

Hillstone 山石网科

多核Plus[®] G2安全架构白皮书

1. 概述

随着网络快速发展，更多新的应用不断出现，由此带来新的威胁和管理上的挑战，另外随着数据集中和应用的深入，网络流量也在快速增长，网络变得越来越复杂。我们不得不面临这样的问题：如何有效确保网络不受侵害？如何保护关键应用不受影响？如何应对网络流量的快速增长？如何保护当前投资？当前的设备不能解决以上所述问题，因为它们不能在同时进行千兆数据处理的同时执行深度应用检测。Hillstone 山石网科采用创新的多核Plus[®] G2安全架构可有效解决上述问题。

2. 安全产品的需求

随着网络的快速发展，应用和威胁出现了一些新的改变，网络的使用方式也和以前有所不同，这些变化包括：

网络应用在改变：一方面，网络应用的数量在不断丰富，包括IM（及时通信），P2P下载，视频浏览，网络游戏和SNS(社交网络)等。另一方面，网络应用的方式在改变，为了躲避协议封堵，将应用建立在HTTP等基础协议基之上，或者端口号采用随机产生，或者采用诸如SSL的加密方式来隐藏内容。面对这些新的应用方式，让传统基于端口的应用和行为无法识别，网络变得越来越无法管理。网络可视化是新一代安全网关必须解决的问题。

流量在加剧增长：随着应用的深入发展，数据集中的趋势也越来越明显。一个企业网内部需要大量的服务器，这些服务器会接受来自各个分支和总部的应用请求。一个数据中心也可能拥有几千台服务器。在这种变化中，网络正在从千兆走向万兆甚至10万兆，网络流量越来越大。另一方面是伴随着流量和应用的增加，网络对安全产品也提出了更高的要求，比如高性能、高并发、高容量的需求。

安全设备的功能需要在增加：统一威胁安全管理的解决方案，已经逐渐在取代以多个单点防护串行防护的安全网络。支持多个功能模块统一处理，已经成为了当下安全网关的一个发展趋势。同时，对网络的管理方式也在发生变化，从传统UTM的外网攻击防护，到内网网络管理，如带宽管理、上网行为管理等功能需求已经成为新一代安全网关的必要组成部分。可视化，可管理，可审计等所有的功能模块将在同一个

Hillstone 山石网科多核Plus® G2安全架构白皮书

平台上运行，如何来保证这么多的功能模块并发运行，是新一代安全关必须解决的问题。

安全产品投资回报不能忽视：一方面，具有可用性的统一威胁管理的解决方案在某个层面上已经起到了保护用户投资的需求。另一方面，面对日益增长的应用和流量以及网络安全的需求，如何让用户当前购买的安全产品能够有效的满足未来一定时间段新的需求，充分保护用户对网络安全的建设的投资回报，而不是一旦用户网络升级而被淘汰，就需要重新购买新的安全产品

综上所述，网络的发展对网络安全产品提出了新的需求：

- 面对当今的日益增长的流量需求和应用需求，以及网络管理的需求，新一代安全架构需要提供良好的性能和容量并发来支撑。
- 提供细粒度的网络可视化管理。如果没有细粒度的网络可视化，那么网络安全将无安全可言。这种细粒度的识别包括：用户识别，应用识别和行为识别。
- 用户投资需要兼顾，可扩展的架构设计是新一代安全网关架构的必要组成部分。

3. 安全网关架构的发展趋势

第一代：基于X86架构

X86架构又被称为通用CPU架构，具有开发、设计门槛低，技术成熟等优点，曾经以其高灵活性和扩展性在百兆防火墙上获得过巨大成功。但是缺陷也是显而易见的：在X86平台，所有通过防火墙的数据包都要通过CPU去处理，由于x86架构的硬件并非为了网络数据传输而设计，它对数据包的转发性能相对较弱，内部交换总线则成了处理能力的瓶颈，无法适应日益增长的网络性能要求。



图1 X86硬件架构

Hillstone 山石网科多核Plus® G2安全架构白皮书

第二代：基于NP/ASIC架构

定制的NP/ASIC架构同 X86架构的方案相比，安全规则匹配速度和数据流查询速度提升了几十倍。NP/ASIC能够做到的是高速执行简单的预定义操作。许多网络层的安全功能可以在ASIC内部得到实现。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，一旦开启应用安全功能，性能通常都会大大下降。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。



图2 ASIC/NP硬件架构

新一代安全网关架构

针对第一代X86和第二代NP/ASIC安全产品架构上的不足，Hillstone山石网科推出了多核Plus架构，该架构是专门针对当今的网络安全需求而定制的。多核Plus架构使用多核CPU加速应用层安全，使用ASIC来实现网络级安全，再使用高速交换总线加速各个模块之间的通信。目前，Hillstone山石网科在多核Plus架构基础上又推出了多核Plus® G2架构。该架构立足于当前网络的需求，并结合网络发展趋势，兼顾未来网络发展变化的需求，进一步增强了性能可扩展，实现了存储和接口的扩展，另外软件采用了全并行流检测引擎进一步提升了网络可视化，优化了性能和增强了可靠性，在开启多个功能后，仍然可以实现设备的高吞吐量和低延时。

其主要特点如下：

- 多核处理器+StoneASIC+高速交换总线提供高处理能力，满足网络对可视化，可管理，可审计的需求。
- 可扩展的模块化设计保护用户投资
- 全并行流检测引擎实现高性能，高容量的处理
- 交叉检测实现网络可视化

4. Hillstone山石网科多核Plus® G2安全架构解决方案 硬件平台

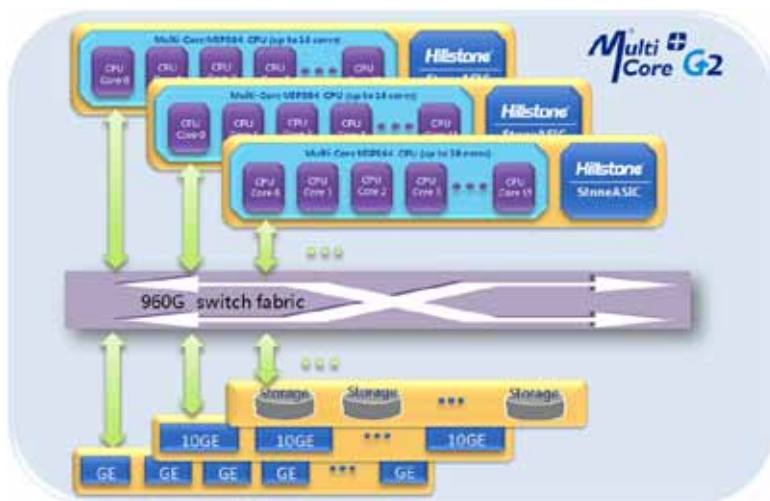


图3 多核Plus® G2架构

- **多核CPU:** Hillstone山石网科利用可扩展的64位高性能多核CPU的行处理能力来为应用层的安全功能提供保障。这其中每个多核CPU可扩展至多达16个核，多核CPU也可扩展成多个CPU。Hillstone山石网科平台还集成了IPSec、SSL、加解密运算、压缩解压缩以及DFA功能的硬件加速芯片。通过采用硬件加速芯片，实现了数据的快速加解密，进一步提升了VPN和应用层安全的处理能力。

- **可扩展模块化:** Hillstone山石网科采用模块化设计，可以实现性能可扩展、存储可扩展和接口可扩展。模块化设计可充分保护投资。通过增加应用处理扩展模块，可以提高本机应用处理能力，让应用处理不再成为性能瓶颈；增加存储扩展模块可以实时记录日志；增加接口扩展模块提高设备的连接性，使设备不会因为网络带宽或应用系统的升级而过时。

- **StoneASIC:** Hillstone山石网科利用StoneASIC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。

- **高速交换总线:** Hillstone山石网科通过采用高达960G的交换总线将多核CPU，网

Hillstone 山石网科多核Plus® G2安全架构白皮书

络接口和StoneASIC连接起来。高容量的交换总线保证所有模块之间快速的无障碍通信。

软件平台

众所周知，操作系统是整个安全设备的核心和基础，任何硬件都是由操作系统进行调度使用。Hillstone山石网科在多核Plus® G2硬件架构的基础上，采用了自主研发的StoneOS® 64位实时并行操作系统。该操作系统采用全并行流检测引擎，通过此技术可保障网络可视化，同时可进一步提升设备性能和可靠性。相关技术如下：

交叉检测

作为状态检测防火墙的进化，随着越来越多的针对应用协议的攻击的出现，深度检测(Depth Inspection)应运而生。深度检测实际上是防火墙里对IDS、IPS技术的一个集成，通过对数据流进行协议的解析，捕获违反协议的交互和一些攻击的行为。随着网络技术的发展，越来越多的应用采取加密、隧道、伪装等绕行技术。新一代安全网关基于用户的管理也对安全检测技术提出了更高的要求。

