NGFW盒式防火墙双向NAT配置实验

NAT 吴超 2020-02-28 发表

组网及说明

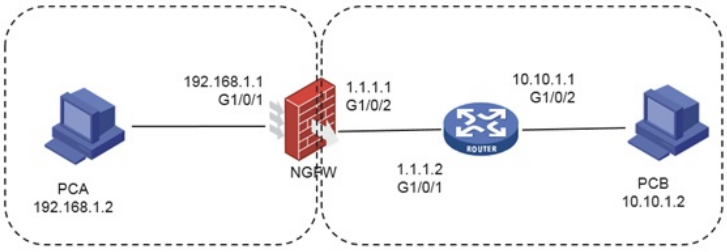


图1-1实验组网

实验组网如图1-1所示，互联方式和IP地址分配见图。

PCA位于私网，网关为FW，FW同时为NAT设备，有1个私网接口和1个公网地址，公网接口与公网路由器RT互联，PCB位于公网，网关为RT。

配置步骤

本实验中，私网客户端PCA需要访问公网PCB，而RT上不能保有私网路由，因此将在FW上配置NAT Outbound，动态为PCA分配公网地址。

步骤一：搭建实验环境

依照图1-1搭建实验环境，配置内网主机的IP地址为192.168.1.2/24，外网主机PCB的IP地址为10.10.1.2/24，防火墙G1/0/1和G1/0/2的IP地址为192.168.1.1/24和1.1.1.1/24。

