网络应用的保护

入侵防护系统（IPS）VS 梭子鱼 Web 应用防火墙

不可否认，IPS 设备和梭子鱼 web 应用防火墙存在共性，但是很大程度上，他们是为不同的需求所开发的完全不同的技术。如同梭子鱼，IPS 设备是部署在网络中并且对经过系统的所有数据包应用策略。他们一般是为了辅助边界防火墙。在 IPS 业界领先的几大厂商也使用了如同梭子鱼一样基于 ASIC 的设计。

一个 IPS 系统提供了常规网络 IDS 系统的功能，并且能够阻断网络流量。所有的流量都必须流经 IPS 系统。不同于普通防火墙，IPS 会通过将数据包和数据库中攻击指纹的比较来判断是否为恶意攻击。如果一个包匹配了某个指纹，相应的动作可以是放行，丢弃或者记录。管理员一般会使用 IPS 设备来监控和管理网络。IPS 的部署对于已经拥有 IDS 系统的网络来说，也是得心应手的，可以做补充的作用。因为 IPS 本身是网络 IDS 系统的升级。

IPS 和梭子鱼的区别

IPS 设备一般而言是基于指纹识别的安全系统。拒绝攻击策略是基于广为人知的攻击类型指纹而建立的，这些攻击类型包含了很大一部分的协议，包括 TCP, IP, SMTP, SNMP, SIP, HTTP, Netbios, Apache, IIS, ASP, NT, Linux, Citrix 等等。

虽然 IPS 的保护覆盖了很大的范围，但是 IPS 在 web 应用保护方面还是相对比较弱势。IPS 不会对包括跨站点脚本攻击，暴力浏览，SQL 注入，命令注入，cookie 密码窃取，URL 编码攻击，unicode 攻击，cookie 篡改，日志篡改等一系列攻击作出任何响应。指纹对这类攻击是无能为力的，同时也不可能有相应的指纹存在。如果需要保护的对象是一个至关重要的 web 应用，那么 IPS 将无用武之地。

IPS 最明显的缺陷在于它不能终止和处理 SSL 流量。目前比较重要的应用都是通过 SSL 进行加密处理的。IPS 无法深入 SSL 加密的内容，也就无法阻挡攻击。

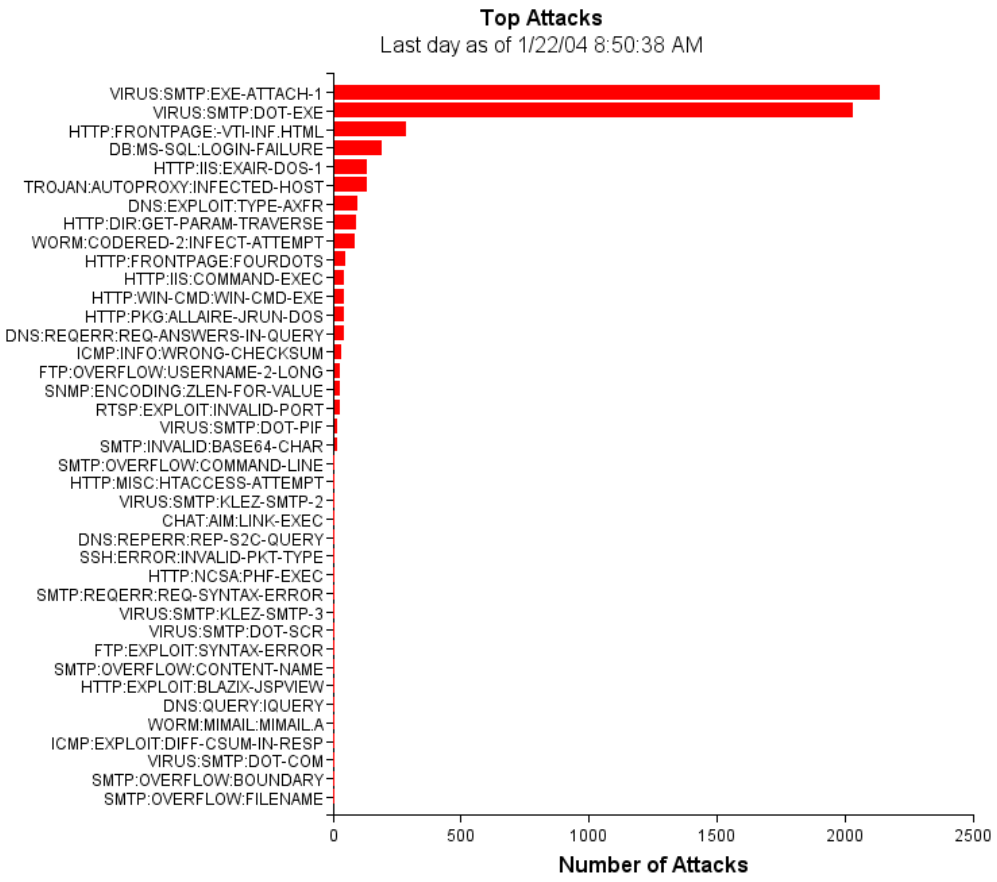
正确的保护 web 应用来阻挡现代化的攻击手段，需要拥有能够深入分析应用层包内容的能力。包括能够检查恶意命令，非法关键字，隐藏字段篡改，参数篡改，被修改的 HTTP 方法，最大长度排除以及非法 URL，然后重定向，丢弃或者记录攻击连接。

