Содержание

Введение

Для конфигурации аварийного переключения необходимы два одинаковых устройства безопасности, соединенные друг с другом с помощью выделенного соединения аварийного переключения или соединения аварийного переключения с отслеживанием состояния. Состояние активных интерфейсов и узлов отслеживается до возникновения условий, отвечающих специфическим заданным параметрам аварийного переключения на другой ресурс. При возникновении условий, соответствующих заданным, происходит аварийное переключение на другой ресурс.

Устройство безопасности поддерживает две конфигурации аварийного переключения.

- Аварийное переключение между активными модулями
- Аварийное переключение между активными и резервными модулями

В каждой конфигурации аварийного переключения используется отдельный способ определения и выполнения аварийного переключения на другой ресурс. При конфигурации аварийного переключения на активный резервный ресурс оба модуля могут пропускать сетевой трафик. Это позволяет использовать выравнивание нагрузки в сети. Конфигурация аварийного переключения на активный резервный ресурс доступна только для модулей, работающих в многоконтекстном режиме. При конфигурации аварийного переключения на резервный ресурс в режиме ожидания сетевой трафик пропускается только одним узлом, в то время как другой находится в режиме ожидания. Конфигурация аварийного переключения на резервный ресурс в режиме ожидания доступна для узлов, работающих как в одноконтекстном, так и в многоконтекстном режиме. Обе конфигурации поддерживают аварийное переключение с отслеживанием состояния и без отслеживания состояния (регулярное).

Прозрачный межсетевой экран — это межсетевой экран уровня 2, который действует как *удар в проводе* или *невидимый межсетевой экран*, он не определяется подключенными устройствами как транзитный участок. Устройство защиты подключается к одной и той же сети на своих внутренних и внешних портах. Так как межсетевой экран не является маршрутизируемым переходом, можно с легкостью встроить прозрачный межсетевой экран в сеть, не прибегая к изменению IP-адресации. Устройство адаптивной защиты может быть настроено для работы в режиме маршрутизируемого межсетевого экрана по умолчанию или в режиме прозрачного межсетевого экрана. При смене режимов устройство адаптивной защиты очищает конфигурацию, так как многие команды поддерживаются только в одном из режимов. Если заполненная конфигурация уже имеется, сохраните ее перед тем, как изменить режим; сохраненную конфигурацию можно использовать для справки при создании новой конфигурации. Для получения подробной информации см. документ Пример конфигурации межсетевого экрана в прозрачном режиме.

В документе описывается настройка конфигурации аварийного перехода на пассивный резервный ресурс в прозрачном режиме для устройствах безопасности ASA Security Appliance.

Примечание. Функция аварийного переключения для VPN-соединений не поддерживается на модулях, работающих в многоконтекстном режиме. Функция аварийного переключения для VPN-соединений доступна только для конфигураций **Active/Standby Failover (Аварийное переключение на резервный ресурс в режиме ожидания)**.

Cisco рекомендует использовать интерфейс управления для аварийного переключения, особенно если используется аварийное переключение с отслеживанием состояния, при котором устройство безопасности постоянно отправляет данные о подключении с одного устройства в другое. Интерфейс для аварийного переключения должен иметь как минимум такую же полосу пропускания, как интерфейсы для передачи обычного трафика, и хотя в ASA 5540 используются интерфейсы Gigabit Ethernet, в качестве интерфейса управления применяется только FastEthernet. Интерфейс управления разработан только для передачи трафика управления и обозначается как management0/0. Однако можно использовать команду **management-only**, чтобы перестроить любой в интерфейс только для управления. Кроме того, для интерфейса Management 0/0 можно отключить режим«только для управления». В результате интерфейс будет передавать трафик как любой другой интерфейс. Для получения подробной информации о команде **management-only** см. документ Справочное руководство по командам системы безопасности Cisco, версия 8.0.

В этом руководстве приведен пример конфигурации, дающий краткие сведения о технологии PIX/ASA 7.x Active/Standby. См. подробное описание принципа работы этой технологии в документе Справочное руководство по командам ASA/PIX.

Предварительные условия

Требования

Требования к оборудованию

Два узла в конфигурации аварийного переключения на другой ресурс при сбое должны обладать одинаковой аппаратной конфигурацией. Они должны быть одной модели, иметь одинаковые номера и типы интерфейсов, а также одинаковые объемы ОЗУ.

Примечание. Не обязательно, чтобы у двух узлов был одинаковый объем флэш-памяти. При использовании узлов с разными объемами флэш-памяти в конфигурации перехода на другой ресурс при сбое убедитесь, что узел с меньшим объемом флэш-памяти обладает достаточным ее объемом для размещения файлов образов программ и файлов конфигурации. Если памяти все же недостаточно, синхронизацию с другим узлом большего объема флэш-памяти выполнить не удастся.

Требования к программному обеспечению

Оба модуля в конфигурации аварийного переключения должны находиться в рабочих режимах (маршрутизируемый или прозрачный, один или несколько контекстов). У них должны быть одинаковые основной (первый) и дополнительный (второй) номера версии ПО, однако можно использовать различные версии ПО в процессе обновления; например, можно обновить один узел от версии 7.0(1) до версии 7.0(2) и при этом использовать активный режим перехода на резервный ресурс. Cisco рекомендует обновить оба модуля до

одинаковой версии, чтобы гарантировать долгосрочную совместимость.

Для получения подробной информации об обновлении ПО для пары аварийного переключения см. раздел Модернизация без простоев для пар аварийного переключения документа *Руководство Cisco по настройке безопасности в командной строке, версия 8.0.*

Требования к лицензии

На платформе устройств безопасности ASA хотя бы один модуль должен иметь **неограниченную (UR) лицензию**.

Примечание. Для получения дополнительных возможностей может потребоваться обновление лицензий пары аварийного переключения. Для получения подробной информации см. документ Обновление ключа лицензий пары аварийного переключения.

Примечание. Лицензируемые функции (такие как одноранговые узлы SSL VPN или контексты безопасности) на обоих устройствах безопасности, участвующих в аварийном переключении, должны быть идентичны.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения и оборудования.

- Устройство защиты ASA с версией 7.x и более поздней

Сведения для данного документа были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только устройства с«пустой» (стандартной) конфигурацией. При работе с реально функционирующей сетью необходимо полностью осознавать возможные результаты использования всех команд.

Родственные продукты

Эта конфигурация может также использоваться со следующими версиями программного/аппаратного обеспечения.

- Устройство защиты PIX Security Appliance версии 7.x или более поздней

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в статье Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Аварийное переключение между активными и резервными модулями

Раздел посвящен описанию конфигурации аварийного перехода на резервный ресурс в режиме ожидания. В разделе рассматриваются следующие темы.

- Обзор аварийного переключения между активными и резервными модулями
- Состояние«основной-вспомогательный» и«активный-резервный»
- Инициализация устройства и синхронизация конфигурации
- Репликация команд
- Триггеры аварийного переключения
- Действия аварийного переключения

Обзор аварийного переключения между активными и резервными модулями

Аварийное переключение с активного на резервный ресурс позволяет передать функции отказавшего модуля устройству защиты, находящемуся в ждущем режиме. Оказавший активный модуль переходит в ждущий режим, а модуль, находившийся в ждущем режиме, переходит в активный режим. Устройство, которое становится активным, перехватывает IP-адреса (или IP-адрес управления для прозрачного сетевого экрана) и MAC-адреса отказавшего модуля и начинает передавать трафик. Устройство, которое переходит в резервное состояние, берет IP-адреса и MAC-адреса бывшего резервного модуля. Поскольку сетевые устройства не видят изменения пар MAC- и IP-адресов, записи ARP в сети не меняются и не устаревают.

Примечание. В режиме с несколькими контекстами устройство безопасности может выполнить полное аварийное переключение модуля (со всеми контекстами), но не для отдельных контекстов.

Состояние«основной-вспомогательный» и«активный-резервный»

Главное различие между модулями в паре аварийного переключения связано с тем, какой из них находится в активном состоянии, а какой в резервном. А точнее, какие IP-адреса используются и какой модуль активно передает трафик.

Некоторые различия связаны с тем, является ли модуль основным (как определено в конфигурации) или вспомогательным.

- Основной модуль всегда становится активным, если оба модуля запускаются одновременно (и оба находятся в исправном состоянии).
- MAC-адреса основного модуля всегда связаны с активными IP-адресами. Исключение из этого правила имеет место, когда вспомогательный модуль активен и не может получить основной MAC-адрес через соединение аварийного переключения. В этом случае используется вспомогательный адрес MAC.

Инициализация устройства и синхронизация конфигурации

Синхронизация конфигурации выполняется при загрузке обоих устройств в паре аварийного переключения. Репликация конфигурации происходит только от активного модуля к модулю в режиме ожидания. Когда резервный модуль выполняет процедуры начального запуска, он удаляет свою рабочую конфигурацию (за исключением команд, необходимых для взаимодействия с активным модулем), и активный модуль передает полную конфигурацию резервному модулю.

Активный модуль определяется по следующим критериям.

- Если модуль загружается и обнаруживает исправный активный модуль, он становится резервным.
- Если вспомогательный модуль загружается и не обнаруживает одноранговый модуль, он становится активным.
- Если модули загружаются одновременно, основной модуль становится активным, а вспомогательный — резервным.

Примечание. Если вспомогательный модуль загружается и не обнаруживает основной модуль, он становится активным. Он использует свои MAC-адреса для активных IP-адресов. Когда основной модуль становится недоступным, вспомогательный модуль изменяет свои MAC-адреса на адреса основного модуля, что может привести к прерыванию потока сетевого трафика. Чтобы избежать этого, необходимо настроить пару аварийного переключения с виртуальными адресами MAC. Дополнительную информацию см. в разделе настоящего документа Настройка конфигурации аварийного перехода на резервный ресурс в ждущем режиме.

В момент начала репликации на консоли устройства безопасности активного модуля выводится сообщение: `Beginning configuration replication: Sending to mate` (Начало репликации настроек: отправка другому члену пары). После завершения этого процесса, на устройстве защиты отобразится сообщение: `End Configuration Replication to mate` (Репликация настроек для другого члена пары завершена). Во время репликации команды, введенные на активном модуле, не будут реплицироваться на резервный модуль должным образом и могут быть перезаписаны конфигурацией, реплицированной с активного модуля. Не вводите команды ни на одном из модулей пары аварийного переключения во время репликации. В зависимости от размера конфигурации репликация может занять от нескольких секунд до нескольких минут.

На вспомогательном модуле можно наблюдать сообщение о репликации (по ходу синхронизации) с основного модуля:

```
ASA> .

       Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

ASA>
```

На резервном модуле конфигурация находится в оперативной памяти. Чтобы сохранить конфигурацию во флэш-память, введите следующие команды:

- Для режима с одиночным контекстом введите команду **copy running-config startup-config** на активном модуле. Команда реплицируется на резервный модуль, который обрабатывает ее и заносит во флэш-память.
- Для режима с несколькими контекстами введите команду **copy running-config startup-config** на активном модуле в системном поле исполнения и для каждого контекста на диске. Команда реплицируется на резервный модуль, который обрабатывает ее и заносит во флэш-память . Контексты с начальными конфигурациями на внешних серверах будут доступны на обоих модулях через сеть, и их не нужно сохранять на каждом модуле. Другой способ: можно скопировать контексты с диска активного модуля на внешний сервер, а затем скопировать их на диск резервного модуля. Контексты будут доступны после перезагрузке модуля.

Репликация команд

При репликации команд в качестве ведомого модуля выступает активный модуль, а в качестве ведущего модуля — резервный модуль. По мере ввода команд в активном модуле они пересылаются (через канал переключения при отказе) на резервный модуль. Для репликации команд не нужно сохранять активную конфигурацию во флэш-память.

Примечание. Команды, введенные в резервном устройстве, не реплицируются в активное устройство. При вводе команды на резервном модуле устройство безопасности выдаст сообщение: `**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit.` Оно уведомляет, что конфигурации больше не синхронизированы. Это сообщение будет отображаться даже при вводе команд, не влияющих на конфигурацию.

Если вы введете команду **write standby** на активном модуле, резервный модуль удалит рабочую конфигурацию (за исключением команд аварийного переключения, используемых для взаимодействия с активным модулем), и активный модуль отправляет свою конфигурацию в резервный модуль.

Для режима с несколькими контекстами при вводе команды **write standby** в системном поле выполнения реплицируются все контексты. Если вы введете команду write standby в контексте, будет реплицирована конфигурация этого контекста.

Реплицированные команды сохранятся в рабочей конфигурации. Чтобы сохранить реплицированные команды во флэш-памяти, введите следующие команды:

- Для режима с одиночным контекстом введите команду **copy running-config startup-config** на активном модуле. Команда реплицируется на резервный модуль, который обрабатывает ее и заносит во флэш-память .
- Для режима с несколькими контекстами введите команду **copy running-config startup-config** на активном модуле в системном поле исполнения и для каждого контекста на диске. Команда реплицируется на резервный модуль, который обрабатывает ее и заносит во флэш-память . Контексты с начальными конфигурациями на внешних серверах будут доступны на обоих модулях через сеть, и их не нужно сохранять на каждом модуле. Другой способ: можно скопировать контексты с диска активного модуля на внешний сервер, а затем скопировать их на диск резервного модуля.

Триггеры аварийного переключения

Модуль может отказать в одном из следующих случаев:

- В модуле произошел аппаратный сбой или отключено питание.
- В модуле произошел сбой ПО.
- Слишком много контролируемых интерфейсов не исправно.
- Вводится либо команда **no failover active** на активном модуле, либо команда **failover active** на модуле, находящемся в режиме ожидания.

Действия аварийного переключения

В конфигурации аварийного перехода на резервный ресурс в ждущем режиме аварийное переключение выполняется на уровне модуля. Даже на системах, работающих в режиме с несколькими контекстами, можно выполнить аварийное переключение для отдельных или групповых контекстов.

В следующей таблице приведены действия аварийного переключения для каждого нештатного события. Для каждого случая отказа в таблице приводятся политики аварийных переключений (возникает или не возникает переход), действия для активных модулей, действия для резервных модулей, а также особые примечания к условиям и действиям аварийных переключений. В таблице показано поведение при аварийном переключении.

Отказ	Политика	Действие активного модуля	Действие резервного модуля	Примечания
Отказ активного модуля (оборудование или питание)	Переключение	н/п	Становится активным; активный отмечается как неисправный	Сообщения приветствия (hello) не принимаются ни на одном контролируемом интерфейсе или канале аварийного переключения.
Бывший активный модуль восстанавливается	Без переключения	Переходит в ждущий режим	Без действий	Нет
Отказ резервного модуля (оборудование или питание)	Без переключения	Резервный модуль отмечается как отказавший	н/п	Если резервный модуль отмечается как отказавший, активный модуль не пытается выполнять аварийное переключение, даже если превышен порог неисправности интерфейса.
		Интерфейс	Интерфейс	Соединение аварийного переключения необходимо восстановить как можно

Сбой канала аварийного переключения в процессе операции	Без переключения	аварийного переключения отмечается как отказавший	аварийного переключения отмечается как отказавший	скорее, так как модуль не сможет переключиться на резервный модуль,если соединение аварийного переключения неисправно.
Сбой канала аварийного переключения при запуске	Без переключения	Интерфейс аварийного переключения отмечается как отказавший	Становится активным	Если соединение аварийного переключения отказывает при запуске, оба модуля становятся активными.
Сбой канала аварийного переключения с отслеживанием состояния	Без переключения	Без действий	Без действий	Информация о состоянии становится устаревшей, и сеансы прекращаются при аварийном переключении.
Неисправность интерфейса на активном модуле превышает пороговое значение	Переключение	Активный модуль отмечается как отказавший	Становится активным	Нет
Неисправность интерфейса на резервном модуле превышает пороговое значение	Без переключения	Без действий	Резервный модуль отмечается как отказавший	Если резервный модуль отмечается как отказавший, активный модуль не пытается выполнять аварийное переключение, даже если превышен порог неисправности интерфейса.

Регулярное аварийное переключение и аварийное переключение с сохранением состояния

Устройство безопасности поддерживает две конфигурации аварийного переключения: регулярное и с сохранением состояния. В этом разделе рассматриваются следующие темы.

- Регулярное аварийное переключение
- Аварийное переключение с сохранением состояния

Регулярное аварийное переключение

При регулярном аварийном переключении все активные подключения сбрасываются. Клиенты должны повторно установить подключения через новый активный модуль.

Аварийное переключение с сохранением состояния

Когда используется аварийное переключение с сохранением состояния, информация о состоянии подключения постоянно передается от активного модуля к резервному. При аварийном переключении предыдущая информация о соединении доступна для нового активного модуля. Поддерживаемые приложения конечного пользователя не требуются для сохранения сеанса связи.

Сведения о состоянии соединения, которые передаются узлу в режиме ожидания, включают следующее.

- Таблица преобразования NAT
- Состояние TCP-подключений
- Состояние UDP-подключений
- Таблица ARP
- Таблица моста уровня 2 (только когда межсетевой экран работает в прозрачном режиме **transparent firewall**)
- Состояния подключения HTTP (если включена репликация HTTP)
- Таблица ISAKMP и IPSec SA
- База данных подключения GTP PDP

Информация, которая не передается в резервный модуль при использовании аварийного переключения с отслеживанием состояния:

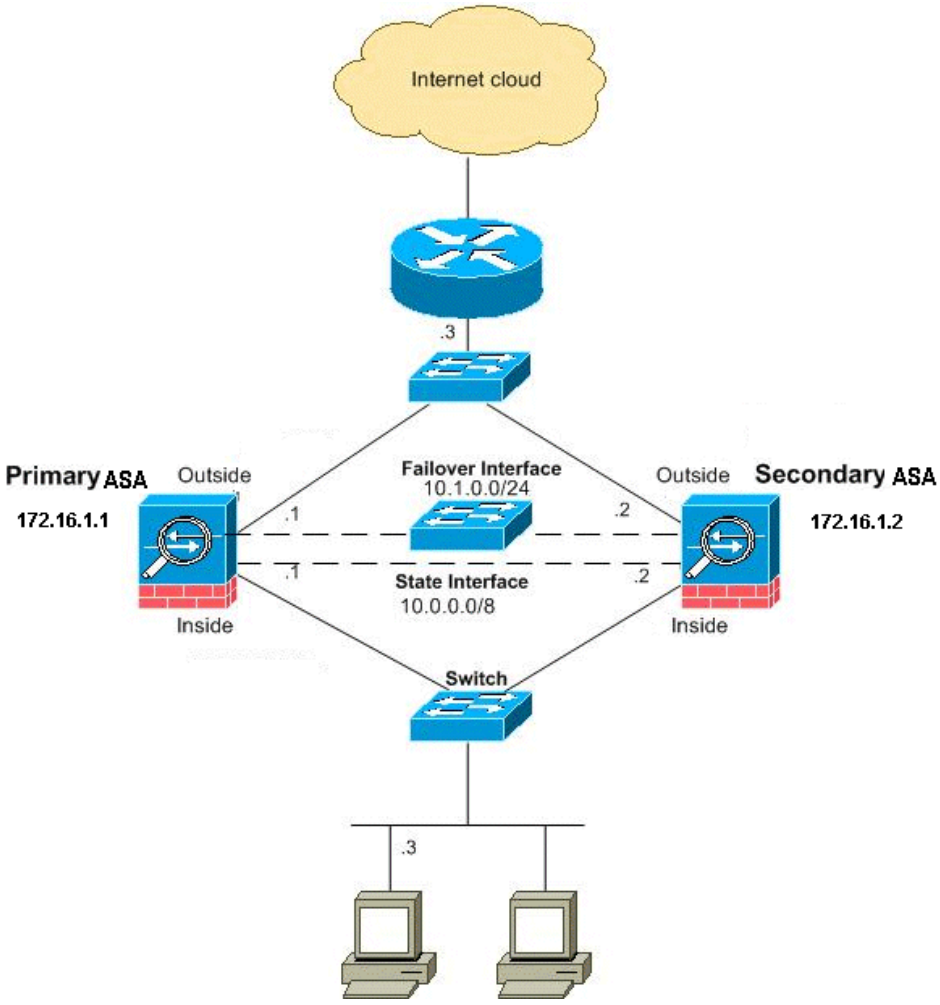
- Таблица подключения HTTP (если не включена репликация HTTP)
- Таблица аутентификации пользователя (uauth).
- Таблицы маршрутов
- Информация о состоянии для сервисных модулей безопасности

