Пример конфигурации проверки подлинности сообщений EIGRP

Содержание

Введение

В этом документе поясняется способ добавления аутентификации сообщений в маршрутизаторах с протоколом EIGRP и защиты таблицы маршрутизации от преднамеренного или случайного искажения.

Добавление аутентификации к сообщениям EIGRP ваших маршрутизаторов гарантирует, что ваши маршрутизаторы только принимают сообщения маршрутизации от других маршрутизаторов, которые знают тот же предварительный общий ключ. Без этой настроенной аутентификации, если кто-то начинает другой маршрутизатор с других или конфликтных сведений о маршруте в сети, таблицы маршрутизации на ваших маршрутизаторах могли стать поврежденными, и атака типа отказ в обслуживании могла последовать. Таким образом, когда вы добавляете аутентификацию к сообщениям EIGRP, передаваемым между вашими маршрутизаторами, она предотвращает кого-то от намеренно или случайно добавляющий другой маршрутизатор к сети и причиняющий проблему.

Внимание. : Когда Аутентификация сообщений по протоколу EIGRP добавлена к интерфейсу маршрутизатора, тот маршрутизатор прекращает получать сообщения

маршрутизации от своих узлов, пока они также не настроены для проверки подлинности сообщений. Это **действительно** прерывает связь маршрутизации в вашей сети. См. сообщения, Когда Только Даллас будет Настроен для получения дополнительной информации.

Предварительные условия

Требования

- Время должно быть должным образом настроено на всех маршрутизаторах. См. NTP Настройки для получения дополнительной информации.
- Рабочая конфигурация протокола EIGRP рекомендуется.

