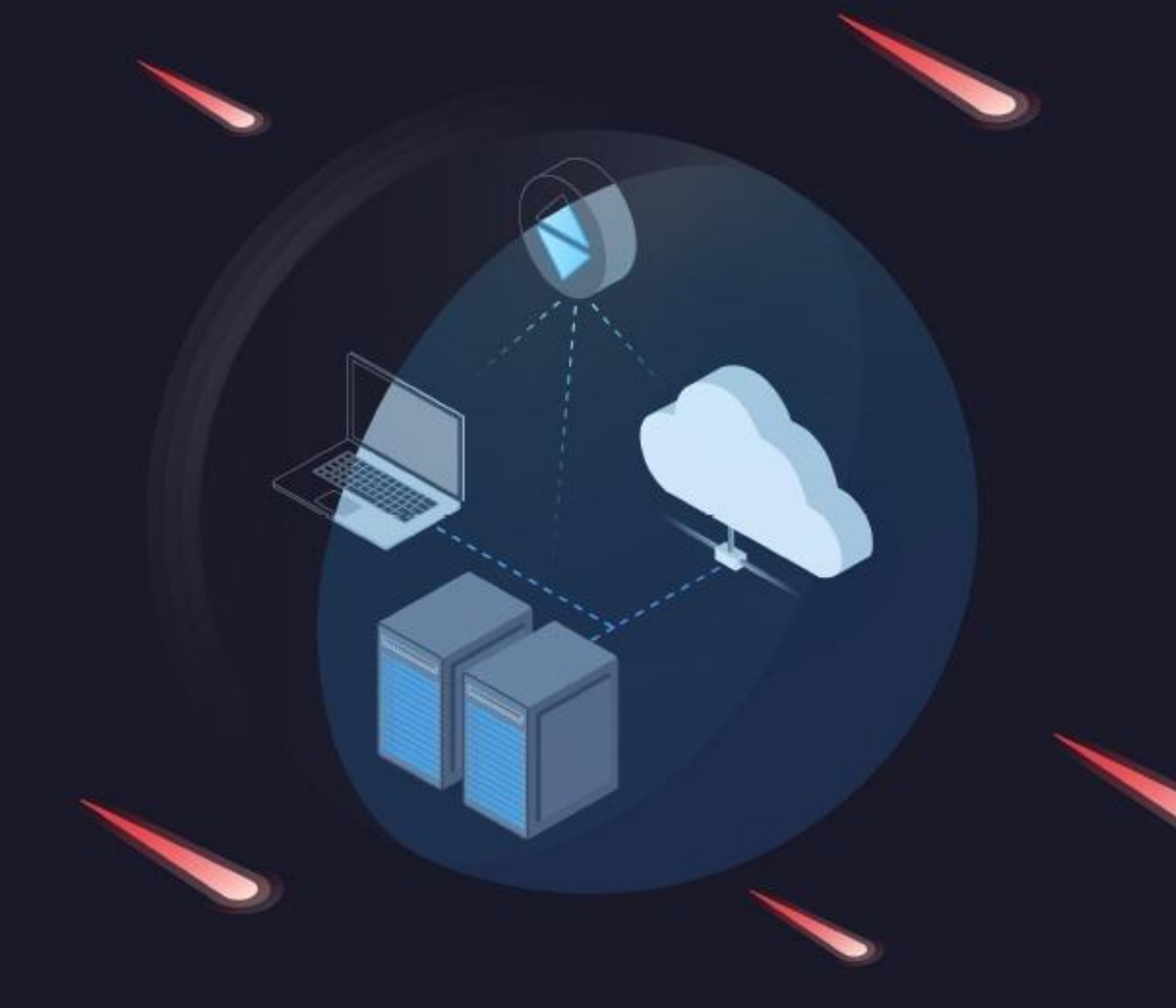
抗 DDoS 攻击

软件定义边界 SDP

作为分布式拒绝服务（DDoS）攻击的防御机制



致谢

主要作者：

Juanita Koilpillai

Jason Garbis

Michael Roza

Nya Murray

CSA 工作人员：

Shamun Mahmud

中文版翻译说明：

由云安全联盟大中华区（CSA GCR）秘书处组织翻译《软件定义边界作为分布式拒绝服务（DDoS）攻击的防御机制》(Software Defined Perimeter as a DDoS Prevention Mechanism)，云安全联盟大中华区专家翻译并审校。

翻译审校工作专家：（按字母顺序排序）

组长：陈本峰（云深互联）

组员：陈俊杰（安全狗）、靳明星（易安联）、余晓光（华为）、于继万（华为）、余强（中宇万通）、袁初成（缔安科技）、姚凯、刘洪森、王安宇、杨洋

CSA GCR 工作人员：

高健凯（CSA GCR 研究助理）

在此感谢以上参与翻译审校工作的专家及工作人员。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：

序言

最近，又一次对亚马逊 AWS 的严重 DDoS 分布式拒绝服务攻击被报道出来。这次攻击持续了一整天，AWS 的防护措施除了吸收大量的攻击流量之外，还误断了一些合法用户机构的访问查询流量，包括排除这些网址并停止它们的访问。平均来讲，这类 DDoS 攻击每个小时会给用户机构造成 2 万至 4 万美金的损失。

云安全联盟 CSA 的“Anti-DDoS: Software-Defined Perimeter as a DDoS Prevention Mechanism”《抗 DDoS 攻击：软件定义边界 SDP 作为分布式拒绝服务（DDoS）攻击的防御机制》的发布正好是一场及时雨，对防护 DDoS 攻击带来了更新颖与更有效的方法。CSA 的研究成果表明，SDP 软件定义边界可以有效地防护多种典型 DDoS 攻击手段，包括 HTTP Flood, TCP SYN, and UDP Reflection 等。产业界和学术界的一些安全实验室也验证了在拒绝服务攻击实验中，SDP 可以允许合法用户机构的访问流量通过，并通知上游路由器区分恶意流量包以迅速对合法网址开绿灯。

CSA 全球（创作）与大中华区（翻译）SDP 工作组的这篇文章为软件定义边界作为防 DDoS 攻击的新工具打开了天窗，希望读者们通过这篇文章能够认识到 SDP 对防御 DDoS 的作用,并在相关工作中加以应用。

李雨航 Yale Li

云安全联盟大中华区主席

目录

1 简介

1.1 DDoS 和 DoS 攻击定义

分布式拒绝服务(DDoS)攻击是一种大规模攻击。在这种攻击中，攻击者使用多个不同的源 IP 地址（通常有数千个）对单一目标进行同时攻击。目的是使（被攻击者的）服务（或网络）过载，使其不能提供正常服务。由于接收到的流量来源于许多不同的被劫持者，使用入口过滤或来源黑名单等简单技术来阻止攻击是不可能的。当（攻击）分散在如此众多的来源点时，区分合法用户流量和攻击流量变得非常困难。一些 DDoS 攻击包括伪造发送方 IP 地址（IP 地址欺骗），进一步提高了识别和防御攻击的难度[1]。

拒绝服务(DoS)攻击是一种来自单一来源的攻击，而上述的 DDoS 攻击是有许多来源的攻击。下图展示了这两种类型的攻击。

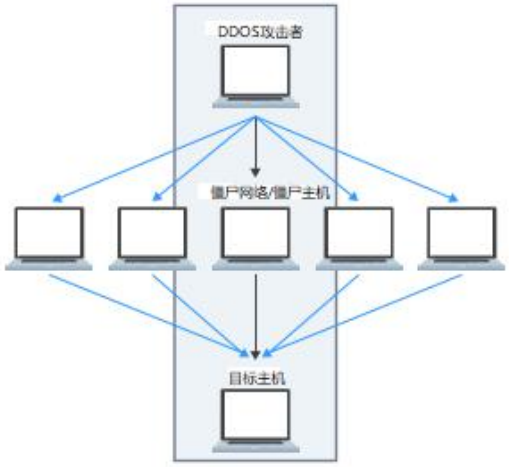


图 1：DoS 与 DDoS 攻击的区别

在本白皮书的其余部分，我们将只提及 DDoS 攻击，但其中的大量内容同样适用于 DoS 攻击。DDoS 的最终目的是压倒一个目标并阻止它向合法用户提供服务。DDoS 攻击通常实施于互联网上面向公众的服务，如 Web 服务器和 DNS 服务器。正如最近的调查所指出的那样，DDoS 当前是并将继续是一个安全问题:

- 依据【https://securelist.com/DDoS-report-q1-2019/90792】的报告内容，在 2019 年的第 1 季度和第 2 季度，“数据显示，所有 DDoS 攻击指标都上升了。攻击总数上升了 84%，持续的 DDoS 会话（超过 60 分钟）的数量刚好翻了一番”；
- 来自网站【https://www.darkreading.com/perimeter/

1 https://en.wikipedia.org/wiki/Denial-of-service_attack

- DDoS-for-hire-services-doubled-in-q1-/d/d-id/1335042】的文章指出，DDoS 出租服务在 2018 年第 4 季度到 2019 年第 2 季度翻了一番。

为了便于分析，我们将计算机服务分为两大类：

公共服务，如 DNS 服务、web 服务和内容分发网络（CDN）

这些服务必须在互联网上保持可自由访问，不需要身份识别、验证或授权。保护这些类型的服务免受 DDoS 攻击不是本白皮书的目标。

私有服务，如私有商用应用、员工或客户的工作门户、电子邮件服务器等

这些服务旨在提供给明确定义的受众。这些受众具有已知的身份，并可以在使用这些服务之前进行身份验证。这些私有服务是本白皮书的讨论重点，非常适合于使用软件定义边界（SDP）技术来保护其免受 DDoS 攻击。

对于上述两种类型的服务，（提供服务的）组织应当关注其网络服务提供商可提供的检测和缓解服务，因为许多 DDoS 攻击将影响网络提供商的网络接入服务，通常防御可以在网络的“上游”进行。

2 目标

本文的主要目标是通过展示 SDP 抵御几种常见攻击（包括 HTTP 泛洪、TCP SYN 和 UDP 反射）的效率和有效性，提高人们对 SDP 作为抵御 DDoS 攻击的工具的认识和理解。

3 阅读对象

本文档的主要目标读者是企业中担任安全、企业架构和法规遵从等角色的人员。这些利害关系人将在很大程度上负责其企业内 DDoS 防御解决方案的评估、设计、部署或运营。其次，解决方案提供商、服务提供商和技术供应商也将从阅读本文档中受益。

4 DDoS 攻击向量

DDoS 攻击向量大致分为资源消耗和带宽攻击两类，且可以根据其针对的 OSI 七层模型中对应层次进行再次分类，如下图所示。此外，还可以根据 TCP/IP 模型查看，两种模型的比较见附录 1 和 2。注意，TCP/IP 四层模型代表了现实世界中的网络当前是如何设置和操作的。OSI 代表了一种理想视图，且由于其更详细的分层，通常用于教学和解释目的，本文将使用 OSI 模型。

图中以蓝色高亮的层通常不是 DDoS 攻击的目标，不包括在我们关注的领域中。从剩下的层中，我们选择了 3 个以绿色高亮的攻击作为重点。

4.1 基于 OSI 和 TCP/IP 模型层的 DDoS 攻击向量

No.	OSI	TCP/IP	协议数据单元	说明	主要攻击焦点
7	应用层	应用层	数据	网络进程到应用程序	HTTP 泛洪攻击和 DNS 查询泛洪攻击
6	表示层		数据	数据表示与加密	TLS/SSL 攻击
5	会话层		数据	主机间通信	N/A
4	传输层	传输层	数据段	端对端连接及可靠性	SYN “TCP“ 泛洪攻击
3	网络层	互联网层	数据包	路径寻址	UDP 反射攻击
2	数据链路层	网络接入层	帧	物理寻址	N/A
1	物理层		比特	媒体、信号和二进制传输	N/A

来源：https://aws.amazon.com/shield/DDoS-attack-protection/

I. 应用层攻击

应用层 DDoS 攻击不如传输层和网络层攻击常见[2]，由于不依赖暴力攻击，通常都更复杂。与 4 层和 3 层攻击相比，这类攻击的流量要小些，但会集中攻击相对昂贵的应用资源部分（请求大量资源=资源枯竭），从而使真正的用户无法得到资源。这样做的例子包括：在第 7 层对登录页面或者昂贵的搜索 API 的 HTTP 洪水式请求[3]。

2 https://securelist.com/DDoS-report-q1-2019/90792/ Distribution of DDoS attacks by duration (hours), Q4 2018 & Q1 2019

3 https://aws.amazon.com/shield/DDoS-attack-protection/

1 HTTP Get 请求和 HTTP Post 请求

最为人所知的两个的资源损耗攻击是 HTTP Get 请求和 HTTP Post 请求攻击（参见 HTTP 洪泛攻击与 SDP 防御）。Get 请求可被用来获取数据，例如图像，Post 请求触发需要被（服务器）处理的动作。Get 请求和 Post 请求都可以由 HTTP 客户端（通常为 Web 浏览器）向 HTTP 服务器（通常为 Web 服务器）请求。就损耗服务器资源而言，Post 请求通常比 Get 请求更高效，因为其处理过程（比如需要数据库访问）更复杂。

近期成功针对亚马逊云（Amazon Cloud）、声田（Spotify）、推特（Twitter）等的 DDoS 攻击是一个很有启发性的事件，需要云安全设计者们认真对待。在介绍对 DDoS 攻击进行检测、分析和缓解的可扩展云防御方案的文章中（见引用），作者们介绍了目前最先进的云 DDoS 防御手段。对 DDoS 攻击者 IP 地址的检测，（能）产生有力的威慑，（从而）为保护云资源提供重要突破，而且已有部分厂商可以提供该项技术。互联网工程任务小组（IETF）在 RFC2827[5] 中建议了一种使用入方向流量过滤的方法，以禁止使用伪造 IP 地址的 DoS 攻击。这些 IP 地址通常从互联网服务提供商（ISP）聚集点传播出来。另一种方法通过监控 ISP 域内的突发流量变化继以识别承载攻击流量的数据流来检测 DDoS 攻击。作者们仍然认为各种检测机制的固有缺陷是其能力局限于检测已知的攻击特征。他们不能应对那些经常改变攻击特征的狡猾攻击者。

II 传输层和网络层攻击

传输层（第 4 层）和网络层（第 3 层）是 DDoS 攻击最常见的攻击目标，比如通常所说的 TCP 的同步（SYN）泛洪攻击和用户数据包（UDP）泛洪攻击等反射性攻击。TCP 和 UDP 都是用于传输数据包的协议。但是，UDP 不具备 TCP 中固有的流控和错误校验机制。第 4 层和第 3 层攻击通常在量级上都是巨大的，旨在使网络带宽或者应用服务器过载从而导致资源耗尽[6]。

1) TCP 泛洪攻击

这种攻击方式（参见 TCP SYN 泛洪攻击与 SDP 防御）涉及攻击者发送 TCP SYN 包以尝试完成三次握手过程（一个完整的连接）。目标服务器随后回复 SYN ACKs（数据包），原本发送方会发送 ACKs 报文来结束本次连接，但实际攻击服务器不执行该动作。由于目标服务器被配置为保持 TCP 连接开放直到攻击者发送 ACK 报文来关闭该连接，一大批类似的不完整的连接将耗尽目标服务器上的资源，包括最大所允许的开放 TCP 连接数等。

[4] DDoS 攻击使亚马逊云客户受到强烈冲击. https://www.datacenterdynamics.com/news/major-DDoS-attack-on-dyn-disrupts-aws-twitter-spotify-and-more/

[5] https://www.ietf.org/rfc/rfc2827.txt

[6] https://aws.amazon.com/shield/DDoS-attack-protection/

2）UDP 泛洪攻击

简单 UDP 攻击的原理与 TCP SYN 同步泛洪攻击类似，数据包被发送到目标服务器，最终形成需要（服务器）分配资源进行处理的未完成的服务请求。更具体一点，UDP 数据包被攻击者直接发送到受害者的特定服务器和端口请求服务。目标系统查询（攻击者）请求但实际并不存在的服务，并回复给攻击者一个 ICMP“目标不可达”报文，指示该项服务是不可达。与 SYN“TCP”泛洪类似，这些无效 UDP 数据包形成的泛洪能够压倒（目标）系统[7]。

UDP 反射攻击：

另一种稍微有所不同的 UDP 攻击（参见 UDP 反射攻击&SDP 防御）需要攻击者假冒目标服务器的 IP 地址并假装以该地址为源头发起对互联网上公开服务的查询，（这些公开服务）将发出响应并传送给目标（服务器）。使用这种攻击方式通常是被挑选的，响应结果的数据量往往远超过请求本身（例如超过 100 倍）。响应会被发送给这个伪造 IP 的真实用户。这种攻击向量允许攻击者生成巨量数据包从而形成巨大的攻击流量，同时使目标（服务器）很难确认攻击流量的原始来源。注意， TCP 反射攻击也是可能的。过去十年中互联网上出现的一些重大的 DDoS 攻击都与反射放大有关。

