南山之桥 Xwall™UTM X6 系列内容墙

技术白皮书

版权声明

信息更新

本产品最新版本信息、升级信息以及相关技术文档将在本公司www.nsbic.com 网站上及时推出，敬请留意。如有升级改动，恕不另行通知。

联系方式：

NSBIC 北京：北京市海淀区之春路 27 号量子芯座

电话：010-82350648

传真：010-82350647－612

NSBIC 上海：上海中山北路 3064 号绿洲广场 A 座

电话：021-62606635

传真：021-62235173

NSBIC 重庆：重庆市九龙坡区渝州路华轩之路 39 号

电话：023－68618432

传真：023－68618432

NSBIC 西安：西安市碑林区文艺路 19 号

电话：029－87487933

传真：029－87487933

NSBIC 成都：成都高新技术产业开发（西区）创新中心 C241

电话：028－66184999/87848739

传真：028－87848739

前言

南山之桥微电子有限公司成立于2002年。公司创办人团队是由硅谷归国，拥有多年数据通信和网络安全芯片设计经验的精英组成。2003年成功开发出华夏网芯®系列芯片，成为全球第三家可以提供高性能路由、交换芯片的高科技企业；不久公司又推出全球首款集成防火墙、路由、交换功能为一体的核心芯片——Xwall™；全球领先的数据包过滤的千兆线速芯片——蓝凤凰™。

南山之桥专注于数据通信与信息安全领域的技术开发，成功地研发出基于自主知识产权ASIC芯片的UTM内容墙系列产品。率先在全球推出全网安全芯片组解决方案，同时也是国内第一家推出UTM内容墙产品的企业。

UTM发展趋势

随着网络的发展和Internet的广泛应用，如今的网络安全威胁已经由原来的正对TCP/IP协议本身的弱点进行攻击，转向针对特定系统和应用漏洞的攻击和入侵。回顾2005年以来，各种蠕虫和木马为主的网络化的病毒，加上利用网络协议以及应用漏洞进行攻击与入侵行为，给全球经济带来极大的损失。据统计，仅2004年，各种攻击给全球造成1690亿美元的经济损失。

越来越多的企业发现，安全威胁不仅来自外部，企业内部的不当互联网访问，滥用互联网以及泄漏行为等等，同样会引起一系列的安全问题。据IDC报告，70%的安全损失是来由企业内部原因造成，而不当的资源利用以及员工上网行为是“罪魁祸首”。比如：网页浏览特别是一些反动的黄色的网页浏览，BT下载，IM实时通信，P2P文件共享等行为。不当的资源利用以及员工上网行为带来了各种间谍软件，恶意程序和各种病毒，导致企业网络资源耗尽、机密外泄、内部网络病毒泛滥等一系列的安全问题。

要解决这样的问题，传统的方法是购买防火墙，防病毒软件以及内容控制产品。把这些产品简单的堆叠起来费力又费钱不说，还不安全。以企业安全系统为例，目前大多数是由防火墙，IDS/IPS，防病毒，流量控制以及内容管理组成。这些价格不菲的产品在物理结构上是可以堆叠在一起的，运营维护起来及其复杂，即使是专业技术水品很高的管理维护人员也很难制定一个科学的整体安全策略以协调各个设备的工作，而且这些设备往往还存在功能重叠的问题，造成了资源的浪费。问题最严重的是，这些安全产品可能来自不同的厂商，没有统一的管理平台，产品之间无法进行有效的信息交流，很容易形成安全盲区。整合式、模块化的UTM产品正是为解决上述问题孕育而生的，随着硬件水平的提高和统一管理平台的成熟，为UTM的发展创造了技术上的支撑。

UTM（统一威胁管理）产品的出现可以称得上是一场及时雨，它是信息安全技术融合趋势得深化和具体表现。

UTM设备应该具备的三大特点

由于UTM设备是串连接入的安全设备，因此UTM设备本身性能和可靠性就要求高，同时，UTM时代的产品形态，实际上是结合了原有的多种产品的技术精华，在统一的产品管理平台下，集成防火墙，VPN，网关防病毒，内容过滤，流量控制，抗DOS攻击等众多产品功能，实现多种防御功能。因此防火墙发展的最终形态就是UTM。

UTM具备3大特点。

一是，建立一个更高，更强，更可靠的墙，除了传统的访问控制以外，防火墙还应具备对拒绝服务、黑客攻击等这样一些外部的威胁起到综合检测网络安全协议防御。真正的安全不能只停留在底层，我们需要构建和治理的效果，能够实现七层协议保护，而不仅局限于二到四层保护。