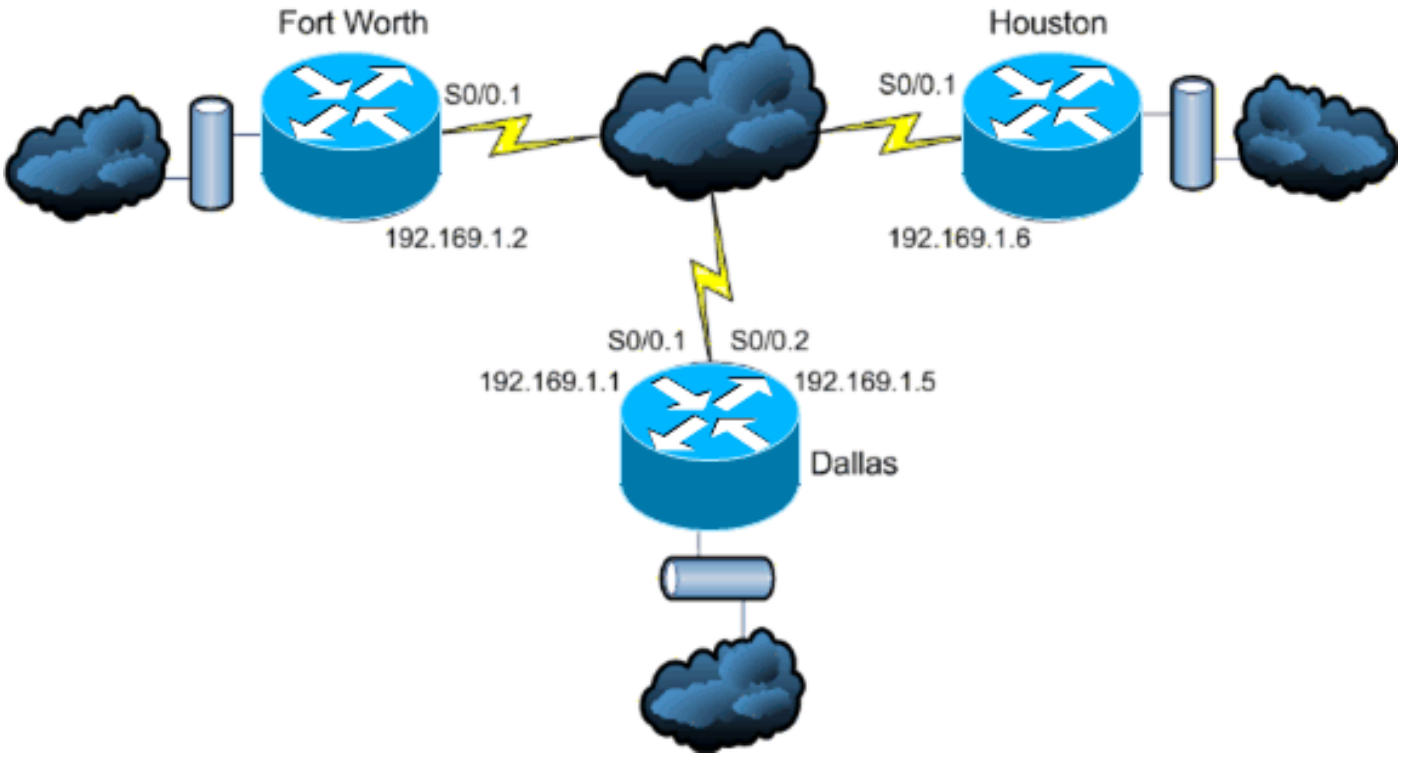
Используемые компоненты

Сведения в этом документе основываются на Выпуске 11.2 программного обеспечения Cisco IOS и позже.

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

Схема сети

В настоящем документе используется следующая схема сети:



Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

В этом сценарии администратор сети хочет настроить аутентификацию для сообщений EIGRP между маршрутизатором концентратора в Далласе и удаленными узлами в Форт-Уэрте и Хьюстоне. Конфигурация протокола EIGRP (без аутентификации) уже завершена на всех трех маршрутизаторах. Выходные данные данного примера из Далласа:

```
Dallas#show ip eigrp neighbors IP-EIGRP neighbors for process 10 H Address Interface Hold Uptime SRTT RTO Q Seq Type (sec) (ms) Cnt Num 1 192.169.1.6 Se0/0.2 11 15:59:57 44 264 0 2 0 192.169.1.2 Se0/0.1 12 16:00:40 38 228 0 3 Dallas#show cdp neigh Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater Device ID Local Intrfce Holdtme Capability Platform Port ID Houston Ser 0/0.2 146 R 2611 Ser 0/0.1 FortWorth Ser 0/0.1 160 R 2612 Ser 0/0.1
```

Настройте аутентификацию сообщений по протоколу EIGRP

Конфигурация Аутентификации сообщений по протоколу EIGRP состоит из двух шагов:

1. Создание цепочки для ключей и ключа.
2. Конфигурация аутентификации EIGRP для использования той цепочки для ключей и ключа.

Этот раздел иллюстрирует шаги для настройки Аутентификации сообщений по протоколу EIGRP на Далласском маршрутизаторе и затем маршрутизаторах Форт-Уэрта и Хьюстона.

Создайте цепочку для ключей на Далласе

Проверка подлинности при маршрутизации полагается на ключ на цепочке для ключей для функционирования. Прежде чем аутентификация может быть включена, цепочка для ключей и по крайней мере один ключ должны быть созданы.

1. Перейдите в режим глобальной настройки.`Dallas#configure terminal`
2. Создайте цепочку ключей. **MYCHAIN** используется в данном примере.`Dallas(config)#key chain MYCHAIN`
3. Задайте ключевой номер. **1** используется в данном примере.**Примечание:** Рекомендуется, чтобы ключевой номер был тем же на всех маршрутизаторах, вовлеченных в конфигурацию.`Dallas(config-keychain)#key 1`
4. Задайте key-string для ключа. **securetraffic** используется в данном примере.`Dallas(config-keychain-key)#key-string securetraffic`
5. Закончите конфигурацию.`Dallas(config-keychain-key)#end Dallas#`

Настройте аутентификацию на Далласе

Как только вы создаете цепочку для ключей и ключ, необходимо настроить EIGRP для выполнения проверки подлинности сообщений с ключом. Эта конфигурация завершена на интерфейсах, на которых настроен EIGRP.

Внимание. : Когда Аутентификация сообщений по протоколу EIGRP добавлена к Далласским интерфейсам, она прекращает получать сообщения маршрутизации от своих

узлов, пока они также не настроены для проверки подлинности сообщений. Это **действительно** прерывает связь маршрутизации в вашей сети. См. сообщения, Когда Только Даллас будет Настроен для получения дополнительной информации.

1. Перейдите в режим глобальной настройки.`Dallas#configure terminal`
2. От режима глобальной конфигурации задайте интерфейс, на котором вы хотите настроить Аутентификацию сообщений по протоколу EIGRP. В данном примере первый интерфейс является **Последовательным 0/0.1**.`Dallas(config)#interface serial 0/0.1`
3. Включите Аутентификацию сообщений по протоколу EIGRP. Эти **10**, используемые здесь, являются номером автономной системы сети. **md5** указывает, что хэш md5 должен использоваться для аутентификации.`Dallas(config-subif)#ip authentication mode eigrp 10 md5`
4. Задайте цепочку для ключей, которая должна использоваться для аутентификации. **10** номер автономной системы. **MYCHAIN** является цепочкой для ключей, которая была создана в Создавании раздела Цепочки для ключей.`Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN` `Dallas(config-subif)#end`
5. Завершите одинаковую конфигурацию на interface Serial 0/0.2.`Dallas#configure terminal` `Dallas(config)#interface serial 0/0.2` `Dallas(config-subif)#ip authentication mode eigrp 10 md5` `Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN` `Dallas(config-subif)#end` `Dallas#`

Настройте Форт-Уэрт

Этот раздел показывает команды, необходимые для настройки Аутентификации сообщений по протоколу EIGRP на маршрутизаторе Форт-Уэрта. Для большего количества подробного объяснения команд, показанных здесь, посмотрите, Создают Цепочку для ключей на Далласе и Настраивают Аутентификацию на Далласе.

```
FortWorth#configure terminal FortWorth(config)#key chain MYCHAIN FortWorth(config-keychain)#key
1 FortWort(config-keychain-key)#key-string securetraffic FortWort(config-keychain-key)#end
FortWorth# Fort Worth#configure terminal FortWorth(config)#interface serial 0/0.1
FortWorth(config-subif)#ip authentication mode eigrp 10 md5 FortWorth(config-subif)#ip
authentication key-chain eigrp 10 MYCHAIN FortWorth(config-subif)#end FortWorth#
```

Настройте Хьюстон

Этот раздел показывает команды, необходимые для настройки Аутентификации сообщений по протоколу EIGRP на Хьюстонском маршрутизаторе. Для большего количества подробного объяснения команд, показанных здесь, посмотрите, Создают Цепочку для ключей на Далласе и Настраивают Аутентификацию на Далласе.

```
Houston#configure terminal Houston(config)#key chain MYCHAIN Houston(config-keychain)#key 1
Houston(config-keychain-key)#key-string securetraffic Houston(config-keychain-key)#end Houston#
Houston#configure terminal Houston(config)#interface serial 0/0.1 Houston(config-subif)#ip
authentication mode eigrp 10 md5 Houston(config-subif)#ip authentication key-chain eigrp 10
MYCHAIN Houston(config-subif)#end Houston#
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Сообщения, Когда Только Настроен Даллас

Как только Аутентификация сообщений по протоколу EIGRP настроена на Далласском маршрутизаторе, тот маршрутизатор начинает отклонять сообщения от маршрутизаторов Форт-Уэрта и Хьюстона, потому что им еще не настроили аутентификацию. Это может быть проверено путем выдачи команды **debug eigrp packet** на Далласском маршрутизаторе:

```
Dallas#debug eigrp packets 17:43:43: EIGRP: ignored packet from 192.169.1.2 (invalid
authentication) 17:43:45: EIGRP: ignored packet from 192.169.1.6 (invalid authentication) !---
Packets from Fort Worth and Houston are ignored because they are !--- not yet configured for
authentication.
```

Сообщения, Когда Настроены Все маршрутизаторы

Как только Аутентификация сообщений по протоколу EIGRP настроена на всех трех маршрутизаторах, они начинают обмениваться сообщениями EIGRP снова. Это может быть проверено путем выдачи команды **debug eigrp packet** еще раз. На этот раз выходные данные от маршрутизаторов Форт-Уэрта и Хьюстона показывают:

```
FortWorth#debug eigrp packets 00:47:04: EIGRP: received packet with MD5 authentication, key id =
1 00:47:04: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.1 !--- Packets from Dallas with
MD5 authentication are received. Houston#debug eigrp packets 00:12:50.751: EIGRP: received
packet with MD5 authentication, key id = 1 00:12:50.751: EIGRP: Received HELLO on Serial0/0.1
nbr 192.169.1.5 !--- Packets from Dallas with MD5 authentication are received.
```

Устранение неполадок

Однонаправленный канал

Необходимо настроить EIGRP Hello и таймеры Времени удержания на обоих концах. При настройке таймеров только на одном конце однонаправленное соединение происходит.

Маршрутизатор на однонаправленном соединении мог бы быть в состоянии получить пакеты приветствия. Однако отосланные пакеты приветствия не получены в другом конце. Это однонаправленное соединение обычно обозначается *превышенными* сообщениями *предела повторной попытки* на одном конце.

Для просмотра *превышенных* сообщений *предела повторной попытки* используйте **команды debug eigrp packet и debug ip eigrp notifications**.

Дополнительные сведения

- Поддержка технологии протокола EIGRP
- Cisco Systems – техническая поддержка и документация