

Integrazione del sistema FireSIGHT con ISE per l'autenticazione utente RADIUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione di ISE](#)

[Configurazione di dispositivi e gruppi di dispositivi di rete](#)

[Configurazione della policy di autenticazione ISE:](#)

[Aggiunta di un utente locale a ISE](#)

[Configurazione della policy di autorizzazione ISE](#)

[Configurazione criteri di sistema Sourcefire](#)

[Abilita autenticazione esterna](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la procedura di configurazione necessaria per integrare un Cisco FireSIGHT Management Center (FMC) o un dispositivo gestito Firepower con Cisco Identity Services Engine (ISE) per l'autenticazione utente RADIUS (Remote Authentication Dial In User Service).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione iniziale del sistema FireSIGHT e del dispositivo gestito tramite GUI e/o shell
- Configurazione dei criteri di autenticazione e autorizzazione su ISE
- Conoscenze base di RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA v9.2.1

- ASA FirePOWER module v5.3.1
- ISE 1.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazione di ISE

Suggerimento: Esistono diversi modi per configurare l'autenticazione e i criteri di autorizzazione ISE in modo da supportare l'integrazione con i dispositivi di accesso alla rete (NAD), ad esempio Sourcefire. Nell'esempio seguente viene illustrato un modo per configurare l'integrazione. La configurazione di esempio è un punto di riferimento e può essere adattata alle esigenze di un'installazione specifica. La configurazione dell'autorizzazione prevede un processo in due fasi. Verranno definiti uno o più criteri di autorizzazione su ISE con ISE che restituirà coppie di valori di attributo RADIUS (coppie av) al FMC o al dispositivo gestito. Tali coppie av vengono quindi mappate a un gruppo di utenti locali definito nella configurazione dei criteri di sistema di FMC.

Configurazione di dispositivi e gruppi di dispositivi di rete

- Dalla GUI di ISE, selezionare **Administration > Network Resources > Network Devices** (Amministrazione > Risorse di rete > Dispositivi di rete). Fare clic su **+Aggiungi** per aggiungere un nuovo dispositivo di accesso alla rete (NAD). Specificare un nome descrittivo e un indirizzo IP del dispositivo. Il CCP è definito nell'esempio seguente.

Network Devices

* Name
Description

* IP Address: /

- In **Gruppo di dispositivi di rete**, fare clic sulla **freccia arancione** accanto a **Tutti i tipi di dispositivo**. Fare clic sull'  icona e selezionare **Create New Network Device Group (Crea nuovo gruppo di dispositivi di rete)**. Nello screenshot di esempio seguente è stato configurato il tipo di dispositivo Sourcefire. Nella definizione della regola dei criteri di autorizzazione verrà fatto riferimento a questo tipo di dispositivo in un passaggio successivo. Fare clic su **Salva**.

Create New Network Device Group...



Network Device Groups

* Parent

* Name

Description

* Type

- Fare di nuovo clic sulla **freccia arancione** e selezionare il gruppo di dispositivi di rete configurato nel passaggio precedente

* Network Device Group

Location

Device Type

- Selezionare la casella accanto a **Impostazioni di autenticazione**. Immettere la chiave privata condivisa RADIUS che verrà utilizzata per questo NAD. Nota La stessa chiave segreta condivisa verrà utilizzata in seguito durante la configurazione del server RADIUS su FireSIGHT MC. Per verificare il valore della chiave in testo normale, fare clic sul pulsante **Mostra**. Fare clic su **Salva**.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

- Ripetere i passaggi precedenti per tutti gli MC FireSIGHT e i dispositivi gestiti che richiedono l'autenticazione/autorizzazione utente RADIUS per l'accesso alla GUI e/o alla shell.

Configurazione della policy di autenticazione ISE:

- Dalla GUI di ISE, selezionare **Policy > Authentication** (Policy > Autenticazione). Se si utilizzano i set di criteri, passare a **Criteri > Set di criteri**. L'esempio seguente viene estratto da un'implementazione ISE che utilizza le interfacce predefinite dei criteri di autenticazione e autorizzazione. La logica delle regole di autenticazione e autorizzazione è la stessa indipendentemente dall'approccio alla configurazione.