Примечание. Когда аварийное переключение происходит во время активной сессии Cisco IP SoftPhone, звонок остается активным, состояние данной сессии реплицируется резервным модулем. Когда звонок заканчивается, клиент IP SoftPhone теряет соединение с Cisco CallManager. Это происходит в результате того, что информация сессии для сообщения отбоя CTIQBE на резервном модуле отсутствует. Когда клиент IP SoftPhone не получает ответа от диспетчера звонков Cisco CallManager в течение некоторого периода времени, тогда для него Cisco CallManager приобретает значение«Недоступный», после чего выполняется отмена регистрации.

Конфигурации аварийного перехода на резервный ресурс в ждущем режиме с использованием локальной сети

Сетевой график

В этом документе используется следующая схема сети.



Данный раздел посвящен настройке аварийного перехода с активного на резервный ресурс в прозрачном режиме с использованием Ethernet-соединения в качестве соединения аварийного переключения. При настройке аварийного переключения с использованием локальной сети необходимо выполнить начальную загрузку вспомогательного модуля, чтобы распознать канал переключения до того, как вторичный модуль сможет получить текущую конфигурацию от основного устройства.

Примечание. При замене кабельного аварийного переключения на аварийное переключение с использованием локальной сети можно пропустить много шагов, например, назначение активного и резервного IP-адресов для каждого интерфейса, которые необходимы для кабельной конфигурации.

Настройка основного модуля

Следуйте данным инструкциям, чтобы создать для основного модуля конфигурацию аварийного перехода с активного на резервный ресурс с использованием локальной сети. Эти шаги обеспечивают минимальную конфигурацию, необходимую для аварийного переключения на основном модуле. Для режима с несколькими контекстами все шаги осуществляются в системном поле выполнения, если не указано иное.

Для настройки основного модуля в паре аварийного перехода с активного на резервный ресурс выполните следующие действия:

1. Если это сделано ранее, настройте IP-адреса активного и резервного модулей для интерфейса управления (прозрачный режим). Резервный IP-адрес используется на устройстве безопасности, которое в данный момент является резервным. Он должен находиться в той же подсети, что активный IP-адрес.

   Примечание. Не выполняйте настройку IP-адреса для канала аварийного переключения с отслеживанием состояния соединения в том случае, если используется выделенный интерфейс для данного переключения. Чтобы назначить выделенный интерфейс для аварийного переключения с отслеживанием состояния, используется команда **failover interface ip**.

```
hostname(config-if)#ip address active_addr netmask
                    standby standby_addr
```

В отличие от маршрутизируемого режима, в котором требуется IP-адрес для каждого интерфейса, в прозрачном межсетевом экране имеется IP-адрес, назначенный для всего устройства. Устройство защиты использует этот IP-адрес в качестве исходного адреса для пакетов, созданных устройством защиты, таких как системные сообщения или сообщения авторизации, аутентификации и учета (AAA). В этом примере IP-адрес для основного ASA настраивается так, как показано ниже:

```
hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
```

Здесь 172.16.1.1 — IP-адрес основного модуля и 172.16.1.2 — адрес вспомогательного (резервного) модуля.

Примечание. В режиме с несколькими контекстами необходимо настроить адреса интерфейсов в каждом контексте. Используйте команду **changeto context**, чтобы переключаться между контекстами. Командная строка принимает значение вида `hostname/context(config-if)#`, где context — имя текущего контекста.

2. (Только устройства безопасности с платформой PIX). Включите аварийное переключение через ЛВС.

```
hostname(config)#failover lan enable
```

3. Назначьте этот модуль основным.

```
hostname(config)#failover lan unit primary
```

4. Задайте интерфейс аварийного переключения.
    1. Задайте интерфейс, который будет использоваться в качестве интерфейса аварийного переключения.

```
hostname(config)#failover lan interface if_name phy_if
```

    В этом документе в качестве интерфейса аварийного переключения используется«failover» (имя интерфейса для Ethernet0).

```
hostname(config)#failover lan interface failover Ethernet3
```

    Параметр *if_name* назначает логическое имя интерфейсу, указанному в параметре *phy_if* . Параметр *phy_if* может задаваться именем физического порта, например Ethernet1, или предварительно созданного подчиненного интерфейса, например, Ethernet0/2.3.

    2. Назначьте активный и резервный IP-адреса соединению аварийного переключения:

```
hostname(config)#failover interface ip if_name ip_addr mask
                      standby ip_addr
```

    В этом документе при настройке канала аварийного переключения значение 10.1.0.1 используется для активного модуля, а значение 10.1.0.2 — для резервного модуля;«failover» — имя интерфейса для Ethernet0.

```
hostname(config)#failover interface ip failover 10.1.0.1
                      255.255.255.0 standby 10.1.0.2
```

    Резервный IP-адрес должен быть в одной подсети с активным IP-адресом. Не требуется указывать маску подсети для пассивного адреса.

    IP-адрес и MAC-адрес 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.

    3. Включите интерфейс:

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

В этом примере для аварийного переключения используется интерфейс Ethernet3:

```
hostname(config)#interface ethernet3
hostname(config-if)#no shutdown
```

5. (Необязательно) Чтобы активировать аварийное переключение с отслеживанием состояния, настройте соединение аварийного переключения с отслеживанием состояния.

   1. Задайте интерфейс, который будет использоваться в качестве соединения аварийного переключения.

      ```
      hostname(config)#failover link if_name phy_if
      ```

      В этом примере«state» используется в качестве имени интерфейса Ethernet2 для обмена данными о состоянии канала аварийного переключения.

      ```
      hostname(config)#failover link state Ethernet2
      ```

      Примечание. Если соединение аварийного переключения с отслеживанием состояния использует соединение аварийного переключения или интерфейс передачи данных, необходимо указать только параметр *if_name*.

