シングル サインオンとキャプティブ ポータル認証（On-Box Management）用に ASDM と Active Directory を設定する

内容

概要

このドキュメントでは、ASDM（Adaptive Security Device Manager）を使用して Firepower モジュールにキャプティブ ポータル認証（アクティブ認証）とシングルサインオン（パッシブ認証）を設定する方法を説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA（適応型セキュリティ アプライアンス）ファイアウォールと ASDM の知識
- FirePOWER モジュールの知識
- Light Weight Directory Service（LDAP）
- Firepower ユーザ エージェント

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 5.4.1 以降を実行する ASA FirePOWER モジュール（ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X）。
- ソフトウェア バージョン 6.0.0 以降を実行する ASA FirePOWER モジュール（ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X）。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

キャプティブ ポータル認証またはアクティブ認証では、ログイン ページが表示され、ホストがインターネットにアクセスするためにユーザ クレデンシャルが必要になります。

シングルサインオンまたはパッシブ認証では、ユーザ クレデンシャルを複数回入力する必要のない、ネットワーク リソースやインターネット アクセスのためのシームレスな認証をユーザに提供します。シングルサインオン認証は、Firepower ユーザ エージェントまたは NTLM ブラウザ認証のいずれかによって実現できます。

> **注**：キャプティブポータル認証、ASAはルーテッドモードである必要があります。

> **注**：キャプティブ ポータル コマンドは、ASA バージョン 9.5(2) 以降で使用できます。

設定

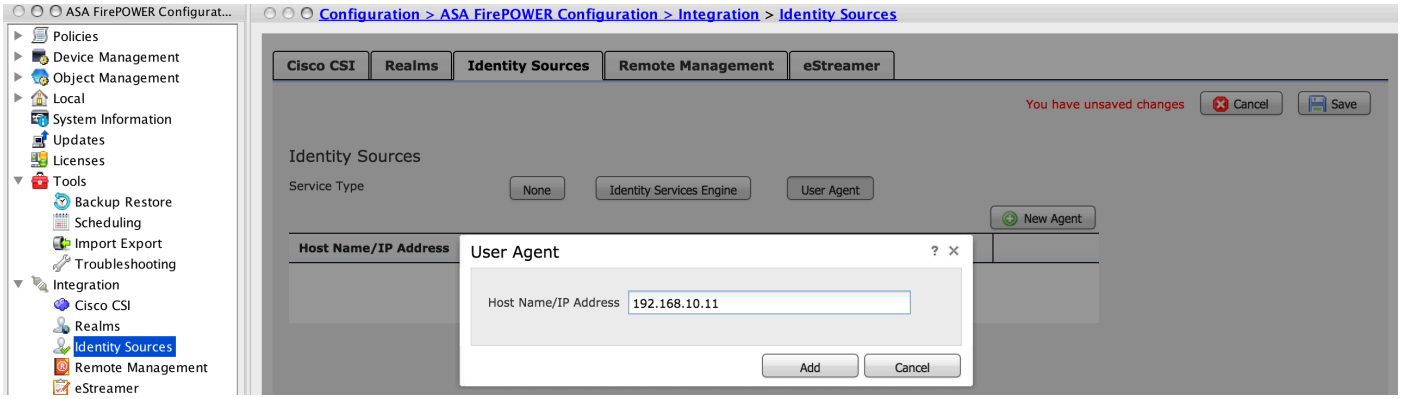
手順 1：シングルサインオン用に Firepower ユーザ エージェントを設定する。

次の記事では、Windows マシンで Firepower ユーザ エージェントを設定する方法について説明します。

Sourcefire ユーザ エージェントのインストールとアンインストール

ステップ 2： Firepowerモジュール(ASDM)をユーザエージェントと統合します。

ASDM にログインし、[Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Identity Sources] に移動して、[User Agent] オプションをクリックします。[User Agent] オプションをクリックした後、ユーザ エージェント システムの IP アドレスを設定します。次の図のように、[Add] をクリックします。



[Save] ボタンをクリックして、変更を保存します。

手順 3：Firepower を Active Directory と統合する。

手順 3.1： レルムを作成する。

ASDM にログインし、[Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] に移動します。[Add a New Realm] をクリックします。

