

シングルサインオン&キャプティブポータル認証用のActive DirectoryとFirepowerアプライアンスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ 1: シングルサインオン用のFirepowerユーザエージェントの設定](#)

[ステップ 2: firepower Management Center\(FMC\)とUser Agentの統合](#)

[ステップ 3: FirepowerとActive Directoryの統合](#)

[手順 3.1 レルムの作成](#)

[手順 3.2 ディレクトリ サーバの追加](#)

[手順 3.3 レルム設定の変更](#)

[手順 3.4 ユーザ データベースのダウンロード](#)

[ステップ 4: アイデンティティポリシーの設定](#)

[手順 4.1 キャプティブ ポータル \(アクティブ認証\)](#)

[手順 4.2 シングルサインオン \(パッシブ認証\)](#)

[ステップ 5: アクセスコントロールポリシーの設定](#)

[手順 6: アクセスコントロールポリシーの導入](#)

[手順 7: ユーザイベントと接続イベントの監視](#)

[確認とトラブルシューティング](#)

[FMCとユーザエージェントの間の接続の確認 \(パッシブ認証\)](#)

[FMCとActive Directoryの間の接続の確認](#)

[Firepower センサーとエンドシステム間の接続の確認 \(アクティブ認証\)](#)

[ポリシー設定とポリシー展開の確認](#)

[イベントログの分析](#)

[関連情報](#)

はじめに

このドキュメントでは、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) の設定について説明します。

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。

- Sourcefire Firepower デバイス
- バーチャル デバイス モデル
- 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。

- Firepower Management Center(FMC)バージョン6.0.0以降
- Firepowerセンサーバージョン6.0.0以降

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、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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は、ネットワークリソースおよびインターネットアクセスに関して、ユーザのクレデンシャルが複数回発生することなく、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の場合、アプライアンスはルーテッドモードである必要があります。

設定

ステップ 1 : シングルサインオン用のFirepowerユーザエージェントの設定

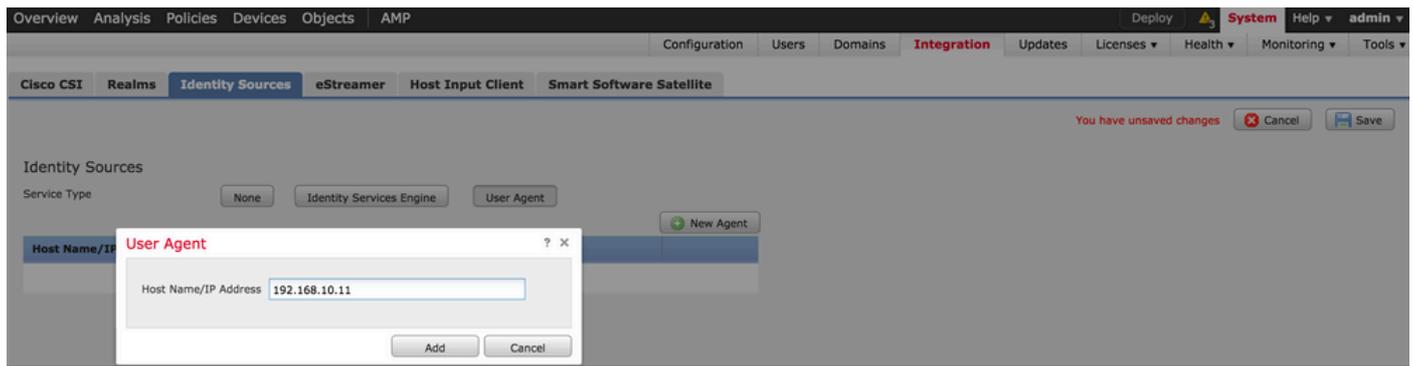
次の記事では Windows マシンで Firepower ユーザ エージェントを設定する方法について説明しています。

[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 Management Center(FMC)とUser Agentの統合

Firepower Management Center にログインし、[System] > [Integration] > [Identity Sources] の順に移動します。[New Agent] オプションをクリックします。ユーザ エージェント システムの IP アドレスを設定して [Add] ボタンをクリックします。

[Save] ボタンをクリックして変更内容を保存します。



ステップ 3 : FirepowerとActive Directoryの統合

手順 3.1 レルムの作成

FMC にログインして [System] > [Integration] > [Realm] の順に移動します。[Add New Realm] オプションをクリックします。

