H3C MSR 系列路由器内网用户通过 NAT 地址访问内网服务器典型配置举例(V7)

目 录

1 简介

本文档介绍 MSR 系列路由器内网用户通过 NAT 地址访问内网服务器典型配置。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 NAT 特性。

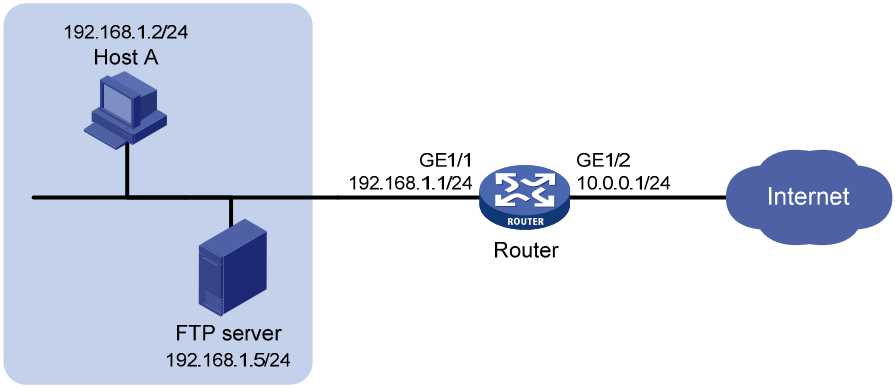
3 配置举例

3.1 组网需求

如 图 1 所示，Host A和FTP服务器同在一个局域网内，Router作为该局域网的网关，具体要求如下：

- 外网主机可以通过 Router 访问内网 FTP 服务器；
- 内网主机在访问 FTP 服务器时，需要通过外网地址访问，从而有效的避免服务器受到来自内部网络的攻击。

图1 内网用户通过外网地址访问内网服务器



3.2 配置思路

- 通过定义 ACL 规则，并将其与 NAT 配置关联，实现只对内网匹配指定的 ACL 规则的报文进行地址转换。
- 为使外网主机可以通过外网地址访问内网 FTP 服务器，需要在外网侧接口配置 NAT 内部服务器功能。
- 为使内网主机通过外网地址访问内网 FTP 服务器，需要在内网侧接口使能 NAT hairpin 功能。

3.3 使用版本

本举例是在 R0106 版本上进行配置和验证的。

3.4 配置步骤

配置 Router 的内网接口 GigabitEthernet1/1 和外网接口 GigabitEthernet1/2 的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/1
[Router-GigabitEthernet1/1] ip address 192.168.1.1 24
[Router-GigabitEthernet1/1] quit
[Router] interface gigabitethernet 1/2
[Router-GigabitEthernet1/2] ip address 10.0.0.1 24
[Router-GigabitEthernet1/2] quit
```

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet1/2 上配置 NAT 内部服务器，允许外网主机使用地址 10.0.0.1 访问内网 FTP 服务器，同时使得内网主机访问内网 FTP 服务器的报文可以进行目的地址转换。

```
[Router] interface gigabitethernet 1/2
[Router-GigabitEthernet1/2] nat server protocol tcp global 10.0.0.1 inside 192.168.1.5 ftp
```

在接口 GigabitEthernet1/2 上配置 Easy IP 方式的出方向动态地址转换，使得内网主机访问内网 FTP 服务器的报文可以使用接口 GigabitEthernet1/2 的 IP 地址进行源地址转换。

```
[Router-GigabitEthernet1/2] nat outbound 2000
[Router-GigabitEthernet1/2] quit
```

在接口 GigabitEthernet1/1 上使能 NAT hairpin 功能。

```
[Router] interface gigabitethernet 1/1
[Router-GigabitEthernet1/1] nat hairpin enable
[Router-GigabitEthernet1/1] quit
```

3.5 验证配置

以上配置完成后，内网主机和外网主机均能够通过外网地址访问内网 FTP Server。通过 **display nat all** 命令查看所有 NAT 的配置信息，可以看到 GigabitEthernet1/1 接口上使能了 NAT hairpin 功能。

```
[Router] display nat all
NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet1/2
    ACL: 2000         Address group: ---    Port-preserved: N
    NO-PAT: N         Reversible: N
NAT internal server information:
  There are 1 internal servers.
  Interface: GigabitEthernet1/2
```

```
    Protocol: 6(TCP)
    Global IP/port: 10.0.0.1/21
    Local  IP/port: 192.168.1.5/21

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT hairpinning:
  There are 1 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet1/1

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL         : ---

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RSH        : Enabled
  RTSP       : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过 **display nat session verbose** 命令查看 NAT 会话的详细信息，可以看到 Host A 访问 FTP server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.2/1694
  Destination IP/port: 10.0.0.1/21
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 192.168.1.5/21
  Destination IP/port: 10.0.0.1/1025
```

```
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2013-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet1/1
Interface(out): GigabitEthernet1/2
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

3.6 配置文件

```
#
interface GigabitEthernet1/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
 nat hairpin enable
#
interface GigabitEthernet1/2
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
 nat outbound 2000
 nat server protocol tcp global 10.0.0.1 21 inside 192.168.1.5 21
#
acl number 2000
 rule 0 permit source 192.168.1.0 0.0.0.255
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”