

Шаги начальной конфигурации систем FireSIGHT

Содержание

[Введение](#)

[Предпосылка](#)

[!--- конфигурацию](#)

[Шаг 1: Первоначальная конфигурация](#)

[Шаг 2: Установите лицензии](#)

[Шаг 3: Примените системную политику](#)

[Шаг 4. : Примените политику в области охраны здоровья](#)

[Шаг 5. : Зарегистрируйте управляемые устройства](#)

[Шаг 6: Включите установленные лицензии](#)

[Шаг 7: Настройте интерфейсы считывания](#)

[Шаг 8: Настройте политику проникновения](#)

[Шаг 9: Настройте и примените политику контроля доступа](#)

[Шаг 10: Проверьте если получения события центра управления FireSIGHT](#)

[Дополнительная рекомендация](#)

Введение

После того, как вы повторно захватите образ Центр управления FireSIGHT или Устройство FirePOWER, необходимо выполнить несколько шагов, чтобы сделать систему полностью функциональной и генерировать предупреждения для событий проникновения; такой как, устанавливая лицензию, регистрируя устройства, применяя политику в области охраны здоровья, системную политику, политику контроля доступа, политика проникновения и т.д. Этот документ является дополнением к Руководству по установке системы FireSIGHT.

Предпосылка

Это руководство предполагает, что вы тщательно читали Руководство по установке системы FireSIGHT.

!--- конфигурацию

Шаг 1: Первоначальная конфигурация

На вашем Центре управления FireSIGHT необходимо завершить процесс установки путем вхождения в веб-интерфейс и определения параметров начальной конфигурации на странице настройки, изображенной ниже. На этой странице вы должны изменить пароль администратора и можете также задать настройки сети, такие как Домен и серверы DNS и конфигурация времени.

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](#)

Можно дополнительно настроить повторяющееся правило и обновления геолокации, а также автоматические резервные копии. Любые характеристики лицензирования могут также быть установлены на этом этапе.

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

На этой странице можно также зарегистрировать устройство к Центру управления FireSIGHT и задать режим обнаружения. Режим обнаружения и другие опции, которые вы выбираете во время регистрации, определяют интерфейсы по умолчанию, встраивают наборы и зоны, которые система создает, а также политика, что это первоначально применяется к управляемым устройствам.

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

Шаг 2: Установите лицензии

Если вы не устанавливали лицензии во время страницы начальной настройки, можно выполнить задачу путем выполнения этих действий:

- Перейдите к следующей странице: **Система > Лицензии**.
- Щелкните по **Add New License**.

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

Если вы не получили лицензию, свяжитесь с Торговым представителем своей учетной записи.

Шаг 3: Примените системную политику

Системная политика задает конфигурацию для Опознавательных Профилей и Временной синхронизации между Центром управления FireSIGHT и управляемыми устройствами. Чтобы настроить или Применить Системную политику перешли к **Системе> Локальный> Системная политика**. Политика системы по умолчанию предоставлена, но должна быть применена к любым управляемым устройствам.

Шаг 4. : Примените политику в области охраны здоровья

Политика в области охраны здоровья используется, чтобы настроить, как управляемые устройства сообщают о своем состоянии здоровья Центру управления FireSIGHT. Чтобы настроить или Применить Политику в области охраны здоровья перешли к **состоянию> Политика в области охраны здоровья**. Политика в области охраны здоровья по умолчанию предоставлена, но должна быть применена к любым управляемым устройствам.

Шаг 5. : Зарегистрируйте управляемые устройства

Если вы не зарегистрировали устройства во время страницы начальной настройки, считайте [этот документ](#) для инструкций по тому, как зарегистрировать устройство к Центру управления FireSIGHT.

Шаг 6: Включите установленные лицензии

Прежде чем можно будет использовать любую характеристику лицензирования на устройстве, необходимо включить его для каждого управляемого устройства.

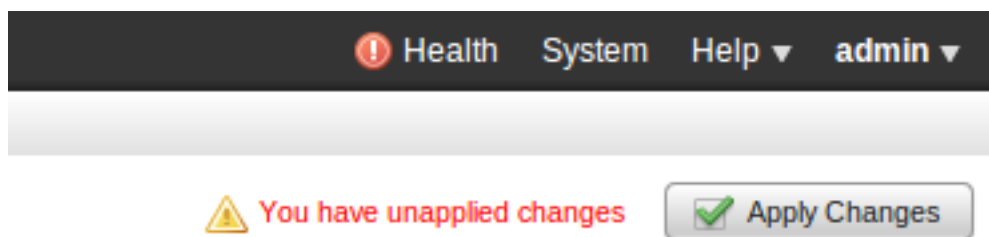
1. Перейдите к следующей странице: **Устройства> Управление устройствами**.
2. Щелкните по устройству, на которое вы хотите включить лицензии и ввести вкладку Device.
3. Нажмите **Edit** (значок карандаша), следующий за Лицензией.

License

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

Включите необходимые лицензии для этого устройства и нажмите **Save**.

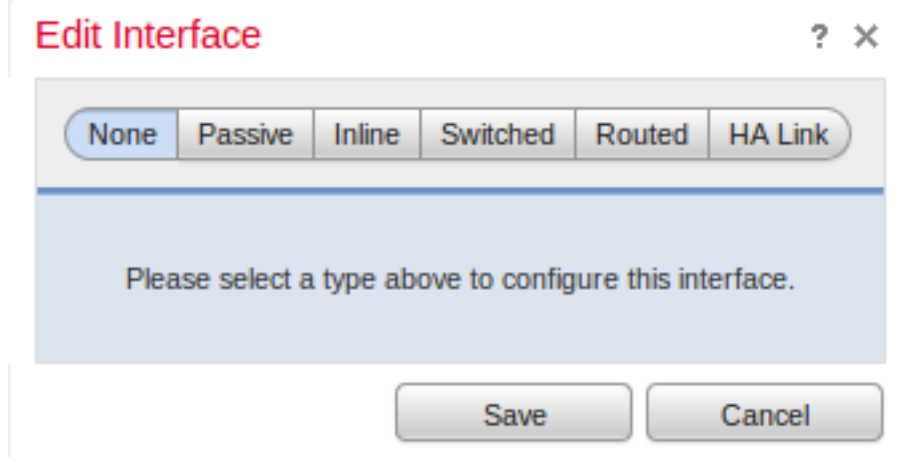
Заметьте сообщение, "*У вас есть остающиеся без применения изменения*" на правом верхнем угле. Это предупреждение остается активным, даже если вы перешли далеко от страницы управления устройствами, пока вы не нажимаете кнопку **Apply Changes**.



Шаг 7: Настройте интерфейсы считывания

1. Перейдите к следующей странице **Devices> Device Management**.

