

# Configure Identity Policy on Secure Firewall Management Center (FMC)

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Configure](#)

[Configurations](#)

### [Verify](#)

---

## Introduction

This document describes the process of how to configure and deploy an Identity Policy for a Secure FTD traffic through Secure FMC.

## Prerequisites

1. Realm already configured in FMC.
2. Identity Source already Configured - ISE, ISE-PIC.

---

**Note:** ISE and Realm configurations instructions are out of the scope of this document.

---

## Requirements

Cisco recommends having knowledge of these topics:

- Secure Firewall Management Center (FMC)
- Secure Firewall Threat Defense (FTD)
- Cisco Identity Services Engine (ISE)
- LDAP/AD servers(s)
- Authentication Methods

1. Passive Authentication : Use of external identity user source such as ISE
2. Active authentication : Use of the managed device as Authenticate source (captive portal or remote vpn access)
3. No Authentication

## Components Used

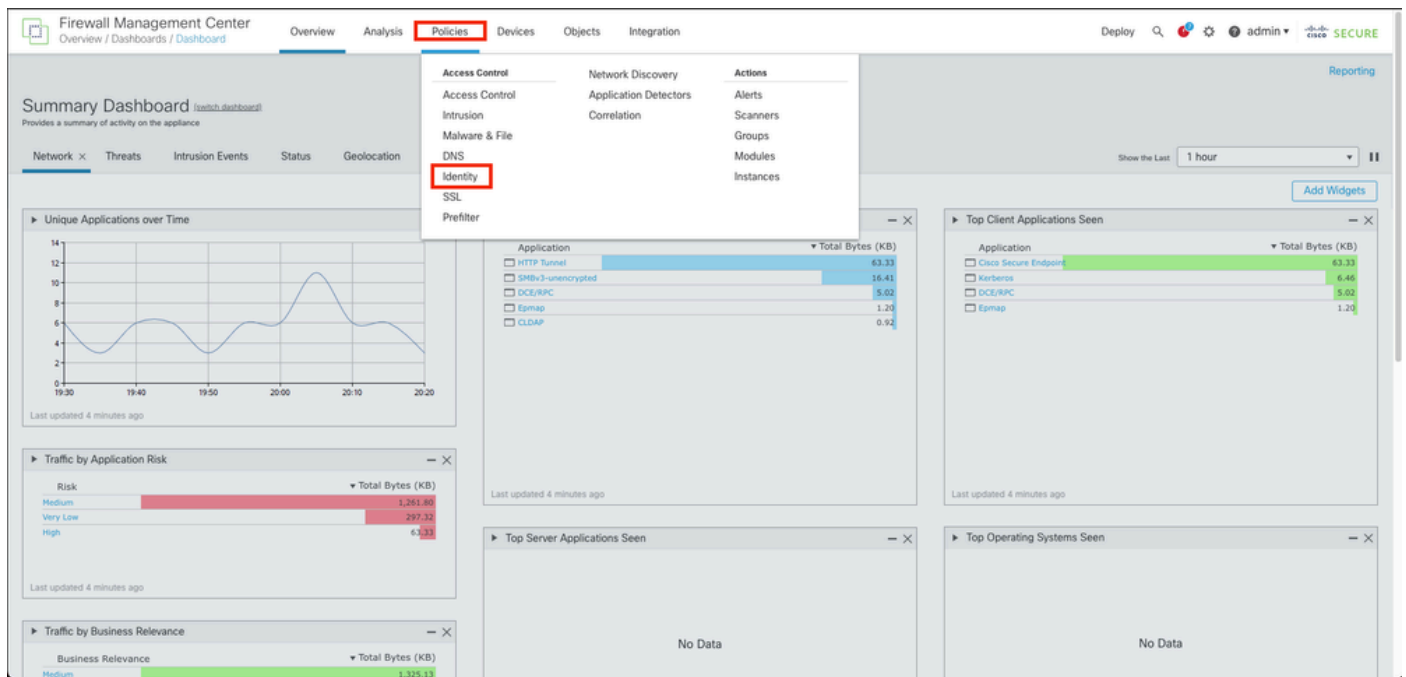
- Secure Firewall Management Center for VMWare v7.2.5
- Cisco Secure Firewall Threat Defense for VMWare v7.2.4
- Active Directory Server
- Cisco Identity Services Engine (ISE) v3.2 patch 4
- Passive Authentication Method

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

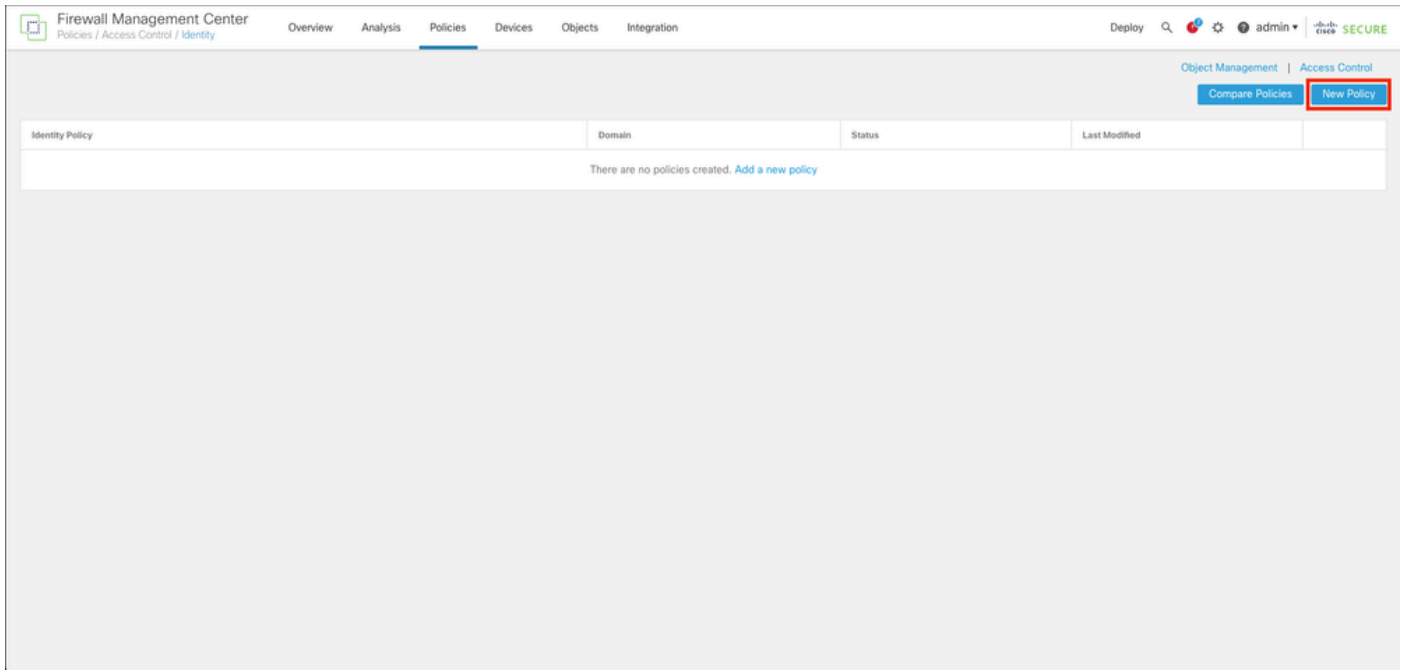
# Configure

## Configurations

