Функциональность обнаружения угрозы ASA и конфигурация

Содержание

Введение

В этом документе описаны функциональность и базовая конфигурация функции обнаружения угроз в устройствах адаптивной защиты Cisco (ASA). Обнаружение угрозы предоставляет администраторам межсетевого экрана необходимые программные средства, чтобы определить, понять, и остановить атаки, прежде чем они достигнут инфраструктуры внутренней сети. В заказе для этого функция полагается на многие другие триггеры и статистику, которая описана более подробно в этих разделах.

Обнаружение угрозы может использоваться на любом межсетевом экране ASA, который выполняет версию программного обеспечения 8.0 (2) или позже. Несмотря на то, что обнаружение угрозы не является заменой для специализированный IDS/РЕШЕНИЕ СИСТЕМЫ IPS, оно может использоваться в средах, где IPS не доступен для обеспечения добавленного слоя защиты к базовой функциональности ASA.

Функциональность обнаружения угрозы

Функция обнаружения угрозы имеет три основных компонента:

1. Базовое обнаружение угроз
2. Расширенное обнаружение угроз
3. Сканирование обнаружения угрозы

Каждый из этих компонентов описан подробно в этих разделах.

Базовое обнаружение угроз (скорости уровня системы)

Базовое обнаружение угроз включено по умолчанию на всех ASA, работающих 8.0 (2) и позже.

Базовое обнаружение угроз контролирует скорости, на которых пакеты отброшены по различным причинам ASA в целом. Это означает, что статистические данные, генерируемые базовым обнаружением угроз только, применяются ко всему устройству и обычно не достаточно гранулированы для предоставления сведения об источнике или специфическом характере угрозы. Вместо этого ASA контролирует отброшенные пакеты для этих событий:

- **Отбрасывание ACL (acl-drop)** - Пакеты запрещены списками доступа
- **Плохие Pkt (bad-packet-drop)** - Форматы недопустимого пакета, который включает L3 и заголовки L4, которые не соответствуют стандартам RFC
- **Предел Коннектикута (conn-limit-drop)** - Пакеты, которые превышают предел глобального соединения или настроенный
- **Атака DoS (dos-drop)** - Атаки отказа в обслуживании (DoS)
- **Межсетевой экран (fw-drop)** - Основные проверки межсетевой защиты
- **Атака ICMP (icmp-drop)** - Подозрительные пакеты ICMP
- **Осмотрите (inspect-drop)** - Отказ контролем приложения
- **Интерфейс (interface-drop)** - Пакеты понизились проверками интерфейса
- **Сканирование (scanning-threat)** - атаки сканирования Сети/хоста
- **Атака SYN (syn-attack)** - Неполные атаки сеанса, который включает Атаки SYN TCP и однонаправленные сеансы UDP , которые не имеют никаких, возвращают данные

Каждое из этих событий имеет определенный набор триггеров, которые используются для определения угрозы. Большинство триггеров скреплено к определенным причинам отбрасывания ASP, хотя также рассматривают определенные системные журналы и инспекционные действия. Некоторые триггеры проверены множественными категориями угрозы. Некоторые наиболее распространенные триггеры выделены в этой таблице, хотя это не полный список:

Основная угроза	Триггер (триггеры) / Причина (причины) Отбрасывания ASP
aCL drop	aCL drop
bad-packet-drop	invalid-tcp-hdr-length invalid-ip-header inspect-dns-pak-too-long inspect-dns-id-not-matched
conn-limit-drop	conn limit
dos-drop	подведенный sp-безопасностью

	inspect-icmp-seq-num-not-matched
	inspect-dns-pak-too-long
fw-drop	inspect-dns-id-not-matched
	подведенный sp-безопасностью
	aCL drop
icmp-drop	inspect-icmp-seq-num-not-matched
inspect-drop	Сбросы кадров инициированы инспекционным механизмом
interface-drop	подведенный sp-безопасностью
	no-route
	tcp-3whs-failed
	tcp-not-syn
	подведенный sp-безопасностью
scanning-threat	aCL drop
	inspect-icmp-seq-num-not-matched
	inspect-dns-pak-too-long
	inspect-dns-id-not-matched
syn-attack	Системный журнал %ASA-6-302014 с причиной разрушения "Времени ожидания S

Для каждого события базовое обнаружение угроз измеряет скорости, что эти отбрасывания происходят по настроенному периоду времени. Этот период времени называют **интервалом средней скорости (ARI)** и может колебаться от 600 секунд до 30 дней. Если количество событий, которые происходят в ARI, превышает пороги настроенной скорости, ASA считает эти события угрозой.

