UNIS W2000-G2 系列 Web 应用防火墙

用户 FAQ

目 录

本文档介绍 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。

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

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。

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 软件类 FAQ

临时授权/正式授权到期后会有什么影响?

临时授权/正式授权到期后，不会影响业务通断性，但是无法使用 WAF 设备功能，直到第二天凌晨 6 点 25 分引擎检查授权过期后不再防护服务器站点，配置不会清除，再次授权时恢复正常使用。

操作系统升级是否会对业务产生影响?

操作系统升级时需要重启，虽说重启过程中有 BYPASS 进行数据透传（对于旁路或者上下行流量不在一对 BYPASS 口下会导致业务中断），但是已经进行的业务会话依然会受到相应的影响，应避免业务高峰期进行设备系统升级操作。

操作系统升级是否会丢失相应配置文件?

操作系统升级后，不会导致配置、日志文件、库文件、license 文件丢失。

3 业务功能类 FAQ

系统升级时采用本地上传升级包的方式，推荐使用什么浏览器？如果本地上传升级包方式失败，如何升级？

本地上传升级包升级时推荐使用 Firefox81+及其以上版本浏览器。若无火狐浏览器，或者火狐浏览器上传升级包失败，可采用命令行 FTP 方式升级。如果客户环境允许，优先推荐使用命令行 FTP 方式升级。

Web防护规则下文件上传检测规则中，真实文件类型显示乱码？

此模块不兼容谷歌浏览器，推荐使用 Firefox81+及其以上版本浏览器。

设备长时间允许，业务网流量较大的情况下，设备会出现主页面请求出错，500错误码，后台登录出错，串口查看内存占用率高，怎么解决？

建议用户关闭访问日志，WAF 的作用是阻断攻击流量。因为访问日志的量较大，数据库写入有极限，因此访问日志现实中默认不开启，也不建议客户开启。若客户现场关闭访问日志之后，仍然较高的内存使用率，则考虑更换性能更好的设备。

恢复出厂操作是否会丢失license？

不会，恢复出厂操作只对配置文件产生影响，不会造成 license 丢失，但会删除原有日志信息和已生成报表。

设备扫描出“SSL证书不可信任”怎么办？

因 WAF 自身证书没有已知公共证书颁发机构的签名，故存在“SSL 证书不可信任”漏洞。

URL黑名单有何限制？

不支持 IPV6。

为何无法打开Web管理界面？

请首先检查 WAF 管理 IP 是否可以 ping 通，再检查网页所输入的地址是否是用 HTTPS 协议，再去 SSH 或串口下使用 bridge –S 查看管理桥下 IsMngtip 是否为 yes，如不是则修改管理地址允许远程管理权限，再使用 remote -S 检查管理 PC 是否在远程管理权限范围下，是否启用 WEB 访问，最后使用 websslport –G 检查 https 管理端口是否使用 443 端口。

基于特征的攻击，如何进行人工误报判断？

在 Web 攻击日志中，打开 HTTP 详细信息，其中有一项分类为匹配特征，可查看到底是哪一部分数据触发了攻击行为，有一点攻防专业技术知识的管理员通过该分类显示内容可进行简单的人工攻击甄别。

WAF部署的网络为隔离网环境，如何更新特征库？

WAF 具备离线升级特征库功能，可通过本地导入的方式手工导入特征库进行升级。

WAF如果设置了Syslog外发，本地还会存储日志么，断电日志会消失么？

本地存储日志是需要在 syslog 配置下需要手动启用本地存储，默认情况下是本地存储是开启的。至于日志存储的位置为硬盘而非内存，所以设备掉电不会丢失日志。

站点是HTTPS协议的，可以防护么？

可以，如果用户的站点为 HTTPS 协议，则通过导入用户保护站点的相关证书和私钥，从而使 WAF 能够进行 HTTPS 协议流量的识别和防护，支持 https 防护的前提是部署模式为代理模式。

为什么部署WAF后，出现了间歇性访问不了的问题？

使用另外一台 PC，登录 WAF，在访问控制下查看动态黑名单中是否有该 PC 的地址，如果客户端对服务器进行攻击，触发封禁动作之后会把攻击源 IP 锁定一段时间，超过锁定时间后会放行，有可能访问行为触发了误拦截并加入到动态黑名单当中。

