NF500

下一代防火墙安全网关

飞鱼星科技股份有限公司

产品概述

飞鱼星 NF500 下一代防火墙是针对政府企业、园区网互联网出口以及广域网分支市场推出的下 一代高性能防火墙产品。

NF500 防火墙将深度内容检测、安全防护、上网行为管理等技术完美的结合在一起。配合实时 更新的入侵攻击特征库，可检测防护多种的网络攻击行为，包含 DoS/DDoS、病毒、蠕虫、僵尸网络、木马、间谍软件、可疑代码、探测与扫描等各种网络威胁。并具有丰富的上网行为管理，可对 P2P、 聊天、在线游戏、虚拟通道等应用，同时支持对 HTTPS 网页、UC 浏览器、SSL 加密邮件的审计，移动应用识别，真正实现细粒度管理控制。同时全面支持高可用性（HA）、日志审计等功能，从而很好 地提供了动态、主动、深度的安全防御。同时支持多种 VPN 业务，如：IPSec VPN 和 SSL VPN 等； 支持 IPv4/IPv6 双协议栈，同时可实现针对 IPV6 的状态防护和攻击防范。

特色功能

下一代多业务特性，建立全面安全体系

全面的应用层流量识别与管理，不仅能在应用层进行识别和管理，同时提供 HTTPS 审计和邮箱解密功能， 对加密流量识别技术，能够对主流的加密网站、加密网站搜索记录、加密邮件等进行行为识别。管理员可以采用自定义的方式，定向审计用户和加密网站，让网络简化透明。入侵防御（IPS），支持 Web 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击等。

集成 VPN 特性，满足移动办公、员工出差的安全访问需求，结合身份认证实现一体化的认证接入。系统开启多重功安全防护后，性能无明显下降，保证业务流畅应用；

防病毒（AV），高性能病毒引擎，可防护 300 万余种的病毒和木马，病毒特征库长期稳定更新。网页应用防护（WD）基于快速扫描引擎解析 Web 交互信息，在进行解码的基

础上，对攻击的形式逻辑进行判断过滤，实现 HTTP 深度识别。同时，开启危险文件下载检测，阻断下载数据库等危险文件，避免攻击者下载用户密码等敏感内部信息。

精细化行为管控，确保上网环境安全

产品具有丰富的内网上网行为管理功能。对数据进行 2-7 层的全面检查和分析，深度识别、管控和审计数百种 IM 聊天软件、P2P 下载软件、炒股软件、网络游戏应用、流媒体在线视频应用等常见应用，并利用智能流控、智能阻断、智能路由、智能 DNS 策略等技术提供强大的带宽管理特性，配合创新的社交网络行为精细化管理功能、清晰易管理日志等功能，同时具备了最精细的用户上网行为的审计功能，提供了业界最全面、完善的上网行为管理解决方案。

P2P 控制：对 Emule、BitTorrent、迅雷、百度网盘等进行阻断、限速。

IM 控制：基于黑白名单的 IM 登录控制、文件传输阻止、查毒；支持主流 IM 软件如：QQ、 MSN、雅虎通、Gtalk、微信。

流媒体控制：对流媒体应用进行阻断或限速，支持优酷、爱奇艺、搜狐视频、腾讯视频、斗鱼 TV、虎牙 TV 等。

网络游戏控制：对常见网络游戏如魔兽世界、征途、QQ 游戏大厅、联众游戏大厅等的阻断。

股票软件控制：对常用股票软件如同花顺、大参考、大智慧等的阻断。

审计内容日志，记录网络行为轨迹

能够贴近各种不同网络架构的需求，并且提供网管人员最友好的管理接口，以及多种实用的报表。直观实时显示，包括实时统计数据，实时事件列表，流量监视器，系统状态监视，交叉查询，样板报表与定期报表。

记录内容丰富：可对防火墙日志、攻击日志、病毒日志、带宽使用日志、Web 访问日志、Mail 发送日志、关键资产访问日志、用户登录日志等进行记录。

日志快速查询：可对 IP 地址、端口、时间、危急程度、日志内容关键字等进行查询。

业界领先的 IPV6，面向未来的竞争力

支持 IPv6 状态防火墙，真正意义上实现 IPv6 条件下的防火墙功能，同时完成 IPv6 的攻击防范。

支持 IPv4/IPv6 双协议栈，并支持 IPv6 数据报文转发、静态路由、动态路由及组播路由等功能。

支持 IPv6 各种过渡技术，包括 NAT-PT、IPv6 Over IPv4 GRE 隧道、手工隧道、6to4 隧道、 IPv4 兼容 IPv6 自动隧道、ISATAP 隧道、NAT444、DS-Lite 等。

