ASA 8. 3 и позже: Наблюдение и устранение неполадок производительности

Содержание

Введение

Этот документ предоставляет сведения о командах ASA, которые можно использовать для монитора и устранить неполадки производительности устройства адаптивной защиты Cisco (ASA).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на устройстве адаптивной защиты Cisco (ASA), который выполняет версию 8.3 и позже.

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 у вас есть выходные данные **команды показа** от вашего устройства Cisco, можно использовать Cisco CLI Анализатор (только зарегистрированные клиенты), чтобы отобразить потенциальные проблемы и исправляете. **Некоторые команды show** Поддержек анализатора Cisco CLI. При использовании Cisco CLI Анализатор необходимо быть зарегистрированным заказчиком, вы должны войтись в ваш аккаунт Cisco, и необходимо было включить JavaScript в браузере.

Настройка скорости и дуплексного режима

Устройство безопасности предварительно сконфигурировано для автоматического обнаружения параметров настройки скорости и дуплексного режима на 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 о дуплексе нужно выполнить согласование, устройство, которое установлено в автосогласование, не может определить параметры настройки на другом устройстве, таким образом, это принимает значение по умолчанию к полудуплексу, как сообщили в стандарте IEEE 802.3u.

Например, если вы настраиваете интерфейс ASA для автосогласования и подключаете его с коммутатором, который жестко закодирован для 100 Мбит/с и полнодуплексный, ASA отсылает 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 это не получает ответа от коммутатора, переходов ASA

в параллель detecion режим и снимает показания длину импульсов в кадрах, которые отсылает коммутатор. Т.е. смыслы ASA, что коммутатор установлен в 100 Мбит/с, таким образом, он устанавливает интерфейсную скорость соответственно. Однако, потому что коммутатор не обменивается FLP, ASA не может обнаружить, если коммутатор может работать полнодуплексный, таким образом, ASA устанавливает интерфейсный дуплекс в полудуплекс, как сообщили в стандарте IEEE 803.2u. Поскольку коммутатор жестко закодирован к 100 Мбит/с и полнодуплексный, и ASA имеет просто автосогласованный к 100 Мбит/с и полудуплекс (как это должно), результатом является несогласованность дуплексных параметров, которая 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 ЦП utlization высок, выполните эти шаги для устранения проблем:

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

2. Убедитесь, что блок памяти функционирует нормально.

3. Проверьте, что количество ACL выше.

4. Выполните **команду show memory detail** и проверьте, что память, используемая ASA, является стандартным использованием.

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 дуплекс и параметры настройки 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 включить [команду ip verify reverse-path interface] на всех интерфейсах, поскольку это отбросит пакеты, которые не сделали, чтобы допустимый источник обратился, который приводит к меньшему количеству использования ЦПУ. Это применяется к FWSM, сталкивающемуся с проблемами высокой загрузки CPU.

8. ‚Другой причиной высокой загрузки ЦП может быть слишком большое количество маршрутов групповой адресации. Выполните **команду show mroute**, чтобы проверить, получает ли ASA слишком много 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 CPU могла бы произойти из-за идентификатора ошибки Cisco CSCsq48636. См. идентификатор ошибки Cisco CSCsq48636 (только зарегистрированные клиенты) для получения дополнительной информации.

Примечание: Если решение, предоставленное выше, не решает вопрос, обновите платформу ASA согласно требованиям. См. Таблицу данных многофункциональных устройств защиты Cisco ASA серии 5500 для получения дополнительной информации о возможностях и мощностях Платформы Устройства адаптивной безопасности. Свяжитесь с TAC (только зарегистрированные клиенты) 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 на внешнем интерфейсе устройства безопасности заставляют устройство безопасности использовать большие значения памяти для блокирования пакетов через указанные порты. Для решения этого вопроса заблокируйте недопустимый трафик в конце интернет-провайдера.
- **Обнаружение угрозы:** функция обнаружения угрозы состоит из разных уровней статистики, собирающейся для различных угроз, а также просматривающей

обнаружение угрозы, которое определяет, когда хост выполняет просмотр. **Выключите** эту функцию для потребления меньшей 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). Также, многие стандартные параметры порта не выбираемы, когда ASA включен в коммутатор. Например, на коммутаторах с ОС Catalyst включение channeling (объединения каналов) и trunking (магистрального соединения) включается автоматически (Auto), а режим PortFast отключен. Если вы подключаете ASA с коммутатором, который выполняет Catalyst OS, отключите канализирование, отключите транкинг 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: На Коммутаторах серии Catalyst XL канализирование является "not set" к Автоматическому по умолчанию. Поэтому необходимо отключить канализирование на любом порте коммутатора, который соединяется с 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 этим причинам рекомендуется включить PortFast на любом порте коммутатора, который соединяется с ASA.

