一体式 WEB 反向代理服务器设计与实施

反向代理作为 web 访问入口，管控所有 web 流量，承担保护壳的功能，其性能，可靠性，以及安全性不可无视。

目标（实际生产环境受限于各种因素，需要评估是否真正实现）

1. 快速 性能衡量方法包括请求延迟，业务请求到达反向代理然后离开反向代理，去往后端服务器，更高的并发处理量，吞吐量
2. 稳定可靠 长时间运行不会崩溃死机，即使遇上故障，也要易于排查恢复
3. 高可用 双机热备，自动检测与切换
4. 安全可控 保障业务访问正常持续，清理掉业务无关流量，尽可能少的到达后端服务器，尽可能少出现预期之外的异常行为，完全采用被动防御技术，收到攻击时丢弃攻击流量请求，不允许将攻击流量引到其他 IP，不允许反击报复攻击者，遭遇无法抵御的攻击时死掉停止业务访问，攻击停止恢复业务。
5. 法律合规要求 符合相关法律要求，符合安全等保要求。
6. 性能容量设计 不仅仅是满足日常业务需求，更需要具备能力应付 DDOS 超限攻击，简而言之机房出口瘫痪，反向代理以及后端服务器依旧可以存活。
7. 易于维护，尽可能减少维护工作量直至实现免维护
8. 设备成本控制：核心业务普通廉价 1U 机架式服务器，非关键业务虚拟机/私有云。
9. 总效费比高：在实现防御目标的前提下，付出的资金、人力、服务器资源、网络带宽等各种开销成本，远比攻击者要小。

方案与实施

1. 系统选择 HardenedBSD 可以隐藏内部真实的服务器信息，从外部用户的角度看服务器，是 HardenedBSD，安全加固的专业 unix 系统，这并不影响正常业务访问，对攻击者却具有较大的威慑力。
2. 系统内核参数调整与配置调优略。
3. 高可用软件 heartbeat ，提供业务虚拟 IP，故障检测与自动恢复。
4. 防火墙 pf（packet filter）pf 高效能的防火墙软件，完全支持 SMP。
   防火墙规则描述
   外网网卡只开放 tcp80 和 443 端口，完全禁止 udp 流量，ssh 管理，dns 解析，时间同步等辅助流量走内网。
   开启 synproxy 对付 synflood
   限制每个 ip 的并发数 100 个
   限制每个 ip 的连接频率 40 次每 5 秒，超过限制封锁 ip 10 分钟
   支持 IP 黑名单与白名单
5. 反向代理软件 nginx，结合内核 accept filter 大幅度提高 http 连接处理效率，只有真正的 http 协议请求存在才会使用 nginx 处理，确保针对网络和系统底层的攻击完全由内核高效处理，静态与资源文件缓存，其他详细配置见 nginx.conf
6. WAF 防火墙模块 modsecurity 功能强大的 web 应用防火墙，也是 waf 开创者，

ModSecurity 是一个免费、开源的 Web（apache、nginx、IIS）模块，可以充当 Web 应用防火墙（WAF）。ModSecurity 是一个入侵探测与阻止的引擎，它主要是用于 Web 应用程

序所以也可以叫做 Web 应用程序防火墙.ModSecurity 的目的是为增强 Web 应用程序的安全性和保护 Web 应用程序避免遭受来自已知与未知的攻击

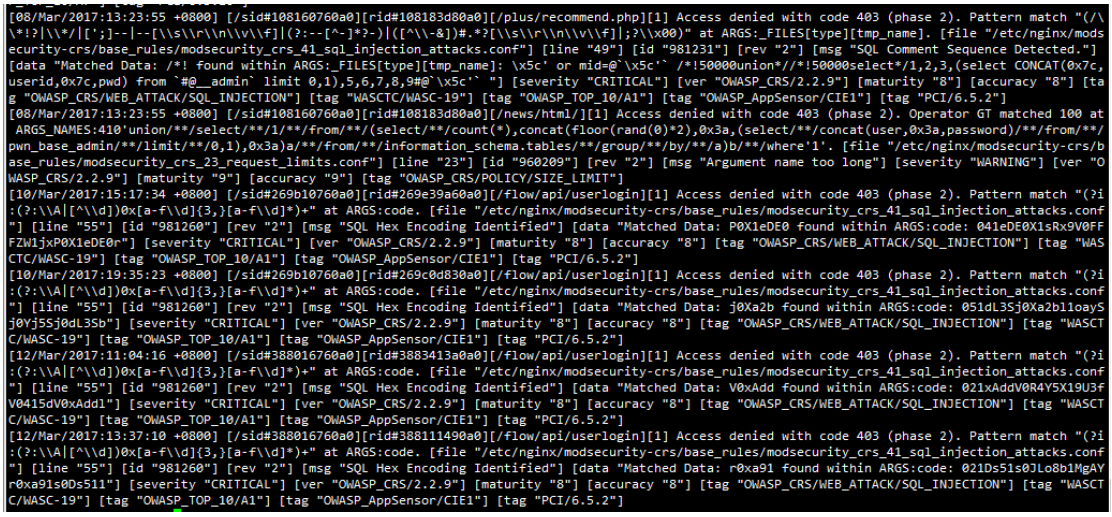
支持 https 加密流量过滤，最新版 3.0 支持 http2，引擎过滤规则和阻断机制与其他高级程序不同，对付扫描器以及 DOS 攻击更加高效。
waf 规则库简介：

OWASP 是一个安全社区，开发和维护着一套免费的应用程序保护规则，这就是所谓 OWASP 的 ModSecurity 的核心规则集（即 CRS）。ModSecurity 之所以强大就在于 OWASP 提供的规则，可以根据自己的需求选择不同的规则，当然 ModSecurity 还有商用的规则

关于 modsecurity 详细描述，参见底部链接

实际结果与数据反馈

生产环境防御效果展示，以 SQL 注入为例



4 天的时间里，总共遭受 6 次无效的攻击，相对于之前每天数千次的扫描，减少了 99.9%以上，web 后端代码即使有 sql 注入漏洞，也不受影响。

附：

1. 为何不用 Linux？
   HardenedBSD 内核特性更加安全高效，并且不为国内以及全球攻击者熟知，在安全攻防对抗中，这将对防守方更加有利。
2. 为何不用 lvs，haproxy，squid，varnish，apache traffic server？
   所有 web 流量最终都要经过 Modsecurity 过滤，以上各软件都不支持，另外从单个软件的角度考虑会有性能更佳的选择，但是从多个软件组合的整体而言，增加额外一层处理与转发会增加全局复杂度、降低系统的全局性能。
3. 为何不用 nginx-naxsi，nginx-lua，或者其他 waf？
   要么功能太弱，需要二次开发，要么收费商业版，modsecurity 在 10 多年的大规模实际使用中表现优异，开源免费并且有强大的规则集，并且可以自主审计、设计规则。

参考

https://hardenedbsd.org/
http://www.modsecurity.org/

https://github.com/SpiderLabs/ModSecurity
https://github.com/SpiderLabs/owasp-modsecurity-crs
https://www.trustwave.com/Resources/SpiderLabs-Blog/ModSecurity-Performance-Recommendations/