Решите проблемы с фильтрацией URL-адресов в системе FireSIGHT

Содержание

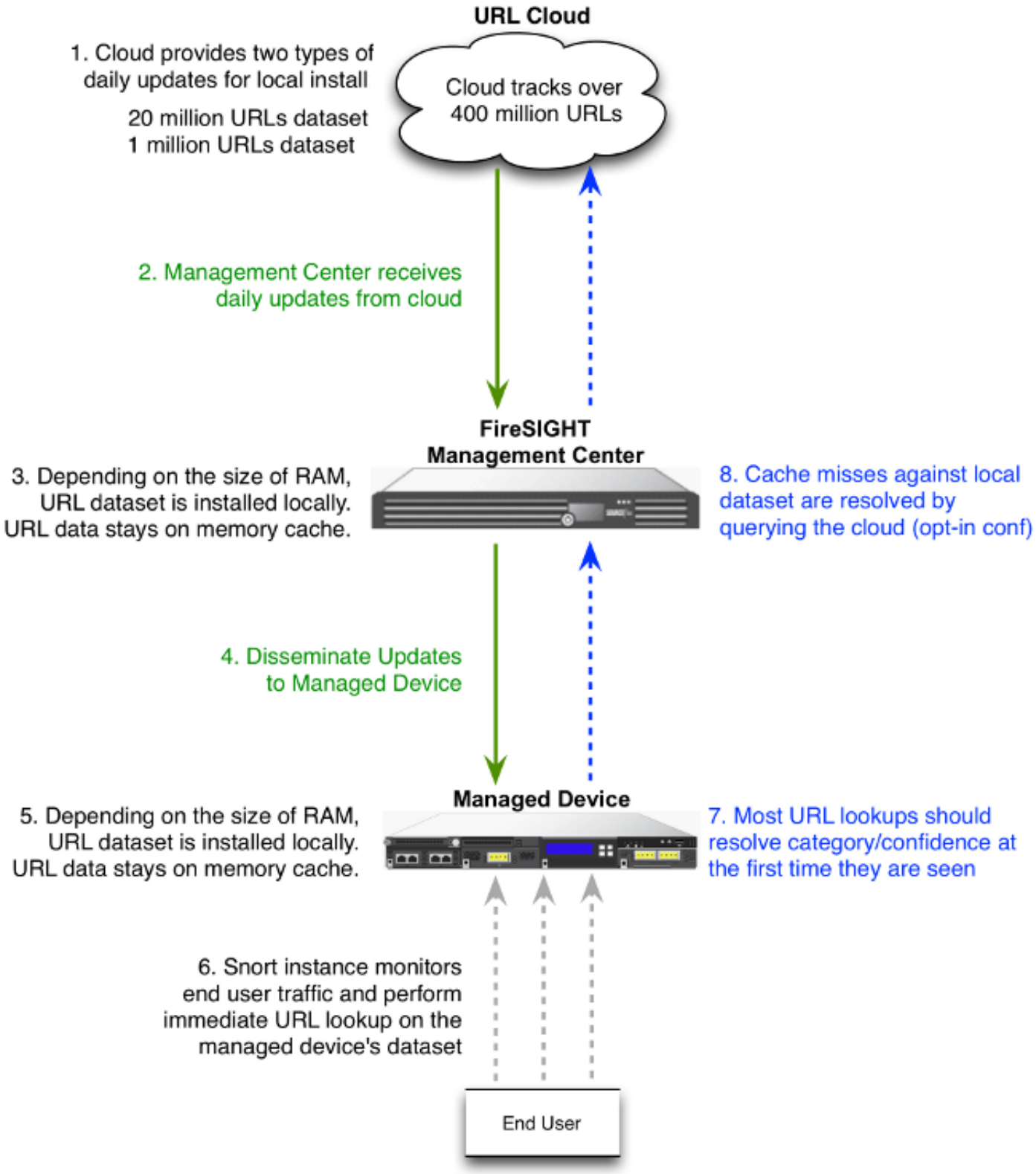
Введение

Этот документ описывает общие проблемы с фильтрацией URL-адресов. Функция фильтрации URL-адресов на Центре управления FireSIGHT категоризирует трафик отслеживаемых хостов и позволяет вам писать условие в правиле управления доступом на основе репутации.

