舟舟科技

第二代防火墙 NGFW

产品白皮书

文档版本 V3.1

发布日期：2022-11

目录

舟舟科技

第二代防火墙 NGFW 产品白皮书

缩略语：

名称缩写	完整拼写	
AD	Active Directory	活　目录
CLI	Command-Line Interface	命令行界面
DOS/DDOS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
DPI	Deep Packet Inspection	深度包检测
CSRF	Cross-Site Request Forgery	跨站请求伪造
HA	High Available	高可用性
HMAC	Hash-based Messa Authentication Code	基于哈希算法的消息认证码
ICMP	Internet Control Message Protocol	互联网报文控制协议
IKE	Internet Key Exchange	互联网密钥交换
IPSec	Internet Protocol Security	互联网协议安全
LDAP	Lightweight Directory Access Protocol	轻量目录访问协议
NAT /DNAT /SNAT	Network Address Translation / Destination Address Translation / Source Address Translation	网络地址转换 /目的地址转换 /源地址转换
NGFW	Next Generation Firewall	第二代防火墙
RDP	Remote Desktop Protocol	远程桌面协议
VPN	Virtual Private Network	虚拟专用网
WAF	Web Application Firewall	Web 应用防火墙
XSS	Cross-Site Scripting	跨站脚本攻击

一、 业务概述

1.1 网络安全新挑战

随着信息技术的飞速发展和广泛应用，网络已经渗透到社会的各个领域，成为人们工作、学习、生活中不可或缺的一部分。互联网的商业和通讯业务也随之得到快速增长，在为组织带来更多商业机会、提升组织生产效率的同时，相应地也降低了组织运营、生产和沟通成本。目前，不论政府、学校、企事业单位或是个人与网络的联系越来越紧密，网络一旦出现故障，将严重影响到工作、学习、生活。但是这些年网络安全安全事故层出不穷，安全风险比以往更加难以察觉，对社会各行各业都产生严重的影响。

随着 Web 2.0 为代表的第二代网络技术的迅猛发展，Web 化应用呈现出爆发式的增长趋势，基于互联网的应用从最初的文件共享、文件传输（FTP）、静态网页浏览（HTML）以及 Telnet 等内容单一、静态的、简单、小规模的应用，逐步发展为包括 E-Mail、ERP、OA、CRM、新闻信息、文件共享、视频会议、VoIP、即时通讯、网络游戏、电子商务、电子政务以及移动终端应用等等在内的动态的、大规模的、复杂的应用。网络承载的内容日益丰富，变得更加复杂、多样化。当今，互联网进入了应用级网络时代，逐步成为一个虚拟的真实社会。P2P 传输、网络电视、网络游戏、在线聊天、Web 视频、股票软件、网上银行、数据库、物流供应链、各种论坛以及大量未知的内容和信息纷纷涌进网络。

传统的网络安全设备，如防火墙、入侵检测系统、防病毒软件、反垃圾邮件系统等，均已远远不能满足用户对自身网络的安全防护诉求。具体表现如下：

- 基于端口的访问控制已失效

传统防火墙只能对网络流量进行基于端口的协议识别。而下一代网络中的大量应用可以直接复用同一标准协议的知名端口（如 80 端口已不再专属 HTTP，可被 P2P 使用）进行传输，或者直接承载在标准协议中（如 Web 视频直接承载在 HTTP 协议中）。因此，传统防火墙仅基于端口的控制方式已无法实现精确管控，比如，允许访问 80 端口的策略很可能会让不期望的非法流量（如 P2P）通过，甚至让黑客程序借此漏洞发动网络攻击，若完全禁止 80 端口则会

殃及 Web 应用，导致正常的网页访问无法进行。

同样，流量控制和管理也到了细分应用种类的地步，传统的基于端口的粗放型流量管理不仅可能会“误伤”应该保证的良性应用，更可能会“助长”不良应用。

- 基于 IP 地址的访问控制已不可靠

传统防火墙通过 IP 地址对各安全区域进行访问控制，同时对威胁和应用来源进行跟踪审计。然而，除了固定的 IP 接入方案，随着无线通信和移动计算设备的飞速发展，越来越多的企业给员工配置移动办公设备，甚至允许员工自带私有设备工作。在这种多网、多终端接入的环境下， IP 地址分配具有极强的随机性和不唯一性，IP 地址本身对用户身份信息的传递已经越来越不具有代表性。进而，传统的通过 IP 地址来进行用户访问控制已不再完全有效。而对网络访问者真正身份的全面有效、深度广泛的鉴定识别，才是适应社会和网络发展的最有效手段

