Содержание

Введение

Этот документ описывает, как решить проблемы с обновлениями Канала Интеллектуальной информационной безопасности. Канал Интеллектуальной информационной безопасности состоит из нескольких регулярно обновляемых списков IP-адресов, которые имеют плохие репутации, как определено Интеллектуальной информационной безопасностью Cisco Talos и исследовательской группой (Talos). Важно поддержать интеллектуальный канал регулярно обновляемым так, чтобы Система Cisco FireSIGHT могла использовать современные данные для фильтрации сетевого трафика.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Центр управления Cisco FireSIGHT
- Канал интеллектуальной информационной безопасности

Используемые компоненты

Сведения в этом документе основываются на Центре управления Cisco FireSIGHT, который работает под управлением ПО версии 5.2 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.

Проблема

Сбой обновления Канала Интеллектуальной информационной безопасности происходит.

Можно проверить сбой или через веб-GUI или через CLI (объясненный далее в разделах, которые придерживаются).

Проверьте проблему от веб-GUI

Когда сбой обновления Канала Интеллектуальной информационной безопасности происходит, предупреждения состояния показов Центра управления FireSIGHT.

Проверьте проблему от CLI

Для определения основной причины сбоя обновления с Каналом Интеллектуальной информационной безопасности введите эту команду в CLI Центра управления FireSIGHT:

Поиск любого из этих предупреждений в сообщениях:

Решение

Чтобы устранить данную проблему, проделайте следующие действия:

1. Проверьте, что *intelligence.sourcefire.com* узел активен. Перейдите к https://intelligence.sourcefire.comin браузер. Необходимо получить улыбающуюся поверхность, которая указывает, что узел является оперативным.

2. Обратитесь к CLI Центра управления FireSIGHT через Secure Shell (SSH).

3. Пропингуйте *intelligence.sourcefire.com* от Центра управления FireSIGHT:

   Необходимо получить выходные данные, подобные этому:

   Если вы не получаете ответ, подобный показанному, то у вас могла бы быть исходящая проблема с подключением, или у вас нет маршрута к *intelligence.sourcefire.com.*

4. Решите имя хоста для *intelligence.sourcefire.com*:

   Необходимо получить ответ, подобный этому:

   Примечание: Вышеупомянутые выходные данные используют Google Public Domain Name System (DNS) Сервер как пример. Выходные данные зависят от параметров настройки DNS, которые настроены в **Системе> Локальный> Конфигурация** под *Сегментом сети*. Если вы не получаете ответ, подобный показанному, то гарантируете, что параметры настройки DNS корректны.**Внимание:** Сервер использует циклическую схему IP-адреса для распределения нагрузки, отказоустойчивости и времени работы без сбоев. Поэтому IP-адреса могли бы измениться, и Cisco рекомендует, чтобы межсетевой экран был настроен с *CNAME* вместо IP-адреса.
5. Проверьте подключение к *intelligence.sourcefire.com* с использованием Telnet:

   Необходимо получить выходные данные, подобные этому:

Примечание: Если вы в состоянии завершить действие второе успешно, но неспособны к Telnet к *intelligence.sourcefire.com* по порту 443, у вас могло бы быть правило межсетевого экрана что порт 443 блоков, исходящий для *intelligence.sourcefire.com*.

6. Перейдите к **Системе> Локальный> Конфигурация** и проверьте параметры прокси *Конфигурации прокси вручную* под *Сегментом сети*.
   Примечание: Если этот прокси делает контроль Уровня защищенных сокетов (SSL), необходимо поместить в место обходное правило, которое обходит прокси для *intelligence.sourcefire.com*.
7. Тест, можно ли выполнить *HTTP-запрос GET* против *intelligence.sourcefire.com*:

   Примечание: Улыбающаяся поверхность в конце *вихревых* выходных данных команды указывает на успешное подключение.**Примечание:** При использовании прокси *вихревая* команда требует имени пользователя. Команда будет **завихрением-U <user>-vvk** https://intelligence.sourcefire.com. Кроме того, после ввода команды вам предлагают, вводят пароль прокси.
8. Проверьте, что Трафик HTTPS, который используется для загрузки канала Интеллектуальной информационной безопасности не проходит через SSL decryptor. Чтобы проверить, что никакая расшифровка SSL не происходит, проверьте информацию о Серверном сертификате в выходных данных от Шага 6. Если Серверный сертификат не совпадает, который отобразился в примере, который придерживается, то у вас мог бы быть SSL decryptor, который оставляет сертификат. Если трафик проходит через SSL decryptor, необходимо обойти весь трафик, который переходит *к intelligence.sourcefire.com*.

   Примечание: Расшифровка SSL должна быть обойдена для Канала Интеллектуальной информационной безопасности, потому что SSL decryptor передает Центру управления FireSIGHT неизвестный сертификат в подтверждении связи SSL. Сертификат, который передается Центру управления FireSIGHT, не подписан доверяемым Sourcefire CA, таким образом, соединение недоверяемо.

Дополнительные сведения

- Автоматический сбой обновления загрузки на центре управления FireSIGHT
- Адреса нужного сервера для операций Усовершенствованной вредоносной защиты (AMP)
- Требуемые коммуникационные порты для работы системы FireSIGHT
- Cisco Systems – техническая поддержка и документация