[2013-09-17]H3C SECPATH1000FE&SECBLADEII-CMW520-R3177版本发布

金山 2013-09-17 发表

H3C SECPATH1000FE&SECBLADEII-CMW520-R3177版本发布

一、 使用范围及配套说明：

H3C SECPATH1000FE&SECBLADEII-CMW520-R3177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	1.51
目标文件名称	SECPATH1000FE-CMW520-R3177.bin
iMC版本号	iMC PLAT 5.2 (E0401P05)
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	1.51
目标文件名称	SECBLADEII-CMW520-R3177.bin
S5800 配套版本	S5800_5820X-CMW520-R1211P08
S7500E 配套版本	S7500E-CMW520-R6701P01
S9500E配套版本	S9500E-CMW520-R1626P01
S12500配套版本	S12500-CMW520-R1728P02
SR6600配套版本	SR6600-CMW520-R2603P06
SR8800配套版本	SR8800-CMW520-R3351
CR16000配套版本	SR8800-CMW710-R6135P01
iMC版本号	iMC PLAT 5.2 (E0401P05)
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-R3177	硬件特性更新	新增特性：无。 增加单板：无。 删除特性：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. 问题ID—201304220334

问题现象：设备长期运行，出现内存泄漏。

问题产生条件：双机热备非对称组网，并且有大量分片报文经设备转发。

2. 问题ID—201307170414

问题现象：启用IPSec NAT穿越功能后，IKE SA表项中的NAT traversal字段错误的显示为NO。

问题产生条件：IPSec穿越NAT组网，打入流量触发建立IPSec隧道。

3. 问题ID—201304020407

问题现象：设备概率出现异常重启。

问题产生条件：设备上的命令行配置非常多，配置文件大小超过100KB，使用带有正则表达式的查看配置的命令，比如：“display current-configuration | include .*.*.*/.”。

4. 问题ID—201306190471

问题现象：部分NAT444表项没有正常建立。

问题产生条件：在同一个接口上配置2条NAT444规则，每条NAT444规则分别引用了源IP地址相同、目的IP地址不同的ACL规则，然后打入能匹配这2个ACL规则的流量并观察NAT444表项。

5. 问题ID—HSD113119
问题现象：导入配置后会返回错误信息。
问题产生条件：通过web页面的“设备管理”-> “配置管理”->“导入配置”页面导入cfg配置。
6. 问题ID—HSD113967
问题现象：设备硬件内存泄露，无法正常转发。
问题产生条件：DNS FLOOD攻击防范处于丢包时，收到TCP标志位非SYN和不带ACK的异常报文。
7. 问题ID—HSD113532
问题现象：设备发生异常重启。
问题产生条件：采用EasyHacker发送icmp异常报文。
8. 问题ID—HSD113882
问题现象：设备发生异常重启。
问题产生条件：设备开启gtp alg功能，并且在gtp业务下长时间运行。
9. 问题ID—HSD106243
问题现象：如果设备的域间策略配置有数百条以上时，修改域间策略配置可能导致远程桌面连接中断
。
问题产生条件：通过远程桌面登录到设备上进行域间策略配置变更。
10. 问题ID—HSD109417
问题现象：重启后设备上配置的URL主机名配置丢失。
问题产生条件：将内容过滤中的URL主机名全部配置为数字，然后保存配置并重启设备。
11. 问题ID—HSD112739
问题现象：通过Web配置页面无法创建地址池索引为1000及以上的NAT地址池。
问题产生条件：无。
12. 问题ID—HSD112914
问题现象：概率出现部分业务报文出接口错误。
问题产生条件：双机热备非对称路径组网，并长期运行。
13. 问题ID—HSD108763
问题现象：所有通过万兆接口板上的接口打入的流量均被丢弃。
问题产生条件：F1000-E插上万兆接口板，并通过万兆接口板打入流量。
14. 问题ID—HSD113119
问题现象：导入配置后会返回错误信息。
问题产生条件：通过web页面的“设备管理”-> “配置管理”->“导入配置”页面导入cfg配置。
15. 问题ID—HSD110073
问题现象：由于SSL VPN ActiveX控件签名证书未能打上时间戳，导致证书过期后无法继续使用SSL V
PN功能。
问题产生的条件：SSL VPN的ActiveX控件签名证书已过期。
16. 问题ID—HSD113326
问题现象：用Nessus 扫描，设备存在用弱加密的算法恢复SSL 连接的漏洞。
问题产生条件：使能SSL VPN 功能。
17. 问题ID—HSD111103
问题现象：开启会话加速后，QoS功能失效。
问题产生条件：防火墙开启会话加速。
18. 问题ID—HSD111480
问题现象：IKE sa第二阶段协商不成功。
问题产生条件：IPSec绑定VPN多实例，并且IPSec policy中security ACL采用per-host模式。
19. 问题ID—HSD111359
问题现象：长时间后防火墙可能出现异常重启。
问题产生条件：开启防火墙会话日志，并同时打入新建10万以上的业务流量。

