Contents

Introduction

This document describes the configuration of Captive portal authentication (Active Authentication) and Single-Sign-On (Passive Authentication) on Firepower Module using ASDM (Adaptive Security Device Manager).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of ASA (Adaptive Security Appliance) firewall and ASDM
- FirePOWER module Knowledge
- Light Weight Directory Service (LDAP)
- Firepower UserAgent

Components Used

The information in this document is based on these software and hardware versions:

- ASA FirePOWER modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) running software version 5.4.1 and above.
- ASA FirePOWER module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) running software version 6.0.0 and above.

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, make sure that you understand the potential impact of any command.

Background Information

Captive Portal Authentication or Active Authentication prompts a login page and user credentials are required for a host to get the internet access.

Single-Sign-On or Passive Authentication provides seamless authentication to a user for network resources and internet access without entering user credential multiple times. The Single-Sign-on authentication can be achieved either by Firepower user agent or NTLM browser authentication.

> **Note**:Captive Portal Authentication, ASA should be in routed mode.

> **Note**: Captive portal command is available in ASA version

Configure

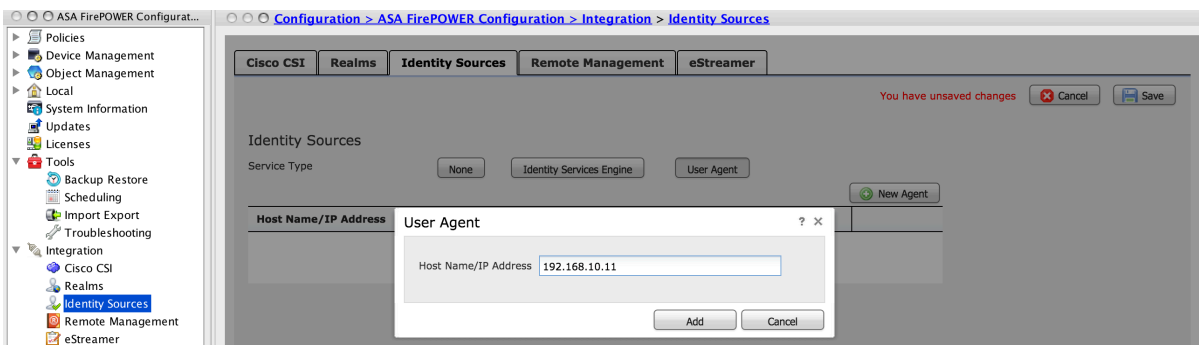
Step 1. Configure the Firepower User Agent for Single-Sign-On.

This article explains how to configure Firepower User Agent in Windows machine:

[Installation and Uninstallation of Sourcefire User Agent]

Step 2. Integrate the Firepower Module (ASDM) with User Agent.

Log in to ASDM, navigate to **Configuration > ASA FirePOWER Configuration > Integration > Identity Sources** and clickthe **User Agent** option. After you click on the **User Agent** option and configure the IP address of User Agent system. click on **Add**, as shown in the image:



Click on **Save** button to save the changes.

Step 3. Integrate

Step 3.1 Create the Realm.

Log in to ASDM, navigate to **Configuration > ASA FirePOWER Configuration > Integration > Realms.** Click on **Add a New Realm**.

Name & Description: Give a name/description to uniquely identify the realm.

Type: AD

AD Primary Domain: Domain name of Active Directory (NETBIOS Name).

