

Intégration de FireSIGHT System à ISE pour l'authentification des utilisateurs RADIUS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configuration ISE](#)

[Configuration des périphériques réseau et des groupes de périphériques réseau](#)

[Configuration de la stratégie d'authentification ISE :](#)

[Ajout d'un utilisateur local à ISE](#)

[Configuration de la stratégie d'autorisation ISE](#)

[Configuration de la stratégie système Sourcefire](#)

[Activer l'authentification externe](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes de configuration requises pour intégrer un périphérique géré Cisco FireSIGHT Management Center (FMC) ou Firepower avec Cisco Identity Services Engine (ISE) pour l'authentification utilisateur RADIUS (Remote Authentication Dial In User Service).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration initiale de FireSIGHT System et de Managed Device via une interface utilisateur graphique et/ou un interpréteur de commandes
- Configuration des stratégies d'authentification et d'autorisation sur ISE
- Connaissances RADIUS de base

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASA v9.2.1

- Module 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.

Configuration

Configuration ISE

Astuce : Il existe plusieurs façons de configurer les politiques d'authentification et d'autorisation ISE pour prendre en charge l'intégration avec les périphériques d'accès réseau (NAD) tels que Sourcefire. L'exemple ci-dessous est une façon de configurer l'intégration. L'exemple de configuration est un point de référence et peut être adapté aux besoins du déploiement spécifique. Notez que la configuration de l'autorisation est un processus en deux étapes. Une ou plusieurs stratégies d'autorisation seront définies sur ISE avec ISE renvoyant les paires de valeurs d'attribut RADIUS (av-paires) au FMC ou au périphérique géré. Ces paires av sont ensuite mappées à un groupe d'utilisateurs local défini dans la configuration de la stratégie système FMC.

Configuration des périphériques réseau et des groupes de périphériques réseau

- À partir de l'interface graphique de l'ISE, accédez à **Administration > Network Resources > Network Devices**. Cliquez sur **+Ajouter** pour ajouter un nouveau périphérique d'accès au réseau (NAD). Indiquez un nom descriptif et une adresse IP de périphérique. Le FMC est défini dans l'exemple ci-dessous.

Network Devices

* Name
Description

* IP Address: /

- Sous **Network Device Group**, cliquez sur la **flèche orange** en regard de **All Device Types**.

Cliquez sur l'  icône et sélectionnez **Créer un nouveau groupe de périphériques réseau**. Dans l'exemple de capture d'écran qui suit, le type de périphérique Sourcefire a été configuré. Ce type de périphérique sera référencé dans la définition de règle de stratégie d'autorisation dans une étape ultérieure. Cliquez **Save**.

Create New Network Device Group... ✕

Network Device Groups

* Parent

* Name

Description

* Type

- Cliquez à nouveau sur la **flèche orange** et sélectionnez le groupe de périphériques réseau configuré à l'étape ci-dessus

* **Network Device Group**

Location

Device Type

- Cochez la case en regard de **Paramètres d'authentification**. Entrez la clé secrète partagée RADIUS qui sera utilisée pour cette NAD. Notez que la même clé secrète partagée sera utilisée ultérieurement lors de la configuration du serveur RADIUS sur FireSIGHT MC. Pour consulter la valeur de la clé en texte brut, cliquez sur le bouton **Afficher**. Click **Save**.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

- Répétez les étapes ci-dessus pour tous les MC et périphériques gérés FireSIGHT qui nécessiteront l'authentification/autorisation utilisateur RADIUS pour l'accès à l'interface utilisateur graphique et/ou au shell.

Configuration de la stratégie d'authentification ISE :

- À partir de l'interface graphique de l'ISE, accédez à **Policy > Authentication**. Si vous utilisez Jeux de stratégies, accédez à **Stratégie > Jeux de stratégies**. L'exemple ci-dessous provient d'un déploiement ISE qui utilise les interfaces de stratégie d'authentification et d'autorisation par défaut. La logique des règles d'authentification et d'autorisation est la même quelle que soit l'approche de configuration.

