高防系统关键技术浅析

Analysis of Key Technologies of High Defense System

赵　通[1]，余思阳[2]，李长连[1]，杨　飞[1]，吴　涛[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Zhao Tong[1], Yu Siyang[2], Li Changlian[1], Yang Fei[1], Wu Tao[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China）

摘　要：

近年来，随着互联网应用的大规模普及，DDoS黑色产业链也日益壮大，大流量、多种类、高频次的DDoS攻击使网络服务提供者蒙受了巨大的损失。为了对抗DDoS攻击，高防系统被广泛使用。阐述了高防系统的概念、部署架构、引流方式及其核心技术和原理。针对实际工作中遇到的高防系统资源编排的痛点，综合考虑高防系统整体架构，总结提炼出一套高防系统资源弹性扩缩容的解决方案，为高防系统资源优化、相关功能开发提供一些思路。

关键词：

高防系统；弹性扩缩容；域名引流

doi：10.12045/j.issn.1007-3043.2022.09.018

文章编号：1007-3043（2022）09-0088-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

In recent years, with the large-scale popularization of Internet applications, the black industry chain of DDoS is also growing. DDoS attacks with large traffic, various types and high frequency have caused huge losses to network service providers. In order to fight against DDoS attacks, high defense systems are widely used. It expounds the concept, deployment architecture, drainage method and its core technologies and principles of the high defense system. Aiming at the pain points of high defense system resource scheduling encountered in actual work, it comprehensively considers the overall architecture of the high defense system, and summarizes and extracts a set of solutions for the elastic expansion and contraction of high defense system resources, which provides some ideas for resource optimization and related function development of high defense system.

Keywords：

High defense system; Elastic expansion and contraction; Domain name drainage

引用格式：赵通，余思阳，李长连，等. 高防系统关键技术浅析[J]. 邮电设计技术，2022（9）：88-92.

0　前言

DDoS攻击又称分布式拒绝服务攻击，是互联网中最常见的网络攻击手段之一，攻击者利用“肉鸡”对目标网站在较短的时间内发起大量请求，大规模消耗目标网站的主机资源，让它无法正常服务。目前网络游戏、互联网金融、电商、直播等行业是DDoS攻击的重灾区。

收稿日期：2022-07-27

DDoS攻击的低成本进一步降低了攻击门槛，卡巴斯基发布过一篇有关DDoS攻击成本分析的文章，据专家估计，使用1 000台基于云的僵尸网络进行DDoS攻击的成本约为每小时18美元。但对企业来说，针对DDoS攻击的防御费用总体成本往往高达数万甚至数百万美元。

除传统的4层DDoS攻击以外，当前互联网中Web应用越来越丰富，导致应用层攻击越来越严重。SQL注入、网页篡改、网页挂马等安全事件频繁发生。对于互联网Web应用来说，Web防护、CC攻击防护（借助

代理服务器生成指向受害主机的大量合法请求）也越来越重要。

高防系统就是为了解决DDoS攻击、CC攻击而设计开发的。

1 高防系统简介

当互联网服务器遭受大流量的DDoS攻击时，高防系统可以保护其应用服务持续可用。高防系统通过多种方式，调度流量到高防网络清洗，以抵御流量型和资源耗尽型DDoS攻击。

高防系统就是一个集合了DDoS攻击防护、CC攻击防护、多协议支持、隐藏源站等安全能力的综合性安全防护系统。此外，高防系统还可以为客户提供CDN服务，大幅降低客户服务器压力，以及客户访问的延迟。

1.1 高防系统的作用

高防系统通过反向代理源站，在攻击者和源站之间构建了一道安全闸，它可以解决下述问题。

1.1.1 避免源IP直接暴露公网

不论是通过域名引流，还是IP引流，高防系统都可以将源站地址进行隐藏，所有的攻击流量都会被引流到高防系统并进行清洗，大大减小源IP被攻击的可能性。

1.1.2 隐藏用户站点敏感信息

由于所有的业务流量都是通过高防系统转发到源站及客户，转发过程中可以对访问信息做筛选及更改，隐藏用户站点敏感信息，可以避免源站开发者因缺乏安全意识导致系统信息（建站程序、版本等信息等）泄露，提高源站安全性。

