网络卫士系列防火墙

NGFWARES 系列

产品说明

天融信
Topsec
北京市海淀区知春路 49 号希格玛大厦 4 层，100080
电话：+8610-82611122
传真：+8610-62304552
服务热线：+8610-8008105119
http://www.topsec.com.cn

网络卫士系列防火墙产品说明

版权声明

商标声明

信息反馈

Email:PLMC@topsec.com.cn

http://www.topsec.com.cn

目　录

1 产品概述

网络卫士系列防火墙 NGFWARES（NetGuard FireWall），是天融信公司结合了多年来的网络安全产品开发与实践经验,在参考了天融信广大用户宝贵建议的基础上，开发的最新一代网络安全产品。该产品基于嵌入式平台，并以天融信公司具有自主知识产权的 TOS（Topsec Operating System）为系统平台，采用开放性的系统架构及模块化的设计，融合了防火墙、入侵检测、VPN、身份认证等多种安全解决方案，构建的一个安全、高效、易于管理和扩展的网络安全产品。

NGFWARES 作为网络卫士系列防火墙中的低端产品，以其安全、高效、可靠、应用广泛、方便灵活等特点，特别适用于行业分支机构、中小型企业、教育行业非骨干节点院校等中小用户，充分满足中小用户的需求。

2 产品特点

● 高性价比的架构

NGFWARES系列产品采用嵌入式硬件设计,并基于自主操作系统TOS(Topsec Operating System）的多功能安全网关，是第一款集路由、交换、无线接入、语音支持的多功能、即插即用的安全网关。

● 自主安全操作系统平台

采用自主知识产权的安全操作系统 — TOS（Topsec Operating System），既提高了产品性能，又提高了产品的灵活性、高效性和安全性。具有高安全性、高可靠性、高实时性、高扩展性及多体系结构平台适应性的特点

● 优化的系统架构

TOS 系统作为安全处理平台，向下可以支持不同的硬件结构（如 X86、NP 以及 ASIC），向上则可以为实现不同安全功能的安全引擎提供相应接口,同时屏蔽了底层硬件平台和操作系统的差异，自身还可以提供诸如日志、管理、监控以及高可用性等服务。

安全引擎作为模块化的组件，用以实现不同的安全应用，比如入侵检测、认证服务、防火墙、VPN 及带宽管理等。安全引擎通过挂接在数据流处理过程中的不同 HOOK 点来完成相应的功能。

● 高安全性和易扩展性

TOS 提供了一个具有开放性、可扩展性和易移植性的安全产品开发平台，能够支持多个安全设备之间的交互和联动。

● 独创的安全技术

在 TOS 上的防火墙安全引擎（SE）采用了基于 OS 内核的会话检测技术，在 OS 内核实现对应用层的访问控制。与包过滤和应用代理防火墙相比，在实现了二到七层的细粒度访问控制的同时，更有效地保证了产品的高性能。

● 先进的设计思想

采用面向资源的设计方法。把安全控制所涉及的各种实体抽象为对象，包括区域、地址、地址组、服务、服务组、时间表、服务器、均衡组、关键字、文件、特殊端口等。不同对象的实体组成资源，用于描述各种安全策略，实现全方位的安全控制。极大地提高了网络安全性，并保证了配置的方便性。

● 独特的安全策略体系

采用面向资源的防火墙策略体系。通过建立独立的防火区域，以及中央管理接口、管理端口协议、节点对象、子网对象的应用，可以实现层次分明而又立体化的策略机制，制

定灵活安全的通信策略和访问策略，策略配置简单，且易于维护，可以方便地定义各种粒度的安全规则。

● 多级过滤的立体访问控制

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的过滤功能；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；在应用层通过深度内容检测机制，可以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、移动代码等实现内容安全控制；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。网络卫士系列防火墙的多级过滤形成了立体的、全面的访问控制机制，实现了全方位的安全控制。

● 超强的防御功能

高级的 Intelligent Guard 技术提供了强大的入侵防护功能,能抵御常见的各种攻击，包括 Syn Flood、Smurf、Targa3、Syn Attack、ICMP flood、Ping of death、Ping Sweep、Land attack、Tear drop attack、IP address sweep option、Filter IP source route option、Syn fragments、No flags in TCP、ICMP 碎片、大包 ICMP 攻击、不明协议攻击、IP 欺骗、IP security options、IP source route、IP record route 、IP bad options、IP 碎片、端口扫描等几十种攻击，网络卫士系列防火墙不但有内置的攻击检测能力，还可以和 IDS 产品 实现联动。这不但提高了安全性，而且保证了高性能。

● 强大的应用代理模块

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，可以实现文件级过滤。

● 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，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。

系统核心层实现传输内容的还原、安全检测，实现高性能的 TOPSEC 内容安全协议，支持病毒检测和垃圾邮件过滤。

● 严格的安全区域保护

采用多安全区域体系，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。

用户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部属在该网络区域内，与内、外网络从物理上隔离开来，以提供专门的安全保护。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，网络卫士系列防火墙提供的 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 区的 Web 服务器，一旦发现服务器被入侵修改，防火墙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。

● 丰富的 AAA 功能，支持会话认证

网络卫士系列防火墙支持对网络用户提供丰富的安全身份认证,如一次性口令(OTP)、S/KEY、RADIUS 、TACACS、LDAP、secuid 、域认证及数字证书等常用的安全认证方法，也可以使用专用的认证客户端软件进行认证。基于用户的安全策略更灵活、更广泛地实现了用户鉴别和用户授权的控制，并提供了丰富的安全日志来记录用户的安全事件。

网络卫士系列防火墙支持会话认证功能，即当开始一个新会话时，需要先通过认证才能建立会话。这个功能可大大提高应用访问的安全性，实现更细粒度的访问控制。

● 强大的地址转换能力

网络卫士系列防火墙拥有强大的地址转换能力。网络卫士系列防火墙同时支持正向、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私有 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。网络卫士系列防火墙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,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，这样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，自身使用私有 IP 地址就可以正常访问公众网，有效的解决了公有 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)的服务器如果是私有 IP 地址，或者想隐藏服务器的真实 IP 地址，都可以使用网络卫士系列防火墙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，同样既可以解决公有 IP 地址不足的问题，又能有效地隐藏内部服务器信息，对服务器进行保护。网络卫士系列防火墙提供端口映射和 IP 映射两种反向地址转换方式，端口映射安全性更高、更节省公有 IP 地址，IP 映射则更为灵活方便。

● 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 等协议，适用网络的范围更加广泛，保证了用户的网络应用。同时，方便用户实施对 VOIP、视频会议、VOD 点播及数据库等应用的使用和控制。

● 灵活的工作模式

网络卫士系列防火墙支持透明接入。将网络卫士系列防火墙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。透明接入极大地方便了防火墙的接入，同时并不降低网络的安全性。

网络卫士系列防火墙还能工作在透明+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，且网络卫士系列防火墙在实现时进行了进一步的优化，又增加了支持透明+路由＋反向地址转换的工作方式，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。

● 丰富的接入方式

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地接入各种网络环境，最大限度地满足了用户的各种需求。

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。

● 适应复杂的核心网络

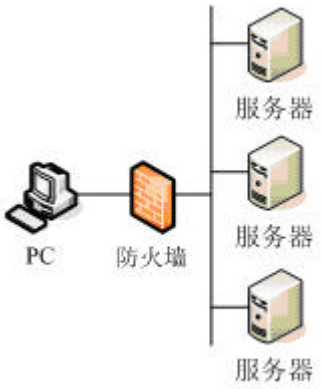
核心网络的安全性、稳定性是当今网络的焦点，如何保证核心网络的安全，保证数据的 24 小时传输成为网络安全的最受关注的问题。网络卫士系列防火墙能够在核心网络中

同所有核心网络设备一起实现高可用性及高安全性的拓扑结构，最大限度地满足了网络的健全性及稳定性，保证了整个核心网络的不间断工作。当核心网络中的某条链路产生故障时，网络卫士系列防火墙能够动态的切换链路，实现数据的不间断传输。同时结合防火墙的其他安全特性，使整个网络无比健壮。

● 智能的负载均衡和高可用性

➢ 服务器负载均衡

网络卫士系列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。



负载均衡方式如下：

1.轮流（顺序选择地址）

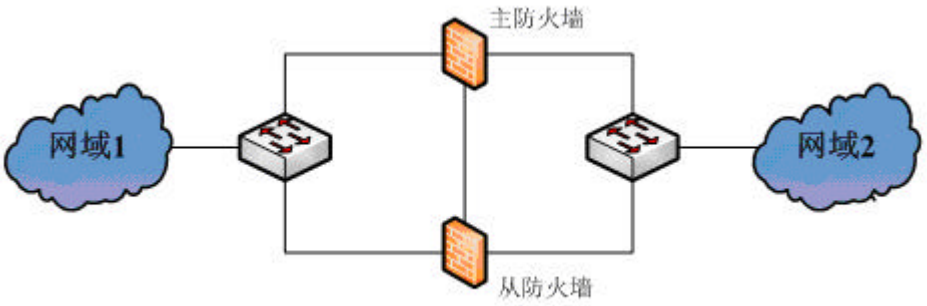
2.根据权重轮流

3.最少连接（将连接分配到当前连接最少的服务器）

4.加权最少连接（最少连接和权重相结合）

➢ 高可用性

为了保证网络的高可用性与高可靠性，网络卫士系列防火墙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，网络卫士系列防火墙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。当主防火墙发生故障时，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

网络卫士系列防火墙支持完整生成树（Spanning-Tree）协议，可以在交换网络环境中支持 PVST 和 CST 等工作模式，在接入交换网络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在使用高可用性的同时实现流量均衡。

● 方便灵活的安全管理方式

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 要求 GUI 客户端对防火墙进行证书认证的同时，防火墙也要对客户端进行证书认证，避免了传统的 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相结合的双因素认证，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 OpenviewNNM、TOPSEC Manager 等，方便了管理和维护。

为了保证远程管理的安全性，网络卫士系列防火墙不论是对管理员还是管理过程都采取了一系列安全措施：对远程管理员主机的限定和对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，网络卫士系列防火墙还支持基于 SSH 的远程登录管理，将管理主机和防火墙之间的通讯进行加密以保证安全。

● 分层次的命令行管理

命令行系统中包括了系统级和组件级命令。独特的分层设计使命令行的使用更为清晰简便。同时，命令行支持“Tab”键自动补齐功能，命令超时，历史命令，命令补齐，命令错误提示以及中英文帮助，大大方便了用户的使用。

● 强大的联动

支持与基于 TopSEC 协议的 IDS、防病毒及其他安全产品的联动，提供智能的网络安全保护。

● 系统升级与容错

网络卫士系列防火墙可以通过命令行及图形方式进行系统升级,同时网络卫士系列防火墙采用双系统设计，在主系统发生故障时，用户可以在启动时选择 BACKUP 方式，用备份系统引导系统。

3 产品功能

功能	描述
工作模式	透明模式 路由模式 混合模式（路由与透明两种模式同时工作）
网络地址转换	支持包括正向、反向 NAT 以及 PAT 等多种地址转换方式
访问控制	包过滤策略：用于控制用户对某种网络服务或端口的访问，可以根据报文特征过滤 IP 报文和非 IP 报文 防火墙访问规则：通过限定访问时间、服务类型及 DPI（深度报文检测）针对对象及区域，进行访问控制。支持基于流、数据报、透明代理三种过滤方式。 支持 HTTP、SMTP、POP3、FTP 等的过滤。 动态端口支持协议包括 FTP、RTSP、SQL*NET、MMS、RPC(msrpc,dcerpc)、H.323、TFTP。
VPN	支持基于标准 IKE 协商的 VPN 通信隧道 支持网关到网关，及远程移动用户到网关的 VPN 隧道 支持多种认证方式，如预共享密钥，数字证书等 支持 SCM 服务器集中管理
防御功能	内置攻击检测模块：抵御包括 Syn Flood，Smurf，Targa3，Syn Attach，ICMP flood，Ping of death，Land，Winnuke、TCP_sscan、IP_option、Teardrop、Targa3、IPspoof 端口扫描等几十种攻击； Topsec 联动：与支持 TOPSEC 协议的其他厂商的 IDS 设备联动，以提高入侵检测效率 端口阻断功能：可以根据数据包的来源和数据包的特征进行阻断设置 SYN 代理：对来自定义区域的 Syn Flood 攻击行为进行阻断过滤
服务保证（QoS）	分级带宽管理：通过接口带宽、带宽组以及带宽组用户等多级带宽管理，可以针对 IP 地址段，时间段，服务优先级等多种条件设置带宽策略。 能够以八种优先等级，为流量分配优先权，从而提供针对用户和服务的优先级控制。
VLAN 与生成树	支持与交换机的 Trunk 接口对接，并且能够实现 Vlan 间通过安全设备进行路由 支持多种生成树协议，包括 PVST+及 CST 等协议 支持 802.1q，能进行 802.1q 的封装和解封装 支持 ISL，能进行 ISL 的封装和解封装 Vlan 内交换，在同一个 Vlan 内能进行二层交换 支持 802.1d 生成树，能进行 802.1d 的生成树协商
认证	可以实现设备认证、会话认证等多种认证类型 支持使用一次性口令（OTP），本地认证，第三方认证如 RADIUS、TACACS/TACACS+、LDAP、域认证等，双因子认证 SecureID，以及数字证书（CA）等常用的安全认证方式 支持 Session 认证，HTTP 会话认证
服务器负载均衡	支持服务器负载均衡，提供轮询、加权轮叫、最少连接、加权最少链接等多种负载均衡方式供用户选择
ADSL 接入	支持 ADSL 接入功能，满足中小企业的多种接入需求
链路备份	支持链路备份功能，提高了用户网络的可靠性
DHCP	防火墙可以作为 DHCP 服务器 防火墙可以作为 DHCP 客户端

	防火墙可以作为 DHCP 代理
多播	IGMP 消息报文透传 IGMP 报文路由转发 生成 IGMP 加入请求 多播报文反向路径检测 多播报文发送 接口状态更新通知 添加、删除、清空、显示多播路由
多种管理方式	基于 SSL 的 TOPSEC 管理中心 本地命令行管理 SSH 的远程管理
配置备份和恢复	可以进行配置文件的备份、下载、删除、恢复和上载。用户可以随时备份安全设备的配置文件，并将配置备份下载到本地管理主机中保存。也可以随时将备份上载到设备中实现配置恢复。
TFTP 升级	支持通过在命令行方式下通过CONSOLE口使用TFTP命令升级安全设备
容错与高可用性	支持备份操作系统，防止因升级失败或其他异常造成系统无法正常工作 支持双机热备
日志	支持 Welf、Syslog 等多种日志格式的输出 支持通过第三方软件来查看日志 通过安全审计系统（TA-L），可获得更详尽的日志分析和审计功能，并能提供员工上网行为管理功能 可选高级日志审计功能模块，除接受防火墙日志外还能接受交换机、路由器、操作系统、应用系统和其他安全产品的日志进行联合分析
报警	内置了“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类别 采用 “邮件”、“NETBIOS”、“声音”、“SNMP”、“控制台”等多种报警方式
实时监控	通过 TOPSEC 管理中心可以同时监控多个安全设备的运行状况，包括网络接口检测，CPU 利用率监测，内存使用率监测，操作系统状况监测，网络状况监测，硬件系统监测，检测进程，错误恢复，加密卡状况检测，进程的内存监测
系统健壮性	支持双系统引导，当主系统损坏时，可以启用备用系统，不影响设备的正常使用 容错模块，监控各应用模块是否工作正常 报文调试、报文过滤、报文输出、策略检查 支持 Watchdog 功能 内置黑匣子，并能导出设备健康运行记录
报文调试	提供强大的报文调试功能，可以帮助网络管理员或安全管理员发现、调试和解决问题。 支持发送虚拟报文
ARP	ARP 代理 ARP 学习 设置静态 ARP
NTP	支持网络时钟协议，可以自动根据 NTP 服务器的时钟调整本机时间
CDP	支持 CDP（CISCO DISCOVERY PROTOCOL）协议，可以接受 CDP 消息，发现并识别相邻的 CISCO 设备
SNMP	支持 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
非 TCP/IP 协议支持	支持对非 IP 协议，如 IPX 或 NetBEUI 的传输与控制

升级方式	**支持双系统，允许升级主系统或备份系统** **远程升级** **CLI 升级** **GUI 升级**

4 运行环境与标准

电源：

电压：AC 190/220V

频率：50/60HZ

电流：3.0A (最大)

功率：260W (最大)

环境：

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

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）

5 产品规格

NGFWARES-V

NGFWARES-V-VPN

NGFWARES-G

NGFWARES-G-VPN

NGFWARES-Q-VPN

NGFWARES-P-VPN

NGFWARES

NGFWARES-VPN(S)

NGFWARES-VPN(E)

NGFWARES-H

NGFWARES-H-VPN(S)

NGFWARES-H-VPN(E)

NGFWARES-S

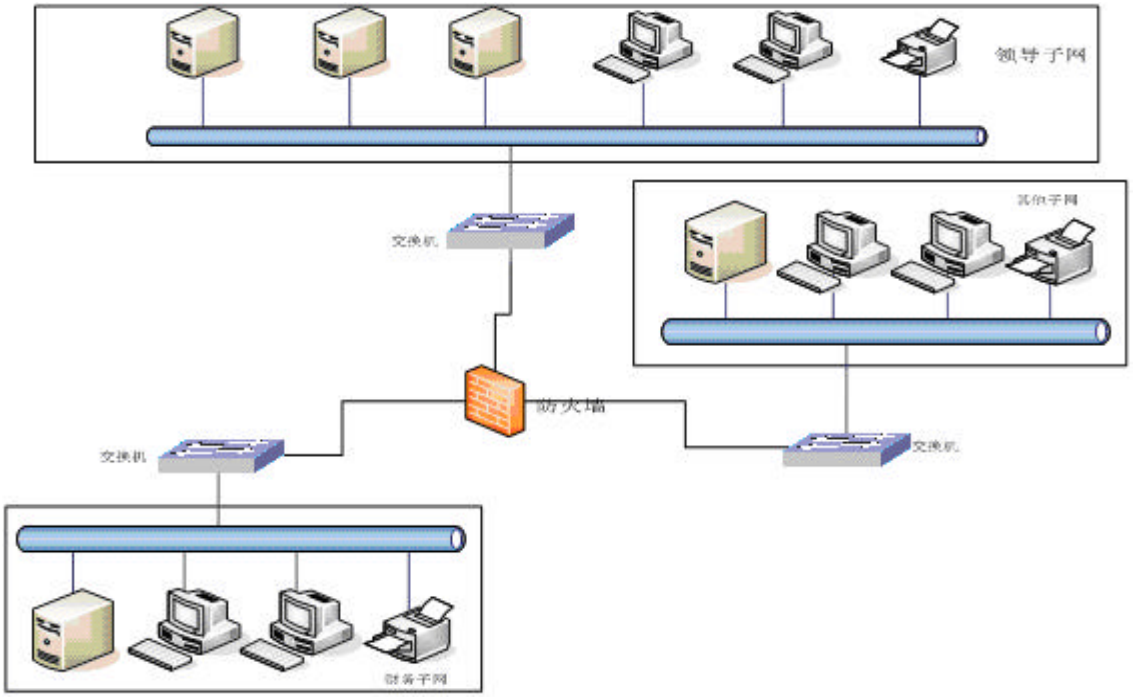
NGFWARES-S-VPN(S)

NGFWARES-M-VPN(S)

.....

6 典型应用

6.1 典型应用一：在企业、政府内部局域网络中的应用



6.2 典型应用二：在企业、政府互联网出口处的应用