Konfigurieren der Identitätsrichtlinie im Secure Firewall Management Center (FMC)

Inhalt

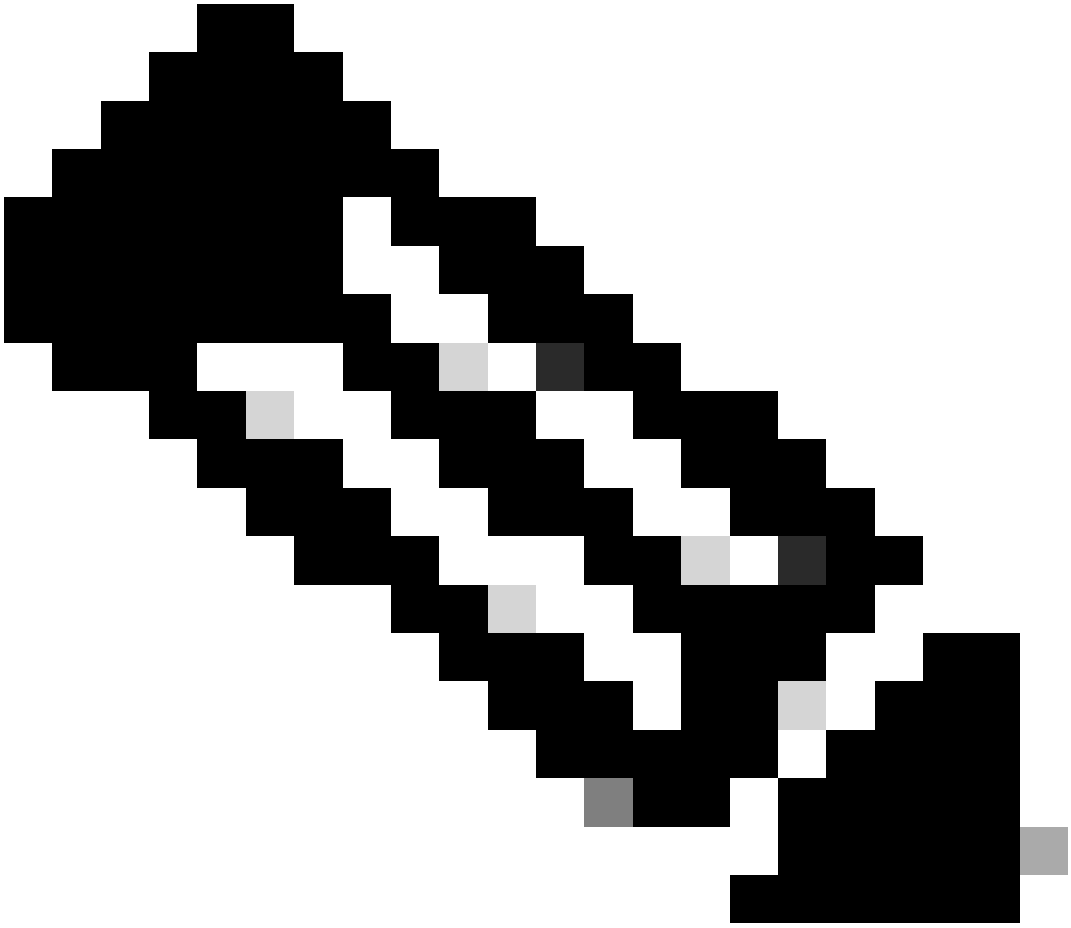
Einleitung

Dieses Dokument beschreibt den Prozess der Konfiguration und Bereitstellung einer Identitätsrichtlinie für einen sicheren FTD-Datenverkehr über Secure FMC.

Voraussetzungen

1. Bereich bereits in FMC konfiguriert.

2. Identitätsquelle bereits konfiguriert - ISE, ISE-PIC.



Hinweis: Konfigurationsanweisungen für ISE und Bereiche werden in diesem Dokument nicht behandelt.

Anforderungen

Cisco empfiehlt, in den folgenden Bereichen über Kenntnisse zu verfügen:

- Secure Firewall Management Center (FMC)
- Sicherer Firewall-Thread-Schutz (FTD)
- Cisco Identity Services Engine (ISE)
- LDAP-/AD-Server
- Authentifizierungsmethoden

1. Passive Authentifizierung: Verwendung einer externen Identitätsbenutzerquelle wie ISE
2. Aktive Authentifizierung: Verwendung des verwalteten Geräts als Authentifizierungsquelle (Captive Portal oder Remote-VPN-Zugriff)