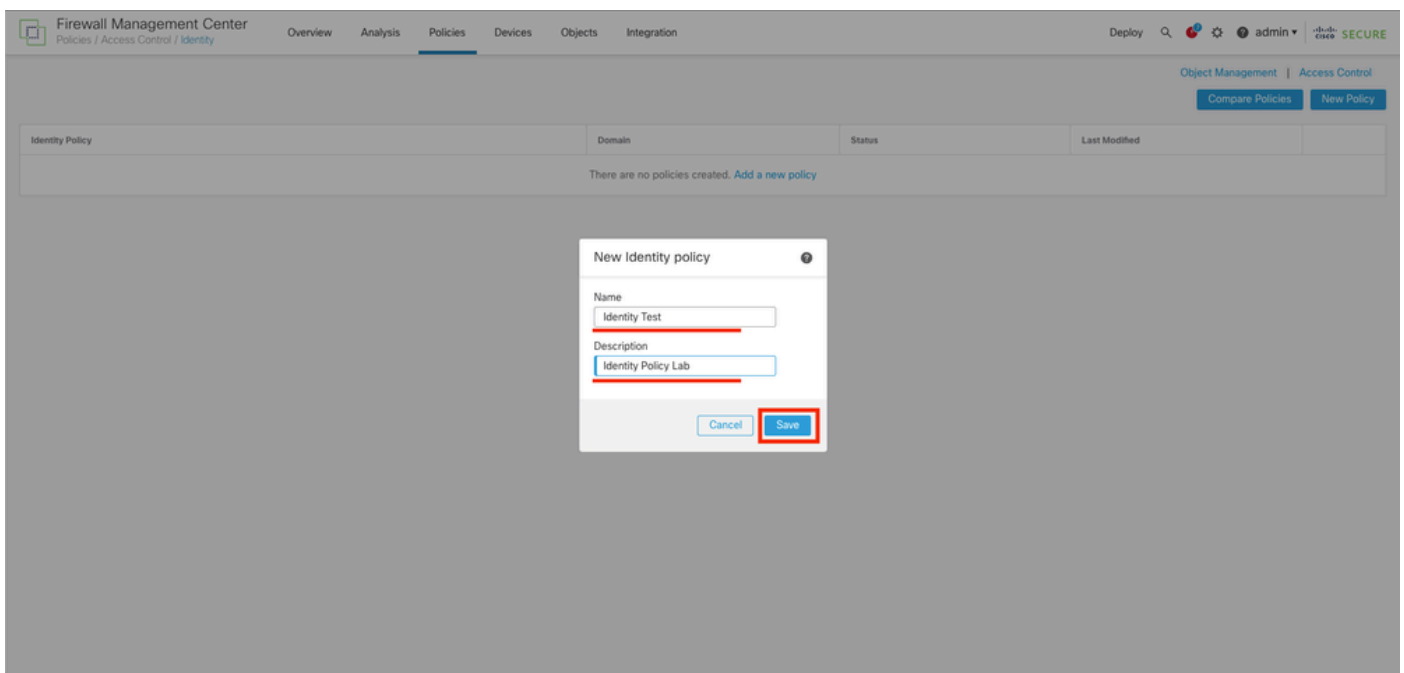
**Step 1.** In the FMC GUI, Navigate to **Policies > Access Control > Identity**



