

FireSIGHT システムと RADIUS ユーザ認証用の ISE の統合

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ISE の設定](#)

[ネットワーク デバイスとネットワーク デバイス グループの設定](#)

[ISE 認証ポリシーの設定 :](#)

[ISE へのローカル ユーザの追加](#)

[ISE 認可ポリシーの設定](#)

[Sourcefire のシステム ポリシー設定](#)

[外部認証の有効化](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco FireSIGHT Management Center (FMC) または Firepower 管理対象デバイスを Remote Authentication Dial In User Service (RADIUS) ユーザ認証用の Cisco Identity Services Engine (ISE) と統合するために必要な設定手順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。

- GUI またはシェルによる FireSIGHT システムおよび管理対象デバイスの初期設定
- ISE 上での認証ポリシーおよび認可ポリシーの設定
- RADIUS の基礎知識

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。

- Cisco ASA v9.2.1
- ASA FirePOWER モジュール v5.3.1
- ISE 1.2

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。

設定

ISE の設定

ヒント：ISE の認証ポリシーおよび認可ポリシーを、Sourcefire などのネットワーク アクセス デバイス (NAD) との統合をサポートするように設定する方法は複数あります。次の例は、この統合を設定するための方法の 1 つです。設定例は一種の評価基準であり、採用して特定の導入のニーズに合わせて変更させられます。認可の設定は、2 つの手順のプロセスであることに注意してください。1 つ以上の認可ポリシーを ISE で定義し、ISE に RADIUS 属性値のペア (av ペア) を FMC または管理対象デバイスに返させます。これらの av ペアは、次に FMC システムのポリシー設定で定義されたローカル ユーザ グループにマッピングされます。

ネットワーク デバイスとネットワーク デバイス グループの設定

- ISE の GUI で、[Administration] > [Network Resources] > [Network Devices] に移動します。[+Add] をクリックして、新しいネットワーク アクセス デバイス (NAD) を追加します。このデバイスの説明になる名前とデバイスの IP アドレスを指定します。次の例では、FMC が定義されています。

Network Devices

* Name
Description

* IP Address: /

- [Network Device Groups] の下で、[All Device Types] の横のオレンジ色の矢印をクリックします。アイコンをクリックし  て、[Create New Network Device Group] を選択します。次のスクリーンショットの例では、[Device Type] の [Sourcefire] が設定されています。この [Device Type] は、後の手順の認可ポリシーの規則の定義で参照されています。[Save] をクリックします。

Create New Network Device Group... ×

Network Device Groups

* Parent Reset to Top Level

* Name

Description

* Type

- オレンジ色の矢印を再度クリックし、上の手順で設定されたネットワーク デバイス グループ を選択します

* Network Device Group

Location Set To Default

Device Type Set To Default

- [Authentication Settings] の横にあるチェックボックスをオンにします。 この NAD に使用する RADIUS 共有秘密キーを入力します。 同じ共有秘密キーが、後で FireSIGHT MC 上で RADIUS サーバを設定する際に再度使用されることに注意してください。 プレーン テキスト (非暗号化テキスト) のキー値を確認するには、[Show] ボタンをクリックします。 [Save] をクリックします。

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret Show

Enable KeyWrap ⓘ

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

- GUI アクセスまたはシェル アクセスに RADIUS ユーザ認証または認可を必要とするすべての FireSIGHT MC と管理対象デバイスについて、上記の手順を繰り返します。

ISE 認証ポリシーの設定 :

- ISE の GUI で、[Policy] > [Authentication] に移動します。 ポリシー セットを使用する場合、[Policy] > [Policy Sets] に移動します。 次の例は、デフォルトの認証ポリシー インターフェイスおよび認可ポリシー インターフェイスを使用する ISE 導入からのものです。 認証および認可規則のロジックは、設定方法に関係なく同じです。
- 使用中の方法が MAC 認証バイパス (MAB) または 802.1X でない NAD からの RADIUS 要求

を認証するために、[Default Rule (If no match)] が使用されます。 デフォルトで設定されているように、この規則では ISE のローカルの [Internal Users] ID ソース内のユーザ アカウントを検索します。 この設定は、[Administration] > [Identity Management] > [External Identity Sources] の下で定義される、Active Directory、LDAP などの外部 ID ソースを参照するように変更できます。 単純にして分かりやすくするために、次の例では ISE のローカルでユーザ アカウントを定義するため、認証ポリシーをさらに変更する必要はありません。

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access	and
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints		
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access	and
<input checked="" type="checkbox"/>	Default	: use Guest_Portal_Sequence		
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : Internal Users	

ISE へのローカル ユーザの追加

- [Administration] > [Identity Management] > [Identities] > [Users] の順に移動します。 [Add] をクリックします。 意味の分かりやすいユーザ名とパスワードを入力します。 [User Groups] の選択で、既存のグループ名を選択するか、または緑の [+] 記号をクリックして新しいグループを追加します。 次の例では、ユーザの「sfadmin」がカスタム グループの「Sourcefire Administrator」に割り当てられています。 このユーザグループは、下の「ISE 認可ポリシーの設定」手順で定義される認可プロファイルにリンクされます。 [Save] をクリックします。

▼ Network Access User

* Name

Status Enabled ▼

Email

▼ Password

* Password [Need help with password policy ? ⓘ](#)

* Re-Enter Password

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ User Groups

- +

ISE 認可ポリシーの設定

- [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] の順に選択します。 **緑の [+] 記号をクリックして新しい認可プロファイルを追加します。**
- Sourcefire Administrator のような意味の分かりやすい名前を [Name] に指定します。 [Access Type] で **[ACCESS_ACCEPT]** を選択します。 [Common Tasks] で、最下部までスクロールして [ASA VPN] の横のチェックボックスをオンにします。 **オレンジ色の矢印をクリックし、[InternalUser:IdentityGroup]を選択します。** [Save] をクリックします。

ヒント：この例ではISEローカルユーザIDストアを使用するため、設定を簡素化するために InternalUser:IdentityGroupグループオプションが使用されます。 外部 ID ストアを使用する場合、ASA VPN の認可属性が引き続き使用されますが、Sourcefire デバイスに返す値は手動で設定します。 たとえば、[ASA VPN] ドロップダウン ボックスに Administrator と手動で入力すると、Sourcefire デバイスに送信される Class = Administrator という Class-25 の av ペア値が生成されます。 この値は、次にシステムのポリシー設定の一部として sourcefire のユーザ グループにマッピングできます。 内部ユーザの場合は、いずれの設定方法も許容されます。

内部ユーザの例

* Name

Description

* Access Type ▼

Service Template

▼ Common Tasks

MACSEC Policy

NEAT

Web Authentication (Local Web Auth)

Airespace ACL Name

ASA VPN

▼

▼ Advanced Attributes Settings

▼ = ▼ - +

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Class = InternalUser:IdentityGroup

外部ユーザの例

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

- [Policy] > [Authorization] に移動し、Sourcefire Administration のセッション用の新しい認可ポリシーを設定します。 次の例では、DEVICE:Device Type条件を使用して、上記の「ネットワーク デバイスとネットワーク デバイス グループの設定」セクションで設定したデバイス タイプに一致するようにしています。 このポリシーは、次に上で設定した Sourcefire Administrator 認可プロファイルに関連付けられます。 [Save] をクリックします。

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Sourcefire Administrator	if DEVICE:Device Type EQUALS All Device Types#Sourcefire	then Sourcefire Administrator
<input checked="" type="checkbox"/>	CWA-PSN1	if Network Access:ISE Host Name EQUALS ise12-psn1	then CWA-PSN1
<input checked="" type="checkbox"/>	CWA-PSN2	if Network Access:ISE Host Name EQUALS ise12-psn2	then CWA-PSN2

Sourcefire のシステム ポリシー設定

- FireSIGHT MC にログインして、[System] > [Local] > [User Management] に移動します。 [Login Authentication] タブをクリックします。 [+ Create Authentication Object] ボタンをクリックして、ユーザ認証または認可用の新しい RADIUS サーバを追加します。
- [Authentication Method] で [RADIUS] を選択します。 この RADIUS サーバの説明になる名前を入力します。 [Host Name/IP Address] と [RADIUS Secret Key] に入力します。 秘密キーは、前に ISE で設定したキーと一致している必要があります。 バックアップの ISE サーバが存在する場合は、[Host Name/IP Address] にオプションで入力します。

Authentication Object

Authentication Method

RADIUS

Name *

ISE

Description

Primary Server

Host Name/IP Address *

10.1.1.254

Port *

1812

RADIUS Secret Key

Backup Server (Optional)

Host Name/IP Address

Port

1812

RADIUS Secret Key

- [RADIUS-Specific Parameters] セクションで、GUI アクセスに一致する Sourcefire のローカルグループ名の横にあるテキストボックスに Class-25 の av ペアの文字列を入力します。この例では、Class=User Identity Groups:Sourcefire Administratorの値が Sourcefire Administratorグループにマッピングされています。この値は、ISE が ACCESS-ACCEPT の一部として返す値です。オプションで、Class-25 グループが割り当てられていない認証済みユーザ用の [Default User Role] を選択します。[Save] をクリックして設定を保存するか、または ISE を使用して認証をテストするために下の「検証」セクションに進みます。

RADIUS-Specific Parameters

Timeout (Seconds)	<input type="text" value="30"/>
Retries	<input type="text" value="3"/>
Access Admin	<input type="text"/>
Administrator	<input type="text" value="Class=User Identity
Groups:Sourcefire Administrator"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text"/>
Network Admin	<input type="text"/>
Security Analyst	<input type="text"/>
Security Analyst (Read Only)	<input type="text"/>
Security Approver	<input type="text"/>
Default User Role	<input type="text" value="Access Admin
Administrator
Discovery Admin
External Database User"/>