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及以上系列版本时，需要注意以下配置是否有问题：
1） 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。
2） 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。
3） 确认是否配置了SYN FLOOD攻击检测，如果已经配置，则升级到F3171及以上系列版本后SYN F
LOOD异常流量检测配置会出现丢失，需要重新配置。
4） 接口上配置nat outbound 中绑定的 address-group地址和接口地址不在同一个网段的情况下，设备不会应答地址池地址的免费arp。需要在接口下配置和地址池地址同一网段的sub地址。

5） 最新版本支持不同vpn实例之间的nat转换，如果从R3166系列版本进行升级，需要调整nat static和nat server的配置。

6） 在F3207、R3206及F3208系列版本上配置的udp flood 检测配置的触发阈值的单位，升级到F3171及以上系列版本后会由原来的连接数每秒变化为报文数每秒。需要根据实际业务进行阈值调整。

7） 在F3207、R3206及F3208系列版本上配置的icmp flood 检测配置的触发阈值的单位，升级到F3171及以上系列版本后会由原来的连接数每秒变化为报文数每秒。需要根据实际业务进行阈值调整。

如果将设备版本从F3171系列版本升级到F3174/R3175及以上系列版本时，需要注意以下配置是否有问题：

1） F3174/R3175系列版本目前不支持“发送会话创建日志”或“发送会话删除日志”两个功能，因此如果从F3171系列版本升级后，会话日志的全局配置中的这两个配置将会丢失。

2） 确认是否使能IPSec双机热备功能，如果使能了，升级到F3174/R3175及以上系列版本时，默认变更为不使能，需要重新配置使能。

2. 在nat outbound的acl中配置 deny ip destination 的rule规则，会影响到alg的正常转换，在有alg的应用中，建议不配置deny ip destination的rule规则。

3. 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/SecBladeII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。

4. 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。

5. SecPath F1000-E/SecBladeII固定4GE端口和SecPath F1000-E 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。

6. 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。

7. 硬件中的USB为预留模块，目前软件不支持。

8. 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。

9. SecPath F1000-E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、32位windows vista操作系统和 32位 windows操作系统，浏览器支持32位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—HSD109369

问题现象：NQA ICMP探测中绑定的VPN实例名称全部自动变为小写。

问题产生条件：配置NQA ICMP探测并绑定名称中包含大写字母的VPN实例。

规避措施：NQA ICMP探测绑定的VPN实例名称全部为小写字母。

2. 问题ID—HSD112168

问题现象：新配置的IPsec/NAT等配置无法同步到备机。

问题产生条件：先创建三层子接口或三层聚合子接口，然后开始双机配置同步功能，再在子接口上配置IPsec/NAT等配置。

规避措施：先开启双机配置同步功能，然后创建三层子接口或三层聚合子接口，再在子接口上进行相关配置。

3. 问题ID—HSD110063

问题现象：物理口接口类型在批量备份下能够备份，但在实时备份下不能备份。

问题产生条件：开启双机配置同步。

规避措施：在双机配置同步情况下，主机上修改物理接口的类型时，需要在备机上手工同步接口类型的配置。

4. 问题ID—HSD100621

问题现象：通过Web管理页面删除的攻击防范配置还存在并可以正常生效。

问题产生条件：通过命令行在安全域上使能攻击防范策略，然后在Web管理页面上删除这部分配置，并重启设备。

规避措施：通过命令行配置的攻击防范配置，如果需要删除也要通过命令行来删除。

5. 问题ID—HSD113033

问题现象：设备概率出现异常重启。

问题产生条件：设备上的命令行配置非常多，配置文件大小超过100KB，使用带有正则表达式的查看配置的命令，比如：“display current-configuration | include .*.*.*/.”。

规避措施：尽量不用正则表达式。如果需要使用，正则表达式中尽量不用或少用匹配任意字符的“*”。

6. 问题ID—TCD003105

问题现象：备用防火墙上的会话出现异常的新建会话或删除会话。

问题产生条件：SecBladeII双机热备组网，HA接口为内部的10GE接口，将内部的10GE接口shutdown并将流量从主用防火墙切换到备用防火墙。

规避措施：不要同时shutdown热备通道及切换主备流量。

7. 问题ID—HSD113409

问题现象：一段时间后，主机设备的双机状态出现异常或异常重启。

问题产生条件：SecBladeII双机热备组网，HA接口为内部的10GE接口，开启Userlog日志功能，并打入200万以上并发会话。

规避措施：在开启了Userlog日志功能并且并发会话达到200万以上时，尽量不要使用内部的10GE作为HA接口。

六、 升级时注意事项：

请务必参照《H3C SECPATH1000FE-CMW520-R3177 版本使用指导书》、《H3C SECBLADEII-CMW520- R3177 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- R3177 版本说明书》、《H3C SECBLADEII-CMW520- R3177 版本说明书》。