- La **regola predefinita (in caso di mancata corrispondenza)** verrà utilizzata per autenticare le richieste RADIUS provenienti da NAD il cui metodo in uso non è MAC Authentication Bypass (MAB) o 802.1X. Come configurato per impostazione predefinita, questa regola cercherà gli account utente nell'origine identità **Internal Users** di ISE locale. È possibile modificare questa configurazione in modo che faccia riferimento a un'origine identità esterna, ad esempio Active Directory, LDAP e così via, come definito in **Amministrazione > Gestione delle identità > Origini identità esterne**. Per semplicità, in questo esempio gli account utente verranno definiti localmente sull'ISE, quindi non saranno necessarie ulteriori modifiche ai criteri di autenticazione.

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	

Aggiunta di un utente locale a ISE

- Passare a **Amministrazione > Gestione delle identità > Identità > Utenti**. Fare clic su **Add**. Immettere un nome utente e una password significativi. Nella selezione **Gruppi utenti**, selezionare un nome di gruppo esistente o fare clic sul **segno + verde** per aggiungere un nuovo gruppo. In questo esempio, l'utente "sfadmin" viene assegnato al gruppo personalizzato "Sourcefire Administrator". Questo gruppo di utenti verrà collegato al profilo di autorizzazione definito nel passaggio **Configurazione dei criteri di autorizzazione ISE** seguente. Fare clic su **Salva**.

▼ 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

▼ - +

Configurazione della policy di autorizzazione ISE

- Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione**. Fare clic sul **segno + verde** per aggiungere un nuovo profilo di autorizzazione.
- Specificare un nome descrittivo, ad esempio Amministratore Sourcefire. Selezionare **ACCESS_ACCEPT** per il **tipo di accesso**. In **Operazioni comuni**, scorrere verso il basso e selezionare la casella accanto a **ASA VPN**. Fare clic sulla **freccia arancione** e selezionare **InternalUser:IdentityGroup**. Fare clic su **Salva**.

Suggerimento: Poiché in questo esempio viene utilizzato l'archivio identità dell'utente locale ISE, l'opzione InternalUser:IdentityGroup viene utilizzata per semplificare la configurazione. Se si usa un archivio identità esterno, viene comunque usato l'attributo di autorizzazione VPN ASA. Tuttavia, il valore da restituire al dispositivo Sourcefire è configurato manualmente. Ad esempio, se si digita manualmente Administrator nella casella a discesa ASA VPN, un valore Class-25 av-pair di Class = Administrator verrà inviato al dispositivo Sourcefire. Questo valore può quindi essere mappato a un gruppo di utenti sourcefire come parte della configurazione dei criteri di sistema. Per gli utenti interni, entrambi i metodi di configurazione sono accettabili.

Esempio di utente 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

Esempio di utente esterno

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

- Passare a **Criteri > Autorizzazione** e configurare un nuovo criterio di autorizzazione per le sessioni di amministrazione di Sourcefire. Nell'esempio seguente viene utilizzata la condizione **DEVICE:Device Type** per stabilire una corrispondenza con il tipo di dispositivo configurato nella Sezione precedente **Configurazione di dispositivi di rete e gruppi di dispositivi di rete**. Questo criterio viene quindi associato al profilo di autorizzazione dell'amministratore di Sourcefire configurato in precedenza. Fare clic su **Salva**.

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

Configurazione criteri di sistema Sourcefire

- Accedere a FireSIGHT MC e selezionare **Sistema > Locale > Gestione utente**. Fare clic sulla scheda **Autenticazione di accesso**. Fare clic sul pulsante **+ Crea oggetto di autenticazione** per aggiungere un nuovo server RADIUS per l'autenticazione/autorizzazione utente.
- Selezionare **RADIUS** per il **metodo di autenticazione**. Immettere un nome descrittivo per il server RADIUS. Immettere il **nome host/indirizzo IP** e la **chiave privata RADIUS**. La chiave segreta deve corrispondere alla chiave configurata in precedenza su ISE. Facoltativamente, immettere un **nome host/indirizzo IP** del server ISE di backup, se esistente.

