

H3C SECPATH1000FE&SECBLADEII-CMW520-F3171P03版本发布

一、使用范围及配套说明：

H3C SECPATH1000FE&SECBLADEII-CMW520-F3171P03版本正式发布，使用范围为国内市场。

表1：版本配套表(F1000-E)

产品系列	H3C SecPath
型号	SecPath F1000-E
内存需求	2G
FLASH需求	4M
CPLD	3.0
BootWare版本号	1.38
目标文件名称	SECPATH1000FE-CMW520-F3171P03.bin
iMC版本号	iMC PLAT 5.0 SP1 (E0101L07)
SecCenter Firewall Manager	SecCenter Firewall Manager E0027
备注	无

表2：版本配套表(SecBlade II)

产品系列	H3C SecBlade
型号	SecBlade II
内存需求	最小2G
FLASH需求	4M
CPLD	3.0
BootWare版本号	1.38
目标文件名称	SECBLADEII-CMW520-F3171P03.bin
S7500E 配套版本	S7500E-CMW520-R6626
S9500 配套版本	S9500-CMW310-R1651P05
S9500E配套版本	S9500E-CMW520-R1235P03
S5800配套版本	S5800_5820X-CMW520-R1211P02
S12500配套版本	S12500-CMW520-R1335P03
SR6600配套版本	SR6600-CMW520-R2603
SR8800配套版本	SR8800-CMW520-R3345P02
iMC版本号	iMC PLAT 5.0 SP1 (E0101L07)
SecCenter Firewall Manager	SecCenter Firewall Manager E0027
备注	无

二、增减特性说明：

表3：特性变更说明

版本号	项目	描述
SECPATH1000FE&SECBLADEII-CMW520-F3171P03	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：支持保持上一跳功能。 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. 问题ID—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载荷报文时出现异常，导致设备重启。

2. 问题ID—HSD97664

问题产生条件：无

问题现象：运行一定时间后，Web页面与命令行的运行时间显示不一致。

3. 问题ID—HSD96549

问题产生条件：网络攻击或流量增大导致会话数增多，引起设备内存升高。

问题现象：流量恢复后，内存依然维持在较高水平，会话占用的内存回收较慢。

4. 问题ID—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。

5. 问题ID—HSD97292

问题产生条件：无

问题现象：防火墙内部10GE接口速率统计错误。

6. 问题ID—HSD95817

问题产生条件：无

问题现象：当设备内存占用率很高的情况下，概率性存在软件处理异常，导致设备重启。

7. 问题ID—HSD93926

问题产生条件：无

问题现象：修改地址组对象失败后点击导航树中的域间策略，设备堆栈重启。

8. 问题ID—HSD94393

问题产生条件：无

问题现象：穿越防火墙的FTP登录，在防火墙的外网配置Nat Server情况下，客户端通过私网地址直接登录，数据通道建立时匹配了Nat Server导致数据通道建立失败。

9. 问题ID—HSD92124

问题产生条件：无

问题现象：FIN报文两次从不同方向经过防火墙以后，一个方向的FIN报文会被防火墙丢弃。

10. 问题ID—HSD94491

问题产生条件：无

问题现象：导入IP地址和地址组资源设备堆栈重启。

11. 问题ID—HSD94379

问题产生条件：无

问题现象：SNMP Test连接设备，使用SHA-3DES方式会导致设备出现异常。

12. 问题ID—HSD95197

问题产生条件：无

问题现象：当会话占用的内存上升到一定峰值后，即使会话数较少，内存占用依然不释放。

13. 问题ID—HSD95989

问题产生条件：无

问题现象：设备快转HASH桶深度有限存在HASH冲突的可能性，导致出现丢包或流量中断。

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F3166、R3166或F3169系列版本升级到F3171系列版本时，需要注意以下配置是否有问题：

- 1) 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。
- 2) 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。
- 3) F3171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F3171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。
- 4) F3166及R3166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F3171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。
- 5) 在F3166、R3166及F3169系列版本上配置的TCP Proxy中的受保护IP，升级到F3171系列版本后会存在配置丢失，需要重新配置受保护IP。
- 6) 确认是否配置了双机热备，如果已经配置，则升级到F3171系列版本后“使能会话双机热备功能”的配置会丢失，需要重新使能。

2. HSD17437

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 F1000-E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ICMP报文。

3. 已知芯片缺陷

MAC地址限制：设置的8个端口的MAC地址前43位必须相同。也由于这个原因，如果在用装备命令设置MAC地址时，MAC地址的最低5位大于0b11001时，就会返回设置失败。属于芯片VSC7326限制。

4. HSD17002 (同步问题单序号HSTB01108)

RMON统计限制: 4GE/10GE对于RMON的报文长度分段统计硬件实现的和RFC规范不符合, 所以对于这两种接口不具有RMON统计功能, 属于硬件限制。

5. HSD18777

Web显示限制: Web上所有的配置概览信息最多只能显示5000条, 如果配置超过5000条, 如会话信息等, 都不能在Web上显示完整, 但可以通过过滤功能显示用户所关心的信息。

6. HSD19705

SecPath F1000-E的固定4GE端口和8GE插卡端口在二层模式下时, 若在它上面配置的子接口的编号和子接口本身所属VLAN的ID相同时, 对于广播报文将导致下游交换机发生MAC地址学习迁移, 属于软件实现限制。

7. HSD21006 (同步问题单序号HSTB01443)

将以太网接口工作模式设定为桥模式(二层口)后, 不支持环回检测(loopback)功能。

8. 硬件鉴定

SecPath F1000-E硬件中的USB为预留模块, 目前软件不支持。

9. MAC芯片缺陷

SecPath F1000-E的扩展4GE和8GE插卡因为MAC芯片存在物理缺陷, 不能支持VRRP的虚MAC模式, 如果必须使用扩展插卡实施VRRP业务, 请使用实MAC模式。

10. SSL VPN使用限制

F3171系列版本仅支持SSL VPN IP接入方式, 不支持TCP和Http接入方式。

SSL VPN支持Windows XP、Windows vista 32位操作系统, 浏览器支持IE6.0/7.0/8.0、Firefox3.0/3.5。

五、版本存在问题与规避措施:

1. 问题ID—HSD76879

遗留问题: 链路聚合子接口跨VPN双机组网, 没有流量的情况, 删除聚合口, 设备CPU100%, 命令行操作十分延迟, 不能恢复。

规避措施: 尽量不使用跨VPN的链路聚合功能。

2. 问题ID—HSD96450

遗留问题: 设备长时间处在高温运行状态, 温度告警仅在越过门限值的时候打印一次告警, 不会持续告警。

规避措施: 设备告警一次后可能会持续处于高温状态, 直到设备温度恢复到正常状态。用户需要特别注意设备的温度告警。

3. 问题ID—HSD98186

遗留问题: 无法通过三层子接口将Userlog日志信息发送到IPv6日志主机。

规避措施: 改用物理接口发送, 或者发送到IPv4日志主机。

4. 问题ID—HSD98308

遗留问题: 聚合口上配置的NAT Static地址会导致相同网段的其他地址的ARP学习不成功。

规避措施: 改用物理接口配置。

六、升级时注意事项:

请务必参照《H3C SECPATH1000FE-CMW520-F3171P03 版本使用指导书》、《H3C SECBLADEII-CMW520-F3171P03 版本使用指导书》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 SECPATH1000FE-CMW520-F3171P03 版本说明书》、《H3C SECBLADEII-CMW520-F3171P03 版本说明书》。