3. Keine Authentifizierung

Verwendete Komponenten

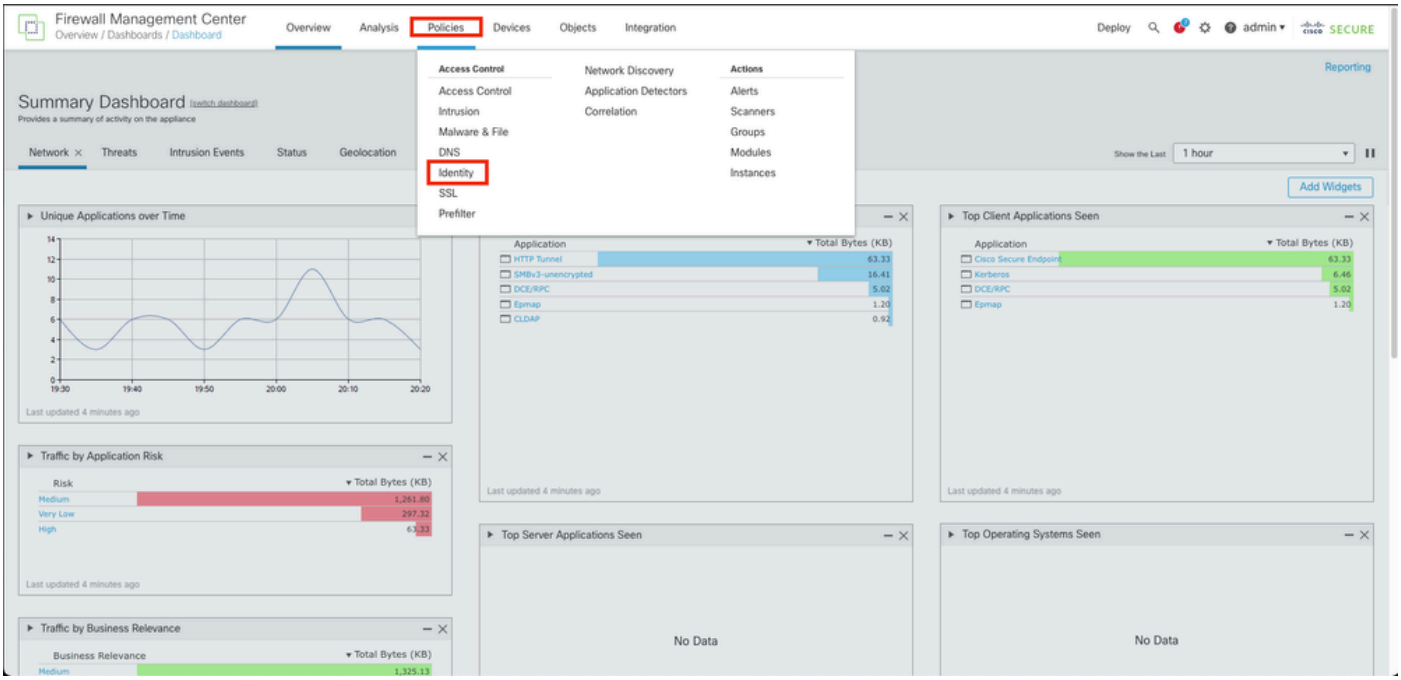
- Secure Firewall Management Center für VMWare v7.2.5
- Cisco Secure Firewall Threat Defense für VMWare v7.2.4
- Active Directory-Server
- Cisco Identity Services Engine (ISE) v3.2 Patch 4
- Passive Authentifizierungsmethode

