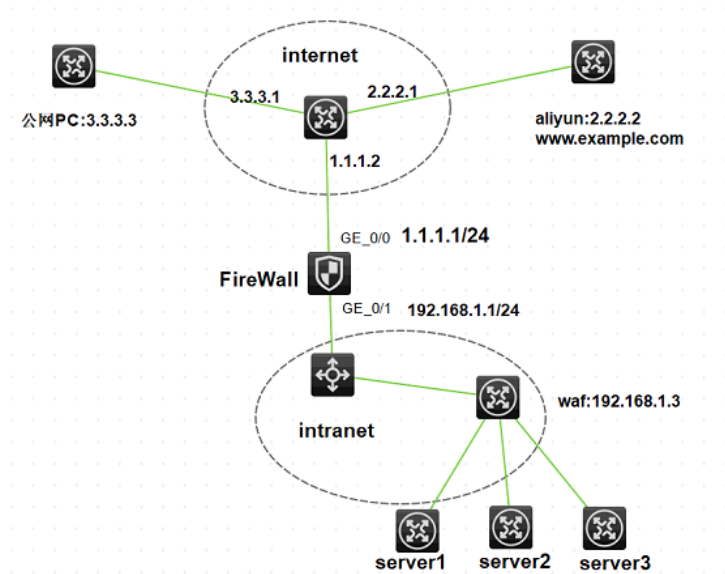


组网及说明

1.组网



问题描述

2.需求

客户的大部分业务部署在内网，内网有一台WEB应用防火墙对访问内网业务的流量进行防护，同时还有一部分业务部署在公网阿里云上，在公网访问此部分业务的流量直接经过公网转发，客户希望能将从公网访问阿里云的流量先引到内网WAF，然后再转发给阿里云。

假设：

公网PC IP: 3.3.3.3

防火墙公网IP: 1.1.1.1

阿里云ip: 2.2.2.2 域名: www.example.com

内网waf ip:192.168.1.3 gateway:192.168.1.1

配置思路：

在公网PC访问阿里云的域名时，通过修改本地host文件，将域名解析为防火墙公网ip。然后在防火墙上做nat server，将目的地址转换为阿里云的IP，然后通过匹配策略路由，将目的地址为阿里云IP的流量引到WAF上面，然后再经由WAF转发到网关，再转发出去。

过程分析

3.关键配置

3.1 PC侧配置：

修改PC的host文件，将域名www.example.com指向防火墙的公网IP: 1.1.1.1。

1、window环境：

hosts文件位置：C:\windows\system32\drivers\etc

刷新方式：

在命令行执行：

```
ipconfig /flushdns #清除DNS缓存内容。
```

```
ipconfig /displaydns //显示DNS缓存内容
```

2、linux环境

文件位置：/etc/hosts

刷新命令：systemctl restart nsd

原文链接：<https://blog.csdn.net/jiahao1186/article/details/83011458>

3.2 防火墙侧关键配置

防火墙关键配置：

#

policy-based-route huqi permit node 0

```

if-match acl 3000 //匹配目的地址为阿里云IP的报文
apply next-hop 192.168.1.3
#
policy-based-route huqi permit node 1
if-match acl 3001 //匹配源地址为阿里云IP的报文
apply next-hop 192.168.1.3
#
interface GigabitEthernet1/0/0
port link-mode route
combo enable copper
ip address 1.1.1.1 255.255.255.0
nat outbound
//为了方便使用模拟器测试，此处假设阿里云上开放的服务为telnet和ssh
nat server protocol tcp global 1.1.1.1 2333 inside 2.2.2.2 23
nat server protocol tcp global 1.1.1.1 2222 inside 2.2.2.2 22
//在公网接口应用策略路由
ip policy-based-route huqi
#
interface GigabitEthernet1/0/1
port link-mode route
combo enable copper
ip address 192.168.1.1 255.255.255.0
#
security-zone name Trust
import interface GigabitEthernet1/0/1
#
security-zone name Untrust
import interface GigabitEthernet1/0/0
#
ip route-static 0.0.0.0 0 1.1.1.2
#
acl advanced 3000
rule 0 permit ip destination 2.2.2.2 0
#
acl advanced 3001
rule 0 permit ip source 2.2.2.2 0
#
security-policy ip
rule 0 name all
action pass
#
return

```

4.测试

在公网PC上telnet 1.1.1.1 2333和ssh 1.1.1.1 2222测试，发现可以正常访问。

```

<H3C>telnet 1.1.1.1 2333
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:

<H3C>dis ip i b

*down: administratively down

(s): spoofing (l): loopback

Interface	Physical	Protocol	IP Address	Description
GE0/0	up	up	2.2.2.2	--

<H3C>quit

The connection was closed by the remote host!

<H3C>ssh 1.1.1.1 2222

Username: admin

Press CTRL+C to abort.

Connecting to 1.1.1.1 port 2222.

admin@1.1.1.1's password:

Enter a character ~ and a dot to abort.

