

NE40/NE80/S8016在版本VRP3.10防攻击的系统漏桶参数说明

NE40/NE80/S8016产品在版本VRP3.10针对出现过多上送主控板的协议报文时，如cmp及telnet、ftp等报文，根据实际情况，需要考虑调整系统漏桶来为防止攻击。具体可以用display system - bucket查看漏桶丢弃计数，对丢弃频繁的漏桶进行限流配置。

比如：

```
[8016]display system-bucket 1
****Token information****
#The slot number: 1 /*板号*/
#The token ID: 1 /*漏桶号*/
The time of the last packets arrive:36403113 /*上次报文到来的时间ms*/
The number of present tokens: 32716 /*当前剩余的令牌*/
The traffic rate of the token: 32K /*漏桶通道大小*/
The height of the token bucket:32768 /*漏桶深度*/
The number of the discarded packets: 0 /*丢弃报文数*/
```

如果丢弃报文数变化比较频繁，则考虑限制此漏桶的通道大小，可能有攻击。一般来说，根据实际业务情况，对相应的漏桶做一定的配置，如对1、2、3、22、31做相应的限制。例如：

```
apply system-bucket 1 2 traffic-rate 2
/*将1号板的2号漏桶ARP MISS配置为2K*/
apply system-bucket 1 3 traffic-rate 2
/*将1号板的3号漏桶FIB MISS配置为2k，对于subvlan较多的点，建议将此漏桶上送报文字节配置为2 */
apply system-bucket 1 6 traffic-rate 2
/*将1号板的6号漏桶ARP response配置为2K*/
apply system-bucket 1 31 traffic-rate 2
/*将1号板的31号漏桶ICMP配置为2K*/
```

另外，由于ARP攻击，需要根据实际的业务量大小做相应的限制。根据网上设备运行经验：如果单板ARP数小于100个，则漏桶可以配置为2K；如果单板的ARP数小于500个，对于ARP攻击建议将漏桶配置成4K；如果大于500个，建议漏桶配置值为8K。通过上述的配置，在一般情况或者攻击很少的情况对正常业务影响不大。具体配置请参见：

```
apply system-bucket 1 22 traffic-rate 4
/*将1号板的22号漏桶ARP配置为4K*/
```

每个漏桶的报文类型可以通过如下命令查看

```
"display system-bucket <slotno> ?"
```

```
<8016> display system-bucket 7 ?
```

- 1 Default bucket , any packet not list here use this bucket
缺省类型，也就是表中没有列出的其他类型报文都公用这一个桶
- 2 ARP Miss message , use it to form ARP entry
ARP MISS 消息（请求下一跳的ARP）
- 3 FIB Miss Message , use it to form host route entry
FIB MISS消息（扫描网段时经常发生，上送触发ARP请求）
- 4 PPP protocol control frame
PPP控制报文
- 5 Packet MFIB Miss , use it to form (S,G) route
组播路由MISS后导致的上送消息
- 6 ARP response packet
回应S8016的ARP应答报文
- 8 ISIS protocol packet
ISIS报文
- 9 IP multicast packet which destIP address is 224.0.0.2(used by IGMP, LDP etc)
224.0.0.2：所有组播路由器，应用的协议：IGMP、LDP
- 10 IP multicast packet which destIP address is 224.0.0.5(used by OSPF)
224.0.0.5：OSPF路由器
- 11 IP multicast packet which destIP address is 224.0.0.6(used by OSPF)
224.0.0.6：OSPF指定路由器

- 12 IP multicast packet which destIP address is 224.0.0.9(used by RIP2)
224.0.0.9 : RIP2路由器
- 14 IP multicast packet which destIP address is 224.0.0.13(used by PIM)
- 15 Other IP multicast packet which destIP address is in
224.0.0.0-224.0.0.255(excluded.2 .5 .6 .9 .10 .13 .18)
其他组播报文应用不多，本参数应该可以满足
- 16 HGMP protocol packet
HGMP报文上送
- 17 GVRP protocol packet
GVRP报文上送
- 19 BPDU protocol packet
BPDU报文上送
- 21 Packet length exceed MTU and DF flag is set , it is used by host to
discover the MTU in the route
MTU超值且DF位置上送
- 22 ARP request packet send by all the host , use it to learning host route
ARP 请求报文，一般用户发出或者下级设备发出
- 23 DHCP protocol packet
DHCP报文
- 24 Arp request packet witch destIP is in NAT pool
NAT地址池的ARP请求报文，应用很少
- 25 Register packet used in PIM SIM protocol
组播注册报文
- 27 Packet which destIP is ip address of gateway, exclude ICMP and TCP
目的地址为网关的报文，不包括ICMP和TCP，通常为UDP报文等
- 28 ICMP request packet witch destIP is webswitch's VIP
和CLPU板相关，应用很少
- 30 IP multicast packet which destIP address is 224.0.0.18(used by VRRP)
VRRP组播报文，如果有VRRP配置时会有
- 31 ICMP packet which destIP is ip address of gateway, for example, ping pack
et
目的地址为网关的ICMP报文，典型的为ping
- 32 TCP packet which destIP is ip address of gateway, for example, FTP, BGPpe
er, LDP session
目的地址为网关的的TCP报文，如果没有BGP和LDP，注意此漏桶的攻击，默认带宽
较大，有256K
- 33 RIP1 protocol packet
RIP协议报文