Примечание: Релизы операционной системы Catalyst 5.4 и позже включают *<mod>* **set port host /** команда *<port>*, которая позволяет вам использовать одиночную команду, чтобы отключить канализирование, отключить транкинг и включить PortFast.

!--- преобразования сетевых адресов (NAT)

Каждой перегрузке NAT или перегрузке NAT (PAT) сеанс назначают слот преобразования, известный как *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 всего трафика через устройство может произойти когда вы глобально clear xlate на устройстве безопасности.

Типовая конфигурация ASA для PAT, который 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].

Вот типовая конфигурация 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 вам решать проблемы на ASA. Cisco предлагает свободный сервер системного журнала для Windows NT, названного Сервером системного журнала Межсетевого экрана ASA (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.

Когда вы устанавливаете сервер системного журнала, настраиваете ASA для передачи журналов к нему.

Пример:

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

> **Примечание:** Данный пример настраивает ASA для передачи Отладки (уровень 7) и больше важных системных журналов к серверу системного журнала. Поскольку эти журналы ASA являются самыми многословными, используйте их только, когда вы решаете проблему. 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- .).`) Проверка для сообщений, которые указывают на внешний сервер, пыталась обратиться к внутреннему IP-адресу на порте TCP 113 (для Протокола идентификации или Идентификатора), но ASA запретил пакет. Это сообщение должно выглядеть примерно так:

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

Если вы получаете это сообщение, выполняете команду service resetinbound к ASA. ASA тихо не отбрасывает пакеты; вместо этого, эта команда заставляет ASA сразу перезагружать любое входящее подключение, которое запрещено 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 развертываний в масштабе предприятия. Cisco ASA поддерживает мониторинг сети с версиями SNMP 1, 2c и 3.

Можно настроить Устройство безопасности для передачи trap-сообщений к Серверу управления сетью (NMS), или можно использовать NMS для просмотра MIB на устройстве безопасности. MIB являются набором определений, и устройство безопасности

поддерживает базу данных значений для каждого определения. Для получения дополнительной информации об этом, обратитесь к SNMP Настройки на Cisco ASA.

Все поддерживаемые MIB для Cisco ASA могут быть найдены в **Списке поддержки MIB ASA**. Из этого списка эти MIB полезны для мониторинга производительности:

- MIB МЕЖСЕТЕВОГО ЭКРАНА CISCO----Содержит Объекты, полезные для аварийного переключения
- CISCO-PROCESS-MIB----Содержит Объекты, полезные для Загрузки ЦПУ
- CISCO-MEMORY-POOL-MIB----Содержит Объекты, полезные для Объектов Memory.

Обратный поиск DNS

Если вы испытываете низкую производительность с ASA, проверяете, что у вас есть Указатель Системы доменных имен (PTR DNS) записи, также известные как записи Обратного поиска DNS, в авторитетном сервере DNS для внешних адресов, которые использует ASA. Это включает любой адрес в вашу глобальную трансляцию сетевых адресов (NAT) пул (или внешний интерфейс ASA, если вы перегружаетесь на интерфейсе), любой статический адрес и внутренний адрес (если вы не используете NAT с ними). 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

Если у вас есть всплеск трафика, отброшенные пакеты могут произойти, если пакет превышает емкость буферизации буфера FIFO на NIC и буферах кольца приема. Включение фреймов паузы для управления потоками может облегчить эту проблему. Пауза (XOFF) и кадры XON генерируются автоматически NIC, аппаратным на использовании буфера FIFO. Когда использование буфера превышает наибольшее возможное значение, фрейм паузы передается. Для включения паузы (XOFF) кадры для управления потоками используйте эту команду:

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

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

См. Включение Физического интерфейса и Параметров Ethernet Настройки для получения дополнительной информации.

команды "show"

show cpu usage

Команда отображения загруженности процессора используется для определения трафика, размещенного в ЦП ASA. Во время пиковой нагрузки, переполнения сети или атак, наблюдаются резкий кратковременный скачок загрузки CPU.

ASA имеет одно CPU для обработки множества задач; например, это обрабатывает пакеты и распечатывает сообщения отладки к консоли. У каждого процесса есть своя цель и некоторые из них требуют больше времени CPU для выполнения, чем другие. Шифрованием является, вероятно, большая часть Процесса с высокой загрузкой ЦПУ, поэтому если ваш ASA передает много трафика через зашифрованные туннели, необходимо рассмотреть более быстрый ASA, специализированный Концентратор VPN, такой как VPN 3000. VAC разгружает шифрование и расшифровку от ЦП ASA и выполняет его в аппаратных средствах на карте. Это позволяет ASA шифровать и дешифровать 100

Мбит/с трафика с 3DES (168-разрядное шифрование).

Регистрация – это еще один процесс, который может потреблять большой объем системных ресурсов. Из-за этого рекомендуется отключить консоль, монитор и буфер, входящий 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 график на вкладке Monitoring, которая позволяет вам просматривать использование ЦПУ ASA в течение долгого времени. Можно использовать этот график для определения загрузки на ASA.

Команда show cpu usage служит для отображения статистики использования CPU.

Пример

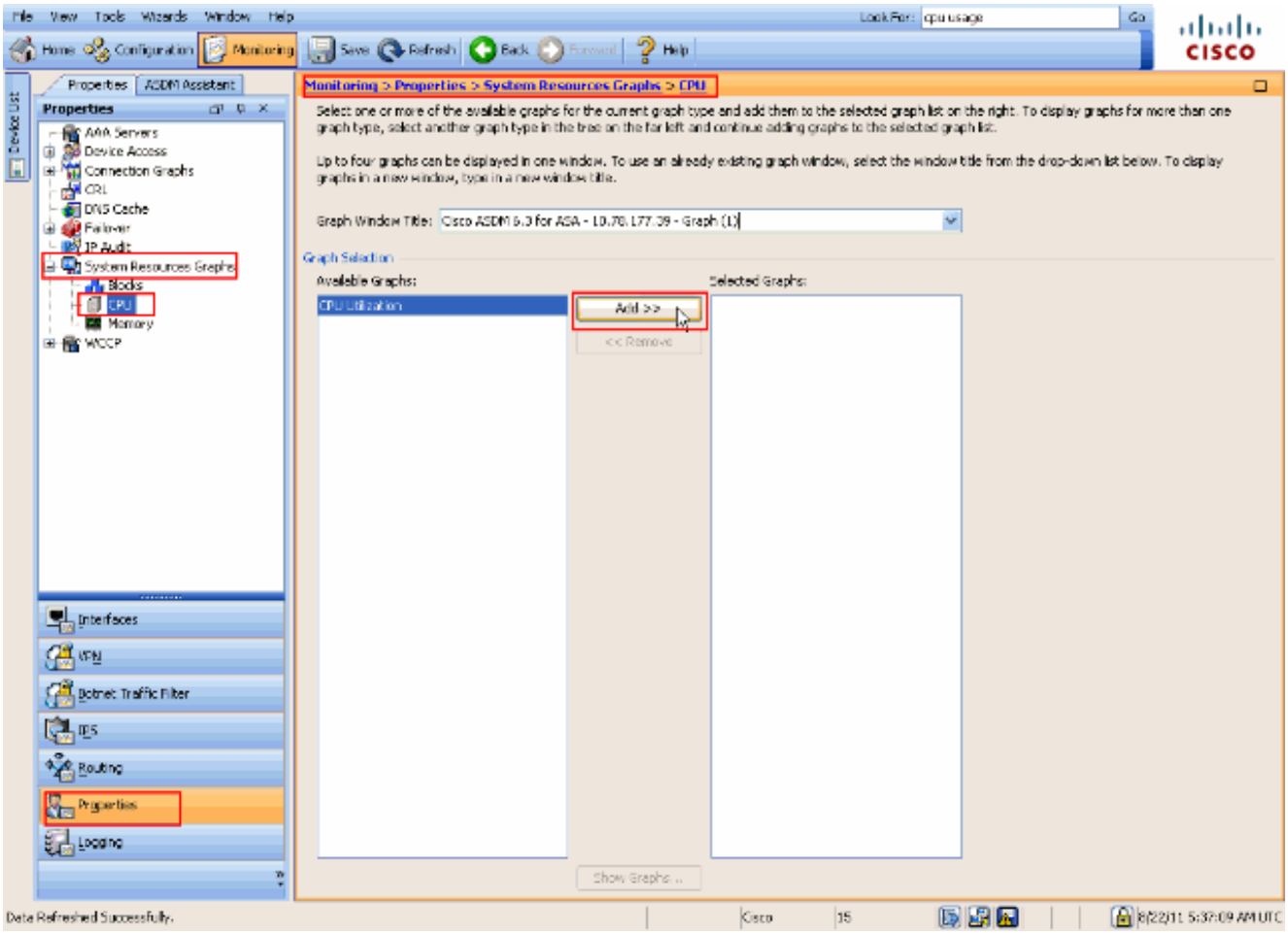
```
Ciscoasa#show cpu usage

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

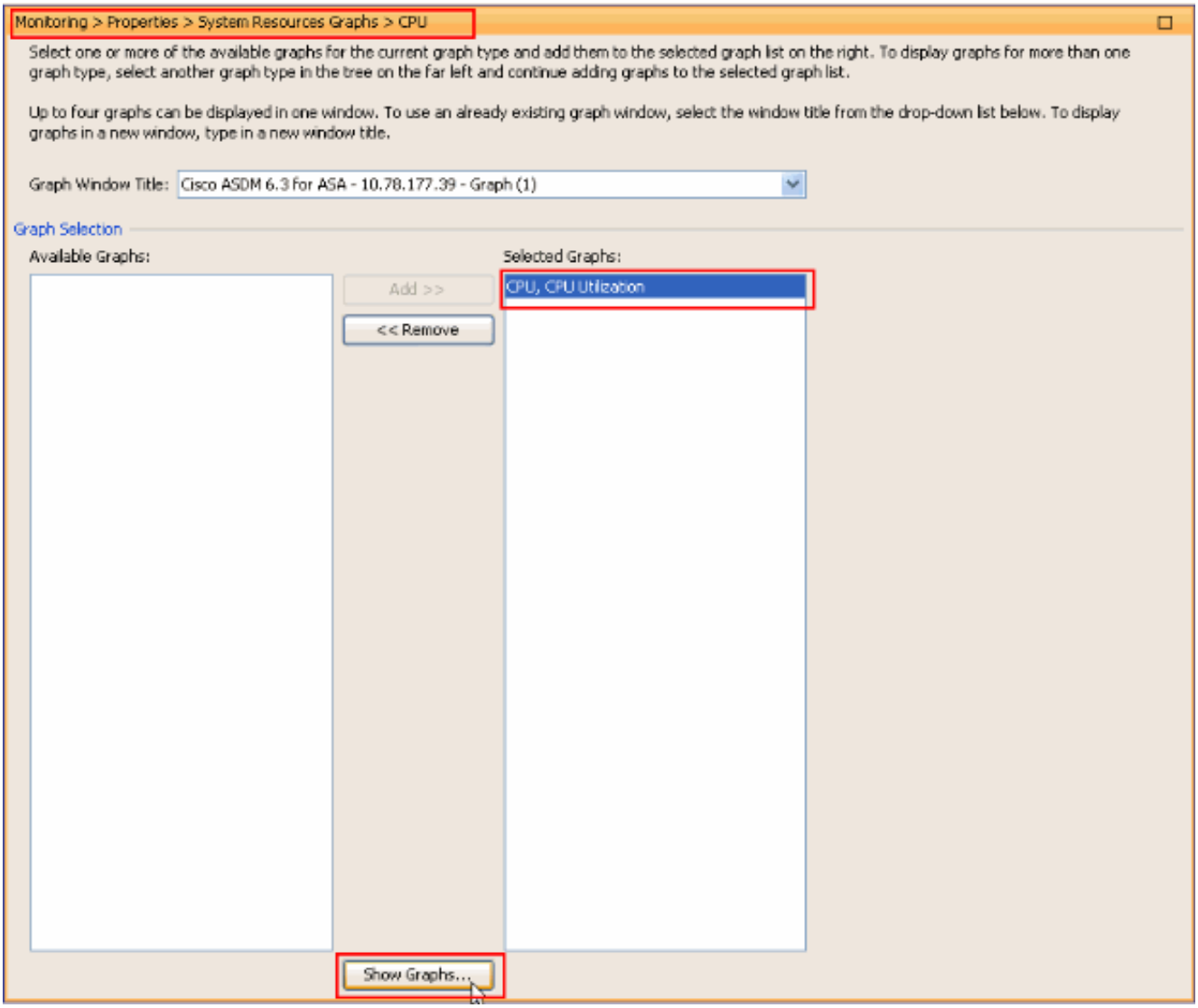
Просмотр использования ЦПУ на ASDM

Выполните эти шаги для просмотра использования ЦПУ на ASDM:

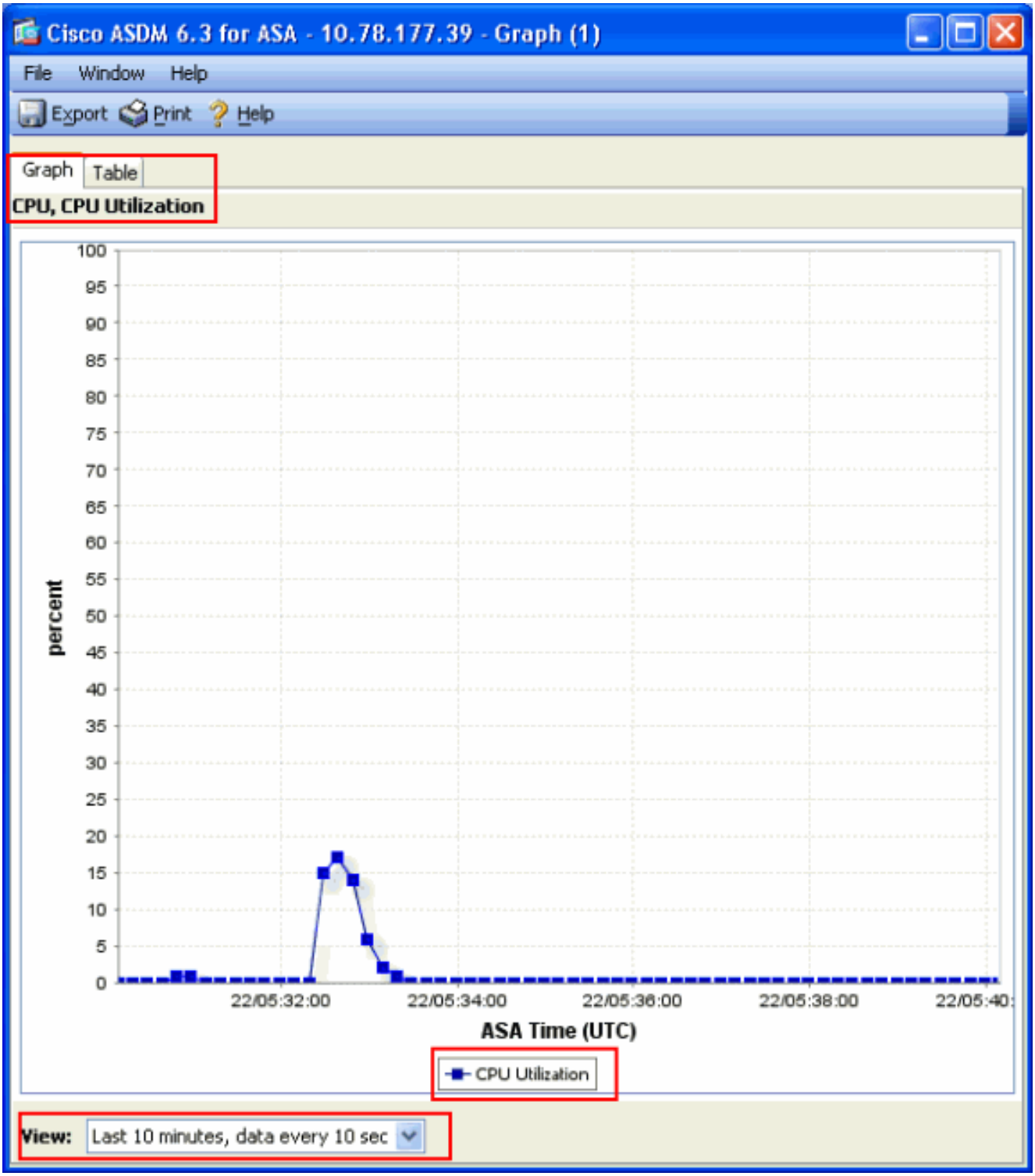
1. Перейдите **к Мониторингу> Свойства> Графика Ресурсов системы> ЦП** в ASDM и выберите **Graph Window Title**. Затем выберите требуемые графики из списка **Доступных Графиков** и **нажмите Add** как показано.



2. Как только требуемое название графика добавлено под **Выбранным** разделом **Графиков**, нажмите **Show Graphs**.



Следующий образ показывает график **Использования ЦПУ** на ASDM. Различные взгляды этого графика доступны и могут быть изменены путем выбора представления от Обзорного выпадающего списка. Эти выходные данные могут быть распечатаны или сохранены к компьютеру как требуется.



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 показывает, сколько трафика, который проходит через ASA за установленный срок времени. 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** для определения, сколько трафика проходит 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 сумма входящего и исходящего трафика на внешнем интерфейсе должна равняться сумме 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 суммы и типов трафика, которые осматривает 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
Xlates	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 пакетов TCP, что ASA вперед в секунду
Перехват TCP	Число SYN-пакетов в секунду, превышающее начальный фиксированный предел
HTTP Fixup	**Количество пакетов, назначенных на порт 80 в секунду (требуется применить команд 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

Наряду с командой отображения загруженности процессора, можно использовать команду show blocks, чтобы определить, перегружен ли ASA.

Блоки обработки пакетов (1550 и 16384 байт)

Когда это входит в интерфейс ASA, пакет размещен в очередь входного интерфейса, прошел до ОС и разместил в блок. Для пакетов Ethernet используется 1550-байтные блоки, для пакетов, приходящих с платы 66 МГц Gigabit Ethernet используются 16384-байтные блоки. ASA определяет, разрешен ли пакет или запрещен на основе Алгоритма адаптивной безопасности (ASA) и обрабатывает пакет через к очереди вывода на исходящем интерфейсе. Если ASA не может поддержать трафик, количество доступных 1550-байтовых блоков (или 16384-байтовых блоков для GE на 66 МГц) парения близко к 0 (как показано в столбце CNT выходных данных команды). Когда нуль соответствий столбца CNT, ASA пытается выделить больше блоков максимум до 8192. Если больше блоков не доступно, 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 передает пакеты резервному ASA для обновления трансляции и таблицы подключений. В течение периодов пульсирующего трафика, где высокие скорости соединений созданы или разъединены, количество доступных 256-байтовых блоков может спасть 0. Это отбрасывание указывает, что одно или более соединений не обновлены к резервному ASA. Как правило, это приемлемо, поскольку протокол аварийного переключения с синхронизацией состояния будет перехватывать xlate или подключение, которое было разорвано. Однако, если столбец CNT для 256-байтовых блоков остается почти заполнен 0 для длительных периодов времени, ASA не может не отставать от трансляции и таблиц подключений, которые синхронизируются из-за количества соединений в секунду, которые обрабатывает ASA. Если это последовательно происходит, обновите ASA к более быстрой модели.

Сообщения системного журнала, передаваемые из ASA также, используют 256-байтовые блоки, но они обычно не освобождаются в таком количестве, которое вызывает истощение 256-байтового пула 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. Это обозначено линией прерывания регистрации в конфигурации ASA. 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, в байтах, пула блоков. Каждый размер представляет определенный тип
МАКС.	Максимальное число блоков, доступных для указанного пула блоков байта. Максимально число блоков вырезано из памяти в загрузке. Обычно максимальное количество блоков неизменно. Исключение для 256-и 1550-байтовых блоков, где устройство адаптивной безопасности может динамично создать больше при необходимости максимум до 8192.
Низкий	Нижний предел. Этот номер указывает на самое низкое количество этого размера блоки, доступные, так как устройство адаптивной безопасности было включено, или начиная с последнего сброса блоков (с командой clear blocks). Нуль в столбце LOW указывает на предыдущее событие, где память была полна.
CNT	Текущий номер блоков, доступных для того определенного пула блоков размера. Нуль в столбце CNT означает, что память полна теперь.

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

Значение SIZE	Описание
0	Используемый блоками dupb.

4	Копирует существующие блоки в приложениях, таких как DNS, ISAKMP, фильтрация URL адресов, uauth, TFTP и модули TCP. Кроме того, этот размерный блок может обычно использоваться кодом для передавания пакеты драйверам и т.д.
80	Используемый в перехвате TCP для генерации пакетов подтверждения и для приветстве сообщений аварийного переключения.
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 Перехвата управления при отказе с синхронизацией состо Активное устройство адаптивной безопасности генерирует и передает пакеты резервном устройству адаптивной безопасности для обновления трансляции и таблицы подключени пульсирующем трафике, где высокие скорости соединений созданы или разъединены, количество доступных блоков могло бы спасть 0. Эта ситуация указывает, что одно или более соединений не были обновлены к резервному устройству адаптивной безопасност Протокол Перехвата управления при отказе с синхронизацией состояния ловит недостак трансляцию или соединение в следующий раз. Если столбец CNT для 256-байтовых бло остается почти заполнен 0 для длительных периодов времени, то устройство адаптивной безопасности испытывает затруднения при хранении трансляции, и таблицы подключени синхронизировались из-за количества соединений в секунду, которые обрабатывает устройство адаптивной безопасности. Сообщения системного журнала, передаваемые и устройства адаптивной безопасности также, используют 256-байтовые блоки, но они обы не освобождаются в таком количестве для порождения истощения 256-байтового пула блоков. Если столбец CNT показывает, что количество 256-байтовых блоков близко 0, гарантируйте, что вы не регистрируете при Отладке (уровня 7) к серверу системного журнала. Это обозначено линией прерывания регистрации в конфигурации устройства адаптивной безопасности. Мы рекомендуем установить регистрацию в Уведомлении (уро 5) или ниже, пока вы не запрашиваете дополнительную информацию для отладки целей.
1550	Используемый для хранения Пакетов Ethernet для обработки через устройство адаптивн безопасности. Когда пакет вводит интерфейс устройства адаптивной безопасности, он размещен в очередь входного интерфейса, прошел до операционной системы и размест блок. Устройство адаптивной безопасности определяет, должен ли пакет быть разрешен запрещен на основе политики безопасности и обрабатывает пакет через к очереди выво исходящем интерфейсе. Если устройство адаптивной безопасности испытает затруднен не отстающие от трафика, то количество доступных блоков будет колебаться близко к 0 показано в столбце CNT выходных данных команды). Когда столбец CNT является нулем устройство адаптивной безопасности пытается выделить больше блоков максимум до 81 Если больше блоков не доступно, устройство адаптивной безопасности отбрасывает пак
16384	Только используемый для 64-разрядных, карт Гигабитного Ethernet на 66 МГц (i82543). С описание на 1550 для получения дополнительной информации о Пакетах Ethernet.
2048	Контроль или управляемые кадры используются для обновлений контроля.

show memory

Команда show memory отображает общую физическую память (или ОЗУ) для ASA, наряду с количеством в настоящее время доступных байтов. Для использования этой информации необходимо сначала понять, как ASA использует память. Когда ASA загружается, он копирует ОС с Флэша в ОЗУ и выполняет ОС от ОЗУ (точно так же, как маршрутизаторы). Затем, ASA копирует загрузочную конфигурацию с Флэша и размещает его в ОЗУ. Наконец, ASA выделяет ОЗУ для создания пулов блоков, обсужденных в разделе блоков показа. Как только это выделение завершено, ASA нужно дополнительное ОЗУ, только если

конфигурация увеличивается в размере. Кроме того, ASA хранит трансляцию и соединения в ОЗУ.

Во время нормальной работы доступная память на ASA должна измениться очень мало, если вообще. Как правило, единственное время, необходимо испытать нехватку памяти, - то, если вы под атакой, и сотни тысяч подключений проходят ASA. Для проверки соединений выполните **команду show conn count**, которая отображает ток и максимальное число соединений через ASA. Если ASA исчерпывает память, он в конечном счете завершается катастрофическим отказом. До катастрофического отказа вы могли бы заметить сообщения ошибки выделения памяти в системном журнале (%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 ток и максимальное число трансляций через 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. Выходные данные Command показывают трансляции "в использовании", которое обращается к количеству активных трансляций в ASA, когда выполнена команда; "наиболее используемый" ссылается на максимальные преобразования, которые когда-либо замечались на ASA, так как он был включен.

> **Примечание:** На одном узле возможно несколько соединений с разными местами назначения и только одна трансляция. 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 ваш внутренний

хост поставился под угрозу, он имитирует адрес источника и передает пакеты ASA.

Примечание: Когда vpnclient конфигурация включена, и внутренний хост отсылает запросы DNS, **команда show xlate** могла бы перечислить множественный xlates для статического преобразования.

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 является Переадресацией Порта TCP для порта хоста (10.1.1.15, 1026) на внутренней сети к порту хоста (192.150.49.1, 1024) на 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 показывает ток и максимальное число соединений через ASA. Подключение сопоставляет сведения уровня 4 от внутреннего адреса внешнему адресу. Соединения созданы, когда ASA получает SYN - пакет для сеансов TCP или когда поступает первый пакет на сеансе UDP. Соединения разъединены, когда ASA получает последний пакет ACK, который происходит, когда квитирование сеанса TCP закрывает или когда таймаут истекает на сеансе UDP.

Счетчики подключения чрезвычайна высокого (50-100 раз обычный) могли бы указать, что вы под атакой. Выполните **команду show memory**, чтобы гарантировать, что число высокоскоростных соединений не заставляет ASA исчерпывать память. 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. См. Справочники по командам многофункциональных устройств защиты Cisco ASA серии 5500 для получения дополнительной информации.

Пример

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

show interface

Команда show interface может помочь определять проблемы несогласованности дуплексных параметров и проблемы с кабелем. Это может также предоставить дальнейшее понимание относительно того, переполнен ли интерфейс. Если ASA исчерпывает возможности ЦПУ, количество 1550-байтовых парений блоков близко к 0. (Посмотрите на 16384-байтовые блоки на картах Концерта на 66 МГц. Другим показателем является увеличение «no buffers» в интерфейсе. Никакое буферное сообщение не указывает, что интерфейс неспособен передать пакет к ASA ОС, потому что нет никакого доступного блока для пакета, и пакет

отброшен. Если увеличение никаких буферных уровней регулярно происходит, выполните **команду show proc cpu** для проверки использования ЦПУ на ASA. Если использование ЦПУ высоко из-за большой информационной нагрузки, обновления к более мощному ASA, который может обработать загрузку.

Когда пакет впервые поступает в интерфейс, он помещается во входную аппаратную очередь. Если входная аппаратная очередь заполнена, пакет помещается во входную программную очередь. Пакет передают из его входной очереди и размещают в 1550-байтовый блок (или в 16384-байтовый блок на Интерфейсах Gigabit Ethernet на 66 МГц). ASA тогда определяет выходной интерфейс для пакета и размещает пакет в соответствующую очередь аппаратных ресурсов. Если аппаратная очередь заполнена, пакет помещается в исходящую программную очередь. Если максимальное число блоков в любой из программных очередей велико, интерфейс переполняется. Например, если 200 Мбит/с входят в ASA, и все выходят одиночный интерфейс на 100 Мбит/с, исходящая программная очередь указывает на большие числа на исходящем интерфейсе, который указывает, что интерфейс не может обработать 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. Кабель мог бы быть неисправным также. 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 вы видите определенный счетчик, который регулярно инкрементно увеличивается, производительность на вашем ASA, скорее всего, страдает, и необходимо найти основную причину 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 коллизий, поздних коллизий 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). Помните, что коллизии 10%-го среднего значения, что ASA понижается на 10% пакетов, которые проходят тот интерфейс; каждый из этих пакетов должен быть ретранслирован.

См. **интерфейсную** команду в Справочниках по командам многофункциональных устройств защиты Cisco ASA серии 5500 для получения дальнейшей информации на счетчиках интерфейса.

show processes

Команда show processes на ASA отображает все активные процессы, которые работают на ASA в то время, когда выполняется команда. 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 результат показывает вам, сколько Времени процессора (в миллисекундах) процесс получил в тот интервал времени. 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:** Исследование каждого процесса ASA вне области этого документа, но упомянуто кратко для полноты. См. Команду show processes ASA для получения дополнительной информации о процессах ASA.

Перечень команд

Таким образом, используйте **команду отображения загруженности процессора** для определения загрузки, под которой находится ASA. Помните, что выходные данные являются рабочим средним числом; ASA может иметь более высокие скачки использования ЦПУ, которые замаскированы рабочим средним числом. Как только ASA достигает 80%-го использования ЦПУ, задержка через ASA медленно увеличивается приблизительно до 90%-го ЦП. Когда использование ЦПУ составляет больше чем 90%, ASA начинает отбрасывать пакеты.

Если уровень загрузки CPU высокий, используйте команду show processes, чтобы определить процесс, который использует больше всего процессорного времени. Используйте эту информацию для сокращения части времени, которое использовано интенсивными процессами (такими как регистрация).

Если ЦП не работает горячий, но вы полагаете, что пакеты все еще отброшены, используют **команду show interface** для проверки интерфейса ASA ни для каких буферов и коллизий, возможно вызванных несогласованностью дуплексных параметров. 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 текущий столбец CNT в **выходных данных show blocks** близко к 0 на 1550-байтовых блоках (16384-байтовые блоки для карт Концерта на 66 МГц), ASA, скорее всего, отбрасывает Пакеты Ethernet, потому что это слишком занято. В этом случае наблюдаются резкие кратковременные повышения нагрузки CPU.

При испытании проблемы при создании новых соединений через ASA используйте **команду show conn count** для проверки текущего числа подключений через ASA.

Если текущее количество высоко, проверьте **выходные данные show memory**, чтобы гарантировать, что ASA не исчерпывает память. **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 использовать другие команды для измерения объема трафика, который проходит через ASA. **Команда show traffic** отображает суммарные пакеты и байты для интерфейса, и **perfmon показа** разламывает трафик на различные типы, которые осматривает ASA.

Дополнительные сведения

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