

FireSIGHT系統與ISE的整合，用於RADIUS使用者身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[ISE 組態](#)

[配置網路裝置和網路裝置組](#)

[配置ISE身份驗證策略：](#)

[將本地使用者新增到ISE](#)

[配置ISE授權策略](#)

[Sourcefire系統策略配置](#)

[啟用外部身份驗證](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹將Cisco FireSIGHT管理中心(FMC)或Firepower受管裝置與思科身份服務引擎(ISE)整合以進行遠端身份驗證撥入使用者服務(RADIUS)使用者身份驗證所需的配置步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 通過GUI和/或外殼進行FireSIGHT系統和受管裝置的初始配置
- 在ISE上配置身份驗證和授權策略
- 基本RADIUS知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA v9.2.1
- ASA FirePOWER模組v5.3.1
- ISE 1.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

ISE 組態

提示：有多種方法可以配置ISE身份驗證和授權策略以支援與網路訪問裝置(NAD) (如 Sourcefire) 的整合。 以下範例是設定整合的一種方式。 示例配置是一個參考點，可以對其進行調整以適應特定部署的需要。 請注意，授權配置是一個兩步過程。 將在ISE上定義一個或多個授權策略，ISE將RADIUS屬性值對 (av對) 返回FMC或受管裝置。 然後，這些av對對映到在FMC系統策略配置中定義的本地使用者組。

配置網路裝置和網路裝置組

- 在ISE GUI中，導航到**管理>網路資源>網路裝置**。 按一下**+Add**新增新的網路接入裝置(NAD)。 提供描述性名稱和裝置IP地址。 FMC定義在下列中。

Network Devices

* Name

Description

* IP Address: /

- 在Network Device Group下，按一下**All Device Types**旁邊的**橙色箭頭**。 按一下圖示並  選擇**Create New Network Device Group**。 在後面的示例螢幕截圖中，已配置裝置型別 Sourcefire。 在後續步驟中，將在授權策略規則定義中引用此裝置型別。 按一下「**Save**」。

Create New Network Device Group... ✕

Network Device Groups

* Parent Reset to Top Level

* Name

Description

* Type

Save Cancel

- 再次按一下**橙色箭頭**，然後選擇在上面的步驟中配置的網路裝置組

* Network Device Group

Location

Device Type

- 選中Authentication Settings旁邊的框。輸入將用於此NAD的RADIUS共用金鑰。注意：稍後在FireSIGHT MC上配置RADIUS伺服器時，將再次使用相同的共用金鑰。要檢視純文字檔案鍵值，請按一下Show按鈕。按一下「Save」。

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

- 對需要RADIUS使用者身份驗證/授權以進行GUI和/或外殼訪問的所有FireSIGHT MC和受管裝置重複上述步驟。

配置ISE身份驗證策略：

- 從ISE GUI導航至Policy > Authentication。如果使用策略集，請導航到策略>策略集。以下示例取自使用預設身份驗證和授權策略介面的ISE部署。無論採用何種配置方法，身份驗證和授權規則邏輯都是相同的。
- Default Rule (如果沒有匹配) 將用於驗證來自使用的方法不是MAC Authentication Bypass(MAB)或802.1X的NAD的RADIUS請求。預設情況下，此規則將在ISE的本地內部使用者身份源中查詢使用者帳戶。可以修改此配置以引用在管理>身份管理>外部身份源中定義的外部身份源，如Active Directory、LDAP等。為簡單起見，此示例將在ISE本地定義使用者帳戶，因此無需進一步修改身份驗證策略。

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	

將本地使用者新增到ISE

- 導航到管理>身份管理>身份>使用者。按一下「Add」。輸入有意義的使用者名稱和密碼。在

User Groups選擇下，選擇現有組名稱，或按一下綠色+號以新增新組。在本示例中，使用者「sfadmin」被分配到自定義組「Sourcefire Administrator」。此使用者組將連結到下面的配置ISE授權策略步驟中定義的授權配置檔案。按一下「Save」。

Network Access Users List > sfadmin

▼ 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

▼ - +

配置ISE授權策略

- 導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。按一下綠色+號可新增新的授權配置檔案。
- 提供描述性名稱，如Sourcefire Administrator。為Access Type選擇ACCESS_ACCEPT。在Common Tasks下，滾動到底部並選中ASA VPN旁邊的框。按一下橙色箭頭，然後選擇InternalUser:IdentityGroup。按一下「Save」。

提示：由於此示例使用ISE本地使用者身份儲存，因此使用InternalUser:IdentityGroup組選項來簡化配置。如果使用外部身份儲存，則仍使用ASA VPN授權屬性，但手動配置要返回到Sourcefire裝置的值。例如，在ASA VPN下拉框中手動鍵入Administrator將導致將Class-25 av-pair值Class = Administrator傳送到Sourcefire裝置。然後，作為系統策略配置的一部分，可以將此值對映到sourcefire使用者組。對於內部使用者，兩種配置方法都可以接受。