步骤二：基本配置

完成FW、RT的路由、安全策略等基本配置。

FW的配置如下：

将GE1/0/1、GE1/0/2加入到安全域，并且配上IP地址，配置方法如下：

在导航栏中选择“网络>接口>接口”，进入“接口”配置页面，分别点击GE1/0/1、GE1/0/2，右边<编辑>弹出“修改接口设置”配置窗口。

FW的命令行配置如下：

[FW] interface GigabitEthernet 1/0/1

[FW-GigabitEthernet1/0/1]ip address 192.168.1.1 24

[FW-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2

[FW-GigabitEthernet1/0/2]ip address 1.1.1.1 24

[FW-GigabitEthernet1/0/2]quit

RT的命令行的配置如下：

[RT]interface GigabitEthernet 0/1

[RT-GigabitEthernet0/0]ip address 1.1.1.2 24

[RT-GigabitEthernet0/0]quit

[RT]interface GigabitEthernet 0/2

[RT-GigabitEthernet0/1]ip address 10.10.1.1 24

[RT-GigabitEthernet0/1]quit

配置FW的缺省路由，指向公网，配置方法为：

在导航栏中选择“网络>路由>静态路由”，进入“IPv4静态路由”配置页面，点击左上角<新建>弹出“新建IPv4静态路由”配置窗口。

命令行的配置如下：

ip route-static 0.0.0.0 0 1.1.1.2

配置全通的安全策略，配置方法如下：

在导航栏中选择“策略>安全策略>安全策略”，进入“安全策略”配置页面，点击左上角<新建>弹出“新建安全策略”配置窗口。

安全策略的命令行配置如下：

[FW]security-zone name trust

[FW -security-zone-Trust] import interface GigabitEthernet 1/0/1

[FW -security-zone-Trust]quit

[FW]security-zone name untrust

[FW -security-zone-Untrust] import interface GigabitEthernet 1/0/2

[FW -security-zone-Untrust]quit

[FW]security-policy ip

[FW -security-policy-ip]rule name web

[FW -security-policy-ip-0-web]source-zone trust

[FW -security-policy-ip-0-web]destination-zone untrust

[FW -security-policy-ip-0-web]source-zone untrust

[FW -security-policy-ip-0-web]destination-zone trust

[FW -security-policy-ip-0-web]action pass

[FW -security-policy-ip-0-web]source-zone local

[FW -security-policy-ip-0-web]destination-zone local

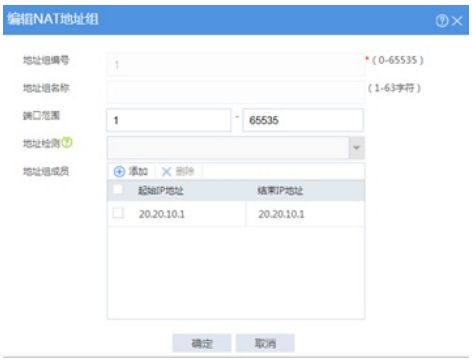
步骤一：配置正向NAT （NAT Outbound）

配置允许做NAT的ACL，配置方法如下：

在导航栏中选择“对象>ACL>IPv4”，进入“IPv4 ACL组”配置页面，点击左上角<新建>弹出“新建IPv4ACL”配置窗口。

配置NAT地址池，配置方法如下：

在导航栏中选择“策略>NAT>NAT动态转换>NAT地址组”，进入“NAT地址组”配置页面，点击左上角<新建>弹出“新建NAT地址组”配置窗口。



配置出方向NAT，配置方法如下：

在导航栏中选择“策略>NAT>NAT动态转换>策略配置”，进入“NAT出方向动态转换（基于ACL）”配置页面，点击左上角<新建>弹出“新建NAT出方向动态转换”配置窗口。

由配置可见，在FW上配置了公网地址池1，地址范围是20.20.10.1~20.20.10.1。此时FW会对公网口上出方向匹配acl 2000的流量做地址转换。

命令行的相关配置如下：

[FW]acl basic 2000

[FW-acl-ipv4-basic-2000]rule permit source 192.168.1.0 0.0.0.255

[FW-acl-ipv4-basic-2000]quit

[FW]nat address-group 1

[FW-address-group-1] address 20.20.10.1 20.20.10.1

[FW-address-group-1]quit

[FW]interface GigabitEthernet 1/0/2

[FW-GigabitEthernet1/0/2]nat outbound 2000 address-group 1

[FW-GigabitEthernet1/0/2]quit

步骤一：配置反向NAT(NAT Server)

本实验中，PCB可以通过访问公网地址1.1.1.1与PCA通信。

在导航栏中选择“策略>NAT>NAT内部服务器>策略应用”，进入“NAT内部服务器”配置页面，点击左上角<新建>。

FW上命令行的配置如下：

[FW]interface GigabitEthernet 1/0/2

[FW-GigabitEthernet1/0/2] nat server protocol icmp global current-interface inside 192.168.1.2

[FW-GigabitEthernet1/0/2]quit

步骤五：检查连通性

在PCA上ping公网PCB，显示如下：

C:\Users\H3C>ping 10.10.1.2

正在 Ping 10.10.1.2 具有 32 字节的数据:

来自 10.10.1.2 的回复: 字节=32 时间<1ms TTL=128

来自 10.10.1.2 的回复: 字节=32 时间<1ms TTL=128

来自 10.10.1.2 的回复: 字节=32 时间<1ms TTL=128

来自 10.10.1.2 的回复: 字节=32 时间<1ms TTL=128

10.10.1.2 的 Ping 统计信息:

数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，

往返行程的估计时间(以毫秒为单位):

最短 = 0ms，最长 = 0ms，平均 = 0ms

结果显示PCA、PCB之间可以通信。

步骤一：检查NAT表项

完成上一步后，立即在FW上检查NAT表项：

[FW]display nat all

NAT address group information:

Totally 1 NAT address groups.

Address group ID: 1

Port range: 1-65535

Address information:

Start address End address

20.20.10.1 20.20.10.1

NAT outbound information:

Totally 1 NAT outbound rules.

Interface: GigabitEthernet1/0/2

ACL: 2000

Address group ID: 1

Port-preserved: N NO-PAT: N Reversible: N

NAT counting: 0

Config status: Active

NAT internal server information:

Totally 1 internal servers.

Interface: GigabitEthernet1/0/2

Protocol: 1(ICMP)

Global IP/port: 1.1.1.1/---

Local IP/port : 192.168.1.2/---

NAT counting : 0

Config status : Active

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 mapping behavior:

Mapping mode : Address and Port-Dependent

ACL : ---

Config status: Active

NAT ALG:

DNS : Enabled

FTP : Enabled

H323 : Disabled

ICMP-ERROR : Enabled

ILS : Disabled

MGCP : Disabled

NBT : Disabled

PPTP : Enabled

RTSP : Enabled

RSH : Disabled

SCCP : Disabled

SIP : Disabled

SQLNET : Disabled

TFTP : Disabled

XDMCP : Disabled

Static NAT load balancing: Disabled

步骤二：查看会话信息

[FW]display nat session verbose

Slot 1:

Initiator:

Source IP/port: 192.168.1.2/260

Destination IP/port: 10.10.1.2/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

Responder:

Source IP/port: 10.10.1.2/3

Destination IP/port: 20.20.10.1/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/2

