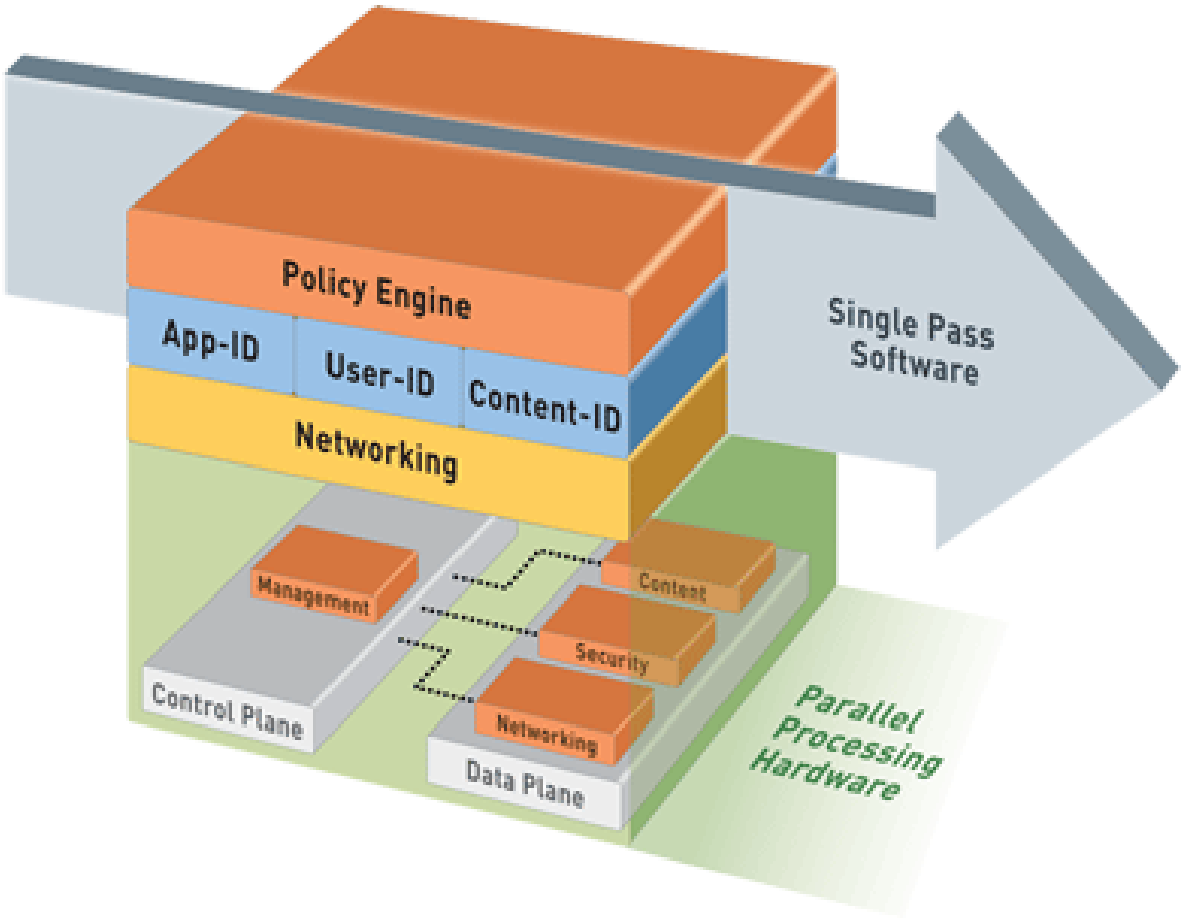
解密价值 35 亿美元的下一代防火墙核心技术

上海泛腾电子科技有限公司 徐鹤军

Palo Alto Networks 是当前网络安全领域炙手可热的公司，其推出的 NGFW 即下一代防火墙产品是网络安全领域新一代领军产品。该公司凭借下一代防护墙概念和产品将全球网络安全领域异军突起。该公司最独特的技术便是称为 SP3（Single-Pass Parallel Processing）的单程并行处理技术。下图就是该 SP3 技术的示意图。