1.1.3 拦截非业务协议请求

由于所有的业务流量都是通过高防系统转发到源站及客户，在转发过程中可以对流量的协议做筛选，清洗掉异常协议的流量，只转发合法协议的流量到源站，在降低源站处理负担的同时，提高源站的安全性。

1.1.4 对接入系统进行4层及7层防护

基于抗DDoS清洗设备以及高防服务器，可以对接入系统进行4层到7层流量的清洗。

1.2 适用客户

娱乐（游戏）行业是DDoS攻击的重灾区，高防系统能保证游戏的可用性和持续性，提高用户体验，在商家活动、节日游戏等旺季时段提供防护。

满足金融行业的合规性要求，保证线上交易的实时性、安全稳定性。

满足国家政务云建设标准的安全需求，为重大会议、活动、敏感时期提供安全保障，确保民生服务正常可用，维护政府公信力。

为用户访问互联网提供防护，使业务正常不中断，在电商大促等活动时段提供防护功能。

保证企业站点服务持续可用，避免DDoS攻击造成经济和企业形象损失，降低维护费用，节省安全成本。

2 高防系统中使用的关键技术

2.1 整体架构

高防系统的整体架构图如图1所示，其主要由以下几个部分组成。

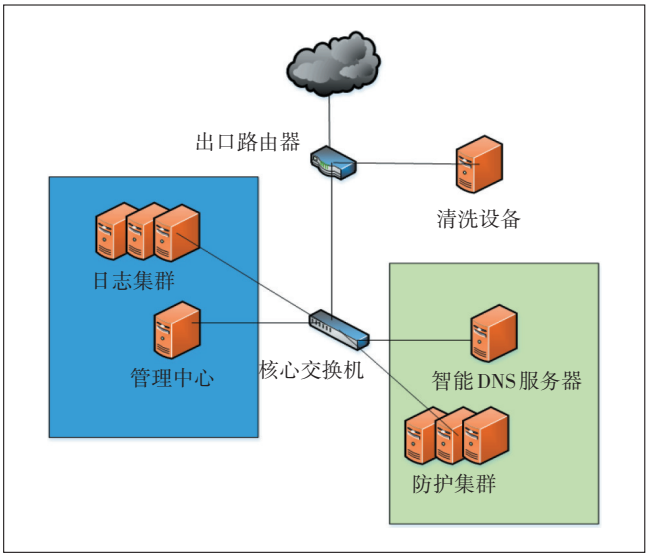

图1　整体架构图

2.1.1 清洗设备

通过对互联网访问公网IP的业务流量进行实时监测，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时为用户生成监控报表，清晰展示网络流量的安全状况。清洗设备主要用于防御4层DDoS攻击。

2.1.2 防护集群

防护用于代理客户业务的服务器，具有多核CPU、大内存、大带宽以及配套的安全软硬件，防护节点可以根据客户需求或者防御大流量DDoS攻击时进行动态调整。

高防系统的防护集群是连接用户及源站的桥梁，也是抵御DDoS攻击和CC攻击的有效屏障。为了处理海量访问和攻击流量，降低访问延迟，最大化利用硬件性能，防护集群一般是由物理机直接部署业务，而不是采用虚拟化部署的方式。

2.1.3 智能DNS服务器

DNS服务器用于配置CNAME记录（又称为别名记录，这种记录允许将多个域名映射到另外一个域名），它可以摆脱源站域名的限制，自由地实现将业务流量引流到防护集群。通过CNAME引流是目前主流的引流方式。

