Настройка IPSec маршрутизатор-маршрутизатор динамический-статический с NAT

Содержание

Введение

В этом примере конфигурации удаленный маршрутизатор получает IP-адрес через часть PPP, называемую управляющим протоколом для IP (IPCP). Удаленный маршрутизатор использует IP-адрес для подключения к центральному маршрутизатору. Данная конфигурация позволяет центральному маршрутизатору принимать динамические IPSec-соединения. Удаленный маршрутизатор использует преобразование сетевых адресов (NAT) для того, чтобы присоединить находящиеся за ним устройства с частными адресами к сети за центральным маршрутизатором, использующей частные адреса. Удаленный маршрутизатор знает оконечное устройство и может инициировать подключения к центральному маршрутизатору. Но центральный маршрутизатор не знает оконечного устройства, поэтому он не может проводить соединения к удаленному маршрутизатору.

В этом примере dr_whoovie – удаленный маршрутизатор, а sam-i-am – центральный. Список контроля доступа определяет состав трафика, подлежащего шифрованию, таким образом маршрутизатор dr_whoovie знает, какой трафик шифровать и где расположено оконечное устройство sam-i-am. Подключение должен инициировать удаленный маршрутизатор. Обе стороны выполняют перегрузку NAT.

Предварительные условия

Требования

Данный документ требует базовых знаний протокола IPSec. Дополнительные сведения о протоколе IPSec можно найти в документе Обзор протокола шифрования для защиты IP-пакетов (IPSec).

Используемые компоненты

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

- ПО Cisco IOS®, выпуск 12.2(24a)
- Маршрутизаторы Cisco серии 2500

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.

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:

- sam-i-am
- dr_whoovie

sam-i-am

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log up time
no service password-encryption
!
hostname sam-i-am
!
ip subnet-zero
!
```

```
!--- These are the IKE policies. crypto isakmp policy 1
!--- Defines an Internet Key Exchange (IKE) policy. !---
Use the crypto isakmp policy command !--- in global
configuration mode. !--- IKE policies define a set of
parameters to be used !--- during the IKE phase I
negotiation. hash md5 authentication pre-share !---
Specifies pre-shared keys as the authentication method.
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 !---
Configures a pre-shared authentication key, !--- used in
global configuration mode. ! !--- These are the IPSec
policies. crypto ipsec transform-set rtpset esp-des esp-
md5-hmac !--- A transform set is an acceptable
combination !--- of security protocols and algorithms.
!--- This command defines a transform set !--- that has
to be matched on the peer router. crypto dynamic-map
rtpmap 10 !--- Use dynamic crypto maps to create policy
templates !--- that can be used to process negotiation
requests !--- for new security associations (SA) from a
remote IPSec peer, !--- even if you do not know all of
the crypto map parameters !--- required to communicate
with the remote peer, !--- such as the IP address of the
peer. set transform-set rtpset !--- Configure IPSec to
use the transform set "rtpset" !--- that was defined
previously. match address 115 !--- Assign an extended
access list to a crypto map entry !--- that is used by
IPSec to determine which traffic !--- should be
protected by crypto and which traffic !--- does not need
crypto protection. crypto map rtptrans 10 ipsec-isakmp
dynamic rtpmap !--- Specifies that this crypto map entry
is to reference !--- a preexisting dynamic crypto map. !
interface Ethernet0 ip address 10.2.2.3 255.255.255.0 no
ip directed-broadcast ip nat inside !--- This indicates
that the interface is connected to the !--- inside
network, which is subject to NAT translation. no mop
enabled ! interface Serial0 ip address 99.99.99.1
255.255.255.0 no ip directed-broadcast ip nat outside !-
-- This indicates that the interface is connected !---
to the outside network. crypto map rtptrans !--- Use the
crypto map interface configuration command !--- to apply
a previously defined crypto map set to an interface. !
ip nat inside source route-map nonat interface Serial0
overload !--- Except the private network from the NAT
process. ip classless ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server ! access-list 115 permit ip 10.2.2.0
0.0.0.255 10.1.1.0 0.0.0.255 access-list 115 deny ip
10.2.2.0 0.0.0.255 any !--- Include the private-network-
to-private-network traffic !--- in the encryption
process. access-list 120 deny ip 10.2.2.0 0.0.0.255
10.1.1.0 0.0.0.255 access-list 120 permit ip 10.2.2.0
0.0.0.255 any !--- Except the private network from the
NAT process. route-map nonat permit 10 match ip address
120 ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end
```

dr_whoovie

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
```

```
ip subnet-zero
!
!--- These are the IKE policies. crypto isakmp policy 1
!--- Defines an Internet Key Exchange (IKE) policy. !---
Use the crypto isakmp policy command !--- in global
configuration mode. !--- IKE policies define a set of
parameters to be used !--- during the IKE phase I
negotiation. hash md5 authentication pre-share !---
Specifies pre-shared keys as the authentication method.
crypto isakmp key cisco123 address 99.99.99.1 !---
Configures a pre-shared authentication key, !--- used in
global configuration mode. ! !--- These are the IPSec
policies. crypto ipsec transform-set rtpset esp-des esp-
md5-hmac !--- A transform set is an acceptable
combination !--- of security protocols and algorithms.
!--- This command defines a transform set !--- that has
to be matched on the peer router. ! crypto map rtp 1
ipsec-isakmp !--- Creates a crypto map and indicates
that IKE will be used !--- to establish the IPSec SAs
for protecting !--- the traffic specified by this crypto
map entry. set peer 99.99.99.1 !--- Use the set peer
command to specify an IPSec peer in a crypto map entry.
set transform-set rtpset !--- Configure IPSec to use the
transform set "rtpset" !--- that was defined previously.
match address 115 !--- Include the private-network-to-
private-network traffic !--- in the encryption process.
! interface Ethernet0 ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast ip nat inside !--- This
indicates that the interface is connected to the !---
inside network, which is subject to NAT translation. no
mop enabled ! interface Serial0 ip address negotiated !-
-- Specifies that the IP address for this interface !---
is obtained via PPP/IPCP address negotiation. !--- This
example was set up in a lab with an IP address !---
assigned with IPCP. no ip directed-broadcast ip nat
outside !--- This indicates that the interface is
connected !--- to the outside network. encapsulation ppp
no ip mroute-cache no ip route-cache crypto map rtp !---
Use the crypto map interface configuration command !---
to apply a previously defined crypto map set to an
interface. ip nat inside source route-map nonat
interface Serial0 overload !--- Except the private
network from the NAT process. ip classless ip route
0.0.0.0 0.0.0.0 Serial0 no ip http server ! access-list
115 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 115 deny ip 10.1.1.0 0.0.0.255 any !---
Include the private-network-to-private-network traffic
!--- in the encryption process. access-list 120 deny ip
10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255 access-list 120
permit ip 10.1.1.0 0.0.0.255 any !--- Except the private
network from the NAT process. dialer-list 1 protocol ip
permit dialer-list 1 protocol ipx permit route-map nonat
permit 10 match ip address 120 ! line con 0 transport
input none line aux 0 line vty 0 4 password ww login !
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 ping —— Используется для диагностики подключения основной сетиВ этом примере показан эхозапрос от интерфейса Ethernet 10.1.1.1 на маршрутизаторе dr_whoovie к интерфейсу Ethernet 10.2.2.3 на маршрутизаторе sam-i-am.`dr_whoovie# ping Protocol [ip]: Target IP address: 10.2.2.3 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 10.1.1.1 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.2.2.3, timeout is 2 seconds: Packet sent with a source address of 10.1.1.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 36/38/40 ms`
- show crypto ipsec sa– показывает ассоциации безопасности, соответствующие второму этапу.
- show crypto isakmp sa– показывает ассоциации безопасности, соответствующие первому этапу.

Образец выходных данных

Ниже показаны выходные данные при выполнении команды show crypto ipsec sa на маршрутизаторе-концентраторе.

`sam-i-am# **show crypto ipsec sa** interface: Serial0 Crypto map tag: rtptrans, local addr. 99.99.99.1 **local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)** current_peer: 100.100.100.1 PERMIT, flags={} #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6 #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 0, #recv errors 0 **local crypto endpt.: 99.99.99.1, remote crypto endpt.: 100.100.100.1** path mtu 1500, ip mtu 1500, ip mtu interface Serial0 current outbound spi: 52456533 **inbound esp sas:** spi: 0x6462305C(1684156508) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: rtptrans sa timing: remaining key lifetime (k/sec): (4607999/3510) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: **outbound esp sas:** spi: 0x52456533(1380279603) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: rtptrans sa timing: remaining key lifetime (k/sec): (4607999/3510) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:`

Эта команда показывает ассоциации безопасности IPSec, устанавливаемые между устройствами с одноранговым соединением. Туннель с шифрованием соединяет интерфейс 100.100.100.1 на маршрутизаторе dr_whoovie с интерфейсом 99.99.99.1 на маршрутизаторе sam-i-am. Этот туннель обслуживает трафик между сетями 10.2.2.3 и 10.1.1.1. Входящий и исходящий потоки формируют две ассоциации безопасности (SA) протокола инкапсулирующей защиты содержимого (ESP). Туннель устанавливается даже несмотря на то, что маршрутизатор sam-i-am не знает IP-адрес другой стороны (100.100.100.1). Ассоциации безопасности заголовка аутентификации (AH) не используются, поскольку AH не настроен.

В примерах выходных данных видно, что последовательный интерфейс 0 на маршрутизаторе dr_whoovie получает IP-адрес 100.100.100.1 посредством протокола IPCP.

- До согласования IP-адреса:`dr_whoovie#**show interface serial0** Serial0 is up, line protocol is up Hardware is HD64570 **Internet address will be negotiated using IPCP** MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, loopback not set`

- После согласования IP-адреса:`dr_whoovie#`**`show interface serial0`** `Serial0 is up, line protocol is up Hardware is HD64570` **`Internet address is 100.100.100.1/32`** `MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, loopback not set`

Этот пример подготовлен в лаборатории с назначением IP-адреса на удаленной стороне интерфейса serial 0 маршрутизатора dr_whoovie командой peer default ip address. Пул IP-адресов определен командой ip local pool на удаленной стороне.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

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".

- 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.
- debug ip nat detailed (дополнительно) – проверяет работоспособность функции NAT, сообщая информацию о каждом пакете, преобразуемом маршрутизатором.**Внимание. :** Эта команда генерирует большое количество выходных данных. Используйте эту команду только при малом трафике в IP-сети.
- clear crypto isakmp– удаляет ассоциации безопасности, связанные с 1-м этапом.
- clear crypto sa– удаляет ассоциации безопасности, связанные со 2-м этапом.
- clear ip nat translation– удаляет динамические преобразования NAT из таблицы преобразования.

Дополнительные сведения

- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems