绿盟抗拒绝服务系统

产品白皮书

目录

插图索引

一. 前言

DoS（Denial of Service 拒绝服务）攻击由于攻击简单、容易达到目的、难于防止和追查越来越成为常见的攻击方式。拒绝服务攻击可以有各种分类方法，如果按照攻击方式来分可以分为：资源消耗、服务中止和物理破坏。资源消耗指攻击者试图消耗目标的合法资源，例如：网络带宽、内存和磁盘空间、CPU 使用率等等。通常，网络层的拒绝服务攻击利用了网络协议的漏洞，或者抢占网络或者设备有限的处理能力，造成网络或者服务的瘫痪，而 DDoS 攻击又可以躲过目前常见的网络安全设备的防护，诸如防火墙、入侵监测系统等，这就使得对拒绝服务攻击的防治，成为了一个令管理员非常头痛的问题。

传统的攻击都是通过对业务系统的渗透，非法获得信息来完成，而 DDoS 攻击则是一种可以造成大规模破坏的黑客武器，它通过制造伪造的流量，使得被攻击的服务器、网络链路或是网络设备（如防火墙、路由器等）负载过高，从而最终导致系统崩溃，无法提供正常的 Internet 服务。

由于防护手段较少同时发起 DDoS 攻击也越来越容易，所以 DDoS 的威胁也在逐步增大，它们的攻击目标不仅仅局限在 Web 服务器或是网络边界设备等单一的目标，网络本身也渐渐成为 DDoS 攻击的牺牲品。许多网络基础设施，诸如汇聚层/核心层的路由器和交换机、运营商的域名服务系统（DNS）都不同程度的遭受到了 DDoS 攻击的侵害。2002 年 10 月，一次大规模黑客攻击的前兆就是十三台根域名服务器中的八台遭受到“野蛮”的 DDoS 攻击，从而影响了整个 Internet 的通讯。

随着各种业务对 Internet 依赖程度的日益加强，DDoS 攻击所带来的损失也愈加严重。包括运营商、企业及政府机构的各种用户时刻都受到了 DDoS 攻击的威胁，而未来更加强大的攻击工具的出现，为日后发动数量更多、破坏力更强的 DDoS 攻击带来可能。

正是由于 DDoS 攻击非常难于防御，以及其危害严重，所以如何有效的应对 DDoS 攻击就成为 Internet 使用者所需面对的严峻挑战。网络设备或者传统的边界安全设备，诸如防火墙、入侵检测系统，作为整体安全策略中不可缺少的重要模块，都不能有效的提供针对 DDoS 攻击完善的防御能力。面对这类给 Internet 可用性带来极大损害的攻击，必须采用专门的机制，对攻击进行有效检测，进而遏制这类不断增长的、复杂的且极具欺骗性的攻击形式。

二. DDoS 的威胁愈演愈烈

DDoS 攻击一般通过 Internet 上那些“僵尸”系统完成，由于大量个人电脑联入 Internet，且防护措施非常少，所以极易被黑客利用，通过植入某些代码，这些机器就成为 DDoS 攻击者的武器。当黑客发动大规模的 DDoS 时，只需要同时向这些将僵尸机发送某些命令，就可以由这些“僵尸”机器完成攻击。随着 Botnet 的发展，DDoS 造成的攻击流量的规模可以非常惊人，会给应用系统或是网络本身带来非常大的负载消耗。

特点：使用有效协议；采用源 IP 欺骗；大量分布；攻击类型多元化。

2.1 攻击影响

DDoS 攻击给运营商、企业和政府都将可能带来巨大的损失。带宽耗尽型的攻击可能极大浪费运营商骨干网络宝贵的带宽资源，严重增加核心设备的工作负荷，造成关键业务的中断或网络服务质量的大幅降低。DDoS 攻击之下的门户网站性能急剧下降，无法正常处理用户的正常访问请求，造成客户访问失败；服务质量协议（SLA）也会受到破坏，带来高额的服务赔偿。同时，公司的信誉也会蒙受损失，而这种危害又常常是长期性的。利润下降、生产效率降低、IT 开支增高以及相应问题诉诸法律而带来的费用增加等等，这些损失都是由于 DDoS 攻击造成的。

此外，攻击的波及面之广也是当前不得不面对的问题。CNCERT 在 2010 年上半年《中国互联网网络安全报告》中指出，CNCERT 2010 年上半年抽样监测结果显示我国大陆约有近 124 万个 IP 地址对应的主机被植入僵尸和木马程序控制，同时监测发现境外有 127559 个 IP 地址作为木马控制服务器参与控制中国大陆地区的木马受控主机。

2.2 攻击分析

那么 DDoS 攻击究竟如何工作呢？从犯罪学角度，任何攻击必须具备三个要素，即攻击手段（Method）、时机（Opportunity）以及攻击动机（Motive）。接下来，我们将从这三方面对 DDoS 攻击进行分析。

2.2.1 攻击手段

在此，先简单回顾 DDoS 攻击采用的手段。通常而言，网络数据包利用 TCP/IP 协议在 Internet 传输，这些数据包本身是无害的，但是如果数据包异常过多，就会造成网络设备或者

服务器过载；或者数据包利用了某些协议的缺陷，人为的不完整或畸形，就会造成网络设备或服务器服务正常处理，迅速消耗了系统资源，造成服务拒绝，这就是 DDoS 攻击的工作原理。DDoS 攻击之所以难于防护，其关键之处就在于非法流量和合法流量相互混杂，防护过程中无法有效的检测到 DDoS 攻击，比如利用基于特征库模式匹配的 IDS 系统，就很难从合法包中区分出非法包。加之许多 DDoS 攻击都采用了伪造源地址 IP 的技术，从而成功的躲避了基于异常模式监控的工具的识别。

一般而言，DDoS 攻击主要分为以下几种类型：

带宽型攻击——这类 DDoS 攻击通过发出海量数据包，造成设备负载过高，最终导致网络带宽或是设备资源耗尽。通常，被攻击的路由器、服务器和防火墙的处理资源都是有限的，攻击负载之下它们就无法处理正常的合法访问，导致服务拒绝。

流量型攻击最通常的形式是 Flooding 方式，这种攻击把大量看似合法的 TCP、UDP、ICMP 包发送至目标主机，甚至，有些攻击还利用源地址伪造技术来绕过检测系统的监控。

应用型攻击——这类 DDoS 攻击利用了诸如 TCP 或是 HTTP 协议的某些特征，通过持续占用有限的资源，从而达到阻止目标设备无法处理正常访问请求的目的，比如 HTTP Half Open 攻击和 HTTP Error 攻击就是该类型的攻击。

2.2.2 攻击时机

目前，融合（Convergence）的趋势正逐渐改变人们生活的模式。我们正逐渐感知来自终端业务的融合，应用服务提供商（ASP）与网络服务提供商（NSP）的融合，以及传统电信网与 IP 网的融合。融合带来了新的商业模式和业务增长点，也蕴藏了多元化的安全威胁。来自 Symantec 的数据表明，Bots 通常会感染通过大型的 ISP、高速连接到 Internet 的主机。带宽资源的扩容，同时也便利了攻击者。

2.2.3 攻击动机

从之前国内发生的多起 DDoS 攻击事件来看，值得关注的是，攻击者的动机从个人爱好或是扬名到追求经济获利的重大转变。黑色产业链的形成与逐渐壮大已经成为网络安全必须面对的问题，根据 Symantec 最新互联网安全威胁调研表明，其趋势在不断升级。

黑色产业链主要特点为：

1. 经济利益驱使，攻击可产生最终价值；
2. 攻击趋于专业化；
3. 攻击者有明确的分工，并形成新型的业务模式；

4. 多层攻击应用：采用多种恶意活动相结合的方式。不直接采用原始攻击，而是将其用于部署随后的攻击。

2.3 发展趋势

绿盟科技多年来实时跟踪、检测和研究 DDoS 攻击情况，并将研究成果产品化，为客户提供专业的解决方案、防护产品和技术支撑。根据最近的研究表明， DDoS 攻击有以下发展趋势：

1. 大量可轻易获得的僵尸网络及僵尸工具用来发动 DDoS 攻击，攻击难度降低，DDoS 攻击发生频率增大。
2. 攻击流量呈海量趋势，可达 N*Gbps，攻击流量占用大量运营商网络出口带宽，大大降低网络设备的运行效率。
3. 针对应用服务的攻击增多，DDoS 攻击已形成成熟的产业链，背后的经济利益成为攻击的原始驱动。
4. 攻击方式更为复杂，带宽型攻击夹杂应用型攻击的混合攻击增多，且极难防御。

2.4 小结

分析了 DDoS 攻击的犯罪三要素、了解了其发展趋势后，可以看出 DDoS 攻击的特点为“经济利益驱使、有明确攻击目标、手段专业化、影响面大”。如何应对来自 DDoS 攻击的严峻挑战，有效进行防护，保护关键业务和重要资源呢？是不是单一一个层面的防护就能解决问题呢？

三. DDoS 防护的必要性

任何需要通过网络提供服务的业务系统，不论是处于经济原因还是其他方面，都应该对 DDoS 攻击防护的投资进行考虑。大型企业、政府组织以及服务提供商都需要保护其基础业务系统（包括 Web、DNS、Mail、交换机、路由器或是防火墙）免受 DDoS 攻击的侵害，保证其业务系统运行的连续性。虽然 DDoS 防护需要增加运营成本，但是从投资回报率上进行分析，可以发现这部分的投资是值得的。

企业/政府网络——对于企业或政府的网络系统，一般提供内部业务系统或网站的 Internet 出口，虽然不会涉及大量的 Internet 用户的访问，但是如果遭到 DDoS 攻击，仍然会带来巨大的损失。对于企业而言，DDoS 攻击意味着业务系统不能正常对外提供服务，势必影响企业正常的生产；政府网络的出口如果遭到攻击，将会带来重大的政治影响，这些损失都是可以通过部署 DDoS 防护系统进行规避的。

电子商务网站、在线游戏、支付业务等互联网业务——电子商务网站、游戏业务、网上支付等互联网业务经常是黑客实施 DDoS 攻击的对象，其在 DDoS 防护方面的投资非常有必要。如果该类型业务系统遭受了 DDoS 攻击，则在系统无法提供正常服务的时间内，由此引起的业务无法访问、支付错误、交易量下降、广告损失、品牌损失、网站恢复的代价等等，都应该作为其经济损失计算在内，甚至目前有些黑客还利用 DDoS 攻击对网站进行敲诈勒索，这些都给网站的正常运营带来极大的影响，而 DDoS 防护措施就可以在很大程度上减小这些损失；另一方面，这些防护措施又避免了遭受攻击的网站购买额外的带宽或是设备，节省了大量重复投资，为客户带来了更好的投资回报率。

电信运营商——对于运营商而言，保证其网络可用性是影响 ROI 的决定因素。如果运营商的基础网络遭受攻击，那么所有承载的业务都会瘫痪，这必然导致服务质量的下降甚至失效。同时，在目前竞争激烈的运营商市场，服务质量的下降意味着客户资源的流失，尤其是那些高 ARPU 值的大客户，会转投其他的运营商，这对于运营商而言是致命的打击。所以，有效的 DDoS 防护措施对于保证网络服务质量有着重要意义。

另一方面，对运营商或是 IDC 而言，DDoS 防护不仅仅可以避免业务损失，还能够作为一种增值服务提供给最终用户，这给运营商带来了新的利益增长点，也增强了其行业竞争能力。

四. 当前防护手段的不足

虽然目前网络安全产品的种类非常多，但是对于 DDoS 攻击却一筹莫展。常见的防火墙、入侵检测、路由器等，由于涉及之初就没有考虑相应的 DDoS 防护，所以无法针对复杂的 DDoS 攻击进行有效的检测和防护。而至于退让策略或是系统调优等方法只能应付小规模 DDoS 攻击，对大规模 DDoS 攻击还是无法提供有效的防护。

4.1 手工防护

一般而言手工方式防护 DDoS 主要通过两种形式：

系统优化——主要通过优化被攻击系统的核心参数，提高系统本身对 DDoS 攻击的响应能力。但是这种做法只能针对小规模的 DDoS 进行防护，当黑客提高攻击的流量时，这种防护方法就无计可施了。

网络追查——遭受 DDoS 攻击的系统的管理人员一般第一反应是询问上一级网络运营商，这有可能是 ISP、IDC 等，目的就是为了弄清楚攻击源头。但是如果 DDoS 攻击流量的地址是伪造的，那么寻找其攻击源头的过程往往涉及很多运营商以及司法机关。再者，即使已经确定了攻击源头，进而对其流量进行阻断，也会造成相应正常流量的丢失。加之目前 Botnet 以及新型 DrDoS 攻击的存在，所以通过网络追查来防护 DDoS 攻击的方法没有任何实际意义。

4.2 退让策略

为了抵抗 DDoS 攻击，客户可能会通过购买冗余硬件的方式来提高系统抗 DDoS 的能力。但是这种退让策略的效果并不好，一方面由于这种方式的性价比过低，另一方面，黑客提高攻击流量之后，这种方法往往失效，所以不能从根本意义上防护 DDoS 攻击。

4.3 路由器

通过路由器，我们确实可以实施某些安全措施，比如 ACL 等，这些措施从某种程度上确实可以过滤掉非法流量。一般来说，ACL 可以基于协议或源地址进行设置，但是目前众多的 DDoS 攻击采用的是常用的一些合法协议，比如 HTTP 协议，这种情况下，路由器就无法对这样的流量进行过滤。同时，如果 DDoS 攻击采用地址欺骗的技术伪造数据包，那么路由器也无法对这种攻击进行有效防范。

另一种基于路由器的防护策略是采用 Unicast Reverse Path Forwarding (uRPF)在网络边界来阻断伪造源地址 IP 的攻击，但是对于今天的 DDoS 攻击而言，这种方法也不能奏效，其根本原因就在于 uRPF 的基本原理是路由器通过判断出口流量的源地址，如果不属于内部子网的则给予阻断。而攻击者完全可以伪造其所在子网的 IP 地址进行 DDoS 攻击，这样就完全可以绕过 uRPF 防护策略。除此之外，如果希望 uRPF 策略能够真正的发挥作用，还需要在每个潜在攻击源的前端路由器上配置 uRPF，但是要实现这种情况，现实中几乎不可能做到。

4.4 防火墙

防火墙几乎是最常用的安全产品，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，防火墙甚至成为 DDoS 攻击的目标而导致整个网络的拒绝服务。

首先是防火墙缺乏 DDoS 攻击检测的能力。通常，防火墙作为三层包转发设备部署在网络中，一方面在保护内部网络的同时，它也为内部需要提供外部 Internet 服务的设备提供了通路，如果 DDoS 攻击采用了这些服务器允许的合法协议对内部系统进行攻击，防火墙对此就无能为力，无法精确的从背景流量中区分出攻击流量。虽然有些防火墙内置了某些模块能够对攻击进行检测，但是这些检测机制一般都是基于特征规则，DDoS 攻击者只要对攻击数据包稍加变化，防火墙就无法应对，对 DDoS 攻击的检测必须依赖于行为模式的算法。

第二个原因就是传统防火墙计算能力的限制，传统的防火墙是以高强度的检查为代价，检查的强度越高，计算的代价越大。而 DDoS 攻击中的海量流量会造成防火墙性能急剧下降，不能有效地完成包转发的任务。

防火墙的部署位置也影响了其防护 DDoS 攻击的能力。传统防火墙一般都是部署在网络入口位置，虽然某种意义上保护了网络内部的所有资源，但是其往往也成为 DDoS 攻击的目标，攻击者一旦发起 DDoS 攻击，往往造成网络性能的整体下降，导致用户正常请求被拒绝。

4.5 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 系统往往不能满足要求。

原因在于入侵检测系统虽然能够检测应用层的攻击，但是基本机制都是基于规则，需要对协议会话进行还原，但是目前 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进行基于特征的有效检测。虽然某些 IPS/IDS 系统本身也具备某些协议异常检测的能力，但这都需要安全专家手工配置才能真正生效，其实施成本和易用性极低。

IPS/IDS 系统设计之初就是作为一种基于特征的应用层攻击检测设备。而大量的传统 DDoS 攻击依旧主要以三层或是四层的协议异常为特点，这就注定了 IPS/IDS 技术不太可能作为 DDoS 的主要检测防护手段。

五. DDoS 防护的基本要求

5.1 优秀的 DDoS 防御能力必要条件

DDoS 防护一般包含两个方面：其一是针对不断发展的攻击形式，尤其是采用多种欺骗技术的技术，能够有效地进行检测；其二，也是最为重要的，就是如何降低对业务系统或者是网络的影响，从而保证业务系统的连续性和可用性。

完善的 DDoS 攻击防护应该从四个方面考虑：

- 能够从背景流量中精确的区分攻击流量；
- 降低攻击对服务的影响，而不仅仅是检测；
- 能够支持在各类网络入口点进行部署，包括性能和体系架构等方面；
- 系统具备很强的扩展性和良好的可靠性；

基于以上四点，抗拒绝服务攻击的设备应具有如下特性：

- 通过集成的检测和阻断机制对 DDoS 攻击实时响应；
- 采用基于行为模式的异常检测，从背景流量中识别攻击流量；
- 提供针对海量 DDoS 攻击的防护能力；
- 提供灵活的部署方式保护现有投资，避免单点故障或者增加额外投资；
- 对攻击流量进行智能处理，保证最大程度的可靠性和最低限度的投资；
- 降低对网络设备的依赖及对设备配置的修改；
- 尽量采用标准协议进行通讯，保证最大程度的互操作性和可靠性；

5.2 防护设计思想的演进

DDoS 防护的设计思想从最早的“堵塞”攻击流量发展到现在的“疏导”。而部署方式也从单一的串联模式，发展为旁路和串联相结合的方式，针对不同的用户、不同的环境，采用不同的部署方式。

串联模式适用于非运营商的用户，在出口带宽一般小于 1-2G 的情况下，采用专业抗 DDoS 串联部署，提供精细化的小流量检测能力，可以实时在线对 DDoS 进行清洗。

对于运营商或者大型网络，利用旁路部署技术，抗拒绝服务产品可以不必串联在原有网络中，除了减少故障点，而且由于大多数带宽不必实时通过抗拒绝服务产品，因此一个较小的抗 DDoS 清洗容量就可以适用于一个大带宽的网络中，有效的降低投入成本。旁路工作原理如下：

1. **攻击检测**：通过流量镜像或 Netflow 方式检测到异常流量，判断是否有 DDoS 攻击发生。
2. **流量牵引**：确定有 DDoS 攻击后，通过路由技术的应用，将原来去往被攻击目标 IP 的流量牵引至旁路 DDoS 防护设备。被牵引的流量为攻击流量与正常流量的混合流量；
3. **攻击防护/流量净化**：DDoS 防护设备通过多层的攻击流量识别与净化功能，将 DDoS 攻击流量从混合流量中分离、过滤；
4. **流量注入**：经过防护设备净化之后的合法流量被重新注入回网络，到达目的 IP。此时从服务器看，DDoS 攻击已经被抑止，服务恢复正常。

采用旁路部署，具有以下优势：

5. 提供按需防护，即仅对可疑流量进行牵引，而通往其它目的地的流量将不受任何影响、按正常路径进行转发。网络正常的业务和性能将不受影响。
6. 可实现全网范围的防护，而不局限在网络的入口或者服务器前端进行串联防护。
7. 可避免网络单点故障，设备自身问题不会影响正常业务流量的转发。
8. 提供海量清洗，以应对带宽耗尽型的海量攻击，从而增强网络可靠性。
9. 支持远程牵引，根据防护需要、可以灵活“转移”远程流量。
10. 通过多流量净化中心的部署，提供异地/不同区域的冗余防护。

六. 绿盟抗拒绝服务系统

针对目前流行的 DDoS 攻击，包括未知的攻击形式，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各种类型的攻击流量，NSFOCUS ADS 可以迅速对攻击流量进行过滤或旁路，保证正常流量的通过。产品可以在多种网络环境下轻松部署，不仅能够避免单点故障的发生，同时也能保证网络的整体性能和可靠性。

6.1 三位一体的解决方案

绿盟科技推出了三位一体的异常流量清洗解决方案，可满足电信运营商对大型 Anti-DDoS 系统“可管理、可运营”的需求。该解决方案由异常流量检测系统（NSFOCUS NTA）、异常流量净化系统（NSFOCUS ADS）及管理和取证系统（NSFOCUS ADS-M）组成。解决方案由三类组件产品构成：

- **NSFOCUS ADS（绿盟抗拒绝服务攻击产品）**——作为绿盟流量清洗产品系列中的关键设备，其中 NSFOCUS ADS 提供了单台最大 10G 的 DDoS 线速防护能力，通过部署 NSFOCUS ADS 设备，可以对网络中的 DDoS 攻击流量进行清除，同时保证正常流量的通过。NSFOCUS ADS 设备可以通过旁路方式部署在网络中，同时利用万兆级别的 NSFOCUS ADS 组成的多台设备的集群，防护容量可以高达数十 G，提高整个系统抵御海量 DDoS 攻击的能力。
- **NSFOOCUS NTA（绿盟网络流量分析产品）**——绿盟流量清洗产品系列中第二类设备，称之为 NSFOCUS NTA，该设备主要应用于异常流量检测，需要和 NSFOCUS ADS 设

备配合工作。NSFOCUS NTA 设备可以应用 Netflow 等方式对流量数据进行采集，并对采集到的数据进行深入分析。一旦发现异常的网络流量，NSFOCUS NTA 会根据预先由系统管理员定义的方式触发 NOC（Network Operation Center）控制台报警或自动联动异常流量净化系统进行流量的牵引和净化。

- **NSFOCUS ADS-M（绿盟抗拒绝服务攻击综合管理产品）**——绿盟流量清洗产品系列中第三类设备，称之为 NSFOCUS ADS-M，负责收集来源于不同网络位置的多个 NSFOCUS ADS 设备的状态数据，进行关联分析和处理；基于防护群组、流量群组等逻辑对象进行高效的业务用户分组防护管理，并分别提供类型丰富的报表；对于网络不同节点的防护/监控产品进行集中的配置管理和权限分配；为攻击溯源提供抓包取证的功能。除此之外，NSFOCUS ADS-M 更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。

6.2 部署方式

绿盟科技的抗拒绝服务解决方案采用了业内先进的智能检测算法，对 DDoS 攻击进行专业的判断和识别，并进一步实时清除攻击流量。无论中小企业，还是数据中心，或是电信运营商网络，绿盟科技都提供相应环境下的抗拒绝服务的应用方式。

6.2.1 串行部署方式

针对少量服务器或出口带宽较小的企业内部网，绿盟抗拒绝服务产品提供串行部署方式，通过 ADS 设备透明地“串联”在网络入口端，对 DDoS 攻击进行检测、分析和阻断。部署拓扑图如下所示：

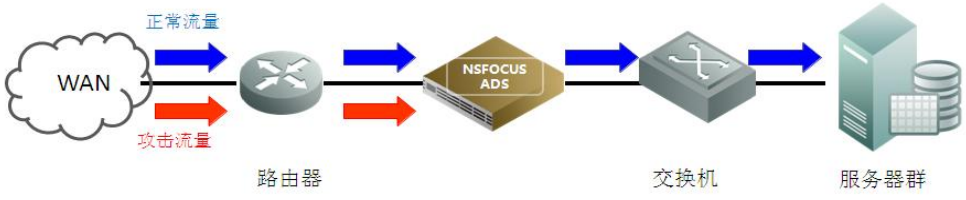

图 6.1 ADS 的串行部署方式

6.2.2 旁路部署方式

针对 IDC、ICP 或运营商关键业务系统，绿盟抗拒绝服务系统提供了基于流量牵引技术的旁路部署方式。通常，流量监测设备 NTA 部署在网络任意位置，ADS 设备“旁路”部署在网络入口。NTA 设备主要对网络入口的流量提供监控功能，及时检测 DDoS 攻击的类型和来源。当发现 DDoS 攻击发生时，NTA 设备会及时通知 ADS 设备，随后由 ADS 设备启动流量牵引机制，从路由器或交换机处分流可疑流量至 ADS 设备，在完成 DDoS 攻击的过滤后，ADS 再将“干净”的流量注入回网络当中。在这个过程中 ADS-M 系列的管理系统参与整体协调和记录管理。

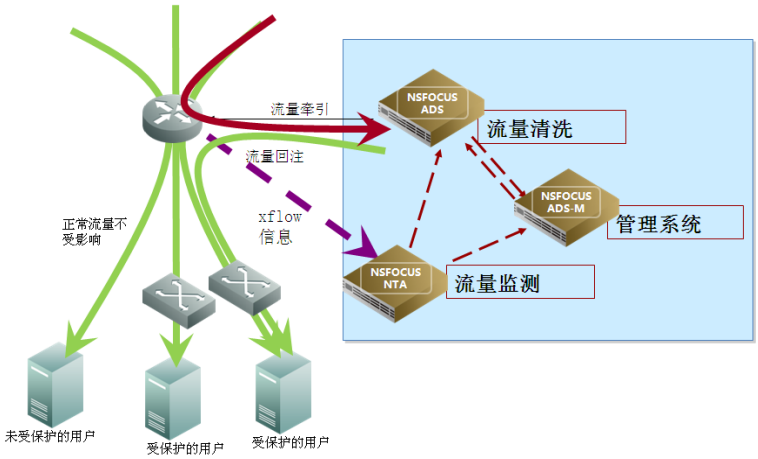

图 6.2　ADS 产品的旁路部署方式

针对大型 IDC、城域网或骨干网，当发生海量 DDoS 攻击时，绿盟抗拒绝服务产品还能够提供集群部署的方式。在旁路集群部署中，若干台 ADS 设备并联在网络中，在某台 ADS 设备接收到NTA 设备的攻击告警后，会启动流量牵引机制，将可疑流量均衡分配到若干台 ADS 上进行流量过滤。

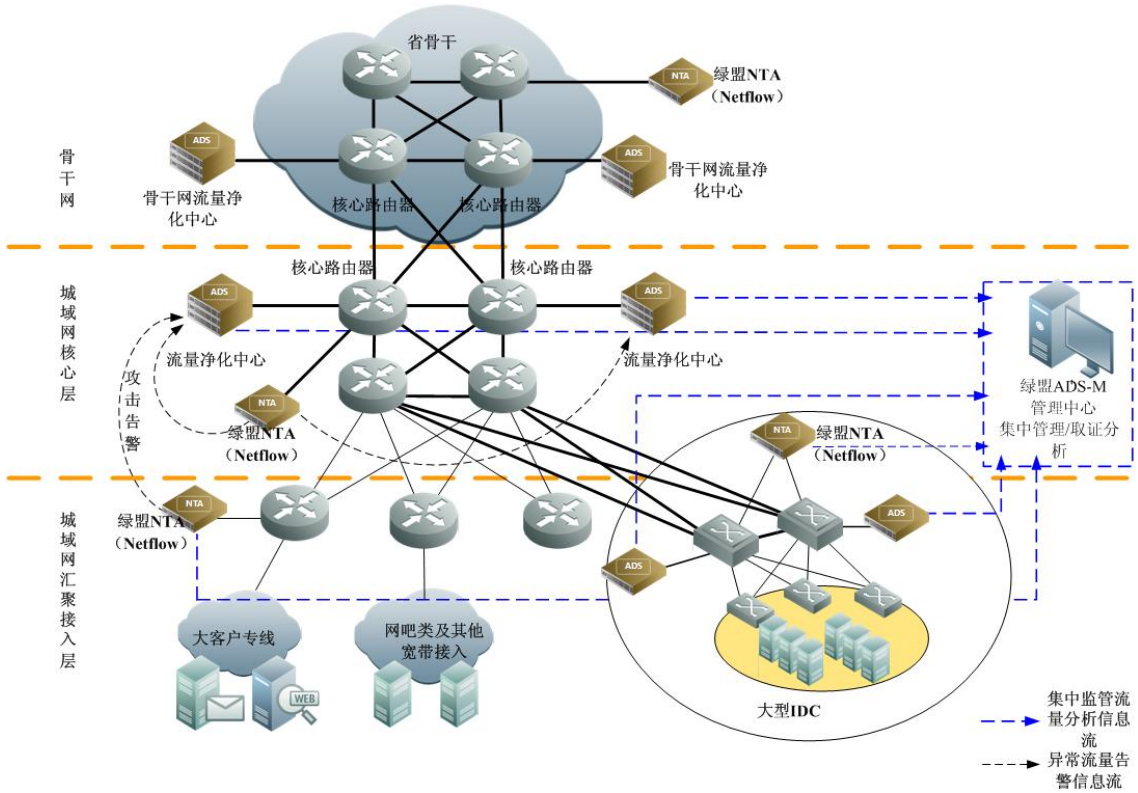

图 6.3　运营商级三位一体分层部署方式

6.3 核心原理

绿盟抗拒绝服务产品基于嵌入式系统设计，在系统核心实现了防御拒绝服务攻击的算法，创造性地将算法实现在协议栈的最底层，避免了 TCP/UDP/IP 等高层系统网络堆栈的处理，使整个运算代价大大降低，并结合特有硬件加速运算，因此系统效率极高。该方案的核心技术架构如图 6.4 所示。

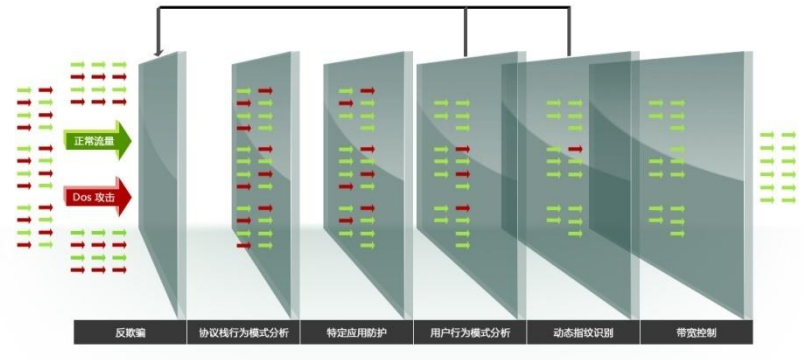

图 6.4　绿盟抗拒绝服务系统核心架构

反欺骗——绿盟 Anti-DoS 技术将会对数据包源地址和端口的正确性进行验证，同时还对流量在统计和分析的基础上提供针对性的反向探测。

协议栈行为模式分析——根据协议包类型判断其是否符合 RFC 规定，若发现异常，则立即启动统计分析机制；随后针对不同的协议，采用绿盟专有的协议栈行为模式分析算法决定是否对数据包进行过滤、限制或放行。

特定应用防护——ADS 产品还会根据某些特殊协议类型，诸如 DNS、HTTP、VOIP SIP 等，启用分析模式算法机制，进一步对不同协议类型的 DDoS 攻击进行防护。

用户行为模式分析——网络上的真实业务流量往往含有大量的背景噪声，这体现了网络流量的随机性；而攻击者或攻击程序，为了提高攻击的效率，往往采用较为固定的负载进行攻击。ADS 产品对用户的行为模式进行统计、跟踪和分析，分辨出真实业务浏览，并对攻击流量进行带宽限制和信誉惩罚。

动态指纹识别——作为一种通用算法，指纹识别和协议无关，绿盟 Anti-DoS 技术采用滑动窗口对数据包负载的特定字节范围进行统计，采用模式识别算法计算攻击包的特征。对匹配指纹特征的攻击包进行带宽限制和信誉惩罚。

带宽控制——对经过系统净化的流量进行整形输出，减轻对下游网络系统的压力。

6.4 系统特性

6.4.1 精准的攻击流量识别

绿盟抗拒绝服务系统应用了自主研发的抗拒绝服务攻击算法，在对网络数据报文进行概率统计的基础上，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）进行识别，从而准确地区分出恶意的 DDoS 报文和正常访问的网络数据报文。另一方面，产品采用的攻击检测和识别的算法效率非常之高，可以承受各类大流量 DDoS 的攻击，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。

6.4.2 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类基于网络层、混合型、连接耗尽型等的拒绝服务攻击，如 SYN Flood、UDP Flood、UDP DNS

Query Flood、(M)Stream Flood、ICMP Flood、 ACK Flood/ DrDoS 等，系统还可针对 HTTP Get Flood 攻击、游戏服务攻击、音视频服务攻击等危害更大的应用层拒绝服务攻击进行有效防护。

NSFOCUS ADS 系统提供了流量限制特性，用于应对突发的流量异常变化。系统还提供了访问控制列表（ACL）功能，可以让管理员直接设置黑白名单，简化对一些特定应用的控制难度。另外，深层包检查规则允许管理员根据攻击包的源/目的 IP，源/目的协议端口，以及协议类型或 Tcp Flag/ICMP Type/ICMP Code 等特征字节定义模版，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，对用户加以区分，并对不同的用户组提供细粒度的防护策略。

由于当前黑客技术发展越来越迅速，所以新的 DDoS 攻击技术也日新月益。绿盟科技拥有一支强大的安全技术研究队伍，专职于安全攻击及防护技术的研究，能够及时跟踪并发现互联网上新出现的 DDoS 攻击类型。基于绿盟 Anti-DoS 系统本身很强的扩展性，当新的攻击类型出现时，绿盟抗拒绝服务攻击系统能够在一周之内迅速升级，以保证客户网络在新的攻击之下的安全性。

6.4.3 海量的攻击防护性能

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及 NP+ASIC 硬件构架。单台设备最高可具有 10G 流量的线速分析和 DDoS 攻击防护能力。以最具代表性的 64 字节 SYN Flood 为例，NSFOCUS ADS 6000 可以承受 1,480 万 PPS 的攻击流量。多台 ADS 集群后，可以使得整体防护集群的容量和处理性能进一步提升。系统可以依据攻击的目的、流量、类型等多种因素进行流量牵引，拥有对更大规模、更复杂的 DDoS 攻击防御的能力。即使电信运营商或者大型企业在面临最严重的 DDoS 攻击威胁时也能提供最佳的防护实践。

另一方面，基于保障全网可用性的思路，系统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，从而保证了网络服务的品质。

6.4.4 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、串联集群、旁路以及旁路集群等不同方式，不同的部署方式和对各类网络协议的支持使得 NSFOCUS ADS 系统能够适应各种复杂的网络环境，为独立服务器、中小企业或是大型企业，以及电信运营商网络提供代价最小的应用方案，便于系统的部署和管理。

针对大型 IDC、ICP 及运营商骨干网出口的旁路部署模型可实现针对防护对象的“按需防护”，在发现流量的可疑特征后，系统采用动态流量牵引技术将去往受保护区域或主机的流量的下一跳重定向到流量净化设备上，而不影响去往其它区域或主机的流量转发路径。当可疑流量经过防护设备的识别并剥离出有害数据流后，干净的流量将被注回原来的网络中并抵达原来的目的地。为了适应复杂的运营商和大型企业网络环境，并满足便于部署、对现网环境影响小等实际需求，系统提供了丰富的流量牵引和回注特性以便在现网中选择实施。

6.4.5 友好的系统/报表管理

配合 NSFOCUS ADS-M 系列管理设备进行旁路部署应用时，系统可以提供直观而便利的设备运行监控、策略配置、报表生成和抓包取证等管理：

分级分权管理特性，使得网络工程师、安全管理员和客户可以看到不同级别的实时统计信息和监控、报表内容。

攻击报表提供了对攻击事件、攻击类型、攻击特征、攻击来源等信息的详细记录，一方面便于管理员实时监控攻击发生情况，另一方面还可以提供历史信息，对攻击行为进行追踪与取证。

系统还提供了诸如流量监控报表、日志信息通告和攻击历史报表等工具，便于最终使用者根据攻击情况来实时调整防护策略。

利用 NSFOCUS ADS-M 系列的管理产品，可以对多台 NSFOCUS ADS 设备集中管理、集中监控、集中控制、集中维护。集中管理功能可以让用户同时查看和修改多台 NSFOCUS ADS 设备，并将修改结果统一下发。集中监控功能可以让用户同时查看多台 NSFOCUS ADS 设备上的流量和运行状态。集中控制功能可以同时下达远程启动和抓包取证命令。多台 NSFOCUS ADS 设备的配置文件和流量统计数据、告警信息都可以集中存贮在 NSFOCUS ADS 管理平台上以便集中维护。

6.4.6 独特的增值业务管理

结合 NSFOCUS ADS-M 系列的管理产品，系统可提供特有的运营维护和自服务系统的增值服务平台，从而获取服务收益。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，而大客户可通过登录本系统开放的自服务界面，查看自己的实时网络流量、应用协议分布情况、攻击防护等关键业务信息。该平台，一方面提高了大客户对其系统安全状况的感知度；另一方面提升客户服务质量和内涵。

6.5 专业的攻击支持经验

基于绿盟科技自2002年以来抗拒绝服务商用产品多年的商用案例和服务支持积累的丰富经验，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，不仅帮助客户建立坚固的防御系统、提供防御支撑，还帮助客户建立起专业的攻击防御团队。

七. 结论

随着 DDoS 攻击工具不断的普遍和强大，Internet 上的安全隐患越来越多，以及客户业务系统对网络依赖程度的增高，可以预见的是 DDoS 攻击事件数量会持续增长，而攻击规模也会更大，损失严重程度也会更高。由于这些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。

为了弥补目前安全设备（防火墙、入侵检测等）对 DDoS 攻击防护能力的不足，我们需要一种新的工具用于保护业务系统不受 DDoS 攻击的影响。这种工具不仅仅能够检测目前复杂的 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。这类工具相对于目前常见的安全产品，必须具备更细粒度的攻击检测和分析机制。对于运营商来说，通过在网络骨干出口及 IDC 出口的部署，这类工具还可为运营商创造一种新的安全增值服务提供平台支撑。

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。