IPSec/GRE с NAT на примере конфигурации маршрутизатора IOS

Содержание

Введение

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

Перед началом работы

Условные обозначения

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

Предварительные условия

Этот тип конфигурации мог использоваться, чтобы туннелировать и зашифровать трафик, который обычно не будет проходить межсетевой экран, такой как IPX (как в нашем примере здесь) или обновления маршрута. 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 адреса порта (PAT).

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Cisco IOS® 12.4
- Межсетевой экран Cisco PIX 535
- Выпуск 7.x Программного обеспечения Cisco PIX Firewall и позже

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.

Настройка

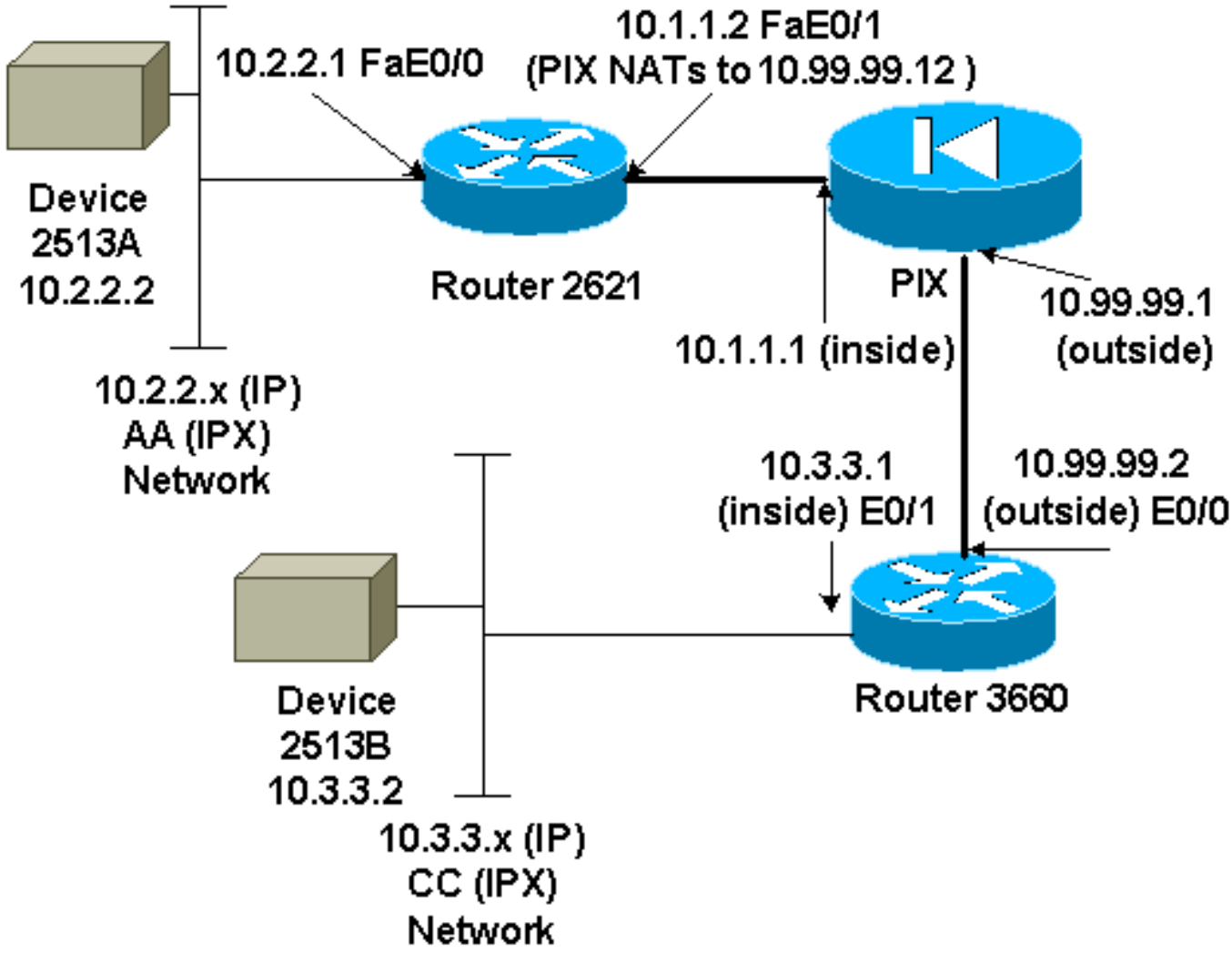
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

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

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 данном документе используется сетевая установка, показанная на следующей схеме.



Примечание: IP-адреса, используемые в этой конфигурации, не юридически маршрутизируемы в Интернете. [Это адреса RFC 1918, которые использовались в лабораторной среде.]

Примечания к сетевым диаграммам

- Туннель GRE от 10.2.2. От 1 до 10. 3.3.1 (BB сети IPX)
- Туннель IPSec от 10.1.1.2 (10.99.99.12) к 10.99.99.2

Конфигурации

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 *!--- Output Suppressed*

2621
version 12.4 service timestamps debug uptime service timestamps log uptime

```
no service password-encryption
!
hostname 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 10.99.99.2
!
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 10.99.99.2
 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 10.99.99.0 255.255.255.0 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
```

```
!--- Output Suppressed
```

PIX

```
pixfirewall# sh run
: Saved
:
PIX Version 7.0
!
hostname pixfirewall
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.99.99.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
global (outside) 1 10.99.99.50-10.99.99.60
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0
access-list 102 permit esp host 10.99.99.12 host
10.99.99.2
access-list 102 permit udp host 10.99.99.12 host
10.99.99.2 eq isakmp


route outside 0.0.0.0 0.0.0.0 10.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1

!--- Output Suppressed
```

3660

```
version 12.4
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname 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 10.99.99.12
!
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 10.99.99.12
```

```
 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 10.99.99.2 255.255.255.0
 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 10.99.99.70 10.99.99.80 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 10.99.99.1
ip route 10.99.99.12 255.255.255.255 10.99.99.1
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
!--- Output Suppressed
```

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

!--- Output Suppressed
```

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.

- команда show crypto ipsec sa – отображает связи безопасности, соответствующие второму этапу.
- show crypto isakmp sa- Показывает текущие активные соединения шифрованного сеанса для всех ядер шифрования.
- *Дополнительно: команда show interfaces tunnel number – Отображает данные интерфейса туннеля.*
- show ip route- Показывает всем статическим IP - маршрутам или тем установленное использование AAA (аутентификация, авторизация и учет) функция загрузки маршрута.
- show ipx route- Показывает содержание таблицы маршрутизации IPX.

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.

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

- "debug crypto engine" - отображается зашифрованный трафик.
- команда debug crypto ipsec отображает согласование IPSec на втором этапе.
- debug crypto isakmp– показывает согласование протокола ISAKMP (протокол управления ассоциациями безопасности и ключами в Интернете) на 1-м этапе.
- *Дополнительно:* команда debug ip routing – отображает данные обновления таблицы маршрутизации протокола маршрутной информации и обновления кэша маршрутизации.
- ipx - маршрутизация отладки {действие | события} - ipx - маршрутизация отладки {действие | события} - Показывают информацию о пакетах Ipx - маршрутизации, что маршрутизатор передает и получает.

Очистка сопоставлений безопасности (SA)

- clear crytpo ipsec sa - Очищает все Сопоставления безопасности IPSec.
- clear crypto isakmp – удаляет связи безопасности операций обмена ключами в Интернете (IKE).
- *Дополнительно:* clear ipx route * – удаляет все маршруты из таблицы маршрутизации IPX.

Дополнительные сведения

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