Пример конфигурации для аутентификации в RIPv2

Содержание

Введение

В этом документе показаны примеры конфигураций аутентификации процесса обмена данными маршрутизации для протокола маршрутизации информации версии 2 (RIPv2).

Внедрение Cisco RIPv2 поддерживает два режима аутентификации: аутентификация с нешифрованным паролем и аутентификация MD5 (Message Digest 5). когда аутентификация включена, режим аутентификации с нешифрованным паролем является настройкой по умолчанию в каждом пакете RIPv2. Аутентификация с нешифрованным паролем не должна использоваться, когда безопасность является проблемой, потому что пароль незашифрованной проверки подлинности передается в каждом пакете RIPv2.

Примечание: Версия RIP 1 (RIPv1) не поддерживает аутентификацию. Если вы передаете и получаете пакеты RIPv2, можно включить аутентификацию RIP на интерфейсе.

Предварительные условия

Требования

У читателей данной документации должно быть основное понимание придерживающегося:

- RIPv1 и RIPv2

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования. Начало с Версии 11.1, RIPv2 программного обеспечения Cisco IOS поддерживается, и поэтому все команды, данные в конфигурации, поддерживаются на Версии 11.1 программного обеспечения Cisco IOS и позже.

Конфигурация в документе протестирована и обновила использование этих версий программного и аппаратного обеспечения:

- Cisco 2500 Series Router
- Версия программного обеспечения Cisco IOS 12.3 (3)

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

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие сведения

Сегодня безопасность – одна из главных забот проектировщиков сети. Защита сети включает в себя организацию безопасности обмена маршрутной информацией между маршрутизаторами, такую как проверка, что информация, введенная в маршрутную таблицу, верна и не была введена или изменена кем-то, пытающимся разрушить сеть. Взломщик может попытаться внедрить недопустимые обновления, чтобы обмануть маршрутизатор и заставить его отправлять данные в неверный пункт назначения или чтобы значительно снизить производительность сети. **Кроме того, обновления недопустимого маршрута могут прекратиться в таблице маршрутизации из-за недостаточной конфигурации (например, без использования команд пассивного интерфейса на границе сети) или из-за неисправного маршрутизатора.** Из-за этого благоразумно аутентифицировать процесс обновления маршрута, работающий на маршрутизаторе.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В данном документе используется сетевая установка, показанная на следующей схеме.

Сеть выше, который используется для следующих примеров конфигурации, состоит из двух маршрутизаторов; маршрутизатор и RB маршрутизатора, оба из которых выполняют RIP и периодически обмены обновлениями маршрута. Необходимо, чтобы этот обмен сведений маршрутизации по последовательному каналу проходил аутентификацию.

Конфигурации

Выполните эти шаги для настройки аутентификации в RIPv2:

1. Определите цепочку ключей с названием.**Примечание:** Цепочка ключей определяет набор ключей, которые могут использоваться на интерфейсе. Если цепочка ключей не настроена, никакая аутентификация не выполнена на том интерфейсе.
2. Определите ключ, или включает цепочку ключей.
3. Задайте пароль или key-string, который будет использоваться в ключе.Это - строка проверки подлинности, которая должна быть передана и получена в пакетах с помощью аутентифицируемого протокола маршрутизации. (В примере, данном ниже, значение строки 234.)
4. Включите аутентификацию на интерфейсе и задайте цепочку ключей, которая будет использоваться.Так как аутентификация включена на на интерфейсное основание, маршрутизатор рабочий RIPv2 может быть настроен для аутентификации на некоторых интерфейсах и может воздействовать без любой аутентификации на другие интерфейсы.
5. Задайте, будет ли интерфейс использовать открытый текст или Аутентификацию MD5.Когда аутентификация включена в предыдущем шаге, проверка подлинности по умолчанию, используемая в RIPv2, является аутентификацией с нешифрованным паролем. Так, при использовании аутентификации с нешифрованным паролем не требуется этот шаг.
6. Настройте управление ключами (Этот шаг является дополнительным).Управление ключами является методом управления ключами проверки подлинности. Это используется для миграции формы один ключ проверки подлинности на другого. Для получения дополнительной информации обратитесь к Секции "Manage Authentication Keys" Настройки Независимые от протокола IP - маршрутизация Функции.