2.1.4 日志集群

日志集群保存了所有流经防护集群的流量日志，该日志保存了每个请求处理后的关键信息，用于发现异常流量时的回溯查询以及流量分析。

2.1.5 管理中心

管理中心用于向DNS服务器发送域名解析记录，管理防护集群的防护策略，管理清洗设备策略，根据日志集群数据生成运营报告，实时监控其他组件的运行状态等，它是高防系统的统一管理平台。

2.2 引流方式

2.2.1 域名CNAME引流

防护对象通过更改自己的域名记录，将域名记录（一般为A记录）更改为高防系统生成的CNAME记录，高防系统就可以通过更改CNAME记录指向的IP地址，控制访问防护对象的流量访问高防系统，高防系统收到用户业务流量，进行4层和7层流量清洗后转发给防护对象源站，防护对象源站的返回结果再由高防系统转发给用户。

CNAME引流过程如图2所示，在其中高防系统充当了部署在云端的防火墙以及防护对象的反向代理服务器。

2.2.2 对于IP地址类服务的引流

在生产环境中，并不是所有业务系统都配置有域名，对于直接使用IP访问的业务系统，可以通过配置高防系统，分配一个独立的高防IP地址，实现网站IP地址与高防IP地址资源的一对一配置，从而将访问流量牵引至高防平台系统。IP地址引流过程如图3所示。

2.3 防护节点的资源编排

由于高防系统出色的抗DDoS和抗CC攻击能力，吸引了很多容易受到攻击的业务系统接入。通常来

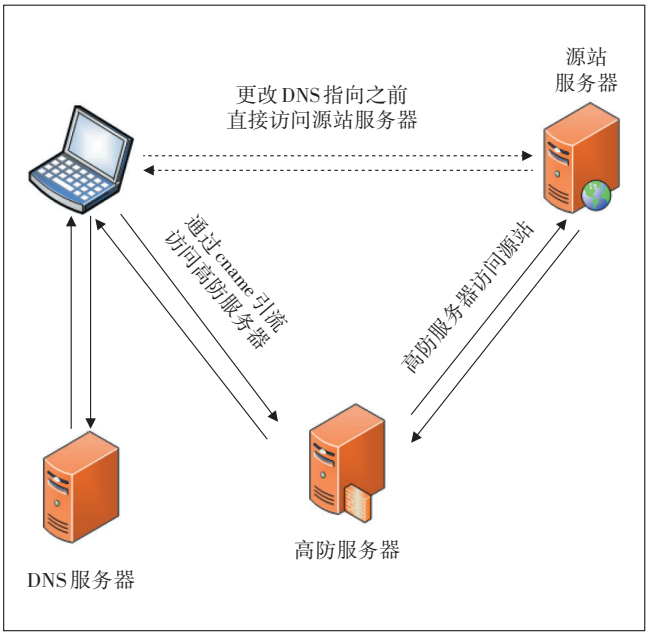

图2　CNAME引流过程

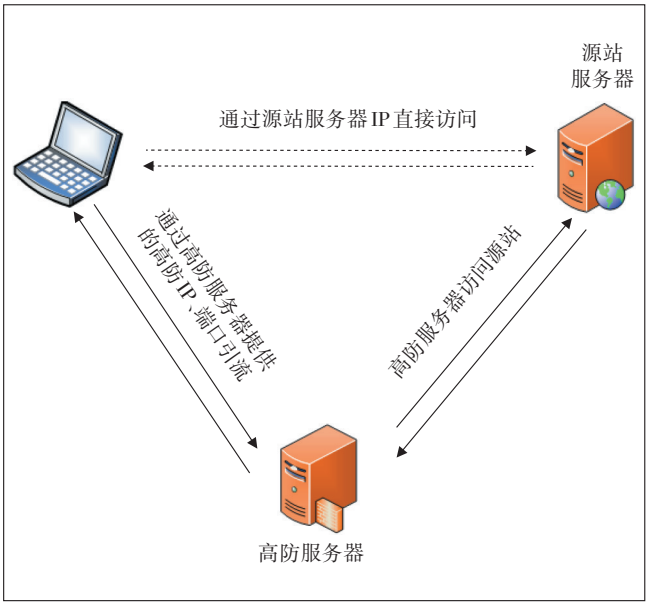

图3　IP地址引流

说，高防服务提供厂商会建设多个高性能的高防能力资源池，用来负载客户的业务流量。

但是在实际运营过程中，存在以下痛点。

a）资源池计算能力有限，提供过多的计算资源会导致浪费。

b）不同业务系统的需求不同。

c）同一个业务系统，在不同时间对资源的需求不同。

d）遇到攻击时，需要的资源和日常运营过程中的

需求不同。

e）业务供给需要手动调整，操作复杂，也无法保证实时性。

弹性扩缩容技术可以解决上述痛点。

自动化弹性扩缩容的技术可以将资源合理地分配给用户。简单来说，弹性扩缩容主要分为2个步骤：监测业务指标的波动和自动调整资源编排。

2.3.1 弹性扩缩容监测技术

监测业务指标的波动情况会涉及到弹性扩缩容监测技术，监测的主要原则如下。

a）对于业务有固定高峰和低谷的系统，可以使用定时功能，差异化的配置高峰时间段和低谷时间段的计算资源数量（高防服务器节点数量）。高防系统可以根据设定的时间，自动调整分配给该业务的资源数量。

b）如果业务量变动不规律，难以预测，可以通过云监控系统来监控使用中的资源的负载情况，自动执行扩缩容的策略。例如，设定CPU负载超过50%或者内存超过70%，或者QPS大于20 000时，自动扩容一台新的高防服务器。当CPU负载低于20%，或者内存使用率低于20%时，自动缩容一台高防服务器。