- 入侵防御设备

应用安全防护体系不完善，只能针对操作系统或者应用软件的底层漏洞进行防护，缺乏针对 Web 攻击威胁的防御能力，对 Web 攻击防护效果不佳。缺乏攻击事后防护机制，不具备数据的双向内容检测能力，对未知攻击产生的后果无能为力，如入侵防御设备无法应对来自于 Web 网页上的 SQL，XSS 漏洞，无法防御来自内网的敏感信息泄露或者敏感文件过滤等等。

- 网络应用可见性差，存在法律风险

来自于 IDC 的权威数据显示：80%以上的 IT 管理人员无法准确了解自己的网络。对网络管理来说，自己的网络就像一个黑盒子，里面都跑了些什么应用以及网络的状况根本不清楚，而管理员无法知道异常流量的类型、来源、具体流向、流量大小、持续的时间等，也无法有效规划网络资源的使用，导致网络管理处于无序状态。

为了加强对互联网的控制和管理，公安部 151 号令要求各机构要保存至少 3 个月的访问日志，以便协助公安调查取证。因此，如无有效的管理手段，企业内部对互联网资源的非法访问，比如访问色情、赌博、犯罪网站、发表反动言论、泄露重大机密等，都会触犯相关法律，给企业带来法律风险。

1.2 产品背景

随着云计算、Web2.0、移动互联网、物联网等新兴应用技术一起被广泛使用，我国的网络安全形势变得日益严峻，传统防火墙的定义已无法覆盖细节技术需求传统定义的防火墙产品在国内的网络环境下并不能产生很好的防护效果。

我司通过深入解读公安部的《GA/T1177-2014 信息安全技术 第二代防火墙安全技术要求》的第二代防火墙标准，又针对应用和用户识别、应用安全控制、内容安全防护、性能处理能力四个方面对防火墙产品进行改进与优化，推出全新第二代防火墙产品。

二、 产品介绍

2.1 产品特点

第二代防火墙是面向应用层设计，能够精确识别用户、应用和内容，具备完整安全防护能力，能够全面替代传统防火墙，并具有强劲应用层处理能力的全新网络安全设备，第二代防火墙解决了传统安全设备在应用管控、应用可视化、应用内容防护等方面的巨大不足，同时开启所有功能后性能不会大幅下降。

第二代防火墙不但可以提供基础网络安全功能，如状态监测、VPN、抗 DDOS、NAT 等；还实现了统一的应用安全防护，可以针对一个入侵行为中的各种技术手段进行统一的检测和防护，如应用扫描、漏洞利用、Web 入侵、非法访问、蠕虫病毒、带宽滥用、恶意代码等。第二代防火墙可以为不同规模的行业用户的数据中心、广域网边界、互联网边界等场景提供更加精细、更加全面、更高性能的应用内容防护方案。

其核心理念是在用户网络边界建立以应用为核心的网络安全策略，通过逐层递进方式实现用户/应用行为的可视、可控、合规和安全，最终保障网络应用被安全高效的使用。

- 更精细的应用层安全控制：

1、贴近国内应用、持续更新的应用识别规则库

2、支持包括 AD 域、Radius 等多种用户身份识别方式

3、面向用户与应用策略配置，减少错误配置的风险

- 更全面的内容级安全防护：

1、基于攻击过程的服务器保护，防御黑客扫描、入侵、破坏三步曲

2、强化的 Web 应用安全，支持多种 SQL 注入防范、XSS 攻击、CSRF、权限控制等

3、完整的终端安全保护，支持漏洞、病毒防护等

4、双向内容检测，功能防御策略智能联动

2.2 技术特点

随着网络带宽的增加，网络应用以成倍的速度增加，应用层应用在无情地免费地侵蚀着宝贵的网络带宽，而网络安全的威胁更多的来源于应用层，对应用层的网络访问控制需要采用新的解决方案。精确的识别出应用、阻断有安全隐患的应用、保证合法应用正常使用、防止端口盗用等问题，已成为现阶段企事业用户对网络安全担忧的主题之一。

2.2.1 精细的应用层安全防护

产品采用 DPI 的识别方式使得应用层协议可视化可控，可以根据应用的行为和特征实现对应用进行识别和控制，而不仅仅依赖于端口或标准协议，摆脱了传统设备只能通过 IP 地址或者五元组控制的粗粒度，即使加密过的数据流也能进行管控。

品可以识别 6000 多种应用，识别上千种网络行为动作，还可以与多种认证系统（AD、LDAP、Radius 等）无缝对接，自动识别出网络当中 IP 地址【MAC 地址、用户身份】对应的用户信息，并建立组织的用户分组结构；满足了普通互联网边界行为管控的要求。可以识别和控制丰富的内网应用，如迅雷 P2P、RDP、Lotus Notes、RTX、Citrix、Oracle EBS、金蝶 EAS、用友 NC、U8、SAP、LDAP 等，针对用户应用系统更新服务的诉求，第二代防火墙还可以精细识别 Microsoft SHAREPOINT、奇虎 360、Symantec、 Sogou、Kaspersky、金山毒霸、

江民杀毒等软件更新，保障在安全管控严格的环境下，系统软件更新服务畅通无阻。

因此，通过应用的协议识别制定的二到七层的应用访问控制策略，可以为用户提供更加精细和直观化控制界面，在一个界面下完成多套设备的运维工作，提升工作效率。

2.2.2 Web 应用的安全防护

产品融合了漏洞防护、Web 安全防护等多种安全技术，具备 10000 多条 Web 应用威胁特征库，可以全面识别各种应用层和内容级别的各种安全威胁。提供 URL 过滤、文件过滤、ActiveX 过滤、脚本过滤等多种 Web 安全防护手段通过对应用流中的数据报文内容进行探测，从而确定数据报文的真正应用。

Web 应用防护通过主动防御已知和未知攻击，实时阻断各种黑客攻击，如 SQL 注入、XSS 攻击、网站扫描、Web SHELL、会话劫持攻击等。

1. 防 SQL 注入攻击

SQL 注入攻击产生的原因是由于在开发 Web 应用时，没有对用户输入的数据做合法性检查和判断，用户在提交一段数据库查询代码，根据程序返回的结果，获得默写他想得知的数据，这就是所谓的 SQL 注入。第二代防火墙通过高效的 URL 过滤技术，过滤 SQL 注入的关键信息，从而有效的避免网站服务器受到的 SQL 注入攻击。

2. 防 XSS 跨脚本攻击

跨站攻击产生的原理是攻击者通过向 Web 页面里插入恶意 HTML 代码，从而达到特殊目的。第二代防火墙通过先进的数据包正则表达式匹配原理，可以准确地过滤数据包中包含的跨站式攻击的恶意代码，从而保护用户的 Web 服务器安全。

2.2.3 应用层带宽管理

产品以应用对象设置、用户对象设置、时间对象设置、带宽通道对象设置、用户自定义对象设置基础，通过应用控制、流量管理、内容过滤等策略，最大限度地满足用户在流量管理方面的不同需求，实现用户网络人性化的精确管理。

专业流量管理产品满足了企业不同业务主次之分，系统分为 0-7 共 8 个 QoS 优先级控制策略，从而为指定的应用和通道提供差异化的影响级别。同时也可以为特定的实时应用，如视频会议、VOIP 等，预留固定的带宽，保证实时应用的流畅使用。

2.2.4 IPS 漏洞防护

支持 30000 多种流量异常特征库，并可以按优先级区分不同类型的漏洞攻击，按“高”，“中”，“低”区分；包括敏感信息泄露 DOS 攻击/尝试获取用户特权的攻击/尝试获取管理员特权的攻击/网络流量中发现可执行文件的注入/可疑关键字和可疑文件的注入/远程过程调用告警/网络木马程序注入/客户端使用可疑端口通信/可疑的网络扫描/篡改标准协议和非法事件的告警/潜在的 Web 攻击/ICMP 告警/异常内容告警/公司机密泄露/尝试用默认账号窃取信息等。

2.2.5 网络病毒防护

病毒库数量：2000,000+，定期更新 基于流引擎查毒技术，针对 HTTP、FTP、SMTP、POP3、IMAP 等协议进行查杀。

2.2.6 线速的状态检测防火墙

支持线路的带宽叠加，充分利用多条 Internet 接入；

支持多线路的策略路由，智能选择更快的线路接入 Internet；

支持三种工作模式（NAT 模式、透明桥模式、路由模式）；

支持状态检测防火墙（基于 IP/IP 段/IP 组、IP/MAC、PORT、时间控制等策略组合）；

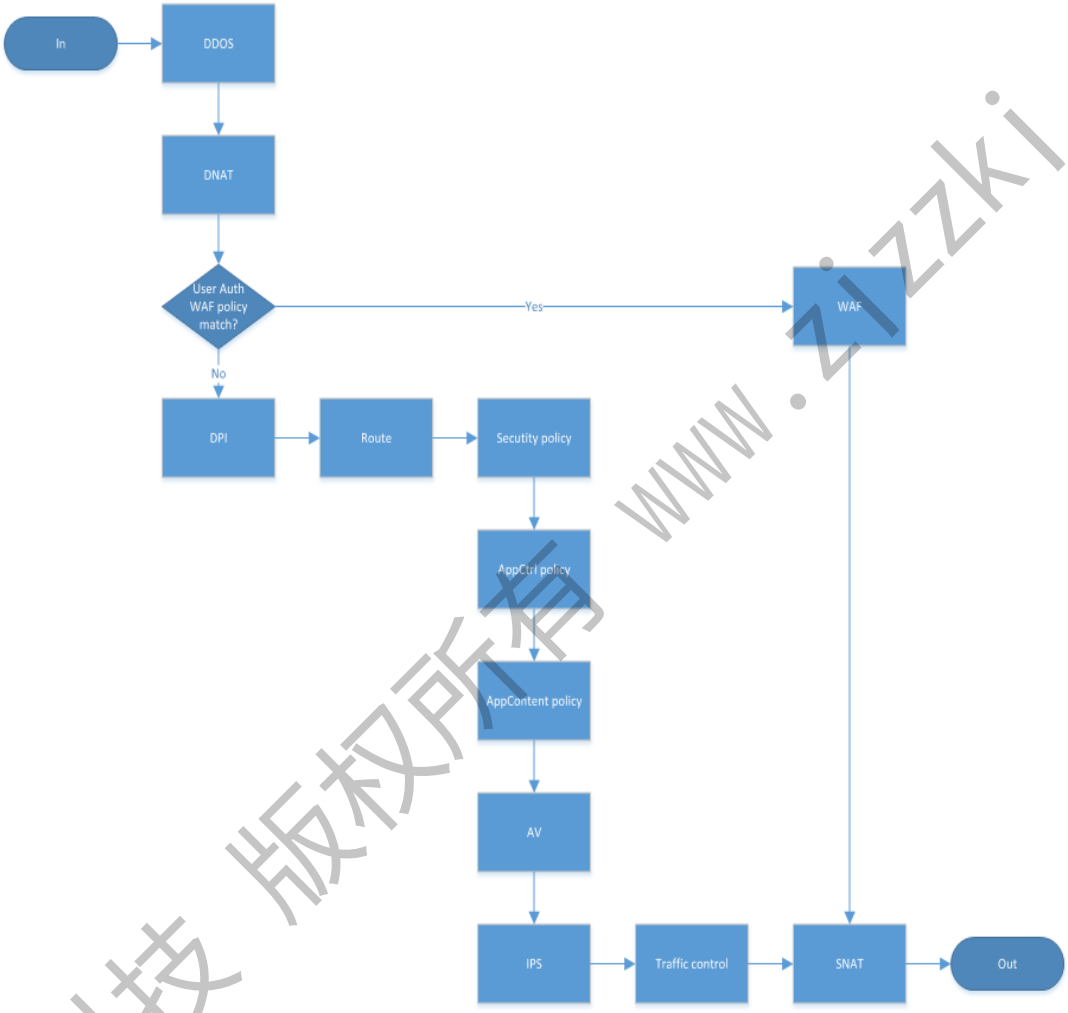
支持关键字、文件类型、域名等内容过滤；

支持 VLAN 与静态路由。

三、 主要业务流程

3.1 防火墙数据处理流程

防火墙功能数据处理工作流程图如下：



如上面流程图所示，进入防火墙设备的流入数据，

1) 首先经过 DDOS 模块的防御性过滤，对于流量中可能存在的分布式拒绝服务攻击进行拦截限制；

2) 经过 DDoS 过滤后的流量，在经过 DNAT（Destination Network Address Translation）的目的地址转换，转换的目的是将一组本地内部的地址映射到一组全球地址；

3) 经过 DNAT 地址转换后的流量，在进行用户鉴权及 Web 应用防护策略匹配

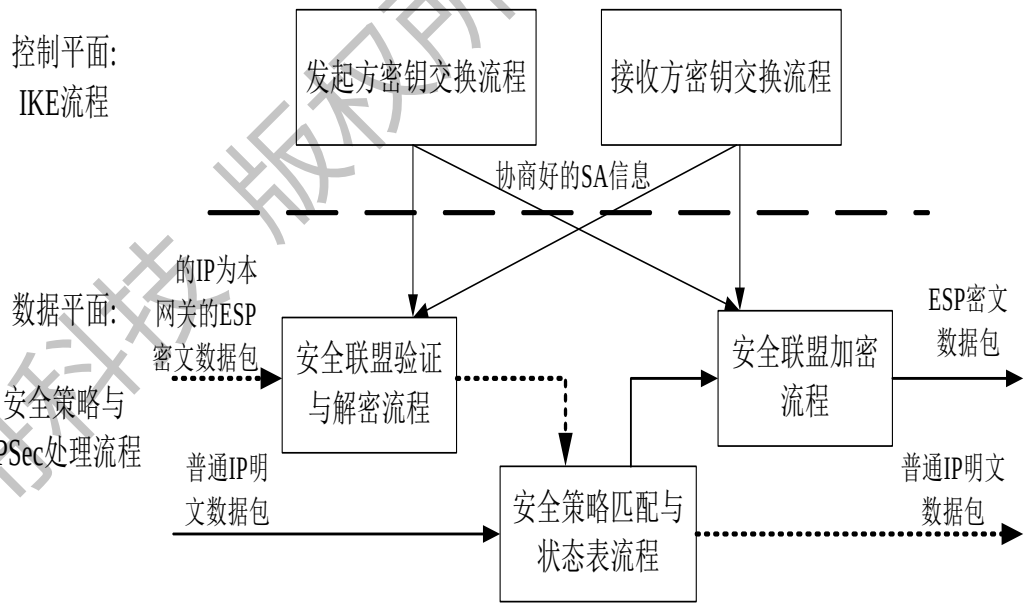
判断，如果能匹配到 WAF 策略的，就根据对应的 WAF 策略进行处理，然后经过 SNAT（源地址转换），将 ip 数据包的源地址转换成另外一个地址，然后作为经过防火墙安全过滤后的出口流量；

4) 如果流量信息未能匹配到 WAF 策略的，则进入到防火墙的 DPI 检测。DPI(Deep Packet Inspection)深度包检测技术是一种基于应用层的流量检测和控制技术，当 IP 数据包、TCP 或 UDP 数据流通过基于 DPI 技术的带宽管理系统时，该系统通过深入读取 IP 包载荷的内容来对 OSI 七层协议中的应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。

5) 经过 DPI 检测的数据紧接着进入安全路由 Route、Secur ty Policy 安全策略、App Ctrl Policy 应用控制策略、App Content Policy、AV 防病毒、IPS 入侵防御和 Traffic Control 流量控制，经过 SNAT（源地址转换），将 ip 数据包的源地址转换成另外一个地址，然后作为经过防火墙安全过滤后的出口流量。

3.2 IPSec 软件框架流程

产品 IPsec 功能数据处理工作流程图如下：



IPSec 软件框架流程包括：

- 流控平面：IKE 流程，包含了发起方秘钥交换流程、接收方秘钥交换流程；

- 数据平面：安全策略与 IPSec 处理流程，包含安全联盟验证与解密流程、安全联盟加密流程和安全策略匹配与状态表流程。

四、 产品功能

4.1 身份识别与控制

4.1.1 用户身份识别

作为第二代防火墙显著特征之一，第二代防火墙对在线用户身份识别功能做了全面细致的支持。与 传统的将用户认证策略混入防火墙策略配置中不同，第二代防火墙将用户认证从防火墙复杂的策略配置中抽离出来，从逻辑上做出更合理清晰的呈现。

用户可对不同的安全区域指定不同的认证策略，并可根据不同场景选择不同的身份识别方案，例如，可从域控制服务器直接获取身份信息，与第三方认证服务器（Radius、AD、LDAP）认证，本地账号库认证，证书认证，以及结合以上多钟认证方式于一体的多因素认证。 同时，为方便用户理解和使用，第二代防火墙对用户账号进行了集中管理和控制。只需集中配置好账户信息（包括 Radius、AD、LDAP、本地数据库、证书账号等）即可在用户认证策略、VPN 授权、设备管理员授权等多处便捷使用。

4.1.2 日志记录和统计报表

第二代防火墙让用户随时可以了解当前网络正在发生什么。具体体现为，可实时了解当前网络中正遭受哪些威胁攻击（包括入侵攻击、病毒、恶意站点及敏感信息 ，以及相应的威胁等级、攻击数目等。

同时，用户可实时了解当前网络中一段时间以来各网络接口带宽使用情况，流量排名前十的应用以及流量使用排名前十的用户，并可实时互查应用与用户流量间的使用关系。除了实时网络状况，第二代防火墙为用户提供按日、按周、按月、按年的安全趋势分析报表以及以往所有的访问控制和安全日志。从而让用户对安全威胁、业务应用、用户流量、网络负载从时间、数量、程度上通过各种形象化图形和数据手段有了高度可视化的跟踪和了解。

4.2 应用层防护

4.2.1 URL 过滤

第二代防火墙具有业界领先的基于云端的 URL 分类库，内含按照不同类型（如不良言论、色情暴力、网络“钓鱼”、论坛聊天等）划分的超过上亿条记录的 URL 信息，可实现对工作无关网站、不良信息、高风险网站的准确、高效过滤；

同时第二代防火墙内置的 Web 信誉库，通过对互联网站点资源（域名、IP 地址、URL 等）进行威胁分析和信誉评级，将含有恶意代码的网站列入 Web 信誉库，可有效阻挡用户对挂马等不良信誉网站的有意或无意访问，实现对终端用户的安全保护。

4.2.2 防病毒

第二代防火墙采用流模式和启发式文件扫描技术，对利用 HTTP、SMTP、POP3、FTP、IM 等多种协议进行传播的病毒进行扫描，完成对木马病毒、蠕虫病毒、宏病毒、脚本病毒等的查杀，同时支持多线程并发控制、深层次压缩文件杀毒、病毒白名单等功能。

此外，第二代防火墙将专业防病毒引擎和多核并行处理技术完美融合，实现高速病毒处理性能。

4.2.3 内容过滤

通过内容安全关键字，第二代防火墙可对任意安全区域间交互的网页内容、搜索引擎信息内容、文件传输（文件名、格式、内容）、邮件收发（包括收发人、标题、内容、文件等）、论坛发言、服务器操作、以及即时通讯内容等进行基于内容关键字的准确检测、阻断、告警、记录和信息还原，实现深度内容安全管理与跟踪，避免用户机密信息、重要文件通过网络外泄，也避免了非法言论及不良信息的传播。

4.3 产品功能列表

编号	功能项	功能描述
1	基础网络功能	支持静态路由、策略路由、均衡策略、路由选路、持续路由、链路备份、子接口、聚合接口、IPv6toIPv4 隧道、网口顺序调整、ADSL 拨号、DHCP 服务器、DHCP 中继、DHCP 客户端、DNS 代理、DNS 缓存、动态 DNS 功能。
2	基础防火墙功能	支持防火墙、安全策略、NAT 转换功能
3	VPN 功能	支持 IPSec VPN、PPTP/L2TP VPN、SSL VPN。
4	IPS 入侵防御功能	支持防 DNS 漏洞攻击、防 Mail 漏洞攻击、防 Worm 漏洞攻击、防 TFTP 漏洞攻击、防 SNMP 漏洞攻击、防 FTP 漏洞攻击、防 Shellcode 漏洞攻击、防 RPC 漏洞攻击、防 Database 漏洞攻击、防 Web 漏洞攻击、防 system 漏洞攻击、防 Malware 漏洞攻击、防 Trojan 漏洞攻击 防 Telnet 漏洞攻击、防 Botnet 漏洞攻击、防 Web Browse 漏洞攻击、防 Web ActiveX 漏洞攻击、防口令暴力破解攻击。
5	DOS/DDOS 防护	支持 ARP 洪水攻击防护、IP 和端口扫描防护、DOS/DDOS 防护（ ICMP 洪水、UDP 洪水、SYN 洪水、DNS 洪水攻击防护）、未知协议类型防护、TearDrop 攻击防护、IP 数据块分片传输防护、LAND 攻击防护、WinNuke 攻击防护、Smurf 攻击防护、异常报文侦测防护等
6	服务器防护	支持 Web 网站隐藏，包括 HTTP 响应报文头出错页面的过滤，Web 响应报文头可自定义； 支持 FTP 服务应用信息隐藏包括：服务器信息、软件版本信息等；

		支持 OWASP 定义 10 大 Web 安全威胁，保护服务器免受基于 Web 应用的攻击，如 SQL 注入防护、XSS 攻击防护、CSRF 攻击防护、支持根据网站登录路径保护口令暴力破解；支持 Web 站点扫描、Web 站点结构扫描、漏洞扫描等扫描防护； 可严格控制上传文件类型，检查文件头的特征码防止有安全隐患的文件上传至服务器，并支持结合病毒防护、插件过滤等功能检查文件安全性；
7	病毒防护功能	基于流引擎查毒技术，支持对 HTTP、FTP、SMTP 和 POP3 协议流量查杀；云端特征库收录亿级病毒文件样本；检测到病毒后支持日志记录、阻断连接。
8	应用内容过滤功能	支持海量 URL 库、URL 过滤、非标准端口 URL 管理 关键字过滤、HTTP 文件传输过滤、FTP 文件传输过滤 非标准端口 FTP 过滤、邮件过滤功能
9	应用控制策略	持基于视频流媒体、P2P 下载类、网络游戏、即时通讯、股票类、网银类、IP 通讯类、网络存储类、Webmail 邮箱类、软件更新、远程控制、数据库等网络应用的策略控制。 同时支持自定义特征库识别，可根据五元组，数据长度，数据报文特征字符串组合自定义特征。
10	流量控制	支持流量优先级、最大带宽控制、保障带宽、预留带宽、基于线路的流控、基于应用的流控、基于 IP 的流控、基于用户组的流控、基于时间段的流控、基于单个用户的流控功能
11	黑名单功能	支持对共享上网、流量配额、速率控制、并发会话数控制、新增会话数控制、基于时间段的控制

		等行为进行黑名单管控功能，同时支持多种惩罚方式、加倍惩罚机制
12	白名单功能	支持基于内网用户的白名单、基于外网 IP 地址白名单、基于时间段的控制白名单控制功能
13	流量实时监控	支持 TOP 50 服务流量监控、服务组流量监控、活跃服务统计、所有服务统计、TOP 50 用户流量监控、在线用户统计、上网行为监控、物理端口监控、动态更新实时监控图、防共享上网监控、当前黑名单监控
14	日志审计策略	支持审计策略和审计选项
15	用户认证	支持组织结构管理、临时账户管理，支持批量生产临时账号； 支持本地认证、AD 域认证、RADIUS 认证 、LDAP 认证 Web 认证、短信认证； 支持 LDAP/AD 导入、用户同步、用户导入、自动创建账户； 支持终端识别、IP/MAC 绑定、VLAN 绑定； 认证通过后，支持显示指定页面、自定义认证页面 支持认证冲突处理，内网主机扫描功能
16	自身安全防护	支持高可靠性(HA)、防 ARP 欺骗、会话加速老化功能
17	故障与告警	支持设备事件日志告警、黑名单告警、CPU、内存、活跃会话数、入侵事件、攻击事件等告警； 支持自动邮件告警、自动短信告警； 支持设备故障、调试信息下载。
18	报表与统计	内置报表中心，支持图形化日志统计工具、分层管理、报表生成；

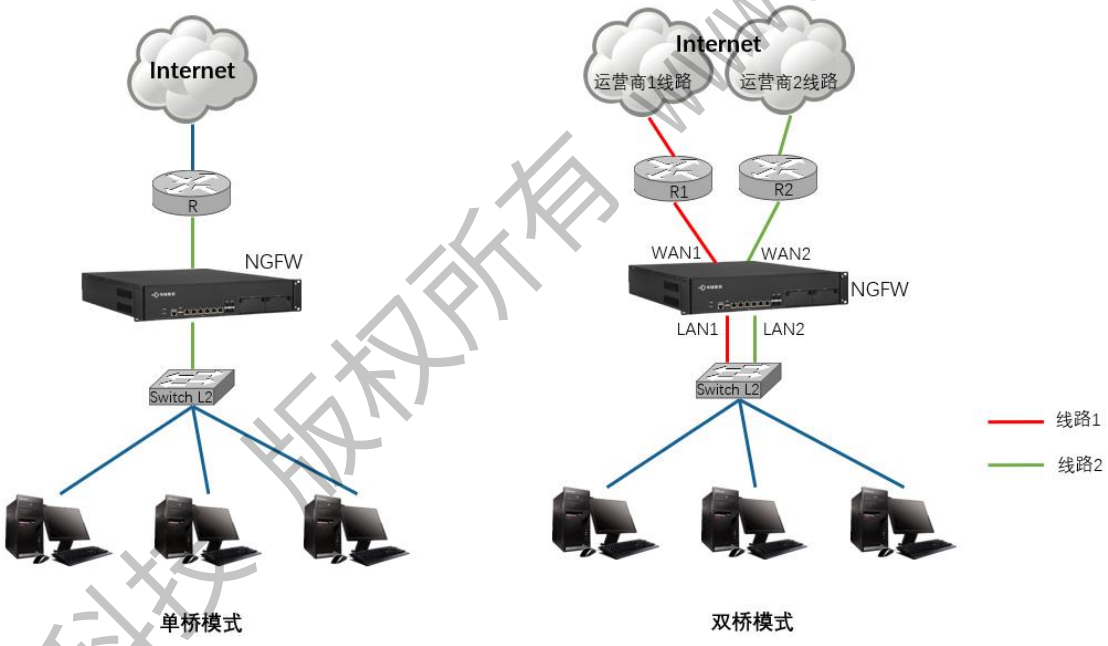
		支持对于设备资源、物理接口统计、用户统计、用户组统计、服务统计、服务类型统计、网站统计、网站类型统计、线路统计、网站访问量排名、网页文件下载排名、上网时长的统计功能
19	日志功能	支持记录 DoS 攻击日志、IPS 日志、Web 应用防护日志、病毒查杀、网页 URL 日志、阻挡记录、会话记录、告警记录，以及对日志信息的高级检索
20	数据管理	支持对于数据存储策略管理、数据列表查询 支持数据删除和数据备份
21	网管方式与网管策略	Web UI 方式：支持以 HTTP 及 HTTPS 协议，支持英语、简体中文、繁体中文界面。 CLI 方式：支持 SSH 管理、Console 管理 支持的网管策略 1）管理权限分立：系统默认有超级管理员、审计管理员、只读管理员，可根据需要灵活定制管理员角色。 2）支持密码强度、口令尝试死锁、账户激活等安全管理功能。 3）通过网管策略，可允许部分 IP 能网管设备，以限制非法管理员访问设备。
22	部署方式	支持路由模式、透明模式、虚拟线路模式、混合模式

五、 产品部署方式

舟舟科技第二代防火墙 NGFW 设备可采用串接方式接入网络，支持网桥（透明）模式、路由模式、旁路模式和混合模式。

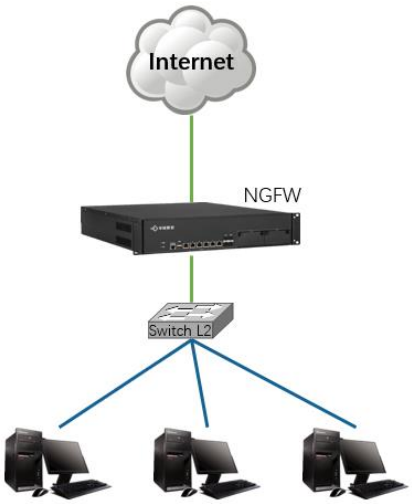
5.1 网桥（透明）模式

以透明网桥方式接入网络，可以部署到网络的网关位置或各部门的出口位置。无需改动用户网络结构和配置，即插即用，支持单网桥，多网桥的部署方式。

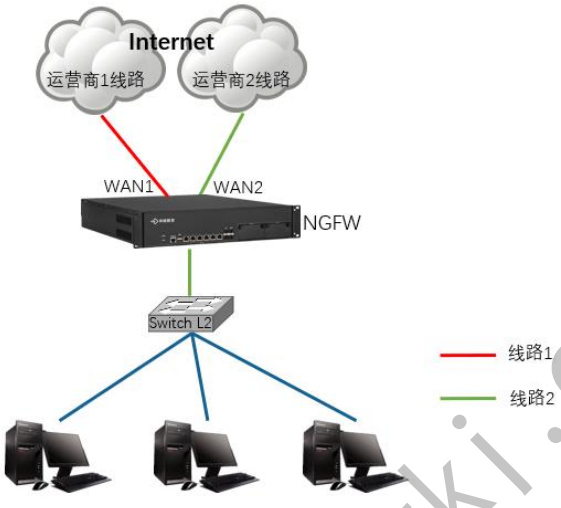


5.2 路由模式

将设备串接网络中，可以放于内网的任意子网边界，或与核心交换机相连。可以代替防火墙或路由器，需要为设备配置内网和外网接口的 IP 地址。



单链路路由模式



双链路路由模式

5.3 旁路模式

以透旁路方式接入网络，可对网络的流量进行全面的监控和记录，无需改动用户网络结构和配置。