Содержание

Введение

Этот документ описывает Cisco Security репутация ИНТЕЛЛЕКТА/IP-АДРЕСА и конфигурация помещения в черный список IP (Блокирование) при использовании пользовательского/автоматического канала низкого IP-адреса доброй славы.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание ASA (Устройство адаптивной безопасности) межсетевой экран, ASDM (Менеджер устройств адаптивной безопасности (ASDM))
- Знание устройства FirePOWER

Примечание: Фильтрация Интеллектуальной информационной безопасности требует лицензии Защиты.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Модули ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, 5508-X ASA, 5516-X ASA) работающий под управлением ПО версии 5.4.1 и выше
- Модуль ASA FirePOWER (5515-X ASA, 5525-X ASA, 5545-X ASA, 5555-X ASA) работающий под управлением ПО версии 6.0.0 и выше

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.

Общие сведения

Интеллект Cisco Security включает несколько регулярно обновляемых наборов IP-адресов, которые полны решимости иметь плохую репутацию Cisco Команда TALOS. Если какие-либо нежелательные действия инициируются из тех IP-адресов, таких как сообщения со спамом, вредоносное ПО, фишинговые атаки и т.д., команда TALOS Cisco определяет низкую репутацию.

Интеллектуальный канал IP-безопасности Cisco отслеживает базу данных Атакующих, Богона, Ботов, CnC, Dga, ExploitKit, Вредоносного ПО, Open_proxy, Open_relay, Фишинга, Ответа, Спама, Подозрительного. Модуль огневой мощи действительно предоставляет возможность создавать пользовательский канал низкого IP-адреса доброй славы.

Обзор канала Интеллектуальной информационной безопасности

Вот некоторые дополнительные сведения о типе наборов IP-адреса, которые могут быть классифицированы как другие категории в Интеллектуальной информационной безопасности.

Атакующие: Набор IP-адресов, которые непрерывно просматривают для уязвимостей или пытаются использовать другие системы.

Вредоносное ПО: Набор IP-адресов, которые пытаются распространиться вредоносное ПО или активно нападают на любого, кто посещает их.

Фишинг: Набор хостов, которые активно пытаются обмануть конечных пользователей во ввод конфиденциальной информации как имена пользователя и пароли.

Спам: Набор хостов, которые были определены как источник передачи сообщений электронной почты спама.

Боты: Набор хостов, которые активно участвуют как часть ботнета и управляются известным контроллером сети роботов.

CnC: Набор хостов, которые были определены как серверы управления для известного Ботнета.

OpenProxy: Набор хостов, которые, как известно, выполняют Открытые Вебы - прокси и предлагают анонимные услуги просмотра веб - ресурсов.

OpenRelay: Набор хостов, которые, как известно, предлагают анонимные услуги передачи электронной почты, используемые атакующими фишинга и спамом.

TorExitNode: Набор хостов, которые, как известно, предлагают выходные услуги узла для

сети Tor Anonymizer.

Bogon: Набор IP-адресов, которые не выделены, но передают трафик.

Подозрительный: Набор IP-адресов, которые отображают подозрительную операцию и находятся под активным расследованием.

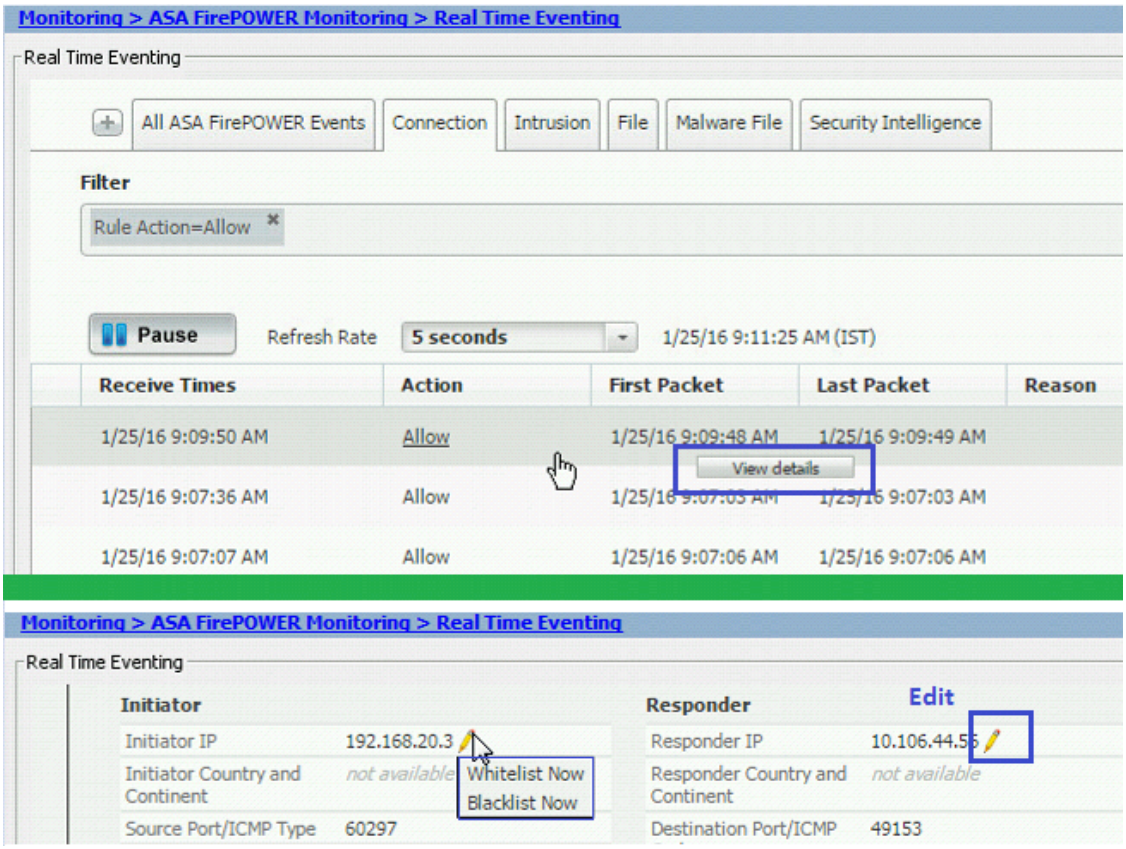
Ответ: Набор IP-адресов, которые неоднократно наблюдались занятые подозрительным или злонамеренным поведением.

Вручную добавьте IP-адреса к Глобальному Черному списку и Глобальному Белому списку

Модуль огневой мощи позволяет вам добавлять определенные IP-адреса к Глобальному Черному списку, когда вы знаете, что они - часть некоторых нежелательных действий. IP-адреса могут также быть добавлены к Глобальному Белому списку, если вы хотите позволить трафик определенным IP-адресам, которые заблокированы IP-адресами черного списка. Если вы добавляете какой-либо IP-адрес к Global-Blacklist/Global-Whitelist, он сразу вступает в силу без потребности применить политику.

Для добавления IP-адреса к Global-Blacklist/Глобальному Белому списку перейдите к **Мониторингу> Мониторинг ASA FirePOWER> Оперативная Обработка событий**, парение мышь на событиях подключения и выберите **View Details**.

Можно добавить или источник или IP - адрес назначения к Global-Blacklist/Глобальный Белый список. Щелкните **по кнопке Edit** и выберите **Whitelist Now/Blacklist Now** для добавления IP-адреса к соответствующему списку, как показано в образе.



Чтобы проверить, что источник или IP - адрес назначения добавлены к Global-Blacklist/Глобальный Белый список, перейдите к **Конфигурации> Конфигурация Огневой мощи ASA>> Security Управления объектами Интеллект> Списки сетей и Подача** и отредактируйте **Global-Blacklist/Глобальный Белый список**. Можно также использовать кнопку delete для удаления любого IP-адреса из списка.

Создайте Пользовательский список IP-адреса черного списка

Огневая мощь позволяет вам создавать пользовательский список СЕТИ/IP-АДРЕСОВ, который может использоваться в помещении в черный список (блокирования). Существует три опции, чтобы сделать это:

1. Вы можете записать IP-адреса в текстовый файл (Один IP-адрес на линию) и можете загрузить файл к Модулю Огневой мощи. Для загрузки файла перейдите к **Конфигурации> конфигурация ASA FirePOWER>> Security Управления объектами Интеллект> Списки сетей и Подача** и затем **нажмите Add Списки сетей и Подачу** **Name:** Задайте название Пользовательского списка. **Введите :** от выпадающего списка. **Список загрузки:** Выберите **Browse** для определения местоположения текстового файла в системе. Выберите **опцию Upload** для загрузки файла.
2. Можно использовать любую стороннюю базу данных IP для пользовательского списка, для которого модуль Огневой мощи связывается с сервером третьей стороны для выборки Списка IP-адресов. Для настройки этого перейдите к **Конфигурации> конфигурация ASA FirePOWER>> Security Управления объектами Интеллект> Списки сетей и Подача** и затем **нажмите Add Списки сетей и Подачу**

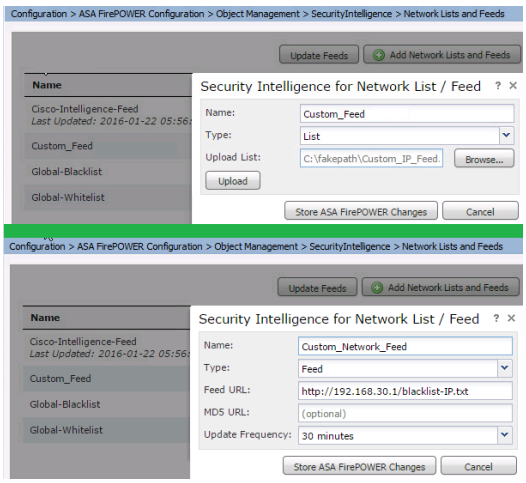
Name: Задайте название Пользовательского Канала.

Введите : Выберите **опцию Feed** от выпадающего списка.

URL канала: Задайте URL сервера, к которому модуль Огневой мощи должен подключить и загрузить канал.

URL MD5: Задайте значение хеш-функции для проверки пути URL Канала.

Частота обновления: Задайте временной интервал в который системное подключение к серверу Канала URL.



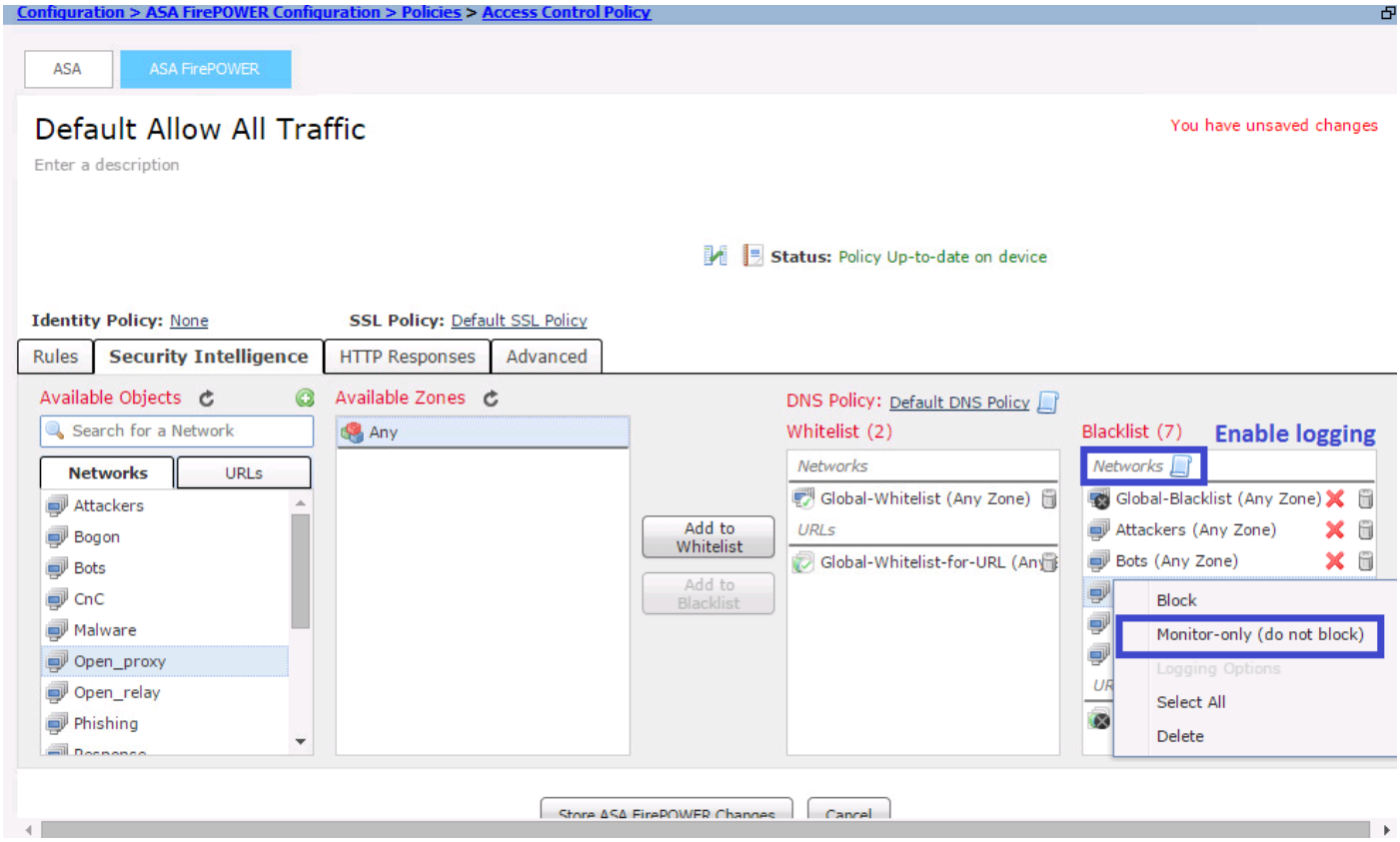
Настройте интеллектуальную информационную безопасность

Для Настройки Интеллектуальной информационной безопасности перейдите к **Конфигурации> Конфигурация Огневой мощи ASA> Политика> Политика контроля доступа,** выберите вкладку **Security Intelligence**.

Выберите канал из Сетевого Доступного Объекта, переместитесь для **Белого списка** столбца **Blacklist /** для разрешения соединения со злонамеренным IP-адресом.

Можно нажать значок и enable logging, как задано в образе.

Если вы просто хотите генерировать событие для злонамеренных IP - подключений вместо того, чтобы блокировать соединение, затем щелкнуть правой кнопкой мыши на канале, выбрать**, Monitor-only (не блокируйтесь)**, как показано в образе:

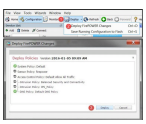


Выберите опцию Store ASA Firepower Changes для сохранения изменений политики AC.

Разверните политику контроля доступа

Для изменений для вступления в силу необходимо развернуть Политику контроля доступа. Перед применением политики посмотрите индикацию это, является ли Политика контроля доступа устаревшей на устройстве или нет.

Для развертывания изменений на датчике нажмите **Deploy** и выберите**, Deploy FirePOWER Changes** тогда выбирают **Deploy** во всплывающем окне для развертывания изменений.

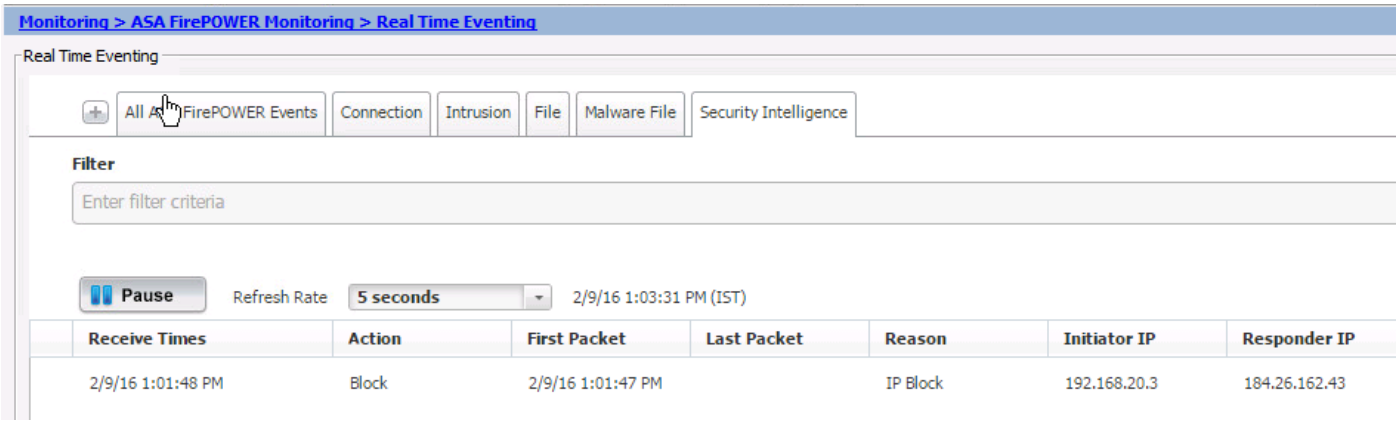


Примечание: В версии 5.4.x, Для применения Политики доступа к датчику необходимо нажать **Apply ASA**

Примечание: Перейдите к **Мониторингу> Мониторинг Огневой мощи ASA> Статус Задачи.** Гарантируйте, что задача должна завершить для применения изменений конфигурации.

Интеллектуальная информационная безопасность? s события Monitoring

Для наблюдения Интеллектуальной информационной безопасности Модулем Огневой мощи перейдите к **Мониторингу> Мониторинг Огневой мощи ASA> Оперативная Обработка событий**. Выберите вкладку **Security Intelligence**. Это разоблачит события как показано в образе:

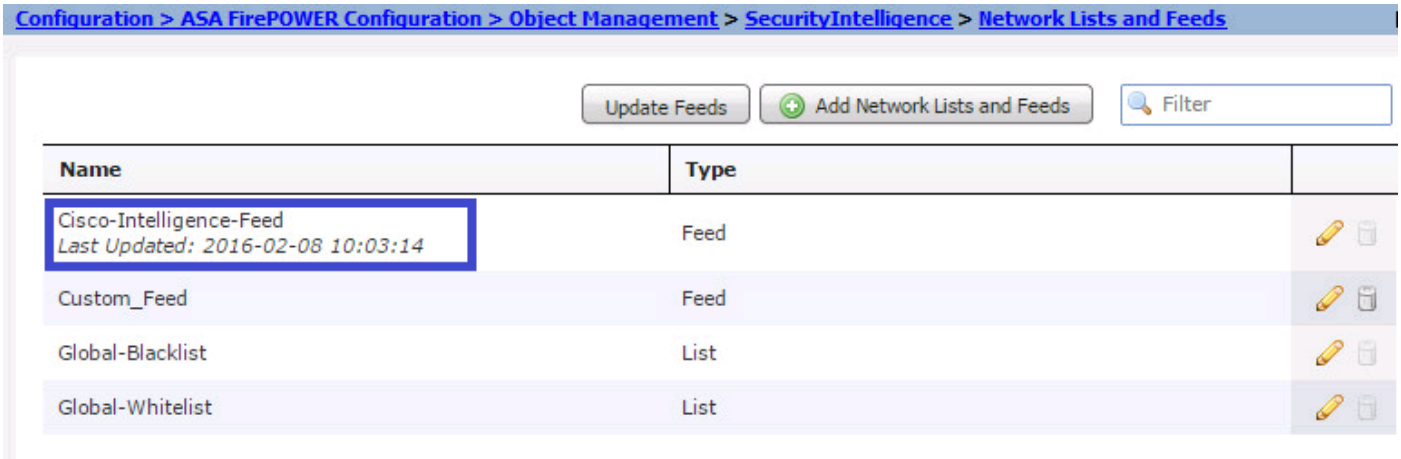


Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Чтобы гарантировать, что Подача Интеллектуальной информационной безопасности актуальна, перейдите к **Конфигурации> конфигурация ASA FirePOWER>> Security Управления объектами Интеллект> Списки сетей и Подача** и проверьте время, когда канал обновился. Можно выбрать кнопку Edit для установки частоты обновления канала.



Гарантируйте, что развертывания Политики контроля доступа завершили успешно.

Контролируйте интеллектуальную информационную безопасность, чтобы видеть, блокируется ли трафик или нет.

Дополнительные сведения

- **Cisco ASA Краткое руководство по началу работы модуля FirePOWER**
- **Cisco Systems – техническая поддержка и документация**