ASA 8.3 и более поздние версии: Наблюдение и устранение неполадок производительности

Содержание

Введение

В этом документе приведена информация о командах ASA, которые можно использовать для отслеживания и устранения проблем с производительностью на устройстве Cisco Adaptive Security Appliance (ASA).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе приведены для устройства Cisco Adaptive Security Appliance (ASA) с установленной версией 8.3 или более поздними версиями.

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. Перед выполнением любых команд в активной сети необходимо осознавать потенциальные последствия их применения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Устранение неполадок

Чтобы обнаружить и устранить проблемы, вызывающие снижение производительности, выполните проверку основных областей, приведенных в настоящем разделе.

Примечание. Если вы располагаете выходными данными команды show с устройства Cisco, можно использовать анализатор Cisco CLI (только для зарегистрированных клиентов), чтобы отобразить возможные проблемы и их решения. Анализатор Cisco CLI поддерживает отдельные команды show. Использовать анализатор Cisco CLI могут только зарегистрированные клиенты, которые выполнили вход в учетную запись Cisco и включили JavaScript в своем браузере.

Настройка скорости и дуплексного режима

На устройстве безопасности предварительно настроено автоматическое обнаружение определение скорости и настроек дуплексного режима в интерфейсе. Тем не менее, в некоторых случаях не удается выполнить процесс автосогласования, что приводит к несоответствию скорости и дуплексного режима (и к снижению производительности). Для критически важной сетевой инфраструктуры, Cisco аппаратно программирует скорость и дуплексный режим на каждом интерфейсе, так что вероятность возникновения ошибок минимальна. Обычно эти устройства не перемещаются, поэтому если настроить их правильно изначально, в дальнейшем не будет необходимости их менять.

В любом сетевом устройстве скорость соединения может быть определена, в то время как дуплексный режим нужно согласовывать. Если два сетевых устройства настроены на автоматическое согласование скорости и дуплекса, они отправляют друг другу кадры (так называемые импульсы быстрого канала, FLP), которые объявляют их возможности скорости и дуплекса. Для неосведомленного партнера по каналу эти импульсы воспринимаются как обычные кадры со скоростью 10 Мбит/с. Для устройства, которое может декодировать импульсы, в FLP содержатся все параметры скорости и дуплекса, которые предоставляет партнер по каналу. Станция, получающая FLP, подтверждает кадры, после чего устройства взаимно соглашаются на установку предельных для обоих параметров скорости и дуплекса. Если одно из устройств не поддерживает автосогласование, другое устройство получает импульсы FLP и переходит в режим параллельного обнаружения. Чтобы определить скорость партнера, устройство "слушает" длину импульсов, а затем устанавливает соответствующую скорость. Проблема возникает при настройке дуплекса. Поскольку дуплексный режим требует согласования, устройство, для которого настроено автоматическое согласование, не может определить настройки на другом устройстве. Таким образом, по умолчанию используется полудуплексный режим, как указано в стандарте IEEE 802.3u.

Например, при настройке автоматического согласования в интерфейсе ASA и подключении интерфейса к коммутатору, для которого жестко закодирована скорость 100 Мбит/с и полнодуплексный режим, ASA отправляет импульсы быстрого соединения (FLP). Однако ответа от коммутатора не последует, т.к. режим дуплекса и параметры скорости для него жестко заданы на аппаратном уровне и он не принимает участия в согласовании. Поскольку

ASA не получает ответа от коммутатора, ASA переходит в режим параллельного обнаружения и определяет длину импульсов в кадрах, отправляемых коммутатором. То есть, ASA определяет, что для коммутатора настроена скорость 100 Мбит/с, и задает соответствующую скорость интерфейса. Однако учитывая, что коммутатор не обменивается импульсами быстрого соединения, ASA не может определить, способен ли коммутатор запустить полнодуплексный режим. Таким образом, ASA задает для интерфейса дуплексный или полудуплексный режим, как указано в стандарте IEEE 803.2u. Поскольку для коммутатора жестко закодирована скорость 100 Мбит/с и полнодуплексный режим и ASA только что автоматически согласовал скорость 100 Мбит/с и полудуплексный режим (как и предполагалось), в результате возникает несоответствие дуплексных режимов, которое может вызвать серьезные проблемы с производительностью.

Несоответствие скорости или дуплекса часто обнаруживается через повышение значений счетчиков ошибок в данных интерфейсах. Наиболее распространенными ошибками являются ошибки кадров, контроля циклическим избыточным кодом (CRC) и карликовых пакетов (с недопустимо малой величиной). Эти значения на интерфейсе увеличиваются из-за несогласованности параметров дуплекса и скорости или проблем с кабелем. Чтобы продолжить, необходимо устранить эту проблему.

Пример

```
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
       379 input errors, 107 CRC, 273 frame, 0 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

Нагрузка на CPU

Если вы заметили, что система потребляет большой объем ресурсов ЦП, выполните следующие действия для устранения проблемы:

1. **Убедитесь что значение счетчика подключений в show xlate count невелико.**

2. Убедитесь, что блок памяти функционирует нормально.

3. Убедитесь, что количество списков ACL увеличилось.

4. **Выполните команду show memory detail и убедитесь в том, что ASA потребляет нормальный объем ресурсов памяти.**

5. **Убедитесь, что значения счетчиков в show processes cpu-hog и show processes memory соответствуют норме.**

6. Любой хост как перед устройством защиты, так и за ним может создавать вредоносный или избыточный трафик, который может быть связан с широковещательной рассылкой и групповой адресацией и вызывать высокий коэффициент загрузки ЦП. **Чтобы решить эту проблему, необходимо настроить список доступа для запрета трафика между хостами (сквозного) и проверить нагрузку.**

7. Проверьте настройки дуплексного режима и скорости в интерфейсах ASA. Несоответствие параметров удаленных интерфейсов может быть причиной повышенной загрузки CPU.

   На данном примере показана ситуация, возникающая при несоответствии параметров скорости, что выражается в повышенном количестве входных ошибок и перегрузок. **Для определения ошибок используйте команду show interface:**

```
Ciscoasa#sh int GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
       7186 input errors, 0 CRC, 0 frame, 7186 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

   Чтобы решить проблему, установите параметр скорости на auto (автоматически) в соответствующем интерфейсе.

   Примечание. Cisco рекомендует дать команду ip verify reverse-path interface на всех интерфейсах, что приведет к отбрасыванию пакетов с недопустимым адресом

источника и снижению загрузки CPU. Это действие применяется также в случаях, когда в FWSM возникают проблемы, связанные с высоким потреблением ресурсов ЦП.

8. ,Другой причиной высокой загрузки ЦП может быть слишком большое количество маршрутов групповой адресации. **Выполните команду show mroute , чтобы проверить, не получает ли ASA слишком большое количество многоадресных маршрутов.**

9. **Для получения сведений о случаях DoS-атак ("отказ в обслуживании") в сети, которые могут свидетельствовать о вирусной атаке, используйте команду show local-host.**

10. Высокая загрузка ЦП может быть связана с ошибкой с идентификатором Cisco CSCsq48636. Дополнительные сведения см. в описании ошибки с идентификатором Cisco CSCsq48636 (только для зарегистрированных клиентов).

