Konfigurieren der Active Directory-Integration mit der FirePOWER-Appliance für die einmalige Anmeldung und Authentifizierung über Captive Portal

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration der Captive Portal-Authentifizierung (Active Authentication) und der Single-Sign-On (Passive Authentication).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sourcefire FirePOWER-Geräte
- Modelle für virtuelle Geräte

- LDAP (Light Weight Directory Service)
- FirePOWER-Benutzeragent

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FirePOWER Management Center (FMC) Version 6.0.0 und höher
- FirePOWER-Sensor Version 6.0.0 und höher

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.

Hintergrundinformationen

Captive Portal Authentication oder Active Authentication fordert eine Anmeldeseite und Benutzeranmeldeinformationen an, damit ein Host den Internetzugriff erhält.

Single-Sign-On oder passive Authentifizierung ermöglicht die nahtlose Authentifizierung von Netzwerkressourcen und Internetzugriff für einen Benutzer, ohne dass es zu mehreren Vorfällen von Benutzeranmeldeinformationen kommt. Die Single-Sign-on-Authentifizierung kann entweder über den FirePOWER-Benutzeragenten oder über die NTLM-Browserauthentifizierung erfolgen.

Hinweis: Für die Captive Portal-Authentifizierung muss sich die Appliance im Routing-Modus befinden.

Konfigurieren

Schritt 1: Konfigurieren des Firepower-Benutzer-Agents für einmaliges Anmelden

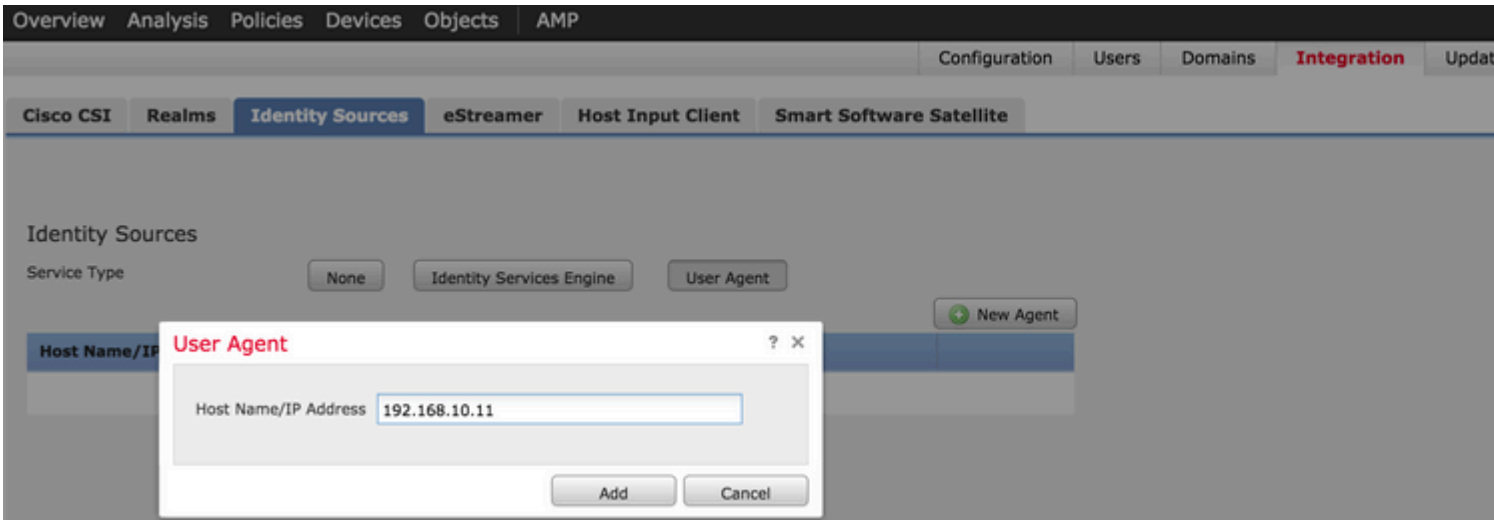
In diesem Artikel wird erläutert, wie der FirePOWER-Benutzer-Agent auf einem Windows-Computer konfiguriert wird:

Installation und Deinstallation von Sourcefire User Agent

Schritt 2: Integration von FirePOWER Management Center (FMC) mit User Agent

Melden Sie sich bei FirePOWER Management Center an, und navigieren Sie zu **System > Integration > Identity Sources.** Klicken Sie auf die Option **Neuer Agent**. Konfigurieren Sie die IP-Adresse des User Agent-Systems, und klicken Sie auf die Schaltfläche **Hinzufügen**.

Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.



Schritt 3: FirePOWER in Active Directory integrieren

Schritt 3.1 Den Bereich erstellen

Melden Sie sich beim FMC an, und navigieren Sie zu **System > Integration > Realm.** Klicken Sie auf die Option **Neuen Bereich hinzufügen**.

Name und Beschreibung: Geben Sie einen Namen/eine Beschreibung ein, um den Bereich eindeutig zu identifizieren.

Typ: AD

Primäre AD-Domäne: Domänenname von Active Directory

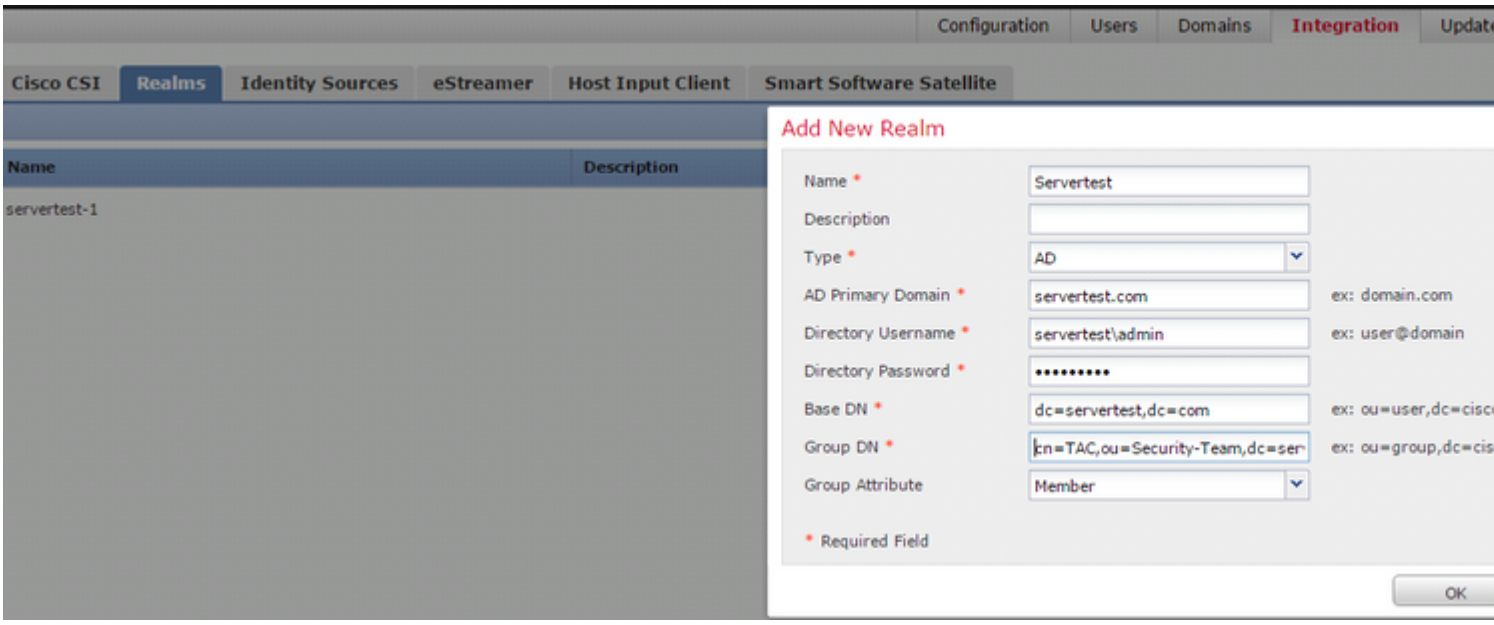
Verzeichnisbenutzername: <Benutzername>

Verzeichniskennwort: <Kennwort>

Basis-DN: Domäne oder spezifische OU-DN, von der aus das System eine Suche in der LDAP-Datenbank startet.

