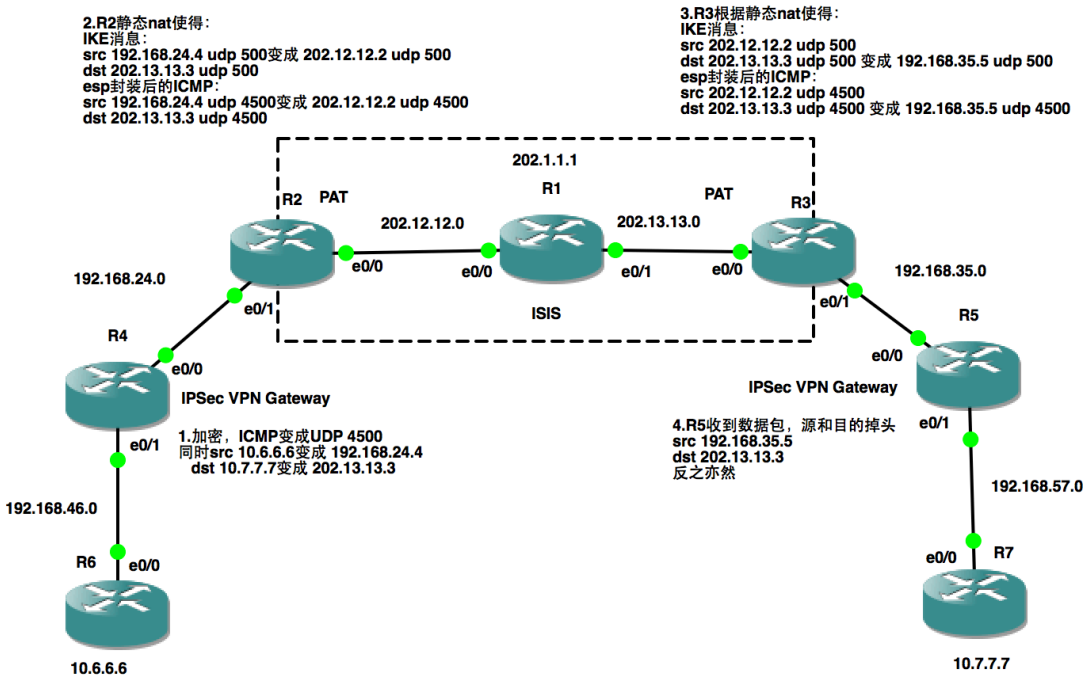
实验： IPsec NAT 分离

2015年1月26日 星期一　下午5:39



R1

```
interface Loopback0
 ip address 202.1.1.1 255.255.255.255
 ip router isis cisco
!
interface Ethernet0/0
 ip address 202.12.12.1 255.255.255.0
 ip router isis cisco
!
interface Ethernet0/1
 ip address 202.13.13.1 255.255.255.0
 ip router isis cisco
!
router isis cisco
 net 49.0001.ca01.0bbc.0000.00
 is-type level-2-only
```

R2

```
interface Ethernet0/0
 ip address 202.12.12.2 255.255.255.0
 ip router isis cisco
 ip nat outside
!
interface Ethernet0/1
 ip address 192.168.24.2 255.255.255.0
 ip nat inside
!
router isis cisco
 net 49.0001.ca02.0bbc.0000.00
 is-type level-2-only
!
router rip
```

R3

```
interface Ethernet0/0
 ip address 202.13.13.3 255.255.255.0
 ip router isis cisco
 ip nat outside
!
interface Ethernet0/1
 ip address 192.168.35.3 255.255.255.0
 ip nat inside
!
router isis cisco
 net 49.0001.ca03.0bbc.0000.00
 is-type level-2-only
!
router rip
```

```
 version 2
 network 192.168.24.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 202.12.12.1
!
ip nat inside source list allow interface Ethernet0/0 overload
//把发往外部数据的源地址IP改为e0/0
ip nat inside source static udp 192.168.24.4 500 202.12.12.2 500
extendable //500是IKE守护进程端口
ip nat inside source static udp 192.168.24.4 4500 202.12.12.2
4500 extendable//4500是esp封装包端口
```

```
 version 2
 network 192.168.35.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 202.13.13.1
!
ip nat inside source list allow interface Ethernet0/0 overload
ip nat inside source static udp 192.168.35.5 500 202.13.13.3
500 extendable
ip nat inside source static udp 192.168.35.5 4500 202.13.13.3
4500 extendable
```

R4

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco address 202.13.13.3
!//对端NAT出接口地址
crypto ipsec transform-set ZJW esp-aes esp-md5-hmac
!
crypto map ZJW 10 ipsec-isakmp
 set peer 202.13.13.3
 set transform-set ZJW
 match address 100
!
interface Ethernet0/0
 ip address 192.168.24.4 255.255.255.0
 half-duplex
 crypto map ZJW
!
interface Ethernet0/1
 ip address 192.168.46.4 255.255.255.0
 half-duplex
!
router rip
 version 2
 network 192.168.24.0
 network 192.168.46.0
 no auto-summary
!
access-list 100 permit ip host 10.6.6.6 host 10.7.7.7
```

R5

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco address 202.12.12.2
!
crypto ipsec transform-set ZJW esp-aes esp-md5-hmac
!
crypto map ZJW 10 ipsec-isakmp
 set peer 202.12.12.2
 set transform-set ZJW
 match address 100
!
interface Ethernet0/0
 ip address 192.168.35.5 255.255.255.0
 half-duplex
 crypto map ZJW
!
interface Ethernet0/1
 ip address 192.168.57.5 255.255.255.0
 half-duplex
!
router rip
 version 2
 network 192.168.35.0
 network 192.168.57.0
 no auto-summary
!
access-list 100 permit ip host 10.7.7.7 host 10.6.6.6
```

R6

```
interface Loopback0
 ip address 10.6.6.6 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.46.6 255.255.255.0
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.46.0
 no auto-summary
```

R7

```
interface Loopback0
 ip address 10.7.7.7 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.57.7 255.255.255.0
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.57.0
 no auto-summary
```

Created with Outline