Hillstone山石网科的交叉检测（Cross Inspection）技术不仅对协议进行深度的分析，还利用解密、解压技术打开包括SSL、GZIP等加密加壳数据流，对协议和内容进行过滤。和认证系统的互动将IP和用户相映射，对用户其他内容和行为相关联，作为应用和行为分析的依据。交叉检测技术通过综合分析用户（User）状态，应用（Application）状态和行为（Behavior）状态，来确认协议的真正含义，实现更精准和更快速的定位。Hillstone山石网科交叉检测技术也为网络可视化和对用户网络行为的管理，创造了坚实的基础。

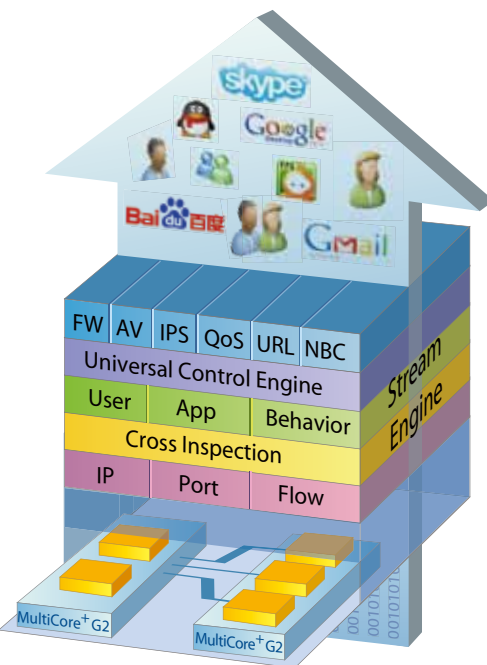


图4 全并行流检测引擎

Hillstone 山石网科多核Plus® G2安全架构白皮书



图5 交叉检测

流检测

传统的威胁检测是基于文件的。这种方法是基于主机的安全解决方案实现的，并且旧一代网关内容安全解决方案也继承这一方法。使用这种方法，首先需要下载整个文件，然后开始扫描，最后再将文件发送出去。从发送者发送出文件到接收者完成文件接收，会经历长时间延迟。对于大文件，用户应用程序可能出现超时。而且，缓存的数据占用大量的内存，系统无法同时对大量的数据流进行扫描。



图6 基于文件检测

Hillstone山石网科的安全扫描引擎完全是基于流的。安全扫描引擎在数据包流到达时进行检查，如果没有检查到威胁，则发送数据包流。大大减少了数据的延时，用户感觉到应用的响应速度大大提高。同时，基于流的扫描引擎因为不需要对每个数据流做大量缓存，极大地提高了系统安全功能的容量。

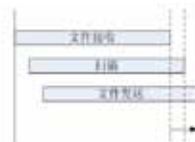


图7 基于流检测

基于流的技术要求系统所有处理环节都是基于流的处理。一个系统如果有一个基于流的TCP代理，基于流的协议分析，但安全扫描却是基于文件的。所带来的效果只能是基于文件的。在处理流水线中最差的环节决定了系统的性能。Hillstone山石网科在多个层面上运用了流引擎技术，为用户带来了完全的基于流引擎技术的数据平面。

- TCP代理
- 解析器：包括协议解析（例如：HTTP，SMTP等），内容解析（例如：MIME，

Hillstone 山石网科多核Plus® G2安全架构白皮书

base64等），内容解压缩（例如：gunzip, unrar等），文件解析（例如：PE格式等），SSL解密

- 安全处理：包括协议控制，内容控制，AV扫描，IPS扫描，异常发现等
- 应用处理：包括ALG，应用代理，应用隧道，应用优化等

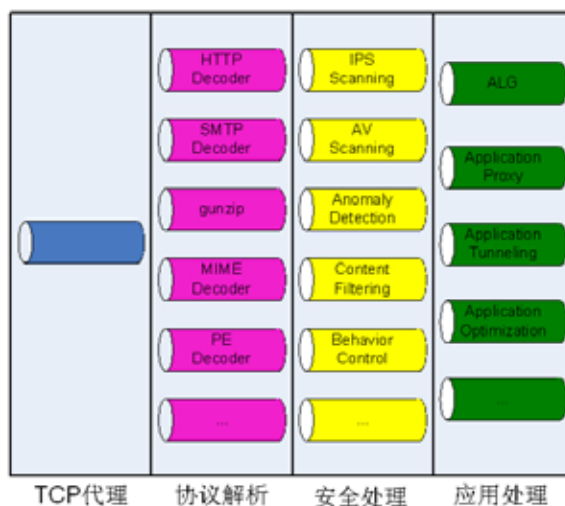


图 8 流引擎

全并行的架构

Hillstone山石网科在多核Plus® G2硬件架构的基础上，采用全并行架构，实现更高的执行效率。Hillstone山石网科的新一代UTM即使在开启了多种功能后，仍然可以实现设备的高吞吐量和低延迟。

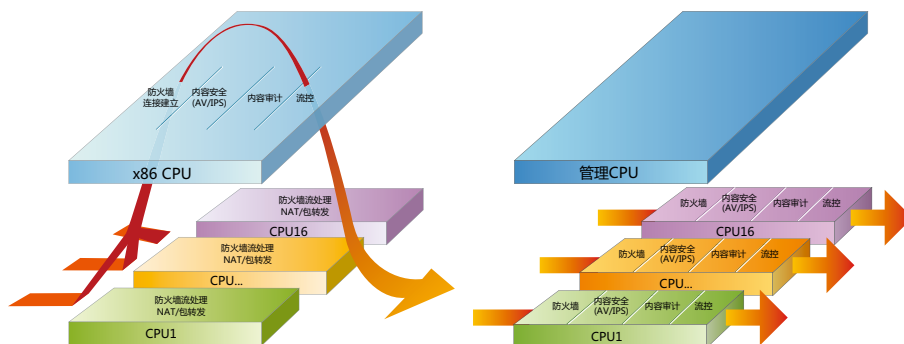
目前许多多核系统以多核处理器代替NP/ASIC的位置。在这种系统里，多核处理器带来了比NP/ASIC更好的可编程性。但多核处理器只担任网络安全处理的任务，应用处理和内容安全仍然由主控CPU处理。许多平台上，新建连接等防火墙功能也是由主控CPU实现的。

在Hillstone山石网科并行操作系统里，所有的流处理都是针对多CPU多核系统而开发，重复利用了硬件平台的平行性。在新建连接等防火墙指标上站在业界的前列。在应用处理方面，所有流引擎都为高度并行化编程开发。降低数据结构的相互依赖，使性能和容量可以和CPU和CPU核数接近线性地增长。Hillstone山石网科的全并行处理方式能够所保障多个安全功能开启的情况下，仍然能保证非常高的吞吐量和低延迟。

图 9 普通多核方案

图 10 全并行多核方案

Hillstone 山石网科多核Plus® G2安全架构白皮书



另外Hillstone山石网科的多核控制技术能够使多核调度的花费最小化的同时允许每个核的独立运行,从而在一个核遇到故障的时候, 整个系统保持正常运行。

优化的处理流程

在传统的UTM设备中, 流量需要流经几个独立的网络引擎, 分类引擎, 模式匹配引擎和策略引擎。这种重复劳动不仅效率低而且性能低。

图 11 传统UTM软件处理流程



Hillstone山石网科采用优化的统一处理流程。一旦数据包进入处理流水线, 流水线的处理阶段只会处理一次, 这包括: 网络功能, 协议解析, 协议安全处理, 内容解析, 内容安全处理, 用户、应用、行为识别, 应用处理等。每个阶段模块处理结果会分别输入需要的下阶段模块处理, 减少重复的分析和处理流程。大幅降低数据包的处理延时, 提高系统容量和性能。

独立的控制和数据平面设计

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。独立的控制平面设计, 不会因为流量过大或异常攻击而导致设备无法管理和日志无法记录。独立的数据平面则可实现安全和网络处理的高度并行, 同时能够保证数据包的保序质量, 为用户营造高性能、高可信的网络。

5. 结论

现在,安全网关的发展正在超越传统的解决方案,进入一个全新的时代。网络市场的发展要求更高性能的设备 and 更细粒度的网络可视化,同时能够保护用户投资。Hillstone山石网科正在以创新的多核Plus® G2安全架构来引领这一发展趋势。

北京总部

海淀区上地七街1号
汇众大厦3层
邮编: 100085
电话: 010-8289 7229
传真: 010-8289 9814

上海办事处

上海市闸北区广中西路777弄
88号华清大厦406室
邮编: 200072
电话: 021-6631 8601/02/03
传真: 021-6631 8601-800

广州办事处

天河体育东路122号羊城国际
商贸中心东塔15层1510-1511
邮编: 510620
电话: 020-3825 4309
传真: 020-3825 4311

成都办事处

成都市顺城大街308号
冠城广场7楼S座
邮编: 610017
电话: 028-8652 8597
传真: 028-8652 8306

南京办事处

中山东路300号
长发中心A栋1602室
邮编: 210002
电话: 025-8682 9916
传真: 025-8682 9916-606

西安办事处

高新技术开发区科技路33号
高新国际商务中心7层704B
邮编: 710075
电话: 029-8833 7347
传真: 029-8833 7347