Cisco设备ping直连的S7500E设备虚接口地址丢包问题说明

攻击检测及防范 攻击检测及防范 攻击检测及防范 VRRP **赵国卫** 2012-04-18 发表

Cisco设备ping直连的S7500E设备虚接口地址丢包问题说明

一、 组网：

无

二、 问题描述：

Cisco设备直连S7500E设备，从Cisco设备p i n g 直连的S7500E的虚接口IP地址，发现存在丢包现象。而使用PC ping 同样的虚接口IP地址却不丢包。

三、 过程分析：

Cisco设备发ping包的速率要比普通PC发的ping包速度快。之所以从Cisco设备ping S7500E存在丢包，是因为S7500E交换机对ping自己三层接口的报文设置了漏桶大小，目的是防DOS攻击，在持续ping报文，大流量ping报文，长包持续ping包的情况，会丢弃一部分报文，避免ICMP等恶意攻击耗费CPU资源。这就是我们平常所说的CPU保护机制，此机制包括两方面:硬件Car和软件Car。针对ICMP报文的这两种Car可以通过诊断模式里的命令行关闭，但强烈不建议这样做。关于两种Car的详细说明如下：

1. 硬件Car

关闭对 ICMP的硬件car:

[S7506E]en_diag //进入诊断模式

[S7506E-diagnose]debug rxtx rxacl globaldisable icmp 3 //(3 是对应slot 号)

Disable Protocol Pkt : ICMP for Global Ret = 0

开启ICMP的硬件car:

[S7506E-diagnose]debug rxtx rxacl resume icmp 3 //(3是槽位号)

2. 软件Car

查看软件car是否存在丢包，可以通过下面的命令：

[S7506E]en_diag //进入诊断模式

[S7506E]debug rxtx softcar show [槽位号] //查看软件Car

例如查看3槽位的软件car丢包情况，采用如下命令

[S7506E-diagnose]debug rxtx softcar show 3

The softcar pps auto-adjust switch: On

Index	Type	Number	Pps	Switch	HashMode
0	ROOT	0	200	On	SMAC
1	ISIS	0	200	On	SMAC
2	ESIS	0	100	On	SMAC
3	CLNP	0	100	On	SMAC
4	VRRP	0	300	On	SMAC
5	UNKNOWN_IPV4MC	0	100	On	SMAC
6	UNKNOWN_IPV6MC	0	100	On	SMAC
7	IPV4_MC_RIP	0	150	On	SMAC
8	IPV4_BC_RIP	0	150	On	SMAC
9	MCAST_NTP	0	100	On	SMAC
10	BCAST_NTP	0	100	On	SMAC
……此处省略部分输出……..					
41	ICMP	1022	200	On	SMAC

从上面的输出内容中可以看到软件Car丢弃的报文(红色数字部分)

关闭软件Car的方法:

[S7506E-diagnose]debug rxtx softcar [index-number(报文类型防攻击序号)] [槽位号]

disable Disable————————————关闭软件防攻击功能。

enable Enable————————————启动软件防攻击功能。

portdetail SoftCar set on Port Detail————查看该报文类型各个端口防攻击信息。

pps Pps ————设置防攻击漏桶大小。

例如根据上面的输出可以看到ICMP的index-number是41,槽位是3槽位

41 ICMP 1022 200 On SMAC

则关闭的命令为

[S7506E-diagnose]debug rxtx softcar 41 3 disable

开启的命令为(缺省开启)

[S7506E-diagnose]debug rxtx softcar 41 3 enable

四、 解决方法：

在客户对此问题有疑问的前提下，可以先按照CPU保护的原理跟客户解释，如果客户不认可解释，可以通过上述命令关闭对应的Car演示给客户看，以证实确实是因为CPU的保护机制导致此丢包现象。演示完毕之后，请重新使能对应的Car功能，以确保设备的安全。其他场合禁止在设备上关闭对应的CPU保护功能。