

# 在安全防火墙管理中心(FMC)上配置身份策略

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置](#)

[验证](#)

---

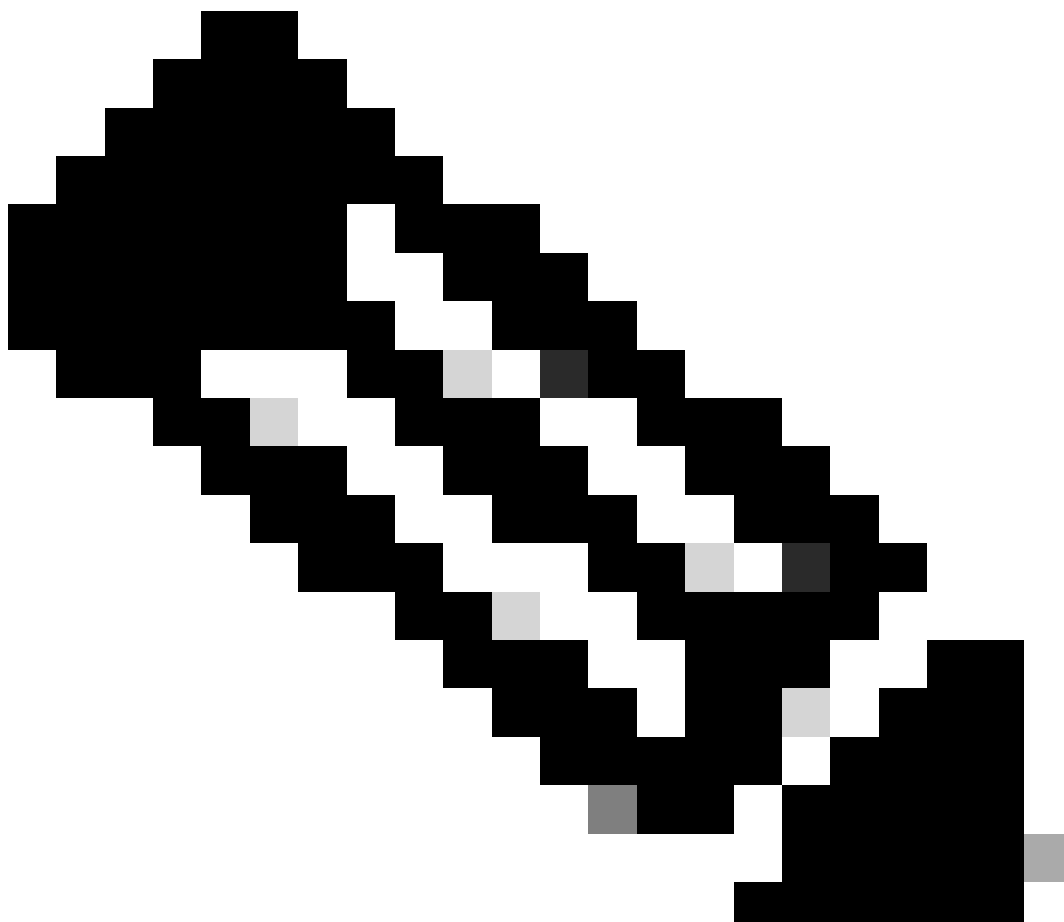
## 简介

本文档介绍如何通过安全FMC为安全FTD流量配置和部署身份策略的流程。

## 先决条件

1. 已在FMC中配置领域。
2. 已配置身份源- ISE、ISE-PIC。

---



注意：ISE和领域配置说明不在本文档的讨论范围之内。

---

## 要求

思科建议了解以下主题：

- 安全防火墙管理中心(FMC)
  - 安全防火墙线程防御(FTD)
  - 思科身份服务引擎(ISE)
  - LDAP/AD服务器
  - 身份验证方法
1. 被动身份验证：使用外部身份用户源（例如ISE）
  2. 主动身份验证：将受管设备用作身份验证源（强制网络门户或远程vpn访问）
  3. 无身份验证

## 使用的组件

- 适用于VMWare v7.2.5的安全防火墙管理中心
- 适用于VMWare v7.2.4的思科安全防火墙威胁防御
- Active Directory 服务器
- 思科身份服务引擎(ISE) v3.2补丁4
- 被动身份验证方法