**Step 2.** Click **New Policy**.

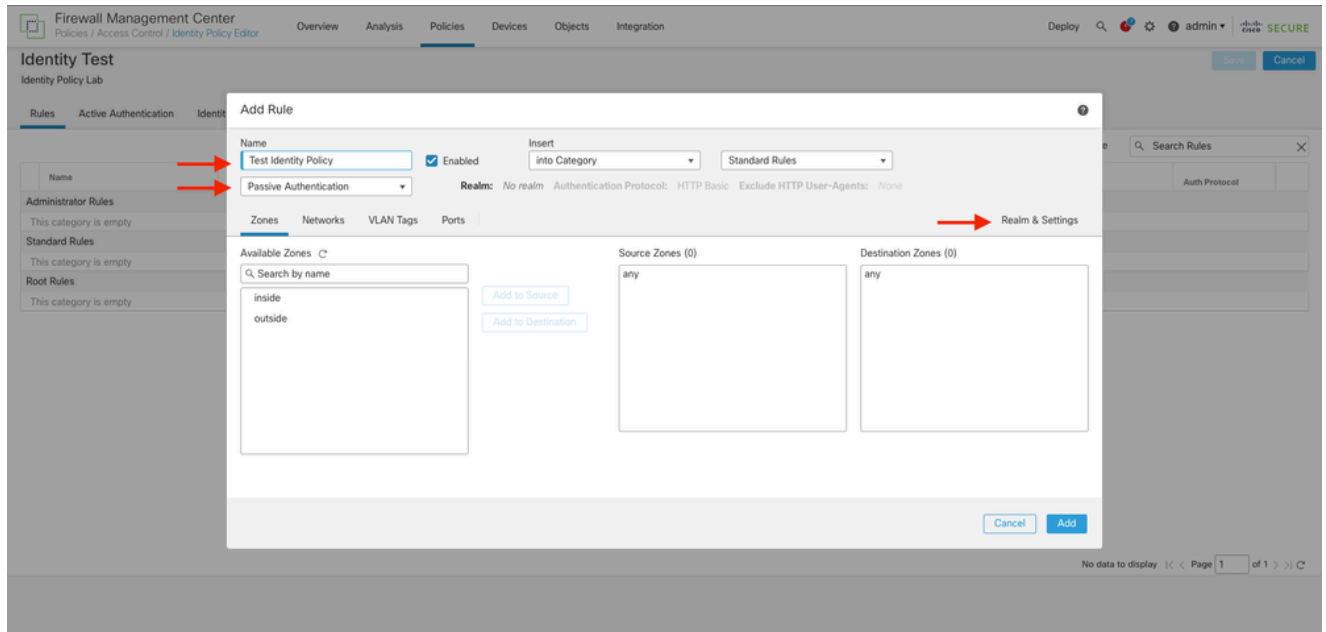


**Step 3.** Assign a **name** and **description** to the new Identity Policy, then click **Save**.

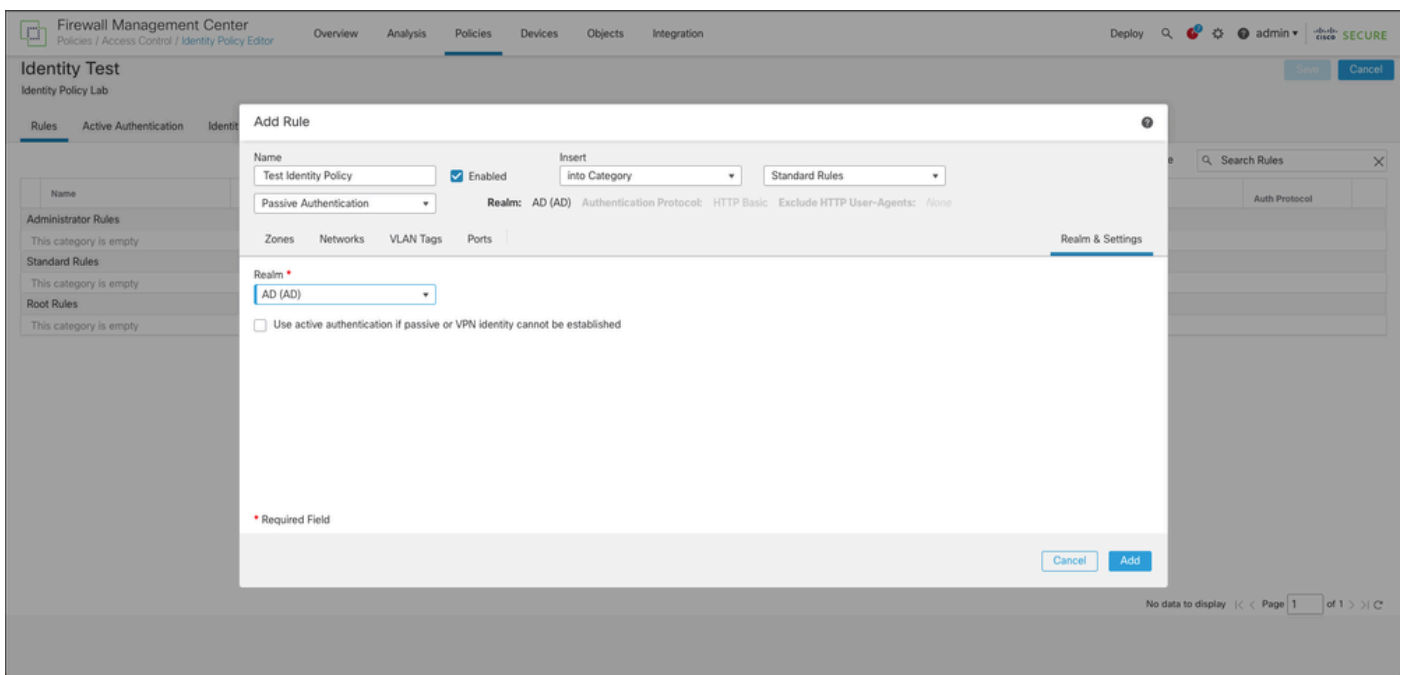


**Step 4.** Click on + **Add Rule** Icon.

1. Assign a name to the new rule.
2. Under the name field, choose the authentication method, select : **Passive Authentication**.
3. At the right of the screen select **Realm & Settings**.



4. Select a **Realm** from the drop down menu.



5. Click on **Zones** at the left of the screen.

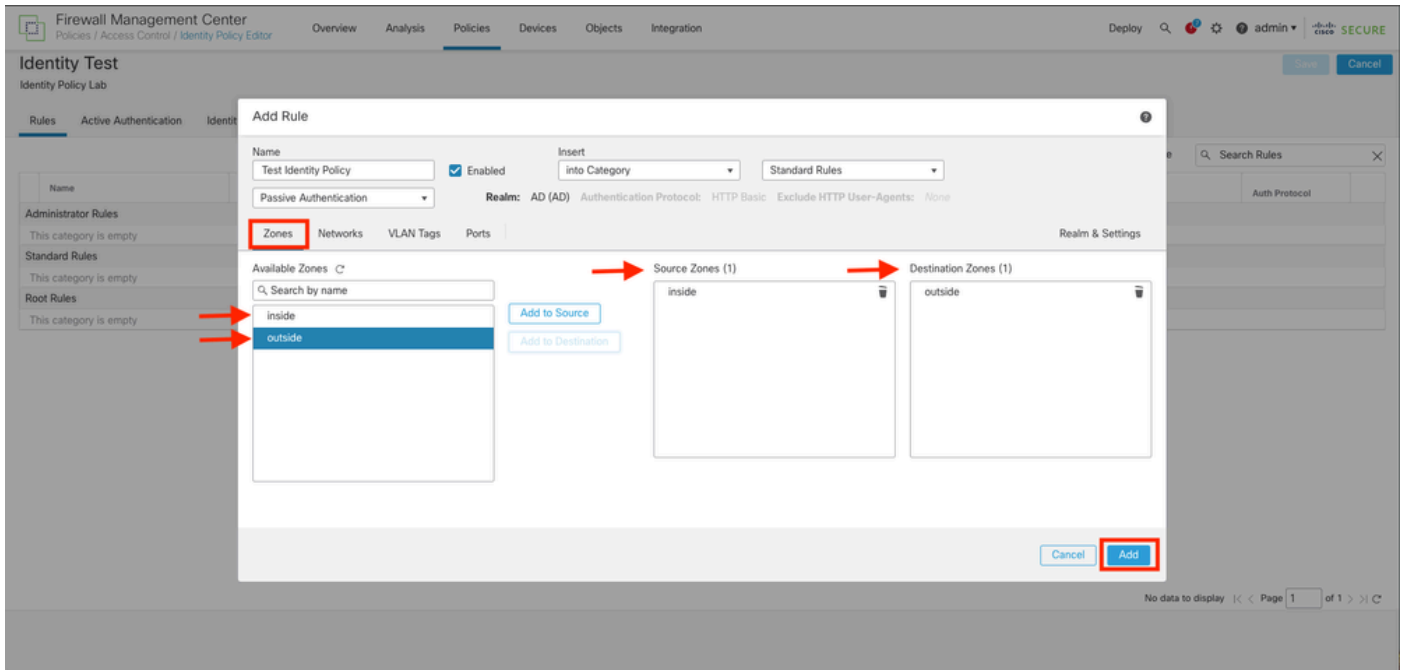
6. From the **Available Zones** menu assign a **source** and **destination** zone based in the traffic path that is needed to detect users. To add a zone click on the name of the zone and then select depending on the case **Add to Source** or **Add to Destination**.



