某局点V7防火墙对接V5防火墙大包不通的经验案例

其他 叶靖 2022-03-31 发表

组网及说明

某局点购买了我司的两台防火墙，分别为V7的F1000-920-AI（版本为Version 7.1.064, Release 9333P26）和V5的F1000-S-AI（版本为Version 5.20, Release 3721P01）。其中V5的防火墙位于总部侧V7防火墙位于分部侧。两台防火墙分别作为总部和分部的出口设备，之间通过专线直连。

问题描述

由于现场两台防火墙之间通过专线互联，仅做简单路由配置，要求两边内网可以互访即可。
现场配置完成之后测试发现，总部和分部两侧的内网主机可以互相ping通，但是现场部分业务异常，后面又经测试发现，总部和分部两侧的内网主机ping小包时可以正常ping通，但是当两侧主机互ping大包时，发现存在丢包甚至不通的情况。现场不断增大ping包的大小，最终测试发现，当报文大小达到23673及以上时，开始出现丢包或者不通的情况。

过程分析

一般交换机等设备支持直接传输大包，但是防火墙产品会对报文进行拆分重组，当报文达到一定大小时会无法正常转发与回应。同时为了避免由于后片先到（报文分片后）的情况而导致设备重组分片报文复杂度过高的问题，设备需要对收到的分片报文先进行虚拟分片重组。IP虚拟分片重组功能可以对分片报文进行检验、排序和缓存，保证后续的报文重组功能处理的都是顺序正确的分片报文。

解决方法

如果现场确实有大包互通的需求，建议如下：

对于V5的防火墙建议配置虚拟分片重组功能，将对应安全域使能勋分片重组功能，可以将分片队列数配置为最大1024，将分片报文数配置为最大255，具体操作如下：

配置虚拟分片重组。

- 在导航栏中选择“防火墙 > 会话管理 > 高级设置”，进行如下配置，如图2-5所示。

图2-5 配置虚拟分片重组

- 选择安全区域为“Trust”。
- 选中“使能虚拟分片重组”前的复选框。
- 单击<确定>按钮完成操作。

通过上面的配置，如果从安全区域为Trust上收到乱序的分片报文，SecPath将会对其进行检验、重新排序

对于V7的防火墙可以开启ip virtual-reassembly enable命令用来开启IP虚拟分片重组功能：

<Sysname> system-view

[Sysname] ip virtual-reassembly enable