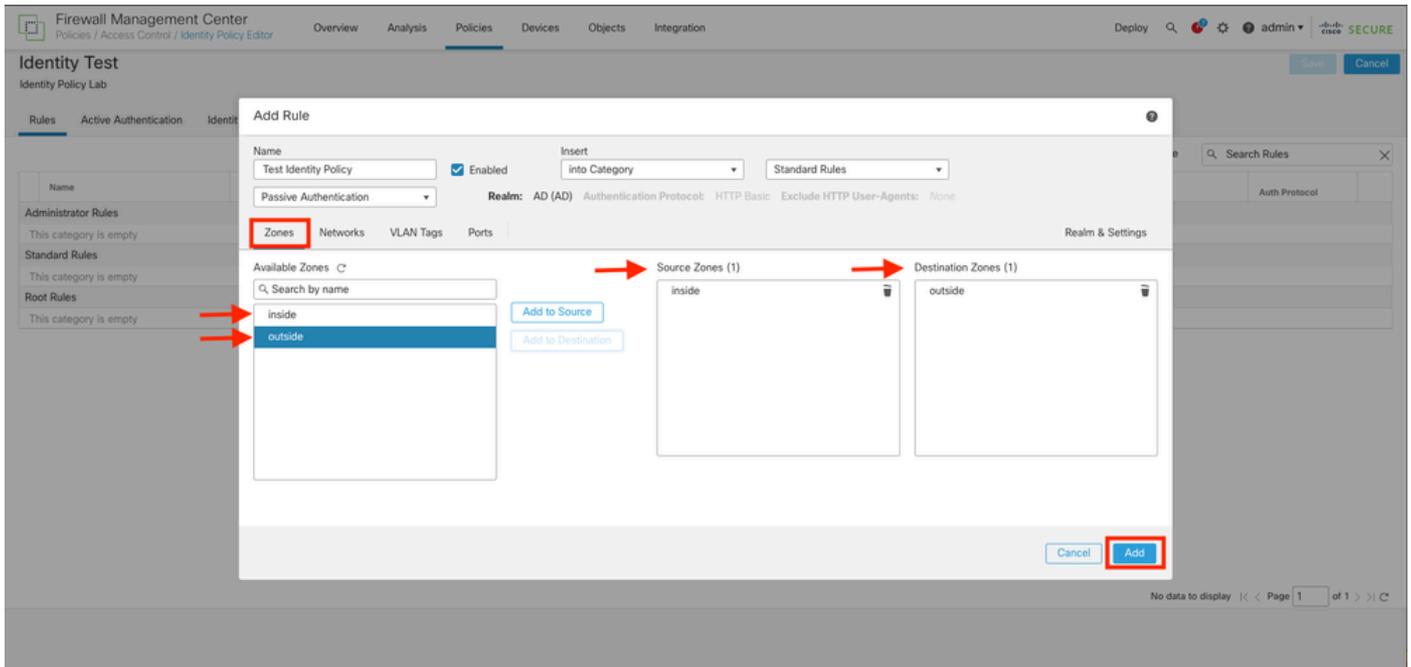
5. Clique em Zonas à esquerda da tela.

6. No menu Zonas disponíveis, atribua uma zona de origem e de destino com base no caminho de tráfego necessário para detectar usuários. Para adicionar uma zona, clique no nome da zona e selecione, dependendo do caso Adicionar à fonte ou Adicionar ao destino.

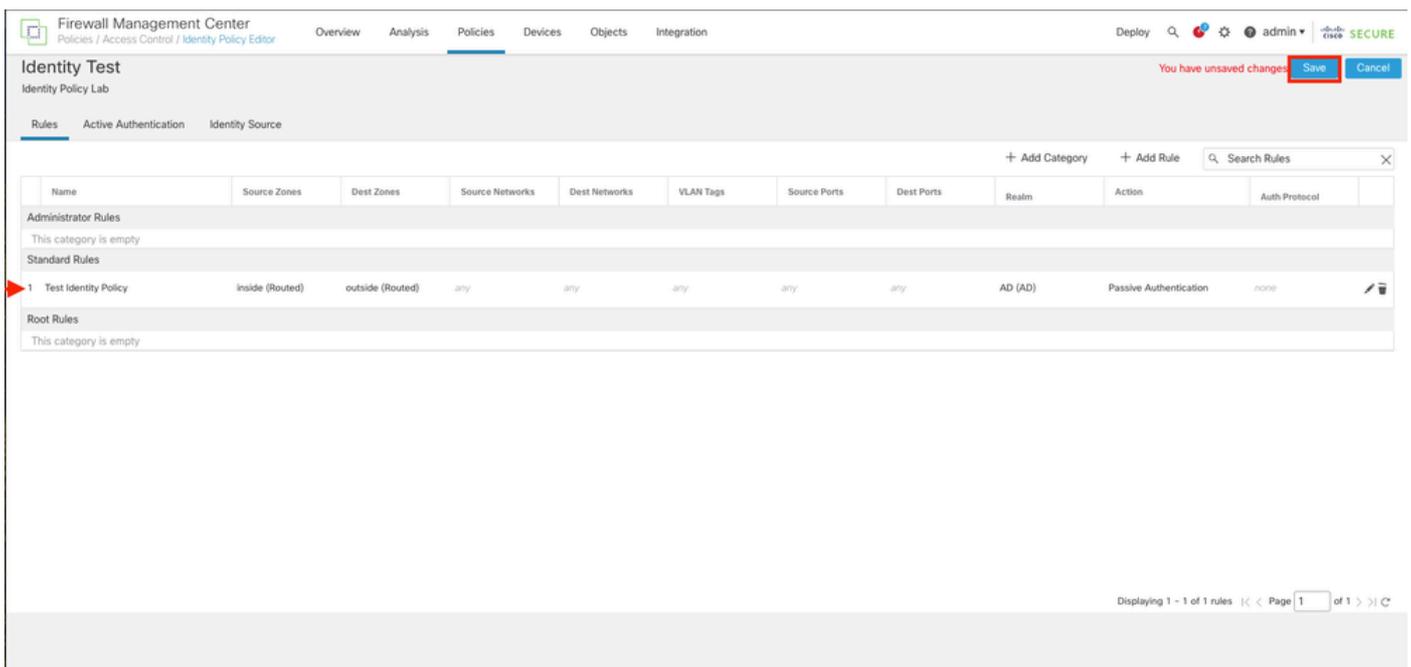


Observação: nesta documentação, a detecção do usuário será aplicada somente ao tráfego que vem da zona interna e é encaminhado para a zona externa.