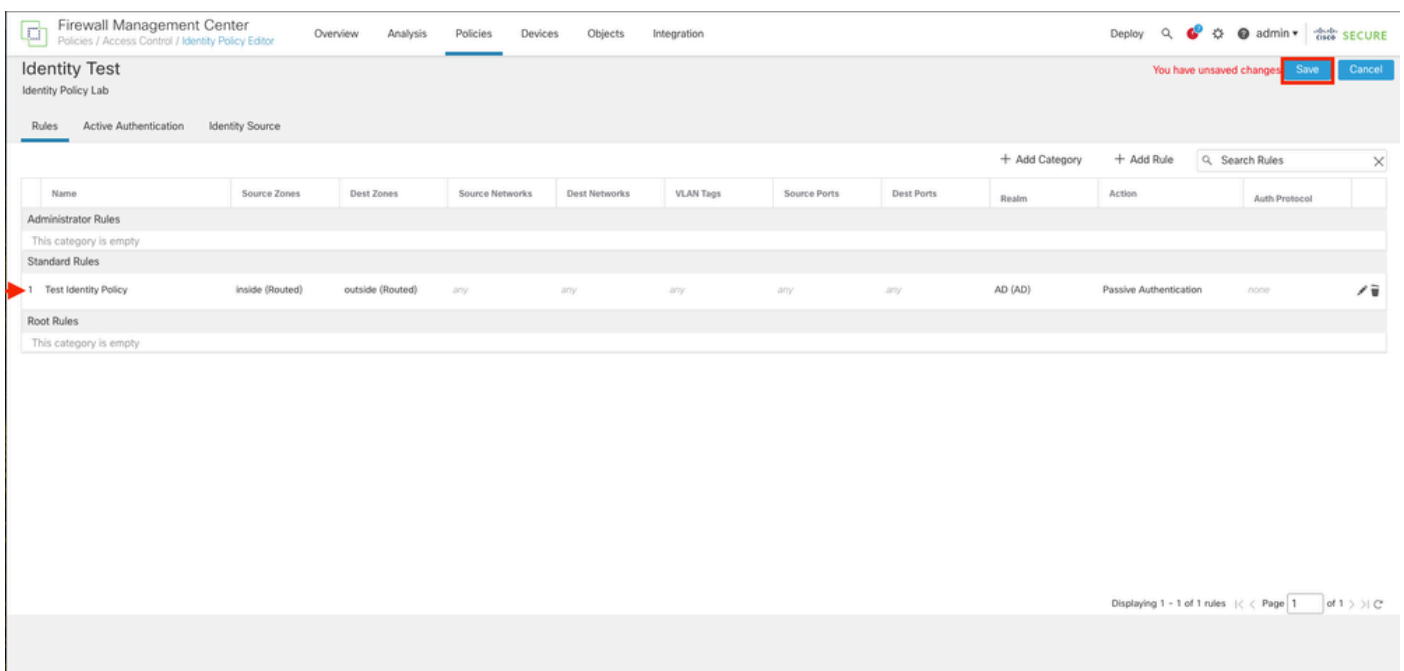
**Note:** In this documentation the user detection is going to be applied only for the traffic comes from the inside zone and it is forwarded to the outside zone.

