

**Hillstone®**

**安全平台**

新一代安全应用架构

山石网科通信技术(北京)有限公司

[www.hillstonenet.com](http://www.hillstonenet.com)

# Hillstone安全平台

## 新一代安全应用架构: 多核CPU+ASIC+高速总线+专用操作系统

### 1. 介绍

随着网络应用的快速发展和更多内、外部威胁的出现，我们不得不面临这样的问题：达到高带宽要求的同时怎样能够保护网络不受侵害。在各种应用安全防护(例如QoS、IDP、网络AV、反垃圾邮件以及内容过滤等)不断出现的同时，用户仍在寻找更高安全级别的设备。

当前的设备不能解决以上所述问题，因为它们没有足够的CPU处理能力，不能在进行千兆数据处理的同时执行安全检测。

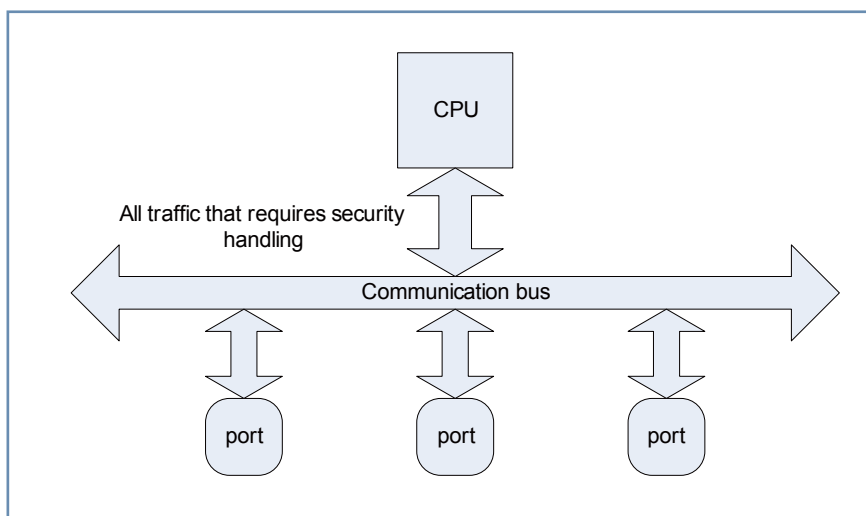
Hillstone的创新解决方案集先进的软硬件技术于一身，创造了一个全新的安全平台，完全能够应对我们当前面临的问题。

### 2. 防火墙技术的发展

1995年，CheckPoint推出了第一代防火墙产品：基于软件的防火墙。它是状态检测防火墙，在当时是技术性的突破。然而，很快问题就出现了：软件解决方案会产生性能变异，这个问题很难控制并且不能适用于需要提供吞吐量保证和低延迟的网络。

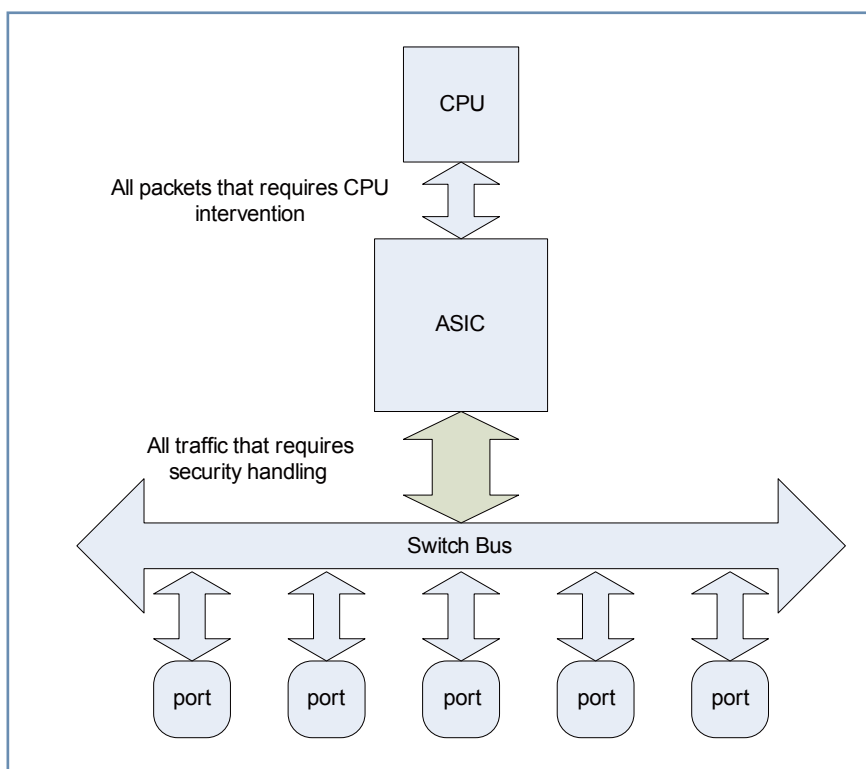
在1996到1997年，出现了第二代防火墙：基于PC架构的防火墙。

图1: 基于PC的防火墙结构 ▶



1997年，NetScreen研发成功了ASIC防火墙。这种定制的ASIC防火墙与软件解决方案相比，安全规则匹配速度和数据流查询速度提升了几十倍。NetScreen防火墙是第一个在网络层安全上达到千兆速率并且提供优异性能的防火墙。

图2: ASIC防火墙结构 ▶



从此，防火墙技术发生了巨大的变化。ASIC防火墙优于传统防火墙，例如在处理NAT和快速数据流查询方面。但是，在集成了应用层安全功能后，CPU就没有足够的处理能力了。对于当前的安全设备，一旦开启应用安全功能，性能通常都会大大下降。

近几年，一些公司开始为应用层安全尝试使用网络处理器（NP）结构。虽然NP在可扩展性上优于ASIC，但是它仍然不能及时响应今天安全需求的快速变化。由于缺乏可扩展性和可维护性，NP结构已经逐步被淘汰。

随着应用层网络功能集成的快速发展，例如QoS，流量优化也需要大量的CPU处理，而现今的安全设备却不能很好的支持这一功能。

### 3. 创新一代安全架构

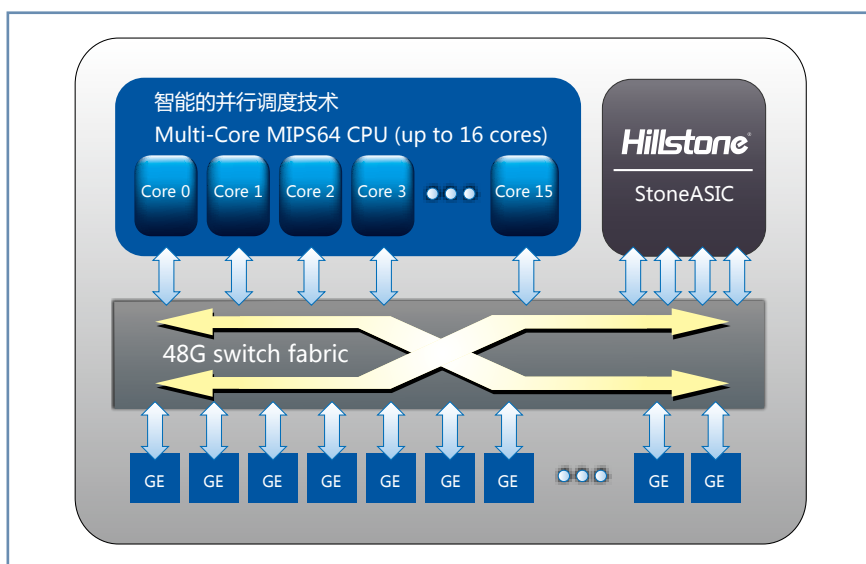
#### 硬件平台

ASIC能够做到的是高速执行简单的预定义操作。已经被证实的ASIC能够实现的技术包括规则查询、会话匹配、数据包交换/路由和QoS队列管理等。许多网络层的安全功能可以在ASIC内部得到实现。

与通用处理器相比，ASIC的缺点在于它的不可改变性和低扩展性，尤其缺乏用户自定义特性。现在的大部分应用安全逻辑都或多或少需要一定程度的CPU干预处理，这也就是多核CPU的主要优势所在。

Hillstone安全平台使用ASIC来实现网络级安全，使用多核CPU加速应用层安全，再使用高速交换总线加速各个模块之间的通信。

图3: Hillstone安全平台硬件架构 ▶



- StoneASIC: Hillstone ASIC解决方案主要用于网络和安全加速，在硬件平台上结合了最新的网络安全处理技术和攻击防护功能。当设备需要快速转发数据包并防护来自僵尸网络(botnet)的各种类型的攻击时，StoneASIC可以提供卓越的性能保证。这样就能够释放处理器性能来处理其它更需要CPU计算的功能。并且，StoneASIC的硬件管道能够为数据流提供稳定的、低延迟的高带宽总线，不需要其它安全处理。

- 多核CPU: Hillstone利用高性能CPU使对网络数据包的处理达到最优化。CPU被固定在硬件的包转发引擎中，用来处理包保序和不同核之间的分发。在专门开发的针对多核并行处理的StoneOS操作系统支持下，基于数据包的细粒度并行调度技术确保每个核都能高负荷运行，从而使整个系统性能达到最优。智能的数据包跟踪技术确保数据包经不同核处理后能按照输入顺序被输出。并行工作的多核CPU能够在网络和安全处理中提供可升级的、高可靠的性能。并且，它能够提供最大限度的灵活适应性来处理现今安全设备面临的各种复杂需求。

- 高速交换总线模块: 这种交换总线通过端口把多核CPU和StoneASIC连接起来，并且保证所有模块之间快速的无阻碍通信。市场中的大量安全设备都是依靠低速总线进行CPU通信的，而Hillstone通过高速交换总线的使用就避免了这一缺陷。

Hillstone平台还集成了IPSec、SSL、加解密运算、压缩解压缩以及DFA功能

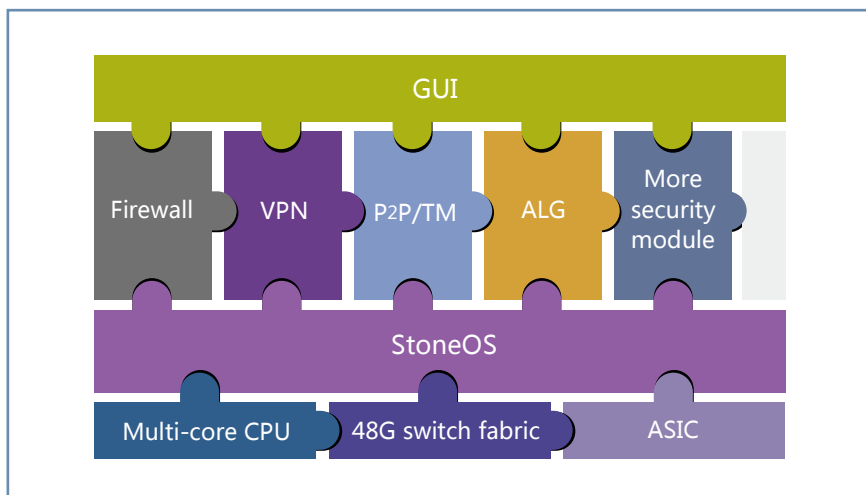
的硬件加速芯片。IPSec VPN支持DES、3DES、AES、AES192、AES256、NULL和SCB2等加密算法，哈希算法包括SHA1、MD5和NULL等。对于DES、3DES、AES、AES192和AES256采用OCTEON的芯片加密引擎进行硬件加速，SCB2国密算法采用了单独的加速芯片进行加速。通过硬件加速，实现了数据的快速加解密，提高了数据的吞吐量，减少了数据处理的延时，从而保证了用户应用的快速处理。

