

FireSIGHT系统的集成与ISE的RADIUS用户认证的

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[ISE配置](#)

[配置网络设备和网络设备组](#)

[配置ISE认证策略：](#)

[添加一个本地用户到ISE](#)

[配置ISE授权策略](#)

[Sourcefire系统策略配置](#)

[Enable \(event\)外部认证](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

本文描述要求的配置步骤用思科身份服务引擎(ISE)集成Cisco FireSIGHT管理中心(FMC)或Firepower可管理的设备远程认证拨入用户服务(RADIUS)用户认证的。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- FireSIGHT系统和可管理的设备初始配置通过GUI和shell
- 配置由于ISE的认证和授权策略
- 基本RADIUS知识

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA v9.2.1
- ASA Firepower模块v5.3.1
- ISE 1.2

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.

Configure

ISE配置

提示：有多种方式配置ISE认证和授权策略支持集成用网络接入设备(NAD)例如Sourcefire。下面的示例是一种方式配置integration。配置示例是参考点，并且可以适应配合特定配置的需要。注意授权配置是一个两步进程。一个或更多授权策略在与返回RADIUS属性值对(AV对)的ISE的ISE将被定义到FMC或可管理的设备。这些AV对然后被映射给在FMC系统策略配置定义的一个本地用户组。

配置网络设备和网络设备组

- 从ISE GUI，请连接到**Administration >网络资源>网络设备**。点击**+Add**添加一新的网络接入设备(NAD)。提供一个描述性名称和设备IP地址。FMC在下面示例被定义。

Network Devices

* Name

Description

* IP Address: /

- 在网络设备组下，请在所有设备类型旁边点击**橙色箭头**。点击  图标并且选择**创建新的网络设备组**。在跟随的示例屏幕画面，配置了设备类型Sourcefire。此设备类型将被参考在一个最新步骤的授权策略规则定义。 Click **Save**.

- 再单击**橙色箭头**并且选择在上面步骤配置的网络设备组

* Network Device Group

- 在**认证设置**旁边检查机箱。输入将使用此NAD的RADIUS被共享的密钥。当配置在FireSIGHT MC时的RADIUS服务器请注释同一被共享的密钥以后再使用。要查看纯文本关键值，请点击**显示**按钮。Click **Save**.

- 重复所有FireSIGHT为GUI和shell访问将要求RADIUS用户认证/授权的MCs和可管理的设备的上述步骤。

配置ISE认证策略：

- 从ISE GUI，请连接对**策略>认证**。如果曾经策略集，请连接对**策略>Policy集**。下面的示例从使用默认认证和授权策略接口的ISE配置采取。不管配置方法，认证和授权规则逻辑是相同的。
- **默认规则(如果没有匹配)**将用于验证从方法在使用中不是MAC验证旁路的NADs的RADIUS请求(MAB)或802.1X。如被配置默认情况下，此规则在艾斯的本地**内部用户**身份来源将寻找用户帐户。可以修改此配置是指一个外部身份来源例如激活目录、LDAP等等如被定义在 **Administration > 身份管理下>外部身份来源**。为了simpliciity缘故，此示例在ISE将定义用户帐户本地，因此没有需要对认证策略的进一步修改。

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	

添加本地用户到ISE

- 连接对 **Administration > 身份管理 > 身份 > Users**。单击 **Add**。输入一个有意义的用户名和密码。在 **用户组基群段** 下，请选择一个现有组名字或点击 **绿色+符号** 添加一个新的组。在本例中，用户“sfadmin”被分配到自定义组“Sourcefire管理员”。此用户组与在 **配置ISE授权** 下面 **策略步骤** 定义的授权配置文件将连接。Click **Save**。

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

Sourcefire Administrator ⌵ - +

配置ISE授权策略

- 连接对**策略>Policy元素>结果>授权>授权配置文件**。 点击**绿色+符号**添加一个新的授权配置文件。
- 提供一描述性名称例如Sourcefire管理员。 为**访问类型**选择**ACCESS_ACCEPT**。 在**普通的任务下**，请移动到底部并且在**ASA VPN旁边**检查机箱。 点击**橙色箭头**并且选择**InternalUser : IdentityGroup**。 Click **Save**.

提示：由于此示例使用ISE本地用户身份存储， InternalUser : IdentityGroup组选项用于简单化配置。 如果曾经外部身份存储，仍然使用ASA VPN授权属性，然而，到Sourcefire设备手工配置将返回的值。 例如， ASA的VPN手工键入的管理员丢弃下来机箱将导致被发送到Sourcefire设备的组=管理员的Class-25 AV对值。 作为系统策略配置一部分，此值可能然后被映射对sourcefire用户组。 对于内部用户，任一个配置方法是可接受的。

* 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

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

- 连接对策略>授权并且配置Sourcefire管理会话的一个新的授权策略。下面的示例使用设备：设备类型匹配设备类型的情况配置在配置网络设备和上面网络设备组部分。此策略与在上面配置的Sourcefire管理员授权配置文件然后产生关联。 Click **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系统策略配置

- 登陆对FireSIGHT MC并且连接对系统>本地>用户管理。 点击洛金Authentication选项。 点击 **+创建认证对象** 按钮添加用户认证/授权的一个新的RADIUS服务器。
- 为认证方法选择RADIUS。 进入RADIUS服务器的一描述性名称。 输入主机名/IP地址和RADIUS密钥。 密钥应该匹配在ISE早先配置的键。 随意地， 如果一个存在， 请输入一个备份的ISE服务器主机主机名/IP地址。

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特定的参数部分下，请输入Class-25 AV对字符串在文本框在为GUI访问将匹配的Sourcefire本地组名字旁边。在本例中，Class=User身份组队：Sourcefire管理员值被映射给Sourcefire管理员组。这是作为ACCESS-ACCEPT一部分，ISE返回的值。随意地，为不安排Class-25组分配的认证的用户请选择**默认用户角色**。点击“Save”保存配置或继续到下面Verify部分测试与ISE的认证。

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Shell访问过滤器下，请进入用户逗号被分离的列表限制shell/SSH会话。

Shell Access Filter

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

Enable (event)外部认证

最后，请完成这些在FMC的步骤为了enable (event)外部认证：

1. 连接对系统>本地>System策略。
2. 选择在左面板的外部认证。
3. 更改状态到启用默认情况下(禁用)。
4. Enable (event)被添加的ISE RADIUS服务器。
5. 保存策略并且重新应用在工具上的策略。

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"/>

Verify

- 对ISE的测试用户认证，请移下来到另外的测试参数部分并且输入ISE用户的一个用户名和密码。点击测试。成功的测试将导致绿色的成功：测试全部的消息在浏览器窗口顶部。

Additional Test Parameters

User Name sfadmin

Password

*Required Field

Save Test Cancel

- 要查看测试认证的结果，去测试输出部分和点击黑色箭头在旁边显示详细资料。在下面示例的屏幕画面，请注释“radiusauth -回应：|Class=User身份组：Sourcefire管理员|”从ISE收到的值。这应该匹配与本地Sourcefire组产生关联的等级值配置在上面FireSIGHT MC。 Click 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:
```

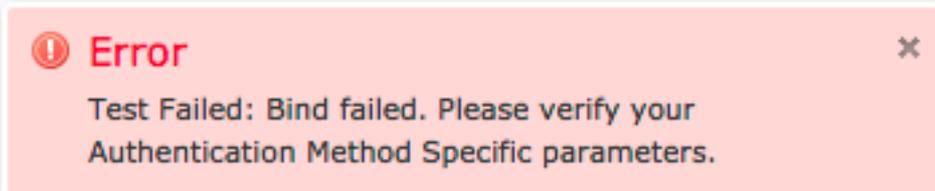
User Test

- 从ISE Admin GUI，请连接对验证用户认证测试的成功或故障的操作>认证。

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...

Troubleshoot

- 当ISE的测试用户认证，以下错误是预示的RADIUS密钥不匹配或一个不正确用户名/密码。



- 从ISE admin GUI，请连接对操作>认证。 当一个**绿色**的事件是预示的授权时的成功的认证/授权/更改一个**红色**事件是预示的故障。 点击  图标查看认证事件的详细资料。

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

Related Information

[Technical Support & Documentation - Cisco Systems](#)