Классический брандмауэр Cisco IOS/IPS: Настройка управления доступом на основе контекста (CBAC) для защиты от атак типа "Отказ в обслуживании"

Содержание

Введение

Этот документ описывает настраивающуюся процедуру для параметров Отказа в обслуживании (DoS) в Cisco IOS® Classic Firewall с CBAC.

CBAC предоставляет усовершенствованную функциональность фильтрации трафика и может использоваться в качестве составляющей часть вашего межсетевого экрана.

DoS обычно обращается к активности сети, которая или преднамеренно или непреднамеренно сокрушает сетевые ресурсы, такие как пропускная способность канала WAN, таблицы подключений межсетевого экрана, память конечного узла, ЦП или работоспособность. В самом неблагоприятном сценарии действие DoS сокрушает уязвимое (или предназначенный) ресурс до такой степени, что ресурс становится недоступным, и это запрещает возможность подключения к глобальной сети (WAN) или сервисный доступ к легальным пользователям.

Межсетевой экран Cisco IOS может способствовать смягчению действия DoS, если это поддерживает счетчики количества “полуоткрытых” TCP - подключений, а также общую скорость подключения через межсетевой экран и программное обеспечение предотвращения вторжений и в Классическом Межсетевом экране **(ip inspect)** и в Zone-Based Policy межсетевом экране.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Полуоткрытые соединения являются TCP - подключениями, которые не завершили квитирование SYN-SYN/ACK-ACK с тремя путями, которое всегда используется узлами TCP для согласования о параметрах их взаимного соединения. Большие числа полуоткрытых соединений могут быть показательными из нежелательных действий, такими как атаки distributed-denial-of-service (DDoS) или DoS. Пример одного типа атаки DoS проводится злонамеренным, преднамеренно разработанным программным обеспечением, таким как черви или вирусы, которые заражают множественные хосты в Интернете и пытаются сокрушить определенные Интернет-серверы с Атаками SYN, куда большие числа соединений SYN передаются серверу множественными хостами в Интернете или в частной сети организации. Атаки SYN представляют опасность Интернет-серверам, так как таблицы подключений серверов могут быть загружены “поддельными” попытками подключения SYN, которые поступают быстрее, чем сервер может иметь дело с новыми соединениями. Это - тип атаки DoS, потому что большое число соединений в списке TCP - подключения сервера жертвы предотвращает доступ легального пользователя к Интернет-серверам жертвы.

Межсетевой экран Cisco IOS также расценивает сеансы Протокола UDP с трафиком только в одном направлении как “полуоткрытые”, потому что много приложений, которые используют UDP для транспорта, подтверждают прием данных. Сеансы UDP без ответного трафика, вероятно, показательны из действия DoS или попыток соединиться между двумя хостами, где один из хостов стал безразличным. Много типов трафика UDP, таких как сообщения журнала, трафик управления сетью SNMP, передавая потоком голос и видео среды и трафик сигнализации, только используют трафик в одном направлении для переноса их трафика. Многие из этих типов трафика применяют специализированный интеллект, чтобы препятствовать тому, чтобы образцы однонаправленного трафика оказали негативное влияние на межсетевой экран и поведение DoS IPS.

Когда инспекционное правило было применено, до программного обеспечения Cisco IOS

версии 12.4(11)T и 12.4 (10), Cisco IOS Проверка пакетов С отслеживанием состояния обеспечила защиту от атак DoS как по умолчанию. Программное обеспечение Cisco IOS версии 12.4(11)T и 12.4 (10) модифицировало параметры настройки DoS по умолчанию так, чтобы защита от атак DoS не была автоматически применена, но счетчики действия соединения все еще активны. Когда защита от атак DoS активна, т.е. когда значения по умолчанию используются на более старых выпусках ПО, или значения были отрегулированы к диапазону, которые влияют на трафик, защита от атак DoS включена на интерфейсе, где контроль применен в направлении, в котором межсетевой экран применен для протоколов конфигурации политики межсетевого экрана для осмотра. Если трафик вводит или оставляет интерфейс с контролем примененным в том же направлении начального трафика (SYN - пакет или первый пакет UDP) для TCP - подключения или сеанса UDP, защита от атак DoS только включена на сетевом трафике.

Контроль Межсетевого экрана Cisco IOS предоставляет несколько корректируемых значений для защиты против атак DoS. Cisco IOS Software Release до 12.4 (11) T и 12.4 (10) имеют значения DoS по умолчанию, которые могут вмешаться в операцию исправной сети, если они не настроены для соответствующего уровня активности сети в сетях, где скорости подключения превышают настройки по умолчанию. Эти параметры позволяют вам настраивать точки, в которых защита от атак DoS вашего межсетевого экрана - маршрутизатора начинает вступать в силу. Когда счетчики DoS вашего маршрутизатора превышают по умолчанию или установленные значения, маршрутизатор перезагружает одно старое полуоткрытое соединение для каждого нового соединения, которое превышает настроенный max-incomplete или одноминутные максимальные значения, пока количество полуоткрытых сеансов не опускается ниже низких значений max-incomplete. Маршрутизатор передает сообщение системного журнала, если регистрация включена, и если система предотвращения вторжений (IPS) настроена на маршрутизаторе, межсетевой экран - маршрутизатор передает сообщение с подписью DoS через стандарт Security Device Event Exchange (SDEE). Если параметры DoS не отрегулированы к нормальному поведению вашей сети, действие стандартной сети может инициировать механизм защиты от атак DoS, который вызывает сбои приложения, плохую производительность сети и высокую загрузку ЦП на маршрутизаторе межсетевого экрана Cisco IOS.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Атака Denial of Service, настраивающаяся для классики программного обеспечения Cisco IOS (IP Inspect) межсетевой экран и система предотвращения вторжений

Межсетевой экран обычного ПО Cisco IOS поддерживает глобальный набор счетчиков DoS для маршрутизатора, и все сеансы межсетевого экрана для всей политики межсетевого экрана на всех интерфейсах применены к глобальному набору счетчиков межсетевого экрана.

Когда Классический Межсетевой экран применен, контроль Межсетевого экрана Классики Cisco IOS обеспечивает защиту от атаки DoS по умолчанию. Защита от атак DoS включена

на всех интерфейсах, где контроль применен в направлении, в котором межсетевой экран применен для каждого сервиса или протокола, который политика межсетевого экрана настроена для осмотра. Классический Межсетевой экран предоставляет несколько корректируемых значений для защиты против атак DoS. Устаревшие настройки по умолчанию (от образов программного обеспечения до Выпуска 12.4 (11) T) показанный в Таблице 1 может вмешаться в операцию исправной сети, если они не настроены для соответствующего уровня активности сети в сетях, где скорости подключения превышают настройки по умолчанию. Параметры настройки DoS могут быть просмотрены с **config ip inspect exec command show**, и параметры настройки включены с выходными данными **sh ip inspect все**.

CBAC использует таймауты и пороги для определения, сколько времени управлять информацией о состоянии для сеанса, а также определить, когда отбросить сеансы, которые не становятся полностью установленными. Эти таймауты и пороги применяются глобально ко всем сеансам.

Пределы защиты от атак DoS межсетевого экрана классики таблицы 1 по умолчанию		
Значение защиты от атак DoS	**До 12.4 (11) T/12.4 (10)**	**12.4 (11) T/12.4 (10) и позже**
максимальное значение max-incomplete	500	Неограниченный
низкое значение max-incomplete	400	Неограниченный
одноминутное *максимальное значение*	500	Неограниченный
одноминутное *низкое значение*	400	Неограниченный
значение хоста tcp max-incomplete	50	Неограниченный

Маршрутизаторы, настроенные для применения Cisco IOS Осведомленный о VRF Межсетевой экран, поддерживают один набор счетчиков для каждого VRF.

Счетчик для “ip inspect one-minute high” и “ip inspect one-minute low” поддерживает сумму всего TCP, UDP и попыток подключения Протокола ICMP в течение предшествующей минуты после использования маршрутизатора, были ли соединения успешны или нет. Возрастающая скорость подключения может быть показательной из заражения червя на частной сети или предпринятой атаки DoS на сервер.

В то время как вы не можете “отключить” защиту от атак DoS своего межсетевого экрана, можно отрегулировать защиту от атак DoS так, чтобы это не вступало в силу, пока очень большое число полуоткрытых соединений не присутствует в таблице сеанса межсетевого экрана - маршрутизатора.

Защита с помощь межсетевого экрана DoS

Выполните эту процедуру для настройки защиты от атак DoS межсетевого экрана к действию сети:

