

技术白皮书

蜜罐 → 审计 → 封停 闭环技术白皮书

诱捕、关联分析与自动处置的设计原理与最佳实践：让攻击者在接触真实资产之前暴露并被挡住。

目录

- 01 摘要
- 02 单点防护的困境
- 03 闭环架构
- 04 蜜罐诱捕：让攻击者先暴露
- 05 审计关联：确认是真的威胁
- 06 自动封停：秒级处置，可控可回滚
- 07 上线最佳实践
- 08 衡量闭环效果

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

摘要

防守方最缺的不是告警，而是时间。NGFW One 把蜜罐诱捕、安全审计和自动封停串成一条闭环：蜜罐让攻击者在接触真实资产之前暴露，审计把多源信号关联成可信的事件，封停按置信度自动或经审批执行，并支持一键回滚。

看得更早

正常用户不会访问诱饵，任何触碰都是高置信攻击信号，内网横向移动在早期即可发现。

判得更准

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。

处置更快

从发现到封停自动完成，不依赖人工值守；误封可一键回滚，所有动作留痕可审计。

本白皮书介绍闭环的设计原理、各环节的关键机制、审计规则示例与上线步骤，供安全负责人与运维工程师参考。闭环能力适用于 NGFW One 企业版与数据中心版。

02

单点防护的困境

多数单位已经部署了防火墙、WAF、IDS 和终端防护，但安全事件仍然频繁发生。问题通常不在于检测能力不足，而在于检测、确认与处置之间的断层。

环节	常见状况	后果
检测	各设备独立告警，每天成百上千条，其中大量是扫描噪声与误报	真实攻击被淹没，值守人员疲于应付
确认	需要在多个系统间切换、手工比对 IP 与时间，查一条告警要十几分钟	确认完成时攻击者已更换地址或进入下一阶段
处置	手动登录防火墙添加封禁，夜间和节假日无人值守	响应时间以小时计，处置不留痕，误封难追溯
内网	边界设备只看南北向流量，内网横向移动缺少检测手段	攻击者潜伏期长，往往在数据泄露后才被发现

闭环要解决的，就是把这三个环节自动串联：用高置信的信号源减少噪声，用关联分析替代人工比对，用分级自动化替代人工值守。

03

闭环架构

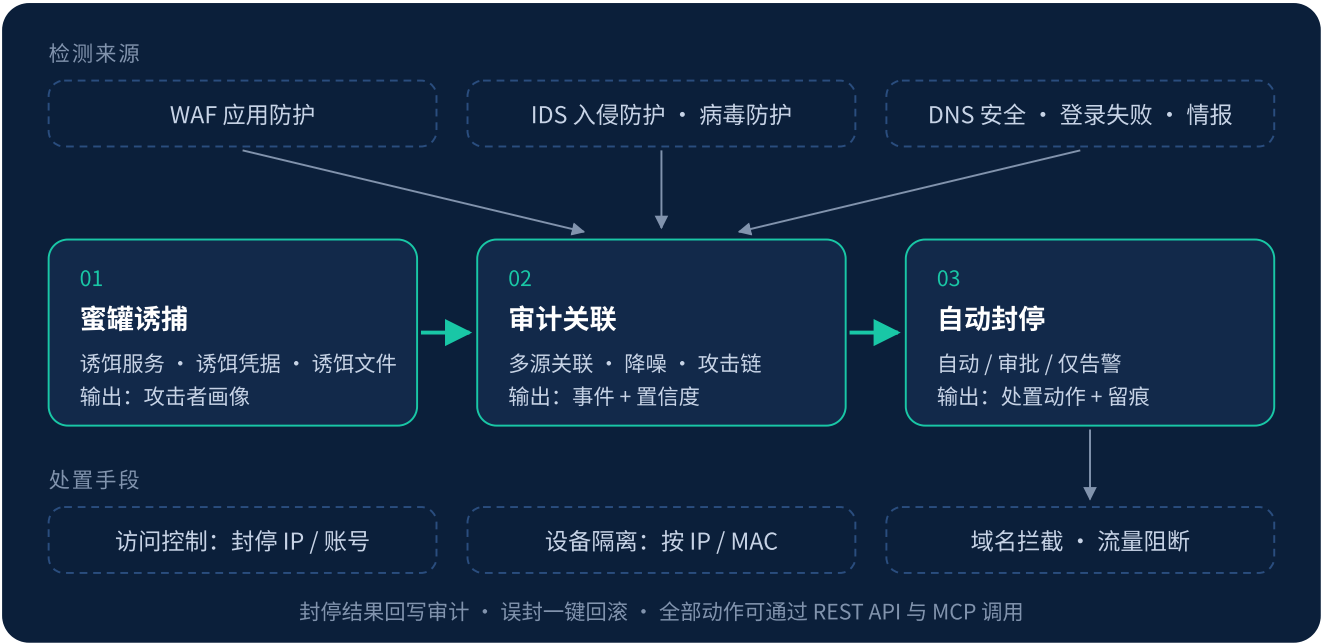


图 1 闭环全景：多源检测汇入审计，按置信度决定处置方式，结果回写审计形成闭环

闭环由三个阶段和两类外围组成：

- **检测来源：**WAF、IDS、病毒防护、DNS 安全、登录失败与威胁情报等模块持续产生信号，与蜜罐信号一起进入审计中心。
- **三个阶段：**诱捕产生高置信信号与攻击者画像；审计把信号关联成事件并给出置信度；封停按规则决定自动执行、提交审批或仅告警。
- **处置手段：**封停对象可以是外部 IP、域名、账号或内网设备，执行手段包括访问控制、设备隔离、域名拦截与流量阻断。
- **回写与开放：**处置结果回写审计，形成证据链；封停、解封、名单管理均可通过 REST API 与 MCP 调用，并通过 Webhook 推送 `block.created` 等事件。

04

蜜罐诱捕：让攻击者先暴露

蜜罐是闭环中信噪比最高的信号源。它们不承载任何真实业务，正常用户没有理由访问，因此一次交互几乎可以直接判定为攻击或违规探测。

诱饵类型

类型	形式	主要发现
诱饵服务	SSH、RDP、数据库、Redis、Web 管理后台、文件共享等	端口扫描、暴力破解、漏洞利用尝试
诱饵凭据	放在真实主机上的假账号、假配置文件、假连接串	攻击者在已控主机上的信息收集与横向移动
诱饵文件	看起来有价值的文档或数据文件	数据窃取与内部人员越权访问

可用诱饵类型以产品实际版本为准。

部署原则

- **像真的一样。**使用各业务网段中未被使用的地址，服务指纹与该网段的普通主机一致。
- **每个重要网段至少一个。**办公网、服务器区、DMZ、运维网段分别部署，覆盖横向移动的必经之路。
- **与生产隔离。**攻击者在蜜罐中的操作不会影响真实系统，交互内容完整记录用于溯源。
- **定期轮换。**调整诱饵地址与内容，避免被长期潜伏的攻击者识别。

攻击者画像

每次蜜罐交互都会记录来源、时间、使用的工具与手法，并与其他模块的事件关联，形成攻击者画像。画像在审计阶段作为高权重证据，也用于攻防演练后的溯源报告。

05

审计关联：确认是真的威胁

审计中心汇聚所有检测来源的事件、访问日志与配置变更记录。关联分析把分散的信号归并为少数几个可信的事件，并给出置信度。

审计规则的构成

每条审计规则由**事件源**、**条件**、**时间窗口**、**处置动作**四部分组成。下表为配置示例，阈值需结合自身业务基线调整：

规则	条件	建议动作
蜜罐即封	外部来源与任意蜜罐交互 1 次	自动封停
WAF 高危累计	同一 IP 10 分钟内触发高危 WAF 规则 ≥ 5 次	自动封停
暴力破解	同一 IP 对 VPN 或后台登录失败 ≥ 10 次	自动封停
内网横向探测	内网主机 5 分钟内扫描 ≥ 20 个地址或端口	提交审批
失陷主机外联	内网主机反复解析恶意域名或命中 C2 特征	提交审批（隔离设备）

降噪与攻击链还原

- **聚合：**同源、同类型、同目标的告警归并为一个事件，识别扫描器噪声与已知误报。
- **关联：**按 IP、设备、账号与时间窗口串联不同模块的事件，例如「蜜罐交互 → WAF 注入尝试 → VPN 暴力破解」。
- **攻击链：**把事件按时间排列成攻击路径，标出从哪来、做了什么、影响到谁。
- **可解释：**每个事件附带判定依据与原始日志链接，便于人工复核。

AI 在审计阶段的作用

AI 对告警聚类降噪、给出置信度与处置建议，并用自然语言解释判定理由。是否自动执行，始终由审计规则的配置决定，AI 不会绕过规则直接处置。

06

自动封停：秒级处置，可控可回滚

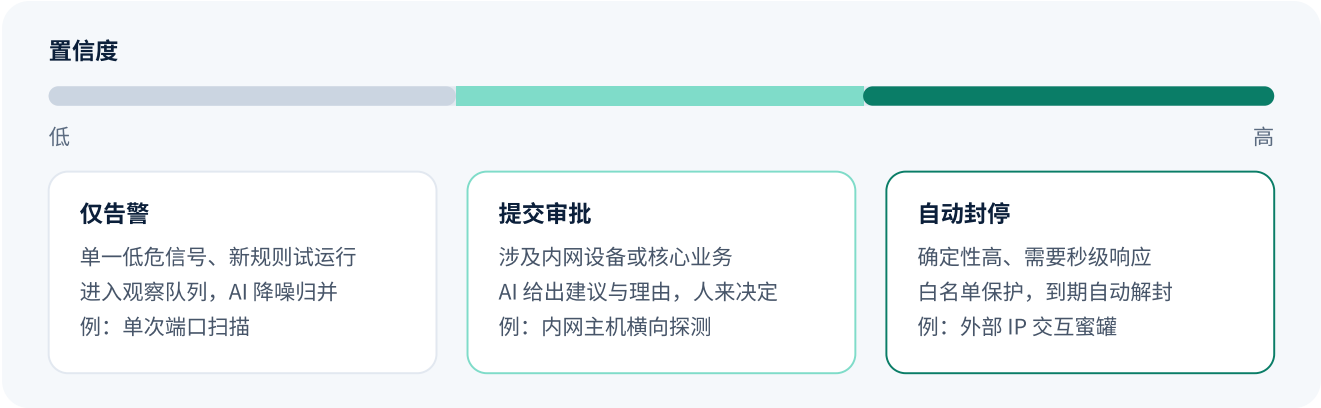


图 2 按置信度分级处置：越确定的威胁越自动化，越接近核心业务越需要人工确认

执行方式

- **自动执行：**适合蜜罐命中、明确的暴力破解等确定性高的规则，秒级生效。
- **审批后执行：**动作进入待审批队列，指定审批人确认后生效，适合涉及内网设备或核心业务的规则。
- **仅告警：**新规则试运行或低置信场景，只记录不处置。

安全护栏

护栏	作用
保护白名单	出口网关、DNS、监控系统、运维堡垒机、合作方接口等地址任何规则都不会封停，包括通过 API 与 MCP 发起的封停
封停时长	可设为 1 小时、24 小时等固定时长或永久；到期自动解封并推送 block.released 事件
一键回滚	误封可立即解封并加入白名单；规则阈值有误时可按规则批量解封
全程留痕	每次封停、解封、审批都记录操作人或触发来源（规则、API、MCP）与证据链
集群联动	数据中心版中，任一节点的封停在全集群同步生效

07

上线最佳实践

闭环涉及自动处置，建议分阶段上线，先建立信任，再逐步放开自动化。

阶段	时间	工作内容	完成标志
1 准备	第 1 周	梳理关键资产与网段；配置封停保护白名单；在每个重要网段部署至少一个蜜罐	白名单经运维确认；蜜罐可被内部测试触发
2 观察	第 2-3 周	启用审计规则但全部设为「仅告警」；每天复核事件与误报	误报率可接受，阈值完成第一次调整
3 半自动	第 4-5 周	蜜罐即封等确定性规则改为自动；其余规则改为审批后执行	自动封停无误封；审批平均响应时间可接受
4 常态化	第 6 周起	按季度复盘规则与阈值；定期轮换蜜罐；接入 Webhook / 工单 / IM	形成月度闭环运行报告

常见问题

- **担心误封业务？** 先跑观察期，并把关键地址加入保护白名单；所有自动封停都可一键回滚。
- **蜜罐会不会被内部员工误触？** 使用未分配地址、不对外宣传，必要时把资产扫描器等内部工具加入例外。
- **和现有 SOC / SIEM 怎么配合？** 审计结果通过 Syslog、Webhook 与 REST API 外发，处置动作也可以由 SOAR 通过 API 或 MCP 触发。

08

衡量闭环效果

建议用以下指标衡量闭环的运行效果，并在月度报告中跟踪变化。系统报表与 AI 周报可直接提供其中大部分数据。

指标	含义	期望趋势
平均发现时间（MTTD）	从攻击行为发生到产生可信事件的时间	持续下降
平均处置时间（MTTR）	从可信事件产生到封停生效的时间	自动规则达到秒级
告警归并率	原始告警数 ÷ 归并后事件数	上升，人工需处理的事件减少
误封率	被回滚的封停数 ÷ 封停总数	保持在低位并持续下降
蜜罐覆盖率	部署了蜜罐的重要网段 ÷ 重要网段总数	达到 100%
自动化比例	自动执行的处置 ÷ 全部处置	在误封率可控的前提下逐步提高

了解更多

配置步骤见文档中心《蜜罐、审计与自动封停》：ngfw.cn/docs/config-honeypot-audit-block/。也可以预约演示，用真实攻击场景观看从诱捕到封停的全过程：ngfw.cn/demo/。