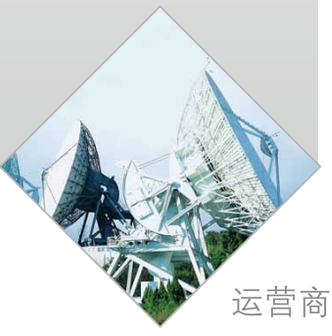
Hillstone NETWORKS

金融

教育

政府

企业



运营商

行业案例精选

Vertical Case Study

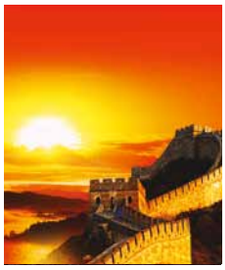
www.hillstonenet.com.cn

目 录 Content

运营商 01

金融 18

政府 36



教育 54

企业 72

公司简介

About us

2006年，参与研发世界上第一款硬件防火墙的五位业界领袖看到中国网络通讯市场的巨大发展前景，怀着“以最先进技术服务中国客户，建立世界一流网络安全厂商”的梦想，创立了Hillstone Networks。从最初的五人创始团队发展至今，Hillstone已拥有员工600余人，在北京、苏州分别成立了研发中心，建立了辐射全国的20多个分支机构，成为中国网络安全领域的领导企业。

Hillstone一直专注于网络安全领域前沿技术的研发，以“为用户打造高可靠的安全网络”为使命，秉承“客户第一、包容坦诚、诚信务实、团队协作、主动承担、精益求精”的价值观，致力于为广大用户提供高性能、可靠、易用的网络安全解决方案。

Hillstone始终把产品创新放在首位，陆续推出模块化系列多核安全网关产品和高性能数据中心防火墙产品，独创了64位全并行实时安全操作系统StoneOS，共申报了几十项专利，取得十余项国家发明专利。据国际权威市场研究机构IDC发布的2010年下半年中国IT安全硬件市场的分析报告显示，Hillstone以13.6%的市场份额占据中国UTM硬件市场第一，在重要行业客户和世界500强公司中得到了广泛的应用和部署。2012年，Hillstone因其快速增长，得到业界的广泛认可：创投界的“硅谷圣经”——《Red Herring》杂志授予Hillstone“2012全球创新百强企业”、全球知名咨询公司Frost & Sullivan授予Hillstone“2012中国区统一威胁管理市场增长领导奖”。

发展历程：

2006

- Hillstone于北京成立

2007

- 发布业界第一个基于多核硬件平台的64位实时并行安全操作系统StoneOS

2008

- 发布全系列多核安全网关产品
- 获得清华科技园“钻石企业”荣誉称号
- 荣获《计算机世界》“安全网关类2008年度产品奖”
- 荣获《IT168》“2008年度产品奖”

2009

- 发布SG系列模块化多核安全网关
- SG-6000系列安全网关首批通过中国国家信息安全产品认证（三级）
- 获得ISO9001：2008质量管理体系认证证书
- 荣获《计算机世界》“2009年度产品奖”
- 荣获《中国计算机报》“2009年度创新技术奖”
- 荣获《网络世界》“2009 UTM年度创新产品奖”
- 荣获《通信世界》“通信安全卫士奖”
- 荣获《比特网》“2009年度技术先锋奖”
- 荣获《电脑商报》“2009年度盛典产品技术应用导向产品奖”
- 荣获《E制造》“2009年度产品奖”

我们的客户

2010

- 发布100G高性能数据中心防火墙
- SG-6000系列网关通过国际IPv6 Ready Logo认证
- 以13.6%的市场份额在UTM硬件市场排名第一（IDC报告2010年下半年）
- 被评为“2010年度中国留学人员创业园百家最具成长性创业企业”
- 成为2010年度中国电信防火墙统谈分签项目入围厂商
- 成功入围腾讯IT内网防火墙采购项目
- 被评为2010中国软件影响力百强企业
- 荣获《计算机世界》“2010年度产品奖”
- 荣获《中国计算机报》“编辑选择年度产品奖”

2011

- 首次组团赴美参加RSA 2011大会
- 首次组团赴德参加CeBIT 2011大会
- 成立苏州研发和服务中心
- 成为2011年度中国移动防火墙集中采购入围厂商
- 成为2011年度中国电信防火墙统谈分签项目入围厂商
- 成功入围华为IT内网防火墙采购项目
- 荣获《网络世界》“2011年度数据中心防火墙创新解决方案奖”
- 荣获《中国计算机报》“2011年度影响力解决方案奖”
- 荣获《赛迪网》“2011年最具前瞻性安全技术奖”
- 荣获《51CTO》“2011年最佳IaaS安全技术推动者”

2012

- 荣获《Red Herring》“2012全球创新百强企业”
- 荣获《Frost & Sullivan》“2012中国区统一威胁管理市场增长领导奖”
- 成立美国研发中心
- 高性能数据中心防火墙X6150获得国际ICSA认证
- 荣获《ZDNet》“最佳数据中心防火墙奖”
- 荣获《通信世界》电信行业值得信赖解决方案供应商奖项
- 荣获《网络世界》2012年度互联网安全创新解决方案奖
- 荣获《中国计算机报》编辑选择创新产品奖
- 荣获《IT168》2012年度产品奖
- 荣获《赛迪网》2012年政府行业信息化最佳解决方案奖
- 发布业界首款32核多核安全网关M8860
- 发布高性能安全审计平台HSA
- 发布高性能多核安全网关M7860、M7260

运营商
Service Provider

典型客户名单

中国电信上海分公司
中国电信江苏分公司
中国电信浙江分公司
中国电信福建分公司
中国电信河北分公司
中国电信新疆分公司
中国电信甘肃分公司
中国电信四川分公司
中国电信山东分公司
中国电信青岛分公司
中国电信重庆分公司
中国电信宁波分公司
中国电信贵州分公司
中国电信武汉分公司
中国电信珠海分公司
中国电信福州分公司
中国电信泉州分公司
中国电信龙岩分公司

中国电信南安分公司
中国电信金华分公司
中国电信广东分公司
中国移动广东公司
中国移动浙江公司
中国移动广西公司
中国移动福建公司
中国移动四川公司
中国移动新疆公司
中国移动杭州公司
中国联通山东分公司
中国联通云南分公司
中国联通陕西分公司
中国联通甘肃分公司
中国联通青岛分公司
中国联通青海分公司
中国联通新疆分公司
中国联通福建分公司

广东广电
河北广电
内蒙广电
天津广电
浙江广电
安徽广电
江西广电
贵州广电
湖北广电
昆明广电
厦门广电
济南广电
青岛广电
扬州广电
河北铁通
陕西铁通
北京世纪互联
上海世纪互联

北京电信通
成都理想网络
宁波合通
北京中宽宏远
方正宽带
上海未来宽带
四川筹胜宽带
长城宽带
四川艾普
ChinaCache

中国电信 WAP 网关互联网出口安全防护

中国电信作为中国主体电信企业和最大的基础网络运营商，拥有世界第一大固定电话和数据宽带网络，覆盖全国城乡，通达世界各地，成员单位包括遍布全国的 31 个省级企业，在全国范围内经营电信业务。

Hillstone 通过在中国电信 WAP 网关的互联网出口部署企业安全网关 SG-6000-G5150，对中国电信 WAP 访问互联网的流量进行网络地址转换（NAT），同时对 WAP 网关进行攻击防护（DDoS），保障中国电信 WAP 业务稳定运行。

需求分析

中国电信手机用户可以通过手机中 APN（接入点网络）的设置菜单选择 CTWAP 进行数据网的服务访问，数据先经过 CTWAP 网关再出互联网，互联网出口则需要部署网络地址转换（NAT）设备，企业安全网关产品成为合适的选择。

解决方案

凭借高性能、高可靠、扩展灵活的特点，Hillstone SG-6000-G5150 企业安全网关成为用户的选择，并以旁挂的方式连接到 CE 上，通过网络地址转换（NAT）功能使手机用户能够访问互联网服务，并体现出如下的技术特点：

- **高性能的安全架构**

Hillstone SG-6000-G5150 企业安全网关是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，相比传统 ASIC 架构安全设备，其并行处理的特点带来了更高的处理能力和可靠性。

- **强大的攻击防护特性**

Hillstone SG-6000-G5150 企业安全网关能够提供全面的攻击防护能力，能够针对 DoS/DDoS 和常见攻击进行有效阻断，有效保护 WAP 网关的可用性。同时，Hillstone SG-6000-G5150 企业安全网关强大的应用层检测能力以及应用层处理性能为分析和阻挡各类攻击提供了强大的支持。

- **高可靠的冗余能力**

Hillstone SG-6000-G5150 企业安全网关能够支持 HA 网络高可靠解决方案，在本项目中使用 A-P 模式部署，为网络层提供会话级别的状态同步机制，保证在设备切换过程中数据传输的连续性及网络的持久畅通，甚至在设备进行主备切换的时候都不会中断业务的运行，保证了网络的高可靠性。

运行效果

通过在 CE 上旁挂部署 Hillstone 企业安全网关，通过网络地址转换（NAT）使得 WAP 用户能够正常访问互联网服务，同时对 WAP 网关进行攻击防护（DDoS），保障中国电信 WAP 业务稳定运行。

中国电信上海分公司 IDC 安全防护

上海电信金桥通汇 IDC 是以电信级的机房和网络资源为依托，为政府企业、应用服务提供商、内容服务提供商、系统集成商、ISP 提供大规模、高质量、安全可靠的服务器托管、租用以及 ASP 等增值服务的网络平台。

为保障 IDC 客户信息系统安全，上海电信选择 Hillstone SG-6000-X6150 数据中心防火墙部署于 IDC 网络出口，保障整体网络和客户业务安全。

需求分析

IDC 机房中部署了大量不同客户的系统和数据。对于 IDC 而言，保护客户系统与数据安全是关系到 IDC 服务质量与商业声誉的一项重要工作。从网络安全的角度，IDC 的安全需求包括:

- 高性能防护：IDC 数据中心的一个典型特点是海量的数据吞吐。超大规模、不间断运行给 IDC 机房的安全设备带来了极高的负荷，要求使用的安全设备具备大吞吐、高新建、高并发等特殊设计。
- 高可靠运行：IDC 业务的另一个特点是 7X24 小时不间断运行。IDC 机房的高可靠性是很多用户选择业务托管的一个重要原因。一旦网络出现故障，影响客户业务运行，则会带来商业损失和信誉受损，甚至法律诉讼。
- 数据有效隔离：不同客户、不同业务均对系统与数据的安全隔离有所要求，但 IDC 作为共用平台，需要提供有效技术手段进行安全区域隔离，保护系统与数据安全，为 IDC 客户提供安全信心。
- 经济适用性：IDC 业务发展通常有个过程，很难一开始便达到饱和状态，这就需要采取渐进建设策略。在安全建设时，应考虑经济适用性，挑选具有高可扩展性的设备，以便在节约当前投资的同时为将来升级留有余地。

解决方案

结合上海电信金桥通汇 IDC 自身安全建设需求与 Hillstone 在运营商行业的丰富建设经验。上海电信最终选择 Hillstone SG-6000-X6150 高性能数据中心防火墙作为 IDC 核心防火墙，保障整体网络安全与客户业务安全。

- **全并行多核架构提供高性能安全**

SG-6000-X6150 是 Hillstone 山石网科公司专门为数据中心提供的电信级高性能、高容量防火墙产品。产品采用业界领先的多核 Plus®G2 硬件架构，其分布式、全并行设计为设备提供了高效的处理能力，处理能力最高可达 100Gbps，满足数据中心 10GE 网络环境下对安全防护性能的高要求。

- **多层次可靠性设计保障连续运行**

SG-6000-X6150 采用电信级高可靠、全冗余设计。例如系统控制模块、安全服务模块等均采用了冗余、热插拔设计，配合自主研发的 64 位全并行实时安全操作系统 StoneOS 可以做到设备级（双主，主 / 备）、主控板卡级、业务级冗余，为 IDC 数据中心 7X24 小时不间断服务保驾护航。

- **虚拟防火墙实现IDC业务隔离保护**

SG-6000-X6150 支持虚拟防火墙功能，能够在单一物理设备上，为不同业务、不同客户划分虚拟防火墙，提供类似于单独物理防火墙的防护效果。既能够有效隔离客户业务数据，同时也能满足不同客户个性化的策略控制和防护需求，提升 IDC 安全服务品质和商业价值。

- **绿色节能与高可扩降低IDC运营成本**

SG-6000-X6150 具备强大的扩展能力，可用端口数量和业务处理性能可以随着接口模块和安全服务模块的增加而线性提高，从而在将来业务扩展时，降低升级成本，有效保护当前投资。同时，SG-6000-X6150 采用了业界领先的绿色节能技术，与业界同能性能产品相比，大幅降低了运行功耗，帮助 IDC 节约运营成本。

运行效果

上海电信金桥通汇 IDC 通过部署 SG-6000-X6150，依托其高性能、高可靠与强大的安全防护功能为 IDC 计算环境与客户业务系统提供了高品质的安全服务能力，在保护客户及业务数据安全的同时，也有效提升金桥通汇 IDC 商业价值及品牌美誉。

中国电信 SOC 平台安全域防护

作为中国主体电信企业和最大的基础网络运营商，中国电信拥有世界第一大固定电话和数据宽带网络，覆盖全国城乡，通达世界各地，为提升网络安全管理效能，中国电信在全国主干节点建设了 SOC 平台。

中国电信 SOC 平台域间部署的 Hillstone SG-6000-M6110 企业安全网关，为 SOC 平台的安全、稳定、可靠运行发挥作用，对 SOC 平台域间的访问进行有效的安全防护，

需求分析

中国电信通信网络和支撑系统是国家基础信息设施，从国家要求和企业自身业务的要求考虑，都迫切需要提高信息安全保障水平。为了保证中国电信的网络安全，提高中国电信的网络安全保护水平，促进中国电信的网络安全管理工作流程化，需要建设网络安全管理（SOC，Security Operation Center）平台为安全管理工作提供一个强有力的技术支撑平台。SOC 平台域间防火墙的部署是整个系统的重要组成部分。

解决方案

凭借设备高可靠、配置灵活的特点，Hillstone SG-6000-M6110 企业安全网关成为用户的选择，部署在 SOC 平台的域间，实现 SOC 平台与不同承载网之间的隔离与访问控制，同时通过 HA 的部署模式，保证了整个部署方案的可靠性，其中体现出如下的技术特点：

- **高性能的安全架构**

Hillstone SG-6000-M6110 企业安全网关是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，相比传统 ASIC 架构安全设备，其并行处理的特点带来了更高的处理能力和可靠性。

- **功能丰富的软件特性**

Hillstone SG-6000-M6110 企业安全网关是 Hillstone 推出的广泛适用于中小企业、分支机构的新一代多核安全网关系列产品，除基本的防火墙特性，还可为用户提供基于角色、深度应用安全的访问控制、IPSec/SSL VPN、应用带宽管理、病毒过滤、入侵防御等多种安全服务。

- **高可靠的冗余能力**

Hillstone SG-6000-M6110 企业安全网关支持设备级别的 HA 解决方案，能够为网络层提供会话级别的状态同步机制，保证在设备切换过程中数据传输的连续性及网络的持久畅通，甚至在设备进行主备切换的时候都不会中断会话，为 SOC 平台组网提供高可靠的网络冗余解决方案。

运行效果

通过 Hillstone 的解决方案，部署 Hillstone SG-6000-M6110 企业安全网关后，中国电信 SOC 平台域间访问得到了坚实的安全防护。同时，通过实施 Hillstone 解决方案，中国电信的信息安全和运维管理能力显著提升，安全体系建设日趋完善。

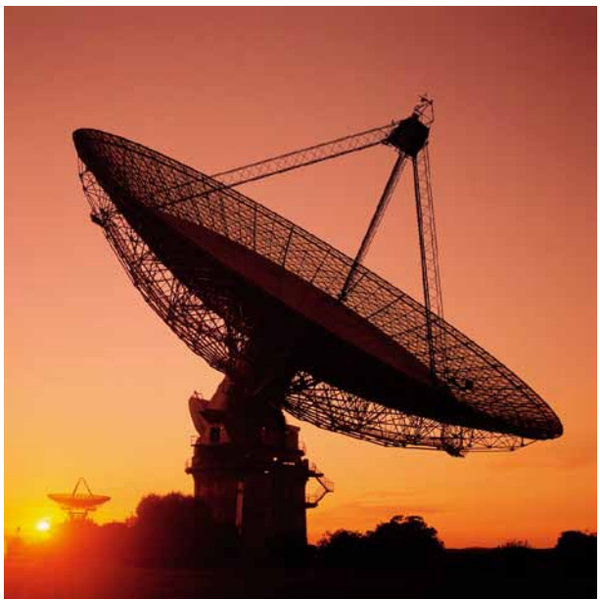
江苏电信商务领航企业客户安全防护

“商务领航”是江苏电信面向所有企业客户推出的服务品牌，将众多 IT 软、硬件产品与电信的基础通信业务和增值业务相融合，为商企客户搭建一个专业的电信级网络和服务平台，但其中安全问题成为商企客户选择“商务领航”的关键要素。

江苏电信将 Hillstone SG-6000 系列企业安全网关部署在其数据线路、专线用户的网络节点上，为企业用户提供安全、高效、有保障的宽带接入解决方案，达到保存宽带客户，增长业务收入的目的。

需求分析

江苏电信发现其企业客户的网络流量中含有大量的病毒、P2P、DDoS 攻击，造成用户关键业务无法正常运行，企业客户单独购买防病毒、入侵防御、流量控制设备的成本又很高。因此江苏电信大量采购安全网关为企业用户提供安全防护服务。



解决方案

江苏电信经过对安全网关的选型测试，最终选择了 Hillstone SG-6000 系列企业安全网关做为其商务领航项目中安全网关设备。安全网关部署在其数据线路、专线用户的网络节点上，为企业用户提供安全、高效、有保障的宽带接入全面解决方案，其中体现出如下的技术特点:

- **高性能的安全架构**

Hillstone SG-6000 系列企业安全网关是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，相比传统 ASIC 架构安全设备，其并行处理的特点带来了更高的处理能力和可靠性。

- **功能丰富的软件特性**

Hillstone SG-6000 系列企业安全网关是 Hillstone 推出的广泛适用于中小企业、分支机构的新一代多核安全网关系列产品，除基本的防火墙特性，还可为网络提供基于角色、深度应用安全的访问控制、IPSec/SSL VPN、应用带宽管理、病毒过滤、入侵防御等多种安全服务。

运行效果

通过 Hillstone 的解决方案，江苏电信为企业客户部署 Hillstone SG-6000 系列企业安全网关后，其企业客户的网络流量得到了全面的安全防护，极大提高了企业客户的网络使用体验和满意度。

福建移动 ICT 企业客户安全防护

ICT 业务是福建移动一项重要的增值业务，为中小企业客户提供高质量的信息化服务，特别是安全的 ICT 业务是福建移动在 ICT 市场的重要战略。

福建移动 ICT 项目通过采购 Hillstone SG-6000 系列企业安全网关，部署在其数据线路、专线用户的网络节点上，为企业用户提供安全、高效、有保障的宽带接入解决方案。

需求分析

ICT 即信息和通信技术，随着互联网技术的发展，企业业务运行对网络依赖程度越来越高，但面临的威胁也越来越严峻。通过分析福建移动发现其企业客户的网络流量中含有大量的病毒、P2P、DDoS 攻击，造成用户关键业务无法正常运行，企业客户单独购买防病毒、入侵防御、流量控制设备的成本又很高。因此福建移动通过采购安全网关以赠送和租用的方式为企业用户提供安全防护，以达到巩固原有客户、吸引新客户、增加业务收入的目的。

解决方案

福建移动经过长达 5 个月的产品评测选型，最终选择了 Hillstone SG-6000 系列企业安全网关做为其 ICT 项目中安全网关设备，部署在其数据线路、专线用户的网络节点上，为企业用户提供安全、高效的宽带接入全面解决方案，其中体现出如下的技术特点:

- **高性能的安全架构**

Hillstone SG-6000 系列企业安全网关是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，相比传统 ASIC 架构安全设备，并行处理带来了更高的处理能力和可靠性。

- **强大的病毒过滤功能**

Hillstone SG-6000 系列企业安全网关的病毒过滤功能集成了卡巴斯基病毒库和自研库，因此能够识别和过滤互联网中大部分的病毒，使用户在上网过程中免受病毒威胁的困扰。

- **丰富的QoS功能**

Hillstone SG-6000 系列企业安全网关在识别应用协议流量的同时，能够采用多种缓存、队列调度算法对用户带宽进行质量保障（QoS）。限制非关键业务流量如 P2P，保障关键业务流量如 VoIP、WEB，提高了用户带宽使用效率并节约了宽带费用。

运行效果

通过 Hillstone 的解决方案，福建移动为企业客户部署 Hillstone SG-6000 系列企业安全网关后，其企业客户的网络流量得到了全面的安全防护，极大提高了企业客户的网络使用体验和满意度。

长城宽带高速可靠宽带接入

作为一家成立 12 年之久的全国最大的驻地网服务企业，长城宽带在全国 30 个大中城市建立了分支机构，开展互联网接入业务，网络覆盖用户近千万。长城宽带的接入用户主要由公司集团类客户，及小区客户组成，用户对链路质量要求很高，长城宽带高度重视用户体验，特别是关注优质客户对服务的评价。

从 2009 年起，长城宽带大规模采用 Hillstone 高性能 NAT 及日志审计解决方案，通过 Hillstone SG-6000-G6100 企业安全网关，及 Hillstone 高性能日志审计系统 HSA，在提升用户体验，合理节约成本，满足监管部门要求等层面，发挥了积极的作用。

需求分析

以长城宽带的重要分支机构上海长宽为例，Hillstone 的方案和产品帮助上海长宽在合理控制链路成本，更合理的使用链路资源，保障用户上网连续性，满足监管要求等层面，起到了切实的效果。在改造前用户提出的具体的需求包括:

- **错峰上网影响链路利用率**

上海长宽接入用户的类型比较复杂，既有公司集团类用户，也有小区个人类用户，而两类人员的上网特点截然不同，公司集团类用户的上网高峰期在白天工作时间，但到了晚上上网流量很低；小区个人类用户则恰恰相反。这种特点使得两类链路都没有用满，造成浪费。

- **满足差异化服务要求**

上海长宽租用了多个运营商的多条链路，为不同级别用户提供差异性的上网接入服务，这些链路的资费、链路质量、带宽是不同的，其相对优质且高价的链路主要提供给优质用户使用。为此如何在不影响客户上网体验下，合理节约优质链路带宽，减少运营成本是上海长宽考虑的要点。

- **保障上网连续性**

上海长宽因存在多运营商多链路的状况，在 NAT 服务器的工作模式下，经常出现因链路故障，或者因 NAT 服务器工作故障，造成部分接入用户无法访问互联网的情况，影响用户满意度，甚至造成投诉以及用户流失。

- **应对监管要求**

根据公安部 82 号令要求，上海长宽需要提供可追溯日志。

解决方案

经过对比测试，长城宽带最终选择 Hillstone SG-6000-G6100 企业安全网关，作用在互联网出口，启用 NAT 和日志记录功能，以便更可靠、更有效的支持宽带接入业务的正常运营。并发挥了如下的作用:

- **错峰上网节约链路成本**

在采用了 Hillstone 高性能 NAT 及日志审计解决方案后，通过 Hillstone SG-6000-G6100 企业安全网关提供的错峰上网功能，满足了上海长宽的需求，每台 Hillstone SG-6000-G6100 企业安全网关连接了多条互联网链路，以共享的方式提供给公司集团类用户和小区个人类用户，按照预先配置的策略，在白天通过链路切换、流量控制手段，将带宽资源尽量分配给公司集团用户；晚上则按照策略自动进行切换，将带宽资源尽量分配给小区个人用户。从总体上提升了链路带宽的利用率，节约链路成本。

- **精细化带宽管理提升用户满意度**

在使用 Hillstone SG-6000-G6100 企业安全网关后，通过网关提供的基于应用的路由策略，在对应用进行深度识别的基础上，将 P2P 类应用，包括迅雷、电驴、微盘、BT 等，自动转发到非优质链路上，执行策略后发现优质链路的流量至少有近 20% 的下降，接入的优质用户也反映，在线的一些应用比以前更流畅了，而且 P2P 类应用也没有受到影响，优质用户的满意度有明显提升。

- **保障上网连续提升用户体验**

通过 Hillstone SG-6000-G6100 企业安全网关支持的链路负载均衡功能，有效提升了接入用户的上网访问连续性。在正常工作状态时，Hillstone SG-6000-G6100 企业安全网关可智能分析链路的状态，并根据链路的负载状态、带宽余量、延时状态等因素，并将访问流量根据预定义的策略分配到不同链路上；当某条链路故障，Hillstone SG-6000-G6100 企业安全网关则自动将此链路上的访问流量调整到正常链路上，从而保障了用户上网访问的连续性。

- **应对监管要求的高性能日志检索**

Hillstone 高性能日志审计平台帮助上海长宽有效应对监管要求，在上海长宽部署的单台 Hillstone 高性能日志审计平台，即可集中收集上海长宽部署的所有 Hillstone SG-6000-G6100 企业安全网关的日志，这样网络运维人员在单台设备上即可查询到所有的相关记录，加快了检索的速度，降低了汇总所需要的时间；高性能日志平台具有极高的入库速度，即使在上海长宽接入用户的访问高峰期，也能够轻松应对，做到日志无丢失，满足监管部门的要求。

运行效果

事实证明 Hillstone SG-6000-G6100 企业安全网关和高性能日志审计平台 HSA，是值得信任和依托的。Hillstone 的产品从部署至今，在高峰期 3Gbps 的流量下，仍然能够保持高性能处理能力；产品的高性能抗攻击，在几次大规模 DDoS 攻击下，仍然保障了上网的持续和稳定；产品提供的可溯源日志记录，使系统管理员实施掌握网络的安全状态，做到安全可视。

电信通高速可靠宽带接入

北京电信通是电信通在北京地区分支机构，也是北京地区最大的 ISP 运营商，市场占有率达 80% 以上，依托雄厚的出口资源，和涵盖全市大部分网吧、近万企业用户、逾十万社区个人用户的城域网链路，为用户提供稳定、高效、可靠的互联网接入服务。

为了能够更好的为企业、网吧用户提供高速、稳定的接入服务，电信通引入了 Hillstone SG-6000-X6150 数据中心防火墙，作用在互联网出口，在为接入用户提供 NAT 转换的同时，为各类上网访问提供高效、可靠、稳定的支撑，并且数据中心防火墙提供的应用流量，BGP 协议协商，可溯源日志，也为电信通的接入业务提供了有力保障。

需求分析

电信通出口一共有三类，包括:

- BGP 出口：主要由一级运营商提供地址，宣告地址，实现互联网接入访问控制。
- NAT 出口：主要由一级运营商分配地址，属于普通路由线路。
- 内部地址的 BGP 出口：主要由一级运营商代理宣告地址。

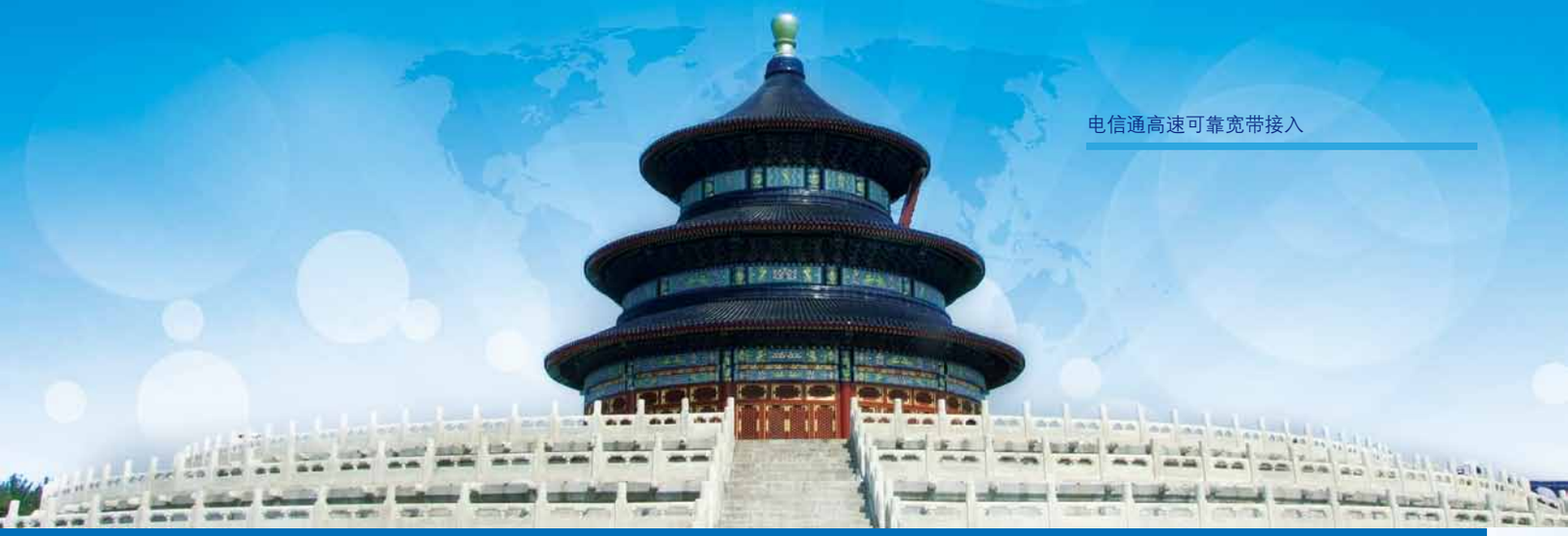
其中 BGP 出口是三种线路中费用最高的线路，通常分配给企业用户。而 NAT 出口是三种线路中费用最低廉的线路，通常分配给社区用户。具体的需求包括:

- 实现高性能的互联网接入：设备应支持几十万人同时并发访问互联网，单台设备应支持几十 G 的吞吐能力，并具有良好的新建会话支持能力，可以应对突发的访问量;
- 对流量进行识别和引流：对访问的数据量进行应用类型的识别，并通过策略路由和地址转换功能将识别出的 P2P 流量，引到廉价线路上。
- 支持 BGP 协议：接入后应支持电信通现网使用的 BGP 协议，能够参与 BGP 的协商。
- 提供有效的日志记录：审计记录在发生安全事件后能够有效追溯，满足监管要求。

解决方案

在考察了相关的技术后，从高性能、高可靠、高可扩、应用识别和基于应用的策略路由支持等角度，电信通决定选择 Hillstone SG-6000-X6150 数据中心防火墙，该设备最大可支持 100G 的大包吞吐量，和最大 5000 万个并发会话数，以及 100 万个新建并发支持能力，经过测试被证明可以支撑电信通的上网访问性能要求。

Hillstone 的 SG-6000-X6150 数据中心防火墙被部署在电信通互联网出口，即企业用户、网吧用户应用线路的三层设备之间，对接入访问进行控制，保障上网。



SG-6000-X6150 数据中心防火墙启用的安全策略包括:

- **高性能NAT**

通过 Hillstone SG-6000-X6150 数据中心防火墙强大的 NAT 功能，保障极佳的接入用户上网体验;

- **多链路负载均衡**

Hillstone SG-6000-X6150 数据中心防火墙可在多条出口链路间进行负载均衡，当某条互联网链路故障，设备可自动将通过该链路上网的用户切换到其他正常链路上，保障上网的连续性;

- **BGP协议支持**

Hillstone SG-6000-X6150 数据中心防火墙支持 BGP 协议，能够有效引入原有的 BGP 路由表，保持原有的稳定性设计;

- **应用引流**

Hillstone SG-6000-X6150 数据中心防火墙能够自动识别近千种应用，在此基础上针对不同的应用案例制定策略路由，可将 P2P 等引流到低质量低费用链路上，从而为接入用户的重要业务节约资源，同时也降低了电信通自己的运营成本;

- **日志审计**

Hillstone SG-6000-X6150 数据中心防火墙的日志审计功能，可将接入用户的互联网访问行为进行有效记录，以备后续查询和追溯，符合监管部门的相关要求。

运行效果

经过几个月的运行，Hillstone SG-6000-X6150 数据中心防火墙在电信通核心网络中，体现出很好的效果，其在 16G 的背景流量，和每秒新建 15 万并发访问的压力下，经过几个月的运行，设备表现良好，对此电信通表示认可。

此外，Hillstone SG-6000-X6150 数据中心防火墙提供的详细的上网行为日志，符合相关监管部门的要求，在多次网络安全案件的配合调查过程中，发挥了积极的作用。

四川艾普高速可靠宽带接入

作为中国最大的民营宽带服务提供商，四川艾普为全国 21 个大中城市的四百万企业和小区用户提供高速光纤上网服务，仅总部成都，四川艾普的接入用户规模就已达数十万级。

为了给接入用户提供更稳定、快捷的上网服务，同时又能够合理控制接入成本，四川艾普从 2008 年前起，分批次引入多台多个型号的 Hillstone 高性能安全网关，并全面采纳 Hillstone 高性能 NAT 及日志审计方案，提升接入用户体验、合理控制接入成本、有效应对监管方面，发挥了积极的作用。

需求分析

由于业务发展的需要，艾普网络有限公司于 2008 年初开始进行网络出口层安全的改造建设。在改造之前，艾普网络的网络出口层上统一接入部署了数十台 NAT 服务器，对内部的接入用户通过 NAT 地址转换以接入 Internet 公网。随着业务的增长，这些 NAT 服务器处理性能越来越不能继续支撑日益增长的 Internet 访问量，同时这些 NAT 服务器之间都是单独控制、独立运行，管理维护上投入的人力和时间成本很高，尤其是对于多 Internet 链路负载均衡及备份，网络攻击的防御等诸多新的网络挑战，NAT 服务器更是显得力不从心。因此，维护 Internet 边界的安全运营的需求已经成为艾普网络的重中之重。为此四川艾普决心引入更专业、更高性能、更稳定的安全网关来取代 NAT 服务器，并达到合理控制接入成本，保障上网持续以及有效应对监管的要求。

解决方案

自 2008 年起，凭借高性能、高可靠、高可扩的特点，Hillstone 高性能安全网关成为四川艾普的选择。起初，四川艾普在各链路边界处部署了多台 Hillstone SG-6000-G6100 企业安全网关，作为其安全防护的网关设备。在 2011 年 Hillstone 推出了 SG-6000-X6150 数据中心防火墙之后，艾普网络又陆续采购了三台高吞吐、高冗余、高扩展性的 SG-6000-X6150 数据中心防火墙，进一步提升了系统的总体处理性能。

这些 Hillstone 高性能安全网关的使用，为四川艾普实现了如下的支持及保障:

- **有效节约设备投入成本**

在引入 Hillstone SG-6000-X6150 数据中心防火墙后，仅用了三台即可替代原有的数十台 NAT 服务器，大大节约了设备的数量。而三台 Hillstone SG-6000-X6150 数据中心防火墙在支持数十 Gbps 互联网出口链路中，性能还有很大的裕量，为后续链路带宽的升级提供了一定的空间。

- **Full Cone NAT节约链路流量降低成本**

Hillstone SG-6000-X6150 数据中心防火墙支持的 Full Cone NAT，是 NAT 的一种模式，在此模式下当内网两台接入用户之间进行通讯时，比如进行网络游戏，或者进行 P2P 下载时，该模式可以让接入用户直接在内部进行数据交换，而不是将数据包发送到互联网，从而大大减低了四川艾普互联网链路的流量。

- **保障上网连续提升用户体验**

Hillstone SG-6000-X6150 数据中心防火墙对四川艾普运营商，多链路的特点，启用了链路负载均衡技术，来保障上网访问的连续性。在正常工作状态时，Hillstone SG-6000-X6150 数据中心防火墙可智能分析链路的状态，并根据链路的负载状态、带宽余量、延时状态等因素，并将访问流量根据预定义的策略分配到不同链路上；当某条链路故障，Hillstone SG-6000-X6150 数据中心防火墙则自动将此链路上的访问流量调整到正常链路上，从而保障了用户上网访问的连续性。

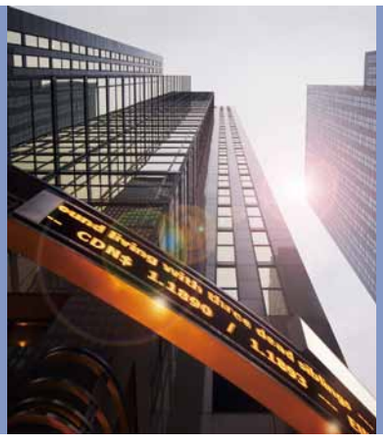
- **应对监管要求的高性能日志检索**

Hillstone 高性能日志审计平台最终帮助四川艾普解决了此问题，日志审计平台集中收集了 Hillstone 高性能 NAT 网关的日志，特别是 NAT 日志、IM 上下线日志和 URL 日志，其入库性能最高可达 100,000EPS，在四川艾普完全做到了日志无丢失；同时日志审计平台提供高速日志检索功能，日志记录平均检索时间小于 20 秒，大大降低了由此带来的运维成本。

运行效果

艾普网络全面采用了 Hillstone 的高性能 NAT 及日志解决方案后，通过 Hillstone SG-6000-X6150 数据中心防火墙，及 Hillstone 高性能日志审计平台 HSA，在有效节约宽带运营费用的同时，还有效地提升了用户上网体验，并满足了监管部门的要求。为此四川艾普表示非常满意。

金融
Finance



典型客户名单

中国人寿

中国邮政储蓄银行

深圳发展银行

上海证券交易所

中国人民银行天津分行

中国建设银行四川分行

中信银行青岛分行

广东省银监局

云南省银监局

江苏省农信社

浙江省农信联社

河南省农信社

中信万通证券

华泰证券

中融人寿保险有限公司

河南中原证券

红塔证券

厦门证券

东方证券

新湖期货

江信国盛期货

汉口银行

盛京银行

福建泉州银行

杭州银行股份有限公司

鞍山银行股份有限公司

深圳农村商业银行

镇江农村商业银行

江苏盐城市农村信用合作联社

江苏响水农村信用社

江苏贾汪农村信用合作联社

江苏建湖农信社

江苏紫金农村商业银行

江苏靖江农商行

江苏扬中农村合作银行

浙江温岭农村信用合作社

浙江瑞安农村合作银行

浙江乐清农村合作银行

浙江苍南农村合作银行

河南省平顶山农信社

人民银行清算总中心二代支付系统安全防护

中国人民银行清算总中心是为中央银行、商业银行和全社会提供支付清算及相关服务的全国性金融服务组织。清算中心维护的支付清算系统是我国重要的金融基础设施，是国家和社会资金流动的大动脉。

清算中心北京、上海、广州等多个城市处理中心的网络外联区域，通过部署 Hillstone SG-6000-G3150 企业安全网关，保护二代支付系统安全、可靠运行。

需求分析

清算中心二代支付系统引入了先进的支付清算管理理念和技术，通过丰富系统功能，提高清算效率，拓宽服务范围，加强运行监控，完善灾备系统，为参与者提供了更加先进、便捷的支付清算服务。二代支付清算系统由一系列子系统组成，包括大额实时支付系统 HVPS、小额批量支付系统 BEPS、全国支票影像交换系统 CIS 以及网上支付跨行清算系统 IBPS 等等。由于需要和各个商业银行、资金清算组织等外部金融机构互联，因此，网络的外联出口成为主要的风险集中区域。此外，二代支付系统在我国金融支付体系中的重要地位也要求其具备极高的可靠性。因此，从网络安全层面来看，其需求主要包括攻击防护、网络高可靠性支撑等。