Примечание. Если вышеуказанный способ не помогает устранить проблему, обновите платформу ASA в соответствии с требованиями. Дополнительные сведения о возможностях и функциях платформы Adaptive Security Appliance (ASA) см. в разделе Техническая документация по устройствам безопасности Cisco ASA серии 5500. Свяжитесь с TAC (только для зарегистрированных клиентов) для получения дополнительной информации.

Высокая загрузка памяти

Ниже приводятся возможные причины высокой загрузки памяти и некоторые решения этой проблемы:

- **Регистрация событий:** Регистрация событий может задействовать значительные ресурсы памяти. Чтобы избежать этой проблемы, выполняйте установку и регистрацию всех событий на внешнем сервере, например, на сервере системного журнала.
- **Утечка памяти:** Известная проблема ПО устройства защиты, приводящая к интенсивному использованию ресурсов памяти. Для решения этой проблемы требуется обновить ПО устройства защиты.
- **Включение режима отладки:** При включенном режиме отладки задействуются большие ресурсы памяти. , `undebug all.`
- **Блокирующие порты:** Блокирующие порты во внешнем интерфейсе устройства безопасности заставляют устройство безопасности потреблять больше памяти для блокирования пакетов, проходящих через указанные порты. Чтобы устранить эту проблему, заблокируйте неправомерный трафик на стороне интернет-провайдера.

- **Обнаружение угроз:** Функция обнаружения угроз включает различные уровни сбора статистики по разным угрозам, а также обнаружение сканирований, которое позволяет выявить сканирование, выполняемое тем или иным хостом. **Отключите эту функцию, чтобы снизить потребление памяти.**

Режимы PortFast, Channeling и Trunking

Во многих коммутаторах, в частности, в коммутаторах Cisco с операционной системой Catalyst (OS), предусмотрена функция автообнаружения и самонастройки (plug-and-play). По сути многие параметры порта по умолчанию нежелательно использовать, если ASA физически подключено к коммутатору. Например, на коммутаторах с ОС Catalyst включение channeling (объединения каналов) и trunking (магистрального соединения) включается автоматически (Auto), а режим PortFast отключен. Если ASA подключается к коммутатору, на котором запущена ОС Catalyst OS, отключите создание каналов и магистралей и включите PortFast.

Режим объединения каналов, называемый также Fast EtherChannel или Giga EtherChannel, используется для объединения двух или нескольких физических портов в логическую группу для увеличения объема потока данных по каналу. Если порт настроен на автоматическое объединение каналов, он отправляет кадры по протоколу агрегации портов (Port Aggregation Protocol, PAgP) как только канал становится активным, чтобы определить, участвует ли он в объединении каналов. Эти PAgP-кадры могут стать источником проблем в случае, если другое устройство выполняет в это время автоматическое согласование скорости и дуплекса на данном канале. Если на порте установлено автоматическое объединение каналов, это может вызвать трехсекундную задержку передачи трафика через данный порт после включения канала.

> **Примечание. В коммутаторах Catalyst серии XL автоматическое объединение каналов по умолчанию не установлено.** По этой причине необходимо отключить создание каналов на всех портах коммутатора, подключенных к ASA.

Магистральное соединение, которое относится к общим протоколам магистральных каналов (другое название — межкоммутаторное соединение (ISL) или Dot1q) объединяет несколько сетей VLAN на одиночном порту (или канале). Транкинг обычно используется между двумя коммутаторами, когда оба коммутатора имеют более одной назначенной VLAN. Если порт настроен на автоматическое магистральное соединение, он рассылает кадры протокола динамического магистрального соединения (DTP; Dynamic Trunking Protocol) при включении канала, чтобы определить, нужно ли порту, к которому он подключается, группировать магистрали. Данные кадры DTP могут вызвать проблемы автосогласования канала. Если на порте установлено автоматическое магистральное соединение, это вызывает 15-секундную задержку передачи трафика через данный порт после включения канала.

Режим PortFast, также называемый Fast Start, — это функция, которая сообщает коммутатору о подключении устройства уровня 3 из порта коммутатора. В этом случае 30-секундное ожидание порта (15 секунд на "прослушивание" и 15 — на "обучение"), заданное по умолчанию, отменяется, а порт переводится в состояние передачи немедленно после включения канала. Важно иметь ввиду, что при включении режима PortFast связующее дерево не отключается. Оно остается активным на данном порту. При включении PortFast коммутатор лишь получает сведения о том, что на другом конце канала нет подключенных коммутаторов или концентраторов (т.е. устройств только уровня 2). Коммутатор обходит обычную 30-секундную задержку, одновременно пытаясь определить, возникнет ли в результате активации этого порта петля на втором уровне. После активации канала он все равно представлен в связующем дереве. Элементы BPDU будут отправляться с порта, а коммутатор будет продолжать прослушивать данный порт на наличие BPDU. По этой причине рекомендуется включить PortFast на всех портах коммутатора, которые подключены к ASA.

Примечание. В ОС Catalyst выпуска 5.4 и более поздних включена команда set port host <mod>/<port>, которая позволяет использовать одну команду для отключения объединения каналов и магистрального соединения и включения PortFast.

!--- преобразования сетевых адресов (NAT)

Всем сеансам NAT или NAT Overload (PAT) назначается слот трансляции (т. н. xlate). Эти xlate-слоты могут сохраняться даже после изменения правил NAT по отношению к ним. Это приводит к истощению слотов трансляции или непредсказуемому поведению трафика, который подвергается трансляции, или к обоим последствиям. В данном разделе поясняется, как просмотреть и удалить xlate-слоты в устройстве защиты.

Внимание. : Мгновенное прерывание потока трафика, проходящего через устройство, происходит при глобальном удалении слотов xlate с устройства безопасности.

Пример конфигурации ASA для PAT, которая использует IP-адрес внешнего интерфейса:

```
Ciscoasa#sh int GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
```

```
Input flow control is unsupported, output flow control is unsupported
MAC address 0013.c480.b2b8, MTU 1500
IP address 192.168.17.4, subnet mask 255.255.255.0
311981 packets input, 20497296 bytes, 0 no buffer
Received 311981 broadcasts, 157 runts, 0 giants
7186 input errors, 0 CRC, 0 frame, 7186 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
121 packets output, 7744 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 1 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/249)
output queue (blocks free curr/low): hardware (255/254)
```

Трафик, передаваемый через устройство защиты, почти всегда подвергается NAT. Просмотреть трансляции, используемые в устройстве защиты, можно с помощью команды show xlate:

```
Ciscoasa#show xlate

5 in use, 5 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

NAT from any:192.168.1.10 to any:172.16.1.1/24

    flags s idle 277:05:26 timeout 0:00:00
```

Слоты трансляции могут сохраняться даже после ключевых изменений. Чтобы удалить слоты текущей трансляции в устройстве защиты, используйте команду clear xlate:

```
Ciscoasa#clear xlate
```

```
Ciscoasa#show xlate
0 in use, 1 most used
```

Команда clear xlate удаляет всю текущую динамическую трансляцию в таблице xlate-слота. Чтобы удалить определенную IP-трансляцию, используйте команду clear xlate с ключевым словом global [ip-адрес].