名前と説明：レルムを一意に識別するための名前と説明を指定します。

タイプ： AD

ADプライマリドメイン： Active Directoryのドメイン名（NETBIOS名）。

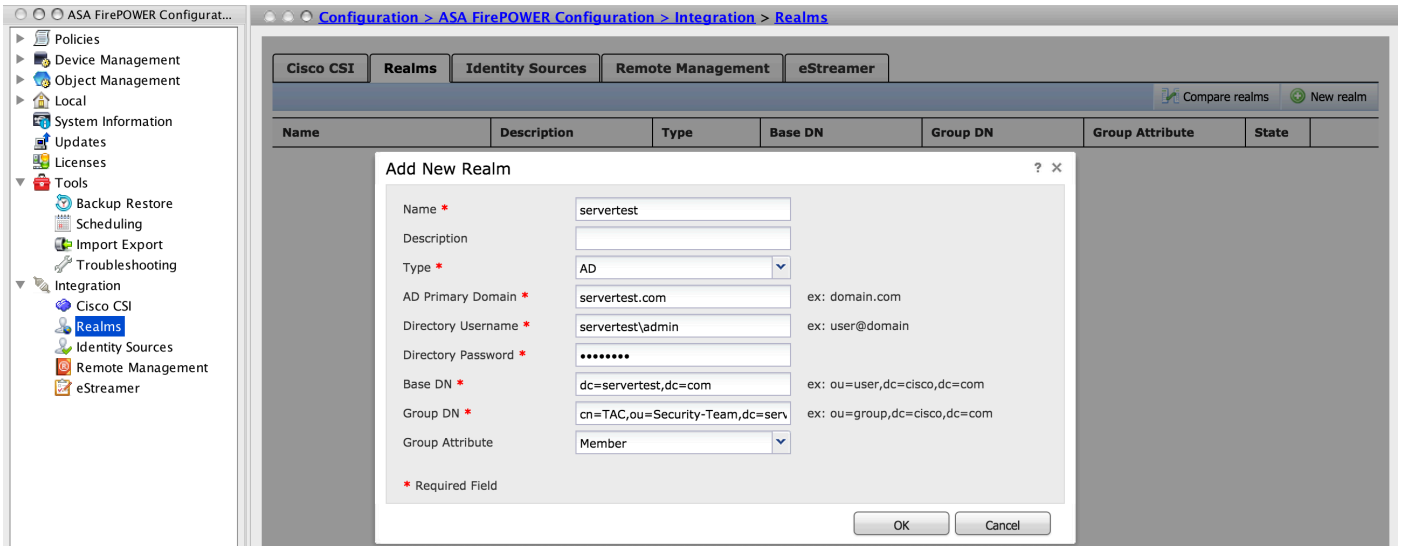
Directory Username: <username>を指定します。

[Directory Password]： <パスワード> を指定します。

ベースDN:システムがLDAPデータベース内で検索を開始するドメインまたは特定のOU DN。

[Group DN]：グループの DN を指定します。

[Group Attribute]：ドロップダウン リストからオプションの [Member] を指定します。



[OK] をクリックして、構成を保存します。

次の記事は、ベース DN およびグループ DN の値を決めるのに役立ちます。

[Active Directory LDAP オブジェクトの属性の特定]

手順 3.2： ディレクトリ サーバの IP アドレスとホスト名を追加する。

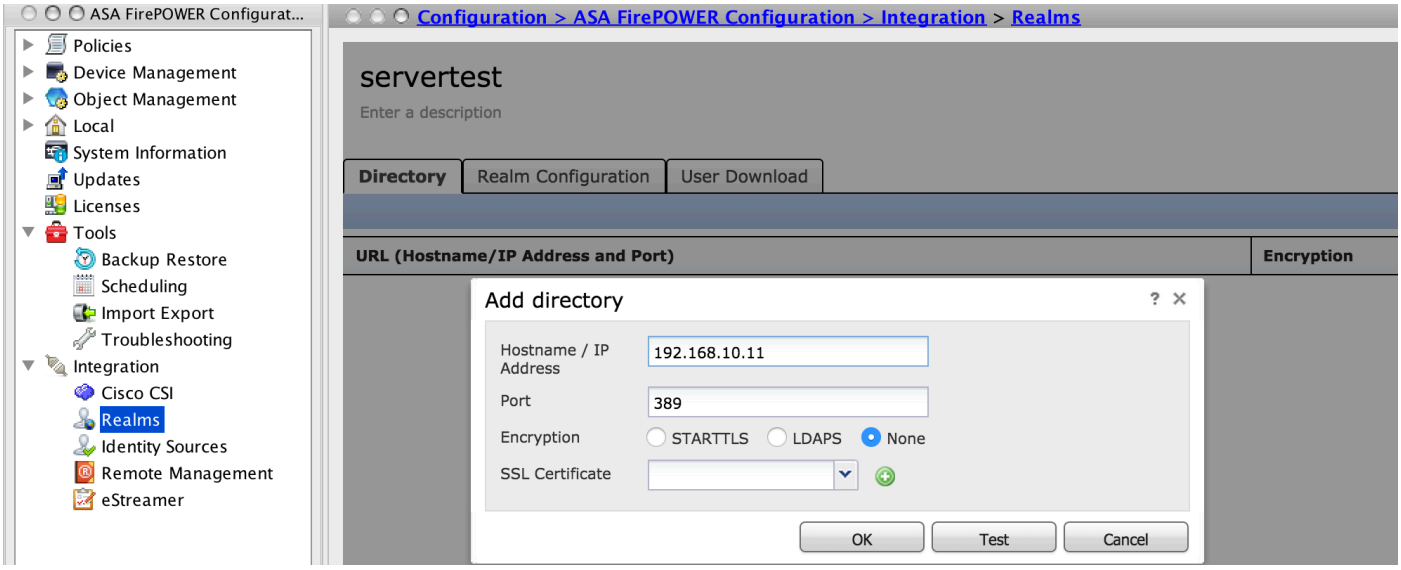
AD サーバの IP またはホスト名を指定するには、[Add directory] をクリックします。

