Journal of System Simulation

Volume 29 | Issue 11 Article 40

6-5-2020

Line-rate Defenses Approach against 10 Gbps DDoS Attacks

Su Cheng
1. 3 JiLing University of Tech., Najing 211106, China, China;;

Wentong Wang
2. JiangSu Senseit Electronics Tech. Co. Ltd, Wuxi 214135, China;;

Shibao Yang
1. 3 JiLing University of Tech., Najing 211106, China, China;;

Xv Linlin
3. Henuo Tech. Beijing Co. Ltd, Beijing 100055, China;;

See next page for additional authors

Line-rate Defenses Approach against 10 Gbps DDoS Attacks

Abstract

Abstract: Defenses approach against DDoS(Distributed Denial of Service) attacks is currently an important hot issues. We propose a new efficient defenses approach which adopts a detection system based on *metadata analysis* to identify the packages of DDoS attacks. The flow control rules are formed based on the summarized experience data. ACL (Access Control List) is applied through inline devices (firewalls and load balancers) or divider to limit rate, clean flow or drop package. *10Gbps bandwidth HTTP requests*, which contain malicious DDoS attacks packages, can be detected and cleaned completely in *line-rate speed*. *We especially summarize th traffic characteristics of main domestic DDoS attacks.*

Keywords

DDOS, HTTP GET flooding attacks, meta-data analysis, intelligence probe

Authors

Su Cheng, Wentong Wang, Shibao Yang, Xv Linlin, and Xinan Tang

Recommended Citation

Su Cheng, Wang Wentong, Yang Shibao, Xv Linlin, Tang Xinan. Line-rate Defenses Approach against 10 Gbps DDoS Attacks[J]. Journal of System Simulation, 2017, 29(11): 2898-2902.

第 29 卷第 11 期 系统仿真学报© Vol. 29 No. 11
2017 年 11 月 Journal of System Simulation Nov., 2017

万兆 DDoS 攻击的线速防护方法

苏成[1]，王稳同[2]，杨仕宝[1]，徐琳琳[3]，唐锡南[4]
（1.金陵科技学院，江苏 南京 211106；2. 江苏感创电子科技有限公司，江苏 无锡 214135；
3. 鹤诺科技（北京）有限公司，北京 100055；4.南京云利来软件科技有限公司，江苏 南京 211100）

摘要：DDoS(Distributed Denial of Service)攻击防护是目前的重要热点问题之一。我们提出了一套高效率的 DDoS 攻击防护方法，采用了一种基于元数据大数据分析的检测系统识别 DDoS 攻击包，总结经验数据而形成流量控制规则，通过分流器或者是内联设备(inline device，指内网防火墙 APS，ADS 或者负载均衡设备)采用了 ACL(访问控制列表)进行了速率限制、流量清洗或丢包处理。我们的方法还实现了万兆流量线速处理，并且通过了运行商在网测试。总结了国内常见的主要的 DDoS 攻击，特别是应用型的 DDoS 攻击的流量特征。

关键词：DDoS；HTTP GET 型洪水攻击；元数据分析；智能探针
中图分类号：TP391.7 文献标识码：A 文章编号：1004-731X (2017) 11-2898-05
DOI: 10.16182/j.issn1004731x.joss.201711040

Line-rate Defenses Approach against 10 Gbps DDoS Attacks

Su Cheng[1], *Wang Wentong*[2], *Yang Shibao*[1], *Xv Linlin*[3], *Tang Xinan*[4]
(1.3 JiLing University of Tech., Najing 211106, China, China; 2. JiangSu Senseit Electronics Tech. Co. Ltd, Wuxi 214135, China;
3.Henuo Tech. Beijing Co. Ltd, Beijing 100055, China; 4.Nanjing Yunlilai software tech. Co. Ltd, Nanjing 211100, China)

Abstract: Defenses approach against DDoS(Distributed Denial of Service) attacks is currently an important hot issues. We propose a new efficient defenses approach which adopts a detection system based on *metadata analysis* to identify the packages of DDoS attacks. The flow control rules are formed based on the summarized experience data. ACL (Access Control List) is applied through inline devices (firewalls and load balancers) or divider to limit rate, clean flow or drop package. *10Gbps bandwidth HTTP requests*, which contain malicious DDoS attacks packages, can be detected and cleaned completely in *line-rate speed*. *We especially summarize th traffic characteristics of main domestic DDoS attacks.*

Keywords: DDOS; HTTP GET flooding attacks; meta-data analysis; intelligence probe

引言

DDoS 攻击，就是黑客企图针对电商，在线游戏，DNS 服务等云服务提供商，以及大型企事业的数据中心网络和服务器发起海量的访问服务，导致服务器端拒绝服务[1]。根据我们在线检测统计，目前单个数据中心被攻击频率不低于 200 次/月。作为数据中心的第一道防线，负载均衡器或者防火墙的第一重任是保证请求快速被响应，往往来不及识别 DDoS 攻击。因此旁路部署检测设备，不影响关键业务往来，可将分析结果反馈给负载均衡器或防火墙，生成命令，拦截攻击源，组成 DDOS 攻击防护系统就成为技术研究热点。

收稿日期：2016-05-31 修回日期：2016-11-02；
基金项目：江苏省重点建设实验室数字媒体艺术创意与应用实验室资金项目；江苏高校品牌专业建设工程资助项目；
作者简介：苏成(通讯作者 1970-)，男，吉林，博士，研究员，研究方向为数字媒体和未来网络技术。

1 背景介绍

DDoS 攻击通常分为洪水型攻击和应用型攻击。我国常见的 DDoS 攻击种类包括：

洪水型攻击，例如 SYN Flood、UDP Flood，WINDOW size zero 等；针对 HTTP 协议的攻击包括：Hashdos 攻击，Slowloris 攻击，Slowpost 攻击，Get flooding 攻击等；针对 SSL 的攻击包括：Multiple request 攻击，Key renegotiation 攻击等。

本文的 DDoS 防护系统采用以下 3 步法：

(1) 采集元数据，检测攻击类型；

(2) 分析攻击源，设置流量控制规则；

(3) 根据需要采用内联设备 ACL 规则限制，或者采用分流器对 DDoS 流量迁移或者丢包处理。

我们采用了基于名为 TAP 的智能探针的增强版本作为检测系统，采用通用的多核体系结构并行处理算法，通过元数据分析实现了对国内主要类型 DDoS 攻击 10 G 带宽线速防护。

2 相关工作

HTTP GET 型洪水攻击是最常见的应用层攻击[2-3]，其次还有 DNS 反射型攻击，零日(ZERO-DAY)攻击等。近几年新报告的系统很多，例如 2008 年 Srivasta 等[4]提出了一种两步方法，首先在防火墙进行阻塞控制未授权客户访问，其次在服务器端对授权客户赋予优先级管理的方法，但这种方法的应用很受局限，只能处理小规模的低速 DDOS 攻击；2009 年 Ranjan 等[5]提出对于每个会话分配一个可疑测度的方法，然而由于计算量巨大导致大带宽下成本无法控制导致无法部署；2010 年 Jinghe Jin 等[6]提出了采用 NetFPGA 开发部署硬件，收集黑名单进行访问控制的方法，并实现了 GB 带宽之下的 HTTP GET 型洪水攻击。2011 年 S. Suriadi 等[7]提出了采用客户端提问的方法，对于一些低速的攻击比较有效，但对于有些攻击，例如 Key renegotiation 攻击，如果要求对每一次访问进行客户端提问，提问本身就会成为系统的瓶颈；2013 年 Junho 等[3]总结了以往基于模式识别和访问控制的方法，提出通过修改 NetFPGA 平台的硬件描述语言 Verilog 过滤 HTTP GET 数据包，使用哈希表高效提取 URL，形成攻击者的 IP 地址黑名单的方法；2014 年 Seung Yeob Nam 等[8]提出的白名单访问控制和基于忙时流控制的方法，对高速访问做出了有限的改进，但是白名单地址过多，大多数的网络设备不一定支持。这些算法大都没考虑大规模攻击的情况，没有考虑采用黑名单进行丢包或者限速处理。我们采用黑名单，而不是白名单解决这一问题，应该是聚焦于发起攻击的地址本身，把检测系统旁路部署在一个被保护的 10G 带宽网络上，通过大数据分析产生黑名单，高效率地解决 IP 地址聚合问题，形成数目很少的 ACL 规则，发送到内联设备或分流器去执行 DDOS 流量清洗。本文认为这是防御 DDoS 攻击的最佳策略。

3 问题描述

检测系统一般通过分光、端口镜像等方式旁路部署在被检测的网络中。实时防护的系统必须串接在网络中，放在被防护设备的前面，发现攻击以后实现流量限速或者做丢包处理。表 1 为防护系统组成。

表 1 防护系统组成

Tab. 1 Defence system component

网络层次	程序名称	程序功能
(L1)光纤连接		GB 或 10GB 多模光纤接口接收在线流量，并输出到防护设备
(L2/L3)	分流器及分流或丢包程序	按照系统设置的特征字对异常流量分流或者丢包
(L3/L4)	内联设备及配置 ACL 文件	按照系统设置的 IP 地址段或端口配置 ACL 规则，对异常流量限速
	与检测系统接口程序	把检测系统分析形成的特征字，IP 地址段和端口规则导入防护系统
(L7)以上通过管理端口	特征设置程序	(1) 输入和维护分流器的特征字或 IP 地址段；(2) 输入和维护内联设备的黑名单和规则

DOI: 10.16182/j.issn1004731x.joss.201711040

第 29 卷第 11 期 系统仿真学报 Vol. 29 No. 11
2017 年 11 月 Journal of System Simulation Nov., 2017

防护系统与位于本地的，旁路部署的 DDoS 检测系统位于同一个局域网中，通过软件接口把检测系统分析形成的特征字，IP 地址段和端口规则导入防护系统，防护系统设置程序通过管理端口访问和维护分流器和内联设备的文件。

防护系统中的分流器和内联设备以串接的方式，通过多模光纤接口接收可能随时发生攻击的流量，按照系统的实际需求采取不同的部署策略。如果采取限速措施，就串接内联设备，例如防火墙或者负载均衡设备；如果采取分流或者丢包处理，就串接一台有 Bypass 功能(旁路保护功能)的分流器，可以选择 GB 接口或者 10GB 接口。通过防护系统处理过的流量才可以通过被防护设备。

综上我们解决 HTTP GET 型洪水攻击的方法可概括为：

(1) 研究 HTTP GET 型洪水攻击 DDOS 流量特征；

(2) 按照设备支持的规则限制，对攻击流量限速、分流或丢包处理。

4 主要算法原理

下面介绍主要的算法原理。要注意的是，系统是由多台设备、分布其上的程序，配置文件组成，系统发挥作用需要每个部分的精细的考虑。

4.1 DDoS 流量特征和检测经验数据

HTTP DDoS 攻击有多种变化的形式。HTTP GET 型洪水攻击可以根据单客户端访问频率来检测，表 2 是我们判断主要 DDoS 攻击的经验数据。

4.2 防护系统设置程序

检测系统采用多核并行结构服务器，效率很高。检测系统做出 DDoS 攻击类型判断后，我们可以根据攻击的特点和前文描述的经验数据配置防护系统，形成过滤规则，为内联设备或者分流器使用。

4.3 基于规则的限速

在内联设备中 ACL 规则数目是有限的。基于规则的限速通常适用于最主要的 HTTP 洪水攻击，我们通过 IP 地址聚合，辅助内联设备对 DDOS 流量限速或者迁移、丢包处理。

表 2 主要 DDoS 攻击的流量特征
Tab. 2 Key flow feather of DDoS attack

攻击类型	识别原理
(L4) SYN Flood	统计一分钟内 SRCIP 处于半连接状态的 TCP 连接超过指定阀值(如 10 000)包括以下三种：
Tsunami SYN-Flood	(1) SYN 包包长在 950—1 080 之间
DNS Flood	(2) 类似暴风影音 DNS 劫持式的 SYN 攻击(特征：SRCIP 分布广泛，DSTIP 瞬间连接和流量很大)
TCP/UDP Flood	(3) 普通 64 字节 SYN 攻击
WINDOW size zero	统计一分钟内 SRCIP 的出现 Window-size 为 0 的次数超过指定阀值(如 3 000)
HTTP Get Flood	统计一分钟内 SRCIP 的 HTTP Get 请求的个数超过指定阀值(如 10 000)
Hashdos	统计 HTTP 请求中 Hash Key 的个数，超过指定阀值(如 80)
Slowloris	统计 HTTP 请求中 Header 的个数，超过指定阀值(如 15)且 Header 平均长度小于阀值(如 128 字节)
Slowpost	统计 HTTP 请求中 Body 的个数，超过指定阀值(如 15)且 Postdata 平均长度小于阀值(如 128 字节)
SSL Flood	统计一分钟内 SRCIP 的目的端口为 443 的 TCP 连接个数超过指定阀值(如 2 000)
SSL Alert (Multiple request)	统计一分钟内 SRCIP 的 SSL Alert 次数，超过指定阀值(如 1 000)
Key renegotiation	统计 SSL 会话过程中 Key 重协商的个数超过指定阀值(如 10)