7. Selecione Adicionar e Salvar.

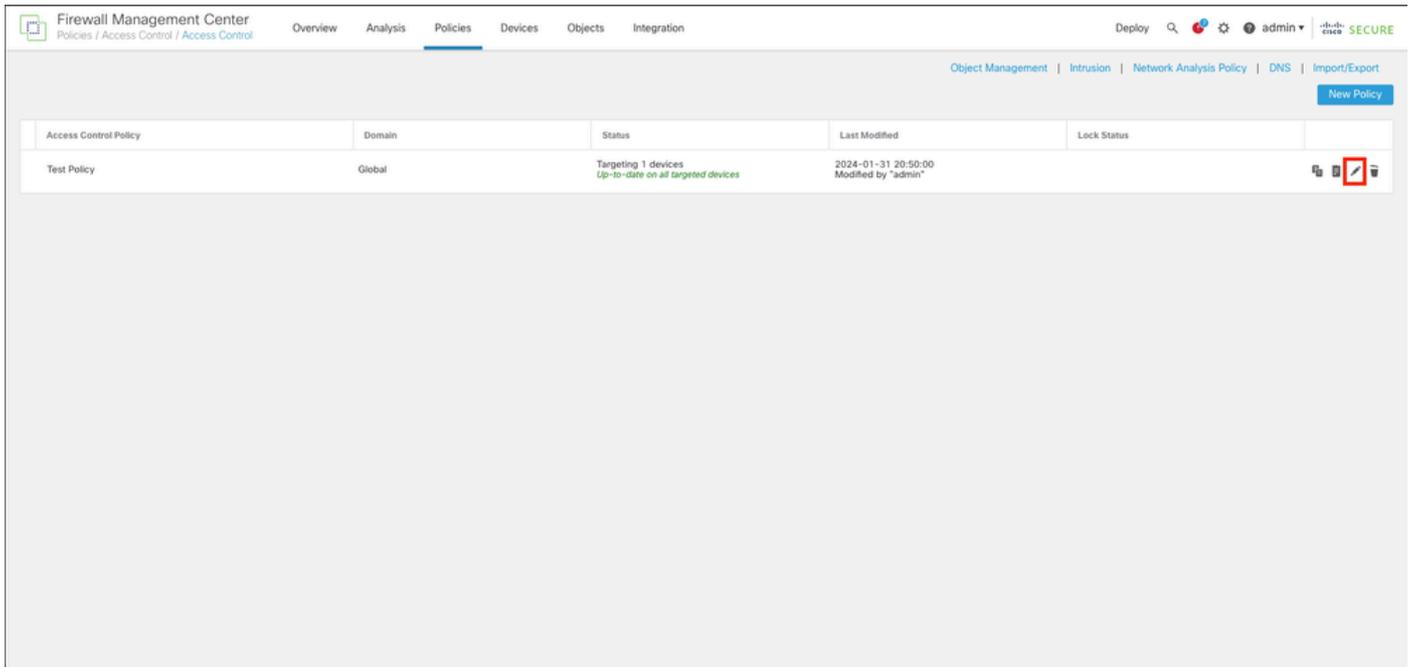


Etapa 5. Valide se a nova regra está na política de identidade e clique em Salvar.

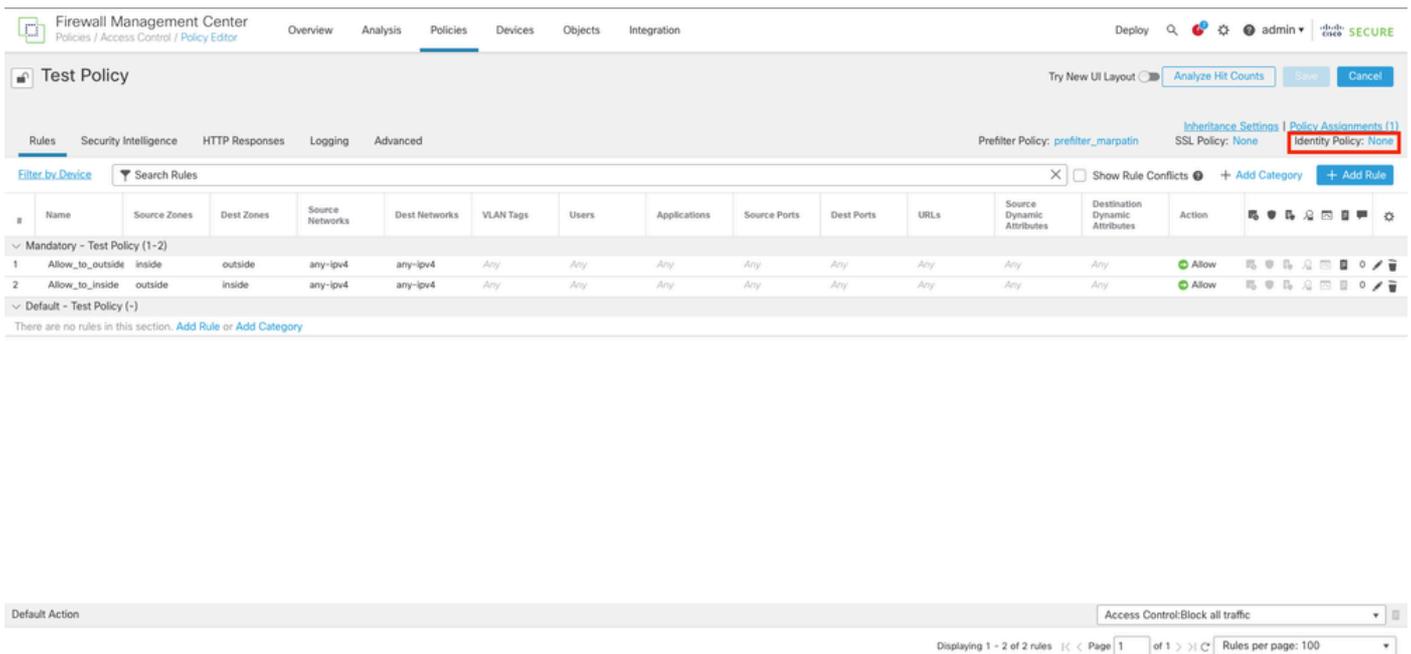


Etapa 6. Navegue até Políticas > Access Control (Políticas > Controle de acesso)

