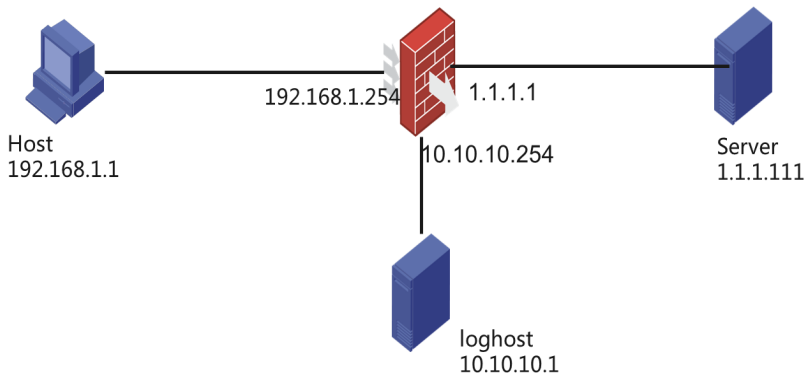
NGFW防火墙NAT444典型配置

NAT444 李瑞麟 2018-12-12 发表

组网及说明



实验组网如图所示。内网网段192.168.1.254/24(GigabitEthernet 1/0/1)通过防火墙的 GigabitEthernet 1/0/3 作为出口去访问公网上的，防火墙上需要配置NAT 444用于进行公网地址和私网地址的转换。在防火墙上旁挂一个日志主机用于接收防火墙生成的NAT转换日志。

配置步骤

1. 配置动态NAT444功能

1.1将接口加入安全域、配置安全策略

将GigabitEthernet 1/0/1加入到Trust域中：

```
[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface GigabitEthernet 1/0/1
[H3C-security-zone-Trust] quit
```

将GigabitEthernet 1/0/3加入到Untrust域中：

```
[H3C]security-zone name Untrust
[H3C-security-zone-Untrust]import interface GigabitEthernet 1/0/3
[H3C-security-zone-Untrust]quit
```

创建地址对象组Client包含内网Client的地址：

```
[H3C]object-group ip address Client
[H3C-obj-grp-ip-Server] 1 network subnet 192.168.1.1 24
[H3C-obj-grp-ip-Server] quit
```

创建安全策略规则Client_to_Server：

```
[H3C]security-policy ip
[H3C-security-policy-ip]rule name Client_to_Server
```

放通Trust域的Client到Untrust域的Server的访问：

```
[H3C-security-policy-ip-1-Client_to_Server]source-zone Trust
[H3C-security-policy-ip-1-Client_to_Server]destination-zone Untrust
[H3C-security-policy-ip-1-Client_to_Server]source-ip Client
[H3C-security-policy-ip-1-Client_to_Server]action pass
```

1.2 配置动态NAT 444功能：

进入系统视图，创建编号为0的NAT地址组，设置地址组成员为1.1.1.2——1.1.1.10，设置端口范围为：1024——65535，设置端口块大小为512：

```
[H3C]nat address-group 0
[H3C-address-group-0]address 1.1.1.2 1.1.1.10
[H3C-address-group-0]port-range 1024 65535
[H3C-address-group-0]port-block block-size 512
[H3C-address-group-0]quit
```

进入外网口GigabitEthernet1/0/3在接口下配置NAT 444功能：

```
[H3C]interface GigabitEthernet 1/0/3
[H3C-GigabitEthernet1/0/3]nat outbound address-group 0
[H3C-GigabitEthernet1/0/3]quit
```

1.3 验证动态NAT 444功能

配置终端地址为192.168.1.1，在外网模拟服务器的PC上开启FTP服务器服务。从内网终端发起向服务器的访问，在防火墙上观察NAT转换信息：

```
display nat port-block dynamic
Slot 1:
Local VPN     Local IP        Global IP       Port block   Connections
---           192.168.1.1     1.1.1.5         3584-4095    1
Total mappings found: 1
```

可以看到当终端发起访问，流量到达防火墙上以后，在防火墙上生成了一个动态端口块分配表项，终端地址被随机分配到地址1.1.1.5的3584——4095号端口，终端发起的对外访问都会使用该地址的这些端口进行。

我们在防火墙上查看NAT会话：

```
dis nat session destination-ip 1.1.1.111 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.1/58946
  Destination IP/port: 1.1.1.111/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 1.1.1.111/21
  Destination IP/port: 1.1.1.5/3584
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: FTP
Start time: 2018-09-06 23:08:36  TTL: 3596s
Initiator->Responder:           0 packets          0 bytes
Responder->Initiator:           0 packets          0 bytes

Total sessions found: 1
```

