

初始配置步骤FireSIGHT系统

目录

[简介](#)

[前提条件](#)

[配置](#)

[步骤 1：初始设置](#)

[步骤 2：安装许可证](#)

[步骤 3：运用系统策略](#)

[步骤 4：运用卫生政策](#)

[步骤 5：寄存器受管理设备](#)

[步骤 6：Enable \(event\)已安装许可证](#)

[步骤 7：配置感觉接口](#)

[步骤 8:配置入侵策略](#)

[步骤 9：设定及适用访问控制策略](#)

[步骤 10：如果FireSIGHT管理中心接收事件，请验证](#)

[其它建议](#)

简介

在您再镜像FireSIGHT管理中心或FirePOWER设备后，您需要完成几个步骤使系统充分地运行和生成入侵事件的警报;例如，安装许可证，注册设备，应用卫生政策、系统策略、访问控制策略，入侵策略等。本文是补充对于FireSIGHT系统安装指南。

前提条件

此指南假设，您仔细阅读FireSIGHT系统安装指南。

配置

步骤 1：初始设置

在您的FireSIGHT管理中心，您必须通过登录Web接口和指定在设置页的初始配置选项完成安装过程，如下所示。在此页，您必须更改管理员密码，并且能也指定网络设置例如域和DNS服务器和时间配置。

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	<input type="password" value="*****"/>
Confirm	<input type="password" value="*****"/>

Network Settings

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

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Both
IPv4 Management IP	<input type="text"/>
Netmask	<input type="text"/>
IPv4 Default Network Gateway	<input type="text"/>
Hostname	<input type="text"/>
Domain	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Tertiary DNS Server	<input type="text"/>

Time Settings

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

Set My Clock	<input checked="" type="radio"/> Via NTP from <input type="text"/>
	<input type="radio"/> Manually <input type="text" value="2013"/> / <input type="text" value="July"/> / <input type="text" value="19"/> : <input type="text" value="9"/> : <input type="text" value="25"/>
Current Time	2013-07-19 09:25
Set Time Zone	America/New York

您能或者配置循环规则和geolocation更新以及自动备份。所有功能许可证可能这时也安装。

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
------	-------------	---------

在此页，您能也注册设备到FireSIGHT管理中心和指定检测模式。您在注册时选择的检测模式和其它选项确定系统创建的默认接口、轴向集和区域，以及最初适用于受管理设备的策略。

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"/>	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

步骤 2：安装许可证

在初始设置页期间，如果没有安装许可证，您能通过遵从这些步骤完成任务：

- 导航对以下页：**系统>许可证**。
- 单击**添加新的许可证**。

Add Feature License

License Key

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.

如果没有收到许可证，请与您的帐户联系销售代表。

步骤 3：运用系统策略

系统策略指定验证配置文件的在FireSIGHT管理中心和受管理设备之间的配置和时间同步。要配置或运用系统策略请导航到**系统>本地>System策略**。提供默认系统策略，但是需要应用到所有受管理设备。

步骤 4：运用卫生政策

卫生政策用于配置受管理设备如何他们的健康状态向FireSIGHT管理中心报告。要配置或运用卫生政策请导航对**健康>卫生政策**。提供默认卫生政策，但是需要应用到所有受管理设备。

步骤 5：寄存器受管理设备

在初始设置页期间，如果没有注册设备，请读说明的[本文](#)关于怎样注册设备到FireSIGHT管理中心。

步骤 6 : Enable (event)已安装许可证

在您能使用在您的设备前的所有功能许可证，您需要为每受管理设备启用它。

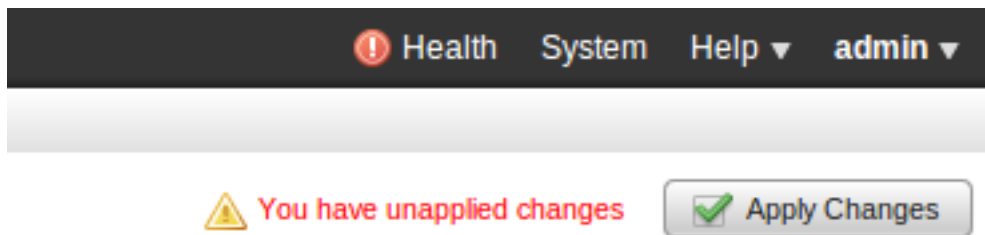
1. 导航对以下页：**设备>设备管理**。
2. 点击您要启用许可证并且参与设备选项卡的设备。
3. 在许可证旁边单击**编辑**(铅笔图标)。

