面向高防业务的互联网网络优化

王羽　刘红云

（中国联合网络通信有限公司河北省分公司 云网运营中心　河北　石家庄　050000）

[摘　要]随着网络攻击规模及攻击手段、攻击频率的不断演化，高防业务逐步成为新的收入增长点。同时，高防业务的突发性、跨省牵引流量、集中性等特点给现有网络的运营带来极大的挑战。本文为河北高防业务引发的首例问题，通过对新出现的高防业务流量流向特点及风险进行描述，重点就现网省间丢包故障进行深入分析，发现并提出解决单边流量的优化方案。分别从流量特点、理论分析、方案制定、优化改造、模型建立等角度入手，最终成功完成流量符合分担调整，建立基于IP地址段的动态调整机制。

[关键词]高防业务；丢包；单边；MED；优化；模板

【DOI】10.12252/j.issn.2096-6288.2021.07.059

一、问题分析

1.高防业务

高防业务是指使用数通技术将网络流量调度至运营商IDC机房内部署的高防服务器，实现L2至L7的攻击防御服务。其特点主要包括高容量、高性能、高可靠性并支持应用层深度清洗。

1.1 IDC引入高防业务存在的风险

高防业务尤其是为客户提供的流量清洗服务是通过大流量攻击触发的，IDC引入高防业务存在以下风险：

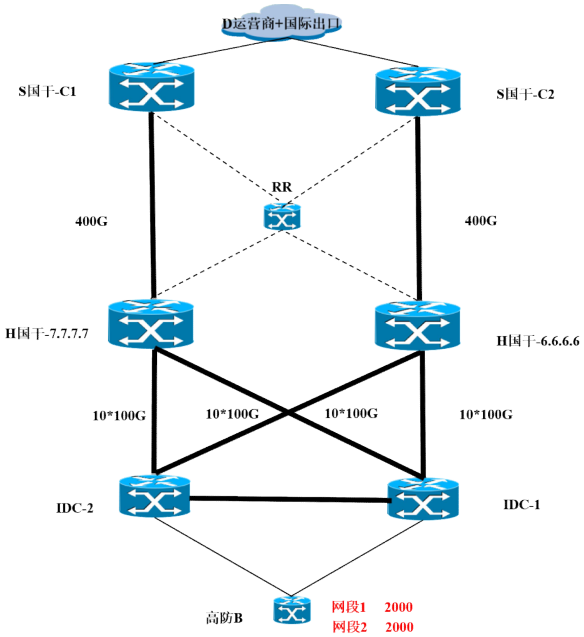
1、牵引流量很难捕捉和定位牵；2、引流量范围具备不确定性；3、牵引流量时间具备不确定性；4、牵引流量叠加具备不确定性。

2.IDC引入高防业务服务商导致省间中继丢包问题分析

IDC在引入高防业务服务商（以下简称高防B）的半年后，开始有客户投诉我省（以下简称H）到S省存在丢包现象。登录支撑系统发现客户投诉时间H省到S省单边中继存在瞬时丢包现象，流量图存在短时毛刺。根据影响客户范围初步判定可能是由于IDC流量过高引起的，将IDC出口流量图和高防业务服务商流量图比对后确认本次丢包故障是由高防业务引起。

2.1 牵引流量分析

利用支持系统对高防B牵引的流量进行流量流向分析，发现：牵引流量2/3来自D运营商，1/3来自国际出口，网内流量不到1%；牵引流量最大为380G，超出部分会被丢弃；牵引的高防IP分布在2个C类地址段上（1.1.1.1和2.2.2.2）。



2.2 H省到S省中继能力分析

根据骨干网路由策略，源地址为D运营商或国际、目的地址为1.1.1.1和2.2.2.2的流量均通过S省到达H省。S省到H省的中继带宽为2*400G，单边为400G，峰值带宽利用率为30%。当牵引流量将中继占满时，就会发生丢包现象。

2.3 牵引流量S省到H省单边流量分析

高防B接入组网分析

高防B到D运营商和国际出口网络结构如图网络结构-1所示：

网络结构-1

（1）高防B通过2组中继双上联到两台IDC核心路由器，高防B通过静态路由与IDC出口路由器互通。

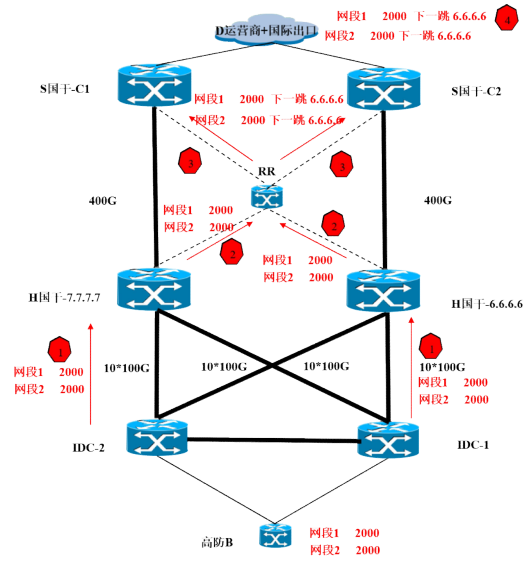
（2）两台IDC出口路由器之间通过OSPF协议建立邻接关系，两台IDC出口路由器通过交叉连接分别和本省2台国干路由器建立EBGP邻接关系。IDC出口路由器向本省两台国干宣告地址段时统一将MED（MULTI_EXIT_DISC　BGP的路径属性）值设置为2000。

（3）H国干和S国干之间通过路由反射器（RR）交换路由信息。

（4）D运营商和国际出口均和S国干设备建立EBGP邻接关系。

3.高防B网段1和网段2路由宣告过程分析

高防B从IDC获得2个C的高防IP地址（网段1　1.1.1.1/24、网段2　2.2.2.2/24），通过IDC向H国干设备宣告，其地址宣告过程如图地址宣告-1所示：



地址宣告-1

（1）IDC出口路由器向H国干发布路由策略时，网段1和网段2设置的MED值均为2000。H国干两台路由器收到网段1和网段2的路由信息后，均将网段1的MED值为2000、网段2的MED值为2000宣告给RR设备，同时将路由的下一跳地址改为自己的LOOPBACK地址。

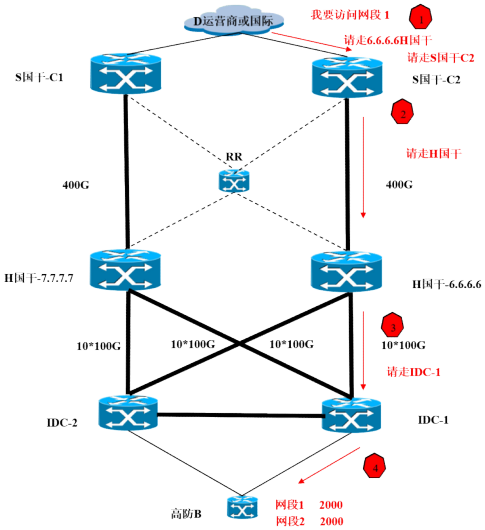
（2）RR设备收到的路由信息是：到网段1有两条路由条目，下一跳分别为6.6.6.6和7.7.7.7；到网段2有两条路由条目，下一跳分别为6.6.6.6和7.7.7.7.RR

（3）设备经过路由优选后，RR将网段1下一跳为6.6.6.6、网段2下一跳为6.6.6.6宣告给S国干设备。

（4）最终，D运营商和国际局收到的路由均可以迭代到网段1和网段2的下一跳是6.6.6.6

4.高防B从D运营商或国际局牵引流量过程分析

当高防B需要对流量进行牵引时，流量的源地址为D运营商或国际地址、目的地址为网段1和网段2，路由逐级查询结果如图引流过程-1所示：



引流过程-1

D运营商或国际流量要访问网段1，选择走S国干-C2。

S国干-C2查找本地路由表，到达网段1下一跳为H国干-6.6.6.6。此时由D运营商或国际到网段1的流量只选择走S国干到H国干的单边。

H国干查找本地路由表，到达网段1下一跳为IDC-1。

二、解决方案

1.原因分析

根据以上分析，我们确定造成H省到S省单边中继丢包的根本原因是IDC出口路由器向H国干宣告网段1和网段2时的路由策略未能区分，导致RR在进行路由优选时只选择了单边。