Gruppen-DN: Gruppen-DN

Gruppenattribut: Mitglied



Dieser Artikel hilft Ihnen, die Werte für Basis-DN und Gruppen-DN herauszufinden.

Active Directory-LDAP-Objektattribute identifizieren

Schritt 3.2 Hinzufügen des Verzeichnisservers

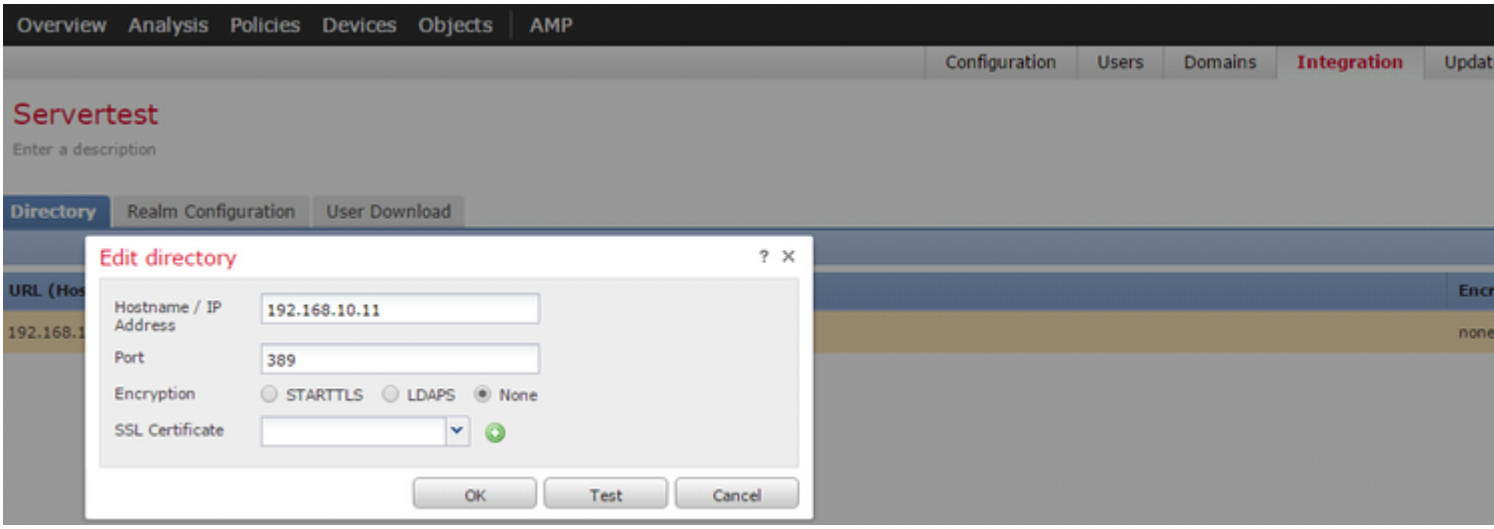
Klicken Sie auf die Schaltfläche **Hinzufügen**, um zum nächsten Schritt zu navigieren, und klicken Sie anschließend auf die Option **Verzeichnis hinzufügen**.

Hostname/IP-Adresse: Konfigurieren Sie die IP-Adresse/den Hostnamen des AD-Servers.

Port: 389 (Active Directory-LDAP-Portnummer)

Verschlüsselung/SSL-Zertifikat: (optional) Informationen zur Verschlüsselung der Verbindung zwischen FMC- und AD-Server finden Sie im

Artikel: **Verification of Authentication Object on FireSIGHT System for Microsoft AD Authentication Over SSL/TLS**



Klicken Sie auf die Schaltfläche **Test**, um zu überprüfen, ob FMC eine Verbindung zum AD-Server herstellen kann.

Schritt 3.3 Ändern der Bereichskonfiguration

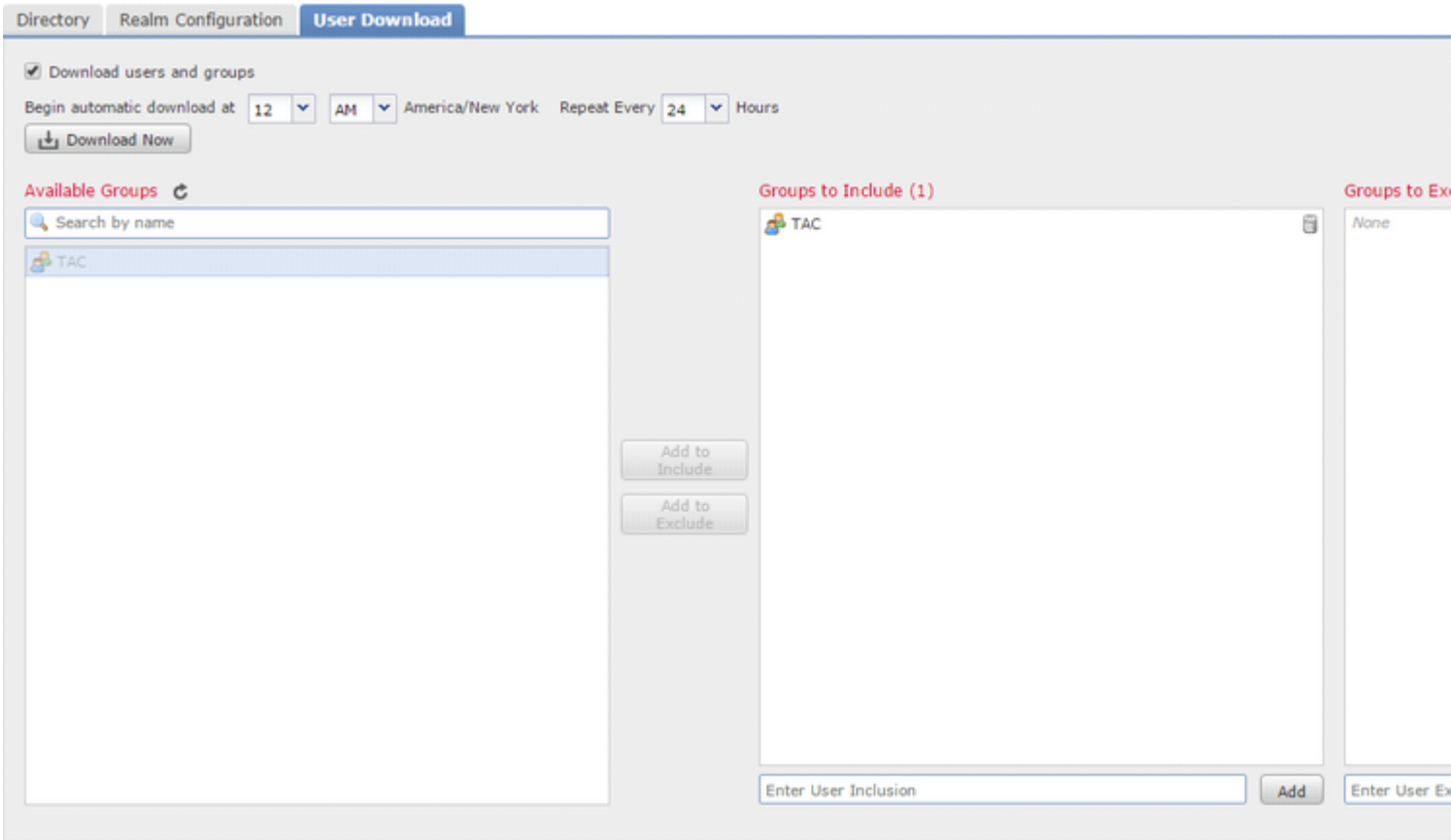
Navigieren Sie zu **Realm Configuration**, um die Integrationskonfiguration des AD-Servers zu überprüfen, und können Sie die AD-Konfiguration ändern.

Schritt 3.4 Benutzerdatenbank herunterladen

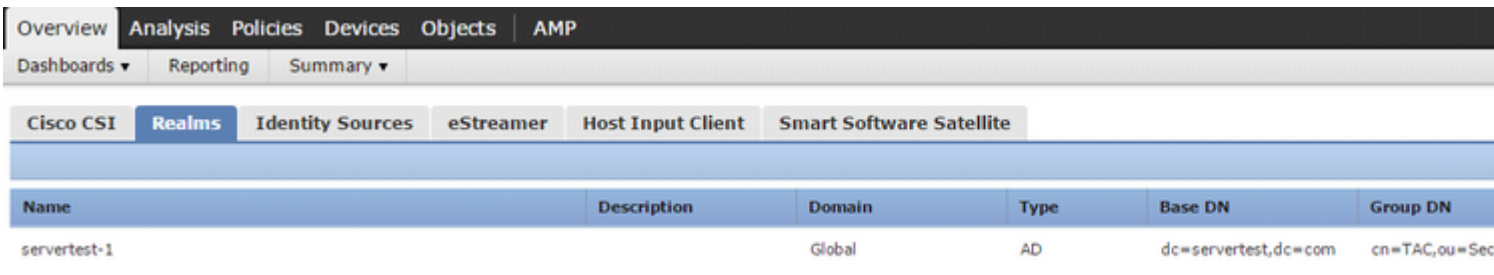
Navigieren Sie zur Option **User Download** (Benutzerdownload), um die Benutzerdatenbank vom AD-Server abzurufen.

Aktivieren Sie das Kontrollkästchen zum Herunterladen von **Download-Benutzern und -Gruppen,** und legen Sie das Zeitintervall fest, in dem angegeben ist, wie oft FMC AD kontaktiert, um die Benutzerdatenbank herunterzuladen.

Wählen Sie die Gruppe aus, und legen Sie sie in die **Include**-Option ab, für die Sie die Authentifizierung konfigurieren möchten.



Aktivieren Sie den AD-Status, wie im Bild gezeigt:



Schritt 4: Konfigurieren der Identitätsrichtlinie

Eine Identitätsrichtlinie führt eine Benutzerauthentifizierung durch. Wenn sich der Benutzer nicht authentifiziert, wird der Zugriff auf Netzwerkressourcen verweigert. Dadurch wird eine rollenbasierte Zugriffskontrolle (RBAC) für das Netzwerk und die Ressourcen Ihres Unternehmens umgesetzt.

Schritt 4.1 Captive Portal (Aktive Authentifizierung)

Bei der aktiven Authentifizierung wird nach Benutzername/Kennwort im Browser gefragt, um eine Benutzeridentität zu identifizieren, die eine Verbindung zulässt. Der Browser authentifiziert den Benutzer über eine Authentifizierungsseite oder im Hintergrund über eine NTLM-Authentifizierung. NTLM verwendet den Webbrowser zum Senden und Empfangen von Authentifizierungsinformationen. Bei der aktiven Authentifizierung werden verschiedene Typen verwendet, um die Identität des Benutzers zu überprüfen. Folgende Authentifizierungstypen sind verfügbar:

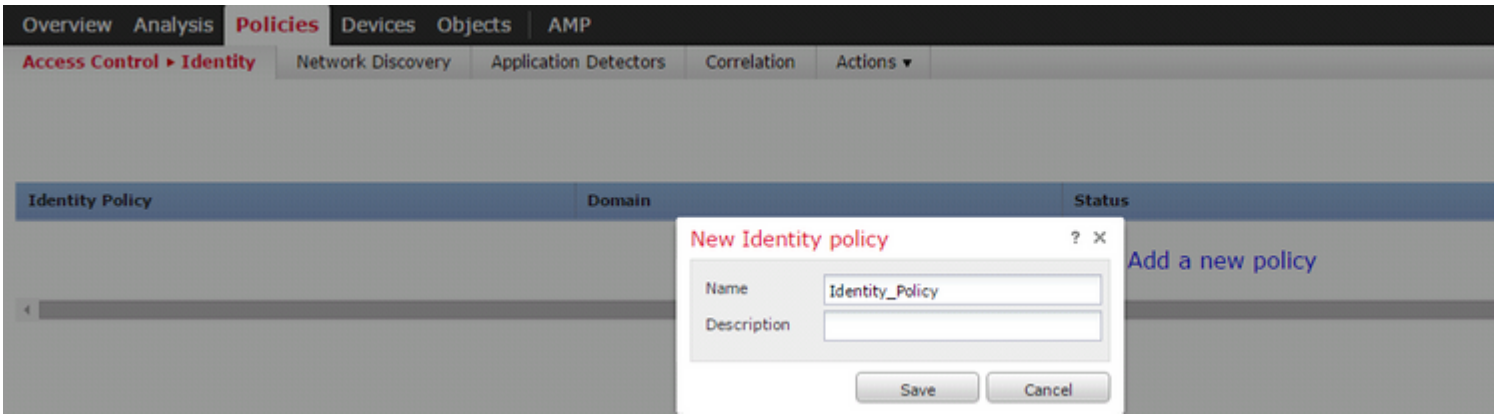
1. **HTTP Basic (Grundlegende HTTP**-Funktion): Bei dieser Methode fordert der Browser Benutzer zur Eingabe von Anmeldeinformationen auf.
2. **NTLM:** NTLM verwendet Windows-Workstation-Anmeldeinformationen und handelt diese über einen Webbrowser mit Active Directory aus. Sie müssen die NTLM-Authentifizierung im Browser aktivieren. Die Benutzerauthentifizierung erfolgt transparent und ohne Aufforderung zur Eingabe von Anmeldeinformationen. Es bietet Benutzern eine einmalige Anmeldemöglichkeit.
3. **HTTP Negotiate**: Bei diesem Typ versucht das System, sich mit NTLM zu authentifizieren. Wenn dies fehlschlägt, verwendet der Sensor den Authentifizierungstyp HTTP Basic als Fallback-Methode und fordert ein Dialogfeld zur Eingabe von Benutzeranmeldeinformationen auf.
4. **HTTP-Antwortseite:** Dies ähnelt dem HTTP-Basistyp. Hier wird der Benutzer jedoch aufgefordert, die Authentifizierung in einem HTML-Formular auszufüllen, das angepasst werden kann.

Jeder Browser verfügt über eine bestimmte Möglichkeit, die NTLM-Authentifizierung zu aktivieren. Daher befolgen sie die Richtlinien des Browsers, um die NTLM-Authentifizierung zu aktivieren.

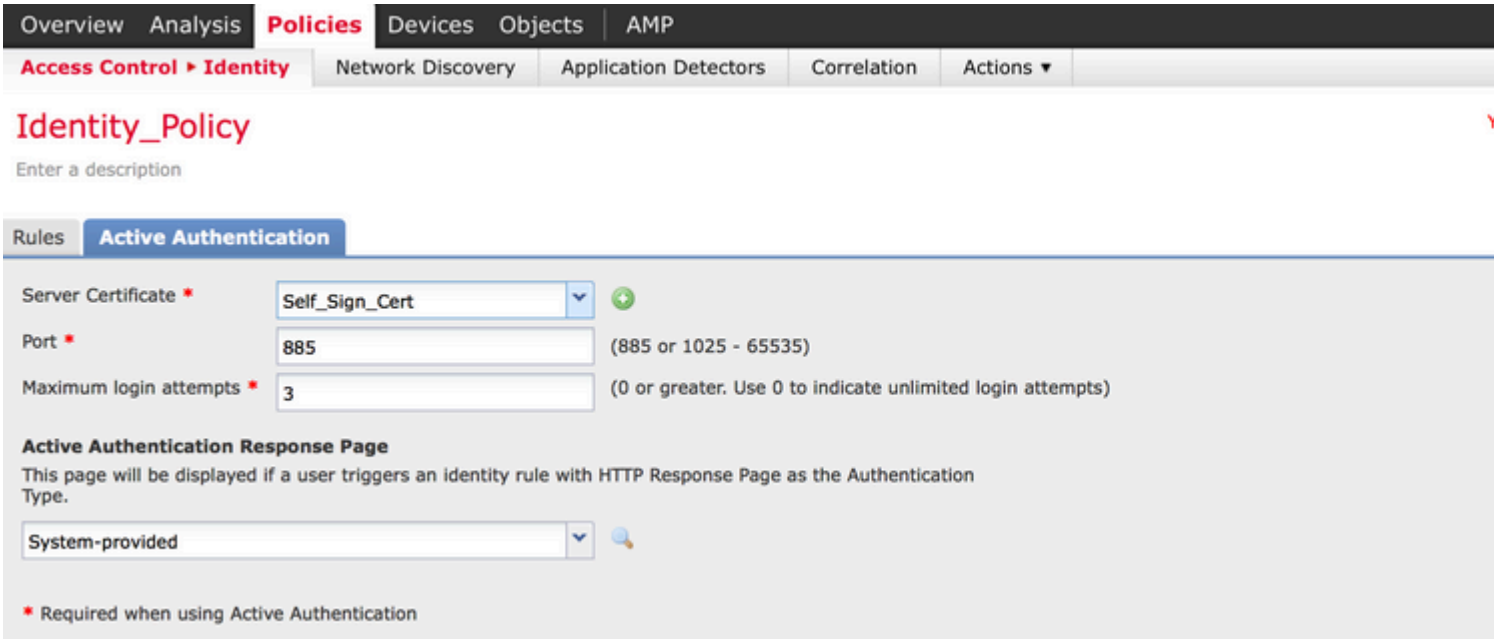
Um die Anmeldeinformationen sicher für den gerouteten Sensor freizugeben, müssen Sie entweder ein selbstsigniertes Serverzertifikat oder ein öffentlich signiertes Serverzertifikat in der Identitätsrichtlinie installieren.

```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
               openssl genrsa -des3 -out server.key 2048

Step 2.   Generate Certificate Signing Request (CSR)
               openssl req -new -key server.key -out server.csr

Step 3.   Generate the self-signed Certificate.
               openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Identität**. Klicken Sie auf **Richtlinie hinzufügen** & geben Sie einen Namen für die Richtlinie ein, und speichern Sie sie.

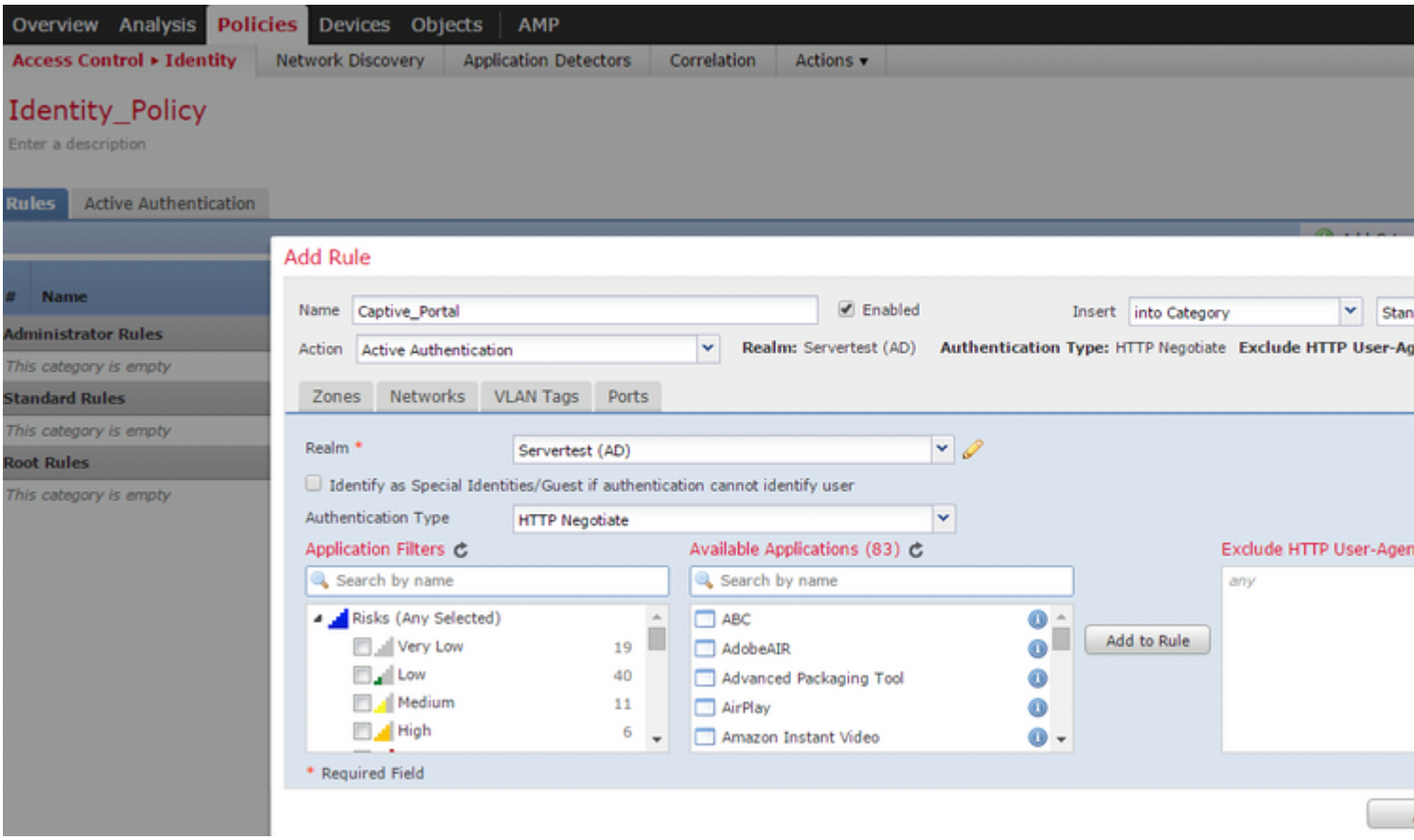


Navigieren Sie zur Registerkarte **Active Authentication (Aktive Authentifizierung)** und klicken Sie in der Option **Server Certificate (Serverzertifikat)** auf das **Symbol (+),** und laden Sie das Zertifikat und den privaten Schlüssel hoch, die Sie im vorherigen Schritt mit openSSL generiert haben.



Klicken Sie nun auf die Schaltfläche **Regel hinzufügen**, geben Sie der Regel einen Namen und wählen Sie die Aktion als **Aktive Authentifizierung**. Definieren Sie die Quell-/Zielzone, das Quell-/Zielnetzwerk, für das Sie die Benutzerauthentifizierung aktivieren möchten.

Wählen Sie den **Bereich aus**, den Sie im vorherigen Schritt konfiguriert haben, und den Authentifizierungstyp, der am besten zu Ihrer Umgebung passt.



ASA-Konfiguration für Captive Portal

Konfigurieren Sie für das ASA-FirePOWER-Modul diese Befehle auf der ASA, um das Captive Portal zu konfigurieren.