1. Убедитесь, что ваша сеть не заражена вирусами или червями, которые могут привести к ошибочно большим значениям полуоткрытого соединения или предпринятым скоростям подключения. Если ваша сеть не является “чистой”, нет никакого способа должным образом отрегулировать защиту от атак DoS вашего межсетевого экрана. Необходимо наблюдать действие сети в течение периода типичного действия. При настройке параметров настройки защиты от атак DoS сети в течение периода низкой или простаивающей активности сети уровни нормальной работы, вероятно, превышают параметры настройки защиты от атак DoS.
2. Придайте большое значение max-incomplete к очень максимальным значениям: **`ip inspect max-incomplete high 20000000 ip inspect one-minute high 100000000 ip inspect tcp max-incomplete host 100000 block-time 0`** Это препятствует тому, чтобы маршрутизатор предоставил защиту от атак DoS, в то время как вы наблюдаете образцы соединения своей сети. Если вы хотите оставить защиту от атак DoS отключенной, остановите эту процедуру теперь.**Примечание:** Если ваш маршрутизатор выполняет программное обеспечение Cisco IOS версии 12.4(11)T или позже, или 12.4 (10) или позже, вы не должны повышать значения защиты от атак DoS по умолчанию; они уже установлены в их ограничения максимального значения по умолчанию.**Примечание:** Если вы хотите включить более агрессивному TCP специфичное для хоста предотвращение атаки Denial of Service, которое включает блокирование инициирования соединения к хосту, необходимо установить блочно-разовое, заданное в **команде ip inspect tcp max-incomplete host**
3. Очистите статистику межсетевого экрана Cisco IOS с этой командой: **`show ip inspect statistics reset`**
4. Оставьте маршрутизатор настроенным в этом состоянии в течение некоторого времени, возможно целых 24 - 48 часов, таким образом, можно наблюдать сетевой образец по крайней мере за один полный день цикла действия типичной сети.**Примечание:** В то время как значения отрегулированы к очень высоким уровням, ваша сеть не извлекает выгоду из защиты от атак DoS IPS или межсетевого экрана Cisco IOS.
5. После периода наблюдения проверьте, что DoS отвечает этой командой: **`show ip inspect statistics`** Параметры, которые необходимо наблюдать, с которым можно настроить защиту от атак DoS, выделены **полужирным**:`Packet inspection statistics`
   `[process switch:fast switch]`
  `tcp packets: [218314:7878692]`
  `udp packets: [501498:65322]`
   `packets: [376676:80455]`
   `packets: [5738:4042411]`
  `smtp packets: [11:11077]`
  `ftp packets: [2291:0]`
`Interfaces configured for inspection 2`
`Session creations since subsystem`
   `startup or last reset 688030`
`Current session counts`
   `(estab/half-open/terminating) [0:0:0]`
`Maxever session counts (estab/half-open/terminating) [207:56:35]` `Last session created 00:00:05 Last statistic reset never Last session creation rate 1` **`Maxever session creation rate 330`** `Last half-open session total 0 TCP reassembly statistics received 46591 packets out-of-order; dropped 16454 peak memory usage 48 KB; current usage: 0 KB peak queue length 16`

6. Настройте **ip inspect max-incomplete high** к значению на 25 процентов выше, чем обозначенное число сеансов maxever полуоткрытое значение вашего маршрутизатора. A #1. 25 высот 25 процентов предложений множителя выше наблюдаемого состояния, например:`Maxever session counts (estab/half-open/terminating) [207:56:35]`
`56 * 1.25 = 70`
Настройка:`router(config) #ip inspect max-incomplete high 70`**Примечание:** Этот документ описывает использование множителя 1.25 раза типичного действия вашей сети для установления пределов для привлечения защиты от атак DoS. Если вы наблюдаете свою сеть в пиках действия типичной сети, это должно предоставить достаточное место для предотвращения активации защиты от атак DoS маршрутизатора под почти нетипичными обстоятельствами. Если ваша сеть периодически видит большие пакеты легитимной активности сети, которые превышают это значение, маршрутизатор затрагивает возможности защиты от атак DoS, которые могут вызвать негативное воздействие на части сетевого трафика. Необходимо контролировать журналы маршрутизатора для обнаружений действия DoS и отрегулировать **ip inspect max-incomplete high** и/или пределы **ip inspect one-minute high**, чтобы избежать инициировать DoS, после того, как вы решаете, что с пределами встретились в результате легитимной активности сети. Можно распознать приложение защиты от атак DoS присутствием сообщений журнала, таких как это:
7. Настройте **ip inspect max-incomplete low** к значению ваш маршрутизатор, отображенный для его числа сеансов maxever полуоткрытое значение, например:`Maxever session counts (estab/half-open/terminating) [207:56:35]`Настройка:`router(config) #ip inspect max-incomplete low 56`
8. Счетчик для **ip inspect one-minute high** и **одна минута низко** поддерживает сумму всего TCP, UDP и попыток подключения Протокола ICMP в течение предшествующей минуты после работы маршрутизатора, были ли соединения успешны или нет. Возрастающая скорость подключения может быть показательной из заражения червя на частной сети или предпринятой атаки DoS на сервер. Дополнительная инспекционная статистическая величина была добавлена к **выходным данным statistics show ip inspect** в 12.4 (11) T и 12.4 (10) для раскрытия верхнего порога для скорости создания сеанса. При выполнении Cisco IOS Software Release ранее, чем 12.4 (11) T или 12.4 (10) инспекционные статистические данные не содержат эту линию:`Maxever session creation rate [value]`Cisco IOS Software Release до 12.4 (11) T и 12.4 (10) не поддерживают значение для инспекционной скорости подключения одной минуты maxever, таким образом, необходимо вычислить значение, вы применяетесь на основе наблюдаемых “значений” числа сеансов maxever. Наблюдения за несколькими сетями, которые используют проверку трафика потоком Выпуска 12.4 (11) T межсетевого экрана Cisco IOS в производстве, показали, что скорости создания сеанса Maxever имеют тенденцию превышать сумму трех значений (установленный, полуоткрытый, и завершающийся) в “числе сеансов maxever” примерно на десять процентов. Для вычисления значения ip inspect one-minute low умножьте обозначенное “установленное” значение на 1.1, например:`Maxever session counts (estab/half-open/terminating) [207:56:35]`
`(207 + 56 + 35) * 1.1 = 328`
Настройка:`ip inspect one-minute low 328`Если маршрутизатор выполняет программное обеспечение Cisco IOS версии 12.4(11)T или позже, или 12.4 (10) или позже, можно просто применить значение, показанное в “Статистической величине контроля”

