PIX/ASA: Пример конфигурации переключения при отказе по схеме «активный/активный»

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 обеспечения безопасности поддерживает два типа конфигураций аварийного переключения: аварийное переключение на активный резервный ресурс и аварийное переключение на резервный ресурс в режиме ожидания. 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 распределение 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).

В этом документе описывается настройка конфигурации аварийного переключения на активный резервный ресурс для устройств защиты Cisco PIX/ASA Security Appliance.

Для получения дополнительной информации о конфигурации аварийного переключения на резервный ресурс в режиме ожидания см. документ PIX/ASA 7.x: пример конфигурации аварийного переключения на резервный ресурс в режиме ожидания.

Примечание: Аварийное переключение VPN не поддерживается на модулях, которые работают в многоконтекстном режиме, поскольку VPN не поддерживается в составном контексте. Аварийное переключение VPN доступно только для **Активных/Резервных Конфигураций аварийного переключения** в одиночных конфигурациях контекста.

Это руководство по конфигурации предоставляет пример конфигурации для включения

краткого введения в PIX/ASA 7.x Активная/Активная технология. См. Справочник по командам Cisco Security Appliance Версия 7.2 для более всестороннего смысла теории базировалась позади этой технологии.

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. Если в конфигурации аварийного переключения используются узлы с разными объемами флэш-памяти, 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 в процессе обновления можно использовать различные версии ПО; например, можно обновить один узел с версии 7.0(1) до версии 7.0(2) и при этом оставаться в режиме активного узла аварийного переключения. Cisco рекомендует обновить оба модуля до одинаковой версии, чтобы гарантировать долгосрочную совместимость.

См. Осуществление модернизации с нулевым периодом простоя для Пар аварийного переключения для получения дополнительной информации об обновлении программного обеспечения на паре аварийного переключения.

Требования к лицензии

На платформе PIX/ASA Security Appliance по меньшей мере один из узлов должен иметь неограниченную лицензию (UR). Другой модуль может иметь Аварийное переключение Только Активно-активная лицензия (FO_AA) или другая лицензия UR. Узлы с ограниченной лицензией (Restricted) не могут использоваться для организации перехода на другой ресурс при сбое, так же нельзя использовать два узла с лицензией типа FO_AA.

Примечание: Вы, возможно, должны были бы обновить лицензии на паре аварийного переключения для получения дополнительных характеристик и преимуществ. Для получения дополнительной информации об обновлении обратитесь к Обновлению Лицензионного ключа на Паре аварийного переключения

Примечание: Лицензированные функции, такие как узлы VPN SSL или контексты безопасности, на обоих устройствах безопасности, которые участвуют в аварийном переключении, должны быть идентичными.

Примечание: Лицензия FO не поддерживает Активное/Активное Аварийное переключение.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

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

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.

Родственные продукты

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

- ASA с 7.x версия и позже

Примечание: Активное/Активное аварийное переключение не доступно на устройстве адаптивной безопасности ASA 5505 серии.

Условные обозначения

См. Cisco Technical Tips Conventions для получения дополнительной информации условные обозначения в документации.

Аварийное переключение между активными модулями

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

Конфигурация аварийного перехода на активный резервный ресурс — обзор

Активное/Активное аварийное переключение только доступно устройствам безопасности в многоконтекстном режиме. В Конфигурации "активный-активный" оба устройства безопасности могут передать сетевой трафик.

В Активном/Активном аварийном переключении вы делите контексты безопасности на устройстве безопасности в группы аварийного переключения. Группа аварийного переключения является просто логической группой одного или более контекстов безопасности. Можно создать максимум двух групп аварийного переключения на устройстве

безопасности. Контекст администратора всегда является участником группы аварийного переключения 1. Любые неназначенные контексты безопасности являются также участниками группы аварийного переключения 1 по умолчанию.

Группа аварийного переключения формирует базовый блок для аварийного переключения в Активном/Активном аварийном переключении. Мониторинг отказа интерфейса, аварийное переключение и активное/резервное состояние являются всеми атрибутами группы аварийного переключения, а не модуля. Когда активная группа аварийного переключения отказывает, она изменяется на резервное состояние, в то время как резервная группа аварийного переключения становится активной. Интерфейсы в группе аварийного переключения, которая становится активной, принимают MAC и IP-адреса интерфейсов в группе аварийного переключения, которая отказала. Интерфейсы в группе аварийного переключения, которая находится теперь в резервном состоянии, принимают резервный MAC и IP-адреса.

Примечание: Группа аварийного переключения, отказывающая на модуле, не подразумевает, что отказал модуль. Модуль может все еще иметь другой проходящий трафик группы аварийного переключения на нем.

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

Как и для конфигурации аварийного переключения режиме ожидания, в конфигурации аварийного переключения на активный резервный ресурс в паре перехода один модуль является главным, а другой — второстепенным. В отличие от конфигурации аварийного переключения в режиме ожидания, в конфигурации аварийного переключения на активный резервный ресурс не указывается, какой узел становится активным при одновременном запуске обоих узлов. Вместо этого основное/вторичное обозначение делает две вещи:

- Определения узла, который обеспечивает рабочую конфигурацию для пары при синхронной загрузке.
- Определения узла, на котором каждая группа аварийного переключения активизируется при одновременной загрузке узлов. Каждая группа аварийного переключения при сбое в конфигурации настраивается в соответствии с параметрами главного или второстепенного узла. Можно установить параметры обеих групп перехода одного узла, работающих в паре, для установки в активном состоянии, в то время как на другом узле группы перехода будут находиться в режиме ожидания. Однако более типичной конфигурацией является установка различного состояния каждой группы перехода узла, чтобы на каждом узле одна из групп оставалась активной, при этом трафик распределяется между узлами.**Примечание:** Устройство безопасности **не** предоставляет сервисы распределения нагрузки. Распределение нагрузки должно быть обработано проходящим трафиком маршрутизатора к устройству безопасности.