Далее приведен пример конфигурации ASA для NAT:

```
Ciscoasa#show xlate
0 in use, 1 most used
```

Просмотрите выходные данные show xlate для трансляции с внутреннего 10.2.2.2 на глобальный внешний 10.10.10.10:

```
Ciscoasa#show xlate
2 in use, 2 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri
idle 62:33:57 timeout 0:00:30
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri
idle 62:33:57 timeout 0:00:30
```

Удалите трансляцию для глобального IP-адреса 10.10.10.10:

```
Ciscoasa# clear xlate global 10.10.10.10
```

В данном примере трансляция для IP-адресов от внутреннего 10.2.2.2 до внешнего глобального 10.10.10.10 удалена:

```
Ciscoasa#show xlate
1 in use, 2 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri
idle 62:33:57 timeout 0:00:30
```

Системные журналы

Системные журналы позволяют устранять неполадки на ASA. Cisco предлагает бесплатный сервер системных журналов для Windows NT — ASA Firewall Syslog Server (PFSS). Загрузить PFSS можно на странице Software Downloads (только для зарегистрированных пользователей).

Другие поставщики ПО, такие как Kiwi Enterprises, предлагают серверы системных журналов для других платформ Windows, например, Windows 2000 и Windows XP. В большинстве компьютеров с ОС UNIX или Linux серверы системных журналов установлены по умолчанию.

При настройке сервера системных журналов следует настроить ASA для получения журналов.

Пример:

```
logging on
logging host <ip_address_of_syslog_server> logging trap debugging
```

Примечание. В этом примере ASA настраивается для отправки на сервер системных журналов отладки (уровень 7) и более критически важных журналов. Поскольку в этих журналах ASA содержится больше всего данных, их следует использовать только в процессе диагностики и устранения неполадок. Для обычной работы настройте уровень регистрации на "Предупреждение" (уровень 4) или "Ошибка" (уровень 3).

При снижении производительности откройте системный журнал в текстовом файле и выполните поиск IP-адреса источника, связанного с данной проблемой производительности. (UNIX grep IP- .).) Проверьте наличие сообщений, указывающих на то, что внешний сервер пытался получить доступ к внутреннему IP-адресу на TCP-порте 113 (для протокола идентификации или Ident), но ASA отклонила пакет. Это сообщение должно выглядеть примерно так:

```
logging on
logging host <ip_address_of_syslog_server> logging trap debugging
```

Если вы видите это сообщение, выполните команду service resetinbound на ASA. ASA не отбрасывает пакеты в фоновом режиме; вместо этого эта команда заставляет ASA сразу сбрасывать все входящие подключения, запрещенные политикой безопасности. В данной ситуации сервер не будет ожидать пакет Ident, чтобы прервать TCP-соединение, он получит пакет перезагрузки сразу же.

SNMP

Мониторинг производительности Cisco ASA с помощью SNMP является рекомендуемым методом для корпоративных сетей. Cisco ASA поддерживает мониторинг сети с использованием SNMP версий 1, 2c и 3.

Можно настроить отправку trap-сообщений с устройства безопасности на сервер управления сетью (NMS) или использовать NMS для просмотра MIB на устройстве безопасности. MIB представляют собой набор определений, и устройство безопасности хранит базу данных значений для каждого такого определения. Дополнительные сведения см. в разделе Настройка SNMP на Cisco ASA.

Все поддерживаемые MIB для Cisco ASA приведены в перечне поддерживаемых ASA таблиц MIB . Таблицы MIB, указанные в этом списке, удобно использовать для мониторинга производительности:

- CISCO-FIREWALL-MIB---- Содержит объекты, используемые для переключения при отказе
- CISCO-PROCESS MIB---- Содержит объекты, используемые для анализа потребления ЦП
- CISCO-MEMORY-POOL-MIB---- Содержит объекты, используемые объектами памяти.

Обратный поиск DNS

Если ASA демонстрирует низкую производительность, проверьте наличие записей указателя системы доменных имен (PTR DNS) (т. н. записи обратного поиска DNS) на авторитетном сервере DNS для внешних адресов, которые используются ASA. К ним относятся все адреса в глобальном пуле трансляции сетевых адресов (NAT) (или внешний интерфейс ASA, если в интерфейсе перегрузка), все статические адреса и внутренние адреса (если для них не используется NAT). Некоторые приложения, например, серверы

протокола передачи файлов (File Transfer Protocol, FTP) и серверы Telnet, могут использовать обратный поиск DNS, чтобы определить, откуда пользователь вошел в сеть и является ли он допустимым узлом. Если проблему не удалось решить с помощью обратного поиска DNS, то вероятная причина падения производительности — превышение времени ожидания запроса.

Чтобы убедиться в том, что на этих хостах имеется запись PTR, выполните команду nslookup на ПК или компьютере с ОС UNIX, включив в поиск глобальный IP-адрес, который используется для подключения к Интернету.

Пример

```
% nslookup 198.133.219.25
25.219.133.198.in-addr.arpa     name = www.cisco.com.
```

После чего будет получен ответ, содержащий DNS-имя устройства, назначенного на данный IP-адрес. Если ответа получено не было, обратитесь к специалисту, ответственному за DNS, чтобы получить дополнительные записи PTR для каждого глобального IP-адреса.

Переполнения на интерфейсе

В случае неравномерности трафика возможно отбрасывание пакетов, если число пакетов превышает вместимость буфера FIFP на сетевой плате и буфера входного кольца. С этой проблемой поможет справиться включение кадров-пауз для управления потоками. Кадры-паузы (XOFF) и кадры XON генерируются автоматически сетевой платой, когда задействуется буфер FIFO. Кадр-пауза отправляется тогда, когда объем потребления буфера превышает максимально допустимый. Чтобы включить кадры-паузы (XOFF) для управления потоками, используйте эту команду:

```
hostname(config)#interface tengigabitethernet 1/0

hostname(config-if)#
flowcontrol send on
```

Дополнительные сведения см. в разделе Включение физического интерфейса и настройка параметров Ethernet.

команды "show"

show cpu usage

Команда show cpu usage используется для определения нагрузка трафика на ЦП ASA. Во время пиковой нагрузки, переполнения сети или атак, наблюдаются резкий кратковременный скачок загрузки CPU.

ASA использует один ЦП для обработки множества различных задач; например, ЦП обрабатывает пакеты и выводит сообщения об отладке на консоль. У каждого процесса есть своя цель и некоторые из них требуют больше времени CPU для выполнения, чем другие. Процесс шифрования потребляет, вероятно, наибольший объем ресурсов ЦП, поэтому если ASA передает большой объем трафика по шифрованным туннелям, необходимо выбрать более быструю платформу ASA — специализированный VPN-концентратор, такой как VPN 3000. VAC разгружает шифрование и дешифрование с ЦП ASA и выполняет их на оборудовании сетевой платы. Это позволяет ASA шифровать и дешифровать трафик 100 Мбит/с с использованием 3DES (168-разрядное шифрование).

Регистрация – это еще один процесс, который может потреблять большой объем системных ресурсов. По этой причине рекомендуется отключить консоль, монитор и ведение журнала буфера при входе в систему ASA. Эти процессы можно запустить при устранении неполадок, однако при выполнении обычных операций, особенно если ресурсы CPU недостаточны, их лучше отключать. Также следует установить уровень 5 (Уведомление) или ниже для регистрации в системном журнале или регистрации простого протокола управления сетью (Simple Network Management Protocol, SNMP) (истории регистраций). *В дополнение можно отключить особые идентификаторы сообщений системного журнала с помощью команды no logging message <идентификатор_системного_журнала>.*

Cisco Adaptive Security Device Manager (ASDM) также предоставляет на вкладке "Мониторинг" график, который позволяет просматривать потребление ресурсов ЦП ASA в динамике. Можно использовать этот график для определения загрузки ASA.

Команда show cpu usage служит для отображения статистики использования CPU.

Пример

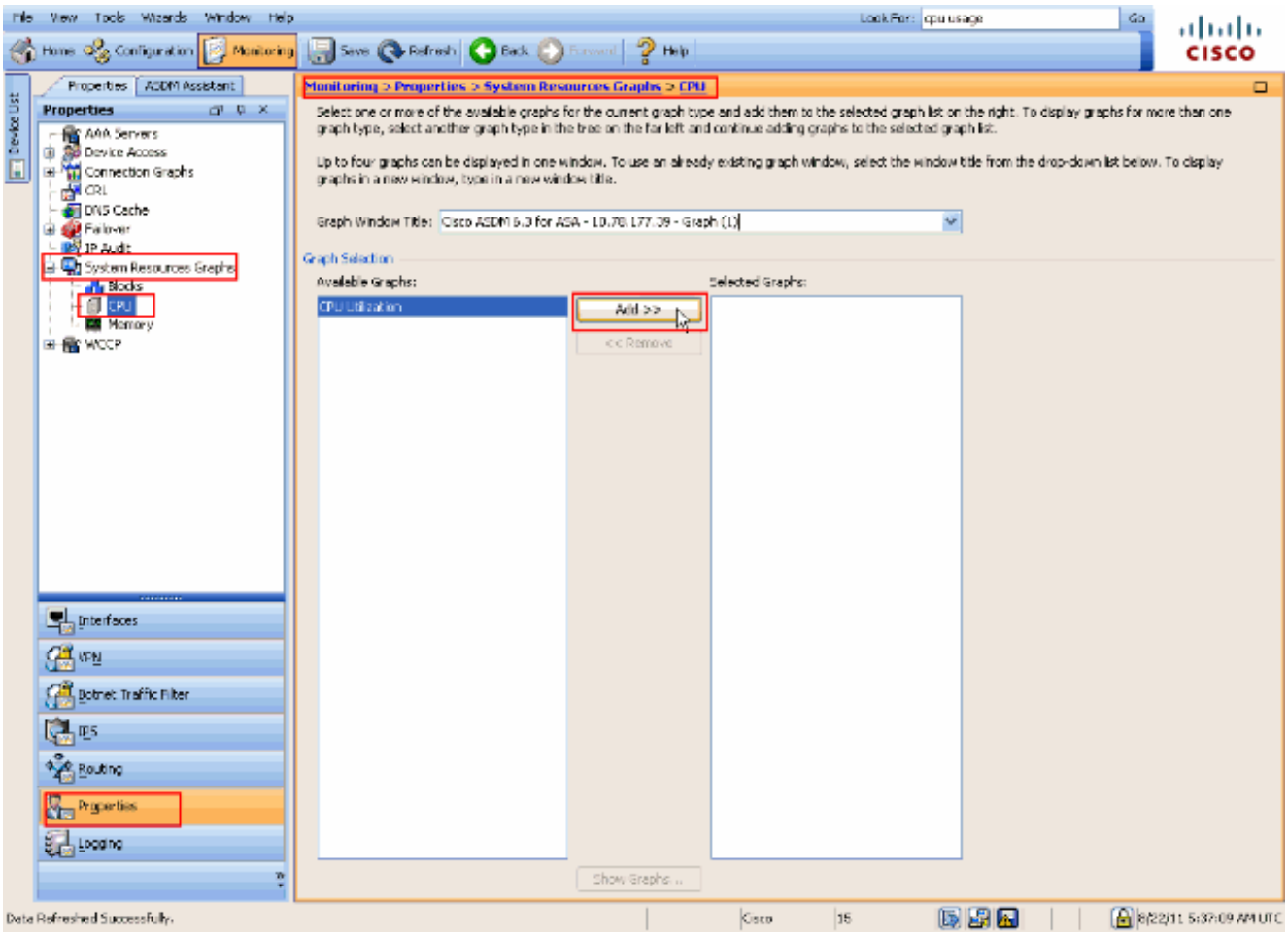
```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

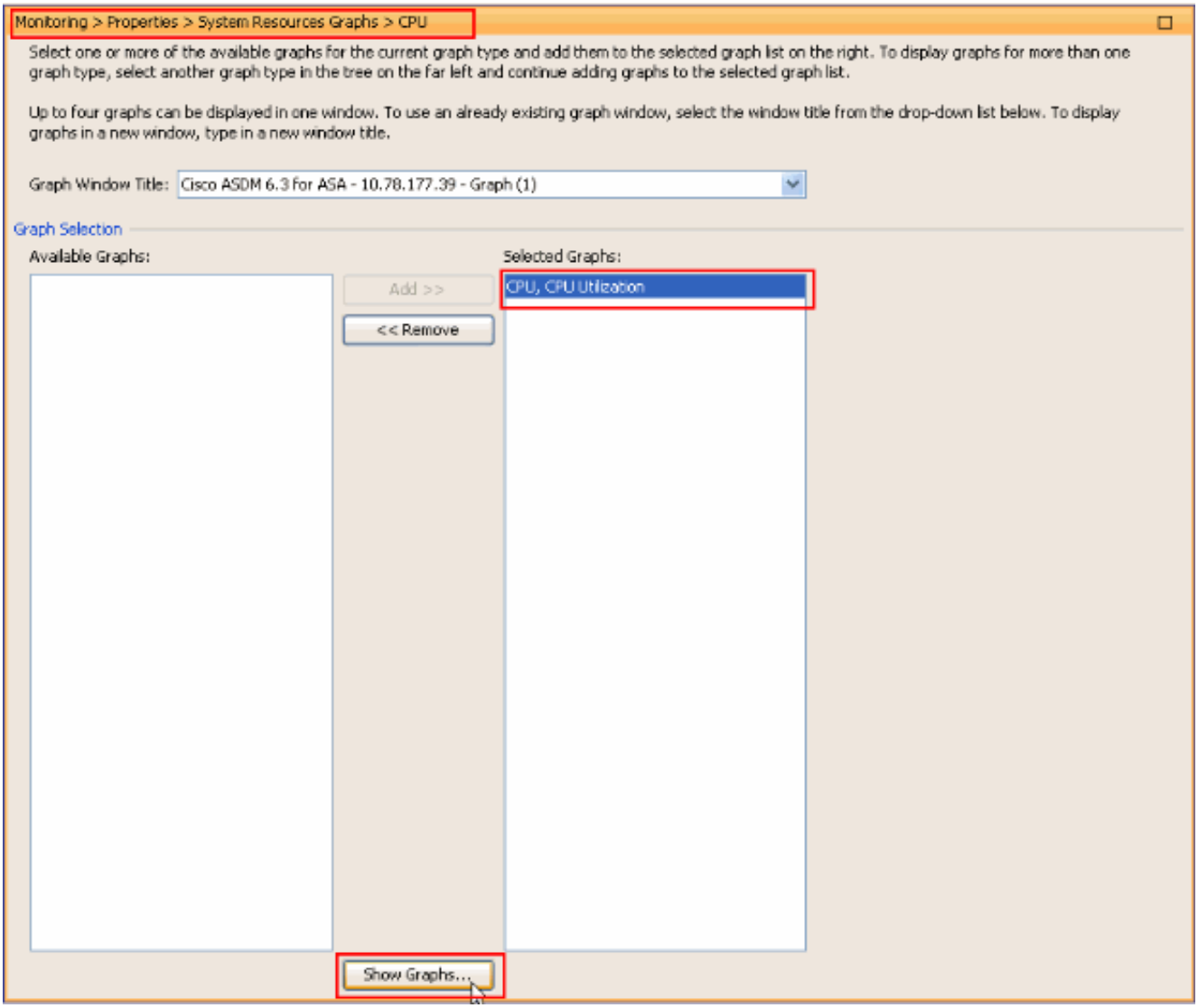
Просмотр данных об использовании ЦП на ASDM

Выполните следующие действия для просмотра данных о потреблении ресурсов ЦП на ASDM:

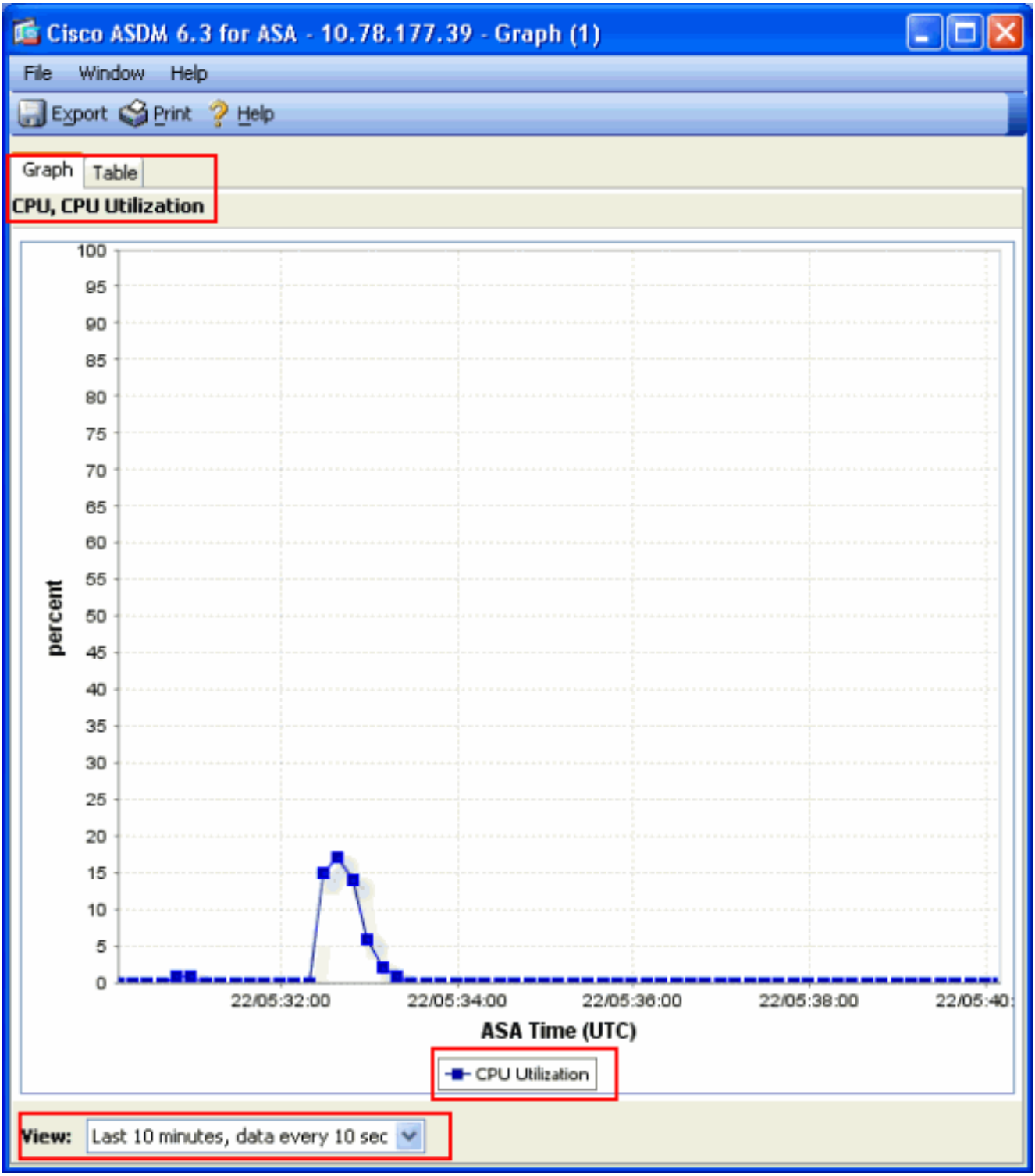
1. **Перейдите в раздел Мониторинг > Свойства> Графики ресурсов системы> ЦП в ASDM и выберите Заголовок окна графика. Затем выберите требуемые графики из списка Доступные графики и нажмите Добавить в соответствии с инструкциями.**



2. **Как только название нужного графика будет добавлено в разделе Выбранные графики, нажмите Показать графики.**



На следующем изображении показан график Потребление ЦП в ASDM. Можно просмотреть также другие представления этого графика или изменить его, выбрав нужное представление в раскрывающемся списке "Вид". Эти выходные данные можно вывести на печать или сохранить на компьютер.



Описание выходных данных

В данной таблице приводится описание полей выходных данных команды show cpu usage.

Поле	Описание
Загрузка CPU за 5 секунд	Уровень загрузки CPU за последние 5 секунд
1 минута	Средняя загрузка CPU по 5-секундным периодам за последнюю минуту

5 минут	Среднее значение для 5-секундных замеров использования CPU за послед пять минут

show traffic

Команда show traffic отображает объем трафика, передаваемый через ASA за определенный период. Результат подсчитывается за время, прошедшее с момента последнего выполнения данной команды. **Чтобы получить точный результат, выполните команду clear traffic, а затем подождите 1-10 минут перед тем, как выполнить команду show traffic. Также можно выполнить команду show traffic дважды с интервалом в 1-10 минут, однако достоверными, в этом случае, будут выходные данные второго выполнения команды.**

Можно использовать команду show traffic, чтобы определить объем трафика, который проходит через ASA. При наличии нескольких интерфейсов с помощью этой команды можно определить, какой из интерфейсов отправляет и получает больше всего данных. Для устройств ASA с двумя интерфейсами общий объем входящего и исходящего трафика на внешнем интерфейсе должен быть равен общему объему входящего и исходящего трафика на внутреннем интерфейсе.

Пример

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

Если объем трафика приближается или достигает пропускной способности одного из интерфейсов, следует обновить интерфейс на более быстрый или ограничить объем трафика, проходящий через этот интерфейс. В противном случае возможно отбрасывание пакетов. [Как уже говорилось в разделе show interface чтобы получить подробные сведения о пропускной способности, можно проверить счетчики интерфейса.]

show perfmon

Команда show perfmon используется для мониторинга общего объема и типов трафика, проверяемого ASA. Это единственный способ определить количество трансляций (xlates) и соединений (conn) в секунду. Соединения дополнительно разрушены в соединениях TCP и пользовательского протокола данных(UDP). **Описание выходных данных при выполнении команды см. в разделе Описание выходных данных.**

Пример

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

Описание выходных данных

В данной таблице приводится описание выходных данных show perfmon.

Поле	Описание
Xlate	Трансляции, выполненные за секунду
Соединения	Подключений, установленных за секунду
TCP Conns	Количество TCP-соединений в секунду
UDP Conns	Соединения UDP на секунду
URL Access	Количество URL-адресов (веб-узлов), к которым получен доступ за секунду
URL Server Req	**Количество запросов, отправленных в приложения Websense и N2H2 в секунду (требу ввод команды filter),**
TCP Fixup	Количество TCP-пакетов, перенаправляемых ASA за секунду
Перехват TCP	Число SYN-пакетов в секунду, превышающее начальный фиксированный предел

HTTP Fixup	**Количество пакетов, назначенных на порт 80 в секунду (требуется применить команду fixup protocol http),**
FTP Fixup	Количество проверенных FTP-команд в секунду
AAA Authen	Запросы на аутентификацию в секунду
AAA Author	Количество запросов авторизации в секунду
AAA Account	Учетные требования в секунду

show blocks

Помимо команды show cpu usage можно использовать команду show blocks для определения перегрузки ASA.

Блоки обработки пакетов (1550 и 16384 байт)

Когда пакет поступает в интерфейс ASA, он помещается во входную очередь интерфейса. передается в ОС и размещается в блоке. Для пакетов Ethernet используется 1550-байтные блоки, для пакетов, приходящих с платы 66 МГц Gigabit Ethernet используются 16384-байтные блоки. ASA определяет, принять или отклонить пакет, используя для этого адаптивный алгоритм безопасности (ASA), и обрабатывает пакет на всех этапах, вплоть до помещения его в очередь интерфейса вывода. Если ASA не поддерживает нагрузку трафика, количество блоков размером 1550 байт (или блоков размером 16384 байта для GE 66 МГц) снижается почти до 0 (как показано в столбце CNT выходных данных команды). Когда значение столбца CNT достигнет нуля, ASA пытается выделить большее количество блоков (максимум 8192). Если дополнительные блоки недоступны, ASA отбрасывает пакет.

Блоки переключения при отказе и системного журнала (256 байт)

256-байтовые блоки в основном используются для сообщений аварийного переключения с синхронизацией состояния. Активный ASA генерирует и отправляет пакеты на резервный ASA, чтобы обновить трансляцию и таблицу подключений. В периоды неравномерности трафика, когда создается и разрывается большое количество соединений, число доступных блоков 256 байт может снизиться до 0. Такое отбрасывание пакетов говорит о том, что одно или несколько соединений не обновляются на резервном ASA. Как правило, это приемлемо, поскольку протокол аварийного переключения с синхронизацией состояния будет перехватывать xlate или подключение, которое было разорвано. Однако, если значение столбца CNT для 256-байтовых блоков сохраняется близким к 0 в течение длительного периода, ASA не сможет соответствовать скорости трансляции и скорости в таблицах соединений, которые синхронизируются в связи с количеством соединений в секунду, обрабатываемых ASA. Если это происходит регулярно, необходимо обновить ASA, выбрав

более высокоскоростную модель.

Сообщения системного журнала, отправляемых с ASA, также используют 256-байтовые блоки, однако они, как правило, не выдаются в таком количестве, чтобы исчерпать пул 256-байтовых блоков. Если в столбце CNT количество 256-байтных блоков близко к нулю, убедитесь, что вход на сервер системного журнала в режиме отладки (уровень 7) не производился. В конфигурации ASA это выражается строкой trap-сообщений журнала. В этом случае рекомендуется установить для регистрации уровень 5 (Уведомление) или ниже, пока не будут получены дополнительные данные для отладки.

Пример

```
Ciscoasa#show blocks
  SIZE    MAX    LOW    CNT
     4   1600   1597   1600
    80    400    399    400
   256    500    495    499
  1550   1444   1170   1188
 16384   2048   1532   1538
```

Описание выходных данных

В данной таблице приводится описание выходных данных show blocks.

Столбец	Описание
РАЗМЕР	Размер E, в байтах, пула блоков. Каждый размер соответствует определенному типу
Макс	Максимальное число блоков, доступных для указанного пула блоков байта. Максимально число блоков выделяется из памяти при загрузке. Обычно максимальное количество блок неизменно. Исключение составляют 256-и 1550-байтовые блоки, где устройство адаптивн безопасности может при необходимости динамически создавать большее количество (максимум 8192).
Низкий	Нижний предел. Это число обозначает минимальное количество блоков этого размера, доступное с момента включения устройства адаптивной безопасности с момента последн сброса блоков (с помощью команды clear blocks). Ноль в столбце LOW указывает на предыдущее событие, при котором память была заполнена.
CNT	Текущее количество блоков, доступных для пула блоков этого конкретного размера. Ноль столбце CNT означает, что память теперь заполнена.

В данной таблице приводится описание значений строки SIZE в выходных данных команды show blocks.

Значение SIZE	Описание
0	Используется блоками dupb.
4	Создает дубликаты существующих блоков в приложениях, таких как DNS, ISAKMP, фильтрация URL-адресов, uauth, TFTP и модули TCP. Кроме того, блок такого размера м стандартно использоваться кодом для отправки пакетов в драйверы и т. д.
80	Используется в процессе перехвата TCP для создания пакетов подтверждения и сообще о переключении при отказе.
256	Используется для обновлений переключений при отказе с синхронизацией состояния, ведения системного журнала и выполнения других функций TCP. Эти блоки в основном используются для сообщений о переключении при отказе с синхронизацией состояния. Активное устройство адаптивной безопасности создает и передает пакеты резервному устройству адаптивной безопасности для обновления трансляции и таблицы соединений неравномерном трафике, где создается и разрывается большое количество соединений, число доступных блоков может снизиться до 0. Такая ситуация указывает на то, что одно несколько соединений не обновлены на резервном устройстве адаптивной безопасности Протокол переключения при отказе с синхронизацией состояния в следующий раз найде недостающую трансляцию или соединение. Если столбец CNT для 256-байтовых блоков остается на 0 или стремится к 0 длительные периоды времени, то устройство адаптивно безопасности испытывает затруднения при поддержании синхронизированными таблиц подключений и трансляций из-за количества соединений в секунду, которые обрабатыва устройство адаптивной безопасности. Сообщения системного журнала, передаваемые с платформы Adaptive Security Appliance, также используют 256-байтовые блоки, однако он обычно не выдаются в таком количестве, которое исчерпывает пул 256-байтовых блоков Если в столбце CNT указано, что количество 256-байтовых блоков близко к 0, убедитесь том, что ведение журналов на сервере системных журналов не выполняется на уровне отладки (уровень 7). В конфигурации Adaptive Security Appliance это выражено строкой tr сообщений журнала. Если вам не требуется дополнительная информация для отладки, рекомендуется задать ведение журнала на уровне уведомлений (уровень 5) или ниже.
1550	Используется для хранения пакетов Ethernet в целях обработки посредством платформы Adaptive Security Appliance. Когда пакет поступает в интерфейс Adaptive Security Appliance помещается во входную очередь интерфейса, передается в операционную систему и помещается в блок. Adaptive Security Appliance определяет, принять или отклонить пакет учетом политики безопасности и обрабатывает пакет на всех этапах до выходной очереди интерфейса вывода. Если Adaptive Security Appliance не может поддерживать нагрузку трафика, количество доступных блоков снизится почти до 0 (как показано в столбце CNT выходных данных команды). Когда значение столбца CNT равно нулю, Adaptive Security Appliance пытается выделить большее количество блоков (максимум 8192). Если дополнительные блоки недоступны, Adaptive Security Appliance отбрасывает пакет.
2600	Используется только для 64-разрядных сетевых плат Gigabit Ethernet 66 МГц (i82543). Дополнительные сведения о пакетах Ethernet см. в описании модели 1550.
2048	Контрольные или управляемые кадры, используемые для контрольных обновлений.

show memory

Команда show memory отображает общий объем физической памяти (ОЗУ) для ASA, а также количество текущих доступных байтов. Чтобы воспользоваться этими данными,

необходимо сначала понять, как ASA использует память. Когда ASA загружается, он копирует ОС с флеш-накопителя в ОЗУ и запускает ОС из ОЗУ (точно так же, как маршрутизаторы). Затем ASA копирует загрузочную конфигурацию с флеш-накопителя и размещает ее в ОЗУ. Наконец, ASA выделяет ОЗУ для создания пулов блоков, которые рассматривались в описании команды show blocks. После такого выделения дополнительное ОЗУ потребуется ASA только в случае увеличения размера конфигурации. Кроме того, ASA хранит в ОЗУ записи трансляции и соединения.

В процессе стандартной эксплуатации объем свободной памяти на ASA изменяется незначительно или вовсе не изменяется. Как правило, дефицит памяти может возникнуть только в случае атаки с созданием несколько сотен тысяч соединений, проходящих через ASA. **Чтобы проверить соединения, выполните команду show conn count , которая отображает текущее и максимальное количество соединений через ASA.** Если в ASA возникает дефицит памяти, происходит сбой. До сбоя в журнале могут отображаться сообщения о сбое при выделении памяти (%ASA-3-211001). В случае нехватки памяти по причине целенаправленной атаки обратитесь в Центр технической поддержки Cisco (TAC).

Пример

```
Ciscoasa#
show memory
Free memory:        845044716 bytes (79%)

Used memory:        228697108 bytes (21%)

-------------      ----------------

Total memory:      1073741824 bytes (100%)
```

show xlate

Команда show xlate count отображает текущее и максимальное количество трансляций посредством ASA. Трансляция — это сопоставление внутренних адресов внешним адресам и может представлять собой сопоставление «один-к-одному», как в случае трансляции сетевых адресов (Network Address Translation, NAT), и «несколько-к-одному», как в случае трансляции адресов портов (Port Address Translation, PAT). **Эта команда является подмножеством команды show xlate, которая выводит каждую трансляцию через ASA.** В выходных данных команды отображаются "используемые" трансляции, то есть, число активных трансляций в ASA на момент выполнения команды; "наиболее используемые" относится к трансляциям, которые чаще всего наблюдались на ASA с момента включения.

Примечание. Один хост может содержать несколько соединений с различными целевыми местоположениями, но при этом использовать только одну трансляцию. Если счетчик xlate значительно превышает количество узлов во внутренней сети, то есть вероятность того, что на один из внутренних узлов был совершен несанкционированный доступ. Если внутренний хост скомпрометирован, он подделывает исходный адрес и отправляет пакеты с ASA.

Примечание. Если включена конфигурация vpn-клиента и выполняется отправка DNS-запросов с внутреннего узла, с помощью команды show xlate можно просмотреть список xlate-слотов статической трансляции.

Пример

```
Ciscoasa#
show xlate count
84 in use, 218 most used
```

```
Ciscoasa(config)#show xlate

3 in use, 3 most used

Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,

       o - outside, r - portmap, s - static

TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
idle 62:33:57 timeout 0:00:30
UDP PAT from 10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
idle 62:33:57 timeout 0:00:30
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
idle 62:33:57 timeout 0:00:30
```

Первая запись — трансляция адреса порта TCP от порта хоста (10.1.1.15, 1026) во внутренней сети к порту хоста (192.150.49.1, 1024) во внешней сети. Флаг "r" обозначает, что данная трансляция является трансляцией адресов портов. Флаг "i" означает, что данная трансляция применяется к внутреннему адресу или порту.

Вторая запись иллюстрирует трансляцию адресов UDP-порта хоста (10.1.1.15, 1028) внутренней сети в порт хоста (192.150.49.1, 1024) внешней сети. Флаг "r" обозначает, что данная трансляция является трансляцией адресов портов. Флаг "i" означает, что данная трансляция применяется к внутреннему адресу или порту.

Третья запись иллюстрирует трансляцию адресов ICMP-порта для host-ICMP-id (10.1.1.15, 21505) внутренней сети в host-ICMP-id (192.150.49.1, 0) внешней сети. Флаг "r" обозначает, что данная трансляция является трансляцией адресов портов. Флаг "i" означает, что данная трансляция применяется к внутреннему адресу или ICMP-id.

Поля внутренних адресов появляются в пакетах, которые проходят от более защищенных интерфейсов к менее защищенным. И наоборот, они появляются в качестве адресов назначения в пакетах, которые проходят от менее защищенных интерфейсов к более защищенным.

show conn count

Команда show conn count отображает текущее и максимальное число соединений через ASA. Подключение сопоставляет сведения уровня 4 от внутреннего адреса внешнему адресу. Соединения создаются при получении ASA пакета SYN для TCP-сеансов или при поступлении первого пакета в рамках UDP-сеанса. Соединения разрываются, когда ASA получает последний пакет ACK. Это происходит при закрытии квитирования установления связи для сеанса TCP или после истечения тайм-аута для UDP-сеанса.

Чрезмерно большое число соединений (в 50-100 раз выше нормы) может быть признаком атаки злоумышленников. **Выполните команду show memory, чтобы предотвратить дефицит памяти в ASA из-за большого числа соединений.** Под воздействием атаки можно ограничить максимальное число подключений, приходящихся на одну статическую запись, а также максимальное количество начальных подключений. Это защитит внутренние серверы от переполнения. Дополнительные сведения см. в разделе Справочник по командам для платформы Cisco ASA серии 5500.

Пример

```
Ciscoasa#show conn count
2289 in use, 44729 most used
```

show interface

Команда show interface позволяет выявить проблемы, связанные с несоответствием дуплексного режима и неполадки в системе кабелей. Кроме того, она предоставляет дополнительную аналитическую информацию о возможности переполнения интерфейса. Если на ASA возникает дефицит ресурсов ЦП, количество 1550-байтовых блоков снижается почти до 0. (проанализируйте 16384-байтовые блоки на платах Gig 66 МГц. Другим показателем является увеличение «no buffers» в интерфейсе. Сообщение "Нет буферов" указывает на то, что интерфейс не может отправить пакет в ОС ASA, так как нет доступного блока для пакета, поэтому пакет отбрасывается. **Если число сообщений "Нет буфера" регулярно увеличивается, выполните команду show proc cpu, чтобы проверить потребление ресурсов ЦП платформой ASA.** Если из-за высокой нагрузки трафика потребляется большой объем ресурсов ЦП, следует перейти на более мощную платформу ASA, которая способна справиться с нагрузкой.

Когда пакет впервые поступает в интерфейс, он помещается во входную аппаратную очередь. Если входная аппаратная очередь заполнена, пакет помещается во входную программную очередь. Пакет передается из входной очереди и помещается в 1550-байтовый блок (или в 16384-байтовый блок в интерфейсах Gigabit Ethernet 66 МГц). Затем ASA определяет интерфейс вывода для пакета и помещает пакет в соответствующую очередь на оборудовании. Если аппаратная очередь заполнена, пакет помещается в исходящую программную очередь. Если максимальное число блоков в любой из программных очередей велико, интерфейс переполняется. Например, если на ASA трафик поступает со скорпроостью 200 Мбит/с и отправляется из одного интерфейса 100 Мбит/с, для программной очереди вывода отображаются высокие значения в интерфейсе вывода, что указывает на неспособность интерфейса обработать такой объем трафика. При возникновении такой ситуации следует рассмотреть вопрос о замене интерфейса на более быстрый.

Пример

```
Ciscoasa#show interface
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
 Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
       Input flow control is unsupported, output flow control is unsupported
       MAC address 0013.c480.b2b8, MTU 1500
       IP address 192.168.17.4, subnet mask 255.255.255.0
       311981 packets input, 20497296 bytes, 0 no buffer
       Received 311981 broadcasts, 157 runts, 0 giants
       379 input errors, 107 CRC, 273 frame, 0 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       121 packets output, 7744 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 1 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops, 0 tx hangs
       input queue (blocks free curr/low): hardware (255/249)
       output queue (blocks free curr/low): hardware (255/254)
```

Вам следует так же проверить интерфейс на наличие ошибок. Получение карликовых кадров, входных ошибок, CRC, или ошибок в кадрах является признаком несоответствия дуплексных режимов. Кроме того, может быть неисправен кабель. Дополнительные сведения о проблемах дуплексных режимов см. в разделе Настройка скорости и дуплексного режима. Помните, что каждый счетчик ошибок показывает количество пакетов, отброшенных по той или иной конкретной причине. Если отображается конкретный счетчик, показания которого регулярно увеличиваются, это означает, что производительность ASA, скорее всего, снижена и необходимо выяснить причину этой проблемы.

При проверке счетчиков интерфейса учтите, что если для него установлен режим полного дуплекса, то не должно наблюдаться никаких конфликтов, поздних конфликтов или задержанных пакетов. Наоборот, если для интерфейса установлен полудуплексный режим, могут возникнуть конфликты, поздние конфликты и, возможно, задержанные пакеты. Общее число конфликтов, поздних конфликтов и задержанных пакетов не должно превышать 10% суммы счетчиков входящих и исходящих пакетов. Если конфликты превышают 10% общего трафика, то канал имеет чрезмерную нагрузку и необходимо произвести обновление до полнодуплексного канала или канала с более высокой скоростью (с 10 на 100 Мбит/с). Следует помнить, что показатель конфликтов 10 % означает, что ASA отбрасывает 10 % пакетов, проходящих через этот интерфейс; каждый из этих пакетов должен быть ретранслирован.

Дополнительные сведения о счетчиках интерфейса см. в разделе о команде interface в Справочнике по командам для Cisco ASA серии 5500.

show processes

Команда show processes на ASA отображает все активные процессы, запущенные на ASA на момент выполнения команды. Эти данные используются для определения того, какой из процессов получает слишком много времени CPU, а какой не получает вовсе. **Для получения этих данных выполните команду show processes дважды с перерывом в 1 минуту.** Для сомнительного процесса отнимите значение времени выполнения из второго результата от значения времени выполнения из первого результата. Этот показатель демонстрирует объем потребления процессом времени ЦП (в мс) за этот периода. Учтите, что запуск некоторых процессов запланирован через определенные промежутки времени, а некоторые процессы запускаются только тогда, когда получены данные для выполнения. У процесса 577poll, вероятно, будет самое большое время выполнения по сравнению с другими процессами. Такая ситуация не выходит за пределы нормы, поскольку процесс 577poll опрашивает интерфейсы Ethernet для определения их потребности в обработке тех или иных данных.

> **Примечание. Изучение каждого из процессов ASA не рассматривается в этом документе и упоминается только в справочных целях.** Дополнительные сведения о

процессах ASA см. в разделе Команда show processes ASA.

Перечень команд

В целом команду show cpu usage рекомендуется использовать для определения нагрузки на ASA. Необходимо помнить, что значение вывода представляет собой скользящее среднее значение; на ASA могут наблюдаться более высокие значения пикового потребления ресурсов ЦП, которые маскируются скользящим средним. Как только объем потребления ЦП на ASA достигает 80 %, значение задержки на ASA медленно увеличивается прибл. до 90 % ЦП. Если объем потребления ресурсов ЦП превышает 90 %, ASA начинает отбрасывать пакеты.

Если уровень загрузки CPU высокий, используйте команду show processes, чтобы определить процесс, который использует больше всего процессорного времени. Эти данные можно использовать, чтобы сократить время ЦП, потребляемое ресурсоемкими процессами (например, ведение журналов).

Если объем потребления ЦП невелик, но при этом вы считаете, что пакеты по-прежнему отбрасываются, используйте команду show interface, чтобы проверить интерфейс ASA на наличие сообщений о конфликтах и отсутствии буферов, которые могли появиться в результате несоответствия дуплексного режима. Если значения счетчиков буферов не растет, но загрузка CPU остается высокой, то интерфейс не в состоянии осуществлять поддержку проходящего через него трафика.

Если с буферами все хорошо, проверьте состояние блоков. **Если значение текущего столбца CNT в выводе команды show blocks стремится к 0 в 1550-байтовых блоках (или в 16384-байтовых блоках для плат Gig 66 МГц), ASA, вероятнее всего, будет отбрасывать пакеты Ethernet из-за перегруженности.** В этом случае наблюдаются резкие кратковременные повышения нагрузки CPU.

Если возникают проблемы при создании новых соединений на ASA, используйте команду show conn count, чтобы проверить текущее число соединений на ASA.

При большом количестве соединений необходимо проверить выходные данные команды show memory, чтобы убедиться в том, что на ASA нет дефицита памяти. Если ресурсов памяти недостаточно, следует проанализировать источник соединений с помощью команды show conn или show local-host, чтобы убедиться в отсутствии атак, направленных на отказ в обслуживании.

Можно также использовать другие команды для измерения объема трафика, проходящего через ASA. **Команда show traffic отображает агрегированные пакеты и байты отдельно для каждого интерфейса, а команда show perfmon выполняет разбивку трафика по типам, которые проверяются ASA.**

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Техническая поддержка - Cisco Systems