скорости создания сеанса Maxever:`Maxever session creation rate 330`Настройка:`ip inspect one-minute low 330`

9. Вычислите и настройте **ip inspect one-minute high**. Значение ip inspect one-minute high должно быть на 25 процентов больше, чем расчетное одноминутное низкое значение, например:`ip inspect one-minute low (330) * 1.25 = 413` Настройка:`ip inspect one-minute high 413`**Примечание:** Этот документ описывает использование множителя 1.25 раза типичного действия вашей сети для установления пределов для привлечения защиты от атак DoS. Если вы наблюдаете свою сеть в пиках действия типичной сети, это должно предоставить достаточное место для предотвращения активации защиты от атак DoS маршрутизатора под почти нетипичными обстоятельствами. Если ваша сеть периодически видит большие пакеты легитимной активности сети, которые превышают это значение, маршрутизатор затрагивает возможности защиты от атак DoS, которые могут вызвать негативное воздействие на части сетевого трафика. Необходимо контролировать журналы маршрутизатора для обнаружений действия DoS и отрегулировать **ip inspect max-incomplete high** и/или пределы **ip inspect one-minute high**, чтобы избежать инициировать DoS, после того, как вы решаете, что с пределами встретились в результате легитимной активности сети. Можно распознать приложение защиты от атак DoS присутствием сообщений журнала, таких как это:
10. Необходимо определить значение для **ip inspect tcp max-incomplete host** в соответствии со знанием возможности серверов. Этот документ не может предоставить рекомендации для конфигурации защиты от атак DoS на хост, так как это значение значительно различается на основе производительности программного и аппаратного обеспечения конечного узла. Если вы не уверены в соответствующих пределах для настройки для защиты от атак DoS, у вас эффективно есть две опции, с которыми можно определить пределы DoS:Предпочтительная опция должна настроить основанную на маршрутизаторе защиту от атак DoS на хост к максимальному значению (меньше чем или равный максимальному значению 4,294,967,295) и применить специфичную для хоста защиту, предлагаемую операционной системой каждого хоста или внешней основанной на хосте Системы Защиты от проникновения, такой как Cisco Security Agent (CSA).Исследуйте действие, и производительность входит в систему ваших сетевых хостов, и определите их пиковую поддерживаемую скорость подключения. Так как Классический Межсетевой экран только предлагает один глобальный счетчик, необходимо применить максимальное значение, которое вы определяете после проверки всех сетевых хостов для их скоростей максимального числа подключений. Все еще желательно, чтобы вы использовали специфичные для ОС пределы действия и основанный на хосте IPS, такие как CSA.**Примечание:** Межсетевой экран Cisco IOS предлагает ограниченную защиту от направленных атак на определенную операционную систему и уязвимости приложения. Защита от атак DoS межсетевого экрана Cisco IOS не предлагает гарантии защиты от компромисса на сервисах конечного узла, которые представлены потенциально враждебным окружениям.
11. Контролируйте действие защиты от атак DoS ваша сеть. Идеально, необходимо использовать сервер системного журнала, или идеально, Отслеживание и сообщение станций (MARS) Cisco для записи вхождений обнаружения атак DoS. Если обнаружение происходит очень часто, необходимо контролировать и отрегулировать параметры защиты от атак DoS.Для получения дополнительной информации об атаках DoS SYN TCP, обратитесь к Определению Стратегий Защитить Против Атак "отказ в обслуживании" SYN TCP.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация