

# AnchivaOS 白皮书

## 目录

- ◆ 概览-----1
- ◆ 功能全面的秘密-----1—2
- ◆ 高性能的秘密之一-----2—3
- ◆ 高性能的秘密之二-----4—6
- ◆ 良好网络适应性的秘密---6—8
- ◆ AnchivaOS 的自身可靠性---8
- ◆ 总结-----8

▶ AnchivaOS 是一个从头全新打造的软件架构，专门优化重写 TCP 协议栈，开发出了业界首个真正意义上的完全并行处理操作系统，突破了应用安全网关真正的性能瓶颈，使 Web 安全网关随着硬件配置的升高性能近似线性增长。

▶ 安启华先进的架构结合了安全和网络两个元素，融合了 NetScreen、Fortinet、趋势科技和 Juniper Networks 等公司在安全、反病毒、内容过滤、软件和系统架构方面的专长。安启华的使命是为客户提供可以无缝连接到网络中的世界级 Web 安全设备。

## 功能全面、高性能且具有良好网络适用性的 Web 网关幕后技术

### 概览

Gartner 报告中指出，2007 年 75% 的企业感染未被发现的，具有经济动机，有针对性的，并且回避传统外围设备和主机防线的恶意软件。这表明网络信息架构中，除了具有传统的外围设备和主机防线软件外，还应该具有针对网络应用层进行防护的网关设备，以此加强网络边界安全，将 Web 威胁在网络边界处进行拦截。

然而 IT 管理员在选择应用层防护网关时，会发现目前市面上的类似设备存在功能不全面、性能不足以及部署复杂等问题。

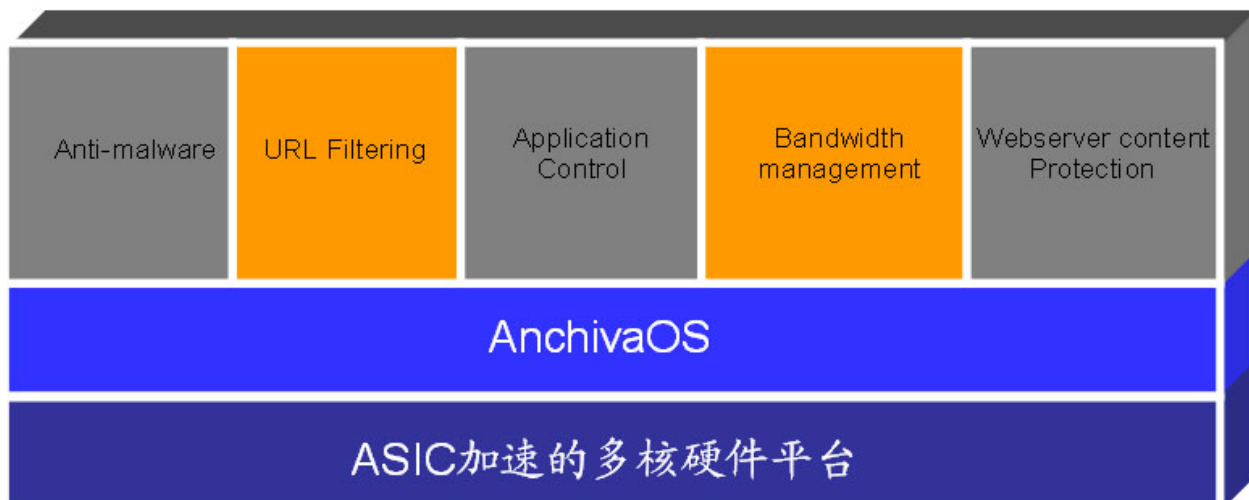
因此，市场需要在功能和性能上能够按需扩展并且能够灵活部署于现有网络架构之中的应用安全网关，以确保即使在大规模病毒爆发或网络威胁发生的时候，应用安全网关有超强的防护功能，同时具备很高的处理性能和网络适用性。

为此安启华在兼顾设备自身的可靠性与安全性的同时，为满足 Internet 应用安全网关功能需求和性能要求，耗时一年半，推出了业界首款功能全面、高性能且易于部署的 Web 安全网关，其幕后的技术就是 AnchivaOS。

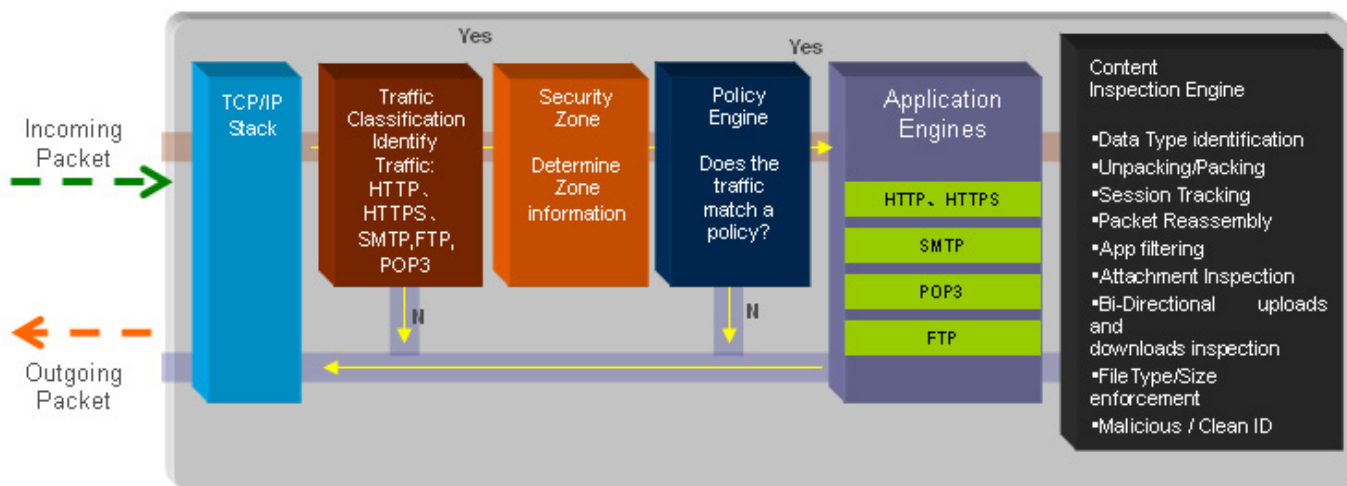
### 功能全面的秘密

#### ——功能可扩展性

为了实现 Web 安全网关超强的应用防护功能，安启华自主开发的 AnchivaOS 具有模块化的应用处理架构，能够根据 Internet 应用安全的需要将多种功能集成到一起，为设备功能的扩展鉴定了良好的基础，并且能够实现多引擎的并行处理。



如上图所示 Anchiva Web 安全网关各个功能模块并不是简单的功能堆叠，更不是穿糖葫芦；而是经过 Anchiva 研发团队在系统周密设计的基础上开发出来的，使得各个应用引擎之间的数据处理相互调用配合工作协调有序。因此数据并不是串行穿越 Anchiva Web 安全网关的各个功能模块，下图为 Anchiva 数据包处理流程：

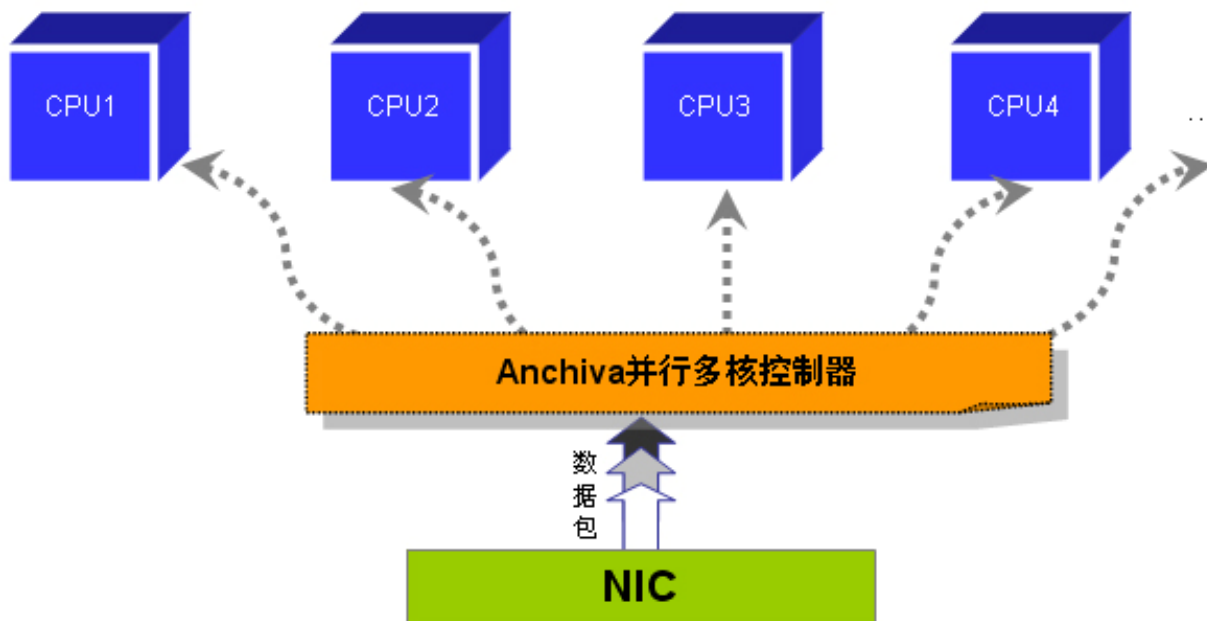


## 高性能的秘密之一 ——硬件架构可扩展性

AnchivaOS 结合了多核和 ASIC 两个硬件元素的架构支持。

### 支持多核的幕后技术

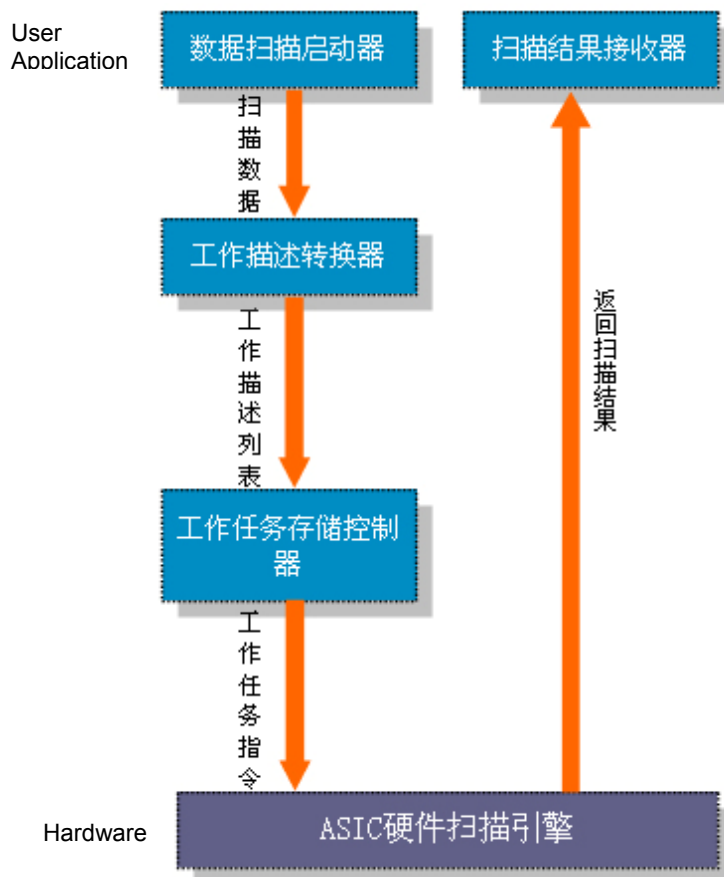
多核并不是简单的 CPU 叠加，需要 Web 安全网关从硬件到软件，从操作系统底层到上层应用进程去全方位支持多核 CPU，为此安启华专门研发了自己的并行多核控制器，充分处理核内核间任务的分工与调度。如下图所示，来自网络层的数据包进入并行多核控制器后，并行多核控制器将流量数据均衡分配到各个不同的 CPU，以便完成后续多颗 CPU 的并行事务处理。



图：并行多核控制器将处理数据均衡分配到各个不同的 CPU

### 支持 ASIC 加速卡的幕后技术

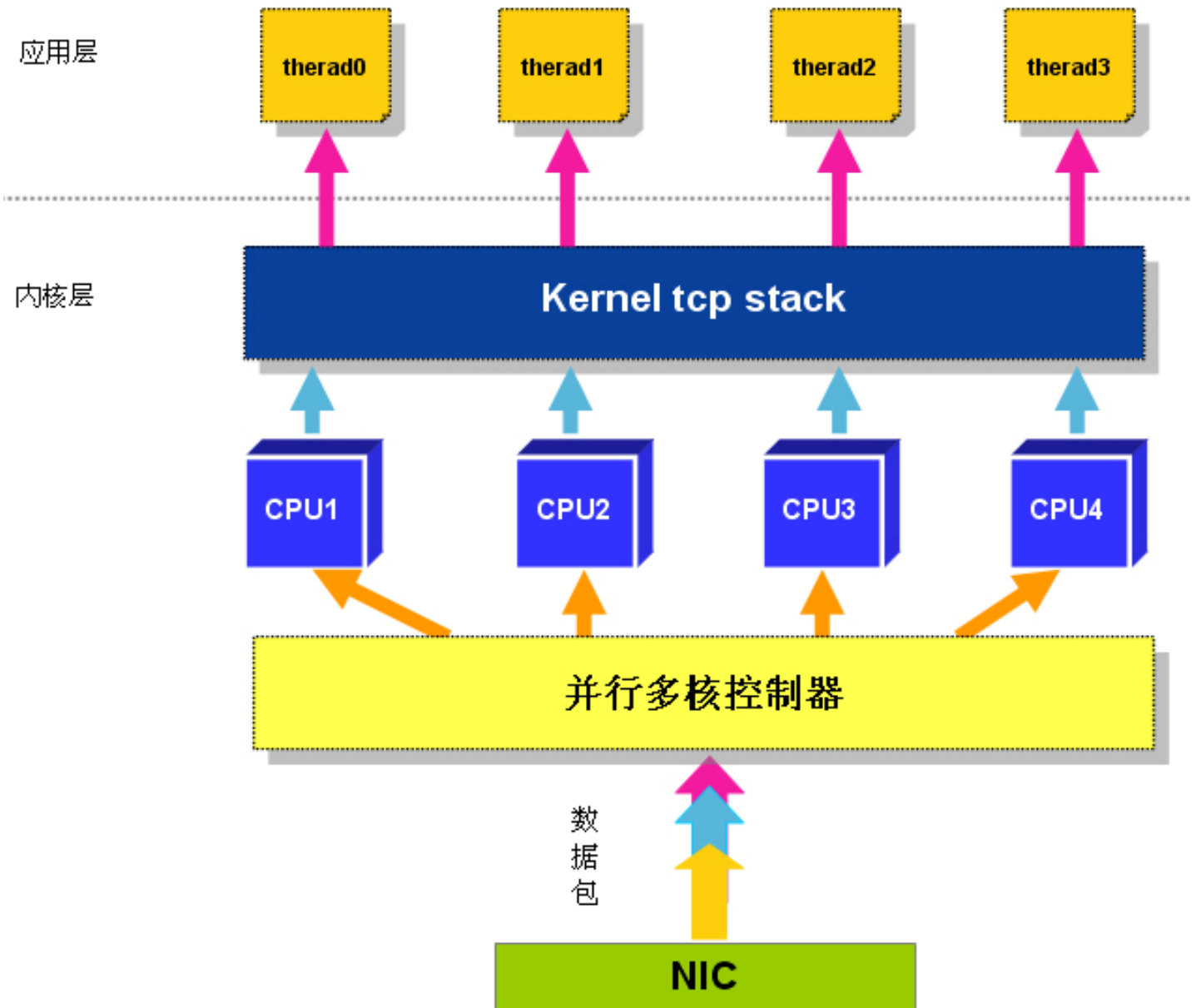
ASIC 硬件加速卡并不是孤立的运行器件，同时也需要操作系统的支持，安启华通过自主设计开发的 ASIC 驱动技术，如右图所示，应用层数据扫描启动器将扫描数据传入工作描述转换器，工作描述转换器将扫描数据转换为工作描述列表写入工作任务存储控制器，工作任务存储控制器下达工作任务指令到 ASIC 硬件扫描引擎，ASIC 扫描引擎进行数据的扫描与特征匹配，完成后将扫描结果返回给系统应用层的扫描结果接收器。（关于 ASIC 加速卡的详细技术请查看“Anchiva 硬件扫描引擎白皮书”）



## 高性能的秘密之二

### ——性能可线性增长的幕后技术

传统的经过优化的透明传输 OS 架构，如下图所示，在操作系统应用层可以进行多线程的并行处理，但是基于操作系统内核层的 TCP 协议栈存在共享锁，CPU 在进行事务处理时，要等待 TCP 共享锁的释放，因此并行度受限于 TCP 协议栈共享锁，并不能达到完全的并行事务处理。



图：传统的经过优化的透明传输 OS 架构

## 传统经过优化的透明传输 OS 架构优缺点分析

### 优点:

- 多核并行事务处理
- 多线程的并行处理

### 存在问题:

- 系统内核层 TCP Stack 存在共享锁
- 事务处理需要等待 TCP Stack 共享锁的释放

### 缺点: 转发层面不能达到完全的并行事务处理

安启华公司在成立之初就决定优化重写 TCP 协议栈, 在兼顾安全性的基础上, 开发了横跨操作系统内核层和操作系统应用层的 TCP 协议栈, 同时将 TCP 协议栈与应用代理进程并行结合, 如下图所示, 打破了通用操作系统基于 kernel 的 TCP 协议栈共享锁的限制, 从而开发出了业界首个真正意义上的多核完全并行处理操作系统 AnchivaOS, 在转发层面和应用层面都做到完全的并行处理, 突破 Web 安全网关性能瓶颈, 并且随着硬件配置的升高, Anchiva Web 安全网关的性能近似线性增长。

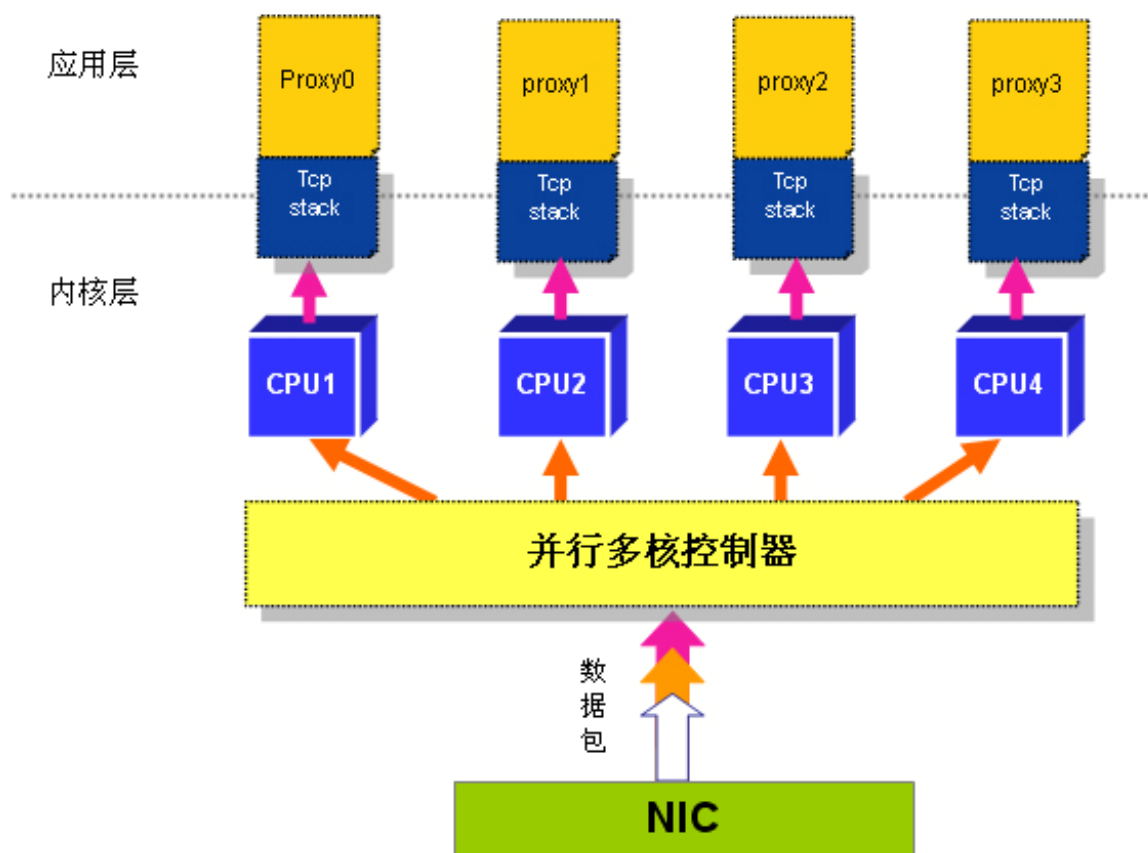


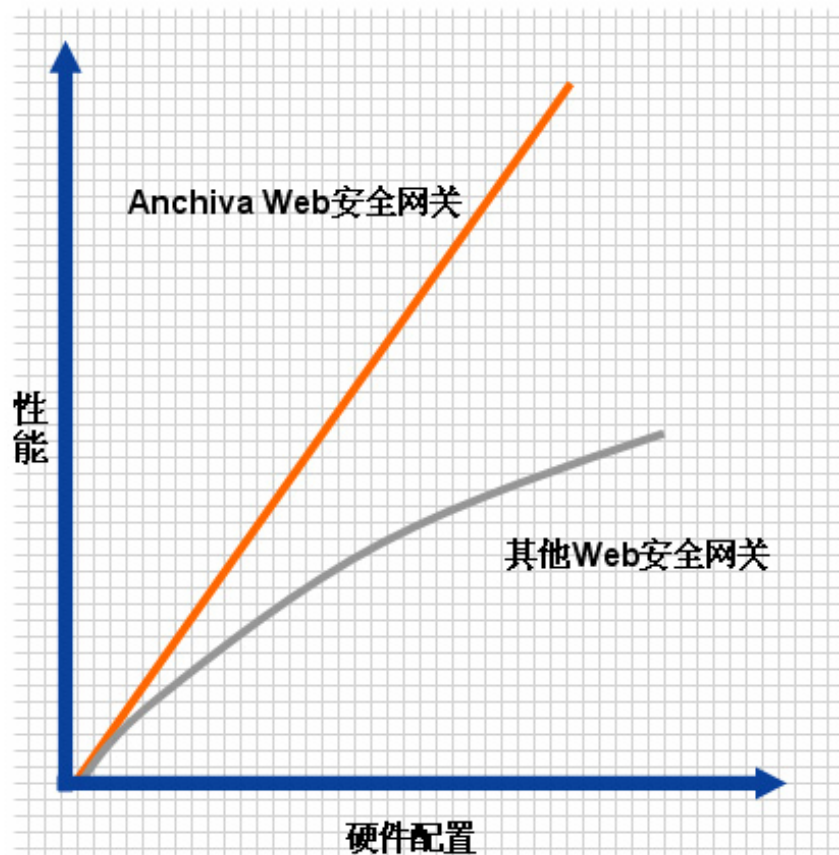
图: AnchivaOS 架构

## AnchivaOS 优点:

解决问题:

- 多核并行事务处理
- 多代理引擎并行处理
- 优化重写 TCP 协议栈，实现完全的 TCP 并发。

优点: 使 Anchiva Web 安全网关的性能随着硬件配置的提升，近似线性增长。



### 良好网络适用性的秘密

AnchivaOS 专用的会话跟踪引擎和策略引擎，智能的跟踪和确认每个会话的源和目的及其路由信息，为 Anchiva Web 安全网关的网络适用性奠定了良好的基础，从而使 Anchiva Web 安全网关很轻松的实现对 VLAN、非对称路由、单臂路由、HA 等网络环境的支持，并且是业界真正透明的 Web 安全网关，安装部署简单，无需改造应用，无需改变网络。

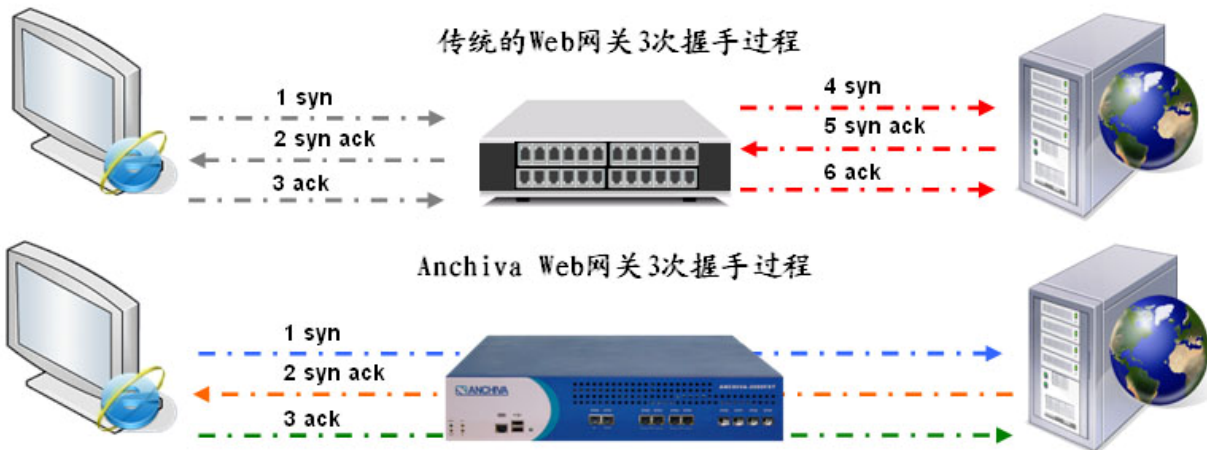
智能会话状态跟踪 (ISST) 引擎

策略引擎

跟踪和确认每个会话的源和目的及其路由信息

- ▶ 适应各种网络环境
  - 支持非对称路由
  - 支持单臂路由环境
  - 支持多区域
  - 支持VLAN
  - 支持HA
- ▶ 真正透明Web安全网关

Anchiva Web 安全网关良好的网络适应性的表现之一就是：它是真正的纯透明 Web 安全网关。对用户的现有网络没有任何影响，如下图对比所示：



数据包经过Anchiva SWG扫描前后，包头信息不会改变。

DST MAC	SRC	SRC IP	SRC Port	DST	Payload / Data	
00-10-10-20-20-	00-10-10-20-20-	10.1.5.205	45.1.2.3	10456	80	Payload / Data
MAC		IP	TCP			

由上图可以看出，与传统的透明代理 Web 安全网关相比，Anchiva Web 安全网关没有中断客户机和服务器之间的三次握手，最大程度的保留了数据的原有信息，实现了真正意义上的透明。因此一些传统透明 Web 网关很难解决的问题，比如 OSPF 路由协议的透传问题等，在 Anchiva Web 安全网关上就可以轻松实现。

## AnchivaOS 的自身可靠性

AnchivaOS 具备良好的功能和性能可扩展架构的同时，也具有很强的自我防范机制：

1. 完全由 Anchiva 定制的内核，没有通用系统的漏洞。
2. 没有开启任何无用端口，黑客无法通过嗅探器获取任何有用的系统信息。
3. 采用 HTTPS 及 SSH 进行安全访问，从而能有效防御来自外界的各种攻击。
4. 采用多极管理员权限，防止管理员权限滥用。
5. 强制使用复杂密码，防止字典攻击。
6. 启用账号锁定功能，防止暴力破解。

## 总结

支持多核、ASIC 硬件加速、多引擎并行处理，且优化重写 TCP 协议栈的 AnchivaOS 让 Anchiva Web 安全网关处理 Internet 应用威胁的效率大大提升，并且随着功能的增加，处理性能不受影响；AnchivaOS 智能的会话跟踪引擎和策略引擎，使 Anchiva Web 安全网关能够适应各种网络环境；从而缔造了业界功能全面、高性能且具有良好网络适用性的 Web 安全网关。

## 多核硬件平台 + ASIC加速卡 + AnchivaOS

=可线性增长的高性能