解决方案

经过长时间的实地测试，Hillstone SG-6000-G3150 企业安全网关无论是功能或是性能均达到了客户的期望。因此，清算中心最终选择 Hillstone SG-6000-G3150 企业安全网关作为二代支付系统的出口安全防护设备，部署在北京、上海、广州等规模较大的城市处理中心节点。在 Hillstone SG-6000-G3150 企业安全网关上开启了攻击防护、访问控制、NAT 转换等功能，屏蔽各种网络攻击，过滤非法及越权访问，保障系统的安全性。同时，每个节点均采用双机 HA 部署模式，最大程度的保障了网络可靠性。

- **高性能保障业务运行效率**

Hillstone SG-6000-G3150 企业安全网关采用领先的多核平台设计，相比传统防火墙，硬件处理性能有了大幅提升。同时，在操作系统层面，StoneOS 并行设计架构使防火墙各个功能模块能够同时进行工作，充分发挥多核处理器的性能优势，使 Hillstone SG-6000-G3150 企业安全网关能够完全满足清算中心出口链路大量数据传输对防火墙的高性能要求。

- **攻击防护保障业务安全性**

清算中心网络连接着大量金融机构。因此，从风险管理的角度，加强网络出口的安全防护是重中之重。Hillstone SG-6000-G3150 企业安全网关具备丰富的攻击防护特性，除了能够抵御如泛洪攻击、地址欺骗、畸形报文等传统攻击方式外，还能够防范各种新型网络攻击，如 CC 攻击等。Hillstone SG-6000-G3150 企业安全网关强大的攻击防护特性有效保障着资金清算业务的安全性。

- **HA双机热备保障网络高可靠**

清算中心支付系统是我国现代金融支付体系中最重要的一个环节。因此，支付系统对可靠性有着极高的要求。网络作为系统运行的基础设施，必须具备不间断运行能力。本项目中，Hillstone SG-6000-G3150 企业安全网关除了设备自身具备高可靠性外，更采用 HA 部署模式。网络会话在两台设备中实时同步，即使一台设备出现故障，也能够保障网络连接不中断，满足支付系统对高可靠性的苛刻要求。

运行效果

清算中心通过在北京、上海、广州等多个城市处理中心部署 Hillstone SG-6000-G3150 企业安全网关，充分发挥了 Hillstone SG-6000-G3150 企业安全网关的高性能和丰富的攻击防护特性，从而有效保障了二代支付系统的安全、高效运行。同时，HA 高可靠组网方式也为支付系统的连续运行提供最高的可靠性保证。

深圳发展银行构建互联网综合安全防线

深圳发展银行是一家全国性股份制商业银行，在全国 20 多个经济中心城市拥有 300 多家分支机构。网上查询、网上支付转账、网上理财、网上基金买卖等全面的产品网络和可靠的安全保障，使得深发展的个人用户和企业用户，均可以全天候地体验到“穿越时空”的现代金融服务。

通过在深圳发展银行总行及各支行的互联网出口部署 Hillstone SG-6000-G2110 企业安全网关，保障了深发展办公业务系统安全和内网用户上网安全。

需求分析

深圳发展银行总行及各支行的互联网出口是保障办公业务系统安全和内网用户上网安全的关键节点。因此，如何防范来自于互联网的网络攻击及各类恶意代码，同时避免出现由于多个单一功能的安全设备串联部署而带来的单点故障风险，是深发展此次安全建设重点考虑的问题。

解决方案

多链路负载均衡、低延时病毒过滤、网络入侵防御、用户上网行为控制等功能成为深发展网络安全设备选型的主要条件。深圳发展银行经过综合比较，最终选择了 Hillstone 企业安全网关产品，通过在总行及各支行的互联网出口部署 Hillstone SG-6000-G2110 企业安全网关，实现网络出口的安全防御，有效保障了办公业务系统及内网用户的上网安全。

- **领先的安全架构实现业务高性能安全**

Hillstone SG-6000-G2110 企业安全网关是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，相比传统 ASIC 架构安全设备，其并行处理的特点带来了更高的处理能力和可靠性。

- **丰富的安全功能实现网络综合防御**

Hillstone SG-6000-G2110 企业安全网关除基本的防火墙特性外，融合了多种安全功能，可为用户提供深度应用识别控制、IPSec/SSL VPN、应用带宽管理、病毒过滤、入侵防御等多种安全功能，从而实现全面的网络安全保护。

- **高可靠性设计保障业务安全稳定运行**

Hillstone SG-6000-G2110 企业安全网关能够支持设备级别的 HA 解决方案，在深发展网络中使用 A-P 模式部署，为网络层提供会话级别的状态同步机制，保证在设备切换过程中数据传输的连续性及网络的持久畅通，甚至在设备进行主备切换的时候都不会中断业务的运行，保证了网络的高可靠性。

运行效果

深圳发展银行通过部署 Hillstone SG-6000-G2110 企业安全网关，有效屏蔽了各类恶意代码和网络黑客攻击，保障了办公业务系统和内网用户上网安全，为金融业务的正常运行提供安全支撑。

长沙银行数据中心安全防护

长沙银行成立于 1997 年 5 月，是湖南首家区域性股份制商业银行。从成立之初，长沙银行便高度重视信息化、信息安全与银行业务的协调发展、相互推动。目前，长沙银行已连续四年被银监会评为当前中国银行业最高等级的二类行。

随着长沙银行业务的快速增长，长沙银行决定建立异地灾备中心。在原数据容灾的基础上，通过系统升级和改造，实现灾备中心核心业务系统的可实时接管，达到《信息系统灾难恢复规范》第 5 级标准。在本次建设过程中，长沙银行选择 Hillstone SG-6000-X6150 数据中心防火墙，依托其高性能、高可靠、多功能，保护灾备数据中心的网络安全。

需求分析

长沙银行应用级灾备数据中心的设计目标是可实现核心业务的实时灾备。因此，网络结构设计上，灾备数据中心同时连接着主数据中心和各分支机构。同时，其信息系统应处于热备状态，并可保证银行柜面业务的实时可用。而在网络安全上，其安全需求则与主数据中心一致，实现同等水平的安全防护。典型需求包括:

- 高性能安全：金融大集中带来的最重要的变化是业务和数据的集中，各网点需要和数据中心进行实时快速的数据交换，在这过程中，还需要对网络数据进行各种安全检查和策略控制，这就需要高性能的安全设备，能够进行快速处理。
- 网络高可靠：金融业务具有一个典型的特点“3A”，即 Anytime，Anywhere，Anyhow，这就要求业务能够提供连续运行保障。安全设备作为系统运行链条中必不可少的一个环节，需要能够提供极高的可靠性保证。
- 设备可扩展：长沙银行的业务近年来增长迅速，这就要求在进行安全建设时，除了满足当前的需求，还需要考虑到未来几年业务的发展趋势，要求设备支持良好的扩展能力，能够不断升级以保护前期投资。

解决方案

经过认真选型和详细测试，最终长沙银行选择 2 台 Hillstone SG-6000-X6150 作为灾备数据中心的核心防火墙，互为热备，保护核心业务系统连续运行。

- **高性能保障海量数据安全**

Hillstone SG-6000-X6150 是一款 100Gbps 级的数据中心防火墙，采用了业界领先的多核 Plus G2 分布式硬件架构，在配置多块业务处理板卡后，整机最高可达 100Gbps 吞吐、100 万的新建连接速率和 5000 万并发连接数。完全能够满足长沙银行灾备数据中心海量数据深度识别与攻击防护的安全要求。

- **高可靠设计支撑业务连续运行**

SG-6000-X6150 采用电信级高可靠、全冗余设计。例如系统控制模块、安全服务模块等均采用了冗余、热插拔设计，配合自主研发的 64 位全并行实时安全操作系统 StoneOS 可以做到设备级（双主，主 / 备）、主控板卡级、业务级冗余。本案例中，即采用双机热备高可靠性组网技术保障长沙银行业务网络的 7 × 24 小时不间断运转。

- **高可扩为业务增长提供扩容空间**

SG-6000-X6150 具备强大的扩展能力，整机提供 10 个通用扩展插槽，最多可为用户提供 144 个千兆接口或 36 个万兆接口。此外，SG-6000-X6150 还支持安全服务模块（SSM）的扩展，业务处理性能可以随着安全服务模块的增加而线性提高。通过这些可扩展性设计，长沙银行可在业务增长时，通过增加扩展模块即可满足新的安全需求，有效保护当前投资。

运行效果

Hillstone SG-6000-X6150 是一款高性能、高可靠并支持高度可扩的数据中心防火墙，特别适用于对性能、可靠性有很高要求的数据中心场合，如金融行业数据中心。长沙银行灾备数据中心选择 Hillstone SG-6000-X6150，其优秀的性能表现与极高的可靠性，为灾备中心实时业务切换提供安全保障，使长沙银行的业务运行安全得到了提升。

中国人寿数据中心安全防护

中国人寿保险（集团）公司属国有大型金融保险企业，业务范围涵盖寿险、财产险、养老保险（企业年金）、资产管理、实业投资、海外业务等多个领域，是我国最大的、同时也是唯一一家资产过万亿的商业保险集团。

中国人寿通过在各省分公司和下属的支公司互联网出口部署 Hillstone 企业安全网关，实现网络地址转换、入侵防御、流量管理功能，保障业务安全、快速、稳定运行。

需求分析

随着中国人寿保险集团公司业务的发展，保险代理点以及保险营销员规模的不断扩展，中国人寿建设了基于互联网的业务系统，保险代理点以及保险营销员可以通过 Internet 访问中国人寿的寿险业务系统、核保核赔处理系统、新车险理赔系统、车险通赔系统、综合业务处理系统等业务系统，从而提高了各项业务的办理和运行效率。同时，为保障业务安全、快速、稳定运行，需要在业务系统互联网出口部署防火墙实现业务的安全保护。

解决方案

凭借高性能、高可靠、配置灵活的特点，Hillstone SG-6000-M6110/M6115 企业安全网关成为用户的选择，部署在中国人寿各省分公司或者下属的支公司的互联网出口，实现网络地址转换、入侵防御、流量管理等功能，体现了如下的技术特点:

- **高性能的安全架构**

Hillstone SG-6000-M6110/M6115 企业安全网关是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，相比传统 ASIC 架构安全设备，其并行处理的特点带来了更高的处理能力和可靠性。

- **强大的攻击防护特性**

Hillstone SG-6000-M6110/M6115 企业安全网关能够提供全面的攻击防护能力，能够针对 DoS/DDoS 和常见攻击进行有效阻断。同时，Hillstone SG-6000-M6110/M6115 安全网关强大的应用层检测能力以及应用层处理性能为分析和阻挡各类攻击提供了强大的支持。

- **丰富的QoS功能**

Hillstone SG-6000-M6110/M6115 企业安全网关能够对百余种网络应用，甚至包括加密的 P2P 应用和即时消息流量进行识别和标记，然后根据应用识别和标记结果对流量带宽进行控制并且区分优先级，为每个用户控制应用流量并对该用户的应用流量区分优先级，同时能够实时探测网络出入带宽的利用率，进而动态调整特定用户的带宽，为客户充分利用带宽资源提供极大的灵活性，又能保证高峰时段的网络使用性能。

- **高可靠的冗余能力**

Hillstone SG-6000-M6110/M6115 企业安全网关能够支持设备级别的 HA 解决方案，在中国人寿中使用 A-P 模式部署，为网络层提供会话级别的状态同步机制，保证在设备切换过程中数据传输的连续性及网络的持久畅通，甚至在设备进行主备切换的时候都不会中断业务的运营，保证了网络的高可靠性。

运行效果

通过部署 Hillstone SG-6000-M6110/M6115 企业安全网关后，中国人寿保险公司省分公司以及支公司信息安全保障能力得到了很大提升，实现了业务系统的安全、稳定运行，为中国人寿信息化推动业务发展的战略提供有力的安全支撑。

上海证交所建立数据中心综合安全防御

上海证券交易所作为中国证券交易的核心机构之一，对业务连续性有着极高的要求，因此希望通过加强数据中心的安全建设，提升整体业务网络的安全性和可靠性。

上海证券交易所通过在两个数据中心部署 Hillstone SG-6000-G2120 企业安全网关，实现两地数据中心的安全、可靠互联，建立起综合安全防御体系，保障数据中心业务安全稳健运行。

需求分析

随着上海证券交易所业务的日益发展和网络规模的不断扩大，面临的木马、病毒、黑客等安全威胁越来越频繁。上海证券交易所针对当前网络的安全现状，需要在现有的网络体系下建立一套可靠的网络病毒防护和入侵防御体系。

解决方案

Hillstone 通过对上海证券交易所的网络现状、安全需求进行深入分析，在不改变数据中心的原有的网络体系架构的基础上，分别在上证所两个数据中心的网络出口部署 Hillstone SG-6000-G2120 企业安全网关，搭建全面高效的病毒防护和入侵防御体系，该方案体现出以下技术特点：

- **高性能病毒过滤有效防范各种威胁**

Hillstone SG-6000-G2120 企业安全网关，对通过 HTTP、FTP、SMTP、POP3、IMAP 等协议进出网络的所有流量进行全并行流扫描，实时阻断木马、病毒、蠕虫、间谍软件通过 Web 页面、邮件等应用向内网渗透。避免网络成为病毒传播的途径，解决了网络防护和网络杀毒的问题。

- **深度应用识别有效抵御各种网络攻击**

Hillstone SG-6000-G2120 企业安全网关有强劲的处理能力，能够满足深度应用分析和攻击分析的需求，其入侵防御功能是建立在 Hillstone 新一代基于应用行为和特征的应用识别基础上，可支持针对 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，有效地保障了数据中心安全。

运行效果

上海证券交易所通过在两个数据中心部署 Hillstone SG-6000-G2120 企业安全网关，通过精准防御、快速过滤和积极攻击响应等功能，满足了数据中心网络复杂多元的攻击防护需求，为上海证券交易所日常业务的开展提供了有力的保障。

国泰君安建设互联网边界安全防线

国泰君安证券股份有限公司是国内最大的综合类证券公司之一，公司营业网点涵盖全国各省市，其风险控制、合规体系、信息技术等方面处于行业领先水平。

此次国泰君安选择 Hillstone SG-6000-M3100 企业安全网关，部署在全国各营业部互联网出口，保障营业部信息网络安全、可靠运行。

需求分析

随着营业部网络带宽的升级与各种互联网应用的出现，国泰君安需要一款能够在性能和功能上满足营业部各种网络应用需求的安全设备。例如，需要高性能以应对网络带宽升级带来的性能压力；需要多功能，包括安全防护、QoS、负载均衡等多种功能以满足复杂网络环境下的管理需求。

解决方案

经过广泛比较和深入测试，Hillstone SG-6000-M3100 企业安全网关最终以优异成绩赢得了客户的选择。国泰君安将其部署在全国各地营业部的互联网出口，以保障办公及业务系统的网络安全。在这个方案中，Hillstone SG-6000-M3100 企业安全网关除了提供强大的网络安全防护功能外，其技术优势还在于:

- **高性能从容应对网络扩容压力**

经过几年的发展，营业部的网络出口带宽已经由原来的几兆升级为几十兆，甚至一百兆。原有 X86 架构的防火墙已经成为网络中的性能瓶颈。Hillstone SG-6000-M3100 企业安全网关采用领先的多核硬件平台与全并行软硬件设计，使安全网关能够提供高性能的安全防护，从容应对网络扩容压力。

- **深度应用识别实现网络流量管控**

在办公网中，由于传统防火墙专注于网络层的防护而短于应用层的管理，因此各种不断涌现的互联网应用为网络管理带来了新的难题。Hillstone SG-6000-M3100 企业安全网关具备强大的应用识别能力，能够通过协议特征准确识别应用类型，从而帮助管理员识别各种网络流量，并通过安全网关灵活的 QoS 策略实现网络流量的有效管控。

- **智能负载均衡技术提升网络可用性**

传统出口链路负载均衡技术多是根据 ECMP 或是 ISP 路由来实现的，可用性及灵活性均有限，Hillstone 对此进行创新，提出智能负载均衡技术。在原有技术基础上，支持出站链路的动态探测，可智能识别互联网访问的最佳路径，从而在提供可用性的基础上，提升出口带宽的利用率和用户体验。

运行效果

通过在营业部互联网出口部署 Hillstone SG-6000-M3100 企业安全网关，凭借其高性能的软硬件架构和深度应用识别能力，国泰君安显著提升了各营业部的网络安全防护效果和应用管控能力，满足新环境下业务系统对网络性能、安全性和可用性提出的更高的要求。

东方证券互联网出口安全防护

东方证券股份有限公司是一家经中国证券监督管理委员会批准的综合类证券公司。成立十几年来经营能力逐年提高，资产质量保持优良，各项主要业务指标位居全国同行业前列。同时，东方证券努力完善治理结构，建立健全合规与风险管理长效机制，管理水平不断提高。

Hillstone 通过在东方证券总部和各营业部的互联网出口部署 Hillstone SG-6000-G2120 企业安全网关，为东方证券的互联网出口提供了整体的网络安全解决方案。

需求分析

东方证券总部和各营业部都需要通过 Internet 接入来为员工提供办公网终端日常上网需要。根据对网络安全的需求，需要在互联网出口处部署安全网关设备，实现数据流量的安全防护与访问控制。

解决方案

凭借高性能、高可靠、配置灵活的特点，Hillstone SG-6000-G2120 企业安全网关成为用户的选择，分别部署在总部和营业部的互联网出口，提供了整体网络安全解决方案，同时体现出如下的技术特点：

- **高性能的安全架构**

Hillstone SG-6000-G2120 企业安全网关是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，相比传统 ASIC 架构安全设备，其并行处理的特点带来了更高的处理能力和可靠性。

- **强大的攻击防护特性**

Hillstone SG-6000-G2120 企业安全网关能够提供全面的攻击防护能力，能够针对 DoS/DDoS 和常见攻击进行有效阻断。同时，Hillstone SG-6000-G2120 企业安全网关强大的应用层检测能力以及应用层处理性能为分析和阻挡各类攻击提供了强大的支持。

- **丰富的QoS功能**

Hillstone SG-6000-G2120 企业安全网关能够对百余种网络应用进行分类，甚至包括对加密的 P2P 应用和即时消息流量进行识别。此两种设备首先根据流量的应用类型对流量进行识别和标记，然后根据应用识别和标记结果对流量带宽进行控制，同时能够实时探测网络的出入带宽的利用率，进而动态调整特定用户的带宽，为客户充分利用带宽资源提供极大的灵活性，又能保证高峰时段的网络使用性能。

- **高效的链路负载均衡功能**

Hillstone SG-6000-G2120 企业安全网关支持 ECMP、ISP 路由等多种链路负载均衡算法，自动调度流量，向各条链路上进行分配，达到流量负载均衡的效果，大大提升链路资源的使用效率。

运行效果

部署 Hillstone SG-6000-G2120 企业安全网关后，东方证券总部及营业部的互联网出口网络安全得到了很大的保障。同时，使得东方证券整个网络安全及管理上了新的台阶，安全水平提升到了更高的层次。。

太平保险银保通安全防护

太平保险 1929 年 11 月 20 日始创于上海，是一家全国性的国有金融保险集团，业务范围包括各种财产保险、意外险、短期健康险及再保险业务，国家法律、法规允许的各类保险业务和资金运用业务。

太平保险银保通系统是为了实现银行柜台代理销售保险产品而开发的 IT 系统，银行和保险公司通过系统互联实现在线核保、实时出单，是一种重要的保险销售渠道。为保证系统安全，太平保险选择 Hillstone 企业安全网关打造安全银保通。

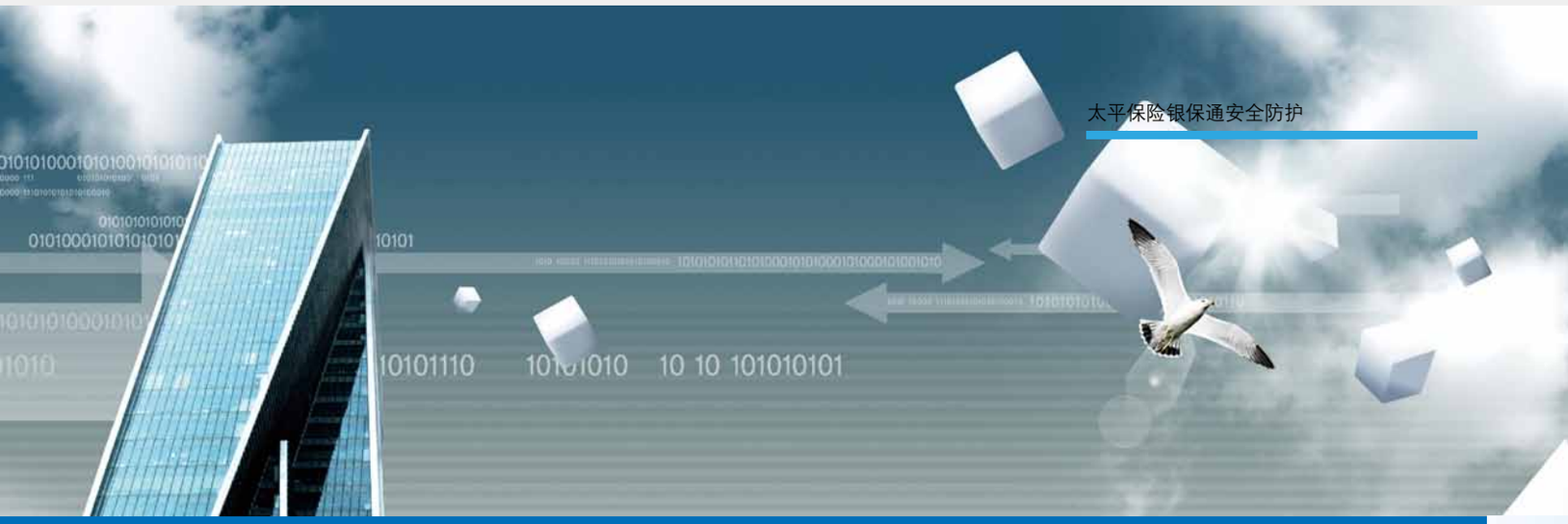
需求分析

银保通系统是保险公司和银行的连接桥梁，一端连接着银行的综合业务系统，另一端连接着保险公司的核心业务系统，运行时，投保单数据经保险公司系统核保后，银保通系统将承保信息通过网络及时传递给代理银行，由银行业务终端直接为投保人打印出保险单，该系统拓展了保险销售渠道，简化了投保过程。但作为一个中间系统，对保险公司和银行端来说，均存在一定的安全风险，需要采取相应措施。

- 业务安全多维度保障 银保通系统涉及投保客户敏感信息，同时与保险公司、银行的核心业务系统均有通信连接，因此在安全性上，有着较高要求，需从多个层面、多个维度进行威胁过滤和安全控制。
- 业务运行可靠性保障 各分支机构银保通系统与总部数据中心之间采用专线连接，网络可靠性主要取决于安全网关设备的可靠性，因此为保障业务连续运行，安全网关应当具备高稳定性与可靠性。

解决方案

太平保险经过多方考察及严格测试，最终选择 Hillstone SG-6000-M3100 作为分支机构银保通系统的边界安全网关，各安全网关和总部之间通过专线连接，从而使全公司银保通数据从柜台到核心共享服务中心上下贯通。



- **高性能满足业务快速处理要求**

传统安全网关虽然实现了多种安全功能在一个平台上的集成，但限于 X86 架构，无法实现高性能的安全。Hillstone 企业安全网关则采用了先进的 Plus®G2 多核硬件平台以及 64 位 StoneOS 操作系统，通过软硬件全并行处理，大幅度提升多功能安全网关的硬件处理性能，满足业务快速处理要求。

- **多功能实现业务综合安全防御**

Hillstone SG-6000-M3100 融合了多种安全功能，除了基础防火墙功能外，还包括深度应用识别、IPS、AV、URL 过滤等多种安全检测与防护技术，能够全方位、多维度屏蔽各种网络安全威胁，包括黑客及恶意代码攻击，保护保险公司及银行核心业务系统免遭安全威胁。

- **高可靠设计保障业务连续运行**

可靠稳定性是金融行业业务系统的基本要求，Hillstone SG-6000-M3100 企业安全网关的硬件平台及操作系统均采用高可靠设计，历经市场广泛检验。其分布式硬件及软件设计提供了底层可靠性保障，结合端口 Bypass 功能与 HA 组网技术，完全能够满足金融业务的高可靠性要求。

运行效果

本项目中 Hillstone SG-6000-M3100 优秀的产品设计和完善的安全防护解决方案，有效保障了银保通业务的安全快速运行。其基于应用识别的安全检测技术与灵活、人性化的管理方式设计，在简单管理的基础上，实现了高效、可靠安全。

政府
Government

典型客户名单

中国国家气象局
中国国家海关总署
中国国家疾病预防控制中心
国家互联网信息中心
黄河水利委员会
北京市气象局
北京市环保局
上海市财政局
上海市公安局
上海市铁路公安局
上海市药监局
上海市绿化管理局
江苏省办公厅
江苏省信息中心
江苏省机要局
江苏省财政厅
江苏省地税局
江苏省工商局
江苏省质监局
江苏省检察院
江苏省互联网管理中心
广东省信息中心
广东省财政厅
广东省出入境检验检疫局
安徽省经济信息中心
山东省政府
山东政法委
山东省党务网
山东省林业局
山东省卫生厅
山东省民政厅
山东省委组织部
山东省环保厅
山东省质监局
江西省人保厅
江西省水利厅
江西省数字证书认证中心
陕西省交通厅
福建省高级人民法院
河南省政府
云南省公安厅
云南省电子政务
辽宁省环保厅
辽宁省政府采购中心
浙江省电子政务网
浙江省测绘局
浙江省工商局
浙江诸暨市政府
浙江桐乡市市政府
浙江宁波市工商局
浙江宁波市发改委
新疆公安厅
湖北省公安厅
湖北省财政厅
湖北省高法
湖北省农业厅
吉林省卫生厅
四川省档案馆
四川省宜宾市信息中心
江苏南通市政府
江苏南通市公安局
江苏南通市水利局
江苏泰州市政府
江苏宿迁市政府
江苏连云港市政府
江苏常州市政府
江苏昆山市政府
江苏昆山市财政局
江苏张家港市政府
江苏张家港国家税务局
江苏苏州工业园区管委会
江苏苏州新区管委会
江苏苏州市卫生局
江苏苏州市地税局
陕西省榆林市卫生局
广东珠江海市公安局
山东省滨海市公安局
广东省惠州市政府
广东省广州市审计局

中国气象局提升核心业务安全

中国气象局是国务院直属事业单位，经国务院授权，承担全国气象工作的政府行政管理职能，负责全国气象工作的组织管理。

Hillstone 通过部署 SG-6000-G6100 企业安全网关对服务器区域进行安全防护，抵御外网的恶意入侵，保证气象信息的收集和发布等业务顺利进行。

需求分析

中国气象局服务器区中部署着气象信息、天气预报、卫星监测、应急预案等系统，近几年，经常受到来自互联网的 DDoS 攻击，影响网络通讯或者服务器的对外服务，严重时导致卫星气象信息不能正常接收，气象数据不能正常对外发布。因此，如何有效防护来自外网的恶意攻击，成为用户迫切的需求。

解决方案

中国气象局服务器区两条 ISP 链路分别连接华星机房和中关村数据机房，带宽为 450Mbps。华星机房链路为主链路，中关村数据机房链路为备份线路，每条链路分别部署一台 Hillstone SG-6000-G6100 企业安全网关，进行安全防护。该方案体现出如下技术特点:

- **入侵防御有效解决网络攻击问题**

Hillstone SG-6000-G6100 企业安全网关对不同网络节点的流量进行 2—7 层的分析，在定位异常流量后进行有效处理，从而快速消除异常流量造成的危害。Hillstone 的入侵防御功能提供了强大的抗攻击能力，能够充分满足中国气象局对网络攻击防护的需求。

- **应用层检测增强安全防御效果**

Hillstone SG-6000-G6100 企业安全网关提供全面的防攻击能力，能够针对 DoS/DDoS 和常见攻击进行有效阻断，同时还能够针对零日攻击进行及时的判断和阻断，有效保护用户的网络安全不受侵害。此外，Hillstone 强大的应用层检测能力以及应用层处理性能为分析和阻挡各类攻击提供了强有力的支持。

运行效果

Hillstone SG-6000-G6100 企业安全网关经受住了高强度的 DDoS 攻击，保障服务器区信息系统与网络的正常运行，设备部署以后未发生因攻击而导致网络中断或者服务中断的事件，为中国气象局业务系统的正常运行提供了安全保障。

助力国家疾控中心等保建设

隶属国家卫生部的中国疾病预防控制中心（简称国家疾控中心），高度重视信息化建设，经过多年建设形成三大类应用，涵盖全国各级疾控中心重要业务的大型信息网络。2011 年，国家疾控中心在昌平新址重新构建了网络、安全系统及配套基础设施，并进行了等级保护的相关检查与测评，根据检查结果，2012 年国家疾控中心实施了相关的整改工作。

Hillstone 提供的企业安全网关，综合运用多种安全技术，符合等级保护综合防御的建设原则。在国家疾控中心等级保护整改项目中，Hillstone 企业安全网关被运用在疾控中心的免疫规划信息系统和办公网系统内，实施综合防御，在网络安全层面帮助用户达到等级保护三级所要求的内容。

需求分析

国家疾控中心网络安全建设项目的目标非常明确，就是通过引入综合性的安全设备，在防护能力上使国家疾控中心信息系统达到等级保护三级要求的高度，同时也为国家疾控中心重要的业务信息系统提供完善的保障，提升系统的访问控制、对抗攻击、防范恶意行为的能力。

从符合等级保护，和保障业务连续性要求的两个角度，国家疾控中心提出了如下的安全需求:

- 综合安全防御：等级保护的网络安全建设内容涉及网络结构安全、网络控制、网络审计、入侵防御、恶意代码防范等多条要求，为此需要引入多种安全技术，更多地覆盖上述建设要求;
- 保障业务安全性：疾控中心免疫规划信息系统是国家疾控中心的核心应用，面向全国各级疾控业务工作人员，实现关键业务的操作。免疫规划信息系统对业务连续性、安全性的要求很高，需要采取综合性的防御技术进行保障，确保国家疾控中心正常业务的开展;
- 提升系统对异常的检测能力：通过持续化的安全检测与流量监测手段，对疾控中心业务活动状态进行实时监测，并对异常能够快速报警;
- 监控员工上网行为：对疾控中心业务人员访问互联网的行为进行有效管控，限制访问非法网站，并对互联网的攻击、病毒等行为实施阻断，保障受控上网。

解决方案

根据国家疾控中心在满足等级保护要求，保障业务安全，控制上网行为等层面的需求，Hillstone 进行了详尽的沟通与设计，采用具有多种安全防护功能的 Hillstone 企业安全网关，分别作用在疾控中心关键业务服务器的边界，以及疾控中心互联网边界，实现综合性的防护，在网络安全层面满足等级保护的相关要求，同时严密的安全防护功能也保障了关键业务的安全性，以及疾控中心员工访问互联网的合规性。

在国家疾控中心信息网络中，Hillstone 企业安全网关部署在两个位置：其中两台 SG-6000-M8860 企业安全网关被部署在免疫规划信息系统的服务器区域边界，综合启用防火墙、入侵防御、病毒过滤、VPN 等功能，保障关键的业务安全性；两台 SG-6000-X5100 企业安全网关被部署在疾控中心互联网出口，重点对员工上网行为进行有效监控，启用深度识别防火墙、URL 过滤、病毒过滤、入侵防御等功能，杜绝员工的非法上网访问。四台 Hillstone 企业安全网关发挥了如下的安全作用。

- **综合防御符合等级保护要求**

Hillstone 企业安全网关在网络结构安全、网络访问控制、网络访问审计、入侵防御、恶意代码阻断、数据安全传输保障等层面，分别提供了防火墙、入侵防御、病毒过滤、VPN、安全审计等技术，充分满足等级保护三级在网络安全层面提出的建设要求。

- **保障业务安全性**

针对本次项目安全建设的重点，免疫规划信息系统，在其服务器区域出口节点上部署的 Hillstone SG-6000-M8860 企业安全网关，启用的多种安全技术，实现了层层防御，访问控制技术限制了其他终端对业务系统的访问，入侵防御有效检测并阻断了恶意入侵行为，病毒过滤则将恶意代码排除在服务器区域外，VPN 则为远程的访问提供加密传输保护，综合的技术增强了免疫规划信息系统的抗攻击能力。

- **高性能安全异常检测**

Hillstone SG-6000-M8860 企业安全网关具有极高的性能，最大可支持 40Gbps 的吞吐量，在此基础上提供了多种安全检测技术，综合运用特征匹配、行为识别等技术，能够更有效的防范对国家疾控中心关键业务的攻击。

- **上网合规性保障**

部署在疾控中心互联网出口的 Hillstone SG-6000-X5100 企业安全网关，对员工的互联网访问进行深度检测与控制，限制员工访问非法网站、防止互联网的病毒传入疾控中心，有效抵抗来自互联网的恶意攻击等，从而保障了疾控中心上网访问的合规性。

运行效果

Hillstone 企业安全网关被部署在疾控中心关键业务节点后，进行了一段时间的试运行，设备运行稳定，提供的各类安全报表也符合了疾控中心安全运维的要求，同时系统支持的各种功能，为疾控中心的安全防护发挥了积极的作用，在等保检查中，也被监管部门认可能够达到相关政策要求。

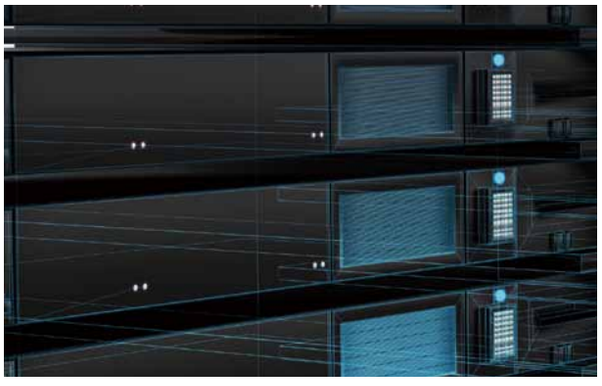
云南省电子政务综合安全防护

作为国家电子政务外网一期工程的组成，云南省电子政务外网要进行纵向拓展部署，按照分域管控原则，综合运用多种安全技术，对政务外网实施安全防护。

Hillstone SG-6000-M6115 企业安全网关，运用包含访问控制、入侵防御、VPN、病毒过滤、带宽管理等多种安全技术，为云南电子政务网提供有效隔离和安全管控。

需求分析

参照国家电子政务外网建设意见的规定，云南省电子政务外网建设的安全规划是：以省政务外网平台建设为核心，构建省到州（市）及州（市）到县（区）平台的广域网联接，同时，采用综合防护技术，针对互联网出口、核心业务服务器边界，实施有效隔离和安全管控，保障政务业务的连续性和政务数据的安全性。



解决方案

Hillstone 的解决方案是通过在省级的 VPN 平台接入区、省级 3G 无线平台接入区，省级公共服务器群区以及十六个州（市）级的互联网区域统一部署 Hillstone SG-6000-M6115 企业安全网关。使用 VPN 技术建立专网，为省与州（市）之间的各种业务、数据交互及通讯提供安全保障；同时，开启访问控制、入侵防御、病毒过滤等功能来为服务器区域及不同安全域之间实施有效隔离与管控。本方案体现出如下技术特点:

- **专业的VPN技术保证安全互联**

Hillstone SG-6000-M6115 企业安全网关支持的 VPN 技术利用隧道、加密、认证等特性在互联网上组建专网，可以有效避免重要数据被非法截获破解，保证政务信息在整个 VPN 网络中安全传输。

- **安全隔离与控制保护业务安全**

Hillstone SG-6000-M6115 企业安全网关通过划分安全域对服务器等重点区域进行隔离和管控，通过基于角色和身份认证的访问控制分配网络资源，进行日志审计，对业务访问实现更为全面的保护。

- **深度攻击检测防范恶意攻击**

Hillstone SG-6000-M6115 企业安全网关可在深度应用识别的基础上，针对特定应用行为和特征进行攻击检测与防护，可有效防范互联网黑客的攻击，避免服务器瘫痪；对恶意攻击行为进行阻断，保障政务网络的安全。

运行效果

Hillstone SG-6000-M6115 企业安全网关的部署，有效保证了不同地域电子政务平台之间的数据传输安全，为省核心业务服务器提供了业务隔离和防护，为整个云南省电子政务外网的安全防护提供了全面而高效的安全保障。

福建省人民法院政务网安全防护

随着福建省人民法院系统信息化建设不断深入，网络规模的不断增长，原有的安全保护系统已经无法充分覆盖各个节点，因此需要部署安全设备对于增加的节点进行防护。

Hillstone 针对三级专网系统中所有基层法院以及未进行安全部署的厦门海事法院进行安全防护，通过设置合理的安全防护策略，保障广域专网安全。

需求分析

福建省法院三级广域专网由各市中级人民法院与所辖各基层人民法院联网组成，均采用星型网络架构。本次安全建设就是需要将原本网络安全设备没有覆盖到的二级和三级节点进行完善，同时考虑各基层法院及海事法院的安全管理，具体需求如下:

- 各基层法院和上级中院之间网络资源的访问控制
- 厦门海事法院和省高院之间网络资源的访问控制
- 实现对安全网络有效便捷的管理维护

解决方案

针对福建省人民法院广域专网的网络结构和安全需求，Hillstone 通过在各基层法院出口和海事法院出口前部署 Hillstone SG-6000-M3105 企业安全网关，同时在省高院网络中心部署一套 HSM 安全管理平台，来满足网络安全防护需求，该方案体现出如下技术特点:

- **基于应用的访问控制实现信息合法传播**

通过 Hillstone SG-6000-M3105 企业安全网关支持的深度应用识别技术对业务应用进行细分，根据不同部门的业务需求，配置基于应用的安全策略进行控制，杜绝非授权的访问行为，严格控制信息资源的传播范围

- **攻击防护抵御恶意攻击**

Hillstone SG-6000-M3105 企业安全网关可在深度应用识别的基础上，针对特定应用进行攻击检测与防护，能够针对 DoS/DDoS 和常见攻击进行有效阻断，有效保护用户的网络安全不受侵害，大大提升了二级和三级节点信息网络的抗攻击能力。

- **集中管理平台整合安全网络管理**

提供对部署在各基层法院和厦门海事法院的 Hillstone SG-6000-M3105 企业安全网关设备的管理维护，使设备保持一致的安全定义和策略应用，提高整个系统的安全级别，达到动态安全防护。

运行效果

福建省人民法院部署 Hillstone SG-6000-M3105 企业安全网关和 HSM 安全管理平台，其中安全网关的访问控制和攻击防护等功能有效解决了法院网络的安全问题。而 HSM 平台通过对海量日志的集中收集和深度挖掘，提升对安全事件的分析能力；集中的策略配置，增强对安全事件的快速响应能力。

山东省民政厅搭建民政系统安全网络

作为“金民工程”的二期工程，山东省民政厅信息网络建设在近些年得到快速发展，为更好地保障民政业务的稳定开展，山东省民政厅规划了以数据加密、访问控制、病毒过滤、攻击防护为主的全面安全保障体系，而 Hillstone 企业安全网关，在单台设备上融合多种安全技术，可满足安全保障体系的所有需求，成为山东省民政厅安全建设的必然选择。

需求分析

山东省民政系统网络不仅要实现各地市民政局、区县民政局与省厅服务器之间的安全互联，保证数据的安全传输；对于服务器区域的访问控制、攻击防护等防护监管措施也是十分必要。同时，省民政厅办公网以及各地市区县的内部网络，也需要高效的病毒防护和网络流量、上网行为的管控。

解决方案

Hillstone 的解决方案是通过在省、各地市、各区县的民政单位网络出口处部署高性能安全网关，使用 VPN 技术建立专网，为省厅与各区县、市局之间的各种业务、管理和相关通讯提供安全保障；同时，开启访问控制和攻击防护等功能来保护省厅核心区的服务器安全；通过 Hillstone 企业安全网关为接入互联网的民政单位办公网提供安全的上网保障。本方案体现出如下技术特点:

- **专业的VPN保证远程互联安全**

在 Hillstone SG-6000-M2105，SG-6000-M6110，SG-6000-G3150 企业安全网关上启用 VPN 功能。VPN 技术利用隧道、加密、认证等特性在互联网上组建虚拟专网，可以有效避免政府重要数据被非法截获破解，保证山东省民政厅信息在整个 VPN 网络中安全传输。

- **高可靠冗余部署提升业务连续性**

在省厅的互联网出口处放置两台 SG-6000-G3150 企业安全网关以冗余架构部署，主设备将会话状态等信息实时的通过 HA 接口同步给备份设备，使两台设备间的会话表、状态信息及配置等保持一致。一旦主设备出现异常会立即将网络流量切换到备份设备，切换过程中会话不会中断，网络传输正常。

- **区域隔离保护资源安全**

在 Hillstone SG-6000-M2105，SG-6000-M6110，SG-6000-G3150 企业安全网关上划分安全域，将内部员工、服务器、VPN 安全区逻辑分开；通过访问控制策略保证各地市民政局对省厅服务器的分权限访问。

- **流量管理和病毒过滤防范恶意攻击**

流量管理功能可以对关键业务的网络应用提供带宽保证。病毒过滤功能可以对内外网的病毒进行过滤与查杀，有效防范蠕虫、木马等网络型病毒，并配置日志服务器，记录完整的病毒攻击行为。

运行效果

通过部署 Hillstone 企业安全网关，解决了山东省民政厅 VPN 高速互联的需求，使得各地之间形成虚拟的局域专网，实现了各单位数据应用的集中存储和集中管理，保证数据的安全。同时也做到了精确的应用监控和高效的带宽管理，为民政厅提供了高效、安全、可靠、舒适的网络环境。

江苏省工商局移动执法安全数据传输

随着移动应用的普及，越来越多的政务系统采用移动技术，实现全天候的政务处理，江苏工商局移动执法系统及时在这样的背景下产生的，经过了两期的建设，全省工商工作人员使用配备的专用工商移动监管执法终端（下简称“执法终端”，包括智能手机终端和笔记本电脑终端），通过基于安全的 3G 移动通信网络接入平台，访问到省市两级工商政务平台，实时地进行各类工商内网业务系统、办公系统的相关业务处理。

而对于移动政务应用，由于数据在公共网络中传输，因此对于涉及到敏感的工商监管数据，很容易遭到窃听和非法篡改，为此 Hillstone 企业安全网关提供的 SSL VPN 能够很好的为数据传输提供保护，对于使用笔记本电脑及智能手机进行移动执法的人员，能够对数据进行机密性和完整性保障；此外，企业安全网关支持的防火墙、防病毒、流量管理等功能，在部署到江苏省工商局的省级和地市节点，为工商信息系统也提供了有效的安全保护。

需求分析

江苏工商移动监管执法系统从 2009 年开始在全省范围内部署实施。移动通信网络采用中国电信 CDMA 移动通信网络系统，执法终端采用了 Dopod S900c，执法终端操作系统是 Windows Mobile，信息网络覆盖到省局、地市局、区县局以及工商所（分局）四级，在安全建设层面，江苏省工商局提出的建设目标有：

- 数据传输安全性保护：对于使用笔记本电脑及智能手机进行移动执法的访问数据包，进行机密性和完整性的保护，有效防范数据在公共通信网络中被窃听和篡改的风险；
- 有效的接入认证：对于远程接入的移动终端，应进行有效的认证，并且根据访问目标的重要性差异，采取不同强度的认证手段，防范非授权的接入以及伪造身份接入访问行为；
- 保护关键的政务应用：对于省、市级节点的工商移动监管执法系统，由于其通过公共互联网提供给移动设备访问，因此有必要在其边界采取隔离措施，并实施有效的访问控制、病毒过滤，防止非法的外部访问，同时限制病毒、攻击等外部威胁；
- 集中管理：部署的安全设备应支持集中化的管理，在省级节点通过一台设备，即可实现对部署在市级节点，以及各县级节点的多台企业安全网关的集中管理，包括日志的集中收集与统计，安全策略的统一配置。

解决方案

由于在一期的试点项目中，用户已经使用了 Hillstone 的企业安全网关，并且运行良好，这对于后续的项目发挥了积极的推动作用，而本次项目中，用户从性能、功能的角度进行了全面的对比后，Hillstone 企业安全网关提供的强身份认证、SSL VPN、防火墙、AV、IPS、QoS 等功能得到用户的认可，成为江苏省工商移动执法系统安全防护的选择。具体的部署方法示意如下：

江苏省工商移动执法系统的一期工程在无锡进行了试点，当时共部署了 30 套 Hillstone SG-6000-G3150 企业安全网关，部署在市、县级工商部门移动执法系统的网络出口，二期工程扩展到全省，包含省局及 11 个地市局，共 12 套 Hillstone SG-6000-G3150，后续还将持续进行采购，确保每个节点都为双机运行。部署的企业安全网关在江苏省工商移动执法系统中发挥了如下的安全作用:

- **强身份认证保障系统接入安全**

Hillstone 企业安全网关支持多种认证技术，即包括简单的用户名 / 口令认证，还支持双向数字证书认证、动态口令认证和双因素认证等更可靠的认证机制，在本次项目中，对于重要的工商移动执法系统，安全网关整合了工商局已有的数字认证技术，实现对移动接入用户的身份识别与控制。

- **SSL VPN实现数据安全传输**

Hillstone 企业安全网关支持的 SSL VPN 功能，在移动终端上配置客户端，建立 VPN 隧道，对访问工商移动执法系统的数据包进行机密性和完整性保障，使移动终端在通过 3G, 以及公共互联网访问过程中，避免数据遭到窃听和篡改，确保正常的移动执法。

- **多种技术保障关键应用安全**

Hillstone企业安全网关在江苏省工商局的省、市级平台，分别被部署到各级节点的服务器区域与运营商公共互联网之间，开启防火墙、病毒过滤、IPS 以及 QoS，严格控制外部的访问，并对病毒、攻击行为进行有效过滤，同时也对不同类型的业务访问流量进行有区别的限制，从而保障了关键政务应用系统的安全性。

- **集中安全管理提高管理效率**

在省工商局部署的 Hillstone 集中管理平台，可对全网部署的所有 Hillstone 企业安全网关实施集中化的管理，包括日志的集中查询统计，以及全局性策略的集中下发，集中管理提高了省工商局对安全事件的检索和响应效率，更好地保障安全防护的效果。

运行效果

集成了强身份认证、SSL VPN 数据安全传输、综合安全控制与防御等技术的 Hillstone 企业安全网关，在部署后对江苏省工商移动执法系统实施了有效的保护，实现了认证、加密、控制、防护为一体的远程安全访问方案，在一期的无锡试点中便收到很好的效果，在本期项目中更是进一步完善了安全覆盖的广度和深度，实现更全面的安全防护。

江苏省质监局纵向政务网安全防护

江苏省质监局全省政务纵向网络是国家“金质”工程的重要组成，目前已经实现了省、市、县三级政务节点的互联互通，依托政务网络开展质量管理、认证认可、质量监督、食品监管、标准化、计量管理和特种设备等业务。

Hillstone 企业安全网关部署在江苏省质监局全省政务纵向网各个节点，对重要的业务应用系统进行隔离，并启用防火墙、防病毒、IPS、流量管理等安全功能，为应用系统安全可靠运行提供保障；同时各节点部署的 Hillstone 企业安全网关启用 VPN 功能，对纵向政务网上传输的访问数据进行机密性、完整性保障，防止重要的政务访问被窃听或重要的数据被非法篡改；在江苏省质监局门户网站的互联网出口，部署的 Hillstone 企业安全网关，启用防火墙、抗攻击等功能，阻止来自互联网的非法或异常访问行为，保障门户网站的正常运行。

需求分析

江苏省质监局政务纵向网的安全建设经历了两期的建设，一期项目包含省质监局和 13 个地市质监局，分别部署了 Hillstone SG-6000-G3150 企业安全网关，Hillstone SG-6000-G2110 企业安全网关；二期项目是一期项目的延续，包含各个县质监分局，需要的安全措施包括:

- 综合安全防护：类似于一期项目，用户提出需要引入具有综合防护技术的安全设备，能够为县质监分局节点的网络和应用系统提供更完善的保护；
- 数据安全传输：部署在县质监分局节点的安全设备，应能够支持 VPN 功能，能够与一期项目中部署的设备实现 VPN 互通，从而保障质监政务纵向网上传输数据的机密性和完整性，防范被非法窃听或篡改数据；
- 简单易用：由于二期项目的安全设备要被部署到各个县级节点，而江苏省质监局县级节点的专业网管人员比较匮乏，因此用户期望设备的管理和维护应尽量简单，策略更易于配置和检查；
- 集中管理：部署的安全设备应支持集中化的管理，在省级节点通过一台设备，即可实现对部署在市级节点，以及各县级节点部署的多台企业安全网关的集中管理，包括日志的集中收集与统计，安全策略的统一配置。

解决方案

经过性能、功能、易用性、集中管理等方面的对比，特别是基于一期项目中部署的 Hillstone 企业安全网关稳定运行的基础上，用户最终选择了 3 套 Hillstone SG-6000-M6110 企业安全网关，及 67 套 Hillstone SG-6000-M3100 企业安全网关，全部部署到各个区县的质监分局节点，进行有效的隔离和防护，两期项目中整体的部署结构如下图所示:

在二期项目中还引入了 Hillstone 集中管理平台 HSM，实现对全省部署的所有的 Hillstone 企业安全网关的集中管理，部署的安全设备为江苏省质监局政务网络提供了如下的保护:

- **综合防御保障边界安全**

部署的 Hillstone 企业安全网关，在一台设备上即实现了防火墙、防病毒、IPS、流量管理等功能，实施综合防御。防火墙为各类应用系统提供严格的访问控制，限制非法访问；在访问控制的基础上，防病毒过滤功能对进入或流出县级节点的数据包实施深度检测，过滤其中的病毒，同时也防止某个县级节点感染病毒后在全省范围内蔓延；启用的 IPS 功能则有效防范了攻击行为；流量管理功能则对各县级节点的业务访问进行控制，保障在多个县级节点同时访问业务时，每个节点都能够分配到一定的带宽，确保业务连续。

- **VPN实现数据安全传输**

各县级节点部署的 Hillstone 企业安全网关，启用 VPN 功能，与部署在地市节点的Hillstone企业安全网关配合使用，对县级节点发出的业务访问数据包实施有效的机密性和完整性保护，防止非法窃听和非法篡改。Hillstone 企业安全网关特有的 PnPVPN（即插即用型 VPN）技术，大大降低了 VPN 实施的难度，部署时只需要在省级或市级的企业安全网关上完成配置，在县级节点部署的企业安全网关上简单配置极少的网络参数即可完成 VPN 互联。

- **一体化策略简化配置维护难度**

Hillstone 企业安全网关采用一体化策略，在一个界面上即可完成大部分安全功能的策略配置，减少了页面的跳转并降低配置的难度；通过集中的日志审计和统计页面，运维人员可灵活定义需要查看的日志条件，系统便可输出相关的访问和安全控制日志，简化了日志查询和统计的难度。

- **集中安全管理提高管理效率**

在省质监局部署的 Hillstone 集中管理平台，可对全网部署的所有 Hillstone 企业安全网关实施集中化的管理，包括日志的集中查询统计，以及全局性策略的集中下发，集中管理提高了省质监局对安全事件的检索和响应效率，更好地保障安全防护的效果。

运行效果

在江苏省质监一期工程建设后，Hillstone 企业安全网关稳定的运行能力，以及应对安全事件的综合防御功能，便得到了用户的一致认可，在二期工程建设后，Hillstone 专有的即插即用型 VPN 技术，简化了部署的难度；而集中安全管理平台的部署，又进一步简化了配置和维护的难度，还提高了对安全事件的检索和响应的效率，使江苏省质监局信息网络的安全性得到了进一步的保障。

苏州工业园云数据中心安全防护

云计算的应用在近几年得到快速的发展，对于政务系统而言，基于云计算技术搭建的数据中心，可实现更为灵活的资源配给、更可靠的应用系统迁移，因此也得到了广泛的应用，苏州市园区管委会，既是利用云计算相关的技术，搭建其私有云数据中心，为园区内的各个接入的政府单位提供弹性的计算资源，目前私有云数据中心包含一个主数据中心和一个备份数据中心。

但云计算技术的使用又往往对现有的网络安全技术带来新的挑战，由于关键的应用系统均集中在云数据中心，这使得云计算中心的并发访问量极高；虚拟化技术的应用，在一台服务器内出现了虚拟交换层，很多流量特别是虚拟机间的流量不再通过外部的硬件交换设备；虚拟机可在不同的物理服务器上迁移，而防火墙的安全策略是预先配置好的，是静态工作的，当迁移后无法随动时，也会形成防护上的漏洞。Hillstone SG-6000-X6150 数据中心防火墙正是根据云数据中心的挑战而研发出来的，在苏州市园区管委会云数据中心边界得到很好的应用。

需求分析

区别于传统政务网络，云数据中心的建设，特别是虚拟化技术的使用，对传统网络安全技术带来了挑战，为此苏州市园区管委会提出了如下的安全建设需求:

- 高性能高可靠：由于云数据中心集中了苏州市园区内各个政府职能部门的重要应用系统，这使得云数据中心往往面临着极高的并发访问量，因此当需要在云数据中心边界部署安全设备时，要求设备也应具有极高的性能，同时也支持更好的可靠性，保障政务业务的正常处理;
- 支持虚拟防火墙： 部署的安全设备应提供虚拟防火墙，对于不同的政务系统，提供不同的虚拟防火墙，从逻辑上保证不同政务系统的访问控制是隔离的，避免不同政务系统之间的相互影响;
- 不同虚拟机间的控制：对于采用虚拟化后在物理服务器内部出现的虚拟交换层，部署的安全设备可配合虚拟机操作系统，将原本在服务器内部进行交换的数据包迁移到外部防火墙上，进行相关的检测与控制。
- 支持多链路：苏州园区云数据中心出口租用了多个运营商的多条链路，用户期望部署的单台安全设备上可同时连接多个出口链路，并能够根据不同链路的质量和负载自动进行平衡，在提升链路利用率的同时还能够保障政务 系统访问的可靠性。

解决方案

苏州市园区管委会云数据中心在两年前便开始了建设，当时即采购了两台 Hillstone SG-6000-X6150 数据中心防火墙，部署在云数据中心的网络边界，实施有效的隔离与访问控制;随后苏州市园区管委会又继续建成了备份云数据中心，采取与主数据中心一样的结构，实现更高的可靠性，在边界上继续引入两台 Hillstone SG-6000-X6150 数据中心防火墙，实施有效的隔离与访问控制。并达到如下的建设效果:

前后引入的四套 Hillstone SG-6000-X6150 数据中心防火墙，分别部署在主数据中心及备份数据中心的网络边界，实现如下的安全建设效果:

- **高性能高可靠保障政务业务稳定**

Hillstone SG-6000-X6150 数据中心防火墙采用了分布式多核架构，整机具有极高的工作性能，单台设备最高可支持 100Gbps 吞吐量，和最大 5000 万并发连接，完全可满足苏州市园区管委会云数据中心海量政务访问的需要。同时数据中心防火墙采取全并行全冗余架构，大大提升了设备的稳定性；在本次项目中通过 HA 部署，又进一步提升了整体系统的可靠性。

- **虚拟防火墙为不同政务应用提供独立的安全平面**

Hillstone SG-6000-X6150 数据中心防火墙最大可支持到 500 个虚拟防火墙，这些虚拟防火墙为不同的政务系统提供了独立的安全平面，从逻辑上将不同政务系统的业务数据流进行了隔离，防止相互干扰相互影响，同时安全策略也是基于虚拟防火墙的，这样系统管理人员能够更好地根据政务系统的具体要求配置不同强度的安全策略，比如不同强度的身份认证策略。

- **实现不同虚拟机间的隔离与控制**

Hillstone SG-6000-X6150 数据中心防火墙与虚拟操作系统配合，将虚拟机间的流量强制性地牵引出来，并经过边界的数据中心防火墙，实施有效的检测与访问控制，在确认符合安全策略后，方可允许虚拟机间的访问。

- **多链路负载均衡**

Hillstone SG-6000-X6150 数据中心防火墙支持的多链路负载均衡技术，单台设备上连接了苏州园区管委员多个运营商的多条链路，并主动探测链路的带宽和负载状态，并根据链路忙闲状态自动将负载分配到不同链路上，即提高了链路的利用率，也提高了政务访问的可靠性。

运行效果

Hillstone SG-6000-X6150 数据中心防火墙是根据云数据中心特点而研发的，其高性能、高可靠的特点，能够为数据中心海量的接入访问提供保障；虚拟防火墙技术能够为不同的政务系统提供独立的安全控制平面；与虚拟操作系统配合将原本在服务器内部交换的流量引出，并进行有效的检测，解决虚拟化后带来的挑战；多链路负载均衡技术使得数据中心的多链路得到更充分的使用。设备部署后运行稳定，有力保障了苏州园区管委会云数据中心的安全。

教育
Education

典型客户名单

教育部
清华大学
中央财经大学
北京工业大学
北京科技大学
北京师范大学珠海学院
中国农业大学
中国社会科学院
中国劳动关系学院
首都师范大学
上海市教委
上海师范大学
上海交通大学
上海财经大学
上海华东政法大学
上海外国语大学
上海大学
上海商学院
上海音乐学院
上海应用技术学院
上海崇明教育城域网
上海电力学院
西安交通大学
西安科技大学
天津外国语学院
天津音乐学院
天津轻工业学院
天津石油技术学院
青海省西宁市教委
哈尔滨工业大学
哈尔滨商业大学
辽宁工业大学
河北工业大学
河北大学
河北农业大学
长安大学
山东政法学院
山东电子职业学院
青岛农业大学
青岛市教育局
青岛理工大学
连云港教育局
江门市教育局
湖南师范大学
武汉理工大学
武汉软件工程职业学院
武汉商贸职业学院
华南师范大学
华南理工大学
西南政法大学
河南高招办
郑州市教育局
郑州大学
江苏省广播电视大学
南京师范大学
南京体育学院
南京信息工程大学
扬州大学
西交利物浦大学
石湖科技学院
常州技师学院
苏州大学
徐州建筑职业学院
暨南大学
广州大学
广州军事体育学院
南方医科大学
杭州萧山教育城域网
连云港赣榆县教育城域网
成都教育城域网
西华师范大学
成都理工大学
泸州医学院
南昌大学

上海交大打造安全可靠的校园 IDC 网络

上海交通大学闵行校区于 1985 年开始筹建，历经 20 多年，现已建立了完善的内部校园 Intranet 网，包括校 IDC 中心，学校内部 OA 系统，教学和办公网。

Hillstone SG-6000-G5150 企业安全网关部署在 IDC 中心的出口，保护 IDC 业务抵御互联网威胁并实现业务之间的安全隔离，为上海交大 IDC 进行安全防护。

需求分析

优质的网络需要优质的安全支撑，因此对部署在 IDC 的核心安全设备来说，提出了更高的要求，首先要求设备需具有高性能，高吞吐等特点；设备需支持较高的最大并发连接数，并且每秒新建会话数在 10 万以上；其次设备需支持多千兆端口，并且易于网管人员管理设备及流量。

解决方案

上海交通大学闵行校区已经建立了完善的内部校园网，有多条链路出口，分别连接上海教科网，CERNET2 和电信的 Internet 链路。为了对校园网进行保护，在学校出口部署了防火墙进行安全防护，用作抵御和过滤来自于外部的安全威胁和进行数据流的访问控制，同时对外部到内部访问的数据流量进行安全控制。Hillstone 解决方案具有以下特点:

- **高性能的安全过滤能力和防护能力**

Hillstone SG-6000-G5150 企业安全网关有着强大的安全功能和处理能力，能够充分满足 IDC 中心所有服务器群组对性能的需求，保障在进行充分安全加固的同时不会降低服务器的可访问性，不会降低服务器的服务品质。

- **根据实际情况划分安全域，将内网分级别防护**

Hillstone SG-6000-G5150 企业安全网关有 GE 口和 SFP 光口，且有扩展槽位可用于后续千兆接口及万兆接口、BYPASS 接口的扩展。

可以将 IDC 内部分成若干个不同安全级别的安全域。通过安全域的规划和细粒度访问控制策略的设定，有效加强了对各服务器群组的安全保护。

- **实时查看用户使用流量情况**

Hillstone SG-6000-G5150 企业安全网关具有强大的统计功能，包括日志收集、设备实时监控、历史数据汇总查询以及安全审计报表功能，并可以以波形图或柱状图的形式展现给用户，能够清晰的了解到 IDC 内部各服务器的流量情况、各个应用的流量情况，甚至能够看到一个特定 IP 内部各种应用的流量情况，对于用户网络管理员监控网络使用情况、定位网络问题以及优化网络结构都是必不可少的工具。

运行效果

Hillstone SG-6000-G5150 企业安全网关作为 IDC 出口防护设备，设备出色的性能满足了用户需求，使管理上更加简单易行；高性能的安全防护和过滤功能，保证了 IDC 服务器的正常工作，为用户提供了一个安全、有效的解决方案。

西安交通大学打造畅通安全的校园网

西安交通大学简称西安交大，是国家教育部直属重点大学。西安交大网络中心机房作为西北教育网的总出口，同时承载着校园教职师生访问互联网的重任。目前该校率先升级了校园骨干网到万兆级。

Hillstone SG-6000-X5100 数据中心防火墙部署在校园网连接 Internet 的核心出口处，承担着 4 万多 IP 访问互联网的地址转换和安全防护，保证了学校的教学业务正常运行。

需求分析

伴随着万兆网络的成功应用，万兆级网络的安全防护、应用层管理和访问控制等需求也应运而生。高性能和高稳定性是首要的，而在此基础上构建可靠、可控的网络也同样重要。

解决方案

西安交大看重 Hillstone SG-6000-X5100 数据中心防火墙强大的抗攻击和防病毒功能以及灵活的带宽管理等功能，为校内本科、研究生、博士生等共四万余学生的认证及上网做良好的保证。本项目中，西安交大采用 Hillstone SG-6000-X5100 数据中心防火墙作为网络安全防护的解决方案，主要呈现出以下特点:

- **Hillstone 数据中心防火墙的抗攻击能力**

Hillstone SG-6000-X5100 数据中心防火墙部署在出口可以同时防御内外网攻击。 强大的抗攻击能力，每秒 20 万 TCP 或 50 万 UDP 的新建会话能力，在极限背景流量情况下仍可以对攻击流进行识别和阻断，保障内外网安全。

- **Hillstone 数据中心防火墙的QoS带宽管理功能**

本方案中，通过以下几点对带宽进行了精细且全面的管理:

a. 基于每个 IP 地址的最大带宽限制;

b. 基于每个 IP 地址的会话限制;

c. 基于应用的带宽管理。

- **Hillstone 数据中心防火墙的Web认证功能实现与西安交大计费认证系统的联动**

为了方便管理学生客户端访问互联网的认证和计费问题，西安交大网络中心搭建了认证计费服务器，这是一种基于标准 Radius 协议的认证服务计费系统。

Hillstone SG-6000-X5100 数据中心防火墙作为互联网接入的必经设备同时提供了 Web 认证功能:

a. 用户在未经认证的情况下打开任意网页都将被定向到交大用户登陆页面

b. 输入正确的用户名口令后，Hillstone SG-6000-X5100 数据中心防火墙将接收到的认证信息发送给 Radius 认证服务器，由认证计费系统来判断用户请求是否允许通过

c. 认证计费系统将审核信息返回给 Hillstone SG-6000-X5100 数据中心防火墙，安全网关通过用户名映射的角色来自动赋予相应的访问权限。同时 Web 认证还具备连接心跳功能，这将为客户端用户提供更加便捷的登陆管理和自动下线功能。

运行效果

Hillstone SG-6000-X5100 数据中心防火墙的性能和功能都达到了用户所要求的网络安全设备应具备的各种标准，满足了在攻击防护、流量管理、NAT、收费认证等方面的具体要求，全面保障了学校 4 万多 IP 访问互联网的安全防护。

武汉理工大学校园网安全建设

武汉理工大学整个校园网内用户已经达到 5 万人左右，随着信息技术在学校内部管理中的广泛应用，已经建立完善的数字化校园网络。

Hillstone SG-6000-X5100 数据中心防火墙分别部署在网络出口和服务器集群出口，保护学校整个应用系统抵御互联网威胁，保障服务器集群不受外界病毒侵袭，使校园信息化建设更加完善。

需求分析

随着数字化校园用户数的增长和系统开放程度的增加，给整个应用系统带来了安全压力。之前部署的基于三层包检测的安全设备已不能满足现有需求，学校整个应用系统经常受到外网的攻击和入侵。另外，内网用户可能也会不小心将病毒和间谍软件带入内网服务器，导致感染整个系统。

基于上述原因，武汉理工大学迫切希望能有一套先进、可靠、安全、经济的系统解决方案来解决以上问题，并确保系统有一定的扩展性从而满足学校信息化业务的后续发展和规模扩大。

解决方案

通过采用新一代多核硬件架构以及配合 64 位实时并行操作系统的软件平台，对武汉理工大学数万需要访问 Internet 用户进行高效转发，并开启相应的带宽管理策略，保障关键业务，限制非正常流量，并通过使用 ISP 路由功能实现了电信、联通线路的优选，有效的保障了武汉理工大学内部用户访问 Internet 需求。

Hillstone 解决方案特点如下:

- **HA双机热备**

武汉理工大学在服务器区安全防护升级中采用冗余部署的 Hillstone SG-6000-X5100 数据中心防火墙解决方案，有效地保障了武汉理工大学新推出的视频点播、在线教学等大量关键应用稳定运行;

- **ISP路由提升上网体验**

Hillstone SG-6000-X5100 数据中心防火墙内置了中国电信和中国网通的地址路由表，实现智能的 ISP 路由选路，根据目的地址来自动判断并选择相应的出口链路，有效提升访问速度;

- **深度应用识别**

利用 Hillstone SG-6000-X5100 数据中心防火墙基于深度应用识别及深度攻击检测的精准 IPS 功能，为武汉理工大学的内网应用提供了立体的安全防护。

运行效果

Hillstone SG-6000-X5100 数据中心防火墙凭借高性能、丰富的功能和电信级的高可靠性赢得了武汉理工大学用户的认可。设备特有的混合模式安全防护，HA 高可靠功能实现了不断业务的毫秒级切换。

广东工业大学校园网出口综合防护

广东工业大学是一所以工为主、工理经管文法结合的、多科性协调发展的省属重点大学。随着信息化建设的深入和师生规模的不断增加，原有校园互联网出口链路和设备已无法支撑海量访问，互联网出口带宽及出口设备的扩容升级已势在必行。

在广东工业大学实施出口带宽扩容项目中，具有高性能、高可靠、高可扩特点的 Hillstone SG-6000–X6150 数据中心防火墙，部署在校园网互联网出口链路上，设备不但可有效支撑当前的上网规模，其可扩展性也为未来的网络持续扩容留有余地，此外，设备支持的多链路负载、智能带宽管理、ISP 路由等技术，也进一步提升了用户的上网体验，为精细化的上网管理提供更有效的手段。

需求分析

广东工业大学需要对原有校园网络进行扩容改造，以满足不断增长的校园网用户的上网需要，为此，提出了下面的需求:

- 高性能保障：广东工业大学校园网最多同时在线 1 万多用户，高峰时流量接近 2G。因此，需要高性能安全网关来满足海量接入访问量;
- 多链路负载均衡：广东工业大学校园网共有 2 条电信链路和 1 条教育网链路。为此广东工业大学期望引入多链路负载均衡技术，平时能够更智能地在多条链路上均衡负载，更合理地使用链路资源；而当某条链路故障，系统也能够将故障链路上转发的流量自动切换到其他正常链路上，从而保障用户的上网持续;
- 有效的带宽管理：广东工业大学校园网中存在大量的 P2P 下载和网络视频的流量，占用了大量的带宽资源，导致正常网络访问受到影响，为此学校期望引入精细化的带宽管控手段，在保障正常的互联网浏览、电子邮件发送等访问的同时，尽量控制 P2P 和网络视频的流量，提升带宽的利用率;
- 合理控制设备升级成本：随着广东工业大学校园网规模的扩大和网络应用的增多，未来会需要不断增加设备来满足校园网的需求。为此用户期望引入的安全设备必须支持可扩展性，在扩展性能的同时能够保护前期投资。

解决方案

在进行了长达一年多的测试和对比之后，广东工业大学最终选择了 HillstoneSG-6000-X6150 数据中心防火墙，设备部署在互联网出口处，发挥了如下作用:

广东工业大学校园网出口综合防护

- **高性能的安全架构**

Hillstone SG-6000–X6150 数据中心防火墙是基于新一代多核网络安全架构和 64 位并行处理的 StoneOS 安全内核的硬件安全网关，其吞吐量、每秒新建会话数以及最大的并发会话等性能指标都是传统防火墙的数倍。高性能很好地保障了上网访问的速率，同时大大减少网络出口接入设备的数量，简化了网络结构，降低了网络延时。

- **多链路负载均衡**

HillstoneSG-6000–X6150 数据中心防火墙支持多链路 Outbound 流量的负载均衡，并可针对每条链路建立全路径健康检查，并针对链路负载状态自动分配上网流量，使出口链路的使用更加合理。在此基础上支持的链路智能切换功能，确保当单条链路故障时，能够将故障链路上转发的上网访问自动切换到其他正常链路上，从而保障上网访问的连续性。而且，设备内置了 ISP 路由信息，按照目标地址自动在多条运营商链路上智能路由，加快上网访问速度。

- **智能带宽管理**

Hillstone SG-6000–X6150 数据中心防火墙支持基于应用和基于 IP 的带宽控制技术，在广东工业大学，通过该技术将带宽资源尽量分配给网页浏览、邮件收发等正常业务的访问，而尽量压缩 P2P、网络视频的流量，从而使带宽资源利用率更加优化。

- **性能可灵活按需配置按需扩展**

HillstoneSG-6000–X6150 数据中心防火墙的弹性架构，在需要扩容时，通过增加相应的业务处理板卡即可实现，对于广东工业大学，当上网用户规模增加时，无需另外购买设备，从而有效保护了前期投资，更合理的控制了网络改造和设备升级的成本。

运行效果

HillstoneSG-6000–X6150 数据中心防火墙上线以后，设备运行稳定，在高峰期流量达到 2 个 G 左右，设备 CPU 使用率在 30%到 40%左右，并且用户体验良好，P2P 下载和网络视频得到了控制，保障了网页浏览、邮件收发等的正常业务的高效访问。同时也为广东工业大学提供极大的性能扩展空间，有效保护广东工业大学的前期投资。

湖北省教育考试城域网安全互联建设

教育考试中心全称为“国家教育考试考务管理与服务平台”，是国家教育部考试中心“十一五”事业发展规划的重点项目，平台利用现代数字通讯、网络技术、视频技术、系统工程、管理技术，在全国范围按照五级架构进行建设，而作为二级节点的湖北教育考试中心，经过几年的建设，已形成覆盖网上巡查、应急指挥、考务综合管理、视频会议、考生服务、网上考试和诚信档案等七大功能的，分布在全省各地市、区县、学校的大型综合网络。

而集成了应用识别与访问控制技术、VPN 技术以及带宽管理技术的 Hillstone 企业安全网关，为湖北教育考试中心提供了综合性的防范，设备部署在湖北教育考试中心的区县节点，通过 VPN 技术实现了同级考试中心间，以及与上级考试中心间的安全业务通信；通过深度应用识别，对各节点的上网行为进行了有效控制，杜绝违规的访问；通过管理技术，整合身份认证、应用识别，对不同角色的不同业务访问进行了有效的带宽限定，保障湖北教育考试平台的正常运行。

需求分析

湖北省教育考试中心的区县节点（四级节点）建立在互联网平台上，即利用各个节点的互联网链路，与湖北省的地市节点以及省级节点互联，完成相关的业务访问和操作，而互联网的开放性使得平台上各类业务访问面临很大的安全隐患，为此湖北省教育考试中心提出了如下的安全建设需求:

- 更安全的数据传输保障：由于互联网平台的开放性，使得运行在互联上的视频数据、业务数据在访问过程中，很容易遭到窃听和篡改的风险，为此需要设备提供 IPSec VPN 功能，对传输数据进行加密和完整性保护，保障数据传输的安全性;
- 更智能的应用识别：湖北考试中心各个区县节点的互联网链路，除了运行与教育考试相关的业务应用，也有各个节点办公人员的上网访问，而根据考试中心的规定，工作时间内不得从事 P2P、网上炒股等与工作无关且过度占用带宽的行为，为此需要提供针对性的访问控制;
- 更有效的带宽控制：正如前面所述，各个区县节点互联网链路上，既有与教育考试相关的业务应用，也有各个节点办公人员的上网访问，不同业务存在着对带宽资源的争夺，为此有效控制带宽的分配就显得非常重要;
- 抗攻击：教育考试平台内存在着一些涉及考生的敏感信息，自然会存在被攻击的威胁，特别是湖北考试中心的区县节点与互联网直连，为此应采取必要的抗攻击措施。

解决方案

针对湖北省教育考试中心提出的安全建设需求，Hillstone 通过集成多种安全防护技术的企业安全网关，部署在各个区县节点的互联网出口，对业务访问进行保护，同时限制一些特定的上网访问，提升教育考试平台的安全性。具体的配置部署示意如下:

在本项目中，Hillstone 企业安全网关除了提供多种安全防护技术以外，设备的高可靠性、易用性，在前期测试阶段得到了用户的认可，设备部署后，为湖北教育考试中心发挥了如下的作用:

- **保障数据安全传输**

Hillstone 企业安全网关提供的 IPSec VPN，作用在湖北教育考试中心的区县节点互联网出口，对关键的业务访问，特别是网上巡查指挥系统的访问数据包，通过加密、摘要等手段，有效保障了数据传输的机密性和完整性。Hillstone 企业安全网关还支持与第三方支持标准 IPSec 协议的 VPN 进行互联互通，在本项目实施中，无需更换地市节点已有的 VPN 设备，保护用户投资。

- **深度应用访问控制**

Hillstone 企业安全网关能够识别当前近千种互联网应用，在本项目中通过应用访问控制技术，有效限制了 P2P、网上炒股、网络游戏等应用，为考试中心的安全管理提供有力支持。

- **智能带宽管理**

Hillstone 企业安全网关支持的带宽管理功能，从用户维度、应用维度制定更精准的 QoS 策略，在本项目中通过该功能，针对区县不同节点间，以及区县与上级的地市节点，以及省级节点间的业务访问，按照业务类型和等级定义不同的带宽控制策略，保障重要业务的资源配给。在此基础上，Hillstone 企业安全网关提供的弹性带宽策略，还能够根据链路的忙闲状态，在一定范围内弹性增加或减少给不同业务分配的带宽，进一步提升各节点互联网链路带宽的利用率。

- **防范非法攻击**

Hillstone 企业安全网关内置的专业抗攻击模块，可对互联网上常见的攻击行为进行检测与阻断，保障各节点网络的稳定、可靠、安全运行。

- **安全集中管理**

在引入 Hillstone 企业安全网关的基础上，湖北教育考试中心部署了 Hillstone 安全管理平台，对各区县节点部署的安全网关设备实施集中管理，包括安全日志、访问日志的集中分析，并通过深入的数据挖掘，有效分析出当前是否存在安全威胁，提升了网络安全事件的分析和响应能力。

运行效果

Hillstone企业安全网关从部署后运行至今，运行非常稳定，建成后的系统，在企业安全网关的配合下，既能保证原有考点流量的正常运行，又可保证灵活增加学校考点的规模，部署的 Hillstone 安全管理平台，可以让用户从市级统一管理平台即可实现对各个区县节点部署的 Hillstone 企业安全网关的远程集中管理，用户为此感到非常满意。

河南省教育招生办城域网综合安全防御

根据国家教育部下发的《教育部关于做好国家教育考试考务管理与服务平台相关工作的通知》，河南省招生办公室从 2007 年起，即在本省开展了教育考试平台的建设与开发工作，经过几年建设已取得一定的成效，根据项目计划在 2014 年需要完成覆盖全省各个考点学校的四级电子在线巡查监控系统，有效防范高、中考的各种作弊行为。

随着教育考试中心平台的建设，信息安全逐渐被重视起来，河南省教育厅对此提出了综合防御，积极防范的建设要求，而整合了多种安全功能的 Hillstone 企业安全网关，作为网络安全建设的重要内容，被部署在河南省各市级教育中心平台，主要用以保护高、中考电子在线巡查的视频监控，保障河南省教育厅正常的考务管理。

需求分析

利用电信 MPLS VPN 广域网链路，河南省教育考试中心将市、县招生办，以及各个考点院校的网络连接在一起，完成相关的业务访问和操作，其中省招办出口为 100M、市县招办出口均为 30M 链路，而各个考点院校的出口大多为 10M 链路。

电信 MPLS VPN 广域网链路的相对开放性，使得河南省教育考试中心的各类业务访问依然面临着较大的安全隐患，为此河南省教育考试中心提出了如下的安全建设需求:

- 更安全的数据传输保障：系统能够对广域网上传输的数据进行机密性和完整性的保护，能够有效对抗黑客非法的窃听或篡改行为，保护数据安全;
- 更有效的带宽控制：正如前面所述，各个区县节点链路上，既有与教育考试相关的业务应用，也有各个节点办公人员的上网访问，不同业务存在着对带宽资源的争夺，为此有效控制带宽的分配就显得非常重要;
- 有效的访问控制：限制河南省教育考试中心的纵向非法访问，并对关键的网上巡查业务进行有效保障。

解决方案

针对河南省教育考试中心提出的安全建设需求，Hillstone 通过集成多种安全防护技术的企业安全网关可有效应对，在本期项目中，Hillstone 企业安全网关部署在郑州、濮阳及下辖的各区县招生办，以及作为考点的院校，重点对网上巡查业务进行安全防护，并通过集成的 VPN、QoS 功能，保障了业务访问的安全性和稳定性。具体的配置部署示意如下:

- **保障数据安全传输**

Hillstone 企业安全网关提供的 IPSec VPN，作用在河南省招生办 Hillstone 企业安全网关与此项目中发挥的作用为郑州市及濮阳市各县级招生考点院校的广域网边界，通过加密、摘要等技术手段，有效保障了数据传输的机密性和完整性。

Hillstone 企业安全网关提供即插即用的 VPN，部署时只需要进行预先的简单配置，即可在大规模多节点部署的 Hillstone 企业安全网关间实现 VPN 隧道的建立与通信，非常适合河南省教育考试中心类的场景使用。

- **智能带宽管理**

Hillstone 企业安全网关支持的带宽管理功能，从用户维度、应用维度制定更精准的 QoS 策略，在本项目中通过该功能，针对区县不同节点间，以及区县与上级的地市节点，以及省级节点间的业务访问，按照业务类型和等级定义不同的带宽控制策略，保障重要业务的资源配给。在此基础上，Hillstone 企业安全网关提供的弹性带宽策略，还能够根据链路的忙闲状态，在一定范围内弹性增加或减少给不同业务分配的带宽，进一步提升各节点广域网链路带宽的利用率。

- **安全集中管理**

在郑州市及濮阳市区县及各个考点院校大规模部署 Hillstone 企业安全网关的基础上，在省招生办节点部署了 Hillstone 安全管理平台，对各点部署的安全网关设备实施集中管理，包括安全日志、访问日志的集中分析，并通过深入的数据挖掘，有效分析出当前是否存在安全威胁，提升了网络安全事件的分析和响应能力。

运行效果

Hillstone 企业安全网关提供的简单易用的 IPSec VPN，在河南省教育考试城域网中部署非常方便，并且 Hillstone 企业安全网关运行稳定，在实施后的一段时间内没有出现一次中断性故障，在 2012 年河南省高考期间，为网上巡查系统的正常运行提供了有力支撑，通过严格的访问控制和带宽控制策略，杜绝了非法访问，保障了考试的顺利进行，为此用户感到非常满意。

成都市教育城域网安全建设

成都教育专网是成都市教育系统自建、非虚拟的全程光纤网络。覆盖全市约 1200 多个学校、教育机关、事业单位和教学机构。是成都市内部教育业务专用信息网络。

Hillstone SG-6000-M2105 企业安全网关部署在各个学校、教育机关等子网络出口，保护各个子网络抵御互联网威胁并实现各网络间的安全隔离，实现业务安全、快速、稳定运行。

需求分析

在成都教育专网接入网关设备的选型上，主要依据中小学校园网的典型特点：一是遏制校园网内 ARP 病毒攻击，网络缓慢和掉线等问题，二是为校园网内存在的多个小网络，根据不同的需求和管理方式，设置不同的权限和带宽。

解决方案

根据以上两点要求，Hillstone SG-6000-M2105 企业安全网关凭借很好的稳定性和完善的功能，最终成为用户的选择，部署在各网络出口，实现对网内部及网络间的安全隔离。

在此项目中，Hillstone SG-6000-M2105 企业安全网关的优势尽显无遗:

- **细粒度的安全策略**

可以将各个接口分别被划分到 trust、untrust、dmz 等三个不同的安全域。通过对各域之间配置策略，对各域之间的所有连接进行传输层协议以及应用层协议状态的检测，从而实现域间的访问控制以及应用状态监控。

- **IP地址与MAC地址绑定**

地址绑定功能，实现学校各 IP 地址和相应终端的绑定，确保各终端与 IP 地址一一对应，并实现系统控制功能。

- **ARP欺骗攻击防御及其他常见网络攻击防护**

Hillstone SG-6000-M2105 企业安全网关独有的 Secure Defender 安全客户端，可以完美地解决 ARP 欺骗攻击，且可以选择性地在 untrust、dmz 等安全域上启用了攻击防范功能，识别并阻断主流网络攻击。同时，在开启攻击防范功能之后，可以查看设备所检测到的每种攻击次数和丢包次数。

- **灵活的带宽管理**

可以对校园网内部的每个 IP 或网段的带宽限制，有效防止 P2P 应用过度消耗资源。在较为大型的中学等网络高负荷环境中，灵敏高效的“弹性流控”充分利用带宽总资源，获得最好的使用体验。

- **监控功能**

Hillstone SG-6000-M2105 企业安全网关可以提供内容详尽、分析透彻、功能强大的日志报表及统计系统。

运行效果

通过在成都范围内 1200 多个学校、教育机关、事业单位、教学机构的教育城域网部署 Hillstone SG-6000-M2105 企业安全网关，在实际网络使用环境中，安全网关在性能、稳定性、技术支持服务等诸多方面全面满足了用户的需求。

杭州市教育城域网安全建设

杭州市教育技术中心承担杭州教育城域网运行管理的职责，2012 年，杭州市教育局开始启动网络高安全性、高稳定性、高可用性的改造，根据对网络安全的需求，需要在各节点办公内网与 Internet、教育城域网边界处部署安全网关设备，实现办公网边界防护与内网安全访问控制，同时在服务器区前部署数据中心防火墙，实现内部访问数据服务器的安全防护。

杭州市教育局中采用 Hillstone SG-6000-X5100 数据中心防火墙以路由模式部署在杭州市教育局办公网 Internet 和教育城域网出口处，实现 HA 双机热备。防火墙创建三个区域：内网、互联网、教育城域网，在数据中心前部署 Hillstone SG-6000-G5150 企业安全网关进行服务器安全防护。在普教出口处以路由模式部署 Hillstone SG-6000-G2120 企业安全网关或者 Hillstone SG-6000-M3108 企业安全网关，连接教育城域网。

需求分析

杭州市教育局启动网络改造，提出了下面的网络建设需求：

- 边界隔离与访问控制：杭州教育局需要划分出内网、互联网、教育城域网三个区域，互联网用户对门户网站的访问，只能通过指定的访问类型（如 HTTP 或 HTTPS）来访问到门户网站。同时还需要禁止非授权用户对数据中心的访问；
- 抗攻击：对于互联网上的访问，进行攻击检测与防护，重点针对拒绝服务攻击进行有效阻断，防止因攻击导致的网络中断；
- 流量控制：保障关键业务的流量，限制无关业务流量，更合理地使用带宽；
- 上网合规性管控：对用户访问互联网和教育城域网的行为进行有效日志记录，以便提供给系统管理人员，在发生安全事件后进行备查；

解决方案

针对杭州市教育局的网络现状、实际需求和投资预算，Hillstone 建议用户采购高性能、多功能的一体化企业安全网关是经济实惠、性价比高且适用于用户的解决方案。在和用户进行了深入细致的技术交流和方案探讨以及一段时间的模拟环境测试对比后，用户最终选择 Hillstone 的一体化企业安全网关作为整体的安全解决方案。

- **安全隔离与控制保护业务安全**

Hillstone 企业安全网关通过划分安全域对服务器等重点区域进行隔离和管控，将内网、互联网与教育城域网分别放在不同的安全域中，实现各区域之间的安全互访。通过基于角色和身份认证的访问控制分配网络资源，进行日志审计，对业务访问实现更全面的保护。

- **全面的攻击防护保障业务安全**

Hillstone 企业安全网关能够提供全面的攻击防护能力，能够针对 DoS/DDoS 和常见攻击进行有效阻断，有效保护企业网关的可用性。同时，Hillstone 企业安全网关强大的应用层检测能力以及应用层处理性能为分析和阻挡各类攻击提供了强大的支持。

- **带宽管理保障关键业务流量**

Hillstone 企业安全网关的混合 QoS 功能，对特定的 IP 地址以及端口应用的访问进行带宽保证操作，对 P2P 视频、P2P 下载应用进行带宽限制操作。保障关键业务流量，限制无关业务流量，实现带宽利用的最大化。

- **上网合规性管控符合监管要求**

Hillstone 企业安全网关，在实现对上网访问控制的基础上，对上网行为进行全面日志记录，来控制上网行为，并结合基于角色的管理技术，实现“实名制”记录。既符合了网监的审查要求，又方便的网管人员的维护管理。

运行效果

Hillstone 企业安全网关从性能处理能力、扩展能力、安全性、应用的便利性等方面，都充分满足用户对应用的需求，同时又可以满足未来几年内网络规模扩大和业务发展的需要。

企业
Enterprises

典型客户名单

腾讯公司
华为
三一重工
伊利集团
中粮集团
中国邮政
中船重工
五粮液集团
中国南车集团
中国北车集团
波司登集团
温莎集团
金地集团
石药集团
中金岭南
许继集团
苏宁集团

比亚迪汽车
京东方集团
汉庭酒店
乔丹体育股份
营口港务集团
贝朗卫浴
国药控股
上海烟草
上海益盟软件
步步高集团
欧亚达集团
中国中铁建工集团
中国中元国际工程公司
易程科技
上海宝钢集团
紫金矿业集团
武汉钢铁集团

广东省韶钢集团有限公司
福建三明钢铁
红孩子
苏州迪欧咖啡
首都在线
江西铜业
马应龙药业
天津天药药业股份有限公司
飞鹤乳业
温州人本超市
湖南益丰大药房
上海欧姆龙有限公司
上海少思网络科技有限公司
宁波市欧琳厨具有限公司
深圳华大基因
福建省邮政公司

伊利集团建设坚固的企业安全堡垒

随着伊利集团业务的发展以及对网络业务的需求，实现伊利集团的办公一体化，伊利集团着手建设集团 VPN 网络，欲借 VPN 通道，实时接管骨干线路上业务流量，确保无间断的给用户提供网络访问平台。

Hillstone 通过在伊利集团核心以及各个分支机构部署 Hillstone 企业安全网关，开启 VPN，确保了通过 VPN 专线的网络服务的不间断提供。同时，通过开启 Hillstone 企业安全网关的攻击防护以及流量管理、负载均衡等功能，对非关键业务流量进行控制，极大地提高了伊利集团的网络利用率。

需求分析

为了实现伊利集团总部以及分支机构的数据通信互连，伊利集团需要通过组建专网专线的方式来实现，但是由于专线的成本较大，且有可能由于不可抗拒的原因（电力中断、自然灾害等）造成专线长时间中断，影响业务系统的正常应用；随着员工的增多、业务对网络依赖程度的增加，同时也需要安全网关设备对集团网络进行攻击防护及管理， 因此，伊利集团急需高效稳定的安全网关来实现 VPN 互连并且对集团网络进行管理以提高运行效率。

解决方案

伊利集团经过长达半年的产品评测选型，最终选择了 Hillstone 提供的解决方案：Hillstone SG-6000-G2110 企业安全网关做为搭建高吞吐量 VPN 通道的安全设备，部署在总部作为核心 VPN 网关，各个分支机构部署 Hillstone SG-6000-M 系列企业安全网关做为分支线路的 VPN 网关。

部署方案如下图所示:

在本项目中，Hillstone 安全解决方案的主要特点如下：

- **多链路负载均衡优化链路**

为充分利用每条链路的资源，使用 Hillstone 企业安全网关的链路负载均衡功能，通过对多条链路权重的设定，来平均分配网络资源请求，保障用户正常上网。

- **增强内外网安全防护**

Hillstone企业安全网关通过病毒过滤，内外部攻击防范，IPS 入侵防御可以实现更高级别的安全防护。

- **QoS带宽控制管理网络流量**

Hillstone 企业安全网关提供专业 QoS 带宽管理解决方案来协助用户管理网络流量，杜绝单个IP占用流量过多问题，保障关键业务的可用带宽。

- **独有PnPVPN技术帮助伊利快速部署和简便维护**

Hillstone 在建立 VPN 时推荐使用特有的 PnPVPN 技术，该功能开启后，只需在总部设备建立 VPN 账户，分支机构就可以随时使用 Hillstone 企业安全网关通过输入账户密码的方式，快速有效地建立分支与总部之间的 VPN 通道，保障了伊利集团 VPN 网络的畅通，实现助力伊利集团企业发展的目标。

运行效果

通过在伊利集团部署 Hillstone 企业安全网关，不仅实现了企业总部和各分支机构的安全高速互联，同时依托 Hillstone 高性能多核安全网关的综合安全功能，解决了高性能线路备份问题，同时还为企业的网络环境提供了更加安全、高效的保障。

苏宁集团构建安全高效的企业数据中心

苏宁集团视信息化为企业神经系统，建立了集数据、语音、视频、监控于一体的信息网络系统，有效支撑了全国300 多个城市、数千个店面、物流、售后、客服终端运作和十多万人的一体化管理。

Hillstone 提供了 4 台 SG-6000-G3150 企业安全网关组成的解决方案，其中两台部署在集团互联网出口，为内网员工提供互联网接入服务；两台部署在应用服务器区域前，开启 IPS 功能，为服务器提供各类攻击防御的安全服务。

需求分析

2011 年苏宁集团总部员工入住新办公大楼，并将集团数据中心搬迁至新大楼。同时随着苏宁集团应用增多，苏宁易购等 B2C 服务访问量加大，员工不断增加，原有网关设备及服务器区域安全设备已经不堪重负，亟需高性能高可靠性安全解决方案以实现有效的访问控制，保护数据中心安全，保障网络的连续性并且对网络行为控制和监督。

解决方案

Hillstone 在了解到用户的需求后，整个项目解决方案的拓扑如下图所示:

- **访问控制管控不同用户的访问权限**

Hillstone SG-6000-G3150 企业安全网关部署在互联网出口及数据中心处，实现 HA 双机热备，创建多个安全域，将服务器，内部办公网、互联网分别放在不同的安全域中，起到控制、隔离、和防护的作用。

- **开启IPS功能避免黑客入侵**

为保证各类应用服务特别是 B2C 电子商务的可靠性和安全性，在服务器区域的两台 SG-6000-G3150 企业安全网关开通 IPS 功能，提供 2-7 层全方位的安全防护可以对当前常见的攻击手段进行报警和阻断，并且通过配置日志服务器，完整的记录攻击来源。

- **高可靠的冗余备份**

通过 Hillstone SG-6000-G3150 企业安全网关的 HA 功能为网络层提供会话级别的状态同步机制，保证在设备切换过程中数据传输的连续性及网络的持久畅通，甚至在设备进行主备切换的时候不会中断会话，有效增强了网络的可靠性。

- **网络行为控制规范员工上网行为**

通过部署的 Hillstone SG-6000-G3150 企业安全网关，开启对 P2P 应用控制，节省网络资源；通过 URL 和关键字过滤，禁止员工访问不健康网站或发布不负责任的言论，彰显苏宁集团的社会责任心。

运行效果

Hillstone SG-6000-G3150 企业安全网关在苏宁集团部署上线后，设备运行稳定，高性能保证 CPU 和内存负载一直持续在较低水平。在近 5 个月内，服务器区域前的开启 IPS 功能的设备，为苏宁集团阻挡近 5000 次各类攻击，为各类应用提供了有力的安全保障。

保利房地产远程接入安全传输保障

保利房地产（集团）股份有限公司是中国保利集团控股的大型国有房地产上市公司，也是中国保利集团房地产业务的主要运作平台，目前公司已完成以广州、北京、上海为中心，覆盖 40 个城市的全国化战略布局，拥有 119 家控股子公司，业务拓展到包括房地产开发、建筑设计、工程施工、物业管理、销售代理以及商业会展、酒店经营等相关行业。随着业务的发展以及对网络业务的需求，保利房地产（集团）股份有限公司需要在总部和各分支机构间建设安全可靠的企业网络，保障数据传输的安全。

Hillstone 通过在保利房地产（集团）股份有限公司总部和各分支机构的互联网接入处部署 Hillstone 高性能企业安全网关，开启安全防御、带宽管理、VPN 功能，确保通过 VPN 专线提供不间断的安全、稳定的网络服务。

需求分析

保利房地产（集团）股份有限公司建设可靠安全的企业网络，对总部及分支机构进行网络的安全整改，需要防火墙设备具备安全防护、带宽管理、VPN 高速互联的特点。具体需求有：

- 高性能安全：随着业务的发展，保利房地产（集团）股份有限公司总部及分支机构网络规模及流量不断扩大。同时，网络中时常会受到攻击，病毒威胁也越来越多。因此，需要高性能安全网关来保障业务的高效、稳定、安全；
- 保障用户正常业务访问：保利房地产（集团）股份有限公司需要对网络中过渡占用带宽的 P2P 下载及网络视频进行流量控制，保障其他正常的业务访问；
- VPN 专网：保利房地产（集团）股份有限公司总部和各分支机构之间需要通过 VPN 专网来保障各种业务、数据交互及通讯的安全，防止数据被窃听和篡改造成企业损失。

解决方案

Hillstone SG6000-M6110 企业安全网关部署在保利房地产（集团）股份有限公司总部和各分支机构互联网接入处，分支机构通过 IPSec VPN 和总部互联，移动办公人员通过 SSL VPN 进行安全远程接入，并在各出口设备上开启网络攻击防御、带宽管理等功能保障业务和数据安全。本方案有如下特点：

- **高性能一体化综合安全防御保障业务安全**

Hillstone 企业安全网关能够实现集成多种安全技术的一体化综合防御，不但能针对 DoS/DDoS 和常见攻击进行有效的攻击防护，还能够在深度应用识别基础上可针对 HTTP、FTP、SMTP、POP3、IMAP 协议的应用进行全并行流扫描和病毒过滤，采用统一检测引擎技术，按照优化后的最佳处理流程，一次解包全并行处理，减少延时提升效率，实时阻断木马、病毒、蠕虫、间谍软件通过 web 页面、邮件等应用向内网渗透，保障了企业网的业务安全。

- **细粒度流量控制保障正常业务访问**

Hillstone 企业安全网关在在识别应用协议流量的同时，能够采用多种缓存、队列调度算法对用户带宽进行质量保障（QoS）。对企业网内 P2P、网络视频等过渡占用带宽的行为进行细粒度限制，为其他人员的正常的 Web 浏览、电子邮件等业务提供更好的保障。

- **专业VPN保障数据传输安全**

Hillstone 企业安全网关上开启 VPN 功能，VPN 技术通过隧道、加密、认证等特性在网络中建立专网，有效避免服务器重要数据被恶意拦截和窃取，为保利房地产（集团）股份有限公司总部和分支机构间的数据安全传输提供保障。

运行效果

通过部署 Hillstone 企业安全网关，解决了保利房地产（集团）股份有限公司 VPN 高速互联的需求，使得总部和各分支机构形成虚拟的局域专网，保证了数据的安全。设备上线以来，运行非常稳定，为保利房地产（集团）股份有限公司打造了安全可靠的企业网络。

紫金矿业集团打造安全可靠的企业网络

紫金矿业集团股份有限公司集团为满足新办公大楼的网络应用需求及进一步提升集团信息安全，为集团信息化应用提供稳定、安全的网络环境，需要对集团总部网络系统进行重新规划建设。

Hillstone 针对紫金矿业集团的网络现状、实际需求和投资预算，在总部新大楼及矿山区域各部署一台 Hillstone SG-6000-G2120 企业安全网关。Hillstone 针对新机房改造项目，在紫金新数据中心核心区域部署 2 台 SG-6000-X5100 数据中心防火墙对集团网络进行综合安全管理，提升网络利用率以及安全防护等效果。

需求分析

紫金矿业集团原有的中心机房网络拓扑按照：核心——汇聚——接入的三层架构搭建，不同级别的交换设备及防火墙、SSL VPN 等设备，60 余台服务器，运行着 OA、ERP、内外网站、档案管理、综合报表平台、财务公司资金管理系统、视频会议系统等多项应用，租用了包括电信、移动、联通等三条互联网宽带专线。原网络在互联网边界部署了防火墙设备，但是随着网络的发展，需要支持包括多线路负载均衡，应用识别，防病毒及流控等功能，原设备无法支持，需要对现有设备进行更新。

解决方案

总部新大楼及矿山区域各部署一台 Hillstone SG-6000-G2110 企业安全网关，具有如下特点：

- 多线路负载均衡，根据 ISP 路由，实现运营商线路优选，并实现线路冗余互；
- 网关防病毒，对大楼办公区 1100 多个信息点、酒店及矿山区域提供网关防病毒扫描；
- 抗攻击模块，抵御内外网地址扫描，欺骗，洪水等一些列攻击；
- QoS：针对办公区域实现按 IP 及应用结合的 QoS 管控，并通过统计集功能实现内网流量趋势查看；
- 结合 MIB 库，通过 SNMP 协议纳入到现有的网管监控；

