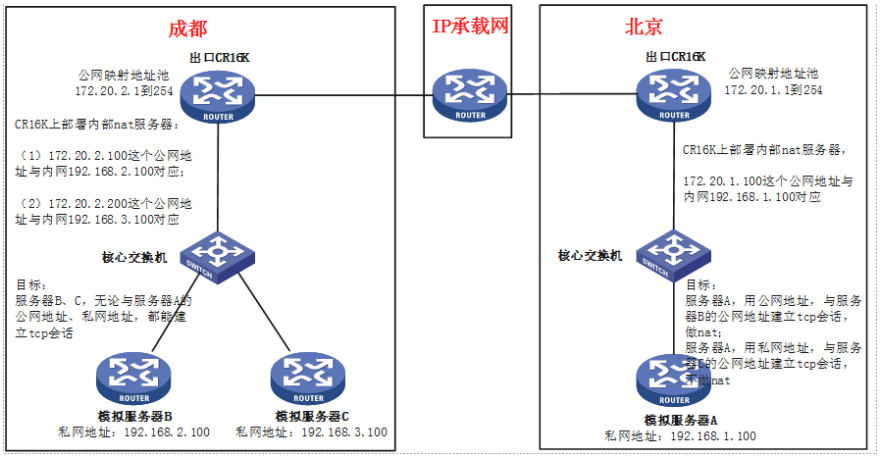
某局点 CR16010-F 内网服务器对外需要同时使用NAT后地址和原内网地址的提供服务

NAT　林宇阳　2019-03-20 发表

组网及说明



问题描述

客户需要使服务器A同时使用公网地址和私网地址，从外部访问。

模拟服务器A 与模拟器服务器B 建立tcp会话时，从CR16K出去时**进行NAT**

模拟服务器A 与模拟器服务器C 建立tcp会话时，从CR16K出去时**不进行NAT**

过程分析

根据客户要求，实验室模拟组网：

SR88-L（10.10.0.2）——（10.10.0.1）SR88X-UP（30.0.0.1）——（30.0.0.2）SR88X-down

静态路由打通，可以互ping。SR88-L模拟服务器提供ftp和Telnet服务。在88X-UP配置nat模拟CR16K-F的配置。

分析配置，计划从nat outbound的ACL中对不同访问地址的需求进行划分，为固定的目的网段的流量进行转换，而目的地址是需要私网访问的网段时不主动转换目的段。

目前实验室验证可以实现88X-down访问88X-UP接口nat-server的地址和内部服务器的地址。

将outbound接口的ACL改为限制部分目的地址触发也可以实现

[SR88X-UP]dis cu int g1/5/1/7

interface GigabitEthernet1/5/1/7

port link-mode route

ip address 30.0.0.1 255.255.255.0

nat outbound 3999 address-group 1

nat server protocol tcp global 20.0.0.3 20 inside 10.10.0.2 20

nat server protocol tcp global 20.0.0.3 21 inside 10.10.0.2 21

nat server protocol tcp global 20.0.0.3 23 inside 10.10.0.2 23

nat server protocol tcp global 20.0.0.3 40022 inside 10.10.0.2 22

nat server protocol tcp global 20.0.0.3 40023 inside 10.10.0.2 23

nat service chassis 1 slot 5

#

[SR88X-UP]dis acl 3999

Advanced IPv4 ACL 3999, 2 rules,　　使从SR88-L上ping30.0.0.2和50.0.0.1，只有后者会触发nat

ACL's step is 5

rule 0 permit ip source 10.10.1.0 0.0.0.255

rule 5 permit ip source 10.10.0.2 0 destination 50.0.0.0 0.0.0.255 (1 times matched)　//**限制仅访问50.0.0.0地址时触发nat**

[SR88X-UP]*Jan 11 14:28:18:163 2019 SR88X-UP NAT/7/COMMON: -MDC=1-Chassis=1-Slot=5; //**SR88X-down上Telnet natserver地址触发的转换**

PACKET: (GigabitEthernet1/5/1/7-in) Protocol: TCP

　　30.0.0.2:11706 -　　20.0.0.3:　23(VPN:　0) ------>

30.0.0.2:11706 - 10.10.0.2: 23(VPN: 0)
*Jan 11 14:28:18:166 2019 SR88X-UP NAT/7/COMMON: -MDC=1-Chassis=1-Slot=5;
PACKET: (GigabitEthernet1/5/1/7-out) Protocol: TCP
10.10.0.2: 23 - 30.0.0.2:11706(VPN: 0) ------>
20.0.0.3: 23 - 30.0.0.2:11706(VPN: 0)

[SR88X-UP]*Jan 11 14:29:22:090 2019 SR88X-UP NAT/7/COMMON: -MDC=1-Chassis=1-Slot=5; //
SR88-L ping 50.0.0.1 触发的nat转换
PACKET: (GigabitEthernet1/5/1/7-out) Protocol: ICMP
10.10.0.2: 0 - 50.0.0.1: 0(VPN: 0) ------>
20.0.0.1: 0 - 50.0.0.1: 0(VPN: 0)
*Jan 11 14:29:22:092 2019 SR88X-UP NAT/7/COMMON: -MDC=1-Chassis=1-Slot=5;
PACKET: (GigabitEthernet1/5/1/7-in) Protocol: ICMP
50.0.0.1: 0 - 20.0.0.1: 0(VPN: 0) ------>
50.0.0.1: 0 - 10.10.0.2: 0(VPN: 0)

<SR88X-DOWN>tel 10.10.0.2 //**验证从外网可以直接访问内网地址**
Trying 10.10.0.2 ...
Press CTRL+K to abort
Connected to 10.10.0.2 ...
****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
****
Login authentication
Username:admin
Password:
<SR88-L>
<SR88-L>qu
The connection was closed by the remote host!
<SR88X-DOWN>
<SR88X-DOWN>
<SR88X-DOWN>tel 20.0.00.3 //**访问nat server转换后的global地址**
Trying 20.0.0.3 ...
Press CTRL+K to abort
Connected to 20.0.0.3 ...
****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
****
Login authentication
Username:admin
Password:
<SR88-L>

解决方法

实验室证实，同时访问功能需要根据访问的网段在外网NAT接口调用的ACL进行划分，需要实现私网地址直接被外部访问的外网网段不进行nat。
因此只有在明确访问网段地址的情况下才可以使用该方案，且访问功能不支持互换网段使用。
内网口依旧需要将所有有关流量都引流到NAT板。