ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс CSP VPN Gate. Версия 3.11

Руководство администратора

Использование RRI

РЛКЕ.00005-02 90 03

20.04.2012

Содержание

Использование RRI

RRI (Reverse Route Injection) – это новый механизм связи управления топологией VPN и системой маршрутизации, позволяющий маршрутам к удаленным защищенным подсетям и клиентам, автоматически принимать участие в процессе маршрутизации.

Смысл механизма RRI состоит в том, что после создания защищенного соединения IPsec SA, в таблицу маршрутизации CSP VPN Gate с включенным RRI автоматически вносится запись о маршруте к удаленной сети партнера или клиенту. При нарушении защищенного соединения добавленный маршрут из таблицы маршрутизации шлюза удаляется.

Механизм RRI может использоваться в сетях большого размера для обеспечения надежности – в схемах резервирования с балансировкой сетевой нагрузки.

Для оповещения соседних сетевых устройств, стоящих за CSP VPN Gate, о доступных ему хостах, сетях, новых маршрутах, соответствующих изменениям в топологии VPN, используются протоколы динамической маршрутизации, например, RIP. Такие протоколы маршрутизации реализованы в пакете программ Quagga.

Рассмотрим пример использования механизма RRI в сети, изображенной на Рисунок 1. Подсеть Lan2 защищена шлюзом безопасности GW3, а подсеть Lan1 – двумя шлюзами безопасности GW1 и GW2, включенными в схему резервирования с распределением нагрузки, т.е. доступ в подсеть Lan1 можно получить либо через шлюз GW1, либо через шлюз GW2. Оба канала работают. На шлюзах безопасности установлен продукт CSP VPN Gate 3.11, на GW1 и GW2 включен RRI. В сеть включены маршрутизаторы Cisco. После создания IPsec SA между шлюзами GW3 и GW1, в таблицу маршрутизации GW1 добавляется запись о маршруте до сети Lan2 (обратный маршрут).

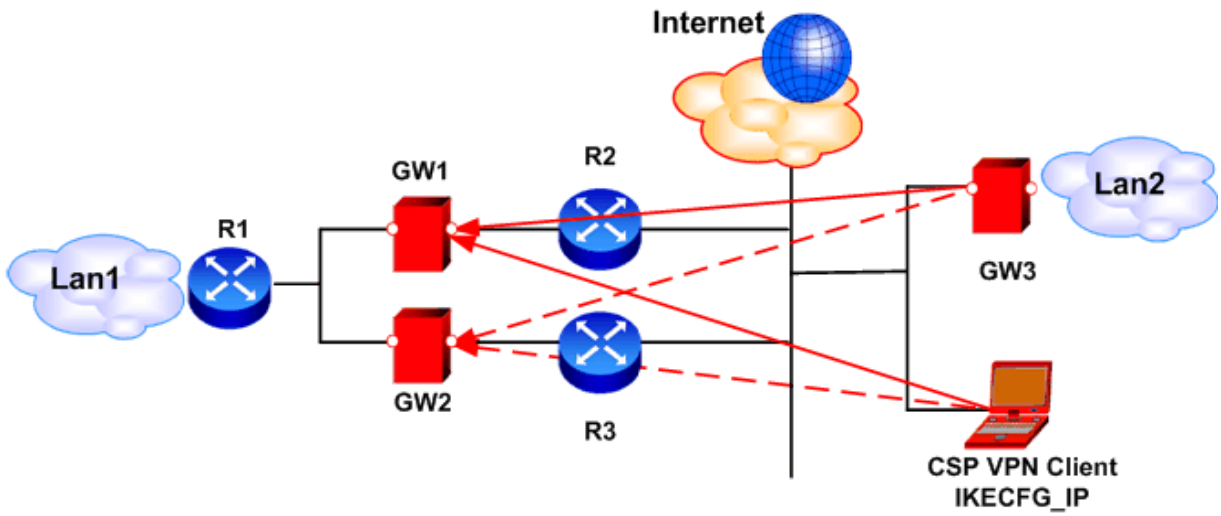

Рисунок 1

При нарушении установленного защищенного соединения (GW3 – GW1), запись об обратном маршруте в таблице маршрутизации шлюза GW1 удаляется. В случае, если соединение от шлюза GW3 будет перестроено на шлюз безопасности GW2, то в таблицу маршрутизации шлюза GW2 будет добавлен маршрут к сети Lan2.