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

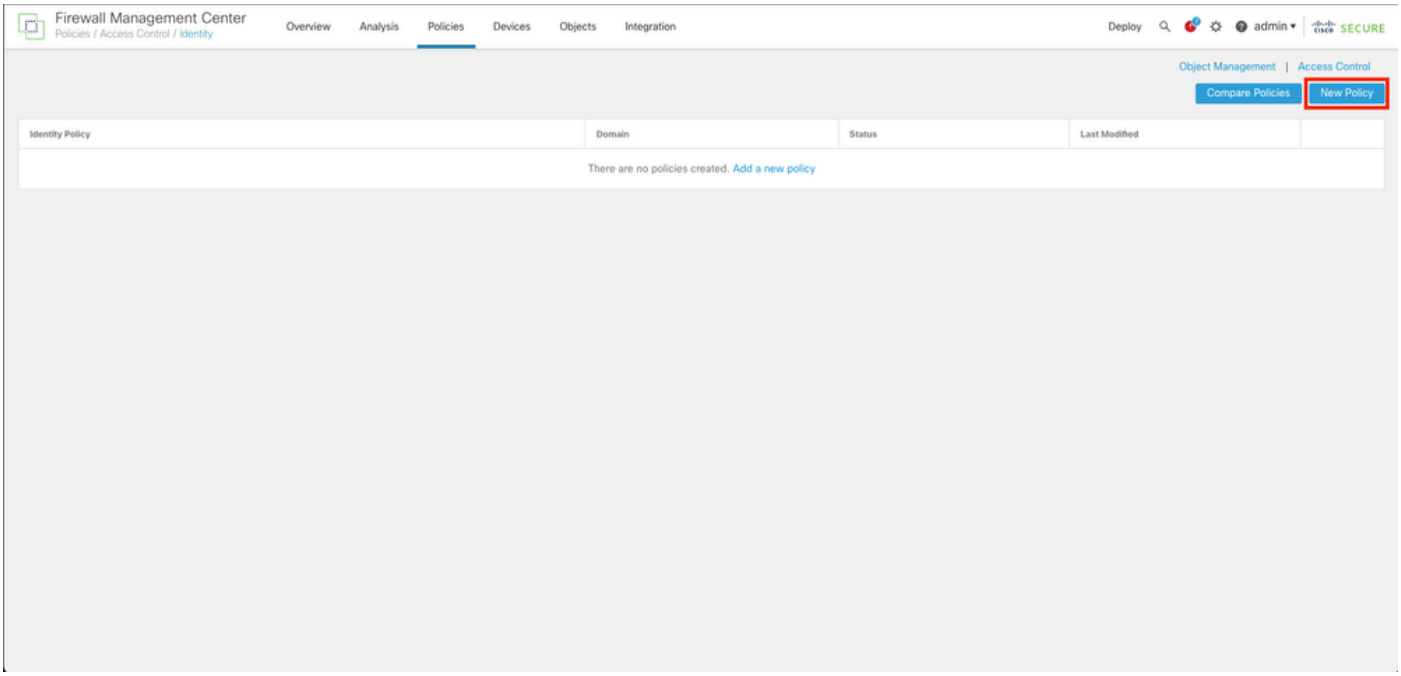
Konfigurieren

Konfigurationen

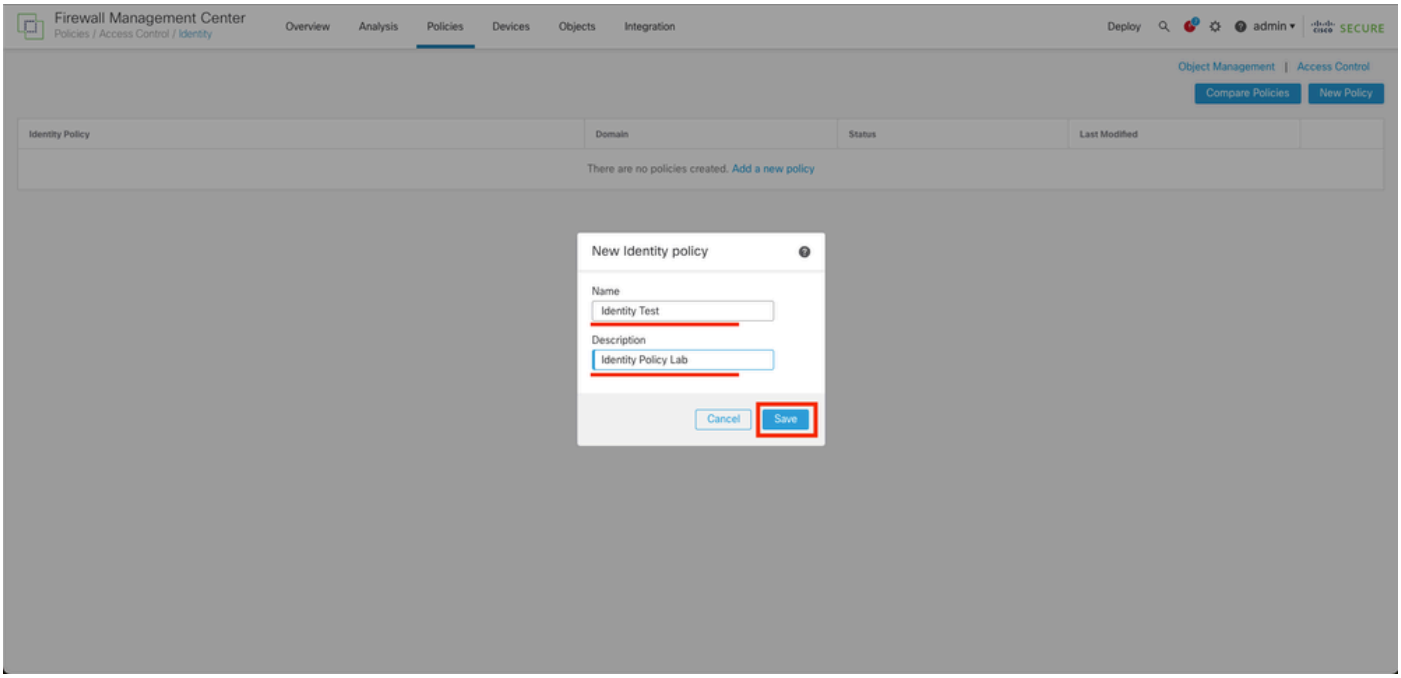
Schritt 1: Navigieren Sie in der FMC-GUI zu Policies > Access Control > Identity.



Schritt 2: Klicken Sie auf Neue Richtlinie.

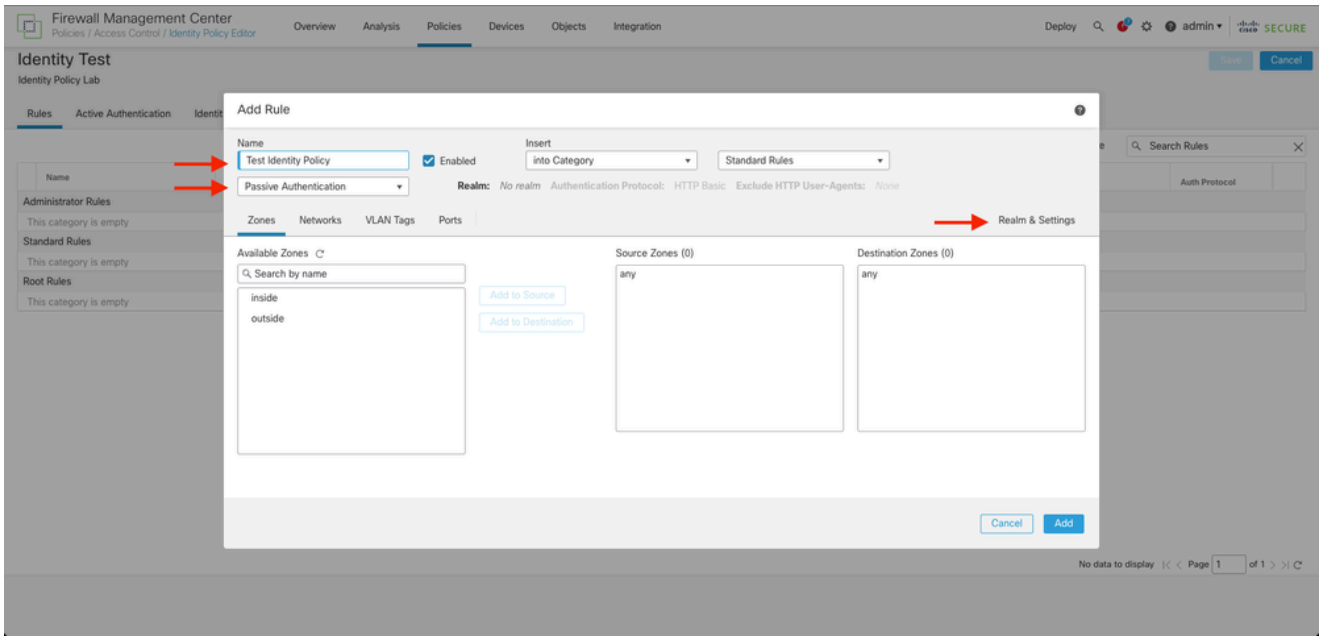


Schritt 3: Weisen Sie der neuen Identitätsrichtlinie einen Namen und eine Beschreibung zu, und klicken Sie dann auf Speichern.