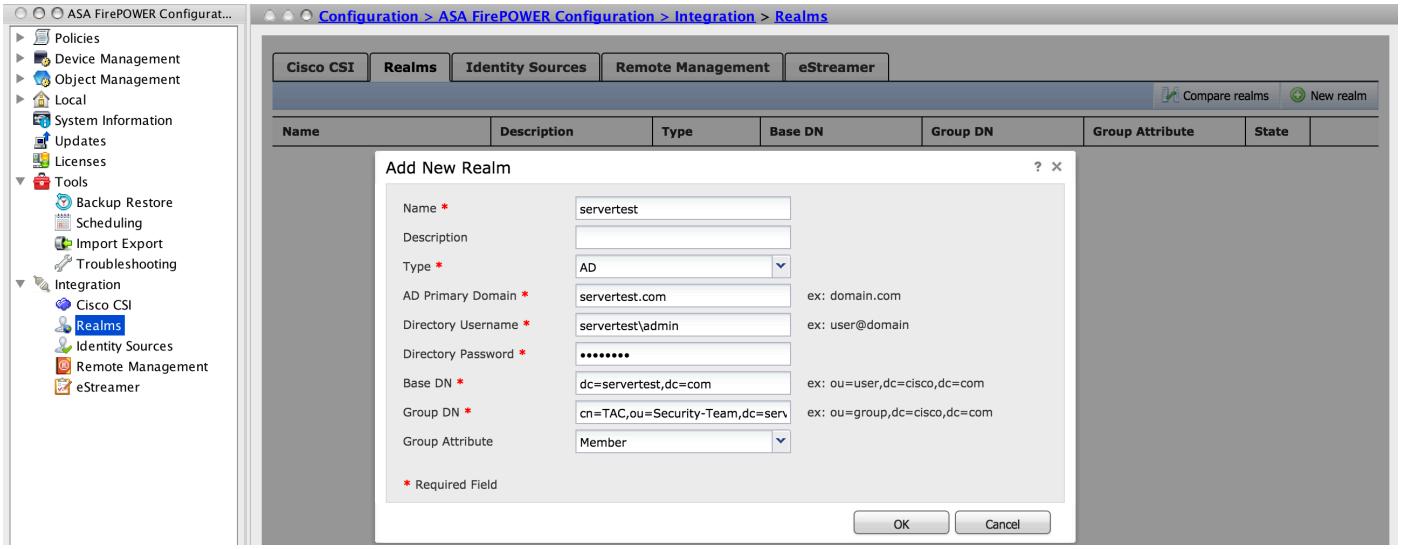
Directory Username: Specify the <*username*>.

Directory Password: Specify the <*password*>.

Base DN: Domain or Specific OU DN from where the system will start a search in LDAP database.

Group DN: Specify the group DN.

Group Attribute: Specify the option **Member** from the drop-down list.



Click on **OK** to save the configuration.

This article can help you to figure out the Base DN and Group DN values.

[Identify Active Directory LDAP Object Attributes]

Step 3.2 Add the Directory Server IP address/hostname.

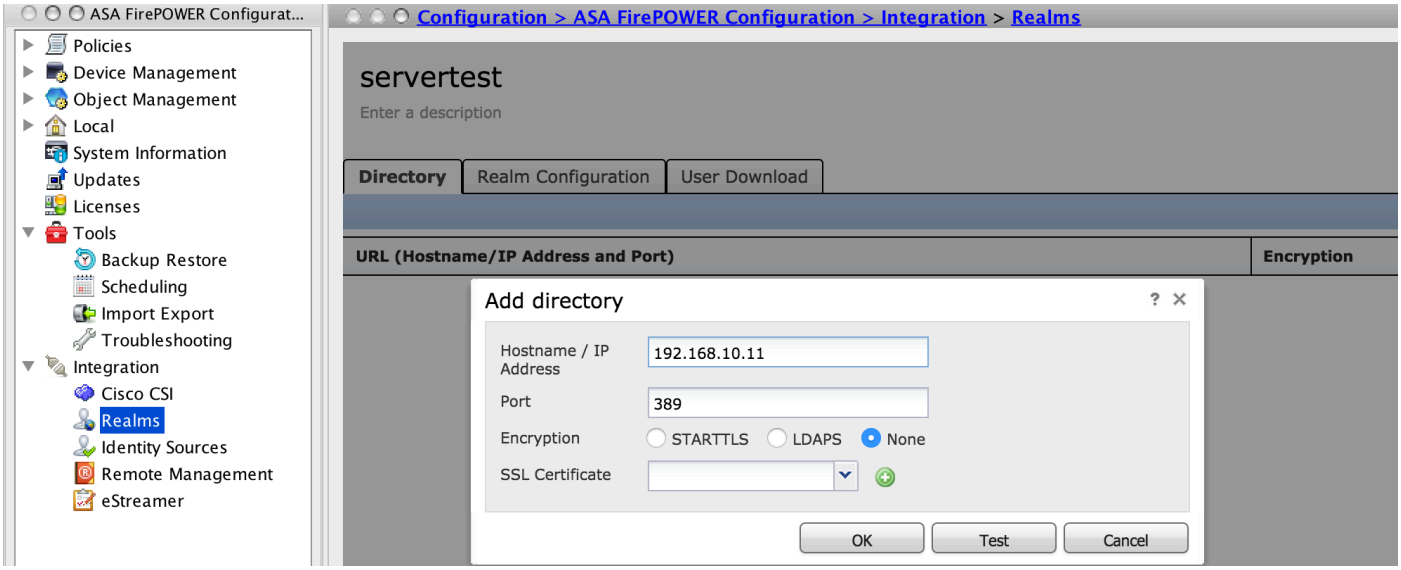
To specify AD Server IP/hostname, click on **Add directory**.

Hostname/IP Address: configure the IP address/hostname of the AD server.

Port: Specify the Active Directory LDAP port number (Default 389).

Encryption/SSL Certificate: (optional)

[Verification of Authentication Object on FireSIGHT System for Microsoft AD Authentication Over SSL/T...]



Click **Test** in order to verify the connection of FMC with the AD server. Now click **OK** to save the configuration.

Step 3.3 Modify the Realm Configuration.

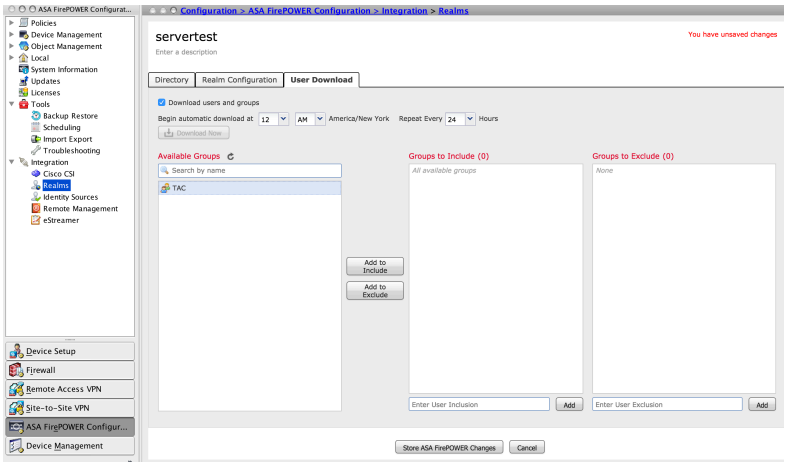
In order to modify and verify integration configuration of AD server, navigate to **Realm Configuration**.

Step 3.4 Download User database.

Navigate to **User Download** to fetch the user database from the AD server.

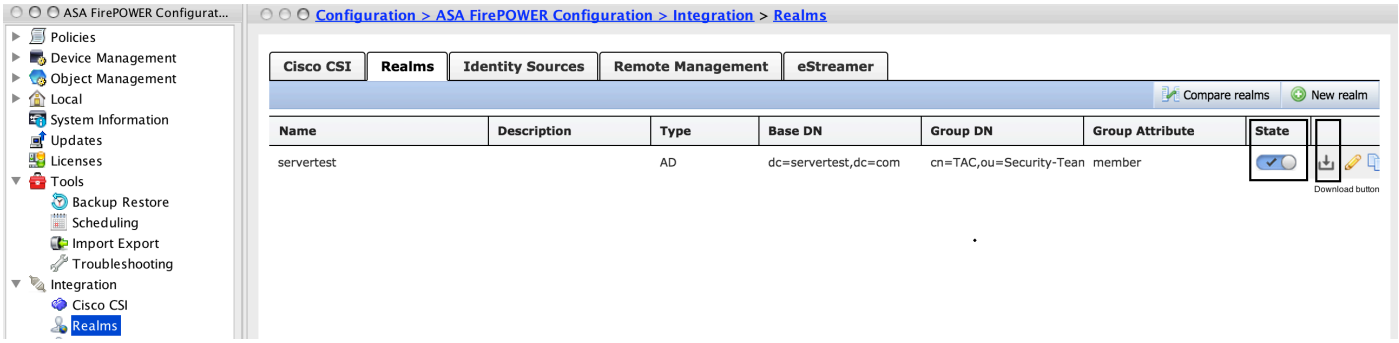
Enable the check box to download **Download users and groups** and define the time interval about how frequently Firepower module contacts AD server to download user database.

Select the group and add it to the **Include** option for which you want to configure the authentication. By default, all groups are selected if you do not choose to include the groups.



Click on **Store ASA Firepower Changes** to save the realm configuration.

Enable the realm state and click the download button to download the users and groups, as shown in the image.



Step 4. Configure the Identity Policy.

An identity policy performs user authentication. If the user does not authenticate, access to network resources is refused. This enforces Role-Based Access Control (RBAC) to your organization's network and resources.

Step 4.1 Captive portal (Active Authentication).

Active Authentication asks for username and password at the browser to identify a user identity to allow any connection. Browser authenticates user either by presenting authentication page or authenticates silently with NTLM authentication. NTLM uses the web browser to send and receive authentication information. Active Authentication uses various types to verify the identity of the user. Different types of Authentication are:

1. **HTTP Basic:** In this method, the browser prompts for user credentials.
2. **NTLM:** NTLM uses windows workstation credentials and negotiates it with Active directory using a web browser. You need to enable the NTLM authentication in the browser. User Authentication happens transparently without prompting credentials. It provides a single sign-on experience for users.
3. **HTTP Negotiate:**In this type, the system tries to authenticate using NTLM, if it fails then the sensor uses HTTP Basic authentication type as a fallback method and prompts a dialog box for user credentials.
4. **HTTP Response page:** This is similar to HTTP basic type, however, here user is prompted to fill the authentication in an HTML form which can be customized.

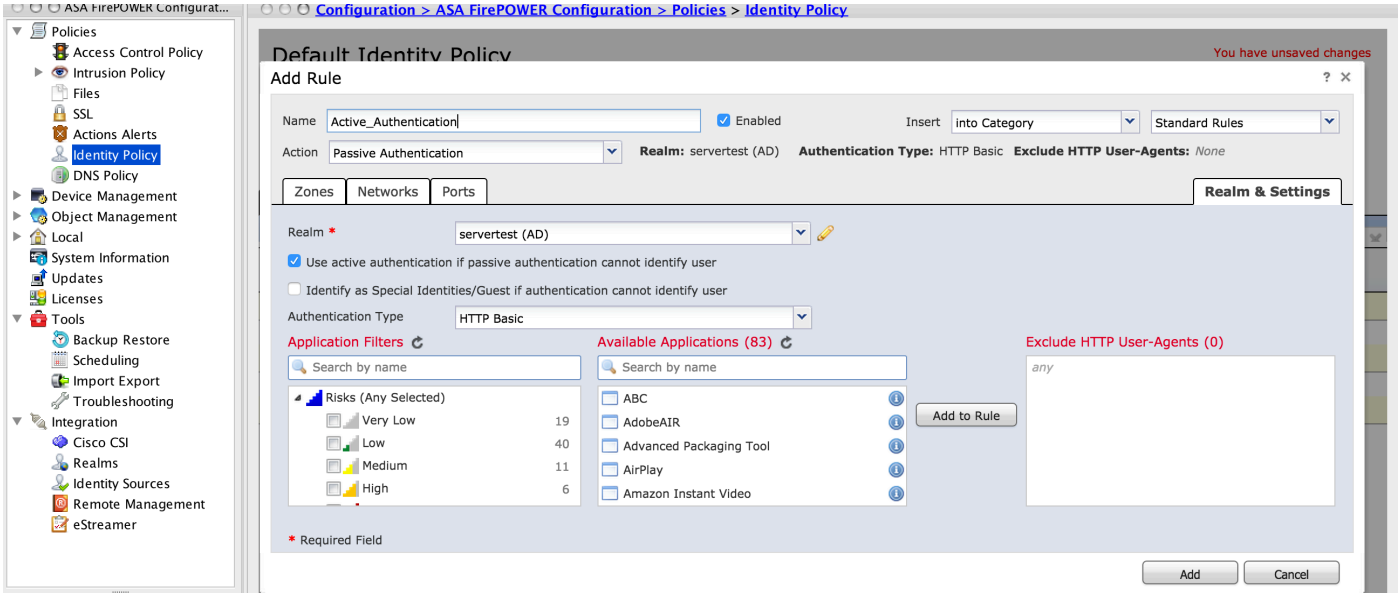
Each browser has a specific way to enable the NTLM authentication and hence, you can follow browser guidelines in order to enable the NTLM authentication.

To securely share the credential with the routed sensor, you need to install either self-signed server certificate or publicly-signed server certificate in the identity policy.