```
*****
* 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.                   *
*****
```

<H3C>dis ip i b

*down: administratively down

(s): spoofing (l): loopback

Interface	Physical	Protocol	IP Address	Description
GE0/0	up	up	2.2.2.2	--

同时在WAF上面可以看到，来回的流量都会途经WAF。

waf:

//收到由网关做PBR引过来的流量，其中目的地址已经由NAT server 转换为了阿里云的ip

*Dec 21 14:53:25:958 2019 H3C IPFW/7/IPFW_PACKET:

Receiving, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 192,

pkthlen = 60, pktid = 696, offset = 0, ttl = 253, protocol = 6,

checksum = 45114, s = 3.3.3.3, d = 2.2.2.2

prompt: Receiving IP packet.

//WAF上有到网关的默认路由，流量到达WAF后，又发回网关

*Dec 21 14:53:25:958 2019 H3C IPFW/7/IPFW_PACKET:

Sending, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 192,

pkthlen = 60, pktid = 696, offset = 0, ttl = 252, protocol = 6,

checksum = 45370, s = 3.3.3.3, d = 2.2.2.2

prompt: Sending the packet from GigabitEthernet0/0 at GigabitEthernet0/0.

//阿里云侧回应的流量再次经由PBR引到WAF上

*Dec 21 14:53:25:961 2019 H3C IPFW/7/IPFW_PACKET:

Receiving, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 192,

pkthlen = 60, pktid = 675, offset = 0, ttl = 253, protocol = 6,

checksum = 45135, s = 2.2.2.2, d = 3.3.3.3

prompt: Receiving IP packet.

//流量到达WAF后，又发回网关

*Dec 21 14:53:25:961 2019 H3C IPFW/7/IPFW_PACKET:

Sending, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 192,

pkthlen = 60, pktid = 675, offset = 0, ttl = 252, protocol = 6,

checksum = 45391, s = 2.2.2.2, d = 3.3.3.3

prompt: Sending the packet from GigabitEthernet0/0 at GigabitEthernet0/0.

防火墙的debug信息:

//收到公网PC访问的报文

<H3C>*Dec 21 14:53:28:209 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;

Receiving, interface = GigabitEthernet1/0/0

version = 4, headlen = 20, tos = 192

pkthlen = 60, pktid = 696, offset = 0, ttl = 254, protocol = 6

checksum = 45372, s = 3.3.3.3, d = 1.1.1.1

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Receiving IP packet from interface GigabitEthernet1/0/0.

Payload: TCP

source port = 8467, destination port = 2333

sequence num = 0xaadaccf7, acknowledgement num = 0x00000000, flags = 0x2

window size = 64512, checksum = 0x157d, header length = 40.

//匹配NAT server 先做目的地址和端口转换

*Dec 21 14:53:28:209 2019 H3C NAT/7/COMMON: -Context=1;

PACKET: (GigabitEthernet1/0/0-in-config) Protocol: TCP

3.3.3.3: 8467 - 1.1.1.1: 2333(VPN: 0) ----->

3.3.3.3: 8467 - 2.2.2.2: 23(VPN: 0)

//匹配上策略路由，将流量引到WAF

*Dec 21 14:53:28:209 2019 H3C PBR4/7/PBR Forward Info: -Context=1; **Policy: huqi, Node: 0, match succeeded.**

*Dec 21 14:53:28:209 2019 H3C PBR4/7/PBR Forward Info: -Context=1; **apply next-hop 192.168.1.3.**

//从内网接口将报文发给WAF

*Dec 21 14:53:28:209 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;

Sending, interface = GigabitEthernet1/0/1

version = 4, headlen = 20, tos = 192

pklen = 60, pktid = 696, offset = 0, ttl = 253, protocol = 6

checksum = 45114, s = 3.3.3.3, d = 2.2.2.2

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Sending IP packet received from interface GigabitEthernet1/0/0 at interface GigabitEthernet1/0/1.

Payload: TCP

source port = 8467, destination port = 23

sequence num = 0xaadaccf7, acknowledgement num = 0x00000000, flags = 0x2

window size = 64512, checksum = 0x1c81, header length = 40.

//又在内网接口收到经由WAF发回的此报文

*Dec 21 14:53:28:210 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;

Receiving, interface = GigabitEthernet1/0/1

version = 4, headlen = 20, tos = 192

pklen = 60, pktid = 696, offset = 0, ttl = 252, protocol = 6

checksum = 45370, s = 3.3.3.3, d = 2.2.2.2

