Report of IGW network traffic integrity test report

Publish Date: 12/30/2022

Contact Information

[redacted]

Copyright

[redacted]

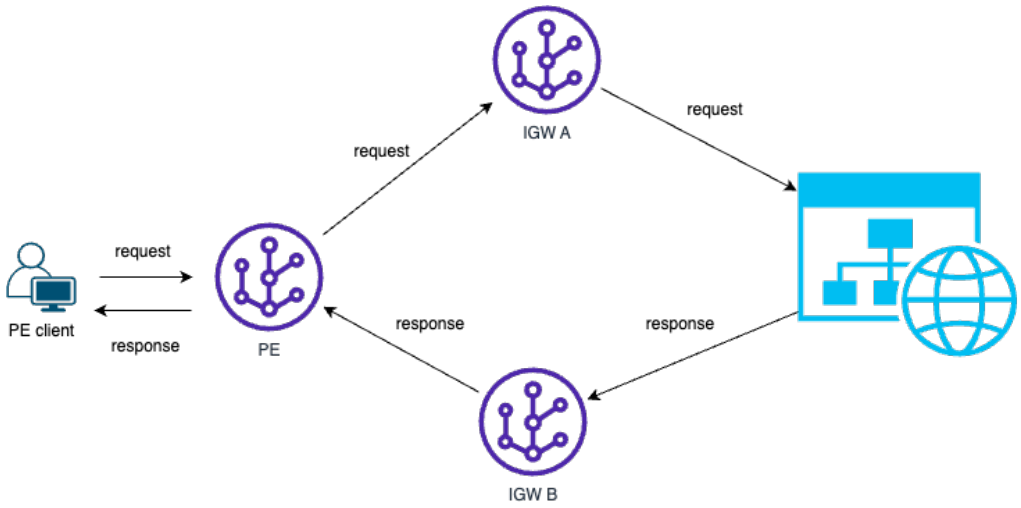
Table of Contents

1 Background 1
2 Methodology 2
3 Test Results 3
4 Conclusions 6

1 Background

We received a ticket about the ineffective blocking of some websites at the IGW level. After some troubleshooting, we believe this is related to the incomplete IGW traffic. Moreover, the high proportion of asymmetric traffic worsens this situation.

Asymmetric routing is a situation where packets follow a different route in an outbound direction than they follow when returning in the inbound direction. As shown in the following figure, the client request (c2s, client to server) goes path PE->IGW-A, but the response (s2c, server to client) is returned through IGW-B→PE.



In general, an asymmetric configuration is fairly normal in many network environments. Asymmetric routing becomes a problem when a firewall is added to the network, and the asymmetry prevents the firewall from seeing both directions of the flow. For example, if a security rule uses the SNI (server name indicator) as a condition, it only enforces at c2s flow. Missing c2s flow jeopardizes security policy enforcement.

2 Methodology

We set up several tests to verify the traffic integrity. There are two main steps： bidirectional

- **Step 1**：For the IP to be tested, execute the following command to initiate an SSL connection, repeat it N times, and record the command execution results.

```
openssl s_client  -connect [test IP]:443 -state
```

- **Step 2:** Query the related log in the TSG session record, and compare the log information on IGW and PE, including quantity and session direction (unidirectional or bidirectional). If there is no traffic missing， for the bidirectional sessions, the number of logs should be equal to N, and for the unidirectional sessions, the number of logs should be equal to 2N.

3 Test Results

The following table summarizes our test records:

2022-12-19 15:40-16:17 client in PE.

IGW c2s traffic missing ratio = (5*5-3-0-2-0-0)/(5*5) = 20/25 = 80%

Test Server IP	**Test Time**	**PE session logs**	**IGW A session logs**	**IGW B session logs**	**Traffic missing ratio**
172.217.169.238 (Googe IP)	15:40-15:42 N=5	Oldairport-PE bidirectional session：5	Bole-IGW **c2s:3** s2c:0	MWV-IGW c2s:0 **s2c:2**	IGW c2s traffic missing rate:40%
104.244.42.65 （Twitter IP)	15:43-16:10 N=5	Oldairport-PE bidirectional session：5	Bole-IGW **c2s:0** s2c:0	MWV-IGW c2s:0 s2c:5	IGW c2s traffic missing rate:100%
157.240.3.35 （Facebook IP)	16:17-16:49 N=5	Oldairport-PE bidirectional session：5	Bole-IGW **c2s:2** s2c:0	DIR-IGW c2s:0 **s2c:3**	IGW c2s traffic missing rate:60%
175.27.8.138 （Tencent IP)	16:49-16:55 N=5	Oldairport-PE bidirectional session：5	Bole-IGW **c2s:0** s2c:0	MWV-IGW c2s:0 **s2c:3**	IGW c2s traffic missing rate:100%

Test Server IP	Test Time	PE session logs	IGW A session logs	IGW B session logs	Traffic missing ratio
123.57.205.17 (AliCloud IP)	16:11-16:17 N=5	Oldairport-PE bidirectional session：5	Bole-IGW **c2s:0** s2c:0	MWV-IGW c2s:0 **s2c:5**	IGW c2s traffic missing rate:100%

2022-12-23 03:00-05:56 client in GGSN.

IGW C2S traffic missing ratio = (120*4+96-115-120-120-90-120)/(120*4+96)=11/576=1.9%

Test Server IP	Test Time	GGSN	IGW A	IGW B	Traffic missing ratio
172.217.169.238 (Googe IP)	03:00-04:55 N=120	NFS-GGSN bidirectional session：120	Bole-IGW **c2s:115** s2c:0	MWV-IGW c2s:0 **s2c:61**	IGW c2s traffic missing rate:4.1%
104.244.42.65 （Twitter IP）	04:00-05:56 N=120	NFS-GGSN bidirectional session：120	MWV-IGW c2s:120 s2c:0	BJR-IGW c2s:0 s2c:120	0%
157.240.3.35 （Facebook IP）	04:00-05:56 N=120	NFS-GGSN bidirectional session：120	Bole-IGW c2s:120 s2c:0	BJR-IGW c2s:0 s2c:120	0%

Test Server IP	**Test Time**	**GGSN**	**IGW A**	**IGW B**	**Traffic missing ratio**
175.27.8.138 (Tencent IP)	03:00-04:55 N=96	NFS-GGSN bidirectional session：96	Bole-IGW **c2s:90** s2c:0	BJR-IGW c2s:0 **s2c:95**	IGW c2s traffic missing rate:6.6%
123.57.205.17 (AliCloud IP)	04:00-05:56 N=120	NFS-GGSN bidirectional session：120	Bole-IGW c2s:120 s2c:0	BJR-IGW c2s:0 s2c:120	0%

4 Conclusions

During the test, we initiated 601 connections to 4 destination IP addresses of YouTube, Facebook, Twitter, Tencent, and AliCloud. The test is performed at internet peak hours (2022-12-19 15:40-16:17) and off-peak hours(2022-12-23 03:00-05:56).

At PE/GGSN level, all 601 connections are found in the system's session record. On the contrary, at the IGW level, only 570 c2s flows are found in the session record, which means 5% of sessions are missing. It's worth noting that during internet peak hours, 20 out of 25 connections are missing.