# 绿盟抗拒绝服务系统

# 产品白皮书

# 目录

# DDoS 攻击发展趋势

全球范围内，DDoS 攻击威胁从未减弱，反而愈演愈烈。

DDoS（Distributed Denial of Service） 分布式拒绝服务是最常见的网络攻击之一。不法分子通过控制大量主机对互联网上的目标进行攻击，致使业务中断，造成客户直接经济损失。而多数客户由于缺乏专业知识或经验储备，对 DDoS 攻击威胁的感知不灵敏，更是无法应对日新月异的 DDoS 攻击侵害。

由于 DDoS 攻击工具的易得性和易用性增强，越来越多的人可以轻松操纵攻击工具对网络造成威胁和侵害，低成本攻击带来的高收益回报催生了黑产，形成恶性循环。为了持续获得高额报酬，DDoS 攻击手段不断变化，准确把握攻击发展趋势才能从容应对，在攻防对抗中占领先机。

通过近几年对市场的观察，DDoS 攻击呈现出三大趋势特征。

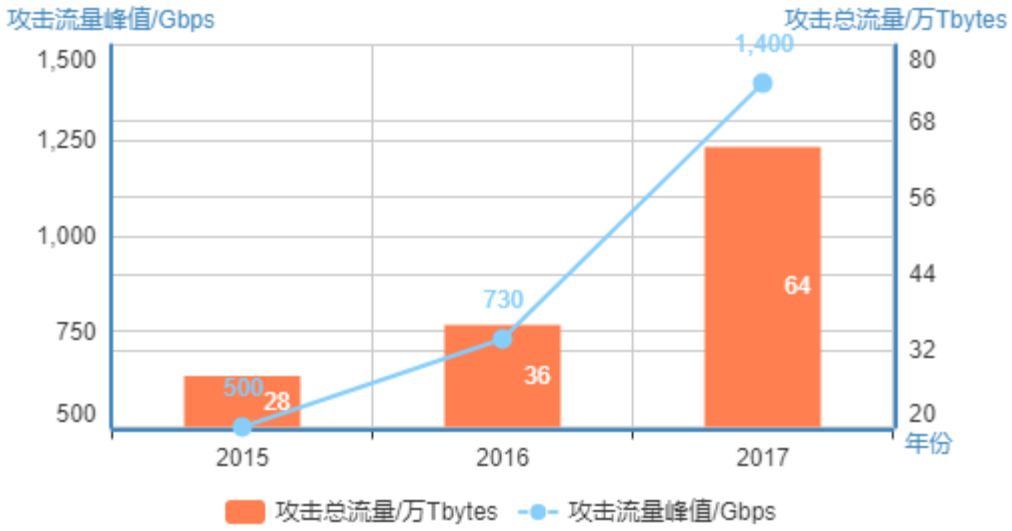
第一，峰值流量大。物联网的快速发展给 DDoS 僵尸主机提供了滋生的温床，IoT 设备被黑客入侵、操纵，形成 DDoS 放大攻击。近年来 DDoS 攻击总流量，单次攻击最高峰值，大流量攻击占比等数据都有不同程度的增长，部分数据如下图。

第二，发生频率高。2017 年，国内发生了 20 万次攻击，月度攻击事件发生频率环比上涨。DDoS 攻击频繁骚扰各行业客户的正常业务运行。

第三，攻击复杂化。混合攻击是当前 DDoS 的主流，单次攻击事件包含大容量泛洪、应用层攻击、连接耗尽型攻击等攻击类型，而新型攻击也在不断涌现，攻击手段的复杂化迫使防守手段也需要随之改善进步。除了 DDoS 的攻击手段在发展，攻击的复杂性还体现在攻击者利用 DDoS 作为障眼法，转移客户焦点并伺机进行蠕虫和挂马，造成篡改主机授权，窃取资产信息。

那么作为防守方又应如何应对 DDoS 攻击？防火墙和入侵检测系统等网络设备，或者传统的边界安全设备可以做到有效防御吗？单一层面的防护还可以解决问题吗？而采用专业且具有针对性的 DDoS 攻击检测和防护方案，又会有什么不同？

2015-2017 年度 DDoS 攻击流量统计



# 现有 DDoS 防护手段分析

## 1 路由器

我们可以通过路由器实施某些安全措施，比如 ACL 等，过滤部分非法流量。然而 ACL 通常基于协议或源地址进行配置，目前众多的 DDoS 攻击采用的是常见的合法协议，比如 HTTP 协议。这种情况下，路由器就无法有效过滤攻击。同时，如果 DDoS 攻击采用地址欺骗的技术伪造数据包，路由器也无法有效应对。

## 2 防火墙

防火墙是最常用的安全产品之一，但是防火墙设计原理中并没有考虑针对 DDoS 攻击的防护。在某些情况下，防火墙甚至会成为 DDoS 攻击的目标而导致整个网络拒绝服务。

首先，防火墙作为三层包转发设备部署在网络中，主要是保护内部资产，并为内部用户提供网络通路。DDoS 采用合法协议请求服务器时，防火墙无法从背景流量中准确区分攻击流量。而防火墙内置的攻击检测模块一般基于特征规则，DDoS 攻击者只要对攻击数据包稍加变化，防火墙就无法应对。

其次，防火墙计算能力有限。防火墙通常采用逐包检查的方式，检查强度高，性能消耗大。DDoS 攻击的海量数据会引起防火墙性能急剧下降，甚至设备瘫痪，无法完成正常流量的转发任务。

最后，是防火墙的部署位置影响了其防护 DDoS 攻击的能力。防火墙一般部署在网络入口，虽然某种意义上保护了网络内部的所有资源，但是往往也成为 DDoS 攻击的目标。攻击者一旦发起 DDoS 攻击就会造成网络性能整体下降，导致用户正常请求被拒绝。

## 3 IPS/IDS

目前 IPS/IDS 系统是最广泛的攻击检测或防护工具，但是在面临 DDoS 攻击时，IPS/IDS 系统往往不能满足防护要求。入侵检测系统虽然能够检测应用层的攻击，但是工作机制都是基于规则，需要对协议会话进行还原。而目前 DDoS 攻击大部分都是采用基于合法数据包的攻击流量，所以 IPS/IDS 系统很难对这些攻击特征进行有效检测。虽然某些 IPS/IDS 系统本身也具备协议异常检测的能力，但都需要安全专家手工配置才能真正生效，实施成本高而易用性极低。IPS/IDS 系统设计之初就是基于特征的应用层攻击检测设备，而大量的 DDoS 攻击主要以三层或是四层的协议异常为特点，注定了 IPS/IDS 技术不太可能成为 DDoS 的主要检测和防护手段。

# 绿盟抗 DDoS 解决方案

针对目前流行的已知和未知的 DDoS 攻击形式，绿盟科技提供了自主研发的抗拒绝服务产品——NSFOCUS Anti-DDoS System，简称 NSFOCUS ADS。通过及时发现背景流量中的攻击行为，NSFOCUS ADS 可以迅速对攻击流量进行过滤，保护正常业务运营。ADS 产品可以在多种网络环境下轻松部署，可以有效避免单点故障，保证网络可用性和网络的整体性能。

绿盟科技提供丰富多维、针对不同客户需求的抗 DDoS 解决方案，主要包括三位一体解决方案、混合清洗方案、增值运营方案。

## 三位一体解决方案

绿盟科技提供三位一体的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。该解决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。解决方案的三类组件产品特点如下：

### 1 NSFOCUS ADS（绿盟抗拒绝服务攻击系统）

作为绿盟流量清洗产品系列中的关键组成，NSFOCUS ADS 提供了单台最大 240Gbps 的 DDoS 线速防护能力。通过部署 NSFOCUS ADS 设备，可以对网络中的 DDoS 攻击流量进行清洗，同时保证正常流量的访问。NSFOCUS ADS 采用集群模式可以实现 T 级防护容量，提高整个系统抵御海量 DDoS 攻击的能力。

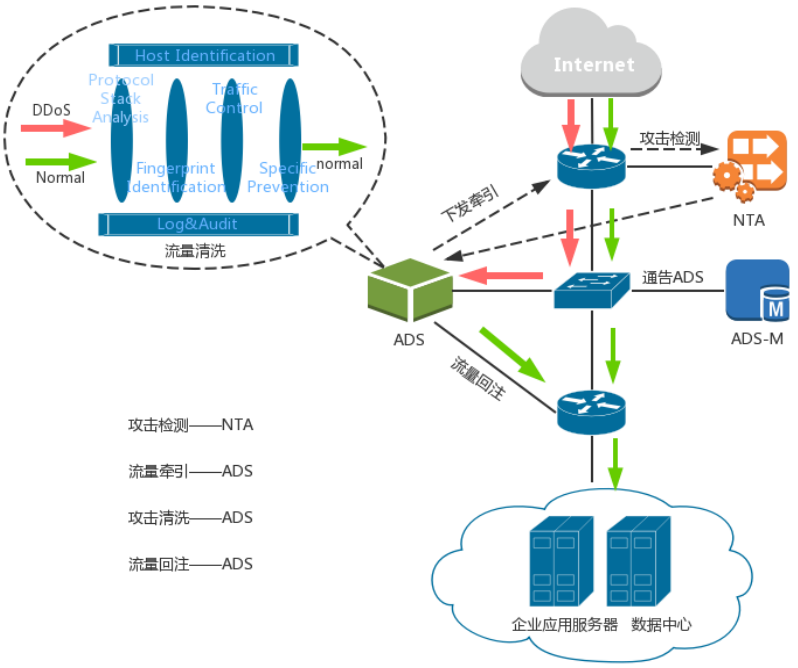
### 2 NSFOCUS NTA（绿盟网络流量分析系统）

绿盟流量清洗产品系列中的另外一款 NSFOCUS NTA 主要用于异常流量监控和检测。NSFOCUS NTA 设备通过收集 flow 数据对流量进行建模和分析，监控网络流量并进行分析，采用动态告警基线分析攻击行为。通过与 NSFOCUS ADS 进行联动配合，当 NTA 发现异常的网络流量时，会根据预先由系统管理员定义的方式和策略触发报警，并同时 NSFOCUS ADS 展开流量的牵引和清洗。还可以通过 BGP Flow spec 技术与路由器进行联动，提高防护效率，优化清洗方案资源调配。另外，产品支持硬件部署与软件部署两种形态，满足不同场景和方案的建设需求。

### 3 NSFOCUS ADS-M（绿盟抗拒绝服务系统管理中心）

NSFOCUS ADS-M 是绿盟流量清洗产品系列中的管理平台，负责将来源于多个 NSFOCUS ADS 设备的数据进行关联分析和处理；基于防护群组、业务域等逻辑对象进行业务用户分组管理，提供群组化的账号管理和策略控制；实现对 NSFOCUS ADS 和 NSFOCUS NTA 的集中管理功能。此外，ADS-M 还能提供类型丰富的报表。NSFOCUS ADS-M 还能提供用户自服务系统，满足运营商利用 DDoS 做增值服务的需要。另外，产品支持硬件部署与软件部署两种形态，满足不同场景和方案的建设需求。

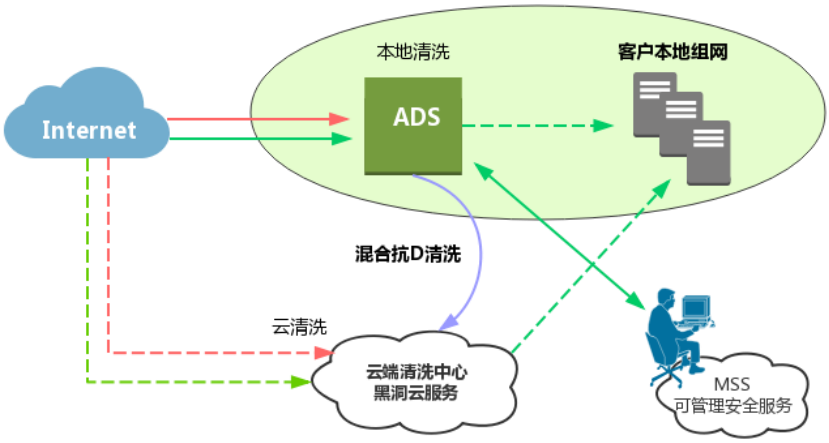
绿盟抗 DDoS 三位一体解决方案示意图




# 混合清洗解决方案

DDoS 攻击防护是全球互联网用户的共同难题，而混合清洗防护是目前最受推崇的完整抗 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，有效抵御复杂 DDoS 攻击，并快速过滤大流量攻击侵害，保障业务安全平稳运行。本地防护以 ADS 为主，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事件。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，全面保证业务带宽、基础路由和业务主机的安全性和可用性。

绿盟抗 DDoS 混合清洗解决方案示意图

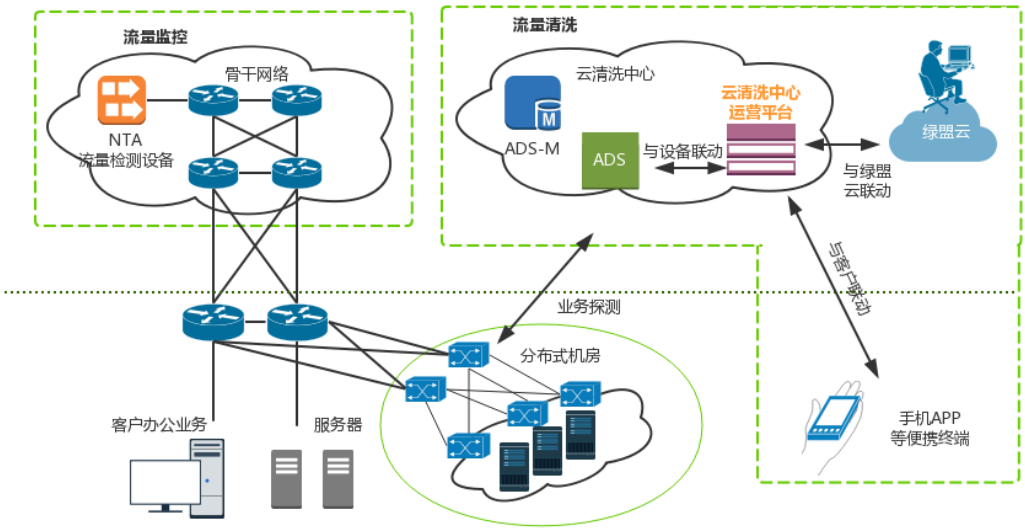



# 增值运营解决方案

绿盟科技在 DDoS 防护领域有着 14 年的攻防技术研究经验和运营能力积累。为了充分体现绿盟抗 DDoS 产品的能力，贴合市场业务发展的需求，绿盟科技推出了流量清洗业务运营系统 ADBOS（Anti-DDoS Business Operation System），实现运维自动化、清洗可视化和操作简单化，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，实现搭建规模化运营和增值创收。此外，平台自带的业务拨测系统可以辅助流量分析系统提高 DDoS 监测准确率，ADBOS 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，如利用 IP 信誉数据快速甄别恶意 IP 提高异常流量的清洗速度和性能。方案示意图参考下图。

在增值运营场景中，平台还提供移动自助终端 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，帮助客户随时掌握攻击告警和清洗详情。整个清洗过程自主可控，且支持多名运营管理人员同步清洗结果，完整实现了产品功能与运营业务的高效结合。

绿盟抗 DDoS 云清洗平台解决方案示意图



# 绿盟抗 DDoS 方案优势

## 精准的攻击流量识别

应用自主研发的抗拒绝服务攻击算法，针对不同种类的 DDoS 攻击采用不同的算法（例如流量建模、反欺骗、协议栈行为模式分析、特定应用防护、用户行为模式分析、动态指纹识别等）识别，从而准确地区分出恶意 DDoS 报文。产品的攻击检测和识别的算法效率非常高，可以承受各类大流量 DDoS 攻击，以 Syn Flood 防护为例，连接维持率和新发起连接可用率都可达 100%——其效率远远超过了 Syn-cookie 和 Random-drop 等算法。