- [Shell Access Filter] で、シェル セッションまたは SSH セッションを制限するユーザのカンマ区切りリストを入力します。

Shell Access Filter

Administrator Shell Access User List	<input type="text" value="user1, user2, user3"/>
--------------------------------------	--

外部認証の有効化

最後に以下の手順を実行して、FMC で外部認証を有効にします。

1. に移動 システム > Local > システムポリシー。
2. 選択 外部認証 左側のパネル
3. ステータスを次のように変更します 有効（デフォルトでは無効）。
4. 追加された ISE RADIUS サーバを有効にします。
5. ポリシーを保存し、アプライアンスにポリシーを再度適用します。

Access Control Preferences

- Access List
- Audit Log Settings
- Dashboard
- Database
- DNS Cache
- Email Notification
- External Authentication**
- Intrusion Policy Preferences
- Language
- Login Banner
- Network Analysis Policy Preferences
- SNMP
- STIG Compliance
- Time Synchronization
- User Interface
- Vulnerability Mapping

Save Policy and Exit Cancel

Status: Enabled

Default User Role: Access Admin, Administrator, Discovery Admin, External Database User

Shell Authentication: Disabled

CAC Authorization: Disabled

Name	Description	Method	Server:Port	Encryption	
ISE		RADIUS	10.1.1.254:1812	no	<input checked="" type="checkbox"/>

確認

- ISE に対してユーザ認証をテストするには、[Additional Test Parameters] セクションまでスクロールして、ISE ユーザのユーザ名とパスワードを入力します。 [Test] をクリックします。 テストに成功すると、緑色の成功が返されます。 Test Complete というメッセージがブラウザ ウィンドウの先頭に表示されます。

Additional Test Parameters

User Name: sfadmin

Password:

*Required Field

Save Test Cancel

- テスト認証の結果を表示するには、[Test Output] セクションに移動して、[Show Details] の横にある黒の矢印をクリックします。 次のスクリーンショットの例では、「radiusauth - response: |Class=User Identity Groups:Sourcefire Administrator|」の値をISEから受信しました。 この値は、上で FireSIGHT MC 上で設定した Sourcefire ローカル グループに関連付けられた Class の値と一致するはずですが、[Save] をクリックします。

Test Output

Show Details

```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTHITJqLx/radiusclient_0.conf
radiusauth - response: [User-Name=sfadmin]
radiusauth - response: [State=ReauthSession:0ac9e8cb0000006539F4896]
radiusauth - response: [Class=User Identity Groups:Sourcefire Administrator]
radiusauth - response: [Class=CACS:0ac9e8cb0000006539F4896:ise12-psn1/191969386/7]
"sfadmin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=User Identity Groups:Sourcefire Administrator] - [Class=User Identity Groups:Sourcefire Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

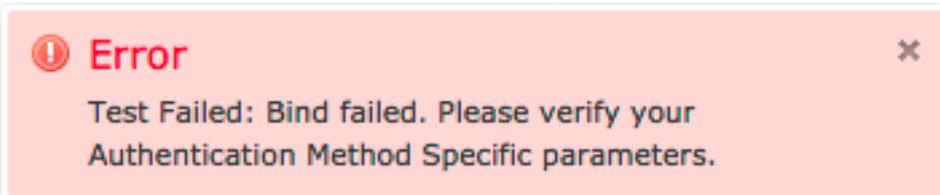
User Test

- ISE の管理 GUI で、[Operations] > [Authentications] に移動して、ユーザ認証テストの成功または失敗を検証します。

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2014-06-16 18:41:55.940	Success		1	sfadmin			Sourcefire3D-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication S...
2014-06-16 18:41:24.947	Failure		1	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:41:10.088	Failure		1	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:40:00.856	Success		1	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication S...
2014-06-16 18:44:55.751	Success		1	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication S...
2014-06-16 18:41:02.876	Success		1	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication S...
2014-06-16 18:39:30.388	Failure		1	sfadmin			SFR-DC			User Identity Groups...		ise12-psn1	Authentication f...

トラブルシューティング

- ISE に対してユーザ認証をテストした場合、次のエラーは RADIUS 秘密キーの不一致、あるいはユーザ名またはパスワードの誤りを示しています。



- ISE の管理 GUI で、[Operations] > [Authentications] に移動します。赤のイベントは失敗を示し、緑のイベントは認証、認可、または認可変更の成功を表しています。アイコンをクリックして、認証イベントの詳細を確認します。

Overview

Event	5400 Authentication failed
Username	sfadmin
Endpoint Id	
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-06-16 20:01:17.438
Received Timestamp	2014-06-16 20:00:58.439
Policy Server	ise12-psn1
Event	5400 Authentication failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	sfadmin
User Type	User
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	Internal Users

関連情報

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