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

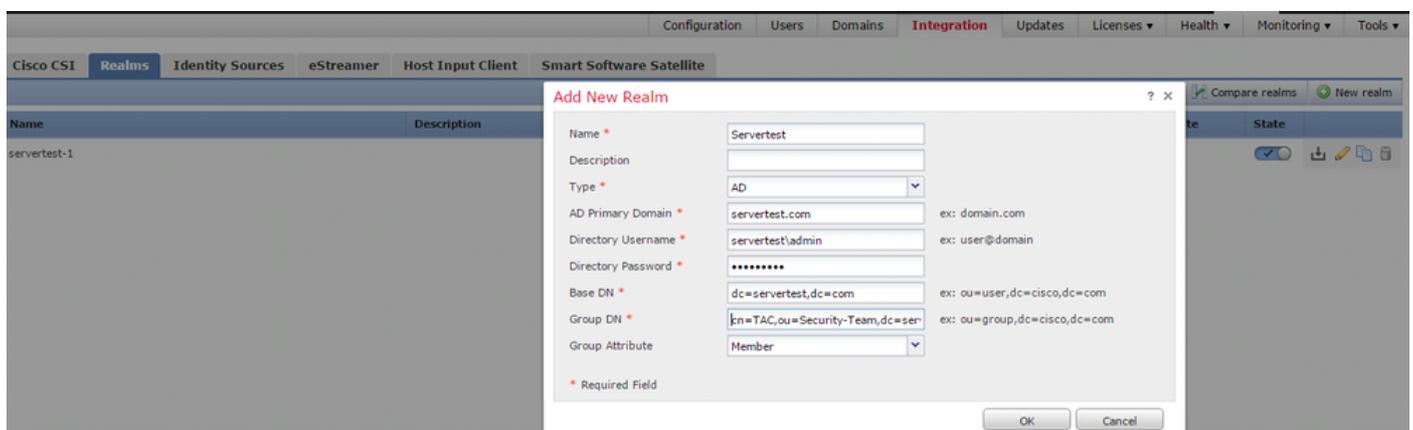
ディレクトリユーザ名 : <username>

ディレクトリパスワード : <password>

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

グループDN:グループDN

グループ属性 : メンバー



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 サーバの追加

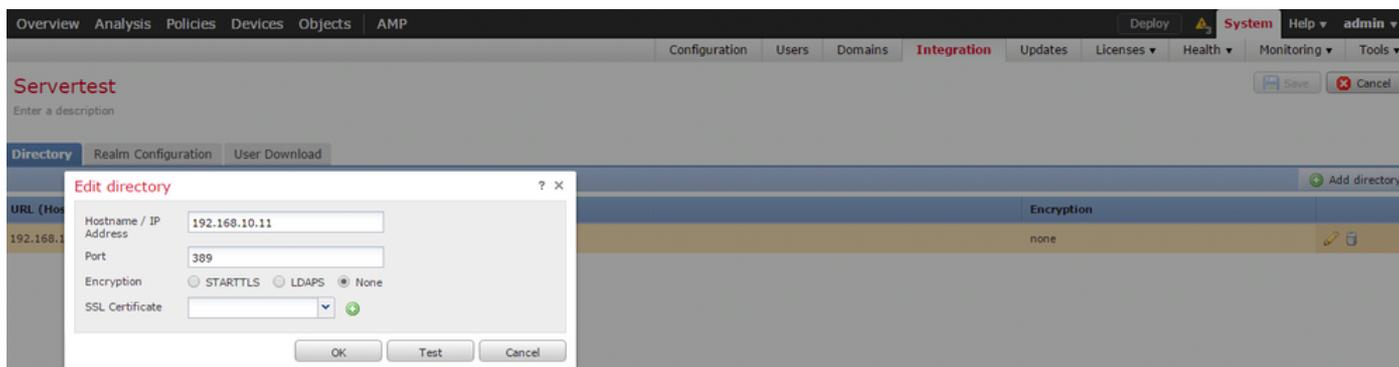
次の手順に進むために [Add] ボタンをクリックし、[Add directory] オプションをクリックします。

Hostname/IP Address:ADサーバのIPアドレス/ホスト名を設定します。

ポート : 389 (Active Directory LDAPポート番号)

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、

記事 : [FireSIGHTシステムでのSSL/TLSを介したMicrosoft AD認証のための認証オブジェクトの検証](#)



FMC が AD サーバに接続できるかどうかを確認するには、[Test] ボタンをクリックします。

手順 3.3 レルム設定の変更

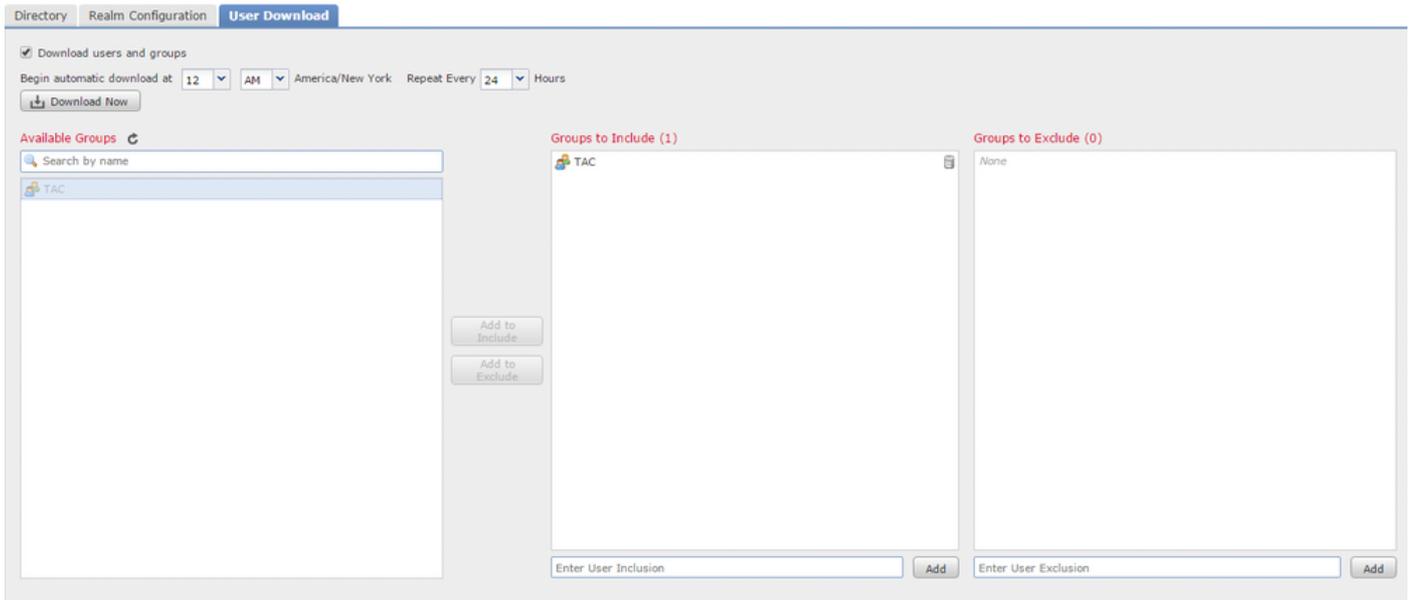
AD サーバの統合設定を確認したり AD の設定を変更したりするには、[Realm Configuration] に移動します。

手順 3.4 ユーザ データベースのダウンロード

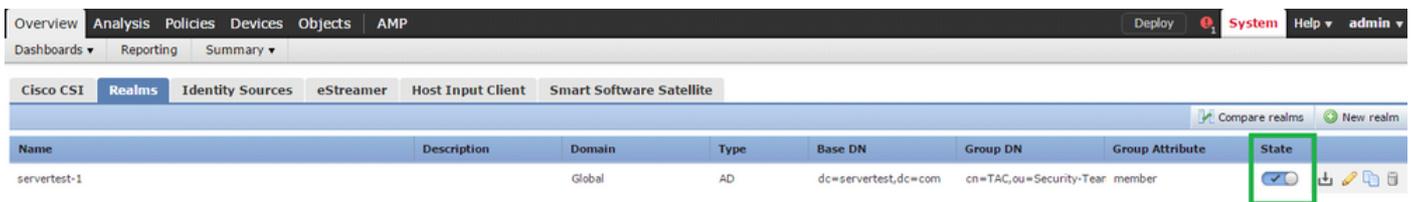
AD サーバからユーザ データベースを取得するために、[User Download] オプションに移動します。

[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 FMC が AD 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。



図に示すように、AD の状態を有効にします。



ステップ 4 :

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求め、ユーザIDを特定して接続を許可します。ブラウザは、認証ページを使用してユーザを認証するか、NTLM認証を使用してサイレントモードで認証します。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、ブラウザはユーザクレデンシャルの入力を求めます。
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ブラウザを介して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、クレデンシャルのプロンプトなしで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ネゴシエーション：このタイプでは、システムはNTLMによる認証を試行します。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入力を求める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、このページでは、カスタマイ

ズ可能なHTMLフォームに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るため、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
```

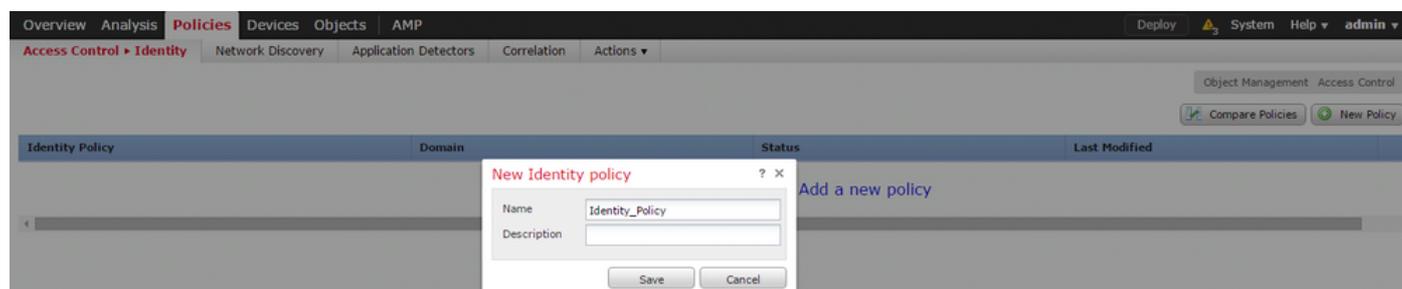
Step 2. Generate Certificate Signing Request (CSR)

```
openssl req -new -key server.key -out server.csr
```

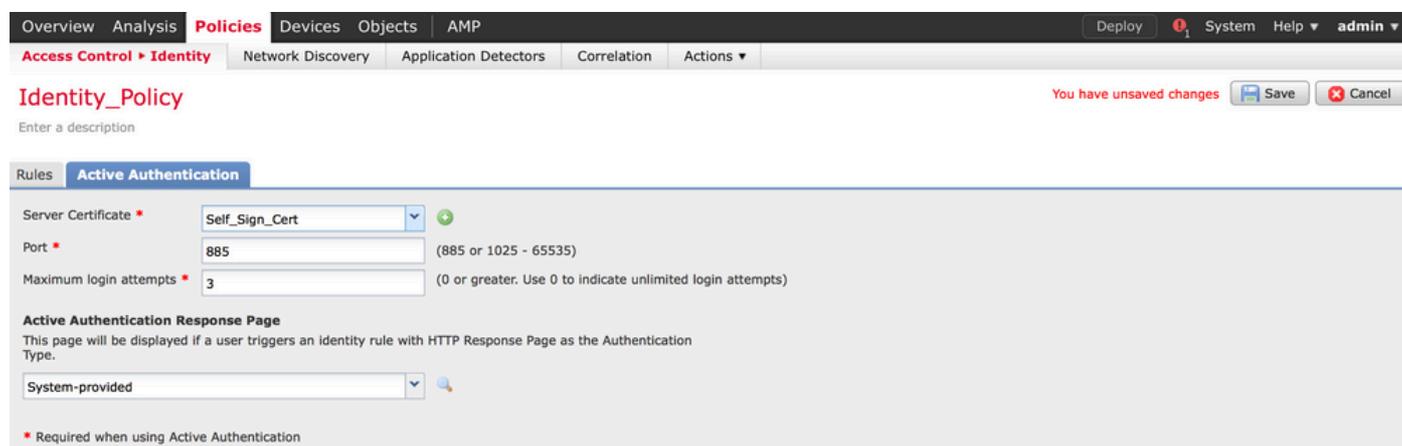
Step 3. Generate the self-signed Certificate.

```
openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

[Policies] > [Access Control] > [Identity] の順に移動します。[Add Policy] をクリックし、ポリシーに名前を付けて保存します。



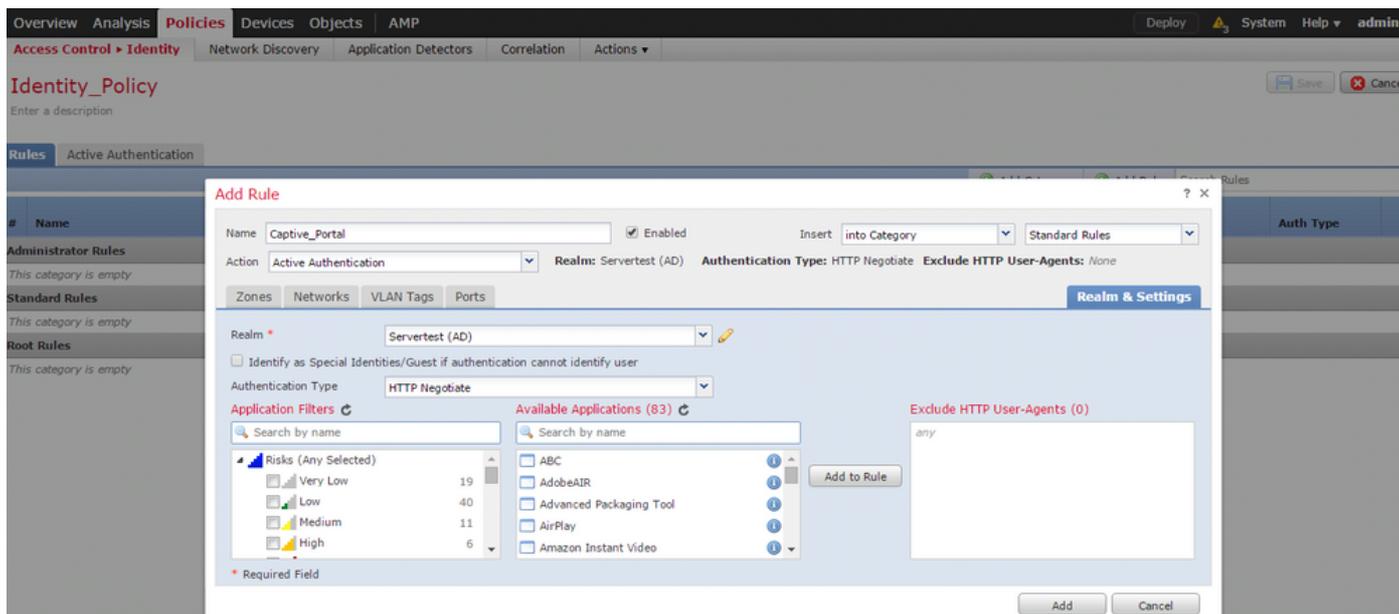
Active Authenticationタブに移動し、Server Certificateオプションでアイコン(+)をクリックし、opensslで前の手順で生成した証明書と秘密キーをアップロードします。



