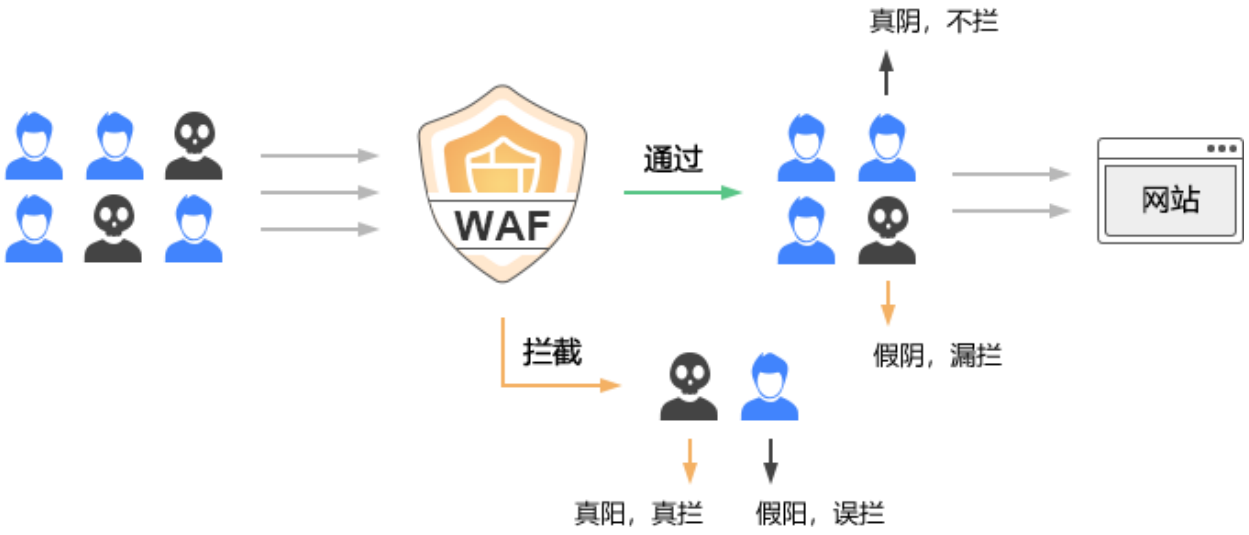
一文讲清四个很烧脑的 WAF 名词

Gartner 在 2012 年预测 2024 年 70%的组织会选用 WAF 服务，看来这个预测还是比较准的。WAF(Web 应用防火墙)已经成为一个网站安全必须品，不仅是为了等保合规需要，而是为了保障网站系统的可靠运行。用户可选购 WAF 硬件设备或者选购云 WAF 服务，都可以实现 WAF 防护。但是，用户被市场上的琳琅满目的 WAF 设备和 WAF 云服务的各种防护指标搞得不知如何选择产品了，本文就讲清楚四个很烧脑的 WAF 名词：真阴、假阴、真阳、假阳，并实例讲解这些名词在 WAF 防护中的实际含义和意义。

一、 什么是真阴、假阴、真阳、假阳？

这 4 个名词是英文 True Negative(真阴), False Negative(假阴), True Positive(真阳), False Positive(假阳)的直译，很绕口，但是真正想用 WAF 的用户还绕不过去。WAF 的工作原理是放行正常流量，拦截攻击流量，有些厂商也称之为流量清洗。如下图所示：蓝色用户是正常访问网站的用户，黑色用户是试图攻击网站的用户，这些用户流量混在一起访问网站，通过 WAF 时，WAF 必须能正确识别出正常的流量而放行，这就是**真阴**流量，不拦截。而如果 WAF 未能识别出攻击流量同样放行了，这就是**假阴**流量，属于漏拦，说明 WAF 的检测能力有问题。而如果 WAF 真的成功拦截了攻击流量，这是**真阳**流量，真的被拦截，说明 WAF 真正有能力拦截真的攻击流量。但是，如果 WAF 拦截了正常流量，这是**假阳**流量，就属于错误拦截，这说明 WAF 的识别能力是有问题的。



