

知 ERG3及UR设备 纯lan口透传 dns无法解析

DNS ChandlerBing 2023-12-07 发表

组网及说明

组网1: 防火墙—交换机-- (vlan1) erg3 (vlan1) —ap

组网2:

光猫-ER8300G2---交换机---pc1



Pc2 (192.168.3.182)

问题描述

组网1、2问题均为纯lan口透传 dns无法解析, 具体来看

组网1问题: ERG3设备做纯二层透传, 终端通过ap可以ping通外网百度的IP, 但是ping不通百度域名

组网2问题:

1、ur使用两个lan口, 一个上联主路由ER, 一个直连pc, 如果是当交换机使用, 下联的pc获取到地址之后能ping通公网地址, 但是不通域名, dns无法解析, ur替换成交换机也正常; 2、如果ur接wan口, 当网关使用正常能上网

过程分析

以组网1为例, 经过抓包排查 (测试地址为86.80), erg3有收发dns报文, 但是交换机上没有收到dns Er抓包: 收到且发了

No.	Time	Source	Destination	Protocol	Length	Info
4	0.275869	10.0.86.80	202.106.196.115	DNS	73	Standard query 0x4786 A www.baidu.com
8	0.837818	10.0.86.80	114.114.114.114	DNS	78	Standard query 0x6970 A edge.microsoft.com
12	1.280430	10.0.86.80	114.114.114.114	DNS	73	Standard query 0x4786 A www.baidu.com
16	1.843530	10.0.86.80	202.106.196.115	DNS	78	Standard query 0x6970 A edge.microsoft.com
22	2.771485	10.0.86.80	114.114.114.114	DNS	73	Standard query 0x135b A wpad.aten.com
23	2.771485	10.0.86.80	202.106.196.115	DNS	73	Standard query 0x135b A wpad.aten.com
24	2.850980	10.0.86.80	114.114.114.114	DNS	78	Standard query 0x6970 A edge.microsoft.com
26	3.288217	10.0.86.80	114.114.114.114	DNS	73	Standard query 0x4786 A www.baidu.com
27	3.288671	10.0.86.80	202.106.196.115	DNS	73	Standard query 0x4786 A www.baidu.com
31	3.569415	10.0.86.80	202.106.196.115	DNS	84	Standard query 0x6785 A minorshort.weixin.qq.com
32	3.569415	10.0.86.80	114.114.114.114	DNS	84	Standard query 0x6785 A minorshort.weixin.qq.com
43	4.868296	10.0.86.80	114.114.114.114	DNS	78	Standard query 0x6970 A edge.microsoft.com
44	4.868592	10.0.86.80	202.106.196.115	DNS	78	Standard query 0x6970 A edge.microsoft.com
59	6.847687	10.0.86.80	114.114.114.114	DNS	78	Standard query 0x2020 A edge.microsoft.com
60	6.847687	10.0.86.80	114.114.114.114	DNS	78	Standard query 0x536e Unknown (65) edge.microsoft.com
62	7.302543	10.0.86.80	114.114.114.114	DNS	73	Standard query 0x4786 A www.baidu.com

交换机抓包: 无86.80地址

No.	Time	Source	Destination	Protocol	Length	Info
44440	64.626520	10.0.86.82	202.106.196.115	DNS	79	Standard query 0x8233 A updatem.360safe.com
44441	64.626621	10.0.86.82	202.106.196.115	DNS	79	Standard query 0x8233 A updatem.360safe.com
44442	64.629133	202.106.196.115	10.0.86.82	DNS	317	Standard query response 0x8233 A updatem.360safe.com CNA
44443	64.629133	202.106.196.115	10.0.86.82	DNS	317	Standard query response 0x8233 A updatem.360safe.com CNA

经过定位, 为ERG3、UR设备的转发机制问题, DNS劫持把DNS相关的报文走到了CPU而没走二层转发

解决方法

升级到R0136P04版本