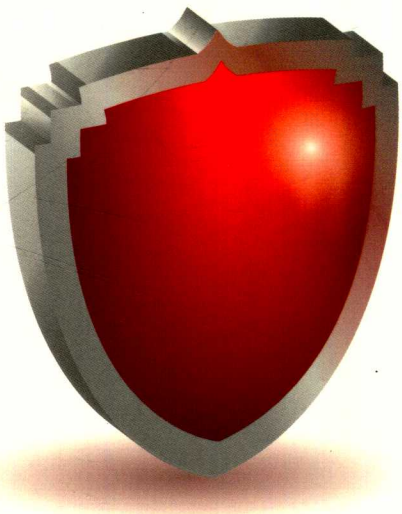
HUAWEI

“十三五”
国家重点图书出版规划项目
ICT认证系列丛书

华为技术认证

华为Anti-DDoS技术漫谈

韩 姣 主编



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

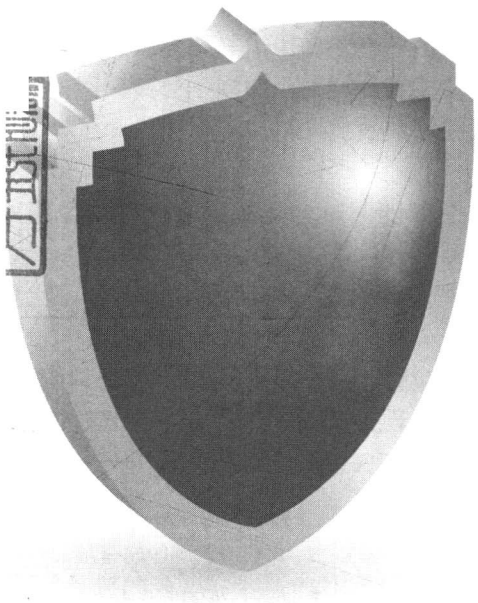
HUAWEI

“十三五”
国家重点图书出版规划项目
ICT认证系列丛书

华为技术认证

华为Anti-DDoS技术漫谈

韩 姣 主编



人民邮电出版社
北京

图书在版编目（CIP）数据

华为Anti-DDoS技术漫谈 / 韩姣主编. -- 北京 : 人民邮电出版社, 2018.8
（ICT认证系列丛书）
ISBN 978-7-115-48754-4

Ⅰ. ①华… Ⅱ. ①韩… Ⅲ. ①计算机网络－计算机安全 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第132783号

内 容 提 要

本书以现实网络中的热点攻击事件为入口，深入分析了各种 DDoS 攻防原理，并结合华为 Anti-DDoS 技术给出了详细解决方案。同时，作者总结多年维护和服务经验，将其作为配置要点呈献给读者，内容涵盖华为 Anti-DDoS 解决方案的组成、产品介绍、要点配置和实战案例等。

本书适合于服务或者渠道工程师，以及想学习或对 DDoS 攻防技术感兴趣的读者；同时，本书也可作为理论学习用书，帮助企业员工学习 Anti-DDoS 技术，帮助他们熟悉和理解华为 Anti-DDoS 的相关技术应用，提升工作效率。

◆ 主　　编　韩　姣
责任编辑　李　静
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：16　　2018 年 8 月第 1 版
字数：230 千字　　2018 年 8 月北京第 1 次印刷

定价：59.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

随着云计算的快速发展，各行各业的业务越来越多地向云化转变，DDoS 攻击已经成为互联网的首要威胁。越是竞争激烈的在线业务，被攻击的频度越高，攻击越复杂。随着 IoT 的快速发展，越来越多的 IoT 终端成为攻击端，由于各类开放服务器放大了攻击，攻击流量峰值也越来越高。目前，多矢量混合攻击更成为常态，在这种形势下，DDoS 攻防对抗技术难度一再被提升。另一方面，易遭受攻击的游戏、视频聊天等应用，大多采用私有协议，私有协议的广泛使用也进一步提升了防御技术的难度。

当 DDoS 防御作为一种 SaaS 服务企业客户时，防御系统不仅要求它能快速响应攻击，还要求它在过滤攻击时尽可能降低客户对访问体验的影响。因此，当前的 DDoS 防御技术远不是限速和 SYN Cookie 那么简单。一个好的防御系统应当有丰富多样的防御策略，即使对于同一类攻击，针对不同的业务系统也可提供不同的防御策略。但丰富灵活的防御策略也是把双刃剑，对懂这些技术的人而言，丰富灵活的防御策略提供了更多的运维手段；而对不懂这些技术的人来说，防御策略的配置太复杂，配置不当往往容易引起防御误判。配置复杂和运维成本高，已成为 DDoS 防御系统的代名词。因此，运维人员对攻防技术原理理解的深入程度直接决定了防御系统发挥作用的大小。而且 DDoS 防御方案的部署对网络有很强的依赖性，不同的网络需要不同的引流回注方案，如何实现 Anti-DDoS 方案在典型场景的快速部署，同样是安全运维或交付人员需要掌握的基础知识。

华为 16 年安全产品的成功经验，不仅奠定了华为在信息安全领域的地位，同样造就了一支精锐的安全产品研发团队。华为一贯重视产品资料，要求服务团队、客户甚至资料团队能按照资料说明，完成设备上线，这一近乎无情的苛刻要求无形中造就了华为安全产品资料团队人人都是安全专家。《华为 Anti-DDoS 技术漫谈》是继《华为防火墙技术漫谈》之后的华为安全产品资料团队推出的又一精品力作，是华为 Anti-DDoS 产品资料专家团队在华为 10 多年的 DDoS 攻防技术持续研究及 Anti-DDoS 产品研发经验的基础上，推出的一本难得的针对企业安全运维人员的 DDoS 攻防技术教科书。本书用幽默、形象的语言，结合现网几次著名攻击事件，深入浅出地揭开每一种攻击防御技术神秘的面纱，让安全运维人员理解攻击本质，掌握防御技术要点，同时结合典型防御场景，总结 Anti-DDoS 方案部署的要点，为从前期网络规划到后期部署、策略配置，提供了详细的配置举例说明。

最初，华为 Anti-DDoS 产品资料专家团队只是将每一种攻防技术内容在华为企业论坛上分期发表，没想到此项举措引起业内外人士广泛关注，好评如潮。因而团队萌发了将其装订成册的想法，让它以 DDoS 攻防专业技术书籍的形式呈现给华为的客户，期望华为 10 多年的 DDoS 攻防技术积累能直接使客户的网络更加安全。

华为 Anti-DDoS 产品经理　杨莉

前　言

适用读者对象

- 华为 Anti-DDoS 方案的用户

本书可作为华为 Anti-DDoS 用户的自学用书，帮助他们更快地熟悉 Anti-DDoS 方案，了解 Anti-DDoS 方案的关键防御原理，掌握 Anti-DDoS 方案部署技巧，找到解决问题的思路。

- ICT 从业人员

本书可作为工具用书，帮助 ICT 从业人员更快地熟悉 Anti-DDoS 方案，了解 Anti-DDoS 方案关键防御原理，掌握 Anti-DDoS 方案部署技巧，找到解决问题的思路。

本书可作为 HCIE 安全培训认证参考书，帮助 ICT 从业人员尽快通过华为认证，提升个人价值。

- 高校学生

本书可作为计算机通信等相关专业学生的自学参考书，帮助学生快速地熟悉 Anti-DDoS 防御技术，使他们在今后的职业生涯中有一个更好的起步。

- 对信息和网络技术感兴趣的爱好者

本书可作为学习信息和网络技术的参考书籍，使爱好者了解华为产品和技术的特点，掌握华为产品和技术的应用，并为其进一步的技术研究提供指导。

本书主要内容

全书共分为 7 篇，包括方案篇、DNS 篇、HTTP 篇、TCP 篇、UDP 篇、配置篇和实战篇。方案篇介绍了华为 Anti-DDoS 方案的组成、关键技术及应用场景；DNS 篇、HTTP 篇、TCP 篇、UDP 篇主要通过近几年的几次热点 DDoS 攻击案例，介绍不同协议类型的攻击防御原理；配置篇主要介绍引流和回注的配置要点，以及防御策略的关键配置；实战篇共包含 4 个实际案例，采用了先介绍场景，再介绍配置，一边介绍配置一边点评的写作方式，向读者传授理论应用于实践时的技巧。

第 1 篇　方案

本篇首先介绍了 DDoS 攻击的定义、特点和分类，然后介绍了华为 Anti-DDoS 方案关键技术以及华为云清系统；另外，还介绍了华为 Anti-DDoS 的硬件产品型号、部署方式和部署模式，这些是读者了解华为 Anti-DDoS 方案必须掌握的入门级概念。

第 2 篇　DNS

本篇首先以近几年轰动全国的视频软件断网事件为背景，介绍 DNS 攻击过程以及关键防御思路；然后系统解析 DNS 协议报文的格式和交互过程，并分别介绍华为 Anti-DDoS 方案如何防御 DNS Request Flood 攻击、DNS Reply Flood 攻击以及 DNS 缓存

投毒攻击的原理。

第 3 篇　HTTP

本篇首先通过跨站脚本攻击事件，介绍 HTTP 攻击过程及关键防御思路；然后系统解析 HTTP 请求报文和响应报文的格式和交互方式，并分别介绍华为 Anti-DDoS 方案如何防御 HTTP GET Flood、HTTP POST Flood 以及 HTTP 慢速攻击的原理。

第 4 篇　TCP

本篇首先分析近几年一次较大的 SYN Flood 攻击事件，并引出 SYN Flood 攻击的关键防御思路；然后详细分析 TCP 的报文格式及三次握手和四次握手交互过程，并分别介绍针对 SYN Flood、SYN-ACK Flood、ACK Flood、FIN/RST Flood 攻击的防御原理，以及防御 TCP 连接耗尽攻击和 TCP 异常报文攻击等常见的 TCP 类攻击的原理。

第 5 篇　UDP

本篇首先以近几年越来越猖獗的 NTP 反射放大攻击为背景，介绍反射放大攻击的攻击原理和防御思路；然后在深入分析 UDP 报文格式和报文特点的基础上，介绍华为 Anti-DDoS 方案针对 UDP Flood 攻击的防御关键技术及原理。

第 6 篇　配置

本篇介绍了华为 Anti-DDoS 方案在部署过程中常用的关键配置，包含引流和回注配置、引流回注配置结果验证，以及防御策略和阈值的配置要点等。

第 7 篇　实战

1. 城域网防护

本章介绍了华为 Anti-DDoS 方案部署在城域网出口，如何为城域网提供 DDoS 防护的规划和配置思路，以及结合城域网特点给出配置建议。

2. 小型数据中心防护

本章介绍了华为 Anti-DDoS 方案部署在小型数据中心出口，如何为单链路的数据中心提供 DDoS 防护的规划和配置思路，以及结合单链路数据中心特点给出配置建议。

3. 大型数据中心防护

本章介绍了华为 Anti-DDoS 方案部署在大型数据中心出口，如何为双链路的数据中心提供 DDoS 防护的规划和配置思路，以及结合双链路数据中心特点，从可靠性等多方面考虑给出配置建议。

4. 企业园区防护

本章介绍了华为 Anti-DDoS 方案部署在企业园区出口，如何为企业网提供 DDoS 防护的规划和配置思路，以及结合企业网的特点，从可靠性等多方面考虑给出配置建议。

鸣谢

本书由华为技术有限公司网络资料开发部安全网关资料组编写，经人民邮电出版社出版上市。在此期间，培训认证部的领导、资料部的领导、安全网关产品部的领导给予了很多的指导、支持和鼓励，人民邮电出版社的老师给予了严格、细致的审核。在此，诚挚感谢相关领导的扶持，感谢人民邮电出版社各位编辑老师以及本书各位编委的辛勤工作！

以下是本书主编介绍。

韩姣，具有 10 年华为 Anti-DDoS 产品资料开发经验，负责华为 Anti-DDoS 产品文档的写作。她曾作为《强叔侃强》作者之一，参与《华为防火墙技术漫谈》中攻击防范部分的写作。

以下是参与本书编写和技术审校人员名单。

策　　划：李学昭、金德胜

作　　者：韩姣、白　杰、金德胜、卢宏旺、房雪艳

美术编辑：申洪文

技术评审：杨　莉、吴　波、李　翔、潘永波、胡　伟、黄治登、袁　方、陶倚天、闫广辉、矫翠翠、沈海峰、朱旭德、吴永清、陈　佳、张凯程、邓福祥、姜　昊、付　佳、李　帅

参与本书编写和审稿的老师虽然有多年 ICT 从业经验，但因时间仓促，错漏之处在所难免，望读者不吝赐教，在此表示衷心的感谢。读者对于本书有任何意见和建议可以发送邮件至 hanjiao09@huawei.com，或直接登录华为企业论坛《华安解密》汇总帖反馈。

目　录

第1篇 方 案

1.1 什么是 DDoS 攻击

1.2 华为 Anti-DDoS 方案

1.3 华为云清洗方案与云清洗联盟

1.4 华为 Anti-DDoS 产品集

1.1 什么是 DDoS 攻击

1.1.1 DDoS 攻击的定义

DDoS 的前身是 DoS（Denial of Service，拒绝服务），最基本的 DoS 攻击是指攻击者利用大量合理的服务请求来占用过多的攻击目标的服务资源，从而使合法用户无法得到服务响应的过程。DoS 攻击一般采用一对一的方式，当攻击目标各项性能指标不高时（例如 CPU 速度低、内存小或者网络带宽小等），它的效果是明显的，如图 1-1 所示。

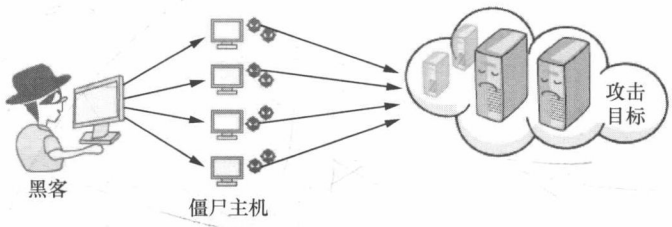


图 1-1 DDoS 攻击过程示意

随着计算机处理能力的不断提高，网络带宽迅速增长，以往的受攻击目标对这些恶意请求的“消化能力”增强了很多，这就使得 Dos 攻击的困难程度大大增加。一个攻击者无法使目标“拒绝服务”，那么攻击者会同时发起多个攻击，这时 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击也就应运而生了。DDoS 攻击是指攻击者控制僵尸网络中的大量僵尸主机向攻击目标发送大流量数据，耗尽攻击目标的系统资源，导致其无法正常地响应服务请求。

1.1.2 DDoS 攻击的特点

1. DDoS 攻击很容易被发起

DDoS 攻击的发起很容易，攻击者可以很方便地从互联网获取各类 DDoS 攻击工具，从而发起攻击。比较出名的发起 DDoS 的免费工具有卢瓦（LOIC）、HOIC（LOIC 升级版）、XOIC、Hulk、DAVOSET、黄金眼等。DDoS 攻击者还可以购买僵尸网络或者 DDoS 攻击服务，有的攻击者甚至可以借助正常的软件或网站发起攻击。

2. DDoS 攻击防御难度大

DDoS 攻击防御难度大，攻击会损害受害者的金钱、服务和信誉。报告显示，65% 以上的 DDoS 攻击每小时给受害企业造成的损失高达一万美元。例如 2016 年 10 月，针对美国 DNS 服务提供商 Dyn 公司的一系列 DDoS 攻击导致 Twitter、GitHub、BBC、华尔街日报、Xbox 官网、CNN、HBO Now、星巴克、纽约时报、The Verge、金融时报等大量站点无法正常访问，造成的损失不可估量。

1.1.3　DDoS 攻击的分类

DDoS 攻击根据攻击方式划分有以下三种类型：泛洪攻击（Flood）、畸形报文攻击（Malformation）和扫描探测类攻击（Scan&Probe）。

1. 泛洪攻击

泛洪攻击是一种攻击者通过僵尸网络、代理或直接向攻击目标发送大量伪装的服务请求报文，最终耗尽攻击目标的资源的攻击方式，如图 1-2 所示。攻击者发送的大量报文可以是 TCP 的 SYN 和 ACK 报文、UDP 报文、ICMP 报文、DNS 报文、HTTP/HTTPS 报文等。

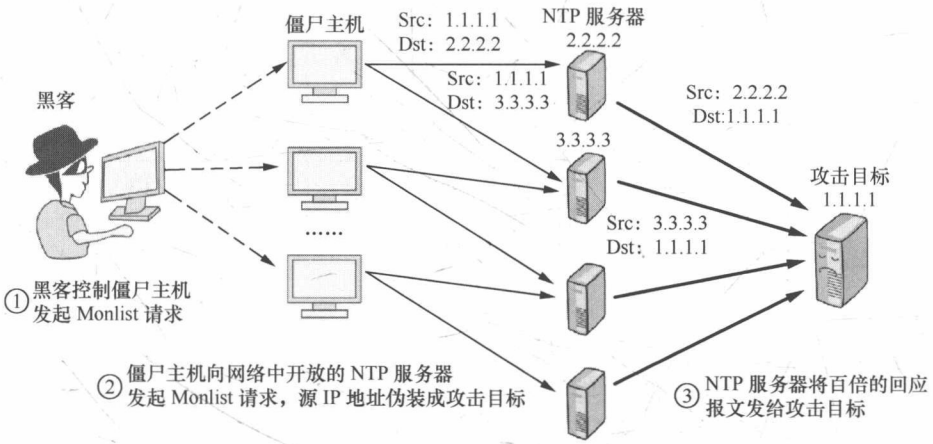


图 1-2　泛洪攻击

近年来，泛洪攻击又发展出了一种高级形式，即反射攻击。反射攻击并不是攻击者直接向攻击目标发起大量的服务请求，而是攻击者控制僵尸网络中的海量僵尸主机，将其伪装成攻击目标，然后这些僵尸主机以攻击目标的身份向网络中的服务器发起大量服务请求。网络中的服务器会响应大量的服务请求，并发送大量的应答报文给真正的攻击目标，从而造成真正的攻击目标性能耗尽。

反射攻击大多是由 UDP flood 变种而来的，它反射的是 UDP 报文，例如 NTP、DNS、SSDP、SMTP、Chargen 等。攻击者为什么会选中 UDP 报文呢？因为 UDP 的响应（Response）报文大小要大于请求（Request）报文，这样攻击者就实现了放大攻击流量的目的。

以 NTP 报文为例，NTP 的 Monlist 命令被用来查询最近所有和服务器通信的记录，服务器会返回最多 600 个通信记录，这样流量就被放大了数百倍。如果攻击者控制成千上万的僵尸主机，并将其伪装成攻击目标，并向 NTP 服务器发送大量此命令，那么反射给攻击目标的流量数量可想而知！

2. 畸形报文攻击

畸形或特殊报文攻击通常是指攻击者发送大量有缺陷或具有特殊控制作用的报文，从而造成主机或服务器在处理这类报文时造成系统崩溃的过程。常见的畸形报文攻击有

Smurf、Land、Fraggle、Teardrop、WinNuke 攻击等。特殊控制报文攻击包括超大 ICMP 报文、ICMP 重定向报文、ICMP 不可达报文和各种带选项的 IP 报文攻击。

3. 扫描探测类攻击

扫描探测类攻击是一种潜在的攻击行为，并不具备直接的破坏行为。它通常是指攻击者发动真正攻击前的网络探测行为，例如 IP 地址扫描和端口扫描等。

DDoS 攻击从网络层次的划分见表 1-1。

表 1-1 攻击分类

网络层次	DDoS 攻击
网络层	IP 地址扫描攻击 大部分特殊控制报文攻击 Teardrop 攻击 Smurf 攻击 IP 分片报文攻击 ICMP flood 攻击
传输层	SYN flood SYN-ACK flood ACK flood FIN/RST flood TCP 连接耗尽攻击 UDP flood（包括各种反射攻击） TCP/UDP 分片报文攻击 DNS flood DNS 缓存投毒 其余各种与 TCP、UDP 报文和端口相关的攻击
应用层	HTTP flood HTTP 慢速攻击 HTTPS flood SSL DDoS 攻击 SIP flood

1.1.4 DDoS 攻击分析

1. DDoS 攻击类型

通过以上描述，大家应该对 DDoS 攻击有了初步的了解。下面我们再为大家分析一下当前 DDoS 攻击的趋势，让大家对我们当今所处的网络环境中的 DDoS 攻击有一个初步的认识。

如图 1-3 所示，华为未然实验室现网络攻击事件统计数据显示，SYN flood、UDP flood（包括 UDP 类反射放大攻击）、HTTP get flood、DNS query flood 等依然是 DDoS 攻击的惯用手段。

（1）SYN flood

SYN flood 攻击是 DDoS 攻击中的经典方式，也是最古老和原始的 DDoS 攻击方式。在网络发展初期，SYN flood 攻击就是 DDoS 攻击的代名词。SYN flood 攻击具有攻击简