[Add rule] ボタン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] で前の手順で設定したレルムを選択し、環境に適した認証タイプを選択します。



キャプティブ ポータル用の ASA の設定

ASA Firepower モジュールについて、キャプティブ ポータルを設定するために ASA で次のコマンドを設定します。

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

アイデンティティポリシーのアクティブ認証タブのportオプションで、サーバポートTCP 1055が設定されていることを確認します。

アクティブなルールとそのヒットカウントを確認するには、次のコマンドを実行します。

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



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。

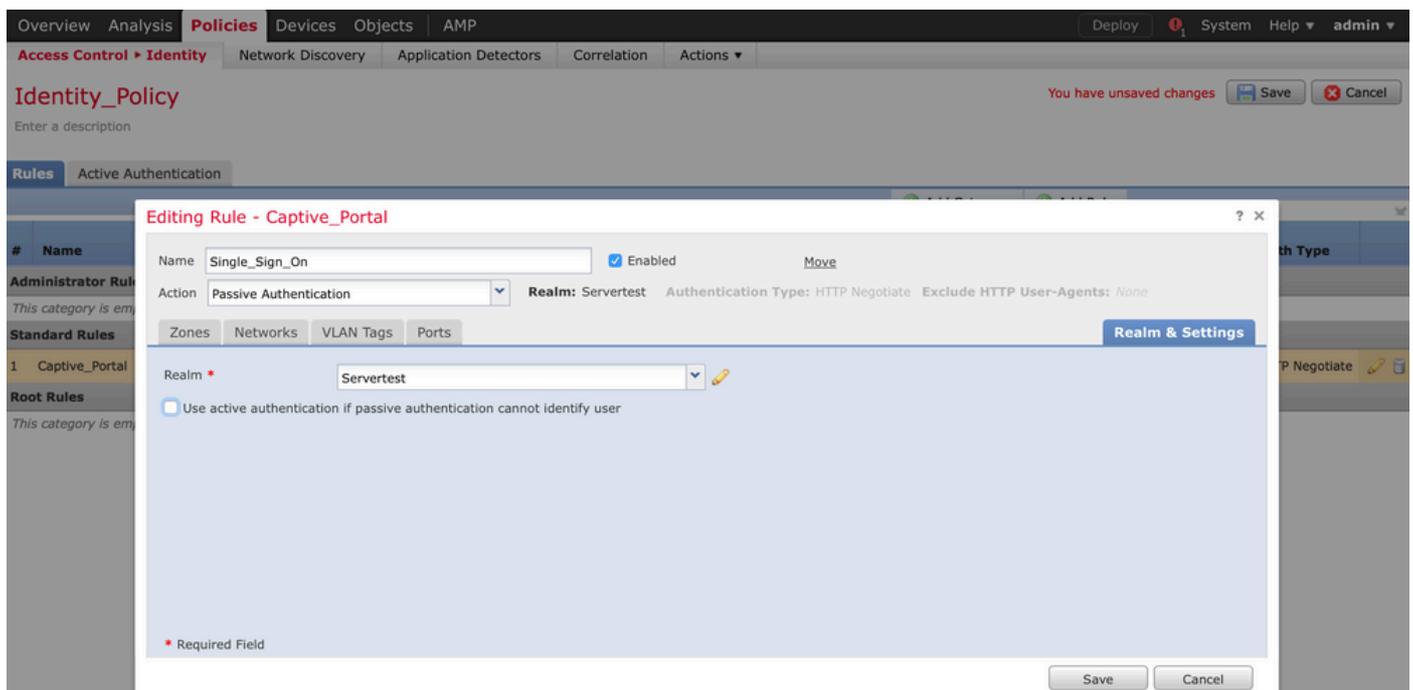
手順 4.2 シングルサインオン (パッシブ認証)

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 のマッピングの詳細情報をポーリングし、この情報を Firepower Management Center (FMC) と共有します。FMC はアクセス制御を強化するために、その詳細情報をセンサーに送信します。

[Add rule] ボタンをクリックしてルールの名前を指定し、[Action] で [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。

次の図に示すように、[Realm] で前の手順で設定したレルムを選択し、環境に適した認証タイプを選択します。

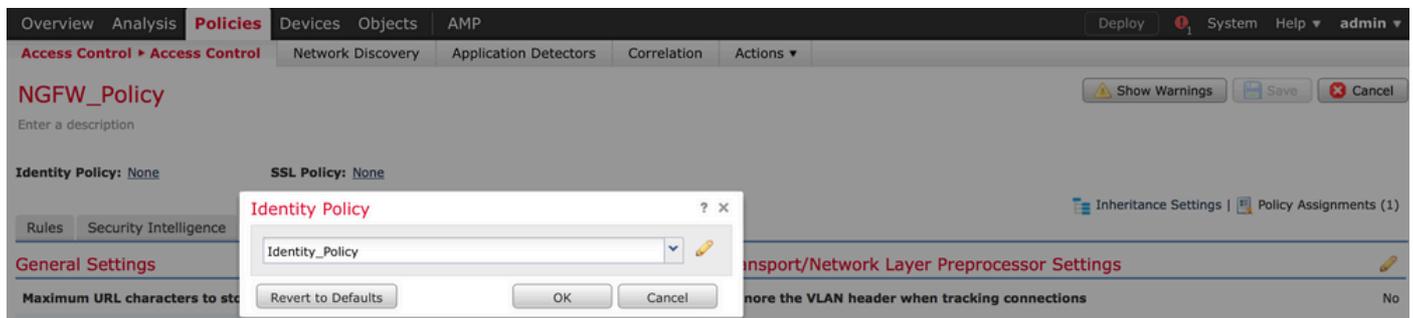
フォールバック方法として、[Active authentication if passive authentication cannot identify the user identity] を選択できます。



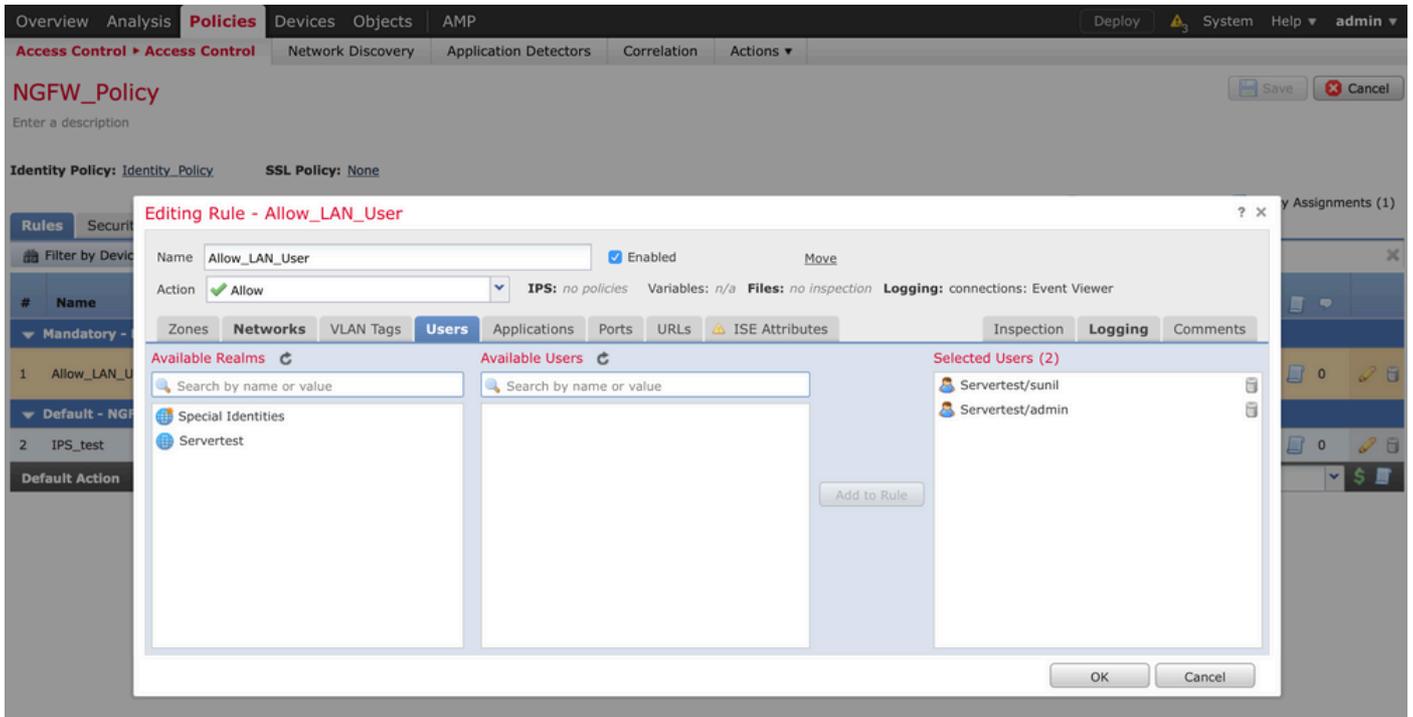
ステップ 5 :

[Policies] > [Access Control] > [Create/Edit a Policy] の順に移動します。

[Identity Policy] (左上隅) をクリックして、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)。

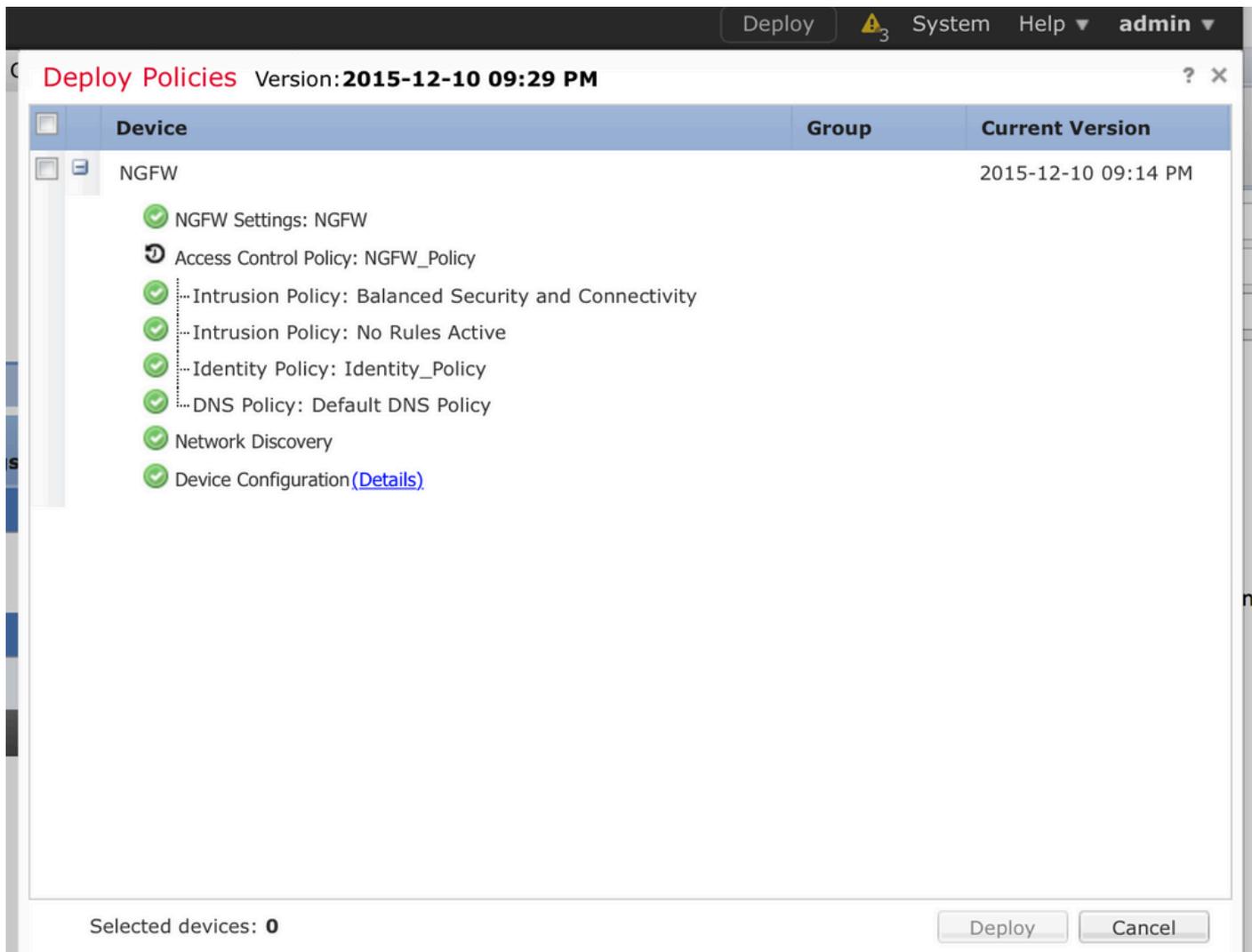


Add rule ボタンをクリックして、新しいルールを追加します。次の図に示すように、Users に移動し、アクセスコントロールルールが適用されるユーザを選択します。OK をクリックし、次に Save をクリックして変更を保存します。



手順 6 :

[Deploy] オプションに移動し、[Device] を選択して [Deploy] オプションをクリックします。これによって設定の変更がセンサーにプッシュされます。[Message Center] アイコン ([Deploy] オプションと [System] オプションの間のアイコン) によってポリシーの展開をモニタし、ポリシーが正常に適用されたことを確認します (次の図を参照)。



手順 7: ユーザ モニタするイベントと接続のイベント

現在アクティブなユーザ セッションは、[Analysis] > [Users] > [Users] セクションで確認できます。

ユーザ アクティビティのモニタリングは、ユーザに関連付けられている IP アドレスの確認や、アクティブ認証とパッシブ認証のいずれによってユーザがシステムに検出されたかの確認に役立ちます。[Analysis] > [Users] > [User Activity]

User Activity

[Table View of Events](#) > [Users](#)

No Search Constraints ([Edit Search](#))

	Time	Event	Realm	Username	Type	Authentication Type	IP Address
↓	2015-12-10 11:15:34	User Login	Servertest	sunil	LDAP	Active Authentication	192.168.20.20
↓	2015-12-10 10:47:31	User Login	Servertest	admin	LDAP	Passive Authentication	192.168.0.6

