IDS 4.0/AIP-SSM/IPS 5.0 и Более поздние часто задаваемые вопросы

Содержание

Введение

Этот документ отвечает на большинство Часто задаваемых вопросов (часто задаваемые вопросы), отнесенные к Cisco Secure Intrusion Detection System (IDS) 4.0, Усовершенствованный Модуль Сервисов безопасности Контроля и Предотвращения (SSM AIP), и система предотвращения вторжений Cisco (IPS) (IPS) 5.0 и позже.

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

IDS 4.0

Вопрос. . Я установил MC IDS и SecMon по новому серверу, и теперь я хочу к конфигурациям import all (пользователь, устройство, и т.д) от старого сервера до нового. Как я делаю это?

O. Самый легкий способ выполнить это состоит в том, чтобы перевести ваш новый сервер VMS в рабочее состояние, и затем [обнаружить](#) Датчики с этой новой коробкой.

Примечание: Когда вы добавите Датчик, не добавляйте его вручную. Установите **обнаружить** флажок **параметров настройки**.

Как только Датчик обнаружен, импортируйте его в **SecMon**. Все конфигурации сохранены на Датчике. Параметры настройки подписи, фильтры, и т.д должны столкнуться после построения нового сервера. Удостоверьтесь, что вы обновляете MC IDS к последним подписям.

Вопрос. . IDS-4215 получает `idsPackageMgr:` сообщение об ошибках , в то время как это пытается обновить раздел восстановления IDS. Что я должен сделать для решения этого вопроса?

O. Это - проблема качества изготовления. Некоторые клиенты получили IDS-4215 с плохим базовым образом (4.0). Выполните следующие действия.

1. Загрузите образ для восстановления раздела (только зарегистрированные клиенты).
2. Примените обновление образа для восстановления раздела через CLI: `sensor#configure terminal sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/ IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg`
3. Как только образ для восстановления раздела применен, эти 4215 восстановлен нормальной работе 4.1 (1) 4215 ядер. `sensor(config)#recover application-partition`

Вопрос. . Когда я обновляю от 2-разрядного до 3-разрядных пакетов уровня сигнала, таких как S100 или позже, например, 4.1 (4) S99 к 4.1 (4) S100, сбои функциональности автоматического обновления. Как это исправить?

Примечание: VMS Cisco и клиенты CLI не испытывают эту проблему.

Причиной проблемы является логика сортировки, которая используется, когда проанализировано имя файла. Это - алфавитно-цифровой вид, когда это должно быть числовым. Обходной путь должен использовать CLI (или VMS) для обновления к 3-разрядным пакетам уровня сигнала, таким как S100 или позже. Как только это завершено, автоматическое обновление начинает функционировать снова. См. идентификатор ошибки Cisco CSCef07999 (только зарегистрированные клиенты) для получения дополнительной информации.

Вопрос. . Что делает " ". среднее значение сообщения об ошибках?

O. Для решения этой проблемы используйте пароль по умолчанию (Cisco) два раза и затем измените пароль от режима конфигурации. Идентификаторы требуют, чтобы пароль по умолчанию был введен дважды.

Пример:

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re-enter new password: ***
```

Вопрос. . Как я удаляю IDSM из Коммутатора?

O. Модуль должен быть удален только после отключения питания. Выполните следующие действия:

1. От CLI датчика выполните **команду reset powerdown**.
2. Как только датчик завершает завершение, от CLI коммутатора, проблема или **команда no power enable module (module_number)** для Cisco IOS или **команда set module power down (module_number)** для CatOS.
3. Нажмите кнопку shutdown на панели.
4. Физически выключите электропитание стойки маршрутизатора. Когда световой индикатор состояния отображает более длинный зеленый, можно удалить модуль безопасно.

IPS 5.0 и позже

Вопрос. . У меня есть настроенное избегание, но я смущен тем, как настроить блокирование на подписях. Каково различие между блочным хостом и блочным соединением?

О. Блочный хост блокирует все пакеты от того адреса источника. Блочное соединение только блокирует одно соединение на основе/port IP - адреса назначения и источника. PIX работает немного отличающимся способом. Поскольку автоматический избегает, Датчик передает source IP, IP - адрес назначения, исходный порт и порт назначения. PIX блокирует все пакеты, которые происходят из того IP-адреса. Дополнительные сведения используются PIX для удаления того одного соединения из его таблиц подключений. Если соединение не было удалено из таблицы подключений, то теоретически возможно что, если избегание удалено вскоре после того, как это применено, то исходное соединение еще, возможно, не испытало таймаут. Это позволяет атакующему продолжать атаку на исходное соединение. Удаление соединения от таблицы гарантирует, что исходное соединение не может использоваться для продолжения атаки после того, как удалено избегание. Датчик не может избежать одиночного соединения на PIX, потому что PIX не поддерживает использование **избегать** команды для избегания одиночного соединения. PIX **избегает** команды, всегда избегает адреса источника независимо от того, предоставлена ли дополнительная информация о соединении.

Вопрос. . Что делает **": . . MUST , ".** среднее значение сообщения об ошибках?

О. Эта ошибка означает, что ваш шлюз по умолчанию является неправильным или сообщение об ошибках общего назначения, которое означает, что или IP, маска подсети или шлюз по умолчанию являются неправильными. часть сообщения означает, что после первого сбоя, предыдущая конфигурация была применена и также подведена. **Ifconfig** проблем Датчика и команды **маршрута** и один или они оба отказывают.

Вопрос. . Автоматическое обновление отказывает с **" HTTP response:500 mainApp [343] Cid/E errSystemError". .** Что означает это сообщение об ошибках?

О. Эта проблема могла бы быть функцией автоматического обновления, которая не работает, потому что это собирается загрузить в ровный час. Попытайтесь установить автоматическое обновление до произвольного момента времени; даже маленькое смещение восемь или ночные минуты может решить эту проблему.

В целом вопрос решен, и сообщение об ошибках `Error: http error response: 500` быть замеченным при изменении времени поиска на непочасовую границу.

Примечание: IPS отказывает автоматическое обновление подписей и возвращается с этим сообщением об ошибках:

```
AutoUpdate exception: HTTP connection failed [1,110] name=errSystemError
```

Проверьте эти элементы для решения этого вопроса:

- Проверьте, препятствует ли межсетевой экран тому, чтобы датчик достиг Cisco.com.
- Проверьте, становится ли маршрутизация проблемой.
- Проверьте, настроено ли преобразование посредством NAT должным образом на устройстве шлюза для нисходящего устройства.

- Проверьте, корректны ли учетные данные пользователя.
- Измените время начала обновления на нечетные часы.

Вопрос. . Что делает ": execUpgradeSoftware: AnalysisEngine . ".. среднее значение сообщения об ошибках?

O. Для решения этого вопроса попытайтесь повторно загрузить датчик или повторно захватить образ датчик.

Вопрос. . Как делают я решаю сообщение об ошибках Cid/W - DNS HTTP , DNS -. - HTTP DNS ''?

O. Выполните эти задачи для решения этого вопроса:

- Отключите глобальную корреляцию.
- Добавьте прокси/конфигурацию DNS.

Вопрос. . Как делают я решаю эти ошибки, которые IPS получает для глобальных проблем со здоровьем корреляции: "23Jan2010 15:50:39.831 38.001 collaborationApp[655] rep/E : TLS HTTP X.X.82.127:443: TLS " И "collaborationApp[459] rep/E : ibrs/1.1/drop/default/1296529950: URI IP - "?

O. IPS неспособен получить к Интернету из-за проблемы порта, например, межсетевого экрана в пути, который не имеет правильных портов открытыми для доступа в Интернет или это может быть проблема NAT.

Для глобальной корреляции для функционирования полностью датчик сначала связывается посредством **обновления-manifests.ironport.com** https для аутентификации пользователя и затем соединения HTTP для загрузки обновлений GC. Файлы, что загрузки датчика от HTTP (updates.ironport.com) являются данными репутации та глобальная корреляция использование. Обновление-manifests.ironport.com https должно всегда решать к адресу X.X.82.127, но http **updates.ironport.com** IP-адрес может измениться, который зависит в Интернете, к которому вы обращаетесь. Таким образом, необходимо проверить IP-адрес. Если фильтрация URL-адресов включена, добавьте исключение для IP интерфейса управления IPS в фильтре URL, так, чтобы IPS мог соединиться с Интернетом.

Когда существует повреждение в предыдущем обновлении GC, эта ошибка происходит:

```
collaborationApp[459] rep/E A global correlation update failed: Failed download of
ibrs/1.1/drop/default/1296529950 : URI does not contain a valid ip address
```

Эта проблема может обычно исправляться путем выключения сервиса GC и затем снова включения его. В IDM выберите **Configuration> Policies> Global Correlation> Inspection/Reputation**, установите Глобальный Контроль Корреляции (и **фильтрация Репутации** если **На**) к **Выключено**, примените изменения, ждите в течение 10 минут, включите функции и монитор.

Вопрос. . : openConnection: IpAddrException badAddrString. HTTP DNS. . сообщение об ошибках получено в "Категории" сбоя обновления репутации. Как решить этот вопрос?

O. Проверьте эти элементы:

- У вас должна быть допустимая лицензия IPS, чтобы позволить глобальным функциям корреляции функционировать.
- У вас должны быть Прокси-сервер HTTP или сервер DNS, настроенный, чтобы позволить глобальным функциям корреляции функционировать.
- Поскольку обновления глобальной взаимосвязи происходят через интерфейс управления датчика, межсетевые экраны должны позволить tcp 443/80 и трафик udp 53.
- Удостоверьтесь, что ваш датчик поддерживает глобальные функции корреляции. Если вы не хотите это, отключите глобальную опцию совместной работы от IDM:Перейдите **к Конфигурации> Политика> Глобальная Корреляция> Контроль/Репутация** и установите Глобальный Контроль Корреляции (и фильтрация Репутации если **На**) к **Выключено**.

Вопрос. . Как делают я решаю **" : openConnection: IpAddrException badAddrString"** ошибка, которую IPS получает для глобальной проблемы со здоровьем корреляции?

O. При использовании глобальную корреляцию (GC), тогда удостоверяются, что разрешение имен работает, например, DNS достижим. Также проверьте, существует ли блокированный порт межсетевого экрана 53. В противном случае, если вы хотите избавиться от этого сообщения, можно выключить функцию GC.

Вопрос. . Как я решаю сообщением об ошибках **MySQL**, которое я получаю, когда я запускаю IME от браузера?

O. Эта проблема обычно происходит когда попытка клиента выполнить IME на неподдерживаемых операционных системах, таких как Windows 7.

Вопрос. . Как делают я решаю **": IDM 88-nsmc-c1 : Cisco Systems. : JAR JNLP ". " , x. x. x. x: 443, idm"** ошибка, которую получает IDM, который происходит во время запуска приложения?

O. Очистите кэш-память обозревателя для решения этого вопроса.

Вопрос. . Конфигурируем Асимметричный режим на IPS при использовании GUI?

O. В версии 6.0, Асимметричном режиме на IPS, который является конфигурируемым CLI использования только и не доступный на GUI. Но, в версии 6.1 эта функция также доступна в GUI.

Вопрос. . Как я решаю вопрос задержки с сенсором IPS?

O. Для решения этого вопроса включите асимметричную обработку режима, чтобы позволить датчику синхронизировать состояние с потоком и поддерживать контроль для тех механизмов, которые не требуют обоих направлений. Используйте эту конфигурацию:

```
IPS_Sensor#configure terminal IPS_Sensor(config)#service analysis-engine IPS_Sensor(config-
ana)#virtual-sensor vs0 IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

Проблема задержки происходит, когда запрещать действие встраивает и запрещает пакет, включены для каждой подписи в VS0. Включение всех подписей приведет к задержке, поскольку IPS осматривает каждое пакетное прохождение. Хорошо включить только определенную подпись, требуемую согласно потоку сетевого трафика для решения вопроса задержки.

Вопрос. . SSM AIP помогает блокировать Skype?

O. PIX/ASA не в состоянии заблокировать трафик skype. Skype имеет емкость выполнить согласование о динамических портах и использовать зашифрованный поток данных. С зашифрованным потоком данных фактически невозможно обнаружить его, поскольку нет никаких образцов для поиска.

Вы могли в конечном счете использовать Cisco IPS (Система предотвращения вторжений)/AIP-SSM. Это имеет некоторые подписи, которые в состоянии обнаружить Windows Skype Client, который соединяется с сервером Skype для синхронизации его версии. Когда клиент инициируется соединение, это обычно делается. Когда датчик берет начальное соединение Skype, можно быть в состоянии найти человека, кто использует сервис и блокируется, все соединения инициировали от их IP-адреса.

Вопрос. . Почему считывание взаимодействует или часто переходит к нерабочему состоянию в IPS?

O. Во время обновления подписи и изменений конфигурации, sensorApp останавливается для обработки пакетов, поскольку он обрабатывает новые подписи в обновлении. Сетевой драйвер обнаруживает, что sensorApp остановил и вытягивает любые новые пакеты от буфера. Таким образом, сетевой драйвер делает разные вещи, который зависит от модели датчика и конфигурации:

Разнородный Интерфейс — Это переводит ссылку в нерабочее состояние на интерфейсах и приносит резервное копирование ссылки, как только sensorApp начинает контролировать снова.

Встроенный Интерфейс или Встроенная Пара Vlan — Это зависит от Обходной установки:

- **Автоматический обход** — драйвер поддерживает соединение и начинает передавать пакеты через без анализа. Это тогда возвращается назад к передаче пакетов через sensorApp, как только sensorApp начинает контролировать снова.
- **Обход Выключено** — драйвер переводит в нерабочее состояние ссылку на интерфейсах, которая совпадает с в случайном режиме и приносит им, резервное копирование однажды sensorApp начинает контролировать снова.

Так, если приложение датчика не вытягивает пакеты от буфера, который возможно происходит, потому что нет никакого интерфейса, настроенного для обработки пакетов, тогда драйвер может поместить интерфейс в состояние `down`.

Когда считывание взаимодействует откидные створки, эти журналы замечены:

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
```

```
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

Вопрос. . IDS или датчик Системы предотвращения вторжений (IPS) поддерживают историю пароля?

O. Нет, датчик не поддерживает историю пароля. Пароли не доступны для просмотра никогда.

Вопрос. . IDS или датчик Системы предотвращения вторжений (IPS) поддерживают сервер системного журнала для передачи журналов?

O. Нет.

Вопрос. . Каково ограничение максимального значения хранения событий в IPS?

O. Локальное событие датчика хранит только 30 МБ и начинает перезаписывать себя, как только достигнут предел на 30 МБ. Этот предел неизменяем.

Вопрос. . Как я пишу подпись для обнаружения фотографии [a-z] \.zip файл в какой-либо входящей электронной почте или исходящей почте?

O. Используйте STRING.TCP для записи подписи, которая обнаруживает прикрепление. Ищите что-то подобное этому:

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["][Ff][Oo]
             [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
ResetAfterIdle 15
ServicePorts 25
StorageKey =STREAM
```

Вопрос. . Как вы настраиваете таймаут клиента FTP?

O. Введите следующие команды:

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

Вопрос. . Как вы преобразовываете Время начала и Время окончания в iplog-статусе к удобочитаемому формату?

O. Эти выходные данные являются десятичным представлением текущего времени начиная с эпохи UNIX. Используйте программу расчета Epoc UNIX, такую как та, расположенная на

узле Калькулятора Даты/Времени UNIX. Введите первые 10 цифр, потому что этот калькулятор гранулирован к только секундам и Хранениям наносекунд системой IDS. Это означает, что являются неизолированными последние девять цифр. Со Времени начала в этих выходных данных `1084798479 =  17  12:54:39 (GMT) 2004` - то, что вы получаете.

От CLI введите **iplog-статус** для получения этих выходных данных:

```
"
Log ID:             138343946
IP Address:         xxx.xxx.xxx.xxx
Group:              0
Status:             completed
Start Time: 1084798479512524000 End Time: 1084798510136582000 Bytes Captured: 2833 Packets
Captured: 14 "
```

Вопрос. . "IOException, : Java. . . CertificateExpiredException". сообщение об ошибках появляется. Как это может быть решено?

O. Для решения этого сообщения об ошибках, входят в SSM AIP и для выдачи ключевой для tls генерирует команды в привилегированном режиме EXEC как показано в данном примере:

```
sensor#tls generate-key
```

Примечание: Это разрешение использования ключа tls генерирует команды также решает вопрос о SSM AIP, не бывшем способном соединиться с IME.

Вопрос. . "IOException: refused:connect. IME IME . , " сообщение об ошибках, появляется, в то время как я добавляю IPS в IME. Как решить эту проблему?

O. Для решения этого сообщения об ошибках выберите **Control Panel>> Services Admin Tools** и перезапустите сервисы IME.

Вопрос. . / config [IOException - ,], сообщение об ошибках получено, когда я добавляю сенсор IPS к IME. Как решить эту проблему?

O. Это указывает на сломанную связь между IME и сенсором IPS. Удостоверьтесь, что нет никакого программного обеспечения, которое блокирует SDEE.

Вопрос. . " IME: ( )". сообщение об ошибках появляется. Как решить эту проблему?

O. Для решения этого сообщения об ошибках проверьте, что правильный IP-адрес используется, когда вы добавляете IPS в IME и также проверяете любой программный брандмауэр, который работает на компьютере IME, который может заблокировать соединение.

Вопрос. . Могут IDS или датчик Системы предотвращения вторжений (IPS) передают почтовые предупреждения?

O. Детектор обнаружения несанкционированного доступа (IDS Sensor) не имеет способности передать почтовые предупреждения самостоятельно. Когда Правило События

инициировано датчиком, монитор безопасности, когда используется с IDS имеет способность передать почтовые уведомления.

См. Настраивают Уведомления по электронной почте для получения дополнительной информации о том, как настроить почтовые уведомления с Монитором Безопасности.

Когда Правила События инициированы датчиками Cisco IPS, Cisco IPS Manager Express (IME) может быть настроен для передачи сообщения почтового уведомления (предупреждения). См. IPS 6. X и позже: Почтовые уведомления с помощью Примера конфигурации IME для получения дополнительной информации.

Вопрос. . : `mainApp (getVersion). .` когда я пытаюсь соединиться с моим датчиком, сообщение об ошибках появляется. Как решить эту проблему?

O. Перезагрузите датчик для решения этого вопроса.

Вопрос. . : `% Warning: , regexes. . , .` сообщение об ошибках появляется подпись, настраивающаяся на моем датчике. Как решить эту проблему?

O. Исключите подписи, которые не используются для решения этого вопроса, и также количество подписей клиента с regexes должно быть сокращено. Кроме того, не рекомендуется использовать * и + метасимволы в regexes.

Вопрос. . Почему проблемы задержки происходят на системе предотвращения вторжений Cisco (IPS) (IPS) датчики? Как решить эту проблему?

O. Проблема задержки может произойти из-за асимметричной маршрутизации. Попытайтесь отключить подпись 1330 для решения этого вопроса.

Вопрос. . Действительно ли возможно отключить SSHv1 и уехать, только SSHv2 включил на системе предотвращения вторжений Cisco (IPS) (IPS) датчики?

O. Прямо сейчас не возможно отключить SSHv1 и уехать, только SSHv2 включил. И SSHv1 и SSHv2 включены вместе и не могут быть отключены индивидуально.

Вопрос. . : `, =, 115000 /usr/cids/idsRoot/var, 110443 .` когда я обновляю датчик к версии 4.1 (5), сообщение появляется. Как решить эту проблему?

O. Это сообщение об ошибках происходит из-за недостаточной памяти в датчике.

Выполните эти задачи для решения этого вопроса:

1. Войдите в учетную запись сервиса и станьте root
2. Удалите следующие каталоги как показано ниже: `# rm -rf /usr/cids/idsRoot/var/updates/files/S69`

```
# rm -rf /usr/cids/idsRoot/var/updates/files/common
# rm /usr/cids/idsRoot/var/virtualSensor/*
# rm /usr/cids/idsRoot/var/.tmp/*
```

3. Теперь попытайтесь обновить датчик. См. идентификатор ошибки Cisco CSCsb81288 (только зарегистрированные клиенты) для получения дополнительной информации.

Вопрос. . Я добираюсь, `mainApp [396] cplane/E - (), -1` сообщение об ошибках во входе в систему ASA. Как может быть решена эта ошибка?

O. `mainApp [396] cplane/E - (), ,-1` сообщение об ошибках указывает, что Web-сервер не может считать файл и принять () подведенную программу, который приводит к дескрипторам файла, когда существуют TLS подключение. Но этот файл не необходим для нормального поведения. Это безопасно.

Вопрос. . Как делают я решаю `tls/W errTransport WebSession:: TLS sessionTask:` сообщение об ошибках?

O. Это сообщение об ошибках указывает, что сертификат больше не действителен на модуле. Чтобы устранить эту проблему, выполните следующие действия:

1. Восстановите сертификат от CLI:Войдите к командной строке датчика.Выполните **команду tls generate** и нажмите **Enter**. Обратите внимание на отпечатки пальца, которые отображены.
2. Втяните новый сертификат к IME:Откройте IME и найдите название датчика в списке на Домашней странице.Щелкните правой кнопкой мыши датчик и нажмите **Edit**.При достижении Экрана устройства Редактирования нажмите **OK**. Обойдите любое предупреждение о неспособности получить время датчика.Вам предложат с новым сертификатом безопасности (тот, который вы просто генерировали). Проверьте, чтобы удостовериться соответствие отпечатков пальца и нажать **Yes**.После нескольких секунд датчик должен показать "Связанный" в конечном счете Статус снова.

Вопрос. . Когда я пытаюсь войти к IPS, я получаю это сообщение об ошибках: `errSystemError-ct-sensorAPP.450, , clientpipe, .` Как исправить эту ошибку?

O. Для решения этой ошибки используйте **команду reset** для перезагрузки IPS.

Вопрос. . Время на SSM AIP расходится со времени в устройстве адаптивной защиты Cisco (ASA). Как решить эту проблему?

O. Для решения этого вопроса используйте сервер NTP для синхронизации времени на устройстве адаптивной защиты Cisco (ASA) и SSM AIP.

См. NTP Настройки на сенсорах IPS для получения дополнительной информации.

Вопрос. . Как я могу применить множественные действительные датчики на SSM AIP?

O. Действительные датчики на SSM AIP не могут быть применены для интерфейса, потому что SSM AIP имеет только один интерфейс. При создании множественных действительных датчиков необходимо назначить этот интерфейс только на один действительный датчик. Вы не должны определять интерфейс для других действительных датчиков.

После создания действительных датчиков необходимо сопоставить их с контекстом безопасности на Устройстве адаптивной защиты (ASA) с помощью **команды allocate-ips**. Можно сопоставить много контекстов безопасности со многими действительными датчиками. См. *Назначающие Действительные Датчики к* разделу *Контекстов Устройства адаптивной безопасности* SSM AIP Настройки для получения дополнительной информации.

Вопрос. . Каково максимальное число действительных датчиков, поддерживаемых SSM AIP?

O. Максимальное число четырех действительных датчиков может поддерживаться.

Вопрос. . Если я использую SSH или IDM для входа в систему к IPS тогда, действительно ли возможно настроить IPS 4240/IDSM/IDSM2 для проверки административных пользователей против RADIUS/TACACS + сервер?

O. Это не возможно с TACACS +, сервер, но RADIUS поддерживается от IPS 7.0. (4) выпуск E4. См. *Новое и Измененные сведения* и *Ограничения и* разделы *Ограничений* Комментариев к выпуску для системы предотвращения вторжений Cisco (IPS) 7.0 (4) E4 для получения дополнительной информации. Кроме того, обратитесь к IPS 7. X: Аутентификация Регистрационной информации пользователя для входа использование ACS 5. X как Пример Конфигурации сервера RADIUS для примера конфигурации.

Вопрос. . Каково влияние лицензии с истекшим сроком на IPS funcationality?

O. Единственное влияние, которое лицензия с истекшим сроком оказывает на датчик, - то, что это останавливает обновления подписи.

Вопрос. . Обновления подписи IPS оказывают влияние на сервисы или сетевое подключение?

O. Нет. Обновления подписи IPS не оказывают влияние на сервисы или сетевое подключение.

Вопрос. . Каков точный URL, который я должен ввести для Модуля ips для обновления автоматически с последними подписями?

O. Ссылка, требуемая позволять Модулю ips обновлять автоматически с последней подписью: https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl.

Необходимо использовать ID пользователя Cisco и пароль для завершения обновления Модуля ips.

Примечание: В 6.x серия кода, не поддерживаются автоматические обновления от Cisco.com. Необходимо вручную загрузить Файлы цифровой подписи и применить их к датчику. Существует функция auto-update в 6.x код; однако, это возможно только от локального файл-сервера, в котором Файлы цифровой подписи должны быть вручную загружены также.

Вопрос. . Сенсор IPS, уязвимый для переадресации портов X11, открывают

сеанс уязвимость налета?

O. Нет. Это не уязвимо по этим причинам:

- Датчик не имеет библиотек X11. Поэтому нет никаких сеансов для угона.
- Переадресация портов X11 не включена в конфигурации SSH.
- IPv6 не скомпилирован в ядро датчика. Это требуется для использования уязвимости.

Вопрос. . Когда ASA показывает много журналов предупреждения и атаки, почему SSM AIP не показывает журналов?

O. Это происходит, потому что, когда ASA блокирует что-то, его не передают к IPS для двойного контроля. Поэтому вы не видите, что копия входит в систему ASA и IPS.

Вопрос. . После того, как пользователь развертывает набор подписи S518, " **invalidValue:Editng string-xl-tcp XXXX** " сообщение об ошибках, происходит. В чем причина?

O. Это - завершенное сообщение об ошибках:

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=-240 timeZone=GMT-05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string-xl-tcp
sig 21619 has NO effect
```

Эта проблема подходит, потому что string-xl-tcp или string-tcp-xl механизм не поддерживаются на аппаратных средствах. Для получения дополнительной информации обратитесь к Механизму IPS Комментарии к выпуску E4.

Вопрос. . Когда я автоматически обновляю подписи на ASA-SSM-10 с функцией автоматического обновления, я получаю это сообщение об ошибках: , **status=true**. Как устранить эту проблему?

O. Эти выходные данные показывают завершенное сообщение об ошибках:

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi-bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Эта ошибка генерировалась, и подписи автоматически не обновляют, потому что обновления определения Подписи после S479 требуют механизма E4. Для решения этого необходимо вручную обновить Датчик к 7.0 (2) E4.

Примечание: Датчик не в состоянии автоматически обновить себя к E4, потому что это требует 7.0 (2) и перезагрузка Датчика.

Вопрос. . Автоматическое обновление feauture на IPS 5.0 для модуля NIDS не работает. Как устранить эту проблему?

O. Эти выходные данные показывают завершенное сообщение об ошибках:

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Эта проблема происходит из-за неподходящего стиля составления списка каталогов с сервером FTP. Для решения этого переключитесь к составлениям списка каталогов стиля UNIX из существующих составлений списка каталогов стиля MS-DOS.

Для изменения параметров настройки составления списка каталогов выберите**> Program Files Start> Средства администрирования** для открытия диспетчера служб Интернета. Затем перейдите к вкладке Home Directory и измените стиль составления списка каталогов от MS-DOS до UNIX.

Вопрос. . IPS 4255 получает сбои SensorApp в TcpRootNode:: expireNow () сообщение об ошибках во время обновления. Как решить этот вопрос?

O. Эта проблема происходит из-за сбоя аналитического механизма и решена в идентификаторе ошибки Cisco CSCtb39179 (только зарегистрированные клиенты). Обновите датчик к версии 7.0 (4) E4 для устранения этой проблемы.

Вопрос. . Когда я пытаюсь выполнить обновление лицензии после того, как я purchanse новая лицензия данные устройства эта ошибка: **" update license ". "ErrExpiredLicense , , . ?**

O. Когда полученный файл лицензии недопустим, эта проблема происходит. Для получения действительного файла лицензии войдите к Cisco.com как зарегистрированный пользователь и загрузите соответствующий файл лицензии. Как только вы получаете действительный файл лицензии, установите его на своем датчике.

Если вы устанавливаете новый файл лицензии, и вы все еще получаете ошибку, могла бы быть проблема с существующим файлом неверного номера лицензии. Для решения этого вопроса выполните эти шаги для удаления существующего файла неверного номера лицензии:

1. Войдите к учетной записи сервиса путем ввода имени пользователя учетной записи сервиса.Если вы не имеете учетной записи сервиса, открываете командную строку IPS, введите режим конфигурации и введите эту команду*пароль* **сервисного пароля привилегии** *названия* **имени пользователя**
```
ciscoasa# session 1
Opening command session with slot 1.

Connected to slot 1. Escape character sequence is 'CTRL-^X'.
login:
Password:

IPS#
IPS#conf t
IPS(config)# username name privilege service password password
```
2. Как только вы входите к своей учетной записи сервиса, введите **su** команду, чтобы перейти к root (использование того же пароля как учетная запись сервиса).
3. Удалите файлы в/usr/cids/idsRoot/shared/каталоге.**Примечание:** Не удаляйте host.conf файл.Введите **CD/usr/cids/idsRoot/shared/**команда, чтобы перейти к общему

каталогу.Введите **ls** команду для просмотра файлов в каталоге.Введите команду *file_name* **rm** для удаления файлов.**Примечание:** Не удаляйте host.conf файл.

4. Введите **команду/etc/init.d/cids restart** для перезапуска датчика.
5. Установите новую лицензию.

Ошибка Cisco была подана для адресации к этому поведению. Для получения дополнительной информации обратитесь к CSCtg76339 (только зарегистрированные клиенты).

Вопрос. . Что делает `errorMessage: IpLog 1712041197 - .` среднее значение сообщения об ошибках `name=ErrLimitExceeded`? Как решить этот вопрос?

O. Эта ошибка вызвана дополнительной оплатой пакетов на регистрации IP. Отключите характеристику входа в систему IP для решения этого вопроса. Регистрация IP предназначается для устранения проблем только; Cisco рекомендует не включить ее для всех подписей.

Вопрос. . Когда я обновляю датчик от s550 до s551, я получаю эту ошибку: `"signatureDefinition" "sig0".` Как устранить эту проблему?

O. Модификация подписи 23899.0 вызывает эту проблему. См. идентификатор ошибки Cisco CSCtn84552 (только зарегистрированные клиенты) для получения дополнительной информации.

Вопрос. . Я получаю эту ошибку на датчике: `: cisco.com, : HTTP.` Как устранить эту проблему?

O. Проверьте, существует ли фильтрация URL-адресов, фильтрация содержимого или подарок прокси-сервера, который блокирует автоматическое обновление от случая. Удостоверьтесь, что автоматическое обновление не блокируется, и также проверьте, что предоставленные учетные данные пользователя корректны.

Вопрос. . Я получаю это сообщение ошибки XML на сенсоре IPS, который выполняется с версией 6.2 (3) E4: `: IPS XML (). () XML '*'.` Как устранить эту проблему?

O. Это поведение было обращено идентификатором ошибки Cisco CSCsq50873 (только зарегистрированные клиенты). Это - косметическая проблема и не создает в рабочем состоянии издержек кроме дополнительной оплаты получаемых журналов. Временный обходной путь должен удалить связанную конфигурацию NTP на датчике. Для постоянного решения обновите к версии, в которой исправлена эта ошибка.

Вопрос. . Почему рабочая станция IME делает постоянные подключения к управляемым серверам несмотря на клиента закрытыми?

O. IME функционирует как две службы Windows и графический клиент. Когда клиент закрыт, эти две службы Windows (Cisco IPS Manager Express и MySQL-IME) продолжают выполнять и собирать события от управляемых датчиков и хранить их в локальной базе данных MySQL; это обеспечивает историческое создание отчетов для появления.

Клиент IME должен открыть одиночную подписку SDEE для управляемого датчика и снова использовать эту подписку для последующего действия извлечения события. Постоянное подключение с рабочей станции IME на управляемые датчики является нормальным поведением.

Вопрос. . Модуль SSM AIP может использоваться в качестве цели SPAN?

О. Нет. Модуль SSM AIP не может использоваться в качестве цели SPAN, как он используется только для мониторинга потока трафика через интерфейс ASA.

Вопрос. . Почему высокая загрузка ЦП наблюдается после того, как IPS обновлен к механизму E3?

О. С обновлениями механизма E3 IPS использует другой алгоритм для управления его временем простоя и проводит больше времени, опрашивая для пакетов для сокращения задержки. Это увеличило причины проверки соответствующее увеличение в использовании ЦПУ. Правильно для измерения ЦП в E3 не использованием ЦПУ, а **процентом Загрузки пакетов**, который показывает корректную загрузку ЦПУ.

Вопрос. . Почему состояние здоровья является светодиодом, покрасневшим периодически на моем устройстве IPS?

О. Это могло произойти из-за неправильного сертификата на удаленной станции управления, рабочее программное обеспечение, такое как MARS CS, CSM, IEV, VMS-IDS/IPSMC, и т.д. Чтобы решить эту проблему, выполните следующие действия:

1. Примените сертификат TLS датчика на удаленную управляющую станции.
2. Настройте допустимый сервер DNS.

Вопрос. . Как IPS можно мешать задержать трафик HTTP при пересечении его интерфейсов?

О. Настройка датчик для работы в асимметричном режиме решит вопрос. Для помещения датчика в асимметричную защиту режима выполните эти шаги:

1. Перейдите **к Конфигурации> Политика> политика IPS**.
2. Дважды нажмите **действительный датчик**.
3. Перейдите **к опциям усовершенствования**.
4. Под нормализуют режим, выбирают **Asymmetric mode protection**.
5. **Нажмите кнопку ОК.**
6. Перезагрузите модуль для изменений для вступления в силу.

Дополнительные сведения

- Страница технической поддержки системы предотвращения вторжений Cisco Secure
- Устранение неполадок AIP-SSM
- Уведомления о дефекте для специалистов по продуктам безопасности (включая обнаружение несанкционированного доступа CiscoSecure)

- Cisco Systems – техническая поддержка и документация