## 强大的攻击防护能力

基于绿盟科技自主研发的独特的防护算法，绿盟抗拒绝服务攻击系统可高效防护各种类型的 DDoS 攻击，例举如下：

- 各种传输层的拒绝服务攻击，如 SYN Flood，SYN-ACK Flood，ACK Flood，FIN/RST Flood ，UDP Flood，ICMP Flood，IP Fragment Flood、Stream flood 等。
- 来自 web 的安全威胁。如 HTTP get /post flood 攻击，慢速攻击，TCP 连接耗尽攻击，TCP 空连接攻击，如 HTTPS 重协商攻击，非法包攻击等。
- 危害巨大的应用层拒绝服务攻击，如 DNS 服务攻击，游戏服务攻击、音视频服务攻击等。
- 利用各种代理服务器如 CDN，WAP 网关等发起的 DDoS 攻击。
- 利用各种 annoymous 攻击工具和僵尸工具发起的 DDoS 攻击。

除防护以上攻击外，NSFOCUS ADS 系统还拥有流量限制功能，用于应对突发的流量异常变化；提供访问控制列表（ACL）功能，可直接设置黑白名单简化对特定应用的控制难度；另有深层包检查规则允许管理员根据攻击包的特征字节定义模版，进行快速防护。

针对运营商网络中客户众多、且对 DDoS 防护需求不同的特点，ADS 设备提供防护群组功能，对用户加以分组，并对不同的用户组提供细粒度的防护策略。同时，为了降低运维的成本，ADS 设备能够对防护对象中各种服务的流量进行自动学习，并根据学习的结果生成防护策略。

此外，ADS 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 信誉数据快速甄别恶意 IP 提高异常流量的清洗速度和性能。绿盟科技安全攻防团队通过大数据分析提炼出攻击威胁情报，及时发现新 DDoS 攻击，并将情报信息与业务防护相结合，提升 DDoS 攻击防护的智能性与先进性。

## T 级的攻击防护性能

根据型号不同，电信级高端 NSFOCUS ADS 系统分别采用先进的多核处理器硬件构架。单台设备最高可具有 240Gbps 流量的线速分析和 DDoS 攻击防护能力，同时支持多台设备通过 BGP 路由负载均衡和 portchannel 方式进行扩容，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，从而保证网络服务的品质。

## 灵活的应用部署方式

由于客户网络环境和规模不同，绿盟抗拒绝服务攻击系统也包含了多种产品形态和部署方式，包括串联、旁路以及旁路集群等不同方式，NSFOCUS ADS 系统能够适应各种复杂的网络环境，为独立服务器、各体量的企业，以及电信运营商网络提供代价最小的应用方案，可灵活部署和管理。

针对中小企业客户业务带宽较小，无法承载大流量攻击的痛点，绿盟科技还提供本地防护+云端清洗的解决方案。客户通过在本地部署的 ADS 设备进行小流量攻击的清洗以及精细化防护，当攻击流量超过带宽负荷时，一键通告云端清洗中心展开防护，从高处拦截大流量攻击，保障本地带宽的可利用性。

## 友好的系统/报表管理

绿盟科技集中管理平台 NSFOCUS ADS-M 提供硬件和软件两种形态，可对 ADS 进行管理和数据整合，提供直观便利的设备运行监控、策略配置、报表生成和抓包取证等功能。ADS-M 可以对多台 NSFOCUS ADS 设备进行集中式管理、监控、控制、维护,让防护更加高效简洁。

## 独特的增值业务管理

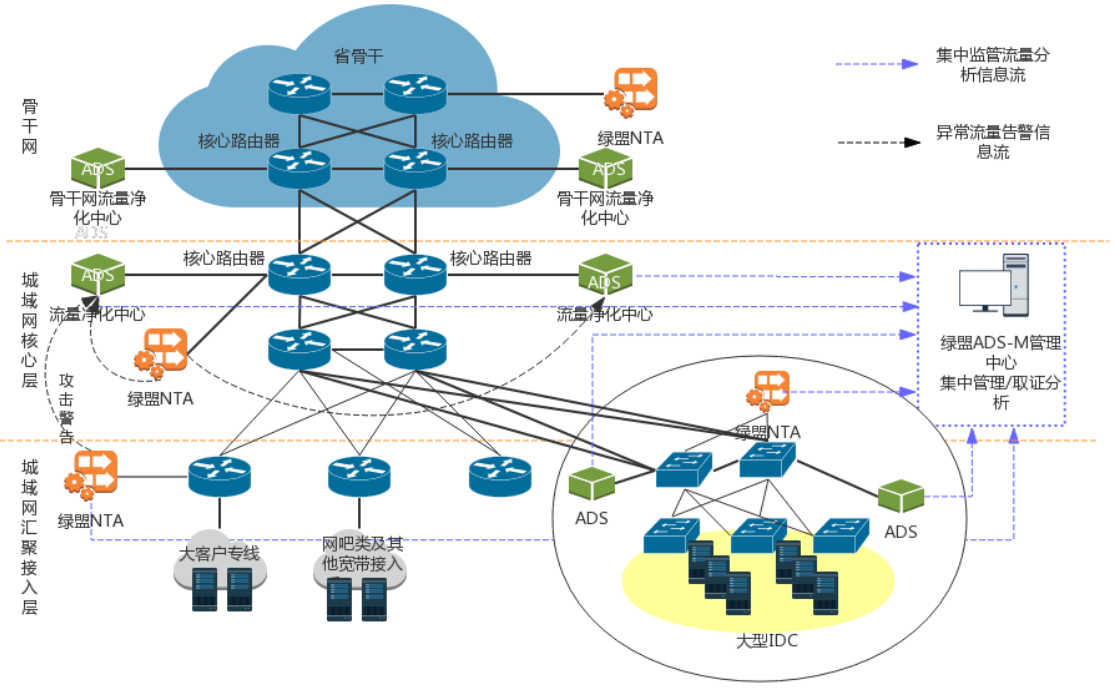
结合 NSFOCUS ADS-M 系列的管理产品，系统提供特有的运营维护和自服务系统的增值服务平台，用户可获取服务收益。运营商藉此对有强烈防护需求的大客户（网吧、证券、珠宝商场、电力、政府、酒店、IPTV 提供商等）提供安全防护增值服务，该平台既提高了大客户对其系统安全状况的感知度，又提升了客户的服务质量与内涵。

## IPv6&IPv4 双栈支持

Ipv6 的时代大幕正在逐渐开启，互联网向 ipv6 过渡已经开始进入实施阶段。绿盟科技积极接应客户需求，产品支持 IPv6&v4 双栈协议，解除客户后顾之忧。

# 行业场景展示

## 场景案例一 运营商案例 大型网络出口




场景特点：网络结构复杂，出口流量大，出口核心路由旁挂

推荐型号：ADS 8000/ ADS 10000

工作流程：检测设备发现 DDoS 攻击后通知 ADS；ADS 与核心路由基于配置好的 BGP 邻居关系宣告路由更新条目；流量经过 ADS 清洗后注入回核心路由；清洗结果上传给 ADS-M 形成汇总报告。

方案价值：运营商在本地出口自建清洗节点，为其下用户提供增值清洗服务，增加创收点。或绿盟与运营商共建清洗节点，减少单一建设的投入成本，实现合作共赢。

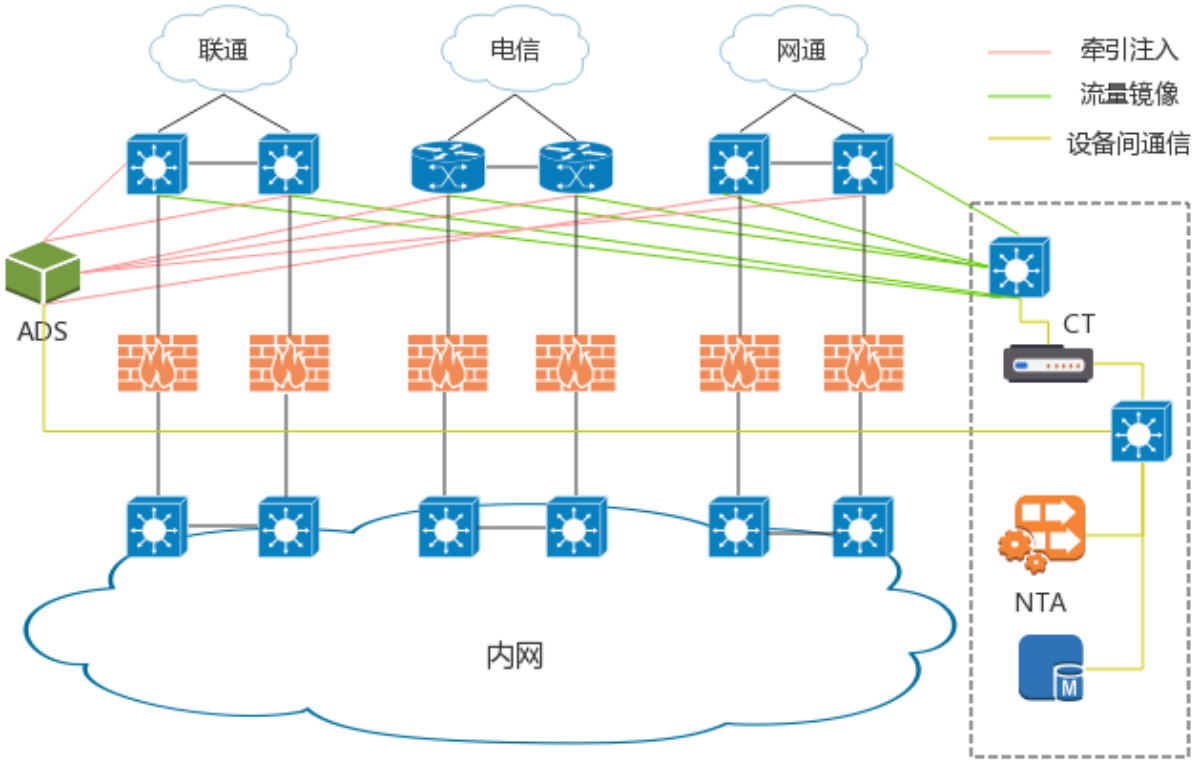
## 场景案例二 金融行业案例 多出口场景

场景特点：安全要求高，网络稳定性要求高，金融客户多出口牵引

推荐型号：ADS 4020E/ ADS 6025E/ ADS 8000

工作流程：ADS、NTA、ADS-M 及 CT（非必须）的管理口接到一台交换机，CT 将镜像流量转化为 flow 后发给 NTA，NTA 向 ADS 发送告警；ADS-M 集中管理，汇总数据，形成报表。

方案价值：将多个出口的流量引到同一个清洗节点进行本地防护，大流量攻击超过本地带宽承载能力时，通过云端清洗服务进行过滤后指向本地，形成混合清洗的抗 D 方案。减少本地带宽扩容的采购费用以及运维投入。



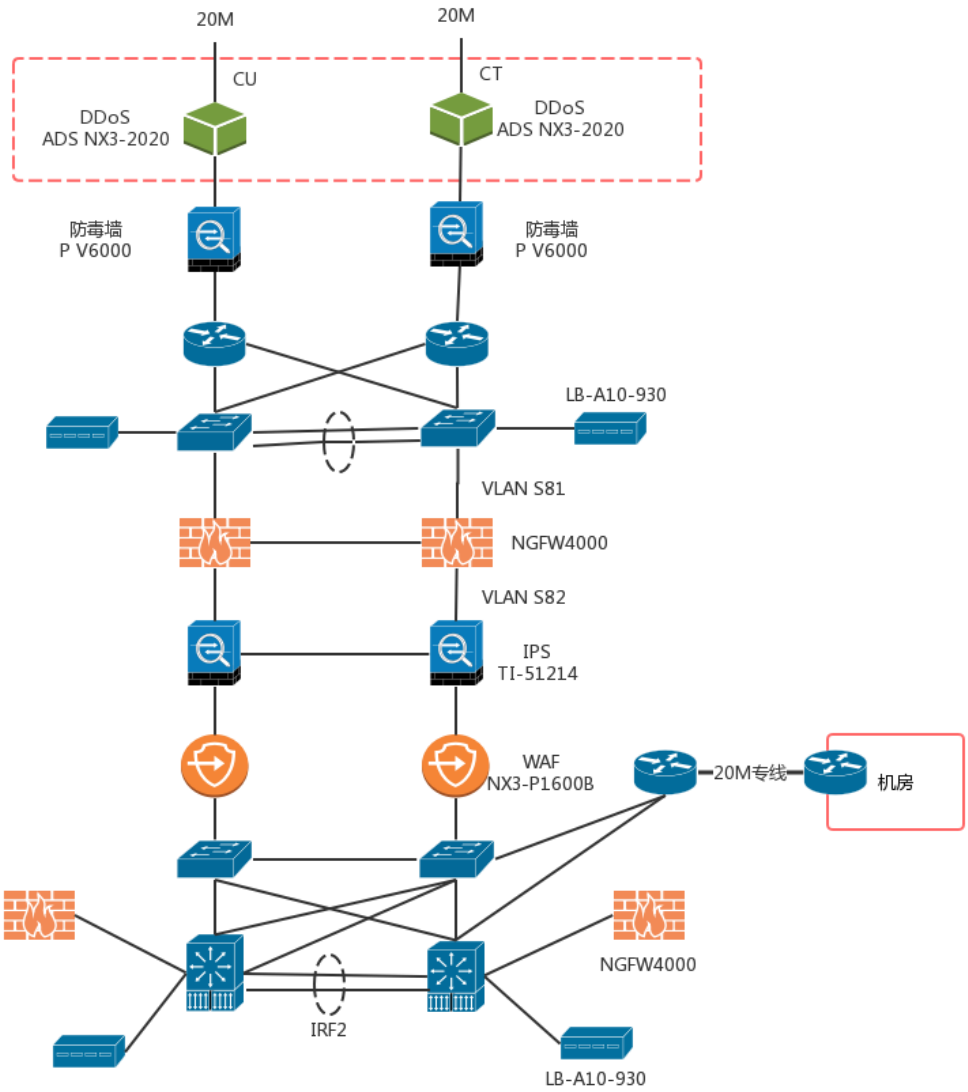

## 场景案例三 企业案例 串行部署

场景特点：带宽小，串行部署

推荐型号：ADS 4020E/ ADS 6025E

工作流程：流量从互联网方向流入 ADS，触发阈值后 ADS 开展清洗，并将清洗后的流量从 OUT 口转发向下。由内向外的流量从 OUT 口流入，并从 IN 口流向互联网，此时 ADS 不进行清洗

方案价值：清洗设备串联部署在网络出口边界。大流量攻击超过本地带宽承载能力时，通过云端清洗服务进行过滤后指向本地，形成混合清洗的抗 D 方案。减少本地带宽扩容的采购费用以及运维投入。




# 巨人背后的专家

绿盟科技自创立之初至今，一直致力于做巨人背后的专家。自 2002 年绿盟抗拒绝服务产品发布至今，持续投入研发资源，不断丰富产品功能，优化产品性能。凭借着十余年商用案例和服务支持的丰富经验，绿盟科技服务专家可提供快速的现场防御支持及攻击防御咨询/部署/培训等服务。公司提供 7*24 小时 DDoS 防护解决方案，ADS with MSS 可将客户本地的 ADS 和 NTA 设备与绿盟安全云对接同步，由绿盟安全专家团队协助企业对 DDoS 攻击全天候监视、响应、防护。

总结而言，DDoS 攻击威胁持续增长，由于攻击带来的损失增长，运营商、企业或是政府必须有所对策以保护其投资、利润和服务。为了弥补传统安全设备 DDoS 攻击防护能力的不足，我们需要专业的系统保护业务不受 DDoS 攻击影响。这种工具不仅能够检测复杂的 DDoS 攻击，而且必须在不影响正常业务流量的前提下对攻击流量进行实时阻断，需具备更细粒度的攻击检测和分析机制。绿盟抗拒绝服务攻击产品提供了业界领先的 DDoS 防护能力，通过多种机制的分析检测机制以及灵活的部署方式，绿盟科技的产品和技术能够有效的阻断攻击，保证合法流量的正常传输，这对于保障业务系统的运行连续性和完整性有着极为重要的意义。