Настройка IPSec/GRE с NAT

Содержание

Общие сведения

Этот пример конфигурации показывает, как настроить общую инкапсуляцию маршрутов (GRE) через протокол IP-безопасности (IPSec), где туннель GRE/IPSec проходит через брандмауэр, выполняющий трансляцию сетевых адресов (NAT).

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. в статье "Технические советы Cisco. Условные обозначения".

Предварительные условия

Этот вид настройки может быть использован для туннелирования и шифрования трафика, который обычно не идет через брандмауэр, такого как IPX (как в приведенном примере) или обновления маршрутов. В данном примере туннель между 2621 и 3660 работает только тогда, когда трафик генерируется устройствами в сегментах LAN (не расширенной проверкой связи IP/IPX с маршрутизаторов IPSec). Соединение IP/IPX было протестировано с помощью проверки доступности IP/IPX между устройствами 2513A и 2513B.

Примечание: это несовместимо с трансляцией адресов портов (PAT).

Используемые компоненты

Сведения, содержащиеся в данном документе, приведены на основе следующих версий программного и аппаратного обеспечения:

- Cisco IOS® 12.0.7.T

Данные для документа были получены в специально созданных лабораторных условиях. При написании данного документа использовались только устройства с пустой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное

воздействие всех команд до их использования.

Настройка

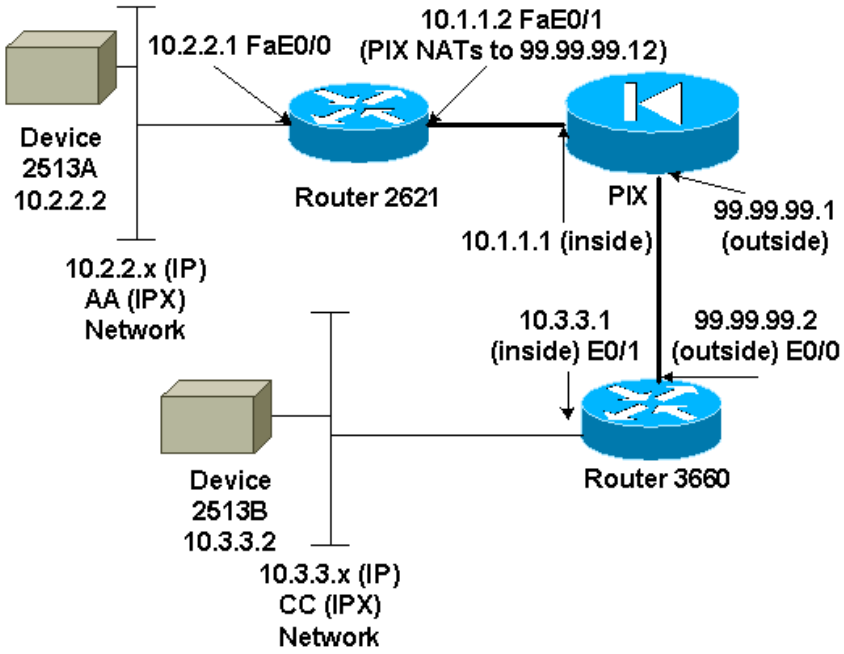
В этом разделе приводятся сведения о настройке функций, описанных в данном документе.

Примечание: для поиска дополнительной информации о командах в данном документе используйте средство Command Lookup Tool (только для зарегистрированных заказчиков) .

Примечания по конфигурации IOS: С кодами Cisco IOS 12.2(13)T и более поздними кодами (коды последовательности T с большими номерами, коды 12.3 и более поздние коды) настраиваемую "криптокарту" IPSEC необходимо применять только к физическому интерфейсу и больше не требуется применять в интерфейсе туннелирования GRE. "Криптокарта" по-прежнему будет работать на физическом и туннельном интерфейсах при использовании 12.2.(13)T и более поздних кодов. Тем не менее, настоятельно рекомендуется применять ее только к физическому интерфейсу.

Схема сети

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



Примечания к схеме сети

- Туннель GRE из 10.2.2.1 к 10.3.3.1 (IPX network BB)
- Туннель IPSec из 10.1.1.2 (99.99.99.12) к 99.99.99.2

Настройки

Устройство 2513A
ipx routing 00e0.b064.20c1 ! interface Ethernet0 **ip address 10.2.2.2 255.255.255.0** no ip directed-broadcast **ipx network AA**

```
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
```

2621

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ipx routing 0030.1977.8f80
isdn voice-call-failure 0
cns event-service server
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/1
crypto map mymap 10 ipsec-isakmp
set peer 99.99.99.2
set transform-set myset
match address 101
!
controller T1 1/0
!
interface Tunnel0
ip address 192.168.100.1 255.255.255.0
no ip directed-broadcast
ipx network BB
tunnel source FastEthernet0/0
tunnel destination 10.3.3.1
crypto map mymap
!
interface FastEthernet0/0
ip address 10.2.2.1 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
 ipx network AA
!
interface FastEthernet0/1
ip address 10.1.1.2 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
crypto map mymap
!
ip classless
ip route 10.3.3.0 255.255.255.0 Tunnel0
ip route 10.3.3.1 255.255.255.255 10.1.1.1
ip route 99.99.99.0 255.255.255.0 10.1.1.1
no ip http server
!
access-list 101 permit gre host 10.2.2.1 host 10.3.3.1
!
line con 0
transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

PIX

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
global (outside) 1 99.99.99.50-99.99.99.60
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask 255.255.255.255 0 0
conduit permit esp host 99.99.99.12 host 99.99.99.2
conduit permit udp host 99.99.99.12 eq isakmp host 99.99.99.2
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

3660

```
version 12.0
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname goss-e4-3660
!
memory-size iomem 30
ip subnet-zero
no ip domain-lookup
!
ipx routing 0030.80f2.2950
cns event-service server
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0
crypto map mymap 10 ipsec-isakmp
set peer 99.99.99.12
set transform-set myset
match address 101
!
interface Tunnel0
ip address 192.168.100.2 255.255.255.0
no ip directed-broadcast
ipx network BB
tunnel source FastEthernet0/1
tunnel destination 10.2.2.1
crypto map mymap
!
interface FastEthernet0/0
ip address 99.99.99.2 255.255.255.0
no ip directed-broadcast
ip nat outside
duplex auto
speed auto
crypto map mymap
!
interface FastEthernet0/1
ip address 10.3.3.1 255.255.255.0
no ip directed-broadcast
ip nat inside
duplex auto
speed auto
 ipx network CC
!
ip nat pool 3660-nat 99.99.99.70 99.99.99.80 netmask 255.255.255.0
ip nat inside source list 1 pool 3660-nat
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route 10.2.2.1 255.255.255.255 99.99.99.1
ip route 99.99.99.12 255.255.255.255 99.99.99.1
no ip http server
!
access-list 1 permit 10.3.3.0 0.0.0.255
access-list 101 permit gre host 10.3.3.1 host 10.2.2.1
!
```

```
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Устройство 2513B

```
ipx routing 00e0.b063.e811
!
interface Ethernet0
ip address 10.3.3.2 255.255.255.0
no ip directed-broadcast
ipx network CC
!
ip route 0.0.0.0 0.0.0.0 10.3.3.1
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Определенные команды **show** поддерживаются средством Output Interpreter Tool (только для зарегистрированных заказчиков), которое позволяет просматривать и анализировать выходные данные команды **show**.

- **show crypto ipsec sa** - показывает сопоставления безопасности этапа 2.
- **show crypto isakmp sa** - показывает активные зашифрованные соединения сеанса для всех криптоустройств.
- *Дополнительно:* **show interfaces tunnel *number*** - отображает данные интерфейса туннеля.
- **show ip route** - показывает все статические IP-маршруты или установленные с использованием функции загрузки маршрута AAA.
- **show ipx route** - показывает содержание таблицы маршрутизации IPX.

Устранение неполадок

В данном разделе описывается процесс устранения неполадок конфигурации.

Команды устранения неполадок

Некоторые команды **show** поддерживаются средством Output Interpreter Tool (только для зарегистрированных заказчиков), которое позволяет просматривать и анализировать выходные данные команды **show**.

Примечание: перед применением команд **debug** ознакомьтесь с разделом "Важные сведения о командах отладки".

- **debug crypto engine** - показывает зашифрованный трафик.
- **debug crypto ipsec** - показывает согласования IPSec во второй фазе.
- **debug crypto isakmp** - показывает согласования первой фазы протокола ISAKMP (Протокол управления ключами Ассоциации безопасности Интернет)

- *Дополнительно:* **debug ip routing** - показывает данные обновления таблицы маршрутизации RIP и обновления кэша маршрутизации.
- **debug ipx routing {activity | events}** - показывает информацию о пакетах маршрутизации IPX, которые отправляет и принимает маршрутизатор.

Очистка сопоставлений безопасности (SA)

- **clear crytpo ipsec** - очищает все сопоставления безопасности IPSec.
- **clear crypto isakmp** - очищает все сопоставления безопасности IKE.
- *Дополнительно:* **clear ipx route *** - удаляет все маршруты из таблицы маршрутизации IPX.

Дополнительные сведения

- **Страницы поддержки продуктов IP Security (IPSec)**
- **Страницы поддержки GRE**
- **Техническая поддержка - Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92061/ipsecgrenat.shtml