参见附录 4： 最大的 DDoS 攻击事件

4.2 应对 DDoS 攻击（通过非 SDP 防御）

DDoS 攻击能够通过组合使用检测、转移、过滤、分析等方法进行应对（除进行阻止的 SDP 应对措施外）。检测的目的是在达到危害级别前就识别出攻击。检测之后，流量被转移进行过滤，继而被丢弃或者驻留供分析。没有被丢弃的流量将被过滤以便正常流程通过。非法流量将被丢弃或者驻留供分析。驻留流量需要被分析以获取各种信息，帮助安全系统在将来更具韧性[9]。

7 层：应用层-数据

一种应对方法是采用 Web 应用防火墙（Web Application Firewall，WAF）。WAF 带有被设计用于识别过大流量的规则，一旦检测到（过大流量）就使系统限制流量（速率限制）。

6 层：表示层-数据

避免此层攻击的一种方法是将安全的套接字层(Secure Socket Layer, SSL)请求卸载到应用程序交付平台(Application Delivery Platform, ADP)。该平台完成会话报文的解密、检查工作之后再通过 SSL 或者 TLS 协议重新加密请求。这可以消除该部分对 Web 服务器的过载（避免资源耗尽），释放 Web 应用资源，从而使得这些资源不被 DDoS 攻击。

[7] Here's a clear explanation: https://www.cloudflare.com/learning/DDoS/udp-flood-DDoS-attack/

[8] https://www.usenix.org/system/files/conference/woot14/woot14-kuhrer.pdf

[9] https://www.incapsula.com/DDoS/DDoS-mitigation-services.html

4 层：传输层- 数据段

空路由(黑洞, Black Holing)把网络流量引导到一个并不存在的 IP 地址,沉洞(Sinkholing)基于恶意 IP 地址列表把网络流量进行转移，而边界网关协议（Border Gateway Protocol，BGP）可以把所有网络报文转移到清洗服务器上。

3 层：网络层- 数据包

除了上述技术外，ICMP 速率限定可以用来限制网络数据流。速率限制配置在防火墙上，路由器和交换机也具备速率限制的能力。正如泛洪攻击可以被认为是暴力攻击一样，速率限制可以被认为是暴力攻击的一种应对方式。

不适用的：

5 层：会话层- 数据

2 层：数据链路层- 帧

1 层：物理层 -比特

5 SDP 作为一种 DDoS 的防御机制

上文所述的检测，转移，过滤和分析等技术适用于与 DDoS 攻击相关的大量数据包。与资源损耗 DDoS 攻击相关的许多小型畸形数据包由于很难被检测到，通常会绕过这些技术，因此它们很难被检测到。 此外，这些技术很昂贵，而且经常会过滤掉正常的数据包。SDP 被设计为在丢弃所有攻击数据包的同时仅允许正常的数据包通过。总的来说，对于 SDP，主机是隐藏的，客户端与（通常有多个）边界协作，从而使正常数据包能被 SDP 知晓而上游路由器能获知要被阻止的坏数据包。为了说明 SDP 能被如何用作 DDoS 防御机制，我们将以开源参考实现为例。 在参考实现中，客户端（用户通过设备）以加密的方式登录边界。

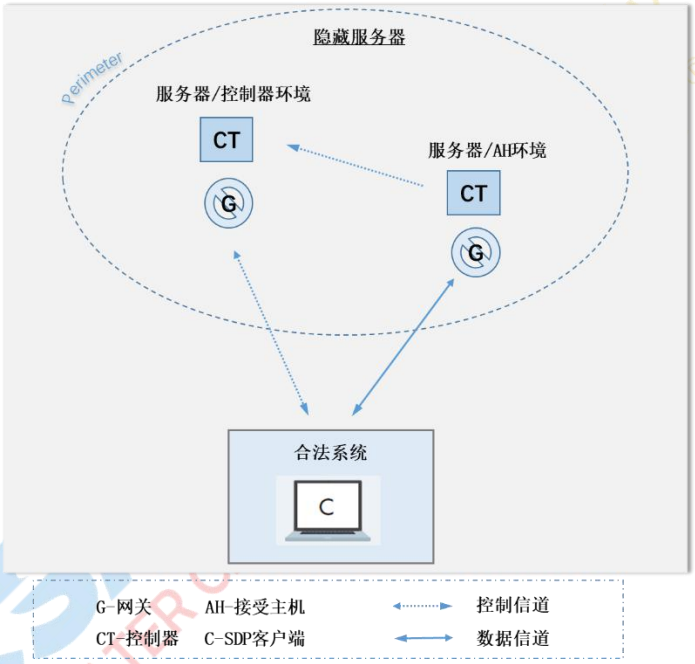


图 2：参考实现

参考 SDP 标准，服务器所有面向互联网的接口（AH 环境）只有在向 SDP 控制器（CT）和网关（G）环境中注册后才可用。通常遵循以下顺序，建立一个配置为 DDoS 防御机制的 SDP：