Настройка открытой аутентификации

Один из этих двух путей, которыми могут аутентифицироваться обновления RIP, использует аутентификацию с нешифрованным паролем. Настройку можно произвести так, как показано в таблице ниже.

PA
key chain kal *!--- Name a key chain. A key chain may contain more than one key for added security. !--- It need not be identical on the remote router.* **key 1** *!--- This is the Identification number of an authentication key on a key chain. !--- It need not be identical on the remote router.* **key-string 234** *!--- The actual password or key-string. !--- It needs to be identical to the key-string on the remote router.* ! interface Loopback0 ip

```
address 70.70.70.70 255.255.255.255 ! interface Serial0
ip address 141.108.0.10 255.255.255.252 ip rip
authentication key-chain kal !--- Enables authentication
on the interface and configures !--- the key chain that
will be used. ! router rip version 2 network 141.108.0.0
network 70.0.0.0
```

RB

```
key chain kal key 1 key-string 234 ! interface Loopback0
ip address 80.80.80.1 255.255.255.0 ! interface Serial0
ip address 141.108.0.9 255.255.255.252 ip rip
authentication key-chain kal clockrate 64000 ! router
rip version 2 network 141.108.0.0 network 80.0.0.0
```

Для получения дальнейшей информации на командах, обратитесь к Справочнику по командам IP Cisco IOS.

Настройка аутентификации MD5

Аутентификация MD5 – это дополнительный режим аутентификации, добавленный компанией Cisco к исходной аутентификации на основе обычного текста, определенной RFC 1723. **Конфигурация аналогична конфигурации для аутентификации с нешифрованным паролем за исключением использования дополнительной команды ip rip authentication mode md5.** Пользователи должны настроить интерфейсы маршрутизатора с обеих сторон ссылки для метода Аутентификации MD5, удостоверившись ключевой номер и соответствие строки ключа с обеих сторон.

PA

```
key chain kal !--- Need not be identical on the remote
router. key 1 !--- Needs to be identical on remote
router. key-string 234 !--- Needs to be identical to the
key-string on the remote router. ! interface Loopback0
ip address 70.70.70.70 255.255.255.255 ! interface
Serial0 ip address 141.108.0.10 255.255.255.252 ip rip
authentication mode md5 !--- Specifies the type of
authentication used !--- in RIPv2 packets. !--- Needs to
be identical on remote router. !-- To restore clear text
authentication, use the no form of this command. ip rip
authentication key-chain kal ! router rip version 2
network 141.108.0.0 network 70.0.0.0
```

RB

```
key chain kal key 1 key-string 234 ! interface Loopback0
ip address 80.80.80.1 255.255.255.0 ! interface Serial0
ip address 141.108.0.9 255.255.255.252 ip rip
authentication mode md5 ip rip authentication key-chain
kal clockrate 64000 ! router rip version 2 network
141.108.0.0 network 80.0.0.0
```

Для получения дальнейшей информации на командах, обратитесь к ссылке Команды Cisco IOS.

Проверка

Контроль аутентификации на основе открытого текста

Этот раздел предоставляет сведения, чтобы подтвердить, что ваша конфигурация работает должным образом.

Настройка маршрутизаторов, показанная выше, подразумевает, что все обмены обновлениями маршрутизаторов должны пройти проверки подлинности перед принятием. Это можно проверить, наблюдая за выводом команд debug ip rip и show ip route.

Примечание: Прежде чем вызывать команды debug, обратитесь к разделу Важные сведения о командах отладки.

```
RB#debug ip rip RIP protocol debugging is on *Mar 3 02:11:39.207: RIP: received packet with text
authentication 234 *Mar 3 02:11:39.211: RIP: received v2 update from 141.108.0.10 on Serial0
*Mar 3 02:11:39.211: RIP: 70.0.0.0/8 via 0.0.0.0 in 1 hops RB#show ip route R 70.0.0.0/8 [120/1]
via 141.108.0.10, 00:00:25, Serial0 80.0.0.0/24 is subnetted, 1 subnets C 80.80.80.0 is directly
connected, Loopback0 141.108.0.0/30 is subnetted, 1 subnets C 141.108.0.8 is directly connected,
Serial0
```

Использование аутентификации с нешифрованным паролем улучшает организацию сети путем предотвращения добавления обновлений маршрута, инициируемых маршрутизаторами, не предназначенными для принятия участия в локальном процессе обмена маршрутизации. Однако этот тип аутентификации не безопасен. Паролем (234 в данном примере) обмениваются в открытом тексте. Его можно без труда захватить и потом исследовать. Как было сказано выше, аутентификацию MD5 следует предпочесть аутентификации с помощью простого текста, если есть проблемы с безопасностью.