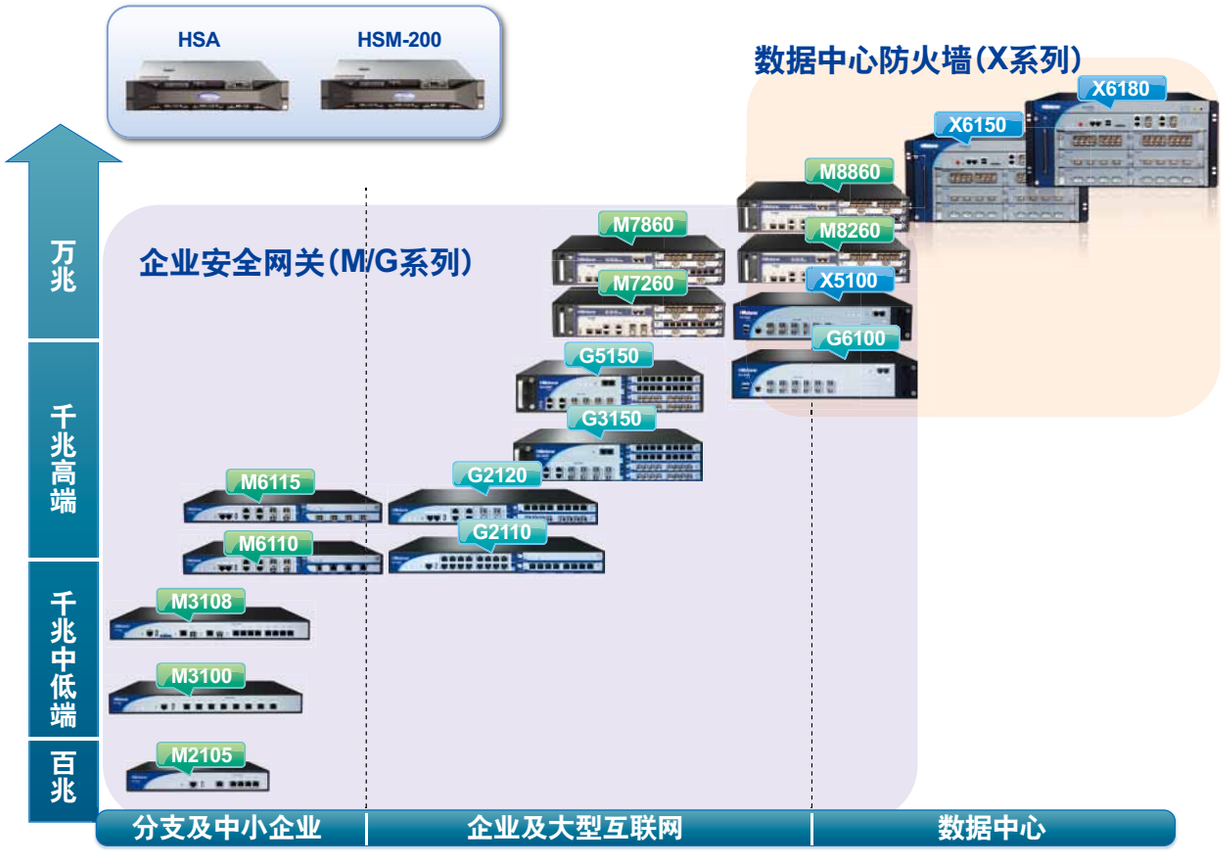
- **新数据中心核心区域部署2台SG-6000-X5100数据中心防火墙，具有如下特点：**
  - 双向 20G 万兆核心接入，高可靠 HA 部署；
  - 针对不同的部门及服务器资源，自定义不同的安全域以实现有效的权限管控，并通过策略命中数功能可以全面了解策略执行情况；
  - 启用抗攻击模块，抵御内外区域地址扫描，欺骗，洪水，ARP 欺骗等一些列攻击；
  - 结合 MIB 库，通过 SNMP 协议纳入到现有的网管监控；

拓扑图如下所示:

运行效果

通过在数据核心区域以及总部大楼、矿山部署 Hillstone 企业安全网关及数据中心防火墙，有效的提升了紫金矿业集团网络的整体安全性，以及可管理性。Hillstone 安全设备简单易用的操作界面，丰富专业的功能，灵活的组网方式，为集团信息化安全提供了保障。

Hillstone 安全产品介绍



数据中心防火墙 X 系列产品介绍

X 系列是专为数据中心设计的电信级高性能、高容量、高可扩展性、高可靠性防火墙产品。其全并行设计为设备提供了高达 20~100Gbps 的处理能力，有效地满足了数据中心数据集中化以及虚拟化带来的高性能和高容量的业务处理需求；可扩展设计为设备提供了丰富的业务扩展能力，在满足数据中心业务动态性增长需求的同时有效地保护用户投资；电信级可靠性设计保障了数据中心业务网络的 7 × 24 小时不间断运转。

Hillstone 企业安全网关产品介绍

Hillstone 企业安全网关是 Hillstone 推出的一系列新一代多核安全网关产品，其基于角色、深度应用的安全架构，突破了传统防火墙只能基于 IP 和端口来防范的限制。Hillstone 企业安全网关模块化设计提供了强大的性能扩展和丰富的业务扩展能力，有效保护用户投资。Hillstone 企业安全网关处理能力达到 600M~40Gbps，并为用户网络提供基于角色、深度应用安全的访问控制、 IPSec/SSL VPN、应用带宽管理、病毒过滤、入侵防御等安全服务。

Hillstone SG 系列产品功能规格表

防火墙	• 全新一代基于应用的防火墙 • 支持路由功能（静态路由、动态路由、ISP 路由、策略路由等） • 支持 NAT/PAT 功能（SNAT、DNAT 功能），支持各种应用协议的 NAT 穿越（FTP、TFTP、HTTP、SUN RPC、RTSP、Microsoft RPC、H323、SIP、RSH、SQL NETv2） • 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
访问控制	• 基于安全域的访问控制 • 基于时间的访问控制 • 基于 MAC 的访问控制 • IP-MAC 端口地址绑定
网页访问控制	• 提供网页分类，并支持基于网页分类类别的访问控制 • 支持自定义 Web 页面类别
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
高可用性 (HA)	• 关键部件冗余 • 主 / 主模式（A/A）和主 / 备模式（A/P） • 配置同步 • 基于会话级别的同步 • 对等模式，解决非对称流量问题
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
攻击防护	• 支持 TCP/IP 攻击防护 • 支持扫描保护 • 支持 Flood 保护 • 支持二层攻击防护
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 • 支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描 • 超过 90 万的病毒特征库，病毒库可以在线更新、本地更新
入侵防御 (IPS)	• 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 • 特征库在线更新、本地更新 • IPS 在线帮助

用户认证	• 支持本地用户认证 • 支持外部服务器用户认证（RADIUS、LDAP、MS AD） • Web 认证 • 802.1X
管理	• 支持命令行管理 • 支持通过 WebUI（HTTP、HTTPS）进行管理 • 支持通过 Console 口管理 • 支持通过 Telnet 远程进行管理
日志	• 支持用户行为流日志、NAT 转换日志、攻击实时日志、流量警告日志、上网行为管理日志、网络入侵监测日志 • 支持地址绑定协议 • 支持实时流量统计和分析功能 • 支持安全事件统计功能
LLB 负载均衡	• 在多链路环境下，同时提供了入方向和出方向的负载均衡功能 • Outbound 相关功能 PBR 支持 ECMP 以及权重、支持内置 ISP 路由和动态探测 • Inbound 相关功能支持 SmartDNS（支持 DNS A 记录解析）、支持动态探测 • 链路健康检查支持 arp、ping、dns
IPv6	Interface：支持手动配置、Linklocal 地址自动生成、无状态地址自动配置、EUI-64 NDP：NS/NA、RS/RA、DAD IPv6 选项：TCP、UDP、ICMP、Fragment、Hop_by_hop dest、mobility（只支持正常转发，不支持移动 IPv6）、esp、ah、none、route（支持转发但不支持对路由其选项处理） Flow：分片重组 ICMPv6 DNSv6 PMTU 路由：静态路由 安全：AD、NDP defender、Policy、ACL、DENY Session、LongTime Session、ALG 过渡技术：dual stack、6in4 手工 tunnel、6to4 自动 tunnel、NAT-PT、DS-lite、DNS64 and Nat64 管理和维护：SNMP、MIB、Telnet、SSH、ftp 客户端、http/https server、PING 模式：支持透明模式、路由模式和混合模式
APP	• 全新一代基于应用行为和特征的应用识别 • APP 识别引擎单独升级，方便用户升级应用识别模块，不必每次都要更换 OS 版本 • 超过几百种以上的应用特征库 • 应用特征库可以通过网络实时更新
虚拟防火墙	• 物理防火墙可以在逻辑上划分成多个虚拟防火墙 • 每个虚拟防火墙系统都可以被看成是一台完全独立的防火墙设备，拥有独立的系统资源 • 每个虚拟防火墙都可以被独立管理 • 不同型号的物理防火墙设备支持的最大虚拟防火墙个数不同，支持 License 控制虚拟防火墙个数的扩展

除非另有说明，否则所列出的性能，容量和特性是基于运行 StoneOS®5.0 的系统，实际结果可能会因 StoneOS® 版本和部署情况而异。

注：SG-6000-X6150、SG-6000-X6180 不支持病毒过滤、入侵防御、网页访问控制

Hillstone SG 系列产品性能规格表——X 系列

指 标	SG-6000-X6180	SG-6000-X6150	SG-6000-X5100
			
防火墙吞吐量（标配 / 最大）	100Gbps	100Gbps	20Gbps
IPSec 吞吐量 (1)	72Gbps	42Gbps	8Gbps
最大并发连接数（标配 / 最大）	6,000 万	5,000 万	500/1,000 万
防病毒吞吐量 (2)	/	/	1.5Gbps
IPS 吞吐量 (3)	/	/	3Gbps
每秒新建连接数	180 万 (4)	100 万 (5)	20 万 (5)
IPSec 隧道数	20,000	20,000	20,000
最大 SSL VPN 用户数	10,000	10,000	10,000
管理接口	1 个配置口，1 个 AUX 口，2 个 USB 2.0 口	1 个配置口，1 个 AUX 口，2 个 USB 2.0 口	1 个配置口，1 个 AUX 口，2 个 USB 2.0 口
网络接口	4 个千兆 Combo 接口 (1 个管理接口 +3 个 HA 接口）	4 个千兆 Combo 接口 (1 个管理接口 +3 个 HA 接口）	1 个千兆电口，12 个 SFP 口，2 个 XFP 口
扩展模块槽	10 个通用扩展槽、2 个系统控制模块扩展槽	10 个通用插槽、2 个系统控制模块插槽	/
扩展模块选项	SCM-20，SSM-80，QSM-80，IOM-16SFP-80，IOM-4XFP-80，IOM-2MM-B，IOM-2SM-B	SCM-20、SSM-20、QSM-20、IOM-16SFP、IOM-4XFP，IOM-2MM-B，IOM-2SM-B	/
电源规格	2+2 冗余热插拔电源，最大功率 1300W	2+2 冗余热插拔电源，最大功率 1300W	双冗余热插拔电源，200W
外形尺寸 (W × D × H, mm)	5U (440 x 590 x 225)	5U (440 x 590 x 225)	2U (440 x 520 x 88)

注：(1) IPSec 吞吐量用 Presharekey+AES256+SHA-1，用 1400 字节数据流测试得到；
(2) 防病毒吞吐量使用带附件的 HTTP 流量测试得到；
(3) IPS 吞吐量使用 HTTP 流量，启用所有 IPS 规则，并打开双向检测方式下得到；
(4) 每秒新建连接数使用 HTTP 的方法测试得到；
(5) 每秒新建连接数使用持续建立 TCP 三次握手连接的方法测试得到。

Hillstone SG 系列产品性能规格表——G 系列

指 标	SG-6000-G6100	SG-6000-G5150	SG-6000-G3150
			
防火墙吞吐量（标配 / 最大）	10Gbps	8/10Gbps	6/8Gbps
IPSec 吞吐量 (1)	8Gbps	4Gbps	2.5Gbps
最大并发连接数（标配/最大）	400/800 万	300/400 万	250/400 万
防病毒吞吐量 (2)	1.2Gbps	800Mbps	500Mbps
IPS 吞吐量 (3)	3Gbps	2.5Gbps	1.2Gbps
每秒新建连接数 (4)	20 万	12 万	6 万
IPSec 隧道数	20,000	10,000	6,000
最大 SSL VPN 用户数	10,000	6,000	4,000
管理接口	1 个配置口，1 个 AUX 口， 2 个 USB 口 2.0 口	1 个配置口，1 个 AUX 口， 1 个 USB 2.0 口	1 个配置口，1 个 AUX 口， 1 个 USB 2.0 口
网络接口	1 个千兆电口，12 个 SFP 口	4 个千兆电口，8 个 SFP 口	4 千兆电口，8 个 SFP 口
扩展模块槽	/	4 个通用扩展槽	4 个通用扩展槽
扩展模块选项	/	8 端口千兆电口模块， 8 端口千兆 SFP 模块，4 端口千兆 Bypass 模块，存储扩展模块，2 端口万兆 XFP 模块	8 端口千兆电口模块， 8 端口千兆 SFP 模块，4 端口千兆 Bypass 模块，存储扩展模块
电源规格	双冗余热插拔电源，200W	双冗余热插拔电源，450W	热插拔单电源 450W，可选双冗余
外形尺寸 (W × D × H, mm)	2U (440 x 520 x 88)	2U (440 x 520 x 88)	2U (440 × 520 × 88)

指 标	SG-6000-G2120	SG-6000-G2110
		
防火墙吞吐量（标配 / 最大）	4Gbps	2Gbps
IPSec 吞吐量 (1)	1.5Gbps	1Gbps
最大并发连接数（标配 / 最大）	100/200 万	100/200 万
防病毒吞吐量 (2)	350Mbps	250Mbps
IPS 吞吐量 (3)	800Mbps	500Mbps
每秒新建连接数 (4)	4.5 万	3 万
IPSec 隧道数	4,000	2,000
最大 SSL VPN 用户数	2,000	1,000
管理接口	1 个配置口，1 个 AUX 口，1 个 USB 2.0 口	1 个配置口，1 个 USB 2.0 口
网络接口	4 个千兆电口，4 个 SFP 口	16 个千兆电口
扩展模块槽	2 个通用扩展槽	1 个通用扩展槽，1 个存储模块槽
扩展模块选项	8 端口千兆电口模块，8 端口千兆 SFP 模块，4 端口千兆 Bypass 模块，存储扩展模块	
电源规格	冗余 150W	单 75W，可选双冗余
外形尺寸 (W × D × H, mm)	1U (436 x 366 x 44)	1U (436x366x44)

注：(1) IPSec 吞吐量用 Presharekey+AES256+SHA-1，用 1400 字节数据流测试得到；
(2) 防病毒吞吐量使用带附件的 HTTP 流量测试得到；
(3) IPS 吞吐量使用 HTTP 流量，启用所有 IPS 规则，并打开双向检测方式下得到；
(4) 每秒新建连接数使用持续建立 TCP 三次握手连接的方法测试得到。

Hillstone SG 系列产品性能规格表——M 系列

指 标	SG-6000-M8860	SG-6000-M8260	SG-6000-M7860	SG-6000-M7260
				
防火墙吞吐量(标配/最大)	40Gbps	32Gbps	25Gbps	16/20Gbps
IPSec 吞吐量 (1)	25Gbps	18Gbps	15Gbps	9/12Gbps
最大并发连接数（标配 / 最大）	1000 万	800 万	700 万	500/600 万
防病毒吞吐量 (2)	4Gbps	3Gbps	2.5Gbps	1.5/2Gbps
IPS 吞吐量 (3)	7Gbps	4Gbps	3.5Gbps	2/3Gbps
每秒新建连接数	40 万 (5)	30 万 (5)	25 万 (5)	15/20 万 (5)
IPSec 隧道数	20,000	20,000	20,000	20,000
最大 SSL VPN 用户数	10,000	10,000	10,000	10,000
管理接口	1 个配置口，1 个 AUX 口，1 个 USB 口，1 个 HA 口，1 个管理口	1 个配置口，1 个 AUX 口，1 个 USB 口，1 个 HA 口，1 个管理口	1 个配置口，1 个 AUX 口，1 个 USB 口，1 个 HA 口，1 个管理口	1 个配置口，1 个 AUX 口，1 个 USB 口，1 个 HA 口，1 个管理口
网络接口	4 个千兆电口，4 个 SFP 口	4 个千兆电口，4 个 SFP 口	4 个千兆电口，4 个 SFP 口	4 个千兆电口，4 个 SFP 口
扩展模块槽	4 个通用扩展槽	4 个通用扩展槽	4 个通用扩展槽	4 个通用扩展槽
扩展模块选项	IOC-8GE-M、IOC-8SFP-M、IOC-4GE-B-M、IOC-2XFP-Lite-M、IOC-4XFP	IOC-8GE-M、IOC-8SFP-M、IOC-4GE-B-M、IOC-2XFP-Lite-M、IOC-4XFP	IOC-8GE-M、IOC-8SFP-M、IOC-4GE-B-M、IOC-2XFP-Lite-M	IOC-8GE-M、IOC-8SFP-M、IOC-4GE-B-M、IOC-2XFP-Lite-M
电源规格	双冗余热插拔电源，最大功率 450W	双冗余热插拔电源，最大功率 450W	双冗余热插拔电源，最大功率 450W	双冗余热插拔电源，最大功率 450W
外形尺寸 (W × D × H,mm)	2U (440 × 520 × 88)	2U (440 × 520 × 88)	2U (440 × 520 × 88)	2U (440 × 520 × 88)

指 标	SG-6000-M6115	SG-6000-M6110	SG-6000-M3108	SG-6000-M3100	SG-6000-M2105
					
防火墙吞吐量(标配/最大)	4Gbps	2/4Gbps	1/2Gbps	1Gbps	600Mbps
IPSec 吞吐量 (1)	1.5Gbps	1Gbps	500Mbps	500Mbps	200Mbps
最大并发连接数（标配 / 最大）	100/200 万	100/200 万	60/100 万	40/100 万	10/ 20 万
防病毒吞吐量 (2)	350Mbps	250Mbps	70Mbps	70Mbps	50Mbps
IPS 吞吐量 (3)	800Mbps	500Mbps	200Mbps	200Mbps	100Mbps
每秒新建连接数 (4)	4.5 万 (4)	3 万	1.2 万	1 万	0.4 万
IPSec 隧道数	4,000	4,000	1,000	1,000	512
最大 SSL VPN 用户数	2,000	2,000	500	500	128
管理接口	1 个配置口，1 个 AUX，1 个 USB 2.0 口	1 个配置口，1 个 AUX，1 个 USB 2.0 口	1 个配置口，1 个 USB 2.0 口	1 个配置口，1 个 USB 2.0 口	1 个配置口，1 个 USB 2.0 口
网络接口	4 个千兆电口，8 个 SFP 口	8 个千兆电口，4 个 SFP 口	8 个千兆电口，2 个 GE/SFP 口	8 个千兆电口	5 个千兆电口
扩展模块槽 (6)	1 个存储模块槽	1 个存储模块槽	1 个 SD 卡槽	/	/
扩展模块选项	存储扩展模块	存储扩展模块	/	/	/
电源规格	单 100W，可选双冗余	单 100W，可选双冗余	单 45W，可选双冗余	单 45W	单 15W
外形尺寸 (W × D × H,mm)	1U (436 × 366 × 44)	1U (436 × 366 × 44)	1U (442 × 241 × 44)	1U (442 × 241 × 44)	桌面型 (300 × 165 × 44)

注：(1) IPSec 吞吐量用 Presharekey+AES256+SHA-1，用 1400 字节数据流测试得到；
(2) 防病毒吞吐量使用带附件的 HTTP 流量测试得到；
(3) IPS 吞吐量使用 HTTP 流量，启用所有 IPS 规则，并打开双向检测方式下得到；
(4) 每秒新建连接数使用持续建立 TCP 三次握手连接的方法测试得到；
(5) 每秒新建连接数使用 HTTP 的方法测试得到；
(6) SD 卡 (SDHC 格式) 由用户自己购买，推荐 : 金士顿 /SanDisk 等。

Hillstone NETWORKS

网络无际 安全有界

Hillstone 专注网络安全 坚持技术创新 保障业务稳健

www.hillstonenet.com.cn

销售与服务热线: 400-828-6655

版权所有 © 2012，Hillstone Networks 保留所有权利。

北京总部
地 址: 北京市海淀区王庄路1号清华同方科技广场D座6层
邮 编: 100083
电 话: +86(10)8236 6000
传 真: +86(10)8236 6018

销售与服务热线: 400-828-6655

Copyright © 2013，Hillstone Networks版权所有，保留所有权利。
Hillstone、Hillstone Networks标识、山石网科、StoneOS、StoneManager、Hillstone PnPVPN、UTM Plus均为Hillstone Networks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 Networks网站(www.hillstonenet.com.cn)。

文档编号：IN-10.01-0000-0000-0308-Ch-06