Настройка сети Private-to-Private туннеля IPSec маршрутизатора с NAT и статическим свойством

Содержание

Введение

Этот пример конфигурации показывает, как:

- Зашифровать трафик между двумя частными сетями (10.1.1.x и 172.16.1.x).
- Назначить статический IP-адрес (внешний адрес 200.1.1.25) устройству сети в 10.1.1.3.

Вы можете использовать списки контроля доступа (ACL), чтобы указать маршрутизатору не применять трансляцию сетевых адресов (NAT) к трафику из частной сети в частную сеть, который затем шифруется и направляется в туннель, как только покидает маршрутизатор. В сети 10.1.1.x в этом примере конфигурации существует также статическая NAT для внутреннего сервера. Этот пример использует параметр route-map в команде NAT, чтобы остановить работу NAT, если трафик уже направлен через зашифрованный туннель.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Программное обеспечение Cisco IOS®, версия 12.3.14T
- Два маршрутизатора Cisco

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 см. в документе Условные обозначения технических терминов Cisco.

Почему инструкция запрета в ACL указывает на трафик NAT?

При использовании Cisco IOS IPsec или VPN вы, в принципе, заменяете сеть туннелем. Вы заменяете облако Интернет туннелем Cisco IOS IPsec, который на приведенной ниже диаграмме проходит от 200.1.1.1 к 100.1.1.1. Необходимо сделать сеть прозрачной с точки зрения двух частных сетей LAN, соединенных друг с другом туннелем. По этой причине обычно не используют NAT для трафика, который проходит из одной частной LAN в другую, удаленную частную LAN. Необходимо видеть пакеты, которые приходят из сети маршрутизатора 2 с исходным IP-адресом из сети 10.1.1.0/24 вместо 200.1.1.1, когда эти пакеты достигают внутренней сети маршрутизатора 3.

Подробнее о настройке NAT см. "Порядок работы NAT". В этом документе показывается, что NAT происходит до криптографической проверки на этапе, когда пакеты проходят изнутри наружу. Поэтому нужно указать эту информацию в конфигурации.

```
ip nat inside source list 122 interface Ethernet0/1 overload

access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

Примечание: Также возможно создать туннель и все еще использовать NAT. Вы задаете трафик NAT как "представляющий интерес трафик для IPsec" (называемый ACL 101 в других разделах этого документа) в этом сценарии. Подробнее о построении туннеля с активной NAT см. "Настройка IPsec-туннеля между маршрутизаторами с дублированными подсетями LAN".

И все же насчет статической NAT - почему я не могу обратиться к тому адресу через туннель IPsec?

Эта установка включает также статическую NAT "один-в-один" для сервера в 10.1.1.3. Он преобразуется NAT в 200.1.1.25, так что к нему могут получить доступ пользователи Интернет. Введите следующую команду:

```
ip nat inside source static 10.1.1.3 200.1.1.25
```
Эта статическая NAT не дает пользователям в сети 172.16.1.x получать доступ к 10.1.1.3 через зашифрованный туннель. Поэтому необходимо запретить преобразовывать зашифрованный трафик через NAT с помощью ACL 122. Однако команда статической NAT всегда предпочтительнее, чем генерирование инструкции NAT для всех соединений, направленных из и к 10.1.1.3. Инструкция статической NAT конкретно не запрещает обработку зашифрованного трафика NAT. Ответы с 10.1.1.3 транслируются NAT в 200.1.1.25, когда пользователь в сети 172.16.1.x соединяется с 10.1.1.3 и, таким образом, не возвращаются обратно через зашифрованный туннель (NAT происходит до шифрования).

Следует запретить обработку зашифрованного трафика NAT (даже статически, "один-в-один") с помощью команды route-map в инструкции статической NAT.

Примечание: Опция route-map на статическом NAT только поддерживается от Cisco IOS Software Release 12.2 (4) T и позднее. Подробнее см. "NATвозможность использовать карты маршрутов со статическими преобразованиями".

Следует задать данные дополнительные команды, чтобы разрешить зашифрованный доступ к 10.1.1.3, узлу, подвергаемому статической NAT:

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```
Эти инструкции указывают маршрутизатору применять статическую NAT только к трафику, который соответствует ACL 150. ACL 150 гласит, что не следует применять NAT к трафику, исходящему из 10.1.1.3 и направляющемуся через зашифрованный туннель к 172.16.1.x. Однако ее следует применять ко всему остальному трафику, исходящему из 10.1.1.3 (трафик на основе Интернет).

Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- Маршрутизатор 2
- Маршрутизатор 3

R2- Настройка маршрутизатора

```
R2#write terminal
Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
 authentication pre-share
!
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 175 interface Ethernet1/0
overload
!
```

```
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

R3 - конфигурация маршрутизатора

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
```

```
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 122 interface Ethernet1/0
overload
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: access-list
150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Подробнее см. "Устранение неполадок IP-безопасности – общие сведения и использование команд debug".

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

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

- **debug crypto ipsec sa**– показывает процесс согласования по протоколу IPSec на этапе 2.
- **debug crypto isakmp sa** — Видит Isakmp - согласование фазы 1.
- **debug crypto engine**– служит для просмотра шифруемых сеансов.

Дополнительные сведения

- IPSec Negotiation/IKE Protocols - Cisco Systems
- Cisco Systems – техническая поддержка и документация