```
ASA(config)# captive-portal global port 1055
```

Stellen Sie sicher, dass der Server-Port, TCP 1055, in der **Port**-Option der Registerkarte Identity Policy **Active Authentication** konfiguriert ist**.**

Führen Sie den folgenden Befehl aus, um die aktiven Regeln und die Anzahl der Treffer zu überprüfen:

```
ASA# show asp table classify domain captive-portal
```

Hinweis: Der Captive Portal-Befehl ist in ASA-Version 9.5(2) und höher verfügbar.

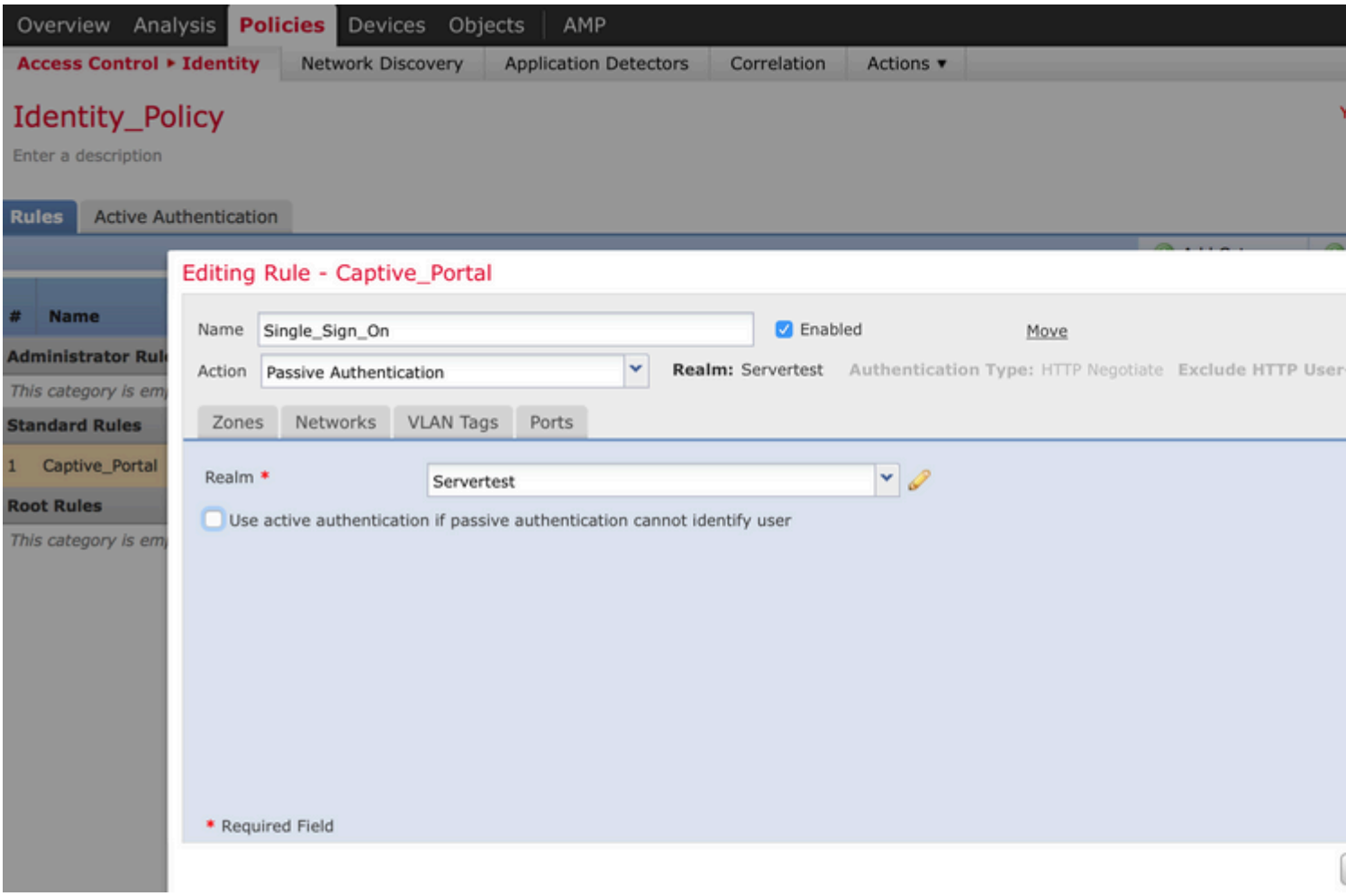
Schritt 4.2 Single-Sign-On (passive Authentifizierung)

Wenn sich ein Domänenbenutzer bei der passiven Authentifizierung anmeldet und das AD authentifizieren kann, fragt der Firepower-Benutzer-Agent die Details der Benutzer-IP-Zuordnung aus den Sicherheitsprotokollen von AD ab und gibt diese Informationen an das Firepower Management Center (FMC) weiter. FMC sendet diese Details an den Sensor, um die Zugriffskontrolle durchzusetzen.

Klicken Sie auf die Schaltfläche **Regel hinzufügen**, geben Sie der Regel einen Namen, und wählen Sie die **Aktion** als **passive Authentifizierung aus**. Definieren Sie die Quell-/Zielzone, das Quell-/Zielnetzwerk, für das Sie die Benutzerauthentifizierung aktivieren möchten.

Wählen Sie den **Bereich,** den Sie im vorherigen Schritt konfiguriert haben, und den Authentifizierungstyp aus, der am besten zu Ihrer Umgebung passt, wie in diesem Bild gezeigt.

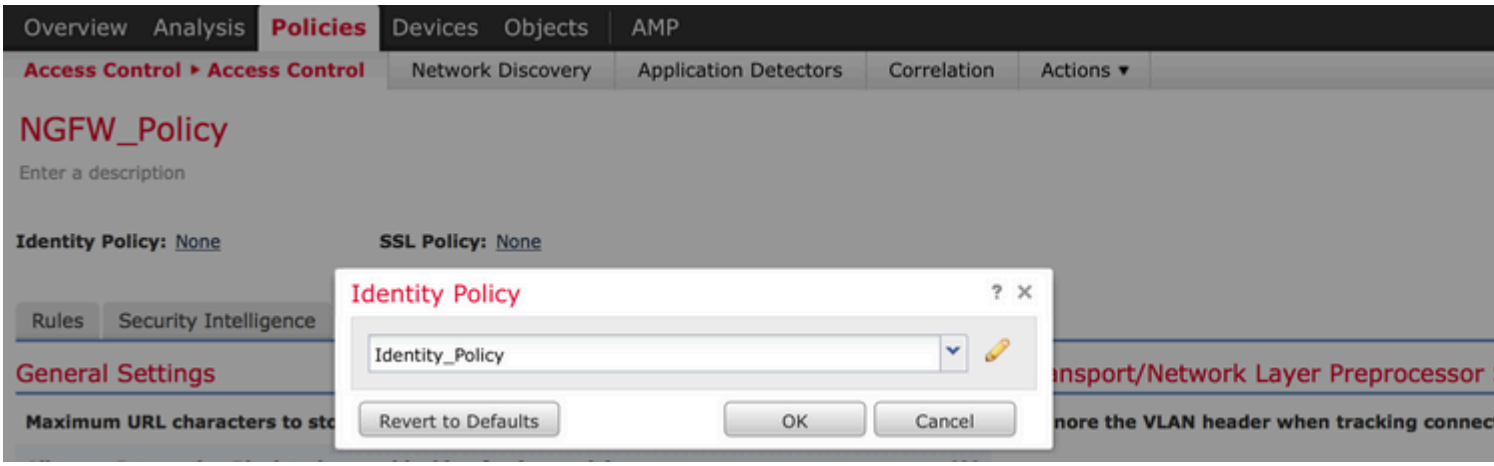
Hier können Sie die Fallback-Methode als **aktive Authentifizierung** auswählen**, wenn die passive Authentifizierung die Benutzeridentität nicht identifizieren kann**.



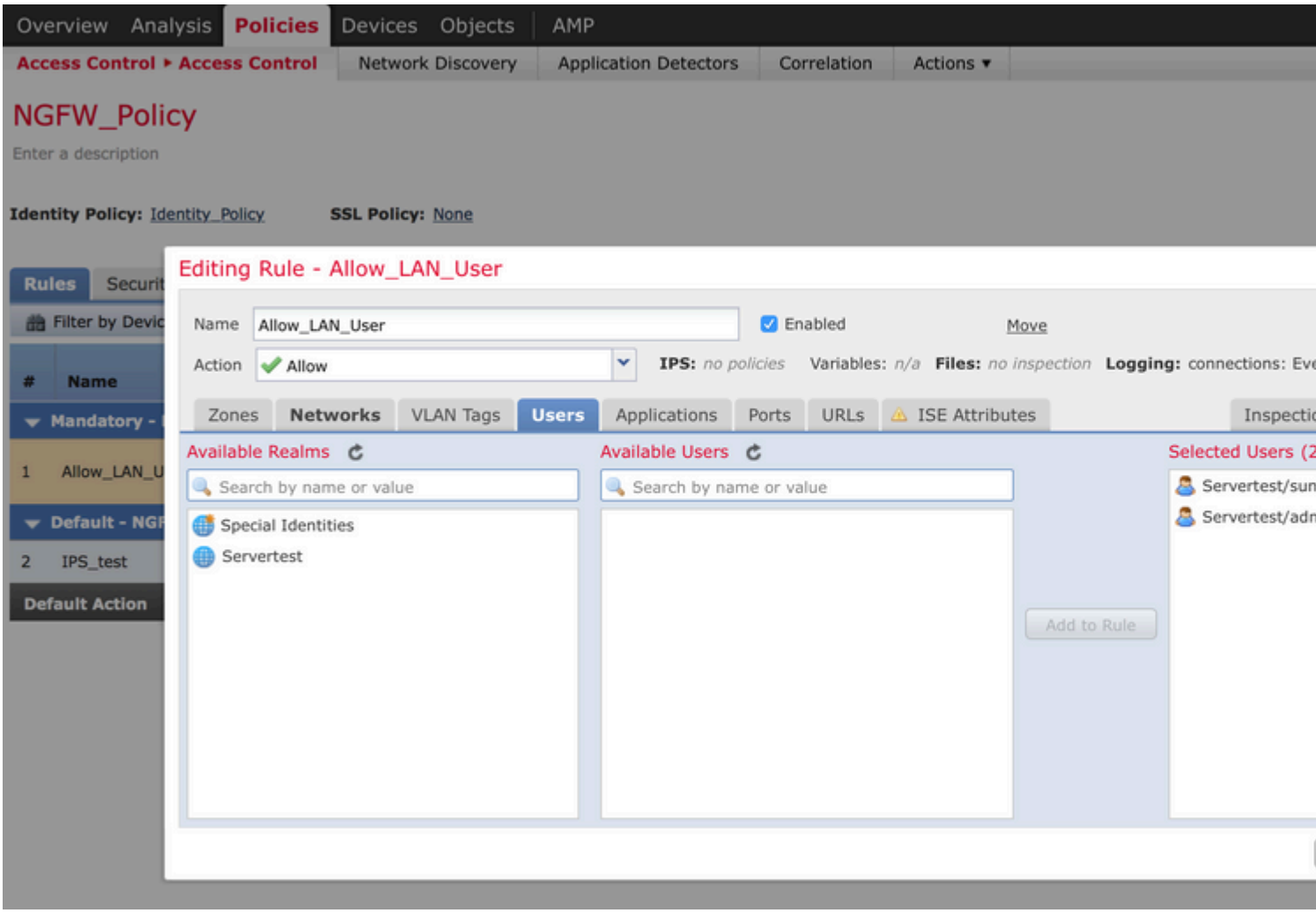
Schritt 5: Konfigurieren der Zugriffskontrollrichtlinie

Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Erstellen/Bearbeiten** einer Richtlinie.

Klicken Sie auf die **Identitätsrichtlinie** (linke obere Ecke), wählen Sie die Identitätsrichtlinie aus, die Sie im vorherigen Schritt konfiguriert haben, und klicken Sie auf die Schaltfläche **OK,** wie in diesem Bild dargestellt.

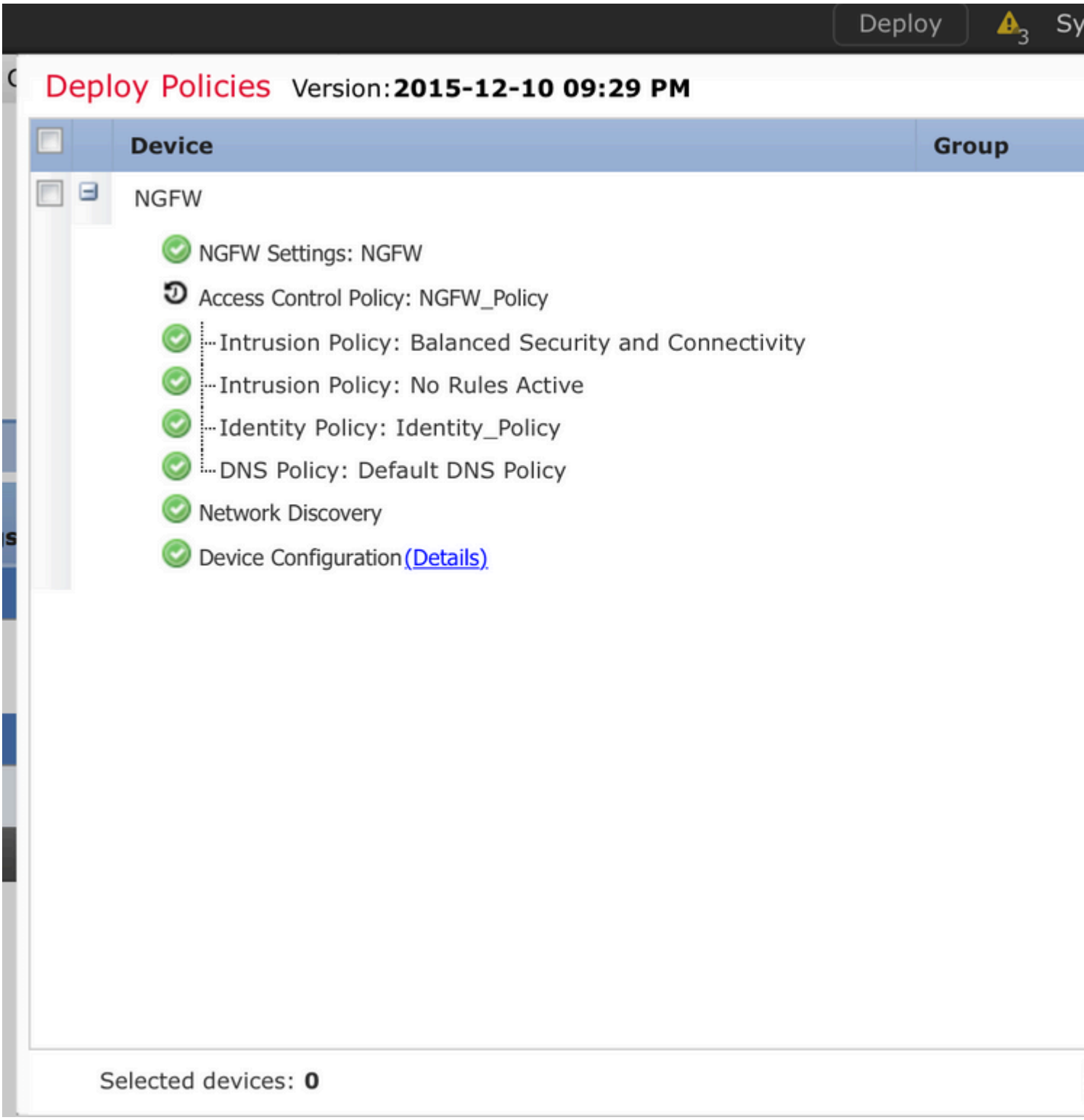


Klicken Sie auf **Regel hinzufügen**, um eine neue Regel hinzuzufügen. Navigieren Sie zu **Benutzer**, und wählen Sie die Benutzer aus, für die die Zugriffskontrollregel gilt, wie in diesem Bild dargestellt. Klicken Sie auf **OK** und dann auf **Speichern**, um die Änderungen zu speichern.



Schritt 6: Bereitstellen der Zugriffskontrollrichtlinie

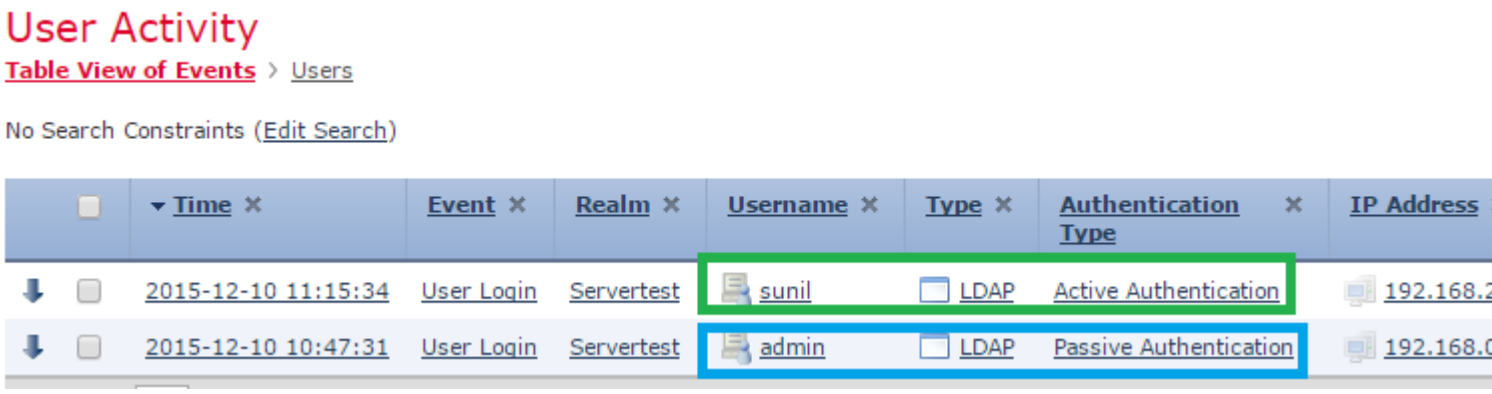
Navigieren Sie zur Option **Deploy (Bereitstellen**), wählen Sie das **Gerät aus**, und klicken Sie auf die Option **Deploy (Bereitstellen)**, um die Konfigurationsänderung an den Sensor weiterzuleiten. Überwachen Sie die