      Параметр *if_name* назначает логическое имя интерфейсу, указанному в параметре *phy_if* . Параметр *phy_if* может задаваться именем физического порта, например Ethernet1, или предварительно созданного подчиненного интерфейса, например, Ethernet0/2.3. Этот интерфейс не должен использоваться для любой другой цели (кроме ссылки перехода на другой ресурс с отслеживанием состояния соединений).

   2. Назначьте активный и резервный IP-адреса соединению аварийного переключения.

      Примечание. Если соединение аварийного переключения с отслеживанием состояния использует соединение аварийного переключения или интерфейс передачи данных, пропустите этот шаг. Вы уже задали активный и резервный IP-адреса для интерфейса.

      ```
      hostname(config)#failover interface ip if_name ip_addr
                          mask standby ip_addr
      ```

      В этом примере 10.0.0.1 — активный и 10.0.0.2 — резервный IP-адрес для соединения аварийного переключения с отслеживанием состояния.

      ```
      hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                          standby 10.0.0.2
      ```

      Резервный IP-адрес должен быть в одной подсети с активным IP-адресом. Не требуется указывать маску подсети для пассивного адреса.

      MAC-адрес и IP-адрес соединения аварийного переключения с отслеживанием состояния меняются при аварийном переключении только в том случае, если они используют интерфейс передачи данных. Активный адрес IP всегда остается присвоенным главному узлу, в то время как пассивный адрес IP всегда останется присвоенным вторичному узлу.

   3. Включение интерфейса.

      Примечание. Если соединение аварийного переключения с отслеживанием состояния использует соединение аварийного переключения или интерфейс передачи данных, пропустите этот шаг. Включение интерфейса было уже выполнено.

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

Примечание. Например, в этом сценарии Ethernet2 используется для канала аварийного переключения с отслеживанием состояния:

```
hostname(config)#interface ethernet2

hostname(config-if)#no shutdown
```

6. Включите аварийное переключение.

```
hostname(config)#failover
```

Примечание. Используйте команду **failover** сначала на основном модуле, а затем на вспомогательном. После использования команды **failover** на вспомогательном модуле, этот модуль немедленно принимает конфигурацию от основного модуля и определяет себя как *резервный*. Основной ASA пропускает трафик в нормальном режиме и определяет себя как *активное* устройство. С этого момента, при возникновении отказа на активном модуле резервный модуль занимает место активного.

7. Сохраните конфигурацию системы на флэш-память.

```
hostname(config)#copy running-config startup-config
```

Конфигурация вспомогательного модуля

Для вспомогательного модуля необходимо настроить только интерфейс аварийного переключения. Для взаимодействия с основным модулем на вспомогательном модуле необходимо задать следующие команды. После того как основной модуль отправит свою конфигурацию вспомогательному, единственным постоянным различием между двумя конфигурациями будет команда **failover lan unit** , которая определяет основной и вспомогательный модули.

Для режима с несколькими контекстами все шаги осуществляются в системном поле выполнения, если не указано иное.

Чтобы настроить вспомогательный модуль, выполните следующие действия.

1. (Только устройства безопасности с платформой PIX). Включите аварийное переключение через ЛВС.

```
hostname(config)#failover lan enable
```

2. Задайте интерфейс аварийного переключения. Используйте те же параметр, что для основного модуля.
    1. Задайте интерфейс, который будет использоваться в качестве интерфейса аварийного переключения.

```
hostname(config)#failover lan interface if_name phy_if
```

В этом документе в качестве интерфейса аварийного переключения ЛВС используется Ethernet0.

```
hostname(config)#failover lan interface failover Ethernet3
```

Параметр *if_name* назначает логическое имя интерфейсу, указанному в параметре *phy_if*.

2. Назначьте активный и резервный IP-адреса соединению аварийного переключения.

```
hostname(config)#failover interface ip if_name ip_addr mask
                      standby ip_addr
```

В этом документе при настройке канала аварийного переключения значение 10.1.0.1 используется для активного модуля, а значение 10.1.0.2 — для резервного модуля;«failover» — имя интерфейса для Ethernet0.

```
hostname(config)#failover interface ip failover 10.1.0.1
                      255.255.255.0 standby 10.1.0.2
```

Примечание. Используйте команду **failover** сначала на основном модуле, а затем на вспомогательном.

3. Включите интерфейс.

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

Например, в этом сценарии для аварийного переключения используется интерфейс Ethernet0.

```
hostname(config)#interface ethernet3
hostname(config-if)#no shutdown
```

3. (Необязательно) Назначьте этот модуль вспомогательным.

```
hostname(config)#failover lan unit secondary
```

Примечание. Это действие необязательно, так как по умолчанию модули назначаются вторичными, если не настроены раньше.

4. Включите аварийное переключение.

```
hostname(config)#failover
```

Примечание. После включения аварийного переключения активный модуль отправит конфигурацию в оперативной памяти резервному модулю. Во время синхронизации конфигурации на консоли основного модуля появятся сообщения: *Beginning configuration replication: Sending to mate* и *End Configuration Replication to mate*.

5. После завершения репликации текущей конфигурации сохраните ее на флэш-память.

```
hostname(config)#copy running-config startup-config
```

Конфигурации

В этом документе используются следующие конфигурации:

Основной ASA

```
ASA#show running-config
ASA Version 7.2(3)
!

!--- Чтобы установить для межсетевого экрана прозрачный режим,
!--- используйте команду firewall transparent
!--- в глобальном режиме конфигурации.

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
nameif failover

 description LAN Failover Interface
!
interface Ethernet1
nameif inside
security-level 100
!
interface Ethernet2
nameif outside
security-level 0


!--- Настройте no shutdown в интерфейсе перехвата управления при отказе с синхронизацией состояния
!--- на основном и дополнительном модулях ASA.

interface Ethernet3
nameif state
description STATE Failover Interface
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500


!--- Назначьте IP-адреса для основного и
!--- дополнительного устройств защиты ASA.


ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby 10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
```

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Вспомогательный ASA

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
```

Проверка

Использование команды show failover

В этом разделе приведено описание выходных данных команды **show failover**. Для каждого модуля можно проверить состояние аварийного переключения с помощью команды **show failover**.

Основной ASA

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
```

```
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 00:08:03 UTC Jan 1 1993
       This host: Primary - Active
               Active time: 1820 (sec)
                 Interface inside (172.16.1.1): Normal
                 Interface outside (172.16.1.1): Normal
       Other host: Secondary - Standby Ready
               Active time: 0 (sec)
                 Interface inside (172.16.1.2): Normal
                 Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
       Link : state Ethernet3 (up)
       Stateful Obj    xmit       xerr       rcv        rerr
       General         185        0          183        0
       sys cmd         183        0          183        0
       up time         0          0          0          0
       RPC services    0          0          0          0
       TCP conn        0          0          0          0
       UDP conn        0          0          0          0
       ARP tbl         0          0          0          0
       L2BRIDGE Tbl    2          0          0          0
       Xlate_Timeout   0          0          0          0

       Logical Update Queue Information
                       Cur     Max     Total
       Recv Q:         0       1       7012
       Xmit Q:         0       1       185
```

Вспомогательный ASA

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 16:39:12 UTC Aug 9 2009
       This host: Secondary - Standby Ready
               Active time: 0 (sec)
                 Interface inside (172.16.1.2): Normal
                 Interface outside (172.16.1.2): Normal
       Other host: Primary - Active
               Active time: 1871 (sec)
                 Interface inside (172.16.1.1): Normal
                 Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics
       Link : state Ethernet3 (up)
       Stateful Obj    xmit       xerr       rcv        rerr
       General         183        0          183        0
       sys cmd         183        0          183        0
       up time         0          0          0          0
       RPC services    0          0          0          0
       TCP conn        0          0          0          0
       UDP conn        0          0          0          0
       ARP tbl         0          0          0          0
       L2BRIDGE Tbl    0          0          0          0
       Xlate_Timeout   0          0          0          0

       Logical Update Queue Information
                       Cur     Max     Total
       Recv Q:         0       1       7043
       Xmit Q:         0       1       183
```

Для проверки состояния используйте команду **show failover state**.

Основной ASA

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure            00:02:36 UTC Jan 1 1993

====Configuration State===
       Sync Done
====Communication State===
       Mac set
```

Вторичный узел

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
       Sync Done - STANDBY
====Communication State===
       Mac set
```

Для проверки IP-адресов модуля аварийного переключения используйте команду **show failover interface**.

Основной модуль

```
ASA#show failover interface
       interface failover Ethernet0
               System IP Address: 10.1.0.1 255.255.255.0
               My IP Address    : 10.1.0.1
               Other IP Address : 10.1.0.2
       interface state Ethernet3
               System IP Address: 10.0.0.1 255.255.255.0
               My IP Address    : 10.0.0.1
               Other IP Address : 10.0.0.2
```

Вторичный узел

```
ASA#show failover interface
       interface failover Ethernet0
               System IP Address: 10.1.0.1 255.255.255.0
               My IP Address    : 10.1.0.2
               Other IP Address : 10.1.0.1
       interface state Ethernet3
               System IP Address: 10.0.0.1 255.255.255.0
               My IP Address    : 10.0.0.2
               Other IP Address : 10.0.0.1
```

Просмотр контролируемых интерфейсов

Чтобы просмотреть состояние контролируемых интерфейсов, сделайте следующее. В режимах одиночного контекста и глобальной настройки введите команду **show monitor-interface**. В многоконтекстном режиме введите команду **show monitor-interface** внутри контекста.

Основной ASA

```
ASA(config)#show monitor-interface
       This host: Primary - Active
               Interface inside (172.16.1.1): Normal
               Interface outside (172.16.1.1): Normal
       Other host: Secondary - Standby Ready
               Interface inside (172.16.1.2): Normal
               Interface outside (172.16.1.2): Normal
```

Вспомогательный ASA

```
ASA(config)#show monitor-interface
       This host: Secondary - Standby Ready
               Interface inside (172.16.1.2): Normal
               Interface outside (172.16.1.2): Normal
       Other host: Primary - Active
               Interface inside (172.16.1.1): Normal
               Interface outside (172.16.1.1): Normal
```

Примечание. Если IP-адрес не введен, команда **show failover** отображает для IP-адреса значение 0.0.0.0, а мониторинг интерфейса остается в состоянии *ожидания*. Для получения подробной информации о различных состояниях аварийного переключения см. раздел Показать аварийное переключение *Справочника по командам устройств безопасности Cisco, версия 7.2*.

Отображение команд аварийного переключения в текущей конфигурации

Чтобы просмотреть команды аварийного переключения в текущей конфигурации, введите команду:

```
hostname(config)#show running-config failover
```

Будет выполнено отображение всех команд, связанных с переходом на другой ресурс при сбое. Для модулей, работающих в режиме с несколькими контекстами, введите команду **show running-config failover** в системном поле исполнения. Введите команду **show running-config all failover**, чтобы отобразить команды аварийного переключения в текущей конфигурации и включить команды, для которых не были изменены значения по умолчанию.

Проверка функциональности аварийного переключения

Для проверки функциональности аварийного переключения выполните следующие шаги.

1. Проверьте, что активный модуль и резервная группа пропускают трафик, как требуется для FTP (например), послав файл с одного узла на другой с различными интерфейсами.
2. Вызовите аварийное переключение на резервный модуль с помощью следующей команды:

   Для аварийного переключения с активного на резервный ресурс введите следующую команду на активном модуле:

   ```
   hostname(config)#no failover active
   ```

3. Используйте FTP для передачи другого файла между теми же двумя узлами.
4. Ели тест кончился неудачей, введите команду **show failover**, чтобы проверить состояние аварийного переключения.
5. После завершения проверки можно восстановить активный статус модуля или резервной группы с помощью следующей команды:

Для аварийного переключения с активного на резервный ресурс введите следующую команду на активном модуле:

```
hostname(config)#failover active
```

Принудительное аварийное переключение

Чтобы принудительно перевести узел из режима ожидания в активное состояние, введите одну из следующих команд.

Введите следующую команду на ждущем модуле:

```
hostname#failover active
```

Введите следующую команду на ждущем модуле:

```
hostname#no failover active
```

Отключение аварийного переключения

Чтобы отключить переход на другой ресурс при сбое, введите команду:

```
hostname(config)#no failover
```

Если отключить переход на другой ресурс при сбое на паре Active/Standby (активный/ожидающий), то активное и пассивное состояние каждого узла будет применено до перезапуска системы. Например, узел находится в режиме ожидания, и оба узла не начнут транслировать трафик. Процедура переключения резервного модуля в активное состояние (даже при отключенном аварийном переключении) описана в разделе Принудительное аварийное переключение.

Если отключить аварийное переключение с активного на активный ресурс, резервные группы останутся в активном состоянии в том модуле, в котором они в настоящее время активны, независимо от того, какой модуль в их конфигурации задан как предпочтительный. Команда **no failover** может быть введена в системном пространстве выполнения.

Восстановление неисправного модуля

Чтобы вернуть неисправному модулю статус исправного, введите следующую команду:

