Настройка туннеля IPSec между маршрутизаторами с дублированными подсетями локальной сети

Содержание

Введение

В этом документе представлен пример организации сети, моделирующий слияние двух компаний с одинаковой схемой IP-адресации. Два маршрутизатора связаны VPN-туннелем, а сети за этими маршрутизаторами одинаковы. Чтобы с одного объекта получить доступ к хостам на другом объекте, используется преобразование сетевых адресов (NAT) на маршрутизаторах, заменяющее адреса источника и получателя на другие подсети.

Примечание: Эта конфигурация не рекомендуется как постоянная настройка, потому что она сбила бы с толку с точки зрения управления сетью.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Маршрутизатор A: Маршрутизатор Cisco 3640 рабочий релиз 12.3 программного обеспечения Cisco IOS (4) T
- Маршрутизатор B: Маршрутизатор Cisco 2621 рабочий релиз 12.3 программного обеспечения Cisco IOS (5)

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 в документах см. Cisco Technical Tips Conventions.

Общие сведения

В данном примере, когда хост 172.16.1.2 на Узле доступы тот же обращенный к IP хост на Узле B, это соединяется с 172.19.1.2 адресами, а не с фактическими 172.16.1.2 адресами. Когда хост на Узле B к Узлу доступов A, это соединяется с 172.18.1.2 адресами. NAT на маршрутизаторе A преобразует любой адрес 172.16.x.x в адрес, соответствующий записи узла 172.18.x.x. NAT на маршрутизаторе B изменяется 172.16. x. x для сходства с 172.19. x. x.

Крипто-функция на каждом маршрутизаторе шифрует преобразованный трафик через последовательные интерфейсы. Обратите внимание на то, что NAT происходит *перед* шифрованием на маршрутизаторе.

Примечание: Эта конфигурация только позволяет этим двум сетям связываться. Это не обеспечивает интернет-соединение. Вам нужны дополнительные пути к Интернету для подключения к местоположениям кроме этих двух узлов; другими словами, необходимо добавить другой маршрутизатор или межсетевой экран на каждой стороне с несколькими маршрутов, настроенными на хостах.

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 настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- Маршрутизатор A
- Маршрутизатор B

Маршрутизатор A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10 encr 3des hash md5
authentication pre-share crypto isakmp key cisco123
address 10.5.76.57 ! !--- These are the IPSec
parameters. crypto ipsec transform-set myset1 esp-3des
esp-md5-hmac ! ! crypto map mymap 10 ipsec-isakmp set
peer 10.5.76.57 set transform-set myset1 !--- Encrypt
traffic to the other side. match address 100 ! ! !
interface Serial0/0 description Interface to Internet ip
address 10.5.76.58 255.255.0.0 ip nat outside clockrate
128000 crypto map mymap ! interface Ethernet0/0 ip
address 172.16.1.1 255.255.255.0 no ip directed-
broadcast ip nat inside half-duplex ! ! !--- This is the
NAT traffic. ip nat inside source static network
172.16.0.0 172.18.0.0 /16 no-alias ip http server no ip
http secure-server ip classless ip route 0.0.0.0 0.0.0.0
Serial0/0 ! !--- Encrypt traffic to the other side.
access-list 100 permit ip 172.18.0.0 0.0.255.255
172.19.0.0 0.0.255.255 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! ! end
```

Маршрутизатор B

```
Current configuration : 1255 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-15
!
boot-start-marker
boot-end-marker
```

```
!
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- These are the IKE parameters. crypto isakmp policy
10 encr 3des hash md5 authentication pre-share crypto
isakmp key cisco123 address 10.5.76.58 ! !--- These are
the IPSec parameters. crypto ipsec transform-set myset1
esp-3des esp-md5-hmac ! crypto map mymap 10 ipsec-isakmp
set peer 10.5.76.58 set transform-set myset1 !---
Encrypt traffic to the other side. match address 100 ! !
interface FastEthernet0/0 ip address 172.16.1.1
255.255.255.0 ip nat inside duplex auto speed auto !
interface Serial0/0 description Interface to Internet ip
address 10.5.76.57 255.255.0.0 ip nat outside crypto map
mymap ! !--- This is the NAT traffic. ip nat inside
source static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server no ip http secure-server ip classless ip
route 0.0.0.0 0.0.0.0 Serial0/0 ! !--- Encrypt traffic
to the other side. access-list 100 permit ip 172.19.0.0
0.0.255.255 172.18.0.0 0.0.255.255 ! ! line con 0 line
aux 0 line vty 0 4 ! ! ! end
```

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.**
- **команда show crypto isakmp sa вЂ отображает сопоставления безопасности, соответствующие первому этапу.**
- **show ip nat translation** — Показывает текущие NAT - преобразования в использовании.

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 вызывать команды debug, обратитесь к разделу Важные сведения о командах отладки.

- 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.
- "debug crypto engine" - отображается зашифрованный трафик.

Дополнительные сведения

- Страница поддержки IPSec
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Техническая поддержка - Cisco Systems