



Anchiva 硬件扫描引擎白皮书

目录

- ◆ 概览-----1
- ◆ 应用层内容扫描硬件加速技术--1--2
- ◆ 并行特征匹配技术-----2
- ◆ 多个高速扫描引擎并行处理技术---2
- ◆ Malware 特征多变性处理技术-----3
- ◆ Malware 特征多态性处理技术--3--4

基于 ASIC 架构具有专利算法的应用层内容扫描技术

概览

Anchiva Web 安全网关以自主研发的操作系统 AnchivaOS 为基础，在多核硬件架构上同时融合了 ASIC 硬件加速卡。

为什么有了多核硬件平台还需要有 ASIC 硬件加速卡呢？

在 web 安全网关产品中，需要深度的内容级检测过滤从而达到准确识别网络数据流中恶意内容的目的，因此是非常消耗系统资源的；为了进一步提高 Web 安全网关的性能，满足企业级大客户对性能的需求，安启华 Web 安全网关产品利用 CPU 进行基础的流量识别与策略匹配，而内容的深度检测过滤则由 ASIC 硬件加速卡完成。

Anchiva 自主研发实现了一系列的 ASIC 硬件加速技术，在全面查杀病毒、木马、间谍软件、恶意代码等 Malware 的同时也将 Web 安全网关设备的性能推向顶峰，让 Web 安全网关部署到大型网络之中成为可能。

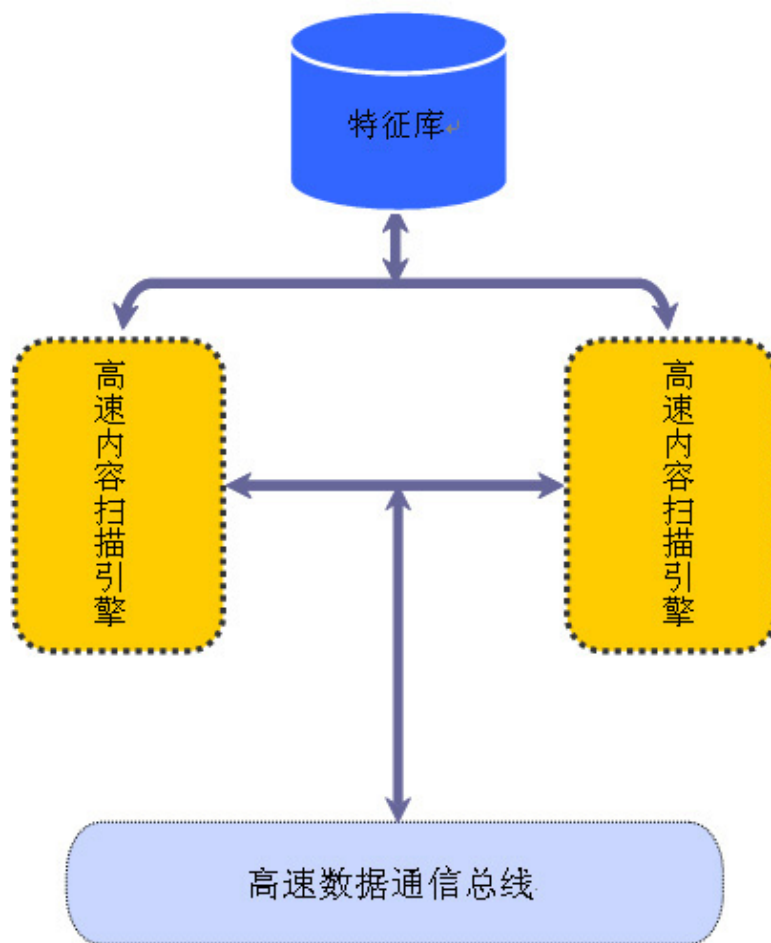
应用层内容扫描硬件加速技术

——应用层硬件加速器

传统网络安全产品的硬件加速技术，仅是网络层的硬件加速，并没有处理应用层的数据，仅仅处理网络传输过程中少量的数据，如数据链路层、网络层、传输层的头信息，而对应用层的数据并没有进行扫描。

一个完整的 web 安全解决方案，扫描分析应用层的数据是最基本的工作，同时也会带来扫描数据大幅度增加，性能下降的问题。

安启华 ASIC 硬件加速卡，如下图所示，采用内置的高速数据通信总线，无需 CPU 参与的情况下，作为通信过程中的 host，自动获得扫描数据提交给高速内容扫描引擎；高速内容扫描引擎首先会识别出需要深度内容过滤的文件类型，比如 PE 文件、TXT 文件、Bin 文件等，然后会对相关文件进行每一个字节的逐一扫描与 Malware 特征匹配，从而实现了应用层的硬件内容加速。



并行特征匹配技术

——避免病毒特征串行扫描带来的性能下降问题

现阶段 Malware 的种类和数量，大大增加，传统的软件扫描引擎，采用一定的加速扫描算法之后，必须串行处理 Malware 特征，因而会存在随着 Malware 特征数量增加而性能下降的问题。

安启华基于 ASIC 的高速扫描引擎，采用特有的并行扫描技术，在内部时钟驱动下，所有的 Malware 特征都能完全并行完成匹配过程，因而可以避免病毒特征串行扫描带来的性能下降问题。

多个高速扫描引擎并行处理技术

——扫描性能成倍上涨

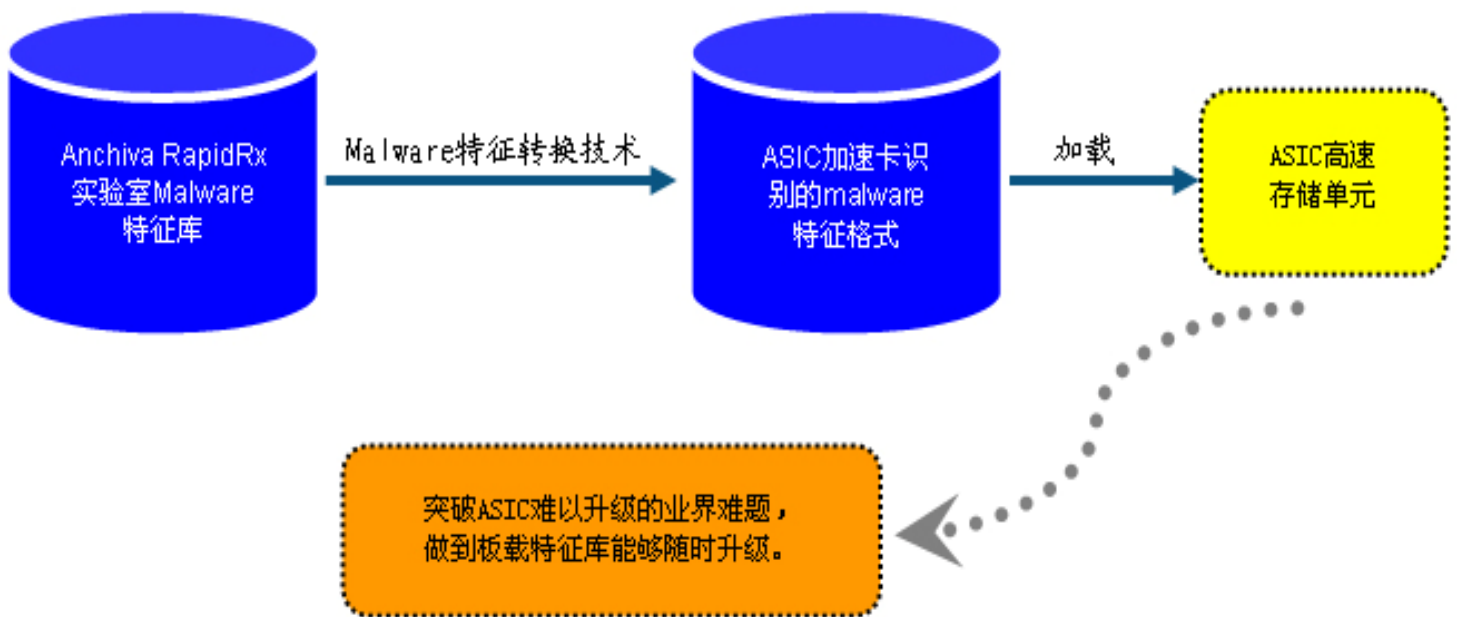
为了进一步提升硬件加速卡的扫描性能，在 ASIC 加速卡中将并连多个高速扫描器，在实现过程中，多个高速扫描器同时工作，从而使整个硬件加速卡的扫描性能成倍上涨。

Malware 特征多变性处理技术 ——突破 ASIC 难以升级的业界难题

Malware 特征在现实环境中具有多变性的特点，因而在对 Malware 的检测过程中，其特征库必须能够随时升级。

传统的 ASIC 硬件系统由于自身的限制，在出厂时，其运行和工作方式已经固化在硬件中，因而很难解决随时升级的问题。

安启华 ASIC 硬件加速卡内嵌高速动态存储单元，在 Malware 特征升级过程中，通过软件将 Malware 特征转换为加速卡识别的特征格式，并将其写入高速存储单元，从而突破了 ASIC 难以升级的业界难题，做到动态刷新 ASIC 硬件加速卡内的特征。



Malware 特征多态性处理技术 ——多级匹配技术

真实的网络环境中，Malware 特征具有多态性的特点，因而在创建特征时，文件类型、偏移地址、通配符等都存在 Malware 特征中，所有的这些都使得 Malware 特征匹配逻辑越来越复杂，因此扫描耗费的时间也会更多。

为了解决 Malware 特征匹配的复杂性以及提高特征匹配的速率，安启华自主设计的硬件扫描算法，如下图所示，数据传输控制器将数据传输到数据缓存器，同时基本特征并行扫描器开启，完成基本特征库的并行扫描匹配；通过基本特征扫描过滤以后，可能存在恶意的流量会继续发送给 Malware 扫描器进行下一步的精确匹配。这样在很短的时间内通过基本特征并行扫描器的第一遍筛选匹配后，又经过 Malware 扫描器的精确匹配，这样的多级匹配扫描技术不仅扫描匹配时间大大缩短，而且不影响扫描效果。