4.4 基于流的分流或丢包

串联方式是指将分流器串联在网络链路中，配合 Bypass 设备作为链路保护，成为网络系统中的一个节点。串联的应用模式有 2 种：

(1) 浅串指串接业务数据流都直接在分流器中进行处理，后台服务器仅仅对分流器进行控制实现串联；

(2) 深串指串接业务数据流通过分流器交由后台处理，并由后台通过分流器返还给原线路。

基于流的分流或者丢包，可以根据 4.1 节中的经验数据，也可以提取 DDOS 流量的特征数字或者特征字，进行丢包处理。

5 实验结果及应用

5.1 测试平台

实验检测系统和防护系统都采用 Sandy Bridge (E5-2650)多核处理器，2.0GHz 主频，每内核有 64KB L1 缓存和 256KB L2-缓存，8 核 20MB L3 缓存，Intel 82599 网卡，操作系统为 64 位 Linux 2.6.32 内核。实验检测系统和防护系统通过局域网与分流器的管理口连接，检测系统通过 10GB SFP 接口与分流器相连，分流器以浅串方式连接在网络中。

5.2 DDoS 攻击检测判定的典型案例

以下为某电信运营商网管中心使用本文所述的检测系统判定 DDoS 攻击的真实案例：

1.在日常页面巡视中发现在 2014-12-12T 12:00:00 左右，部署在某机房的检测设备监控流量剧增，从正常运行的 4.6Gbps 猛增到 8Gbps 左右。且新增流量以入方向流量为主。时间持续约 5min。

2.按照总流量降序排列结果，可以看到在所选时段内，服务器 A 总流量最大，达到 200.79GB。

3.查看服务器 A 的流量历史曲线，其它时间正常，只有在 12:00---12:05 之间，该服务器的流量达到峰值，服务器连接数达到了 53 471 821，这一连接数已远远超过了服务正常的连接范围。显然是遭到了攻击。

4.查询该服务器地址目的端口发现连接行为集中在端口：7 104。

5.查看有关连接数页面情况。活跃的 TCP 连接数并没有显著提升。只有完成 3 次握手的连接，才会被计入到活跃连接。新建连接数也无大幅提升，但是关闭连接数从 50 K/s 骤升到了 500 K/s。查看结束状态，可以很明显的看到关闭连接的原因是由于超时关闭的。表明这是一次 scan 攻击。

6.通过该服务器地址的目的端口 7 104 查询源地址 TOPN，发现至少有 100 台来自欧洲，美国及亚洲，中国等地的服务器参与到这次 scan 攻击中。

5.3 互联网缓存设备防护

下面的测试在某运营商省网管中心核心数据机房进行。由于在省网核心节点到第三方运营商出口网关之间采用单臂连接方式部署了互联网缓存设备 Bluecoat CacheFlow 5000，其部署本意是在省市各级国产缓存设备没有缓存到的内容资源，通过国外不同技术体系的缓存设备再次缓存，实验证明缓存比高达 25%，这样就节约了出口带宽结算成本。部署几个月以后，由于 DDoS 攻击，缓存系统变得很不稳定。

实验如图 1 所示，防护系统清洗 DDoS 流量，分流器采用恒扬 FC1400 浅串方式连接。互联网缓存设备 Bluecoat 的原理是对出网的一条 TCP 访问，Bluecoat 立刻保持这条连接，如果本地没有相关内容，就向外网启动一条模拟的 TCP 访问，回传给出网的那条 TCP 访问。如果正常访问重复内容较多，就实现较显著的缓存效果，可是如果是 DDoS 攻击内容，特别是 64 K 以下的小包攻击，访问频繁内容又不同，就会增加巨大的计算量，造成系统不稳定。我们通过特征识别检测，配置相应的攻击特征使分流器自动丢包，缓存系统恢复了正常。

5.4 IDC 防护

图 1 的测试环境在某运营商省核心 IDC 机房。

由于存在昂贵的互联网出网流量结算成本，运营商省公司自建了 400 台服务器规模的 IDC 中心，用于引导内网移动和 PC 终端用户上网时，尽可能地把热点资源的流量在网内 IDC 完成。由于经常存在 DDoS 攻击行为，IDC 系统变得很不稳定，影响用户体验，经常产生投诉。

