

SecPath F5000-C(V7) IMC官网平台告警该设备519、518、520等接口出现链路Down告警

Syslog日志 刘嘉炜 2019-10-16 发表

组网及说明

不涉及

问题描述

IMC日志平台经常会收到来自该防火墙519、518、520等接口的两路Down告警，但是告警端口为接口索引值无法确认防火墙那个端口出现了问题。

IMC信息如图所示：

告警详细信息

名称	链路DOWN
级别	重要
OID	1.3.6.1.6.3.1.1.5.2
告警时间	2019-08-09 15:35:00
告警来源	CZHK-F5020-HX(10.6.9.17) 更多告警...
类型	Trap
告警分类	接口/链路状态告警
恢复状态	未恢复
确认状态	未确认
详细信息	接口519的状态DOWN。
告警原因	链路状态由UP变为DOWN，可能的原因：1、用户disable接口；2、连接该接口的网线被拔掉或者损坏；3、接口配置中，接口的IP被删除；4、链路中对接口故障。
修复建议	1、检查该接口的配置是否为disable，如果是，请使能该接口；2、检查连接该接口的网线是否松动或者损坏；3、检查设备配置，确定该接口是否有正确的IP地址；4、检查对接口是否故障。
挂载信息	
维护经验	
备注	--[修改]
考核部门	--[修改]

参数名称	参数值
*Interface Index	519
Interface Description	519
Interface Admin Status	1
Interface Operate Status	2

过程分析

通过MIB browser读取设备IFDescr节点信息，发现告警端口索引值并不在端口列表中。

The screenshot shows the MIB browser interface with a tree view on the left and a query results window on the right. The tree view shows the hierarchy: dod -> internet -> deviceloc -> mgmt -> mib-2 -> system -> interfaces -> ifTable -> IFDescr (highlighted in red). The query results window shows the output of an SNMP query for the IFDescr table, listing 33 interfaces (1 to 33) with their corresponding IP addresses. Interface 519 is not present in this list.

查看设备对应的接口列表信息：

```

[CZHK-F5020-HX]display interface brief
Brief information on interfaces in route node:
Link: ADM - administratively down; Sby - standby
Protocol: (s) - spoofing
Interface      Link Protocol Primary IP      Description
GE1/0/0       DOWN DOWN      100.100.0.1
GE1/0/1       UP UP        10.6.11.251    link-liantong
GE1/0/2       DOWN DOWN      ---
GE1/0/3       DOWN DOWN      ---
GE1/0/4       UP UP        60.277.100.13  60.277.100.13
GE1/0/5       DOWN DOWN      ---
GE1/0/6       DOWN DOWN      1E.1.1.1       1E.1.1.1
GE1/0/7       DOWN DOWN      ---
GE1/0/8       DOWN DOWN      ---
GE1/0/9       DOWN DOWN      ---
GE1/0/10      DOWN DOWN      ---
GE1/0/11      DOWN DOWN      ---
GE1/0/12      ADM DOWN     1P.1.1.1       1P.1.1.1
GE1/0/13      UP UP        10.6.9.17      10.6.9.17
GE1/0/14      DOWN DOWN      ---
GE1/0/15      DOWN DOWN      ---
GE1/0/16      DOWN DOWN      ---
GE1/0/17      DOWN DOWN      ---
GE1/0/18      DOWN DOWN      ---
GE1/0/19      DOWN DOWN      ---
GE1/0/20      DOWN DOWN      ---
GE1/0/21      DOWN DOWN      ---
GE1/0/22      DOWN DOWN      ---
GE1/0/23      DOWN DOWN      ---
InLoop0      UP UP(s)
Loop0        UP UP(s)
NULL0        UP UP(s)
REG0         UP ---
XGE1/0/24    DOWN DOWN      ---
XGE1/0/25    DOWN DOWN      ---
XGE1/0/26    DOWN DOWN      ---
XGE1/0/27    DOWN DOWN      ---
UT1          DOWN DOWN      ---
[CZHK-F5020-HX]

```

通过接口索引值判断告警端口应该为设备虚拟接口，因为虚拟接口的索引值全部以500+开始。



排查设备配置中发现客户在设备上使能了L2TP VPN，测试发现L2TP VPN用户登录后该告警就会产生，基本可以判断此UP/Down端口与L2TP有关。

当L2TP用户上线后设备默认为该用户分配一个VA接口，当L2TP用户下线后该端口就会Down掉，最终判断该索引值为VA接口索引值，对现场业务没有影响。

```

<CZHK-F5020-HX>display interface va
Virtual-Access0
Current state: UP
Line protocol state: UP
Description: Virtual-Access0 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.6.11.254/24 <primary>
Link layer protocol: PPP
LCP: opened, IPCP: opened
Physical: L2TP, baudrate: 100000000 bps
Main interface: Virtual-Template1
Last clearing of counters: Never
Last 300 seconds input rate: 1985 bytes/sec, 15880 bits/sec, 23 packets/sec
Last 300 seconds output rate: 59618 bytes/sec, 476944 bits/sec, 43 packets/sec
Input: 8478 packets, 717014 bytes, 0 drops
Output: 15383 packets, 21091892 bytes, 0 drops

```

解决方法

1、该问题还是由于IMC服务器告警中显示了端口索引导致，正常情况下IMC应当显示接口真实编号。

解决方法请参考案例：<http://kms2.h3c.com/View.aspx?id=58173>

1>告警组件没有加载成功设备的接口信息；

规避方式：重启IMC的imcfauldm进程；或者升级iMC到7.3E0506及以上版本。

2>设备的接口信息发生变化，例如动态建立VLAN，虚接口变化等情况。

这种情况暂时没有规避方案，因为设备上的接口的索引已经变化了，iMC不能通过此索引找到接口信息。

2、该告警没有实际意义，可以在IMC侧将此告警过滤后续就不会再收到此类告警信息了。

告警详细信息

名称	链路DOWN
级别	重要
OID	1.3.6.1.6.3.1.1.5.2.0
告警时间	2015-07-23 16:14:03
告警来源	H3C(10.153.42.11) 更多告警...
类型	Trap
告警分类	接口/链路状态告警
告警接口	GigabitEthernet5/0/11 Interface
恢复状态	未恢复
确认状态	未确认
详细信息	接口GigabitEthernet5/0/11的状态DOWN.
告警原因	链路状态由UP变为DOWN, 可能的原因: 1. 用户disable接口; 2. 连接该接口的网线被拔掉或者损坏; 3. 接口配置中, 接口的IP被删除; 4. 链路中对称端口故障.
修复建议	1. 检查该接口的配置是否为disable, 如果是, 请使能该接口; 2. 检查连接该接口的网线是否松动或者损坏; 3. 检查设备配置, 确定该接口是否有正确的IP地址; 4. 检查对称接口是否故障.
维护经验	

动作

- 恢复
- 确认
- 删除
- 过滤该告警**
- 修改Trap定义级别
- 编辑维护经验
- 故障根源和影响度分析
- 故障根源和影响度分析V2
- 上一条
- 下一条