Для обмена маршрутной информацией с маршрутизатором R1, на сетевых интерфейсах шлюзов GW1 и GW2, через которые происходит соединение с R1, нужно включить протокол RIP. Демоны RIP на шлюзах нужно настроить таким образом, чтобы они только передавали информацию о маршрутах соседним устройствам, но не добавляли маршруты, полученные от соседних устройств в свою таблицу маршрутизации. Маршрут до подсети Lan2, посланный по протоколу RIP шлюзом GW1, должен добавиться в таблицу маршрутизации R1, но не

добавиться в таблицу маршрутизации GW2, и наоборот. Эти сведения используются сетевым устройством R1 для динамического перенаправления сетевого трафика.

В случае с мобильным пользователем – на основании предъявленного им сертификата и запроса, шлюз GW1 выдает ему адрес из IKECFG пула. После создания защищенного соединения, на шлюзе GW1 в таблицу маршрутизации вносится запись о маршруте до мобильного клиента, о чем по протоколу динамической маршрутизации уведомляется маршрутизатор R1. Если мобильный клиент построит сначала соединение с GW1, а затем – с GW2, то это приведет к появлению двух маршрутов до мобильного клиента на маршрутизаторе R1. Такая ситуация может быть разрешена стандартными средствами DPD. При разрыве соединения шлюз GW1 оповещает R1, что адрес, выданный из пула, ему более недоступен.

Примечание:

При физическом обрыве связи между шлюзом GW1 и маршрутизатором R2 (next hop), шлюз безопасности GW1 не может, используя DPD (Dead Peer Detection), обнаружить разрыв соединения с шлюзом GW3 (или с клиентом), так как сессия DPD запускается только при отправке исходящего пакета. А исходящий пакет не отправляется, так как ОС не может найти куда его отправить, потому что маршрутизатор R2 на arp запрос не отвечает и GW1 не может получить MAC-адрес устройства R2.

Поэтому могут возникать проблемы с переключением с GW1 на GW2 при физическом обрыве связи между шлюзом GW1 и маршрутизатором R2 (next hop). SA умрет только по истечению времени жизни и после этого из таблицы маршрутзации GW1 будет удален маршрут в подсеть Lan2 (или до мобильного клиента) и об этом будет уведомлен маршрутизатор R1. Для решения этой проблемы можно необходимую запись в arp-таблице сделать статической, добавьте на GW1 запись в arp-таблицу:

```
arp –s <IP_address_R2> <mac_address_R2>
```

Аналогично, добавьте на шлюз GW2 запись в arp-таблицу:

```
arp –s <IP_address_R3> <mac_address_R3>
```

Пример сценария, в котором используется RRI, приведен на сайте в разделе «Поддержка – Типовые сценарии» (http://www.s-terra.com/documents/scenario_t/Scen14_key.pdf).

Включение механизма RRI на CSP VPN Gate

При создании политики безопасности посредством командной строки включение механизма RRI производится в режиме конфигурирования криптокарты командой:

```
reverse-route
```

В конфигурационном файле для включения RRI в структуре `IPsecAction` необходимо атрибуту `ReverseRoute` присвоить значение `TRUE`.

Краткое описание продукта Quagga

Продукт Quagga входит в комплект поставки ПК «CSP VPN Gate» и инсталлирован на нем.

Quagga состоит из пакета программ, реализующих протоколы динамической маршрутизации, основанных на TCP/IP – RIPv1, RIPv2, OSPFv2, OSPFv3, BGPv4. Для работы с CSP VPN Gate используется только протокол RIPv2, тестирование с другими протоколами не проводилось. Дальнейшее описание работы с Quagga касается только протокола RIPv2.

