

# Hillstone山石网科入侵防御白皮书

## 1. 概述

### 互联网的发展趋势表明:

1. 网络攻击正逐渐从简单的网络层攻击向应用层转变，单纯的防火墙功能已经不能满足当下应用安全的需求。旁路的入侵检测方式又不能满足对攻击源实时屏蔽的需求，与防火墙联动的入侵检测一直没有标准的联动协议来支撑。入侵检测解决方案正在被入侵防御取代。

2. 安全漏洞、安全隐患的发生似乎是不可避免的，互联网的应用和业务却正在爆炸式的增长。应用类型在增加，应用特征却更复杂，比如现在有很多应用都是基于HTTP等基础协议，让传统基于端口来识别应用的入侵防御解决方案已经不能适用。如何识别出这些新的应用，从而去检测防御针对这些应用的攻击，是新一代入侵检测网关需要解决的问题。

3. 网络带宽在增加，应用类型在增加，应用协议在复杂化，攻击类型在增加，攻击方式在隐蔽化。传统入侵防御设备受限于自身处理能力，已经不能胜任这样的趋势，如何去进行深度应用分析、深度攻击原理分析，也许所有的厂家都知道简单的攻击特征匹配已经不能满足时下用户对入侵防御漏判误判的要求，却受限与设备自身的处理能力，从而误判漏判的行为时有发生。

Hillstone山石网科的入侵防御是基于多核plus<sup>®</sup> G2架构、全并行的流检测引擎和基于攻击原理的入侵防御检测引擎。基于多核plus<sup>®</sup> G2的安全架提供了高性能的入侵防御解决发难，并为入侵防御需要的深度应用分析和攻击原理分析提供了强劲的处理能力。全并行流检测引擎则使用较少的系统资源，并且在并行扫描会话和开启其他多项应用处理功能提供了高可用性。基于攻击原理的入侵防御有助于提高攻击检测率和降低攻击误判率。

### Hillstone山石网科入侵防御解决方案具有以下特性:

- 基于深度应用识别，积极防范复杂应用攻击
- 基于多核Plus<sup>®</sup> G2构架满足深度应用分析、入侵防御功能的高CPU和高内存资源需求
- 基于深度应用原理、攻击原理的入侵防御解决方案
- 支持HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、

## Hillstone山石网科入侵防御白皮书

FINGER、MSSQL、ORACLE、NNTP、DHCP、LDAP、VOIP、NETBOIS、TFTP等多种常见的应用和协议的攻击防护。

- 定期攻击特征库更新，安全专家积极响应新的攻击和漏洞
- 基于策略或者安全域的入侵防御，可针对不同的服务器对象定制不同的规则集合。

## 2. Hillstone山石网科入侵防御解决方案

### 基于深度应用识别

Hillstone山石网科采用了全新一代基于应用行为和特征的应用识别，其基于深度应用识别的技术，突破传统基于端口的网络防御方式，只有真实的识别出流量对应的应用，才能有针对性的去防范针对应用的攻击。StoneOS®支持超过几百种以上的应用特征库，同时，应用特征库是支持定时自动升级，无需更换软件版本。在对网络应用可视化的前提下，StoneOS®入侵防御支持针对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。

### 可扩展的全并行多核Plus® G2硬件架构

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。

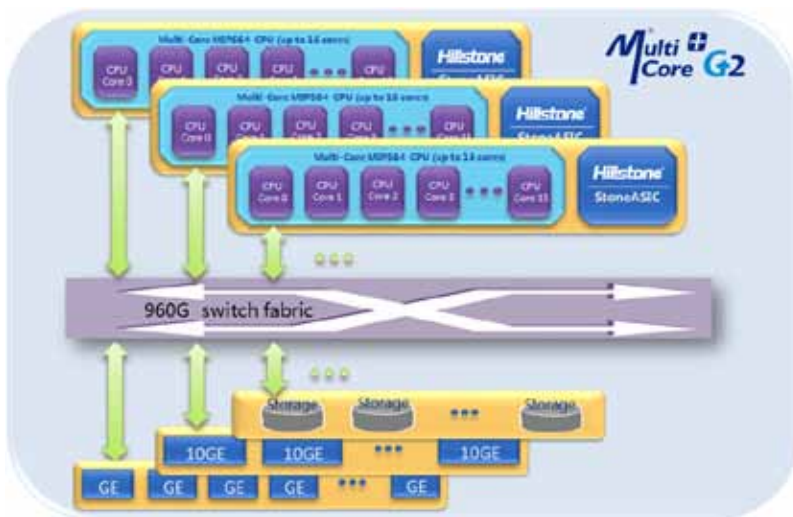


图 1: 可扩展的全并行多核Plus G2硬件架构

## Hillstone山石网科入侵防御白皮书

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，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。同时，其基于模块化的设计可以实现：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。

### 基于深度应用原理和攻击原理的入侵防御

简单的入侵防御规则匹配，肯定已经不能满足用户对入侵防御检测率和误报率的需求。从技术原理来分析，如何才能保证入侵防御具有精准的检测率呢？一是系统本身需要有强劲的处理能力，能够满足深度应用分析和攻击分析的需求；二是精准防御是建立在深度应用识别之上的；三是对攻击的分析应该是基于原理的而不仅仅是基于简单的规则匹配的。基于深度应用和攻击原理的入侵防御手段能防御一些攻击的躲避技术，提高攻击检测的准确率。从基于深度应用的状态检测，协议规范检测等，再到攻击原理的分析，最后才会是规则特征库的模式匹配。



图 2: 基于深度应用和攻击原理的入侵防御

### 攻击迅速响应 防御最新攻击

支持超过3,000种的攻击检测和防御，安全专家，安全专员分析，积极应对新攻击，支持攻击特征库离线在线更新，定期自动更新多种方式。

## Hillstone山石网科入侵防御白皮书



图 3: 积极攻击响应，防御最新攻击

### 基于策略的入侵防御功能

Hillstone山石网科入侵防御功能与策略引擎完全集成。管理员能够完全控制以下各方面：哪些域流量需要进行入侵防御，以及哪些服务器和应用被保护，并且可以根据服务器的具体应用定制入侵防御规则集。

### 3. 结论

Hillstone山石网科入侵防御提供了以深度应用，多核Plus® G2为架构，以精准防御、快速过滤为前提，积极攻击响应为后盾，满足了现今复杂多元的攻击防护需求。

#### 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5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

销售与服务热线: 400-650-0259

Copyright © 2009, Hillstone山石网科版权所有，保留所有权利。

Hillstone Networks, Hillstone Networks 标识, Hillstone, Hillstone山石网科, Hillstone标识, StoneOS, StoneManager, Hillstone PnPVPN, 多核Plus, Multi-Core Plus, Hillstone SA-2001A, Hillstone SA-2001, Hillstone SA-2001B, Hillstone SA-2003, Hillstone SA-2005, Hillstone SA-2010, Hillstone SA-5020, Hillstone SA-5040, Hillstone SA-5050, Hillstone SA-5180, Hillstone SR-320, Hillstone SR-330, Hillstone SR-530, Hillstone SR-550和Hillstone SR-560为Hillstone山石网科公司所属商标。所有其他商标和注册商标均为其各自公司的财产。本文所包含信息可能会有所修改，恕不另行通知，如需最新信息请浏览 Hillstone山石网科网站(www.hillstonenet.com)。