

产品白皮书

NGFW One 企业版 产品白皮书

以「蜜罐 → 审计 → 封停」闭环为核心、AI 贯穿全程的下一代防火墙：产品架构、五大能力域、部署方式与典型场景。

目录

01	产品概述
02	产品架构
03	五大能力域
04	核心差异：蜜罐到封停闭环
05	部署方式
06	典型场景
07	版本对比
08	服务与支持

关于本白皮书

本白皮书为草案版本，描述 NGFW One 产品的设计理念与规划能力。功能清单、版本归属、型号规格、菜单名称与参数均以产品正式发布版本和产品规格书为准。

01

产品概述

NGFW One 是一款以「蜜罐 → 审计 → 封停」闭环为核心、AI 贯穿全程的下一代防火墙。企业版面向中大型企业、政企单位、教育与医疗机构，一台设备覆盖出口防护、内网安全、上网管理、远程接入与合规审计。

要解决的问题

告警太多，处置太慢

WAF、IDS、病毒防护各自报警，安全人员在多个系统之间切换比对，确认完攻击者早已换了地址。

设备多、配置难

防火墙、上网行为管理、VPN、WAF 分别采购、分别配置，真正懂全部配置的人很少。

新风险没人管

员工把数据交给大模型，AI Agent 直接操作业务系统，传统边界设备看不到也管不住。

合规压力持续

等保测评、日志留存、国密与信创要求，需要设备能力和证据同时到位。

产品家族

版本	定位	适用对象	交付方式
WAF 免费版	入门级 Web 应用防护，免费下载即用	个人站长、开发者、小微企业	Docker 部署 / 云部署
NGFW One 企业版	全能下一代防火墙，蜜罐 → 审计 → 封停闭环	中大型企业、政企单位、教育与医疗机构	硬件一体机 / Docker 部署 / 云部署
NGFW One 数据中心版	高吞吐、高可用、多租户的机房级防护	IDC、云服务商、大型集团总部	硬件一体机 / 云部署

三个版本共享同一套检测引擎与管理体验，可以从 WAF 免费版起步，随业务增长平滑升级。

企业版核心价值

- 蜜罐 → 审计 → 封停闭环：诱捕节点提前暴露攻击者，审计关联全量日志，高置信威胁秒级自动封停，误封可一键回滚。
- 完整 WAF + AI 语义检测：在规则引擎之上叠加 AI 语义分析，识别变形与未知攻击，并自动调优规则减少误报。
- 网关病毒防护：在 HTTP、SMTP、FTP、SMB 等协议上拦截恶意文件与勒索软件。
- IDS 入侵防护：识别扫描、漏洞利用与 C2 通信，告警直接联动封停。

- **网内设备与流量管理：**自动发现内网资产，识别应用流量，按业务优先级分配带宽。
- **AI 助手：**用自然语言查日志、生成策略、接收周报；内置 MCP，让外部 AI Agent 安全地调用防火墙能力。
- **AI 应用与 Agent 安全：**管控员工使用大模型时的敏感数据外发，审计内部 AI Agent 的每一次工具调用。
- **零信任与 SD-WAN：**按身份和设备授权访问内网应用，分支机构零配置上线、智能选路。
- **国密 · 信创 · 等保：**国密 VPN、信创适配型号与等保合规中心，满足政企采购与测评要求。

02

产品架构

NGFW One 采用分层架构：网络与接入层负责把流量接进来、送出去；安全检测与处置层在同一引擎内完成多种检测，并把结果汇入统一的审计与封停闭环；管理与开放层提供图形界面、AI 助手和完整的开放接口。



图 1 NGFW One 产品架构：三种交付形态承载同一套引擎，五大能力域共享策略、日志与闭环

设计原则

- **一套引擎，多种形态。**硬件、Docker 与云部署运行相同的软件，策略与配置可以互相迁移。
- **检测结果统一入闭环。**所有检测模块的告警进入审计中心，按置信度决定自动处置还是人工确认。
- **AI 只给草稿，人做决定。**AI 生成的策略和处置以草稿形式呈现，写操作默认需管理员确认，全部记入审计。
- **一切可编程。**策略、名单、日志、报表都可以通过 REST API 与 MCP 访问，方便接入 SOC、SIEM 与自动化平台。

03

五大能力域

NGFW One 的 28 项能力按五大能力域组织。下表列出每项能力的定位与版本归属（✓ 表示包含）。

闭环与核心防护

蜜罐 → 审计 → 封停闭环，WAF、病毒防护、IDS 与设备、流量、域名管控。

能力	说明	免费版	企业版	数据中心版
蜜罐到封停闭环	诱捕、审计、封停自动串联，攻击还没得手就被挡住	—	✓	✓
WAF 应用防护	拦截注入、XSS、爬虫与 CC 攻击	✓	✓	✓
病毒防护	网关层拦截恶意文件与勒索软件	—	✓	✓
IDS 入侵防护	识别扫描、漏洞利用与 C2 通信	—	✓	✓
网内设备管理	自动发现内网资产，异常设备及时告警	—	✓	✓
流量管理	应用识别、QoS 与多线路，关键业务不卡顿	✓	✓	✓
域名黑白名单	封堵恶意、违规与分心类网站	✓	✓	✓

AI 安全

AI 助手与开放接口之外，管住大模型和 AI Agent 带来的新风险。

能力	说明	免费版	企业版	数据中心版
AI 助手	用一句话查日志、写策略、看周报	—	✓	✓
AI 应用防火墙	管住员工使用大模型时的数据外泄，防护自建 AI 应用	—	✓	✓
Agent 与 MCP 安全网关	审计并管控 AI Agent 调用了哪些工具、动了哪些数据	—	✓	✓
AI 自动研判与处置	告警自动调查、给出结论与证据，按剧本一键处置	—	✓	✓
API 与 MCP	REST API、Webhook 与 MCP，让 AI Agent 安全地调用防火墙	✓	✓	✓

威胁防护进阶

上网行为、加密流量、DNS、数据防泄漏、威胁情报、API 与暴露面。

能力	说明	免费版	企业版	数据中心版
上网行为管理	应用管控、上网审计与实名认证，上网行为可管可查	—	✓	✓
加密流量检测	SSL 解密检测与免解密识别，不让威胁藏在 HTTPS 里	—	✓	✓
DNS 安全	识别 DNS 隧道、DGA 域名与解析劫持，定位失陷主机	—	✓	✓
数据防泄漏	识别网页、邮件、网盘与 AI 应用中的敏感数据外发	—	✓	✓
威胁情报联动	情报订阅与 IOC 自动下发，已知攻击者直接拒之门外	—	✓	✓
API 与 Bot 防护	API 资产发现、越权检测、恶意 Bot 识别与业务防刷	✓	✓	✓
暴露面与弱口令检测	从攻击者视角盘点暴露端口、高危漏洞与弱口令	—	✓	✓

网络与接入

基础网络、零信任、SD-WAN、SASE 与数据中心微隔离。

能力	说明	免费版	企业版	数据中心版
基础网络功能	ACL、NAT、路由、VPN、认证、高可用	✓	✓	✓
零信任访问（ZTNA）	按身份和设备授权到应用，替代或补充传统 VPN	—	✓	✓
SD-WAN 多分支组网	分支零配置上线、智能选路，总部集中管理	—	✓	✓
SASE 云端安全接入	安全能力云端交付，人在哪里，防护就在哪里	—	✓	✓
微隔离	东西向流量可视化与最小权限隔离，阻断横向移动	—	—	✓

国产化与合规

国密 VPN、信创适配、等保合规中心与攻防演练模式。

能力	说明	免费版	企业版	数据中心版
国密 VPN	支持 SM2 / SM3 / SM4 的 IPSec 与 SSL VPN	—	✓	✓
信创适配	适配国产 CPU 与操作系统，提供信创硬件型号	—	✓	✓
等保合规中心	配置基线检查、日志留存保障与一键迎检报表	—	✓	✓
攻防演练模式	演练期一键加固、蜜罐溯源，自动生成防守报告	—	✓	✓

04

核心差异：蜜罐到封停闭环

单点防护只能告诉你「出事了」。NGFW One 把诱捕、确认和处置自动串联，让攻击者在接触真实资产之前就暴露并被挡住。

01 诱捕
让攻击者先暴露

在内网与 DMZ 布置 SSH、RDP、数据库、Web 后台等诱饵。正常用户不会访问，任何触碰都是高置信信号。

02 审计
确认是真的威胁

蜜罐、WAF、IDS、病毒、登录失败等事件按 IP、设备、时间窗口关联打分，AI 降噪并还原攻击链。

03 封停
秒级处置，可回滚

高置信威胁自动封停 IP、域名、账号或设备；低置信进入审批；误封一键回滚，全程留痕。

闭环的设计原理、审计规则示例与上线最佳实践，见《蜜罐 → 审计 → 封停闭环技术白皮书》。

05

部署方式

交付形态

形态	说明	适用版本
硬件一体机	专用硬件，开箱上架，适合总部与数据中心对吞吐、稳定性要求高的场景。	NGFW One 企业版、NGFW One 数据中心版
Docker 部署	一行命令跑在任意 Linux 服务器上，适合开发者、中小企业和测试环境。	WAF 免费版、NGFW One 企业版
云部署	云市场镜像或 SaaS 方式开通，保护部署在公有云、私有云上的业务。	WAF 免费版、NGFW One 企业版、NGFW One 数据中心版

网络接入模式

模式	说明	适合场景
路由（网关）模式	作为出口网关，承担 NAT、路由、DHCP 与 VPN，所有安全能力可用。	新建网络或替换旧防火墙
透明（网桥）模式	串接在现有网关之后，不改变 IP 规划即可启用检测与阻断。	不便改动网络的存量环境
旁路模式	通过流量镜像只做检测与审计，对业务零影响。	试运行、评估或纯审计需求

高可用

- 企业版支持双机热备，配置自动同步，故障时自动切换。
- 数据中心版支持多节点集群，按业务增长横向扩展，封停策略全集群同步。

硬件型号

型号	定位	适用规模	威胁防护吞吐
N1-E1100	入门型	300 人以内的分支与中小总部	1.5 Gbps
N1-E2100	标准型	1000 人以内的企业总部	3 Gbps
N1-E3100	高性能型，双电源	3000 人以内的总部与多业务出口	6 Gbps
N1-E5100	园区型，2U 可扩展	大型园区与集团出口	12 Gbps

型号与性能为规划目标，以硬件选型实测和产品规格书为准；另有信创型号（后缀 -X）与虚拟化规格。

06

典型场景

中小企业

面向没有专职安全团队的中小企业：一台设备统一承担出口网关、网站防护、上网管理与远程接入，借助 AI 助手用自然语言完成日常运维，可从免费版起步。

- **一体化出口网关：**在出口处统一提供 ACL、NAT、路由、DHCP 和 VPN，替代多台独立设备，策略在一个界面中完成。
- **为对外业务加上 WAF：**为官网和业务系统开启 Web 防护，拦截常见注入、跨站脚本和恶意扫描；部署在云上的网站可直接使用 WAF 免费版。
- **域名黑白名单过滤：**拦截恶意软件、钓鱼和挖矿相关域名，也可按需限制与工作无关的网站，减少终端被感染的入口。

教育

面向高校与中小学的出口安全方案：统一上网认证实现实名可追溯，按区域与时段管理宿舍流量，通过域名过滤管控不良内容，同时摸清校园网内各类设备资产。

- **统一上网认证：**通过 Web 认证对用户实名上网，可对接学校现有统一身份认证（对接方式以产品规格书为准），上网记录与账号关联。
- **分区分时流量管理：**按宿舍、教学、办公区域以及时段设置带宽策略，对下载、视频等应用限速，保障教学科研和关键业务。
- **域名黑白名单过滤：**拦截不良、恶意和钓鱼网站；中小学可采用更严格的白名单策略，仅允许访问教学相关网站。

医疗

面向各级医院的安全方案：对 HIS、PACS 等核心系统分区隔离，摸清并管控医疗设备资产，结合防病毒、入侵检测与蜜罐闭环，在勒索软件扩散前发现并阻断。

- **核心业务分区隔离：**将 HIS、PACS 等服务器区与办公区、设备区划分为独立安全区域，通过 ACL 仅放行业务必需的访问。
- **医疗设备资产管理：**通过网内设备管理识别接入的医疗设备，建立资产清单，对无法加固的设备限定其只能访问对应的业务服务器。
- **勒索软件多层检测：**在区域边界开启防病毒和入侵检测，识别恶意文件传输和漏洞利用、内网扫描等勒索传播行为。

政务

面向各级政务单位的安全方案：围绕等保 2.0 落实边界防护、入侵防范与安全审计，满足日志留存与三权分立要求，保护对外政务服务，并支持国产化环境部署评估。

- **对照等保要求部署：**在区域边界部署访问控制、入侵检测与防病毒，覆盖等保 2.0 中边界防护、访问控制、入侵防范和恶意代码防范等控制点。
- **完整审计与留存：**管理操作、安全事件以及 API 调用均写入审计日志，可外发至统一日志审计平台集中留存与分析。
- **防护对外政务服务：**为政务门户和在线办事系统启用 WAF，防御注入、篡改与恶意扫描；高危来源可通过闭环流程封停。

IDC 与云服务商

面向 IDC、云服务商与集团数据中心：以高性能硬件或云上集群承载大流量，提供租户间隔离的安全策略，并通过 REST API 与 MCP 实现自动化开通与运维。

- **高性能与集群部署：**采用数据中心版高性能硬件或云上集群部署，按业务增长横向扩展，避免安全能力成为瓶颈。
- **多租户策略隔离：**为不同租户划分独立的策略空间与日志视图，租户之间相互隔离，平台侧统一运维。
- **API 驱动自动化：**通过 REST API 与云管平台、工单系统对接，租户开通、策略变更与下线全部自动完成，API 调用统一纳入审计。

07

版本对比

功能	WAF 免费版	NGFW One 企业版	NGFW One 数据中心版
闭环与核心防护			
WAF Web 应用防护	基础规则	完整规则 + AI 语义检测	完整规则 + 集群负载均衡
蜜罐诱捕	—	✓	多租户蜜罐
安全审计与日志	7 天	180 天，合规报表	自定义，对接 SIEM
自动封停	手动	AI 自动封停 + 审批流	自动 + 跨节点联动
病毒防护	—	✓	✓
IDS 入侵防护	—	✓	高性能引擎
网内设备管理	—	✓	✓
流量管理	基础限速	应用识别 + QoS	大带宽 + 多线路
域名黑白名单	✓	+ AI 威胁情报	+ 全局同步
AI 安全			
AI 助手	—	✓	✓
AI 应用防火墙（大模型使用管控与脱敏）	—	✓	+ 多租户策略
Agent 与 MCP 安全网关	—	✓	✓
AI 自动研判与处置	—	研判 + 内置剧本	+ 自定义剧本编排
威胁防护进阶			
上网行为管理	—	✓	✓
加密流量检测	—	SSL 解密检测	+ 免解密 AI 识别
DNS 安全（隧道 / DGA）	—	✓	✓
数据防泄漏（DLP）	—	✓	✓
威胁情报联动	—	内置情报 + 第三方接入	+ 集群 / 租户间共享
API 与 Bot 防护	CC 防护	API 发现 + Bot 管理	+ 集群级防刷

功能	WAF 免费版	NGFW One 企业版	NGFW One 数据中心版
暴露面与弱口令检测	—	✓	✓
网络与接入			
基础网络（ACL / NAT / 路由 / VPN / DHCP）	基础	完整	完整 + 多 WAN
高可用	—	双机热备	集群
零信任访问（ZTNA）	—	✓	+ 大规模并发
SD-WAN 多分支组网	—	✓	+ 大规模分支
SASE 云端安全接入	—	云端接入	+ 自建 SASE 节点
微隔离	—	—	✓
多租户	—	—	✓
国产化与合规			
国密 VPN（SM2 / SM3 / SM4）	—	✓	✓
信创适配型号	—	✓	✓
等保合规中心	—	✓	+ 多租户合规报表
攻防演练模式	—	✓	+ 多节点协同值守
开放接口			
REST API 与 API 管理	只读接口	完整接口 + Key 管理	完整 + 多租户隔离
Webhook 事件推送	—	✓	✓
MCP Server / Client	—	✓	✓
交付与服务			
交付方式	Docker / 云	硬件 / Docker / 云	硬件 / 云（集群）
技术支持	社区	5×8 专属	7×24 专属
价格	免费	联系销售	联系销售

表中功能与版本归属为规划口径，以正式发布版本为准。

08

服务与支持

版本	技术支持	获取方式
WAF 免费版	社区支持与文档中心	官网免费下载
NGFW One 企业版	5×8 专属技术支持	联系销售获取报价，可申请演示与试用
NGFW One 数据中心版	7×24 专属支持与重大事件应急响应	联系销售，可申请 POC 测试

下一步

- 文档中心：ngfw.cn/docs/，包含快速开始、安装部署、配置手册、REST API 与 MCP 接入指南。
- 申请演示：ngfw.cn/demo/，用真实攻击场景演示从诱捕到封停的全过程。
- 版本对比：ngfw.cn/products/compare/