Analysis > Connections > Eventsの順に移動し、ユーザが使用するトラフィックのタイプを監視します。

First Packet	Last Packet	Action	Initiator IP	Initiator User	Responder IP	Access Control Rule	Ingress Interface	Egress Interface	Count
2015-12-11 10:31:59	2015-12-11 10:34:19	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1
2015-12-11 10:31:59		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1
2015-12-11 09:46:28	2015-12-11 09:46:29	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
2015-12-11 09:46:28		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
2015-12-11 09:46:07	2015-12-11 09:46:58	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
2015-12-11 09:46:07		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
2015-12-11 09:45:46	2015-12-11 09:46:36	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1

確認とトラブルシューティング

[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。

FMC とユーザ エージェントの間の接続の確認 (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 Management Center (FMC) は TCP ポート 3306 を使用します。

FMC 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がユーザエージェントからユーザログインの詳細を受信するかどうかを確認するには、Analysis > Users > User Activityの順に移動します。

FMC と Active Directory の間の接続の確認

FMCはTCPポート389を使用して、ユーザデータベースを Active Directory.

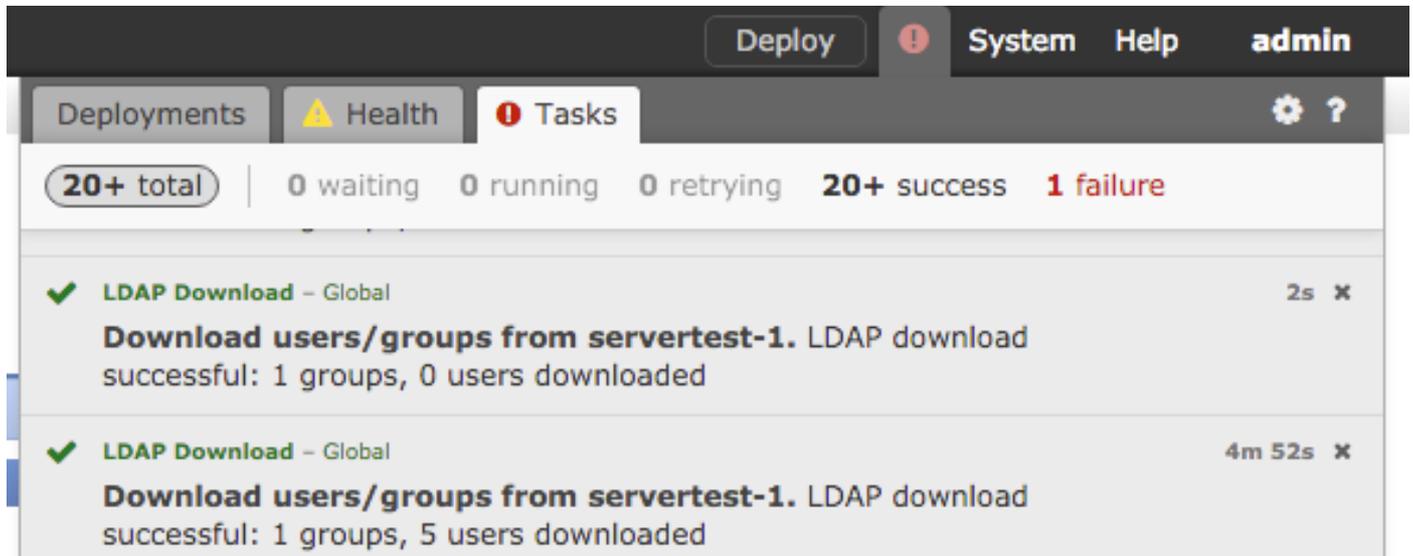
Active Directory との接続を確認するには、FMC でパケット キャプチャを実行します。

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

FMCレールの設定で使用されているユーザクレデンシャルに、ADユーザデータベースを取得するための十分な権限があることを確認します。

FMCレールの設定を調べて、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。

[Message Center] > [Tasks] に移動して、次の図に示すように、ユーザまたはグループのダウンロードのタスクが正常に完了していることを確認します。



Firepower センサーとエンド システムの間の接続の確認 (アクティブ認証)

アクティブ認証の場合は、証明書とポートがFMCアイデンティティポリシーで正しく設定されていることを確認します。デフォルトでは、FirepowerセンサーはTCPポート885でアクティブ認証をリッスンします。

ポリシー設定とポリシー展開の確認

[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。

[Message Center] > [Tasks] に移動して、ポリシーの展開が正常に完了したことを確認します。

イベント ログの分析

接続イベントとユーザアクティビティイベントは、ユーザログインが成功したかどうかを診断するために使用できます。これらのイベントは、

どのアクセスコントロールルールがフローに適用されているかも確認できます。

[Analysis] > [User] に移動して、ユーザ イベント ログをチェックします。

[Analysis] > [Connection Events] に移動して、接続イベントをチェックします。

関連情報

- ・ [テクニカルサポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。