ホスト名/IPアドレス： ADサーバのIPアドレス/ホスト名を設定します。

[Port]： Active Directory の LDAP ポート番号 (デフォルトは 389) を指定します。

暗号化/SSL証明書： (オプション)FMCとADサーバ間の接続を暗号化するには、次の記事を参照してください。

[「SSL/TLS 経由で Microsoft AD 認証を行うための FireSIGHT システム上の認証オブジェクトの検証」]



クリック **テスト** ADサーバとのFMCの接続を確認します。[OK] をクリックして、構成を保存します。

手順 3.3： レルムの設定を変更する。

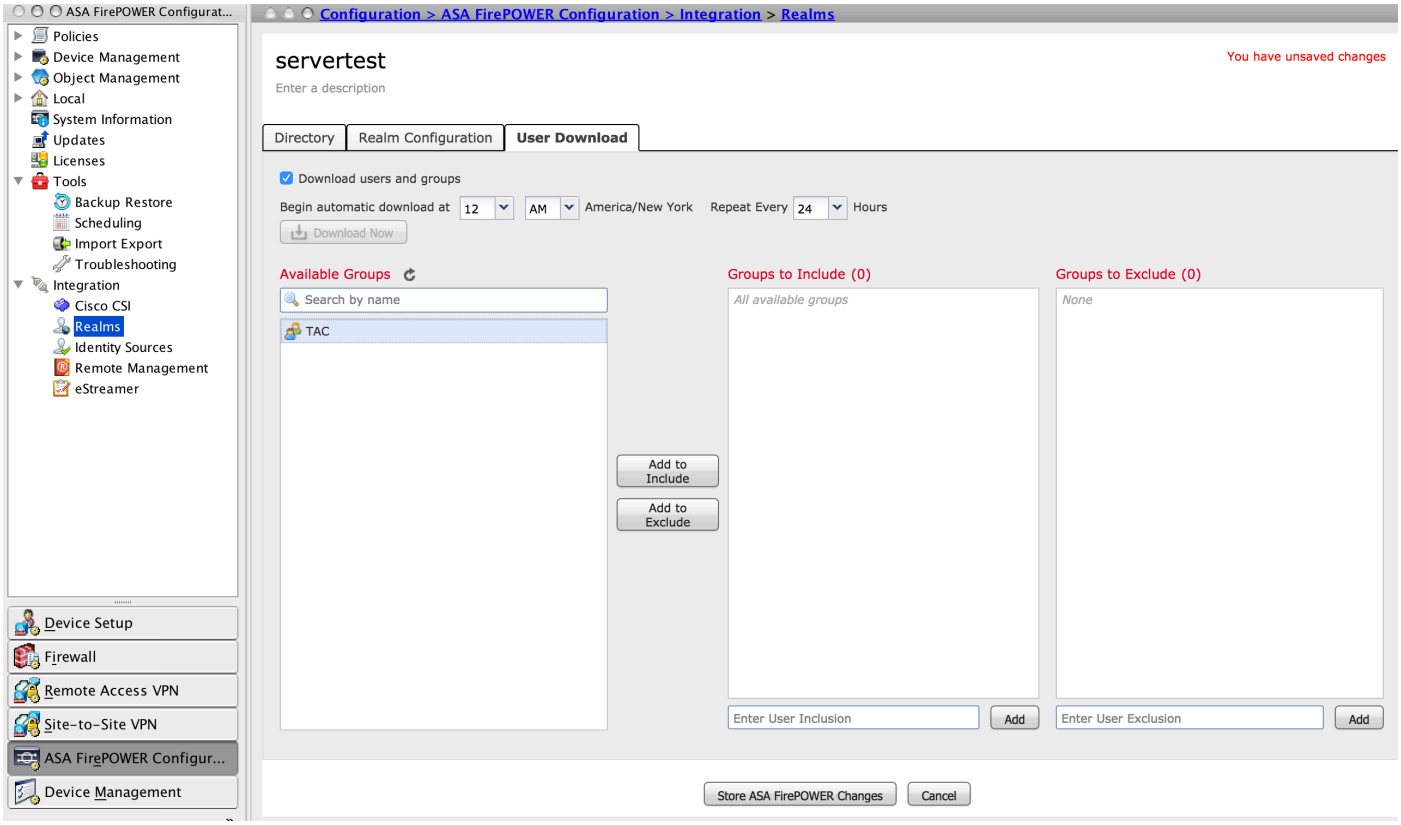
AD サーバの統合構成を変更して確認するには、[Realm Configuration] に移動します。

