

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Чек-лист аварийного переключения](#)

[Проверьте интерфейсы](#)

[Лицензии](#)

[Режим контекста](#)

[Требования к программному обеспечению](#)

[Минимальная конфигурация FWSM для перехвата управления при отказе с синхронизацией состояния](#)

[Минимальная конфигурация коммутатора](#)

[Устранение неисправностей](#)

[Несоответствие версии](#)

[Несовместимые лицензии](#)

[Другие Режимы \(одиночный по сравнению с составным контекстом\)](#)

[Два FWSM становятся активными](#)

[Несогласованность VLAN](#)

[Аварийное переключение Отключено](#)

[Дополнительные сведения](#)

Введение

Этот документ объясняет процедуры, которые можно использовать для решения проблем с Модулем Сервиса межсетевого экрана (FWSM) конфигурация аварийного переключения.

Этот документ также предоставляет чек-листа общих процедур для попытки, прежде чем вы начнете устранять неполадки соединения в режиме обхода отказа.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на FWSM 2.3 и позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

Общие сведения

Функция аварийного переключения позволяет резервному FWSM принимать функциональность отказавшего FWSM. Эти два включенные FWSM должны иметь того же майора (первый номер) и незначительный (второй номер) версия программного обеспечения, лицензия и рабочие режимы (маршрутизированный или прозрачный, одиночный или составной контекст). В то время как резервный модуль перемещается в активное состояние, когда активный модуль отказывает, изменения состояния к резерву. При аварийном переключении предыдущая информация о соединении доступна для нового активного модуля.

Для дополнительных сведений обратитесь к разделу [Аварийного переключения Настройки](#) Использования Аварийного переключения.

Чек-лист аварийного переключения

Этот чек-лист помогает вам успешно настраивать аварийное переключение в FWSM:

- [Проверьте интерфейсы](#)
- [Лицензии](#)
- [Режим контекста](#)
- [Требования к программному обеспечению](#)
- [Минимальная конфигурация FWSM для перехвата управления при отказе с синхронизацией состояния](#)
- [Минимальная конфигурация коммутатора](#)

Проверьте интерфейсы

Проверьте, что все интерфейсы на FWSM имеют настроенный резервный IP - адрес. Если вы поэтому уже не сделали, настройте активное и резервные IP - адреса для каждого интерфейса (режим маршрутизации), или для адреса управления (прозрачный режим). Резервный IP - адрес используется на FWSM, который в настоящее время является резервным модулем. Он должен находиться в той же подсети, что активный IP-адрес.

Это - пример конфигурации:

Примечание: Не настраивайте IP-адрес для канала аварийного переключения или для ссылки состояния (если вы переходите к Перехвату управления при отказе с синхронизацией состояния использования).

Примечание: Не требуется указывать маску подсети для пассивного адреса. IP-адрес и MAC-адрес соединения не меняются при аварийном переключении. Активный адрес IP для канала аварийного переключения всегда остается присвоенным основному модулю, в то время как пассивный адрес IP всегда останется присвоенным вспомогательному модулю.

[Лицензии](#)

Оба активных и резервных устройства должны иметь ту же лицензию.

[Режим контекста](#)

Если первичный модуль находится в одиночном режиме контекста, вспомогательный модуль должен также быть в одиночном режиме контекста и в том же режиме межсетевого экрана как первичный модуль.

Если первичный модуль находится в многоконтекстном режиме, вспомогательный модуль должен также быть в многоконтекстном режиме. Вы не должны настраивать режим межсетевого экрана контекстов безопасности на вспомогательном модуле, потому что аварийное переключение и ссылки состояния находятся в системном контексте. Вспомогательный модуль получает конфигурацию контекста безопасности из первичного модуля.

Примечание: не становится реплицированным во вспомогательный модуль.

Примечание: Групповая адресация не поддерживается в многоконтекстном режиме устройства безопасности. См. [Неподдерживаемые характеристики](#) разделяют для получения дополнительной информации.

[Требования к программному обеспечению](#)

Эти два модуля в конфигурации аварийного переключения должны иметь того же майора (первый номер) и незначительный (второй номер) версия программного обеспечения. Однако можно использовать другие версии программного обеспечения во время процесса обновления. Например, можно обновить один модуль от Версии 3.1 (1) до Версии 3.1 (2) и иметь аварийное переключение, остаются активными. Cisco рекомендует обновить оба модуля к той же версии для обеспечения долгосрочной совместимости.

[Минимальная конфигурация FWSM для перехвата управления при отказе с синхронизацией состояния](#)

Основной FWSM

Вторичный FWSM

Для получения дополнительной информации о том, как настроить Активное и Резервное аварийное переключение, обратитесь к [Настройке Активное/Резервное Аварийное переключение](#).

[Минимальная конфигурация коммутатора](#)

- VLAN, передаваемые основному FWSM Catalyst, который содержит основного, должны совпасть с VLAN, передаваемыми вторичному FWSM Catalyst, который содержит вторичное устройство. (Выходные данные команды `show run | i firewall` должны быть идентичными.)

Основное шасси
`cat6k-7(config)#do sh run | i fire` firewall
multiple-vlan-interfacesfirewall module 9 vlan-group 1firewall vlan-group 1 3,4,100-

Вторичное шасси
`cat6k-7(config)#do sh run | i fire` firewall multiple-
vlan-interfacesfirewall module 9 vlan-group 1firewall vlan-group 1 3,4,100-106

- Все VLAN, которые передаются, должны присутствовать в Базе данных VLAN и быть активными. Для выполнения этого выполните эти команды на коммутаторе в режиме конфигурации: `vlan 10no shut` Чтобы проверить, находятся ли VLAN в базе данных и активны, выходные данные команды `show vlan` и на шасси должны содержать VLAN, передаваемые FWSM, и показать как активные. Ниже показан пример выходных данных:

Основное шасси
`cat6k-7(config)#do sh vlan`

Status	Ports	VLAN Name			
active	3	VLAN0003	active	Fa4/474	VLAN0004
active	Fa4/48				

Вторичное шасси
`cat6k-7(config)#do sh vlan`

Status	Ports	VLAN Name			
active	3	VLAN0003	active	Fa4/474	VLAN0004
active	Fa4/48				

- Удостоверьтесь, что эти два FWSM имеют подключение Layer2 в каждой VLAN (они должны быть в той же подсети). **Прозрачные требования межсетевого экрана:** Во избежание петель при использовании аварийного переключения в прозрачном режиме необходимо использовать программное обеспечение коммутатора, которое поддерживает передачу Блока данных протокола моста (BPDU). Кроме того, необходимо настроить FWSM для разрешения BPDU. Для разрешения BPDU через FWSM настройте EtherType? ACL и применяет его к обоим интерфейсам. **Примечание:** В противоположность PIX и платформе ASA, аппаратные средства двух блейдов FWSM всегда являются тем же, нет никаких других моделей или конфигураций памяти.

Устранение неисправностей

Когда FWSM перезагрузится, сценарии, объясненные в этом разделе, заставят аварийное переключение быть отключенным.

FWSM может перезагрузиться по причинам, таким как катастрофический отказ, перезагрузить от шасси, повторная загрузка, выполненная от CLI FWSM, или это может просто быть новый модуль, который вставлен или переустановлен в другой слот или привел резервное копирование в действие от шасси.

Несоответствие версии

Эти два модуля в конфигурации аварийного переключения должны иметь того же майора (первый номер) и незначительный (второй номер) версия программного обеспечения.

Связанное сообщение системного журнала: [105040](#)

Несовместимые лицензии

Вы могли бы получить этот системный журнал из-за несовместимой лицензии:

```

cat6k-7(config)#do sh vlan
VLAN Name              Status Ports
-----1              default
VLAN0003              active Fa4/474 VLAN0004
Fa4/48                active

```

Связанные сообщения системного журнала: [105045](#) и [105001](#)

Другие Режимы (одиночный по сравнению с составным контекстом)

И основной и вторичный FWSM должен быть в том же режиме (одиночный или множественен). Например, если основной будет настроен как один режим и вторичное устройство как составной режим, и вторичное устройство повторно загружено, то оба модули выключат аварийное переключение.

Основной в одном режиме:

```

cat6k-7(config)#do sh vlan
VLAN Name              Status Ports
-----1              default
VLAN0003              active Fa4/474 VLAN0004
Fa4/48                active

```

Вторичный в составном режиме (этот блейд повторно загружен):

```

cat6k-7(config)#do sh vlan
VLAN Name              Status Ports
-----1              default
VLAN0003              active Fa4/474 VLAN0004
Fa4/48                active

```

Основной в составном режиме:

```

cat6k-7(config)#do sh vlan
VLAN Name              Status Ports
-----1              default
VLAN0003              active Fa4/474 VLAN0004
Fa4/48                active

```

Связанные сообщения системного журнала: [105044](#), [103001](#), [105001](#)

Два FWSM становятся активными

Когда вы видите это сообщение об ошибках в журнале:

```

cat6k-7(config)#do sh vlan
VLAN Name              Status Ports
-----1              default
VLAN0003              active Fa4/474 VLAN0004
Fa4/48                active

```

Причина для этой ошибки состоит в том, потому что рекомендуемое число port-channel в коммутаторе превысило максимум (128, максимально в программном обеспечении Cisco IOS release 12.2 (33) SXH4 на Cat6000/6500). Поэтому предел Interface Descriptor Block (IDB) исчерпывается.

Из-за этого вы могли бы закончить с этими двумя проблемами:

- Когда у вас есть два коммутатора с модулями FWSM каждый для действия как активные и резервные, два модуля FWSM становятся активными в то же время.
- Вы не можете создать дополнительный port-channel.

Как часть решения вопроса, удалите port-channel, которые не необходимы и повторно загружают FWSM.

Несоответствие VLAN

Проблема

FWSM получает это сообщение об ошибках: 'Обнаруженный Активный Разъем' 'Несоответствие Vlan configuration' 'аварийное переключение будет отключен'.

Или

Конфигурация модулей сервиса межсетевого экрана и соответствующей конфигурации коммутатора, кажется, завершена. Однако FWSM неспособны синхронизировать друг друга. Это сообщение получено на вторичном хосте:

```
cat6k-7(config)#do sh vlan
VLAN Name                Status      Ports-----
-----1      default                active      3
VLAN0003                active      Fa4/474    VLAN0004    active
Fa4/48
```

Или

Выходные данные команды **show failover** показывают, что статусом аварийного переключения на вторичном модуле является OFF, состояние аварийного переключения FWSM в Failover Off (pseudo-Standby).

```
FWSM-secondary(config)#show failover
Failover Off (pseudo-Standby)
```

Решение

Проблемой могло бы быть назначение VLAN несоответствия через межсетевой экран (FWSM и супервизоры). Например, в группе VLAN Межсетевого экрана 1 оператор, то же количество VLAN, назначенных на каждом коммутаторе на межсетевой экран, может варьироваться. Это могло бы вызвать проблему. Если вы назначите то же количество VLAN в межсетевом экране, то аварийное переключение будет работать.

Во избежание получения ошибки несоответствия конфигурации VLAN выходные данные команды **show vlan** должны быть идентичными на обоих FWSM. Когда вы модифицируете или загружаете конфигурацию аварийного переключения на FWSM, это сообщение об ошибках только происходит. Например, когда FWSM загружается, он загружает startup-config из флэш-памяти и пытается инициализировать аварийное переключение. В это время это проверяет, чтобы удостовериться, что оба модуля получают корректные VLAN. Если VLAN не совпадают, сообщение об ошибках отображено, и аварийное переключение остается отключенным.

Примечание: Для аварийного переключения для работы FWSM требует одинаковых конфигураций и назначений порта. Возможно сделать аварийное переключение межшасси, но каждая VLAN, назначенная на межсетевой экран, должна быть в транке между двумя шасси.

FWSM не включает внешних физических интерфейсов. Вместо этого это использует интерфейсы виртуальной локальной сети (VLAN). Присвоение VLAN к FWSM подобно присвоению VLAN к порту коммутатора. FWSM включает внутренний интерфейс в Модуль матрицы коммутации (если есть) или общую шину. Для получения дополнительной информации обратитесь к [Присвоению VLAN к Модулю Сервисов межсетевого экрана](#).

Знайте, что сопоставление VLAN может модифицироваться во время рабочей настройки FWSM и откажет во время следующей начальной загрузки.

[Аварийное переключение Отключено](#)

При отключении аварийного переключения с помощью команды [no failover](#) текущее состояние модуля поддержано (или активный или резервный), пока не повторно загружен модуль. Это используется только для отключения аварийного переключения. Для изменения состояния модуля от активного до резерва или наоборот, необходимо использовать команду [\[no\] failover active](#).

[Дополнительные сведения](#)

- [FWSM : Аварийное переключение Настройки](#)
- [FWSM : Системные сообщения](#)
- [Cisco Systems – техническая поддержка и документация](#)