舟舟科技

第二代防火墙 NGFW

产品功能列表

文档版本 V3.0

发布日期：2022-11

第二代防火墙 NGFW 产品功能列表

具体指标	功能描述
1. 部署模式	
路由模式	支持路由模式部署，可以作为出口网关，包括单出口和多出口的部署模式。
透明模式	支持透明模式部署，类似于普通的交换接口。
混合模式	支持透明和路由混合部署模式。
2. 网管方式与网管策略	
Web 管理	支持以 HTTP 及 SSL 加密的 Web 图形化接口进行设备配置和管理，支持英语、简体中文、繁体中文接口。
SSH 管理	支持 SSH 命令行管理方式。
Console 管理	支持 Console 管理。
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。
3. 网络功能	
静态路由	支持 IPv4、IPv6 静态路由功能。
策略路由	支持 IPv4、IPv6 策略路由功能。
均衡策略	支持 IPv4、IPv6 链路的负载均衡。
运营商路由选路	支持运营商路由选路。
持续路由	支 IPv4、IPv6 链路持续路由算法。
链路备份	支持 IPv4、IPv6 主备链路的备份功能。
邻居表	支持 IPv6 邻居表功能。
OSPF 路由	支持标准 OSPF 路由
RIP 路由	支持标准 RIP 路由
子接口	支持物理接口添加子接口功能。
聚合接口	支持将多个以太网物理端口捆绑成一条逻辑端口，不仅增加链路带宽，同时增加链路备份。
6to4 隧道	支持纯 IPV6 环境间跨过 IPV4 环境互相通信
NAT66	支持 IPV6 到 IPv6 的内网代理上网，一对一地址转换，端口映射，服务器负载均衡。
NAT64	支持 IPv6 到 IPv4 的代理上网，IPv4 到 IPv6 的端口映射，IPv6 到 IPv4 的端口映射。
DNS64	支持代理 IPv6 的 DNS 请求，把 DNS AAAA 记录请求转换为 DNS A 请求发送出去，并在收到响应后，返回把 DNS AAAA 给客户端。也配合 NAT64 功能使用，可以达到在 IPv6 网络中访问到 IPv4 资源的目的。

网口模式	支持 Web 页面改变网口的排列顺序
ADSL 拨号	支持 ADSL 拨号功能，支持多条 PPPOE 拨号做负载均衡。
DHCP 服务器	支持 DHCP 服务器功能。
DHCP 中继	支持 DHCP 中继功能。
DHCP 客户端	支持 IPv4、IPv6 DHCP 客户端功能。
DHCPv6	支持 IPv6 无状态自动配置。
DNS 代理	支持 DNS 代理功能。
DNS 缓存	设备作为 DNS 透明代理，缓存 DNS 记录。
动态 DNS 功能	支持动态 DNS 功能（花生壳）
智能 DNS	对于多 IP 的 DNS 解析，支持根据用户的来路而做出一些智能化的处理，然后把智能化判断后的 IP 返回给用户，而不需要用户进行选择。智能 DNS 均衡算法包括:按权重、按上行流量、按下行流量、按总流量。
代理配置	支持 SSL 透明代理、HTTP 代理、强制代理、二级代理
4. 基础防火墙功能	
防火墙	支持基于状态监测的防火墙，不仅保障网关设备安全，还能保护组织内网安全。
安全策略	支持包过滤检测功能，默认情况下，拒绝所有的数据包通过，以保证网络的安全性，且不能修改、移动和删除。
NAT 转换	支持多对一的 PAT 转换、一对一的地址转换、多对多等多种 NAT 转换策略。
ARP 欺骗防护	防护设备本身或者网关本身的 ARP 攻击。
VPN 功能	
PPTP VPN	支持 PPTP VPN
IPSec VPN	支持标准的 IPSec VPN 功能。
SSL VPN	支持标 的 SSL VPN 功能
L2TP VPN	支持标准的 L2TP VPN 功能
GRE 隧道	支持 GRE 隧道功能。
6. IPS 入侵防御	
防 DNS 漏洞攻击	DNS 类规则识别各种 DNS 服务器漏洞，防止攻击者通过 DNS 服务器漏洞攻击用户。
防 mail 漏洞攻击	邮件库类规则识别各种邮件服务器漏洞，如 Sendmail、Foxmail、MS Exchange 等，防止攻击者通过邮件服务器漏洞攻击用户。
防 worm 漏洞攻击	蠕虫程序是一种可以自我复制的恶意程序，可以通过网络进行传播，消耗网络和系统资源。蠕虫规则识别蠕虫程序的传播，防止攻击者通过蠕虫程序破坏目标系统。
防 TFTP 漏洞攻击	TFTP 类规则识别各种 TFTP 服务器漏洞，如 3CDeamon、FutureSoft 等，防止攻击者通过 TFTP 服务器漏洞攻击用户。
防 SNMP 漏洞攻击	SNMP 类规则识别各种 SNMP 服务器漏洞，防止攻击者通过 SNMP 服务器漏洞攻击用户。

防 ftp 漏洞攻击	Ftp 类规则识别各种 ftp 服务器漏洞，如 Serv-U、WU-FTPD、WS_FTP、3CDeamon 等，防止攻击者通过 ftp 服务器漏洞攻击用户。
防 shellcode 漏洞攻击	Shellcode 是一段小的程序，作为漏洞执行的负载，执行某种功能。Shellcode 规则识别 shellcode 代码，防止攻击者远程执行 shellcode 代码。
防 RPC 漏洞攻击	RPC 类规则识别各种 RPC 服务器漏洞，如 tooltalk、sadmind 等，防止攻击者通过 RPC 服务器漏洞攻击用户。
防 database 漏洞攻击	数据库类规则识别各种数据库服务器漏洞，如 Oracle、SQL server、MySQL 等，防止攻击者通过数据库服务器漏洞攻击用户。
防 Web 漏洞攻击	Web 类规则识别各种 Web 服务器漏洞，如 IIS、Apache 等，防止攻击者通过 Web 服务器漏洞攻击用户。
防 system 漏洞攻击	系统类规则识别各种操作系统漏洞，如 Windows、Linux、Unix 等操作系统，防止攻击者通过操作系统漏洞攻击用户。
防 malware 漏洞攻击	Malware 就是植入你电脑中的恶意代码，它可以完全控制、破坏你的 PC、网络以及所有数据。malware 类规则识别各种 malware 程序，防止攻击者利用 malware 漏洞攻击用户。
防 trojan 漏洞攻击	木马软件是一种恶意软件，可以安装在用户计算机上，通过木马软件远程操控目标系统并执行各种操作。木马规则类识别木马软件的网络操作，防止攻击者通过木马软件控制目标系统。
防 Telnet 漏洞攻击	Telnet 类规则识别各种 Telnet 服务器漏洞，防止攻击者通过 Telnet 服务器漏洞攻击用户。
防 botnet 漏洞攻击	botnet 类规则识别各种客户端 botnet 行为，防止攻击者通过 botnet 漏洞控制用户。
防 Web_browse 漏洞攻击	Web 浏览器类规则识别各种 Web 浏览器漏洞，如 IE、Firefox、Chrome 等，防止攻击者通过 Web 浏览器漏洞攻击用户。
防 Web_activex 漏洞攻击	ActiveX 是可以重用的软件组件程序，可以嵌入到 Web 浏览器中使用。Web_activeX 类规则识别各种嵌入到浏览器的 ActiveX 控制漏洞，防止攻击者通过 ActiveX 控件漏洞攻击用户。
防口令暴力破解攻击	攻击者在限定时间频繁登录 FTP、Telnet、POP3、MYSQL 等服务器失败，可能存在暴力破解攻击。
7. DoS/DDoS 防护	
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
8. 服务器防护	

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；
9. 内容安全	
9.1病毒防护	
病毒防护	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。
9.2应用内容过滤	
海量 URL 库	预分类的海量 URL 地址库；支持手工添加新的 URL 地址和分类。
URL 过滤	支持 URL 过滤。
非标准端口 URL 管理	可以识别和管理部分论坛、网络聊天室等采用的非 TCP/80 端口的 URL 地址
关键字过滤	对搜索引擎中输入的关键词、论坛微博发帖关键字、网页内容关键字、Telnet 关键字进行过滤，自动对搜索到的网址页面进行屏蔽，帮组企事业单位将涉及低俗的、非法的不良言论封堵掉。
HTTP 文件传输过滤	可识别 HTTP 网页的文件上传和文件下载，并对文件的上传和下载进行过滤。
FTP 文件传输过滤	可识别 FTP 网页的文件上传和文件下载，并对文件的上传和下载进行过滤。
非标准端口 FTP 过滤	支持对非标准端口的 FTP 行为的识别；可过滤通过非标准端口的 FTP 进行文件的上传和下载。
邮件过滤	基于 WebMail 发件、SMTP 发件、POP3 收件，可根据发件人邮箱、关键字、附件类型、附件大小过滤。
9.3应用控制策略	
常用协议	如 FTP、SMTP、TFTP、IMAP 等常用协议。
自定义协议	1、可自定义基于协议和端口的协议； 2、可根据协议、端口、报文长度、报文特征、目的 IP 等等信息自定义协议规则。
自定义特征识别	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。
协议剥离	支持将特殊协议（如 MPLS、PPPoE、VLAN（Q-in-Q）、L2TP、

	GRE、CAPWAP 等）的协议头剥离掉，这样可以对特殊协议封装内的原始数据进行认证、审计和控制。
HTTP 应用	网页文档下载、网页音频、HTTP 多线程下载、伪 IE 下载等多种方式的 HTTP 下载行为以及 QQ 空间应用、人人网、Facebook 等网页应用。
FTP 应用	FTP 上传文件、FTP 下载文件、FTP 命令。
视频网站浏览	凤凰视频、乐视网、优酷、土豆、搜狐视频、奇艺视频等网站的浏览。
Web 视频	六间房、土豆、新浪视频、优酷视频、我乐网、酷六视频、搜狐视频等。
P2P 下载	电驴、迅雷、PP 点点通、酷狗、BT、网际快车、QQ 旋风、百度下吧、酷我八音盒等。
流媒体	PPLive、PPStream、蚂蚁电视、Qvod、风行网络电视、QQLive、UUsee 网络电视、皮皮影视（PPFilm）SopCas 等。
网络游戏	QQ 游戏、浩方对战平台、新浪游戏大厅、梦幻西游、问道、武林外传、泡泡堂、天龙八部、大话西游、征途、魔兽世界等。
即时通讯	QQ/TM、MSN、网易泡泡、淘宝旺旺、雅虎通、阿里旺旺、百度 HI、新浪 UC 等。
股票行情	同花顺、大智慧、东方财富通、和讯财经、安信行情、齐鲁证券等。
股票交易	同花顺、大智慧、安信行情、齐鲁证券、大福星、通达信等。
网上银行	中国银行、农业银行、建设银行、工商银行、招商银行等。
网络电话	Skype、ET263、YY 语音、Netmeeting 等。
网络存储	360 云盘、七牛云、新浪微云、腾讯微云、百度网盘、金山快盘等。
移动应用	移动终端的新闻资讯、社交通讯、购物支付、移动游戏、综合服务等分类。
网页邮箱	新浪邮箱、QQ 邮箱、163 邮箱、126 邮箱、搜狐邮箱等。
软件更新	诺顿、金山毒霸、趋势科技、网秦安全、熊猫卫士、360 安全卫士等。
远程控制	QQ 远程协助、SSH、Windows 远程桌面、VNC、teamview 等。
数据库	DB2、MySQL、Oracle、SQL 等。
10. 流量控制	
流量优先级	可将应用流量划分为 高、中、低等共三个优先级，优先级越高的流量，优先传送。
最大带宽	为某些用户或特定应用指定最大带宽。
基于线路的流控	可以根据线路进行流量管理。
基于应用的流控	结合应用协议识别功能，可以根据用户的应用协议类别进行流量管理。
基于 IP 的流控	根据源 IP 地址/地址组进行流量管理。

基于用户组的流控	可以为不同用户组采取不同的流量管理措施。
基于时间段的流控	可以根据不同的时间段，进行差异化的流量管理。
基于单个用户的流控	可根据主机的 IP 地址或者用户名称，对单个主机进行如下控制： ✧ 最大上行/下行带宽限制； ✧ 最大上行/下行会话控制； ✧ 分类服务的带宽控制，即限制单主机的总带宽的同时，再对某些服务进行控制。如限制单个主机的上行/下行带宽分别为 500K/1M 的同时，再限制 P2P 的带宽为 100K/200K、网络电视为 100K/100K 等； ✧ 以上参数均可分时段管理。
11. 白名单管理	
基于内网用户的白名单	可对内网用户（IP 地址、地址范围、IP 组、用户组）进行白名单的控制。
基于外网 IP 地址白名单	可对内网用户访问特定的互联网 IP 地址（IP 地址、地址范围、IP 组）进行白名单的控制。
基于时间段的控制	可根据时间段进行白名单的控制。
12. 流量实时监控	
TOP 50 服务流量监控	查看前五十名服务流量的实时监控。
服务组流量监控	将各服务分类统计，实时查看服务组流量监控图。
活跃服务统计	查看当前活跃服务的最新速率、最近一小时流量、最近一小平均速率、每个服务对应有哪些用户在使用，及每个用户的使用情况。
所有服务统	查看当前活跃服务的最新速率、最近一小时流量、最近一小时平均速率。
TOP 50 用户流量监控	查看前五十名用户的传输速率、新建会话速率、活跃会话数。
线用户统计	实时查看当前在用户的详细信息：在线流量、最新速率、会话数、上线时间等信息。
物理端口	查看物理端口接收报文的情况，以及每个端口传输流量的趋势图。
动态更新实时监控图	支持动态显示网络流量监控图。
实时攻击日志	支持查看实时 DoS、IPS、病毒防护和服务器防护的攻击日志，并支持自定义过滤对象和刷新频率。
待处理风险	支持查看待处理的问题和修复建议，支持展示风险主机，风险服务器和外部威胁清单。

13. 用户认证	
组织结构	可建立与企业组织结构相同的网络组织结构，将用户划分到对应用户组中。每个用户或用户组都可以有自己的上网策略及权限。
本地认证	将用户信息存储于设备内，认证时无须第三方服务器。
AD 域认证	支持 AD 域认证，便于与组织内部原有域认证融合。
RADIUS 认证	支持与第三方 RADIUS 服务器联动认证。
LDAP 认证	支持 LDAP 认证，便于与组织内部原有 LDAP 认证融合。
PORTAL 认证	支持跟 PORTAL 服务器联动认证。
AWIFI 认证	支持跟 AWIFI 服务器联动做 PORTAL 鉴权认证。
Web 认证	结合本地数据库、POP3、AD、LDAP 或 RADIUS 服务器等认证方式，为接入用户提供 Web 认证功能。
短信认证	支持通过短信验证码、密码/短信认证组合的认证方式。（第三方短信网关联动认证）
微信认证	✧ 支持微信点一点认证方案，通过微信关注认证的用户，需要进入微信公众号中重新点击“申请上网”，才可以继续上网。 ✧ 支持微信连一连认证方案，通过调用微信连 Wi-Fi 接口，进行微信认证获取 openid 或者 tid 或手机号，其中解析手机号需要在微信公众平台申请 key。 ✧ 支持微信连一连支持区域微信认证，一个设备，可以支持多个门店接入微信认证。
LDAP/AD 导入	可按照 LDAP/AD 等服务器组织架构导入用户/用户组信息。
用户同步	可将 LDAP、AD 等外部服务器的用户信息同步到设备中，无须在手动添 用户信息。
用户导入	可将已导出的用户信息的文件，或根据规定的用户格式编辑文件，批量导入用户信息。
自动创建账户	对于未创建的账户，可根据其 IP 地址、MAC 地址、主机名或者 VLAN ID 等作为新用户名自动创建账户，并可同时绑定 IP、绑定 MAC、绑定 IP+MAC、绑定 VLAN，并自动分配到指定用户组，享有指定网络权限。
终端识别	支持终端类型（PC，android，苹果）识别，可识别操作系统类型及对应 IP 地址。
IP/MAC 绑定	支持绑定 IP、绑定 MAC、绑定 IP+MAC。
VLAN 绑定	支持 VLAN 绑定。
认证通过后显示指定页面	可将认证通过的用户强制导向到企业入口网页，如组织的公告页面等。
自定义认证页面	支持自定义的用户认证登录页面。
认证冲突处理	支持账户重复登入，当超出最大登入允许数后，支持是否踢掉前一次登入。
内网主机扫描	可通过 NetBIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理。

14. 自身安全防护	
高可靠性(HA)	支持一主一备、主/主模式的 HA 功能。
防 ARP 欺骗	定期发送 ARP 广播，防止网关设备 ARP 被篡改。
会话加速老化	对某些会话进行快速老化，防止会话表被写满。
15. 故障排除	
调试信息下载	一键下载故障信息，以便研发人员分析故障。
16. 报表中心	
内置报表中心	设备内置报表中心系统，实现上网行为记录与日志的存储、查询、审计，以及报表的生成等。
图形化日志统计工具	通过图形化的报表中心，方便用户对行为记录的查询、审计统计，并支持以饼状图、柱状图、曲线图等形式直观显示统计结果。
分层管理	根据管理员的权限，可以查看到只属于其管辖范围的用户的统计资料。
报表生成	可将报表中心相关内容转换为 Excel、PDF 报表，大大简化了管理员手工制作报表。
16.1 统计分析	
设备资源	分时段对设备资源，包括 CPU 使用率、内存使用率、活跃会话数、在线用户数等信息进行统计分析。
物理接口	分时段对物理接口的收发的流量、速率等进行统计分析。
用户统计	基于用户，对其流量 新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个用户使用了哪些服务、访问了哪些网站、通过了哪些链路等更加详细的信息。
用户组统计	基于用户组，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个用户组使用了哪些服务、访问了哪些网站、通过了哪些链路等更加详细的信息。
服务统计	基于服务名称，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务在各条链路上的分配情况。
服务类型统计	基于服务类型，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种类型的服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务类型在各条链路上的分配情况。
网站统计	基于 URL，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个 URL 的服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务类型在各条链路上的分配情况。
网站类型统计	基于网站类型，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种类型的网站有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务类型在各条链路上的分配情况。
线路统计	基于出口链路，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每条链路上的用户、用户组、

	服务、服务类型、网站、网站类型的详细信息。
网站访问量排名	1、基于用户/用户组对 URL 的访问次数，进行统计排名。 2、基于网站/网站类型被访问的次数，进行统计排名。
网页文件下载排名	1. 基于用户/用户组，通过网页下载的文件次数，进行统计排名。 2. 基于文件类型被下载的次数，进行统计排名。
上网时长统计	统计用户上网的总时长，并统计每类服务使用时间的情况。
16.2 日志查询	
DoS 攻击日志	记录 DoS 攻击日志，包括攻击类型、源区域、源目 IP 地址、目的 IP 地址、匹配策略名、描述、严重级别、记录时间
IPS 日志	记录 IPS 日志，包括攻击类型、源区域、源目 IP 地址、目的端口、漏洞 ID、漏洞名称、匹配策略名、描述、严重级别、记录时间。
Web 应用防护日志	记录 Web 应用防护日志，包括攻击类型、协议、URL/目录、源/目的区域、源/目的 IP、源/目的端口、详细信息、规则名称、严重等级、动作、时间等
病毒查杀	记录病毒查杀日志，包括应用类型、行为、协议、文件名、文件类型、病毒名称、源目区域、源目 IP、源目端口、所属组、记录时间。
网页 URL 日志	能够记录用户所访问网站的 URL 地址。
阻挡记录	记录安全策略、应用控制策略、应用内容过滤、防病毒、Web 应用防护、IPS、DoS/DDoS 中被阻挡的日志，包括源/目的端口、协议类型、应用类型、规则名称、记录时间等
会话记录	详细记录每一个会话的信息，包括：用户名、用户组、源 IP/端口、目的 IP/端口、转换 IP/端口、MAC 地址、协议类型、协议名称、发送流量、接收流量、会话持续时间、会话结束时间。并可导出为 EXCEL 或者 HTML 格式的报表。
认证日志	分别支持查看 IPv4、IPv6 认证日志，包括用户名/用户组、IP 地址/MAC 地址、上线时间、下线时间、发送流量、接受流量、认证类型、认证结果等信息查询。
16.3 数据管理	
数据存储策略	支持按磁盘百分比、按保留天数、系统硬盘最大化三种存储方式。
数据列表查询	支持查询磁盘空间使用和剩余空间、百分比，包括每一种数据类型的使用空间、磁盘占用率，时间范围。
数据删除	基于时间范围、数据类型明细、系统日志明细删除日志。
数据备份	支持备份本地存储日志到 FTP 服务器，为日志审计提供冗余备份。