手順 3.4： ユーザ データベースをダウンロードする。

AD サーバからユーザ データベースを取得するために、[User Download] **に移動します。**

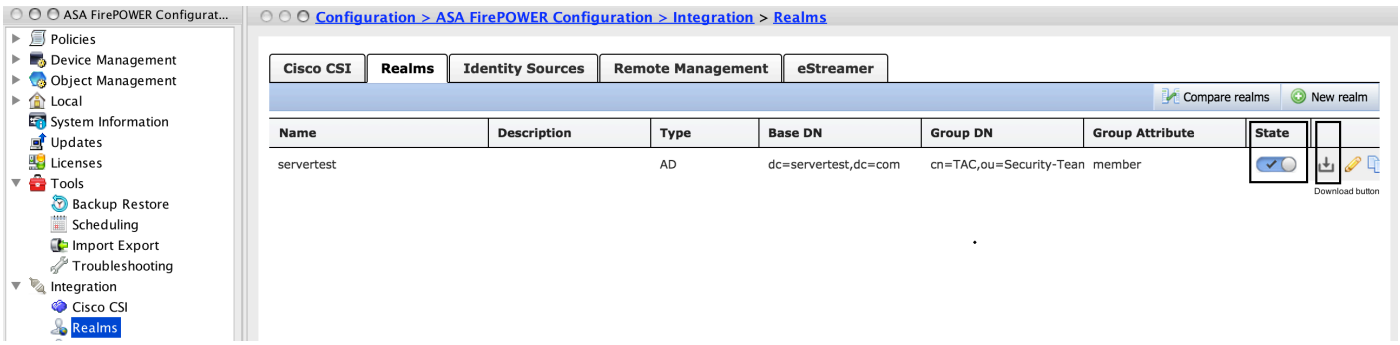
[Download users and groups] **チェックボックスをオンにしてダウンロードを有効にし、ユーザ データベースをダウンロードするために Firepower モジュールが AD サーバに接続する頻度を時間間隔で定義します。**

認証を設定するグループを選択し、[include] **オプションに追加します。**含めるグループを選択しないと、デフォルトですべてのグループが選択されます。



[Store ASA Firepower Changes] をクリックして、レルムの構成を保存します。

レルムの状態を有効にし、ダウンロード ボタンをクリックしてユーザとグループをダウンロードします（次の図を参照）。



ステップ 4：アイデンティティ ポリシーを設定する。

アイデンティティ ポリシーはユーザ認証を実行します。ユーザが認証されないと、ネットワークリソースへのアクセスが拒否されます。ポリシーを設定すると、ロールベース アクセス コントロール（RBAC）が組織のネットワークとリソースに適用されます。

手順 4.1： キャプティブ ポータル（アクティブ認証）。

アクティブ認証は、ブラウザでユーザ名とパスワードの入力を要求し、ユーザのアイデンティティを特定して、接続を許可します。ブラウザは、認証ページを表示することで、または NTLM 認証を使用してサイレントに、ユーザを認証します。 NTLM は、Web ブラウザを使用して、認証情報を送受信します。アクティブ認証は、さまざまな方式を使用してユーザのアイデンティティを確認します。認証の方式は次のとおりです。

