

知 防火墙配置ipsec业务如何通过安全NAT功能deny感兴趣流

NAT

王奎银 2021-11-12 发表

问题描述

组网不涉及

场景：防火墙配置ipsec时，同时使用全局NAT做源地址转换，因为全局NAT下在全局配置方式不同于接口NAT，易引发一些网上问题

解决方法

配置方式如下：

- 1.配置感兴趣流对应的源地址的对象组

```
#
object-group ip address sou
  0 network subnet 10.150.0.0 255.255.0.0
```

#

- 2.配置感兴趣流对应的目的地址的对象组

```
#
object-group ip address dest
  10 network subnet 10.100.0.0 255.255.0.0
```

#

3. 配置全局NAT对应的源地址转换规则

```
#
nat global-policy
rule name 123
  source-zone trust
  destination-zone untrust
  action snat easy-ip
```

#

4. 配置deny掉感兴趣流的全局NAT规则

```
nat global-policy
rule name test
  source-ip sou
  destination-ip dest
  source-zone trust
  destination-zone untrust
  action snat no-nat
```

注意事项：

1. 如果新配置的deny规则在后面，可以移动规则（move）到前面进行deny掉感兴趣流

RBM_P[M9010_1-nat-global-policy]rule ?

move Move the rule

name Specify a name for the NAT rule

2. 全局NAT优先级高于接口NAT

