

# Hillstone山石网科UTM Plus技术白皮书

## 1 概述

### 从防火墙到UTM

早期的安全设备基本上都是单点串行的接入方式。安全设备独立运行，管理复杂，单点故障多带来的可靠性极低，同时，安全状态分析复杂，并且投资较高，维护成本高，使用的处理的数据在所有的设备上都需要处理以便，对性能的牺牲也是极大的。

### 从UTM到UTM Plus

UTM（统一威胁管理）的出现似乎解决了这问题，UTM的部署方式不再是单点串行部署，而是将所有的安全引擎都内置在同一安全设备上，从理论上讲，UTM的出现解决了传统防火墙，防病毒，入侵防御等单点式安全产品串行部署带来的一系列如安全管理，投资高，维护成本大，单点故障多的问题。但是，是不是UTM的出现就能解决所有的问题了呢？

- 从传统的UTM实现来看，只是将安全功能简单的叠加，导致系统性能急剧下降，系统不可用。所有安全功能单独运行，仅是简单集成到了一个系统平台上，安全模块没有做到内部互动，安全问题依然存在，传统UTM越来越成为了概念，离使用越来越远…



图1 传统UTM 串行软件处理架构

- 从当前用户对网络安全需求的角度来看，之前网络安全的管理的重心主要是集中在在外网到内网的攻击防护和阻断，但随着互联网业务的发展，业务带宽被P2P等下载软件蚕食，无序的、不受约束的上网行为导致不良网站访问、“安全门”、

## Hillstone山石网科UTM Plus技术白皮书

“泄密门”等信息泄密事件的产生等。全网安全管理，而不仅仅是外网攻击防护，已经让传统UTM只能“防外不防内”的解决方案失去了意义。

### UTM Plus是什么

UTM Plus是建立在传统UTM解决方案之上，能应对当今复杂多变的网络应用，能满足当下用户对安全应用的需求，并且不管从系统架构层面到软件设计，都具备良好的处理能力来支持所有庞大的功能模块正常运行。

- 从网络应用的变化角度来看，UTM Plus解决方案必须能识别和处理新型复杂多变的应用，只有可视化的识别这些应用才能针对应用进一步做对应安全引擎处理。
- 从用户对网络安全的应用角度来看，UTM Plus解决方案对用户的网络的防护将不再仅仅是局限于防护来自外网安全问题，流量控制，员工上网行为管理和入侵防御、病毒过滤，VPN，访问控制等功能将有机的成为UTM Plus的必要功能集合。
- 从功能可用性上，UTM Plus强调的是开启安全引擎之后，所有的功能都能系统的运行起来，而不能仅仅是把多项功能做简单堆叠。

从UTM 到 UTM Plus，将是符合新的网络应用趋势，满足用户对复杂多元的网络需求，并最终解决多种功能开启后整机功能的可用性。

### Hillstone 山石网科UTM Plus解决方案

Hillstone 山石网科集合多年网络安全经验，积极应对复杂多变的网络管理需求和新的业务应用需求。其推出的UTM Plus解决方案主要由下面这些方面组成：

- 全新的多核PlusTM(Multi-Core Plus)架构(多核处理器+ASIC+高速交换总线+StoneOS)
  - 面向用户的网络服务(RBNS)
  - 超强的DDoS抗攻击能力
  - 高度灵活、高性能的QoS流量控制能力(基于角色及应用(如P2P)的限流)
  - 高性能、细粒度的会话控制能力
  - 超大容量IPSec VPN链接(多达20,000条)
  - 高性能、高容量的第三代SSL VPN
  - 快速简洁的大规模VPN部署(PnVPN)
  - 高性能的应用层检测能力
  - 高性能、高容量的病毒过滤(AV)
  - 高性能、高容量、精准过滤的入侵防御(IPS)
  - 基于超过2千万域名的分类网页访问控制 (URL filtering)
  - 高可靠性和稳定性、易于使用和维护、最低的总体拥有成本

## 2 Hillstone 山石网科UTM Plus特点

### 全并行处理的安全架构(多核Plus® G2)

Hillstone山石网科自主开发的64位实时安全操作系统StoneOS®, 具备强大的并行处理能力。StoneOS®采用专利的多处理器全并行架构, 和常见的多核处理器或NP/ASIC只负责三层包转发的架构不同; StoneOS®实现了从网络层到应用层的多核全并行处理。

因此SG-6000较业界其他的多核或NP/ASIC系统在同档的硬件配置下有多达5倍的性能提升, 为同时开启多项防护功能奠定了性能基础, 突破了传统安全网关的功能实用性和性能无法两全的局限。

