[2012-03-01]H3C SecPath5000FA-CMW520-F3210P03版本发布

金山 2012-03-01 发表

H3C SecPath5000FA-CMW520-F3210P03版本发布

一、 使用范围及配套说明：

H3C SecPath5000FA-CMW520-F3210P03版本正式发布，使用范围为国内市场。

表1：版本配套表

产品系列	H3C SecPath
型号	SecPath F5000-A5
内存需求	主控插卡: 4GB 业务插卡: 512MB
FLASH需求	4M
CLDP	主控板基本段:3.0，扩展段: 1.0 LPUA线卡板基本段:1.0，扩展段: 1.0 12GE接口板: 2.0，2*10GE接口板:1.0
BootRom版本号	1.09
目标文件名称	SECPATH5000FA-CMW520-F3210P03.bin
iMC版本号	iMC PLAT 5.1 (E0202)
SecCenter	SecCenter Firewall Manager E0027P04
备注	无

二、 增减特性说明：

表2：特性变更说明

版本号	项目	描述
SECPATH5000FA-CMW520-F3210P03	硬件特性更新	新增特性：无。 删除特性：无。 修改特性：无。
	软件特性更新	新增特性：无。 删除特性：无。 修改特性：无。

三、相比前一版本解决的问题说明：

1. HSD97657

问题产生条件：开启FTP ALG及NAT功能。

问题现象：当FTP并发连接比较多时，可能出现FTP控制连接截取某些特殊FTP载荷报文时出现越界，从而导致设备重启。

2. HSD97664

问题产生条件：设备连续运行497天。

问题现象：Web页面与命令行的运行时间显示不一致。

3. HSD96862

问题产生条件：开启Userlog日志功能。

问题现象：发送到日志主机的Userlog日志内容不完整，并且多出了20个字节的非法数据。

4. HSD100172

问题产生条件：F5000-A5 开启会话加速，二层转发。

问题现象：会话建立后不删除，导致会话打满后出现大量失败。

5. HSD100253

问题产生条件：三层Vlan Interface配合双机热备组网。

问题现象：长时间H.323应用协议流量下，设备异常重启。

6. HSD84654

问题产生条件：防火墙二层组网，网络中运行H.323视频业务。

问题现象：H.323视频中的分片报文会导致防火墙异常重启。

7. HSD100338

问题产生条件：域间策略引用时间段对象。

问题现象：当时间段生效的时候，部分会话的可能会出现接口安全域错误，导致无法匹配域间策略。

四、版本使用限制及注意事项：

1、版本升级注意事项

如果将设备版本从R3206、F3207、F3208系列版本升级到F3210系列版本时，需要注意以下配置是否有问题：

a）确认设备上是否配置了NAT Server以及NAT Server配置中是否有绑定ACL的配置，如果有该配置，则其中已绑定ACL的NAT Server配置在升级后会丢失。

b）确认接口下是否配置了NAT静态地址映射（NAT Static）、NAT地址池（NAT address-group）及服务器映射(NAT Server)，如果有该配置并且NAT配置中的global地址与接口地址不在同一网段，则防火墙接口默认对于收到的针对NAT global地址的ARP请求不会进行响应。在防火墙对端设备未配置指

向NAT global地址的路由时可能引发NAT中断问题，可以通过在该接口下配置与NAT global在同一网段的sub地址来实现ARP响应。
c）F3210系列版本新增虚拟设备最大会话数的配置，升级版本前确认设备上是否配置了虚拟设备，如果已经配置了，从其他版本升级到F3210系列后，最大会话数会默认设置为0，需要根据用户实际情况调整每个虚拟设备的最大会话数。
d）F3207及R3206部分版本的地址资源（含主机地址、范围地址、子网地址）名称、自定义服务资源名称、服务组资源名称可以配置允许配置某些特殊字符（包括：“!”、“#”、“?”、“@”、“~”、“(”、“)”），但是F3210系列版本不支持这些特殊字符，因此需要在版本升级前将这些字符替换成其他字符。
2、在F3207、R3206及F3208系列版本上配置的TCP Proxy中的受保护IP，升级到F3210P01系列版本后会存在配置丢失，需要重新配置受保护IP。
3、已知硬件总线缺陷。
设备开启虚拟报文重组，如果数据报文分片数超过五个，SPI4.2总线会在发送第六个分片的时候出现报文反压导致的分片报文丢弃。
4、已知PHY芯片缺陷。
BCM 5464芯片在强制模式下， 不支持交叉/直联网线自适应，表现为BCM 5464与BCM 5464对接，两端都是强制模式下时只能使用交叉网线，否则不能link up，F5000-A5的12GE线卡采用了BCM 5464，存在此限制。
5、RMON统计限制。
主控和12GE线卡的网口不具有RMON统计功能，属于硬件限制。
6、ICMP分片报文发送限制。
ping 35000以上大包时，可能不通，原因是设备回应ICMP报文的时候由于报文超过接口MTU需要将报文分片发送，报文越大分片数量就越多，由于SecPath F5000A5 产品裁减了QoS的队列功能，导致接口物理发送失败的时候报文会被直接丢弃，而RMI固定口配置的发送credit数量是有限的，这样在突然连续发送大量分片报文的时后可能因瞬间发送速率大于接口的物理发送速率而引起分片的发送失败，这样在PC侧因为无法收到所有的分片而不能重组成ICMP报文。
7、2*10GE模块无法提供错包统计的功能。
2*10GE模块使用的MAC芯片不支持错包统计，所以2*10GE模块不提供错包统计的功能。

五、 版本存在问题与规避措施：

1. 问题ID—HSD51584
遗留问题：新配置安全策略时，如果此时与该策略匹配的会话已经存在，那么策略下发后不会立即生效，数据流仍然按照原有会话转发。
规避措施：可以通过reset session进行规避。
2. 问题ID—HSD60317
遗留问题：配置OSPF等价路由，F5000A5做中间设备，tracert信息异常。
规避措施：设备把TTL为1的报文丢弃，但不影响正常使用。
3. 问题ID—HSD61584
遗留问题：F5000A5 ARP detection功能不生效。
规避措施：F5000A5 不支持ARP detection功能，不要使用ARP detection功能。
4. 问题ID—HSD51584
遗留问题：在更换下次启动版本文件时，出现bfd中断
规避措施：需要配置，加长BFD检测时间进行规避
5. 问题ID—HSD100172
遗留问题：F5000-A5 开启会话加速，进行二层业务转发，设备异常重新启动。
规避措施：F5000-A5进行二层业务转发时，关闭会话加速。

六、 升级时注意事项：

请务必参照《H3C SECPATH5000FA-CMW520-F3210P03版本使用指导书.doc》中的版本升级指导进行升级。
如要完整的了解该版本累计解决的问题，请参看配套的《H3C SECPATH5000FA-CMW520-F3210P03版本说明书.doc》。