- La **règle par défaut (si aucune correspondance)** sera utilisée pour authentifier les requêtes RADIUS des NAD où la méthode utilisée n'est pas MAB (MAC Authentication Bypass) ou 802.1X. Comme configuré par défaut, cette règle recherche les comptes d'utilisateurs dans la source d'identité **Utilisateurs internes** locaux d'ISE. Cette configuration peut être modifiée pour faire référence à une source d'identité externe telle qu'Active Directory, LDAP, etc, telle que définie sous **Administration > Identity Management > External Identity Sources**. Par souci de simplicité, cet exemple définit les comptes d'utilisateurs localement sur ISE, de sorte qu'aucune modification supplémentaire de la stratégie d'authentification n'est requise.

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	

Ajout d'un utilisateur local à ISE

- Accédez à **Administration > Identity Management > Identities > Users**. Cliquez sur **Add**. Entrez un nom d'utilisateur et un mot de passe significatifs. Sous la sélection **Groupes d'utilisateurs**, sélectionnez un nom de groupe existant ou cliquez sur le **signe vert +** pour ajouter un nouveau groupe. Dans cet exemple, l'utilisateur « sfadmin » est affecté au groupe personnalisé « Administrateur Sourcefire ». Ce groupe d'utilisateurs sera lié au profil d'autorisation défini à l'étape **Configuration de la stratégie d'autorisation ISE** ci-dessous. Cliquez sur **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

▼ - +

Configuration de la stratégie d'autorisation ISE

- Accédez à **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation**. Cliquez sur le **signe vert +** pour ajouter un nouveau profil d'autorisation.
- Indiquez un nom descriptif tel que Sourcefire Administrator. Sélectionnez **ACCESS_ACCEPT** pour le **type d'accès**. Sous **Tâches courantes**, faites défiler jusqu'en bas et cochez la case en regard de **VPN ASA**. Cliquez sur la **flèche orange** et sélectionnez **InternalUser : IdentityGroup**. Cliquez **Save**.

Astuce : Comme cet exemple utilise le magasin d'identités d'utilisateur local ISE, l'option de groupe InternalUser:IdentityGroup est utilisée pour simplifier la configuration. Si vous utilisez un magasin d'identité externe, l'attribut d'autorisation VPN ASA est toujours utilisé, mais la valeur à renvoyer au périphérique Sourcefire est configurée manuellement. Par exemple, si vous tapez manuellement Administrator dans la liste déroulante VPN ASA, une valeur de paire av Class-25 de Class = Administrator sera envoyée au périphérique Sourcefire. Cette valeur peut ensuite être mappée à un groupe d'utilisateurs sourcefire dans le cadre de la configuration de la stratégie système. Pour les utilisateurs internes, l'une ou l'autre méthode de configuration est acceptable.

Exemple d'utilisateur interne

* 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

Exemple d'utilisateur externe

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

- Accédez à **Policy > Authorization** et configurez une nouvelle stratégie d'autorisation pour les sessions d'administration Sourcefire. L'exemple ci-dessous utilise la condition **DEVICE:Device Type** pour correspondre au type de périphérique configuré dans le **Configuration des périphériques réseau et des groupes de périphériques réseau** ci-dessus. Cette stratégie est ensuite associée au profil d'autorisation Administrateur Sourcefire configuré ci-dessus. Cliquez **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

Configuration de la stratégie système Sourcefire

- Connectez-vous à FireSIGHT MC et accédez à **System > Local > User Management**. Cliquez sur l'onglet **Authentification de connexion**. Cliquez sur le bouton **+ Créer un objet d'authentification** pour ajouter un nouveau serveur RADIUS pour l'authentification/autorisation utilisateur.
- Sélectionnez **RADIUS** pour la **méthode d'authentification**. Entrez un nom descriptif pour le serveur RADIUS. Entrez le **nom d'hôte/l'adresse IP** et la **clé secrète RADIUS**. La clé secrète doit correspondre à la clé précédemment configurée sur ISE. Le cas échéant, entrez un **nom**

d'hôte/adresse IP du serveur ISE de sauvegarde.

