

Stappen voor configuratie van FireSIGHT-systemen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Configuratie](#)

[Stap 1: Eerste instelling](#)

[Stap 2: Installeer licenties](#)

[Stap 3: Het systeembeleid toepassen](#)

[Stap 4: Het gezondheidsbeleid toepassen](#)

[Stap 5: Beheerde apparaten registreren](#)

[Stap 6: Geïnstalleerde licenties inschakelen](#)

[Stap 7: Gebiedsinterfaces configureren](#)

[Stap 8: Het inbraakbeleid configureren](#)

[Stap 9: Een toegangscontrolebeleid instellen en toepassen](#)

[Stap 10: Controleer of het FireSIGHT Management Center gebeurtenissen heeft ontvangen](#)

[Aanvullende aanbeveling](#)

Inleiding

Nadat u een FireSIGHT Management Center of een FirePOWER-apparaat hebt gereinigd, dient u verschillende stappen te ondernemen om het systeem volledig functioneel te maken en waarschuwingen te genereren voor inbraakgebeurtenissen; zoals het installeren van licenties, het registreren van de apparatuur, het toepassen van gezondheidsbeleid, systeembeleid, toegangscontrolebeleid, inbraakbeleid enz. Dit document is een aanvulling op de FireSIGHT System Installatie Guide.

Voorwaarden

Deze handleiding gaat ervan uit dat u de FireSIGHT System Installatie Guide zorgvuldig hebt gelezen.

Configuratie

Stap 1: Eerste instelling

Op uw FireSIGHT Management Center moet u het installatieproces voltooien door in de webinterface te loggen en de eerste configuratieopties in de setup-pagina te specificeren, die hieronder wordt weergegeven. Op deze pagina moet u het beheerwachtwoord wijzigen en kunt u ook netwerkinstellingen instellen zoals Domain en DNS-servers en de tijdconfiguratie instellen.

Change Password

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password

Confirm

Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

Protocol IPv4 IPv6 Both

IPv4 Management IP

Netmask

IPv4 Default Network Gateway

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Time Settings

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock Via NTP from

Manually 2013 / July / 19 : 9 : 25

Current Time 2013-07-19 09:25

Set Time Zone [America/New York](#)

U kunt optioneel terugkerende regel en geolocation updates evenals automatische back-ups configureren. Alle functiekaarten kunnen ook op dit punt worden geïnstalleerd.

Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

Install Now

Enable Recurring Rule Update Imports

Recurring Geolocation Updates

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

Install Now

Enable Recurring Weekly Updates

Automatic Backups

Use this field to schedule automatic configuration backups.

Enable Automatic Backups

License Settings

To obtain your license, navigate to _____ where you will be prompted for the license key _____ and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key _____

Add/Verify

Type	Description	Expires
------	-------------	---------

Op deze pagina kunt u een apparaat ook registreren in het FireSIGHT Management Center en een detectiemodus instellen. De detectie modus en andere opties die u tijdens de registratie kiest, bepalen de standaardinterfaces, inline sets en zones die het systeem maakt, evenals het beleid dat het eerst op beheerde apparaten van toepassing is.

Device Registration

Use this section to add, license, and apply initial access control policies to pre-registered devices. Note that you do not need to add devices to the secondary Defense Center in a high availability pair. If you enable the Apply Default Access Control Policies option, the applied policy for each device depends on the detection mode (Inline, Passive, Access Control, or Network Discovery) you configured for the device.

Click Add to add each device.

Apply Default Access Control Policies

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Add"/>

End User License Agreement

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, THEN SOURCEFIRE IS UNWILLING TO LICENSE THE LICENSED MATERIALS TO YOU, IN WHICH CASE YOU MAY NOT DOWNLOAD, INSTALL OR USE ANY OF THE LICENSED MATERIALS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT INITIATE USE OF THE PRODUCT. BY SELECTING "I ACCEPT," "OK," "CONTINUE," "YES," "NEXT" OR BY INSTALLING OR USING THE LICENSED MATERIALS IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE PRODUCT.

If You are located outside of the United States, then Sourcefire International GmbH, a subsidiary located in Switzerland, shall be a party to this Agreement with You and the party licensing the Licensed Materials to You hereunder. This Agreement governs Your access and use of the Sourcefire Products, except to the extent there is a separate written agreement signed by both You and Sourcefire that expressly states that it governs Your use of the Sourcefire Products. In the event of a conflict between the provisions of such a written agreement and this Agreement, the order of precedence shall be (1) the separate signed agreement, and (2) this Agreement.

1. DEFINITIONS

The following capitalized terms shall have the following meanings in this EULA:

1.1. "Appliance" means any Sourcefire-branded network security appliance made available to You, consisting of Hardware and pre-installed Sourcefire Software and/or

I have read and agree to the END USER LICENSE AGREEMENT

Stap 2: Installeer licenties

Als u tijdens de eerste setup-pagina geen licenties hebt geïnstalleerd, kunt u de taak als volgt voltooien:

- Navigeren naar de volgende pagina: **Systeem > Licenties**.
- Klik op **Nieuwe licentie toevoegen**.

Add Feature License

License Key

License

Get License

Verify License

Submit License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to

Using the license key, follow the on-screen instructions to generate a license.

Return to License Page

Als u geen licentie hebt ontvangen, neemt u contact op met de vertegenwoordiger van uw account.

Stap 3: Het systeembeleid toepassen

Het systeembeleid specificeert de configuratie voor verificatieprofielen en tijdsynchronisatie tussen het FireSIGHT Management Center en de beheerde apparaten. Om het systeembeleid te configureren of toe te passen, navigeer het **stelsysteem > Local > System Policy**. Een standaardstelsysteembeleid wordt geleverd, maar moet worden toegepast op alle beheerde apparaten.

Stap 4: Het gezondheidsbeleid toepassen

Het gezondheidsbeleid wordt gebruikt om te configureren hoe beheerde apparaten hun gezondheidstoestand rapporteren aan het FireSIGHT Management Center. Om het gezondheidsbeleid te configureren of toe te passen, dient u te **navigeren** naar **Gezondheid > Gezondheidsbeleid**. Er is een standaard gezondheidsbeleid voorzien, maar dat moet worden toegepast op alle beheerde apparaten.

Stap 5: Beheerde apparaten registreren

Als u apparaten tijdens de eerste setup-pagina niet hebt geregistreerd, raadpleegt u [dit document](#) voor instructies voor het registreren van een apparaat in een FireSIGHT Management Center.

Stap 6: Geïnstalleerde licenties inschakelen

Voordat u een functielicentie op uw apparaat kunt gebruiken, moet u dit voor elk beheerd apparaat inschakelen.

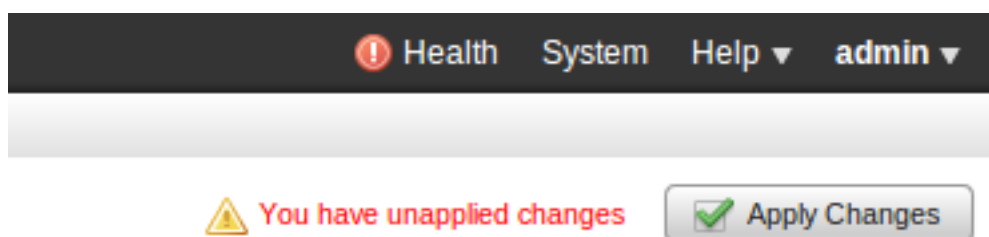
1. Navigeren naar de volgende pagina: **Apparaten > Apparaatbeheer**.
2. Klik op het apparaat waarvoor u de licenties wilt activeren en voer het tabblad Apparaat in.
3. Klik op het pictogram **Bewerken** (*potlood*) naast Licentie.