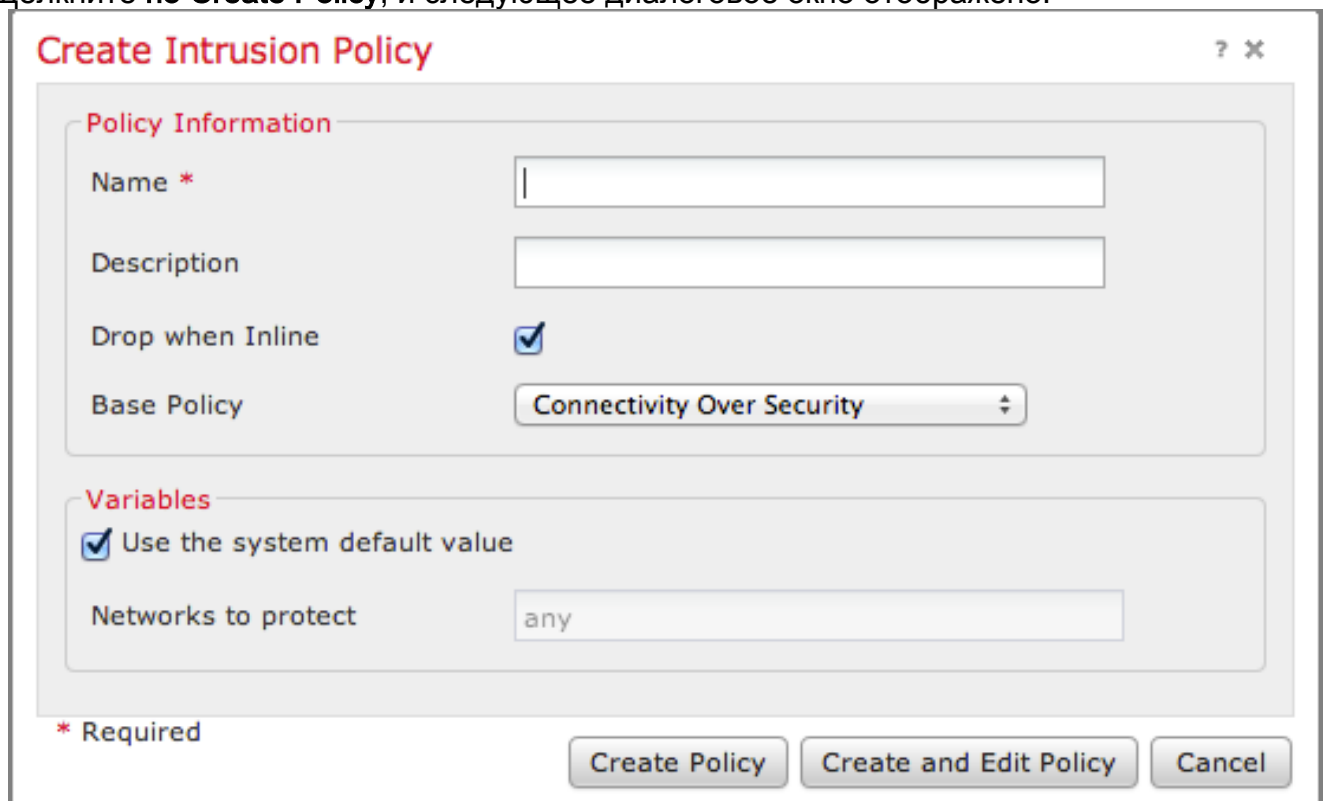
2. Нажмите **Edit** (карандаш) значок для датчика по Вашему выбору.
3. Под вкладкой **Interfaces** нажмите **Значок редактирования** для интерфейса по Вашему выбору.



Выберите Passive or Inline interface configuration. Коммутированный и Маршрутизируемые интерфейсы выходят за рамки этой статьи.

Шаг 8: Настройте политику проникновения

- Перейдите к следующей странице: **Политика > Проникновение > Политика Проникновения**.
- Щелкните по **Create Policy**, и следующее диалоговое окно отображено:



Необходимо назначить название и определить основную политику, которая будет использоваться. В зависимости от ваших развертываний вы можете, принял решение иметь опцию **Drop**, когда **Встроенный** включил. Определите сети, которые вы хотите защитить,

чтобы уменьшить ошибочные допуски и улучшить производительность системы.

Щелчок по **Create Policy** сохранит ваши настройки и создаст политику IPS. Если вы хотите сделать какую-либо модификацию к политике проникновения, можно выбрать **Create и Edit Policy** вместо этого.

Примечание: Политика проникновения применена как часть Политики контроля доступа. После того, как политика Проникновения применена, любые модификации могут быть применены, не повторно применяя целую Политику контроля доступа путем нажатия кнопки **Reapply**.

Шаг 9: Настройте и примените политику контроля доступа

1. Перейдите к **Политике > Управление доступом**.
2. Щелкните по **New Policy**.