Базовое обнаружение угроз имеет два настраиваемых пороговых значения для того, когда оно полагает, что события угроза: **средняя скорость** и **пиковая скорость**. Средняя скорость является просто средним количеством отбрасываний в секунду в периоде времени настроенного ARI. Например, если порог средней скорости для отбрасываний ACL настроен для 400 с ARI 600 секунд, ASA вычисляет среднее количество пакетов, которые были отброшены ACL за прошлые 600 секунд. Если этот номер, оказывается, больше, чем 400 в секунду, ASA регистрирует угрозу.

Аналогично, пиковая скорость подобна, но посмотрела на меньшие периоды данных снимка, названных **интервалом пиковой скорости (BRI)**. BRI всегда меньше, чем ARI. Например, основываясь на предыдущем примере, ARI для отбрасываний ACL является все еще 600 секундами и теперь имеет пиковую скорость 800. С этими значениями ASA вычисляет среднее количество пакетов, отброшенных ACL за прошлые 20 секунд, где 20 секунд являются BRI. Если это расчетное значение превышает 800 отбрасываний в секунду, угроза зарегистрирована. Для определения, какой BRI используется, ASA вычисляет значение 1/30-го из ARI. Поэтому в примере, ранее используемом, 1/30-м из 600 секунд, 20 секунд. Однако обнаружение угрозы имеет минимальный BRI 10 секунд, поэтому, если 1/30-й ARI меньше чем 10, ASA все еще использует 10 секунд в качестве BRI. Кроме того, важно обратить внимание, что это поведение было другим в версиях до 8.2 (1), который использовал значение 1/60-го из ARI вместо 1/30-го. Минимальный BRI 10 секунд является тем же для всех версий программного обеспечения.

Когда основная угроза обнаружена, ASA просто генерирует системный журнал %ASA-4-733100, чтобы предупредить администратора, что была определена потенциальная угроза. Среднее, текущее, и общее число событий для каждой категории угрозы могут быть замечены с **командой show threat-detection rate**. Общее число кумулятивных событий является суммой количества событий, замеченных в последних 30 выборках BRI.

Базовое обнаружение угроз не принимает мер, чтобы остановить недопустимый трафик или

предотвратить будущие атаки. В этом смысле базовое обнаружение угроз является чисто информационным и может использоваться в качестве мониторинга или механизма создания отчетов.

Расширенное обнаружение угроз (Статистика уровня объектов и вершина N)

В отличие от Базового обнаружения угроз, Расширенное обнаружение угроз может использоваться для отслеживания статистики для большего количества гранулированных объектов. Поддержки ASA, отслеживающие статистику для IP - адресов хоста, портов, протоколов, ACL и серверов, защищены перехватом TCP. Расширенное обнаружение угроз только включено по умолчанию для статистики ACL.

Для хоста, порта и объектов протокола, Обнаружение Угрозы отслеживает количество пакетов, байтов и отбрасываний, которые были и переданы и получены тем объектом в определенном периоде времени. Для ACL Обнаружение Угрозы отслеживает лучшие 10 ACE (и разрешают и запрещают), которые были поражены больше всего в определенном периоде времени.

Периоды времени, отслеженные во всех этих случаях, составляют 20 минут, 1 час, 8 часов и 24 часа. В то время как сами периоды времени не конфигурируемы, количество периодов, которые отслежены на объект, может быть отрегулировано с ключевым словом 'номера скорости'. Посмотрите Раздел конфигурации для получения дополнительной информации. Например, если 'номер скорости' установлен в 2, вы видите всю статистику в течение 20 минут, 1 часа и 8 часов. если 'номер скорости' установлен в 1, вы видите всю статистику в течение 20 минут, 1 часа. Независимо от того, что, всегда отображается 20-минутная скорость.