支持 IPv6 ACL、Radius 等安全技术。

技术参数

硬件参数	
设备型号	NF500
处理器	64 位多核处理器
内存	2GB DDRIII
闪存	4GB EMMC
硬盘	500GB HDD
接口	10 个千兆自适应 Rj45 口，2 个千兆光电复用口，USB2.0*1 CONSOLLE*1
典型带机量	500 上网终端
尺寸	19 寸 1U（440*263*44mm）
电源电压	100-240V AC
最大功耗	≤20W

使用环境	工作温度：0℃ 到 40℃；存储温度：-40℃ 到 70℃

技术参数

硬件特性	
部署方式	单接口监听交换机镜像流量 支持透明，路由、混合（透明+路由）、多组桥、多口桥 支持旁路和串行混合部署
DHCP	DHCP 服务器 DHCP 中继代理 网络配置：网关、子网、开始结束 IP 地址 租约：无限、有限时长 高级属性：DNS 支持 2 个，Wins 支持 2 个域 支持排除地址 支持 IP-MAC 绑定 显示 IP 地址和 MAC 地址及开始时间、结束时间 清除条目 支持 VLAN 子接口，各接口对应不同 DHCP Server，DHCP Option43；
IPV4 路由	支持静态、策略、ISP、RIP、OSPF、BGP 等
NAT	支持日志发送 地址池 支持配置的增删改查、移动

	源地址转换类型：出接口、地址池、不转换 支持配置的增删改查、移动 目的地址转换类型：地址池、转换端口、不转换 支持配置的增删改查、移动 动态端口支持协议 ALG：H.323、SIP、FTP、TFTP、PPTP FTP、TFTP、SIP 支持非标准端口设置
VPN	支持 L2TP VPN、IPSec VPN、SSL VPN
负载均衡	支持基于带宽的链路负载均衡 支持基于优先级的链路负载均衡 支持基于接口的链路负载均衡 支持基于服务器的链路负载均衡
二层支持	vlan 子接口 子接口都支持 IEEE 802.1Q，能进行封装和解封。 支持对报文进行二次基于 802.1Q 封装的 VLAN-VPN 应用。（QinQ） 支持 802.1d 的 STP 生成树协议。 支持二层解封装和再封装，对上层透明
IPv6	IPv6 路由通告 IPv6 静态路由、OSPFv3 支持用户和应用均为任意的 7 元组策略 扩展报文头的逐跳报文的处理、分片报文等的处理 隧道支持：手工隧道，6to4 隧道，ISATAP Nat64 防畸形报文攻击

IPv4 安全策略	支持策略增删改查、启用/禁用、移动 支持策略匹配次数清零 支持修改默认策略动作：允许/拒绝 七元组策略匹配条件：用户、应用、源地址、源接口、目的地址、目的接口、服务 支持基于时间表的策略配置 支持应用选择过滤 支持基于应用的应用类型组选择支持策略动作为：允许、拒绝、IPSec 基于策略的长连接（老化时间） 支持动作为拒绝的策略进行日志记录
IPv6 安全策略	支持策略增删改查、启用/禁用、移动 支持策略匹配次数清零 支持修改默认策略动作：允许/拒绝 支持用户和应用均为任意的 7 元组策略 支持基于时间表的策略配置 支持策略动作为：允许、拒绝 支持动作为拒绝的策略进行日志记录
应用过滤策略	增删改查 启用禁用 描述 支持根据应用/应用类来区分不同的应用行为 支持根据应用行为来区分不同应用的审计内容 根据应用行为确定审计内容 支持基于关键字或者数字的内容审计