Source security zone: Untrust

State: ICMP_REPLY

Application: ICMP

Rule ID: 0

Rule name: web

Start time: 2018-09-08 05:53:03 TTL: 29s

Initiator->Responder: 5 packets 420 bytes

Responder->Initiator: 5 packets 420 bytes

Initiator:

Source IP/port: 10.10.1.2/246

Destination IP/port: 1.1.1.1/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/2

Source security zone: Untrust

Responder:

Source IP/port: 192.168.1.2/246

Destination IP/port: 10.10.1.2/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

State: ICMP_REPLY

Application: ICMP

Rule ID: 0

Rule name: web

Start time: 2018-09-08 05:53:01 TTL: 27s

Initiator->Responder: 5 packets 420 bytes

Responder->Initiator: 5 packets 420 bytes

Total sessions found: 2

通过查看NAT会话信息可以看出，对于内网用户PCA的地址192.168.1.2访问公网地址10.10.1.2时，源地址在公网出接口由NAT outbound转换成公网地址20.10.10.1，外网访问内网地址时，目的地址由NAT server配置映射成内网地址192.168.1.2。

[FW]display session table ipv4 verbose

Slot 1:

Initiator:

Source IP/port: 10.10.1.2/247

Destination IP/port: 1.1.1.1/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/2

Source security zone: Untrust

Responder:

Source IP/port: 192.168.1.2/247

Destination IP/port: 10.10.1.2/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

State: ICMP_REPLY

Application: ICMP

Rule ID: 0

Rule name: web

Start time: 2018-09-08 05:55:57 TTL: 29s

Initiator->Responder: 5 packets 420 bytes

Responder->Initiator: 5 packets 420 bytes

Initiator:

Source IP/port: 192.168.1.2/261

Destination IP/port: 10.10.1.2/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

Responder:

Source IP/port: 10.10.1.2/4

Destination IP/port: 20.20.10.1/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/2

Source security zone: Untrust

State: ICMP_REPLY

Application: ICMP

Rule ID: 0

Rule name: web

Start time: 2018-09-08 05:55:56 TTL: 27s

Initiator->Responder: 5 packets 420 bytes

Responder->Initiator: 5 packets 420 bytes

Total sessions found: 2

查看防火墙会话也可以看到，PCA主动访问的ICMP报文中192.168.1.2被转换成了20.20.10.1的公网地址。PCB主动访问的报文中，目的地址1.1.1.1转换为了192.168.1.2。

步骤三：查看debug信息。

两个PC进行互访做ping测试，开启debugging nat packet命令查看打印信息，可以看出ICMP报文首先达到配置的G1/0/2口，出方向源地址转换成公网地址，然后回程的报文匹配NAT会话进行目的地址转换，实现内网用户访问外部网络或者公网用户访问内部网络时隐藏了内部主机的源IP和公网用户的目的IP的功能。

debugging nat packet

terminal monitor

The current terminal is enabled to display logs.

terminal debugging

The current terminal is enabled to display debugging logs.

*Sep 8 06:09:49:049 2018 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/2-out-config) Protocol: ICMP

192.168.1.2: 262 - 10.10.1.2: 2048(VPN: 0) ------>

20.20.10.1: 5 - 10.10.1.2: 2048(VPN: 0)

*Sep 8 06:09:49:065 2018 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/2-in-session) Protocol: ICMP

10.10.1.2: 5 - 20.20.10.1: 0(VPN: 0) ------>

10.10.1.2: 262 - 192.168.1.2: 0(VPN: 0)

*Sep 8 06:09:55:440 2018 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/2-in-config) Protocol: ICMP

10.10.1.2: 255 - 1.1.1.1: 2048(VPN: 0) ------>

10.10.1.2: 255 - 192.168.1.2: 2048(VPN: 0)

*Sep 8 06:09:55:441 2018 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/2-out-session) Protocol: ICMP

192.168.1.2: 255 - 10.10.1.2: 0(VPN: 0) ------>

1.1.1.1: 255 - 10.10.1.2: 0(VPN: 0)

综上所述，双向NAT技术有效界定了用户所在网络的范围，保证了用户访问内网服务器的最佳快速访问路由走向，同时可以隐藏报文的源地址，使得内网服务器回应数据包也能按照最快速的路由达到客户端。双向NAT为内网主机访问外网服务器以及外网主机访问内网服务器提供了有效的技术支持。

配置关键点

如果要写详细的安全策略，应该如何放通?

答：NAT Outbound：放通内部私网地址访问外部公网地址；NAT Server：放通外部公网地址访问内部私网地址。