内部使用者示例

* 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

外部使用者示例

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

- 導航到 **Policy > Authorization**，並為Sourcefire管理會話配置新的授權策略。以下示例使用 **DEVICE:Device Type** 條件與 **配置網路裝置和網路裝置組** 一節。然後此策略與上面配置的Sourcefire管理員授權配置檔案相關聯。按一下「**Save**」。

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系統策略配置

- 登入到FireSIGHT MC，然後導航到 **System > Local > User Management**。按一下 **Login Authentication** 頁籤。按一下 **+ Create Authentication Object** 按鈕，為使用者身份驗證/授權新增新的RADIUS伺服器。
- 選擇 **RADIUS** 作為 **驗證方法**。輸入RADIUS伺服器的描述性名稱。輸入 **主機名/IP地址** 和 **RADIUS金鑰**。金鑰應與之前在ISE上配置的金鑰匹配。（可選）輸入備份ISE服務器 **主機名/IP地址** (如果存在)。

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

- 在RADIUS特定引數部分下，在要為GUI訪問匹配的Sourcefire本地組名稱旁邊的文本框中輸入Class-25 av-pair字串。 在本示例中，Class=User Identity Groups:Sourcefire Administrator值對映到Sourcefire Administrator組。 這是ISE作為ACCESS-ACCEPT的一部分返回的值。 或者，為未分配Class-25組的已驗證使用者選擇**Default User Role**。 按一下**Save**儲存配置，或繼續到下面的Verify部分以使用ISE測試身份驗證。

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"/>

- 在外殼訪問過濾器下，輸入逗號分隔的使用者清單以限制外殼/SSH會話。

Shell Access Filter

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

啟用外部身份驗證

最後，完成以下步驟，以便在FMC上啟用外部驗證：

1. 導航至 **系統 > 本地 > 系統策略**。
2. 選擇 **外部驗證** 在左側面板上。
3. 將 *Status* 更改為 **已啟用**（預設情況下禁用）。
4. 啟用新增的ISE RADIUS伺服器。
5. 儲存策略並在裝置上重新應用策略。

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

驗證

- 要針對ISE測試使用者身份驗證，請向下滾動至**Additional Test Parameters**部分，並輸入ISE使用者的使用者名稱和密碼。按一下「**Test**」。成功測試將導致綠色成功：瀏覽器視窗頂部的Test Complete消息。

Additional Test Parameters

User Name: sfadmin

Password:

*Required Field

Save Test Cancel

- 要檢視測試身份驗證的結果，請轉到**測試輸出**部分，然後按一下**顯示詳細資訊**旁邊的**黑色箭頭**。在下面的示例螢幕截圖中，請注意「radiusauth - response: 從ISE接收的|Class=User Identity Groups:Sourcefire Administrator|」值。此值應與上面在FireSIGHT MC上配置的本地Sourcefire組關聯的Class值匹配。按一下「**Save**」。

Test Output

Show Details ▼

```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTH1T3qLx/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:
```

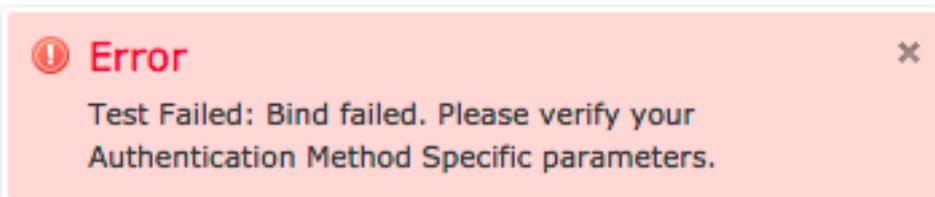
User Test

- 在ISE管理員GUI中，導航到操作>身份驗證以驗證使用者身份驗證測試是否成功。

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	✓		0	sfadmin			Sourcefire3D-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:41:24.947	✗		0	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:41:10.088	✗		0	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:46:00.856	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:44:55.751	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:41:02.876	✓		0	sfadmin			SFR-DC		Sourcefire_Admin		NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:39:30.388	✗		0	sfadmin			SFR-DC					ise12-psn1	Authentication f...

疑難排解

- 根據ISE測試使用者身份驗證時，以下錯誤表示RADIUS金鑰不匹配或使用者名稱/密碼不正確。



- 從ISE管理員GUI導航到操作>身份驗證。紅色事件表示失敗，而綠色事件表示成功的身份驗證/授權/授權更改。按一下圖示  檢視身份驗證事件的詳細資訊。

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

相關資訊

[技術支援與文件 - Cisco Systems](#)