Authentication Object

Authentication Method	<input type="text" value="RADIUS"/>
Name *	<input type="text" value="ISE"/>
Description	<input type="text"/>

Primary Server

Host Name/IP Address *	<input type="text" value="10.1.1.254"/>
Port *	<input type="text" value="1812"/>
RADIUS Secret Key	<input type="password" value="....."/>

Backup Server (Optional)

Host Name/IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
RADIUS Secret Key	<input type="password"/>

- Dans la section **Paramètres spécifiques à RADIUS**, saisissez la chaîne de paire av Class-25 dans la zone de texte en regard du nom du groupe local Sourcefire à associer pour l'accès à l'interface utilisateur graphique. Dans cet exemple, la valeur Class=User Identity Groups:Sourcefire Administrator est mappée au groupe Sourcefire Administrator. Il s'agit de la valeur renvoyée par ISE dans le cadre de ACCESS-ACCEPT. Le cas échéant, sélectionnez un **rôle d'utilisateur par défaut** pour les utilisateurs authentifiés qui n'ont pas de groupes de classe 25 affectés. Cliquez sur **Enregistrer** pour enregistrer la configuration ou passez à la section Vérifier ci-dessous pour tester l'authentification avec 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"/>

- Sous **Shell Access Filter**, entrez une liste d'utilisateurs séparés par des virgules pour restreindre les sessions shell/SSH.

Shell Access Filter

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

Activer l'authentification externe

Enfin, complétez ces étapes afin d'activer l'authentification externe sur FMC :

1. Accéder à **système > Municipal > Stratégie système**.
2. Sélectionner **Authentification externe** dans le panneau de gauche.
3. Modifier le *statut* en **Activée** (désactivé par défaut).
4. Activez le serveur ISE RADIUS ajouté.
5. Enregistrez la stratégie et réappliquez-la sur l'appliance.

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"/>

Vérification

- Pour tester l'authentification des utilisateurs par rapport à ISE, faites défiler la page jusqu'à la section **Paramètres de test supplémentaires** et saisissez un nom d'utilisateur et un mot de passe pour l'utilisateur ISE. Cliquez sur **Test**. Un test réussi donnera lieu à un message **vert** Succès : Test terminé en haut de la fenêtre du navigateur.

Additional Test Parameters

User Name sfadmin

Password

*Required Field

Save Test Cancel

- Pour afficher les résultats de l'authentification de test, accédez à la section **Résultats du test** et cliquez sur la flèche **noire** en regard de **Afficher les détails**. Dans l'exemple de capture d'écran ci-dessous, notez le « radiusauth - response : Valeur |Class=User Identity Groups:Sourcefire Administrator|" reçue d'ISE. Cette valeur doit correspondre à la valeur Class associée au groupe Sourcefire local configuré sur FireSIGHT MC ci-dessus. Cliquez **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:
```

- À partir de l'interface utilisateur graphique d'ISE Admin, accédez à **Operations > Authentications** pour vérifier la réussite ou l'échec du test d'authentification de l'utilisateur.

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 f...
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...

Dépannage

- Lors du test de l'authentification utilisateur contre ISE, l'erreur suivante indique une non-correspondance de clé secrète RADIUS ou un nom d'utilisateur/mot de passe incorrect.

 **Error** ✕

Test Failed: Bind failed. Please verify your Authentication Method Specific parameters.

- À partir de l'interface utilisateur graphique de l'administrateur ISE, accédez à **Operations > Authentications**. Un événement **rouge** indique un échec tandis qu'un événement **vert** indique un succès de l'authentification/autorisation/changement d'autorisation. Cliquez sur l'  icône pour consulter les détails de l'événement d'authentification.

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

Informations connexes

[Support et documentation techniques - Cisco Systems](#)