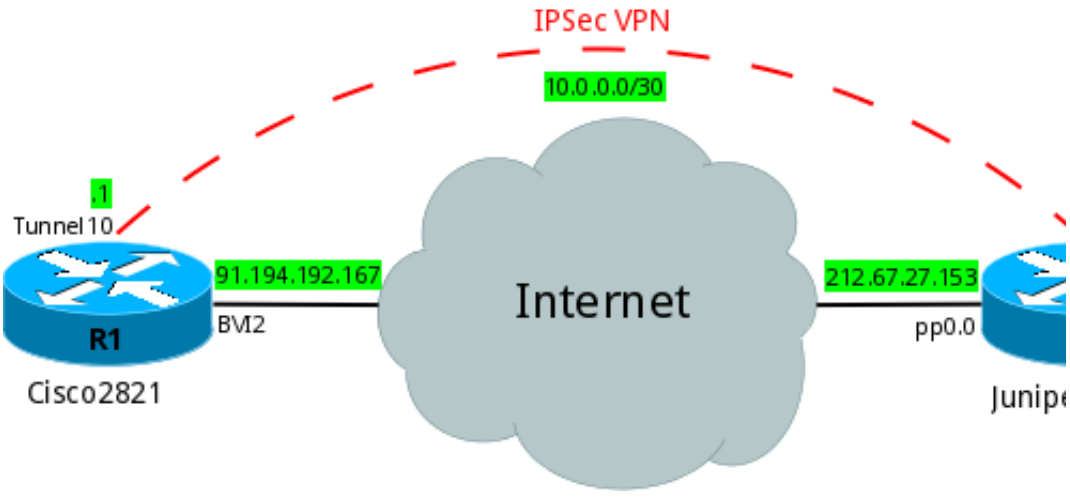
Практический пример настройки IPSec VPN между маршрутизатором Cisco серии ISR и Juniper SRX

30.03.2010 21:36 Григорий Марфицин

В данной статье я приведу практический пример настройки IPSec VPN между двумя устройствами: маршрутизатором Cisco2821 и Juniper SRX100.

Логическая схема для данного примера изображена на рисунке.



Маршрутизатор Cisco2821 использует следующее программное обеспечение Cisco IOS.

```
R1#show version | include IOS
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
R1#
```

Juniper SRX100 использует следующее программное обеспечение Junos.

```
root@R2> show version
Hostname: R2
Model: srx100-lm
JUNOS Software Release [10.0R2.10]

root@R2>
```

Juniper SRX100 имеет DSL-подключение к сети Интернет с использованием протокола PPPoE, в связи с этим его внешним интерфейсом является логический интерфейс pp0.0. (обозначен на логической схеме). Маршрутизатор Cisco2821 подключен к сети Интернет с помощью группы Ethernet-интерфейсов, его внешним интерфейсом является логический интерфейс BVI2 (обозначен на логической схеме).

НОВОСТИ

Адрес источника IP-пакета и ip local policy

Практический пример настройки IPSec VPN между маршрутиза Cisco серии ISR и Juniper SRX

Трансляция сетевых адресов outside-to-inside с использован механизма reversible

Условное анонсирова маршрутов BGP (Conditionall Advertising BGP Routes)

Cisco Integrated Services Routers Generation 2

Приступим к настройке. Сначала настроим R1.

Политики IKE.

R1

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption des
R1(config-isakmp)#group 2
R1(config-isakmp)#hash sha
```

Общий ключ IKE для участников туннеля.

R1

```
R1(config)#crypto isakmp key password address 212.67.27.153
```

Параметры безопасности IPSec.

R1

```
R1(config)#crypto ipsec transform-set DES_SHA esp-des esp-sha-hmac
```

Профиль параметров IPSec.

R1

```
R1(config)#crypto ipsec profile VTI
R1(ipsec-profile)#set transform-set DES_SHA
```

Настраиваемый IPSec VPN будет построен с использованием виртуальных туннельных интерфейсов. Данный способ удобен тем, что туннелируется и шифруется любой IP-трафик, направляемый в интерфейс туннеля.

Виртуальный туннельный интерфейс.

R1

```
R1(config)#interface Tunnel10
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#tunnel source BVI2
R1(config-if)#tunnel destination 212.67.27.153
R1(config-if)#tunnel mode ipsec ipv4
R1(config-if)#tunnel protection ipsec profile VTI
```

Настройка R1 окончена, настраиваем R2.

Политики IKE.

R2

```
root@R2# set security ike policy IKE1 mode main
root@R2# set security ike policy IKE1 proposal-set compatible
root@R2# set security ike policy IKE1 pre-shared-key ascii-text
password
```

Параметры локальной точки терминирования протокола IKE.

R2

```
root@R2# set security ike gateway R1 ike-policy IKE1
root@R2# set security ike gateway R1 address 91.194.192.167
root@R2# set security ike gateway R1 external-interface pp0
```

Политики IPSec (фаза 2).

R2

```
root@R2# set security ipsec policy IKE2 perfect-forward-secrecy
keys group2
root@R2# set security ipsec policy IKE2 proposal-set compatible
```

Виртуальный туннельный интерфейс.

R2

```
root@R2# set interfaces st0 unit 0 family inet address 10.0.0.2/30
```

Параметры локальной точки терминирования IPSec (фаза 2).

R2

```
root@R2# set security ipsec vpn R1_R2 bind-interface st0.0
root@R2# set security ipsec vpn R1_R2 ike gateway R1
root@R2# set security ipsec vpn R1_R2 ike ipsec-policy IKE2
root@R2# set security ipsec vpn R1_R2 establish-tunnels
immediately
```

Настройка IPSec VPN завершена. Теперь необходимо его протестировать. Убедимся в наличии согласованных параметров безопасности для первой и второй фазы (IKE SA и IPSec SA) на устройствах R1 и R2.

Результат команды **show crypto isakmp sa detail** для R1.

```
R1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Has

1043  91.194.192.167  212.67.27.153            ACTIVE des  sha
       Engine-id:Conn-id =  SW:43

IPv6 Crypto ISAKMP SA

R1#
```

Результат команды **show crypto ipsec sa address** для R1.

```
R1#show crypto ipsec sa address
fvrf/address: (none)/10.0.0.1
   protocol: ESP

fvrf/address: (none)/91.194.192.167
   protocol: ESP
      spi: 0x27F11503(670110979)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2121, flow_id: NETGX:121, sibling_flags 80000
        sa timing: remaining key lifetime (k/sec): (4472410/79
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

fvrf/address: (none)/212.67.27.153
   protocol: ESP
      spi: 0x2E9241D2(781337042)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2122, flow_id: NETGX:122, sibling_flags 80000
        sa timing: remaining key lifetime (k/sec): (4472410/79
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

R1#
```

Результат команды **show security ike security-associations** для R2.

```
root@R2> show security ike security-associations
Index   Remote Address  State  Initiator cookie  Responder coo
81      91.194.192.167  UP     84cb6f841b8c796e  907eea38c5ee6

root@R2>
```

Результат команды **show security ipsec security-associations** для R2.

```
root@R2> show security ipsec security-associations
  Total active tunnels: 1
  ID    Gateway          Port  Algorithm       SPI      Life:s
  <131073 91.194.192.167 500   ESP:des/ sha1   ebe55d1a 3590/
  >131073 91.194.192.167 500   ESP:des/ sha1   74fb879c 3590/

root@R2>
```

Из листингов видно, что параметры безопасности для первой и второй фазы согласованы. Пропингуем удаленный конец туннеля каждого устройства.

Результат команды **ping 10.0.0.2** для R1.

```
R1#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 secon
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28
R1#
```

Результат команды **ping 10.0.0.1** для R2.

```
root@R2> ping 10.0.0.1 count 5
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=255 time=30.953 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=30.411 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=29.883 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=31.906 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=255 time=29.747 ms

--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.747/30.580/31.906/0.788 ms

root@R2>
```

Листинги подтверждают, что IPSec VPN между R1 и R2 настроен и функционирует корректно.

YOU ARE HERE: СТАТЬИ ▸ ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN) ▸ ПРАКТИЧЕСКИЙ ПРИМЕР НАСТРОЙКИ IPSEC VPN МЕЖДУ МАРШРУТИЗАТОРОМ CISCO СЕРИИ ISR И JUNIPER SRX TOP