什么情况下设备会启动软BYPASS？

只要开启过载保护后，当设备超过半数的 cpu 利用率均超过 80%或内存超过 95%，WAF 进入软件 bypass 状态，不再起防护作用。

为什么路由表有时会添加失败。

要确保下一跳是可以 ping 通，路由可达。

WAF反向代理部署时，是否支持 “X-Forwarded-For”功能？

支持该功能。

WAF是否具备抗扫描器扫描功能，如具备，则能防哪些扫描器扫描？

支持抗扫描器扫描，WAF 支持抗扫描器扫描功能，能抗 Appscan、WVS、Nikto、nessus、Hp Webinspect 等业内一流的扫描器扫描。

WAF能记录攻击事件哪些信息？

WAF 能详细记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，Cookie 等所有的请求头内容。

支持哪些告警方式？

WAF 支持 Syslog、手机短信、邮件等多种告警方式。

告警页面是否支持重定向？

WAF 支持告警页面重定向至其它 URL。

CPU、负载、内存、磁盘多少范围内是正常的？

CPU、内存使用率在 80%以下； 磁盘使用率在 80%以下。

VWAF是否支持castools安装呢？

不支持该功能。

VWAF是否支持克隆呢？

不支持该功能。

支持部署模式有哪些？

WAF 支持透明代理、镜像监测、反向代理、路由牵引等多种部署方式，以适应各种环境的需要；同时，支持双机主备模式。不但复杂的网络环境可以适应，针对网上银行、电子商务环境中的 https、CDN、多级代理均能够良好的兼容。从而能广泛的应用于金融、运营商、政府、教育、企业等众多复杂多变的网络环境。

各组网模式下，有何限制？

反向代理部署：

(1) 黑白名单优先遵循 IP 最长匹配原则，匹配长度相同时黑名单优先；

(2) 支持防护 HTTPS 服务器；

(3) 支持 IPV6 功能；

旁路检测/阻断部署：

仅支持 HTTP 协议校验、SQL 注入防护、XSS 防护、命令注入防护、组件漏洞防护、Web 扫描防护、XPATH 注入防护、XML 注入防护、SSI 注入防护、JSON 注入防护、LDAP 注入防护、Webshell 防护、Web 敏感信息防护、数据库信息保护、弱密码检测、CGI 安全防护、跨站请求伪造防护、业务流程控制、DDOS 攻击防护、安全扫描；无法 100%阻断，阻断效果受组网环境影响较大；；

透明代理部署：

普通服务器配置中，客户端 IP 还原必须选择“是”，WAF 网桥上无需配有能跟客户端、服务器通信的 IP；

透明流部署：

规则处理动作不支持重定向；防护效果不如代理模式；

代理模式部署（包括透明代理、透明反代和旁路反代）：

(1) 代理模式下，最大允许 1G 大小的文件进行上传下载；

(2) 代理模式下，敏感信息检测无法对如下字段进行防护：Date、Content-Type、Content-Length、Location、Transfer-Encoding、Connection、Keep-Alive、Vary；

(3) Cookie 加密和 Cookie 加固功能仅代理模式下生效；

负载均衡功能限制如下：

仅在代理模式下支持；

HA管理的使用限制：

(1) VRRP 实例配置主/备状态和优先级时，必须遵循优先级高者为主机的原则配置，否则以优先级高者为实际主机；

(2) 不支持自动同步配置到备机，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；

(3) 仅支持旁路反向代理部署和透明反向代理部署；

(4) 仅支持主备部署；

触发WAF规则的匹配位置在HTTP响应时，有什么限制？

触发 WAF 规则的匹配位置在 HTTP 响应时，WAF 不支持重定向、自定义的错误页面标题、和错误页面内容功能。

配置同步功能有何使用限制？

仅支持在同型号、同版本、相同物理接口的设备间使用；不支持日志、报表、备份文件、端口联动、动态学习的 ARP、防篡改、系统账户、IPV6 地址、BGP 路由牵引、SNAT 回注，域名，管理中心的同步；建议使用管理桥 IP 作为配置同步接口。

