

Integratie van FireSIGHT System met ACS 5.x voor RADIUS-gebruikersverificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[ACS 5.x-configuratie](#)

[Netwerkapparaten en netwerkapparaatgroepen configureren](#)

[Een identiteitsgroep in ACS toevoegen](#)

[Een lokale gebruiker aan ACS toevoegen](#)

[ACS-beleid configureren](#)

[Configuratie van FireSIGHT Management Center](#)

[Configuratie van FireSIGHT Manager-systeembeleid](#)

[Externe verificatie inschakelen](#)

[Verificatie](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

Dit document beschrijft de configuratiestappen die nodig zijn om een Cisco FireSIGHT Management Center (FMC) of een FirePOWER Managed-apparaat met Cisco Secure Access Control System 5.x (ACS) te integreren voor verificatie op afstand van verificatie, bellen in gebruikersverificatie (RADIUS).

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
- Het configureren van authenticatie- en autorisatiebeleid voor ACS 5.x
- Basiskennis van RADIUS

Gebruikte componenten

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

- Cisco beveiligde toegangscontrole Systeem 5.7(ACS 5.7)
- Cisco FireSIGHT Manager Center 5.4.1

Bovenstaande versies zijn de meest recente versies die momenteel beschikbaar zijn. De functie wordt ondersteund op alle ACS 5.x-versies en FMC 5.x-versies.

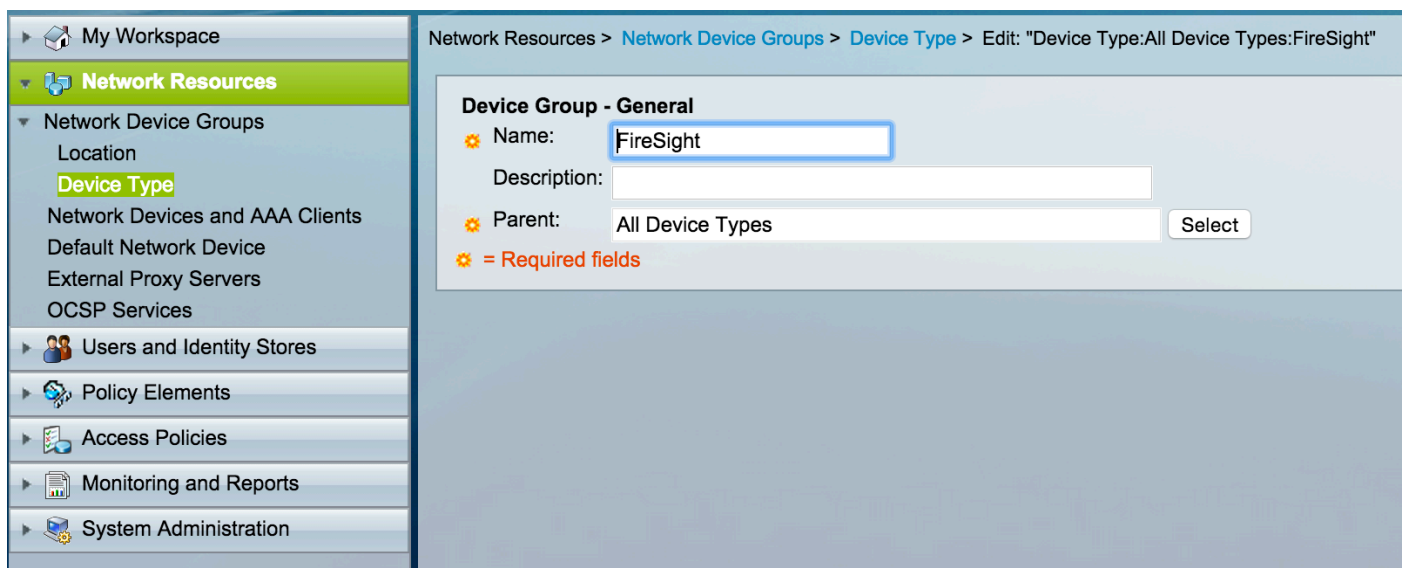
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configuratie

ACS 5.x-configuratie

Netwerkapparaten en netwerkapparaatgroepen configureren

- Vanuit de ACS GUI, navigeer naar de **Groep van het Netwerkapparaat**, klik op het **Type apparaat** en creëren een Apparaatgroep. In het voorbeeld screenshot dat hieronder volgt, is het apparaattype FireSight geconfigureerd. Dit type apparaat zal in een latere stap worden vermeld in de definitie van de regel betreffende het autorisatiebeleid. Klik op **Opslaan**.



