NSFOCUS

黑洞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 Internent 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。

本文内容将包含如下部分：

- DDoS 威胁的发展趋势以及攻击案例介绍
- 为什么传统安全设备无法防御 DDoS 攻击
- 对 DDoS 攻击防护所必须考虑的一些因素

◆ 绿盟科技的抗拒绝服务攻击整体解决方案

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。

2.1 攻击影响

成功的 DDoS 攻击所带来的损失是巨大的。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。

2.2 攻击分析

那么 DDoS 攻击究竟如何工作呢？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 攻击主要分为以下两种类型：

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、ICPM 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。

2.3 发展趋势

DDoS 攻击有两个发展趋势：其一是黑客不断采用更加复杂的欺骗技术，用于躲避各类防护设备检测；其二是 DDoS 攻击更多地采用了合法协议构造攻击，比如利用某些游戏服务的验证协议等。这些技术的使用造成 DDoS 攻击更加隐蔽，也更具有破坏性。尤其是那些利用了合法应用协议和服务的 DDoS 攻击，非常难于识别和防护，而采用传统包过滤或限流量机制的防护设备只能更好的帮助攻击者完成 DDoS 攻击。

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——电子商务网站经常是黑客实施 DDoS 攻击的对象，其在 DDoS 防护方面的投资非常有必要。如果一个电子商务网站遭受了 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 攻击如果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 入侵检测

目前 IDS 系统是最广泛的攻击检测工具，但是在面临 DDoS 攻击时，IDS 系统往往不能满足要求。

原因其一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 IDS 系统很难对这些攻击有效检测。虽然某些 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。

原因之二就在于 IDS 系统一般对攻击只进行检测，但是无法提供阻断的功能。IDS 系统需要的是特定攻击流检测之后实时的阻断能力，这样才能真正意义上减缓 DDoS 对于网络服务的影响。

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 DDoS 攻击主要以三层或是四层的协议异常为其特点，这就注定了 IDS 技术不太可能作为 DDoS 的检测或是防护手段。

五. DDoS 防护的基本要求

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；

六. 绿盟科技抗拒绝服务系统

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——黑洞（Collapsar）。通过及时发现背景流量中各种类型的攻击流量，黑洞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 产品功能

6.1.1 攻击检测和防护

“黑洞”系列抗拒绝服务产品应用了自主研发的抗拒绝服务攻击算法，对 SYN Flood、UDP Flood、UDP DNS Query Flood、(M)Stream Flood、ICMP Flood、HTTP Get Flood 以及连接耗尽这些常见的攻击行为能够有效识别，并通过集成的机制实时对这些攻击流量进行阻断。

6.1.2 海量 DDoS 防护

绿盟科技抗拒绝服务系统采用专用硬件架构，同时结合业界独创的攻击检测算法，所以能够针对海量 DDoS 进行防护。由于系统支持旁路部署方式，可对 DDoS 攻击流量进行牵引，同时通过部署若干台黑洞设备形成集群，更加增强了系统抵御巨大规模的 DDoS 攻击的能力，保证了正常流量的顺畅通过。

6.1.3 强大的部署能力

由于客户类型不同，所以抗拒绝服务所面临的网络环境也非常复杂，企业网、IDC、ICP 或是城域网等多种网络协议并存，给抗拒绝服务系统的部署带来了不同的挑战。绿盟科技的抗拒绝服务系统具备了多种环境下的部署能力，支持多种网络协议，诸如 OSPF、RIP、BGPv4、VRRP、VLAN 等，加之其基于应用的负载均衡能力，帮助整个产品成为多种客户环境下抗拒绝服务攻击的首选。

6.1.4 丰富的管理功能

绿盟科技抗拒绝服务系统具备强大的设备管理能力，提供基于 Web 和串口的管理方式，支持本地或远程的升级。同时，其丰富的日志和审计功能也极大地增强了设备的可用性，不仅能够针对攻击进行实时监测，还能对攻击的历史日志进行方便的查询和统计分析，便于对攻击事件进行有效的跟踪和追查。

在集群部署环境下，还可以通过专用的集中管理设备 DataCenter 同时对黑洞产品进行集中管理和集中监控。

6.2 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 6.1 所示。

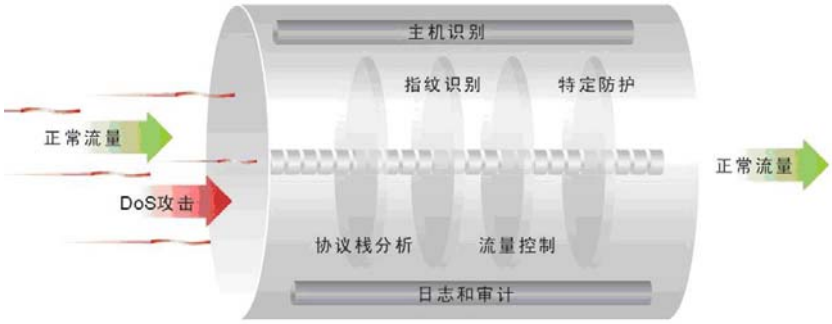

图 6.1 绿盟科技抗拒绝服务系统核心架构

攻击识别——绿盟 Anti-DoS 技术利用了多种技术手段对 DDoS 攻击是否发生进行有效的识别，除了采用先进的流量梯度算法对是否发生攻击进行判断外，还通过衡量承受能力的参照物的方式提高攻击发生判断的准确度。

协议分析——针对不同协议的数据包，绿盟 Anti-DoS 技术采用了不同的处理方法，比如 TCP 协议就采用了反向探测算法、指纹识别算法；而 UDP 或 ICMP 协议往往采用指纹识别算法进行攻击分析。

主机识别——如果 DoS 攻击受保护网段中的一台主机的某些端口，那么绿盟 Anti-DoS 技术将会保证同网段内其他主机或受攻击主机的其他端口的正常访问不会受到 DoS 攻击；

概率统计——绿盟 Anti-DoS 技术通过流量梯度算法对攻击进行判断，如果发现攻击，则进一步对数据包的特征进行统计，其内容包括目标 IP 地址、端口、包长、包内特征字以及校验和等。

反向探测——针对 TCP 协议，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。

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 技术通过采样自学习模式，取数据包的某些固定位置进行比较，进而对背景流量和攻击流量进行有效的区分。

6.3 组件产品

绿盟抗拒绝服务方案由三类组件产品构成：

- NSFocus Collapsar Defender （COLLAPSAR-D）
- NSFocus Collapsar Probe （COLLAPSAR-P）
- NSFocus Collapsar DataCenter （COLLAPSAR-DC）

COLLPSAR DEFENDER——作为黑洞产品系列中的关键设备，Collapsar Defender 提供了对 DDoS 攻击流量的防护能力，通过部署 Collaspar-D 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。Collaspar-D 设备可以通过串行、旁路两种方式部署在网络中，同时多台 Collaspar-D 设备可以形成集群，提高整个系统抵御海量 DDoS 攻击的能力。Collapsar-D 设备按照硬件平台的不同，可以划分为 Collapsar-200D、Collapsar-600D、Collapsar-1600D 和 Collapsar-2000D 四个产品系列，同时在每种产品系列中还根据被保护系统的数量分为 5IP，50IP 和无限 IP 三种类型。

Collapsar-200D/600D/1600D 这三种产品型号都是基于 X86 体系架构，Collapsar-2000D 基于全新的 NP 架构，虽然体系架构不同，但相应产品在功能上保持一致，主要区别体现在性能方面。

COLLAPSAR PROBE——黑洞产品系列中还有一类设备，称之为 Collapsar Probe，该设备主要应用于黑洞旁路部署方式下，需要和 Collapsar-D 设备配合工作。Collapsar-P 设备可以通过网络设备支持的流量采集协议（如 netflow 协议）对网络中的 DDoS 攻击流量进行监控和告警，在发现 DDoS 攻击流量后， Collapsar-P 设备可实时通知 Collapsar-D 设备，将相关可疑流量分流至 Collapsar-D 设备进行清除。

COLLAPSAR DataCenter——黑洞产品系列中第三类设备，称之为 Collapsar DataCenter，该设备主要应用于黑洞集群部署方式下，用来对多个黑洞设备进行集中管理并生成统计报表。Collapsar-DataCenter 从 Defender 设备和 Probe 设备上收集流量信息和告警信息，统一呈现在用户界面上。用户可以在 DataCenter 的集中管理界面上对多台黑洞设备修

改配置文件，并统一下发。在 DataCenter 上可以同时监控多台黑洞设备上的流量和运行状态，下发远程启动和抓包取证等命令。

6.4 部署方式

无论中小企业，还是数据中心，或是运营商网络，绿盟科技都提供不同环境下的抗拒绝服务攻击系统。

1. 串行部署方式

针对少量服务器或出口带宽较小的网络，绿盟科技抗拒绝服务产品提供串行部署方式，通过 Collapsar-D 设备“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：

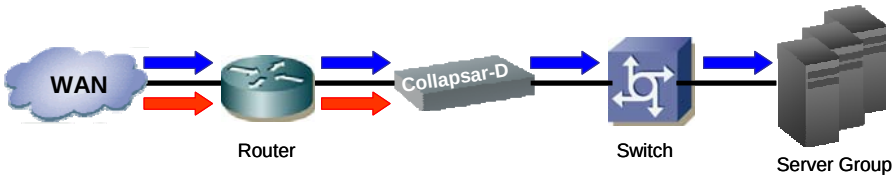

图 6.2 “黑洞”产品的串行部署方式

2. 旁路部署方式

针对 IDC、ICP 或关键业务系统，绿盟科技抗拒绝服务产品提供了旁路部署的方式。通常，Collapsar-P 设备部署在网络任意位置，Collapsar-D 设备“旁路”部署在网络入口下端。Collapsar-P 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，Collapsar-P 设备会及时通知 Collapsar-D 设备，随后由 Collapsar-D 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 Collapsar-D 设备，在完成 DDoS 攻击的过滤后，Collapsar-D 再将“干净”的流量注入网络中。

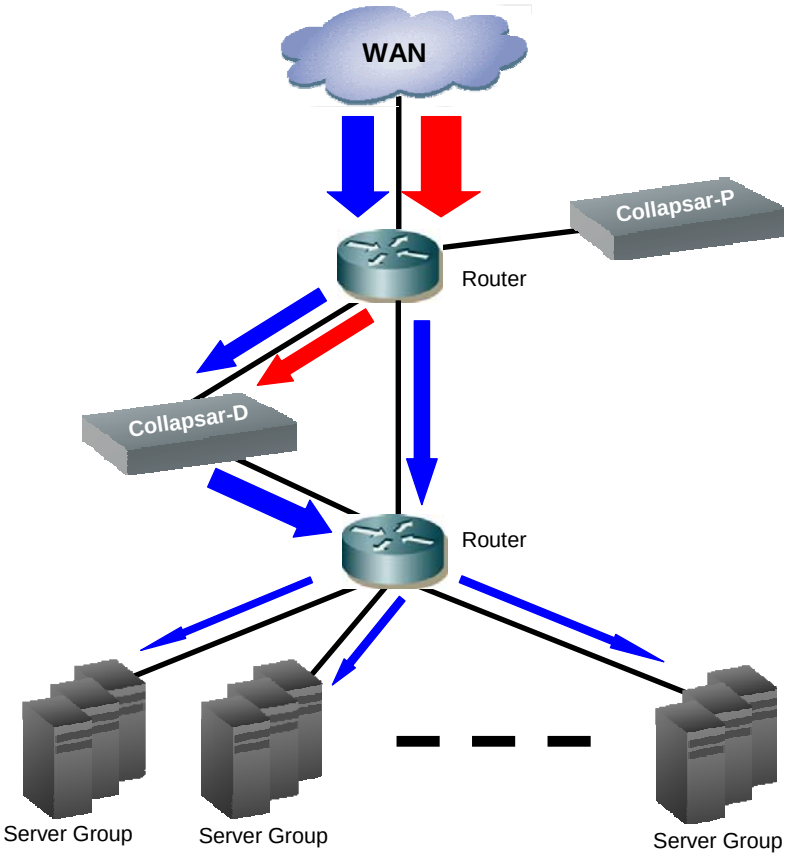

图 6.3 “黑洞”产品的旁路部署方式

3. 集群部署方式

针对大型 IDC、城域网或骨干网，当发生海量 DDoS 攻击时，绿盟科技抗拒绝服务产品还能够提供集群部署的方式。集群部署方式分为串联集群部署和旁路集群部署两种形式。分别如图 6.4 和图 6.5 所示：

在串联集群部署方式中，作为 Master 角色的 Collapsar-D 和其他若干台作为 Slave 角色的 Collapsar-D 设备“并联”在网络入口端。在攻击流量较小时，作为 Master 的 Collapsar-D 设备完成对 DDoS 攻击流量的异常检测和攻击清除的工作；当攻击流量增大时，Master 角色设备会及时启动流量牵引机制，分流攻击流量至 Slave 角色设备，以均衡系统负载，保证整个网络的正常运行。

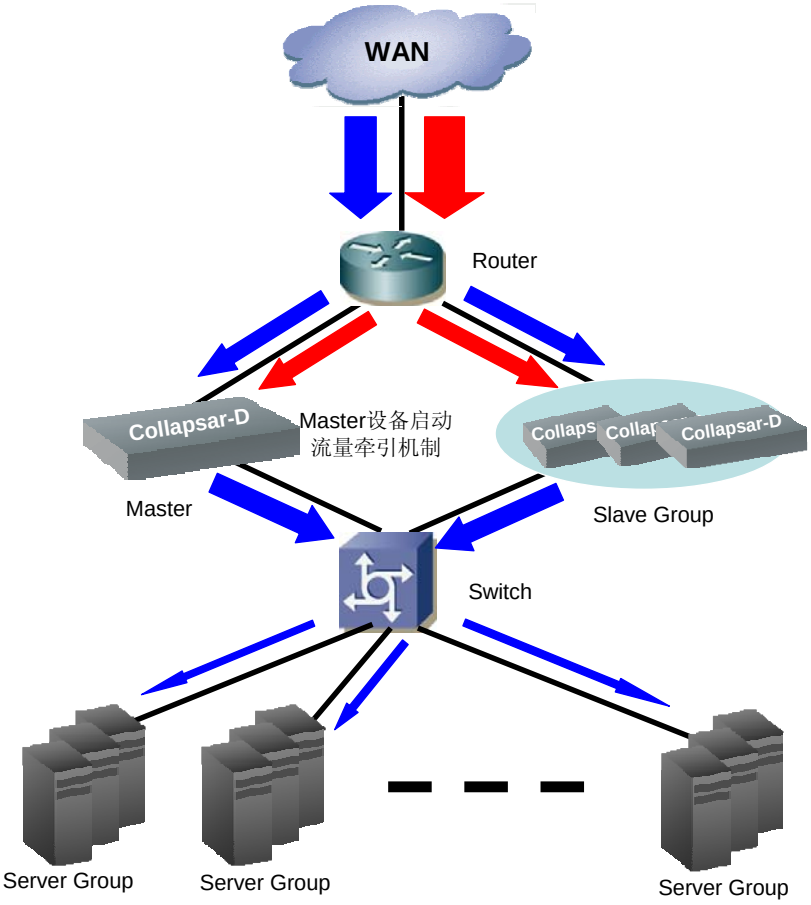

图 6.4　串联集群部署方式

在旁路集群部署中，若干台 Collapsar-D 设备并联在网络中，在某台 Collapsar-D 设备接收到 Collapsar-P 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 Collapsar-D 上进行流量过滤。

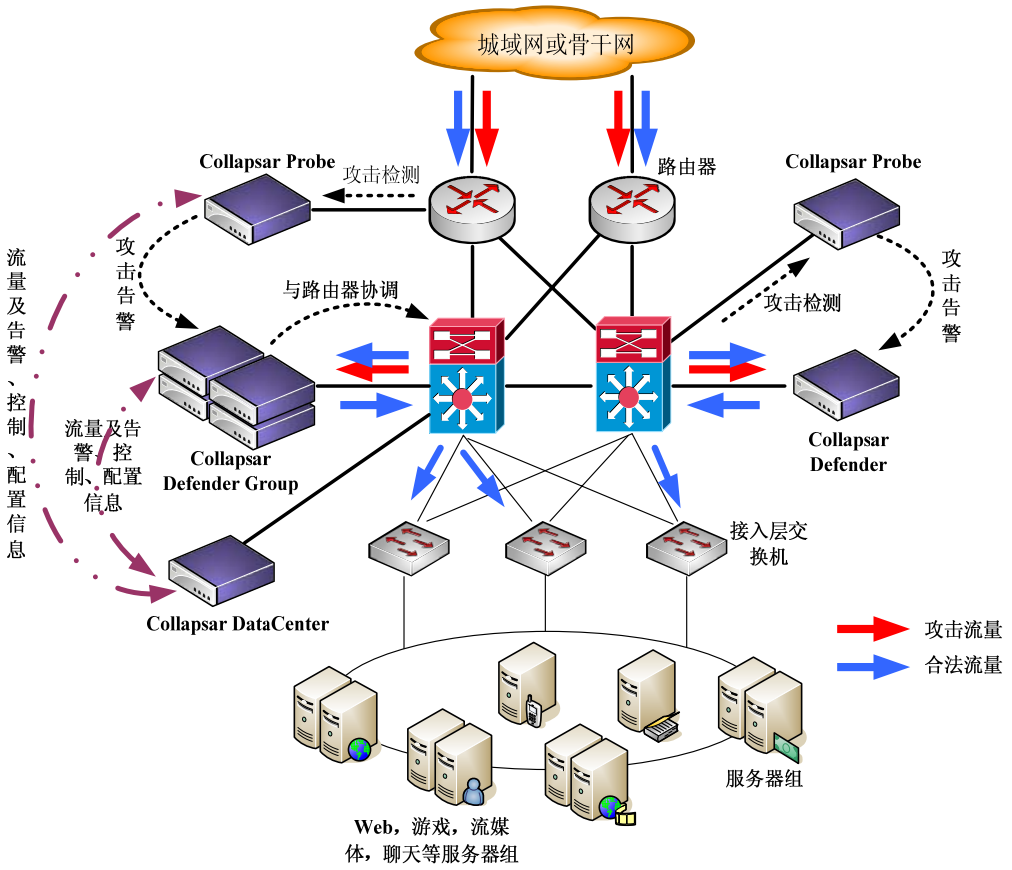

图 6.5　旁路集群部署方式

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。

绿盟科技的“黑洞”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。