黑白名单功能在旁路代理模式下有何限制？

黑白名单功能在旁路代理模式下，黑名单的目的地址应该设置反代地址；白名单目的地址应该设置真实服务器地址。

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>网桥接口，检查管理网桥下新增的 IP 是否已配置为“管理 IP”，需要对新增 IP 配置“管理 IP”，才能使用该 IP 管理 WAF，如下图示例。

图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。

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，在用户管理>账户管理找到对应的用户，选中对应用户点击“重置密码”，设置新密码后可重新登录。若 account 密码忘记，需联系相关技术人员需求支持。

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，用户管理>账户管理>用户管理>封禁列表，点击对应用户，可进行解封。

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，状态监控>系统预览，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。

配置了syslog服务器后，产品可以向syslog服务器发送哪些信息？

可以发送审计日志、攻击日志、DDoS 日志。

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”；旁路反向代理组网时，“客户端 IP 还原”应选择“否”。

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包括透明流模式和旁路镜像模式，代理模式下不支持配置网段。

是否支持防护HTTPS服务器和ipv6防护

当前版本仅在代理模式下支持防护 HTTPS 和 IPV6。

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。

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。

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，配置同步必须同版本同型号且接口配置相同

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，选择待防护的服务器，并开启策略。

设备防护功能正常，但不记录访问日志

基础配置>防护资产，查看防护资产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。

WAF是否支持服务器负载均衡功能

负载均衡功能仅在代理模式下支持。

WAF对文件上传是否有大小限制

流模式下无限制。代理模式下，考虑到设备性能，默认上传文件最大为 1G。

安全态势监测页面为啥看不到HTTPS的地址

态势监测页面不支持 HTTPS 地址的展示。

WAF是否支持对所有HTTP协议字段进行防护

无法对如下字段进行防护：Date、Content-Type、Content-Length、Location、Transfer-Encoding、Connection、Keep-Alive、Vary。

旁路反代模式对代理端口是否有限制？

有的，如下端口不可用作代理端口：22、53、1081、1800、1801、5081、5082、5432、6379、6998、6999、9996、9997、9998、9999、60443。另外，443 不可用于 HTTP 代理端口。

4 常用配置类 FAQ

WAF上线后客户忘记密码，无法登录设备

account 账户忘记密码需要联系技术服务工程师处理。

其余管理员忘记密码可以使用 account 账户登录系统，在用户管理>账户管理找到对应的用户，点击对应用户，重置账户信息，重新输入密码后可重新登录。

WAF上线后，网站访问不了或者部分业务无法正常进行。访问或提交数据时显示404或者链接已重置

排查思路:

第一步，看显示 404 或者链接已重置，查看 WAF 是哪种部署模式。

第二步，查看访问不了的业务 URL。

第三步，查看攻击日志，在攻击日志中查看该 URL 的攻击详情。

第四步，在策略里排除这条规则：

注：建议使用通用规则，积累大，防护效果好，误拦截低。

1、在日志中找到相应的攻击日志，点击排除规则，将 URL 排除。（较常使用）

2、在安全防护，找到相应的模板，将规则的勾选去掉排除这条规则。

WAF串联/旁路部署后网络正常，服务器可访问，但是WAF上无访问日志和攻击日志

排查思路:

1、基础排查：检查 Web 有无（是否配置了防护资产），白名单有无（是否添加了防护白名单），服务器有无（是否添加了代理服务器），防护策略有无（是否忘记添加防护策略），防护策略选择哪一条。

2、查看网络拓扑，看流量怎么走，是否做 nat 以及 WAF 上看到的是哪个 IP。

可能的原因及解决办法：

1、服务器地址填写错误导致，更改正确的地址即可。

2、部署模式选错可能导致，更改部署模式即可。

3、服务器的端口填写错误，一般为 80 端口，某些服务器是 8080 端口或其它端口，可询问客户。

4、未开启防护策，增加防护策略选择对应的服务器即可。

5、开启了策略但是未开启访问日志，开启访问日志即可。

CLI命令行升级方式

1、搭建 ftp 服务器升级

2、登录后台用户名：admin 密码：WAF 命令行密码与登录界面密码相同。

使用命令：upgradeapp/upgradepatch FTP 用户名 FTP 密码 FTP 文件地址

命令：upgradeapp ftp://用户名:密码@本地 ip/xxxxx.img(升级包的名称)

注：upgradeapp 用于升级版本，upgradepatch 用于升级特征库及补丁包等。

WAF启用策略之后网站无法打开，服务器处策略停用后恢复正常。

此问题多为路由不通导致，WAF 使用的代理机制决定了必须保证 WAF 能与服务器通信同时将代理的数据包回指到正确的网关地址。问题出现一般存在下列几种情况：

1、WAF 配置的网关不对，或者没有设置路由，导致启用代理防护之后，服务器返回的数据包无法回到正确的网关，导致页面访问不正常。

2、WAF 和服务器之间链路上不通，启用防护之后无法访问到网页。

防护的服务器在不同网段时，一条默认路由可能无法解决问题，需要增加多条静态路由。

部署WAF后访问网站导致网站出现500错误

1、如果 WAF 使用的是反向代理模式，请排查路由问题，是否 WAF 到服务器不可达。

2、如果 WAF 使用的是透明代理模式，请将模式改成流模式。建议客户使用流模式。

抓包分析

抓包分析主要应用于以下几个场景：

1、给网站加防护策略后，无攻击、访问日志，攻击无防护，检查所有配置无误的场景。

2、无法确认防护策略是否与服务器 IP、端口匹配。

3、确认流量是否经过 WAF，排查是否有多链路情况、Trunk，或数据未流经 WAF。

4、启用网站之后，网站访问不了（多为路由问题）。

5、其它异常情况抓包命令：

tcpdump

tcpdump usage:

tcpdump [ip arp rarp] -i/--interface [-c/--count host/--ip]

tcpdump [tcp udp] -i/--interface [-c/--count port/--port]

tcpdump [icmp] -i/--interface [-c/--count]

例：

a、如何抓取 GE0/0 上的数据包

tcpdump ip -i GE0/0

b、如何抓取 ICMP 的数据包

tcpdump icmp -i GE0/0 -c 20

c、如何抓取 TCP 端口 80 的数据包

tcpdump tcp -i GE0/0 port 80

d、如何抓取 host 1.1.1.1 的报文

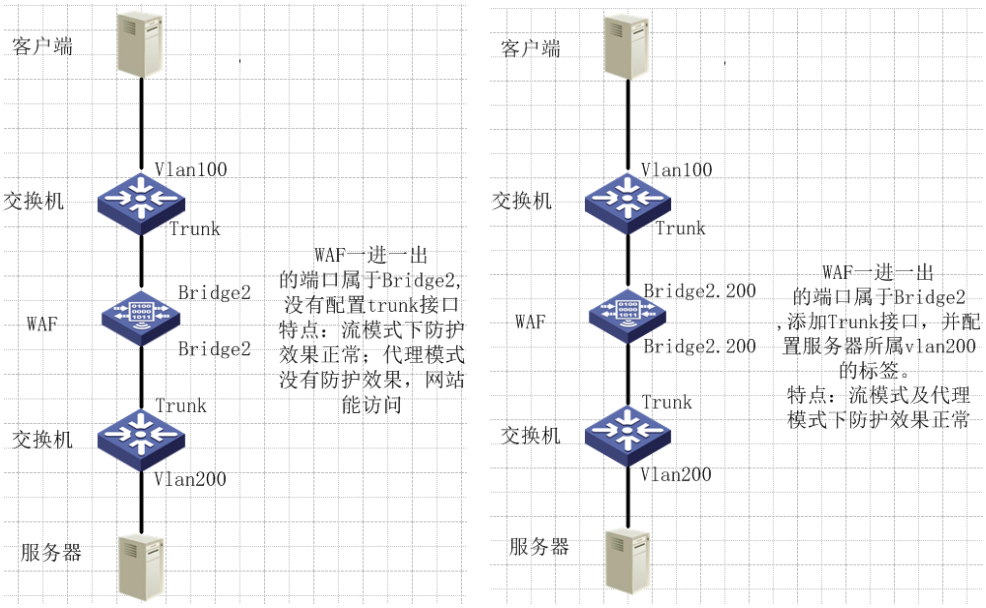
tcpdump ip -i GE0/0 host 1.1.1.1

正式license和临时license区别

正式 license 和临时 license 的主要区别是，临时 license 有时间限制，而正式 license 没有时间限制，临时 license 过期后，所有安全功能将失效，仅仅只有转发数据包的功能，并且管理中心不能再使用，shell 的命令行也不能使用。

WAF部署在两台trunk模式交换机之间的注意事项

图2 示意图



注意：正常情况下来说，WAF 部署在两台 trunk 模式交换机之间，不配置 trunk 标签的话，所有流量都可以正常通过；但是个别环境中，可能会出现访问服务器的时候时断时续，或者根本不通，这种情况则必须加上防护服务器对应的标签。

WAF流模式部署时，出现网站无法访问的问题，绕过WAF就正常

排查思路：排查此类问题，可从二层入手，通过抓包分析，分析过程如下

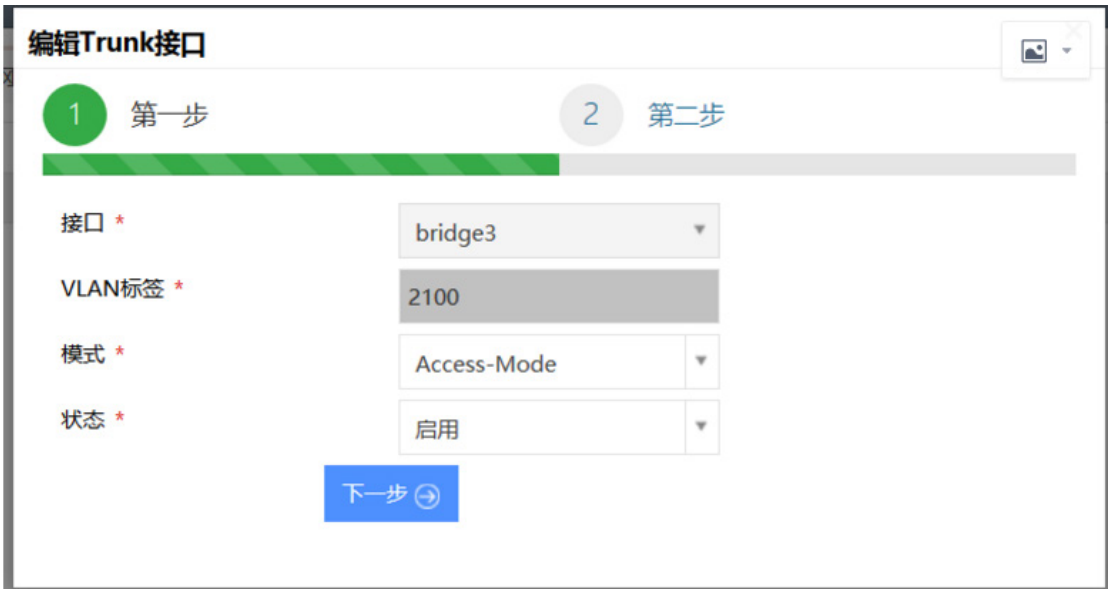
1、查看服务器 MAC

图3 示意图

```
16:35:39.368527 00:15:5d:fd:05:03 > 00:1a:a9:15:c0:70, ethertype IPv4 (0x0800), length 2934: 192.168.254.61.80 > 125.33.195.82.56535: . 25921:28801(2880) ack 409 win 54
16:35:39.370539 00:1a:a9:15:c0:70 > 00:15:5d:fd:05:03, ethertype IPv4 (0x0800), length 60: 125.33.195.82.56537 > 192.168.254.61.80: . ack 477 win 256
16:35:39.372203 00:1a:a9:15:c0:70 > 00:15:5d:fd:05:03, ethertype IPv4 (0x0800), length 60: 125.33.195.82.56535 > 192.168.254.61.80: . ack 19905 win 258
16:35:39.372214 00:1a:a9:15:c0:70 > 00:15:5d:fd:05:03, ethertype IPv4 (0x0800), length 60: 125.33.195.82.56537 > 192.168.254.61.80: F 364:364(0) ack 477 win 256
16:35:39.372708 00:15:5d:fd:05:03 > 00:1a:a9:15:c0:70, ethertype IPv4 (0x0800), length 2934: 192.168.254.61.80 > 125.33.195.82.56535: . 28801:31681(2880) ack 409 win 54
16:35:39.372758 00:15:5d:fd:05:03 > 00:1a:a9:15:c0:70, ethertype IPv4 (0x0800), length 54: 192.168.254.61.80 > 125.33.195.82.56537: . ack 365 win 54
16:35:39.372762 00:15:5d:fd:05:03 > 00:1a:a9:15:c0:70, ethertype IPv4 (0x0800), length 1494: 192.168.254.61.80 > 125.33.195.82.56535: . 31681:33121(1440) ack 409 win 54
^C
275 packets captured
328 packets received by filter
0 packets dropped by kernel
netentsecOS:~# tcpdump -nei eth4 host 125.33.195.82
```

