Juniper基本配置

2016年6月9日 14:42

Juniper防火墙系统级别的配置
包括设置主机名、设置登录用户、设置系统改时间和时区

Juniper防火墙网络配置
配置接口IP地址
配置Zone
配置路由（静态路由、RIP、OSPF、重分发）

配置主机名：set system host-name 主机名
设置Root密码：set system root-authentication plain-test-password
root密码必须包含字母和数字，长度最小为6位

配置时区和时间
一定要把配置时区的命令提交以后再配置时间
配置时间是在操作模式下（>模式）下进行，命令行中出现“>”的表示该操作在操作模式下进行

配置时区：set system time-zone Asia/Shanghai
配置时间：>set date yyyymmddhhmm.ss
查看时间和时区：>show system uptime

设置DNS服务器：set system name-server DNS服务器的地址
设置与查看NTP
设置NTP：set system ntp server NTP服务器的地址
>show ntp associations
>show ntp status

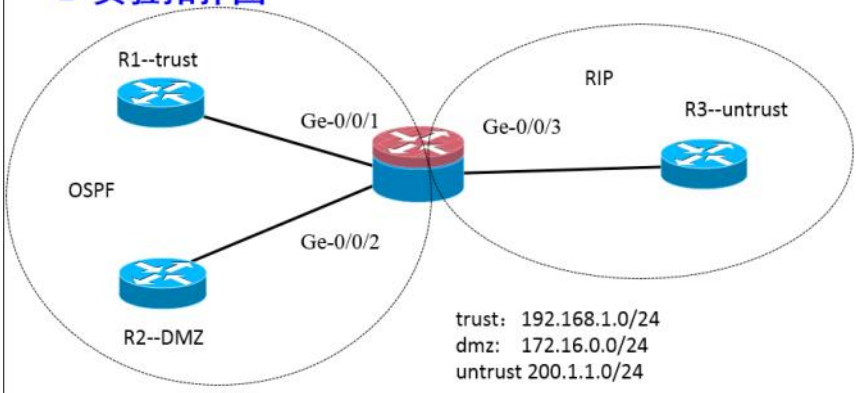
创建管理用户
set system login user 用户名 class 用户类型 authentication plain-text-password
用户类型：
operator：可以进行网络操作和查看
read-only：仅可以查看配置
super-user：权限仅次于root

如果想重置这个用户的密码，就把创建用户的命令重新输入一遍

防火墙必须设置区域：zone
trust：信任区域，一般为连接局域网的用户区的接口设置为trust，Cisco ASA把trust解释为inside，trust区域通常是私有IP地址
dmz：非军事化区域，一般为连接局域网中的服务器的区域的接口设置为dmz，dmz区域也是私有IP地址
untrust：非信任区域，一般为接Internet的接口设置为untrust，untrust可以是私有IP地址，也可以是公网IP地址

Cisco ASA防火墙默认有接口安全级别：inside > DMZ > outside
Juniper SRX没有默认的安全级别

■ 实验拓扑图



在配置接口IP地址的时候
使用> show interface terse查看接口的物理名称

给接口配置IP地址：

```
set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 172.16.0.1/24
set interfaces ge-0/0/3 unit 0 family inet address 200.1.1.1/24
```

Juniper在配置的时候不支持点分十进制的子网掩码，所有的子网掩码必须写成位数

给Juniper配置IP地址，只能配置在子接口上
Juniper的接口也支持二层模式，支持划分到VLAN或者改成trunk，模拟器不支持

防火墙的接口必须加入Zone以后才可以通信
set security zones security-zone trust interfaces ge-0/0/1.0 host-inbound-traffic system-services ping
set security zones security-zone dmz interfaces ge-0/0/2.0 host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/3.0 host-inbound-traffic system-services ping

注意：
如果在写接口的时候，只写ge-0/0/3，则系统会认为你操作的是ge-0/0/3.0
如果你的子接口编号不是0
在把接口加入zone的时候，就一定要写明子接口的编号

设置静态路由与默认路由
set routing-options static route 网段/掩码位数 next-hop 下一跳地址
set routing-options static route 0.0.0.0/0 next-hop 下一跳地址

设置RIP

set protocols rip group 组名 neighbor 需要发布的接口（必须在该接口上放行rip协议）
本案例的配置：
在Ge0/0/3上放行RIP
set security zones security-zone untrust interfaces ge-0/0/3.0 host-inbound-traffic protocols rip
把Ge0/0/3接口宣告RIP
set protocols rip group untrust_rip neighbor ge-0/0/3.0

设置OSPF

在Ge-0/0/1和Ge-0/0/2上放行OSPF
set security zones security-zone trust interfaces ge-0/0/1.0 host-inbound-traffic protocols ospf
set security zones security-zone dmz interfaces ge-0/0/2.0 host-inbound-traffic protocols ospf

把Ge-0/0/1和Ge-0/0/2宣告到OSPF中
set protocols ospf area 0.0.0.0 interface ge-0/0/1.0
set protocols ospf area 0.0.0.0 interface ge-0/0/2.0

查看OSPF
root@Test-SRX240# run show ospf neighbor

Address	Interface	State	ID	Pri	Dead
192.168.1.2	ge-0/0/1.0	Full	1.1.1.1	1	36
172.16.0.2	ge-0/0/2.0	Init	2.2.2.2	1	34

把RIP重分发到OSPF

设置策略，名称为R-into-O，包含协议为rip，策略的操作设置为accpet
set policy-options policy-statement R-into-O from protocol rip
set policy-options policy-statement R-into-O then accept

设置OSPF，调用策略R-into-O
set protocols ospf export R-into-O

把OSPF重分发到RIP

设置策略，名称为O-into-R，包含协议OSPF，策略的操作设置为accept
set policy-options policy-statement R-into-O from protocol rip
set policy-options policy-statement R-into-O then accept

设置RIP，调用策略O-into-R
set protocols rip group untrust_rip export O-into-R

放行trust到untrust的所有流量
set security policies from-zone trust to-zone untrust policy PERMITANY match source-address any
set security policies from-zone trust to-zone untrust policy PERMITANY match destination-address any
set security policies from-zone trust to-zone untrust policy PERMITANY match application any
set security policies from-zone trust to-zone untrust policy PERMITANY then permit

设置SSH远程访问
开启SSH服务：set system services ssh
禁止ROOT使用SSH远程登录：set system services ssh root-login deny

在相应的接口上放行SSH流量
set security zones security-zone trust interfaces ge-0/0/1.0 host-inbound-traffic system-services ssh