1. **HTTP Basic：この方法では、ブラウザがユーザーの資格情報を要求します。**

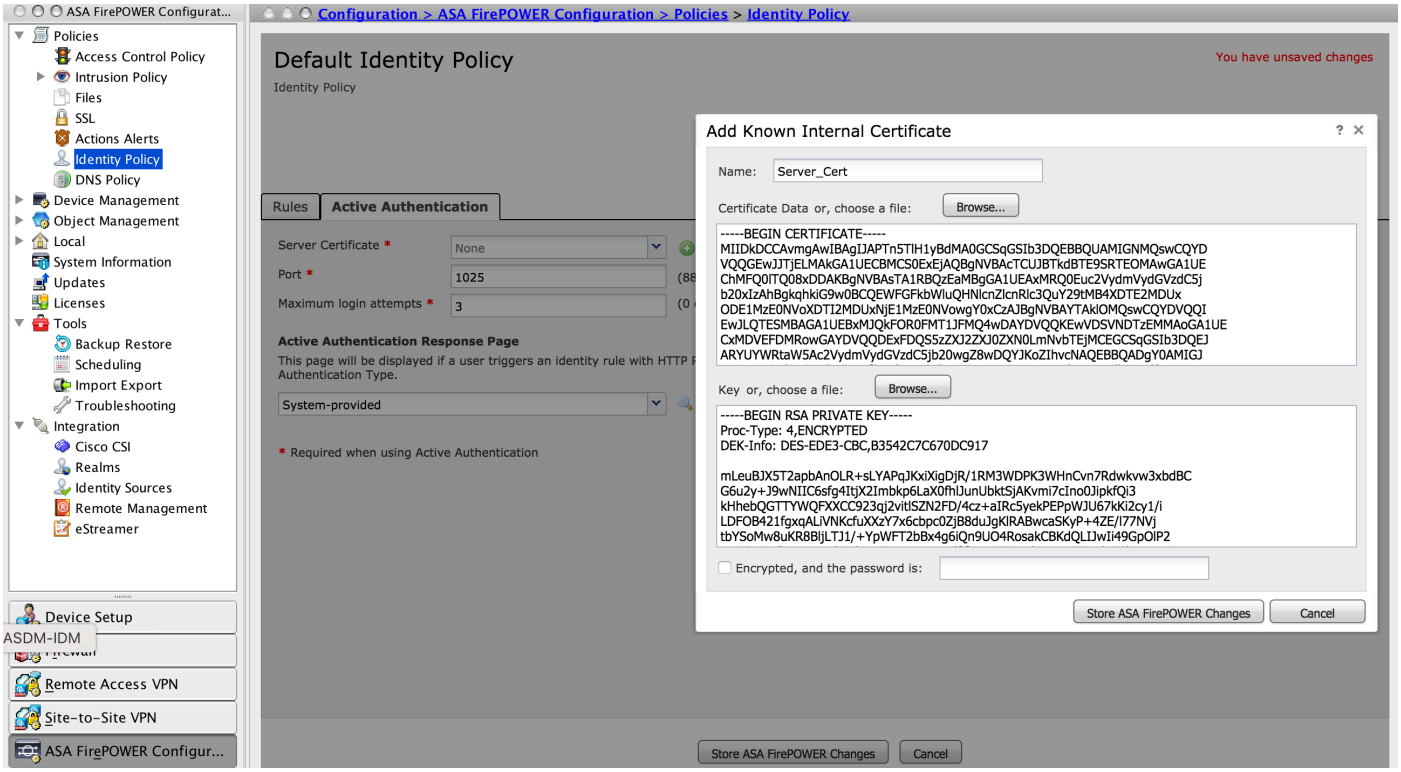
2. **NTLM： NTLM は、Windows ワークステーション クレデンシャルを使用し、Webブラウザを使用してそれを Active Directory とネゴシエートします。ブラウザで NTLM 認証を有効にする必要があります。ユーザ認証は、クレデンシャルを要求することなく透過的に行われます。ユーザにシングルサインオン環境を提供します。**
3. **HTTP Negotiate:**このタイプでは、システムはNTLMを使用して認証を試みます。失敗した場合、センサーはフォールバック方式としてHTTP Basic認証タイプを使用し、ユーザクレデンシャルのダイアログボックスを表示します。
4. **HTTP応答ページ：これはHTTP基本タイプに似ていますが、ここでユーザはカスタマイズ可能なHTML形式で認証を入力するように求められます。**

各ブラウザには NTLM 認証を有効にする固有の方法があり、そのため、NTLM 認証を有効にするにはブラウザのガイドラインに従います。

ルーテッド センサーとクレデンシャルを安全に共有するには、自己署名サーバ証明書または公開署名サーバ証明書をアイデンティティ ポリシーにインストールする必要があります。

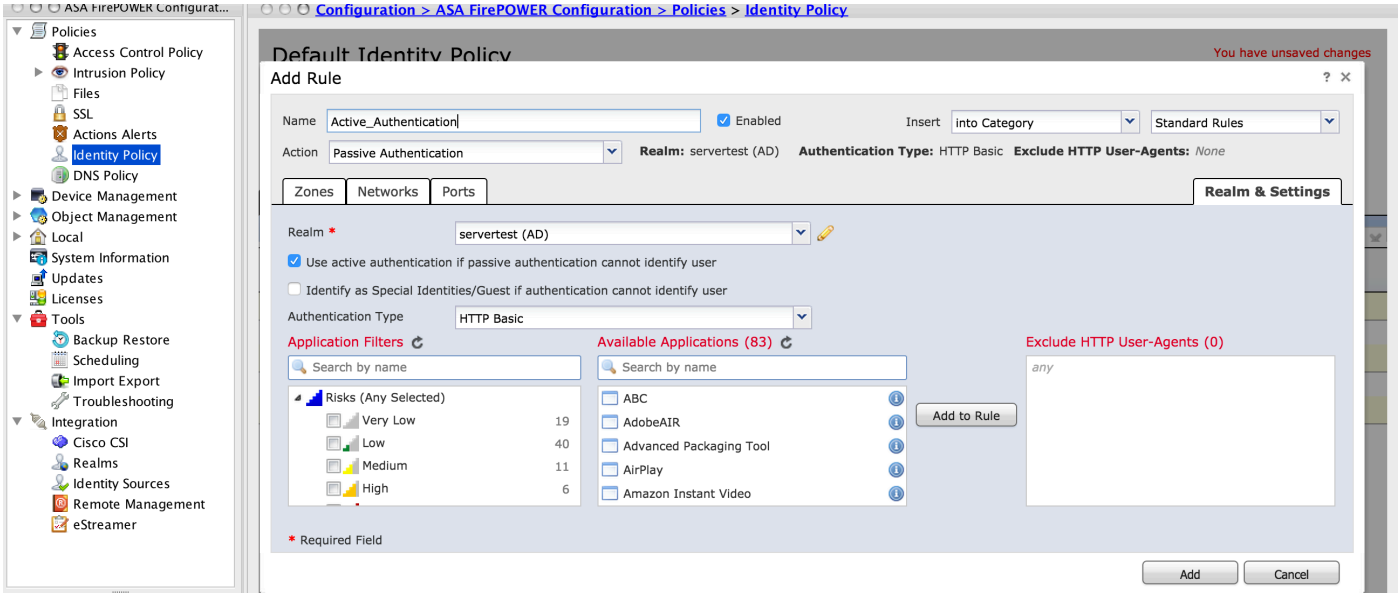
```
Generate a simple self-signed certificate using openSSL -

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
```

[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy]に移動します.次に、[Active Authentication]**タブに移動**し、[Server Certificate]オプション**で**、アイコン(+)を**クリックします** 図に示すように、openSSLを使用して前の手順で生成した証明書と秘密キーをアップロードします。



[Add rule] をクリックしてルールの名前を指定し、アクションとして [Active Authentication] を選択します。ユーザ認証を有効にする送信元/宛先ゾーンと送信元/宛先ネットワークを定義します。

[Realm & Settings] **タブに移動します。**[Realm] **ドロップダウン リストから前の手順で設定したレルムを選択し、[Authentication Type]** ドロップダウン リストからネットワーク環境に最適な認証方式を選択します。



手順 4.2 : キャプティブ ポータルの ASA 構成。

手順 1 : 検査のために Sourcefire にリダイレクトするインタレスティング トラフィックを定義します。

```
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
```

手順 2 : キャプティブ ポータルを有効にするために ASA で次のコマンドを設定します。

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

captive-portal

[Active Authentication]　TCP 1025

手順 4.3 : シングルサインオン (パッシブ認証) 。

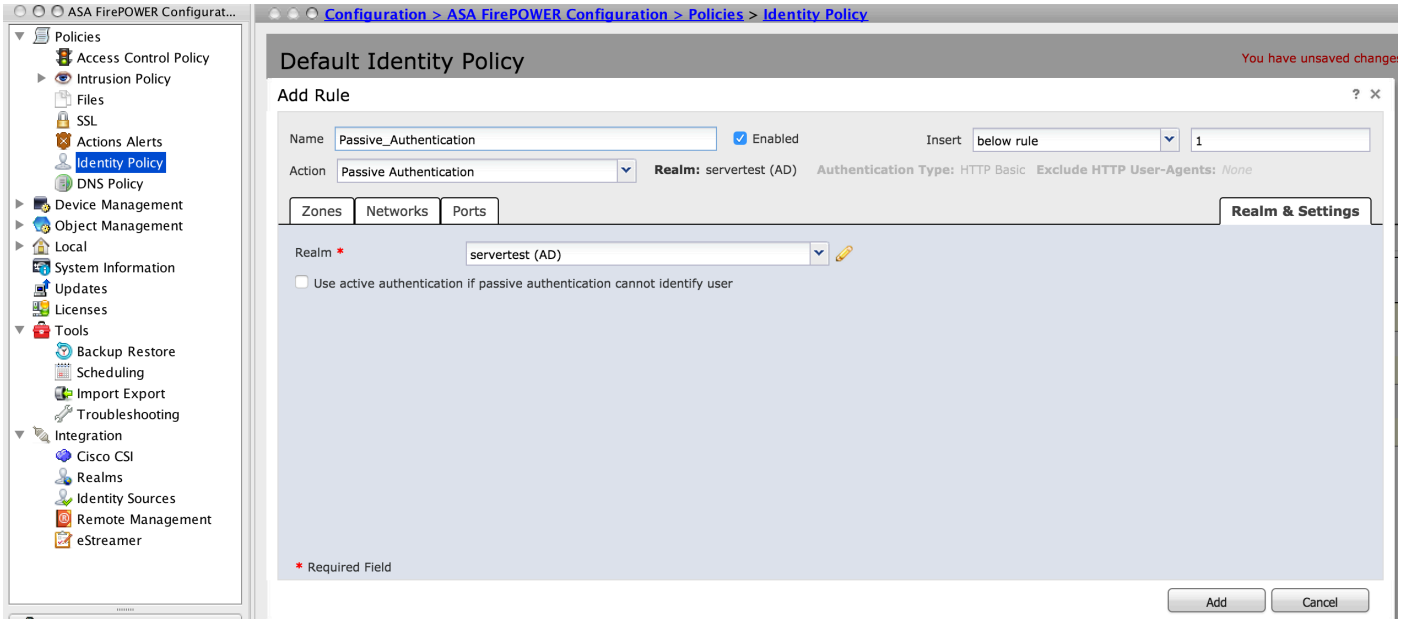
パッシブ認証では、ドメイン ユーザがログインして、AD の認証を行うことができる場合、Firepower ユーザ エージェントは AD のセキュリティ ログから ユーザと IP マッピングの詳細を