Процесс поиска фильтрации URL-адресов

Для ускорения процесса поиска URL фильтрация URL-адресов предоставляет набор данных, который установлен в Системе Огневой мощи локально. Зависящий от количества памяти (ОЗУ), доступное на устройстве, существует два типа наборов данных:

Тип набора данных	Требования к памяти	
	На версии 5.3	На Версии 5.4 или выше
20 миллионов наборов данных URL	>2GB	>3.4 ГБ
1 миллион наборов данных URL	<= 2GB	<= 3.4 ГБ



Облачные проблемы с подключением

Шаг 1: Проверьте лицензии

Лицензия установлена?

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.

Лицензия истекается?

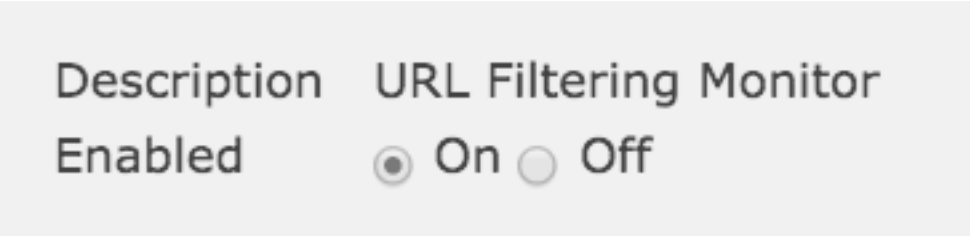
Если лицензия Фильтрации URL-адресов истекает, правила управления доступом с категорией и основанными на репутации условиями URL прекращают фильтровать URL, и Центр управления FireSIGHT больше не связывается с облачным сервисом.

> **Совет:** Считайте Фильтрацию URL-адресов на Примере Конфигурации системы FireSIGHT , чтобы изучить, как активировать опцию Фильтрации URL-адресов в Системе FireSIGHT и применить лицензию Фильтрации URL-адресов на управляемое устройство.

Шаг 2: Проверьте предупреждения состояния

Модуль мониторинга Фильтрации URL-адресов отслеживает связь между Центром управления FireSIGHT и облаком Cisco, где система получает свою фильтрацию URL-адресов (категория и репутация) данные для обычно посещаемых URL. Модуль мониторинга Фильтрации URL-адресов также отслеживает связь между Центром управления FireSIGHT и любыми управляемыми устройствами, где вы включили фильтрацию URL-адресов.

Для включения Модуля мониторинга Фильтрации URL-адресов перейдите **к Странице конфигурации Политики в области охраны здоровья**, выберите **URL Filtering Monitor**. Нажмите кнопку с зависимой фиксацией **On** для опции **Enabled** для включения использования модуля для тестирования состояния здоровья. Необходимо применить политику в области охраны здоровья к Центру управления FireSIGHT, если вы хотите, чтобы ваши параметры настройки вступили в силу.



- **Важное Предупреждение**: Если Центр управления FireSIGHT не в состоянии успешно связываться с или получать обновление из облака, классификация статусов для того модуля изменяется на *Важный*.
- **Предупреждение Предупреждения**: Если Центр управления FireSIGHT успешно связывается с облаком, состояние модуля изменяется на *Предупреждение*, если Центр управления не может выдвинуть новые данные фильтрации URL-адресов к своим управляемым устройствам.

Шаг 3: Проверьте параметры настройки DNS

Центр управления FireSIGHT связывается с этими серверами во время облачного поиска:

```
database.brightcloud.com
```

service.brightcloud.com

Как только вы удостоверяетесь, что оба сервера позволены на межсетевом экране, выполняют эти команды на Центре управления FireSIGHT и проверяют, в состоянии ли Центр управления решить названия:

admin@FireSIGHT:~$ **sudo nslookup database.brightcloud.com** admin@FireSIGHT:~$ **sudo nslookup service.brightcloud.com**

Шаг 4. : Проверьте подключение к требуемым портам

Системы FireSIGHT используют порты 443/HTTPS и 80/HTTP для передачи с облачным сервисом.

Как только вы подтверждаете, что Центр управления в состоянии выполнить успешный `nslookup`, проверьте подключение к порту 80 и порту 443 с `telnet`. В то время как неизвестные запросы URL сделаны в `service.brightcloud.com` в порту 80, база данных URL загружена `database.brightcloud.com` в порту 443.

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

Эти выходные данные являются примером успешного `соединения TELNET` к `database.brightcloud.com`.