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Receiving IP packet from interface GigabitEthernet1/0/1.

Payload: TCP

source port = 8467, destination port = 23

sequence num = 0xaadaccf7, acknowledgement num = 0x00000000, flags = 0x2

window size = 64512, checksum = 0x1c81, header length = 40.

//在出接口匹配NAT outbound做源地址和端口转换

*Dec 21 14:53:28:210 2019 H3C NAT/7/COMMON: -Context=1;

PACKET: (GigabitEthernet1/0/0-out-config) Protocol: TCP

3.3.3.3: 8467 - 2.2.2.2: 23(VPN: 0) ----->

1.1.1.1: 1030 - 2.2.2.2: 23(VPN: 0)

//做完转换之后从公网口发出

*Dec 21 14:53:28:210 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;

Sending, interface = GigabitEthernet1/0/0

version = 4, headlen = 20, tos = 192

pklen = 60, pktid = 696, offset = 0, ttl = 251, protocol = 6

checksum = 46654, s = 1.1.1.1, d = 2.2.2.2

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Sending IP packet received from interface GigabitEthernet1/0/1 at interface GigabitEthernet1/0/0.

Payload: TCP

source port = 1030, destination port = 23

sequence num = 0xaadaccf7, acknowledgement num = 0x00000000, flags = 0x2

window size = 64512, checksum = 0x3d92, header length = 40.

//收到阿里云的回包，可以看到源IP地址是阿里云IP 2.2.2.2

*Dec 21 14:53:28:212 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;

Receiving, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 675, offset = 0, ttl = 254, protocol = 6
checksum = 45907, s = 2.2.2.2, d = 1.1.1.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/0.
Payload: TCP
source port = 23, destination port = 1030
sequence num = 0x0e6dcd5e, acknowledgement num = 0xaadaccf8, flags = 0x12
window size = 4096, checksum = 0xa63b, header length = 40.

//匹配会话先做目的地址转换，转换目的地址为PC ip
*Dec 21 14:53:28:212 2019 H3C NAT/7/COMMON: -CContext=1;
PACKET: (GigabitEthernet1/0/0-in-session) Protocol: TCP
2.2.2.2: 23 - 1.1.1.1: 1030(VPN: 0) ----->
2.2.2.2: 23 - 3.3.3.3: 8467(VPN: 0)

//再次根据源IP地址为阿里云ip匹配上策略路由，将回包引到WAF
*Dec 21 14:53:28:212 2019 H3C PBR4/7/PBR Forward Info: -CContext=1; **Policy: huqi, Node: 1, match succeeded.**

*Dec 21 14:53:28:212 2019 H3C PBR4/7/PBR Forward Info: -CContext=1; **apply next-hop 192.168.1.3.**

//从内网接口将报文发给WAF
*Dec 21 14:53:28:212 2019 H3C IPFW/7/IPFW_PACKET: -CContext=1;
Sending, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 675, offset = 0, ttl = 253, protocol = 6
checksum = 45135, s = 2.2.2.2, d = 3.3.3.3
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/0 at interface GigabitEthernet1/0/1.
Payload: TCP
source port = 23, destination port = 8467
sequence num = 0x0e6dcd5e, acknowledgement num = 0xaadaccf8, flags = 0x12
window size = 4096, checksum = 0x852a, header length = 40.

//又在内网接口收到经由WAF发回的此报文
*Dec 21 14:53:28:214 2019 H3C IPFW/7/IPFW_PACKET: -CContext=1;
Receiving, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 675, offset = 0, ttl = 252, protocol = 6
checksum = 45391, s = 2.2.2.2, d = 3.3.3.3
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/1.
Payload: TCP
source port = 23, destination port = 8467
sequence num = 0x0e6dcd5e, acknowledgement num = 0xaadaccf8, flags = 0x12
window size = 4096, checksum = 0x852a, header length = 40.

//再次在出接口进行源地址和端口转换
*Dec 21 14:53:28:214 2019 H3C NAT/7/COMMON: -CContext=1;
PACKET: (GigabitEthernet1/0/0-out-session) Protocol: TCP
2.2.2.2: 23 - 3.3.3.3: 8467(VPN: 0) ----->
1.1.1.1: 2333 - 3.3.3.3: 8467(VPN: 0)

//做完转换，将报文从公网接口回给公网PC
*Dec 21 14:53:28:214 2019 H3C IPFW/7/IPFW_PACKET: -CContext=1;
Sending, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 675, offset = 0, ttl = 251, protocol = 6
checksum = 46161, s = 1.1.1.1, d = 3.3.3.3