Когда перехват TCP включен, Обнаружение Угрозы может отслеживать лучшие 10 серверов, которые, как полагают, являются под атакой и защищены перехватом TCP. Статистические данные для перехвата TCP подобны Базовому обнаружению угроз в том смысле, что пользователь может настроить измеренный интервал скорости наряду с определенным средним числом (ARI) и разорвать (BRI) скорости. Статистические данные Расширенного обнаружения угроз для перехвата TCP только доступны в ASA 8.0 (4) и позже.

Статистические данные Расширенного обнаружения угроз просматриваются через **команды статистику обнаружения угрозы и show threat-detection statistics top показа**. Это - также функция, ответственная за начальную загрузку "главных" графиков на информационной панели межсетевого экрана ASDM. Единственные системные журналы, которые генерируются Расширенным обнаружением угроз, являются %ASA-4-733104 и %ASA-4-733105, которые инициированы, когда среднее число и пиковые скорости (соответственно) превышены для статистики перехвата TCP.

Как Базовое обнаружение угроз, Расширенное обнаружение угроз является чисто информационным. Никакие меры не приняты для блокирования трафика на основе статистики Расширенного обнаружения угроз.

Сканирование обнаружения угрозы

Сканирование Обнаружения Угрозы используется для отслеживания подозреваемых

атакующих, которые создают соединения слишком много хостов в подсети или много портов на хосте/подсети. Сканирование Обнаружения Угрозы отключено по умолчанию.

Сканирование Обнаружения Угрозы основывается на понятии Базового обнаружения угроз, которое уже определяет категорию угрозы для атаки сканирования. Поэтому интервал скорости, средняя скорость (ARI) и пиковая скорость (BRI) параметры настройки разделен между Основным и Просматривающим Обнаружением Угрозы. Различие между этими 2 функциями - то, что, в то время как Базовое обнаружение угроз только указывает, что среднее число или пороги пиковой скорости были скрещены, Просмотрев Обнаружение Угрозы, поддерживает базу данных атакующего и целевых IP - адресов, которые могут помочь предоставлять больше контекста вокруг хостов, вовлеченных в просмотр. Кроме того, только трафик, который фактически получен конечным узлом, рассматривают путем Сканирования Обнаружения Угрозы. Даже если трафик отброшен ACL, базовое обнаружение угроз может все еще инициировать угрозу Сканирования.

Сканирование Обнаружения Угрозы может дополнительно реагировать на атаку путем избегания IP атакующего. Это делает Обнаружение Угрозы Сканирования единственным подмножеством функции Обнаружения Угрозы, которая может активно влиять на соединения через ASA.

Когда Сканирование Обнаружения Угрозы обнаруживает атаку, %ASA-4-733101 зарегистрирован для атакующего и/или целевого IPs. Если функция настроена для избегания атакующего, %ASA-4-733102 зарегистрирован, когда Сканирование Обнаружения Угрозы генерирует избегание. Когда избегание удалено, %ASA-4-733103 зарегистрирован. **Команда show threat-detection scanning-threat** может использоваться для просмотра всей базы данных Угрозы Сканирования.

Ограничения

- Обнаружение угрозы только доступно в ASA 8.0 (2) и позже. Это не поддерживается на платформе 1000 B ASA.
- Обнаружение угрозы только поддерживается в одиночном режиме контекста.
- Только угрозы через коробку обнаружены. Трафик, передаваемый самому ASA, не рассматривает Обнаружение Угрозы.
- Попытки TCP - подключения, которые перезагружены предназначенным сервером, не посчитаны как угроза Атаки SYN или Сканирования.

!--- конфигурацию

Базовое обнаружение угроз

Базовое обнаружение угроз включено с **командой threat-detection basic-threat**.

```
ciscoasa(config)# threat-detection basic-threat
```

Стандартные скорости передачи данных могут быть просмотрены с **командой show run all threat-detection**.

```
ciscoasa(config)# show run all threat-detection
```

```
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

Для настройки этих скоростей со значениями custom просто реконфигурируйте **команду threat-detection rate** для соответствующей категории угрозы.

```
ciscoasa(config)# threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate
550
```

Каждая категория угрозы может иметь максимум 3 других определенных скоростей (с ID скорости скорости 1, скорость 2 и скорость 3). На определенный ID скорости, который превышен, ссылаются в %ASA-4-733100 системном журнале.

В предыдущем примере обнаружение угрозы создает системный журнал 733100 только, когда количество отбрасываний ACL превышает 250 отбрасываний/секунда более чем 1200 секунд или 550 отбрасываний/секунда более чем 40 секунд.

Расширенное обнаружение угроз

Используйте **команду threat-detection statistics** для включения Расширенного обнаружения угроз. Если никакое определенное ключевое слово функции не предоставлено, команда позволяет отследить для всей статистики.

```
ciscoasa(config)# threat-detection statistics ?
configure mode commands/options:
access-list Keyword to specify access-list statistics
host Keyword to specify IP statistics
port Keyword to specify port statistics
protocol Keyword to specify protocol statistics
tcp-intercept Trace tcp intercept statistics
<cr>
```

Для настройки количества интервалов скорости, которые отслежены для хоста, порта, протокола, или статистики ACL, используют ключевое слово **номера скорости**.

```
ciscoasa(config)# threat-detection statistics host number-of-rate 2
```

Ключевое слово номера скорости настраивает Обнаружение Угрозы для отслеживания только самого короткого *n* количества интервалов.

Для включения статистики перехвата TCP используйте **команду threat-detection statistics tcp-intercept**.

```
ciscoasa(config)# threat-detection statistics tcp-intercept
```

Для настройки пользовательских скоростей для статистики перехвата TCP используйте **интервал скорости**, **среднюю скорость** и ключевые слова **пиковой скорости**.

```
ciscoasa(config)# threat-detection statistics tcp-intercept rate-interval 45
burst-rate 400 average-rate 100
```

Сканирование обнаружения угрозы

Чтобы позволить Просмотреть Обнаружение Угрозы, используйте **команду threat-detection scanning-threat**.

```
ciscoasa(config)# threat-detection scanning-threat
```

Для регулировки скоростей для scanning-threat используйте ту же **команду threat-detection rate**, используемую Базовым обнаружением угроз.

```
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 250
burst-rate 550
```

Чтобы позволить ASA избегать IP атакующего сканирования, добавьте **избегать** ключевое слово к **команде threat-detection scanning-threat**.

```
ciscoasa(config)# threat-detection scanning-threat shun
```

Это позволяет Просматривать Обнаружение Угрозы для создания одного часа, избегают для атакующего. Для регулировки продолжительности избегания используйте **команду threat-detection scanning-threat shun duration**.

```
ciscoasa(config)# threat-detection scanning-threat shun duration 1000
```

В некоторых случаях можно все еще хотеть препятствовать тому, чтобы ASA избежал определенного IPs. Чтобы сделать это, создайте исключение с **threat-detection scanning-threat, избегают кроме** команды.

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.1
255.255.255.255
ciscoasa(config)# threat-detection scanning-threat shun except object-group no-shun
```

Производительность

Базовое обнаружение угроз имеет очень мало влияния на производительность на ASA. Усовершенствованное и Просматривающее Обнаружение Угрозы является намного большим количеством потребляющих ресурсов, потому что они должны отслеживать различную статистику в памяти. Только Сканирование Обнаружения Угрозы с избегать включенной функцией может активно повлиять на трафик, который иначе был бы позволен.

В то время как версии программного обеспечения ASA развились, загруженность памяти Обнаружения Угрозы была значительно оптимизирована. Однако меры должны быть приняты для мониторинга загруженности памяти ASA прежде и после того, как будет включено Обнаружение Угрозы. В некоторых случаях могло бы быть лучше только включить определенную статистику (например, статистику хоста) временно, активно решая конкретную проблему.

Для большего количества подробного представления использования памяти Обнаружения Угрозы **всем заправляйте обнаружение угрозы кэша приложения памяти [подробность]** команда.

Рекомендуемые действия

Эти разделы предоставляют некоторые общие рекомендации для мер, которые могут быть приняты, когда происходит различная Угроза Связанные с обнаружением события.

Когда Основной Уровень сброса Превышен, и %ASA-4-733100 Генерируется

Определите определенную категорию угрозы, упомянутую в %ASA-4-733100 системном журнале, и коррелируйте это с выходными данными **показа threat-detection скорость**. С этой информацией проверьте выходные данные **отбрасывания asp показа** для определения причин, почему отбрасывается трафик.

Для большего количества подробного представления трафика, который отброшен по определенной причине, используйте перехват отбрасывания ASP с рассматриваемой причиной для наблюдения всех пакетов, которые отбрасываются. Например, если угрозы Отбрасывания ACL зарегистрированы, перехват на причине отбрасывания ASP **acl-drop**:

```
ciscoasa# capture drop type asp-drop acl-drop

ciscoasa# show capture drop

1 packet captured

1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53: udp 34 Drop-reason:
(acl-drop) Flow is denied by configured rule
```

Этот перехват показывает, что отбрасываемый пакет является пакетом UDP/53 от 10.10.10.10 до 192.168.1.100.

Если %ASA-4-733100 сообщает об угрозе Сканирования, может также быть полезно временно позволить Просмотреть Обнаружение Угрозы. Это позволяет ASA отслеживать источник и целевой IPs, вовлеченный в атаку.

Так как Базовое обнаружение угроз главным образом контролирует трафик, который уже отбрасывается ASP, никакое прямое действие не требуется, чтобы останавливать потенциальную угрозу. Исключениями из этого являются Атаки SYN и угрозы Сканирования, которые включают трафик, проходящий через ASA.

Если отбрасывания, замеченные в перехвате отбрасывания ASP, легитимны и/или ожидаются для сетевой среды, настроить интервалы базовой скорости на более соответствующее значение.

Если отбрасывания показывают незаконный трафик, меры должны быть приняты, чтобы заблокировать или ограничить трафик , прежде чем это достигнет ASA. Это может включать ACL и QoS на устройствах восходящего потока данных.

Для Атак SYN трафик может быть заблокирован в ACL на ASA. Перехват TCP мог также быть настроен для защиты предназначенного сервера (серверов), но это могло просто привести к Предельной угрозе Коннектикута, зарегистрированной вместо этого.

Для Сканирования угроз трафик может также быть заблокирован в ACL на ASA. Сканированию Обнаружения Угрозы с **избегать** опцией можно позволить позволить ASA

заранее блокировать все пакеты от атакующего для определенного периода времени.

Когда Угроза Сканирования Обнаружена, и %ASA-4-733101 Зарегистрирован

%ASA-4-733101 должен перечислить или конечный узел / подсеть или IP-адрес атакующего. Для полного списка целей и атакующих, проверьте выходные данные **показа threat-detection scanning-threat**.

Захваты пакета на интерфейсах ASA, стоящих перед атакующим и/или целью (целями), могут также помочь разъяснять природу атаки.

Если обнаруженный просмотр не ожидается, меры должны быть приняты, чтобы заблокировать или ограничить трафик, прежде чем это достигнет ASA. Это может включать ACL и QoS на устройствах восходящего потока данных. Добавление **избегать** опция к config Обнаружения Угрозы Сканирования может также позволить ASA заранее отбрасывать все пакеты от IP атакующего для определенного периода времени. Как последнее прибежище трафик может также быть заблокирован вручную на ASA через политику перехвата TCP или ACL.

Если обнаруженный просмотр является ошибочным допуском, отрегулируйте интервалы скорости Угрозы Сканирования к более соответствующему значению для сетевой среды.