The screenshot displays the ACS GUI interface for configuring a Device Type. The left sidebar shows the navigation menu with 'Network Resources' expanded to 'Device Type'. The main content area shows the configuration form for 'Device Group - General' with the following fields:

- Name:** FireSight (highlighted with a blue border)
- Description:** (empty text field)
- Parent:** All Device Types (with a 'Select' button)

A legend indicates that fields with a gear icon are required fields.

- Vanuit de ACS GUI, navigeer naar **de Groep van het Netwerkapparaat**, klik op **de cliënten van het Netwerk en AAA** en voeg een apparaat toe. Geef een beschrijvende naam en IP-adres voor het apparaat op. Het FireSIGHT Management Center is gedefinieerd in het onderstaande voorbeeld.

Network Resources > Network Devices and AAA Clients > Edit: "FireSight Management Center"

Name: FireSight Management Center
 Description:

Network Device Groups
 Location: All Locations [Select]
 Device Type: All Device Types:FireSight [Select]

IP Address
 Single IP Address IP Subnets IP Range(s)
 IP: 10.150.176.224

Authentication Options
 TACACS+
 RADIUS
 Shared Secret: ***** [Show]
 CoA port: 1700
 Enable KeyWrap
 Key Encryption Key:
 Message Authenticator Code Key:
 Key Input Format ASCII HEXADECIMAL

* = Required fields

Submit Cancel

- In de **Groepen van het Netwerkapparaat**, dient u **het Type apparaat** te configureren net als de apparaatgroep die in de bovenstaande stap is gemaakt.
- Controleer het vakje naast **Verificatieopties**, selecteer RADIUS-selectieteken en voer de **gedeelde geheime** toets 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 het FireSIGHT Management Center. Klik op de knop **Weergeven** om de waarde voor de onbewerkte tekst te bekijken. Klik op **Inzenden**.
- Herhaal de bovenstaande stappen voor alle FireSIGHT Management Centers en Beheerde Apparaten waarvoor RADIUS-gebruikersverificatie/autorisatie voor GUI en/of shell-toegang vereist is.

Een identiteitsgroep in ACS toevoegen

- Navigeer naar **gebruikers en identiteitsopslag**, stel **Identiteitsgroep** in. In dit voorbeeld, is de identiteitsgroep gecreëerd "De administrateur van de Schuin". Deze groep zal worden gekoppeld aan het in de onderstaande stappen gedefinieerde vergunningprofiel.

Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:FireSight Administrator"

General

- Name: FireSight Administrator
- Description:
- Parent: All Groups

= Required fields

Een lokale gebruiker aan ACS toevoegen

- Navigeer naar **gebruikers en identiteitsopslag**, stel **gebruikers** in het gedeelte **Interne identiteitsopslag**. Voer de gewenste informatie in voor de maken van lokale gebruikers. Selecteer de **Identity Group** die in bovenstaande stap is gemaakt en klik op **Inzenden**.

Users and Identity Stores > Internal Identity Stores > Users > Edit: "test"

General

- Name: test Status: Enabled
- Description:
- Identity Group: All Groups:FireSight Administrator
- Email Address:

Account Disable

- Disable Account if Date Exceeds: 2015-Nov-01 (yyyy-Mmm-dd)
- Disable account after 3 successive failed attempts

Password Hash

- Enable Password Hash Applicable only for Internal Users to store password as hash. Authentication types CHAP/MSCHAP will not work if this option is enabled. While disabling the hash, ensure that password is reconfigured using change password option.

Password Lifetime

- Password Never Expired/Disabled: Overwrites user account blocking in case password expired/disabled

User Information

There are no additional identity attributes defined for user records

Creation/Modification Information

- Date Created: Wed Sep 02 13:15:56 UTC 2015
- Date Modified: Wed Sep 02 23:12:39 UTC 2015
- Date Enabled: Wed Sep 02 13:15:56 UTC 2015

= Required fields

ACS-beleid configureren

- In de ACS GUI, navigeer naar **Beleids-elementen > Vergunning en Toestemmingen > Netwerktogang > Verificatieprofielen**. Maak een nieuw vergunningprofiel met een beschrijvende naam. In het onderstaande voorbeeld is beleid gemaakt met een FireSight-beheerder.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"

