

Integratie van FireSIGHT System met ISE voor RADIUS-gebruikersverificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[ISE-configuratie](#)

[Netwerkapparaten en netwerkapparaatgroepen configureren](#)

[Het ISE-verificatiebeleid configureren:](#)

[Een lokale gebruiker aan ISE toevoegen](#)

[ISE-autorisatiebeleid configureren](#)

[Configuratie van Sourcefire-systeembeleid](#)

[Externe verificatie inschakelen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de configuratiestappen die nodig zijn om een Cisco FireSIGHT Management Center (FMC) of een FirePOWER Managed-apparaat met Cisco Identity Services Engine (ISE) te integreren voor externe verificatie, bellen in User Service (RADIUS) gebruikersverificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FireSIGHT System en de eerste configuratie van het beheerde apparaat via GUI en/of shell
- Verificatie- en autorisatiebeleid ten aanzien van ISE configureren
- Basiskennis van RADIUS

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA v9.2.1
- ASA FirePOWER-module v5.3.1

- ISE 1.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

ISE-configuratie

Tip: Er zijn meerdere manieren om ISE-verificatie en -autorisatiebeleid te configureren ter ondersteuning van integratie met Network Access Devices (NAD) zoals Sourcefire. Het voorbeeld hieronder is één manier om de integratie te configureren. De steekproefconfiguratie is een referentiepunt en kan worden aangepast aan de behoeften van de specifieke inzet. Merk op dat de configuratie van de vergunning een tweestappenproces is. Een of meer autorisatiebeleid zal op ISE worden gedefinieerd met ISE met terugkerende RADIUS-waardesparen (av-paren) naar het FMC of het beheerde apparaat. Deze av-paren worden vervolgens in kaart gebracht aan een lokale gebruikersgroep die in de configuratie van het FMC-systeem is gedefinieerd.

Netwerkapparaten en netwerkapparaatgroepen configureren

- Vanuit ISE GUI, navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**. Klik op **+Add** om een nieuw netwerktoegangsapparaat (NAD) toe te voegen. Geef een beschrijvende naam en IP-adres voor het apparaat op. Het VCC wordt in het onderstaande voorbeeld gedefinieerd.

Network Devices

* Name
Description

* IP Address: /

- Klik onder de groep **Netwerkapparaat** op de **oranje pijl** naast alle apparaten. Klik op het  pictogram en selecteer **Groep Nieuw netwerkapparaat maken**. In het voorbeeldscherm dat volgt, is het Type Sourcefire van het apparaat ingesteld. Dit type apparaat zal in een latere stap worden vermeld in de definitie van de regel betreffende het autorisatiebeleid. Klik op **Opslaan**.

Create New Network Device Group...



Network Device Groups

* Parent

* Name

Description

* Type

- Klik nogmaals op de **oranje pijl** en selecteer de netwerkkapparaatgroep die in de bovenstaande stap is geconfigureerd

* Network Device Group

Location

Device Type

- Controleer het vakje naast **verificatie-instellingen**. Voer de gedeelde geheime sleutel van RADIUS in die voor deze NAD zal worden gebruikt. Merk op dat dezelfde gedeelde geheime sleutel later opnieuw gebruikt zal worden bij het configureren van de RADIUS-server op FireSIGHT MC. Klik op de knop **Weergeven** om de waarde voor de onbewerkte tekst te bekijken. Klik op **Opslaan**.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

- Herhaal de bovenstaande stappen voor alle FireSIGHT MC's en beheerde apparaten die RADIUS-gebruikersverificatie/autorisatie voor GUI en/of shell-toegang nodig hebben.

Het ISE-verificatiebeleid configureren:

- Vanuit ISE GUI, navigeer naar **Policy > Verificatie**. Als u beleidssets gebruikt, navigeer dan naar **Beleidsformaten > Beleidsformaten**. Het voorbeeld hieronder wordt ontleend aan een ISE-implementatie die de standaardauthenticatie en autorisatiebeleid interfaces gebruikt. De logica van de authenticatie- en autorisatieregel is hetzelfde, ongeacht de configuratie aanpak.
- De **Default Rule (Als geen match)** zal worden gebruikt om RADIUS-verzoeken van NAD's voor

het echt maken te verklaren waar de gebruikte methode geen MAC Verificatie Bypass (MAB) of 802.1X is. Deze regel is standaard ingesteld op gebruikersaccounts in de lokale **interne gebruikers** van ISE en op de identiteitsbron van deze **gebruikers**. Deze configuratie kan worden gewijzigd om te verwijzen naar een externe identiteitsbron zoals Active Directory, LDAP, etc. zoals gedefinieerd onder **Beheer > Identity Management > Externe Identity Services**. Omwille van de eenvoud zal dit voorbeeld ter plaatse op ISE gebruikersrekeningen definiëren zodat geen verdere wijzigingen in het authenticatiebeleid vereist zijn.

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	

Een lokale gebruiker aan ISE toevoegen

- Navigeer naar **Administratie > identiteitsbeheer > Identiteiten > Gebruikers**. Klik op **Add** (Toevoegen). Voer een betekenisvolle gebruikersnaam en wachtwoord in. Selecteer onder de selectie **Gebruikersgroepen** een bestaande groepsnaam of klik op het **groene + teken** om een nieuwe groep toe te voegen. In dit voorbeeld wordt de gebruiker "sfadmin" toegewezen aan de aangepaste groep "Sourcefire beheerder". Deze gebruikersgroep wordt gekoppeld aan het autorisatieprofiel dat in de onderstaande stap **Het machtigingsbeleid configureren**. Klik op **Opslaan**.

▼ 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

▼ - +

ISE-autorisatiebeleid configureren

- Navigeer in **Policy > Policy Elementen > Resultaten > autorisatie > autorisatieprofielen**. Klik op het **groene + teken** om een nieuw vergunningprofiel toe te voegen.
- Geef een beschrijvende naam op, zoals de Sourcefire-beheerder. Selecteer **ACCESS_ACCEPT** voor het **toegangstype**. Onder **Common Tasks**, scrollen u naar de onderkant en controleren u het vakje naast **ASA VPN**. Klik op de **oranje pijl** en selecteer **Interne gebruiker:IdentityGroup**. Klik op **Opslaan**.

Tip: Omdat dit voorbeeld de lokale opslag van de gebruikersidentiteit ISE gebruikt, wordt de optie `InterneUser:IdentityGroup` gebruikt om de configuratie te vereenvoudigen. Als u een externe identiteitswinkel gebruikt, wordt de `ASA VPN`-autorisatietekening nog steeds gebruikt, maar de waarde die naar het Sourcefire-apparaat moet worden geretourneerd, wordt handmatig ingesteld. Bijvoorbeeld, zal het handmatig typen van beheerder in de afrollijst van `ASA VPN` resulteren in een waarde van klasse-25 av-paar van klasse = beheerder die naar het Sourcefire-apparaat wordt verzonden. Deze waarde kan dan in kaart worden gebracht aan een gebruikersgroep die bron is als onderdeel van de systeembeleidsconfiguratie. Voor interne gebruikers is een van de volgende

configuratiemethoden aanvaardbaar.

Interne gebruikersvoorbeeld

* 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

ASA VPN

Administrator

▼ Advanced Attributes Settings

Select an item =

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

- Navigeer naar **beleid > autorisatie** en stel een nieuw autorisatiebeleid voor de Sourcefire beheersessies vast. Het voorbeeld hieronder gebruikt het **APPARAAT**: de toestand van het **apparaattype** om het apparaattype aan te passen dat in het **APPARAAT** is ingesteld. Het **configureren van netwerkkapparaten en netwerkkapparaatgroepen** hierboven. Dit beleid wordt vervolgens gekoppeld aan het hierboven ingestelde autorisatieprofiel voor de Sourcefire-beheerder. Klik op **Opslaan**.

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

Configuratie van Sourcefire-systeembeleid

- Meld u aan bij FireSIGHT MC en navigeer naar **Systeem > Local > User Management**. Klik op het tabblad **Login-verificatie**. Klik op de knop **+ Verificatieobject maken** om een nieuwe RADIUS-server toe te voegen voor gebruikersverificatie/autorisatie.
- Selecteer **RADIUS** voor de **verificatiemethode**. Voer een beschrijvende naam in voor de RADIUS-server. Voer de **hostnaam/IP-adres in** en **RADIUS-beveiligingssleutel**. De geheime

toets moet overeenkomen met de toets die eerder op ISE is ingesteld. Voer indien er een bestaat, optioneel een reservekopieerserver in **Host Name/IP-adres**.

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:

- Typ onder het gedeelte **RADIUS-specifieke parameters** de string klasse-25 av-paar in het tekstvak naast de lokale groepsnaam Sourcefire die voor GUI-toegang moet worden aangepast. In dit voorbeeld worden de groepen Class=User Identity:Sourcefire Administrator-waarde in kaart gebracht aan de beheerder van het Sourcefire. Dit is de waarde die ISE retourneert als onderdeel van de ACCESS-ACCEPT. Selecteer naar keuze een **Standaardgebruikersrol** voor geauthentiseerde gebruikers die geen klasse-25 groepen toegewezen hebben. Klik op **Save** om de configuratie op te slaan of ga naar de sectie Verifiëren hieronder om de verificatie met ISE te testen.

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"/>

- Voer onder **Shell Access Filter** een komma gescheiden lijst in van gebruikers om shell/SSH sessies te beperken.

Shell Access Filter

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

Externe verificatie inschakelen

Ten slotte moeten deze stappen worden voltooid om externe authenticatie op het VMC mogelijk te maken:

1. Navigeren in om **Systeem > Lokaal > Systeembeleid**.
2. Selecteren **Externe verificatie** op het linker paneel.
3. De *status* wijzigen in **Ingeschakeld** (Standaard uitgeschakeld).
4. Schakel de toegevoegde ISE RADIUS-server in.
5. Bewaar het beleid en pas het apparaat opnieuw toe.

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

Verifiëren

- Om gebruikersauthenticatie tegen ISE te testen, scrollen naar de sectie **Aanvullende testparameters** en voer een gebruikersnaam en wachtwoord voor de ISE-gebruiker in. Klik op **Test**. Een succesvolle test zal resulteren in een **groen** succes: Test Complete bericht boven in het browser venster.

Additional Test Parameters

User Name: sfadmin

Password:

*Required Field

Save Test Cancel

- Om de resultaten van de testverificatie te bekijken, gaat u naar het vak **Uitvoer testen** en klikt u op de **zwarte** pijl naast **Details weergeven**. In het onderstaande voorbeeld, noteer de "radiusauth - response: |Class=User Identity Groepen:Sourcefire Administrator|" -waarde ontvangen van ISE. Dit moet overeenkomen met de waarde van de klasse die is gekoppeld aan de lokale Sourcefire-groep die is ingesteld op FireSIGHT MC hierboven. Klik op **Opslaan**.

Test Output

Show Details

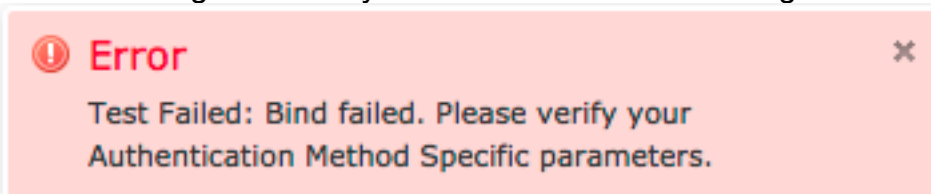
```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTH1T3qLx/radiusclient_0.conf
radiusauth - response: [User-Name=sfadmin]
radiusauth - response: [State=ReauthSession:0ac9e8cb0000006539F4896]
radiusauth - response: [Class=User Identity Groups:Sourcefire Administrator]
radiusauth -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

- Vanuit de ISE Admin GUI, navigeer naar **Operations > Verificaties** om het succes of falen van de gebruikersverificatietest te controleren.

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 18:40:00.856	✓		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...

Problemen oplossen

- Bij het testen van gebruikersauthenticatie tegen ISE is de volgende fout kenmerkend voor een RADIUS geheime Key mismatch of een incorrecte gebruikersnaam/wachtwoord.



- Vanuit de ISE admin GUI, navigeer naar **Operations > Authenticaties**. Een **rood** evenement duidt op een mislukking, terwijl een **groen** evenement wijst op een succesvolle authenticatie/autorisatie/wijziging van autorisatie. Klik op het  pictogram om de details van de authenticatiegebeurtenis te bekijken.

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

Gerelateerde informatie

[Technische ondersteuning en documentatie – Cisco Systems](#)