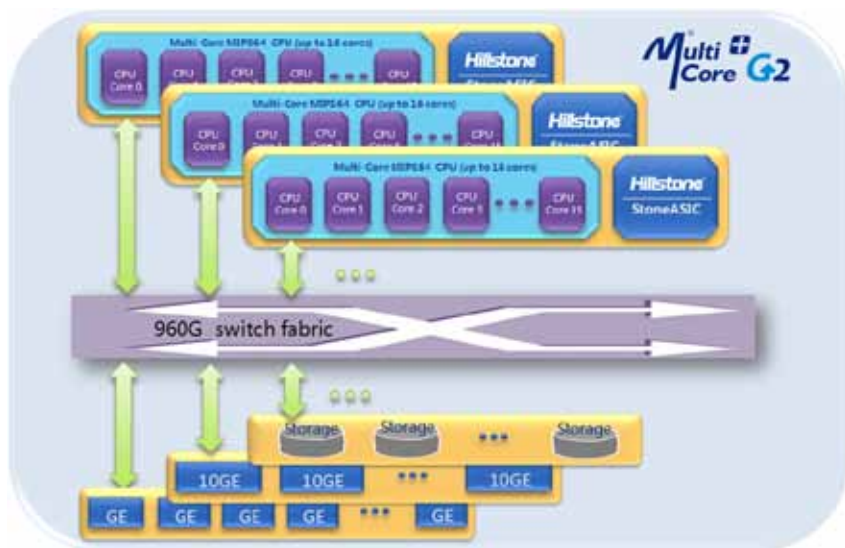


图2 多核Plus G2架构

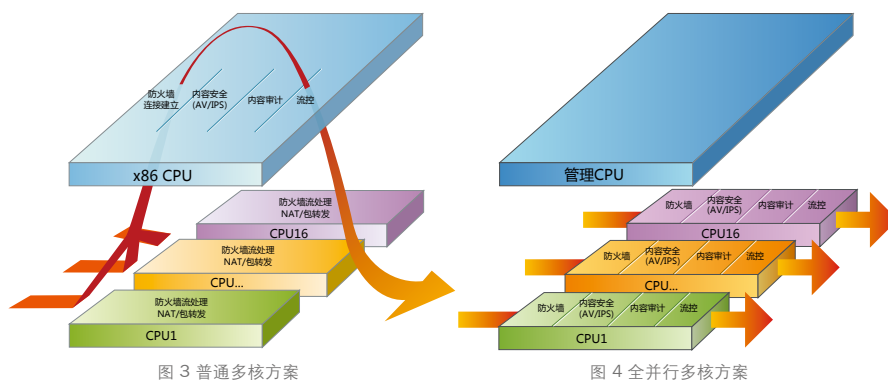
Hillstone山石网科在多核Plus G2硬件架构的基础上, 采用全并行架构, 实现更高的执行效率。Hillstone山石网科的新一代UTM即使在开启了多种功能后, 仍然可以实现设备的高吞吐量和低延迟。

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

## Hillstone山石网科UTM Plus技术白皮书

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。



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。

### 安全可视化 - 基于角色和应用的管理

没有能见度就谈不上安全。StoneOS®的应用和身份识别，能够满足越来越多的深度安全需求。

基于身份和角色的管理(RBNS)让网络配置更加直观和精细化。不同的用户甚至同一用户在不同的地点或时间都可以有不同的管理策略。用户访问的内容也可以记录在本机存储模块或专用服务器中，通过用户的名称审阅相关记录使查找更简单。

基于角色的管理模式主要包含基于“人”的访问控制、基于“人”的网络资源(服务)的分配、基于”人“的日志审计三大方面。基于角色的管理模式可以通过对访问者身份审核和确认，确定访问者的访问权限，分配相应的网络资源。在技术上可避免IP盗用或者PC终端被盗用引发的数据泄露等问题。



## Hillstone山石网科UTM Plus技术白皮书

### 全并行流检测引擎为核心

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。

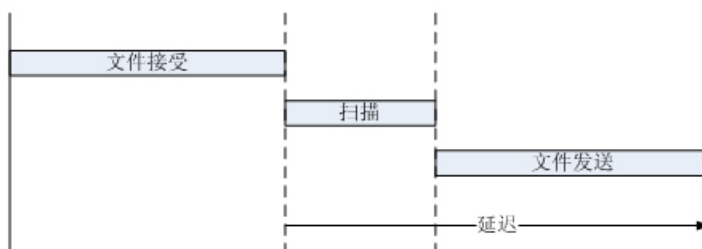


图6 基于文件检测

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。

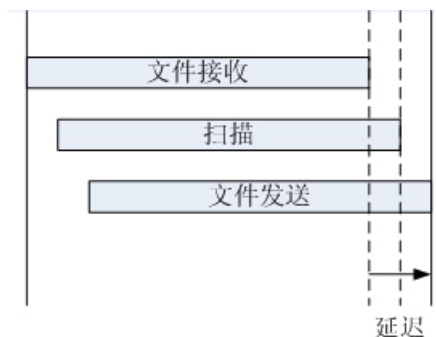


图7 基于流检测

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处理：

- TCP代理

## Hillstone山石网科UTM Plus技术白皮书

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

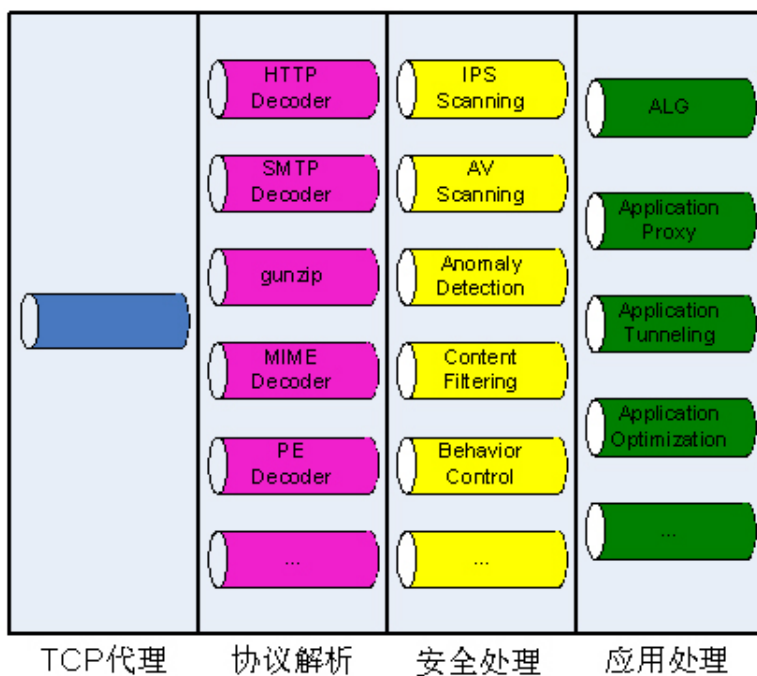


图 8 流引擎

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。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。

### 3 Hillstone 山石网科UTM Plus功能列表



图 9 UTM Plus功能集合

#### 防火墙

- 全新一代基于应用的防火墙
- 基于应用/角色的安全策略
- 可防范DNS Query Flood, Syn Flood, DoS/DDoS等攻击
- 各种畸形报文攻击防护
- ARP 欺骗防护

#### VPN

- 支持各种标准IPSec VPN协议及部署方式
- 创新的PnPVPN® (即插即用VPN)
- 支持 SSL VPN (可选USB-key)
- 支持L2TP VPN

#### 病毒过滤

- 基于流、低延时、高并发、高性能的病毒过滤
- 支持大病毒文件的扫描
- 实时病毒连接阻断，病毒事件记录

## Hillstone山石网科UTM Plus技术白皮书

- 支持常见病毒传输协议HTTP、FTP及各种邮件协议扫描
- 超过40万的病毒特征库，病毒库可以做到实时更新

### 入侵防御

- 基于状态、精准的高性能攻击检测和防御
- 实时攻击源阻断、IP屏蔽、攻击事件记录
- 支持针对HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、FINGER、MSSQL、ORACLE、NNTP、DHCP、LDAP、VOIP、NETBIOS、TFTP等多种协议和应用的攻击检测和防御
- 支持超过3,000种的攻击检测和防御

### 上网行为管理

- 超过2千万条域名的分类Web页面库，轻松控制不良网站访问
- 基于应用(P2P, 即时通讯, 游戏, 办公软件等)的细粒度网络访问控制
- 内容审计, 包括对论坛发帖、外发邮件、IM聊天等内容的审计
- 敏感文件类型过滤, Java Applet/ActiveX阻断

### 流量管理

- 基于角色、应用、IP地址、时间等的流量管理策略
- 支持基于服务等级(CoS)的流控, 兼容DiffServ标记
- 弹性流控, 可以动态分配带宽

### 结论

Hillstone山石网科UTM Plus解决方案是以多核Plus G2为安全架构, 以全并发流检测引擎和安全可视化为基础, 能够满足当下复杂多变的应用, 能满足当下用户对安全应用的需求, 并且不管从都具备良好的处理能力。来支持所有庞大的功能模块正常运行。

#### 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