某局点无线设备引起MSR路由器CPU高经验案例

wlan接入 用户隔离 陈铮 2015-10-16 发表

AC处于总部，AP位于分部。Msr路由器与总部F5000防火墙建立gre over ipsec隧道保护AC、AP之间的流量。AC、AP之间的流量过高导致MSR路由器的IPSEC进程很高从而使MSR路由器整体CPU利用率非常高

从配置看主要有个两个无线服务
（1）服务模板200是普通用户接入，用的是BYOD方案。
用户未真正MAC认证通过之前，流量是集中转发到AC上，做portal认证的。
这部分流量要走ipsec，但因为没有portal认证通过，按理说不会太大的流量，也就是操作系统、手机后台跑的一些流量，我们控制不了，到了AC才会被portal丢弃。Portal认证通过后，BYOD会把用户踢下线，重新MAC认证走本地转发，也就不涉及ipsec了。

（2）服务模板10是个MAC认证，走集中转发，应当是客户业务需要。
这些用户的所有流量都是要进过ipsec的。需要搞清楚这部分流量有多少，占比多大。

另外，AC上对于集中转发的VLAN，没有开启用户隔离，造成广播报文被复制到各个AP，这点确实是浪费带宽。如果走集中转发的终端没有互访需求，那么开启用户隔离，这是还可以做优化的。

从AC的有线口统计看，出方向流量较大，也就是AC->AP方向，大约是56Mbps左右。从占比看，广播复制产生的流量占了大多数。开启用户隔离，可以把下行流量明显减少。

[MasterAC-hidecmd]dis interface Ten-GigabitEthernet
Last clearing of counters: Never
Last 5 seconds input: 3910 packets/sec 724684 bytes/sec 0%
Last 5 seconds output: 39859 packets/sec 6697779 bytes/sec 1%
Input (total): 53503789 packets, 8100950329 bytes
        52305734 unicasts, 720472 broadcasts, 477583 multicasts, 0 pauses
Input (normal): 53503789 packets, 8100950329 bytes
        52305734 unicasts, 720472 broadcasts, 477583 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, - throttles
        0 CRC, - frame, 0 overruns, - aborts
        - ignored, - parity errors
Output (total): 1641563604 packets, 210620739207 bytes
        1638905433 unicasts, 2458585 broadcasts, 199586 multicasts, 0 pauses
Output (normal): 1641563604 packets, 210620739207 bytes
        1638905433 unicasts, 2458585 broadcasts, 199586 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, - buffer failures
        - aborts, 0 deferred, 0 collisions, 0 late collisions
        - lost carrier, - no carrier

增加了一条配置目的是禁止来自有线“非permit-mac”发送的广播报文进行广播（有线进来的广播报文比较多）。
#
user-isolation vlan 100 enable
user-isolation vlan 100 permit-mac 0000-5e00-0102 7425-8ae9-7c60 3891-d528-2d80 7425-8ae9-7c68
user-isolation vlan 200 enable
user-isolation vlan 200 permit-mac 0000-5e00-0103 7425-8ae9-7c60 3891-d528-2d80 7425-8ae9-7c68
undo user-isolation permit broadcast
#

[MasterAC-hidecmd]dis interface Ten-GigabitEthernet
 Ten-GigabitEthernet1/0/1 current state: UP
Last 5 seconds input: 1321 packets/sec 253132 bytes/sec 0%
Last 5 seconds output: 2048 packets/sec 406323 bytes/sec 0%

Ten-GigabitEthernet1/0/2 current state: UP
Last 5 seconds input: 1574 packets/sec 238387 bytes/sec 0%
Last 5 seconds output: 126 packets/sec 43724 bytes/sec 0%

至此MSR路由器CPU压力大幅度降低

通过广播隔离本地转发等优化手段减少AC、AP流量，从而减轻MSR路由器ipsec进程转发压力。