Фильтрация URL-адресов на примере конфигурации системы FireSIGHT

Содержание

Введение

Функция фильтрации URL-адресов на Центре управления FireSIGHT позволяет вам писать условие в правиле управления доступом для определения трафика, который пересекает сетевое на незашифрованных URL-запросах отслеживаемыми хостами. Этот документ описывает шаги для настройки Фильтрации URL-адресов в Системе FireSIGHT.

Предварительные условия

Требования

Этот документ имеет немного некоторые определенные требования для Лицензии Фильтрации URL-адресов и порта.

Требование лицензии фильтрации URL-адресов

Центр управления FireSIGHT требует лицензии Фильтрации URL-адресов для контакта с облаком периодически для обновления на информации URL. Можно добавить категорию - и основанные на репутации условия URL к правилам управления доступом без лицензии Фильтрации URL-адресов; однако, вы не можете применить политику контроля доступа,

пока вы сначала не добавляете лицензию Фильтрации URL-адресов на Центр управления FireSIGHT, затем включаете его на устройствах, предназначенных политикой.

Если лицензия Фильтрации URL-адресов истекает, правила управления доступом с категорией и основанными на репутации условиями URL прекращают фильтровать URL, и Центр управления FireSIGHT больше не связывается с облачным сервисом. Без лицензии Фильтрации URL-адресов отдельные URL или группы URL могут собираться позволить или заблокироваться, но категория URL или данные репутации не могут использоваться для фильтрации сетевого трафика.

Требование порта

Система FireSIGHT использует порты 443/HTTPS и 80/HTTP для передачи с облачным сервисом. Порт 443/HTTPS должен быть открыт двунаправленным образом, и входящий доступ к порту 80/HTTP должен быть позволен на Центре управления FireSIGHT.

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Устройства FirePOWER: серии 7000, серии 8000
- Виртуальное устройство Системы предотвращения вторжений следующего поколения (NGIPS)
- Устройство адаптивной защиты (ASA) FirePOWER
- Версия программного обеспечения 5.2 Sourcefire или позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Включите фильтрацию URL-адресов на центре управления FireSIGHT

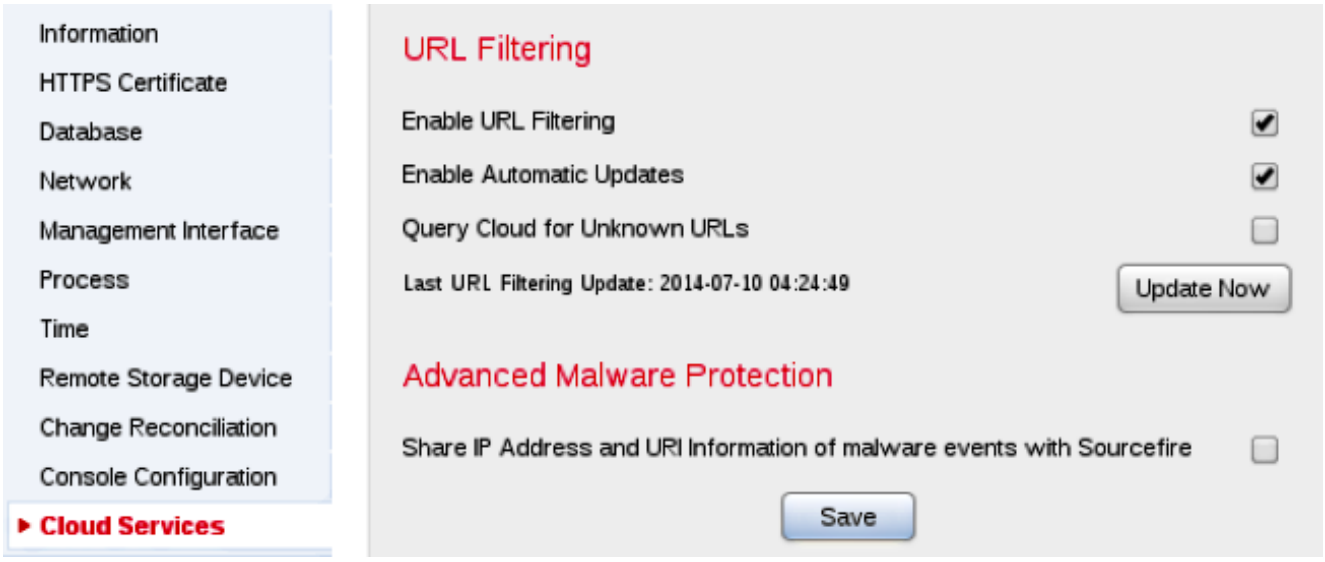
Для включения Фильтрации URL-адресов выполните эти шаги:

1. Войдите в интерфейс веба - пользователя Центра управления FireSIGHT.

2. Перейдите к **Системе> Локальный> Конфигурация**.

3. Выберите **Cloud Services**.

4. Установите флажок **Enable URL Filtering** для включения Фильтрации URL-адресов.



5. Дополнительно, установите флажок **Enable Automatic Updates** для включения автоматических обновлений. Эта опция позволяет системе связываться с облачным сервисом регулярно для получения обновлений данных URL в наборах локальных данных устройства.

   Примечание: Несмотря на то, что облачный сервис, как правило, обновляет свои данные один раз в день при включении автоматических обновлений это вынуждает Центр управления FireSIGHT проверять каждые 30 минут, чтобы удостовериться, что информация является всегда текущей. Несмотря на то, что ежедневные обновления имеют тенденцию быть маленькими, если это были больше чем пять дней, с тех пор как последнее обновление, новые данные фильтрации URL-адресов могли бы занять до 20 минут для загрузки. Как только обновления были загружены, могло бы потребоваться до 30 минут для выполнения самого обновления.

6. Дополнительно, выберите **Облако Запроса для Неизвестных URL** для флажка Unknown URLs для запроса облачного сервиса для неизвестных URL. Эта опция позволяет системе сделать запрос облака Sourcefire, когда кто-то в вашей отслеживаемой сети пытается перейти к URL, который не находится в наборе локальных данных. Если облако не знает категорию или репутацию URL, или если Центр управления FireSIGHT не может связаться с облаком, URL не совпадает с правилами управления доступом с категорией или основанными на репутации условиями URL.

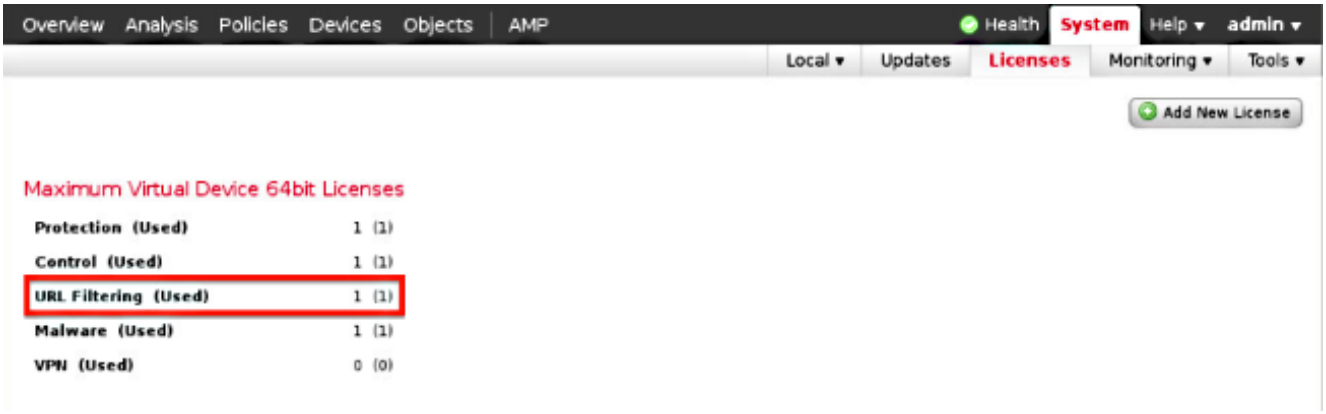
   Примечание: Вы не можете назначить категории или репутации к URL вручную. Отключите эту опцию, если вы не хотите, чтобы ваши некатегоризированные URL каталогизировались облаком Sourcefire, например, по причинам конфиденциальности.