---

7. Select **Add** and **Save**.

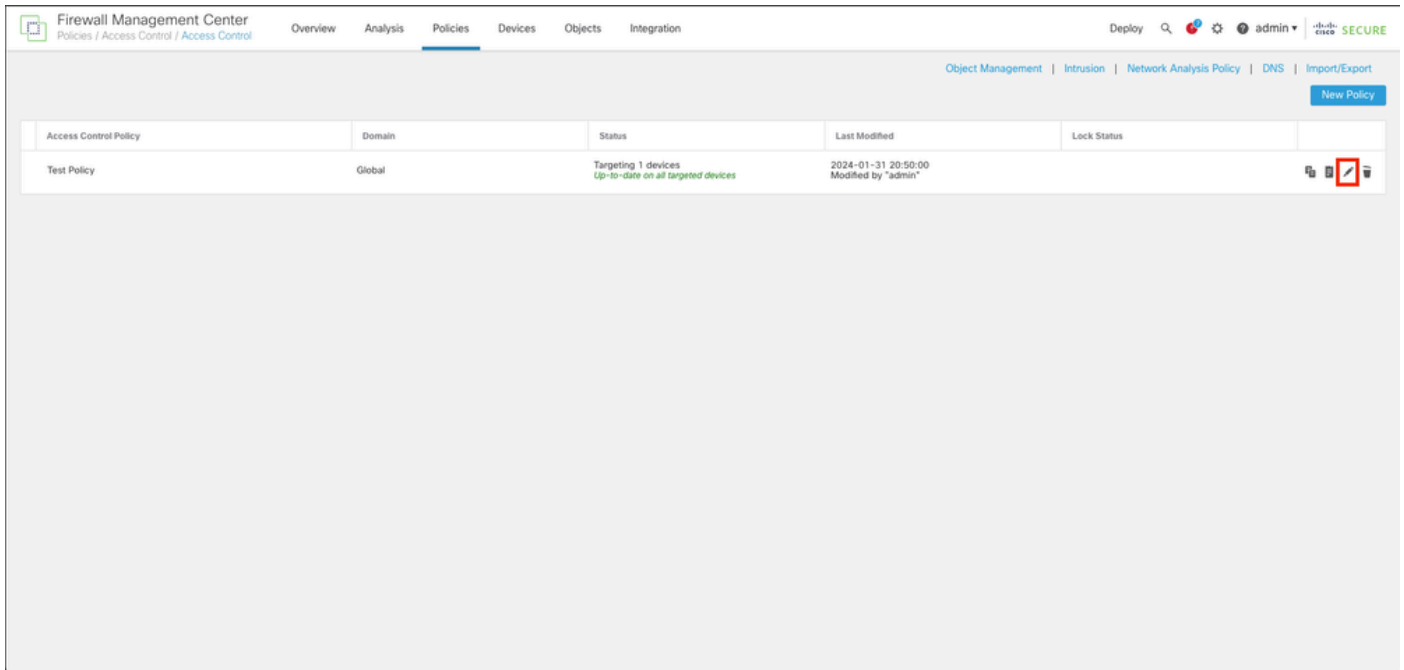


**Step 5.** Validate the new Rule is in the Identity Policy and click on **Save**.

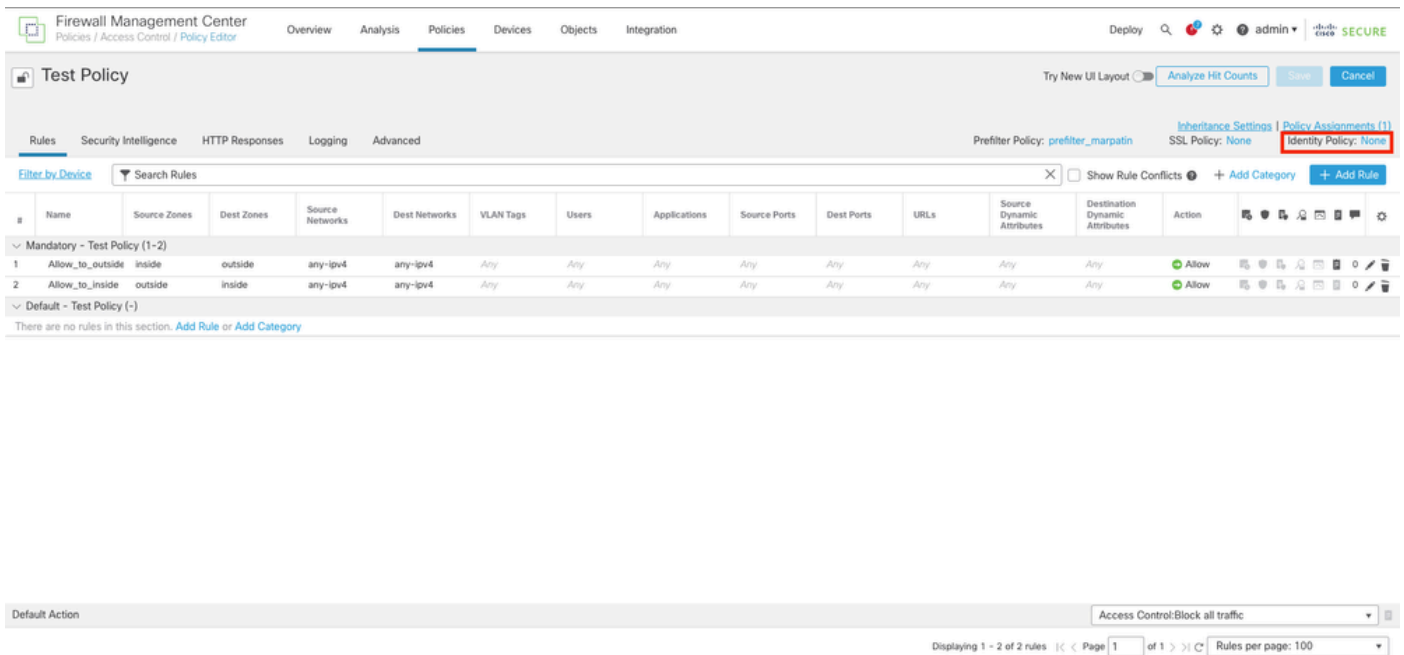


**Step 6.** Navigate to **Policies > Access Control**

**Step 7.** Identify the **Access Control Policy** that it is going to be deployed in the Firewall handling the users traffic and **click** over the **pencil icon** in order to edit the policy.



**Step 6.** Click on **None** in the **Identity Policy** field.



**Step 7.** From the Drop down menu, select the Policy created previously in **step 3**, then, click **OK** to finish the configuration.



Firewall Management Center

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Admin Admin **SECURE**

Test Policy

Try New UI Layout Analyze Hit Counts Save Cancel

Rules Security Intelligence HTTP Responses Logging Advanced

Prefilter Policy: prefilter\_marpatin Inheritance Settings Policy Assignments (1) SSL Policy: None Identity Policy: None

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

| #  | Name             | Source Zones | Dest Zones | Source Networks | Dest Networks | VLAN Tags | Users | Applications | Source Ports | Dest Ports | URLs | Source Dynamic Attributes | Destination Dynamic Attributes | Action |
|--|------------------|--------------|------------|-----------------|---------------|-----------|-------|--------------|--------------|------------|------|---------------------------|--------------------------------|--------|
| Mandatory - Test Policy (1-2)                                |                  |              |            |                 |               |           |       |              |              |            |      |                           |                                |        |
| 1  | Allow_to_outside | inside       | outside    | any-ipv4        | any-ipv4      | Any       | Any   | Any          | Any          | Any        | Any  | Any                       | Any                            | Allow  |
| 2  | Allow_to_inside  | outside      | inside     | any-ipv4        | any-ipv4      | Any       | Any   | Any          | Any          | Any        | Any  | Any                       | Any                            | Allow  |
| Default - Test Policy (-)                                    |                  |              |            |                 |               |           |       |              |              |            |      |                           |                                |        |
| There are no rules in this section. Add Rule or Add Category |                  |              |            |                 |               |           |       |              |              |            |      |                           |                                |        |

Identity Policy

Identity Test

Revert to Defaults Cancel **OK**

Default Action Access Control:Block all traffic

Displaying 1 - 2 of 2 rules Page 1 of 1 Rules per page: 100

**Step 8. Save and deploy** the configuration to the FTD.

## Verify

1. In the FMC GUI navigate to **Analysis > Users: Active Sessions**

No Search Constraints (Edit Search)

Table View of Active Sessions Active Sessions

Jump to...

|   | Login Time          | Last Seen           | User                   | Authentication Type    | Current IP  | Realm | Username | First Name | Last Name | E-Mail             | Department      | Phone | Discovery Application | Device   |
|---|---------------------|---------------------|------------------------|------------------------|-------------|-------|----------|------------|-----------|--------------------|-----------------|-------|-----------------------|----------|
| ▼ | 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. Validation from **Analysis > Connection > Events: Table view of Connections events**

Search Constraints (Edit Search Save Search)

Connections with Application Details Table View of Connection Events

Jump to...

|   | First Packet        | Last Packet | Action | Reason | Initiator IP | Initiator Country | Initiator User         | Responder IP | Responder Country | Security Intelligence Category | Ingress Security Zone | Egress Security Zone | Source Port / ICMP Type | Destination Port / ICMP Code | SSL Status | Application Protocol | Client | CI          | VI |
|---|---------------------|-------------|--------|--------|--------------|-------------------|------------------------|--------------|-------------------|--------------------------------|-----------------------|----------------------|-------------------------|------------------------------|------------|----------------------|--------|-------------|----|
| ▼ | 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 |    |



**Note:** Users matching the traffic criteria for the Identity Policy and Access Control Policy are shown their username in the User field.

---