任子行 SURF-NGSA 下一代防火墙

产品白皮书

■ 文档编号	*(V1.0)*	■ 密级	内部使用
■ 版本编号		■ 日期	2014-06-04

■ 版权声明

■ 版本变更记录

时间	版本	说明	修改人
2014-06-04	1.0	白皮书	张志伟

■ 适用性声明

本文档用于描述任子行下一代防火墙的技术白皮书。本模板用于撰写任子行内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

一. 产品概述

SURF-NGSA是任子行公司基于在互联网内容安全和行为管理领域多年的积累，以及对下一代防火墙技术的深入研究推出的防火墙系列产品，旨在为用户提供面向应用安全的高效、安全、可靠的安全防护。SURF-NGSA防火墙通过多因子身份认证技术，将网络安全、应用安全、管理安全有机地融合在一起，所采用的多核并行处理技术及单次解析引擎系统架构可并行处理所有安全防护功能。

任子行NGSA包含第一代防火墙的所有标准功能，即常见的网络功能，如网络地址转换（NAT）、包过滤和全状态包检测功能。任子行NGSA还集成了网络入侵防御功能，这不仅仅是在传统防火墙架构上简单添加入侵防御子系统这么简单。任子行NGSA集成的入侵防御功能是安全引擎的核心组件，无需经多个独立的安全层传输同样的流量，从而提高了性能，增强了安全性。

任子行NGSA的主要特点是应用感知以及网络堆栈的完全可视化。任子行NGSA不会像传统防火墙一样只依靠端口或协议来阻止流量，而是会根据深度包检测引擎识别到的流量在应用层执行网络安全策略。流量控制不再是单纯地阻止或允许特定应用，而是可用来管理带宽或优先排序应用层流量。深度流量检测让IT部门可针对单个应用组件执行细粒度策略。例如，可允许用户使用即时通讯客户端，但禁止文件共享。

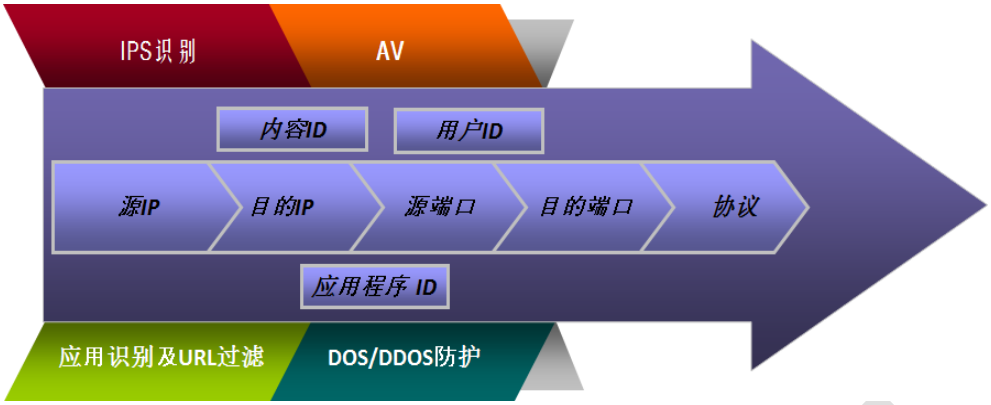
动态应对变化多端的威胁是任子行NGSA的另一大重要特点。设备的签名库将不断更新，用于识别新的威胁，更从容地应对不断升级的恶意软件。

二. 产品特点

■ 突破传统五元组的“八”元组的策略

任子行 NGSA 下一代防火墙在源 IP、目的 IP、源端口、目的端口、协议的基础上，在安全策略中整合了用户 ID、应用程序 ID、以及内容 ID 等三大因素，形成了独具特色的 8 元组

的策略部署思想，使任子行 NGSA 下一代防火墙能够基于用户身份实现 IPS、AV、URL 过滤、DOS/DDoS 防护及应用识别等多种安全特性，从而构建了全方位、立体化的安全防御体系。



■ 20 大类超 2300 种应用识别

任子行 NGSA 下一代防火墙密切贴近国内用户使用习惯，内置 20 大类超过 2300 种应用类别数据库，支持包括 P2P 下载、VoIP、Web/Web 2.0 应用、Web 即时通讯、安全更新、代理和 VPN 软件、股票软件、即时通讯、流媒体、社交网络、数据库、私有协议、通讯网络协议、通用网络软件、网络管理、文件传输、移动应用、邮件和协同软件、游戏、远程控制在内的 20 大类 2300 多种应用和应用协议的识别，全面覆盖国内外日常的应用。而且任子行公司每天都在密切关注应用发展的趋势，不断对应用进行更新。

■ 内容级别的深度过滤

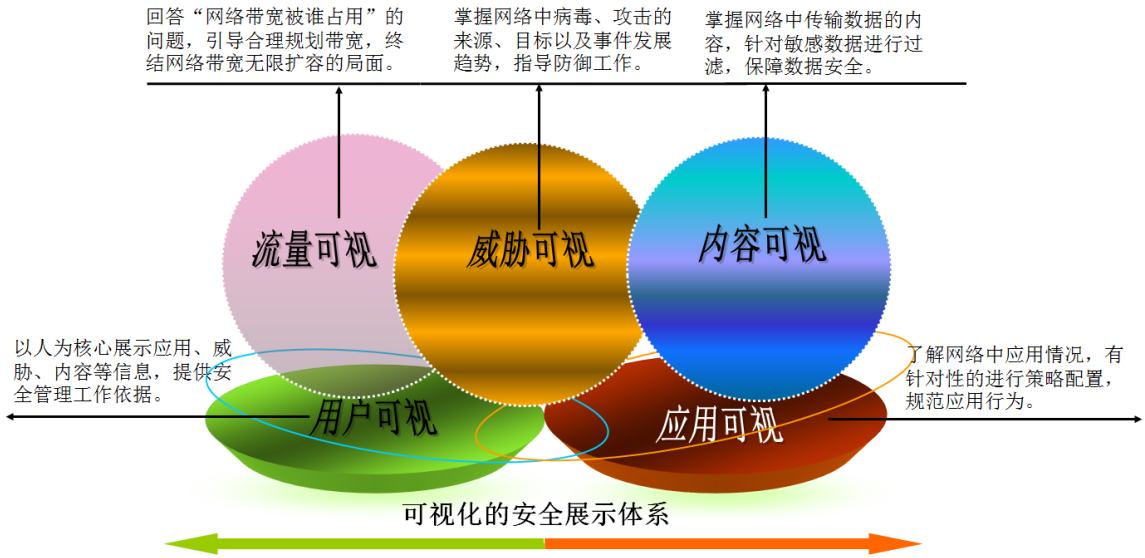
任子行 NGSA 下一代防火墙采用基于攻击过程的内容级安全防护策略，将数据包还原到内容级别进行更加深入、更加全面的检测，提供了 IP 黑名单、DOS 防御、僵尸网络防护、用户认证、应用控制、入侵防御、站点分类过滤、病毒过滤、恶意网址过滤、数据安全等多达十层的基于数据包头和数据内容的精细过滤功能，形成了从网络层到应用层一体化安全防御体系，进行更加精准的特征匹配，并与底层高性能平台结合，实现高效率与高精度并重的内容过滤，确保用户业务系统稳定可靠运行。

■ 基于客户端类型的身份认证方式

任子行 NGSA 下一代防火墙提供多种身份验证功能，并集成了强大的安全准入控制。在针对终端到网关的认证支持多种认证协议与认证方式的同时，通过对认证终端的操作系统环境进行系统服务、软件、文件、进程、注册表等细粒度管控策略。

■ 全方位可视化

任子行 NGSA 下一代防火墙在设计上秉承安全“可视化”的理念，打造了一整套多维度、全方位的实时在线网络安全监测系统，从“应用可视化”、“流量可视化”、“威胁可视化”、“内容可视化”、“用户可视化”五个角度实现了对网络安全状况的综合展示，包括对历史数据的精确还原以及对各种数据的智能统计分析。通过对海量数据进行关联分析和数据挖掘，以形象的图表和数据展现了网络应用、安全威胁、流量分布、内容安全、人员网络使用情况等多方面的信息，帮助用户在使用过程中不断了解自己的网络安全状况，并在此基础上进行更好的策略和配置的优化，使管理者清晰的认知网络运行状态，从而实现对内部任一主机乃至全网络的网络应用情况及安全事件信息进行准确的定位与实时跟踪，实现更为有效的网络安全管理。

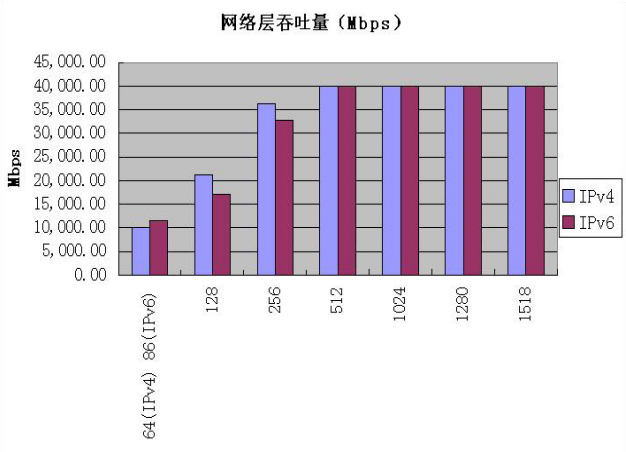


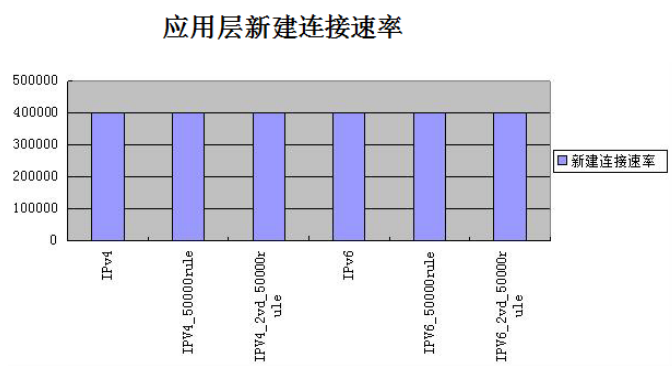
■

电信级转发平台

任子行 NGSA 下一代防火墙采用多核并行处理技术，实现在核内、核间任务的合理分工与调度。来自网络层的数据包进入多核并行控制器后，多核并行控制器将数据包均衡的分配到各个不同的 CPU，以便完成后续多颗 CPU 的并行事务处理。

同时任子行 NGSA 下一代防火墙通过单次解析引擎系统架构，也放弃了 UTM 多引擎，多次解析的架构，将漏洞、病毒、Web 攻击、恶意代码/脚本、URL 库等众多应用层威胁统一进行检测匹配，大大提升了引擎处理效率及系统性能，实现了万兆级的应用安全防护能力，完全满足电信级网络环境要求。





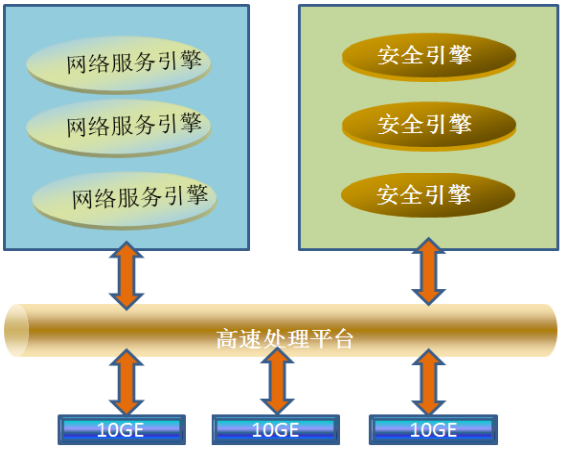
■ 3 大层级冗余的可靠性保障

任子行 NGSA 下一代防火墙支持双机状态热备功能，支持 Active/Active 和 Active/Passive 两种工作模式，实现负载分担和业务备份。由物理级冗余、系统级冗余、方案级冗余共同构成的多层级的冗余化架构体系，为用户提供电信级的高可靠性，确保用户的网络环境永续不断。

三. 关键技术

■ 多核并行处理技术

SURF-NGSA 下一代防火墙采用多核并行处理技术，将时间并行与空间并行进行有机的结合，通过部署多安全引擎、多网络服务引擎的方式来实现整机流量的分布式并行处理，极大地提升了整体的处理性能，可以完全满足电信级网络环境的要求。



■ 单次解析引擎系统架构

SURF-NGSA 下一代防火墙采用先进的一体化的单次解析引擎系统架构，实现网络入侵、安全漏洞、web 攻击、恶意代码/脚本、URL 库多种应用一次匹配，大大提高了系统的处理能力，在所有应用层防护功能均开启的情况下实现万兆级处理性能。

■ 新型恶意软件的检测和防御

随着新型恶意软件功能的不断增强，企业必须能够在威胁已具有定义的特征文件之前立即检测这些威胁。任子行下一代防火墙甚至在特征文件可用之前就能根据对可执行文件和网络流量进行的直接分析，为组织提供保护其网络的多元化方法。

Sow-scan 使用基于云的方法，通过在安全的虚拟化环境中直接查看以前看不到的恶意可执行文件的行为，来封堵查杀这些文件。例如（更改注册表值或操作系统文件、禁用安全机制或者向正在运行的进程中注入代码）。并且会自动开发一个特征文件并在下一个可用内容更新中将其提供给所有客户。

未知流量检测：Protocol-check 可对应用协议级别的所有流量进行分类，以便公开网络中的任何未知流量，这些未知流量通常是恶意软件或其他威胁活动的征兆。例如，多次访问恶意网站、使用动态 DNS 和 IRC 以及其他潜在的可疑行为。结果将显示在列表中，其中包括可能已感染的主机，可能会将这些主机作为僵尸网络的成员加以调查。

■ 双栈道 IPv4 与 IPv6 支持

随着IPv4地址空间的耗尽，许多公司正在迁移到IPv6，下一代互联网通信协议。IPv6彻底的改变了IP地址的供应，从40亿IPv4地址到340万万万亿IPv6地址（2^128地址）。IPv6同时也保证了比IPv4基础之上的功能的增强包括更好的安全性、更好的地址查询、有效的路由与服务质量。IPv6架构包括诸多功能与优势尤其有利全球化的端到端的通信。

当更多的内容与服务提供商开始转换到IPv6的地址时，公司与企业机构必须部署网络安全设备能够提供与IPv4架构下的同等的IPv6架构的安全防御水平。有一些机制可以使只兼容IPv6的设备与之兼容IPv4的设备与网络之间进行通信。两种最常用的是双栈道与通道机制。双栈道更可取，因为它允许安全设备能够处理基于IPv4 与IPv6的数据包。通道机制，在另一方面，将一个IPv6数据包包裹在IPv4数据包头中，允

许设备转发数据包但是不进行检测。这样的IPv6支持限制也意味着通道机制不能检测恶意代码或不需要的内容，直接允许不需要的内容穿越网络。

任子行下一代防火墙加固安全平台支持双栈道架构，能够识别并分离IPv4与IPv6流量，对两种互联网提供相同的核心网络安全技术。重要的网络与内容防御安全功能，包括路由功能，都全部支持。

■ 应用特征

任子行下一代防火墙的主要应用需求与驱动就是应用控制。为了防止数据丢失与防御新的威胁，有效控制旧有的应用以及新出现的基于互联网的应用是必需的。下一代应用控制功能必须能够检测、监控并控制应用，并在网关与终端之间管理与这些应用相关的网络流量，无论这些应用使用任何的端口与协议。另外，应用与终端用户之间需要建立关联以保证在访问应用之前能够执行安全策略。

任子行研发的应用控制功能，可以基于应用分类、行为分析与终端用户关联来检测并限制网络与终端的应用。网络管理员可以对运行于下一代网络与终端的应用定义并执行相应的策略，实现对基于web2.0应用的细粒度的管理与控制

- **应用控制列表**

网络管理员可以通过防火墙策略中的应用控制列表管理各种应用程序。另外，管理员还可以创建多个应用控制列表，对每个列表配置一套允许、屏蔽或对列

表中有关的流量进行控制的动作与策略。应用控制的白名单适合用于有着较高安全系数的网络，例如只允许在该应用列表中的流量通过网关。另一方面，应用控制的黑名单是指屏蔽列表中全部所列应

- **应用控制粒度**

应用控制功能也可以识别来自单个社交网站的多个应用。流量控制可以限制一些应用的网络带宽，优先其他应用。

- **应用流量控制**

应用流量控制功能允许管理员管理所有的应用或某一应用列表中的单个应用，从而限制或保证网络带宽。流量控制也可以配置应用使用的时效性，以限制用户访问或某时间段的可用带宽。

- **应用监控报告**

应用监控与报告功能是指收集应用流量信息并通过可视化的趋势图显示，管理员可以快速获得网络中应用的使用情况。也可以从几个不同类型的应用列表中选择几项，按地区显示使用信息。默认的可视图可用于快速分析。

- **应用控制数据包日志**

应用控制数据包日志功能将应用产生的网络数据包进行日志管理与额外的分析。

- **终端应用控制**

应用控制列表也可以同时应用到终端安全策略。另外，终端的应用使用也可以通过个人防火墙加以控制。

■ 入侵防御系统（IPS）

大范围的更新与补丁需要升级与维护，下一代网络的管理与维护是复杂而耗时的事情。每一次漏洞补丁的发布，大型企业的网络得花费数周甚至一个月的时间去更新修复所有受影响的系统。任子行下一代防火墙设备中的IPS系统可以提供网络中已知漏洞防御或“零日漏洞”的更新服务，使未修复的系统免于攻击。

IPS系统提供了广泛的功能，可用于监控或阻断恶意网络活动，包括预定义与用户定制特征、协议解码、带外模式（或单臂IPS模式）、数据包日志记录与IPS传感器功能等。通过IPS传感器可以迅速且集中的配置。

防御网络边缘或网络核心的重要业务应用受到来自外部或内部的威胁。

- **预定义IPS特征**

通过任子行全球分布式网络提供的预定义IPS特征，任子行下一代防火墙可以检测超过4000种不同的攻击特征，范围可以涵盖从对于未作补丁修复的操作系统漏洞攻击到UDP数据包中包含的无效校验值。

- **自定义IPS特征**

用户也可以创建自定义的IPS特征，扩大预定义特征之外的保护范围。例如，用户自定义特征可以用于保护不常用或者特定的应用，甚至从已知与未知的攻击自定义平台。另外，用户定义的IPS特征也可以用于特殊的网络流量分析与模式匹配。例如，如果一个网络正在处理不常用的或不需要的流量，系统管理员可以创建一条用户自定义IPS特征去监控并分析该流量的模式。

- **协议解码器**

协议解码器可以识别异常流量模式，例如那些不符合已建立的协议需求与标准

的流量。举例说明，HTTP
解码器监控网络流量以识别任何不符合HTTP协议标准的数据包。许多协议解码器能够根据流量的类型而不
是端口识别流量，避免了指定端口的需要。

- **数据包日志记录与攻击隔离**

IPS数据包日志记录功能可以保存与一项或多项IPS特征匹配的数据包。数据包保存为日志消息，并使用日志信息分析工具，可以查看和分析数据包的内容。数据包日志记录功能是设计用于主要诊断工具并在小范围内达到最佳使用状态。
IPS还提供了一种隔离攻击并将其纳入“禁止用户列表”列表中显示。所有攻击根据其IP地址，其IP地址加上受害者的IP地址、根据攻击进入使用的接口而处以隔离。同时也根据时间段，例如小时、天数或者永远禁止该攻击访问网络。

- **IPS带外模式**

IPS也可以部署为带外模式。该模式下作为一个入侵检测系统（IDS）而生效，检测并报告攻击，但不采取任何动作。带外模式可以用于网络诊断

■ URL 过滤

通常URL过滤功能可以防止用户访问危险或不适当的网站。任子行下一代防火墙URL过滤功能可以使管理员能够明确设定允许访问的网站，或配置通过已知良好的网站的往来流量，从而加速网络流量。
通过网络可以实时发送和更新特定的URL类别和等级。本地URL过滤列表可以同时使用文字和正则表达式添加过滤的网站或网址。
在URL过滤列表URL模式的四种不同的处理动作。

- **阻断**

阻断用户访问潜在危险或者含有不适当内容的网站，访问被拒绝后发送警告信息。

- **允许**

明确允许用户访问的某些网站。网站访问流量被允许通过但要接受根据需要设置的安全功能检测。

- **通过**

明确允许用户访问的某些网站。网站访问流量被允许绕过其他安全检测。该选项只有对完全信任网站配
置使用。

- **豁免**

明确允许用户访问的某些网站。网站访问流量被允许绕过其他安全检测。但是，连接得到了豁免意味着随后所有的对现有连接的通讯都将绕过安全检测。当连接超时时，豁免动作被取消

■ 反病毒/反间谍软件

网络、服务器和端点设备中的恶意软件感染问题每年对公司企业、服务提供商和政府机构造成数十亿美元的花费。 任子行公司的防病毒技术结合先进的特征和启发式检测引擎，提供多

层次、实时防御不断发展的新病毒、间谍软件和其他类型的网页、电子邮件、文件传输流量中的恶意攻击。
基于流的选项允许配置扫描任何大小的文件的同时可以保持最佳的性能。此外，基于流的检测可以扫描压缩文件内的文件内容，检测隐藏的威胁。 基于数据流的检测提供了防病毒引擎选择的灵活性，且兼顾性能和安全性的要求。
加密/解密功能适用于所有常见的隧道协议包括的PPTP、L2TP、IPSEC、SSL，按需的主机完整性检查可以检测基于VPN连接的流量。任子行下一代防火墙的防病毒功能支持基于SMTP、POP3、IMAP、FTP、HTTP、IM和P2P协议的内容，以及所有主要的压缩文件格式。

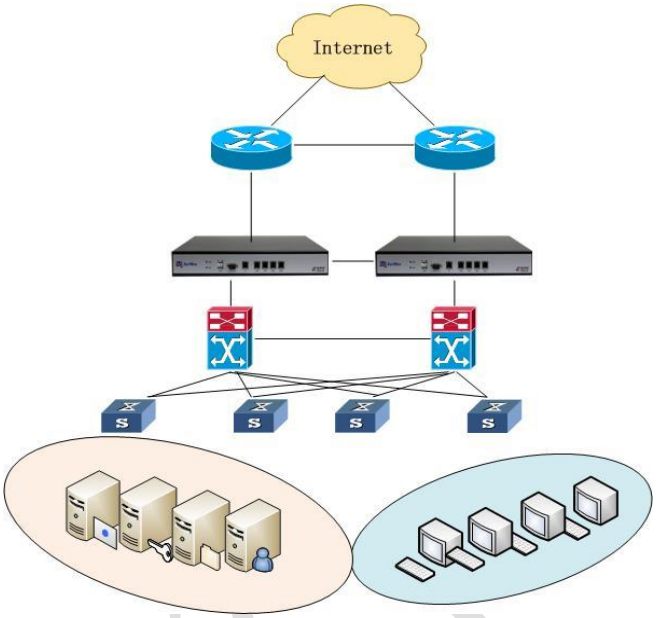
■ 反垃圾邮件

未经请求的电子邮件以垃圾邮件的形式传递，每年对企业和政府机构造成数十亿美元的花费。员工从常规的邮件中识别并删除垃圾邮件，同时也对服务器与网络产生了额外的流量。 此外，垃圾邮件传播是僵尸计算机繁殖的最常见的手段，且往往包含恶意软件和不适当的网站的链接。
任子行下一代防火墙的反垃圾邮件功能提供了防御垃圾邮件的全方位多层次方法。反垃圾邮件过滤的机制是通过任子行反垃圾邮件服务访问任子行全球威胁情报数据库实现实时更新的。
任子行下一代防火墙可以创建自定义的垃圾邮件过滤器，过滤含有被禁止言语的邮件，阻断与允许的邮件发送方地址名单、启发性扫描规则。
配置不当或被病毒感染的主机也会每天发出大量的垃圾邮件。 任子行反垃圾邮件服务一直在维护一个全球性的IP信誉数据库，每个IP地址的信誉是通过从多个来源信息的收集作为衡量基础并进行更新。IP地址的信誉属性包括域名的信息、地理位置、服务提供商、主机服务器等的信息，以及其他更多信息。此外，通过对每个发件人的历史电子邮件与当前电子邮件的数量比较，任子行反垃圾邮件服务更新每个IP地址实时的信誉，提供了一个高效的发送者的IP地址过滤。

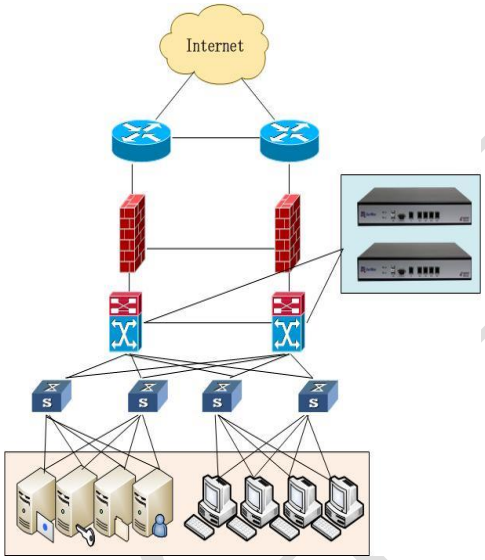
四. 典型部署

一、网桥部署模式：

任子行下一代防火墙也支持以透明模式运行，以便在不影响现有路由、地址转换架构下进行布署，还能做到协助原有安全设备（F/W ，IDP ，Proxy…）分析过去无法掌握的网络使用行为、威胁攻击等信息，使其逐步成为安全控管中心，方便 IT 部门重新评估现有安全设备效益从而进行架构的调整，降低整体持有成本（TCO）。



二、旁路部署模式



任子行下一代防火墙，采用全新设计的软/硬件架构，可在不影响任何服务的前提下，以旁路接模式接入现有网络架构中，协助网管人员进行环境状态分析，并能将分析过程中各类信息进行整理后生成针对整体环境的「应用程序使用状态及风险分析报表」（ALP Report）。在 ALP 报表中可清楚呈现所有客户端行为与网络资源使用状态，更能进一步发现潜在安全风险，作为先行预防可能面临的各种网络威胁与安全策略调整的依据。

三、路由网关模式

任子行下一代防火墙，能支持路由、地址转换等工作模式，主要用于首次部署安全网关的环境。IT部门可于完成初期数据流内容、行为模式分析及用户数据库整合后，依据分析的结果进行安全策略布署。