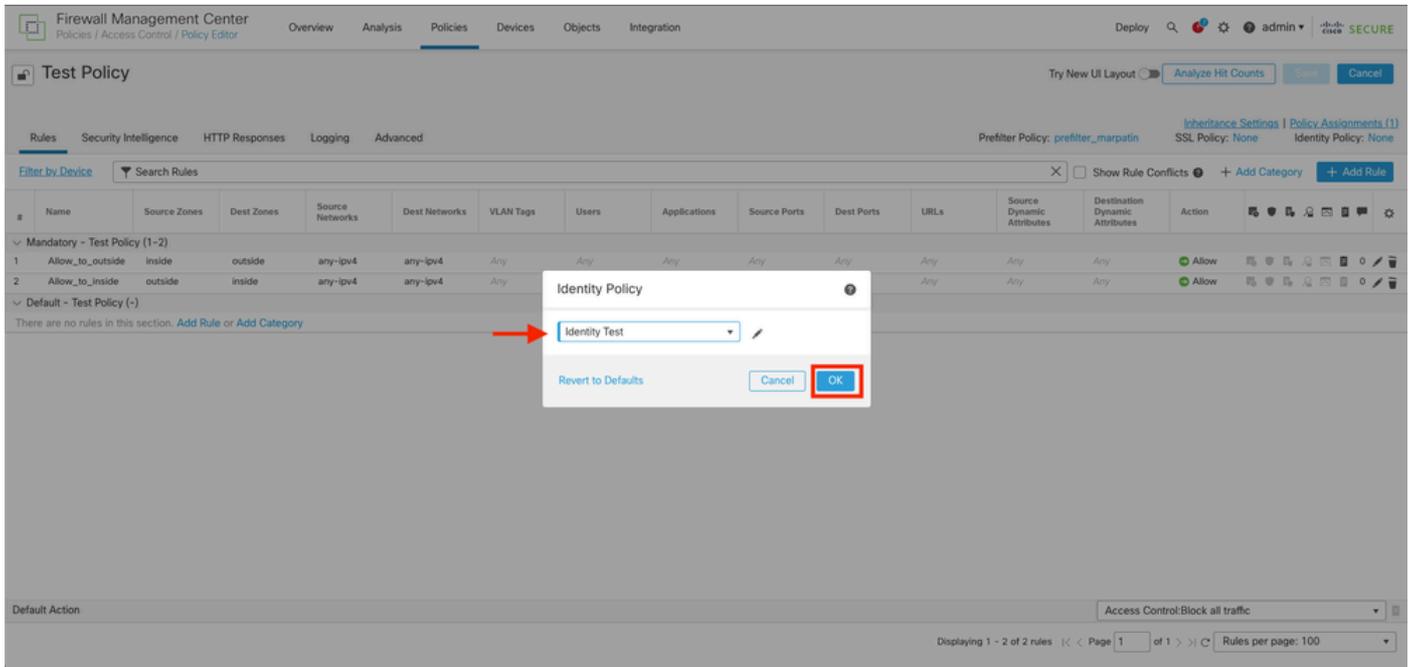
Passo 7. Identifique a Política de Controle de Acesso que será implantada no Firewall que controla o tráfego de usuários e clique sobre o ícone do lápis para editar a política.



Etapa 6. Clique em None no campo Identity Policy.



Passo 7. No menu suspenso, selecione a política criada anteriormente na etapa 3 e clique em OK para concluir a configuração.



Etapa 8. Salve e implante a configuração no FTD.

Verificar

1. Na GUI do FMC, navegue até Analysis > Users: Ative Sessions (Análise > Usuários: Sessões Ativas)

No Search Constraints (Edit Search)

Table View of Active Sessions Active Sessions

Jump to...

<input type="checkbox"/>	↓ 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
<input type="checkbox"/>	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

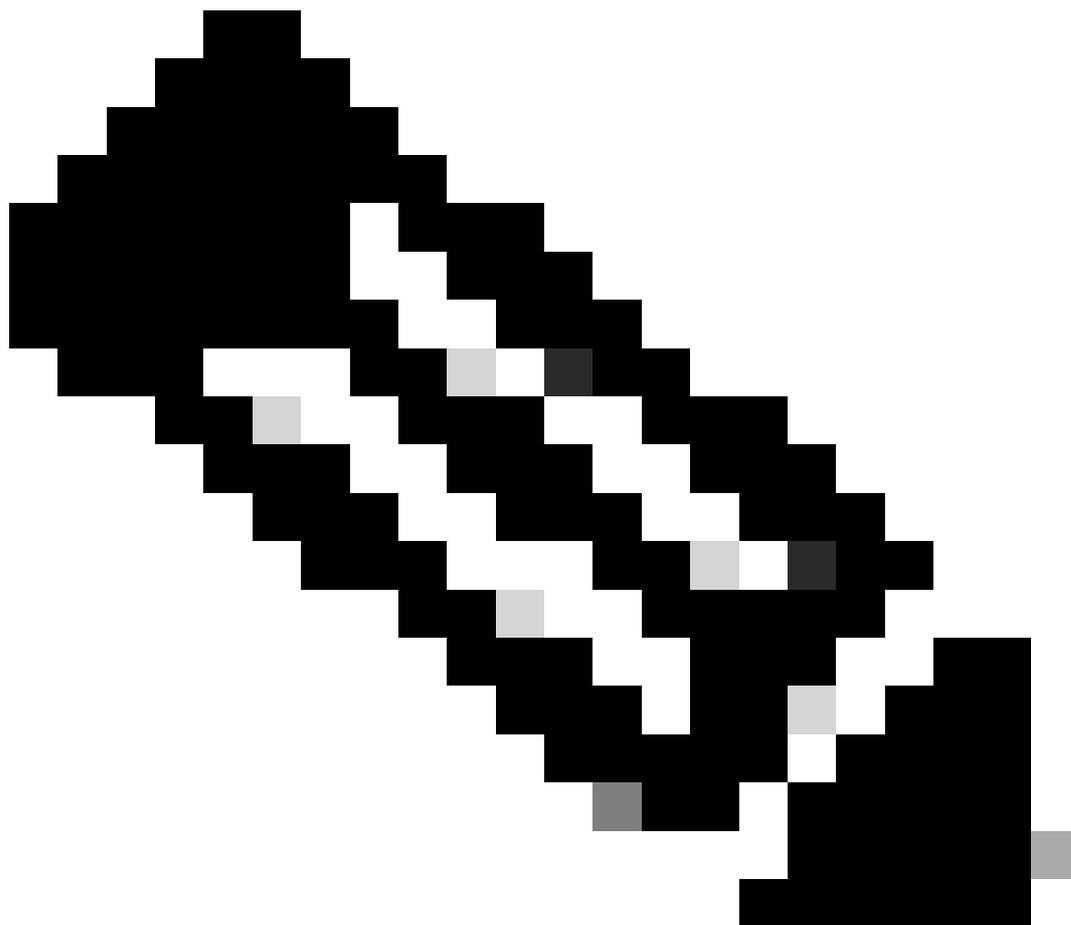
3. Validação de Análise > Conexão > Eventos: Exibição em tabela dos eventos de Conexões

Search Constraints (Edit Search Save Search)

Connections with Application Details Table View of Connection Events

Jump to...

<input type="checkbox"/>	↓ 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 x Zone	Egress Security x Zone	Source Port / ICMP Type x	Destination Port / ICMP Code x	SSL Status x	Application Protocol x	Client x	CI Vx
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	



Observação: os usuários que correspondem aos critérios de tráfego para a Política de identidade e Política de controle de acesso são mostrados com seu nome de usuário no campo Usuário.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.