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Sending IP packet received from interface GigabitEthernet1/0/1 at interface GigabitEthernet1/0/0.

Payload: TCP

source port = 2333, destination port = 8467

sequence num = 0x0e6dcd5e, acknowledgement num = 0xaadaccf8, flags = 0x12

window size = 4096, checksum = 0x7e26, header length = 40.

以下为SSH访问时的debug信息，转换过程同上，不再赘述。

*Dec 21 14:54:15:989 2019 H3C IPFW/7/IPFW_PACKET: -CContext=1;

Receiving, interface = GigabitEthernet1/0/0

version = 4, headlen = 20, tos = 192

pkthlen = 60, pktid = 851, offset = 0, ttl = 254, protocol = 6

checksum = 45217, s = 3.3.3.3, d = 1.1.1.1

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Receiving IP packet from interface GigabitEthernet1/0/0.

Payload: TCP

source port = 8468, destination port = 2222

sequence num = 0x6d3cf89a, acknowledgement num = 0x00000000, flags = 0x2

window size = 64512, checksum = 0x6d4f, header length = 40.

*Dec 21 14:54:15:989 2019 H3C NAT/7/COMMON: -CContext=1;

PACKET: (GigabitEthernet1/0/0-in-config) Protocol: TCP

3.3.3.3: 8468 - 1.1.1.1: 2222(VPN: 0) ----->

3.3.3.3: 8468 - 2.2.2.2: 22(VPN: 0)

*Dec 21 14:54:15:989 2019 H3C PBR4/7/PBR Forward Info: -CContext=1; Policy: huqi, Node: 0, match succeeded.

*Dec 21 14:54:15:989 2019 H3C PBR4/7/PBR Forward Info: -CContext=1; apply next-hop 192.168.1.3.

*Dec 21 14:54:15:989 2019 H3C IPFW/7/IPFW_PACKET: -CContext=1;

Sending, interface = GigabitEthernet1/0/1

version = 4, headlen = 20, tos = 192

pkthlen = 60, pktid = 851, offset = 0, ttl = 253, protocol = 6

checksum = 44959, s = 3.3.3.3, d = 2.2.2.2

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Sending IP packet received from interface GigabitEthernet1/0/0 at interface GigabitEthernet1/0/1.

Payload: TCP

source port = 8468, destination port = 22

sequence num = 0x6d3cf89a, acknowledgement num = 0x00000000, flags = 0x2

window size = 64512, checksum = 0x73e5, header length = 40.

*Dec 21 14:54:15:992 2019 H3C IPFW/7/IPFW_PACKET: -CContext=1;

Receiving, interface = GigabitEthernet1/0/1

version = 4, headlen = 20, tos = 192

pkthlen = 60, pktid = 851, offset = 0, ttl = 252, protocol = 6

checksum = 45215, s = 3.3.3.3, d = 2.2.2.2

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Receiving IP packet from interface GigabitEthernet1/0/1.

Payload: TCP

source port = 8468, destination port = 22

sequence num = 0x6d3cf89a, acknowledgement num = 0x00000000, flags = 0x2

window size = 64512, checksum = 0x73e5, header length = 40.

*Dec 21 14:54:15:992 2019 H3C NAT/7/COMMON: -CContext=1;

PACKET: (GigabitEthernet1/0/0-out-config) Protocol: TCP

3.3.3.3: 8468 - 2.2.2.2: 22(VPN: 0) ----->

1.1.1.1: 1031 - 2.2.2.2: 22(VPN: 0)

*Dec 21 14:54:15:992 2019 H3C IPFW/7/IPFW_PACKET: -CContext=1;

Sending, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 851, offset = 0, ttl = 251, protocol = 6
checksum = 46499, s = 1.1.1.1, d = 2.2.2.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/1 at interface GigabitEthernet1/0/0.
Payload: TCP
source port = 1031, destination port = 22
sequence num = 0x6d3cf89a, acknowledgement num = 0x00000000, flags = 0x2
window size = 64512, checksum = 0x94f6, header length = 40.

*Dec 21 14:54:15:994 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 829, offset = 0, ttl = 254, protocol = 6
checksum = 45753, s = 2.2.2.2, d = 1.1.1.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/0.
Payload: TCP
source port = 22, destination port = 1031
sequence num = 0x956d26b8, acknowledgement num = 0x6d3cf89b, flags = 0x12
window size = 64512, checksum = 0x76bf, header length = 40.

*Dec 21 14:54:15:994 2019 H3C NAT/7/COMMON: -Context=1;
PACKET: (GigabitEthernet1/0/0-in-session) Protocol: TCP
2.2.2.2: 22 - 1.1.1.1: 1031(VPN: 0) ----->
2.2.2.2: 22 - 3.3.3.3: 8468(VPN: 0)
*Dec 21 14:54:15:994 2019 H3C PBR4/7/PBR Forward Info: -Context=1; Policy: huqi, Node: 1, match succeeded.

*Dec 21 14:54:15:994 2019 H3C PBR4/7/PBR Forward Info: -Context=1; apply next-hop 192.168.1.3.

*Dec 21 14:54:15:994 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;
Sending, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 829, offset = 0, ttl = 253, protocol = 6
checksum = 44981, s = 2.2.2.2, d = 3.3.3.3
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/0 at interface GigabitEthernet1/0/1.
Payload: TCP
source port = 22, destination port = 8468
sequence num = 0x956d26b8, acknowledgement num = 0x6d3cf89b, flags = 0x12
window size = 64512, checksum = 0x55ae, header length = 40.

*Dec 21 14:54:15:996 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = GigabitEthernet1/0/1
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 829, offset = 0, ttl = 252, protocol = 6
checksum = 45237, s = 2.2.2.2, d = 3.3.3.3
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/1.
Payload: TCP
source port = 22, destination port = 8468
sequence num = 0x956d26b8, acknowledgement num = 0x6d3cf89b, flags = 0x12
window size = 64512, checksum = 0x55ae, header length = 40.

*Dec 21 14:54:15:996 2019 H3C NAT/7/COMMON: -Context=1;

PACKET: (GigabitEthernet1/0/0-out-session) Protocol: TCP
2.2.2.2: 22 - 3.3.3.3: 8468(VPN: 0) ----->
1.1.1.1: 2222 - 3.3.3.3: 8468(VPN: 0)
*Dec 21 14:54:15:996 2019 H3C IPFW/7/IPFW_PACKET: -Context=1;
Sending, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 192
pktlen = 60, pktid = 829, offset = 0, ttl = 251, protocol = 6
checksum = 46007, s = 1.1.1.1, d = 3.3.3.3
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet1/0/1 at interface
GigabitEthernet1/0/0.
Payload: TCP
source port = 2222, destination port = 8468
sequence num = 0x956d26b8, acknowledgement num = 0x6d3cf89b, flags = 0x12
window size = 64512, checksum = 0x4f18, header length = 40.

在防火墙上查看会话表。

<H3C>dis session table ipv4 destination-ip 1.1.1.1 verbose

Slot 1:

Initiator:

Source IP/port: 3.3.3.3/8476

Destination IP/port: 1.1.1.1/2222

DS-Lite tunnel peer: -

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

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/0

Source security zone: Untrust

Responder:

Source IP/port: 2.2.2.2/22

Destination IP/port: 3.3.3.3/8476

DS-Lite tunnel peer: -

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

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

State: TCP_ESTABLISHED

Application: GENERAL_TCP

Rule ID: 0

Rule name: all

Start time: 2019-12-21 15:27:33 TTL: 3594s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

<H3C>dis session table ipv4 destination-ip 2.2.2.2 verbose

Slot 1:

Initiator:

Source IP/port: 3.3.3.3/8476

Destination IP/port: 2.2.2.2/22

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: 2.2.2.2/22

Destination IP/port: 1.1.1.1/1039

DS-Lite tunnel peer: -

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

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/0

Source security zone: Untrust

State: TCP_ESTABLISHED

Application: SSH

Rule ID: 0

Rule name: all

Start time: 2019-12-21 15:27:33 TTL: 1190s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

解决方法

5.总结

- 1.从公网接口进来的报文如果已经匹配了PBR，引到内网转一圈回来再从公网接口出时，不会再匹配PBR。
- 2.需要对从阿里云回来的流量继续匹配PBR，让它从内网转一圈然后再回到公网接口在源地址转换，不然阿里云回复的报文会直接被防火墙转发给公网PC，此时PC收到的报文的源IP地址是阿里云公网ip，并不会进行处理。