Quagga состоит из нескольких демонов, каждый из которых поддерживает свой протокол маршрутизации. Одновременно работать могут несколько разных демонов в сообществе с управляющим демоном zebra.

- zebra – демон управления процессом маршрутизации. Он обеспечивает взаимодействие между демонами маршрутизации и операционной системой. Демоны маршрутизации получают/устанавливают записи из таблицы маршрутизации через zebra
- ripd – демон маршрутизации, поддерживающий работу протоколов RIPv1 (RFC1058), RIPv2 (RFC2453).

Каждый демон имеет свою консоль конфигурирования, доступную посредством протокола ***telnet***:

```
zebra:        telnet 127.0.0.1 2601
ripd:         telnet 127.0.0.1 2602.
```

Работа через консоль защищена паролем, который нужно задать в конфигурационном файле каждого из демонов (если пароль в конфигурационном файле не задан или конфигурационный файл отсутствует, то работа через консоль невозможна). Адрес и порт, по которым будут доступны демоны, задаются при запуске демонов (в нашем случае они соответствуют вышеуказанным, то есть извне недоступны).

Более подробную информацию о продукте и его настройке можно смотреть в Интернете (например, http://www.quagga.net/docs/quagga.html или http://www.opennet.ru/base/net/zebra_doc.txt.html).

Настройка Quagga для передачи маршрута посредством протокола RIPv2

Продукт Quagga поставляется без конфигурационных файлов.

Сначала необходимо создать конфигурационные файлы демонов zebra и ripd, разместив их в зависимости от ОС по следующим путям:

```
zebra.conf
     ОС RHEL 5:          /etc/quagga/zebra.conf


ripd.conf
     ОС RHEL 5:          /etc/quagga/ripd.conf
```

Примеры конфигурационных файлов демонов размещены в следующих каталогах:

```
zebra.conf.sample
```



```
    ОС RHEL 5:          /etc/quagga/zebra.conf.sample

ripd.conf.sample
    ОС RHEL 5:          /etc/quagga/ripd.conf.sample
```

Рекомендуемый шаблон конфигурационного файла для демона ripd

```
! -*- rip -*-
!
! RIPd template configuration file
!
hostname ripd
password <пароль для входа в консоль управления>
enable password <пароль для входа в привилегированный режим консоли управления>
!
!
router rip
 version 2
 redistribute kernel
 network <имя сетевого интерфейса, на котором включается RIP>
!
! фильтрация исходящих и входящих пакетов RIP (маршрутов RIP) на
! интерфейсе при помощи списков доступа
!
 distribute-list acl-in in
 distribute-list acl-out out
!
!
access-list acl-in deny any
access-list acl-out permit <адреса, до которых интересны изменения маршрутов>
access-list acl-out deny any
!
```

Обратите внимание на команду ***access-list acl-in deny any*** – она запрещает получать информацию о маршрутах от других устройств, шлюз должен только передавать информацию о маршрутах другим сетевым устройствам.

В некоторых случаях ***access-list acl-out*** удобнее задавать так:

```
access-list acl-out deny <адреса, до которых не интересны изменения маршрутов>
access-list acl-out permit any
```


Рекомендуется настроить аутентификацию устройств, работающих по протоколу RIPv2 (см. документацию на Quagga).

Для работы демона `ripd` требуется запущенный демон zebra.

В **ОС RHEL 5** запуск или остановка демона осуществляются скриптом:

```
/etc/init.d/zebra {start|stop}
/etc/init.d/ripd {start|stop}.
```

Для активизации RIPv2 при загрузке ОС выполните команды:

```
chkconfig zebra on
chkconfig ripd on
```

Настройка cisco-маршрутизатора

Для того, чтобы маршутизатор воспринимал посылаемые продуктом Quagga маршруты по протоколу RIPv2, достаточно добавить в его конфигурацию строки:

```
!
router rip
 version 2
 network <подсеть сетевого интерфейса для CISCO RIP>
!
```

Особенности реализации RRI

После построения IPsec SA, на CSP VPN Gate (при включенном RRI) вычисляется обратный маршрут (RR), который вносится в таблицу маршрутизации. Основанием для такого маршрута являются следующие данные:

селектор SA (ID второй фазы IKE)

адрес назначения туннельного заголовка SA (tdst)

системная таблица маршрутизации (без учета маршрутов, добавленных подсистемой RRI).

Вычисление маршрута:

ID партнера[1] второй фазы IKE преобразуется в адрес и маску подсети. Полученные адрес и маска будут адресом назначения создаваемого RR. Если ID имеет протоколы и/или порты, содержит произвольный диапазон адресов, которые невозможно преобразовать в адрес и маску подсети, то обратный маршрут не создается.

В системной таблице производится поиск туннельного адреса SA.

Если правил не найдено (“Destination Unreachable”), RR не добавляется.

Если найдено правило прямой маршрутизации через интерфейс, вычисленный маршрут будет через gateway tdst.

Если найдено правило прямой маршрутизации через gateway GW, вычисленный маршрут будет через gateway GW.

Если маршрут успешно вычислен, проверяется следующее:

Такой же маршрут был ранее добавлен подсистемой RRI для SA с тем же tdst. В этом случае увеличивается счетчик ссылок, маршрут не добавляется.

Маршрут для SA с такими же ID второй фазы и tdst уже добавлен, но отличается. В этом случае существующий маршрут обновляется, увеличивается счетчик ссылок.

Маршрут с такими же параметрами уже добавлен, но для SA с другим tdst. Маршрут не создается, счетчик ссылок не увеличивается.

Маршрут, соответствующий ID партнера есть в системной таблице, но подсистемой RRI он не добавлялся. В этом случае маршрут не создается.

При удалении SA из ядра, счетчик ссылок соответствущего маршрута уменьшается, при обнулении счетчика маршрут удаляется.

В случае аварийного завершения работы сервиса vpnsvc маршруты, добавленные RRI в таблицу маршрутизации, будут удалены.

Предупреждение: недопустимо вручную изменять или удалять правила маршрутизации, которые автоматически формируются при использовании RRI.

В Таблице 1 приведены некоторые возможные конфликтные ситуации.

[1] Поскольку протокол в ID второй фазы один для обоих партнеров, а порты без указания протокола смысла не имеют, присутствие портов и протоколов с обоих сторон не допускается.

Таблица 1

N	Ситуация	Поведение продукта	Отличие в поведении в Cisco IOS
1	Строится IPsec SA, при этом ID партнера второй фазы IKE не является подсетью (содержит диапазон IP-адресов, порты и/или протоколы).	Маршрут RR не добавляется и выдается предупреждение в файл лога 1.2	Диапазоны адресов в Cisco IOS также не поддерживаются. При наличии портов, протоколов в ID партнера в Cisco IOS маршрут создается.
2	Имеется построенный IPsec SA и в таблицу внесен вычисленный RR по нему. Строится другой IPsec SA и по нему также вычисляется RR. Оба IPsec SA имеют разные локальные ID, но одинаковые ID партнеров. Если при этом отличаются туннельные адреса, то для двух таких SA могут потребоваться разные маршруты, а добавить второй маршрут невозможно.	Маршрут RR создается только для первого из конфликтующих SA, а при создании второго SA в файл лога выдается предупреждение 1.1	Создаются два маршрута.
3	При создании IPsec SA вычисляется маршрут RR, который вступает в конфликт с существующими маршрутами.	Если в таблице есть такой же маршрут (адрес назначения совпадает), маршрут RR не добавляется. В файл лога выдается сообщение 1.4 Если есть более приоритетный маршрут, пересекающийся, но не совпадающий с маршрутом RR, то маршрут RR добавляется в таблицу маршрутизации.	Добавляется новый RR маршрут (выбор маршрута при этом строго не определен).
4	Конфликт с более узкими фильтрами без RRI.	Маршрут создается без учета таких конфликтов, то есть через pass или ipsec фильтр без RRI пакет может уйти не туда.	
5	При построении IPsec SA в транспортном или туннельном режиме, ID партнера совпадает с туннельным адресом. Маршрут будет как бы рекурсивным – адрес назначения совпадает с адресом шлюза.	Добавляется RR маршрут.	Маршрут не создается.
6	При попытке создания IPsec SA, отсутствует маршрут до туннельного адреса2, например, произошел разрыв соединения.	Маршрут RR не добавляется, в файл лога выдается диагностика 1.3	

[2] Ситуация экзотическая - маршрут нужен для построения SA. Ошибка возможна, если маршрут удалится в процессе создания SA или из-за ошибки чтения/разбора таблицы роутинга.

N	Ситуация	Поведение продукта	Отличие в поведении в Cisco IOS
7	Рассинхронизация с системной таблицей роутинга, т.е. маршруты для созданных SA не актуальны.	Каждый раз при создании IPsec SA с RRI происходит перезачитывание системной таблицы маршрутизации. Если для вновь создаваемого SA старый маршрут оказывается неправильным, он обновляется (см. 5). Другие, ранее созданные RR маршруты, не проверяются.	

Сообщения протоколирования

1. Ошибки, из-за которых не создался RR для SA:
   - Для двух SA с разными селекторами требуются конфликтующие маршруты.

     ```
     [RRI] SA conflicts with the route created for different SA, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255
     ```

     см. п.2 Таблица 1
   - ID второй фазы не является подсетью.

     ```
     [RRI] SA selector shouldn't have protocols, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255 proto 6

     [RRI] destination part of SA selector shouldn't have ports, route not created: destination 10.0.16.96, SA selector 10.0.16.61:32798->192.168.1.6:23 proto 6

     [RRI] destination part of SA selector shouldn't have arbitrary IP range, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.1..192.168.1.255
     ```

     см. п.1 Таблица 1
   - Нет маршрута до туннельного адреса.

     ```
     [RRI] no route to destination, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255
     ```

     см. п.6 Таблица 1

     Объяснение: в данном случае в таблице маршрутизации нет маршрута до 10.0.16.96
   - В системной таблице уже есть маршрут, соответствующий SA, но подсистема RRI его не создавала.

     ```
     [RRI] route already exists, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255
     ```

     см. п.3 Таблица 1
   - Другие ошибки.

     ```
     [RRI] can't read system routing table, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255
     ```

     Объяснение: системная или внутренняя ошибка - не получилось получить таблицу маршрутизации

     ```
     [RRI] can't add route 10.0.0.0/8 via 192.168.1.4: <rtctl err>
     ```

     Объяснение: не удалось добавить маршрут в системную таблицу (системная или внутренняя ошибка). Возможные варианты <rtctl err> см. ниже.

2. Ошибка удаления правила из системной таблицы маршрутизации.

   ```
   [RRI] can't delete route 10.0.0.0/8 via 192.168.1.4: <rtctl err>
   ```

   Объяснение: Ошибки такого типа не приводят к каким-либо дополнительным действиям кроме выдачи данного сообщения. Возможные варианты <rtctl err> см. ниже.
3. Добавление нового RR.

   ```
   [RRI] created route 192.168.1.0/24 via 10.0.135.1 for destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255
   ```


4. Удаление RR.

```
[RRI] removed route 192.168.1.0/24 via 10.0.135.1 for destination
10.0.16.96
```

   Объяснение: выводится при удалении записи из системной таблицы. То есть когда удалены все SA, использующие данный маршрут.

5. Обновление RR.

```
[RRI] updated route to 192.168.1.0/24: new gw 10.0.16.96, old gw
10.0.135.1
```

   Объяснение: сообщение выдается, если при создании нового SA обнаружено, что изменилась таблица роутинга и надо обновить ранее созданный RR.

6. Ошибки <rtctl err>.

```
out of memory
syscall error
route not found
route already exists
gateway unreachable
```