2、实例：抓包分析了，WAF 的 eth4（靠近 client 端），是有关于此 MAC 的流量；WAF 的接口 eth5（靠近 sever 端）没有关于此 MAC 的流量，最后查看是因为 WAF 处在两个 trunk 环境之间，WAF 在做数据处理时，只根据 IP+Mac 来转发数据，不会带上 vlan 的信息，环境比较特殊，但是没有打标签，打上标签后环境正常。

图4 示意图



WAF部署之后，策略配置正常，但是没有访问日志及攻击日志

WAF 防护的前提是保证 WAF 看到的流量为关于服务器的双向流量（request 包及 response 包），抓上下联接口及网桥接口的数据包，查看客户业务流量是否经过 WAF 及流量是否均为双向。

配置了syslog服务器后，WAF可以向syslog服务器发送哪些信息

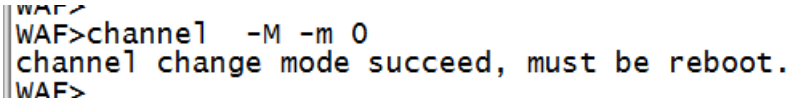
详细信息如下：

图5 Syslog 配置图

如何修改WAF channel模式及模式说明

按照如下方式修改 channel 模式，取值范围是 0-6

图6 示意图



注：改完之后需要重启设备才能生效。

七种 bond 模式说明：

第一种模式：mod=0，即：(balance-rr) Round-robin policy（平衡抡循环策略）

第二种模式：mod=1，即： (active-backup) Active-backup policy（主-备份策略）

第三种模式：mod=2，即：(balance-xor) XOR policy（平衡策略）

第四种模式：mod=3，即：broadcast（广播策略）

第五种模式：mod=4，即：(802.3ad) IEEE 802.3adDynamic link aggregation（IEEE 802.3ad 动态链接聚合）

第六种模式：mod=5，即：(balance-tlb) Adaptive transmit load balancing（适配器传输负载均衡）

第七种模式：mod=6，即：(balance-alb) Adaptive load balancing（适配器适应性负载均衡）

Channel口的端口联动

Channel口的端口联动，判断的是Channel口里面包含的真实物理口的down、up状态，并非Channel口本身的状态

Trunk两种接口模式

Port-mode：WAF 在做数据处理时，只根据 IP+Mac 来转发数据，不会带上 vlan 的信息。

Access-mode：WAF 在做数据处理时，会同时使用 IP+Mac+vlan 信息进行转发，一般默认情况下 trunk 模式下选择 access-mode。

WAF如何开启日志，但是没有防护效果。

在应用安全防护下的 web 防护策略，调用策略的时候选为监控规则，就可以在不对客户实际的业务环境造成影响的前提下，看到相应的日志了。

邮件告警接收异常

解决办法：

1、检查邮箱是否已满，是否将告警邮箱标记为垃圾邮件。

2、检查邮箱名称或手机号是否填写正确。

3、发送测试邮件，看是否能收到。

授权导入时报错，提示授权文件无效。

1、确认核实授权文件的有效性。

2、检查授权文件名是否正确，授权文件名中不能包含中文符号，如中文括号等。

设备部署在channel环境中时，channel接口协商不起来。

1、进行 channel 部署时，先确认客户 channel 环境是静态还是动态，如果是动态，在 WAF 后台执行 channel -M -m 4 命令，并重启设备；

2、如果是静态则保持 WAF 模式不变即可；

3、其它模式参考“如何修改 WAF channel 模式及模式说明”

日志记录机制

存储 200W，显示最近的 10W，超过存储上限，会进行覆盖。

设备关于X-Forwarded-For IP与数据包源IP优先级处理顺序。

1、网络层黑白名单，优先处理 XFF IP。

2、如果处理动作是封禁，优先封禁 XFF IP。