产品概述
Product overview

全球范围内愈演愈烈的 DDoS 攻击给运营商、企业、政府等各行业带来了巨大损失。攻击流量规模逐年攀升，大量占用宝贵的带宽资源，严重增加网络设备和业务系统的工作负荷，造成业务质量降低、用户投诉、IT 开支增高等问题，直接影响企业收益和品牌形象。

2001 年绿盟科技发布首款专业 DDoS 攻击防御产品——绿盟抗拒绝服务系统（NSFOCUS Anti-DDoS System，简称 NSFOCUS ADS）。十多年来坚持进行技术创新和产品研发，推出适配不同行业特点的 DDoS 防御功能和算法，及时发现背景流量中各类复杂的 DDoS 攻击事件并迅速进行清洗，保障业务的正常运行。

客户价值
Customer value

保障业务系统可用性

互联网的快速发展催生了反射服务器、发包机、IoT 僵尸源等构造 DDoS 攻击的危害，绿盟抗拒绝服务系统能够精确过滤网络层、应用层各类 DDoS 攻击，快速应对新型攻击手段，保障链路带宽、网络基础设施及关键业务的正常运行，为客户的网络可用性和业务连续性保驾护航。

提供增值业务创新营收

运营商和数据中心等客户在部署 DDoS 防御能力、保护内部业务安全的同时，还可以利用绿盟抗拒绝服务系统强大的清洗能力向租户提供高级 DDoS 清洗增值服务。优化自身业务结构，增加业绩收入。

满足安全建设合规化

部署抗 DDoS 防护能力是网络安全合规建设不可缺少的一部分，从国家安全到行业法规都有明确的要求。绿盟科技抗拒绝服务系统经过多年的迭代演进，产品发展贴合时代需求，有效满足运营商、金融、政府、企业等各行业的建设规范。

产品优势
Product superiority

○ 强大的攻击防护能力

- 满足运营商及 IDC 客户对 web 网站、游戏、CDN 等关键业务的 DDoS 防护需求；
- 满足金融业客户对 web 网站、在线交易系统、支付平台等场景的 DDoS 防护需求；
- 满足互联网行业客户对 web 网站、音频、视频、移动终端等核心业务的 DDoS 防护需求；
- 满足政府及企业客户等对 web、校园网、DNS 等业务的 DDoS 防护需求；
- 系统与绿盟云威胁情报系统联动，可将最新的威胁情报转化成防护能力，利用 IP 信誉快速甄别恶意攻击源，提高攻击清洗的速度和性能。

○ T 级的攻击防护性能

绿盟抗拒绝服务系统采用先进的多核处理器硬件架构，满足单台设备超百 G 的流量线速分析和 DDoS 攻击防护能力，同时支持通过 BGP 路由负载均衡和 portchannel 方式快速扩容，实现 T 级防护。产品采用了主机识别和流量牵引等多种技术，在过滤攻击流量的同时，确保了正常流量不受影响，保

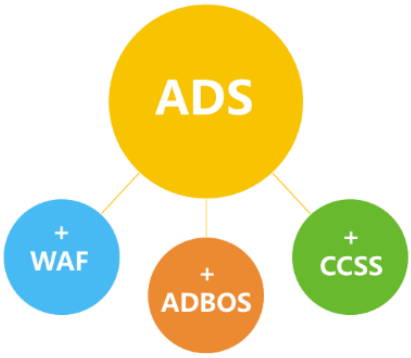
证网络服务的品质。

○ IPv4&IPv6 双栈支持

IPv6 的时代大幕已经开启，绿盟抗拒绝服务系统全面支持 IPv6&v4 双栈协议，满足纯 IPv4、纯 IPv6 以及 IPv4 和各类环境。

○ 灵活多样的能力扩展

绿盟科技以 NSFOCUS ADS 为基础，提供灵活多样的能力扩展方案，包括增值运营方案，混合清洗方案，上下级联动方案等等。



【增值运营能力扩展】通过结合绿盟云清洗运营平台，实现网内全量清洗设备的统一调度、集中管理。运营商客户通过方案丰富的增值运营能力，可以对网内用户进行管理，安全增值管理和统计收费等。

【混合清洗能力扩展】云地联动混合清洗方案将本地 ADS 清洗与云清洗能力结合，多级检测，快速响应，小流量本地清洗精确高效，大流量云端防护快速灵活，轻松应对 T 级攻击防护所需。

【上下级联动能力扩展】通过与其他安全设备（如 NSFOCUS WAF）配合实现从网络层到应用层，从小流量到大流量的智能联动，全面防护。

关键功能
Key features

DDoS 攻击防护

- 传输层攻击防护（SYN Flood，ACK Flood，FIN/RST Flood，UDP Flood，ICMP Flood，IGMP Flood，TCP Fragment，UDP Fragment）
- WEB 攻击防护（HTTP get /post Flood 攻击，慢速攻击，TCP 连接耗尽攻击，CC 攻击，慢速攻击、HTTPS 重协商攻击，非法包攻击）
- DNS 攻击防护（DNS query Flood，DNS reply Flood）
- VOIP 攻击防护（SIP Flood）
- 反射放大攻击（NTP 反射攻击，SSDP 反射攻击，DNS 反射攻击，Chargen 反射攻击，SNMP 反射攻击）
- 利用各种 Annoymous 攻击工具和僵尸工具发起的 DDoS 攻击

包过滤技术

- 基于七元组及数据包负载的模式匹配过滤规则
- 基于七元组的 ACL 过滤规则
- TCP payload 正则匹配过滤
- 针对目标 URL 的访问控制策略
- 基于硬件的访问控制规则
- 基于源 IP 地理位置的 GeoIP 过滤
- 基于云端威胁情报的肉鸡源地址过滤
- 针对群组接收流量的限速规则

部署方式

- 旁路部署
- 串联部署
- 集群部署

协议支持

- IPv4/IPv6
- 802.1Q 回注
- MPLS VPN 回注
- GRE 回注
- 支持 ARP\ICMP
- OSPF 流量牵引
- RIP 流量牵引
- MPLS LSP 回注
- BGPv4 流量牵引
- IS-IS 流量牵引

典型应用
Typical application

绿盟科技提供针对不同需求的抗 DDoS 解决方案，如三位一体解决方案、混合清洗方案、增值运营方案。

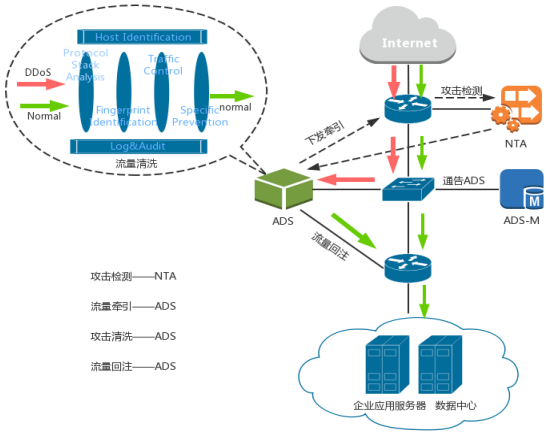
三位一体解决方案

绿盟科技的三位一体异常流量清洗解决方案，满足电信运营商对大型 Anti-DDoS 系统“可管理、可运营”的需求。该方案由绿盟网络流量分析系统（NSFOCUS NTA）、绿盟抗拒绝服务攻击系统（NSFOCUS ADS）及绿盟抗拒绝服务攻击系统管理中心（NSFOCUS ADS-M）组成。

【NSFOCUS ADS】提供单台超百 G 的 DDoS 防护性能。在清洗网络中 DDoS 攻击流量的同时，保证正常流量请求。集群模式下快速实现 T 级防护扩容。

【NSFOCUS NTA】主要用于异常流量监控和检测。通过采集 flow 数据对网络流量进行建模和分析，实时监控业务流量趋势，利用动态告警基线准确识别攻击行为。当 NTA 发现 DDoS 攻击等异常时，产生告警，记录攻击详情，并与 ADS 智能联动，对流量展开牵引和清洗。

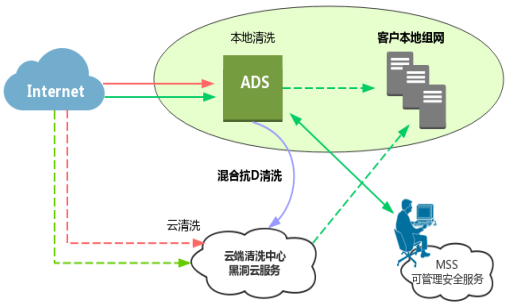
【NSFOCUS ADS-M】绿盟抗拒绝服务攻击系统管理中心可以同一监控和管理检测设备 NTA 和清洗设备 ADS，实现设备集中管理、策略批量下发、数据汇总整合等。通过联合各部件的能力，简化运维，增强数据关联分析和集中呈现。



混合清洗解决方案

混合清洗防护是全球最热门的完整抗 DDoS 解决方案。绿盟科技通过专有抗 DDoS 设备（ADS）与黑洞云清洗服务（CCSS）结合，推出云地联动混合抗 DDoS 解决方案，快速过滤大流量侵害，精准防护高级攻击，保障出口带宽可用性及业务运行平稳度。

本地防护利用 ADS 解决带宽范围内的各类 DDoS 攻击，防护策略自主可控，精细过滤应用层攻击。云端防护着重应对大流量攻击入侵。当出口带宽超荷负载时，云清洗服务可以将业务流量引到高防云清洗中心，将清洗后的流量回注到业务网络中，有效缓解带宽出口拥塞。回注的流量再由本地的 ADS 设备进行二次过滤，彻底清洗应用层高级攻击，全面保证出口带宽、基础路由和业务主机的安全性和可用性。



增值运营解决方案

流量清洗业务运营系统 ADBOS（Anti-DDoS Business Operation System）具备运维自动化、清洗可视化和操作简单化等特性，大幅降低运维成本、提升客户体验。

在业务场景中，流量清洗业务运营系统将异常流量监控检测能力与防护能力进行整合调度，实现规模化运营和增值创收。平台自带的业务拨测系统可以联合流量分析系统双重监控业务可用性，提高 DDoS 告警准确率。此外，平台支持与绿盟云威胁情报系统联动，将最新的威胁情报转化成防护能力，快速应对新型 DDoS 攻击，提升清洗效率。

在增值运营场景中，平台通过移动自助终端 APP 提供可视化业务拨测、告警推送、自主防护、自主报表等功能，帮助客户随时接收攻击告警并掌握清洗详情。整个清洗过程自主可控，多名运营管理人员可以同步共享清洗结果，实现了产品功能与运营业务的高效结合。