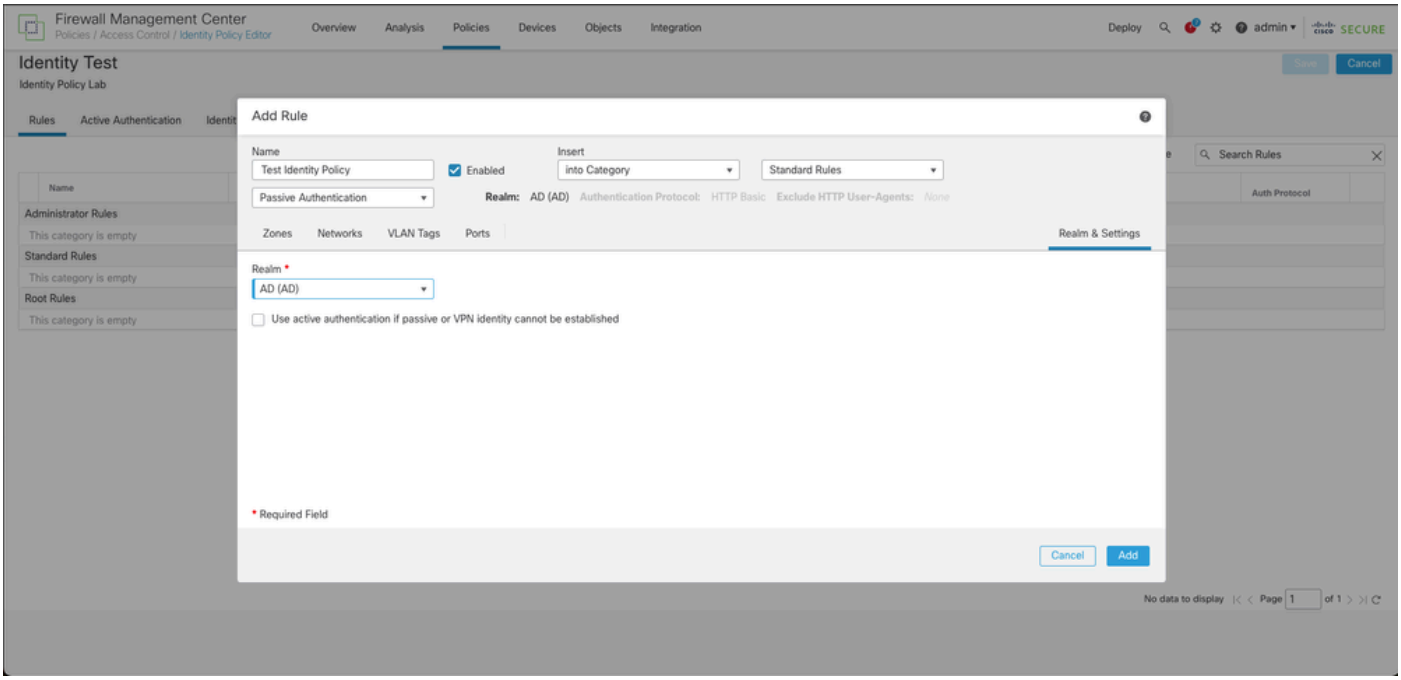


Schritt 4: Klicken Sie auf das Symbol + Regel hinzufügen.

1. Zuweisen eines Namens zur neuen Regel
2. Wählen Sie im Namensfeld die Authentifizierungsmethode aus und wählen Sie : Passive Authentifizierung.
3. Klicken Sie rechts im Bildschirm auf Realm & Settings (Bereich und Einstellungen).

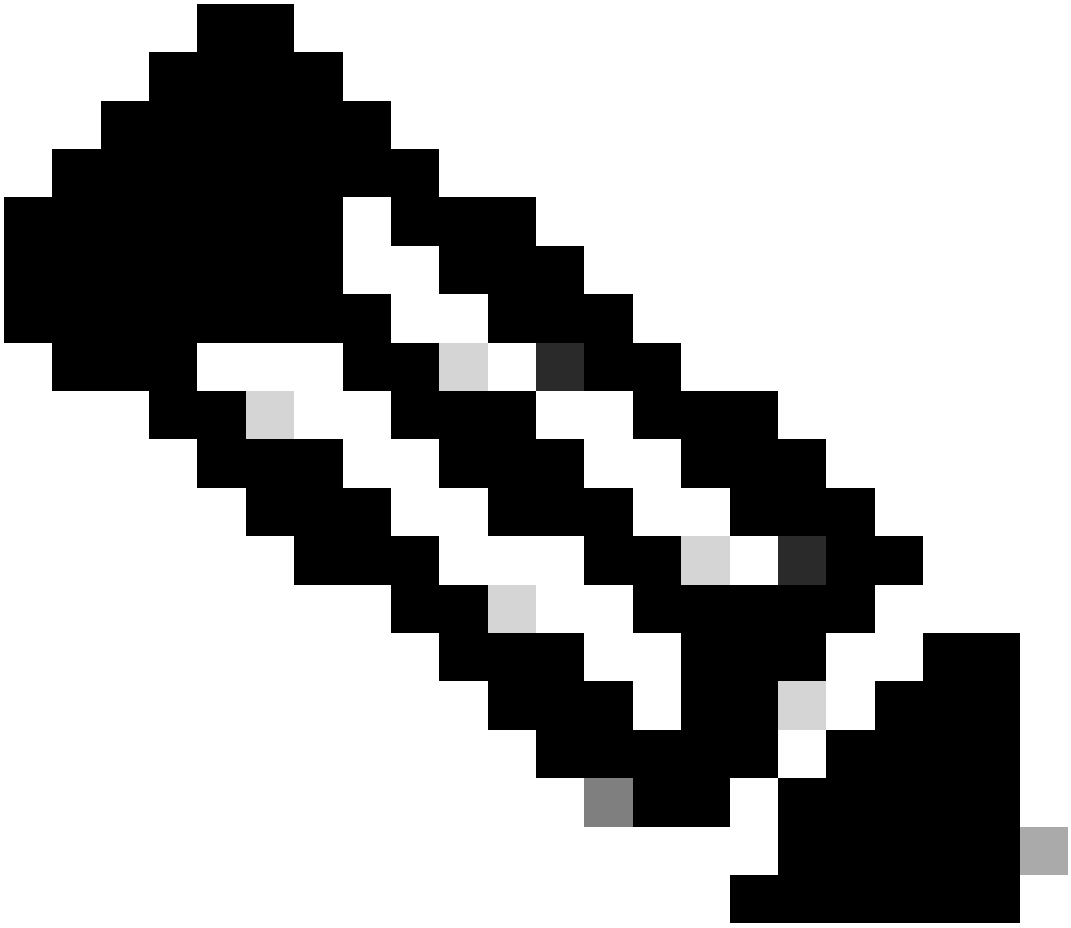


4. Wählen Sie einen Bereich aus dem Dropdown-Menü.



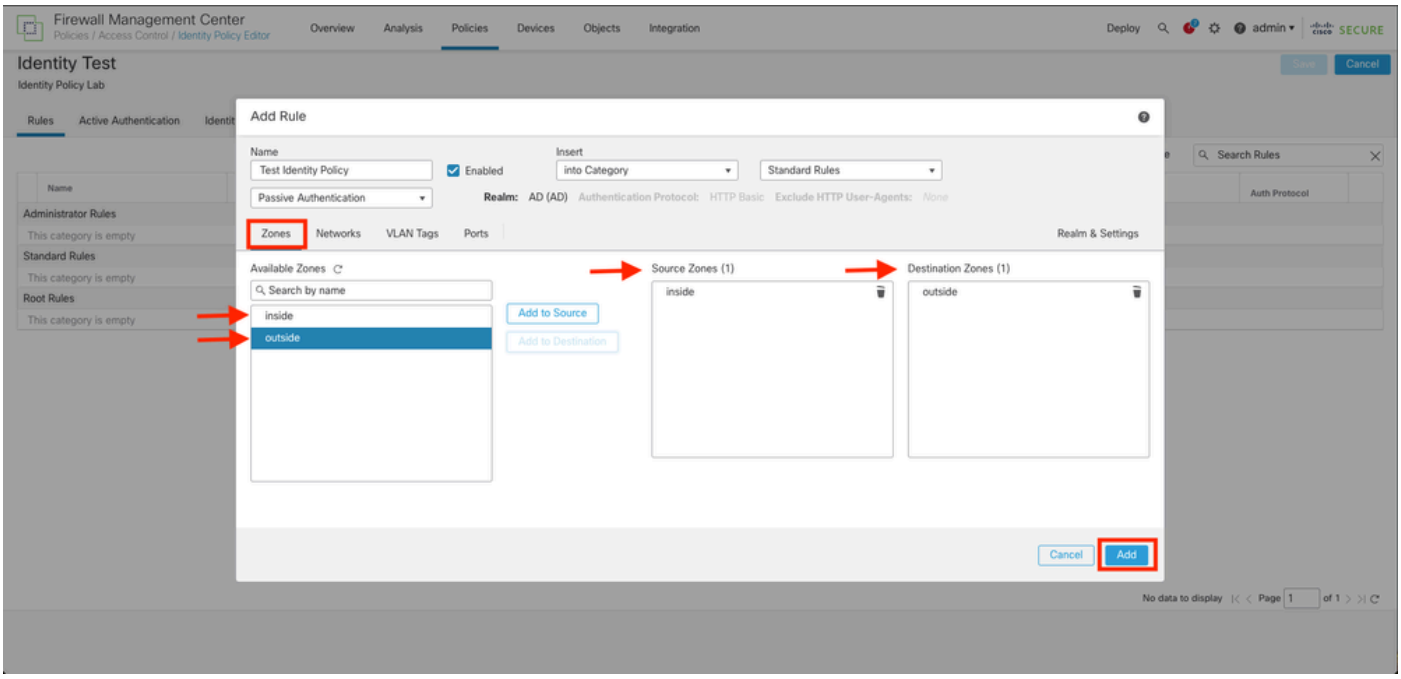
5. Klicken Sie auf Zonen links im Bildschirm.

6. Weisen Sie im Menü Verfügbare Zonen eine Quell- und Zielzone zu, die auf dem Datenverkehrspfad basiert, der zum Erkennen von Benutzern benötigt wird. Um eine Zone hinzuzufügen, klicken Sie auf den Namen der Zone, und wählen Sie sie dann je nach Fall Add to Source (Zur Quelle hinzufügen) oder Add to Destination (Zu Ziel hinzufügen) aus.

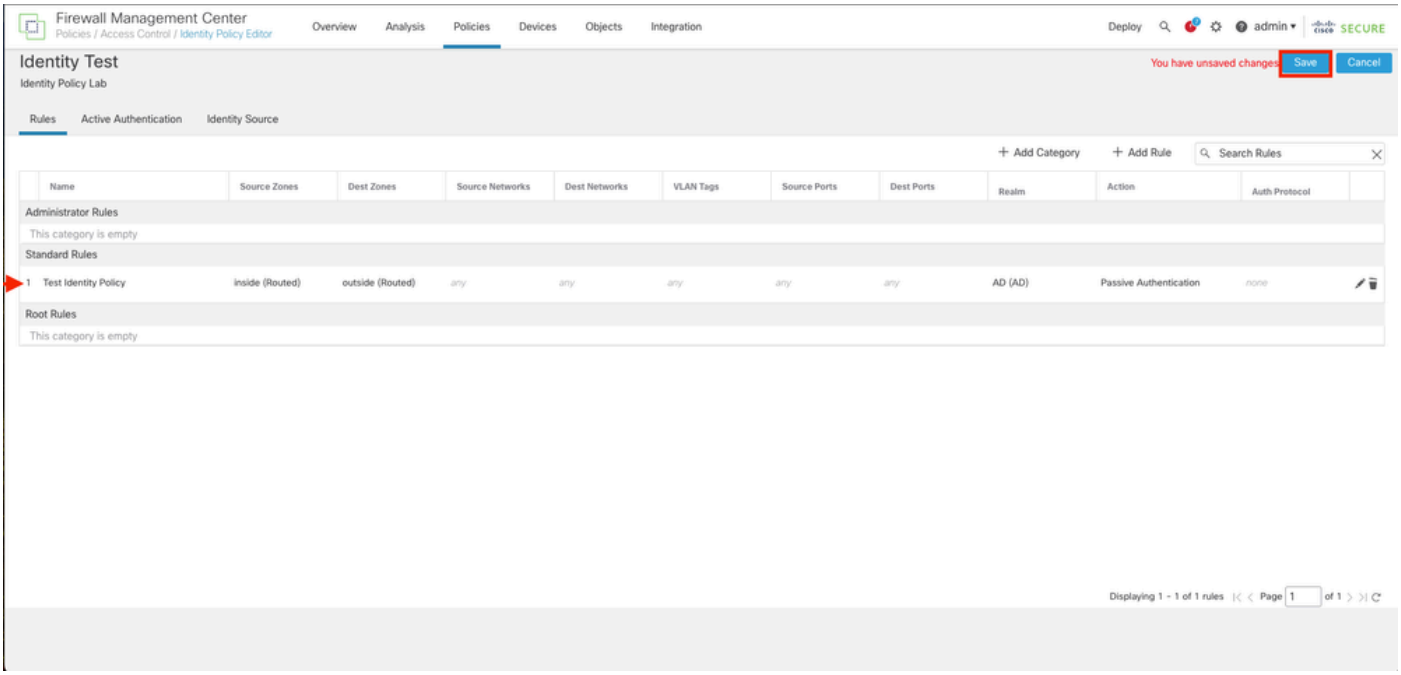


Hinweis: In dieser Dokumentation wird die Benutzererkennung nur für den Datenverkehr angewendet, der aus der Innenzone stammt und an die Außenzone weitergeleitet wird.

7. Wählen Sie Hinzufügen und Speichern.

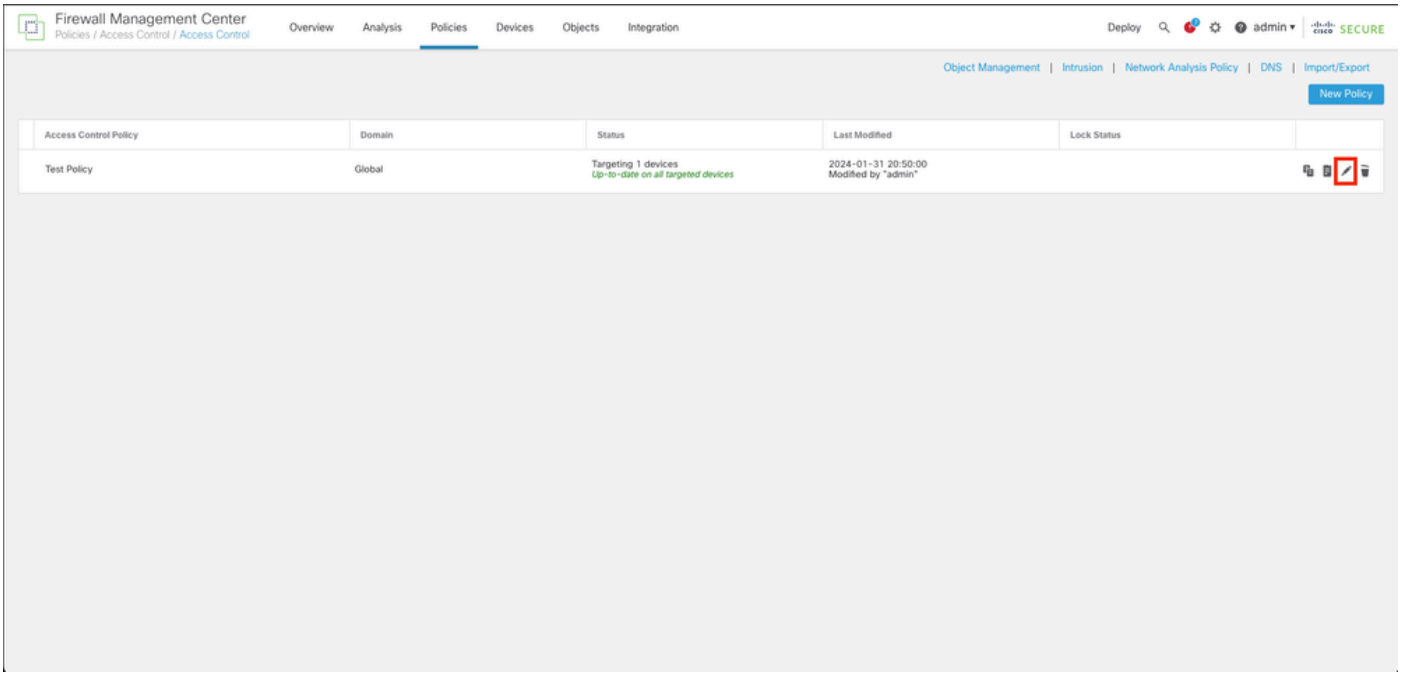


Schritt 5: Überprüfen Sie, ob die neue Regel in der Identitätsrichtlinie enthalten ist, und klicken Sie auf Speichern.

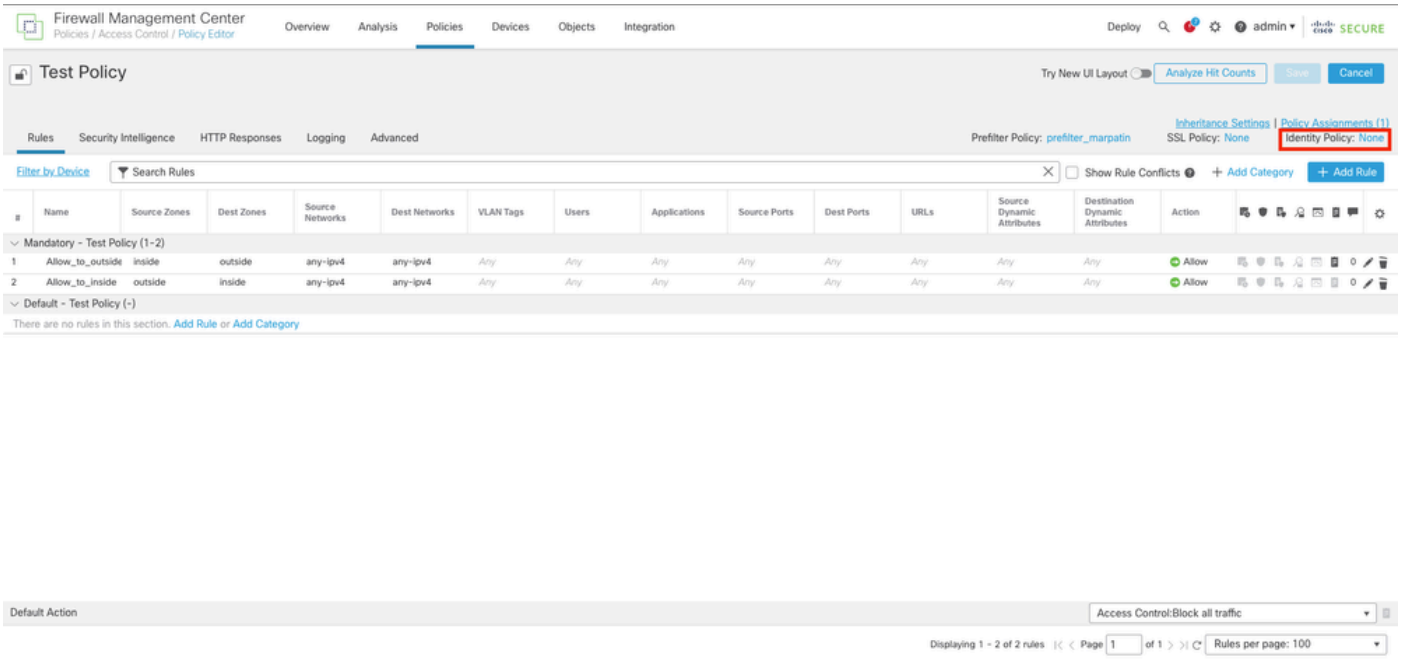


Schritt 6: Navigieren Sie zu Richtlinien > Zugriffskontrolle.

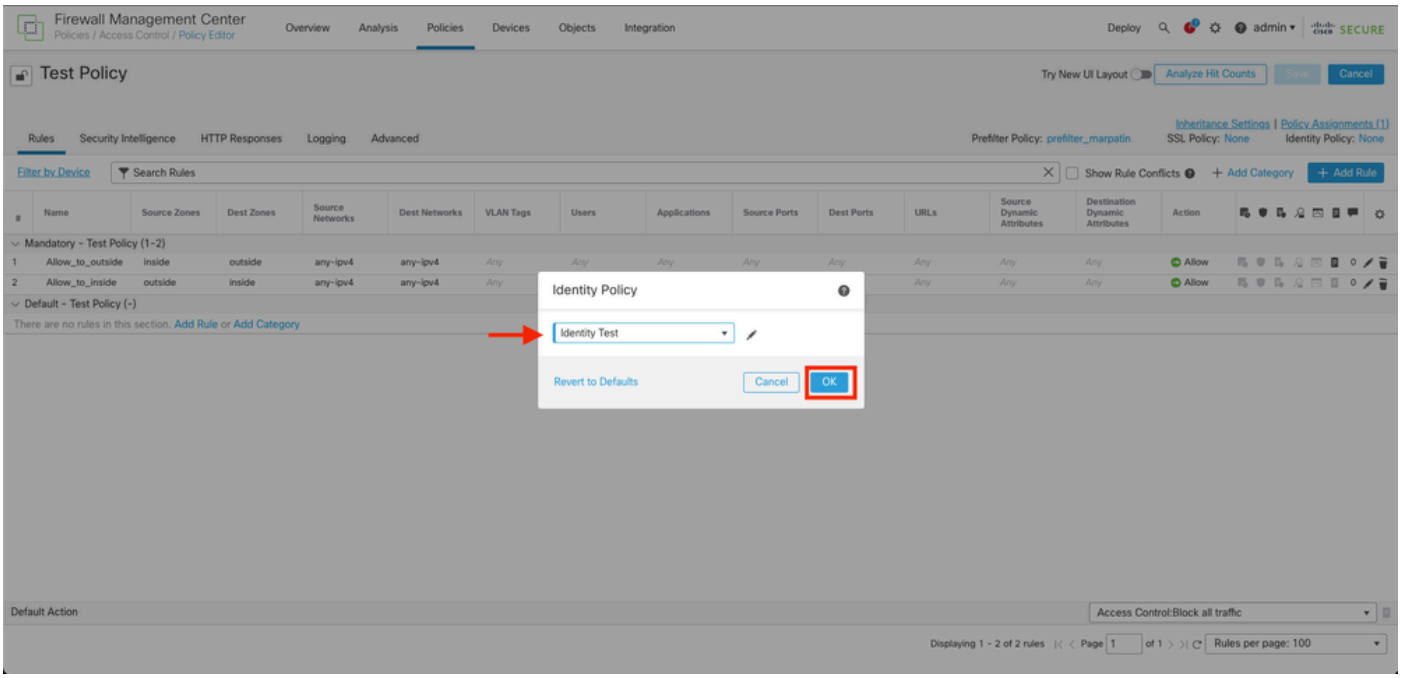
Schritt 7. Identifizieren Sie die Zugriffskontrollrichtlinie, die in der Firewall bereitgestellt werden soll, die den Benutzerdatenverkehr verarbeitet, und klicken Sie auf das Bleistiftsymbol, um die Richtlinie zu bearbeiten.



Schritt 6: Klicken Sie im Feld Identitätsrichtlinie auf Keine.



Schritt 7. Wählen Sie im Dropdown-Menü die zuvor in Schritt 3 erstellte Richtlinie aus, und klicken Sie dann auf OK, um die Konfiguration abzuschließen.

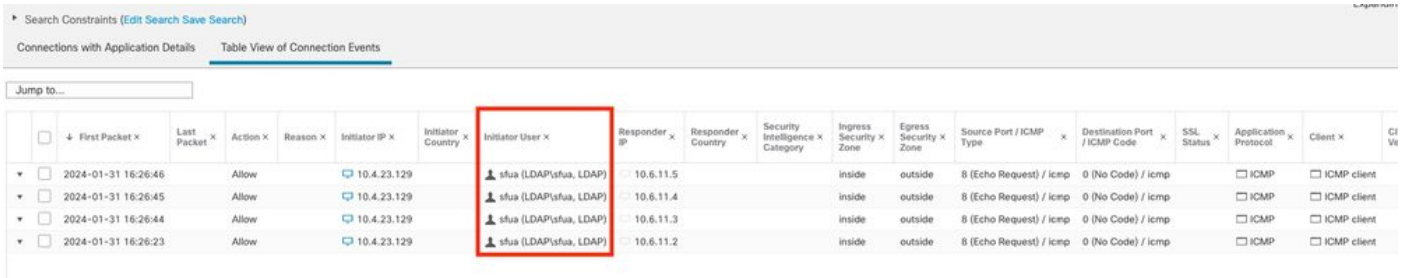


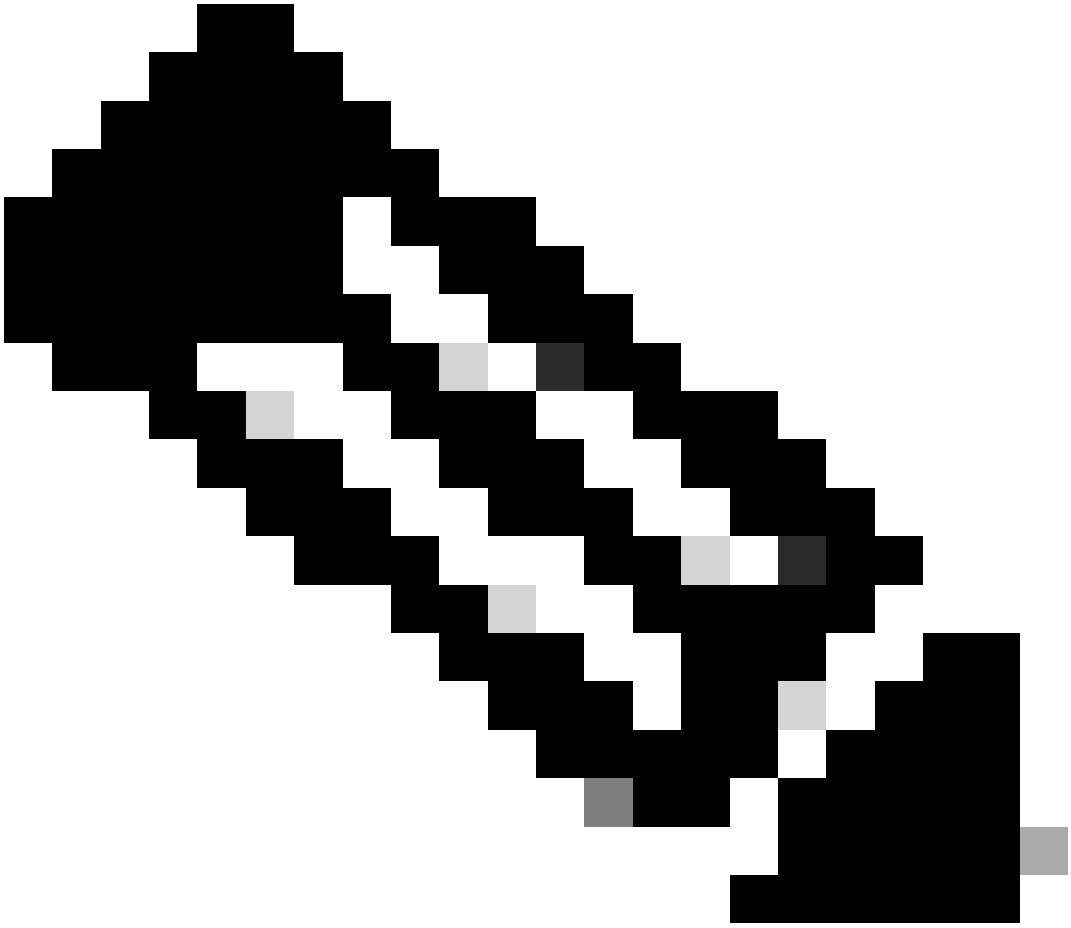
Schritt 8: Speichern und Bereitstellen der Konfiguration im FTD

Überprüfung

1. Navigieren Sie in der FMC-GUI zu Analyse > Benutzer: Aktive Sitzungen

3. Validierung aus Analyse > Verbindung > Ereignisse: Tabellenansicht der Verbindungsereignisse





Hinweis: Benutzer, die die Datenverkehrskriterien für die Identitätsrichtlinie und die Zugriffskontrollrichtlinie erfüllen, erhalten ihren Benutzernamen im Feld "Benutzer".

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.