2.解决实施方案

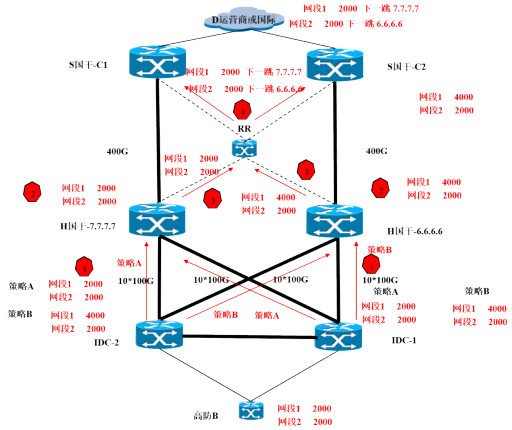
我们通过对不同网段宣告不同MED值的方式，成功让网段1牵引的流量从S国干到H国干的另外一边（7.7.7.7设备侧）经过，解决了牵引流量单边问题。如图解决方案-1所示：

解决方案-1

（1）在IDC1和IDC2上配置策略A和策略B，策略B网段1的MED值设置为4000。

（2）IDC1和IDC2向H国干-6.6.6.6宣告时，应用策略B；IDC1和IDC2向H国干-7.7.7.7宣告时，应用策略A。

（3）H国干-6.6.6.6将策略A汇总后，将下一跳改成自己，宣告给RR；H国干-7.7.7.7将策略B汇总后，将下一跳改成自己，宣告给RR。



（4）RR收到H国干-6.6.6.6和H国干-7.7.7.7宣给自己的路由后，优选结果是：网段1，MED值为2000，下一跳为H国干-7.7.7.7；网段2，MED值为2000，下一跳为H国干-6.6.6.6。

（5）最终，D运营商或国际收到结果是：下一跳为H国干-7.7.7.7；网段2，MED值为2000，下一跳为H国干-6.6.6.6。

经过验证，网段1走S国干-C1-H国干-7.7.7.7、网段2走S国干-C2-H国干-6.6.6.6。实际业务网段1牵引流量峰值为200G，网段2牵引流量峰值为180G，分散到S国干到H国干两边后，瞬时中继峰值占用率未超过80%，中继丢包问题得到圆满解决。

3.动态调整模型

根据以上分析网段1和网段2可以分配到H省到其他省的两侧不同路由。我们可以通过调整网段1和网段2的地址段来调整流量。

（1）分析H省到目标省的中继带宽占用率，按照75%～80%的中继带宽减去实际带宽占用率得到剩余带宽，剩余带宽可以给高防业务使用。

（2）对IDC内部各高防业务服务商的流量流向情况进行分析，预估H省到外省中继的流量大小。

（3）将流量匹配到高防业务IP地址段。

（4）按照H省到不同的目标省分组，每组按照以上分析过程将高防IP分到网段1和网段2进行区分，实现流量的负荷分担。

三、分析总结

河北联通对新出现的高防业务流量进行了近20天的分析，制定出优化改造方案，并通过模拟实验环境、预割接等手段确保优化割接工作一次成功。

优化实施后得到业务部门的充分认可，高防B用户能够按照协议带宽开展高防业务，为公司持续引入高防服务商积累了宝贵经验，建立了动态调整模型。

参考文献

[1]深度分析电商网站产品页设计

作者简介:

1、王羽（1978-03），男，汉族，河北石家庄人，学士，工程师，研究方向：网络运营；

2、刘红云（1976-02），女，汉族，河北石家庄人，学士，高级工程师，研究方向：网络运营。