c）引入深度学习算法，经过一段时间的训练后，对每个业务系统建立业务流量趋势模型，提供给客户进行参考。

d）支持资源设置的上下限，可以避免在负载高的时候分配过多的资源，导致客户无法承受防护成本，也可以避免在资源分配过少时，无法实现高可用的情况。

e）支持异地资源弹性扩缩容，当异地资源故障隔离时，保障业务系统不会因为单点的故障导致业务中断。

f）不同的业务系统所关注的扩缩容指标不尽相同，高防系统应该支持定制化的监测手段，提供对应的API接口，并可以根据客户的需求自由创建扩缩容策略。

2.3.2 弹性扩缩容的过程

自动调整资源编排是弹性扩缩容的核心内容，下面分别对弹性扩容和弹性缩容的过程作出说明。

弹性扩容流程图如图4所示，具体过程如下。

a）用户在管理中心配置动态扩缩容的策略，可以根据流量的“潮汐”效应和单台服务器的负载上限，配置不同时间段使用的高防服务器的数量，同时可以启

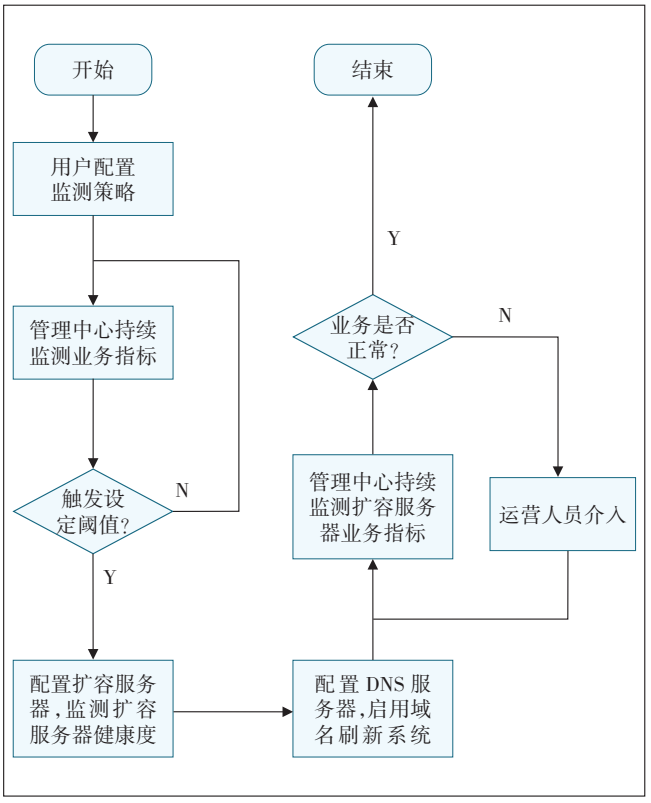

图4　弹性扩容流程图

用不同资源池的服务器，避免单点故障。

b）管理中心采集防护集群服务器的实时流量，负载情况，结合日志服务器数据，计算流量变化趋势。当监控指标触发用户设定的策略时，选定扩容服务器，触发弹性扩缩容动作。

c）触发弹性扩容时，管理中心首先检查新增防护服务器的配置，确认服务器的硬件、数据库和核心进程是否正常，并根据需要负载的业务的情况，同步业务配置数据（如防护规则等）、配置防火墙策略，自动配置上连交换机的ACL策略，确保只开放必要的端口。

d）管理中心向DNS服务器下发指令，添加扩容服务器IP地址到CNAME记录中。域名收敛时间一般为3~5 min，为了保证业务系统平稳地进行弹性扩容，引入DNS刷新系统。在修改CNAME记录后，高防系统会调用DNS刷新系统，强制刷新部署在全国各关键节点的DNS缓存服务器中该CNAME记录，可以将收敛时间缩短到0.5~2 min。

