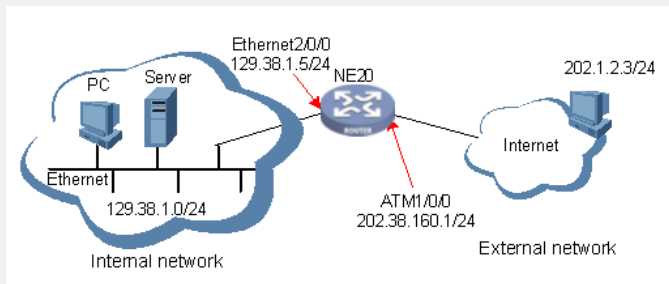


NE20/20E产品基于ACL的访问控制列表的配置

一 组网需求:

某公司采用NE20/20E系列路由器作为出口设备，通过ATM1/0/0接口和Internet进行连接，通过Ethernet2/0/0连接内部网络。要求NE20/20E系列路由器提供如下功能：仅允许内部特定主机访问外部网络、仅允许外部网络中的特定主机访问内部网络、禁止所有其它内部网络和外部网络之间的访问。

二 组网图:



图内NE20或者NE20E版本为VRP5.3。

三 配置步骤:

创建访问控制列表ACL3001，仅允许特定内部主机129.38.1.1和129.38.1.2访问外部网络，禁止其它所有主机的对外访问。

```
[NE20] acl number 3001
[NE20-acl-adv-3001] rule permit ip source 129.38.1.1 0
[NE20-acl-adv-3001] rule permit ip source 129.38.1.2 0
[NE20-acl-adv-3001] rule deny ip
```

创建访问控制列表ACL3002，仅允许特定外部主机202.1.2.3访问内部网络中的服务器129.38.1.105，禁止其它所有的对内访问。

```
[NE20] acl number 3002
[NE20-acl-adv-3002] rule permit tcp source 202.1.2.3 0 destination 129.38.1.10
```

5

```
[NE20-acl-adv-3002] rule deny ip
```

定义两个类，分别匹配ACL3001和ACL3002。

```
[NE20] traffic classifier class1
[NE20-classifier-class1] if-match acl 3001
[NE20] traffic classifier class2
[NE20-classifier-class2] if-match acl 3002
```

定义流行为，启动包过滤防火墙功能。

```
[NE20] traffic behavior behavior1
[NE20-behavior-behavior1] deny
```

定义两个QoS策略，为不同类的报文指定流行为。

```
[NE20] traffic policy mypolicy1
[NE20-trafficpolicy-mypolicy1] classifier class1 behavior behavior1
[NE20] traffic policy mypolicy2
[NE20-trafficpolicy-mypolicy2] classifier class2 behavior behavior1
```

在路由器的Ethernet2/0/0和ATM1/0/0接口上应用策略。

```
[NE20] interface ethernet 2/0/0
[NE20-Ethernet2/0/0] traffic-policy mypolicy1 inbound
[NE20-Ethernet2/0/0] quit
[NE20] interface atm 1/0/0
[NE20-ATM 1/0/0] traffic-policy mypolicy2 inbound
```

四 配置关键点:

无