ICG2000D/ICG3000F系列路由器允许指定范围内的主机互相访问命令行配置

ACL zhiliao_vhNCR 2018-11-25 发表

组网及说明

1 配置需求或说明

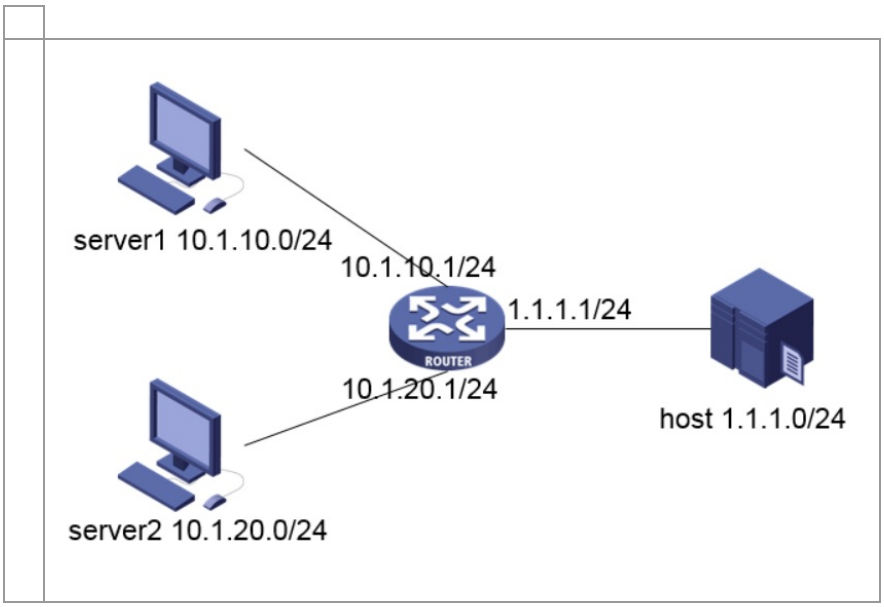
1.1适用产品系列

本案例适用于如ICG2000D、ICG3000F系列的路由器。

1.2配置需求及实现的效果

MSR路由器作为下面三个网段，10.1.10.0/24网段、10.1.20.0/24网段和1.1.1.0/24网段的网关。通过配置ACL，仅允许1.1.1.0/24网段的用户访问10.1.10.0/24网段的服务器，不允许访问10.1.20.0/24网段的服务器。网关地址分别为interface Vlan-interface1 1.1.1.1/24，interface Vlan-interface10 10.1.10.1/24，interface Vlan-interface20 10.1.20.1/24。

2 组网图



配置步骤

3 配置步骤

3.1配置acl，接口下下发过滤策略，调用acl

 # 创建IPv4高级ACL 3000，配置两条规则，分别为允许源地址为1.1.10/24网段，目的地址为10.1.10.0/24网段的IP报文通过，以及拒绝其它IP报文通过。

```
<H3C> system-view
[H3C] acl advanced 3000
[H3C-acl-ipv4-adv-3000] rule permit ip source 1.1.1.0 0.0.0.255 destination 10.1.10.0 0.0.0.255
[H3C-acl-ipv4-adv-3000] rule deny ip
[H3C-acl-ipv4-adv-3000] quit
```

 # 配置包过滤功能，应用IPv4高级ACL 3000，对网关接口收到的IP报文进行过滤。

```
[H3C] interface Vlan-interface1
[H3C-Vlan-interface1] packet-filter 3000 inbound
```

3.2检查配置效果

 # 执行display packet-filter命令查看包过滤功能的应用状态。

```
[H3C]display packet-filter interface vlan 1
Interface: Vlan-interface1
 Inbound policy:
  IPv4 ACL 3000
```

上述信息显示Vlan-interface1接口上已经正确应用了包过滤功能。

在1.1.1.0/24网段的主机上以10.1.10.0/24网段内的服务器为目的进行ping操作，返回正常应答信息；ping其它网段的主机，此操作返回请求超时信息。

4 保存配置信息

```
[H3C]save force
```

配置关键点