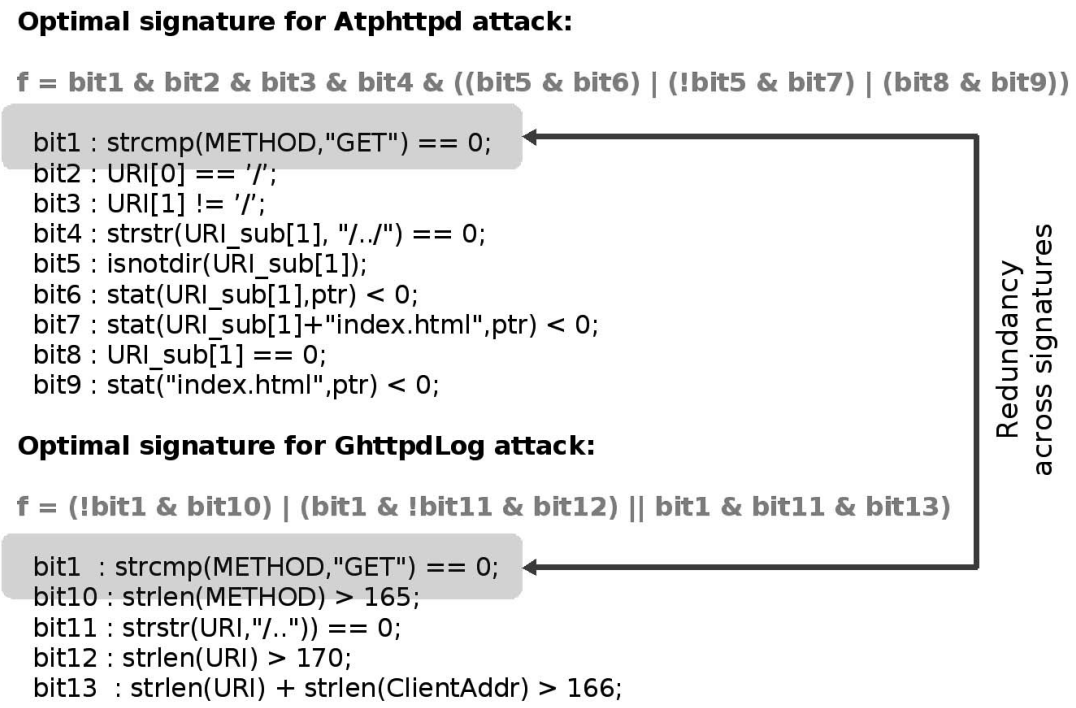


网络安全的防火墙技术已有十多年的发展了，按理已经是个非常成熟的技术方案了。就算引入 DPI（深度包检测）功能后的原理大家也都明白。但是这 SP3 技术却是个新概念，让很多业内人士都感到不理解，甚至认为是个宣传噱头。本人对 SP3 具体实现的原理也非常有兴趣，一项能够支撑 35 亿美元市值的技术必然有其独到之处，一直想一探究竟。

这样的技术不会是从石头缝里不出，或者从天儿降的产生，必然会有前沿性研究做基础。基于许多前沿性技术都会由美国政府和学校资助的这样一个惯例。终于在几年前的一个美国能源部资助项目中找到了 SP3 的基础性研究成果的说明。初步理解消化后，现在与大家共享一下这些信息。

现代基于 DPI 技术的防火墙类产品中会大量使用特征码匹配功能，随着网络应用和攻击类型的爆炸式增加，这里特征码越来越多。处理的性能和延时也受到严重影响。虽然采用了多核处理器并行处理技术，但是随着的网络流量的急剧扩容，简单的特征码匹配加多核处理器的方案也力不从心了。这就需要新的技术方案，也就是要介绍的 Single-Pass Parallel Processing 方案。该方案用到了 SAT，BDD 和 DFA 技术。

