

Integración de FireSIGHT System con ISE para la autenticación de usuario RADIUS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración de ISE](#)

[Configuración de dispositivos de red y grupos de dispositivos de red](#)

[Configuración de la Política de Autenticación de ISE:](#)

[Adición de un usuario local a ISE](#)

[Configuración de la Política de Autorización de ISE](#)

[Configuración de la política del sistema de Sourcefire](#)

[Habilitar autenticación externa](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos de configuración necesarios para integrar un Cisco FireSIGHT Management Center (FMC) o un dispositivo gestionado Firepower con Cisco Identity Services Engine (ISE) para la autenticación de usuario del servicio de acceso telefónico de autenticación remota (RADIUS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración inicial del sistema FireSIGHT y el dispositivo administrado a través de la GUI o shell
- Configuración de políticas de autenticación y autorización en ISE
- Conocimiento RADIUS básico

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA v9.2.1
- Módulo ASA FirePOWER 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.

Configurar

Configuración de ISE

Consejo: Hay varias formas de configurar las políticas de autenticación y autorización de ISE para admitir la integración con dispositivos de acceso a la red (NAD), como Sourcefire. El siguiente ejemplo es una manera de configurar la integración. La configuración de ejemplo es un punto de referencia y puede adaptarse a las necesidades de la implementación específica. Tenga en cuenta que la configuración de autorización es un proceso de dos pasos. Se definirán una o más políticas de autorización en ISE con ISE que devuelvan pares de valores de atributos RADIUS (pares av) al FMC o dispositivo administrado. Estos pares AV se asignan a un grupo de usuarios local definido en la configuración de la política del sistema FMC.


Configuración de dispositivos de red y grupos de dispositivos de red

- Desde la GUI de ISE, navegue hasta **Administration > Network Resources > Network Devices**. Haga clic en **+Agregar** para agregar un nuevo dispositivo de acceso a la red (NAD). Proporcione un nombre descriptivo y una dirección IP del dispositivo. El FMC se define en el siguiente ejemplo.

Network Devices

* Name
Description

* IP Address: /

- En **Grupo de dispositivos de red**, haga clic en la **flecha naranja** junto a **Todos los tipos de dispositivos**. Haga clic en el  icono y seleccione **Crear nuevo grupo de dispositivos de red**. En la captura de pantalla de ejemplo que se muestra a continuación, se ha configurado Device Type Sourcefire. Este tipo de dispositivo se hará referencia en la definición de regla de directiva de autorización en un paso posterior. Click **Save**.

Create New Network Device Group... ✕

Network Device Groups

* Parent Reset to Top Level

* Name

Description

* Type

- Haga clic en la **flecha naranja** de nuevo y seleccione el grupo de dispositivos de red configurado en el paso anterior

* Network Device Group

Location Set To Default

Device Type Set To Default

- Marque la casilla junto a **Authentication Settings**. Introduzca la clave secreta compartida RADIUS que se utilizará para este NAD. Tenga en cuenta que la misma clave secreta compartida se volverá a utilizar más tarde cuando se configure el servidor RADIUS en FireSIGHT MC. Para revisar el valor de la clave de texto sin formato, haga clic en el botón **Mostrar**. Click **Save**.

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

- Repita los pasos anteriores para todos los MCs FireSIGHT y dispositivos administrados que requieran autenticación/autorización de usuario RADIUS para la GUI o el acceso al shell.

Configuración de la Política de Autenticación de ISE:

- Desde la GUI de ISE, navegue hasta **Policy > Authentication**. Si utiliza conjuntos de políticas, navegue hasta **Política > Conjuntos de políticas**. El siguiente ejemplo se toma de una implementación de ISE que utiliza las interfaces de política de autenticación y autorización predeterminadas. La lógica de regla de autenticación y autorización es la misma independientemente del enfoque de configuración.

- La **regla predeterminada (si no hay coincidencia)** se utilizará para autenticar las solicitudes RADIUS de los NAD donde el método en uso no es la omisión de autenticación MAC (MAB) o 802.1X. Tal como se configura de forma predeterminada, esta regla buscará las cuentas de usuario en el origen de identidad de **usuarios internos** locales de ISE. Esta configuración se puede modificar para hacer referencia a un origen de identidad externo como Active Directory, LDAP, etc, como se define en **Administration > Identity Management > External Identity Sources**. En aras de la simplicidad, este ejemplo definirá las cuentas de usuario localmente en ISE, por lo que no se requieren más modificaciones en la política de autenticación.

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

Adición de un usuario local a ISE

- Vaya a **Administration > Identity Management > Identities > Users**. Haga clic en Add (Agregar). Introduzca un nombre de usuario y una contraseña válidos. En la selección **Grupos de usuarios**, seleccione un nombre de grupo existente o haga clic en el **signo +** para agregar un nuevo grupo. En este ejemplo, el usuario "sfadmin" se asigna al grupo personalizado "Sourcefire Administrator". Este grupo de usuarios se vinculará al perfil de autorización definido en el paso **Configuración de la Política de Autorización de ISE** a continuación. 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

▼ - +

Configuración de la Política de Autorización de ISE

- Vaya a **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Haga clic en el **signo verde +** para agregar un nuevo perfil de autorización.
- Proporcione un nombre descriptivo como Sourcefire Administrator. Seleccione **ACCESS_ACCEPT** para el **tipo de acceso**. En **Tareas comunes**, desplácese hacia abajo y marque la casilla junto a **ASA VPN**. Haga clic en la **flecha naranja** y seleccione **InternalUser:IdentityGroup**. Click **Save**.

Consejo: Dado que en este ejemplo se utiliza el almacén de identidad de usuario local de ISE, se utiliza la opción de grupo InternalUser:IdentityGroup para simplificar la configuración. Si se utiliza un almacén de identidad externo, se sigue utilizando el atributo de autorización de VPN ASA; sin embargo, el valor que se devolverá al dispositivo Sourcefire se configura manualmente. Por ejemplo, al escribir manualmente Administrator en el cuadro desplegable ASA VPN, se enviará un valor Clase 25 av-pair de Clase = Administrator al dispositivo Sourcefire. Este valor se puede asignar a un grupo de usuarios de sourcefire como parte de la configuración de la política del sistema. Para los usuarios internos, cualquiera de los métodos de configuración es aceptable.

Ejemplo de usuario interno

* 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

Ejemplo de usuario externo

Advanced Attributes Settings

Select an item = [] - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

- Navegue hasta **Política > Autorización** y configure una nueva política de autorización para las sesiones de administración de Sourcefire. El ejemplo siguiente utiliza la condición **DEVICE:Device Type** para coincidir con el tipo de dispositivo configurado en el Sección anterior **Configuración de Dispositivos de Red y Grupos de Dispositivos de Red**. A continuación, esta política se asocia al perfil de autorización del administrador de Sourcefire configurado anteriormente. Click **Save**.

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

Configuración de la política del sistema de Sourcefire

- Inicie sesión en FireSIGHT MC y navegue hasta **System > Local > User Management**. Haga clic en la pestaña **Login Authentication**. Haga clic en el botón **+ Crear objeto de autenticación** para agregar un nuevo servidor RADIUS para la autenticación/autorización de usuario.
- Seleccione **RADIUS** para el **Método de Autenticación**. Introduzca un nombre descriptivo para el servidor RADIUS. Ingrese el **Nombre de Host/Dirección IP** y la **Clave Secreta RADIUS**. La clave secreta debe coincidir con la clave previamente configurada en ISE. Opcionalmente, introduzca un servidor ISE de respaldo **Nombre de host/dirección IP** si existe alguno.

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

- Bajo la sección **Parámetros Específicos de RADIUS**, ingrese la cadena Clase-25 av-pair en el cuadro de texto junto al nombre del grupo local de Sourcefire que debe coincidir para el acceso a la GUI. En este ejemplo, el valor Class=User Identity Groups:Sourcefire Administrator se asigna al grupo Sourcefire Administrator. Este es el valor que devuelve ISE como parte de ACCESS-ACCEPT. Opcionalmente, seleccione un **rol de usuario predeterminado** para usuarios autenticados que no tienen asignados grupos de clase 25. Haga clic en **Guardar** para guardar la configuración o continúe con la sección Verificar a continuación para probar la autenticación con ISE.

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"/>

- En **Shell Access Filter**, ingrese una lista de usuarios separados por comas para restringir las sesiones shell/SSH.

Shell Access Filter

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

Habilitar autenticación externa

Finalmente, complete estos pasos para habilitar la autenticación externa en el FMC:

1. Vaya a **Sistema > Local > Política del sistema**.
2. Seleccione **Autenticación externa** en el panel izquierdo.
3. Cambiar el *estado* a **Habilitado** (desactivado de forma predeterminada).
4. Habilite el servidor RADIUS ISE agregado.
5. Guarde la política y vuelva a aplicarla en el dispositivo.

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

Verificación

- Para probar la autenticación de usuario con ISE, desplácese hacia abajo hasta la sección **Parámetros de prueba adicionales** e introduzca un nombre de usuario y una contraseña para el usuario de ISE. Haga clic en **Prueba**. Una prueba correcta dará como resultado un mensaje **verde** Correcto: Prueba finalizada en la parte superior de la ventana del navegador.

Additional Test Parameters

User Name: sfadmin

Password:

*Required Field

Save Test Cancel

- Para ver los resultados de la autenticación de prueba, vaya a la sección **Resultados de prueba** y haga clic en la flecha **negra** junto a **Mostrar detalles**. En la captura de pantalla de ejemplo a continuación, observe el mensaje "radiusauth - response: |Class=Grupos de identidad de usuario:Administrador de Sourcefire|" valor recibido de ISE. Esto debe coincidir con el valor Class asociado al grupo Sourcefire local configurado en el MC FireSIGHT anterior. Click **Save**.

Test Output

Show Details

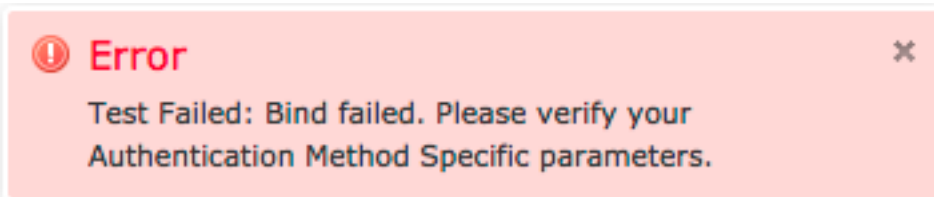
```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTH1T3qLx/radiusclient_0.conf
radiusauth - response: [User-Name=sfadmin]
radiusauth - response: [State=ReauthSession:0ac9e8cb0000006539F4896]
radiusauth - response: [Class=User Identity Groups:Sourcefire Administrator]
radiusauth - 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:
```


- Desde la GUI de administración de ISE, navegue hasta **Operaciones > Autenticaciones** para verificar el éxito o el fracaso de la prueba de autenticación de usuario.

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	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:39:30.388	✗		0	sfadmin			SFR-DC					ise12-psn1	Authentication f...

Troubleshoot

- Al probar la autenticación de usuario con ISE, el siguiente error indica una discordancia de clave secreta RADIUS o un nombre de usuario/contraseña incorrecto.



- Desde la GUI de administración de ISE, navegue hasta **Operaciones > Autenticaciones**. Un evento **rojo** indica una falla mientras que un **evento verde** indica una autenticación/autorización/cambio de autorización exitosa. Haga clic en el  icono para revisar los detalles del evento de autenticación.

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

Información Relacionada

[Soporte Técnico y Documentación - Cisco Systems](#)