```
hostname(config)#failover reset
```

При восстановлении отказавшего модуля в исправное состояние автоматического перехода в активное состояние не происходит; восстановленные узлы или группы продолжают оставаться в режиме ожидания до тех пор, пока они не становятся активными вследствие аварийного переключения (при сбое или принудительно). Исключение составляет группа перехода, настроенная с помощью команды preempt. Если группа аварийного переключения была ранее активной, она снова становится активной, при условии, что она настроена с командой preempt, а модуль, в котором она отказала, является ее предпочтительным модулем.

Поиск и устранение неполадок

При переключении на другой ресурс, оба устройства защиты отправляют системные сообщения. В этом разделе рассматриваются следующие темы.

- Мониторинг восстановления при отказе
- Сбой модуля
- %ASA-3-210005: сбой выделенного подключения LU
- Сообщения системы аварийного переключения
- Сообщения отладки
- SNMP
- Типичные ошибки

Мониторинг восстановления при отказе

В этом примере показано, что происходит, если аварийное переключение не начинает мониторинг сетевых интерфейсов. Функция переключения при отказе не начинает мониторинг сетевых интерфейсов, пока не получит второй пакет сообщений `hello` от другого устройства на этом интерфейсе. Это займет около 30 секунд. Если модуль присоединен к сетевому коммутатору, работающему по протоколу STP, настроенное на коммутаторе время `forward delay` (задержка пересылки), которое обычно оно составляет 15 сек, увеличивается в два раза плюс 30 сек задержки. Это происходит потому, что при загрузке ASA и событии сбоя, которое следует сразу после загрузки, системный коммутатор определяет временную замкнутую петлю. При обнаружении петли коммутатор перестает пересылать пакеты с этих интерфейсов в течение времени `forward delay` (задержка пересылки). Затем он переходит в режим прослушивания `listen` для дополнительной задержки пересылки `forward delay`, в течение которой коммутатор принимает замкнутые петли, но не пересылает трафик (и, следовательно, не пересылает пакеты `hello` переключения при отказе). Поток трафика должен возобновиться по прошествии двойного времени задержки пересылки (30 секунд). Каждый модуль ASA остается в режиме ожидания `waiting`, пока не получит 30-секундную последовательность пакетов приветствия `hello` от другого модуля. Во время передачи трафика межсетевой экран PIX не вызывает сбой в других модулях, исходя из отсутствия пакетов приветствия `hello`. Все остальные виды мониторинга переключения при отказе сохраняются (имеется в виду мониторинг питания, потери интерфейса на канале, а также сообщение `hello` кабеля переключения при отказе).

Cisco настоятельно рекомендует своим клиентам включать функцию portfast на всех портах коммутатора, подключенных к интерфейсам ASA. Кроме того, на этих портах необходимо отключить режим объединения в канал и режим магистрального соединения. Если интерфейс ASA отключается во время аварийного переключения, коммутатор не должен ожидать 30 секунд, пока порт переходит из состояния прослушивания в состояние изучения и далее в состояние переадресации.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
 This host: Primary - Active
  Active time: 6930 (sec)
  Interface inside (172.16.1.1): Normal (Waiting)
  Interface outside (172.16.1.1): Normal (Waiting)
 Other host: Secondary - Standby
  Active time: 15 (sec)
  Interface inside (172.16.1.2): Normal (Waiting)
  Interface outside (172.16.1.2): Normal (Waiting)
```

Ниже приведена сводка проверок, которые необходимо выполнить для локализации проблем аварийного переключения.

- Проверьте сетевые кабели, подключенные к интерфейсу в ждущем/неисправном состоянии, и, если возможно, замените их.
- Если между двумя модулями подключен коммутатор, проверьте, что сети, подключенные к интерфейсу в ждущем/неисправном состоянии, функционируют нормально.
- Проверьте порт коммутатора, подключенный к интерфейсу в ждущем/неисправном состоянии, и, если возможно, попробуйте использовать другой порт FE коммутатора.
- Проверьте, что на подключенных к интерфейсу портах коммутатора функция PortFast включена, а режимы объединения портов в

канал и магистрального соединения отключены.

Отказ модуля

В этом примере в процессе аварийного переключения обнаружена ошибка. Обратите внимание на то, что причиной ошибки является интерфейс 1 на основном модуле. Из-за ошибки модули переводятся в режим ожидания `waiting`. Отказавшее устройство удаляется из сети (интерфейсы отключаются) и больше не отправляет пакеты `hello` в сеть. Активный модуль остается в состоянии ожидания `waiting`, пока отказавший модуль не будет заменен и переключения при отказе не начнутся снова.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
 This host: Primary - Standby (Failed)
  Active time: 7140 (sec)
  Interface inside (172.16.1.2): Normal (Waiting)
  Interface outside (172.16.1.2): Failed (Waiting)
 Other host: Secondary - Active
  Active time: 30 (sec)
  Interface inside (172.16.1.1): Normal (Waiting)
  Interface outside (172.16.1.1): Normal (Waiting)
```

Сбой выделенного подключения LU

Возможен сбой памяти, если получена следующая ошибка:

```
LU allocate connection failed (Сбой выделенного подключения LU)
```

Для решения этой проблемы требуется обновить ПО PIX/ASA.

Сообщения системы аварийного переключения

Устройство безопасности выдает ряд системных сообщений, связанных с аварийным переключением, которым присваивается приоритет 2, что указывает на критическое состояние. Сведения о том, как просмотреть эти сообщения, включить ведение журнала и отобразить описание системных сообщений, см. в документе Настройка ведения журналов модулей защиты Cisco и сообщения системного журнала.

Примечание. При переключении с использованием коммутаторов, аварийное переключение автоматически отключается, и выполняется монтирование интерфейсов с созданием сообщений с номерами **411001** и **411002**. Это стандартное поведение.

Сообщения отладки

Для просмотра сообщений отладки введите команду **debug fover**. Для получения подробной информации см. Справочник по командам устройства защиты Cisco.

Примечание. Поскольку выходным данным отладки назначен высокий приоритет для обработки процессором, это может привести к существенному снижению производительности системы. Поэтому используйте команды **debug fover** только для поиска и устранения определенных проблем или во время сеансов устранения неполадок при участии технических специалистов Cisco.

SNMP

Чтобы получить прерывания системного журнала SNMP для аварийных переключений, настройте агент SNMP для отправки прерывания SNMP на станции управления SNMP, задайте узел системного журнала и скомпилируйте MIB системного журнала Cisco на станции управления SNMP. Дополнительные сведения о командах **snmp-server** и **logging** см. в Справочнике по командам устройств защиты Cisco.

Последовательный опрос при обработке отказов

Чтобы указать время опроса узла аварийного переключения и время удержания, введите команду **failover polltime** в режиме глобальной настройки.

Время `failover polltime unit msec [time]` выражает временной интервал для проверки наличия резервного модуля путем опроса с использованием сообщений приветствия (hello).

Аналогично команда `failover holdtime unit msec [time]` представляет собой временной интервал, во время которого модуль должен получить сообщение приветствия (hello) через соединения аварийного переключения. По прошествии этого периода модуль объявляется отказавшим.

Чтобы указать время опроса интерфейса данных и время удержания в конфигурации аварийного переключения«Активный/резервный», введите команду **failover polltime interface** в режиме глобальной настройки. Чтобы восстановить настройку по умолчанию для времени опроса и времени удержания, используйте аргумент **no** данной команды.