New Access Control Policy ? X

Name:

Description:

Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

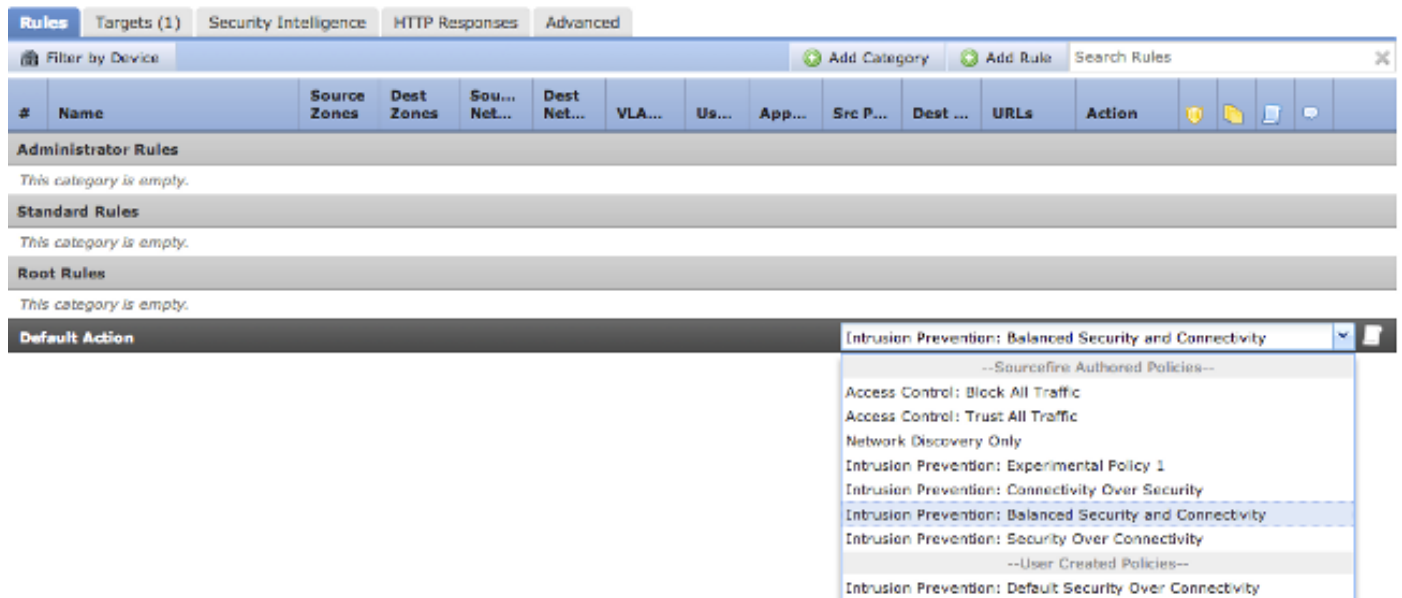
Available Devices

Search

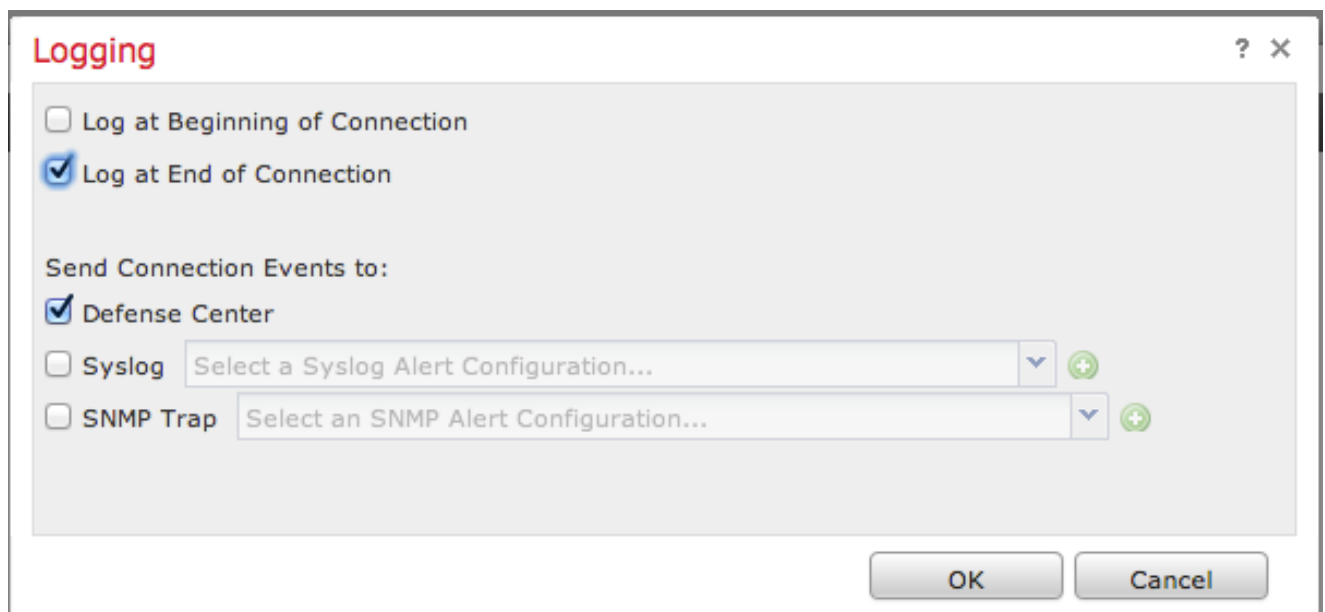
Selected Devices

3. Предоставьте **Название** для политики и **Описания**.
4. Выберите **Intrusion Prevention** как **Действие по умолчанию** Политики контроля доступа.
5. Наконец выберите **Targeted Devices**, к которому вы хотите применить политику контроля доступа и нажать **Save**.

6. Выберите свою политику Проникновения для действия по умолчанию.



7. Регистрации соединения нужно позволить генерировать события подключения. Нажмите выпадающее меню, которое является правильным из Действия по умолчанию.



8. Примите решение регистрировать соединения или в начале или в конце соединения. События могут быть зарегистрированы на Центре управления FireSIGHT, местоположении системного журнала, или через SNMP.

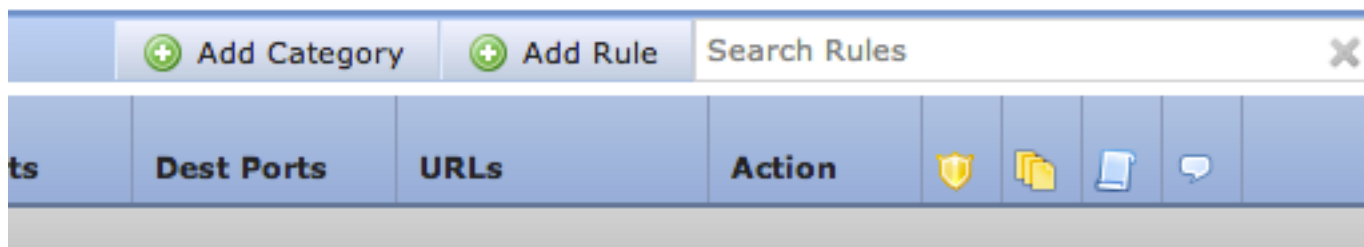
Примечание: Не рекомендуется регистрировать в обоих концах соединения, потому что каждое соединение (кроме заблокированных соединений) будет зарегистрировано дважды. Регистрация вначале полезна для соединений, которые будут заблокированы, и регистрирующий в конце полезно для всех других соединений.

9. Нажмите кнопку ОК. Обратите внимание на то, что цвет значка регистрации изменился.