Ниже показан способ определения группы аварийного переключения, которая становится активной для данного узла

- При загрузке одного узла, в то время как второй отсутствует, обе группы аварийного переключения активируются на одном узле.
- При загрузке узла при активном втором узле (с обеими группами перехода на другой ресурс при сбое в активном состоянии), обе группы остаются в активном состоянии на активном узле, вне зависимости от первичного или вторичного состояния группы, до тех пор, пока не произойдет одно из следующих событий:Аварийное переключение

происходит.**При переподключении вручную группы аварийного переключения с помощью команды no failover activeГруппа аварийного переключения настроена вручную при помощи команды preempt, которая программирует автоматический перенос активной группы аварийного переключения на предпочитаемый узел, когда последний становится доступным.**

- Когда обе начальных загрузки модулей в то же время, каждая группа аварийного переключения становится активной на своем предпочтительном модуле после того, как синхронизировались конфигурации.

Инициализация устройства и синхронизация конфигурации

Когда один или оба модуля в паре аварийного переключения загружаются, синхронизация настроек происходит. Конфигурации синхронизируются как показано:

- При загрузке одного в то время, когда второй остается активным (с обеими группами аварийного переключения в активном состоянии), загружающийся узел связывается с активным узлом для получения рабочих настроек вне зависимости от состояния "первичный" или "вторичный", установленного для загружающегося узла.
- Когда обе начальных загрузки модулей одновременно, вспомогательный модуль получает рабочую конфигурацию из первичного модуля.

При начале процесса репликации, консоль устройства защиты узла, который отправляет параметры настроек, выводит сообщение "Начало репликации настроек: оотправка другому члену пары". После завершения этого процесса, на устройстве защиты отобразится сообщение "Репликация настроек на другого члена пары завершена". Во время репликации команды, которые вводятся на узле, выполняющем отправку настроек, могут неверно отразиться на принимающем узле, а команды, которые вводятся на принимающем узле, могут быть переписаны настройками, полученными от отправляющего узла. Избегайте ввода команд на любом из узлов, находящихся в паре, во время репликации настроек. В зависимости от размера конфигурации репликация может взять от нескольких секунд до нескольких минут.

На принимающем узле настройки имеются только в оперативной памяти устройства. **Чтобы после синхронизации сохранить настройки во флэш-памяти, введите команду write memory all в системном пространстве узла, на котором группа перехода на другой ресурс 1 находится в активном состоянии.** Команда реплицирована в одноранговый модуль, который продолжает писать его конфигурацию во флэш-память. Использование **всего** ключевого слова с этой командой заставляет систему и все конфигурации контекста быть сохраненной.

Примечание: Настройки запуска, сохраняемые на внешних серверах, доступны из любого узла сети, при этом нет необходимости сохранять их отдельно для каждого узла. Как вариант, можно скопировать файлы с настройками контекстов с диска главного узла на внешний сервер, затем скопировать их на диск вторичного узла, где они впоследствии становятся доступными после перезагрузки узла.

Репликация команд

После того, как оба узла запущены, команды реплицируются на другой узел следующим образом:

- Команды, введенные в контексте безопасности, реплицированы от модуля, на котором

контекст безопасности появляется в активном состоянии к одноранговому модулю.**Примечание:** контекст считается находящимся в активном состоянии на узле в том случае, если группа аварийного переключения, которой он принадлежит, находится в активном состоянии на этом узле.
- Команды, введенные в системное поле выполнения, реплицированы от модуля, на котором группа аварийного переключения 1 находится в активном состоянии к модулю, на котором группа аварийного переключения 1 находится в резервном состоянии.
- Команды, введенные в контекст администратора, реплицированы от модуля, на котором группа аварийного переключения 1 находится в активном состоянии к модулю, на котором группа аварийного переключения 1 находится в резервном состоянии.

Вся конфигурация и команды файла (**копия, переименуйте, удалите, mkdir, rmdir,** и так далее) реплицированы, за следующими исключениями. **Команды show, debug, mode, firewall, and failover lan unit** не реплицированы.

Сбой для ввода команд в соответствующий модуль для репликации команд для появления заставляет конфигурации быть вне синхронизации. Те изменения могут быть потеряны в следующий раз, когда синхронизация начальной конфигурации происходит.

Можно использовать команду **резерва записи** для ресинхронизации конфигураций, которые стали из синхронизования. **В конфигурации аварийного перехода на активный резервный ресурс выполнение команды write standby приводит к следующему:**

- При вводе команды **резерва записи** в системное поле выполнения конфигурация системы и конфигурации для всех контекстов безопасности на устройстве безопасности записаны в одноранговый модуль. Это включает сведения о конфигурации для контекстов безопасности, которые находятся в резервном состоянии. Необходимо ввести команду в системное поле выполнения на модуле, который имеет группу аварийного переключения 1 в активном состоянии.**Примечание:** Если существуют контексты безопасности в активном состоянии на одноранговом модуле, команда **резерва записи** заставляет активные соединения через те контексты быть завершенными. Используйте **команду failover active** на модуле, предоставляющем конфигурацию, чтобы удостовериться, что все контексты активны на том модуле прежде, чем ввести команду **резерва записи**.
- При вводе команды **резерва записи** в контекст безопасности только конфигурация для контекста безопасности записана в одноранговый модуль. Необходимо ввести команду в контекст безопасности на модуле, где контекст безопасности появляется в активном состоянии.

Реплицированные команды не сохраняются во флэш-памяти при репликации на вторичный узел. Они добавлены к рабочей конфигурации. **Чтобы сохранить реплицированные команды во флэш-память на обоих узлах, используйте команду write memory или copy running-config startup-config на том узле, на котором были выполнены изменения.** Команда реплицируется на вторичный узел и запускает сохранение конфигурации в его флэш-памяти.

Триггеры аварийного переключения

В конфигурации аварийного перехода на активный резервный ресурс переход на другой ресурс может быть запущен на уровне модуля в случае наступления одного из следующих событий:

- Модуль имеет отказ оборудования.
- Модуль имеет сбой питания.
- В модуле произошел сбой ПО.
- **Активный no failover** или **команда failover active** введен в системное поле выполнения.

Когда одно из этих событий имеет место, аварийное переключение инициировано на уровне группы аварийного переключения:

- Слишком много отслеживаемых интерфейсов в сбое группы.
- **No failover активная группа group_id** или **команда failover active group group_id** введен.

Действия аварийного переключения

В Конфигурации "активный-активный" аварийное переключение происходит на основе группы аварийного переключения, не системном основании. Например, если прописать использование обоих групп аварийного переключения в качестве активных на главном узле, и группа 1 станет сбойной, тогда группа 2 главного узла останется активной, в то время как группа 1 станет активной на вторичном узле.

Примечание: При настройке Активного/Активного аварийного переключения удостоверьтесь, что объединенный трафик для обоих модулей в емкости каждого модуля.

В следующей таблице приведены действия аварийного переключения для каждого нештатного события. Для каждого случая отказа приводятся политика (возникает или не возникает переход), действия для активной группы перехода и действия для резервной группы перехода.

Отказ	Policy	Активные действия группы	Действие резервной группы	Примечания
Модуль испытывает питание или сбой программного обеспечения	Failover	Станьте резервным Марком, как подведено	Переходит в ждущий режим. Активный модуль отмечается как отказавший	Когда модуль в паре аварийного переключения отказывает, любые активные группы аварийного переключения на том модуле отмечены, как подведено и стали активные на однорангово

				м модуле.
Отказ интерфейса на активной группе аварийного переключения выше порога	Failover	Маркируйте активную группу, как подведено	Становится активным	Нет
Отказ интерфейса на резервной группе аварийного переключения выше порога	Без переключения	Без действий	Резервная группа Марка, как подведено	Когда резервная группа аварийного переключения отмечена, как подведено, активная группа аварийного переключения не пытается переключиться при отказе, даже если превзойден порог отказа интерфейса.
Раньше активная группа аварийного переключения восстанавливается	Без переключения	Без действий	Без действий	Пока не настроено с **командой preempt**, группы аварийного переключения остаются активными на своем текущем модуле.
Сбой канала аварийного переключения при запуске	Без переключения	Становится активным	Становится активным	Если канал аварийного переключения не работает при запуске, обе группы аварийного

				переключения на обоих модулях 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.
Канал аварийного переключения отказал во время операции	Без переключения	н/д	н/д	Каждый модуль отмечает интерфейс аварийного переключения, как подведено. Необходимо восстановить канал аварийного переключения как можно скорее, потому что модуль не может переключиться при отказе к резервному модулю, в то время как канал аварийного переключения не работает.

Регулярное аварийное переключение и аварийное переключение с сохранением состояния

Устройство защиты поддерживает две конфигурации аварийного переключения: обычное 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 (когда это выполняется в режиме прозрачного межсетевого экрана),
- 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 вызов завершен, клиент IP SoftPhone теряет соединение с Call Manager. 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 Call Manager в течение некоторого периода времени, тогда для него Call Manager приобретает значение "Недоступный", после чего выполняется отмена регистрации.

Ограничения конфигурации аварийного переключения

Вы не можете настроить аварийное переключение с этими типами IP-адресов:

- IP-адреса получены через DHCP
- IP-адреса получены через PPPoE
- Адреса IPv6

Кроме того, эти ограничения применяются:

- Перехват управления при отказе с синхронизацией состояния не поддерживается на устройстве адаптивной безопасности ASA 5505.
- Конфигурация аварийного перехода на активный резервный ресурс не поддерживается на многофункциональных устройствах защиты серии ASA 5505.
- Когда Easy VPN Remote включен на устройстве адаптивной безопасности ASA 5505, вы не можете настроить аварийное переключение.
- Аварийное переключение VPN не поддерживается в многоконтекстном режиме.

Неподдерживаемые функции

Многоконтекстный режим не поддерживает следующие функции:

- Протоколы динамической маршрутизацииКонтексты безопасности поддерживают только статические маршруты. В многоконтекстном режиме нельзя активировать OSPF или RIP.
- VPN
- Групповая адресация

Основанная на кабеле Конфигурация "активный-активный"

Предварительные условия

Перед началом работы следует убедиться в следующем:

- Оба модуля имеют те же аппаратные средства, конфигурацию ПО и надлежащую лицензию.
- Оба модуля находятся в том же режиме (одиночные или множественны, прозрачны или маршрутизировавшие).

Схема сети

В настоящем документе используется следующая схема сети:

Выполните эти действия для настройки Активного/Активного аварийного переключения с помощью кабеля последовательного порта в качестве канала аварийного переключения. Команды в этой задаче введены в первичный модуль в паре аварийного переключения. Первичный модуль является модулем, который имеет конец кабеля, маркированного "Основной", включил его. Для устройств в многоконтекстном режиме команды введены в системное поле выполнения, если не указано иное.

При использовании кабельного аварийного переключения не нужно загружать вспомогательный модуль в паре аварийного переключения. Пусть вспомогательный модуль останется выключенным, пока мы не предложим включить его.

Примечание: Основанное на кабеле аварийное переключение только доступно на устройстве безопасности серии PIX 500.

Выполните эти шаги для настройки основанного на кабеле, Активного/Активного аварийного переключения:

1. Подключите кабель для аварийного переключения с устройствами безопасности серии PIX 500. Удостоверьтесь, что вы подключаете, конец кабеля отметил "Основной" к модулю, который вы используете в качестве первичного модуля, и что вы подключаете, конец кабеля отметил "Вторичный" к модулю, который вы используете в качестве вспомогательного модуля.
2. Включите первичный модуль.
3. Если эти действия еще не были выполнены, настройте активный и пассивный IP-адрес для каждого интерфейса передачи данных (с использованием маршрутизатора), для IP-адреса для управления (прозрачный режим), или для интерфейса только для управления. Резервный IP-адрес используется на устройстве защиты, которое в данный момент является резервным. Он должен находиться в той же подсети, что активный IP-адрес.Необходимо настроить интерфейсные адреса из каждого контекста. **Use the changeto context command to switch between contexts.** `The command prompt changes to hostname/context(config-if)#, where context is the name of the current context.` Вы должен ввести управление IP-адресами для каждого контекста в прозрачном многоконтекстном режиме межсетевого экрана.**Примечание:** Не выполняйте настройку IP-адреса для соединения аварийного переключения с отслеживанием состояния соединения в том случае, если используется выделенный интерфейс аварийного переключения с отслеживанием состояния. **Команда failover interface ip будет использована на одном из следующих шагов для настройки выделенного интерфейса аварийного переключения с отслеживанием состояния соединения.**`hostname/context(config-if)#` **`ip address`** *`active_addr`* **`netmask standby`** *`standby_addr`* В примере внешний интерфейс для context1 основного межсетевого экрана PIX настроен этот путь:`PIX1/context1(config)#` **`ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2`** Для контекста Context2:`PIX1/context2(config)#` **`ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2`** В маршрутизировавшем режиме межсетевого экрана и для интерфейса толька для управления, эта команда введена в режим конфигурации интерфейса для каждого интерфейса. В режиме прозрачного межсетевого экрана команда введена в режим глобальной конфигурации.
4. Чтобы активировать аварийное переключение с отслеживанием состояния, настройте соединение аварийного переключения.Задайте интерфейс, который будет использоваться в качестве ссылки Перехвата управления при отказе с синхронизацией состояния:`hostname(config)#` **`failover link`** *`if_name phy_if`* В этом примере для обмена данными о состоянии аварийного переключения с отслеживанием состояния через соединение используется интерфейс Ethernet2.`failover link stateful Ethernet2`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 соединения аварийного переключения).Назначьте активный и резервный IP-адреса соединению аварийного переключения:`hostname(config)#` **`failover interface ip`** *`if_name ip_addr`* **`mask standby`** *`ip_addr`* В данном примере, 10.0.0.1 используется, как

активное, и 10.0.0.2 используется в качестве резервного IP - адреса для ссылки перехвата управления при отказе с синхронизацией состояния.`PIX1(config)#`**`failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2`** Резервный IP-адрес должен быть в одной подсети с активным IP-адресом. Определять маску подсети резервного IP-адреса не нужно.IP-адрес ссылки Перехвата управления при отказе с синхронизацией состояния и MAC-адрес не изменяются в аварийном переключении за исключением того, когда Перехват управления при отказе с синхронизацией состояния использует интерфейс регулярных данных. Активный адрес IP всегда остается присвоенным главному узлу, в то время как пассивный адрес IP всегда останется присвоенным вторичному узлу.Включите интерфейс:`hostname(config)#`**`interface`** *`phy_if`* `hostname(config-if)#`**`no shutdown`**

5. Настройте группы аварийного переключения. У вас может быть самое большее две группы аварийного переключения. **Команда failover group** создает указанную группу аварийного переключения, если это не существует и вводит режим конфигурации группы аварийного переключения.Для каждой группы аварийного переключения необходимо задать, есть ли у группы аварийного переключения основное или вторичное предпочтение с помощью **основного** или **дополнительной команды**. Можно установить одинаковые параметры для обеих групп аварийного переключения. Для распределения нагрузки конфигураций необходимо назначить каждую группу аварийного переключения другое предпочтение модуля.Следующий пример назначает группу аварийного переключения 1 основное предпочтение и группа аварийного переключения 2 вторичное предпочтение:`hostname(config)#`**`failover group 1`** `hostname(config-fover-group)#`**`primary`** `hostname(config-fover-group)#`**`exit`** `hostname(config)#`**`failover group 2`** `hostname(config-fover-group)#`**`secondary`** `hostname(config-fover-group)#`**`exit`**
6. Назначьте каждый пользовательский контекст на группу аварийного переключения, использующую **команду join-failover-group** в режиме конфигурации контекста.Любые неназначенные контексты автоматически назначены на группу аварийного переключения 1. Контекст администратора всегда является участником группы аварийного переключения 1.Введите эти команды для присвоения каждого контекста на группу аварийного переключения:`hostname(config)#`**`context`** *`context_name`* `hostname(config-context)#`**`join-failover-group`** `{1 | 2}` `hostname(config-context)#`**`exit`**
7. Включите аварийное переключение:`hostname(config)#`**`failover`**
8. Включите вспомогательный модуль и включите аварийное переключение на модуле, если это уже не включено:`hostname(config)#`**`failover`** Активный модуль отправит конфигурацию в оперативной памяти в резервный модуль. Во время синхронизации конфигурации на консоли основного модуля появятся сообщения: Beginning configuration replication: При передаче разъему" и "Репликация конечной конфигурации для соединения" появляется на основной консоли.**Примечание:** Выполните команду **аварийного переключения** на основном устройстве сначала, и затем выполните его на дополнительном устройстве. **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.
9. Сохраните конфигурацию к флэш-памяти на Первичном модуле. Поскольку команды ввели в первичный модуль, реплицированы во вспомогательный модуль, вспомогательный модуль также сохраняет свою конфигурацию к флэш-

памяти.`hostname(config)#`**`copy running-config startup-config`**

10. Если необходимо, вынудите любую группу аварийного переключения, которая активна на основном к активному состоянию на вторичном устройстве. Чтобы вынудить группу аварийного переключения стать активной на вспомогательном модуле, выполните эту команду в системном поле выполнения на первичном модуле:`hostname#`**`no failover active group`** *`group_id`* Аргумент group_id указывает группу, которую требуется сделать активной на вторичном узле.