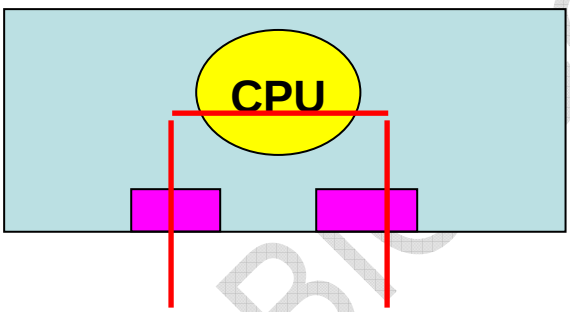
二是，要有高可靠，高性能的硬件平台作平台支撑。对于UTM实现的防火墙，在保障网络安全的同时，不能成为网络应用的瓶颈，

防火墙/UTM 必须以高性能，高可靠性的专用芯片以及专用硬件平台为支撑，以避免 UTM 设备在复杂环境下其可靠性和性能不佳可能带来的对用户核心业务正常运行的威胁。

三是，UTM 一体化的统一管理。由于 UTM 设备集多种功能于一身，因此，它必须具有统一控制和管理的平台，使用户能够有效的管理，从而在应对各种各样攻击威胁的时候，更好的保障用户的网络安全。

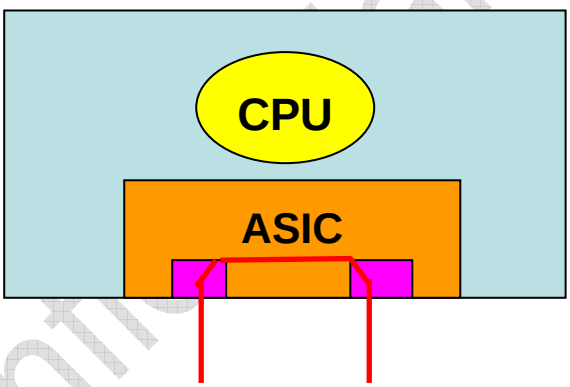
实现 UTM 的三大硬件体系

X86 架构：目前在国内信息安全市场上，防火墙厂商普遍采用的是通用 CPU 配合软件的技术方案。虽然很多的厂商也把它称之为硬件 UTM，但实际上都是基于 X86 架构的服务器或工控机，其使用的是 Intel 通用的 CPU。这类 UTM 设备一般运行在经过裁减的操作系统上（通常是 LINUX 或 BSD），所有的数据包解析和审查工作都由软件来完成。但由于 CPU 处理能力和 PCI 总线速度的制约，所以效能低下，稳定性差。



NP 架构：NP 架构的 UTM 使用的是网络处理器，而网络处理器是面向网络应用领域的特定指令的处理器，是面向数据分组处理的，具有体系结构特征或特定电路的，软件可编程的控制器件。通过灵活的软件体系提供硬件级别的处理。采用多内核并行处理结构，片内处理器分为核心处理器和数据分组协处理器。核心处理器通常负责非实时的管理任务；数据分组处理器进行实时、线速数据分组处理。但是就是由于 NP 这样的多 CPU 内核提供的灵活性，造成软件编写的复杂度提高，成本上升。越是复杂的东西越是不稳定。NP 由于软件的复杂性，造成整个系统的不稳定性。对于一个安全产品来说稳定也是一个很重要的部分。

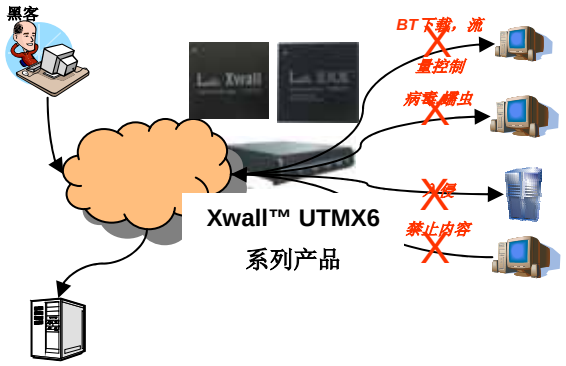
ASIC 架构：ASCI UTM 是南山之桥公司通过专门设计的一系列的 ASIC 芯片逻辑进行硬件加速处理，通过把指令或计算逻辑固化到芯片中去，获得很高的处理能力，由此明显的提升 UTM 的性能。南山之桥设计的高可编程的 ASIC 采用了更灵活的设计，能够通过软件改变应用逻辑，具备更广阔的适应能力。另外，由于 ASIC 芯片架构的 UTM 将包括状态表项，路由表项，VLAN 表项，URL 关键字过滤等存储在芯片中，进一步提高了 UTM 的处理速度。