## 软件

StoneOS是Hillstone客户化定制的64位实时并行操作系统。它支持专有的并行多核处理器控制技术和ASIC控制技术。StoneOS为网络和应用安全功能提供了可升级的、高可靠的计算平台。

StoneOS由完全独立的控制平面和数据平面组成。这种分离机制保证了控制平面的可靠性、稳定性和数据平面的卓越性能。StoneOS数据包转发引擎 – 可升级安全引擎(SSE)是完全用户化定制并且经过安全加固，可实现安全和网络处理的高度并行，能够充分利用多核和ASIC结构的各自优势，同时能够保证数据包的保序质量，为用户营造高性能、高可信赖的网络。

图4: StoneOS软件架构 ▶



StoneOS SSE结合了网络数据包分类、攻击防护、安全规则匹配、QoS、转发、路由和VPN处理等功能，并且将它们并行化，从而在多核处理器上高效运行。Hillstone的多核控制技术能够在最小化多核协调花费的同时允许每个核的单独运行。

对于那些不能通过ASIC完成的、需要安全处理的数据流，将由多核CPU和StoneOS进行处理，并且并行工作的多核CPU的处理速度能够与ASIC的包处理速率相匹配。这样，Hillstone解决了传统纯ASIC系统的CPU瓶颈问题。

Hillstone安全平台采用模块化设计，能够方便地进行软件模块的嵌入集成或者硬件模块的外部扩展，以此来支持更多的网络和安全功能。

## 4. 结论

现在，防火墙技术的发展正在超越传统的ASIC解决方案，进入一个全新的时代。安全和网络市场的结合要求更高计算能力的设备，Hillstone安全网络设备正在以创新的安全应用架构来引领这一发展趋势。

Hillstone解决方案能够为用户提供：

- 一流的攻击防护能力，能够防御各种DoS和DDoS攻击
- 超过目前市场同类产品5到10倍的新建会话能力
- 处理各种数据包以及VPN流量时的卓越性能
- 进行应用安全处理时的卓越性能
- 杰出的QoS性能，支持上万用户的细粒度QoS和会话控制



山石网科通信技术(北京)有限公司

[www.hillstonenet.com](http://www.hillstonenet.com)

### 北京总部

地 址: 北京市海淀区上地七街1号  
汇众大厦3层  
邮 编: 100085  
电 话: +86(10)8289 7229  
传 真: +86(10)8289 9814

### 上海办事处

地 址: 上海市陕西北路1388号  
银座企业中心1721室  
邮 编: 200060  
电 话: +86(21)6149 8205  
传 真: +86(21)6149 8001

### 成都办事处

地 址: 成都市总府路2号  
时代广场A座26层2625  
邮 编: 610016  
电 话: +86(28)6606 7115  
传 真: +86(28)6606 7199

### 广州办事处

地 址: 广州市天河区天河路208号  
粤海天河城大厦13层1363室  
邮 编: 510620  
电 话: +86(20)2826 1950  
传 真: +86(20)2826 1999

服务热线: 400-650-0259

Copyright © 2008, Hillstone Networks, Inc. 版权所有，保留所有权利。

Hillstone Networks、Hillstone Networks标识、Hillstone、Hillstone标识、StoneOS、StoneManager、Hillstone SA-2003、Hillstone SA-2005、Hillstone SA-2010、Hillstone SA-5020、Hillstone SA-5040、Hillstone SA-5050、Hillstone SR-330、Hillstone SR-530和Hillstone SR-550为Hillstone公司的商标。所有其他商标和注册商标均为本公司的财产。

本文所包含信息可能会有所修改，恕不另行通知。