诺基亚 Deepfield Defender 以突破性缓解技术阻断实时 DDoS 攻击

在最近的现场演示中，NL-ix 网络架构师及其团队展示了一套令人印象深刻的分布式拒绝服务（DDoS）缓解方案（他们称之为反 DDoS），该方案基于先进的诺基亚 FP5 网络处理器和 Deepfield Defender 软件。这场现场演示在欧洲最大分布式交换中心 NL-ix 的现网络环境中进行。

挑战：实时抵御 DDoS 攻击

DDoS 攻击通过恶意流量淹没网络，导致基础设施超负荷运转并引发服务中断。成功缓解的关键在于精准快速地区分合法流量与攻击数据包，同时确保正常业务不受影响。NL-ix 网络架构师进一步解释道："必须允许合法流量通过，同时阻断淹没链路的有害流量，这需要由强大处理器支持的精细过滤能力，该处理器需能处理数十万条访问控制列表条目。"

诺基亚 DDoS 解决方案：FP5 芯片与 Deepfield Defender

NL-ix 最初在全网部署基于诺基亚 FP5 的路由器，以提升速度、可扩展性和性能。如今，该公司进一步将诺基亚路由技术应用于网络安全领域。诺基亚 FP5 芯片通过硬件级访问控制列表(ACL)条目高效阻断流量，实现 IP 过滤；而 Deepfield Defender 的人工智能与机器学习算法能快速精准识别 DDoS 攻击模式，并动态协调缓解措施 - 通过管理需应用的 IP 过滤器实现。这种方案将原本耗时耗力的手动检测与恶意流量重定向任务转换为自动化处理，避免了人工操作的高成本、低效率及服务中断问题。

演示过程

团队对对现网的测试网络“Decco”发起真实 DDoS 攻击，该网络日常承载约 1Gbps 合法 VPN 流量。攻击通过随机化每个数据包字段模拟复杂 DDoS 流量。

数秒之内：

- Deepfield Defender 迅速检测异常，在入口端口实时部署 283 个过滤器（ACL 条目）。
- 恶意数据包在抵达客户前即被丢弃。
- 合法流量持续畅通无阻。
- 硬件加速确保零额外延迟与零数据包回流。
- 流量恢复正常后动态移除 IP 过滤器。

方案的核心优势和亮点

- **内嵌防护**：不同于依赖流量转发或清洗中心的传统方案，本方案可无缝集成现有基础设施。
- **海量规模**：支持高达 800Gbps 客户端口，当前总交换连接容量达 50Tbps。
- **全自动化**：采用智能数据库与自动化逻辑，无需人工调试。
- **经实战验证的韧性**：在现网运行近三年，并通过红队演练验证，包括在政府批准的“攻击许可”下对关键基础设施目标进行的受控测试。

现网演示环境：部署与运营

后台基础设施部署简便。两台本地 Deepfield 服务器承载 Deepfield Defender 软件，该平台通过分析网络遥测数据（包括 IP 流量镜像数据包采样，采样率为万分之一）实现防护。Defender 每小时从 Deepfield Secure Genome®（实时“互联网安全地图”）获取最新情报，持续应对新型僵尸网络与攻击变种。现有的诺基亚 FP5 系列 IP 路由基础设施则提供网络层防护。

本次试点演示标志着面向现网环境的二层 DDoS 缓解技术取得重大里程碑。

结语

诺基亚 Deepfield Defender 与 FP5 系列 IP 路由器的协同部署，生动展现了智能软件与专用硬件如何加速实时大规模 DDoS 缓解。这一强力组合赋能运营商和网络交换中心主动保护客户，在最小化运维开销的同时保障网络性能无缝运行。