e）管理中心监测扩容服务器流量信息，超过3 min没有正常流量，会向运营人员发出告警，运营人员介入进行处理。

弹性缩容流程图如图5所示，具体过程如下。

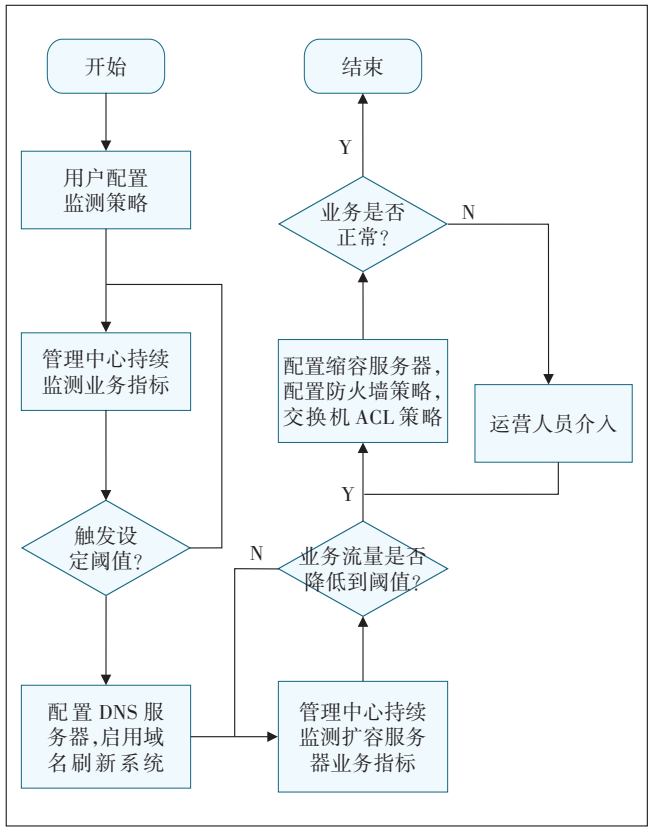

图5　弹性缩容流程图

a）用户配置扩缩容策略。

b）管理平台进行监控，当监控指标触发用户设定的策略时，根据策略选择需要缩容的服务器，触发缩容动作。

c）触发弹性缩容时，管理中心向DNS服务器下发指令，删除CNAME记录中缩容服务器IP地址。同时调用域名刷新系统，减小域名收敛时间。

d）管理中心持续监测缩容服务器中的业务流量，由于DNS缓存的原因，缩容服务器的对应业务流量并不会立刻缩小为0，流量会随着时间逐步减小，当流量减小到用户设定的阈值或者到达用户设定的延迟关闭时间后，管理中心会删除该服务器上的业务配置数据，在该服务器上配置防火墙策略，修改上连交换机的ACL策略。至此，缩容过程完成。

3 总结

本文首先对高防系统整体架构以及核心技术做了简要介绍，接着就高防系统在日常运营过程中的痛点做了深入分析，并且提出了自动化弹性扩缩容的具体目标和实现方法。

随着互联网服务重要性的提高，各行业对网络安全的要求会越来越高。高防系统是与DDoS攻击、CC攻击战斗的有力武器，高防系统的自动化运营也会越来越重要，通过弹性扩缩容技术，可以为客户和高防服务提供商节约成本，减小运营人员压力，提高服务质量，达到事半功倍的效果。

参考文献：

[1] 韩姣. 华为Anti-DDoS技术漫谈[M]. 北京：人民邮电出版社，2018.
[2] 陈国良，明仲，冯禹洪，等. 云计算工程[M]. 北京：人民邮电出版社，2016.
[3] 韩晶，赵锡成，黄文良. 运营商电商业务安全防护体系研究[J]. 邮电设计技术，2019(4)：35-39.
[4] 周婧莹，黎宇，潘俊斌，等. 基于DNS大数据分析的城域网安全防护应用[J]. 邮电设计技术，2018(1)：20-23.
[5] 王李乐，李明，汪浩，等. 云WAF技术系统研究[J]. 信息网络安全，2014(12)：1-6.
[6] 何丹，张悦. 高性能公有云WAF安全方案[J]. 计算机系统应用，2020，29(4)：144-149.
[7] 石祖文. WAF在云安全中的应用研究[C]//2013云计算架构师峰会论文集. 北京：51CTO传媒，2013：1-51.
[8] 杨玉兰. 基于DDoS高防IP系统预防DDoS攻击的原理[J]. 电脑知识与技术，2019，15(32)：57-58，71.
[9] 徐波，王建英. 服务器监控系统实现方案[J]. 电脑编程技巧与维护，2019(3)：43-45.
[10] 陈博豪，李凌. 基于采集任务运行信息的资源扩缩容方法的研究[J]. 广东通信技术，2021，41(11)：50-52，62.
[11] 王涛，陈鸿昶，程国振. 软件定义网络及安全防御技术研究[J]. 通信学报，2017，38(11)：133-160.
[12] 张永铮，肖军，云晓春，等. DDoS攻击检测和控制方法[J]. 软件学报，2012，23(8)：2058-2072.
[13] 王峰，张骁，许源，等. Web应用防火墙的国内现状与发展建议[J]. 中国信息安全，2016(12)：80-83.
[14] 何丹. 一种层次化多阈值DDoS防御模型研究[D]. 南京：南京邮电大学，2014.
[15] 王乐，王叶静，葛永兴，等. Web应用防火墙在高校信息安全中的应用[J]. 长春师范大学学报(自然科学版)，2020，39(2)：80-82，104.

作者简介：
赵通，毕业于中国农业大学，硕士，主要从事网络安全产品及安全技术方向的研究工作；余思阳，毕业于北京邮电大学，工程师，硕士，从事网络安全体系规划及产品研究工作；李长连，毕业于西北工业大学，高级工程师，主要从事网络安全技术方向的研究工作；杨飞，毕业于合肥学院，高级工程师，学士，主要从事网络安全技术的研究工作；吴涛，毕业于天津大学，学士，主要从事IT运维安全管理工作。