也许还有读者还是对这 4 个名词有点糊涂了，笔者想到刚刚过去的疫情，很多人都“阳”过，对比一下就应该更加清晰了。如果你一切正常，没有任何“阳”的迹象，排队去做检测，结果是阴，这就是**真阴**，有绿码，可以正常上班，任何地方都不拦截你。但是，如果你是真的“阳”了，但检测结果仍然是阴，这就是**假阴**，你仍然可以不受阻拦地去上班，这说明检测系统出问题了，这非常危险。而如果你是真的“阳”了，检测时真的检测出来了，你**真阳**了，那说明检测系统很管用，你就要居家隔离或要去隔离治疗，各种出行被拦截。但是，如果你没有阳，但检测结果说你阳了，那就很惨，这是**假阳**，但会被错误地拦截出行和隔离治疗。

可以看出：最坏的情况是假阴，没有拦截应该拦截的恶意攻击流量。次坏的情况是假阳，错误地拦截了正常流量，让正常流量不能正常访问网站。这两种情况都是衡量一个 WAF 检测能力和识别能力的重要指标，最理想的指标当然是 100%没有假阴的情况和 100%没有假阳的情况。

二、 解读零信网关 WAF 内置 WAF 模块的 WAFER 检测报告

理解了以上 WAF 的 4 个重要名词，就应该不能理解零信网关内置 WAF 模块的 WAFER 检测报告了。有读者朋友在阅读文章《零信网关特色之三：超值-WAF 防护》时留言说不知道文章中的 WAFER 测试报告中有些内容是什么意思，本文就详细解释一下。如下图所示，这是同一个网站今天检测的结果，比较 3 月 11 日上文的检测结果，真阳率已经从 85.71%提升到 97.34%，检测能力已经从 B 级提升到 A 级，这说明零信网关的 WAF 防护性能在不断提升中。

第一行是 True Positives (真阳)，测试过程共发起了 413 次真正的攻击，检测到 402 次，真阳识别率高达 97.34%，检测能力为 A 级。第二行是 False Positives (假阳)，测试过程共发起了 72 次假阳攻击，没有误拦截(0)，所以识别能力为 A 级。从检测指标可以看出零信网关具有非常好的 WAF 防护性能。

WAFER Report 2024.05.29

Type	Total Requests	Detected	Error	%
True Positives	413	402	0	97.34%
False Positives	72	0	0	0%

Performance Scores

Detection Ability	Distinguishing Ability
A	A

我们再来看看具体各种攻击类型的检测和拦截情况。SQL 注入(SQL Injection)共发起了 128 次攻击，拦截了 126 次，这就是真阳真拦；还有 2 次是假阴，也就是漏拦，拦截率为 98.44%。对于跨站脚本攻击(Cross Site Scripting)，共发起了 149 次攻击，拦截了 147 次，这就是真阳真拦；还有 2 次是假阴，也就是漏拦，拦截率为 98.66%。对于命令注入攻击(Command Injection)，共发起了 41 次攻击，拦截了 37 次，这就是真阳真拦；还有 4 次是假阴，也就是漏拦，拦截率为 90.24%。对于服务器端包含注入攻击(SSI Injection)，共发起了 24 次攻击，拦截了 24 次，这就是真阳真拦；没有假阴漏拦，拦截率为 100%。其他拦截指标就不一一分析了，对于没有拦截的攻击，需要网关的 WAF 模块能不断完善 WAF 防护规则，并定期更新防护规则。当然也需要用户平时注意分析 WAF 日志，不断根据攻击情况来自定义防护规则。

Attack Type	Total	True Positives	False Negatives	True Positive Rate
SQL Injection	128	126	2	98.44%
Cross Site Scripting	149	147	2	98.66%
Command Injection	41	37	4	90.24%
SSI Injection	24	24	0	100%
File Upload	29	29	0	100%
Directory Traversal	20	17	3	85%
Buffer Overflow	10	10	0	100%
LFI (Local File Inclusion)	10	10	0	100%
RFI (Remote File Inclusion)	2	2	0	100%

为了让读者朋友直观地感受一下没有 WAF 防护的网站和有 WAF 防护的网站有什么不同，笔者同时使用 WAFER 测试了一个没有 WAF 防护的网站，测试结果如下图所示。对应上面有 WAF 防护的检测结果可以看出：SQL 注入攻击、跨站脚本攻击、命令注入攻击和服务器端包含注入攻击等四种攻击的拦截率为 0%，也就是说各种攻击都成功实施，大家可以想象一下这是什么后果，这就是网站必须有 WAF 防护的原因。

Attack Type	Total	True Positives	False Negatives	True Positive Rate
SQL Injection	128	0	128	0%
Cross Site Scripting	149	0	149	0%
Command Injection	41	0	41	0%
SSI Injection	24	0	24	0%

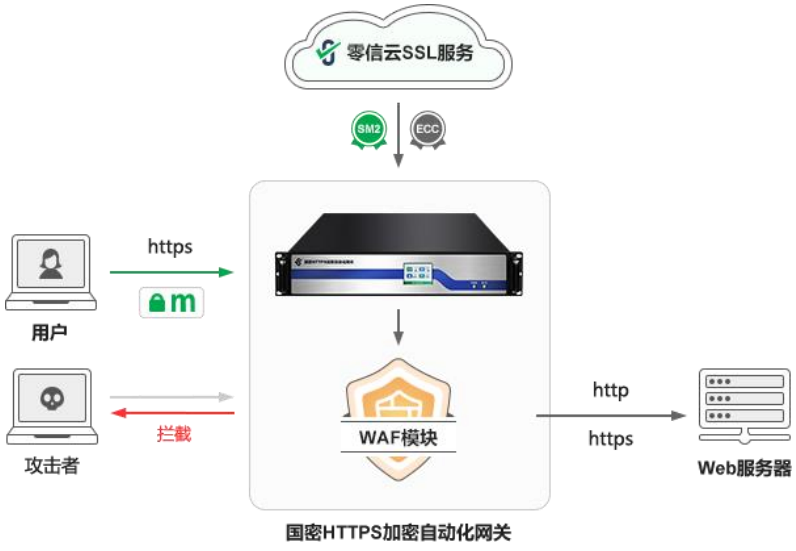
三、 扩展阅读：WAF 设备或云 WAF 服务必须支持 SSL 证书自动化管理

相信读者朋友通过第一部分的内容能真正搞懂“真阴”(True Negative)、“假阴”(False Negative)、“真阳”(True Positive)、“假阳”(False Positive)这四个很难弄清楚的四个名词，因为我们在疫情期间都是“阳”过和“阴”过的过来人。而通过实际解读零信网关的 WAF 性能测试数据，应该可以进一步理解这四个名词，理解为何笔者把这四个名词同实际拦截结果绑定在一起的定义：真阴-不拦、假阴-漏拦、真阳-真拦、假阳-误拦。

本部分为扩展阅读内容，简单讲解一下 WAF 设备或 WAF 云服务必须支持 SSL 证书自动化管理。

大家都知道，网站都必须实现 HTTPS 加密来保障数据的传输通道安全，而 WAF 防护，必须能读取明文流量数据才能分析是否是攻击流量，这就是要求 WAF 必须支持 HTTPS 加密和卸载。传统的方式是用户必须向 CA 申请 SSL 证书，部署到 WAF 设备上使用，才能启用 WAF 防护，这个证书申请和部署配置过程有点痛苦，特别是要大量的网站都需要防护的应用场景。同时，为了满足用户的商密合规要求，WAF 设备和云 WAF 服务都必须支持商密 SSL 证书实现商密 HTTPS 加密。

零信技术的创新解决方案可供借鉴，由零信网关，也可以是第三方 WAF 设备或 WAF 云服务，自动化对接零信云 SSL 服务系统，自动化为需要 WAF 防护的网站配置双算法双 SSL 证书，实现自适应算法的 HTTPS 加密卸载后交给 WAF 模块分析流量而实现 WAF 防护，让正常的流量转给 Web 服务器处理业务，而拦截攻击流量。零信网关支持自动化免费为多达 255 个网站 5 年配置双 SSL 证书(商密 OV SSL 证书+国际 DV SSL 证书)，让用户原 Web 服务器零改造实现商密 HTTPS 加密，同时兼容 RSA 算法 HTTPS 加密，实现 5 年安全无忧，用 HTTPS 加 WAF 双重保障业务数据安全。



也就是说：零信国密 HTTPS 加密自动化网关完美地把 HTTPS 加密自动化和 WAF 防护自动化二者合二为一，让用户一举两得，同时满足了等保合规和密保合规的应用需求，这就是零信网关的创新之处，也是最超值之处。零信网关可以理解为是一个能自动化实现商密 HTTPS 加密的 WAF 设备，能同时满足用户需要 WAF 防护和商密 HTTPS 加密改造的应用需求，欢迎选用。

有诗为证：

真阴真不拦，放行。
假阴不漏拦，拦截。
真阳必真拦，正确。
假阳不误拦，厉害。

王高华

2024 年 5 月 29 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 167 篇(共 45 万 2 千多字)和英文 68 篇(8 万 4 千多单词)。。