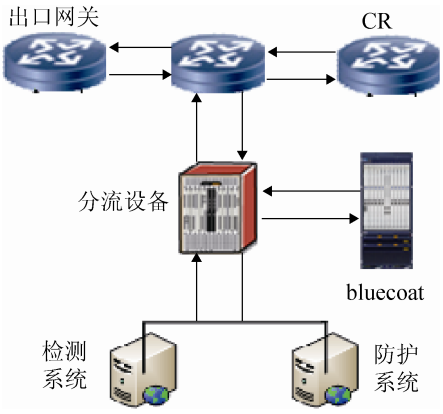

图 1 互联网缓存 DDoS 防护系统部署图
Fig. 1 Internet cache DDoS defence system sketch map

实验采用图 2 所示的防护系统清洗 DDoS 流量，分流器采用恒扬 FS9000，浅串方式，实现了 10G 流量线速处理，系统的峰值处理能力达到单机 1 000 万个并发会话，稳定运行 3 个月无故障。

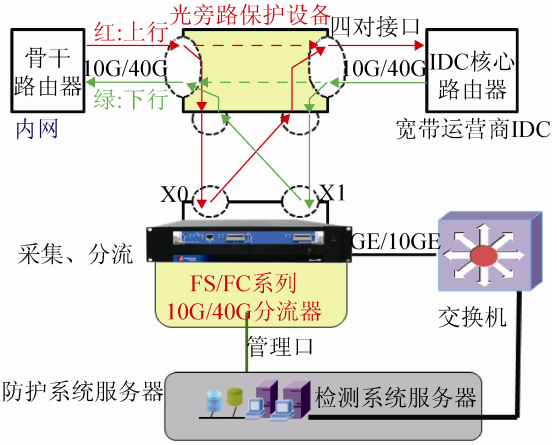

图 2 IDC DDoS 防护系统部署图
Fig. 2 IDC DDoS defence system sketch map

6 结论

实验表明：我们的防护系统与检测系统共同完成了 DDoS 攻击的检测和防护，可以采用旁路部署检测系统，串接带有 Bypass 功能的分流器分流或丢包，也可以配合其它内联设备采用 ACL 做流量控制，可以实现 GB 级和 10GB 级流量的线速防护，有效地实现了互联网缓存和 IDC 安全防护。目前在国内我们尚未见到同类性能的系统报道。

未来我们计划建立 40G 带宽的检测系统，进一步提高 CPU 和资源配置效率。

参考文献：

[1] Saman T Zargar, James Joshi, David Tipper. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks[C]//IEEE Communications Surveys & Tutorials, 2013.

[2] Internet K, Agency S. Study on the detection and mitigation algorithm for session consuming DDoS attacks on web service[R]. Technical report, Korea Internet and Security Agency, 2010.

[3] Suriadi S, Stebila D, Clark A, et al. Defending web services against denial of service attacks using client puzzle [C]//Proc. of the 9th International Conference on Web Services (ICWS'11), Washington DC, USA, 2011(7): 25-32.

[4] Srivatsa M, Iyengar A, Yin J. Mitigating application-level denial of service attacks on web servers: a client-transparent approach[C]. ACM Transactions on the Web, 2008, 2(3):1-15.

[5] Ranjan S, Swaminathan R, Uysal M, et al. DDoS-Shield: DDoS-resilient scheduling to counter application layer attacks[C]//IEEE/ACM Transactions on networking, 2009, 17(1): 26-39.

[6] Jinghe Jin, Nazarov Nodir, Chaetae Im, et al. Mitigating HTTP GET Flooding Attacks through Modified NetFPGA Reference Router[C]//First Asia NetFPGA Developers' Workshop, Daejeon, Korea, 2010.

[7] Suriadi S, Stebila D, Clark A, et al. Defending web services against denial of service attacks using client puzzle[C]//Proc. of the 9th International Conference on Web Services (ICWS'11), Washington DC, USA, IEEE, 2011: 25-32.

[8] Seung Yeob Nam, Sirojiddin Djuraev. Defending HTTP Web Servers against DDoS Attacks through Busy Period-based Attack Flow Detection[C]. KSII Transactions on Internet and Information Systems, 2014, 8(7): 2512-2531.