UNIS W2000-G 系列 Web 应用防火墙

用户 FAQ

目 录

UNIS WEB 应用防火墙 用户 FAQ

本文档介绍 UNIS WEB 应用防火墙产品的用户常见问题及解答

1 硬件类 FAQ

说明

此部分仅适用于硬件类设备。

1.1 设备何时触发硬件BYPASS？

设备在如下情况时，将会触发硬件 BYPASS：

(1) 设备异常掉电情况下，硬件 BYPASS 会触发

(2) 设备重启过程中，硬件 BYPASS 会触发

(3) WAF 上手动强制开启硬件 BYPASS，硬件 BYPASS 会触发

1.2 设备扩展板卡是否支持热插拔？

不支持，当前设备扩展板卡必须在断电情况下进行插拔，否则可能会造成设备硬件损坏。

1.3 电源断电、再上电，中间间隔的时间是否有要求？

电源断电、再上电，建议为：对于 1U 设备，中间间隔 5S 以上；对于 2U 设备，可观察电源旁的指示灯状态，断电后需要等待该指示灯从棕黄色变为完全熄灭后，再进行上电。

如果间隔时间太短，会被电源识别成供电不稳定，可能导致再次上电后启动失败。假如现场瞬间断电后恢复，导致设备出现了开机失败的情况，此时需要将电源线拔掉，按设备后面板上的电源开关按钮 5 次以上（目的是给电源的电容放电）后，重新上电开机。

2 业务功能类 FAQ

2.1 产品上线后，不能用新增的管理地址访问WAF

原因可能如下：

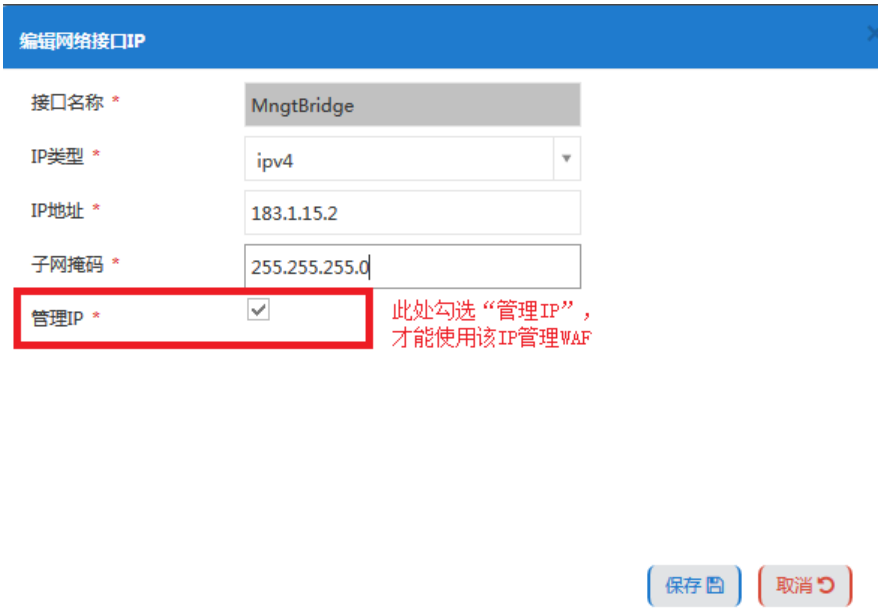
1、网桥下新的 IP 未勾选“管理 IP”

2、远程管理配置有误

对应解决办法：

1、 直连登录设备，查看网络管理>网桥配置，检查管理网桥下新增的 IP 是否已勾选“管理 IP”，需要对新增 IP 勾选“管理 IP”，才能使用该 IP 管理 WAF，如下图示例。

图2-1 配置网络接口 IP 为管理 IP



2、查看系统配置->远程管理配置，默认远程管理地址为：IP 地址：0.0.0.0 子网掩码：0.0.0.0，此处配置的是管理 WAF 的客户端 IP 白名单，请谨慎编辑和删除，否则将导致无法正常访问 WAF 管理端

2.2 产品上线后客户忘记密码，无法登录设备

使用 account 账户登录 WAF 管理端，在系统配置>账户管理>用户管理找到对应的用户，选中对应用户点击“重置”，设置新密码后可重新登录。

2.3 多次登录密码错误导致账号被锁定，如何解封

使用 account 账户登录 WAF 管理端，系统配置>账户管理>用户管理>阻断用户列表，点击对应用户，可进行解封。

2.4 如何查看当前设备的运行状况，硬件信息，cpu信息，内存信息？

使用 admin 账户登录 WAF 管理端，主页面>系统信息，可查看相应的产品型号，系统运行时间，CPU，内存，日志空间等信息。

2.5 配置了syslog服务器后，产品可以向syslog服务器发送哪些信息

可以发送访问日志、攻击日志、DDoS 日志、安全情报日志和流量日志等。

2.6 服务器管理>HTTP/HTTPS服务器配置，防护模式选择“代理模式”时，“客户端IP还原”应该选择“是”还是“否”

透明代理组网时，“客户端 IP 还原”应选择“是”；透明反向代理组网时，“客户端 IP 还原”应选择“否”；反向代理组网时，“客户端 IP 还原”应选择“否”。

2.7 是否支持将防护站点配置为一个网段

当前版本仅在流模式下支持，代理模式下不支持配置网段。

2.8 是否支持防护HTTPS服务器

当前版本仅在透明反向代理模式和反向代理模式下支持防护 HTTPS。

2.9 是否支持接口联动功能

支持，配置方法参考 Web 配置指导。

2.10 是否支持在设备间互相导入配置备份文件

由于备份文件中含有网络配置，因此不支持多设备间互相导入配置，否则会因 ip 冲突导致网络不通。

2.11 为什么触发自定义爬虫防护规则/扫描防护规则时，攻击日志中的目的URL、特征号和规则类型等为空

因为这两种类型的防护原理是通过暗藏陷阱的方式实现，爬虫/扫描工具爬取的链接为暗链接，而非真正的服务器的 url，因此攻击日志中记录的目的 URL、特征号和规则类型等为空。

2.12 HA管理，配置VRRP组后，是否需要点击“应用”按钮

需要，配置 VRRP 组后，需点击“应用”按钮，否则配置不生效。

2.13 HA管理，是否支持配置同步

支持手动同步，不支持自动同步。因此，主机的配置一旦发生改变，需要及时将配置同步到备机，配置同步需要点击“应用”按钮方能生效。

2.14 设备上线后，能正常访问服务器但攻击不被防护，无访问日志及攻击日志

(1) 在 WAF 上抓取业务网桥的数据包，查看到服务器的双向流量（request 包及 response 包）是否都经过 WAF，如果 request 包或 response 包不经过 WAF，WAF 将不能防护

(2) 查看检查服务器管理中配置的服务器信息和部署防护模式是否正确，如果信息填写错误会导致 WAF 不防护

(3) 查看是否配置了 Web 防护策略，如果尚未配置，需要增加 Web 防护策略，并选择待防护的服务器

2.15 设备防护功能正常，但不记录访问日志

应用安全防护>Web 防护策略，查看 Web 防护策略配置中的访问日志是否是“开启”，默认是关闭状态，需要开启才记录访问日志。

2.16 WAF是否支持记录访问控制模块的日志

不支持，匹配访问控制模块的包过滤规则、黑名单、URL 黑名单等被阻断时，在 WAF 上看不到阻断日志。

2.17 WAF是否支持服务器负载均衡功能

负载均衡功能支持负载 http，不支持 https；仅在透明反向代理、反向代理模式下支持。