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

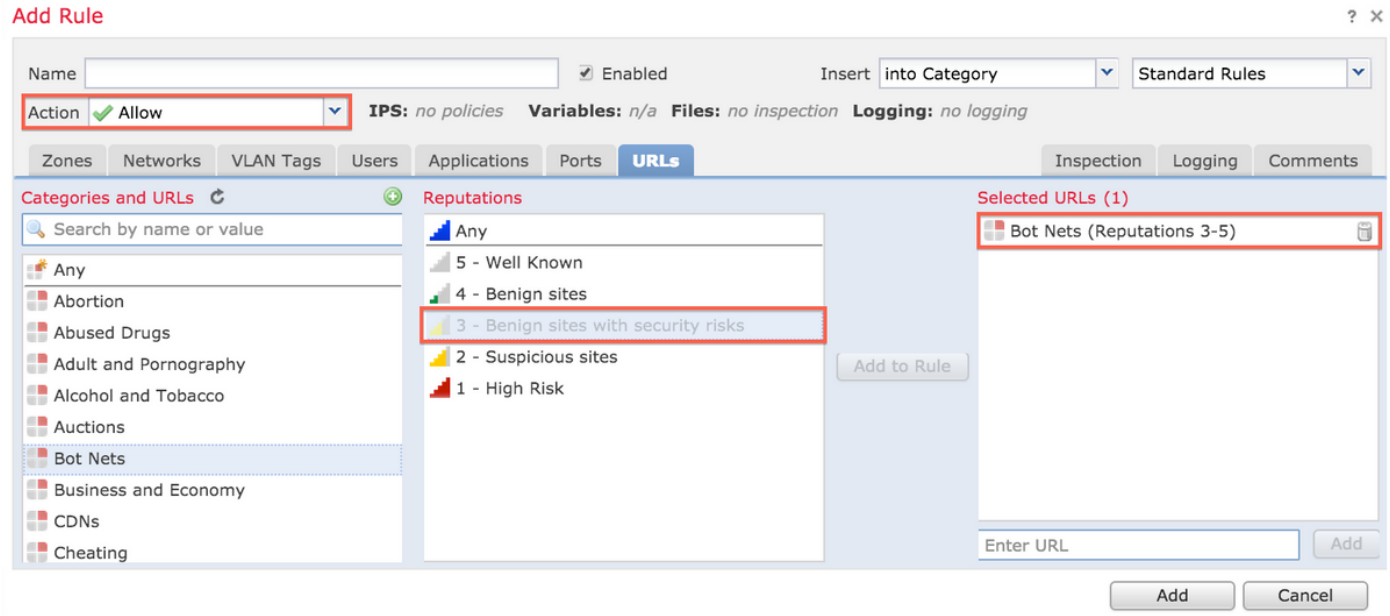
Управление доступом и проблемы Miscategorization

Проблема 1: URL с Отменявшим Уровнем Репутации Позволен / Заблокированный

Если вы замечаете, что URL позволен или заблокирован, но вы не выбрали уровень репутации того URL в вашем Правиле Управления доступом, считайте этот раздел, чтобы понять, как работает правило фильтрации URL-адресов.

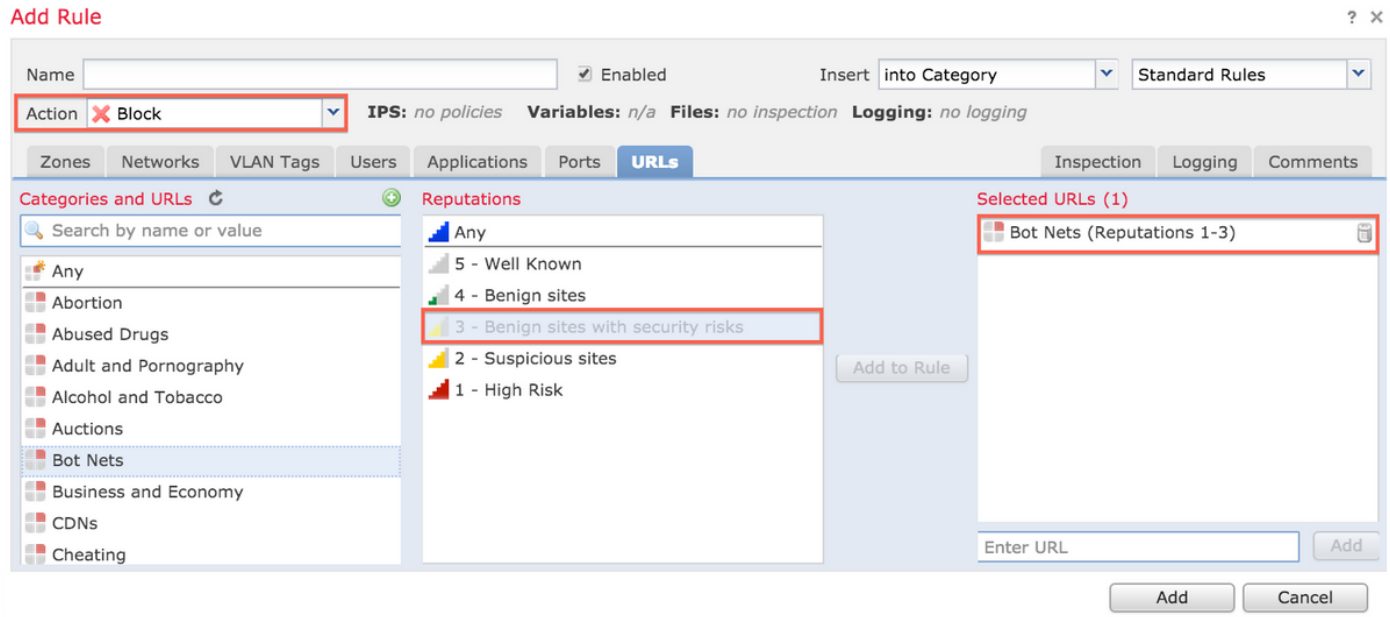
Действие правила, Позволяют

При создании правила **Позволить** трафик на основе уровня репутации выбор уровня репутации также выбирает все уровни репутации, менее безопасные, чем уровень, который вы первоначально выбрали. Например, при настройке правила позволить *Мягкие узлы с угрозами безопасности* (уровень 3) это также автоматически позволяет *Мягкие узлы* (уровень 4) и *Известный* (уровень 5) узлы.



Действие правила является Блоком

При создании правила **Заблокировать** трафик на основе уровня репутации выбор уровня репутации также выбирает все уровни репутации, более серьезные, чем уровень, который вы первоначально выбрали. Например, при настройке правила заблокировать *Мягкие Сайты с угрозами безопасности* (уровень 3) это также автоматически блокирует *Подозрительные сайты* (уровень 2) и *Высокий риск* (уровень 1) узлы.



Матрица выбора URL

Выбранный уровень репутации	Выбранное действие правила				
	Высокий риск	**Подозрительный узел**	**Мягкий узел с угрозой безопасности**	**Мягкий узел**	**Известны**
1 - Высокий риск	,	Allow	Allow	Allow	Allow
2 - Подозрительные узлы		,	Allow	Allow	Allow
3 - Мягкие узлы с угрозой безопасности			,	Allow	Allow

4 - Мягкие узлы , Allow
5 - Известный ,

Проблема 2: Подстановочный знак не Работает в Правиле Управления доступом

Система FireSIGHT не поддерживает спецификацию подстановочного знака в условии URL. Это условие могло бы быть не в состоянии предупреждать на `cisco.com`.

`*cisco*.com`
Кроме того, неполный URL мог бы совпасть против другого трафика, который вызывает нежелательный результат. При определении отдельных URL в условиях URL необходимо тщательно рассмотреть другой трафик, на который можно было бы влиять. Например, рассмотрите сценарий, где вы хотите явно заблокировать `cisco.com`. Однако подстрока, совпадающая со средствами, что блокирующийся `cisco.com` также блокирует `sanfrancisco.com`, который не мог бы быть вашим намерением.

При вводе URL введите доменное имя и опустите информацию о субдомене. Например, введите `cisco.com`, а не `www. cisco . com`. Когда вы используете `cisco.com` в **Позволять** правиле, пользователи могли перейти к любому из этих URL: `http://cisco.com`
`http://cisco.com/newcisco`
`http://www.cisco.com`

Проблема 3: Категория URL и Репутация не Заполнены

Если URL не находится в локальной базе данных, и это первоначально, что URL замечен в трафике, категория или репутация не могли бы быть заполнены. Это означает, что первоначально неизвестный URL замечен, он не совпадает с правилом AC. Иногда поиски URL для обычно посещаемых URL не могли бы решить в первоначально, URL замечен. Эта проблема закреплена на Версии 5.3.0.3, 5.3.1.2, и 5.4.0.2, 5.4.1.1.

Дополнительные сведения

- Конфигурация фильтрации URL-адресов в системе FireSIGHT
- Cisco Systems – техническая поддержка и документация