Центр управления FirePOWER отображает некоторые события TCP - подключения в неверном направлении

Содержание

Введение

Этот документ описывает причины и шаги смягчения для Центра управления FirePOWER (FMC) , отображающего события TCP - подключения в обратном направлении, где IP Инициатора является IP - сервером TCP - подключения, и IP Респондента является IP-адресом клиента TCP - подключения.

> **Примечание:** Существуют множественные причины для возникновения таких событий. Эти документы объясняют наиболее распространенную причину этого признака.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Технология FirePOWER
- Базовые знания об Устройстве адаптивной защиты (ASA)
- Понимание механизма синхронизации Протокола TCP

Используемые компоненты

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

- Защита Угрозы Огневой мощи ASA (5506X/5506H-X/5506W-X, 5508-X ASA, 5516-X ASA), который работает под управлением ПО версии 6.0.1 и позже

- Защита Угрозы Огневой мощи ASA (5512-X, 5515-X, 5525-X ASA, 5545-X ASA, 5555-X ASA, FP9300, FP4100), который работает под управлением ПО версии 6.0.1 и позже
- ASA с модулями Огневой мощи (5506X/5506H-X/5506W-X, 5508-X ASA, ASA, 5516-X, 5515-X, 5525-X ASA, 5545-X ASA, 5555-X ASA, 5585-X ASA), который выполняет Версии программного обеспечения 6.0.0 и позже
- Центр управления огневой мощи (FMC) Версия 6.0.0 и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, используемые в этом документе, запустились с ясной конфигурации (по умолчанию). Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Общие сведения

В TCP - подключении **клиент** обращается к IP, который передает начальный пакет. Когда управляемое устройство (датчик или FTD) видит intial пакет TCP соединения, Центр управления FirePOWER генерирует событие подключения.

Устройствам, которые отслеживают состояние TCP - подключения, определили **время простоя**, чтобы удостовериться, что соединения, которые ошибочно не закрыты оконечными точками, не используют доступную память для длинных периодов времени. Время простоя по умолчанию для установленных TCP - подключений на FirePOWER составляет **три минуты**. TCP - подключение, который оставался простаивающим в течение трех минут или больше, не отслежен сенсором IPS FirePOWER.

Последующий пакет после таймаута рассматривается как новый поток TCP, и решение по перенаправлению взято согласно правилу, которое совпадает с этим пакетом. Когда пакет от сервера, IP сервера зарегистрирован как инициатор этого нового потока. Когда регистрация включена для правила, событие подключения генерируется на Центре управления FirePOWER.

> **Примечание:** Согласно настроенной политике, решение по перенаправлению для пакета, который прибывает после таймаута , отличается от решения для начального пакета TCP. Если настроенное действие по умолчанию является "Блоком", пакет отброшен.

Пример этого признака согласно снимку экрана ниже:

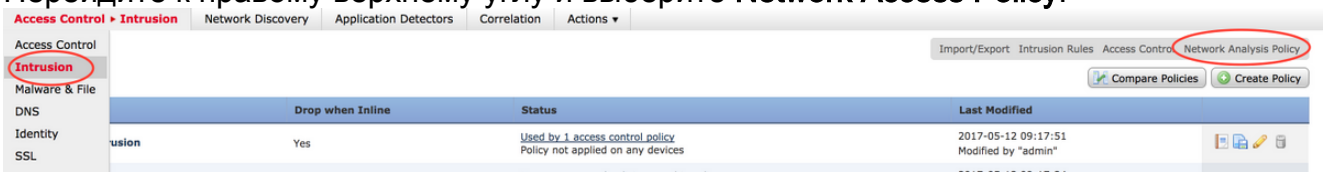
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

Решение

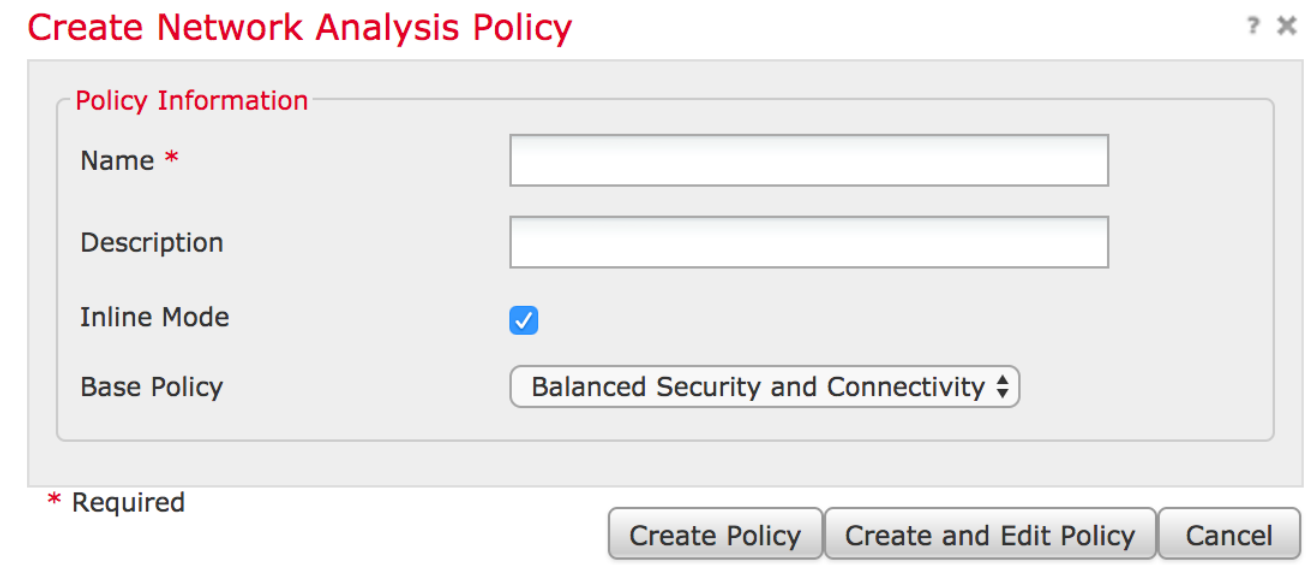
Вышеупомянутая проблема смягчена путем увеличения **Таймаута** TCP - подключений. В заказе изменяют таймаут,

1. Перейдите к **Политике> Управление доступом> Проникновение**.

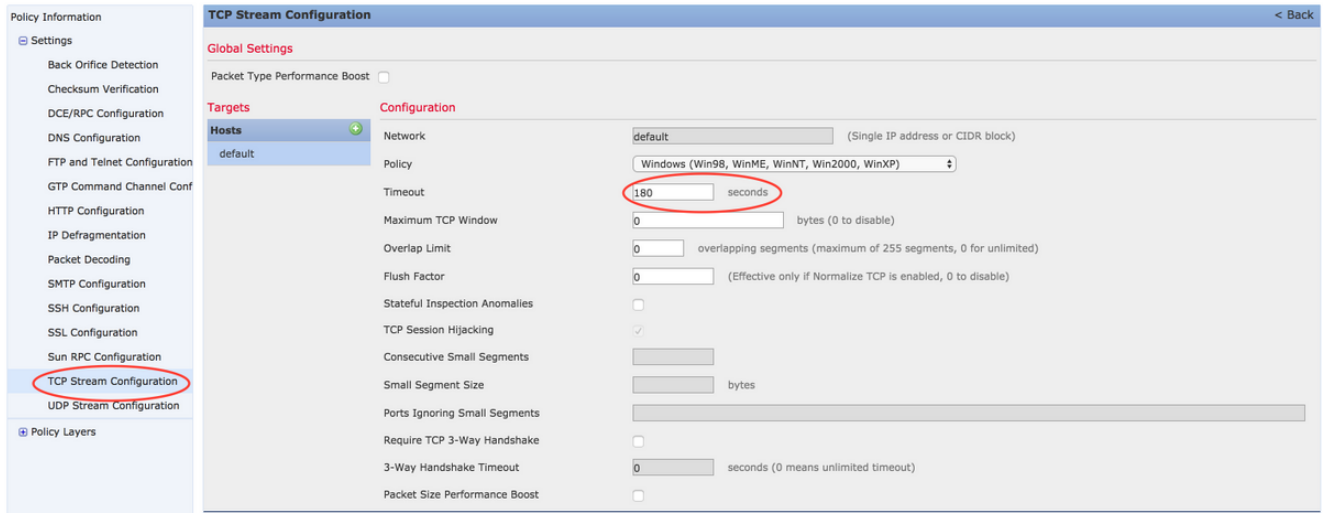
2. Перейдите к правому верхнему углу и выберите **Network Access Policy**.



3. Выберите **Create Policy**, выберите название и щелкните **по Create и Edit Policy**. Не модифицируйте **Основную Политику.**

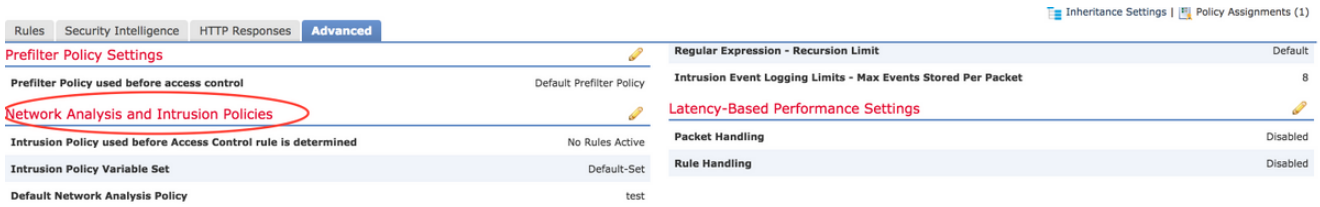


4. Разверните **Параметр настройки** и выберите **TCP Stream Configuration**.
5. Перейдите к разделу конфигурации и измените значение **Таймаута**, как желаемый.



6. Перейдите к **Политике> Управление доступом> Управление доступом**.
7. Выберите **опцию Edit** для редактирования , политика применилась к соответствующему управляемому устройству, или создайте новую политику.

8. Выберите **Вкладку Дополнительно** в Политике доступа.
9. Найдите **Политика Анализа сети и Проникновения** разделяет и щелкает **по Значку редактирования**.



10. От раскрывающегося меню **Аналитической Политики Сети по умолчанию** выберите политику, созданную в шаге 2.
11. Нажмите **OK** и **сохраните** изменения.
12. Щелкните по опции **Deploy** для развертывания полицейских на соответствующих manged устройствах.

Внимание. : Увеличение таймаута, как ожидают, вызовет более высокую загруженность памяти, FirePOWER должен отследить потоки, которые не закрыты оконечными точками в течение более длинного времени. Фактический прирост в загруженности памяти является другим для каждой уникальной сети, поскольку это зависит от того, сколько времени сетевые приложения поддерживают TCP - подключения простаивающими.

Заключение

Сравнительный тест каждой сети для времени простоя TCP - подключений является другим. Это полностью зависит от приложений, которые используются. Оптимальное значение должно быть установлено путем наблюдения, сколько времени сетевые приложения поддерживают TCP - подключения простаивающими. Для проблем, которые принадлежат сервисному модулю FirePOWER на Cisco ASA, когда оптимальное значение не может быть выведено, таймаут может быть настроен путем увеличения его в шагах до значения таймаута ASA.

Дополнительные сведения

- Краткое руководство по началу работы защиты угрозы огневой мощи Cisco для ASA
- Cisco Systems – техническая поддержка и документация
- Краткое руководство по началу работы огневой мощи ASA