Конфигурации

Эти конфигурации используются в данном документе:

- PIX1 - System Configuration
- PIX1 - конфигурация Context1
- PIX1 - конфигурация Context2

PIX1 - System Configuration

```
PIX1#show running-config : Saved PIX Version 7.2(2)
<system> ! hostname PIX1 enable password
8Ry2YjIyt7RRXU24 encrypted no mac-address auto !---
Enable the physical and logical interfaces in the system
execution !--- space by giving "no shutdown" before
configuring the same in the contexts ! interface
Ethernet0 ! interface Ethernet0.1 vlan 2 ! interface
Ethernet0.2 vlan 4 ! interface Ethernet1 ! interface
Ethernet1.1 vlan 3 ! interface Ethernet1.2 vlan 5 ! !---
Configure "no shutdown" in the stateful failover
interface !--- of both Primary and secondary PIX.
interface Ethernet2 description STATE Failover Interface
! interface Ethernet3 shutdown ! interface Ethernet4
shutdown ! interface Ethernet5 shutdown ! class default
limit-resource All 0 limit-resource ASDM 5 limit-
resource SSH 5 limit-resource Telnet 5 ! ftp mode
passive pager lines 24 !--- Command to enable the
failover feature failover !--- Command to assign the
interface for stateful failover failover link stateful
Ethernet2 !--- Command to configure the active and
standby IP's for the !--- stateful failover failover
interface ip stateful 10.0.0.1 255.255.255.0 standby
10.0.0.2 !--- Configure the group 1 as primary failover
group 1 !--- Configure the group 1 as secondary failover
group 2 secondary no asdm history enable arp timeout
14400 console timeout 0 admin-context admin context
admin config-url flash:/admin.cfg ! !--- Command to
create a context called "context1" context context1 !---
Command to allocate the logical interfaces to the
contexts allocate-interface Ethernet0.1 inside_context1
allocate-interface Ethernet1.1 outside_context1 config-
url flash:/context1.cfg !--- Assign this context to the
failover group 1 join-failover-group 1 ! context
context2 allocate-interface Ethernet0.2 inside_context2
allocate-interface Ethernet1.2 outside_context2 config-
url flash:/context2.cfg join-failover-group 2 ! prompt
hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

PIX1 - конфигурация Context1

```
PIX1/context1(config)#show running-config : Saved : PIX
```

```
Version 7.2(2) <context> ! hostname context1 enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
inside_context1 nameif inside security-level 100 !---
Configure the active and standby IP's for the logical
inside !--- interface of the context1. ip address
192.168.1.1 255.255.255.0 standby 192.168.1.2 !
interface outside_context1 nameif outside security-level
0 !--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2 !
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100
extended permit tcp any host 172.16.1.1 eq www pager
lines 24 mtu inside 1500 mtu outside 1500 monitor-
interface inside monitor-interface outside icmp
unreachable rate-limit 1 burst-size 1 no asdm history
enable arp timeout 14400 static (inside,outside)
172.16.1.1 192.168.1.5 netmask 255.255.255.255 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 telnet timeout 5 ssh timeout 5 !
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
Cryptochecksum:00000000000000000000000000000000 : end
```

PIX1 - конфигурация Context2

```
PIX1/context2(config)#show running-config : Saved : PIX
Version 7.2(2) <context> ! hostname context2 enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
inside_context2 nameif inside security-level 100 !---
Configure the active and standby IP's for the logical
inside !--- interface of the context2. ip address
192.168.2.1 255.255.255.0 standby 192.168.2.2 !
interface outside_context2 nameif outside security-level
0 !--- Configure the active and standby IP's for the
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2 !
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100
extended permit tcp any host 172.16.2.1 eq www pager
lines 24 mtu inside 1500 mtu outside 1500 monitor-
interface inside monitor-interface outside icmp
unreachable rate-limit 1 burst-size 1 no asdm history
enable arp timeout 14400 static (inside,outside)
172.16.2.1 192.168.2.5 netmask 255.255.255.255 access-
group 100 in interface outside route outside 0.0.0.0
0.0.0.0 172.16.2.3 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 telnet timeout 5 ssh timeout 5 !
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
Cryptochecksum:00000000000000000000000000000000 : end
```

Основанная на LAN Конфигурация "активный-активный"

Схема сети

В настоящем документе используется следующая схема сети:

В этом разделе описывается настроить Активное/Активное аварийное переключение с помощью канала аварийного переключения Ethernet. При настройке основанного на LAN аварийного переключения необходимо загрузить дополнительное устройство для распознавания канала аварийного переключения, прежде чем дополнительное устройство сможет получить рабочую конфигурацию из основного устройства.

Примечание: Вместо того, чтобы использовать перекрестный кабель Ethernet для прямого соединения модулей Cisco рекомендует использовать специализированный коммутатор между основным и вспомогательными модулями.

Этот раздел включает темы как показано:

- Настройка основного модуля
- Конфигурация вспомогательного модуля

Настройка основного модуля

Выполните эти шаги для настройки первичного модуля в Конфигурации "активный-активный":

1. Если эти действия еще не были выполнены, настройте активный и пассивный IP-адрес для каждого интерфейса передачи данных (с использованием маршрутизатора), для IP-адреса для управления (прозрачный режим), или для интерфейса только для управления. Резервный IP-адрес используется на устройстве защиты, которое в данный момент является резервным. Он должен находиться в той же подсети, что активный IP-адрес.Необходимо настроить интерфейсные адреса из каждого контекста. **Используйте команду changeto context, чтобы переключаться между контекстами**. Командная строка принимает значение вида hostname/context(config-if)#, где context — имя текущего контекста. В режиме прозрачного межсетевого экрана необходимо ввести IP-адрес для управления для каждого контекста.**Примечание:** Не выполняйте настройку IP-адреса для соединения аварийного переключения с отслеживанием состояния соединения в том случае, если используется выделенный интерфейс аварийного переключения с отслеживанием состояния. **Команда failover interface ip будет использована на одном из следующих шагов для настройки выделенного интерфейса аварийного переключения с отслеживанием состояния**

соединения.`hostname/context(config-if)#` **`ip address`** *`active_addr`* **`netmask standby`** *`standby_addr`* В примере внешний интерфейс для context1 основного межсетевого экрана PIX настроен этот путь:`PIX1/context1(config)#` **`ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2`** Для контекста Context2:`PIX1/context2(config)#` **`ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2`** В маршрутизировавшем режиме межсетевого экрана и для интерфейса толька для управления, эта команда введена в режим конфигурации интерфейса для каждого интерфейса. В режиме прозрачного межсетевого экрана команда введена в режим глобальной конфигурации.

2. Настройте основные параметры аварийного переключения, используя системное пространство "Выполнить".(Только устройство безопасности PIX), Включают основанное на LAN аварийное переключение:`hostname(config)#` **`failover lan enable`** Назначьте этот модуль основным:`hostname(config)#` **`failover lan unit primary`** Задайте канал аварийного переключения:`hostname(config)#` **`failover lan interface`** *`if_name phy_if`* В данном примере мы используем интерфейс "Ethernet" 3, поскольку LAN базировала интерфейс аварийного переключения.`PIX1(config)#` **`failover lan interface LANFailover 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. На устройстве адаптивной безопасности ASA 5505 phy_if задает VLAN. Этот интерфейс не должен использоваться ни для какой другой цели (кроме, дополнительно, ссылка Перехвата управления при отказе с синхронизацией состояния).Задайте активный канал аварийного переключения и резервные IP - адреса:`hostname(config)#` **`failover interface ip`** *`if_name ip_addr`* **`mask standby`** *`ip_addr`* В данном примере адрес 10.1.0.1 используется в качестве активного, а 10.1.0.2 используется в качестве пассивного IP-адреса для настройки интерфейсов аварийного переключения.`PIX1(config)#` **`failover interface ip LANFailover 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. Определять маску подсети резервного IP-адреса не нужно. IP-адрес и MAC-адрес соединения не меняются при аварийном переключении. Активный адрес IP всегда остается присвоенным главному узлу, в то время как пассивный адрес IP всегда останется присвоенным вторичному узлу.
3. Чтобы включить переход на другой ресурс при сбое с отслеживанием состояния соединений, следует настроить ссылку перехода на другой ресурс:Задайте интерфейс, который будет использоваться в качестве ссылки Перехвата управления при отказе с синхронизацией состояния:`hostname(config)#` **`failover link`** *`if_name phy_if`* `PIX1(config)#` **`failover link stateful ethernet2`** 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 соединения аварийного переключения).**Примечание:** Если ссылка Перехвата управления при отказе с синхронизацией состояния использует канал аварийного переключения или интерфейс регулярных данных, то только необходимо предоставить if_name аргумент.Назначьте активный и резервный IP-адреса соединению аварийного переключения.**Примечание:** Если ссылка Перехвата управления при отказе с синхронизацией состояния использует канал аварийного переключения или интерфейс регулярных 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* PIX1(config)#**failover interface ip stateful 10.0.0.1 255.255.255.0 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. IP-адрес ссылки состояния и MAC-адрес не изменяются в аварийном переключении. Активный адрес IP всегда остается присвоенным главному узлу, в то время как пассивный адрес IP всегда останется присвоенным вторичному узлу.Включите интерфейс.**Примечание:** Если ссылка Перехвата управления при отказе с синхронизацией состояния использует канал аварийного переключения или интерфейс регулярных данных, пропустите этот шаг. Включение интерфейса было уже выполнено.hostname(config)#**interface** *phy_if* hostname(config-if)#**no shutdown**

4. Настройте группы аварийного переключения. У вас может быть самое большее две группы аварийного переключения. **Команда failover group** создает указанную группу аварийного переключения, если это не существует и вводит режим конфигурации группы аварийного переключения.Для каждой группы аварийного переключения задайте, есть ли у группы аварийного переключения **основное** или **вторичное** предпочтение с помощью основного или дополнительной команды. Можно установить одинаковые параметры для обеих групп аварийного переключения. Для распределения нагрузки конфигураций необходимо назначить каждую группу аварийного переключения другое предпочтение модуля.Следующий пример назначает группу аварийного переключения 1 основное предпочтение и группа аварийного переключения 2 вторичное предпочтение:hostname(config)#**failover group 1** hostname(config-fover-group)#**primary** hostname(config-fover-group)#**exit** hostname(config)#**failover group 2** hostname(config-fover-group)#**secondary** hostname(config-fover-group)#**exit**
5. Назначьте каждый пользовательский контекст на группу аварийного переключения, использующую **команду join-failover-group** в режиме конфигурации контекста.Любые неназначенные контексты автоматически назначены на группу аварийного переключения 1. Контекст администратора всегда является участником группы аварийного переключения 1.Введите эти команды для присвоения каждого контекста на группу аварийного переключения:hostname(config)#**context** *context_name* hostname(config-context)#**join-failover-group** {1 | 2} hostname(config-context)#**exit**
6. Включите аварийное переключение.hostname(config)#**failover**

Конфигурация вспомогательного модуля

При настройке основанного на LAN Активного/Активного аварийного переключения необходимо загрузить вспомогательный модуль для распознавания канала аварийного переключения. Это позволит вторичному узлу взаимодействовать и получать рабочие настройки от основного узла.

Выполните эти шаги для начальной загрузки вспомогательного модуля в Конфигурации "активный-активный":

1. (Только устройство безопасности PIX), Включают основанное на LAN аварийное переключение.hostname(config)#**failover lan enable**
2. Задайте интерфейс аварийного переключения. Используйте те же параметры настройки, как вы использовали для первичного модуля:Задайте интерфейс, который будет использоваться в качестве интерфейса аварийного переключения.hostname(config)#**failover lan interface** *if_name phy_if* PIX1(config)#failover lan interface LANFailover ethernet3Параметр 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. На устройстве адаптивной безопасности ASA 5505 phy_if задает VLAN.Назначьте активный и резервный IP-адреса соединению аварийного переключения:`hostname(config)#`**`failover interface ip`** *`if_name ip_addr`* **`mask standby`** *`ip_addr`* `PIX1(config)#`**`failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2`** **Примечание:** Введите эту команду точно, как вы ввели ее в первичный модуль при настройке интерфейса аварийного переключения.Резервный IP-адрес должен быть в одной подсети с активным IP-адресом. Не требуется указывать маску подсети для пассивного адреса.Включите интерфейс.`hostname(config)#`**`interface`** *`phy_if`* `hostname(config-if)#`**`no shutdown`**

3. Определяйте этот модуль как вспомогательный модуль:`hostname(config)#`**`failover lan unit secondary`** **Примечание:** Этот шаг является дополнительным, потому что модулями по умолчанию определяются как вторичный, пока ранее не настроено иначе.
4. Включите аварийное переключение.`hostname(config)#`**`failover`** 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".Примечание:** Выполните команду **аварийного переключения** на основном устройстве сначала, и затем выполните его на дополнительном устройстве. **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.
5. После того, как рабочая конфигурация завершила репликацию, введите эту команду для сохранения конфигурации к флэш-памяти:`hostname(config)#`**`copy running-config startup-config`**
6. Если необходимо, вынудите любую группу аварийного переключения, которая активна на основном к активному состоянию на вспомогательном модуле. Чтобы вынудить группу аварийного переключения стать активной на вспомогательном модуле, введите эту команду в системное поле выполнения на первичном модуле:`hostname#`**`no failover active group group_id`** Аргумент group_id указывает группу, которую требуется сделать активной на вторичном узле.

Конфигурации

Эти конфигурации используются в данном документе:

Primary PIX

```
PIX1(config)#show running-config : Saved : PIX Version
7.2(2) <system> ! hostname PIX1 enable password
8Ry2YjIyt7RRXU24 encrypted no mac-address auto !
interface Ethernet0 ! interface Ethernet0.1 vlan 2 !
interface Ethernet0.2 vlan 4 ! interface Ethernet1 !
interface Ethernet1.1 vlan 3 ! interface Ethernet1.2
vlan 5 ! !--- Configure "no shutdown" in the stateful
failover interface as well as !--- LAN Failover
interface of both Primary and secondary PIX/ASA.
interface Ethernet2 description STATE Failover Interface
```

```
! interface Ethernet3 description LAN Failover Interface
! interface Ethernet4 shutdown ! interface Ethernet5
shutdown ! class default limit-resource All 0 limit-
resource ASDM 5 limit-resource SSH 5 limit-resource
Telnet 5 ! ftp mode passive pager lines 24 failover
failover lan unit primary !--- Command to assign the
interface for LAN based failover failover lan interface
LANFailover Ethernet3 !--- Command to enable the LAN
based failover failover lan enable !--- Configure the
Authentication/Encryption key failover key *****
failover link stateful Ethernet2 !--- Configure the
active and standby IP's for the LAN based failover
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2 failover interface ip stateful 10.0.0.1
255.255.255.0 standby 10.0.0.2 failover group 1 failover
group 2 secondary no asdm history enable arp timeout
14400 console timeout 0 admin-context admin context
admin config-url flash:/admin.cfg ! context context1
allocate-interface Ethernet0.1 inside_context1 allocate-
interface Ethernet1.1 outside_context1 config-url
flash:/context1.cfg join-failover-group 1 ! context
context2 allocate-interface Ethernet0.2 inside_context2
allocate-interface Ethernet1.2 outside_context2 config-
url flash:/context2.cfg join-failover-group 2 ! prompt
hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

Примечание: Обратитесь Кабель базировал раздел Конфигурации аварийного переключения, PIX1 - Конфигурацию Context1 и PIX1 - Конфигурация Context2 для конфигурации контекста в LAN базировала сценарий аварийного переключения.

Вспомогательный модуль PIX

```
PIX2#show running-config failover failover lan unit
secondary failover lan interface LANFailover Ethernet3
failover lan enable failover key ***** failover
interface ip LANFailover 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.

Primary PIX

```
PIX1(config-subif)#show failover Failover On Cable status: N/A - LAN-based failover enabled
Failover unit Primary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15
seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface
Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(2), Mate 7.2(2) Group 1 last
failover at: 06:12:45 UTC Apr 16 2007 Group 2 last failover at: 06:12:43 UTC Apr 16 2007 This
host: Primary Group 1 State: Active Active time: 359610 (sec) Group 2 State: Standby Ready
Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal context1 Interface
outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal context2 Interface
outside (172.16.2.2): Normal Other host: Secondary Group 1 State: Standby Ready Active time: 0
(sec) Group 2 State: Active Active time: 3900 (sec) context1 Interface inside (192.168.1.2):
```

```
Normal context1 Interface outside (172.16.1.2): Normal context2 Interface inside (192.168.2.1):
Normal context2 Interface outside (172.16.2.1): Normal Stateful Failover Logical Update
Statistics Link : stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 48044 0 48040
1 sys cmd 48042 0 48040 1 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 2 0 0 0 Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1
72081 Xmit Q: 0 1 48044
```

Вспомогательный модуль PIX

```
PIX1(config)#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover
unit Secondary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15
seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface
Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(2), Mate 7.2(2) Group 1 last
failover at: 06:12:46 UTC Apr 16 2007 Group 2 last failover at: 06:12:41 UTC Apr 16 2007 This
host: Secondary Group 1 State: Standby Ready Active time: 0 (sec) Group 2 State: Active Active
time: 3975 (sec) context1 Interface inside (192.168.1.2): Normal context1 Interface outside
(172.16.1.2): Normal context2 Interface inside (192.168.2.1): Normal context2 Interface outside
(172.16.2.1): Normal Other host: Primary Group 1 State: Active Active time: 359685 (sec) Group 2
State: Standby Ready Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal
context1 Interface outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal
context2 Interface outside (172.16.2.2): Normal Stateful Failover Logical Update Statistics Link
: stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 940 0 942 2 sys cmd 940 0 940
2 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 2 0
Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1 1419 Xmit Q: 0
1 940
```

Для проверки состояния используйте команду show failover state.

Primary PIX

```
PIX1(config)#show failover state State Last Failure Reason Date/Time This host - Primary Group 1
Active None Group 2 Standby Ready None Other host - Secondary Group 1 Standby Ready None Group 2
Active None ====Configuration State=== Sync Done ====Communication State=== Mac set
```

Вторичный узел

```
PIX1(config)#show failover state State Last Failure Reason Date/Time This host - Secondary Group
1 Standby Ready None Group 2 Active None Other host - Primary Group 1 Active None Group 2
Standby Ready None ====Configuration State=== Sync Done - STANDBY ====Communication State=== Mac
set
```

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

Основной модуль

```
PIX1(config)#show failover interface interface stateful Ethernet2 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 interface LANFailover
Ethernet3 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
```

Вторичный узел

```
PIX1(config)#show failover interface interface LANFailover Ethernet3 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 stateful Ethernet2
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:

`show monitor-interface.` `show monitor-interface .`

Примечание: Для включения контроля исправности на определенном интерфейсе используйте команду monitor-interface в режиме глобальной конфигурации:

monitor-interface <*if_name*>

Primary PIX

```
PIX1/context1(config)#show monitor-interface This host: Secondary - Active Interface inside
(192.168.1.1): Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby
Ready Interface inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal
```

Вспомогательный модуль PIX

```
PIX1/context1(config)#show monitor-interface This host: Secondary - Standby Ready Interface
inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Secondary -
Active Interface inside (192.168.1.1): Normal Interface outside (172.16.1.1): Normal
```

Примечание: Если вы не вводите IP-адрес аварийного переключения, **команда show failover** отображается 0.0.0.0 для IP-адреса, и мониторинг интерфейсов остается в состоянии "ожидание". Необходимо заставить адрес IP аварийного переключения для аварийного переключения работать. Для получения дополнительной информации о других состояниях для аварийного переключения, обратитесь для показа аварийного переключения.

По умолчанию мониторинг физических интерфейсов включен, и мониторинг подинтерфейсов отключен.

Отображение команд аварийного переключения в текущей конфигурации

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

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

Будут выведены все команды, связанные с аварийным переключением. , , `show running-config failover` . Введите **команду show running-config all failover**, чтобы отобразить команды аварийного переключения в рабочей конфигурации и включать команды, для которых вы не изменили значение по умолчанию.

Проверка функциональности аварийного переключения

Для тестирования функциональности аварийного переключения выполните эти шаги:

1. Протестируйте активный модуль или группу аварийного переключения и убедитесь, что они пропускают трафик, как это ожидается для FTP (например), послав файл с одного хоста на другой с различными интерфейсами.
2. Вызовите аварийное переключение на резервный модуль с помощью следующей команды:Для Активного/Активного аварийного переключения введите следующую команду в модуль, где группа аварийного переключения, содержащая интерфейс, подключающий ваши хосты, активна:`hostname(config)#`**`no failover active group`** *`group_id`*
3. Используйте FTP для передачи другого файла между теми же двумя узлами.
4. Если тест не был успешен, введите **команду show failover** для проверки статуса аварийного переключения.
5. После завершения проверки можно восстановить активный статус модуля или группы аварийного переключения с помощью следующей команды:Для Активного/Активного аварийного переключения введите следующую команду в модуль, где группа аварийного переключения, содержащая интерфейс, подключающий ваши хосты, активна:`hostname(config)#`**`failover active group`** *`group_id`*

Принудительное аварийное переключение

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

Введите эту команду в системное поле выполнения модуля, где группа аварийного переключения находится в резервном состоянии:

```
hostname#failover active group group_id
```

Или, введите эту команду в системное поле выполнения модуля, где группа аварийного переключения находится в активном состоянии:

```
hostname#no failover active group group_id
```

Ввод этой команды в системном поле выполнения заставляет все группы аварийного переключения становиться активными:

```
hostname#failover active
```

Отключение аварийного переключения

Чтобы отключить аварийное переключение, введите команду:

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

Если отключить аварийное переключение на паре "активный/резервный", 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. Для создания резервного модуля активным (даже с аварийным переключением отключенный), посмотрите Принудительный раздел Аварийного переключения.

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

Для восстановления отказавшей Активной/Активной группы аварийного переключения к неотказавшему состоянию введите эту команду:

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

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 аварийного переключения, 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.**

Замените неисправный модуль новым модулем

Выполните эти шаги для замены неисправного модуля новым модулем:

1. Выполните команду **no failover** на первичном модуле.Статус вспомогательного модуля показывает **резервный модуль как не обнаруженный**.
2. Отключите первичный модуль и подключите заменяющий первичный модуль.
3. Проверьте, что сменный модуль выполняет то же программное обеспечение и версию ASDM как вспомогательный модуль.
4. Выполните эти команды на сменном модуле:
   ```
   ASA(config)#failover lan unit primary ASA(config)#failover lan interface failover Ethernet3
   ASA(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
   ASA(config)#interface Ethernet3 ASA(config-if)#no shut ASA(config-if)#exit
   ```
5. Включите заменяющий первичный модуль к сети и выполните эту команду:`ASA(config)#failover`

Устранение неполадок

При аварийном переключении оба устройства защиты отправляют системные сообщения. В этом разделе рассматриваются следующие темы:

1. Сообщения системы аварийного переключения
2. Сообщения отладки
3. SNMP

Сообщения системы аварийного переключения

Устройство защиты 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.

Основные Потерянные Связи аварийных переключений с разъемом на интерфейсе interface_name

Если один модуль пары аварийного переключения больше не может связываться с другим модулем пары, это сообщение об аварийном переключении отображено. Primary (Основной) может также быть заменено на Secondary (Вспомогательный) для вспомогательного устройства.

(Основные) Потерянные Связи аварийных переключений с разъемом на интерфейсе interface_name

Проверьте, что сеть, которая связана с заданным интерфейсом, функционирует правильно.

Сообщения отладки

Для просмотра сообщений отладки введите команду debug fover. См. Справочник по командам Cisco Security Appliance, Версия 7.2 для получения дополнительной информации.

Примечание: Поскольку вывод отладки является назначенным высоким приоритетом в Процессе ЦПУ, это может решительно влиять на производительность системы. **Поэтому используйте команды debug fover только для устранения определенных проблем или во время сеансов устранения проблем при участии специалистов технической поддержки 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. См. **snmp-server** и команды **регистрации** в Справочнике по командам Cisco Security Appliance, Версия 7.2 для получения дополнительной информации.

Последовательный опрос при обработке отказов

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

```
failover polltime unit msec [time]              .

 failover holdtime unit msec [time]    ,            .       .
```

См. время последовательного опроса при аварийном переключении для получения дополнительной информации.

% Warning: Сбой описания сообщения аварийного переключения.

:

```
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.

Дополнительные сведения

- Страница поддержки маршрутизаторов Cisco PIX серии 500
- Модуль сервисов межсетевого экрана (FWSM) конфигурация аварийного переключения
- Устранение неисправностей восстановления после отказа FWSM
- Как аварийное переключение работает на сетевого экранах Cisco Secure PIX
- Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация