Безопасность мостовых соединений

Содержание

Введение

При проектировании беспроводного соединения с помощью моста между сегментами Ethernet необходимо уделять повышенное внимание безопасности. В этом документе показано, как с помощью туннеля IPSec обезопасить трафик, пересекающий мостовое беспроводное соединение.

В данном примере два моста Cisco Aironet серии 350 устанавливают WEP; эти два маршрутизатора устанавливают Туннель IPSec.

Предварительные условия

Требования

Прежде, чем делать попытку этой конфигурации, гарантируйте, что вы довольны использованием их:

- Интерфейс Конфигурации моста Cisco Aironet
- Линейный интерфейс Команды Cisco IOS

Используемые компоненты

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

- Маршрутизаторы серии Cisco 2600 рабочая версия IOS 12.1

- Мосты Cisco Aironet серии 350 рабочая версия микропрограммы 11.08T

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Теоретические сведения

Мосты Cisco Aironet 340, 350 и серии1400 предоставляют WEP-шифрование до уровня128 бит. Эту задачу нельзя решить с помощью безопасного соединения из-за известной проблеме в WEP-алгоритмах и простоты использования, как описано в документе о безопасности WEP-алгоритма («Security of the WEP algorithm») и в документе о наличии проблем безопасности «Cisco Aironet Response to Press - Flaws in 802.11 Security».

Один из способов увеличить безопасность трафика, проходящего по беспроводному мостовому соединению, - это создать шифрованный тоннель IPSec "марштрутизатор-маршрутизатор", который будет пересекать соединение. Это работает, поскольку мосты действуют на слое 2 модели OSI. Можно запустить подключение IPSEC от маршрутизатора к маршрутизатору через соединение между мостами.

Если в безопасности беспроводного соединения есть уязвимые места, то трафик, проходящий по нему, остается шифрованным и защищенным.

Условные обозначения

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

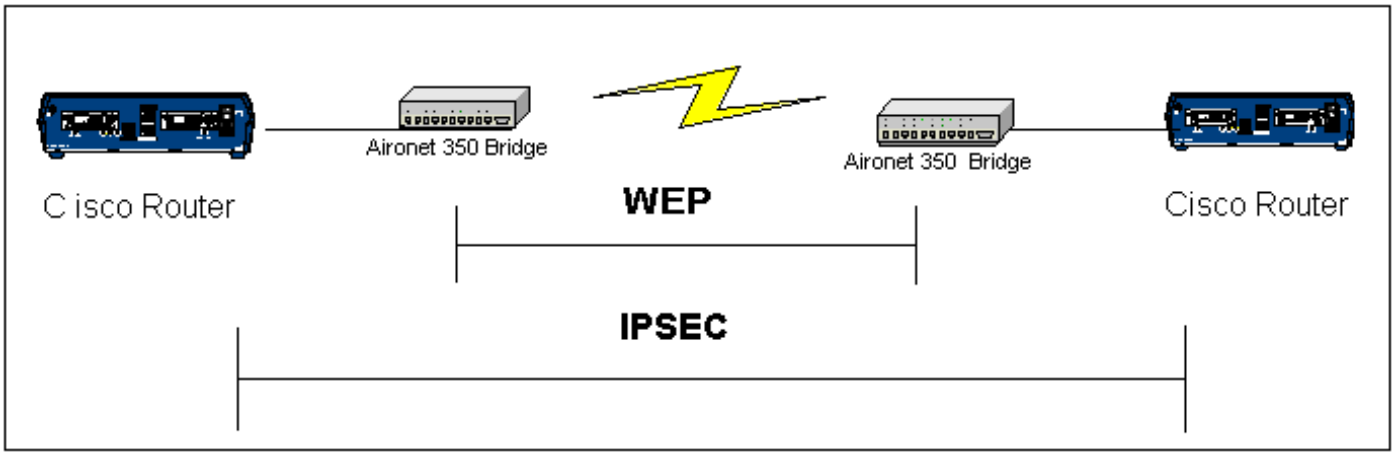
Настройка

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

Примечание: Для получения дополнительной информации о командах, встречающихся в этом документе, используйте средство поиска команд.

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме:



Конфигурации

Эти конфигурации используются в данном документе:

- Маршрутизатор A
- Маршрутизатор B
- Пример моста

Маршрутизатор A (маршрутизатор Cisco 2600)

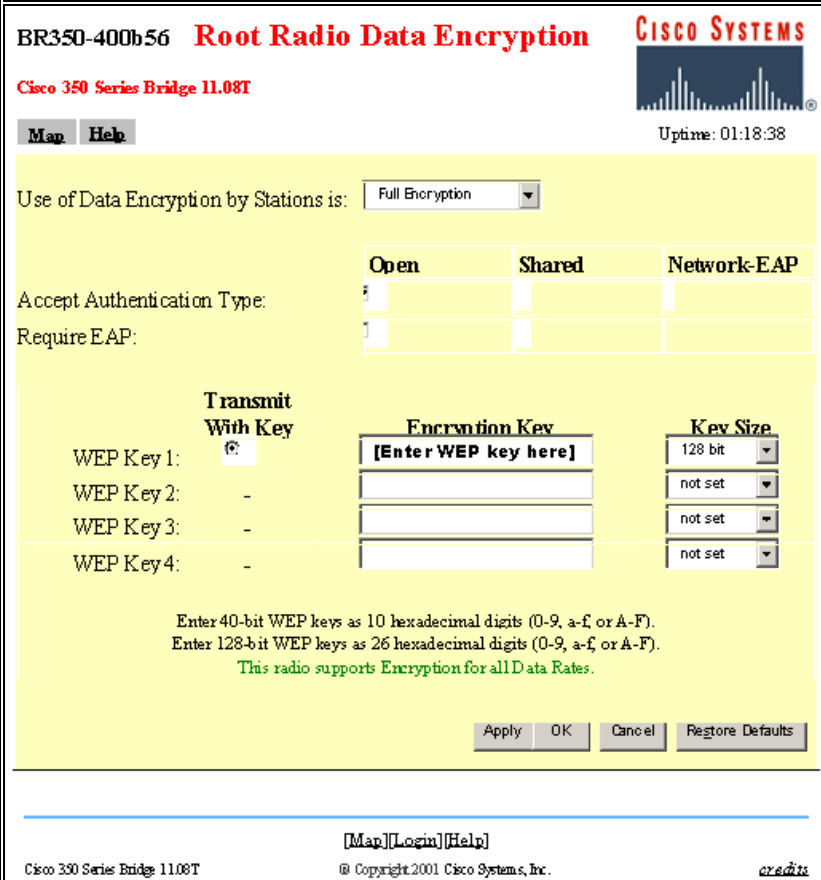
```
RouterA#show running-config Building configuration...
Current configuration : 1258 bytes ! version 12.1 no
service single-slot-reload-enable no service pad service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname RouterA ! logging
rate-limit console 10 except errors ! ip subnet-zero no
ip finger ip dhcp excluded-address 10.1.1.20 ip dhcp
excluded-address 10.1.1.30 ! ip dhcp pool wireless
network 10.1.1.0 255.255.255.0 ! ip audit notify log ip
audit po max-events 100 call rsvp-sync ! crypto isakmp
policy 10 hash md5 authentication pre-share crypto
isakmp key cisco address 10.1.1.30 ! ! crypto ipsec
transform-set set esp-3des esp-md5-hmac ! crypto map vpn
10 ipsec-isakmp set peer 10.1.1.30 set transform-set set
match address 120 ! interface Loopback0 ip address
20.1.1.1 255.255.255.0 ! interface Ethernet0 ip address
10.1.1.20 255.255.255.0 crypto map vpn ! ! ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.30 no ip http server no
ip http cable-monitor ! access-list 120 permit ip
20.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255 ! ! line con 0
transport input none line vty 0 4 ! end
```

RouterB (маршрутизатор Cisco 2600)

```
RouterB#show running-config Building configuration...
Current configuration : 1177 bytes ! version 12.1 no
service single-slot-reload-enable no service pad service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname RouterB ! logging
rate-limit console 10 except errors ! ip subnet-zero no
ip finger ! ip audit notify log ip audit po max-events
100 call rsvp-sync crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco address
10.1.1.20 ! ! crypto ipsec transform-set set esp-3des
esp-md5-hmac ! crypto map vpn 10 ipsec-isakmp set peer
```

```
10.1.1.20 set transform-set set match address 120
interface Loopback0 ip address 30.1.1.1 255.255.255.0 !
interface Ethernet0 ip address 10.1.1.30 255.255.255.0
no ip mroute-cache crypto map vpn ! ip classless ip
route 0.0.0.0 0.0.0.0 10.1.1.20 no ip http server no ip
http cable-monitor ! access-list 120 permit ip 30.1.1.0
0.0.0.255 20.1.1.0 0.0.0.255 ! ! line con 0 transport
input none line vty 0 4 login ! end
```

Мосты Cisco Aironet



Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **show crypto engine connection active** - эта команда используется для просмотра текущих активных соединений шифрованного сеанса

```
RouterA#show crypto engine connection active ID Interface IP-Address State Algorithm Encrypt
Decrypt 1 Ethernet0 10.1.1.20 set HMAC_MD5+DES_56_CB 0 0 2002 Ethernet0 10.1.1.20 set
HMAC_MD5+3DES_56_C 0 3 2003 Ethernet0 10.1.1.20 set HMAC_MD5+3DES_56_C 3 0 RouterB#show
crypto engine connection active ID Interface IP-Address State Algorithm Encrypt Decrypt 1
<none> <none> set HMAC_MD5+DES_56_CB 0 0 2000 Ethernet0 10.1.1.30 set HMAC_MD5+3DES_56_C 0 3
2001 Ethernet0 10.1.1.30 set HMAC_MD5+3DES_56_C 3 0
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Для устранения неисправностей подключения IPSEC обратитесь к следующим документам:

- Устранение проблем IPSec — общие сведения и использование команд debug
- Настройка и устранение неполадок шифрования данных на уровне сети Cisco: IPSec и ISAKMP, часть 1 и часть 2

Для устранения проблем беспроводного соединения обратитесь к:

- Средство из пакета TAC – беспроводная локальная сеть
- Поиск и устранение общих проблем в беспроводных сетях, соединенных через мосты
- Устранение неисправностей связи в беспроводных сетях LAN

Дополнительные сведения

- **Техническая поддержка – беспроводная LAN**
- **Техническая поддержка - протоколы IPSec Negotiation/IKE**
- **Техническая поддержка - Cisco Systems**