Richtlinienbereitstellung über die Option **Nachrichtencenter (**Symbol zwischen Bereitstellung und Systemoption), und stellen Sie sicher, dass die Richtlinie erfolgreich angewendet werden muss, wie in diesem Bild dargestellt.



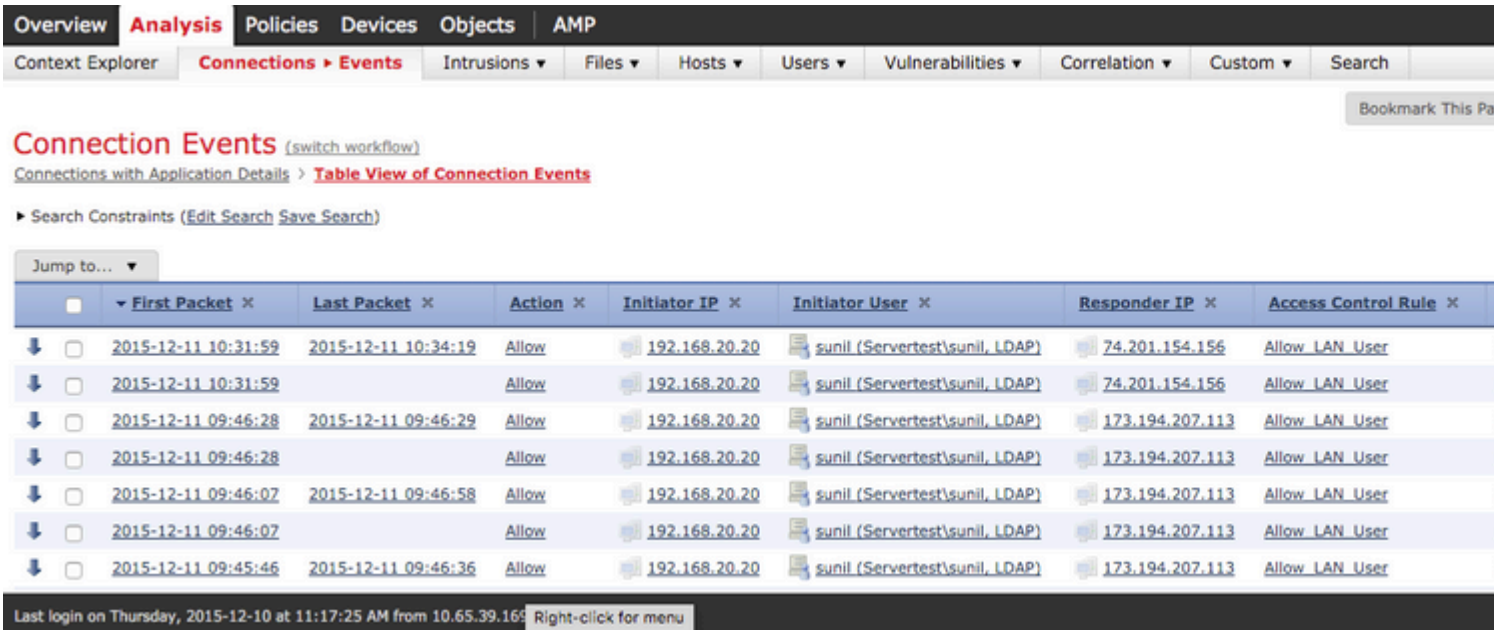
Schritt 7: Überwachen von Benutzerereignissen und Verbindungsereignissen

Aktuell aktive Benutzersitzungen sind im Abschnitt **Analyse > Benutzer > Benutzer** verfügbar.

Die Überwachung der Benutzeraktivität hilft herauszufinden, welcher Benutzer welcher IP-Adresse zugeordnet ist und wie der Benutzer vom System durch aktive oder passive Authentifizierung erkannt wird. **Analyse > Benutzer > Benutzeraktivität**



Navigieren Sie zu **Analyse > Verbindungen > Ereignisse**, um die Art des vom Benutzer verwendeten Datenverkehrs zu überwachen.



Überprüfung und Fehlerbehebung

Navigieren Sie zu **Analyse** > **Benutzer**, um den Benutzerauthentifizierungs-/Authentifizierungstyp/die Benutzer-IP-Zuordnung/Zugriffsregel zu überprüfen, die mit dem Datenverkehrsfluss verknüpft sind.

Überprüfen der Verbindung zwischen FMC und Benutzer-Agent (passive Authentifizierung)

FirePOWER Management Center (FMC) verwendet den TCP-Port 3306, um Protokolldaten zu Benutzeraktivitäten vom Benutzer-Agenten zu empfangen.

Verwenden Sie diesen Befehl im FMC, um den FMC-Dienststatus zu überprüfen.

```
admin@firepower:~$ netstat -tan | grep 3306
```

Führen Sie die Paketerfassung auf dem FMC aus, um die Verbindung mit dem Benutzer-Agenten zu überprüfen.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

Navigieren Sie zu **Analyse > Benutzer > Benutzeraktivität,** um zu überprüfen, ob das FMC Benutzeranmeldedetails vom Benutzer-Agenten empfängt.

Überprüfen der Verbindung zwischen FMC und Active Directory

FMC verwendet den TCP-Port 389, um die Benutzerdatenbank von der Active Directory

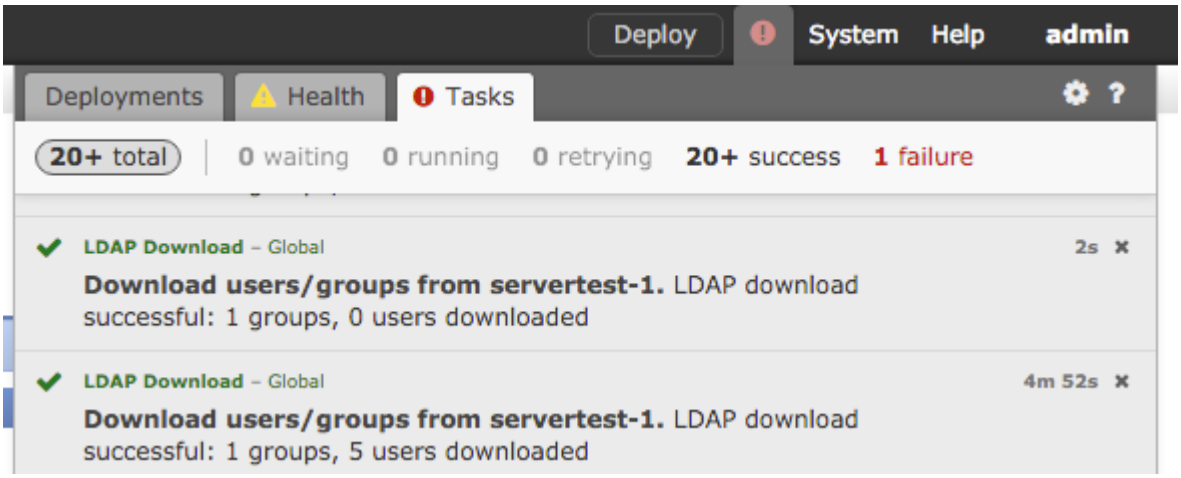
Führen Sie die Paketerfassung auf dem FMC aus, um die Verbindung mit Active Directory zu überprüfen.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

Stellen Sie sicher, dass die in der FMC Realm-Konfiguration verwendeten Benutzeranmeldeinformationen über ausreichende Berechtigungen zum Abrufen der AD-Benutzerdatenbank verfügen.

Überprüfen Sie die FMC-Bereichskonfiguration, und stellen Sie sicher, dass die Benutzer/Gruppen heruntergeladen wurden und das Timeout für Benutzersitzungen richtig konfiguriert wurde.

Navigieren Sie zu **Message Center > Tasks (Nachrichtencenter > Aufgaben**), und stellen Sie sicher, dass der Task-**Download für Benutzer/Gruppen** erfolgreich abgeschlossen wurde, wie in diesem Bild gezeigt.



Überprüfen der Verbindung zwischen FirePOWER-Sensor und Endsystem (aktive Authentifizierung)

Stellen Sie für die aktive Authentifizierung sicher, dass das Zertifikat und der Port in der FMC-Identitätsrichtlinie richtig konfiguriert sind.Standardmäßig überwacht der FirePOWER-Sensor den TCP-Port 885 für die aktive Authentifizierung.

Überprüfen der Richtlinienkonfiguration und Richtlinienbereitstellung

Stellen Sie sicher, dass die Felder Bereich, Authentifizierungstyp, Benutzer-Agent und Aktion in der Identitätsrichtlinie richtig konfiguriert sind.

Stellen Sie sicher, dass die Identitätsrichtlinie der Zugriffskontrollrichtlinie richtig zugeordnet ist.

Navigieren Sie zu **Message Center > Tasks**, und stellen Sie sicher, dass die Richtlinienbereitstellung erfolgreich abgeschlossen wurde.

Analysieren der Ereignisprotokolle

Verbindungs- und Benutzeraktivitätsereignisse können verwendet werden, um festzustellen, ob die Benutzeranmeldung erfolgreich ist.Diese Ereignisse

kann auch überprüfen, welche Zugriffskontrollregel auf den Datenfluss angewendet wird.

Navigieren Sie zu **Analyse > Benutzer**, um die Benutzerereignisprotokolle zu überprüfen.

Navigieren Sie zu **Analyse > Verbindungsereignisse**, um die Verbindungsereignisse zu überprüfen.

Zugehörige Informationen

- **Technischer Support und Dokumentation für Cisco Systeme**

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.