Устранение неполадок высокой загрузки ЦП в процессе IP Input

Содержание

Введение

В этом документе описан поиск и устранение ошибок высокого коэффициента использования CPU вследствие процесса ввода IP.

Примечание: Этот документ не предоставляет стратегии предотвратить различные типы атак.

Предварительные условия

Требования

Cisco рекомендует считать Высокую загрузку ЦП Устранения проблем на маршрутизаторах Cisco перед переходом этот документ.

Используемые компоненты

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

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные

обозначения технических терминов Cisco.

Входные данные IP

Процесс ПО Cisco IOS®, называемый «IP-вход», осуществляет коммутацию процессов IP-пакетов. Если процесс IP-входа использует слишком много ресурсов ЦП, маршрутизатор осуществляет коммутацию большого объема IP-трафика. Проверьте следующее:

- **Прерывание коммутации отключено на интерфейсе (или интерфейсы), который имеет (имеют) много трафика**Прерывание коммутации обращается к использованию алгоритмов коммутации кроме коммутации в контексте процесса. Например, быстрая коммутация, оптимальная коммутация, коммутация Cisco Express Forwarding и т. д. (дополнительную информацию см. в разделе Основы настройки производительности). **По выходным данным команды show interfaces switching определите интерфейс, перегруженный трафиком**. **По выходным данным команды show ip interface можно определить метод коммутации, используемый на каждом интерфейсе**. Отмените запрет на коммутацию при прерывании на этом интерфейсе. Следует помнить, что обычная быстрая коммутация настраивается на выходных интерфейсах: если для интерфейса настроена быстрая коммутация, пакеты, выходящие из такого интерфейса, являются пакетами быстрой коммутации. Метод коммутации Cisco Express Forwarding настраивается на входных интерфейсах. Чтобы создать базу данных переадресации FIB и записи таблицы соседей для определенного интерфейса, настройте коммутацию экспресс-пересылки Cisco на всех интерфейсах, связанных маршрутом с этим интерфейсом.
- **Быстрое коммутирование на том же интерфейсе отключено**Если интерфейс имеет много вторичных адресов или подинтерфейсов и существует много трафика, полученного от интерфейса и предназначенного для адреса на том же самом интерфейсе, то все те пакеты являются процессной коммутацией. **В этой ситуации необходимо включить ip route-cache same-interface на этом интерфейсе.** Когда используется коммутация Cisco Express Forwarding, нет необходимости отдельно включать коммутацию Cisco Express Forwarding на том же интерфейсе.
- **Быстрое коммутирование на маршрутизации в соответствии с политикой обеспечения интерфейса отключено**Если route-map был настроен на интерфейсе, и много трафика обрабатывается route-map, то коммутаторы процесса маршрутизатора этот трафик. **В этой ситуации необходимо включить параметр ip route-cache policy на этом интерфейсе**. Проверьте ограничения, упомянутые в "разделе" Маршрутизации на основе политик Быстрой коммутации Включения Маршрутизации на основе политик Настройки.
- **Трафик, который не может быть коммутируемым с прерываниями, поступает**Это может быть любым из перечисленных типов трафика. Чтобы получить дополнительную информацию щелкните соответствующую ссылку.Пакеты, для которых пока нет записи в кэше коммутацииДаже если быстро, оптимум или Быстрое переключение ретрансляций CISCO (CEF) настроен, пакет, с которым там не идет ни в какое сравнение в кэше быстрой коммутации, или FIB и таблицы соседей обработаны. Затем создается запись в соответствующем кэше или таблице, а все последующие пакеты, соответствующие этим критериям, обрабатываются быстрой, оптимальной или CEF-коммутацией. В нормальных условиях эти обрабатываемые пакеты не приводят к чрезмерной загруженности ЦП. Однако, если в сети имеется устройство, которое: 1) генерирует пакеты с чрезвычайно высокой скоростью для устройств, достижимых через

маршрутизатор, и 2) использует другой IP-адрес источника или назначения, для этих пакетов нет соответствия в кэше коммутации или таблице, тогда пакеты обрабатываются процессом IP-входа (если настроена коммутация NetFlow, TCP порты источника и назначения также сравниваются с записями в кэше NetFlow). Устройство, являющееся источником пакетов, может находиться в аварийном состоянии или осуществлять атаку.(*) Только с подобранными смежностями. См. скоростную маршрутизацию Cisco для получения дополнительной информации о смежностях скоростной маршрутизации Cisco.Пакеты, предназначенные маршрутизаторуЭто примеры пакетов, предназначенные для маршрутизатора:Обновления маршрутизации, которые поступают с чрезвычайно высокой скоростью. Если маршрутизатор получает чрезвычайно большое число обновлений маршрутизации, которые необходимо обработать, эта задача может привести к перегрузке ЦП. Как правило, этого не происходит в стабильной сети. Способ сбора данных зависит от настроенного протокола маршрутизации. **Однако целесообразно начать регулярно проверять выходные данные команды show ip route summary.** Быстро меняющиеся значения – признак нестабильности сети. Частые изменения в таблице маршрутизации означают повышенную обработку протокола маршрутизации, что приводит к повышенной загрузке ЦП. Дополнительную информацию о решении этой проблемы см. в разделе Поиск и устранение неисправностей TCP/IP в руководстве по поиску и устранению неисправностей объединенной сети.Любой другой тип трафика, предназначенного для маршрутизатора. Проверьте, кто зарегистрирован на маршрутизаторе, и просмотрите действия пользователя. Если кто-то зарегистрирован и выполняет команды, которые выдают большой объем выходных данных, за высокой загрузкой ЦП процессом IP-входа последует еще более высокая загрузка ЦП процессом Virtual Exec.Атака на основе подмены адресов (спуфинг). **Чтобы идентифицировать проблему, определите объем IP-трафика с помощью команды show ip traffic.** Если возникла проблема, становится значительным число полученных пакетов с локальным адресатом. **Далее проверьте выходные данные команд show interfaces и show interfaces switching, чтобы определить интерфейс, принимающий пакеты. После определения принимающего интерфейса, включите ip accounting на исходящем интерфейсе и проверьте наличие шаблона.** При атаке адрес источника почти всегда отличается, а адрес назначения остается неизменным. Для временного решения проблемы можно настроить список доступа (предпочтительно на устройстве, ближайшем к источнику пакетов), но полное решение заключается в отслеживании устройства, являющегося источником пакетов, и остановки атаки.Широковещательный трафикПроверьте количество транслируемых пакетов в выходных данных **команды show interfaces**. Если сравнить число широковещательных пакетов с общим числом пакетов, полученных интерфейсом, можно сделать вывод о чрезмерности числа широковещательных пакетов. Если к маршрутизатору подключена локальная сеть с несколькими коммутаторами, тогда это может указывать на проблему с связующим деревом.IP-пакеты с параметрамиПакеты, требующие трансляции протоколовМногоканальный протокол "точка-точка" (поддерживаемый в Быстром переключении ретрансляций CISCO)Сжатый трафикЕсли существует Сервисный адаптер No Compression (CSA) в маршрутизаторе, сжатые пакеты должны быть процессной коммутацией.Зашифрованный поток данныхЕсли нет никакого Модуля сервиса шифрования (ESA) в маршрутизаторе, зашифрованные пакеты должны быть процессной коммутацией.Пакеты, которые проходят последовательные интерфейсы с инкапсуляцией X.25В комплекте протокола X.25 управление потоками внедрено на втором уровне Открытого взаимодействия системы (OSI).

- Большое число пакетов, поступающих с чрезвычайно высокой скоростью для адресата в непосредственно подключенной подсети, для которого нет записи в таблице протокола разрешения адресов (ARP). Это не должно иметь место в случае TCP-трафика из-за оконного механизма, однако может происходить с UDP трафиком. Чтобы определить проблему, повторите действия, рекомендованные для отслеживания атак спуфинга.
- Через маршрутизатор передается большой объем многоадресного трафика. К сожалению, простого способа определения объема многоадресного трафика нет. Команда show ip traffic отображает только сводную информацию. Однако, если на маршрутизаторе настроена многоадресная маршрутизация, можно включить быструю коммутацию многоадресных пакетов командой настройки интерфейса ip mroute-cache (быстрая коммутация многоадресных пакетов выключена по умолчанию).
- Превышен лимит подписки для маршрутизатора. Если маршрутизатор используется чрезмерно интенсивно и не может обработать объем трафика, попробуйте перераспределить нагрузку на другие маршрутизаторы или установите маршрутизатор с более высокой производительностью.
- На маршрутизаторе настроено преобразование сетевых IP-адресов и большое число DNS пакетов передается через маршрутизатор. UDP или пакеты TCP с портом источника или назначения 53 (DNS) всегда плывутся на плоскодонке к уровню процесса NAT.
- Других типов пакетов, переданных на обработку, нет.
- Существует фрагментация Дейтаграммы IP. Существует маленькое увеличение ЦП и служебных данных памяти из-за фрагмента дейтаграммы IP. См. Фрагментацию ip Решения, MTU, MSS и Проблемы PMTUD с GRE и IPSEC для получения дополнительной информации о том, как решить эту проблему.

Чем бы ни была вызвана высокая загрузка ЦП в процессе IP-входа, источник проблемы можно определить путем отладки IP-пакетов. Поскольку загрузка ЦП уже высокая, процесс отладки необходимо осуществлять очень осторожно. Процесс отладки порождает большое число сообщений, поэтому следует настраивать только logging buffered.

Ведение журнала на консоли приводит к излишнему увеличению прерываний для ЦП и повышает его загрузку. Ведение журнала на узле (или контролирующее ведение журнала) генерирует дополнительный трафик на интерфейсах.

Процесс отладки можно начать с команды debug ip packet detail. Этот сеанс должен длиться не более 3 – 5 секунд. Сообщения отладки записываются в буфер регистрации. Перехват типового сеанса Отладки IP предоставлен в разделе Примера сеанса отладки IP - пакета этого документа. После того как будет найдено исходное устройство, от которого поступают нежелательные IP-пакеты, можно будет отключить его от сети, или создать на маршрутизаторе список доступа, при помощи которого будет происходить отбрасывание пакетов с этого устройства.

Пример сеанса отладки IP-пакета

Настроенные приемники данных протоколирования необходимо сначала проверить командой show logging:

```
router#show loggingSyslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: level debugging, 52 messages logged Monitor logging: level debugging, 0 messages logged
```

```
Buffer logging: level debugging, 148 messages logged Trap logging: level informational, 64
message lines logged Logging to 192.168.100.100, 3 message lines logged Logging to
192.168.200.200, 3 message lines logged --More--
```

Отключите все приемники данных протоколирования за исключением буфера регистрации и очистите этот буфер:

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#no logging console router(config)#no logging monitor router(config)#no logging
192.168.100.100 router(config)#no logging 192.168.200.200 router(config)#^Z router#clear logging
Clear logging buffer [confirm]router#
```

Для облегчения восприятия выходных данных отладки следует включить дату и время в миллисекундах:

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#service timestamps log datetime msec router(config)#service timestamps debug
datetime msec router(config)#end router#
```

Теперь можно начать сеанс отладки:

```
router#debug ip packet detail IP packet debugging is on (detailed)
```

Отладка должна длиться не более 3 – 5 секунд. **Сеанс отладки можно остановить командой undebug all:**

```
router#undebug all All possible debugging has been turned off
```

Результаты можно проверить командой show logging:

```
router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: disabled Monitor logging: disabled Buffer logging: level debugging, 145 messages logged
Trap logging: level informational, 61 message lines logged Log Buffer (64000 bytes): *Mar 3
03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204 (Ethernet0/0), g=10.200.40.1,
len 100, forward *Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.324: IP:
s=192.168.40.53 (Ethernet0/1), d=144.254.2.205 (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1),
d=144.254.2.206 (Ethernet0/0), g=10.200.40.1, len 100, forward *Mar 3 03:43:27.328: ICMP type=8,
code=0 ...
```

Содержание журнала:

- Пакет принимается каждые четыре миллисекунды
- IP-адрес источника - 192.168.40.53
- Пакеты поступили на интерфейс Ethernet0/1
- У пакетов разные IP-адреса назначения
- Пакеты были отправлены на интерфейс Ethernet0/0
- IP-адрес следующего узла - 10.200.40.1
- Пакеты были запросами ICMP (type=8)В данном примере вы видите, что высокая загрузка ЦП в Процессе IP - вводе была вызвана затоплением ICMP-пакетами (ping flood) от IP-адреса 192.168.40.53.Затопление пакетами SYN можно без труда обнаружить, поскольку наличие флага SYN указано в выходных данных отладки:
```
*Mar 3 03:54:40.436: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204 (Ethernet0/0),
g=10.200.40.1, len 44, forward *Mar 3 03:54:40.440: TCP src=11004, dst=53,
seq=280872555, ack=0, win=4128 SYN
```

Дополнительные сведения

- Решение проблемы высокой загрузки CPU на маршрутизаторах Cisco
- Команда show processes

- Высокий уровень загрузки CPU при работе коммутаторов Catalyst 2900XL/3500XL
- Основы регулировки пропускной способности
- Cisco Systems – техническая поддержка и документация