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

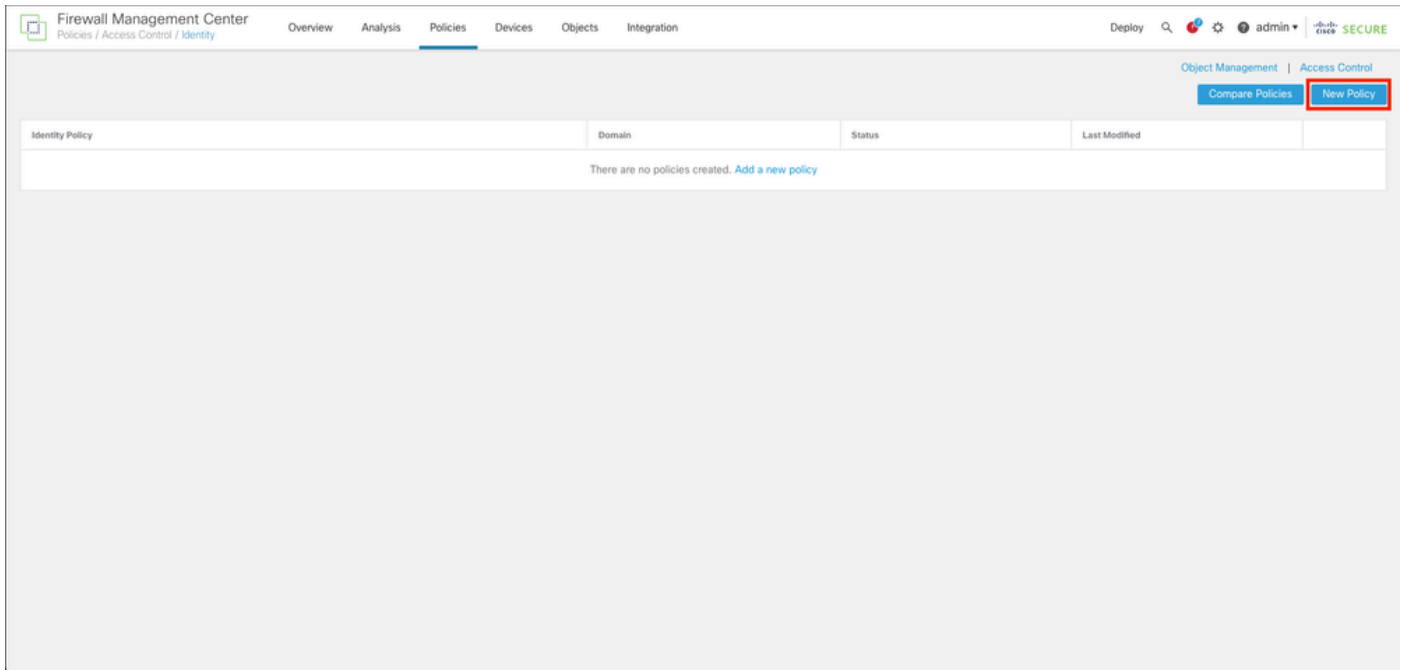
### 配置

第1步：在FMC GUI中，导航至策略>访问控制>身份

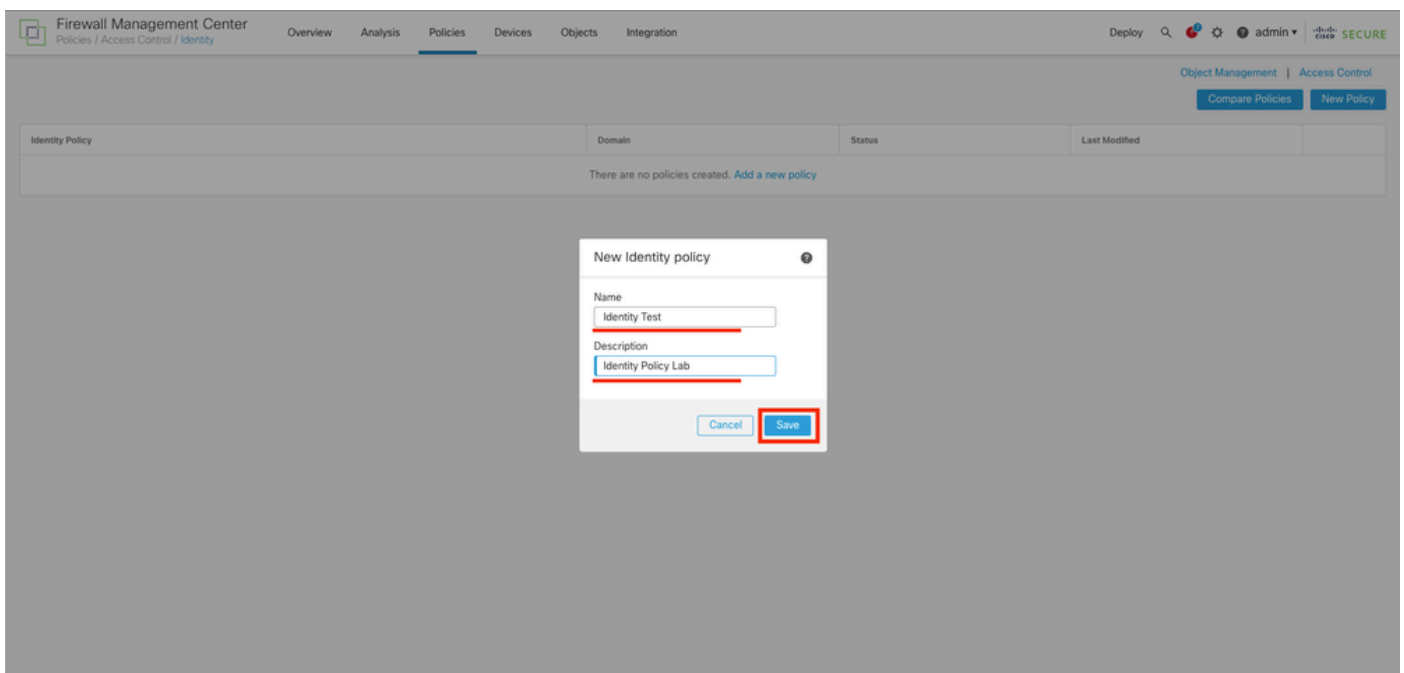
The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Policies' menu is open, showing a list of categories: Access Control, Network Discovery, Actions, Access Control, Application Detectors, Alerts, Intrusion, Correlation, Scanners, Malware & File, DNS, Groups, Modules, Identity, SSL, Instances, and Prefilter. The 'Identity' option is highlighted with a red box. 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' (table), and 'Top Server Applications Seen' (table). The 'Top Client Applications Seen' table shows the following data:

Application	Total Bytes (KB)
Cisco Secure Endpoint	63.33
Kerberos	6.46
DCE/RPC	5.02
Emap	1.24

步骤2.点击New Policy。

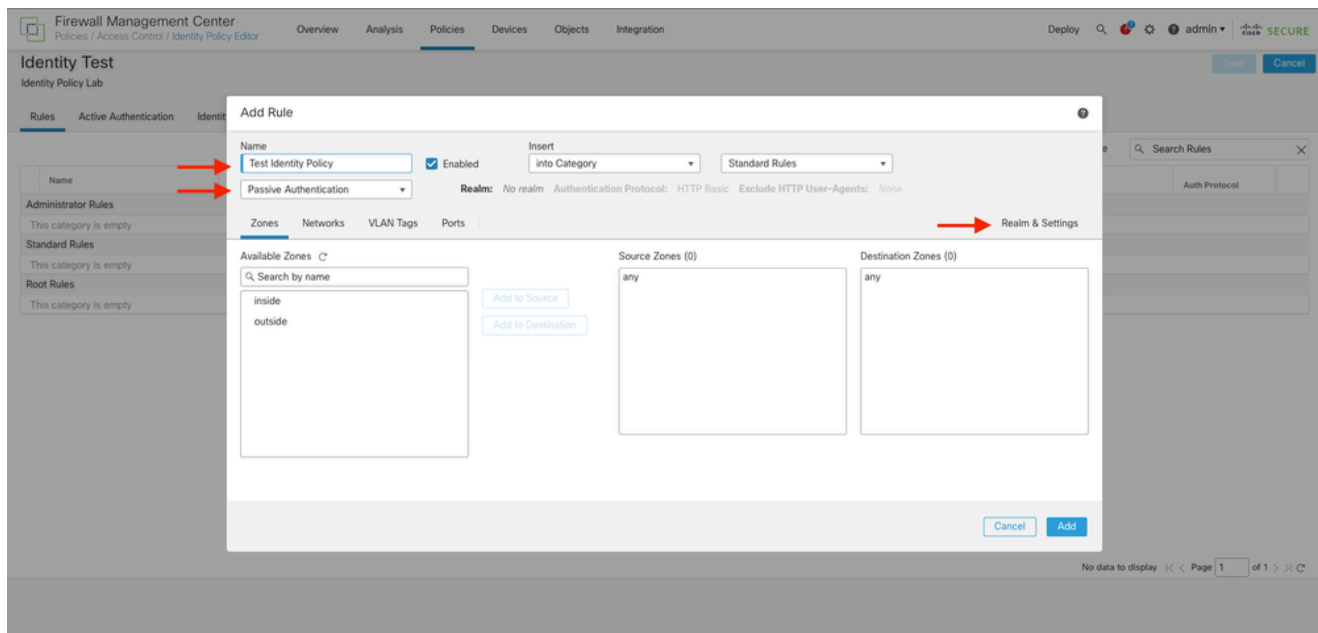


第3步：为新的身份策略分配名称和说明，然后点击保存。

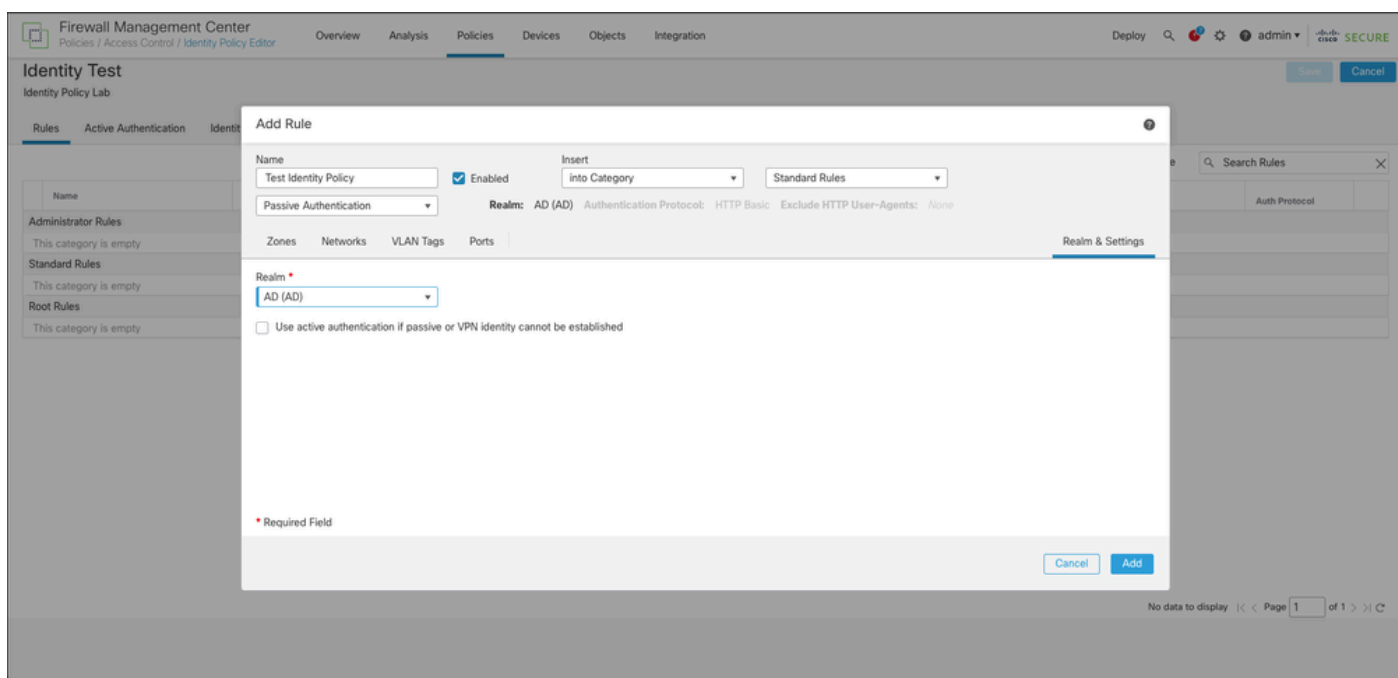


第四步：点击+添加规则图标。

1. 为新规则指定名称。
2. 在name字段下，选择身份验证方法，选择：Passive Authentication。
3. 在屏幕右侧选择Realm & Settings。



4. 从下拉菜单中选择领域。



5. 单击屏幕左侧的Zones。

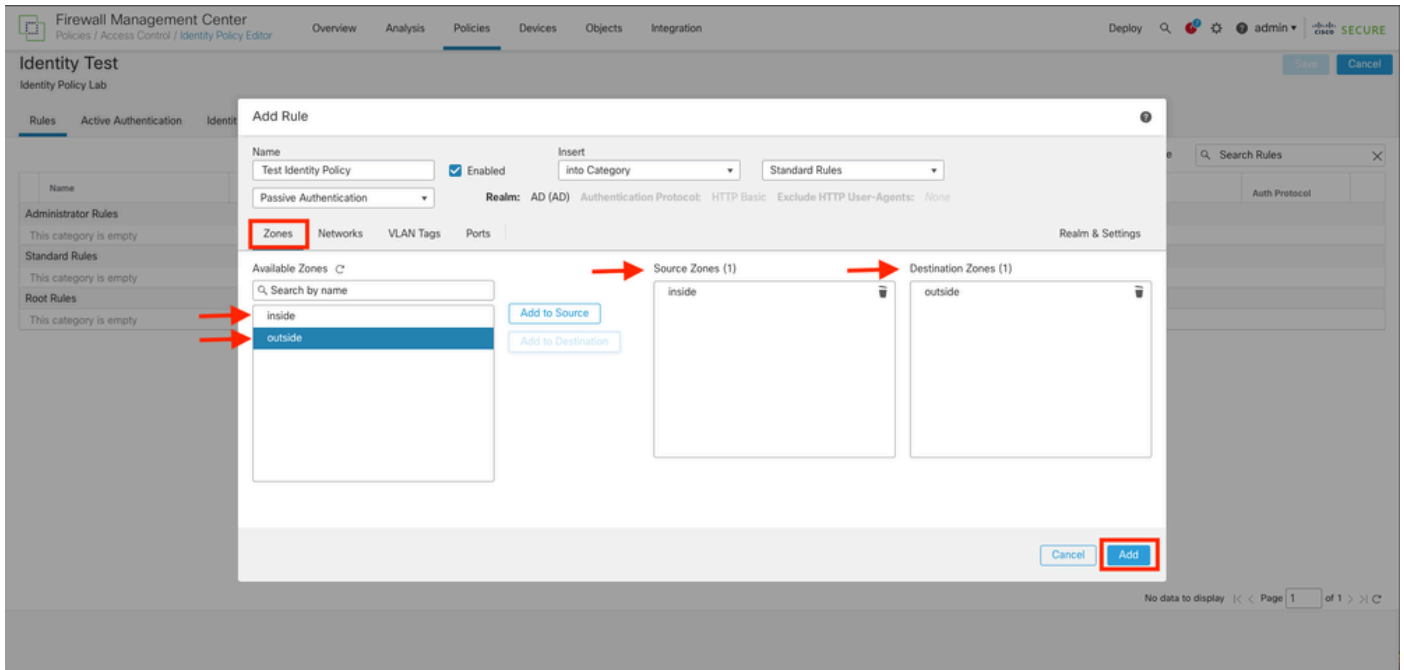
6. 从可用区域菜单中，根据检测用户所需的流量路径分配源和目标区域。要添加区域，请点击区域的名称，然后根据情况选择添加到源或添加到目标。



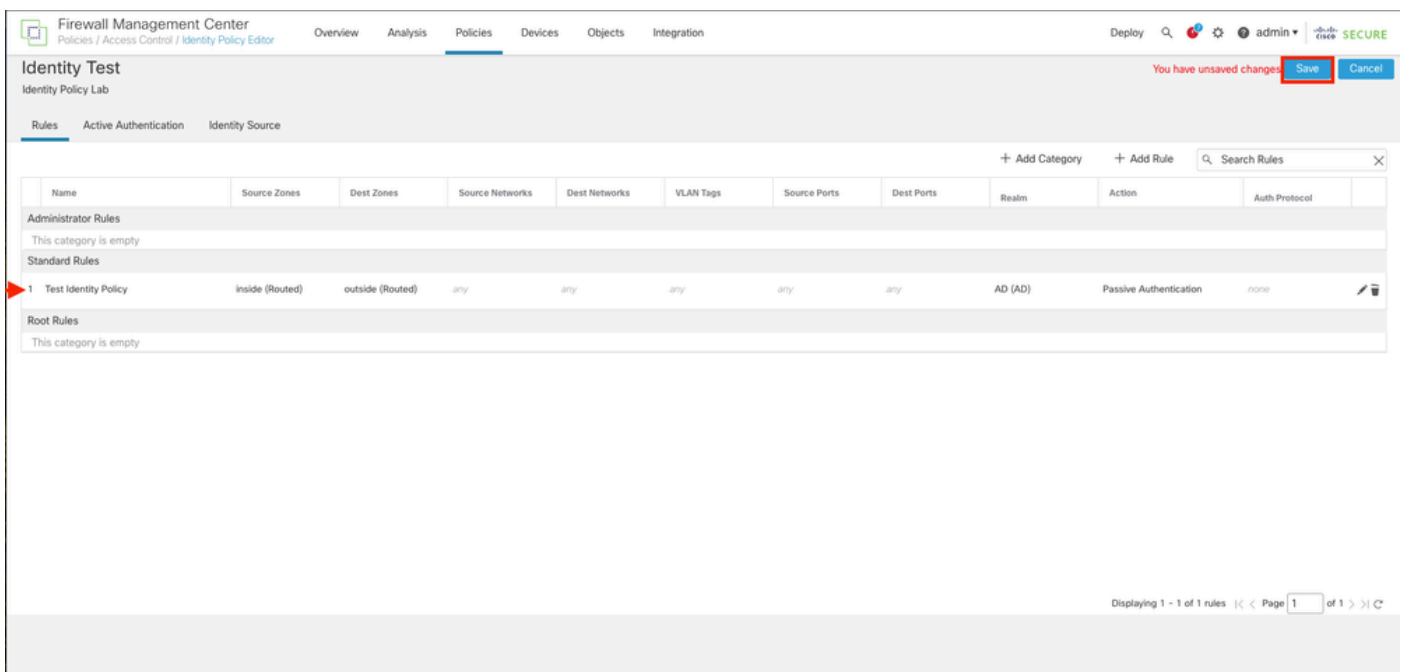
注意：在本文档中，用户检测将仅应用于来自内部区域且被转发到外部区域的流量。

---

7. 选择添加和保存。



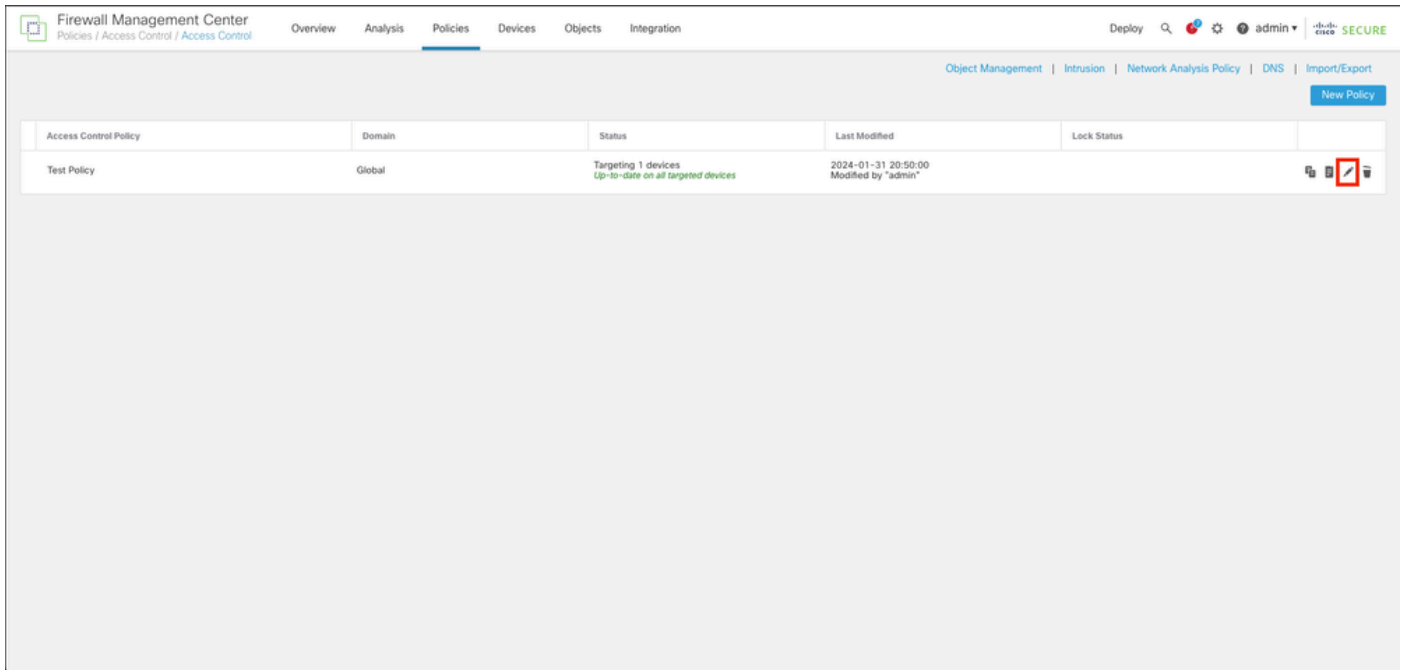
第五步：验证身份策略中的新规则并点击保存。



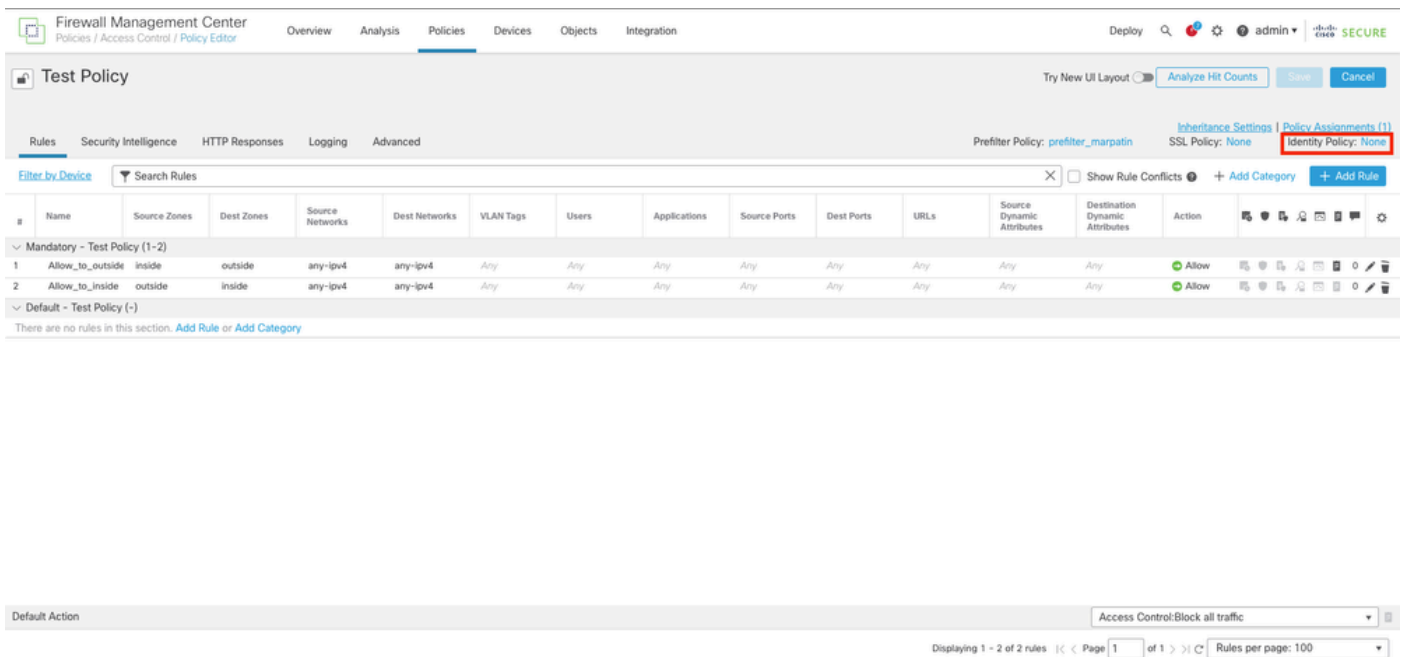
第六步：导航到策略>访问控制

步骤 7. 确定要在处理用户流量的防火墙中部署的访问控制策略，然后单击铅笔图标上的以编辑策略。

。

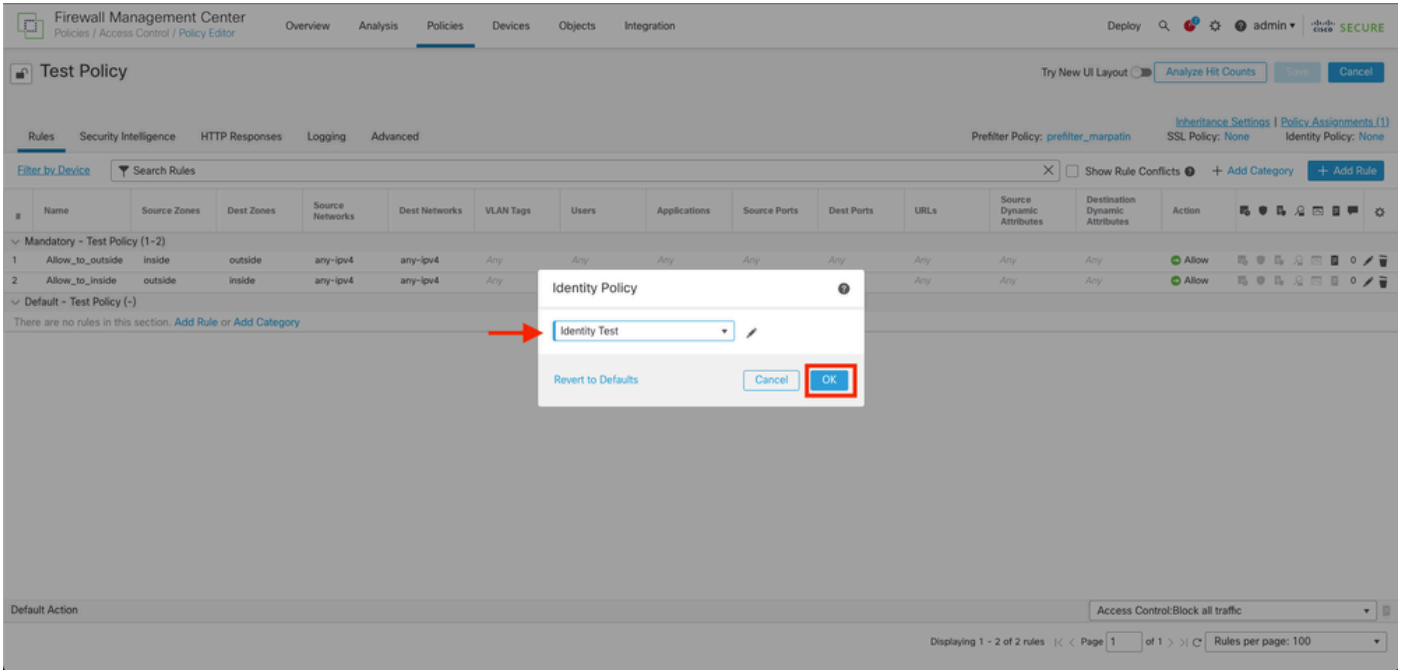


第六步：在Identity Policy字段中单击None。



步骤 7.从下拉菜单中选择之前在步骤3中创建的策略，然后单击OK以完成配置。





第8步：保存配置并部署到FTD。

## 验证

1. 在FMC GUI中，导航至分析>用户：活动会话

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

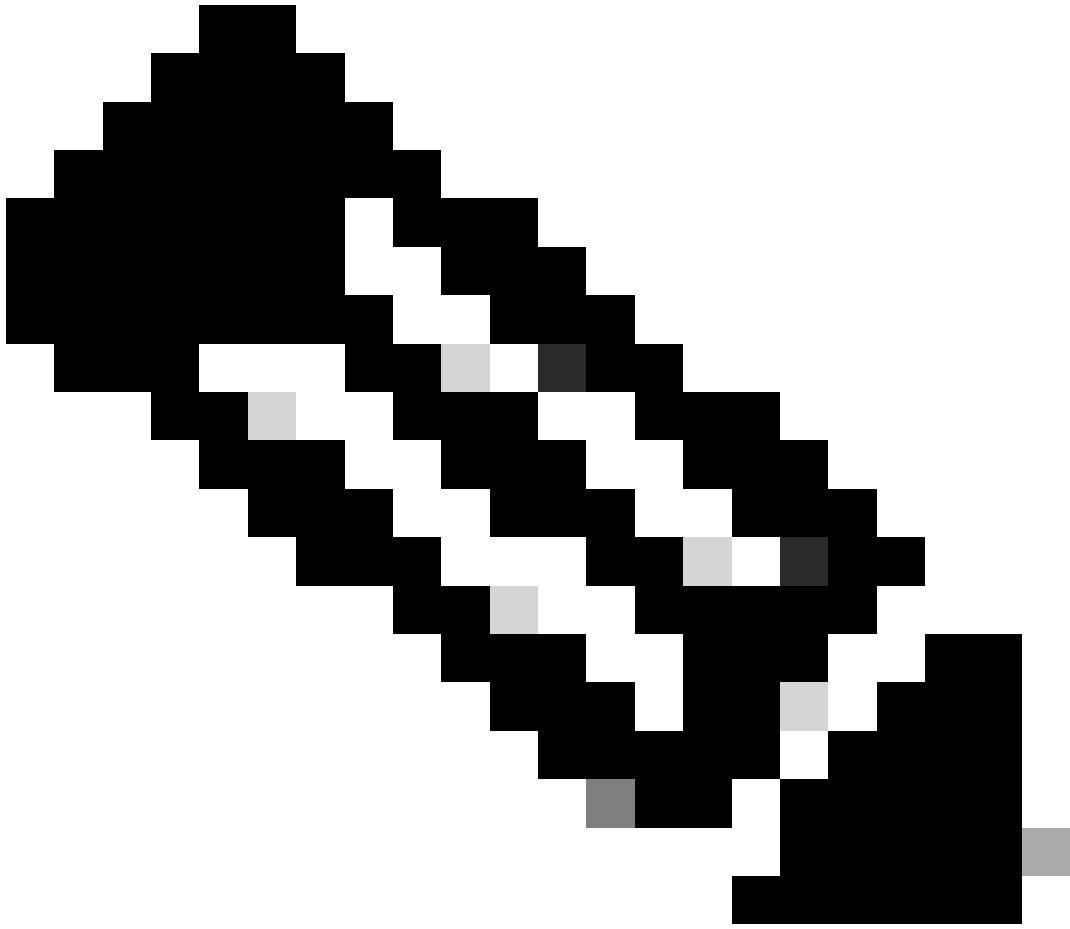
3. 通过分析>连接>事件：连接事件表视图进行验证

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	



注意：与身份策略和访问控制策略的流量条件匹配的用户在User字段中显示其用户名。

---

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。