

组网及说明

ER3108G，WAN口接运营商，LAN口接自己的内网

问题描述

ER3108G内网有50台电脑左右，没有下挂无线路由器，也没有使用VPN，但是设备的CPU超过了90%

过程分析

设备CPU利用率高，一般都为流量或者ARP攻击或者广播报文泛洪引起，跟组网有很大的关系，分析接口信息发现：

在用的5个lan口差不多流量都在七八百兆，但是上行口的WAN口只有34Mbps，这已经快接近这款设备的性能了，所以CPU高也是正常的。

需要排查一下为何内网流量这么大，从流量特征来看，LAN3口的上行流量很大，下行很小，其余LAN口下行都很大，上行比较小，怀疑是LAN3口有人私设下载服务器，其他人下载导致流量大的。

WAN:up packets:10630545, up bytes:77114010352, up packet rate:458pps, up byte rate:3338742Bps.

down packets:7377536, down bytes:29751121736, down packet rate:295pps, down byte rate:938404Bps.

total packets:18008081, total bytes:106865132088, total packet rate:753pps, total byte rate:4277146Bps. //约等于34Mbps

LAN1:up packets:81413784, up bytes:75692684248, up packet rate:5145pps, up byte rate:8458043Bps.

down packets:377604818, down bytes:487788362424, down packet rate:47957pps, down byte rate:86624718Bps.

total packets:459018602, total bytes:563481046672, total packet rate:53102pps, total byte rate:95082761Bps. //约等于760Mbps

LAN2:up packets:4299601365, up bytes:3340265616, up packet rate:263pps, up byte rate:314178Bps.

down packets:432550735, down bytes:501090195840, down packet rate:49657pps, down byte rate:88506780Bps.

total packets:4732152100, total bytes:504430461456, total packet rate:49920pps, total byte rate:8820958Bps. //约等于711Mbps

LAN3:up packets:358512478, up bytes:470078636656, up packet rate:47594pps, up byte rate:86400667Bps.

down packets:159157595, down bytes:134251957200, down packet rate:10083pps, down byte rate:13075013Bps.

total packets:517670073, total bytes:604330593856, total packet rate:57677pps, total byte rate:99475680Bps. //约等于796Mbps

LAN4:up packets:40962555, up bytes:26478131792, up packet rate:2064pps, up byte rate:2152372Bps.

down packets:408670098, down bytes:487770278272, down packet rate:48905pps, down byte rate:87737341Bps.

total packets:449632653, total bytes:514248410064, total packet rate:50969pps, total byte rate:889713Bps. //约等于719Mbps

LAN5:up packets:34359778842, up bytes:5638584, up packet rate:0pps, up byte rate:0Bps.

down packets:71110080, down bytes:78785130336, down packet rate:0pps, down byte rate:0Bps.

total packets:34430888922, total bytes:78790768920, total packet rate:0pps, total byte rate:0Bps.

LAN6:up packets:0, up bytes:0, up packet rate:0pps, up byte rate:0Bps.

down packets:0, down bytes:0, down packet rate:0pps, down byte rate:0Bps.

total packets:0, total bytes:0, total packet rate:0pps, total byte rate:0Bps.

LAN7:up packets:0, up bytes:0, up packet rate:0pps, up byte rate:0Bps.

down packets:0, down bytes:0, down packet rate:0pps, down byte rate:0Bps.

total packets:0, total bytes:0, total packet rate:0pps, total byte rate:0Bps.

LAN8:up packets:34359974984, up bytes:26773360, up packet rate:1pps, up byte rate:1311Bps.

down packets:455934291, down bytes:524352921768, down packet rate:49641pps, down byte rate:88249567Bps.

total packets:34815909275, total bytes:524379695128, total packet rate:49642pps, total byte rate:88250878Bps. //约等于706Mbps

解决方法

排查了LAN3口下的组网，发现有一台服务器在大量给其他内网PC发包，应该是中毒了，首先隔离了

这台服务器，进行全面杀毒后，问题解决了。