ポーリングし、この情報を Firepower モジュールと共有します。Firepower モジュールはこれらの詳細を使用して、アクセス制御を適用します。

パッシブ認証ルールを設定するには、[Add rule] をクリックしてルールの名前を指定し、[Action] **として [Passive Authentication]** を選択します。ユーザ認証を有効にする送信元/宛先ゾーンと送信元/宛先ネットワークを定義します。

次の場所に移動します。 **レルムと設定** tab.選択 **領域** ドロップダウンリストから選択します。

フォールバック方法として、[Active authentication if passive authentication cannot identify the user identity] を選択できます（次の図を参照）。

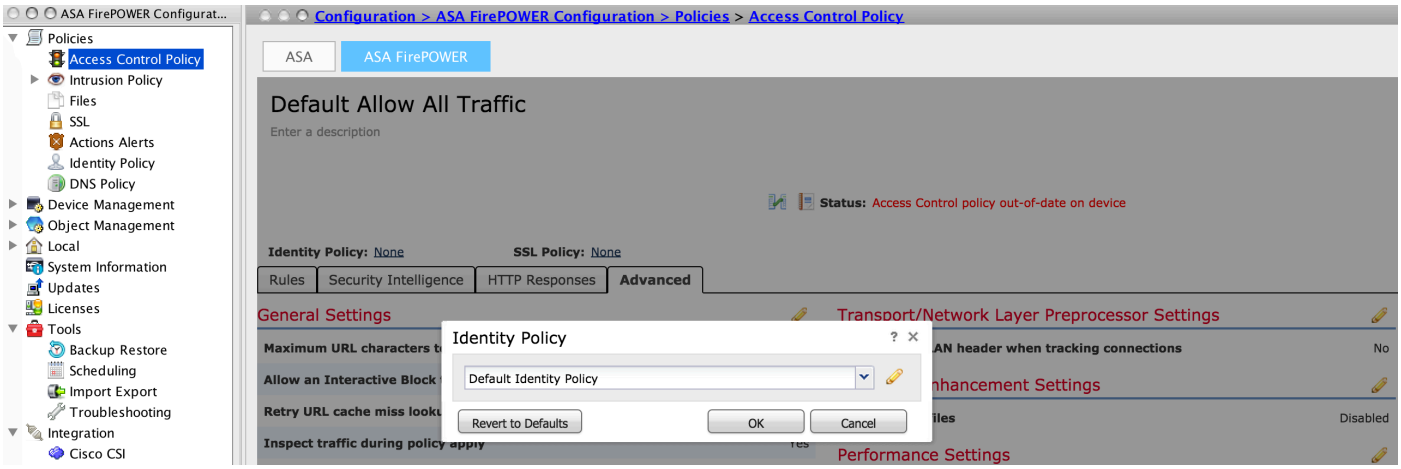


[Store ASA Firepower Changes] をクリックして、アイデンティティ ポリシーの設定を保存します。

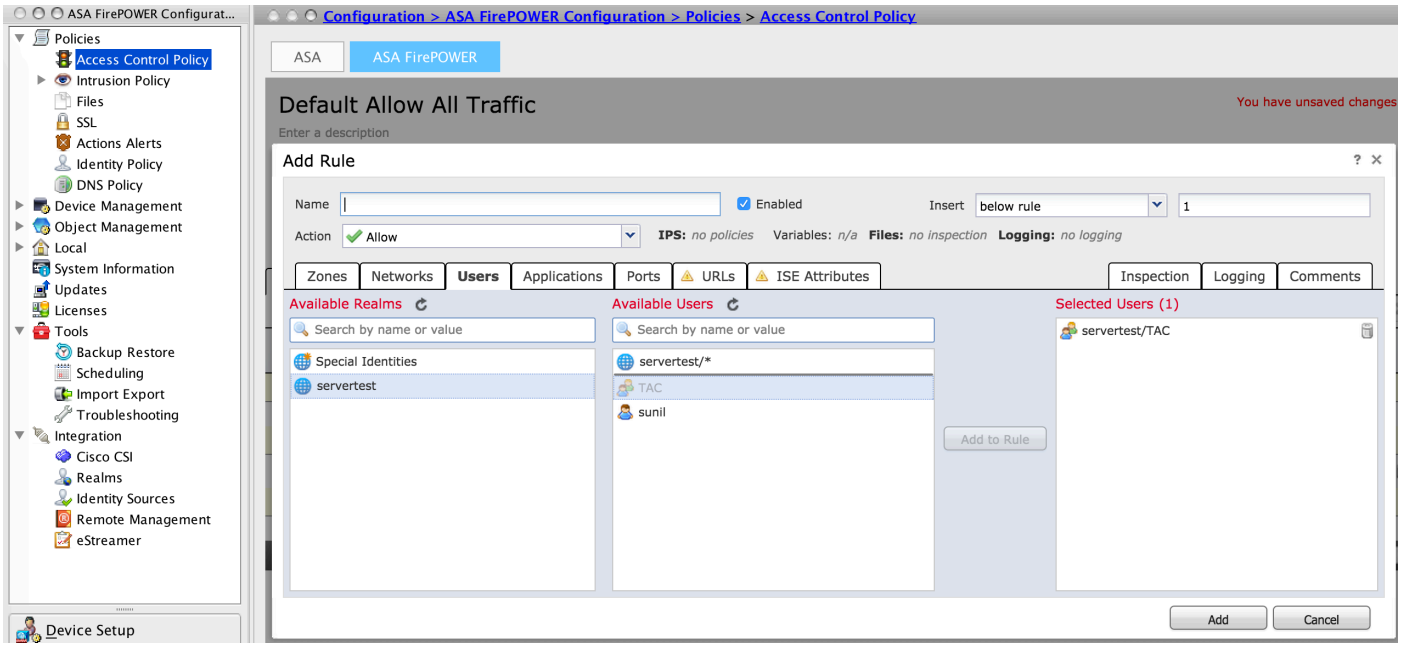
ステップ 5：アクセス コントロール ポリシーを設定する。

[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] に移動します。

[Identity Policy]（左上隅）をクリックして、ドロップダウン リストから前の手順で設定したアイデンティティポリシーを選択し、[OK] をクリックします（次の図を参照）。



クリック **ルールの追加** 新しいルールを追加するには、**[ユーザ (Users)]** 次の図に示すように、アクセスコントロールルールを適用するユーザを選択し、[Add]をクリックします.



クリック **ASA Firepowerの変更の保存** アクセスコントロールポリシーの設定を保存します。

手順 6：アクセス コントロール ポリシーを展開する。

アクセス コントロール ポリシーを展開する必要があります。ポリシーを適用する前に、モジュールにアクセスコントロールポリシーの最新の情報が表示されます。センサーに変更を展開するには、[Deploy]をクリックし、**[Deploy FirePOWER Changes]オプションを選択し**て、ポップアップウィンドウの[Deploy]をクリックします。

> **注**：バージョン 5.4.x では、アクセス ポリシーをセンサーに適用するには、[Apply ASA FirePOWER Changes] をクリックする必要があります。

> **注**：[Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動します。構成の変更を適用するには、タスクを完了する必要があります。

手順 7：

[Monitoring] > [ASA FirePOWER Monitoring] > [Real-Time Eventing] に移動し、ユーザが使用しているトラフィックの種類を監視します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

[Analysis] > [Users] に移動し、トラフィック フローに関連付けられているユーザ認証、認証の種類、ユーザ IP マッピング、アクセス ルールを確認します。