可以看到，对1.1.1.111的FTP访问使用的是1.1.1.5的3584号端口作为源去访问1.1.1.111的21号端口。对应的地址端口映射关系为192.168.1.1:58946→1.1.1.5:3584。

我们更换终端的IP地址将192.168.1.1换成192.168.1.10，观察防火墙上的地址分配会有什么变化：

```
display nat port-block dynamic
Slot 1:
Local VPN     Local IP        Global IP       Port block   Connections
---           192.168.1.10    1.1.1.4         5120-5631    1
---           192.168.1.1     1.1.1.5         3584-4095    0
Total mappings found: 2
```

192.168.1.10这个终端地址被随机分配到的global地址是1.1.1.4，会使用5120到5631号端口访问公网：

```
display nat session destination-ip 1.1.1.111 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.10/58947
  Destination IP/port: 1.1.1.111/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 1.1.1.111/21
  Destination IP/port: 1.1.1.4/5120
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: Untrust
State: TCP_ESTABLISHED
```

Application: FTP
Start time: 2018-09-06 23:20:31 TTL: 3590s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

2 配置静态NAT 444功能

2.1 将接口加入安全域，放通安全策略

同1.1

2.2 配置静态NAT 444：

创建端口块组0，进入端口块视图，设置端口范围为1024-65535，设置端口块大小为512。私网地址成员192.168.1.1——192.168.1.254，公网地址成员1.1.1.2——1.1.1.10：

[H3C]nat port-block-group 0
[H3C-port-block-group-0]port-range 1024 65535
[H3C-port-block-group-0]block-size 512
[H3C-port-block-group-0]local-ip-address 192.168.1.1 192.168.1.254
[H3C-port-block-group-0]global-ip-pool 1.1.1.2 1.1.1.10

进入接口GigabitEthernet 1/0/3，配置静态NAT 444：

[H3C]interface GigabitEthernet 1/0/3
[H3C-GigabitEthernet1/0/3]nat outbound port-block-group 0

验证静态NAT 444功能

配置终端地址为192.168.1.1，在外网模拟服务器的PC上开启FTP服务器服务。从内网终端发起向服务器的访问，在防火墙上观察NAT转换信息：

dis nat port-block static
Slot 1:
Local VPN Local IP Global IP Port block Connections
--- 192.168.1.1 1.1.1.2 1024-1535 1
--- 192.168.1.2 1.1.1.2 1536-2047 0
--- 192.168.1.3 1.1.1.2 2048-2559 0

可以看到防火墙上生成了私网地址和global的地址端口块的映射关系。该映射关系从小按私网地址从小到大排列，一一对应公网端口块，当从192.168.1.1向1.1.1.111发起连接后可以看到192.168.1.1转换为1.1.1.2。

display nat session verbose
Slot 1:
Initiator:
  Source IP/port: 192.168.1.1/26498
  Destination IP/port: 1.1.1.111/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source IP/port: 1.1.1.111/21
  Destination IP/port: 1.1.1.2/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: FTP
Start time: 2018-09-08 13:45:37 TTL: 3584s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

可以看到从192.168.1.1到1.1.1.111的访问，源地址被转换为1.1.1.2，源端口从26498转换为1025端口。

将源地址换为192.168.1.2查看NAT 会话：

dis nat session verbose
Slot 1:
Initiator:
  Source IP/port: 192.168.1.2/26499

```
  Destination IP/port: 1.1.1.111/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 1.1.1.111/21
  Destination IP/port: 1.1.1.2/1536
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: FTP
Start time: 2018-09-08 13:56:50  TTL: 3585s
Initiator->Responder:          0 packets         0 bytes
Responder->Initiator:          0 packets         0 bytes

Total sessions found: 1
```

可以看到源地址被转换为1.1.1.2，源端口从26499转换为1536，符合前面打印的映射关系表。

3 配置NAT 444日志（CLI）

3.1 配置安全域及安全策略：

将GigabitEthernet 1/0/6加入到DMZ域中：

```
[H3C]security-zone name DMZ
[H3C-security-zone-Untrust]import interface GigabitEthernet 1/0/6
[H3C-security-zone-Untrust]quit
```

创建地址对象组loghost包含日志服务器的地址：

```
[H3C]object-group ip address loghost
[H3C-obj-grp-ip-Client]1 network host address 10.10.10.1
[H3C-obj-grp-ip-Client] quit
```

