

Hillstone 山石网科病毒过滤白皮书

高性能网关病毒过滤解决方案

1. 概述

网络安全的发展趋势表明，网络上涌现出越来越多的攻击和感染方式去侵害PC，并且随着越来越多的移动用户和远程用户的接入，也就意味着连接在一起的PC之间同时存在不同的病毒过滤和安全配置。在网络中，对于那些没有足够防护的PC是很容易受到危害的。基于主机的病毒过滤解决方案已经不再能够满足安全需求。病毒过滤网关提供了第二层安全防护，极大地提高了网络安全性。

从技术角度来看，病毒过滤扫描需要消耗大量系统资源，包括内存、总线带宽和CPU。在有限的硬件处理能力的支持下，现有的安全网关在开启病毒过滤功能后，性能都会急剧下降。

Hillstone山石网科的病毒过滤基于多核plus[®] G2架构和全并行的流检测引擎，提供高性能病毒过滤解决方案，能够侦测病毒、木马、蠕虫、间谍软件和其他恶意软件。基于多核Plus[®] G2架构的设计提供了病毒过滤需要的高处理能力，其提供的应用处理扩展模块进一步的提高了病毒过滤的处理能力和总计处理能力，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最大可扫描文件方面提供高升级性。

Hillstone 山石网科病毒过滤解决方案具有以下特性：

- 基于多核Plus[®] G2构架满足病毒过滤应用的高CPU和高内存资源需求
- 支持病毒过滤应用处理扩展模块提高病毒过滤和整机处理能力
- 全并行流检测引擎，提供了高并发，大容量，低延时的病毒过滤
- 基于流的多层解压缩器支持ZIP，RAR等压缩格式
- 定期动态病毒库更新
- 支持HTTP、文件传输和多个电子邮件协议
- 支持多种行为控制，包括中断连接、文件填充和日志记录

2. Hillstone 山石网科病毒过滤架构

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。

Anti Virus高性能网关病毒过滤解决方案

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，其提供的应用处理扩展模块进一步的提高了病毒过滤的处理能力和整机处理能力。

StoneOS[®]，Hillstone山石网科并行操作系统，通过多核处理器上运行病毒过滤扫描引擎从而提供可升级的病毒过滤性能。StoneOS[®]的每一核都可以单独执行病毒过滤扫描或者其它需要的安全功能。网络流量被负载均衡到负荷最小的处理器以实现低延迟安全处理。

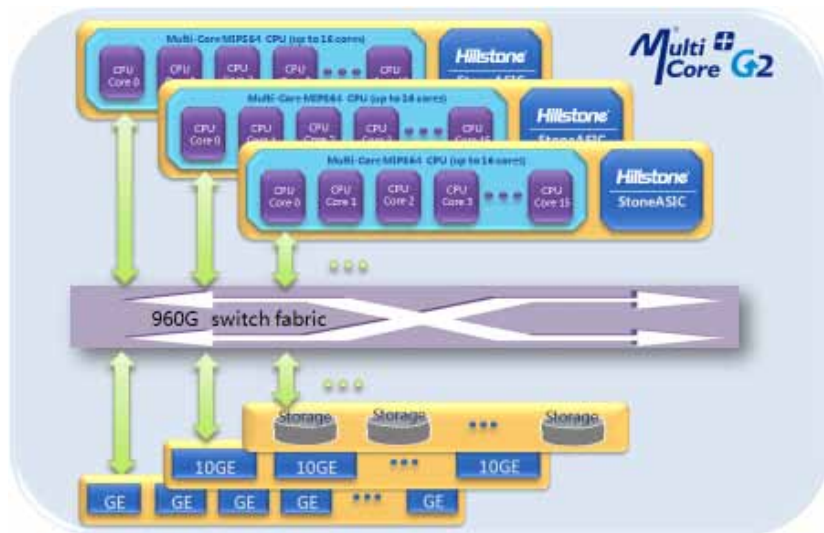


图 1: 可扩展的全并行多核Plus G2硬件架构

软件架构

Hillstone山石网科网关病毒过滤功能采用模块化软件构架。病毒过滤引擎与包转发的分离意味着用户可以有更多的选择进行网络部署。在模块化的硬件平台，用户可以首先使用与包转发引擎同时运行的嵌入式的病毒过滤引擎，当到达预定时间时，再升级到插入式的硬件模块从而获得更高的性能。

Anti Virus高性能网关病毒过滤解决方案

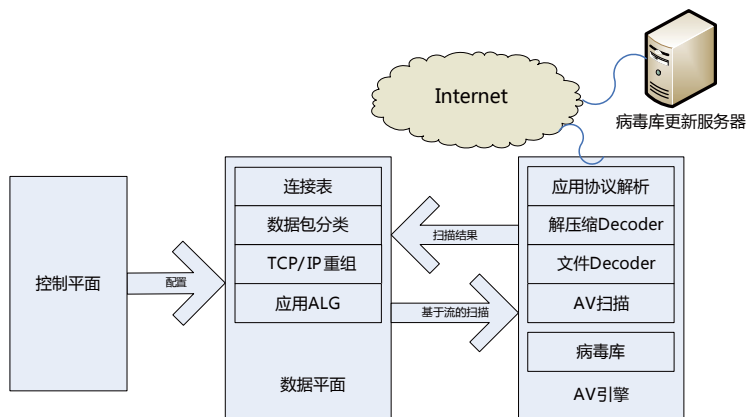


图 2: 软件架构

模块化构架也使病毒过滤功能可以灵活地与StoneOS®其它安全和网络功能相结合使用，例如基于角色的策略规则、IPSec VPN和SSL VPN。

Hillstone山石网科病毒过滤功能可以工作在透明模式、路由模式和混合模式下。

3. Hillstone山石网科病毒过滤解决方案 流扫描技术

传统的病毒过滤扫描是基于文件的。这种方法是基于主机的病毒过滤解决方案实现的，并且旧一代病毒过滤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。

并且，基于文件的扫描并不适合那些不具备足够磁盘存储空间的网关设备。设备不能处理无法存入设备内存的超大文件。能够同时存入设备内存的文件的大小对扫描产生了以下限制：设备可以同时进行的病毒过滤扫描数以及被扫描文件的大小。

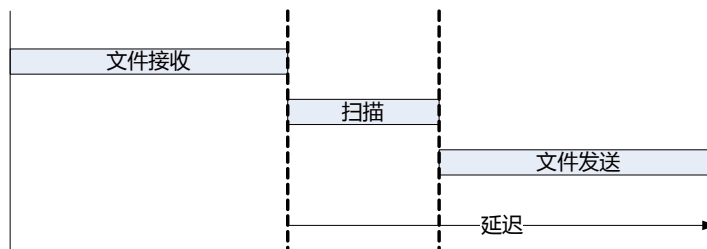


图 3: 基于文件扫描

Anti Virus高性能网关病毒过滤解决方案

Hillstone山石网科扫描引擎是基于流的，病毒过滤扫描引擎在数据包流到达时进行检查，如果没有检查到病毒，则发送数据包流。由此，用户将看到明显的延迟改善，并且他们的应用程序也将更快响应。

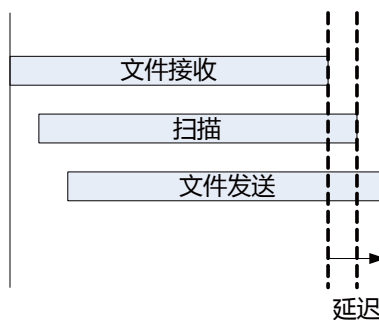


图 4: 基于流的扫描

流扫描技术仅需要缓存有限数量的数据包。它也不像文件扫描那样受文件大小的限制。低资源利用率也意味着更多文件流的同时扫描。出于对高性能、低延迟、高可升级性的首要考虑，流扫描技术适合网关病毒过滤解决方案。

流扫描技术能够在文件传输的前期发现病毒特征时终端连接，从而节省用于缓存整个文件需要的网络带宽和处理能力。当许多可能包含病毒的文件并发传输导致网关病毒扫描称为瓶颈时，这一点就显得尤其有益。

如果没有基于流的解压缩器，流扫描引擎几乎无法处理压缩文件，也就无法检测出在压缩文件里面的病毒。Hillstone山石网科提供流解压缩引擎，可以处理流行的压缩文件类型，例如ZIP、GZIP和RAR。换言之，通过Hillstone山石网科安全设备，压缩文件可以被即时解压缩和扫描。

Hillstone山石网科病毒过滤扫描是高度并行的，从而能够完全利用硬件平台的优势。

基于策略的病毒过滤功能

Hillstone山石网科病毒过滤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病毒过滤扫描，哪些用户或者用户组进行扫描，以及哪些服务器和应用被保护。

Anti Virus高性能网关病毒过滤解决方案

支持病毒过滤应用处理扩展模块

Hillstone山石网科支持的应用处理扩展模块充分保护用户投资，应用处理模块FEC-AV-30和FEC-AV-60可以提高本机应用处理能力，将病毒过滤的处理放在应用处理模块上进行，释放主机处理和运算能力，让病毒过滤不再成为性能瓶颈。同时，病毒过滤的性能上也有1倍左右的提升。

4. 结论

Hillstone 山石网科流扫描技术网关病毒过滤功能通过高性能、高并发的解决方案，满足现今低延迟应用的需求。

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

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)。