Navigate to **Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**. Now n**Active Authentication** tab and in the **Server Certificate** option, click the **icon (+)** and upload the certificate and private key which you have generated in the previous step using openSSL, as shown in the image:

Now click on **Add rule** to give a name to the Rule and choose the action as **Active Authentication**. Define the source/destination zone, source/destination network for which you want to enable the user authentication.

Navigate to the **Realm & Settings** tab. Select the **Realm** from the drop-down list which you have configured in the previous step and select the **Authentication Type** from the drop-down list that best suits your network environment.



Step 4.2

Step 1. Define the interesting traffic that will be redirected to Sourcefire for inspection.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
ASA(config-cmap)# match access-list SFR_ACL


ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

Step 2. Configure this command on the ASA in order to enable the captive portal.

```
ASA(config)# captive-portal interface inside port 1025
```

> **Tip**: captive-portal can be enabled globally or per interface basis.

> **Tip**: Ensure that the server port, TCP 1025 is configured in the port option of Identity policy's Active Authentication tab.

Step 4.3 Single-Sign-On (Passive Authentication).

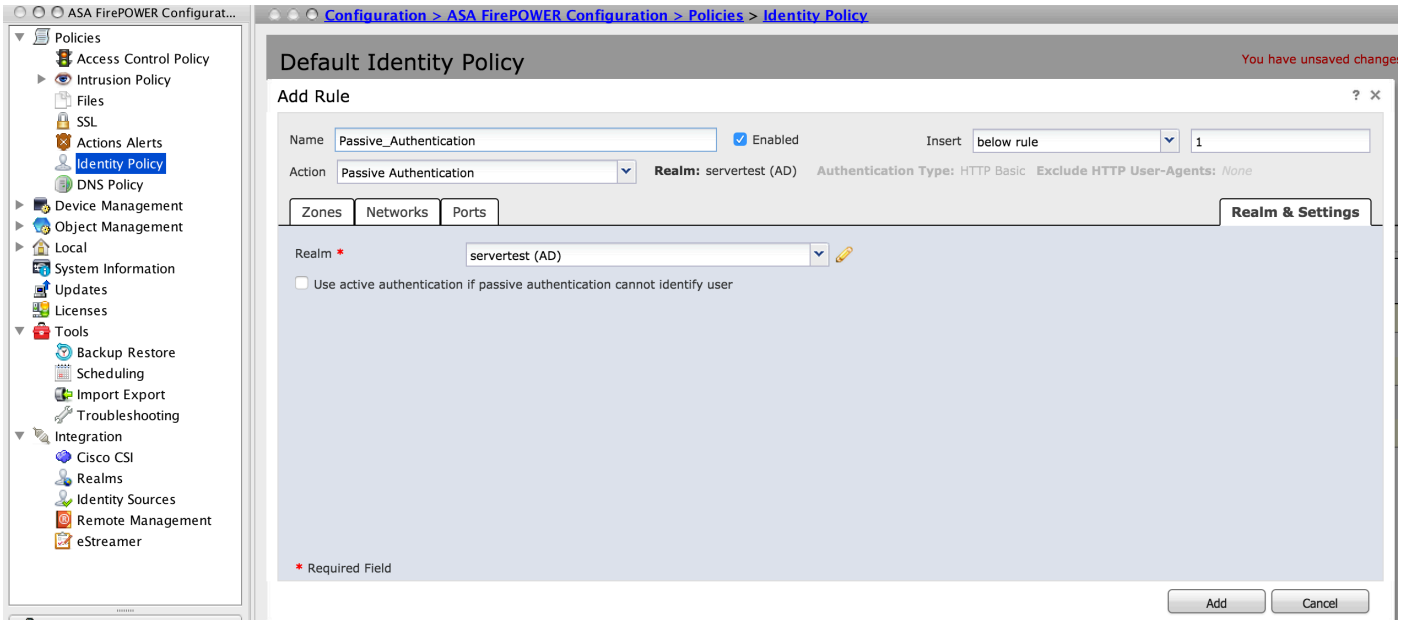
In passive authentication, when a domain user logins and is able to authenticate the AD, the Firepower User Agent polls the User-IP mapping details from the security logs of AD and shares this information with Firepower Module. Firepower module uses these details in order to enforce

the access control.

To configure the passive authentication rule, click on **Add rule** to give a name to the rule and then choose the **Action** as **Passive Authentication**. Define the source/destination zone, source/destination network for which you want to enable the user authentication.

Navigate to the **Realm & Settings** tab. Select the **Realm** from the drop-down list which you have configured in the previous step.

Here you can choose fall back method as **Active authentication if passive authentication cannot identify the user identity**, as shown in the image:

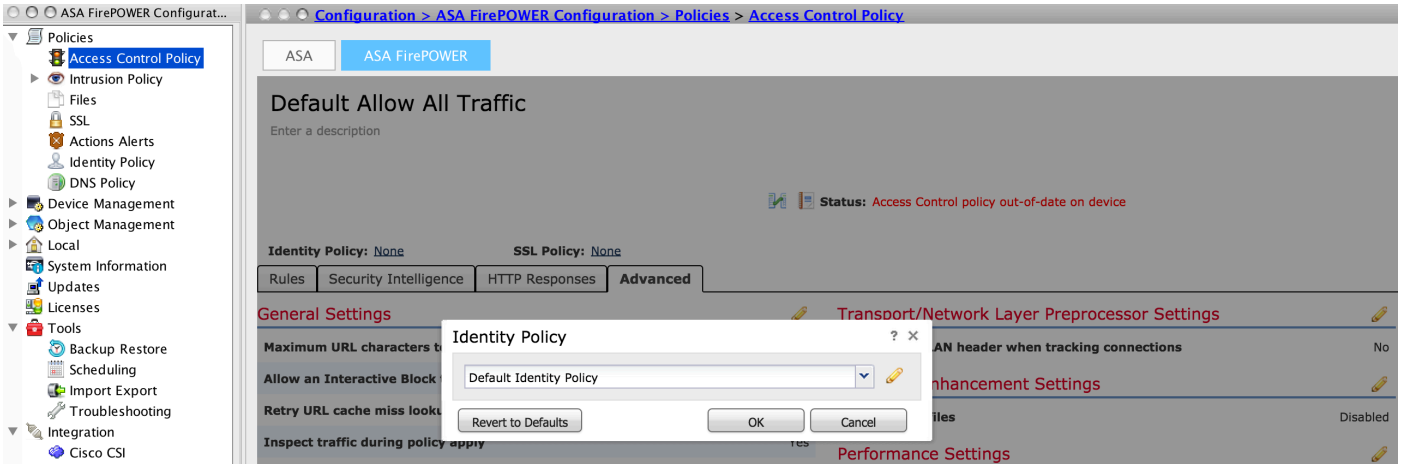


Now click on **Store ASA Firepower Changes** to save the configuration of Identity policy.

Step 5. Configure the Access Control Policy.

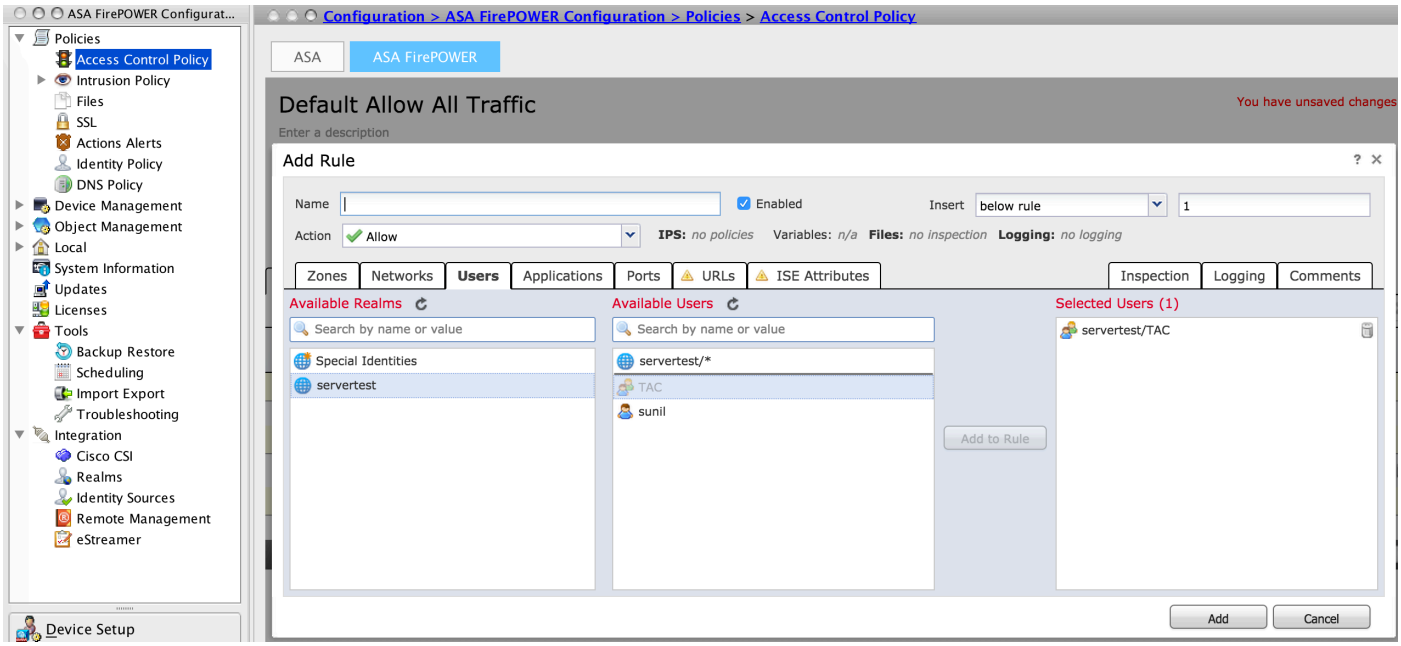
Navigate to **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy.**

Click the **Identity Policy** (left-hand side upper corner), select the Identify Policy that you have configured in the previous step from the drop-down list and click **OK**, as shown in this image.



Click on **Add rule** to add a new rule, navigate to **Users** and select the users for which access

control rule will be enforced, as shown in this image and click **Add**.



Click on **Store ASA Firepower Changes** to save the configuration of Access Control policy.

Step 6. Deploy the Access Control Policy.

You must deploy the Access Control policy. Before you apply the policy, you will see an indication Access Control Policy out-of-date on the module. To deploy the changes to the sensor, Click on **Deploy** and choose **Deploy FirePOWER Changes option** then click on **Deploy** in the pop-up window.

> **Note**: In version 5.4.x, to apply the access policy to the sensor, you need to click Apply ASA FirePOWER Changes

> **Note**: Navigate to Monitoring > ASA Firepower Monitoring > Task Status. Ensure that task must complete applying the configuration change.

Step 7. Monitor User events.

Navigate to **Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing**, to monitor the type of traffic being used by the user.

Verify

Use this section in order to confirm that your configuration works properly.

Navigate to **Analysis > Users** in orderto verify the User authentication/Authentication type/User-IP mapping/access rule associated with the traffic flow.

Connectivity between Firepower Module and User Agent (Passive Authentication)

Firepower Module uses TCP port 3306, in order to receive user activity log data from the User Agent.

In order to verify the Firepower module's service status, use this command in the FMC.

```
ASA(config)# captive-portal interface inside port 1025
```

Run packet capture on the FMC in order to verify connectivity with the User Agent.

```
ASA(config)# captive-portal interface inside port 1025
```

Connectivity between FMC and Active Directory

Firepower module uses TCP port 389 in order to retrieve the User Database from the Active directory.

Run packet capture on the Firepower Module to verify connectivity with the Active Directory.

```
ASA(config)# captive-portal interface inside port 1025
```

Ensure that the user credential used in Realm configuration has sufficient privilege to fetch the AD's User database.

Verify the Realm configuration, and ensure that the users/groups are downloaded and user session timeout is configured correctly.

Navigate to Monitoring ASA Firepower Monitoring Task Status and ensure that the task users/groups download completes successfully, as shown in this image.

Connectivity between ASA and End system (Active Authentication)

active authentication, ensure that the certificate and port are configured correctly in Firepower module Identity policy and ASA (captive-portal command). By default, ASA and Firepower module listen on TCP port 885 for active authentication.

In order to verify the active rules and their hit counts, run this command on the ASA.

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

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

Policy configuration & Policy Deployment

Ensure that the Realm, Authentication type, User agent and Action fields are configured correctly in Identity Policy.

Ensure that the Identity policy is correctly associated with the Access Control policy.

Navigate to Monitoring > ASA Firepower Monitoring > Task Status and ensure that the Policy Deployment completes successfully.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Technical Support & Documentation - Cisco Systems**
- **Configure Active Directory Integration with Firepower Appliance for Single-Sign-On & Captive Portal Authentication**