Модуль сервисов межсетевого экрана (FWSM) часто задаваемые вопросы

Содержание

Введение

В данном документе содержатся ответы на часто задаваемые вопросы о модуле служб межсетевого экрана Catalyst 6500 (FWSM).

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

Поддерживаемые характеристики

Вопрос. . Какова минимальная версия программы, которая может поддерживать работу с FWSM, модулем 2 обнаружения вторжений в систему (IDSM2) и модулем служб VPN (VPNSM)?

О. Соответствующая версия кода зависит от типа Модуля супервизора в ваших 6500 или 7600 шасси, а также типа программного обеспечения, которое вы выполняете (CatOS [Гибрид] или Cisco IOS [Собственный компонент]). См. нижеследующую таблицу для получения сведений о версиях программы и маршрутизаторах многоуровневой коммутации (MSFC).

	Sup1 (с MSFC)		Sup2 (с MSFC)		Sup720	
Модуль	Cisco IOS	CatOS	Cisco IOS	CatOS	Cisco IOS	CatOS
FW	12.1 (13)	7.5 (1)	12	7.5 (1)	12	8.2 (1)

SM	E		.1 (13) E		.2 (14) SX1	
IDSM2	Не поддерживается	7.6 (1)	12.1 (19) E	7.6 (1)	12.2 (14) SX1	8.2 (1)
VPNSM	Не поддерживается	Не поддерживается	12.2 (14) SY	Не поддерживается	12.2 (17a) SX10	Не поддерживается

* Планируется реализовать поддержку.

Примечание: Дополнительные сведения о различиях между операционными системами CatOS (Hybrid) и Cisco IOS (Native) см. в разделе Сравнение операционных систем Cisco Catalyst и Cisco IOS для коммутаторов серии Cisco Catalyst 6500.

Вопрос. . Можно ли использовать в одной стойке FWSM, IDSM2 и VPNSM?

О. Да, можно выполнить эти модули в том же шасси, если коммутатор выполняет программное обеспечение интегрированного Cisco IOS с минимальным номером версии программного обеспечения Cisco IOS версии 12.2(14)SY (Sup2) или 12.2 (17a) SX10 (Sup720). В настоящее время отсутствуют версии операционной системы CatOS, которые поддерживают эти модули служб в одной и той же стойке 6500 или 7600.

Вопрос. . Какие настройки необходимо выполнить для FWSM?

О. Конфигурация и параметры управления включают их.

Параметр	Version	Описание
Центр управления для брандмауэров	Версии 1.1.1 и позже*	Это - интернетный интерфейс для настройки и управления множественными межсетевыми экранами. **Примечание:** Поддержка групп сервисов в рамках объектной группировки ограничена. Группы служб успешно анализируются, но тут же выравниваются. **Это влияет на команды с ключевыми словами**

		icmp-type, protocol и service. Это ограничение применимо к версии 1.3 и более ранним.
Центр контроля безопасности	Версии 1.2 и позже*	Это - интернетный интерфейс для мониторинга устройств Безопасности Cisco. Программное обеспечение централизует управление системным журналом от множественных устройств Безопасности Cisco с гибким созданием отчетов и предупреждением опций.
Центр контроля для производительности	Версии 2.0 и позже*	Это - интернетный интерфейс для мониторинга и устранения проблем состояния и производительности сервисов, которые способствуют сетевой безопасности. Протокол SNMP является используемым базовым протоколом.
PDM	Версия 2.1	Это - интернетный интерфейс для настройки, управления и мониторинга одиночного межсетевого экрана. PIX Device Manager (PDM) должен быть установлен локально на Межсетевом экране PIX.
Telnet	Н/Д	Telnet предоставляет удаленный доступ интерфейса командной строки (CLI) к межсетевому экрану. **Примечание:** Для разрешения доступа программы Telnet к интерфейсу с наименьшей защищенностью (общеизвестного в качестве внешнего интерфейса), необходимо настроить протокол IPsec для управления.
Secure Shell (SSH)	Н/Д	SSH предоставляет безопасный удаленный доступ CLI к межсетевому экрану.
SNMP	Н/Д	SNMP предоставляет метод мониторинга FWSM. **Примечание:** SNMP используется только для чтения на FWSM.
Системный журнал	Н/Д	Системный журнал предоставляет метод мониторинга FWSM.

* Эта программа является частью набора CiscoWorks VPN/Security Management Solution (VMS). Эта программа обеспечивает интегрированный подход к управлению безопасностью устройств Cisco через интерфейс браузера для сетей предприятия.

Вопрос. . Что такое SVI? Можно ли настроить несколько SVI?

О. SVI обозначает Коммутируемый виртуальный интерфейс. Он представляет собой логический интерфейс третьего уровня на коммутаторе. Для CatOS версии ниже 7.6(1) и Cisco IOS версии ниже 12.2(14)SY разрешен только один коммутируемый виртуальный интерфейс в качестве компонента брандмауэра сетей VLAN. Другими словами, только один интерфейс третьего уровня может быть настроен между FWSM и MSFC. Попытка настроить несколько SVI приведет к отображению в интерфейсе командной строки сообщения об ошибке.

Для CatOS версий не ниже 7.6(1) и для Cisco IOS версий не ниже 12.2(14)SY, FWSM поддерживает несколько SVI. По умолчанию поддерживается только один коммутируемый виртуальный интерфейс (SVI). Использование одной из нижеследующих команд разрешает поддержку на коммутаторе нескольких SVI.

- Для CatOS введите set firewall multiple-vlan-interfaces enable.Для Cisco IOS введите firewall multiple-vlan-interfaces.

Если коммутатор настраивается для нескольких FWSM VLAN и выдается сообщение об ошибке, указывающее на наличие более одного SVI, то необходимо проверить настройки коммутатора и (или) MSFC для того, чтобы убедиться в существовании только одного интерфейса третьего уровня (или интерфейса VLAN) в качестве части брандмауэра сетей VLAN.

Примечание: Только используйте один SVI. Это позволяет избежать сложной настройки, включающей наличия маршрутизацию на основе политик.

Вопрос. . FWSM поддерживает SNMPv3?

О. Нет.

Вопрос. . Какое количество VLAN может поддерживать FWSM?

О. Версия FWSM 1.1 поддерживает 100 VLAN, и версия FWSM 2.1 поддерживает 250 VLAN.

Вопрос. . Поддерживает ли FWSM команду access-list compiled?

О. Так как FWSM автоматически компилирует списки доступа в аппаратные средства после 10 секунд бездействия в CLI, нет никакой потребности в турбо списках доступа. FWSM версии 2.1 обеспечивает дополнительную функциональность назначения при трансляции списков управления доступом.

Вопрос. . Поддерживает ли FWSM выполнение команды auto-cost reference-bandwidth в IOS с помощью протокола OSPF?

О. Нет. FWSM не знает о физических портах, связанных с ним. Стоимость OSPF должна быть настроена вручную для каждого интерфейса с командой стоимости ospf.

Вопрос. . Может ли использоваться протокол OSPF в топологии, когда два различных интерфейса FWSM подключены к одной и той же сети?

О. Да. Эта возможность доступна в версии 2.1 и более поздних.

Вопрос. . Какие протоколы маршрутизации поддерживаются FWSM?

О. Протокол OSPF и Протокол RIP являются поддерживаемыми протоколами маршрутизации. Для получения дополнительной информации о FWSM обратитесь к документации, доступной на странице Cisco Catalyst 6500 Series Firewall Services Module.

Вопрос. . Поддерживается ли многоадресность (протокол IGMPv2 и маршрутизация с мультивещанием) на FWSM?

О. Да. Эта возможность доступна в FWSM версии 2.1 и более поздних. Если используется версия 1.1, то в качестве временной меры можно использовать GRE-туннелирование.

Вопрос. . Поддерживает ли FWSM фильтрацию URL-адресов?

О. Да. Функция Websense поддерживается начиная с версии 1.1, а в версии 2.1 добавлена дополнительная поддержка для N2H2.

Вопрос. . Почему фрагментированные пакеты отклоняются FWSM?

О. По умолчанию фрагментированные пакеты не могут пересечь FWSM. **Для настройки этой функции можно использовать команду fragment.** Это поведение отличается от соответствующего поведения для брандмауэра PIX. Протоколами, использующими фрагментированные пакеты, являются OSPF-протокол и NFS-протокол.

Вопрос. . Можно ли прерывать VPN-соединения на FWSM?

О. Функциональные возможности VPN не поддерживаются на FWSM. За прерывание VPN-соединений отвечают коммутатор и (или) модуль служб VPN. Лицензия 3DES предоставляется только для целей управления, например, для подключения к низкозащищенному интерфейсу через Telnet, Secure Shell (SSH) и Secure HTTP (HTTPS).

Вопрос. . Поддерживается ли на FWSM аутентификация, авторизация и ведение учета (AAA) для RADIUS или TACACS+?

О. AAA поддерживается и для управления FWSM и для трафика, проходящего через FWSM. Дополнительные сведения см. в документе под названием Документация по модулю служб брандмауэра.

FWSM обеспечивает функциональность сходную с функциональностью брандмауэра PIX, кроме загружаемых списков управления доступом и VPN. Помня об этом, можно использовать документацию по брандмауэру PIX в качестве руководства для настройки FWSM.

- Как провести аутентификацию и включение на межсетевом экране Cisco Secure PIX (версии с 5.2 до 6.2)
- Аутентификация, авторизация и учет пользователей с помощью PIX версии 5.2 и более поздних версий

Вопрос. . Как выполнить восстановление пароля для FWSM?

О. См. эти документы для получения информации о восстановлении пароля.

- Для версии 1.1(1) см. примечание по настройке 1.1(1) в документе под названием Изменение и восстановление паролей.
- Для версий 1.1(2) и 1.1(3) см. примечание по настройке 1.1(2) в документе под названием Изменение и восстановление паролей.

Вопрос. . Поддерживает ли FWSM работу с джамбо пакетами?

О. Да, FWSM может поддержать кадры большого размера.

Вопрос. . Как FWSM отвечает, когда он получает пакет со своим адресом источника, поскольку петля назад обращается?

О. Это рассматривает пакет как недопустимый и отбрасывает пакет. По умолчанию FWSM понижается, пакеты с недопустимым адресом источника, такие как петля назад обращаются, широковещательный адрес и адрес адресата. Сообщение журнала как показано в данном примере генерируется.

```
%FWSM-2-106016: Deny IP spoof from (IP_address) to
 IP_address on interface interface_name.
```

Вопрос. . Поддерживается ли PVLAN на FWSM?

О. Поддержка PVLAN начинается в версии программного обеспечения 3.1. Если версия программы ниже 3.1, то возможным единственным решением является подключение разнородного порта PVLAN с помощью кросс-кабеля к обычному порту доступа с последующей брандмауэрной защитой VLAN этого порта доступа.

Вопрос. . Поддерживаются ли номера строк списка доступа в FWSM?

О. Эта функция поддерживается только в версии программного обеспечения 3.1 и позже.

Вопрос. . Можно ли ограничить количество соединений, которые пользователь может иметь на FWSM?

О. Да, можно ограничить соединения с помощью Модульной Системы политик. Выполните эти шаги для ограничения количества соединений:

1. Создайте карту классов для соответствия с трафиком.
2. Разместите карту классов в карту политик и используйте ограничение соединения в карте политик.
3. Примените карту политик с помощью политики обслуживания.

См. Ограничения соединения Настройки и Таймауты для получения дополнительной информации и детализированные действия.

Вопрос. . Есть ли какие-либо ограничения в реализации групповой адресации в FWSM?

О. Да. FWSM не поддерживает 232. x. x. x подсеть как имя группы, поскольку это было уже

зарезервировано для модуля служб безопасности (SSM).

Вопрос. . Адресная трансляция позволена через FWSM?

O. Нет. В отличие от маршрутизатора, FWSM не позволяет адресную трансляцию через свои интерфейсы. Более подобный обходной путь должен использовать встроенную характеристику ретрансляции DHCP для передачи широковещательных сообщений от одного интерфейса до другого.

Вопрос. . Механизм Проверки HTTP может обнаружить нетрафик HTTP или нестандартный трафик в сеансе HTTP?

O. Да. Межсетевой экран Приложения с Усовершенствованной Проверкой HTTP может обнаружить и управлять ими трафик. См. Обзор Механизма Контроля приложения для получения дополнительной информации.

Вопрос. . Совместимы функции нормализации в ASA и FWSM?

O. В FWSM Нормализация TCP только применяется к трафику, который поражает комплекс TCP. На плоскость обычных данных (быстрый маршрут) трафик не влияют. Это отличается от ASA в том всем трафике ASA, подвергнут нормализатору.

На FWSM, если нормализатор отключен, модуль переключается на 2.3 поведения. Но при отключении **нормализатора tcp контрольной точки** это предотвращает строгие проверки TCP, такие как обнаружение несвоевременных сегментов и контролирующих параметров TCP, на пакетах TCP, полученных на Уровне управления для контроля Уровня 7 в FWSM, и не выполнено. Таким образом желательно не отключить его. FWSM не позволяет настраивать параметры карты tcp по умолчанию.

Вопрос. . Нам нужно к нормализатору TCP позволить/запретить?

O. Из-за неспособности передать некоторое соединение определенная информация от NP до уровня управления, нормализатор TCP возможно не функционирует должным образом все время в FWSM. Кроме того, уникальные карты tcp, привязанные к соединениям, не могут быть определены. Таким образом FWSM полагается на карту tcp по умолчанию, которые возможно не работают правильно для всех соединений. Из-за этих ограничений существует потребность к нормализатору TCP позволить/запретить в уровне управления для трафика, проходящего межсетевой экран. FWSM не позволяет настраивать параметры карты tcp по умолчанию.

Вопрос. . Каково максимальное число mfib записей, которые может поддержать FWSM?

O. Максимальное число записей является 5000 записей.

Вопрос. . Как я могу перехватить пакеты в FWSM?

O. Пакеты могут быть перехвачены в FWSM. Использование CLI как Захват пакета не поддерживается в ASDM, и команда **перехвата** не поддерживается в ASDM. См. Проигнорированные и Команды Только для представления для получения дополнительной

информации. См. Получение Пакетов для получения дополнительной информации о конфигурации Пакетного Получения в FWSM. См. ASA/PIX/FWSM: Пакетное Получение с помощью CLI и Примера конфигурации ASDM для получения дополнительной информации о примере конфигурации захвата пакета.

Вопрос. . Какую версию ASDM FWSM поддерживает?

О. См. FWSM и Совместимость Выпуска ASDM для получения дополнительной информации о FWSM и ASDM освобождают совместимость.

Лицензирование

Вопрос. . Имеется лицензия для FWSM, функционирующего в режиме параллельных соединений. Можно ли получить лицензию для резервного FWSM в случае выхода из строя аппаратного обеспечения?

О. Можно получить лицензию на запасной FWSM. Однако, необходимо в установленном порядке заказать лицензию для резервного FWSM. В случае выхода из строя аппаратного обеспечения, обратитесь в центр технической поддержки Cisco для устранения неполадок и получения лицензии для запасного FWSM. Для получения сведений о лицензировании см. документ под названием Программа модуля брандмауэра Cisco версии 2.2(1).

Вопрос. . FWSM поддерживает множественные совместно используемые интерфейсы?

О. FWSM не поддерживает множественные совместно используемые интерфейсы, но вместо этого у вас может быть одна VLAN через составные контексты. См. Совместное использование Ресурсов и Интерфейсов Между Контекстами для получения дополнительной информации.

Проблемы VLAN

Вопрос. . Как разместить дополнительные VLAN после FWSM?

О. Используйте **команду nameif**, если вы хотите добавить vlan 200 к конфигурации. Уровень безопасности должен быть между 0 и 100. Завершенный синтаксис команды **<имя интерфейса> <уровень безопасности> nameif vlan200**.

Вопрос. . Какое количество VLAN можно разместить после FWSM, использующего режим одиночной контекстной маршрутизации?

О. Можно разместить 1000 VLAN позади FWSM с помощью Одиночного Контекста, Режима маршрутизации.

Проблемы эхо-запроса

Вопрос. . Почему нельзя проверить соединение с FWSM на интерфейсе с

прямым подключением?

О. По умолчанию каждый интерфейс запрещает Протокол ICMP. **Чтобы разрешить отправку ICMP-пакетов на этот интерфейс, используйте команду icmp.** Это поведение отличается от соответствующего поведения для PIX.

Примечание: Если отправка ICMP-пакетов на интерфейс запрещена с помощью команды icmp, то в ARP-таблице будут, по-прежнему, отображаться корректные MAC-адреса. Если MAC-адреса не отображаются, то перейдите к следующему вопросу.

Вопрос. . Невозможно проверить соединение с FWSM на интерфейсе с прямым подключением и для этого интерфейса отсутствует запись в ARP-таблице. Коммутатор работает под управлением операционной системы CatOS. Какие действия следует предпринять?

О. Настройка интерфейсы в конфигурации FWSM (с командой nameif) или на Функциональной Карте Многоуровневого Коммутатора (MSFC) [с командой interface vlan], прежде чем они будут настроены на коммутаторе (на Модуле супервизора в CatOS) могут заставить интерфейсы появиться, как будто они не отвечают вообще без ответа Записи ARP или Протокола ICMP.

При настройке интерфейса на FWSM или MSFC, принадлежащих к брандмауэру сетей VLAN, перед настройкой коммутатора необходимо удалить запись для FWSM или MSFC, перезагрузить модуль, а затем повторно добавить запись.

Вопрос. . Почему нельзя проверить соединение с FWSM или передать через него какие-либо данные?

О. Технология NAT должна быть настроена с помощью nat 0, nat/глобального или статической команды для трафика для прохождения через FWSM от интерфейса с более высоким уровнем безопасности (внутренний интерфейс) к интерфейсу с более низким уровнем безопасности (внешний интерфейс).

Необходимо также использовать команду access-list для реализации списков управления доступом, которые разрешают прохождение трафика через FWSM. По умолчанию списки управления доступом запрещают весь трафик на все интерфейсы (deny ip any any). Это поведение отличается от конфигурации по умолчанию для PIX, который разрешает трафик по направлению от высокозащищенного к низкозащищенному интерфейсу и запрещает трафик по направлению от низкозащищенного к высокозащищенному интерфейсу. **Настройте список управления доступом с помощью команды permit ip any any и примените его к высокозащищенному интерфейсу, чтобы сделать поведение FWSM аналогичным поведению PIX.**

Вопрос. . Можно проверить соединение с интерфейсом FWSM, который напрямую подключен к сети, однако, нельзя проверить соединение с другими интерфейсами. Это нормальная ситуация?

О. Да. Это встроенный механизм защиты, который также существует в брандмауэре PIX.

Проблемы аварийного переключения

Вопрос. . Можно ли настроить восстановление после отказа между двумя FWSM, использующими различные версии программы?

О. Нет. Аварийное переключение требует, чтобы оба FWSM выполнили ту же версию кода. Во время восстановления после отказа проверяется версия программ узлов и если версии различаются, то восстановление невозможно. По этой причине необходимо обновить оба FWSM в одно и тоже время.

Вопрос. . Можно ли настроить восстановление после отказа между двумя FWSM в различных стойках?

О. Да. Однако, FWSM должны быть соединены с помощью средств второго уровня на всех интерфейсах. Другими словами, все интерфейсы должны иметь возможность обмениваться между собой широковещательными пакетами второго уровня [ARP и т.д.]. Пакеты протокола восстановления после отказа не могут маршрутизироваться на третьем уровне.

Вопрос. . Между двумя FWSM настроено восстановление после отказа, но они не синхронизируются. Какие проблемы могут возникнуть?

О. Гарантируйте, что ваша конфигурация встречает эти требования для успешного переключения при отказе.

- Оба FWSM должны работать с одной и той же версией программы.
- Оба FWSM должны иметь одной и то же число VLAN.
- На FWSM должно существовать соединение второго уровня между всеми VLAN. Если FWSM расположены в различных стойках и имеется магистраль, настроенная между ними, то необходимо проверить, что существуют все VLAN и они разрешены в магистрали.

Вопрос. . Я могу настроить аварийное переключение для трех или больше модулей FWSM, которые распространены по другому шасси коммутаторов?

О. Нет. Настройка аварийного переключения поддерживается только для пары FWSM, например, 2 модулей. Эти два модуля могут быть в том же коммутаторе или двух отдельных коммутаторах. При установке вторичного FWSM в том же коммутаторе как основной FWSM вы защищаете против сбоя уровня модуля. Для защиты против сбоя уровня модуля и а также сбоя уровня коммутатора, можно установить вторичный FWSM в отдельном коммутаторе. FWSM не координирует аварийное переключение непосредственно с коммутатором, но это работает гармонично с операцией аварийного переключения коммутатора. См. внутри - и Размещение Модуля Межшасси для получения дополнительной информации.

Прочее

Вопрос. . На FWSM есть надпись — "Не вытаскивайте плату, если горит зеленый светодиод, так как это может привести к повреждению диска". Что это

означает?

О. Модуль межсетевого экрана должен быть удален только после отключения питания с помощью одного из этих методов. Предпочтения для конкретного метода отсутствуют.)

- Используйте интерфейс командной строки (CLI) коммутатора и выполните одну из этих команд.CatOS - **модуль набора выключает** *mod*Программное обеспечение Cisco IOS - *никакой модульный слот* **power enable**
- **Нажмите кнопку shutdown на панели.**
- Физически выключите электропитание стойки маршрутизатора.

Когда световой индикатор состояния не является зеленым, можно удалить модуль безопасно.

Вопрос. . После использования команды show module, FWSM перешел в состояние "неисправен/другое". Какие действия следует предпринять?

О. См. этого чек-листа для устранения проблем FWSM со статусом /.

- Проверьте, что на коммутаторе используется поддерживаемая версия программы.
- Проверьте, что FWSM совместим с другими панелями, расположенными в той же самой стойке. Дополнительные сведения см. в Замечания к версии Catalyst 6500 и (или) Software Advisor (только для зарегистрированных пользователей).
- Если коммутатор работает под управлением программы CatOS/Hybrid, то необходимо сбросить настройки для разъема, занятого модулем FWSM. Используйте эти команды, чтобы сделать это.**Модуль набора** типа **выключает** *mod* для выключения FWSM.**Введите clear config mod для сброса параметров настройки коммутатора, связанного с этим разъемом, и включения электропитания модуля.**

Для получения дополнительных сведений см. следующую документацию.

- Контрольный список отказов оборудования для Catalyst 4000, 5000, и 6000 Series Switches под управлением CatOS
- Поиск неполадок оборудования и распространенные вопросы по коммутаторам Catalyst 6000, работающих под управлением операционной системы Cisco IOS

Если проблемы не устранены, то необходимо обратиться в центр технической поддержки компании Cisco за дополнительной помощью.

Вопрос. . Где можно найти документацию по FWSM?

О. Комментарии к выпуску для FWSM могут быть найдены в соответствии с Комментариями к выпуску Серии Catalyst 6500. Для получения дополнительной информации обратитесь к документации, доступной на странице Cisco Catalyst 6500 Series Firewall Services Module.

Вопрос. . Где можно найти сведения о сообщениях об ошибках, относящихся к FWSM?

О. Декодер сообщений об ошибках (только зарегистрированные клиенты) предоставляет подробную информацию о многих сообщениях об ошибках FWSM. Документация по системным сообщениям также содержит полезные сведения. Если необходима дальнейшая

помощь, то следует обратиться в центр технической поддержки Cisco.

Вопрос. . Где можно найти сведения о существующих дефектах для FWSM?

О. Подробные данные о существующих дефектах могут быть найдены в Bug Toolkit (только зарегистрированные клиенты).

Вопрос. . В чем разница между брандмауэром PIX и модулем служб брандмауэра?

О. PIX и FWSM основываются на подобном коде. Однако, существует два фундаментальных отличия. PIX поддерживает функциональность VPN и IDS. FWSM не поддерживает функциональность VPN и IDS, так как эти функции реализованы в других линейных платах. Дополнительные сведения о модуле служб IDSM-2 для Catalyst 6500 см. в документе под названием Модуль служб IDSM-2 для Catalyst 6500. Дополнительные сведения о модуле служб IPsec VPN для Catalyst 6500 см. в документе под названием Модуль служб IPsec VPN для Catalyst 6500.

В следующей документации приводятся сведения о незначительных различиях между PIX и FWSM:

- Техническая документация по брандмауэру PIX
- Замечания к версии PIX
- Справочник по командам PIX
- Техническая документация по FWSM
- Примечания к версии FWSM
- Справочник по командам FWSM

Вопрос. . На FWSM для каждого интерфейса невозможно выполнить команды множественного группового доступа. FWSM работает только с одной группой доступа для каждого интерфейса. В чем причина?

О. При выдаче этих команд в FWSM только последняя **команда access-group** появляется:

```
access-group allow_icmp in interface outside
access-group allow_caltech in interface outside
```

Это происходит только из-за того, что FWSM допускает только один список доступа для каждого интерфейса на одно направление.

Вопрос. . Какая информация хранится в записях xlate в FWSM?

О. Записи Xlate хранят эту информацию:

1. **Source Interface** — Это - интерфейс, что пакет получен, например, `outside`.
2. **IP - адрес источника** — Это - IP - адрес источника пакета.
3. **Преобразованный IP-адрес** — В случае никаких Выражений NAT, преобразованного IP-адреса и IP - адреса источника является тем же.
4. **Интерфейс назначения** — интерфейс, который пакет оставляет на основе обращения к таблице маршрутизации IP - адреса назначения пакета.

Вопрос. . Что делает значения и статистика в `perfmon` на FWSM подразумевают?

О. Используйте **команду show perfmon** для получения информации о производительности FWSM.

```
FWSM#show perfmon FWSM#show console-output Context: my_context PERFMON STATS: Current Average
Xlates 0/s 0/s Connections 0/s 0/s TCP Conns 0/s 0/s UDP Conns 0/s 0/s URL Access 0/s 0/s URL
Server Req 0/s 0/s WebSns Req 0/s 0/s TCP Fixup 0/s 0/s TCP Intercept 0/s 0/s HTTP Fixup 0/s 0/s
FTP Fixup 0/s 0/s AAA Authen 0/s 0/s AAA Author 0/s 0/s AAA Account 0/s 0/s
```

Столбец `Current` показывает статистику в текущем интервале, где, поскольку последний столбец `Average` показывает кумулятивное среднее число начиная с прошлый раз, статистика была очищена. Это показывают как `/s`, потому что это - скорость, а не абсолютное значение.

Статистические данные, показанные в выходных данных команды, обновлены в интервале 120 секунд по умолчанию. Интервал может быть изменен с **командой perfmon interval**.

```
FWSM#perfmon interval 20
```

Это означает, что скорость статистики, о которой сообщают в столбце `Current`, вычисляется каждые 20 секунд. Кроме того, каждый раз, когда вы вводите **команду show perfmon**, скорости вычислены со статистикой в том моменте времени.

FWSM не включает последовательный консольный порт, но некоторые сообщения только отображены на консольном порте, который включает выходные данные от **команд покажите perfmon и perfmon**. Используйте **команду show output-console** для просмотра буфера консоли, который включает выходные данные **команды show perfmon**.

Вопрос. . Будет падение производительности на FWSM ни с `servicemodule` команда?

О. Сессия SPAN требуется на FWSM из-за аппаратного ограничения ASIC для репликации трафика. FWSM нужен ASIC для репликации пакетов, и сессия SPAN передает пакеты для коммутации для того использования сессии SPAN. Трафик, на который влияет эта команда, является Распределенным EtherChannel, Групповой адресацией и GRE. Рекомендуется настроить сессию SPAN а не удалить его.

Если по некоторым причинам необходимо удалить его, удостоверьтесь, что у вас нет реплицированного трафика природы, например, Распределенного EtherChannel, на который может влиять Уведомление о дефекте: FN - 61935 - Серия Catalyst 6500 и Несовместимость Сервисного модуля серии 7600 С Распределенным EtherChannel и Пакетной Рециркуляцией.

Вопрос. . Можно ли увеличить память для хранения большего количества Списков контроля доступа (ACL)?

О. Память, выделенная для ACL в FWSM, ограничена. См. Спецификации - Пределы Правила для получения дополнительной информации о выделении ресурсов FWSM.

Когда память, выделенная для ACL в контексте, превышена, можно получить любое из этих сообщений об ошибках:

- : , config access-list
- :
- Unable to add a hole to Policy Rule

Некоторые списки доступа используют большую память, чем другие. Это зависит от типа списка доступа, и фактический предел, который может поддержать система, является меньше, чем максимум. Соответствие между правилами и выделением памяти не является взаимно однозначным. Это фактически зависит от правила и как это запрограммировано в аппаратных средствах.

У вас есть две опции для оптимизации первоклассного использования памяти:

- Суммируйте и упростите свои первоклассные записи — это может быть сделано при завершении этих рекомендованных правил эксплуатации:Используйте непрерывные адреса узлов, когда это возможно. Составные операторы host в ACE/object-group в сети.Используйте any вместо сетей и сетей вместо хостов, если это возможно.Попробуйте упростить группы объектов. Это может сэкономить сотни записей ACE при развертывании списков управления доступом. Пример должен группироваться операторы отдельного порта в диапазон.
- Повторно разделите память, выделенную для ACE на каждом разделении. Это требует перезагрузки модуля FWSM.FWSM в основном делит память, выделенную для ACE в 12 отделений, и выделяет соответствующую память для каждого. Это делается автоматически. От версии 2.3 (2) и позже, можно использовать менеджера ресурсов для перераспределения памяти, которая зависит от количества контекстов, которые вы имеете.Выполните **команду show context count** для проверки, сколько контекстов вы имеете. Можно тогда проверить это с конфигурацией. Затем найдите количество отделений, которые используют **команду show resource acl-partition**. Если у вас есть больше отделений, чем ваш определенный контекст, то можно совпасть с количеством отделений к количеству контекста с командой *номера отделений* **разделения acl ресурса**.Необходимо сохранить конфигурацию и перезагрузить FWSM после этого. Предыдущая команда дает вам большую память для ACE, является ли это достаточно или не снова зависит от ACE, который вы добавляете к контексту.**Внимание. :** Один недостаток предыдущего пересопоставления - то, что, если вы хотите добавить другой контекст, тогда необходимо перераспределить память, сопоставляющую снова. Это вызывает меньше памяти, доступной каждому контексту, и может сломать текущие первоклассные определения. Память на FWSM, выделенном, является ограниченной суммой, и это вырезает его соответственно на предопределенном способе или через ручное выделение ресурсов, как упомянуто ранее.

От версии 4.0 и далее, FWSM представил функцию, названную "оптимизацией ACL", которая эффективно использует ресурсы памяти для хранения множественных записей ACL. Это имеет дело со встроенным алгоритмом, который автоматически объединяет записи ACL по мере возможности, не пропуская эффективность никакой записи ACL. Этот алгоритм объединяется непрерывные подсети, упомянутые в других записях ACL в отдельного оператора, и обнаруживает наложения в диапазонах портов. Эта опция активирована при помощи команды и, после того, как оптимизация выполнена, завершенная конфигурация списков управления доступом (ACL) смотрит по-другому от предыдущей (исходной) конфигурации списков управления доступом (ACL). Эта организованная конфигурация списков управления доступом (ACL) могла быть сохранена после того, как проверка и оптимизация могли быть отключены для сохранения ЦП вычислительная перегрузка. Для получения дополнительной информации об этой функции обратитесь к разделу Оптимизации Access List Group, который описывает функциональность

оптимизации ACL наряду с ее элементами конфигурации.

Версия 4.0 также представила другую функцию, вызванную "Емкость Списка доступа Increasaed". С этой функцией у пользователей теперь есть емкость сохранить 130,000 записей ACL в режиме одиночного контекста и 150,000 записей в режиме мультиконтекста. Для получения дополнительной информации об этой функции обратитесь к "Увеличенному разделу" Емкости Списка доступа в бюллетене Версии 4.0 Программного обеспечения модуля Сервисов межсетевого экрана Cisco.

Вопрос. . Почему перехват дает команду, когда применено к, чтобы FWSM остановил и не перехватывал трафик, как только другая команда перехвата применена на интерфейс?

O. То, когда вы настраиваете перехват 'z' на том же интерфейсе, где перехват 'x' уже применен, затем перехватите 'z', заменяет перехват 'x'. Активный перехват является последним, подключенным к определенному интерфейсу.

Когда access-list на перехвате 'x' накладывается на access-list перехвата 'z', единственное исключение. Если это так, тогда оба перехвата продолжают перехватывать трафик где наложение access-lists.

Вопрос. . Как я могу решить ошибку `NP-PCcmplx` на FWSM?

O. Повторно загрузите модуль FWSM для решения этой ошибки.

Вопрос. . Как я могу настроить FWSM для использования перехвата TCP для защиты от определенных типов атак SYN flood?

O. Можно настроить FWSM для использования перехвата TCP для защиты от определенных типов атак SYN flood. См. перехват TCP FWSM и cookie SYN, объясненные для получения дополнительной информации.

Вопрос. . Были бы какие-либо проблемы производительности для обработки пакетов IPv6?

O. Да. Вы видите проблемы производительности при передаче трафика IPv6, поскольку пакет должен быть обработан ЦП. Из-за различий в обработке трафика IPv4 и трафика IPv6 ЦП, пакетная обработка IPv6 вызовет определенные проблемы производительности с FWSM.

Вопрос. . Как я могу препятствовать тому, чтобы FWSM ответил на удаленный сервер с его собственным MAC-адресом?

O. Необходимо отключить proxyarp опцию на заданном интерфейсе с этой командой:

```
"sysopt noproxyarp <interface>"
```

Для получения дополнительной информации о proxyarp функции обратитесь к Справочнику по командам FWSM.

Вопрос. . Как я могу предотвратить вызовы через FWSM от того, чтобы быть отброшенным?

O. Для решения этой проблемы отключите контроль для H323 и H225:

```
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
```

Вопрос. . Как я могу решить вопросы преобразования NAT o FWSM?

O. Для решения этой проблемы используйте **команду xlate-bypass**. По умолчанию, даже если вы не используете NAT, FWSM создает сеансы NAT для всех соединений. Можно отключить сеансы NAT для непреобразованного трафика, который называют обходом xlate, во избежание максимального предела сеанса NAT. **Команда xlate-bypass** может быть настроена как показано:

```
hostname(config)#xlate-bypass
```

См. Обход Xlate Настройки, для получения дополнительной информации о как к конфигурации обхода xlate.

Дополнительные сведения

- Пример базовой конфигурации FWSM
- Документация модуля сервисов межсетевого экрана
- Страница технической поддержки продукта модуля сервисов межсетевого экрана
- Cisco Systems – техническая поддержка и документация