版本说明 WAF_2.5

发布概述

发布日期：2020年3月13日

本次发布是一次重大发布，新增重点功能如下：

- 新增支持SG-6000-W7600S/W5600S/W3300S平台，HTTP/HTTPS加解密速度更快。
- 新增支持SG-6000-W1060-GC平台，该平台使用国产自研芯片，且系统严格控制不同管理员的操作权限，保密安全性更高。
- vWAF新增高端平台SG-6000-WV08和SG-6000-WV12，在虚拟化环境中可防护更多数量的站点。
- vWAF支持以HA的部署方式部署在腾讯云和华为云的公有云环境中。
- 新增支持用户会话跟踪策略和IP防护策略；
- 支持对防护站点一键断网/恢复网络且支持通过云端操控，可轻松应对紧急断网需求。
- 另外，对防护策略及规则进行了优化和增强，防护更加全面、易用性更高。

版本发布相关信息：https://fr.hillstonenet.com/show_bug.cgi?id=17934

平台和系统文件

产品型号	系统文件
SG-6000-W7600/W7600S	
SG-6000-W5600/W5600S	
SG-6000-W3300/W3300S	
SG-6000-W1800	SG6000-W-5.5R6-2.5.img
SG-6000-W1600	SG6000-W-5.5R6-2.5-v6.img
SG-6000-W1100	
SG-6000-W800	

产品型号	系统文件
SG-6000-W600 SG-6000-W500	
SG-6000-W1060-GC	SG6000-ZW-5.5R6-2.5.img SG6000-ZW-5.5R6-2.5-v6.img
SG-6000-WV02 SG-6000-WV04 SG-6000-WV08 SG-6000-WV12	SG6000-VW-5.5R6-2.5 SG6000-VW-5.5R6-2.5-v6 （请根据云平台要求选择对应的格式，包括：.img、.ova、.vhd、.qcow2和.vmdk格式。）

新增功能

编号	功能描述
平台	
8806	新增支持SG-6000-W7600S/W5600S/W3300S平台，HTTP/HTTPS加解密速度更快。
14564	新增支持SG-6000-W1060-GC平台，该平台使用国产自研芯片。 SG-6000-W1060-GC平台支持通过系统管理员、安全操作员、安全审计员三种角色管理设备，且每个角色的管理权限各不相同，严格控制不同管理员的操作权限，保密安全性更高。
15751	vWAF新增高端平台SG-6000-WV08和SG-6000-WV12，在虚拟化环境中可防护更多数量的站点。
策略	
9938	支持配置用户会话跟踪策略，可对用户会话信息进行跟踪，并通过日志的方式进行记录。
13974	支持Geo IP防护策略，可限制不同国家/地区的IP对站点的访问。

编号	功能描述
11929	支持通过WAF IP信誉库中的特征规则，对访问站点的IP信誉风险主机进行过滤及防护。可防护的IP信誉类别包括：僵尸主机（Bot）、垃圾邮件（Spam）、Tor节点（Tornode）、失陷主机（Compromised）、代理（Proxy）、扫描（Scanner）、暴力破解（Brute-forcer）、DDos攻击者（DDoS-attacker）。
14405	
12799	优化WAF防护规则的命名及界面显示。
13812	——
14735	对策略模板进行优化，支持宽松、严格、常规及调试4种等级的常用策略模板，同时支持安全策略和访问控制策略的克隆功能。
13929	支持在不同时间段设置不同的访问控制策略，可实现基于精确时间的访问控制防护。
站点	
13743	支持配置站点的IP客户端白名单和URL白名单，命中白名单的请求将跳过其他安全策略的检测，可直接访问站点。
系统	
9937	支持显示Web访问流量（HTTP/HTTPS流量）的统计信息及变化趋势。
12973	支持对防护站点一键断网/恢复网络，可轻松应对紧急断网需求； 支持通过云端操控，实现移动端一键断网/恢复网络。
16911	支持TCP Option传递以及解析客户端真实IP。
vWAF	
15572	vWAF支持部署在Xen服务器上。
12314	vWAF支持以HA的部署方式部署在腾讯云和华为云的公有云环境中（暂不支持阿里云环境）。
16797	vWAF支持订阅方式。
15900	当部署在AWS、华为云、Openstack、阿里云平台上时，vWAF支持通过cloud-init进行密钥认证登录；
13783	当选择共享存储时，vWAF支持断开存储后仍可正常工作。

已解决问题

Bug ID	问题描述
站点	
209439	当开启站点防篡改功能且网站中带有的链接地址顶级域名相同而子域名不同时，若检测到有变动的URL位于不同域名下，可能出现配置冲突，进而出现重启引擎错误的问题。
204065	反向代理或单臂部署模式下，当用户下载较大文件时，若客户端到WAF与WAF到服务器的带宽差异大，可能会出现下载中断或无法下载完整的文件的现象。
209933	当开启站点防篡改功能时，若检测到有变动的URL中包含空格，可能会导致引擎加载失败，进而在设备重启后出现页面不显示拦截信息的情况。
206596	当HTTP头部中包含除“数字”、“字母”、“中下划线”之外的特殊字符时，WAF可能会出现处理错误，进而导致网站无法访问。
日志	
213433	当日志数量非常多时，可能会出现无法正常导出的现象。
系统	
211533	少数情况下，clear led alarm命令可能出现不能清除告警灯的问题。

已知问题

Bug ID	问题描述
部署模式	
154453	反向代理和单臂模式下，当设备管理口的IP、端口与站点IP、端口冲突时，可能会导致管理口无法管理设备。 建议：修改系统页面管理接口的服务端口，或者更换管理口及管理IP。
站点	
149760	开启HTTP代理后，当服务器要求验证客户端证书时，客户端可能会出现“502网关错误”的页面。
177132	开启站点自发现功能后，站点自发现页面的刷新时间为1分钟，若此期间用户正在操作页面，部分操作可能会受到影响。

Bug ID	问题描述
	建议：关闭自发现功能后，再执行页面操作。
184555	当站点引用的安全策略为“policy_debug”时，站点黑名单功能可能会不生效。
接口	
179074	当设备管理口与对端协商不一致时，可能会出现无法通过FTP方式导入image文件的现象。
187846	当同时在设备的两个接口上开启防火墙联动功能，然后又取消一个接口的联动功能时，可能会出现另一个接口的联动功能也不生效的现象。 建议:只在一个tap接口上开启防火墙联动功能。
报表&日志	
176935	DOC格式的报表中目录中暂不支持页码显示，用户可按Ctrl键然后点击目录进行跳转。
扫描	
178053	对于内存较小的产品型号如SG-6000-W500/W600，当配置扫描大型的网站时，可能会由于内存占用率太高而被异常终止的现象。 建议：配置扫描任务时，配置较为精确扫描路径进行扫描。
175660	通过Microsoft Edge浏览器打开PDF格式的扫描报告时，部分文字可能会显示乱码。
vWAF	
197054	vWAF部署在Openstack或Vmware上时，命令行接口界面的中文可能显示为乱码。
190643	vWAF升级到版本2.5时，需要先将设备升级到2.3.8及之后的版本，然后再进行升级，否则可能会导致升级失败。 建议：vWAF版本升级顺序为：WAF2.3.8之前版本->WAF2.3.8及之后版本->WAF2.5
180831	vWAF运行一段时间后，添加第二块硬盘时，之前的配置、日志信息及许可证可能会丢失。
181215	在VMware EXSi 6.0，当使用.vmdk格式的安装包部署vWAF且存在二块硬盘时，若对第一块硬盘进行扩容，可能会出现EXSi报错且vWAF无法正常启动的现象。

Bug ID	问题描述
179825	使用关闭电源的方式重启vWAF多次后，系统可能会出现异常报错信息。
182019	初始安装vWAF时，若配置多个网卡，系统启动后可能会出现接口顺序混乱。 建议：初始安装时先配置一个网卡，启动vWAF后，再根据继续添加其他网卡。
183209	vWAF使用网络磁盘的负载较大时，可能会因磁盘读写速度慢，导致设备出现异常进而自动重启。

浏览器兼容性

以下浏览器通过了WebUI测试，推荐用户使用：

- IE11
- Chrome

获得帮助

Hillstone Web应用防火墙 设备配有以下手册：请访问https://docs.hillstonenet.com进行下载。

- 《Web应用防火墙_WebUI用户手册》
- 《Web应用防火墙_CLI命令行手册》
- 《Web应用防火墙_硬件参考指南》
- 《Web应用防火墙典型配置案例手册》
- 《Web应用防火墙日志信息参考指南》
- 《Web应用防火墙SNMP私有MIB信息参考指南》
- 《vWAF_WebUI用户手册》
- 《vWAF_部署手册》
- 《WAF(W1060-GC)_WebUI用户手册》

- 《WAF(W1060-GC)_硬件参考指南》
- 《WAF(W1060-GC)_扩展模块参考指南》

服务热线：400-828-6655

官方网址：https://www.hillstonenet.com.cn