Когда Атакующего Избегают, и %ASA-4-733102 Зарегистрирован

%ASA-4-733102 перечисляет IP-адрес атакующего, которого избегают. Использование **обнаружение угрозы показа избегает** команды для просмотра полного списка атакующих, которых избежало Обнаружение Угрозы в частности. Использование **показ избегает** команды для просмотра полного списка всех IPs, которых активно избегает ASA (включая из источников кроме Обнаружения Угрозы).

Если избегание является частью легитимной атаки, никакие дальнейшие действия не требуются. Однако это было бы выгодно для ручного блокирования трафика атакующего максимально далеко в восходящем направлении к источнику. Это может быть сделано через ACL и QoS. Это гарантирует, что промежуточные устройства не должны тратить впустую ресурсы, обрабатывающие незаконный трафик.

Если угроза Сканирования, которая инициировала избегание, была ошибочным допуском, вручную удалите избегание с **командой clear threat-detection shun [IP_address]**.

Когда Зарегистрированы %ASA-4-733104 и/или %ASA-4-733105

%ASA-4-733104 и %ASA-4-733105 перечисляют хост, предназначенный атакой, которая в настоящее время защищается перехватом TCP. Для получения дополнительной информации на коэффициентах заболеваемости и защищенных серверах, проверьте выходные данные **показа threat-detection перехват TCP вершины статистики**.

```
ciscoasa# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins Sampling interval: 30 secs
------------------------------------------------------------------------------
```

```
1 192.168.1.2:5000 inside 1249 9503 2249245 Last: 10.0.0.3 (0 secs ago)
2 192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3 192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4 192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5 192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6 192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7 192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8 192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9 192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10 192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Когда Расширенное обнаружение угроз обнаруживает атаку этой природы, ASA уже защищает предназначенный сервер через перехват TCP. Проверьте пределы сконфигурированного соединения, чтобы гарантировать, что они обеспечивают адекватную защиту для природы и скорости атаки. Кроме того, это было бы выгодно для ручного блокирования трафика атакующего максимально далеко в восходящем направлении к источнику. Это может быть сделано через ACL и QoS. Это гарантирует, что промежуточные устройства не должны тратить впустую ресурсы, обрабатывающие незаконный трафик.

Если обнаруженная атака является ошибочным допуском, отрегулируйте скорости для атаки перехвата TCP к более соответствующему значению с **командой threat-detection statistics tcp-intercept**.

Как вручную инициировать угрозу

Для тестирования и целей устранения проблем, может быть полезно вручную инициировать различные угрозы. Этот раздел содержит советы для инициирования нескольких типов общей угрозы.

Основная угроза - отбрасывание ACL, межсетевой экран и сканирование

Для инициирования определенной Основной Угрозы обратитесь к таблице в предыдущем разделе Функциональности. Выберите определенное отбрасывание ASP обосновывают и передают трафик через ASA, который был бы отброшен соответствующей причиной отбрасывания ASP.

Например, Отбрасывание ACL, Межсетевой экран и угрозы Сканирования все рассматривают скорость пакетов, отбрасываемых acl-drop. Выполните эти шаги для инициирования этих угроз одновременно:

1. Создайте ACL на внешнем интерфейсе ASA, который явно отбрасывает все пакеты TCP, передаваемые конечному серверу на внутренней части ASA (10.11.11.11):`access-list outside_in extended line 1 deny tcp any host 10.11.11.11`
   `access-list outside_in extended permit ip any any`
   `access-group outside_in in interface outside`
2. От атакующего за пределами ASA (10.10.10.10), используйте nmap для выполнения просмотра SYN TCP против каждого порта на конечном сервере:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`**Примечание:** T5 настраивает nmap для выполнения просмотра максимально быстро. В зависимости от ресурсов ПК атакующего это все еще может не быть достаточно быстро для инициирования некоторых стандартных скоростей передачи данных. Если это верно, просто понизьте настроенные скорости для угрозы, которую вы хотите видеть. Установка ARI и BRI к 0 причинам Базовое обнаружение

