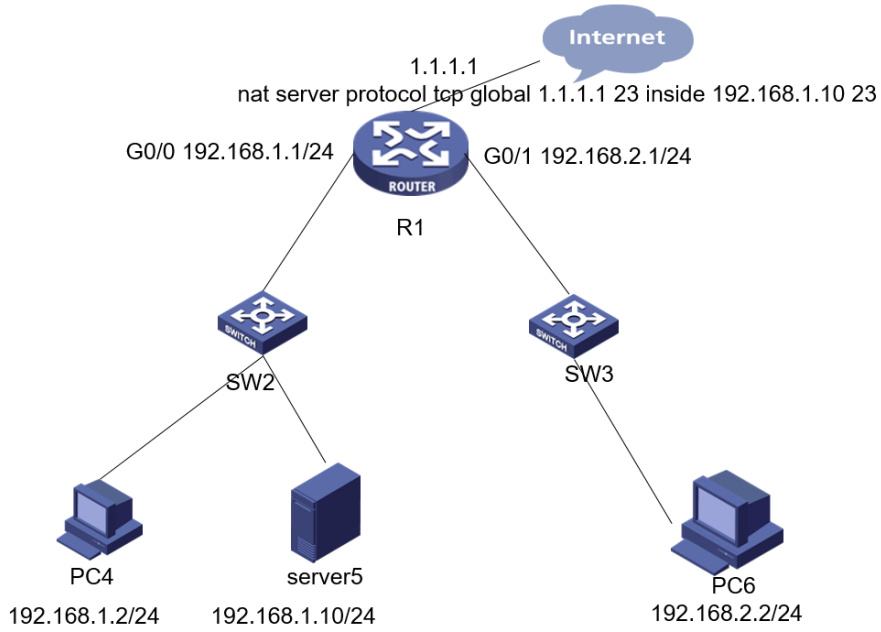
用nat outbound和nat server 实现内网用公网ip访问内部服务器

NAT 胡琪 2020-06-23 发表

组网及说明

1.组网



问题描述

2.需求

不使用nat hairpin,通过做nat server和nat outbound来实现在内网通过公网地址访问内部服务器。

过程分析

3.关键配置

```
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
//终端和服务器在同一网段的时候必须要做源地址转换（不然服务器回包不会到路由器上面匹配nat会话做反向地址转换，而是直接回给终端，由于回给终端的报文的源地址是服务器的内网地址，终端不认，从而无法访问）
 nat outbound 3000
 nat server protocol tcp global 1.1.1.1 23 inside 192.168.1.10 23
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
//终端和服务器不在同一网段的时候可以不做源地址转换
 nat server protocol tcp global 1.1.1.1 23 inside 192.168.1.10 23
#
interface GigabitEthernet0/2
 port link-mode route
 description WAN
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 nat outbound
 nat server protocol tcp global 1.1.1.1 23 inside 192.168.1.10 23
#
acl advanced 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.1.10 0
#
return
```

解决方法

4.测试

PC4访问1.1.1.1 23

<PC4>telnet 1.1.1.1
Trying 1.1.1.1 ...
Press CTRL+K to abort
Connected to 1.1.1.1 ...

```
*******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                  *
* no decompiling or reverse-engineering shall be allowed.                     *
*******************************************************************************
```

login: admin
Password:
<server5>

R1上debug nat paket信息如下：

[R1]*Jun 23 08:06:23:271 2020 R1 NAT/7/COMMON:
//入方向先匹配nat server做目的IP地址转换
PACKET: (GigabitEthernet0/0-in) Protocol: TCP
192.168.1.2:16328 - **1.1.1.1: 23**(VPN: 0) ------>
192.168.1.2:16328 - **192.168.1.10: 23**(VPN: 0)
*Jun 23 08:06:23:271 2020 R1 NAT/7/COMMON:
//出方向匹配nat outbound做源IP地址转换
PACKET: (GigabitEthernet0/0-out) Protocol: TCP
192.168.1.2:16328 - 192.168.1.10: 23(VPN: 0) ------>
192.168.1.1: 1031 - 192.168.1.10: 23(VPN: 0)
*Jun 23 08:06:23:272 2020 R1 NAT/7/COMMON:
//服务器回包入方向匹配会话做目的ip地址抓换
PACKET: (GigabitEthernet0/0-in) Protocol: TCP
192.168.1.10: 23 - **192.168.1.1: 1031**(VPN: 0) ------>
192.168.1.10: 23 - **192.168.1.2:16328**(VPN: 0)
*Jun 23 08:06:23:272 2020 R1 NAT/7/COMMON:
//服务器回包出方向匹配会话做源ip地址抓换
PACKET: (GigabitEthernet0/0-out) Protocol: TCP
192.168.1.10: 23 - 192.168.1.2:16328(VPN: 0) ------>
1.1.1.1: 23 - 192.168.1.2:16328(VPN: 0)

PC6访问 1.1.1.1 23

<PC6>telnet 1.1.1.1
Trying 1.1.1.1 ...
Press CTRL+K to abort
Connected to 1.1.1.1 ...

```
*******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                  *
* no decompiling or reverse-engineering shall be allowed.                     *
*******************************************************************************
```

login: admin
Password:
<server5>

R1上debug nat paket信息如下：

（转换原理与上面类似，不再赘述）
[R1]*Jun 23 08:11:10:286 2020 R1 NAT/7/COMMON:
PACKET: (GigabitEthernet0/1-in) Protocol: TCP
192.168.2.2:31361 - 1.1.1.1: 23(VPN: 0) ------>
192.168.2.2:31361 - 192.168.1.10: 23(VPN: 0)
*Jun 23 08:11:10:288 2020 R1 NAT/7/COMMON:
PACKET: (GigabitEthernet0/1-out) Protocol: TCP

192.168.1.10: 23 - 192.168.2.2:31361(VPN: 0) ------>
  1.1.1.1: 23 - 192.168.2.2:31361(VPN: 0)