防御 DDoS“海啸”与“食人鱼”：为什么现代 DDoS 防护需要两种不同的智能

DDoS 攻击，已经不再只是“大洪流”

长期以来，行业通常用“老鼠与大象”来形容不同规模的 DDoS 攻击。但诺基亚认为，这种比喻已经无法准确描述当前 DDoS 威胁的真实形态。更贴切的描述应该是：海啸（Tsunamis）和食人鱼（Piranhas） 两者都会造成巨大破坏，但攻击模式、防御方式以及所需的安全智能能力完全不同。

“海啸型”DDoS：超大流量、瞬时冲击

“海啸型”DDoS 攻击具有几个典型特征：突发性，超大流量，极高可见性，短时间内造成大规模破坏

2025 年 10 月 9 日，诺基亚 Deepfield 应急响应团队监测到一次针对游戏平台的 33 Tbps DDoS 攻击。诺基亚《Threat Intelligence Report 2025》指出：5–10 Tbps 峰值攻击已经成为“日常现象”；Tbps 级 DDoS 攻击发生频率相比上一年增长约 5 倍。

为了说明 33 Tbps 的规模，诺基亚将其与全球主要互联网交换中心（IXP）的峰值流量进行了对比：

互联网交换平台	**峰值流量（Tbps）**
IX.br aggregate (Brazil, 38 locations)	50
IX.br São Paulo (world's largest IXP by participants)	32

互联网交换平台	峰值流量（Tbps）
DE-CIX global platform (60 exchanges)	27.71
AMS-IX Amsterdam	~15
NL-ix	12.27
LINX global platform	12.07

也就是说，单次 DDoS 攻击流量已经超过多个全球大型 IXP 平台的峰值流量。

“食人鱼型”DDoS：小流量、高并发、持续演化

相比“海啸型”攻击，更危险的其实是“食人鱼型”DDoS。单个攻击流量并不大，但：数量极多，同时发生，高度协同，持续变化，更难检测 诺基亚研究发现：78%的 DDoS 攻击在 5 分钟内结束；37%的攻击持续时间不到 2 分钟 ； 82%的攻击流量低于 50 Gbps 。

单独来看，这些攻击不会触发传统防护阈值。但当成千上万个“小攻击”同时作用于不同目标时，就会形成巨大的整体破坏力。这也是“食人鱼”比喻的核心：单独一条食人鱼不可怕，可怕的是整个鱼群。

为什么现代 DDoS 更难防?

1. 住宅代理网络（Residential Proxy）正在改变攻击源

诺基亚发现：全球已有超过 1 亿个住宅宽带终端可能被住宅代理网络或 Mirai 变种僵尸网络利用。在巴西、中国等热点区域：约 10%的 DDoS 流量来自住宅代理网络。这意味着：攻击流量来自真实家庭宽带 IP，而不是传统伪造源地址。因此：无法简单封禁；Geo-IP 限制效果下降；黑名单机制失效；合法流量与攻击流量边界变得模糊。

2. 僵尸网络生态已经模块化

诺基亚 Deepfield ERT 在 2026 年 4 月发布研究指出：Aisuru、Jackskid、Kimwolf、MossadProxy 与 Cecilio 等多个僵尸网络之间已经形成工具链共享与协同机制。 特点包括：不同 Botnet 攻击不同设备类型，攻击能力可组合，单个 Botnet 被清除后，其它网络仍可继续运行。这意味着：DDoS 攻击能力已经形成“弹性供应链”。

3. 攻击影响已经扩散到网络基础设施层

现代 DDoS 攻击的影响范围，已经不仅仅局限于目标服务器。越来越多攻击开始影响：Peering Fabric，IXP 交换平台，云边缘节点，Backbone 基础网络。即使目标业务没有完全中断：网络队列可能崩溃，自动化防护可能误触发，邻近用户业务可能受到牵连。诺基亚将这种模式称为：“Sub-saturating Swarms”（低于饱和阈值的群体攻击）。

为什么传统 DDoS 防护正在失效?

传统 DDoS 防护通常依赖：固定阈值，静态特征，DPI 深度报文检测，人工响应流程。但这

些机制已经难以应对现代攻击。

原因包括：

- **阈值检测失效：**单个目标流量可能低于检测阈值，但整体攻击已经造成破坏。
- **攻击面横向扩展：**攻击对象已经从单一服务器扩展到：Web，DNS，API，VPN，接入网络。
- **攻击持续变形：**攻击过程中：协议不断切换，IP 地址持续轮换，攻击向量实时变化。

静态规则往往几分钟内就失效。

现代 DDoS 防护需要“两种智能”

现代 DDoS 防护必须同时具备：应对“海啸型”攻击的能力和应对“食人鱼型”攻击的能力，而且两者需要完全不同的防御体系。

如何防御“海啸型”DDoS?

针对超大流量攻击，需要：

- **分布式超大规模清洗能力。**防护能力必须嵌入网络本身，而不是依赖单一 Scrubbing Center。因为：当攻击只有几十秒时，传统 BGP 流量牵引可能还没完成，攻击已经结束。
- **亚秒级检测能力：**需要对以下攻击进行快速识别：Reflection/Amplification 攻击，UDP Flood ,超大规模 HTTP Flood
- **硬件级自动化阻断：**现代 DDoS 攻击速度已经超出人工响应能力。

因此：防护决策必须在线速（Line Rate）条件下由硬件自动完成。

如何防御“食人鱼型”DDoS?

相比容量问题，“食人鱼型”DDoS 本质上更像是一个“智能识别问题”。

需要具备：

- **全网级实时可视化能力：**需要跨以下维度进行关联分析：IP，Prefix，ASN，时间维度。因为攻击影响来自整体聚合行为，而不是单一流量。
- **AI 驱动基线学习能力：**系统必须持续学习：什么是正常流量”。这样才能识别隐藏在海量合法流量中的小规模协同攻击。
- **自适应防护能力：**系统需要识别：持续变形的攻击活动，攻击向量切换，行为模式变化。而不是把每次变化都当作新攻击。
- **实时威胁情报能力，**包括：恶意 IP 源，被攻陷设备类型，住宅代理行为模式，Botnet 关联关系

从而识别“单独正常、整体异常”的攻击流量。

诺基亚的核心观点

诺基亚认为：未来网络运营商真正需要回答的问题，不是：“我们能否防住下一次 50 Tbps 攻击？”而是：“我们能否同时防住 50 Tbps 攻击，以及一万个同时发生的 50 Gbps 以下攻

击？”

这两类问题：不是同一种攻击，不需要同一种防护体系，更不可能用同一种智能能力解决。

现代 DDoS 攻击已经进入：AI 驱动、自动化、高并发、多向量、高动态演化的新阶段。传统依赖：固定阈值、单点清洗、人工响应的防护体系，已经无法满足现实需求。未来 DDoS 防护的核心，将是：网络内生安全能力、AI 驱动大数据分析、全网级实时可视化、自动化闭环防护、自适应智能缓解能力。而真正困难的部分，并不是抵御“海啸”，而是发现并消灭那些隐藏在网络中的“食人鱼群”。