Xwall™ UTM 全系列产品都采用了 ASIC 的设计方案。

产品介绍

Xwall™ UTM X6—F6500 系列产品是针对电信运营商等大型、超大型网络而设计的千兆线速硬件 UTM 产品。高吞吐量以及高稳定性得益于 CPU＋多 ASIC 的架构。内置于芯片中的路由表，VLAN 表，TCP/UDP/ICMP 状态包，在任意数量的规则下，在持续并发 200 万的情况下，Xwall™ UTMF6500 产品可以达到所有包长数据包全线速。通过外加的 CCL-3000 系列插卡模块，在千兆线速下实现 L2-L7 层的全硬件并行全包检测和分流，并支持流的查找，流量控制和应用分流。可以线速的完成病毒检测，P2P 和 IM 即时软件的流量控制管理、细粒度的访问控制、关键字过滤等功能，并支持用户自定义安全特性检查。灵活的模块化设计帮助客户最大限度的保护现有投资，并为用户升级设备提供了方便快捷的方式。



功能特点

- λ 基于自主创新的 ASIC 架构
- λ 灵活模块化的设计保护客户的投资；
- λ 在维持 200 万并发的情况下可以达到 64－1518 的所有包长线速通过；
- λ 最大的新建连接数可以达到 20 万/秒；
- λ 支持策略路由，最大限度方便客户的使用；
- λ 内建抗 DOS 模块，有效的抵御外来的攻击
- λ 每个端口 QOS 单播 8 级，多播 2 级。方便客户保证带宽；
- λ 通过 CCL-3000 系列可以非常方便的实现防病毒，IDS/IPS，URL 过滤以及流量控制等功能；
- λ 支持双机热备，提供秒级的切换；
- λ 系统的管理和系统的网络数据处理平面分离，在提供高性能的同时保证了系统的安全性

系统功能列表

用户管理	用户权限分级
	用户维护
	用户登录验证
	用户非法登录处理
	用户信息加密存储
系统管理	系统升级
	防火墙基本参数维护
	防火墙日志服务器参数维护
	防火墙本地管理
	防火墙远程管理（集中化）
	防火墙配置备份
	防火墙配置恢复
	防火墙启动配置保存
	防火墙状态查看
	防火墙重启
网络工作模式	路由模式
	透明模式
	混合模式
VLAN 支持	支持 vlan 中继、终结、透传
策略配置	基于对象化的规则配置
	基于协议的 ACL 规则控制
	基于源 IP 地址的 ACL 规则控制
	基于目的 IP 地址的 ACL 规则控制
	基于源端口的 ACL 规则控制
	基于目的端口的 ACL 规则控制
	一对一源 NAT/PAT
	多对多源 NAT/PAT
	多对一源 NAT/PAT
	一对多源 NAT/PAT
	基于协议的源 NAT/PAT
	基于源 IP 地址（可取非）的源 NAT/PAT
	基于目的地址（可取非）的源 NAT/PAT
	基于源端口的源 NAT/PAT
	基于目的端口的源 NAT/PAT
	一对一目的 NAT/PAT
	一对多目的 NAT/PAT（负载均衡）
	基于协议的目的 NAT/PAT
	基于源 IP 地址的目的 NAT/PAT
	基于目的地址的目的 NAT/PAT

	基于源端口的目的 NAT/PAT
	基于目的端口的目的 NAT/PAT
	IP/MAC 绑定防地址欺骗
	在策略管理上提供添加、删除、修改、保存、打开、应用等操作
路由管理	基于目的地址的路由
	基于源地址的路由
双机热备	防火墙配置信息实时备份，双机自动检查工作状态进行主从切换
蓝凤凰扩展功能	BT 限流
	关键字过滤
	URL 过滤
	CC 攻击
	病毒过滤
抗 DOS 攻击设置	基于阀值的抗攻击设置
SNMP	支持 SNMP 监控防火墙状态信息
防火墙管理器操作日志审计	方便快捷的查询
	打印功能
	导入数据
	导出数据
防火墙事件日志审计	导入数据
	导出数据
	多种方便快捷的查询
	打印功能
防火墙通信日志审计	基于流的日志记录
	导入数据
	导出数据
	多种方便快捷的查询
	多种方便快捷的统计
	打印功能

Xwall™UTM X6—F6500 系列架构

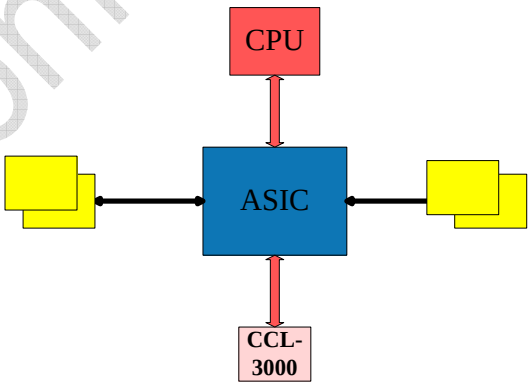
Xwall™ UTM X6—F6500 系列产品是南山之桥公司自主研发的产品。其核心技术来自与 ASIC 芯片的设计和研发。

ASIC 芯片主要功能：

- λ L2－L7 层交换/路由/包过滤
- λ 高效的动态过滤技术
- λ NAT 网络地址转换（SNAT/DNAT/PAT）
- λ QOS 带宽保证
- λ 内容过滤和流量控制

由于管理功能和数据处理功能分开，在保证网络高负载的情况下可以对网络数据进行有效的处理。

南山之桥公司充分的考虑到了客户的需求，推出了 Xwall™ UTM X6—F6500 系列产品，在最大限度的保证网络安全的同时解决了网络管理、网络速度和网络成本的矛盾。



从上图的架构来分析南山之桥的 Xwall™ UTM 全系列产品的拥有领先的技术特点。

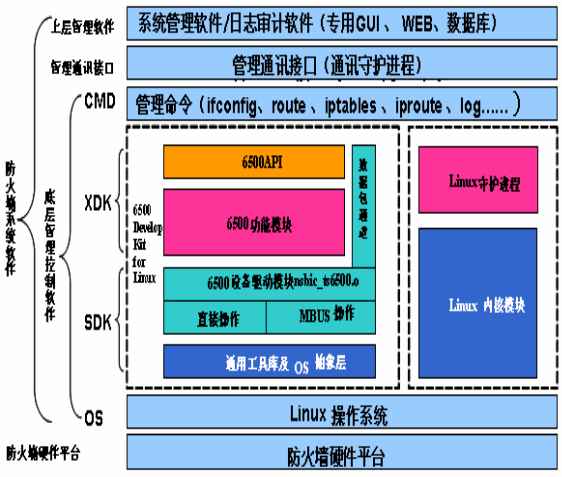
- λ Xwall™ UTM 系列产品的管理通过和芯片完全隔离的端口来访问，提高了安全性。在网络大负载的情况下也可以及时修改和调整策略，增加了设备的稳定性。

- λ 数据的处理全部依靠芯片来处理。保证了在复杂的网络环境如电信等大型超大型中支持 200 万并发连接，同时可以达到 64 字节至 1518 字节数据包全线速转发。避免了因为防火墙造成的网络速度的问题。
- λ 在网络中有很多的用户对视频等及时应用

要求比较高，南山之桥充分的考虑到这点，在芯片中实现了单播 8 级，多播 2 级的 QOS 的功能，最大限度的保证了用户带宽的使用。

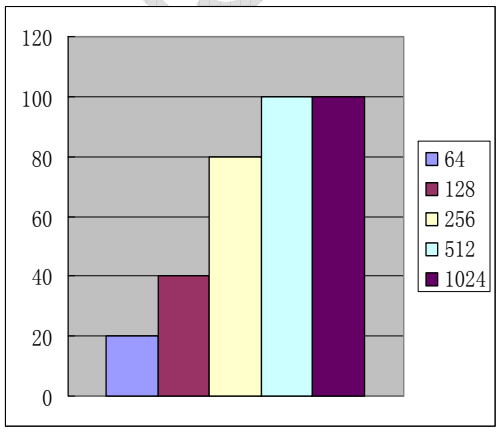
λ 通过自主研发的 CCL-3000 系列模块，可以实现 L2-L7 层的过滤，如：流量控制，内容过滤等一系列的功能。完全可以按照用户的需求，提供拥有不同功能的 CCL-3000 模块（防病毒，IDS/IPS，内容过滤，BT 等流量控制以及反垃圾邮件,VPN 等一系列的功能模块）。

Xwall™UTM x6—F6500 系列软件架构

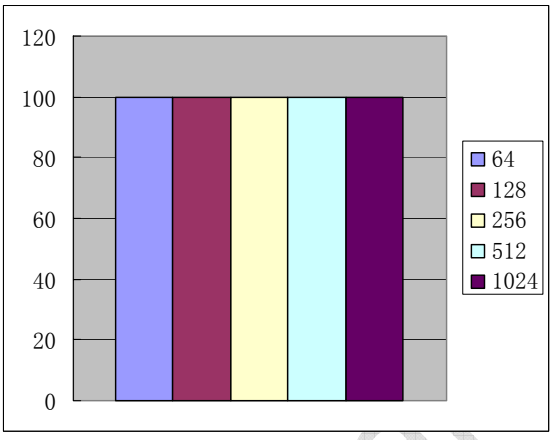


同类产品对比

南山之桥 Xwall™ UTM X6 与同类防火墙的对比

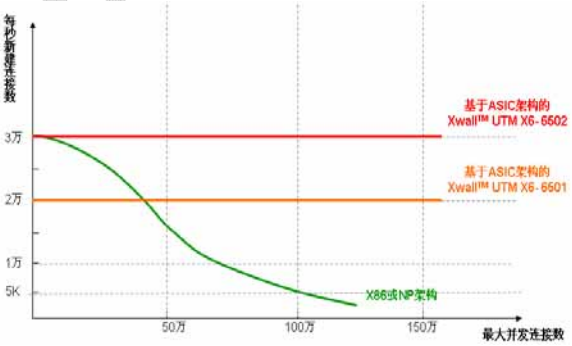


X86 架构吞吐量



基于 ASIC 架构的 Xwall™UTM X6—F6500 吞吐量

从上面两个表中可以很清楚的发现，X86 结构的防火墙产品在小包特别是 64 和 128 包长的吞吐能力一直在 40%不到，而 ASIC 是专门为处理网络而设计的芯片，对 64－1518 任意的包长都是线速。



并发连接数、每秒新建连接数

从上图中可以很清楚的发现，X86 以及 NP 的吞吐能力随着并发连接数的增加，效能逐渐的下降，到 120 万并发连接的时候，新建连接数不到 5K/Sec，这个主要是由于维护并发连接的时候需要消耗大量的资源。而对于专门为网络任务设计的 ASIC，就没有这样的问题。

并发连接数是指防火墙对多数据流的处理能力，是防火墙能够同时处理点对点连接的最大数目。它反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力，因此该性能指标直接影响防火墙所能处理的最大信息量，是电信运营商/ISP/IDC/教育网运营商为大量用户提供服务所依赖的关键技术指标之一。

Xwall™ UTM 的数据平面采用流水线和并行处理技术，在流水线操作中每个数据包会根据不同处理需求使用不同的模块。实际上，一个连接的存在是因为这个连接的数据包得到某一条规则的允许，否则也没有必要建立连接。因此在连接表中并不需要存放数据包的 IP 地址或端口资料，因为这些资料可在规则里找到。

经过上述分析，Xwall™ UTM 采用了 hash 和片上 RAM 等技术，使其能在较小的存储空间存储最大 200 万的并发连接。不管是检测一个连接还是两百万个连接的信息，数据包都能在预知的固定时间内得到处理。这也是 Xwall™ UTM 在任何应用情况下都能保持千兆线速处理能力的一个重要因素。

Xwall™全系列产品

多种工作模式适应不同的环境

一谈到工作模式，通常会想到：透明模式可在不改动现有路由结构下方便部署；路由模式是一种普遍的网络模式；混合模式则可以实现灵活的网络部署。然而现在 NAT 也被列为新的网络模式。在企业越来越依赖 IT 系统的今天，防火墙不仅必须能支持各种不同的网络模式，更重要的是也要能满足企业组建网络和执行访问控制的要求。下图给了一个企业典型的应用环境。

从图可以看到，访问企业的Internet用户都渴望减少在维持IP地址方面的费用，因此拥有DNAT功能是防火墙所必备的基本要求。而有些部门因为需要通过Internet与相关部门联系，因此SNAT也成了对防火墙的基本要求。通过透明网桥连接同一子网内的不同物理端口也成了一个基本的要求。

总结上述的要求，防火墙需要能够同时支持路由/桥接/NAT 功能，而 Xwall™ UTM 在设计时充分考虑了这些复杂的网络环境要求。其交换特性保证任何端口在执行访问控制功能的同时，也能实现透明模式交换。NAT 也是流水线结构上的一个标准模块，不论端口之间采用何种网络连接模式，NAT 总能正常工作，包括 1：1 的映射以及 N：M 多端口映射。

随着企业越来越依赖基于网络的各种应用，包括关键信息系统如 VoIP 和视频会议等，网络应用对网络的服务质量提出了具体的要求指标：最小延迟，最小抖动和保证带宽。因此作为网络中的一个控制信息流的关键设备，防火墙必须能够对不同应用进行带宽管理。

QOS，点对点应用不可缺少的功能要求，并非单独一台防火墙设备所能保证的，如果没有其他安全设备的配合，防火墙无法做到对延迟与带宽的保证。因此在设计防火墙的时候一定要从网络核心的角度设想，考虑到全部需要。有一点必须肯定，如果防火墙本身的数据吞吐能力不能维持线速，延迟时间大而又不够稳定，那么防火墙无论采取什么样的队列分类算法都将无法保证QoS的正确实现。

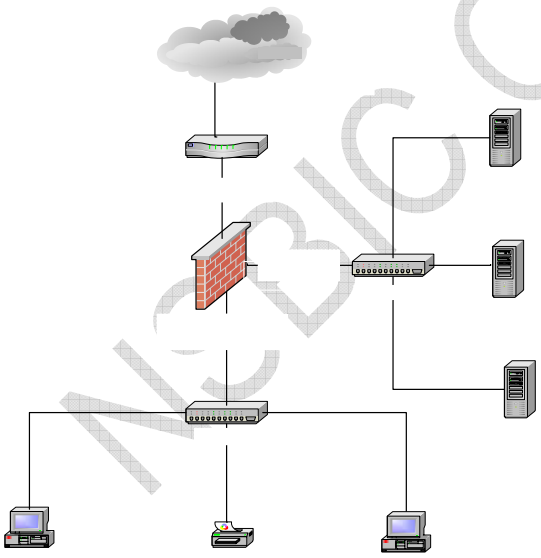
Xwall™ UTM 因为拥有“全天候”的线速处理能力，低至10us的延迟使它具备了对流量进行管理的基础条件。同时，借鉴了核心路由设备在队列管理方面的经验，Xwall™ UTM

也为系统管理员提供了灵活的管理机制，以精确的分类提供保证带宽和最大带宽。在每个端口上 Xwall™ UTM提供了单播8级不同的优先级队列，多播2级的优先级队列，从而能够满足企业将应用分为实时业务、关键业务、非关键业务、非业务类数据等级的需求。

在队列管理方面， Xwall™ UTM充分借鉴了高端路由交换设备的队列管理结构，在物理接口上执行流控制管理，从而保证数据能以稳定的延迟时间进行转发。 Xwall™ UTM为每个物理端口提供了单播8个不同优先级的队列，多播2个不同的优先级的队列充分提高了高优先级、小带宽应用（如VoIP）对队列的利用效率。

为部署保证带宽和最大带宽， Xwall™ UTM提供了最小128Kbps带宽管理粒度，网络管理员能有效地部署带宽管理，从而保证企业宝贵的带宽资源能够被正确的应用。

深刻理解了各类网络需求之后， Xwall™ UTM 的设计完全能够适应各种不同的复杂网络环境。



成功案例

学校网络背景：

四川某大学校园网提供多种接入方式，用户可以自由地使用有线、无线、拨号等手段在任何时间、任何地点连入校园网。基于目录服务的校园网用户管理系统，实现了校园网用户的统一认证、统一管理和统一计费。

在提供普通以文字和图像为主要形式的信息服务的同时，四川某大学校园网上还有丰富的音视频流媒体资源，以及大量的专业信息服务。校园网为四川某大学的教学、科研、行政办公和生活服务创造了一个良好的信息网络环境，在学校的人才培养、学科建设、科学研究、行政管理和师生员工的生活等方面产生了明显的效益。

项目的规划目标：

1. 在极高的网络负载条件下，进行精细的网络访问控制，保证正常的通信；
2. 较低的网络延时，保障视频会议等及时的业务；
3. 有效的过滤非法网站和不良论坛；
4. 完善的日志记录，帮助分析网络。

项目的具体实现方案以及特点：

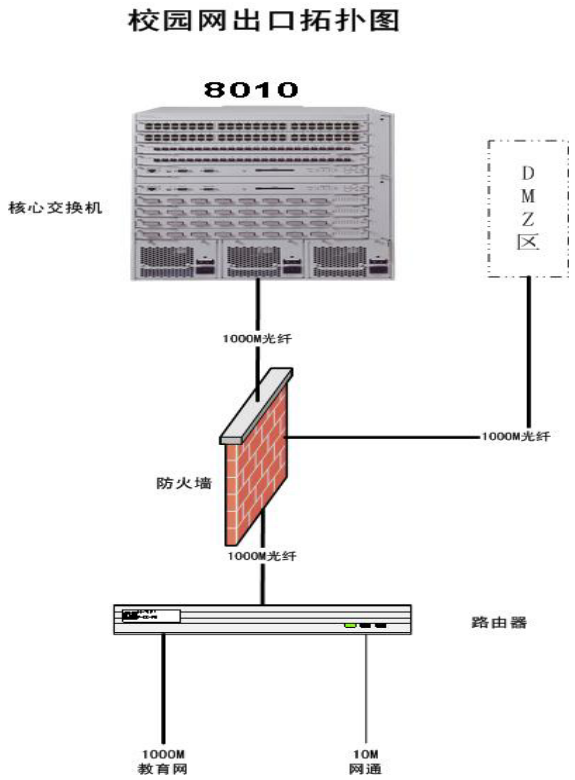


图 1:拓扑图

客户收益：

1、 解决了在无防火墙情况下，内网因病毒发作，病毒数据包阻塞校园网干路的问题
2、 解决了因原有防火墙运行不稳定，不定周期造成学校校园网出口断网的问题
3、 与原有防火墙相比明显提高了校园网出口流量
4、 在 Xwall™ UTM X6—F6500 的保护下，校园网内外网通讯高效、稳定

用户评价：

Xwall™ UTM X6—F6500 防火墙为南山之桥自主开发的电信级的高性能、高可靠性的专业防火墙设备。

从最终用户的角度来说，对南山之桥防火墙在我校校园网总出口的使用情况满意，尤其是其设备优异的性能，及服务的优质高效（组网拓扑详见图 1）。

设备在配置了三千余条访问控制策略的情况下，校园网出口流量最高达到 1.2G 以上（详见图 2，图 3），并发连接数最高达到 100 万，满足整个大学几万用户同时进行网络通讯的需求。

在使用该防火墙前，校园网内部充斥着大量病毒数据包，病毒发作期间，校园网出口流量明显异常，几乎完全阻塞了校园网出口，DMZ 区服务器群也因此近乎瘫痪。在使用了南山之桥防火墙产品后，病毒数据包阻塞校园网出口，攻击服务器群的现象未再出现。
从 2006 年 1 月初开始使用 Xwall™ UTM X6—F6500 防火墙组网，截至到目前为止，该设备 24 小时不间断运行达 3 个月，实际效果良好，运行期间保证了我校校园网良好的运行稳定性和传输的高效性。Xwall™ UTM X6—F6500 防火墙满足了校园网出口的使用需求。

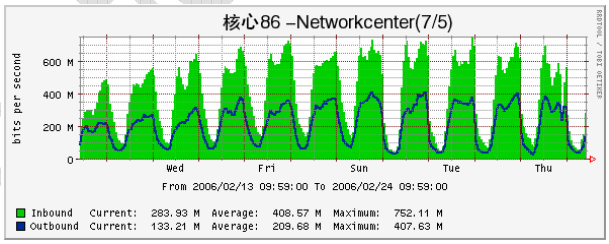


图 2　流量统计图

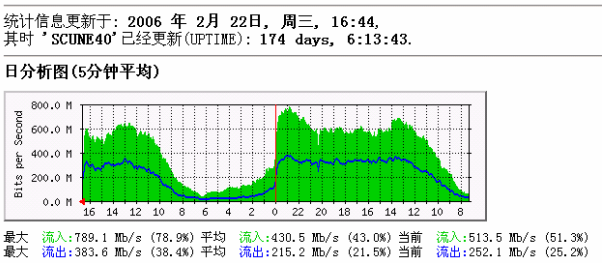


图 3　流量统计图