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

- Nella sezione **Parametri specifici RADIUS**, immettere la stringa della classe 25 a coppia av nella casella di testo accanto al nome del gruppo locale Sourcefire a cui associare l'accesso GUI. In questo esempio, il valore Class=User Identity Groups:Sourcefire Administrator viene mappato al gruppo Sourcefire Administrator. Questo è il valore che ISE restituisce come parte di ACCESS-ACCEPT. È possibile selezionare un **ruolo utente predefinito** per gli utenti autenticati ai quali non sono stati assegnati gruppi di classe 25. Fare clic su **Save** per salvare la configurazione o procedere alla sezione Verify sottostante per verificare l'autenticazione 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"/>

- In **Shell Access Filter**, immettere un elenco di utenti separati da virgole per limitare le sessioni shell/SSH.

Shell Access Filter

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

Abilita autenticazione esterna

Infine, completare i passaggi seguenti per abilitare l'autenticazione esterna nel CCP:

1. Passa a **Sistema > Locale > Criteri di sistema**.
2. Seleziona **Autenticazione esterna** sul pannello sinistro.
3. Cambia *stato* in **Attivato** (disattivata per impostazione predefinita).
4. Abilitare il server ISE RADIUS aggiunto.
5. Salvare il criterio e applicarlo nuovamente all'accessorio.

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	RADIUS	10.1.1.254:1812	no	<input checked="" type="checkbox"/>

Verifica

- Per verificare l'autenticazione dell'utente con ISE, scorrere fino alla sezione **Parametri aggiuntivi di test** e immettere un nome utente e una password per l'utente ISE. Fare clic su **Test**. Un test di successo avrà un successo **ecologico**: Messaggio Test Complete nella parte superiore della finestra del browser.

Additional Test Parameters

User Name sfadmin

Password

*Required Field

Save Test Cancel

- Per visualizzare i risultati dell'autenticazione di test, andare alla sezione **Output test** e fare clic sulla freccia **nera** accanto a **Mostra dettagli**. Nello screenshot di esempio riportato di seguito, notare la risposta "radiusauth: |Class=User Identity Groups:Sourcefire Administrator|" ricevuto da ISE. Questo valore deve corrispondere al valore Class associato al gruppo Sourcefire locale configurato nel MC FireSIGHT sopra riportato. Fare clic su **Salva**.

Test Output

Show Details ▼

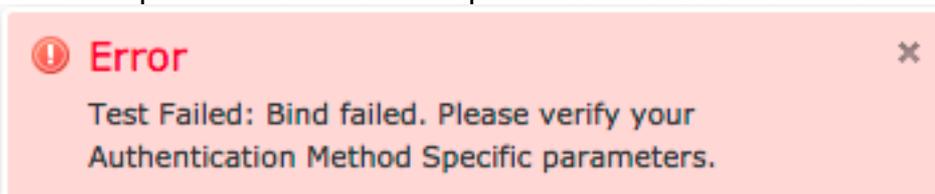
```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTH1T3qLx/radiusclient_0.conf
radiusauth - response: [User-Name=sfadmin]
radiusauth - response: [State=ReauthSession:0ac9e8cb0000006539F4896]
radiusauth - response: [Class=User Identity Groups:Sourcefire Administrator]
radiusauth -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

- Dalla GUI ISE Admin, selezionare **Operations > Authentication** (Operazioni > Autenticazioni) per verificare se il test di autenticazione dell'utente è riuscito o meno.

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			User Identity Groups...		ise12-psn1	Authentication f...

Risoluzione dei problemi

- Durante la verifica dell'autenticazione utente per ISE, l'errore seguente indica una mancata corrispondenza della chiave privata RADIUS o un nome utente/password errato.



- Dalla GUI di amministrazione di ISE, selezionare **Operations > Authentications** (Operazioni > Autenticazioni). Un evento **rosso** è indicativo di un guasto mentre un evento **verde** è indicativo di un'autenticazione/autorizzazione/modifica di autorizzazione riuscita. Fare clic sull'  icona per esaminare i dettagli dell'evento di autenticazione.

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

Informazioni correlate

[Documentazione e supporto tecnico – Cisco Systems](#)