Настройте конфигурацию политики и подписи проникновения в модуле огневой мощи (менеджмент на коробке)

Содержание

Введение

Этот документ описывает Систему предотвращения вторжений (IPS) / Система обнаружения проникновения (IDS) функциональность модуля FirePOWER и различных элементов Политики Проникновения, которые вырабатывают политику обнаружения в Модуле FirePOWER.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

* Знание межсетевого экрана Устройства адаптивной защиты (ASA), Менеджера устройств

адаптивной безопасности (ASDM) (ASDM).

* Знание устройства FirePOWER.

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 данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Общие сведения

IDS/IPS FirePOWER разработан, чтобы исследовать сетевой трафик и определить любые злонамеренные образцы (или подписи), которые указывают на атаку сети/системы. Модуль FirePOWER работает в режиме IDS, если стратегия обслуживания ASA еще в частности настроена в режиме отслеживания (разнородном), это работает во Встроенном режиме.

IPS/IDS FirePOWER является основанным на подписи подходом обнаружения. FirePOWERmodule в режиме IDS генерирует предупреждение, когда подпись совпадает с вредоносным трафиком, тогда как модуль FirePOWER в режиме IPS генерирует аварийный и блочный вредоносный трафик.

> **Примечание:** Гарантируйте, что Модуль FirePOWER должен иметь**, Защищают** лицензию для настройки этой функциональности. Для проверки лицензии перейдите к **Конфигурации> конфигурация ASA FirePOWER> Лицензия.**

!--- конфигурацию

Шаг 1. Настройте политику проникновения

Шаг 1. 1. Создайте политику проникновения

Чтобы настроить Политику Проникновения, войдите Менеджеру устройств адаптивной безопасности (ASDM) (ASDM) и выполнить эти шаги:

Шаг 1. Перейдите к **Конфигурации> конфигурация ASA FirePOWER> Политика> Политика Проникновения> Политика Проникновения**.

Шаг 2. Нажмите **создать политику**.

Шаг 3. Введите **имя** политики проникновения.

Шаг 4. . Введите **описание** (дополнительной) политики проникновения.

Шаг 5. . Задайте **Отбрасывание когда** опция **Inline**.

Шаг 6. Выберите **Base Policy** из выпадающего списка.

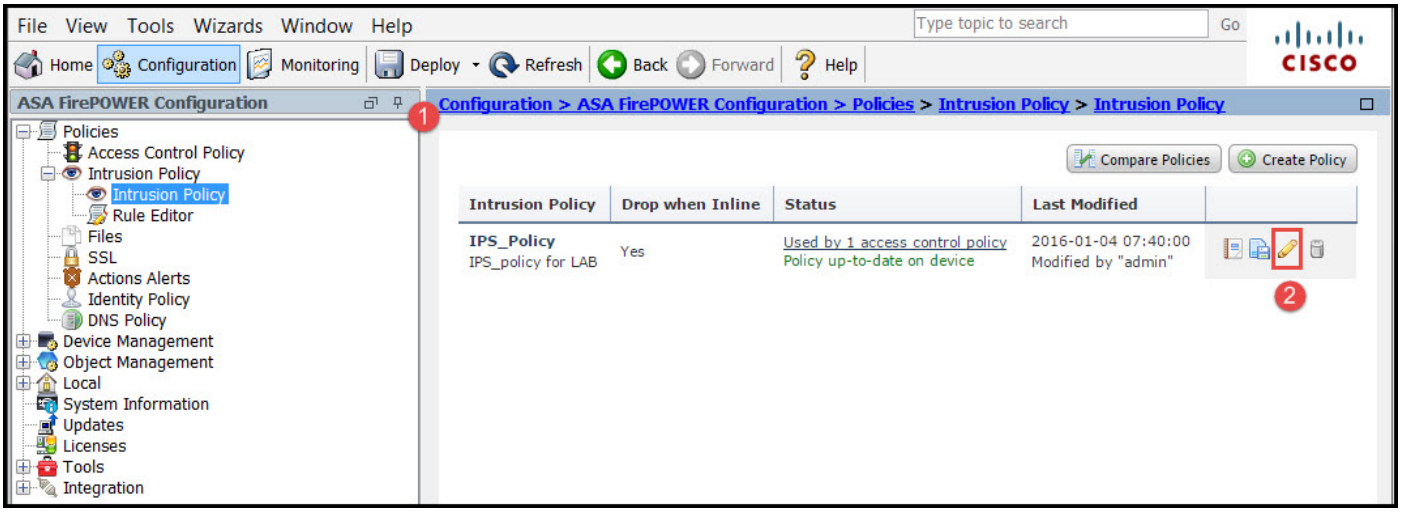
Шаг 7. Нажмите **Create Policy** для завершения создания Политики Проникновения.

> **Совет:** Отбрасывание, когда опция Inline крайне важна для определенных сценариев , когда датчик настроен во Встроенном режиме и это требуется не отбросить трафик даже при том, что это совпадает с подписью, которая имеет действие сброса.

Можно заметить, что политика настроена, однако, она не применена ни к какому устройству.

Шаг 1. 2. Модифицируйте политику проникновения

Для изменения Политики Проникновения перейдите к **Конфигурации> конфигурация ASA FirePOWER> Политика> Политика Проникновения> Политика Проникновения** и выберите **опцию Edit**.



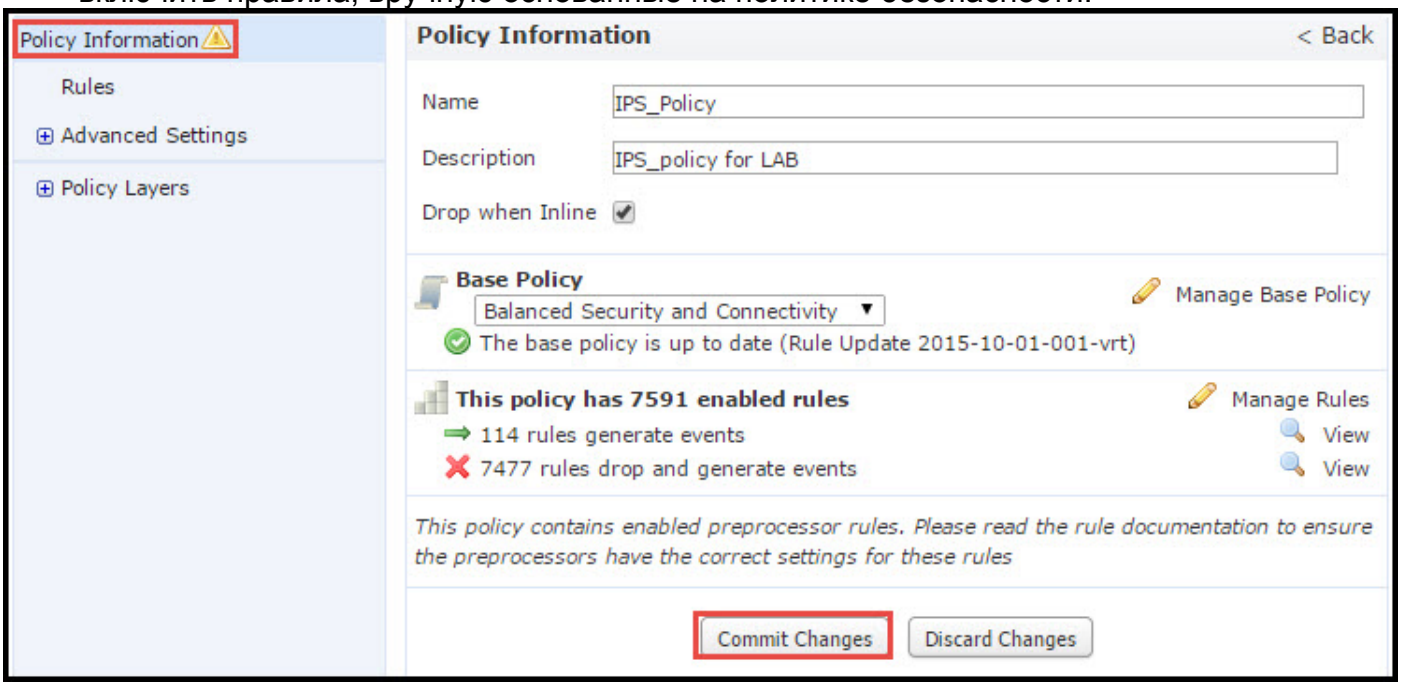
Шаг 1. 3. Модифицируйте основную политику

Страница Intrusion Policy Management дает опцию для изменения Основной Политики / Отбрасывание, когда Встроенный / опция Save и Discard.

Основная Политика содержит некоторую предоставленную системой политику, которая является встроенной политикой.

1. Сбалансированная Безопасность и Подключение: Это - оптимальная политика с точки зрения безопасности и подключения. Эта политика имеет приблизительно 7500 включенных правил, некоторые из них только генерируют события , тогда как другие генерируют события, а также отбрасывают трафик.

2. Безопасность по connectivity:If, ваше предпочтение является безопасностью тогда, которую можно предпочесть безопасности политике подключений, которая увеличивает число включенных правил.
3. Подключение по безопасности: Если ваше предпочтение является подключением, а не безопасностью тогда, можно предпочесть подключение политике безопасности, которая сократит количество включенных правил.
4. Максимальное Обнаружение - Выбирает эту политику для получения максимального обнаружения.
5. Никакое Активное правило - Эта опция не отключает все правила. Необходимо включить правила, вручную основанные на политике безопасности.



Шаг 1. 4. Фильтрация подписи с опцией панели Фильтра

Перейдите к опции **Rules** на навигационной панели, и страница Rule Management появляется. В базе данных Правила существуют тысячи правила. Панель фильтра предоставляет хорошую возможность поисковой системы искать правило эффективно.

Можно вставить любое ключевое слово в панель Фильтра, и система захватывает результаты для вас. Если существует требование для обнаружения подписи для Уровня защищенных сокетов (SSL) heartbleed уязвимостью, можно искать ключевое слово heartbleed в панели фильтра, и это выберет подпись для heartbleed уязвимости.

> **Совет:** Если множественные ключевые слова используются в панели Фильтра тогда, система комбинирует их использующий логику AND для создания составного поиска.

Можно также искать правила при помощи Идентификатора подписи (SID), ID Генератора (GID), Категория: dos и т.д.

Правила эффективно разделены на несколька способов такой как на основе Категории / Классификации / Microsoft Vulnerabilities / Microsoft Worms / Platform Specific. Такая ассоциация правил помогает клиенту получать правильную подпись в простом способе и помогать клиенту эффективно настраивать подписи.

Можно также искать с номером CVE для обнаружения правил, которые касаются их. Можно использовать синтаксис **CVE: <cve-number->.**

Шаг 1. 5. Настройте Состояние правила

Перейдите к опции **Rules** на навигационной панели, и страница Rule Management появляется. Выберите правила и выберите **опцию Rule State** для настройки состояния правил. Существует три состояния, которые могут быть настроены для правила:

1. **Генерируйте События:** Когда правило совпадает с трафиком, эта опция генерирует события.

2. **Отбросьте и Генерируйте События:** Когда правило совпадает с трафиком, эта опция генерирует события и трафик отбрасывания.

3. **Отключите:** Эта опция отключает правило.

Шаг 1. 6. Фильтр события настраивает

Важность события проникновения может основываться на частоте появления, или на источнике или IP - адресе назначения. В некоторых случаях вы не можете заботиться о событии, пока оно не произошло определенное число времен. Например, вы не могли бы быть заинтересованы, пытается ли кто-то войти к серверу, пока они не отказывают определенное число времен. В других случаях вы, возможно, только должны были бы видеть несколько вхождений соответствия правила, чтобы проверить, существует ли широко распространенная проблема.

Существует два пути, которыми можно достигнуть этого:

1. Событие threshold.

2. Подавление события.

Событие Threshold

Можно установить пороги, которые диктуют, как часто событие отображено, на основе количества вхождений. Можно настроить пороговую обработку на событие и на политику.

Шаги в Порог События configure:

Шаг 1. Выберите **Rule, для** которого вы хотите настроить Событие Threshold.

Шаг 2. Нажмите **фильтрацию событий**.

Шаг 3. Нажмите **порог**.

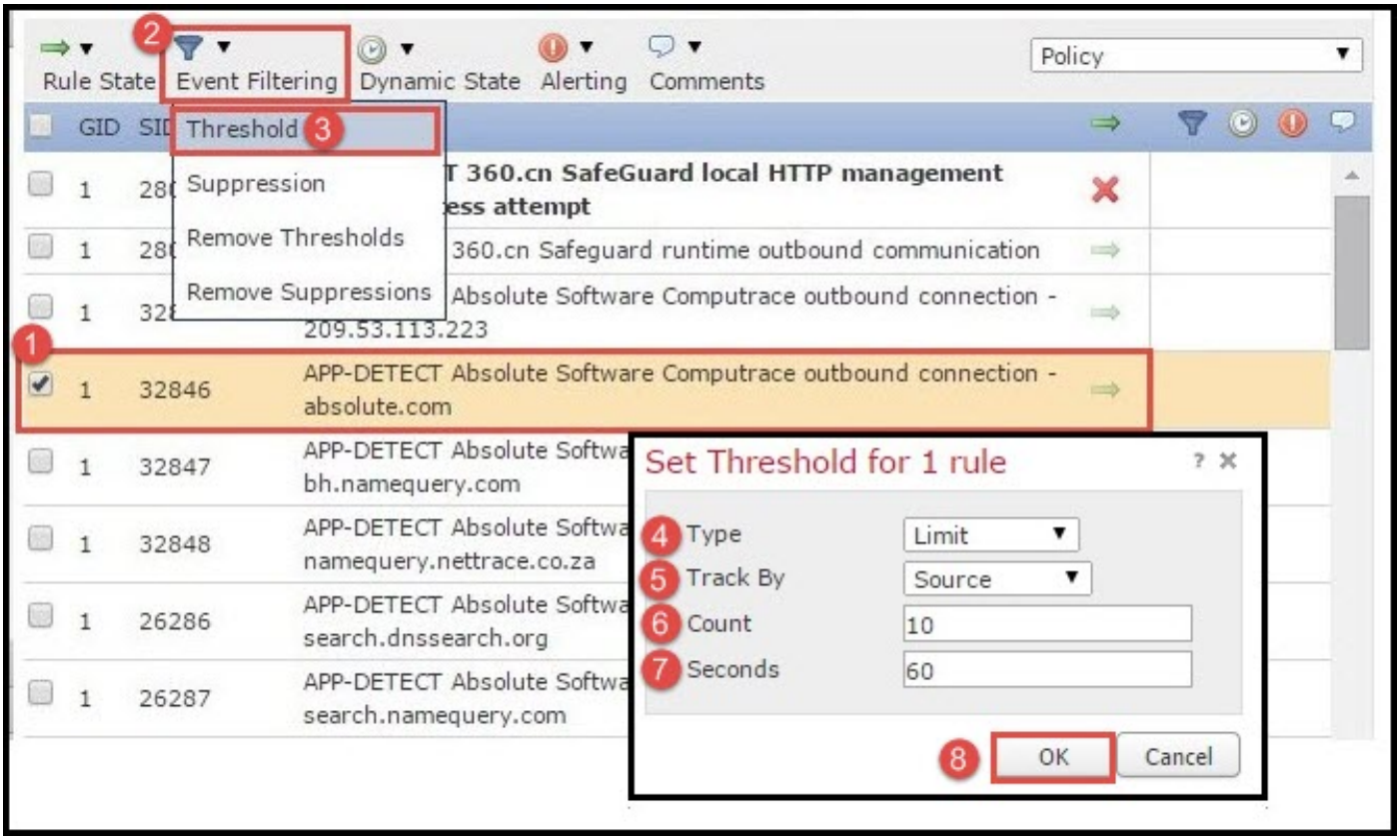
Шаг 4. . Выберите **Type** из выпадающего списка. (Предел или Порог или Оба).

Шаг 5. . Выберите, как вы хотите отследить от **Дорожки** коробкой отбрасывания. (Источник или Назначение).

Шаг 6. Введите **количество** событий для совещания порога.

Шаг 7. Введите **Секунды** для протекания перед сбросом количества.

Шаг 8. **Нажмите ОК для завершения.**



После того, как фильтр события добавлен к правилу, должна существовать возможность для наблюдения значка фильтра рядом с индикацией правила, которая показывает, что существует фильтрация событий, включенная для этого правила.

Подавление события

Указанные уведомления событий могут быть подавлены на основе источника / IP - адрес назначения или на Правило.

Примечание: Когда вы подавление события add для правила. Контроль подписи работает как обычно, но система не генерирует события, если трафик совпадает с подписью. При определении определенного Источника/Назначения тогда, события не появляются только для определенного источника/назначения для этого правила. Если вы принимаете решение подавить завершенное правило тогда, система не генерирует события для этого правила.

Шаги в Порог События configure:

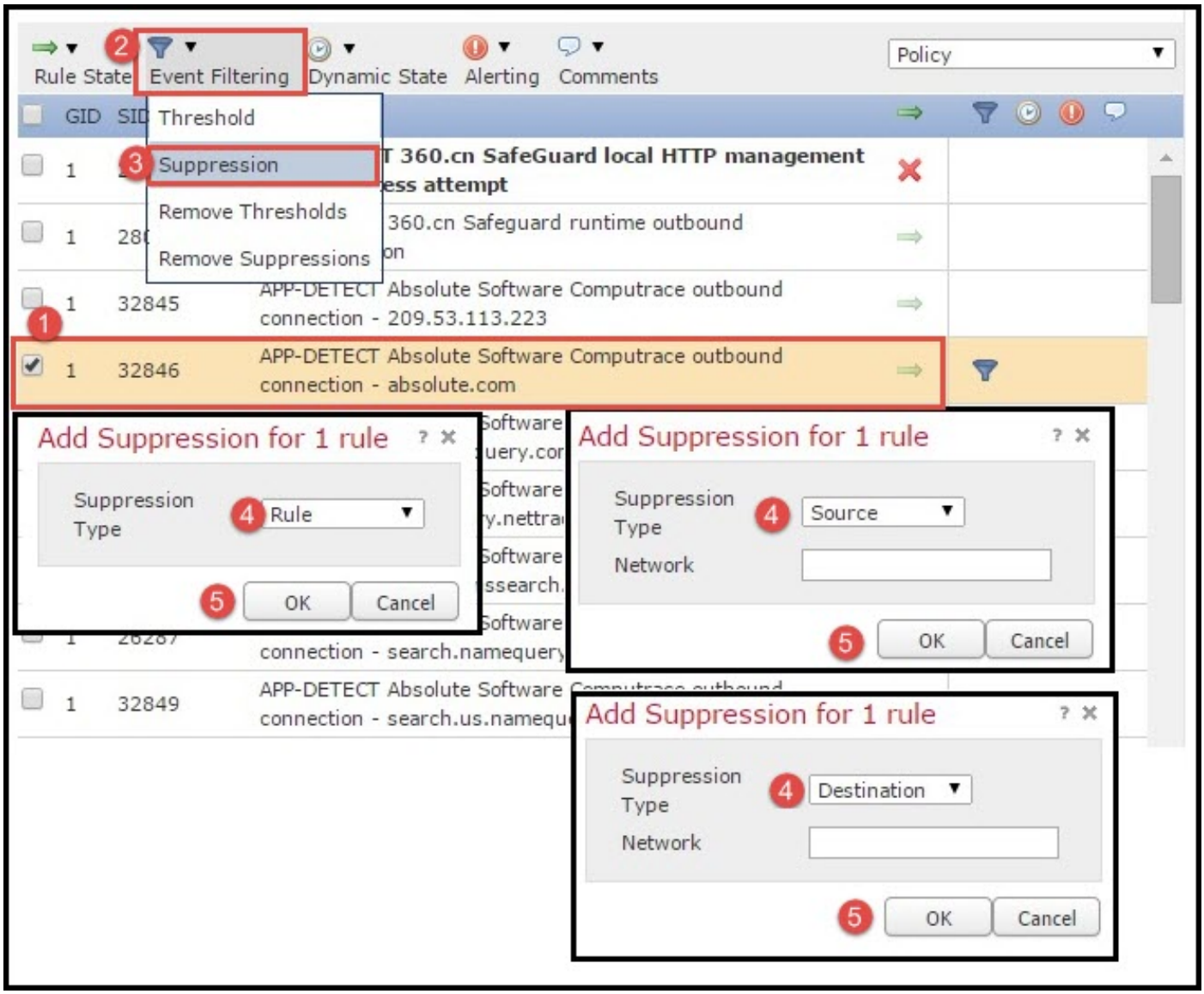
Шаг 1. Выберите **Rule, для** которого вы хотите в Порог События configure.

Шаг 2. Нажмите **Event Filtering**.

Шаг 3. Нажмите **Suppression.**

Шаг 4. . Выберите **Suppression Type** из выпадающего списка. (Правило или Источник или Назначение).

Шаг 5. . **Нажмите ОК для завершения.**



После того, как фильтр события добавлен к этому правилу, должна существовать возможность для наблюдения значка фильтра с количеством два рядом с индикацией правила, которая показывает, что существует два фильтра события, включенные для этого правила.

Шаг 1. 7. Настройте динамическое состояние

Это - функция в чем, мы можем изменить состояние правила, если совпадает указанное условие.

Предположим сценарий лобовой атаки перебором паролей для взламывания пароля. Если подпись обнаруживает попытку сбоя пароля, и действие правила должно генерировать событие. Система продолжает генерировать предупреждение для попытки сбоя пароля. Для этой ситуации можно использовать **Динамическое состояние**, где действие **Генерирует События** , может быть изменен, чтобы **Отбросить и Генерировать События** для блокирования лобовой атаки перебором паролей.

Перейдите к опции **Rules** на навигационной панели, и страница Rule Management появляется. Выберите правило, для которого вы хотите включить Динамическое состояние и выбрать **опции Dynamic State> Add, Тарифная база Управляет государством.**

Для настройки На основе скорости Управляют государством:

1. Выберите **Rule, для** которого вы хотите в Порог События configure.
2. Нажмите **динамическое состояние**.
3. Нажмите **добавление на основе скорости управляют государством**.
4. Выберите, как вы хотите отследить состояние правила от **Дорожки** коробкой отбрасывания. (**Правило или Источник или Назначение**).
5. Введите **Сеть**. Можно задать один IP-адрес, блок адресов, переменную или список comma-separated, который состоит из любой комбинации их.
6. Введите **количество** событий и метки времени в секундах.
7. Выберите **New State,** вы хотите определить для правила.
8. Введите **Таймаут**, после которого вернулось состояние правила.
9. **Нажмите ОК для завершения.**

Шаг 2. Настройте Политику анализа сети (NAP) и (дополнительные) Переменные наборы

Настройте политику анализа сети

Политика Доступа к сети также известна как препроцессоры. Препроцессор делает пакетную повторную сборку и нормализует трафик. Это помогает определять сетевой уровень и аномалии транспортного протокола на идентификации несоответствующих опций header.

NAP делает дефрагментацию дейтаграмм IP, предоставляет проверку трафика потоком TCP и потоковую повторную сборку и проверяющий контрольные суммы. Препроцессор нормализует трафик, проверьте и проверьте стандарт протокола.

Каждый препроцессор имеет свой собственный номер GID. Это представляет, какой препроцессор был инициирован пакетом.

Для настройки Политики Анализа сети Перейдите к **Конфигурации> конфигурация ASA FirePOWER> Политика> Политика контроля доступа> Усовершенствованный> Политика Проникновения и Анализ сети**

Аналитическая Политика Сети по умолчанию является Сбалансированной Безопасностью и Подключением, которое является оптимальной рекомендуемой политикой. Существует предоставленная политика NAP других еще трех систем, которая может быть выбрана от выпадающего списка.

Выберите **опцию Network Analysis Policy List** для создания пользовательской политики NAP.

Настройте переменные наборы

Переменные наборы используются в правилах проникновения определить адреса источника и назначения и порты. Когда переменные отражают вашу сетевую среду более точно, правила являются более эффективными. Переменная играет важную роль в настройке производительности.

Переменные наборы были уже настроены с параметром по умолчанию (Сеть/Порт). Добавьте новые Переменные наборы, если вы хотите изменить конфигурацию по

умолчанию.

Для настройки Переменных наборов перейдите к **Конфигурации > Конфигурация Огневой мощи ASA> Управление объектами> Переменный набор**. Выберите **опцию Add Variable Set** для добавления новых переменных наборов. Введите **Имя** Переменных наборов и задайте **Описание.**

Если какое-либо пользовательское приложение работает на определенный порт, тогда определяют номер порта в поле Номера порта. Настройте параметр сети.

$Home_NET задают внутреннюю сеть.

$External_NET задают внешнюю сеть.

Шаг 3: Настройте Управление доступом для включения политики Проникновения / NAP / Переменные наборы

Перейдите к **Конфигурации> Конфигурация Огневой мощи ASA> Политика> Политика контроля доступа.** Необходимо выполнить эти шаги:

1. Отредактируйте правило Политики доступа, где вы хотите назначить политику Проникновения.
2. Выберите вкладку **Inspection.**
3. Выберите **Intrusion Policy** из выпадающего списка и выберите **Variable Sets** из выпадающего списка
4. **Нажмите Save.**

Так как Политика Проникновения добавлена к этому Правилу Политики доступа. Вы видите значок экрана в Золотом Цвете, который указывает , что включена Политика Проникновения.

Нажмите **изменения Store ASA FirePOWER** для сохранения изменений.

Шаг 4. . Разверните политику контроля доступа

Теперь, необходимо развернуть Политику контроля доступа. Перед применением политики вы будете видеть Политику контроля доступа индикации, устаревшую на устройстве. Развернуть изменения на датчике:

1. Нажмите **Deploy**.
2. Нажмите **Deploy FirePOWER Changes**.
3. Нажмите **Deploy** во всплывающем окне.

Примечание: В версии 5.4.x, для применения политики доступа к датчику необходимо нажать Apply ASA FirePOWER Changes

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

Шаг 5. . Следите за развитием событий проникновения

Для наблюдения событий Intrusion, генерируемых Модулем FirePOWER, перейдите к **Мониторингу> Мониторинг ASA FirePOWER> Оперативная Обработка событий.**

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Шаг 1. Гарантируйте, что Управляют государством Правил, соответственно настроен.

Шаг 2. Гарантируйте, что корректная Политика IPS была включена в Правила Доступа.

Шаг 3. Гарантируйте, что наборы Переменных настроены правильно. Если переменные наборы не будут настроены правильно тогда, то подписи не совпадут с трафиком.

Шаг 4. . Гарантируйте, что развертывания Политики контроля доступа завершают успешно.

Шаг 5. . Контролируйте события подключения и события Intrusion, чтобы проверить, поражает ли трафик корректное правило или нет.

Дополнительные сведения

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