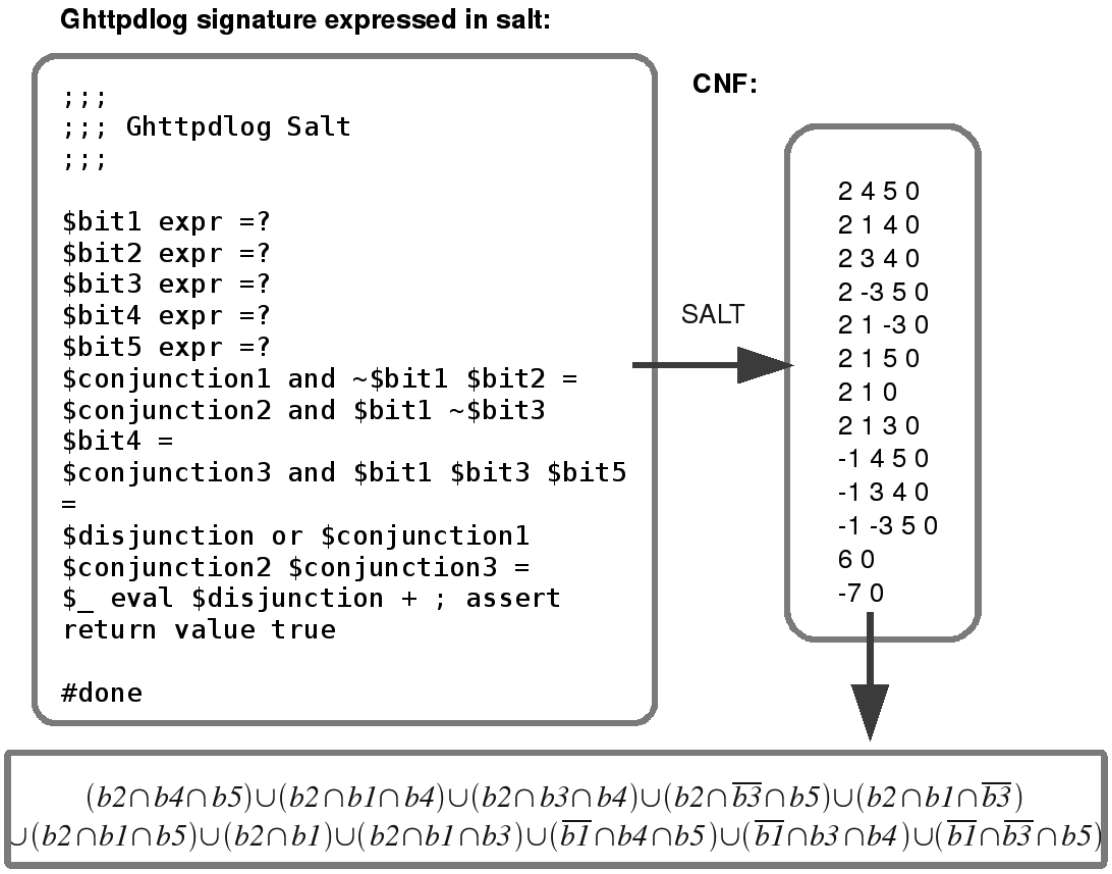
下面是两种网络攻击 Atphttpd 和 GhttpdLog 的特征码表达式。



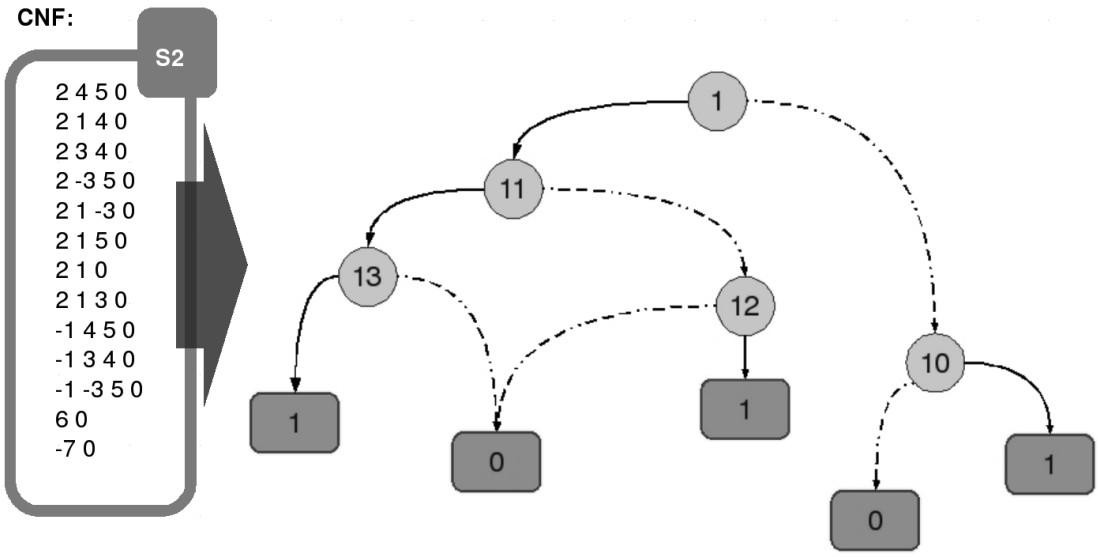
可见上面两种网络攻击特征码表达式中有一项是相同的，也就是冗余项。对于这两种特征表达式采用或（OR）操作，从而产生一个新的特征标准表达式。