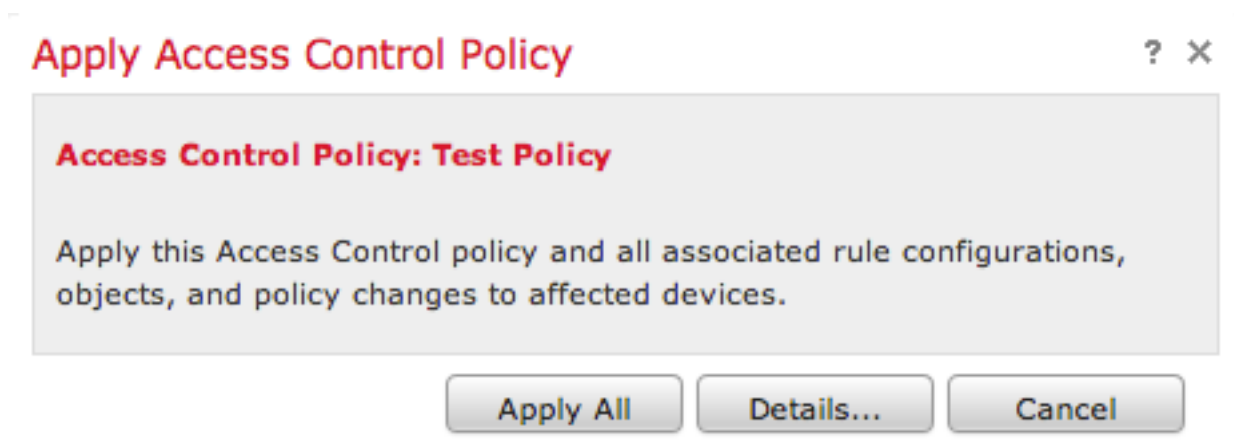
10. Можно добавить Правило Управления доступом в это время. Опции, которые можно использовать, зависят от типа лицензий, которые вы установили.

11. По окончании внесения изменений нажмите кнопку **Save и Apply**. Вы заметите, что сообщение, указывающее на вас, не сохранило изменений на вашей политике по верхнему правому углу, пока не нажата кнопка.

You have unsaved changes



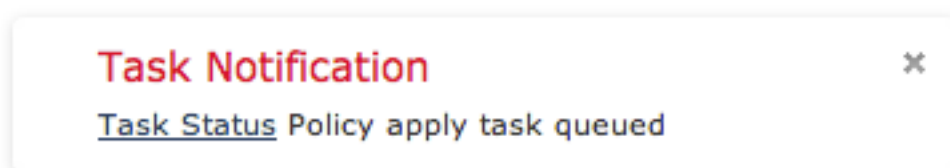
Можно принять решение только **Сохранить** изменения или щелкнуть по **Save и Apply**. Следующее окно появится при выборе последнего.



12. **Применить Все** применят Политику контроля доступа и любую связанную политику (политику) Проникновения к целевым устройствам.

Примечание: Если политика проникновения будет применена впервые, она не может отменяться.

13. Можно контролировать статус задачи, нажимающей на ссылку **Статуса Задачи** на уведомлении, показанном в верхней части страницы, или путем навигации к: **Система> Контролирующий> Статус Задачи**



14. Щелкните по ссылке Статуса Задачи для мониторинга, выполнение Политики контроля доступа применяются.





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	

Шаг 10: Проверьте если получения события центра управления FireSIGHT

После Политики контроля доступа применяются, завершил, необходимо начать видеть события соединений и в зависимости от событий проникновения трафика.

Дополнительная рекомендация

Можно также настроить следующие дополнительные характеристики в системе. См. Руководство пользователя для сведений о внедрении.

- Запланированные резервные копирования
- Автоматическое Обновление ПО, SRU, VDB и загрузки/установки GeoLocation.
- Внешняя проверка подлинности через LDAP или RADIUS