Firepower モジュールとユーザ エージェント間の接続 (パッシブ認証)

ユーザ エージェントからユーザ アクティビティ ログ データを受信するために、Firepower モジュールは TCP ポート 3306 を使用します。

Firepower モジュールのサービス ステータスを確認するには、FMC で次のコマンドを使用します。

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

ユーザ エージェントとの接続を確認するには、FMC でパケット キャプチャを実行します。

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

FMC と Active Directory 間の接続

Active directory からユーザ データベースを取得するために、Firepower モジュールは TCP ポート 389 を使用します。

Active Directory との接続を確認するには、Firepower モジュールでパケット キャプチャを実行します。

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

レルムの設定で使用されているユーザ クレデンシャルに、AD のユーザ データベースを取得するのに十分な権限があることを確認します。

レルムの設定を調べて、ユーザまたはグループがダウンロードされること、およびユーザ セッションのタイムアウトが正しく設定されていることを確認します。

[Monitoring ASA Firepower Monitoring Task Status] に移動し、タスク ユーザとグループのダウンロードが正常に完了したことを確認します（次の図を参照）。

ASA とエンド システム間の接続（アクティブ認証）

アクティブ認証の場合、Firepower モジュールのアイデンティティ ポリシーおよび ASA で証明書とポートが正しく設定されていることを確認します（キャプティブ ポータル コマンド）。 デフォルトでは、ASA と Firepower モジュールは、TCP ポート 885 でアクティブ認証をリッスンします。

アクティブなルールとそのヒット数を調べるには、ASA で次のコマンドを実行します。

```
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
```

ポリシーの設定とポリシーの展開

[Identity Policy] で [Realm]、[Authentication type]、[User agent]、[Action] の各フィールドが正しく設定されていることを確認します。

アイデンティティ ポリシーがアクセス コントロール ポリシーと正しく関連付けられていることを確認します。

[Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動し、ポリシーの展開が正常に完了していることを確認します。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems
- シングルサインオンとキャプティブ ポータルの認証用に FirePOWER アプライアンスを含む Active Directory の統合を設定する