```
failover polltime interface [msec] time [holdtime time]
```

Используйте команду **failover polltime interface**, чтобы изменить частоту отправки пакетов hello на интерфейсе данных. Эта команда доступна только для конфигураций аварийного переключения с активного ресурса на резервный в режиме ожидания. Для конфигураций аварийного переключения с активного ресурса на активный используйте команду **polltime interface** в конфигурации группы аварийного переключения вместо команды **failover polltime interface**.

Можно ввести значение *holdtime*, которое будет в пять раз меньше времени опроса интерфейса. Чем меньше время опроса, тем быстрее устройство защиты обнаружит отказ и выполнит аварийное переключение. Однако слишком быстрое обнаружение приводит к излишним переключениям, когда сеть временно перегружена. Проверка интерфейса начинается, когда пакет hello не принимается интерфейсом дольше половины времени удержания.

В конфигурацию можно включить обе команды failover polltime unit и failover polltime interface.

В приведенном ниже примере время для частоты опроса интерфейса установлено равным 500 миллисекунд, а время удержания составляет 5 секунд.

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

Для получения подробной информации см. раздел Последовательный опрос при обработке отказов (failover polltime) *Справочника по командам устройств безопасности Cisco, версия 7.2.*

Экспорт сертификата/секретного ключа в конфигурации аварийного переключения

Основное устройство автоматически реплицирует сертификат/секретный ключ на вспомогательный модуль. Выполните команду **write memory** на активном модуле, чтобы переписать конфигурацию, включающую сертификат/секретный ключ, в память резервного модуля. Все предыдущие сертификаты/ключи на резервном устройстве удаляются и заменяются конфигурацией активного модуля.

Примечание. Необходимо вручную импортировать сертификаты, ключи и доверенные точки с активного устройства, а затем экспортировать их на резервное устройство.

ПРЕДУПРЕЖДЕНИЕ: сбой описания сообщения аварийного переключения.

Сообщение об ошибках:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

Эта проблема возникает из-за конфигурации ключа аварийного переключения. Чтобы устранить эту проблему, удалите ключ аварийного переключения и создайте новый общий ключ.

Аварийное переключение модулей ASA

Если в активных или резервных устройствах используются модули Advanced Inspection and Prevention Security Services Module (AIP-SSM) или Content Security and Control Security Services Module (CSC-SSM), тогда они работают независимо от ASA в терминах аварийного переключения. **Модули должны настраиваться вручную в активном и резервном модулях, аварийное переключение не реплицирует конфигурацию модуля.**

Для обеспечения аварийного переключения оба устройства ASA с модулями AIP-SSM или CSC-SSM должны относиться к одному аппаратному типу. Например, если основное устройство имеет модуль ASA-SSM-10, вспомогательное устройство также должно содержать модуль ASA-SSM-10.

Сообщение аварийного переключения block alloc failed

Сообщение об ошибке `%PIX|ASA-3-105010: (Primary) Failover message block alloc failed`

Объяснение: память блока исчерпана. Это переходное сообщение, вспомогательное устройство защиты должно быть восстановлено. *Primary (Основной)* может также быть заменено на *Secondary (Вспомогательный)* для вспомогательного устройства.

Рекомендуемое действие: Используйте команду **show blocks**, чтобы контролировать текущую память блока.

Проблемы аварийного переключения модуля AIP

Если в вашей среде установлено два модуля ASA в конфигурации аварийного переключения и каждый из них имеет модуль AIP-SSM, необходимо вручную реплицировать конфигурацию AIP-SSM. Механизм аварийного переключения реплицирует только конфигурацию ASA. Модуль AIP-SSM не участвует в аварийном переключении.

Прежде всего, AIP-SSM работает независимо от ASA в терминах аварийного переключения. Все, что требуется от ASA для обеспечения аварийного переключения — чтобы модули AIP были одного аппаратного типа. Кроме этого, для любой другой части аварийного переключения конфигурация ASA между активным и резервным модулями должна быть синхронизирована.

Что касается настройки модулей AIP, то они являются фактически независимыми датчиками. Между этими двумя модулями нет аварийного переключения, они не получают никакой информации друг о друге. Они могут использовать независимые версии кодов. То есть, для ASA неважно, какие версии кодов используются на модулях AIP в том, что касается аварийного переключения.

ASDM инициирует подключение AIP через интерфейс управления IP, который настроен на AIP. Другими словами, он подключается к датчику обычно через HTTPS, что зависит от того, как настроен датчик.

Можно выполнять аварийное переключение ASA независимо от модулей IPS (AIP). Подключение к тому же модулю сохраняется, поскольку подключение выполняется к его интерфейсу управления IP. Чтобы подключиться к другому AIP, необходимо снова подключиться к его интерфейсу управления IP для настройки и доступа.

Подробная информация и примеры конфигураций для отправки трафика через устройство адаптивной защиты Cisco ASA 5500 Series (ASA) на модуль Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS) о см. документ ASA: пример конфигурации, предназначенной для отправки сетевого трафика, проходящего через устройство Cisco ASA 5500 в модуль AIP-SSM (IPS).

Типичные ошибки

При попытке доступа к ASDM на вспомогательном ASA с версией ПО 8.x и ASDM версии 6.x для настройки аварийного переключения появляется следующая ошибка:

```
Error: The name on the security certificate is invalid or does not match the name of the site
```

В сертификате Issuer (Запрашивающая сторона) и Subject Name (Имя субъекта) являются IP-адресом *активного* модуля, а не IP-адресом *резервного* модуля.

В ASA версии 8.x внутренний (ASDM) сертификат реплицируется с активного модуля на резервный модуль, что приводит к появлению сообщения об ошибке. Однако если тот же межсетевой экран работает с кодом версии 7.x с ASDM 5.x, а пользователь пытается получить доступ к ASDM, появляется стандартное предупреждение системы безопасности:

```
The security certificate has a valid name matching the name of the page you are trying to view
```

При проверке сертификата в качестве данных запрашивающей стороны и имени субъекта используется IP-адрес резервного модуля.

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/107/1074041/asafailover-transparent-mode.shtml