License

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

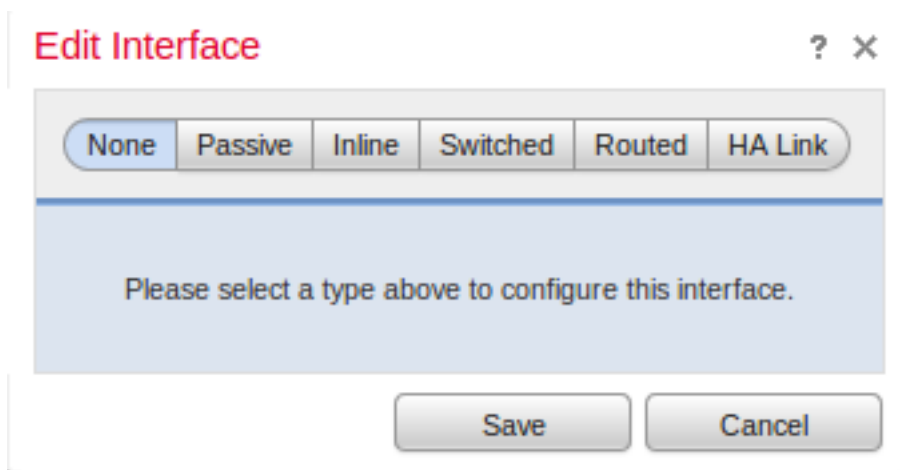
启用此设备的需要的许可证并且点击**“Save”**。

注意消息“您有未应用的更改”在右上角。此警告依然是活动，即使您导航远离设备管理页，直到您点击**应用更改**按钮。



步骤 7 : 配置感觉接口

1. 导航对以下页**设备>设备管理**。
2. 点击您的选择传感器的**编辑**(铅笔)图标。
3. 在**接口**下**请**选中，点击**Edit**图标您的选择接口的。



选择一个被动或轴向接口配置。交换式和路由接口请是超出此条款的范围之外。

步骤 8:配置入侵策略

- 导航对以下页：**策略>入侵>入侵策略。**
- 点击**Create策略**，并且以下的对话框显示：

您必须分配名称和定义将使用的基本策略。根据您的部署选择有选项**丢弃**，**当线型**启用。定义您要保护减少错误肯定和改进系统的性能的网络。

单击在**Create策略**将保存您的设置并且创建IPS策略。如果要做对入侵策略的任何修改，您能选择**创建并且编辑策略**。

注意：作为访问控制策略一部分，入侵策略应用。在入侵策略应用后，所有修改可以应用，无需重新应用全部的访问控制策略通过单击**重新应用**按钮。

步骤 9：设定及适用访问控制策略

1. 导航到策略>访问控制。
2. 点击新建的策略。

New Access Control Policy ? X

Name:

Description:

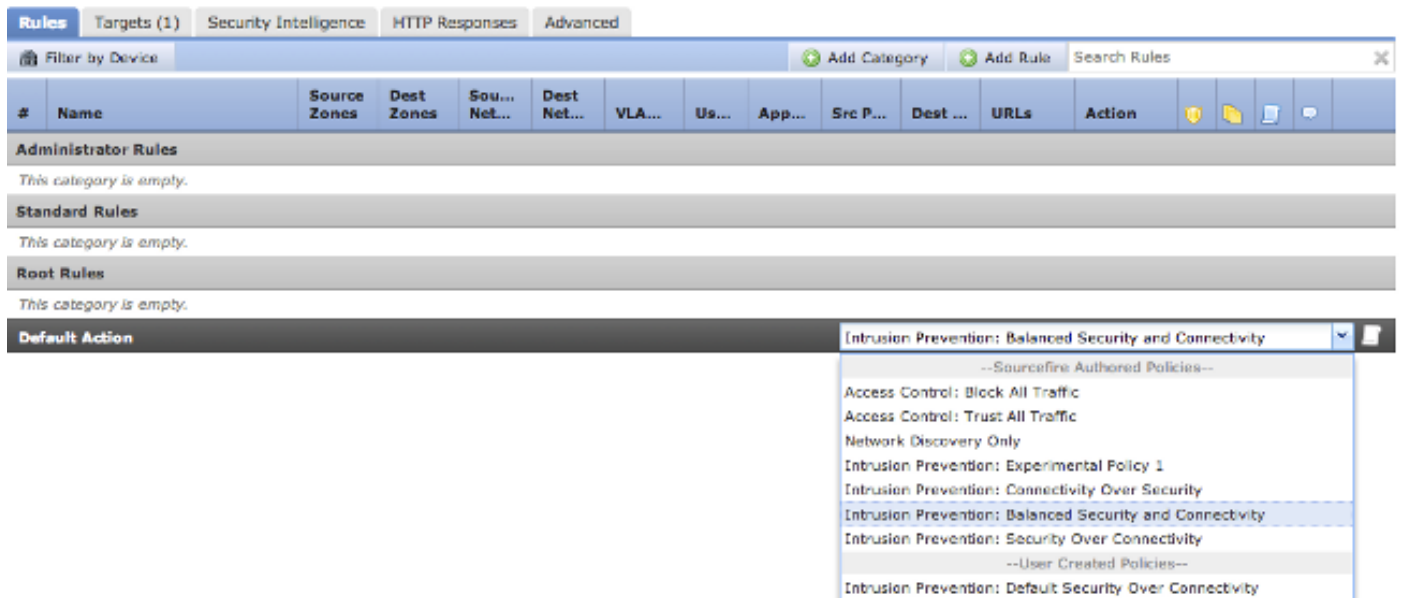
Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

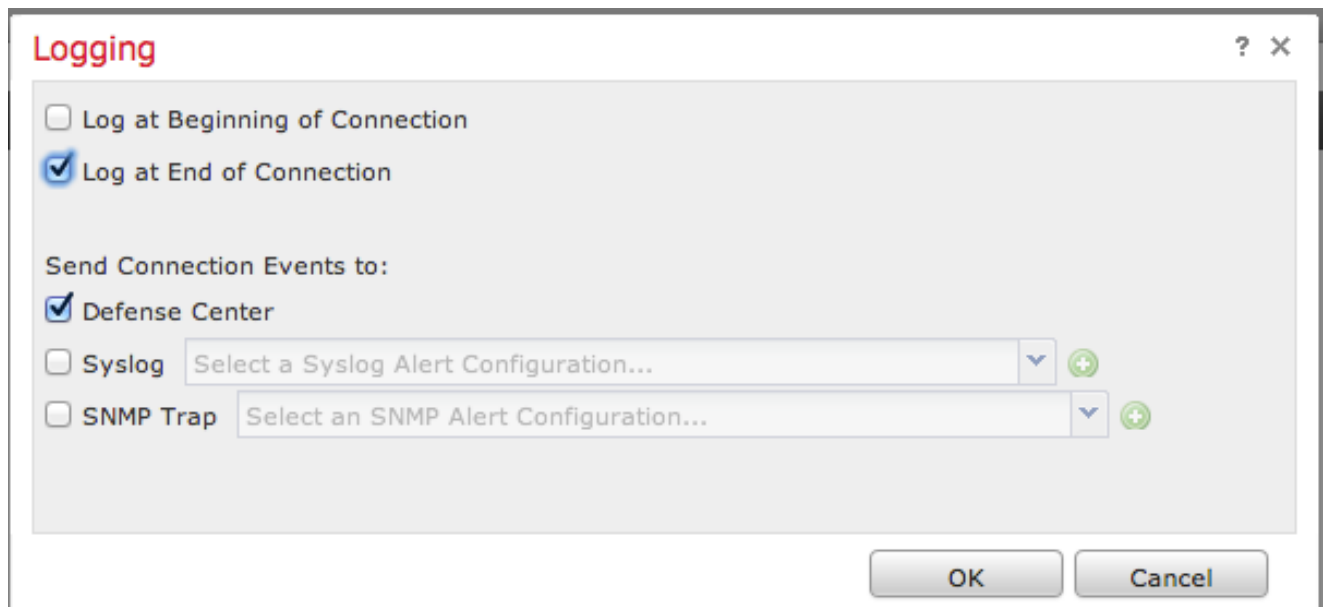
Available Devices

Selected Devices

3. 为策略和说明提供一名称。
4. 选择入侵防御作为访问控制策略的默认操作。
5. 最终请选择您要适用于访问控制策略的目标设备，并且点击“Save”。
6. 选择您的默认操作的入侵策略。



7. 必须启用连接记录日志生成连接事件。单击是默认操作的权利的下拉菜单。



8. 选择记录连接在开始或连接的结束。事件可以被注册FireSIGHT管理中心，一个Syslog位置，或者通过SNMP。

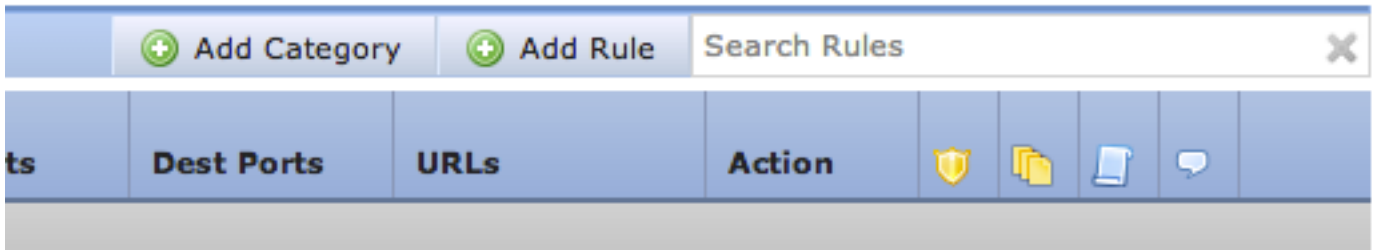
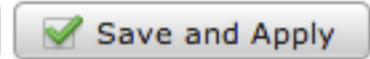
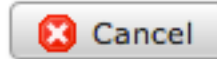
注意：没有推荐记录在连接的两端，因为每连接(除了阻止连接)两次将被记录。首先记录为将阻塞的连接是有用的，并且在末端的记录日志为其他连接是有用的。

9. 单击 **Ok**。注意记录日志图标的颜色更改。

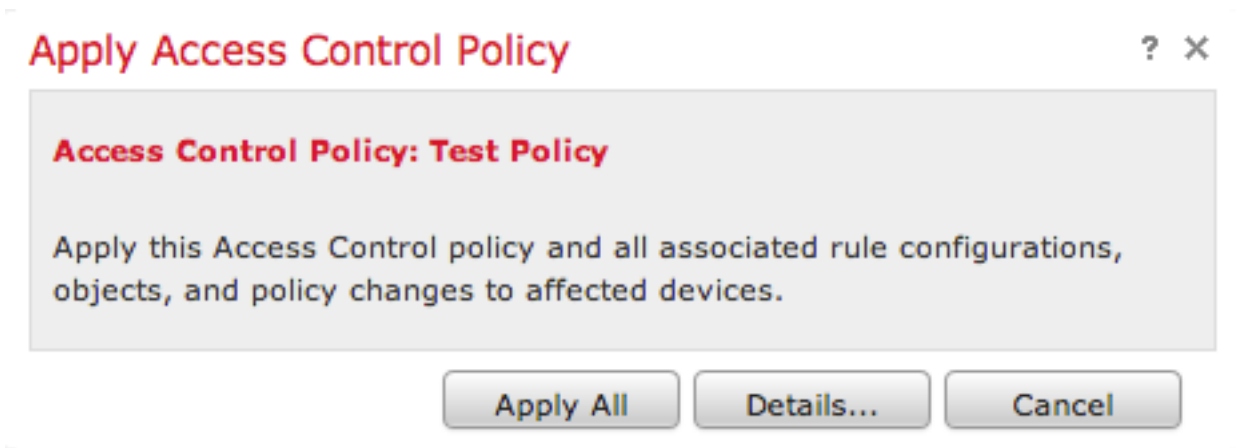
10. 您可以此时增加访问控制规则。您能使用的选项取决于您安装许可证的种类。

11. 当您完成时进行更改。单击“**Save**”和应用按钮。您将注意消息指示您有在您的策略的未获救的更改在右上角，直到按钮点击。

You have unsaved changes



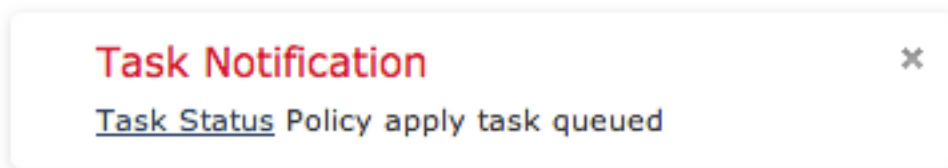
您能选择只保存更改或点击“Save”和应用。 如果选择后者，以下窗口将出现。



12. 运用所有将适用于访问控制策略和所有相关的入侵策略目标设备。

注意：如果入侵策略第一次将应用，不可能取消选择。

13. 您能监控单击在导航显示的在页顶部，或者通知的任务状态链路的任务的状况对：**系统>Monitoring>任务状态**



14. 点击任务状态链路监控访问控制策略的进度应用。





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 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 Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

步骤 10：如果FireSIGHT管理中心接收事件，请验证

在访问控制策略应用完成后，您应该根据流量入侵事件开始看到连接事件和。

其它建议

您能也配置在您的系统的以下其它功能。请参考用户指南关于实施细节。

- 定期备份
- 自动软件更新、SRU、VDB和GeoLocation下载/安装。
- 外部验证通过LDAP或RADIUS