General Common Tasks RADIUS Attributes

Name: FireSight Administrator

Description:

= Required fields

- Voeg in het tabblad **RADIUS-eigenschappen** de handmatige eigenschap toe voor het autoriseren van de hierboven gemaakte identiteitsgroep en klik op **Indienen**

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Class	String	Groups:FireSight Administrator

Add ^ Edit V Replace ^ Delete

Dictionary Type: RADIUS-IETF

RADIUS Attribute: Class Select

Attribute Type: String

Attribute Value: Static

Groups:FireSight Administrator

= Required fields

Submit Cancel

- Navigeren in **toegang Beleid > Toegangsservices > Standaardnetwerktogang > autorisatie** en een nieuw autorisatiebeleid te configureren voor de FireSight Management Center-beheersessies. Het onderstaande voorbeeld gebruikt de **NDG:Apparaattype & toestand** van de **Identity Group** om het apparaattype en de identiteitsgroep te evenaren die in de bovenstaande stappen zijn geconfigureerd.

- Dit beleid wordt vervolgens gekoppeld aan het autorisatieprofiel van de FireSight-beheerder, dat hierboven als **resultaat** is geconfigureerd. Klik op **Inzenden**.

Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | [Exception Policy](#)

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	Status	Name	Conditions	Results	Hit Count	
1	<input checked="" type="checkbox"/>	Rule-1	NDG:Device Type in All Device Types:FireSight	Identity Group in All Groups:FireSight Administrator	Authorization Profiles FireSight Administrator	7

Configuratie van FireSIGHT Management Center

Configuratie van FireSIGHT Manager-systeembeleid

- Meld u aan bij FireSIGHT MC en navigeer naar **Systeem > Local > User Management**. Klik op het tabblad **Externe 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 ACS was ingesteld. Voer naar keuze een **back-up ACS server Host Name/IP-adres** in indien er een bestaat.

Overview Analysis Policies Devices Objects AMP Health System

Local > User Management Updates Licenses Mor

Users User Roles External Authentication

External Authentication Object

Authentication Method: RADIUS

Name *: ACS

Description:

Primary Server

Host Name/IP Address *: 172.18.75.172 ex. IP or hostname

Port *: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address: ex. IP or hostname

Port: 1812

RADIUS Secret Key:

- Onder het **RADIUS-specifieke parameters** In dit voorbeeld wordt de waarde van de beheerder van de klasse=Groepen:De waarde van de bestuurder van FireSight in kaart gebracht aan de groep van de administrator. Dit is de waarde die ACS terug zal geven als deel van de ACCESS-ACCEPT. Klik **Opslaan** om de configuratie op te slaan of naar het gedeelte Verifiëren hieronder te gaan om verificatie met ACS te testen.

RADIUS-Specific Parameters

Timeout (Seconds)

Retries

Access Admin

Administrator

- 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

Externe verificatie inschakelen

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

1. Blader naar **Systeem > Local > System Policy**.
2. Selecteer **Externe Verificatie** in het linker paneel.
3. Wijzig de *status* in **Ingeschakeld** (standaard uitgeschakeld).
4. Schakel de toegevoegde ACS-RADIUS-server in.
5. Bewaar het beleid en pas het apparaat opnieuw toe.

Verificatie

- Om gebruikersauthenticatie tegen ACS te testen, scrollen naar de sectie **Aanvullende Testparameters** en voer een gebruikersnaam en wachtwoord voor de ACS-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

Password



Success



Test Complete.

- 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=Groepen:FireSight Administrator|" -waarde ontvangen van ACS. Dit moet overeenkomen met de waarde van de klasse die is gekoppeld aan de lokale FireSIGHT-groep die hierboven is ingesteld op FireSIGHT MC. Klik op **Opslaan**.

Test Output

Show Details



```
check_auth_radius: szUser: test
RADIUS config file: /var/tmp/_bcEn4h_wF/radiusclient_0.conf
radiusauth - response: |User-Name=test|
radiusauth - response: |Class=Groups:FireSight Administrator|
radiusauth - response: |Class=CACS: ████████-acs/229310634/47|
"test" RADIUS Authentication OK
check_is_radius_member attrib match found: |Class=Groups:FireSight Administrator| - |Class=Groups:FireSight Administrator| *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

Save

Test

Cancel