License


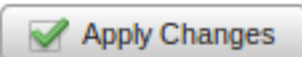
Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes
VPN	Yes

Schakel de gewenste licenties voor dit apparaat in en klik op **Opslaan**.

Merk op dat het bericht "*U hebt de wijzigingen niet toegepast*" in de rechterbovenhoek staat. Deze waarschuwing blijft actief, zelfs als u niet op de pagina voor apparaatbeheer klikt totdat u op de knop **Wijzigingen toepassen** klikt.



Health System Help ▼ admin ▼

 You have unapplied changes 

Stap 7: Gebiedsinterfaces configureren

1. Navigeer naar de volgende pagina-**apparaten > Apparaatbeheer**.
2. Klik op het pictogram **Bewerken** (potlood) voor de sensor van uw keuze.

3. Klik onder het tabblad **Interfaces** op het pictogram **Bewerken** voor de interface van uw keuze.

Edit Interface ? X

None Passive Inline Switched Routed HA Link

Please select a type above to configure this interface.

Save Cancel

Selecteer een passieve of inline interfaceconfiguratie. Switched en Routed interfaces vallen buiten het toepassingsgebied van dit artikel.

Stap 8: Het inbraakbeleid configureren

- Navigeer naar de volgende pagina: **Beleid > Inbraakbeleid > Inbraakbeleid**.
- Klik op **beleid maken** en het volgende dialogvenster wordt weergegeven:

Create Intrusion Policy ? X

Policy Information

Name * |

Description

Drop when Inline

Base Policy Connectivity Over Security

Variables

Use the system default value

Networks to protect any

* Required

Create Policy Create and Edit Policy Cancel

U moet een naam toewijzen en het te gebruiken basisbeleid definiëren. Afhankelijk van uw plaatsing kunt u ervoor kiezen om de optie **Daling** te hebben **wanneer Inline** ingeschakeld. Definieert de netwerken die u wilt beveiligen om valse positieven te verminderen en de prestaties van het systeem te verbeteren.

Als u op **beleid maken** klikt, worden uw instellingen opgeslagen en wordt het IPS-beleid gemaakt.

Als u wijzigingen in het inbraakbeleid wilt aanbrengen, kunt u in de plaats **Beleid maken en bewerken**.

Opmerking: Inbraakbeleid wordt toegepast als onderdeel van het beleid inzake toegangscontrole. Nadat een inbraakbeleid is toegepast, kunnen alle wijzigingen worden toegepast zonder het gehele beleid voor toegangscontrole opnieuw toe te passen door op de knop **Opnieuw** te klikken.

Stap 9: Een toegangscontrolebeleid instellen en toepassen

1. Navigeer naar **beleid > Toegangsbeheer**.
2. Klik op **Nieuw beleid**.

New Access Control Policy ? X

Name:

Description:

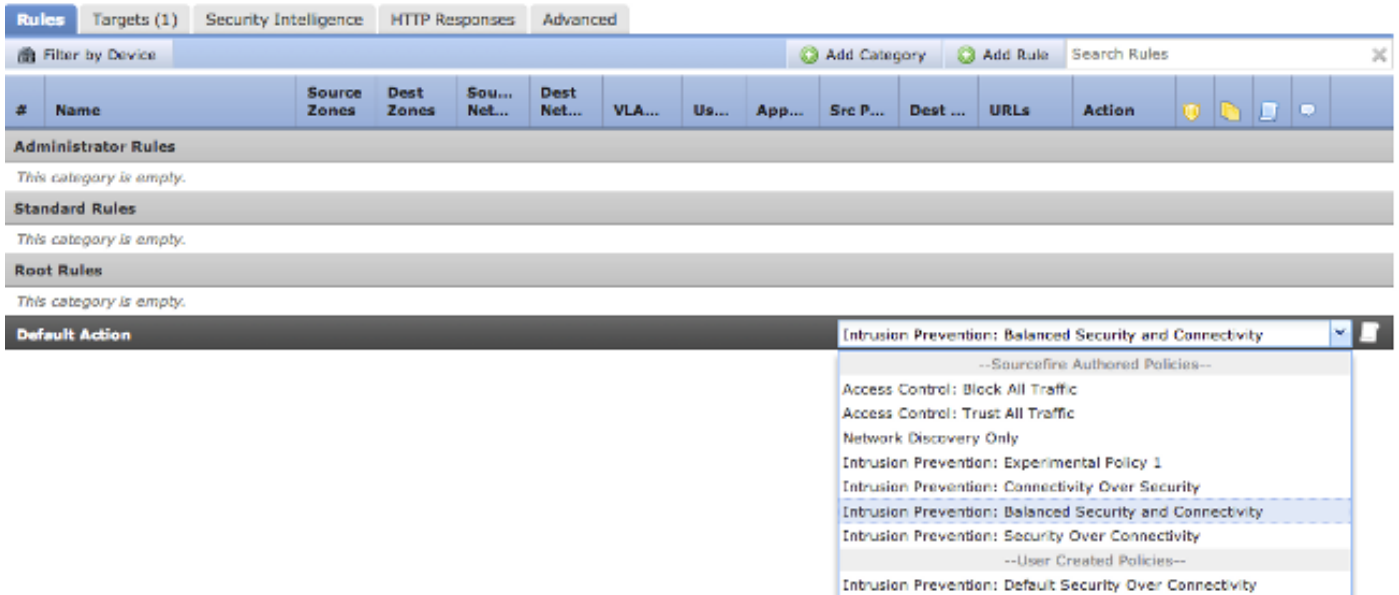
Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

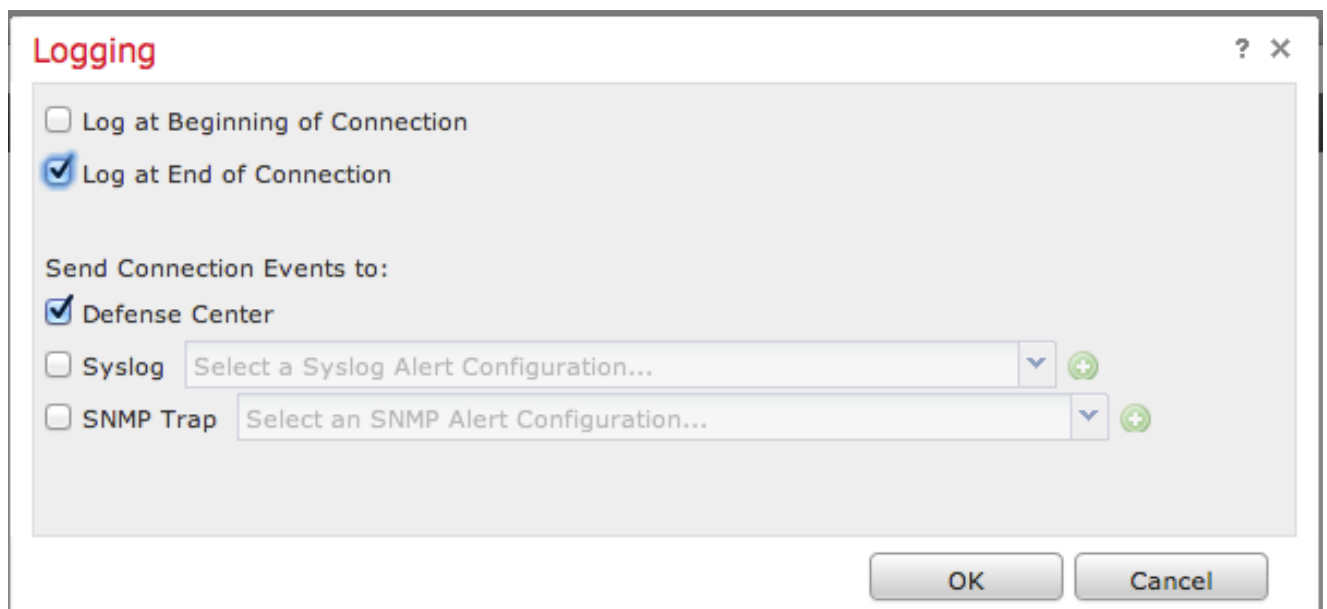
Available Devices

Selected Devices

3. Geef een **naam** voor het beleid en een **beschrijving**.
4. Selecteer **Inbraakpreventie** als de **standaardactie** van het toegangscontrolebeleid.
5. Selecteer ten slotte de **gerichte apparaten** waarop u het toegangscontrolemiddel wilt toepassen, en klik op **Opslaan**.
6. Selecteer uw inbraakbeleid voor de standaardactie.



7. De verbinding registreren moet worden ingeschakeld om verbindingsgebeurtenissen te genereren. Klik op het uitrolmenu dat rechts van de **Standaardactie** is.



8. Klik erop om de verbindingen aan het begin of aan het eind van de verbinding te noteren. De gebeurtenissen kunnen worden vastgelegd op FireSIGHT Management Center, een actieve locatie of via SNMP.

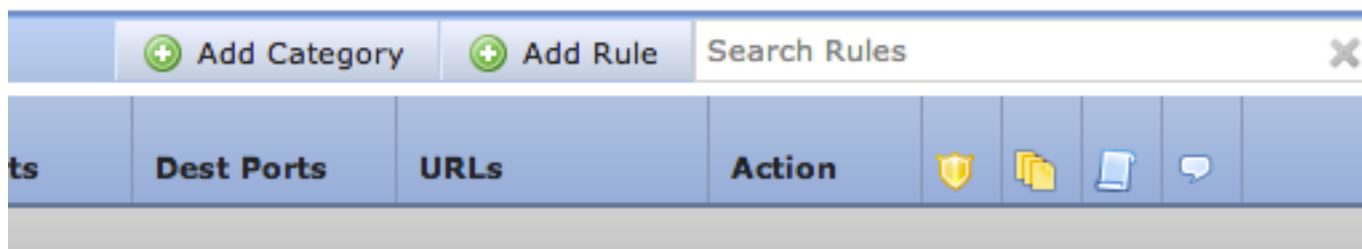
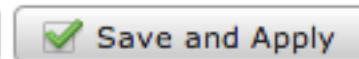
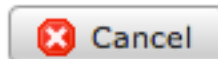
Opmerking: Het is niet aanbevolen om aan beide uiteinden van de verbinding te loggen, omdat elke verbinding (behalve geblokkeerde verbindingen) twee keer zal worden vastgelegd. Loggen aan het begin is handig voor verbindingen die geblokkeerd zullen worden, en het registreren aan het eind is handig voor alle andere verbindingen.

9. Klik op **OK**. Merk op dat de kleur van het loggingpictogram is gewijzigd.

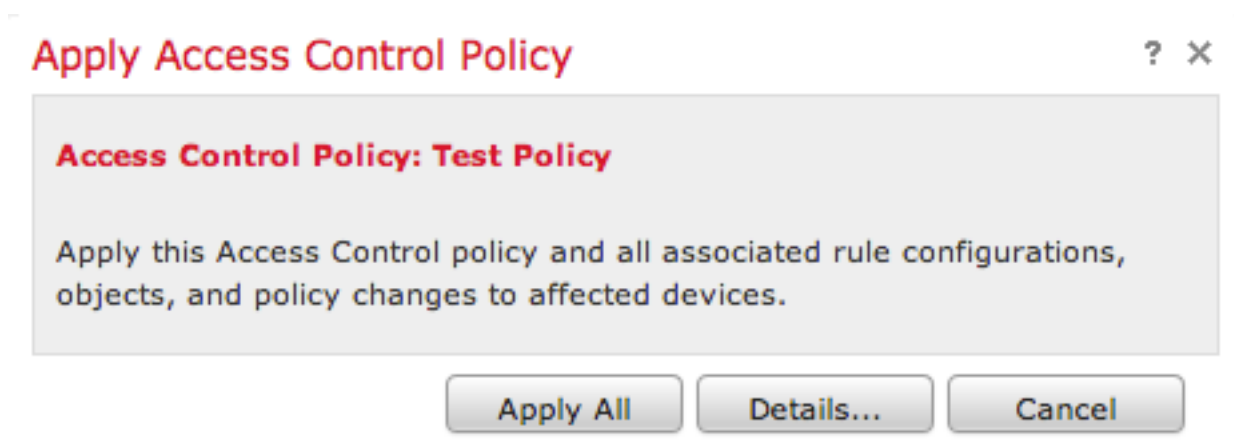
10. U kunt tegelijkertijd een **toegangscontroleregel** toevoegen. De opties die u kunt gebruiken zijn afhankelijk van het type licenties dat u hebt geïnstalleerd.

11. Als u klaar bent met het maken van wijzigingen. Klik op de knop **Opslaan en toepassen**. U merkt een bericht dat aangeeft dat u niet-opgeslagen wijzigingen in uw beleid in de rechterbovenhoek hebt uitgevoerd totdat op de knop is gedrukt.

You have unsaved changes



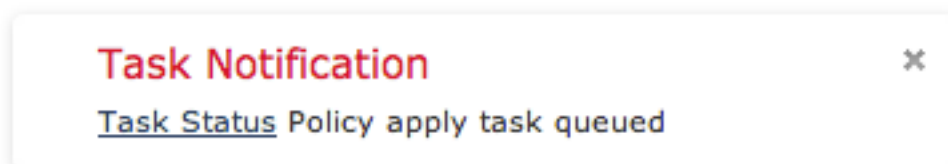
U kunt ervoor kiezen alleen de wijzigingen op te slaan of op Opslaan en Toepassen te klikken. Het volgende venster verschijnt als u het laatste kiest.



12. **Alles toepassen** zal het toegangscontrolebeleid en het (de) daaraan verbonden inbraakbeleid(en) op de beoogde voorzieningen toepassen.

Opmerking: Als een inbraakbeleid voor het eerst wordt toegepast, kan het niet worden gedeselecteerd.

13. U kunt de status van de taak controleren door op de link **Taakstatus** te klikken in het bericht dat boven op de pagina wordt weergegeven, of door naar: **Systeem > Monitoring > Task Status**



14. Klik op de koppeling **Taakstatus** om de voortgang van het beleid voor toegangscontrole te controleren.

Job Summary

Remove Completed Jobs

Remove Failed Jobs

Running	0
Waiting	0
Completed	7
Retrying	0
Failed	0

Jobs

Task Description	Message	Creation Time	Last Change	Status	
 Health Policy apply tasks 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
Health policy apply to appliance [redacted] Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed	
 Policy apply tasks 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
Apply Default Access Control to [redacted] Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

Stap 10: Controleer of het FireSIGHT Management Center gebeurtenissen heeft ontvangen

Nadat het beleid van de Toegangscontrole van toepassing is voltooid, zou u moeten beginnen om connecties gebeurtenissen te zien en afhankelijk van verkeer inbraakgebeurtenissen.

Aanvullende aanbeveling

U kunt ook de volgende aanvullende functies op uw systeem configureren. Raadpleeg de gebruikershandleiding voor meer informatie over de implementatie.

- Geplande back-ups
- Automatische softwareupdates, SRU, VDB en geoLocation downloads/installaties.
- Externe verificatie via LDAP of RADIUS