要完成这项工作需要分三步来做：

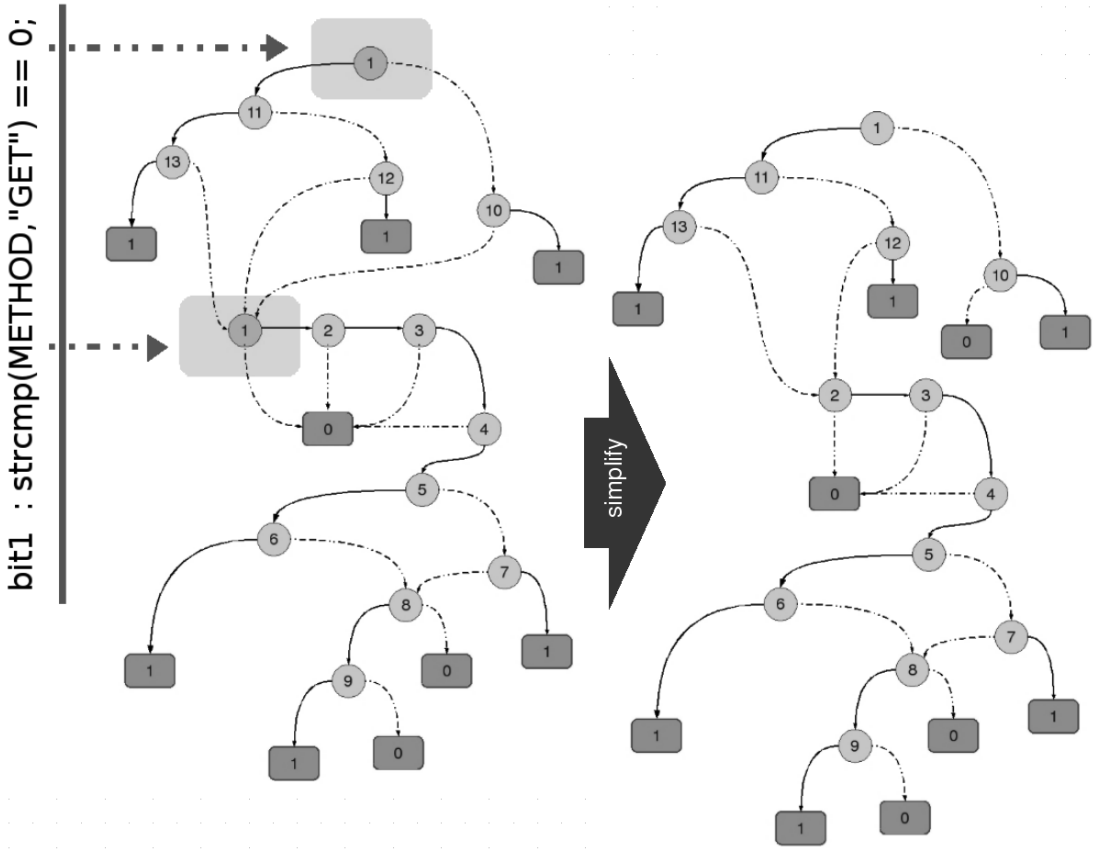
1）使用 SALT 工具（Satisfiability Application Logic Translator）将每个特征码表达式转化为 CNF（Simplified Conjunctive Normal Form）



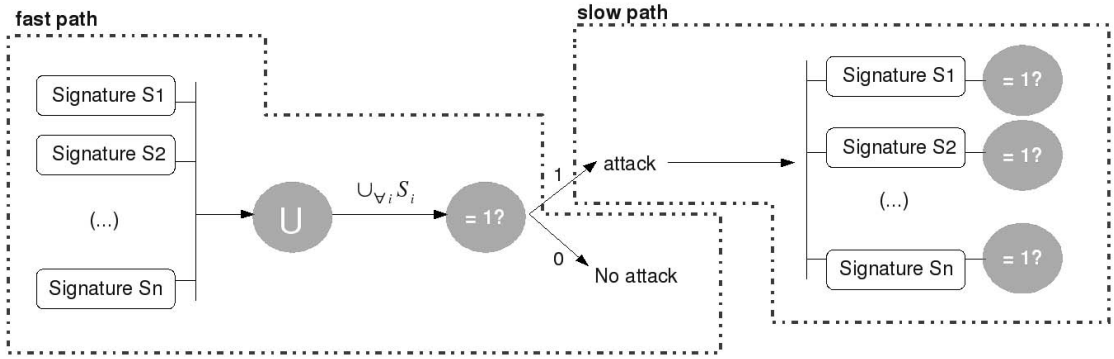
2）将使用工具将 CNF 转化为 BDD（Binary Decision Diagrams）。



3）将所有的 BDD 进行或（OR）操作，简化了冗余项，合成一个大的 BDD，从而生产一个具有 Fast Path 作用的大 BDD。

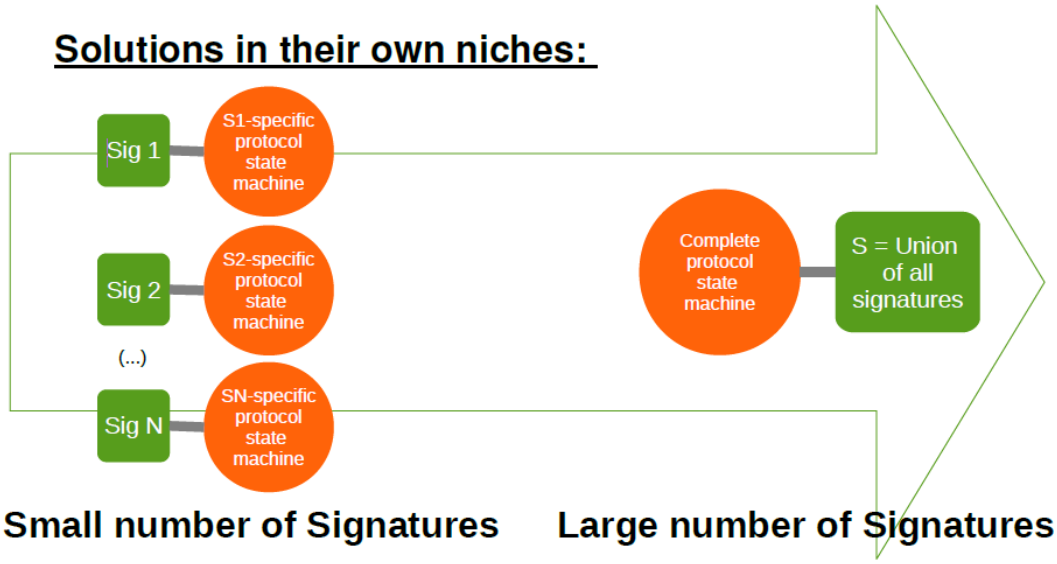


每个 BDD 就相当与一个 DFA（deterministic finite automaton）实现。由于 SALT 工具可以将 CNF 分区化操作，从而产生并行化的 BDD。这样一组特征码表达式平均的转化为多个 DFA 机。就可以采用已有的 DFA 加速方案来实现 Single-Pass Parallel Processing 功能了。

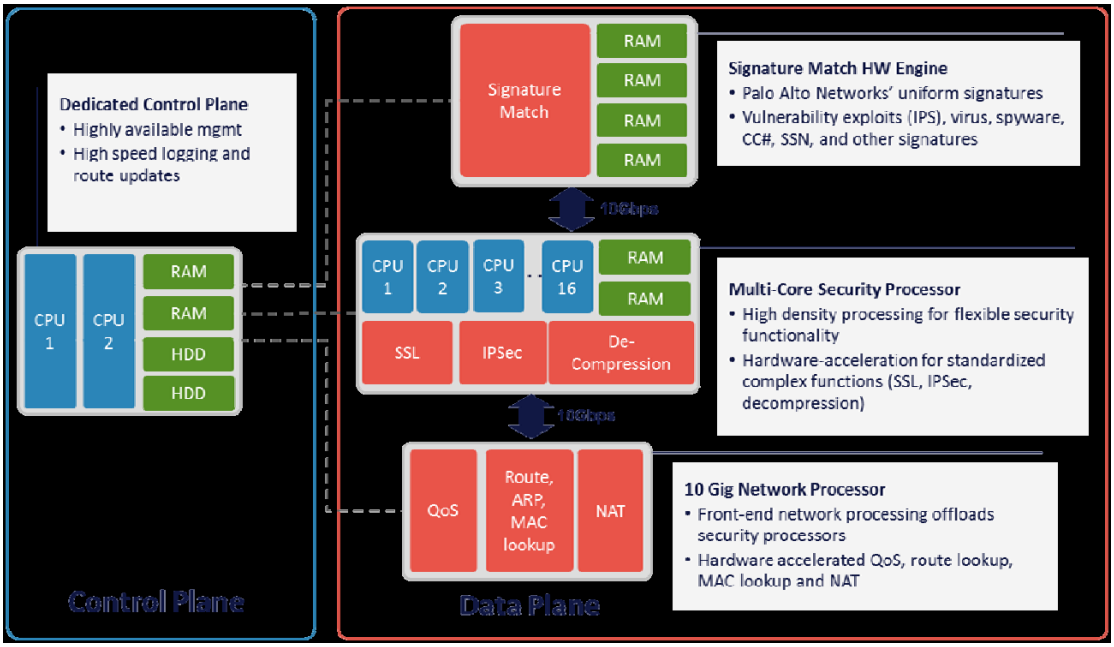


在操作上大 BDD 的 Fast Path 发现攻击信息后转入由独立 BDD 组成 Slow Path，独立判断符合哪类攻击特征。

所以 Single-Pass Parallel Processing 技术的大致效果如下图所示：



了解了上面的 Single-Pass Parallel Processing 技术实现原理的说明，我们再看看 Palo Alto Networks 公司 PA-5000 系列产品的硬件构架说明：



在支持更高吞吐量的设备上将有三个独立的专用处理器。其一是一个硬件加速网络处理器，其二，一个多核 CPU 与之相连处理 SSL 和 IPSec 流量，其三，就是 flash-match 引擎。

Flashmatching 引擎是一个硬件实现的专业正则表达式解析器-专为在数据流量中检查签名而设计。这个引擎实现的算法使得每个查询都在一定时间内完成。它的优点就是速度可预测而不是尽力而为的快。这意味着随机产生处理事件不会带来混乱。这也是实现上述 Single-Pass Parallel Processing 的核心部件。到此我们终于明白 SP3 技术的基本原理。

Single-Pass Parallel Processing 技术除了应用在网络数据安全领域，还是可以应用在其他类似领域，比如生物基因学应用和所有需要模式匹配功能的工作，意义重大。希望本文也能够为国内网络安全企业提供借鉴，从而在下一代防火墙技术上尽快赶上国外同行。