	支持允许/阻断的策略动作
	审计日志选项:不记录、紧急、告警、严重、错误、警示、通知，信息
应用控制及审计	审计用户名、所在组名
	审计应用名、所在应用类
	审计操作系统、平台、终端、供应商
	审计源 IP 地址、目的 IP 地址、目的端口
	基于帐号的登录控制、黑/白名单
	支持非加密收发消息时的关键字内容审计
	识别迅雷
	基于行为（登录、交易、行情）的控制和审计基于行为的控制和审计
	关键字过滤
	支持邮件内容审计，不支持附件审计。
	支持普通版 webmail 审计（QQ、163、126、新浪、139 邮箱）
	支持论坛（BBS、博客）主题过滤（如果有）
	论坛（BBS、博客、微博）内容过滤
	支持以发件人过滤
	支持邮件客户端的主题、内容、附件名过滤
	支持记录邮件内容，需要带本地硬盘
	支持基于命令和操作的审计
	论坛上传下载文件名过滤
入侵防御	支持基于源、目的、规则集的入侵检测。
	支持 5 种自定义动作
	支持软件 bypass（CPU and 内存高于 70%）

	可记录攻击日志和报警。 支持系统规则库手动、自动升级。 支持 IPS 安全报表 支持服务器异常流量学习和非法外联检测 支持自定义 IPS 规则 支持弱密码检测及防护，弱密码扫描 支持发现内网操作系统，应用，服务等 系统定义超过 4000 条规则，包含 Backdoor，bufferoverflow，dosddos，im，p2p， vulnerability，scan，webcgi，worm，game。
防病毒	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀 查杀邮件正文/附件、网页及下载文件中包含的病毒 支持 300 万余种病毒的查杀，病毒库定期与及时更新 支持启发式扫描查杀未知病毒 支持 ZIP/RAR 等压缩文件的病毒查杀 压缩：默认 5 层，最大 20 层 支持 TAR 等多种打包文件的病毒查杀
防护策略	支持 500+条预置 Web 防护规则，包括 SQL 注入，XSS，命令注入等 OWASP Top10 威胁 支持多个字段匹配访问控制，支持或与逻辑，支持匹配后不再继续安全检查 支持 7 种级别日志记录； 支持全站，指定 URL，指定文件类型的防盗链 支持配置站点白名单，允许白名单中的网站调用资源 支持 CSRF 攻击防护，支持配置防护 URL 支持全站、指定 URL 的 CC 攻击防护 支持配置检测时长，访问次数

	支持隐藏 Server 信息 支持隐藏 X-Powered-By 信息 支持替换客户端出错页面 支持替换服务端出错页面 支持配置防篡改起始 URL，支持配置例外 URL
防篡改缓存	支持缓存篡改前的页面 支持手动清理缓存
用户认证	支持短信、微信、WEB、Radius、LDAP 和无感知认证等
系统管理	支持系统时间、系统重启、部署方式、授权、配置文件、系统升级、诊断工具、抓包 工具、信息收集等功能 支持 SNMP 代理模式，兼容 v1、v2、v3。 支持流量统计图形化（以各种图像进行呈现） 支持各种日志查询和备份（事件日志、管理日志、安全日志、IPS 日志、AV 日志）

组网配置

在线部署

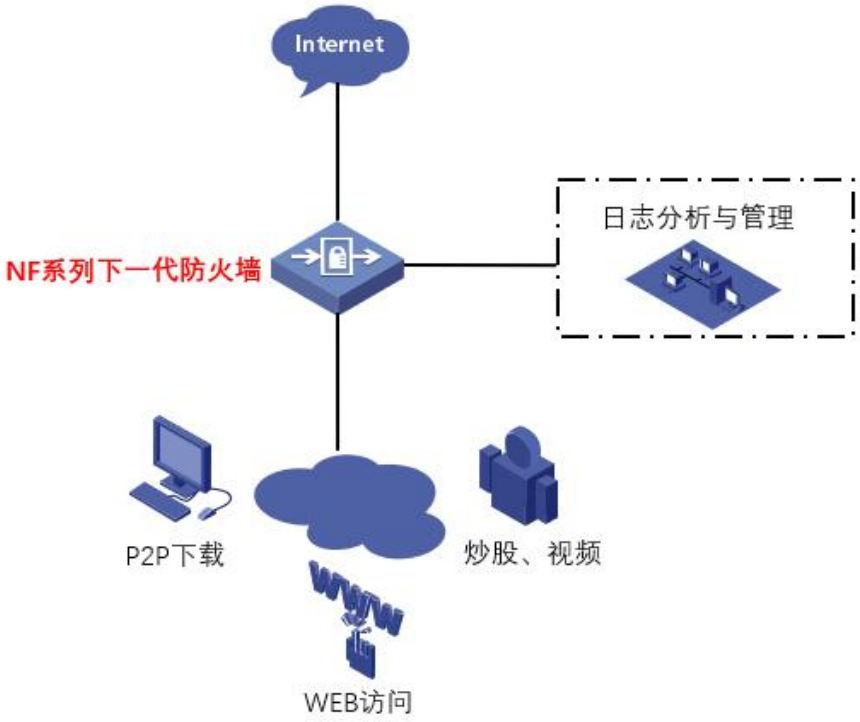
适用于大中型企业用户，以透明方式在线部署于网络出口；无需改变网络拓扑。

对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽

对用户上网行为进行分析与审计

支持 VPN/MPLS/ VLAN/PPPoE 等复杂网络环境；支持设备本地日志记录和集中分析处理，

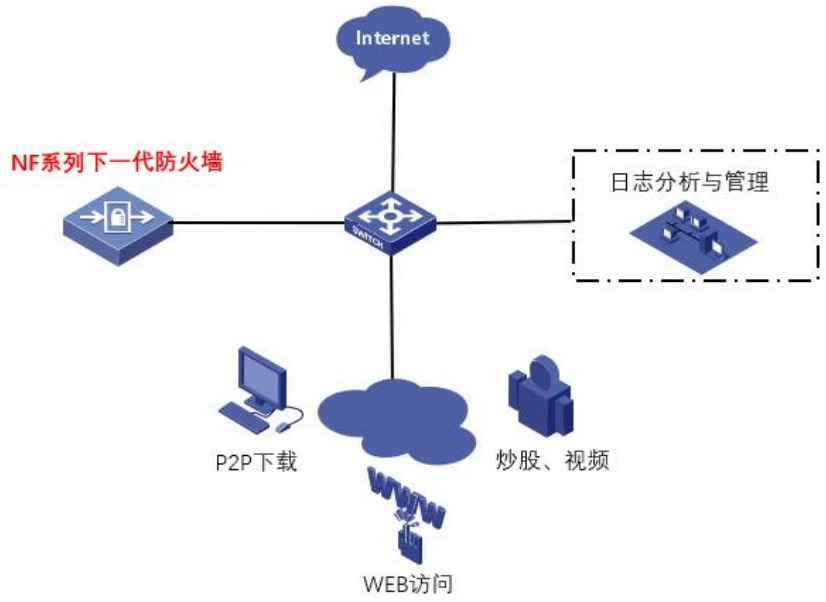
可多台分布式部署统一管理



旁挂部署

适用于大中型企业用户，以旁挂方式部署于核心设备旁；不影响网络结构，部署简单 。对用户网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等的流量、行为进行分析及审计。

支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理。



选配信息

型号	描述	备注
NF500	组合产品-volans NF500 下一代防火墙主机(10GE（电）+2Combo))-不含授权	必配
NF-AV-LIC12	License 授权函-Volans NF 系列防病毒特征库(AV)升级服务（1 年）	必配 1 年
NF-IPS-LIC12	License 授权函-Volans NF 系列防攻击特征库(IPS)升级服务 （1 年）	必配 1 年
NF-AC-LIC12	License 授权函-Volans NF 系列上网行为管理特征库(AC)升级 服务（1 年）	必配 1 年
NF-ALL-LIC12	License 授权函-Volans NF 系列三合一（含 AV/IPS/AC）特征库升级服务（1 年）	必配 1 年
NF-SSL-LICI00	License 授权函-Volans NF 系列 SSL VPN 授权服务 100 个	设备默认支持 10 授权

NF-SSL-LIC500	License 授权函-Volans NF 系列 SSL VPN 授权服务 500 个	

声明

Copyright © 2002-2023

飞鱼星科技股份有限公司

版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

飞鱼星 、 、 飞鱼星 均为飞鱼星科技股份有限公司的商标。对于本文档中出现的其他商标，由各自的所有人拥有。

*由于产品版本升级或其它原因，本文档内容会不定期进行更新，为获得最新版本的信息，请定时访问公司网站。飞鱼星科技试图在本资料中提供准确的信息，但对于可能出现的疏漏概不负责；除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。