7. **Нажмите Save.** Настройки Фильтрации URL-адресов сохранены.

   Примечание: На основе промежутка времени, так как Фильтрация URL-адресов была в последний раз включена, или если это первоначально, вы включили Фильтрацию URL-адресов, Центр управления FireSIGHT получает данные Фильтрации URL-адресов из облачного сервиса.

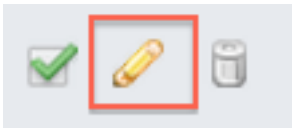
Примените лицензию фильтрации URL-адресов на управляемое устройство

1. Проверьте, установлена ли лицензия Фильтрации URL-адресов на Центре управления FireSIGHT. Перейдите к странице **System> Licenses** для обнаружения списка лицензий.

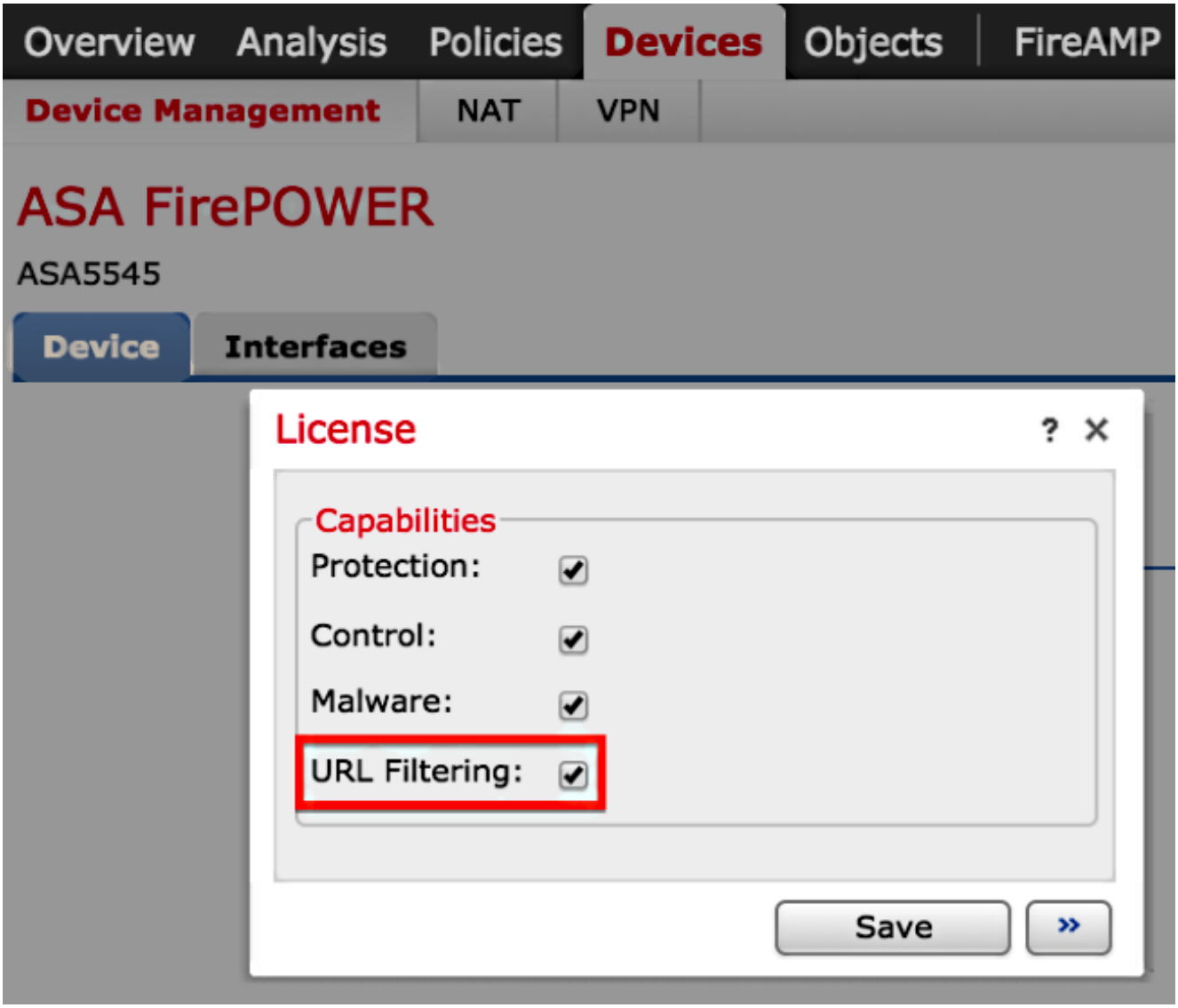


2. Перейдите к странице **Devices> Device Management** и проверьте, применена ли лицензия Фильтрации URL-адресов на устройство, которое контролирует трафик.

3. Если лицензия Фильтрации URL-адресов не применена на устройство, выберите **значок карандаша** для редактирования параметров настройки. Значок расположен рядом с именем устройства.



4. Можно включить лицензию Фильтрации URL-адресов на устройстве от вкладки **Devices**.



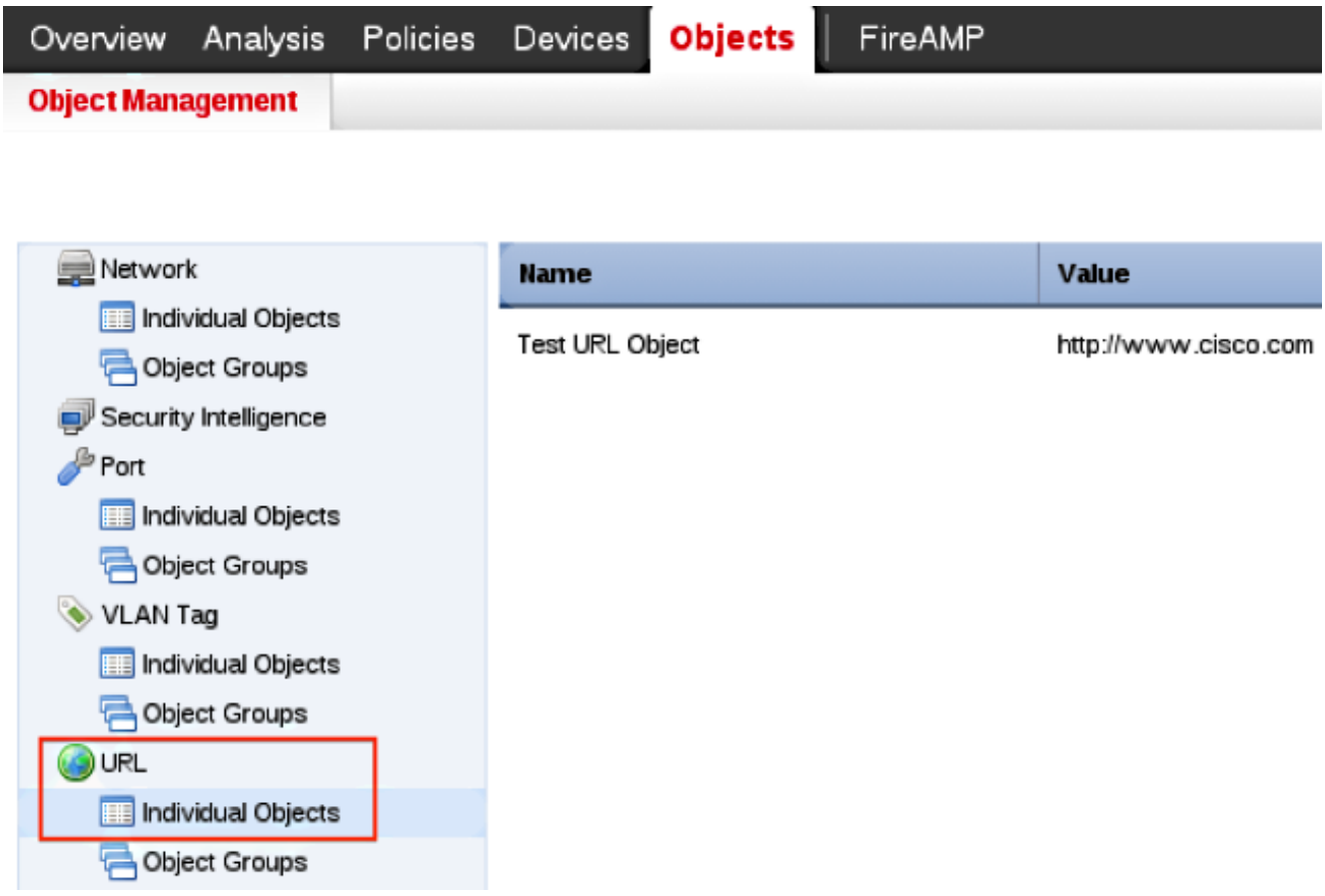
5. После того, как вы включаете лицензию и сохраняете ваши изменения, также необходимо нажать **Apply Changes** для применения лицензии на управляемое устройство.

