网络卫士防火墙4000

NGFW 4000

业界最新一代防火墙——核检测防火墙
基于独创的先进的安全构架和实现技术

技术白皮书

北京天融信公司

2004 年5 月

注意

本白皮书中的内容是天融信网络卫士防火墙NGFW 4000技术说明书。本材料的相关权力归北京天融信公司所有。白皮书中的任何部分未经本公司许可，不得转印、影印或复印。

天融信网络卫士防火墙NGFW 4000

技术白皮书

本资料将定期更新，如欲获取最新相关信息，请访问天融信公司网站：www.topsec.com.cn
您的意见和建议请发送至：PLMC@topsec.com.cn

北京天融信公司
北京市海淀区知春路49号希格玛大厦4层，100080
4F Beijing Sigma Center No.49,Zhichun Road，Hai dian District, Beijing
电话(TEL)：010-82611122
传真（FAX ）：010-62304552
电子信箱：marketing@topsec.com.cn

目　　录

前　　言

北京天融信公司是中国网络安全行业的领先企业，是目前国内最大的专业从事网络安全技术研究、产品开发和安全服务的高科技企业。同时天融信公司正向集团化、国际化迈进，努力成为中国网络安全领域内最优秀最具国际竞争力的企业。

天融信公司最早成立于 1995 年，目前公司总部设在北京，形成北京、武汉、成都三大研发中心，同时在上海、广州、西安、沈阳、成都、长沙、武汉等 29 个省市设有分支机构，拥有 500 多名信息安全专业研发、咨询与服务人员。

天融信公司于 1996 年推出了填补国内空白的中国第一套自主版权的防火墙产品，随后几年又推出了 VPN、IDS、安全监控、安全审计、安全管理、过滤网关等产品。组织并构建了 TOPSEC 联动协议安全标准，提出了一套集各类安全产品及集中管理、集中审计为一体的全面的、联动的、高效的、易于管理的 TOPSEC 安全解决方案。

2000 年至 2003 年，天融信公司连续四年市场份额均居国内安全厂商之首。特别指出的是，国际权威咨询机构 IDC 统计：天融信 2003 年下半年防火墙市场份额达到了 17.28%，名列所有国内外安全厂商第一位，打破了国内安全厂商长期处于弱势地位的局面，为国内网络安全企业树立了新的里程碑。到目前为止，天融信公司拥有覆盖全国，涉及政府、电信、金融、军队、能源、交通、教育、流通、邮政、制造等行业的万余家客户群体。

第一章 网络卫士防火墙NGFW 4000 概述

网络卫士防火墙 4000（NGFW 4000）
业界新一代核检测防火墙

网络卫士防火墙4000 是天融信公司积8年来的防火墙开发经验和应用实践及天融信广大用户宝贵建议基础之上，基于对网络安全的深刻理解，融合网络科技的最新成果，独创的系列安全构架和实现技术，经过多年的研究和近两年的开发所完成的最新一代防火墙产品。

防火墙4000 通过使用大量独创性专利技术，构造了一个安全、高效、可靠、应用广泛、方便灵活的防火墙系统；同时为客户提供最优秀的性能及功能保证；另外成熟的实现和支持了天融信的TOPSEC 协议和体系。

防火墙4000 特别适用于网络结构复杂、应用丰富、高带宽、大流量的大中型企业骨干级网络环境。

第二章 网络卫士防火墙NGFW 4000介绍

1 系统的组成

1.1 系统组成

- **网络卫士防火墙**NGFW4000 **（硬件）：是一个基于安全的操作系统平台的自主版权高级通信保护控制系统。**
- **日志管理器软件系统：是一个可运行于** Linux **、**Windows2000 **系统下，对网络卫士防火墙**NGFW 4000 **提供的访问日志信息进行可视化审计的管理软件。**
- **防火墙集中管理器软件：是一个可运行于**Windows98 **、**Windows2000 **系统下，对处于不同网络中的多个网络卫士防火墙进行集中管理配置的管理软件。**

1 .2 硬件配置

电气性能

a. **电源：**AC 110/220V 50/60HZ **，**3.0A **（最大），**260W **（最大）**

b. **环境规范：**

运行温度： 0 — 45 **摄氏度**

非运行温度： -20 — 65 **摄氏度**

相对湿度： 10 — 90%@40 **摄氏度，非冷凝**

执行的国家标准

GB/T18336-2001

GB/T18019-1999

GB/T18020-1999

参考的安全规范及标准(相对参考)

UL 1950

EN 41003

AS/NZS 3260

AS/NZS 3548 Class A

CSA Class A

FCC Class A

EN 60555-2

VCCI **（**ClassII **）**

抗干扰性

IEC 1000 4 2 **（**ESO **）**

IEC 1000 4 3 **（辐射敏感性）**

IEC 1000 4 4 **（电快速瞬变）**

IEC 1000 4 5 **（电源）**

IEC 1000 3 2 **（谐波）**

2 产品型号和技术指标

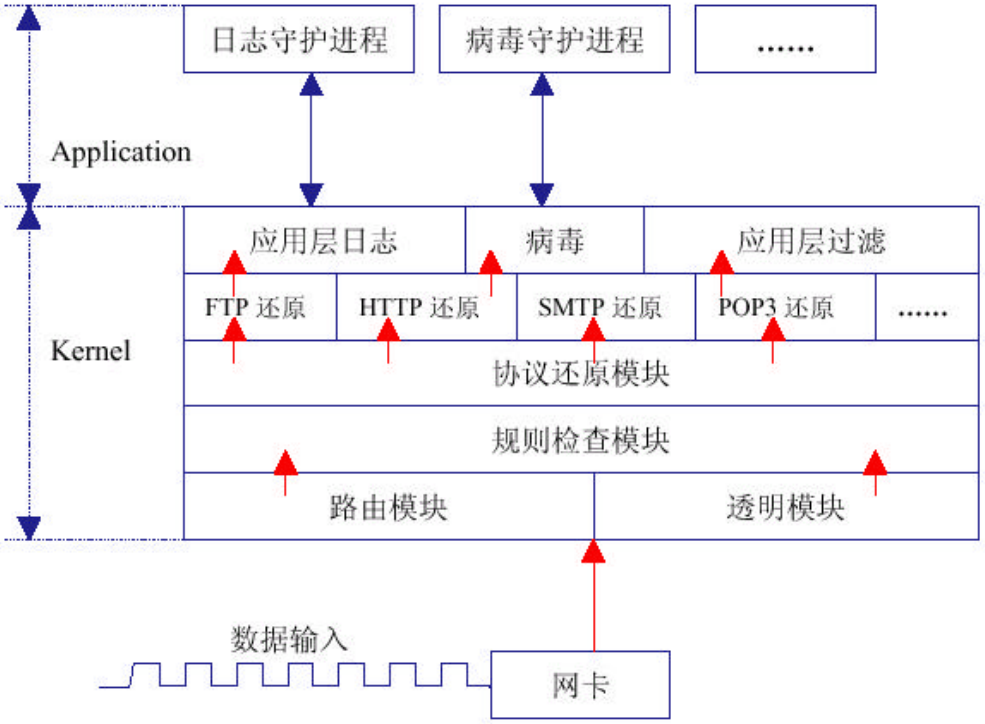
产品名称	产品型号	吞吐率	接口说明
网络卫士防火墙4000（中文） NGFW 4000(英文)	NGFW 4000-E	100M(小包线速)	3个10/100BASE-TX口,最多可扩展7个端口
	NGFW 4000-E-VPN(S)	100M(小包线速)	3个10/100BASE-TX口,最多可扩展7个端口
	NGFW 4000-E-VPN(E)	100M(小包线速)	3个10/100BASE-TX口,最多可扩展7个端口
	NGFW 4000	100M	3个10/100BASE-TX口,最多可扩展7个端口
	NGFW 4000-VPN(S)	100M	3个10/100BASE-TX口,最多可扩展7个端口
	NGFW 4000-VPN(E)	100M	3个10/100BASE-TX口,最多可扩展7个端口
	NGFW 4000-S	100M	3个10/100BASE-TX口,最多可扩展5个端口
	NGFW 4000-S-VPN(S)	100M	3个10/100BASE-TX口,最多可扩展5个端口
	NGFW 4000-S-VPN(E)	100M	3个10/100BASE-TX口,最多可扩展5个端口
	NGFW 4000-T	100M	3个10/100BASE-TX口,最多可扩展5个端口
	NGFW 4000-T-VPN(S)	100M	3个10/100BASE-TX口,最多可扩展5个端口
	NGFW 4000-T-VPN(E)	100M	3个10/100BASE-TX口,最多可扩展5个端口