IPS 系统的定义

一个 IPS 设备，作为安全设备的一种，通常具有如下特征：

- 通常从被动的 IDS 技术进化而来。
- 基于特征的
- 针对典型攻击技术的报警和阻断
- 使用“允许除非明确否认”模式
- 目的是保护广泛的一段网络协议和环境，而不是侧重保护 web 应用

IPS 技术使用模式匹配引擎，以寻找具体的签名，表明攻击。首要的作用是一个综合方案，是它挡住了众所皆知的企业级攻击，如：电子邮件病毒，蠕虫，telnet 的攻击，网站服务器攻击，以及其他攻击。第二个作用是分类报表，例如你可以了解有多少尼姆达攻击被阻断。IPS 对攻击的分类统计，如下：



IPS 不能进行报警和阻断针对某个 web 应用的攻击。没有特殊的特征，IPS 不知道什么是恶意的，并且这些特征只存在于通用的技术和应用（如：微软 IIS 的 bug，Code Red II 蠕虫等。）。例如，IPS 没有基于 PeopleSoft 的特征，将不会保护基于 PeopleSoft 的应用。

本质上说，IPS 是被动的方式。 IPS 厂家推销此为"非侵入性" 。事实上，一个针对已知攻击和技术的 IPS 警报，你可能需要不断的打补丁。

总结

如果你想依靠一种网络 IPS 解决方案来保护关键应用的 web 应用，在这里有几个方面，你应该再考虑下：

1. IPS 使用包含已知特征的特征数据库作为检测机制，只能捕获已知攻击。针对某种特殊应用设计的攻击，将不能防御。IPS 系统并不能防御时下流行的攻击：命令注入攻击合理 SQL 注入攻击。

2. 黑客只需做少许修改，现有的特征将不起作用。

3. SSL 加密使 IPS 设备对所有的 web 攻击失效。

4. IPS 不能对 URL 和 Unicode 编码流量规范化。被攻击者隐藏良好的普通攻击，IPS 也将失去作用。

5. 基于“允许除非明确否认”的模式对所有流量放行，除非明确告知哪些是恶意的流量。但是当遇到 IPS 不能判断是否恶意的流量时该怎么办呢？

6. IPS 只知道包和请求，而不知道网络和应用。IPS 不知道用户特定的网络和应用架构。复杂的特征需要根据用户特定的应用环境来单独制定。制定出符合用户实际应用环境的特征所需的工具，IPS 并没有开放给用户。

7. 典型 IPS 产品通常是商用平台，并不能保持数据，特别是当数据包用来识别是否为攻击时，该数据包可能已经被拆分掉了。

相比之下， 建议使用 Barracuda 解决方案，目的是保护 web 应用，提供一种保护后台包含敏感信息的关键应用。Barracuda 可防止所有的常见的应用攻击，包括攻击应用平台（操作系统和 web 服务器）和用户自己的应用（定制代码和数据库） 。Barracuda 考察每个来袭涉嫌恶意指令，非法关键词，隐藏字段篡改，参数篡改，更改的 http 方式，最大长度例外，非法 URL 来有效地阻止攻击的应用。