Исключение определенного узла от заблокированной категории URL

Центр управления FireSIGHT не позволяет вам иметь локальную оценку URL, которые отвергают предоставленные оценки категории Sourcefire по умолчанию. Для выполнения этой задачи необходимо использовать Политику контроля доступа. Эти инструкции описывают, как использовать объект URL в правиле Управления доступом для исключения определенного узла из блочной категории.

1. Перейдите к странице **Objects> Object Management**.

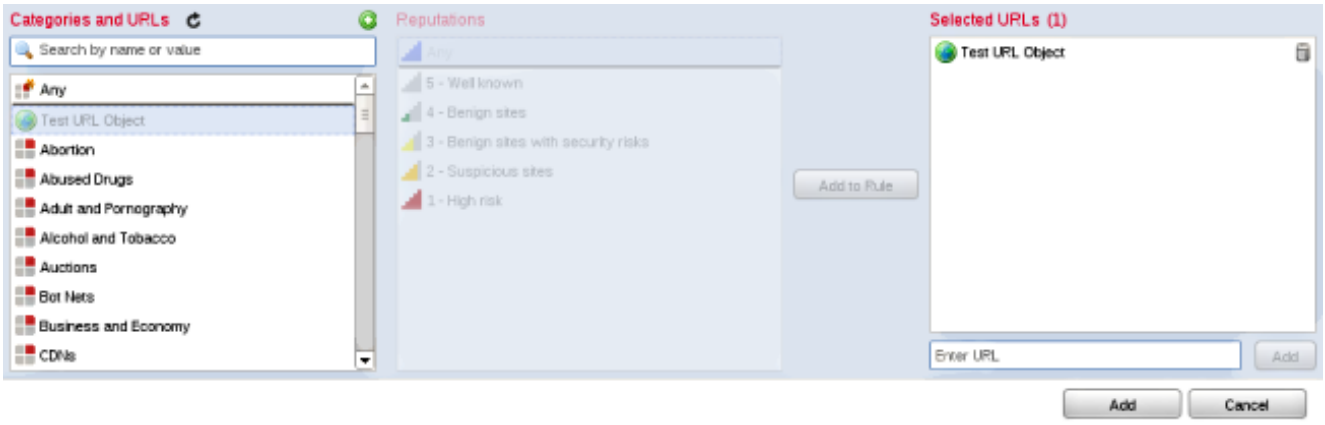
2. Выберите **Individual Objects for URL** и нажмите кнопку **Add URL**. Окно **URL Objects** появляется.



3. После того, как вы сохраняете изменения, перешли к **Политике> Управление доступом** и нажимаете **значок карандаша** для редактирования Политики контроля доступа.

4. Выберите **Add Rule**.

5. Добавьте свой Объект URL к правилу с **Позволять** действием и разместите его выше правила Категории URL, так, чтобы его действие правила было оценено сначала.



6. После добавления правила выберите **Save и Apply**. Это сохраняет новые изменения и применяет Политику контроля доступа к управляемым устройствам.

Проверка

Для Проверяют или информация об Устранении неполадок, ссылаются на статью **Troubleshoot Issues with URL Filtering on FireSIGHT System**, связанную в Разделе связанных сведений.

Устранение неполадок

Для Проверяют или информация об Устранении неполадок, ссылаются на статью **Troubleshoot Issues with URL Filtering on FireSIGHT System**, связанную в Разделе связанных сведений.

Дополнительные сведения

- Решите проблемы с фильтрацией URL-адресов в системе FireSIGHT
- Cisco Systems – техническая поддержка и документация