3 NGFW 4000 体系结构

“网络卫士”防火墙4000 采用独创的最新最先进的技术－核检测技术，即基于OS 内核的会话检测技术，在OS 内核实现对应用层访问控制。它相对于包过滤和应用代理防火墙来讲，不但更加成功地实现了对应用层的细粒度控制，同时，更有效保证了防火墙的性能。

“网络卫士”防火墙4000 的体系结构就是为了实现基于OS 内核的会话检测技术而设计的，具体如下图所示。网卡接收的数据首先交给路由模块和透明模块进行处理，然后将数据交给规则检查模块，如果规则检查模块在规则匹配过程中需要对数据进行还原，那么数据将被提交给协议还原模块，协议还原模块根据具体协议的类型，将数据交给具体协议的还原模块去完成。比如FTP 协议数据就交给FTP 还原模块进行还原、HTTP 协议数据就交给HTTP 协议还原模块去处理、SMTP 协议数据就交给SMTP 还原模块去处理，然后根据还原的结果来执行相应的安全策略。

从图中可以看出，所有的协议还原模块都工作在内核层次，因此其还原的效率非常高，处理的速度也非常快。同 时由于基于OS 内核的会话过滤技术可以对整个通讯会话进行全部或者部分的还原，所以其输出的日志信息将非常完整。包括传统的会话日志（主要描述通讯的时间、源目地址、源目端口、通信流量、通讯协议等）；和命令日志（主要描述使用了那些命令，执行了那些操作）。用户可以根据需要记录不同的日志，从而为日志分析、事后追踪提供了更多的依据。



4 NGFW 4000 系统特点

4.1 采用独创的安全技术

核检测技术，即基于OS 内核的会话检测技术，在OS 内核实现对应用层访问控制。它相对于包过滤和应用代理防火墙来讲，不但更加成功地实现了对二到七层的细粒度控制，同时，更有效保证了防火墙的高性能，NGFW 4000系列防火墙最高能支持240万的并发连接数。

4.2 采用先进的设计思想

NGFW 4000系列防火墙采用面向资源的设计方法，对不同对象的具体的组成资源，如文件、防火区域、节点对象、子网对象、对象组；并提供一些特殊对象用于安全和管理，如：文件资源对象、透明网络对象、应用端口对象、认证数据库对象、用户对象、URL对象，关键词对象，邮件对象和NAT 保留端口对象等等，可以进行全方位安全控制，极大的提高了网络安全性，并保证了配置的方便性。

4.3 独特的防火墙策略体系

面向资源的防火墙策略体系。建立独立的防火区域，通过中央管理接口、管理端口协议、节点对象、子网对象的运用，实现层次分明而又立体化的策略机制，灵活安全的通讯策略和访问策略，使防火墙的策略配置简单，且便于维护，可以方便地定义各种粒度的安全规则。

4.4 更加安全和易于扩展的系统结构

天融信公司通过八年来技术积累和沉淀，在防火墙系统结构设计上，不断的进行技术突破与攻关，NGFW 4000 拥有安全可靠软硬件系统结构，并且具有强大的扩展能力。

NGFW4000 软硬件使用模块化的设计，用户可以根据需要，通过网络下载相应的模块，通过升级程序增加新的功能，以适应动态发展的安全需要。并且还可依据用户的特定安全需求定制特殊功能。硬件上支持对接口的灵活扩展，可以通过灵活的扩展来适应业务发展的需要，从而保护投资。

4.5 多级过滤的立体访问控制

为保证系统的安全性和提高防护能力，增强控制的灵活性，NGFW4000 采用了多级过滤措施：以基于 OS 内核的会话检测技术为核心，提供从链路层到应用层的全面安全控制，在 MAC 层提供基于 MAC 地址的过滤控制能力，同时支持对各种二层协议过滤功能，在网络层和传输层提供基于状态检测的分组过滤，可以根据网络地址、网络协议以及 TCP 、UDP 端口进行过滤，并进行完整的协议状态分析；在应用层通过重写通讯会话的部分或者全部，提供对高层应用协议命令、访问路径、内容、访问的文件资源、关键字、移动代码等的内容安全控制；同时还直接支持丰富的第三方认证，提供用户级的认证和授权控制。NGFW4000 的多级过滤形成了立体的全面的访问控制机制，实现全方位的安全控制。

4.6 超强的防御功能

高级的 Intelligent Guard 技术提供了强大入侵防护的功能，能抵御常见的各种攻击，包括 Syn Flood、Smurf、Targa3、Syn Attach、ICMP flood、Ping of death、Ping Sweep、Land attack、Tear drop attack)、Smurf、IP address sweep option(IP 地址扫描攻击)、Filter IP source route option(过滤 IP 源路由选项)、Syn fragments(同步碎片)、No flags in TCP(TCP 无标记)、ICMP 碎片、大包 ICMP 攻击、不明协议攻击、IP 欺骗、IP security options(IP 安全选项)、IP source route(IP 始发路由)、IP record route(IP 记录路由) 、IP bad options(IP 损害选项)、IP 碎片、端口扫描等几十种攻击，防火墙 4000 不但有内置的攻击检测能力，还可以和 IDS 实现联动。这不但提高了安全性，而且保证了高性能。

4.7 严格的安全区域保护

NGFW4000 采用多安全区域体系，NGFW4000 防火墙的每个物理接口对应一个独立的防火区域，每个区域的安全策略只对该区域有效。每个区域可以单独设置自己的默认安全策略，所有对该区域的访问都将匹配与该区域对应的安全策略。也可以设定是否允许从该区域 PING 、TELNET 以及管理防火墙。

可以定义某个接口连接的网络为安全服务器网络（SSN——Security Server Network ），将提供信息访问服务的服务器安装于该网络区域内，与内、外网络从物理上隔离开来，并提供专门的安全保护。NGFW4000 提出的 SSN 概念有别于传统的所谓 DMZ 停火区模式，它是一种更为积极的安全防护理念：一般情况下，SSN 主机不允许主动向内、外网发起连接请求，只允许向内、外网回应其请求数据包；外网用户也只能访问 SSN 上的主机，不能访问内部网主机。即 SSN 与外部网之间受防火墙保护，同时 SSN 与内部网之间也受防火墙保护，即使 SSN 受破坏，内部网络仍处于防火墙保护之下。同时 NGFW4000 提供的 SSN 保护功能针对用户最常提供的 Web 访问服务进行专门保护，能定时检查 SSN 区 Web 服务器，进行校验，一旦发现服务器被入侵修改，能够根据备份的信息及时恢复服务器内容，将服务器被入侵修改造成的影响减至最小。

4.8 强大的地址转换能力

NGFW4000 拥有强大的地址转换能力。NGFW4000 同时支持正向、反向地址转换，能为用户提供完整的地址转换解决方案。

正向地址转换用于使用保留IP 地址的内部网用户通过防火墙访问公众网中的地址时对源地址进行转换。NGFW4000 支持依据源或目的地址指定转换地址的静态NAT 方式和从地址缓冲池中随机选取转换地址的动态NAT 方式，两种方式总共可以有多达32 个的不同转换地址，可以满足绝大多数网络环境的需求。对公众网来说，访问全部是来自于防火墙转换后的地址，并不认为是来自内部网的某个地址，能够有效的隐藏内部网络的拓扑结构等信息。同时内部网用户共享使用这些转换地址，自身使用保留IP 地址就可以正常访问公众网，有效的解决了全局IP 地址不足的问题。

内部网用户对公众网提供访问服务(如 Web 、FTP 服务等)的服务器如果是保留 IP 地址，或者想隐藏服务器的真实 IP 地址，都可以使用 NGFW4000 的反向地址转换来对目的地址进行转换。公众网访问防火墙的反向转换地址，由内部网使用保留 IP 地址的服务器提供服务，同样既可以解决全局 IP 地址不足的问题，又能有效的隐藏内部服务器信息，对服务器进行保护。NGFW4000 提供端口映射和 IP 映射两种反向地址转换方式，端口映射安全性更高、更节省全局 IP 地址，IP 映射则更为灵活方便。

4 .9 深层的内容安全控制功能

防火墙支持对 HTTP 的 URL 过滤、通过将 HTTP 的命令分为读、写和执行命令来控制命令的使用，达到命令级的过滤；也支持对 FTP 命令和传输文件的过滤功能，通过将文件资源和 URL 资源应用到访问规则中来控制对文件或 URL 的请求，支持对移动代码如 Vbscript、JAVA script、ActiveX、Applet 的过滤，支持页面关键词过滤，支持对邮件主题、发件人、收件人、附件类型和大小的控制功能。

4 .10 丰富的AAA功能

NGFW 4000 防火墙支持对网络用户提供丰富安全身份认证，如一次性口令（OTP）、RADIUS 、S/KEY 、SecureID 、VieCA，TACACS/TACACS+、口令方式、数字证书（CA）等常用的安全认证方法，可以使用专用的认证客户端软件进行认证和也支持 WEB 方式的认证，基于用户的安全策略更灵活、更广泛的实现了用户鉴别和用户授权的控制。并提供丰富的安全日志记录用户的安全事件。

4 .11 卓越的网络及应用环境适应能力

支持众多网络通信协议和应用协议,如 VLAN 、ADSL 、PPP 、ISL 、802.1Q 、Spanning tree 、IPSEC 、H.323 、MMS、RTSP、ORACLE SQL*NET、PPOE、MS RPC 协议等，使 NGFW 4000 防火墙适用网络的范围更加广泛，保证用户的网络应用。方便用户实施对 VOIP、视频会议、VOD 点播、数据库、等应用的使用和控制。

4 .12 灵活的工作模式

NGFW4000 支持透明接入。将NGFW4000 配置为透明工作模式，无需更改用户网络的拓扑结构就能接入用户网络中,用户网络中的主机也无需更改任何网络配置就能在防火墙安全规则的控制进行通讯。透明接入极大的方便了防火墙的接入，同时并不降低网络的安全性。

NGFW4000 还能工作在透明+路由的混合模式下，更能适应各种不同网络环境的接入，独创的混合模式源于天融信智能的路径识别技术和专用的安全协议栈技术，且 NGFW4000 在实现时进一步进行了优化，又增加了支持透明+路由＋MAP 的工作方式，灵活的工作模式方便防火墙接入各种复杂的网络和应用环境。

4 .13 丰富的接入方式

防火墙适应各种 Ethernet 的接入，支持 ISL、Dot1q、MPLS 等封装格式，支持 Trunk 即主干链路工作方式，能够同交换机的 Trunk 接口对接，并且能够实现 Vlan 间通过防火墙进行路由，满足了当今各种业务的建设需要，保证了防火墙无障碍的接入各种网络环境，最大限度的满足了用户的各种需求。千兆防火墙还支持 1000base-tx/sx/lx/zx 等各种规格的 GBIC 接口以适应各种接入方式的需要。

宽带接入已经成为目前许多企业，单位选择的接入方式。天融信防火墙提供对 ADSL 等多种宽带接入方式的支持，支持 ADSL 的按需拨号，自动地址转换等实用功能，保证安全、便捷地通过 ADSL 接入 Internet。

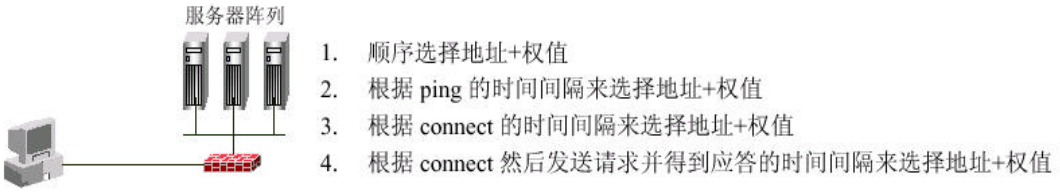
4 .14 适应复杂的核心网络

核心网络的安全性，稳定性是当今网络的焦点，如何保证核心网络的安全，保证数据的 24 小时传输成为网络安全的最关注的问题。天融信防火墙能够在核心网络中同所有核心网络设备一起实现高可用，高安全性的拓扑结构，最大限度的满足了网络的健全性，稳定性，使整个核心网络保证了不间断工作。当核心网络中的某条链路产生故障时，能够动态的切换链路，使数据不间断的传输。同时加上防火墙杰出的安全特性，使整个网络无比强壮。应用参见典型应用四。

4 .15 智能的负载均衡和高可用性

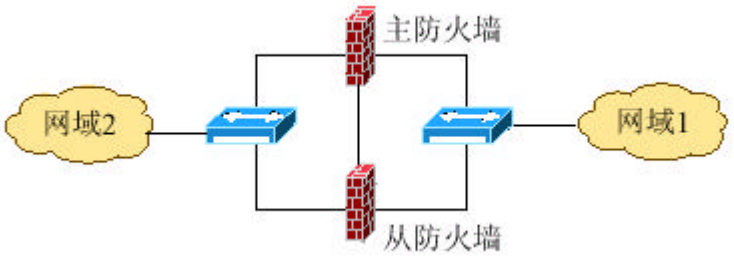
支持服务器的负载均衡

NGFW4000 防火墙可以支持一个服务器阵列，这个阵列经过防火墙对外表现为单台的机器，防火墙将外部来的访问在这些服务器之间进行均衡。



高可用性

为了保证网络的高可用性与高可靠性，NGFW4000 提供了双机备份功能，即在同一个网络节点使用两个配置相同的防火墙。正常情况下一个处于工作状态，为主防火墙，另一个处于备份状态，为从防火墙。当主防火墙发生意外宕机、网络故障、硬件故障等情况时，主从防火墙自动切换工作状态，从防火墙自动代替主防火墙正常工作，从而保证了网络的正常使用， NGFW4000的双机热备功能使用自主专利的智能状态传送协议(ISTP)，ISTP能高效进行系统之间的状态同步，实现了TCP协议握手级别的状态同步和热备。当主防火墙故障时，这台防火墙上的正在建立或已经建立的连接不需要重新建立就可以透明地迁移到另一台防火墙上，网络使用者不会觉察到网络链路切换的发生。



流量均衡

NGFW4000 支持完整生成树（Spanning-Tree）协议，可以在交换的网络环境中支持PVST和CST等工作模式，在接入交换环境时可以通过生成树协议的计算，使不同的VLAN使用不同的物理链路，将流量由不同的物理链路进行分担，从而进行流量均衡，该功能和ISTP协议结合使用还可以实现在使用高可用性的同时采用流量均衡。

4 .16 分层式管理结构

防火墙的管理采用集中的层次管理结构，实现“ 防火墙—防火区--对象—资源 ”的安全策略定义结构。配置简单、配置安全性高；管理简单、维护方便；更好的保证了性能。

4 .17 面向资源的管理机制

NGFW4000中采用面向各种对象的不同组成资源的管理机制。对象是由许多种资源组成的实体，规则建立在这种实体的基础上。资源的概念比对象控制更加细化，简化了用户规则，使规则更为直观；同时，提高了配置管理员的效率，提高了配置的灵活性。

NGFW4000提供了很多种资源，如，网络节点、子网、第三方用户、用户数据库、防火区域、文件资源、透明网络 、特殊端口、URL资源等等。

4 .18 支持远程集中管理

可通过安全的认证及管理信息的加密传输实现全局防火墙设备的集中管理。实现统一的安全策略部署，保证整个系统的安全策略的一致性，提高整个系统的安全强度。

NGFW4000 的主要配置和管理都是基于GUI（Graphic User Interface） 方式的，管理主机只需安装专门的管理软件，就可以在不同操作系统平台、不同地域对防火墙进行配置和管理，并且管理通讯数据使用加密方式。

安全集中管理最多可以同时支持对上万套防火墙设备集中的管理。

4 .19 管理安全、方便灵活

防火墙NGFW 4000 经过简单的配置即可接入网络进行通信和访问控制，GUI 管理界面提供了清晰的管理结构，每一个管理结构元素包含了丰富的控制元和控制模型。对所有管理采用加强的SSL进行加密传输，加强的SSL不仅GUI客户端对防火墙进行证书认证，防火墙也同时对客户端进行证书认证，避免了传统HTTPS不对GUI客户端进行认证的安全问题。管理员认证使用证书和密码的结合的双因素认证，管理过程进行严格的审计，实现了真正的安全管理。同时，可以支持SNMP与当前通用的网络管理平台兼容，如 HP Openview NNM、TOPSEC Manager等，方便管理和维护

4 .20 支持SSH 安全管理

为了保证远程管理的安全性，NGFW4000 不论是对管理员还是管理过程都采取了一系列安全措施：对远程管理员主机限定和同时登陆数量的限制。为了防止远程管理过程被监听和修改，还支持基于SSH 的远程登陆管理，将管理主机和防火墙之间的通讯进行加密以保证安全。

4 .21 完全支持SNMP

目前在计算机网络中应用最为广泛的网络管理标准是简单网络管理协议（SNMP）。

防火墙作为一种网络安全访问控制的基础网络设备，为它提供一种标准的网络管理方式是有必要的，NGFW4000 就提供了对这个标准协议的支持。

为了更好地支持网络集中管理，NGFW4000 提供了对SNMP 的v1 、v2 、v2c 、v3 等不同版本的支持，并与当前通用的网络管理平台兼容，如HP Openview 等，可以通过这些管理平台对防火墙的运行状况进行监控，并接收通过SNMP TRAP 发送的报警信息，帮助网络管理员找出并纠正TCP/IP 互联网中的故障。为了避免由于SNMP 本身的安全性上的缺陷而导致防火墙本身的安全性受到威胁，系统仅允许网管系统查询信息，而不允许改变防火墙的配置。

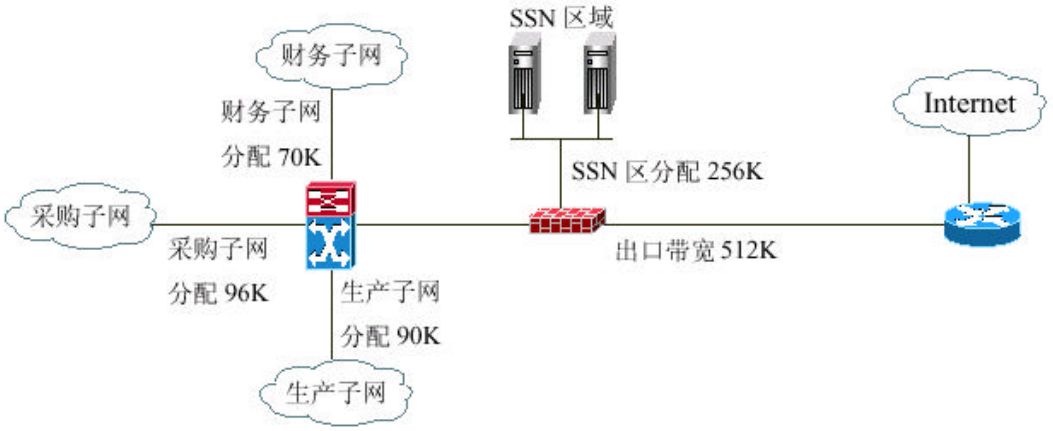
4 .22 方便的实时监控功能

能够通过GUI管理器实时监控当前防火墙上每个接口的各种网络通讯状态、当前管理连接和实时统计数据，如：网卡是否连接、网卡速率的协商方式、双工类型、链路的速率、收发的字节数、收发的报文数；收到的各种具体类型包的统计数如：链路广播报文数、IP字节、TCP字节、UDP字节、ICMP字节、ARP字节、IP广播报文、IP多播报文、分片报文、IP选项报文、校验错误报文、被拒绝请求报文、非校验的其他错误报文；防火墙CPU和内存的使用情况、当前的连接数；还能动态监视网络连接情况，显示连接的状态是正在建立中的连接，已建立的连接、未通过或正在中断的连接，或者是已经删除的连接，并且可手工删除指定连接，便于管理员实时的断开异常的连接。也可以监控当前防火墙管理客户端的连接情况。配置过滤器可以设置网络连接的监控条件，满足过滤条件的连接信息将动态显示在界面上。

4 .23 多层次带宽管理能力

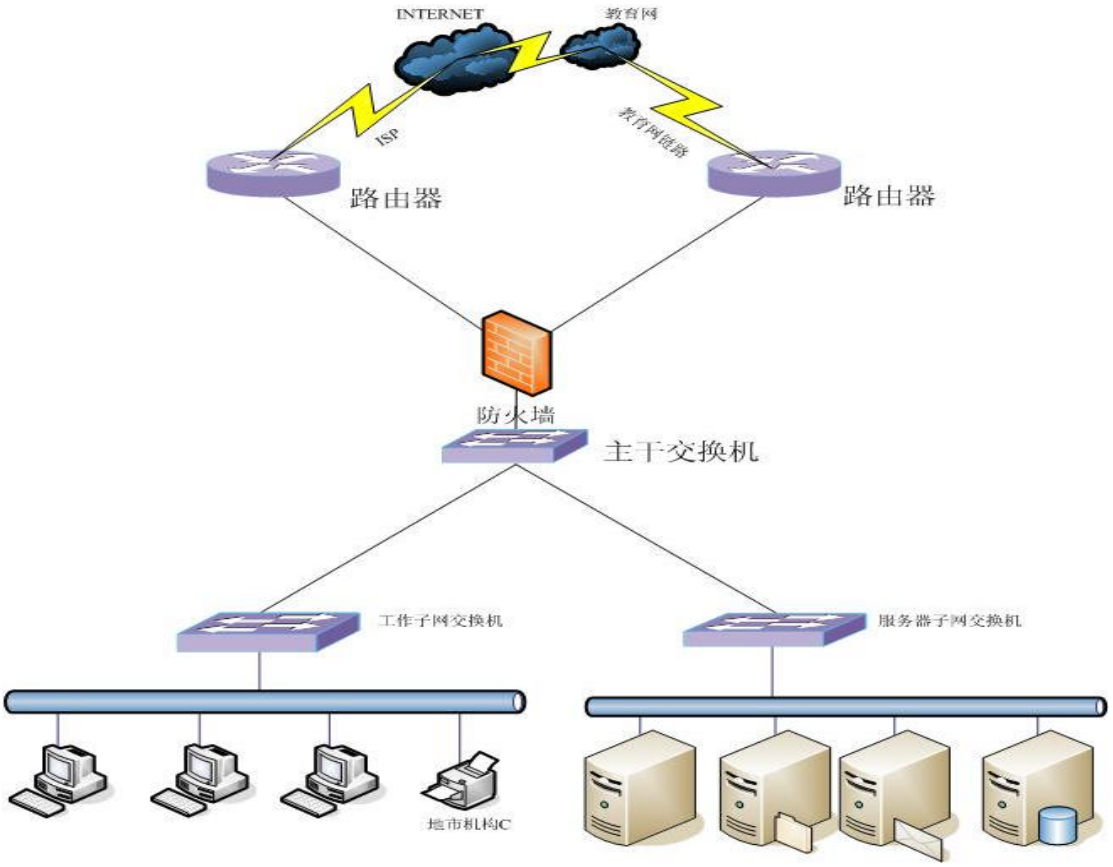
带宽管理完全虚拟了网络带宽应用的实际环境，并实现多层次的分布式管理模式，避免了单层集中管理的缺点；而且，可以实现带宽分层、带宽分级、带宽分配、带宽优化等管理，优化网络资源的应用，提高网络资源应用效率。

NGFW4000 能够允许管理员定义任意两个网络对象之间通信时的最大带宽，而且带宽可以是分层的，例如部门带宽下面有小组带宽然后是个人带宽等，可以防止带宽被滥用，保证重要的通信的顺畅。具体如下图所示：



4 .24 源、目的地址路由功能

天融信NGFW 4000防火墙产品采用一种特殊的路由技术，一般的路由技术只根据目标地址来做出路由选择，而网络卫士防火墙4000 则根据通讯的源地址和目标地址来做出路由选择。这种源目地址路由技术可以很好的支持有多个网络出口的环境，帮助进行网络流量分配。比如对于某些教育系统的网络可能同时有两条互联网出口，一条是通过教育网的线路连接到Internet ，另外一条就是申请电信的线路直接连接到互联网如图所示。



对于这种环境为了更好的利用带宽，让网络中的部分终端走教育网的出口，另外一部分终端走电信线路，这样可以很好的利用现有的带宽资源，不会造成带宽的浪费，但是在这种网络环境下，如果防火墙不支持源目的地址路由技术就很难实现，因为到互联网的目标地址都是一样的，只是来源不一样。

4 .25 优秀的性价比

强大完善的功能、优秀的性能、高的稳定性和可靠性，及方便扩展VPN 、IDS 、认证、审计、应用层安全过滤、管理等安全特性，体现了优秀的性价比，可有效地保护投资。

4 .26 强大的VPN 功能

NGFW 4000支持内建VPN功能模块。用户选择拥有VPN功能的NGFW4000，就能够与VPN 体系中的VPN网关、Windows 客户端，当然也包括另外的启用了VPN 功能的NGFW 4000互通。它们之间可以建立加密隧道进行加密通信，形成虚拟专用网，借助互联网组建安全可靠的私有网络。NGFW 4000防火墙支持内嵌VPN模块支持，支持IPSEC、IKE等国际标准，支持国家有关密码管理部门批准的密码算法；支持网关到网关、网关到远程客户端的隧道。

NGFW 4000无缝集成VPN功能，就相当于一台VPN网关与一台防火墙两套系统组合起来，更好地管理维护，而且由于是内建的功能支持，功能间的结合更加平滑易用，并且可以实现防火墙能对密文和解密后的明文进行多层次的安全控制，提供更高的安全性。

4 .27 支持VPN的大规模部署

NGFW 4000的VPN功能支持静态地址间隧道，动态地址到静态地址间的隧道；并可以和密码机产品，远程客户端产品及VPN安全管理系统（SCM）共同组成完整的VPN解决方案，自主专利的PUDP技术使防火墙支持隧道的NAT穿越，在具有SCM的解决方案中，还能支持灵活的

动态地址到动态地址间的隧道。VPN网络的工作模式支持HUB-SPOKE方式、网状连接方式，和分级的树状连接方式；，并支持数据在多隧道间的路由。

4 .28 深层的、强大的审计分析功能

提供丰富的日志信息，用户可根据特定的需要进行日志选项，可以不做日志、日志会话和日志命令。日志支持Topsec专用格式、Syslog格式及Webtrends等格式的输出，方便第三方系统对安全事件的收集、管理和分析

一个安全防护体系中的审计系统的作用是记录安全系统发生的事件、状态的改变历史、通过该节点的符合安全策略的访问和不符合安全策略的企图,使管理员可以随时审核系统的安全效果、追踪危险事件、调整安全策略。进行信息审计的前提是必须有足够的多的日志信息。NGFW4000 提供了非常强大的日志功能，用户可以根据需要对不同的通讯会话记录不同的日志。

NGFW4000 的审计日志包括如下两个部分：日志会话、日志命令。日志会话也就是传统的防火墙日志，负责记录通讯时间、源地址、目的地址、源端口、目的端口、字节数、是否允许通过。日志会话信息用来进行流量分析已经足够，但是用来进行安全性分析还远远不够；应用层日志命令在日志会话的基础之上记录下各个应用层命令及其参数，比如HTTP 请求及其要取的网页名 ;访问日志则是在应用层命令日志的基础之上记录下用户对网络资源的访问，它和应用层日志命令的区别是：应用层日志命令可以记录下大量的数据，有些用户可能不需要，如协商通信参数过程等。例如针对FTP 协议，日志会话记录下读、写文件的动作；日志命令则是在访问日志的基础之上，记录如用户发送的邮件，用户取下的网页等。天融信新一代防火墙产品可以根据用户的不同需要对不同的访问策略做不同的日志,例如有一条访问策略允许外界用户取FTP 服务器上的文件，如果做命令日志，用户就可以知道到底是哪些文件被下载。

4 .29 简单方便的配置备份与恢复

NGFW4000 提供简单方便的配置文件管理，进行配置文件的备份、下载、删除、恢复和上载。用户可以随时手工备份防火墙的配置文件，可以将备份结果下载到本地管理主机中保存，也可以将备份上载回防火墙进行恢复还原。

4 .30 支持动态IP 地址

NGFW 4000支持运行DHCP 、BOOTP 等协议的动态主机，让用户在管理方便的同时不损失安全性。对于使用DHCP 服务器来动态分配IP 地址的网络环境，很难使用IP 地址来进行访问控制，因为网络中的主机没有固定的静态IP 地址，此时的解决方式有两种：一种是让防火墙自己来充当DHCP 服务器进行IP 地址的分配，此时防火墙自身可以知道主机的动态IP地址，从而进行访问控制，但是在这种方式下，防火墙内部必须开启DHCP 服务，这不仅会增加防火墙的额外负荷,更为严重的是防火墙自身启动过多的服务会影响自身的安全性。

另一种方式是防火墙自身不充当DHCP 服务器，而是在客户端主机上安装一个开机自动运行的小软件，每次在主机开机后，自动将主机获取的动态IP 地址传递给防火墙，这样就可以对指定的主机进行访问控制了。天融信新一代防火墙产品使用的就是后一种方式来解决对DHCP 环境的支持的。

4 .31 支持TOPSEC技术体系的核心技术

支持TOPSEC技术体系的核心技术，可以实现防火墙、IDS、病毒之间的互通与联动，并支持各种网络管理系统的管理,以及接受TopSEC安全审计综合分析系统等审计系统对防火墙进事件进行管理和分析。

5 NGFW4000 系统的功能

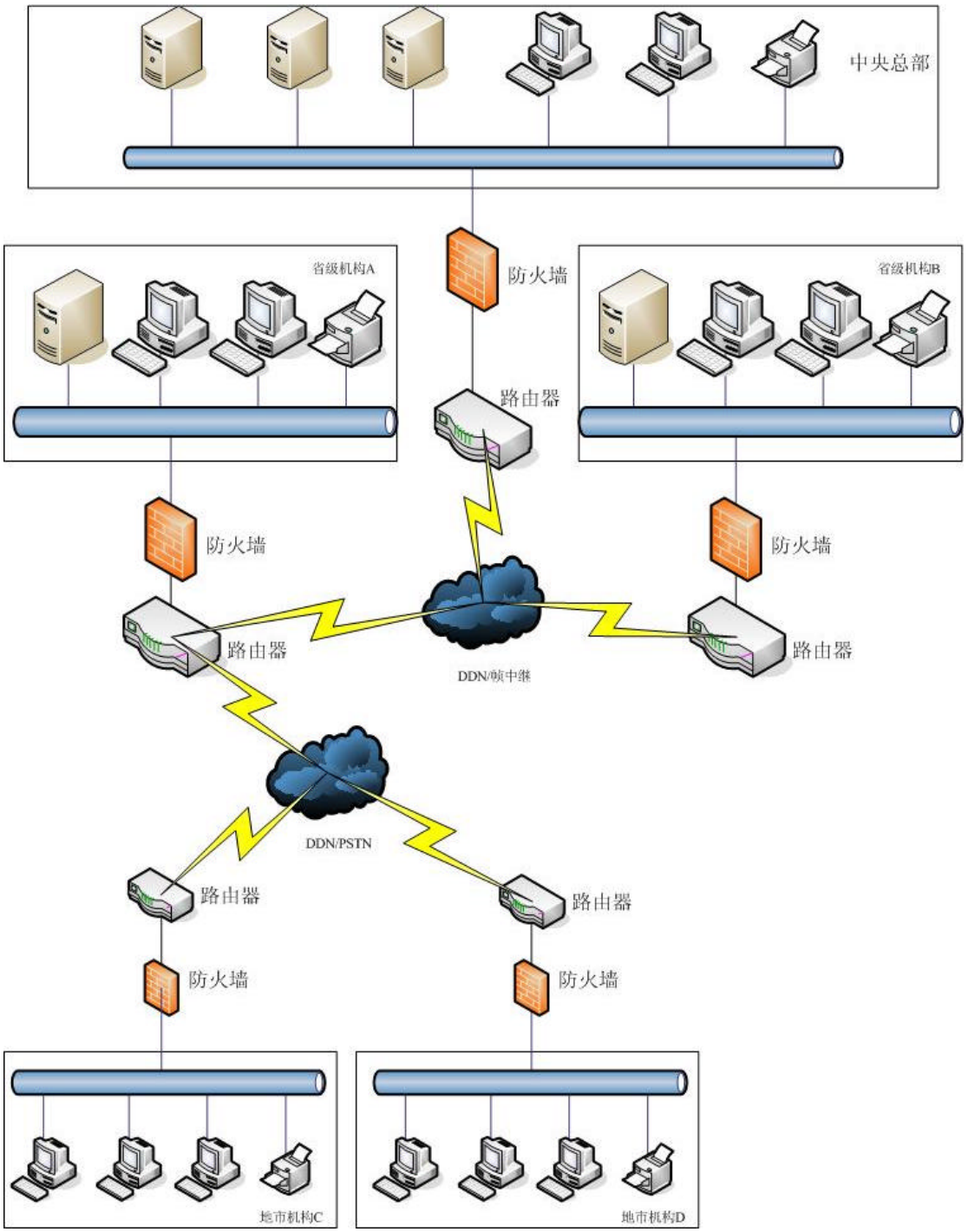
- 平台支持：采用专用硬件平台与专用的安全操作系统
- 基于会话检测的防火墙实现机制：采用基于操作系统内核的会话检测技术（核检测）；
- 更先进的系统结构：硬件上支持对接口的灵活扩展，可以通过灵活的扩展来适应业务发展的需要，从而保护投资。
- 应用代理：具有透明应用代理功能，支持 FTP、HTTP、TELNET、PING、SSH、FTP—DATA、SMTP、WINS、TACACS、DNS、TFTP、POP3、RTELNET、SQLSERV、NNTP、IMAP、SNMP、NETBIOS、DNS、IPSEC—ISAKMP、RLOGIN、DHCP、RTSP、MS-SQL-（S、M、R)、RADIUS-1645、PPTP、SQLNET—1521、SQLNET—1525、H.323、MSN、CVSSERVER、MS-THEATER、MYSQL、QQ、SECURID（TCP、UDP）PCANYWHERE、IGMP、GRE、PPPOE、IPV6 等协议命令级的控制，实现对文件级的过滤。
- 支持众多网络通信协议和应用协议：如 DHCP 、VLAN 、ADSL 、ISL 、802.1Q 、Spanning tree 、NETBEUI 、IPSEC 、H.323 、MMS 等，保证用户的网络应用，方便用户扩展 IP 宽带接入及 IP 电话、视频会议、VOD 点播等多媒体应用。
- 支持核心网络中生成树（STP）的计算：通过生成树计算，防火墙能够同核心交换机一起进行生成树计算，实现了核心网络的全连接拓扑结构，能够进行链路的自动切换，保证了整个网络的稳定。
- 支持交换机主干链路：防火墙的物理接口实现了 DOt1q 封装格式，能够同交换机的 Trunk 接口对接，实现了 Vlan 间路由的功能，保证了防火墙对于各种网络环境的易接入性。
- 地址转换：采用双向网络地址转换（双向 NAT）技术，支持静态 NAT 及动态 NAT（IP POOL)，并能够实现一对一、一对多的地址映射；
- 加密支持：支持 VPN,采用通过国家鉴定的硬件加密卡所提供的 128 位对称加密算法和 128 位 HASH 算法。身份认证采用 1024 位的非对称算法。
- VPN 更高的安全性：将 VPN 的证书和私钥存入 USB 中，只有拥有 USB 的人员才能启动隧道，保证了 VPN 整个过程的安全性。
- 支持多种身份认证：如 OTP 、RADIUS 、S/KEY 、SECUREID 、TACACS/TACACS+、口令方式、数字证书（CA ），更好更广泛的实现了用户鉴别和访问控制。
- 地址绑定：实现 IP 地址与 MAC 地址捆绑，防止 IP 地址非法盗用；
- 安全服务器（SSN）保护：具有对公开服务器保护功能，一旦服务器内容被非法篡改，可以进行快速恢复
- 源、目地址路由功能：根据通讯的源地址和目标地址来做出路由选择，适应有多个网络出口的环境。
- ADSL 接入：防火墙实现了 ADSL 功能，满足了目前中小型公司的网络访问能力，满足了用户的各种接入方式需要。
- 多层次分布式带宽管理（QoS）：可以实现带宽分层、带宽分级、带宽分配、带宽

优化等管理，优化网络资源的应用，提高网络资源应用效率。

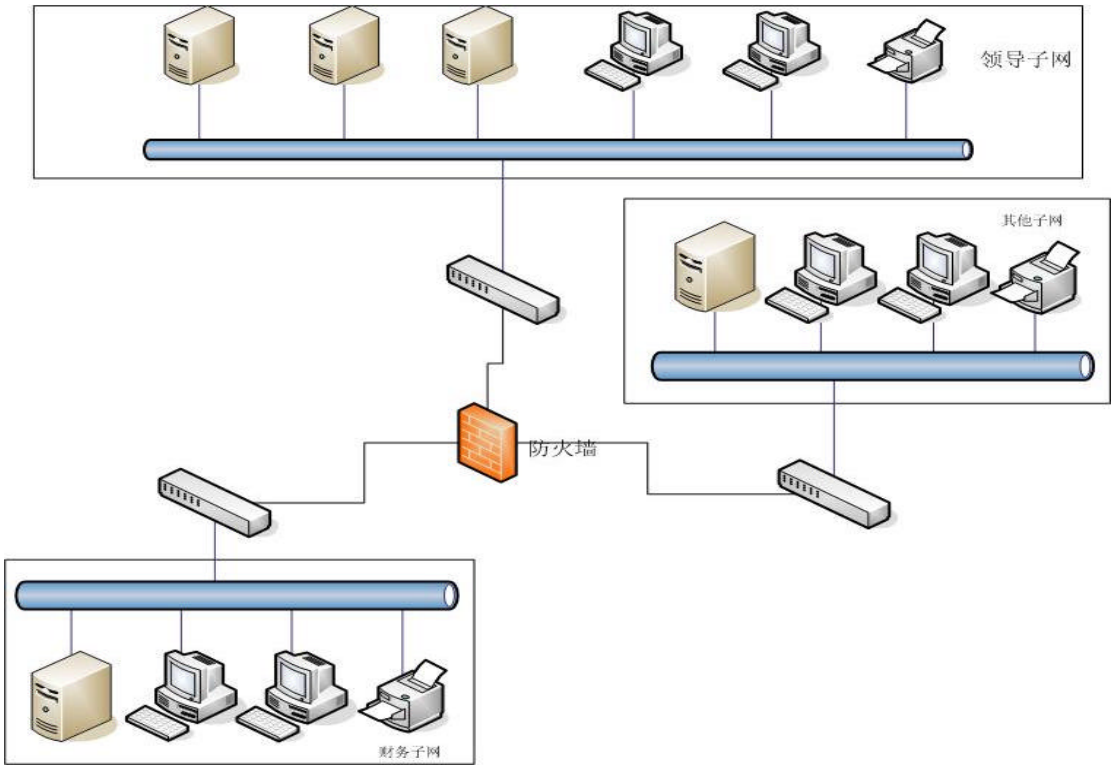
- 防御功能：可防 TCP、UDP 等端口扫描；防源路由攻击、IP 碎片包攻击、DNS/RIP/ICMP 攻击、SYN 攻击； 抗 DOS、DDOS 攻击；可阻止 ActiveX、Java、Javascript 入侵。
- 防火墙支持其它安全产品的联动：支持 TOPSEC 协议，能够与第三方安全产品进行很好的联动，尤其是与 IDS 入侵检测产品的联动；
- 防火墙支持 TopsecManager 与 SAS：支持 TopsecManager 综合管理系统，支持 TopSEC 安全审计系统；
- 实时监控：实时察看防火墙主机的当前负载情况，包括内存的使用情况和连接状况等。
- 防火墙支持多种工作模式：支持路由模式、透明（桥接）模式（防火墙可不配地址）、混合模式（路由与透明两种模式同时工作）
- 管理功能：面向基于对象的管理配置方式；支持 GUI 集中管理及命令行管理方式；支持本地管理、远程管理和集中管理；支持基于 SSH 的远程登陆管理和基于 SSL 的 GUI 方式管理；支持 SNMP 集中管理与监控，并与当前通用的网络管理平台兼容，如 HP Openview ，方便管理和维护。
- 深层日志及灵活、强大审计分析功能：审计日志包括如下几个部分：日志会话、日志命令。日志会话也就是传统的防火墙日志，负责记录通讯时间、源地址、目的地址、源端口、目的端口、字节数、是否允许通过。日志会话信息用来进行流量分析已经足够，但是用来进行安全性分析还远远不够；应用层日志命令在日志会话的基础之上记录下各个应用层命令及其参数，比如 HTTP 请求及其要取的网页名；访问日志则是在应用层命令日志的基础之上记录下用户对网络资源的访问，它和应用层日志命令的区别是：应用层日志命令可以记录下大量的数据，有些用户可能不需要，如协商通信参数过程等。例如针对 FTP 协议，日志会话只记录下读、写文件的动作；日志命令则是在访问日志的基础之上，记录如用户发送的邮件，用户取下的网页等。支持日志的自动导出与自动分析。支持防火墙配置文件的导入与导出（防火墙配置文件信息的备份与恢复）；
- 防火墙双机备份与负载均衡：支持防火墙的双机备份，并通过防火墙自身的负载均衡，提高防火墙在高带宽的网络环境中的有效性能；
- 非协议支持：支持对非 IP 协议 IPX/NetBEUI 的传输与控制。

第三章 NGFW 4000 典型应用

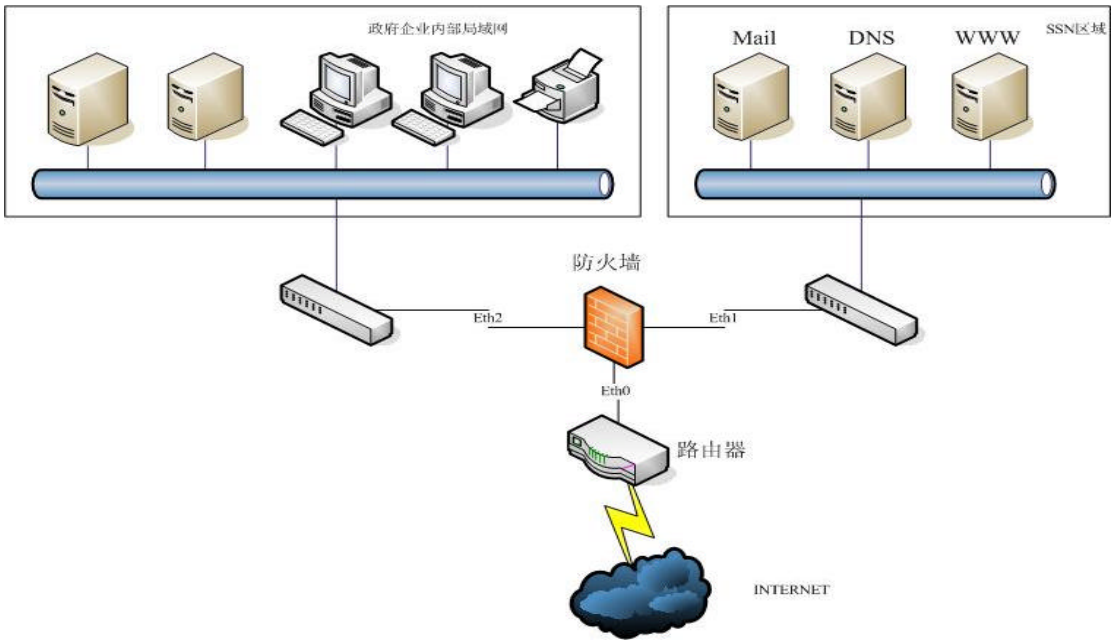
1 典型应用一：在企业、政府纵向网络中的应用：



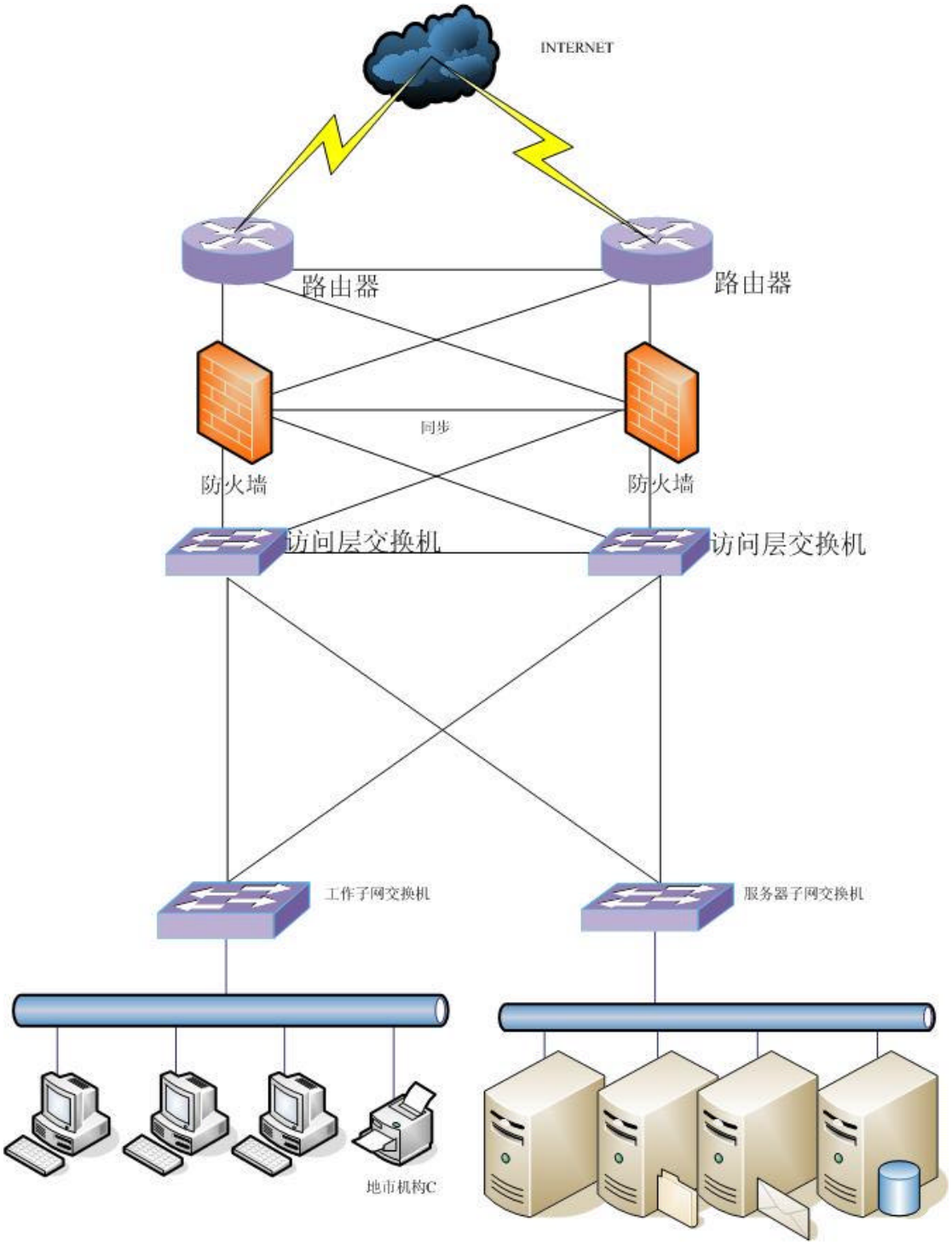
2 典型应用二：在企业、政府内部局域网络中的应用



3 典型应用三：在企业、政府互联网出口处的应用



4 典型应用四：在大型网络中的应用



第四章 NGFW 4000防火墙荣获的认证资质证书

- 公安部颁发的《计算机信息系统安全专用产口销售许可证》，证书编号：XKC33181
- 中国国家信息安全测评认证中心颁发的《国家信息安全认证产品型号证书》，注册号：CNISTEC2002TY1P
- 总参谋部颁发的《国防通信网设备器材进网许可证》，许可证号：ZS251
- 国家保密局监制证书
- 列入国家保密局安全产品推广名单（国保函[1999]85 号）
- 国家密码管理委员会颁发的《商用密码产品生产定点单位证书》，（国密办产字 SSC006 号）
- 国家密码管理委员会颁发的《商用密码产品销售许可证》（国密办销字 SXS008 号）
- 军用信息安全认证证书（军密认字号第 0081 号）