Подтверждение проверки подлинности MD5

Путем настройки RA и маршрутизаторов RB как показано выше, все обмены обновления маршрута будут аутентифицироваться прежде чем быть принятым. Это можно проверить, наблюдая за выводом команд debug ip rip и show ip route.

```
RB#debug ip rip RIP protocol debugging is on *Mar 3 20:48:37.046: RIP: received packet with MD5
authentication *Mar 3 20:48:37.046: RIP: received v2 update from 141.108.0.10 on Serial0 *Mar 3
20:48:37.050: 70.0.0.0/8 via 0.0.0.0 in 1 hops RB#show ip route R 70.0.0.0/8 [120/1] via
141.108.0.10, 00:00:03, Serial0 80.0.0.0/24 is subnetted, 1 subnets C 80.80.80.0 is directly
connected, Loopback0 141.108.0.0/30 is subnetted, 1 subnets C 141.108.0.8 is directly connected,
Serial0
```

Проверка подлинности MD5 использует очень сильный односторонний алгоритм хеширования MD5. В данном режиме аутентификации обновление маршрутизации не содержит пароль для аутентификации. Скорее, 128-разрядное сообщение, которое создается при запуске алгоритма MD5 в пароле, и само сообщение отправляются вместе для аутентификации. Таким образом рекомендуется использовать Аутентификацию MD5 по аутентификации с нешифрованным паролем, так как это более безопасно.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Некоторые команды show поддерживаются Средством интерпретации выходных

данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Команда debug ip rip может использоваться для устранения проблем RIPv2 связанные с аутентификацией проблемы.

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

Примечание: Придерживающееся является примером выходных данных команды debug ip rip, когда не совпадает любой из связанных с аутентификацией параметров, которые должны быть идентичными между соседними маршрутизаторами. Это может привести или к один или к оба маршрутизаторы, не устанавливающие принятые маршруты в их таблице маршрутизации.

```
RA#debug ip rip RIP protocol debugging is on *Mar 1 06:47:42.422: RIP: received packet with text authentication 234 *Mar 1 06:47:42.426: RIP: ignored v2 packet from 141.108.0.9 (invalid authentication) RB#debug ip rip RIP protocol debugging is on *Mar 1 06:48:58.478: RIP: received packet with text authentication 235 *Mar 1 06:48:58.482: RIP: ignored v2 packet from 141.108.0.10 (invalid authentication)
```

Следующий результат от команды show ip route показывает, что маршрутизатор не узнает, что любой направляет через RIP:

```
RB#show ip route Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route Gateway of last resort is not set 80.0.0.0/24 is subnetted, 1 subnets C 80.80.80.0 is directly connected, Loopback0 141.108.0.0/30 is subnetted, 1 subnets C 141.108.0.8 is directly connected, Serial0 RB#
```

Примечание 1: При использовании режима аутентификации с нешифрованным паролем удостоверьтесь, что следующие параметры совпадают на соседних маршрутизаторах для успешной аутентификации.

- Key-string
- Authentication mode

Примечание 2: При использовании режима Аутентификации MD5, для успешной аутентификации удостоверяются, что следующие параметры совпадают на соседних маршрутизаторах.

- Key-string
- Ключевой номер
- Authentication mode

Дополнительные сведения

- Введение к протоколу RIP
- RIP Настройки
- Настройка ip-routing-protocols-независимые функции
- Команды настройки RIP
- Справочник по командам IP Cisco IOS, Громкость 2 из 4: протоколы маршрутизации, релиз 12.3

- Страница поддержки технологии RIP
- Страница поддержки технологии протоколов IP-маршрутизации
- Техническая поддержка - Cisco Systems