угроз, чтобы всегда инициировать угрозу независимо от скорости.

3. Обратите внимание на то, что Основные Угрозы обнаружены для Отбрасывания ACL, Межсетевого экрана и угроз Сканирования:`%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,`
`max configured rate is 10; Current average rate is 9 per second,`
`max configured rate is 5; Cumulative total count is 5538`
`%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,`
`max configured rate is 0; Current average rate is 2 per second,`
`max configured rate is 0; Cumulative total count is 1472`
`%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,`
`max configured rate is 0; Current average rate is 2 per second,`
`max configured rate is 0; Cumulative total count is 1483`**Примечание:** В данном примере отбрасывание ACL и ARI Межсетевого экрана и BRIs были установлены в 0, таким образом, они всегда инициируют угрозу. Это - то, почему Max. настроенные скорости перечислены как 0.

Усовершенствованная угроза - перехват TCP

1. Создайте ACL на внешнем интерфейсе, который разрешает все пакеты TCP, передаваемые конечному серверу на внутренней части ASA (10.11.11.11):`access-list outside_in extended line 1 permit tcp any host 10.11.11.11`
`access-group outside_in in interface outside`
2. Если конечный сервер фактически не существует, или он перезагружает попытки подключения атакующего, настройте поддельную Запись ARP на ASA для помещения в черный список трафика атаки внутренний интерфейс:`arp inside 10.11.11.11 dead.dead.dead`
3. Создайте простую политику перехвата TCP по ASA:`access-list tcp extended permit tcp any any`
`class-map tcp`
`match access-list tcp`
`policy-map global_policy`
`class tcp`
`set connection conn-max 2`
`service-policy global_policy global`От атакующего за пределами ASA (10.10.10.10), используйте nmap для выполнения просмотра SYN TCP против каждого порта на конечном сервере:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`Обратите внимание на то, что Обнаружение Угрозы отслеживает защищенный сервер:`ciscoasa(config)#` **`show threat-detection statistics top tcp-intercept`**
`Top 10 protected servers under attack (sorted by average rate)`
`Monitoring window size: 30 mins Sampling interval: 30 secs`

`---------------------------------------------------------------------------`
`1 10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)`
`2 10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)`
`3 10.11.11.11:46126 outside 0 0 1 Last: 10.10.10.10 (6 secs ago)`
`4 10.11.11.11:3695 outside 0 0 1 Last: 10.10.10.10 (6 secs ago)`

Сканирование угрозы

1. Создайте ACL на внешнем интерфейсе, который разрешает все пакеты TCP, передаваемые конечному серверу на внутренней части ASA (10.11.11.11):`access-list outside_in extended line 1 permit tcp any host 10.11.11.11`
`access-group outside_in in interface outside`**Примечание:** Для Сканирования Обнаружения Угрозы для отслеживания цели и IPs атакующего трафик должен быть

разрешен через ASA.

2. Если конечный сервер фактически не существует, или он перезагружает попытки подключения атакующего, настройте поддельную Запись ARP на ASA для помещения в черный список трафика атаки внутренний интерфейс:`arp inside 10.11.11.11 dead.dead.dead`**Примечание:** Соединения, которые перезагружены конечным сервером, не посчитаны как часть угрозы.
3. От атакующего за пределами ASA (10.10.10.10), используйте nmap для выполнения просмотра SYN TCP против каждого порта на конечном сервере:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`**Примечание:** T5 настраивает nmap для выполнения просмотра максимально быстро. В зависимости от ресурсов ПК атакующего это все еще может не быть достаточно быстро для инициирования некоторых стандартных скоростей передачи данных. Если это верно, просто понизьте настроенные скорости для угрозы, которую вы хотите видеть. Установка ARI и BRI к 0 причинам Базовое обнаружение угроз, чтобы всегда инициировать угрозу независимо от скорости.
4. Обратите внимание на то, что угроза Сканирования обнаружена, IP атакующего отслежен, и атакующего избегают:
```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded.
Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

Дополнительные сведения

- Руководство по конфигурации ASA
- Справочник по командам ASA
- Руководство системного журнала ASA
- Cisco Systems – техническая поддержка и документация