创建安全策略规则To_loghost：

```
  [H3C]security-policy ip
[H3C-security-policy-ip]rule name to_loghost
```

放通Local域到DMZ域loghost的访问：

```
[H3C-security-policy-ip-2-to_loghost]source-zone Local
[H3C-security-policy-ip-2-to_loghost]destination-zone DMZ
[H3C-security-policy-ip-2-to_loghost]destination-ip loghost
[H3C-security-policy-ip-2-to_loghost]action pass
```

3.2 配置NAT 444日志功能：

开启NAT日志功能：

```
[H3C]nat log enable
```

开启NAT新建会话日志和删除会话日志：

```
[H3C]nat log flow-begin
[H3C]nat log flow-end
```

配置NAT 444端口块分配日志功能：

```
[H3C]nat log port-block-assign
```

配置NAT 444端口块回收日志功能：

```
[H3C]nat log port-block-withdraw
```

3.3 配置输出定制日志到日志服务器：

开启快速日志功能：

```
[H3C]customlog format nat cmcc
```

设置快速日志服务器主机：

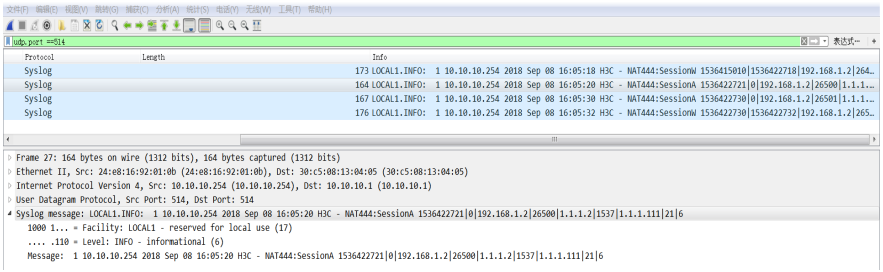
```
customlog host 10.10.10.1 export cmcc-sessionlog
```

设置快速日志输出的源接口地址：

```
[H3C]customlog host source GigabitEthernet 1/0/6
```

3.4 验证NAT 444日志功能

完成以上配置后，我们在模拟日志服务器的主机10.10.10.1上开启Wireshark抓包，抓取和防火墙互联口的流量。在终端触发到服务器的访问，然后使用过滤语法udp.port ==514，过滤出设备产生的日志，我们选取其中一条做解读，如下图所示，流192.168.1.2:26500访问1.1.1.111:21，协议类型是6（TCP）。经过防火墙后源地址被转换为1.1.1.2端口被转换为1537。


文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp.port ==514
表达式…
Protocol Length Info
Syslog 173 LOCAL1.INFO: 1 10.10.10.254 2018 Sep 08 16:05:18 H3C - NAT444:SessionW 1536415010|1536422718|192.168.1.2|264…
Syslog 164 LOCAL1.INFO: 1 10.10.10.254 2018 Sep 08 16:05:20 H3C - NAT444:SessionA 1536422721|0|192.168.1.2|26500|1.1.1…
Syslog 167 LOCAL1.INFO: 1 10.10.10.254 2018 Sep 08 16:05:30 H3C - NAT444:SessionA 1536422730|0|192.168.1.2|26501|1.1.1…
Syslog 176 LOCAL1.INFO: 1 10.10.10.254 2018 Sep 08 16:05:32 H3C - NAT444:SessionW 1536422730|1536422732|192.168.1.2|265…
Frame 27: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
Ethernet II, Src: 24:e8:16:92:01:0b (24:e8:16:92:01:0b), Dst: 30:c5:08:13:04:05 (30:c5:08:13:04:05)
Internet Protocol Version 4, Src: 10.10.10.254 (10.10.10.254), Dst: 10.10.10.1 (10.10.10.1)
User Datagram Protocol, Src Port: 514, Dst Port: 514
Syslog message: LOCAL1.INFO: 1 10.10.10.254 2018 Sep 08 16:05:20 H3C - NAT444:SessionA 1536422721|0|192.168.1.2|26500|1.1.1.2|1537|1.1.1.111|21|6
1000 1... = Facility: LOCAL1 - reserved for local use (17)
.... .110 = Level: INFO - informational (6)
Message: 1 10.10.10.254 2018 Sep 08 16:05:20 H3C - NAT444:SessionA 1536422721|0|192.168.1.2|26500|1.1.1.2|1537|1.1.1.111|21|6

配置关键点