1. 设置控制器环境和网关以建立边界；隐藏服务/服务器。

2. 希望连接到这些隐藏服务器的用户登录并获得一个唯一的 ID（每台设备），一个客户端证书和加密密钥。

a) 作为一种选择，用户可以通过自助服务网站自行注册，该网站也会确认他们（用户）用于连接到隐藏服务器的设备。

b）作为一种选择，用户的地理位置将被 SDP 记录，并用作多因素身份认证的一个属性。

3.用户通过使用设备上的 SDP 客户端建立与隐藏服务器的连接。

4. 客户端发送一个初始的单包授权（SPA[10]）数据包，并由 SDP 控制器和网关进行合法性校验，以匹配注册时提供的用户信息。

5. SPA 数据包中的信息被验证，并与在注册过程中收集的客户端信息进行匹配。

6.如果设备验证和用户信息有效，用户将被授予访问边界内服务的权限。（IP 地址可以通过与存储的位置匹配以便验证，但不是必需）。

7.接受主机网关打开防火墙相应端口以允许连接到隐藏服务。

SDP 给出的上述流程对于允许正常数据包进入而丢弃所有非正常数据包非常有效。1）将服务隐藏在默认拒绝所有(Deny-All)的 SDP 网关后面，2）在打开防火墙以建立连接之前对设备上的用户进行身份验证，和 3）使用动态防火墙机制允许 SDP 在 DDoS 攻击期间像交换机转发一样快速丢弃数据包。一项由 DHS（www.waverleylabs.com/demo）资助和进行的研究表明，在严重的 DDoS 攻击下，即使交换机被正常的和非正常的数据包淹没，超过 80%的正常流量仍会通过。在此基础上的进一步研究以通知上游路由器和交换机有关非正常数据包也将有助于更有效地阻止一种特定的 DDoS 攻击，该攻击通过向单个服务传递大型正常格式的数据包来对服务进行压制。

在服务受到保护而免受 DDoS 攻击的同时，SDP 网关和 SDP 控制器将需要忍受 DDoS 攻击的冲击。但是研究表明，使用初始的基于 UDP 的 SPA 数据包大大减少了 SDP 网关和 SDP 控制器的暴露。更多关于对 SDP 控制器进行负载均衡的研究可能会显示 SDP 网关和 SDP 控制器的其他配置选项是减少 DDoS 攻击威胁的有效技术。

与实现同样功能的其他技术相比，使用轻量级 SPA 协议开启进入边界的入口使得对无效数据包的检测更加有效。通过利用 SPA 的轻量级特性并与拒绝所有（Deny-All）的防火墙默认设置相结合，IoT 和类似系统也可以受益。类似的流程可以被用于上述客户端-服务器模型之外的其他 SDP 模型。这些模型在《SDP 架构指南》中定义。

总之，SDP 具有对抗 DDoS 攻击的韧性，因为它们利用了一种计算上轻量的机制（SPA）以区分授权和未授权用户（即使来自远程系统）。绝大多数 DDoS 流量是由未经授权的用户发起的；因此，DDoS 流量可以被 SDP 网关拒绝而不会在服务器上造成沉重的计算负担。 SDP 应该与来自 ISP 的上游 DDoS 检测和缓解服务（例如内容分发者，如 Akamai；网络硬件提供商，如 Avaya；网络提供商，如 Verizon 等）结合，从而比现今提供的措施更有效和预防性更好。

本文的其余部分将专门用于展现SDP作为针对以下三种广为人知的DDoS攻击类型的阻断机制的操作，这三种攻击类型在基于OSI和TCP/IP模型层的DDoS攻击向量中提到过：HTTP 泛洪攻击，UDP反射攻击，TCP SYN泛洪攻击。

[10] 有关该概念的详细信息，请参见 https://cipherdyne.org/fwknop/docs/SPA.html，并参考 SDP 规范以了解其在 SDP 中的用法。

6 HTTP 泛洪攻击 与 SDP 防御

6.1 战场

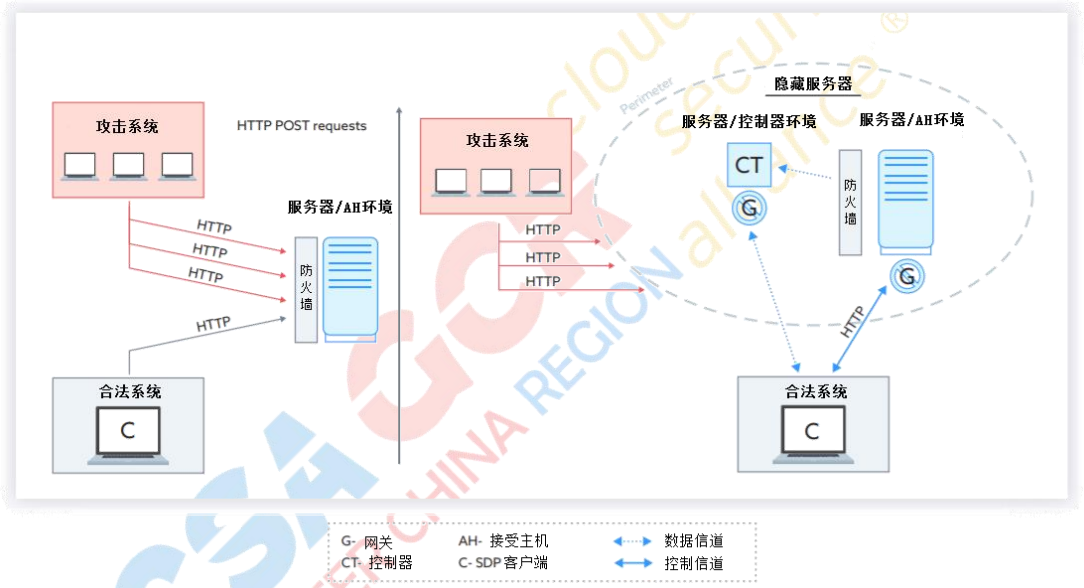


图 3：HTTP 泛洪攻击和 SDP 防御

6.2 攻击解释

此类攻击可归类为OSI第7层应用攻击(参见基于OSI和TCP/IP模型层的DDoS攻击向量)，因为其攻击目标通常是Web服务器/应用。此外，也可以被归类为资源损耗攻击，因为其目标是使服务器/应用程序的资源过载。最后，其通常是由攻击者控制的大量计算机（botnet）将大量数据包发送给单个服务。由于此攻击使用来自表面上合法的设备合法构造的请求，此类攻击很难被检测和阻止。

HTTP 泛洪攻击

- 攻击者通过用恶意软件感染来获取（通过网络钓鱼或其他方式）僵尸网络设备；
- 恶意软件是“命令和控制”类型，允许发送 HTTP POST 请求；
- HTTP POST 请求包含需由目标数据库（DB）处理的表单；
- 僵尸网络浏览器与目标 Web 服务器建立 TCP 连接（三次握手）；
- 僵尸网络浏览器发送带有表单的 HTTP POST 请求以进入目标数据库；
- 目标的 Web 服务器/应用程序尝试处理 HTTP POST 请求
- 大量处理输入到数据库中的表单和资源消耗，会耗尽 Web 服务器/应用资源，减慢了处理速度或使处理停止。

6.3 防御解释

由于此类攻击的关键是使用看起来合法、想要连接到看起来合法的 Post 请求的设备，挫败此类攻击最有效的方法是完全阻止任何连接。SDP 通过使目标服务器对未经授权的设备不可见来防止攻击。

1. 攻击者的僵尸网络无法识别目标 Web 服务器，因为僵尸网络设备尚未注册到 SDP 的控制器。
2. 僵尸网络，即使可以找到隐藏服务器的 SDP 网关，也无法将其连接到 SDP 网关，因为其设备没有安装将所有通信定向到 SDP 控制器的 SDP 客户端。
3. 除了将通信定向之外，缺少的 SDP 客户端还包含唯一 ID（每个设备）、客户端证书和加密密钥。
4. 僵尸网络永远无法连接因为 SDP 控制器无法证明/验证其中包含提供给授权设备的用户信息的单数据包授权（SPA）。
5. 因此，SDP 控制器永远无法验证和匹配所需的客户端信息。
6. 缺少安装在 botnet 设备上并注册过的 SDP 客户端（带有 ID、证书和加密密钥），SDP 控制器和 SDP 网关将不会授权对边界进行访问。
7. 最后，除非被 SDP 控制器授权，保护 web 服务器的 SDP 网关不会打开防火墙以允许连接到隐藏服务。

但是，如果 IP 地址公开或攻击者通过某种方式定位到 IP 地址，SDP 网关将无法识别这些设备并将丢弃所有已传递的数据包（POST 请求）。如果攻击者走到这一步，尝试进入时留下的痕迹和被丢弃的数据包会提供可以被用于分析的证据和数据，以改善防御和/或起诉攻击者。

7 TCP SYN 泛洪攻击与 SDP 防御

7.1 战场

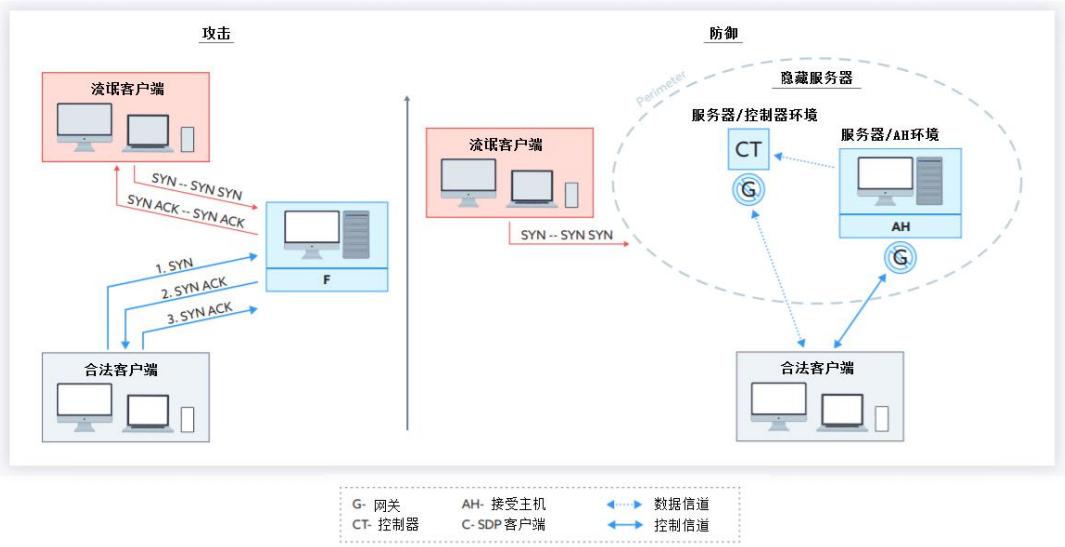


图 4：TCP SYN 洪泛攻击和 SDP 防御

7.2 攻击解释

SYN 泛洪攻击，例如最近每秒 5 亿个数据包的 DDoS 攻击, (https://www.darkreading.com/attacks-breaches/massive-DDoS-attack-generates-500-million-packets-per-second/d/d-id/1333766)通过向目标发送大量发起但不完成 TCP 握手的请求，最终耗尽其接受更多请求的能力，从而导致拒绝服务。通过使用多个恶意客户端执行相同的未完成 TCP 握手，攻击者能够增加针对目标的每秒数据包数（PPS）或数据包速率。大 SYN 数据包或很大的数据包数量也可能压倒目标，导致拒绝服务。

7.3 防御解释

SDP 网关提供了一种防护，将来自恶意客户端的所有数据包丢弃，同时允许来自合法客户端的数据包进入保护目标的边界。其他通过配置网络带宽和检查数据包的防御机制，不区分合法客户端和恶意客户端，对即使是合法的数据包也会限制，从而使 SDP 成为在 SYN 泛洪攻击下继续运行的更有效的解决方案，无论数据包速率或数据包数量如何。

12 SDP 防御的步骤 1-7 顺序已在前面的章节中描述

8 UDP 反射攻击和 SDP 防御

8.1 战场

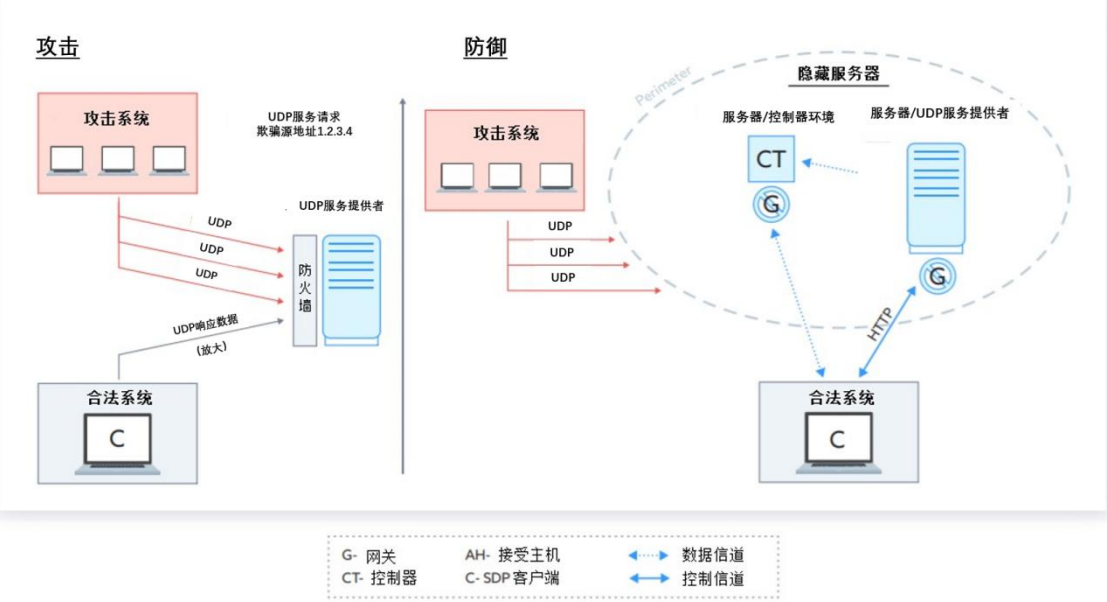


图 5：UDP 反射攻击和 SDP 防御 [13]

8.2 攻击解析

这种类型的攻击基于 UDP 作为一种无认证和无连接协议的内在不安全性。UDP 数据包（具体来说，数据包头）很容易被伪造，所以对被请求的“服务”的响应被导向到了初始 UDP 数据包中伪造的受害者 IP 地址。因此，UDP 请求的响应从攻击者“反射”到受害者。放大是一种反射攻击，其中响应是不成比例的大（放大），因此压倒了受害者的网络或机器。攻击者通常选择具有大放大因子的服务从而可以更有效地 DoS 攻击受害者。

放大因子的大致范围从一个 ICMP ping 命令的 1(没有放大)到某些 DNS 攻击的 28-54 左右，再到某些 NTP 攻击的 550。其它服务可能导致更大倍数的放大，最显著的是 memcached，根据数据库内容的不同，放大因子可达 50000。

链接：https://www.us-cert.gov/ncas/alerts/TA14-017A\

https://www.cloudflare.com/learning/DDoS/memcached-DDoS-attack/

[13]SDP 防御的步骤 1 – 7 顺序已在前面的章节中描述。

UDP 反射攻击能够很有效和隐秘，因为不需要攻击者和目标之间的任何直接沟通。这些攻击通常从一群分散的被劫持系统（僵尸网络）发起，从而进一步模糊了攻击的实际来源。

8.3 防御解析

基于 UDP 的服务自身不能被保护起来，因为 UDP 本质上是一种无须验证或授权就进行数据包传递的开放机制。一些面向公众的 UDP 服务，如 NTP 或 DNS，则必须保持公开，因此可被利用而参与这种类型的 DoS 攻击。但是，非公开的服务，即只被可识别的用户群或服务器群消费的服务，非常适合使用 SDP 进行防护。

通过将这些服务放在 SDP 网关之后，组织能够强化访问控制使得只有授权的用户（或设备及服务器）才能发送 UDP 数据包到这些服务。这就消除了攻击者使用这些 UDP 服务进行反射攻击的能力。

注意，运行恶意软件的授权客户端设备当然可能被用于启动这种类型的反射攻击。

9 总结

本文的目的是通过展示 SDP 防御几种常见攻击的效率和有效性，增强对 SDP 作为防范 DDoS 攻击的工具的意识和理解。为此我们在简介一章中给出了 DDoS 和 DoS 攻击的定义。然后，在下一章 DDoS 攻击向量中我们展示了基于 OSI 和 TCP/IP 模型层的 DDoS 攻击向量。从表格中我们选择了三个著名的攻击作为重点：

1. 第 7 层 应用层 - HTTP 泛洪攻击（与前面保持一致）
2. 第 4 层 传输层 - SYN“TCP”泛洪攻击
3. 第 3 层 网络层 - UDP 反射攻击

选择了关注的攻击向量和攻击后，我们详细地从概念性上解释了他们。在接下去的一章应对 DDoS 攻击（通过非 SDP 防御）中，我们描述了在 OSI 各层中使用的非 SDP 缓解措施。紧接着是 SDP 作为一种 DDoS 的防御机制。这里我们首先描述了部署和配置 SDP 作为 DDoS 防御时应遵循的事件次序。然后我们列举了该部署所提供的保护，包括：

1.拒绝所有（Deny-All）的 SDP 网关之后的不可见服务;

2.在打开防火墙建立连接前认证设备上的用户;

3.使用动态防火墙机制，以允许，或者允许 SDP，在 DDoS 攻击时以与服务他们的交换机类似的速度丢弃数据包。

最后，我们使用 SDP 作为防御机制查看了以下三种攻击:

- HTTP 泛洪攻击及 SDP 防御
- TCP SYN 泛洪攻击及 SDP 防御
- UDP 反射攻击及 SDP 防御

对于上述的每个攻击我们都以图示描述了攻击和防御，并在图例之后附以详细解释。对于每种攻击我们的结论都是 SDP 提供了充分的防御。

总之，对于所讨论的几种攻击，SDP 是一种有效且高效的 DDoS 防御机制。SDP 配置的某些属性如拒绝所有（Deny-All）网关和 SPA 还可用于应对很多其它攻击。如果你将 SDP 与上游 ISP 和内容及网络提供商的 DDoS 检测和缓解服务结合，你就具有全面的 DDoS 纵深防御。

10 术语

BGP	边界网关协议是用于分发和计算组成互联网的成千上万自治网络之间的路径的控制协议。
僵尸网络	已经被攻击者攻陷以用于执行恶意攻击的计算机。
ICMP	互联网控制消息协议，与 TCP 和 UDP 不同，主要用于错误、操作或诊断消息/目的，例如请求服务不可用，主机或路由器不可达，或用于 ping 和 traceroute 分析。
入口过滤	这是一种确保标识为来自一个特定地址的数据包的确来自这一地址的方法。有各种各样的方法实现这一过程，其中最好的方法记录在互联网工程任务组 BCP 38 和 BCP 84 中。
IP 地址欺骗	在创建 IP 数据包时使用一个假的源 IP 地址，这称为欺骗。这样做是为了隐藏攻击者的身份。
畸形数据包	这是任何不能被数据包协议解析器解析的包。该数据包没有遵循对应的协议规范——例如 TCP 或 UDP。
签名（攻击）	攻击所固有的数据、流量或事件。这些信息被入侵检测系统(IDS)用于识别攻击的发生并随之发出告警。

11 其他阅读材料

Cybersecurity Framework DDoS Profile, by the Coalition for Cybersecurity Policy & Law Made Public July 28, 2017, Available @ https://www.cybersecuritycoalition.org/threat-profile-DDoS-nist-framework

NIST, Advanced DDoS Mitigation Techniques Project, by NIST, Department of Homeland / Security Science and Technology Directorate / Cyber Security Division / Distributed DDoS Defense Program, Available @ https://www.nist.gov/programs-projects/advanced-DDoS-mitigation-techniques

NIST, SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Info. Systems and Organizations, by Kelley Dempsey (NIST), Nirali Chawla (PwC), L. Johnson (NIST), Ronald Johnston (DoD), Alicia Jones (BAH), Angela Orebaugh (BAH), Matthew Scholl and Kevin Stine (NIST), Sep. 2011, Available @ https://csrc.nist.gov/publications/detail/sp/800-137/final

ENISA, DoS & DDoS Portal, European Union Agency for Network & Info. Sec. Resilience & Sec. of Comm. Infrastructure, Networks & Services, Oct. 2018, Available @ https://resilience.enisa.europa.eu/internet-infrastructure-security-and-resilience-reference-group/dos-and-DDoS

ENISA, Threat Landscape Report 2017 15 Top Cyber-Threats and Trends, by ENISA ETL Stakeholder group: Pierluigi Paganini, Chief, Security Info. Officer, IT, Paul Samwel, Banking, NL, Jason Finlayson, Consulting, IR, Stavros Lingris, CERT, EU, Jart Armin, Worldwide Coalitions/Initiatives, Int'l., Thomas Häberlen, Member State, DE, Neil Thacker, Consulting, UK, Shin Adachi, Security Analyst, US, R. Jane Ginn, Consulting, US, Andreas Sfakianakis, Industry and CYjAX, NL. T Final Version,1.0, ETL 2017, Chapter 3.6 Denial of Service, January 2018, Available @ https://www.enisa.europa.eu/publications/ enisa-threat-landscape-report-2017

Understanding DDoS Attack & Its Effect In Cloud Environment by Rashmi V. Deshmukha, Kailas K. Devadkarb, Procedia Computer Science Volume 49, 2015, Pages 202-210, December 2015, Available @ https://www.sciencedirect.com/science/article/pii/S1877050915007541

DDoS Attacks: Tools, Mitigation Approaches, and Probable Impact on Private Cloud Environment, by R. K. Deka and D. K. Bhattacharyya; Department of Computer Science and Engineering, Tezpur University, Napaam, Assam, India, and J. Kalita; Department of Computer Science, College of Engineering and Applied Science, University of Colorado, Boulder, CO, United States, October 25, 2017, Available @ https://arxiv.org/pdf/1710.08628.pdf

Defence for Distributed Denial of Service Attacks in Cloud Computing, Andrew Carlin and Mohammad Hammoudeh, School of Computer, Mathematics & Digital Technology, Manchester Metropolitan University, Manchester, UK, Omar Aldabbas, Faculty of Eng., Al-Balqa Applied University, Jordan, 2015, Available @ https://www.sciencedirect.com/science/article/pii/S1877050915034985

Guide to DDoS Attacks November 2017, Center for Internet Security (CIS), Multi-State Information Sharing and Analysis Center (MS-ISAC), November 2017, Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.http://www.us-cert.gov/tlp, Available @ https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-DDoS-attacks/ 21

NIST, SP 800-54 Border Gateway Protocol Security, by Rick Kuhn (NIST), Kotikalapudi Sriram (NIST), Doug Montgomery (NIST), July 2007, to be superceded by SP 800-119 below, Available @ https://csrc. nist.gov/publications/detail/sp/800-54/final

NIST, SP 800-189 Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation, by Kotikalapudi Sriram (NIST), Douglas Montgomery (NIST), March 2019, Available @ https://csrc.nist. gov/publications/detail/sp/800-189/draft

NIST, SP 800-119, Guidelines for the Secure Deployment of IPv6, by Sheila Frankel of the National Institute of Standards and Technology (NIST), Richard Graveman of RFG Security, John Pearce of Booz Allen Hamilton and Mark Rooks of L-1 Identity Solutions (formerly of Booz Allen Hamilton), December 2010, Available @ https://csrc.nist.gov/publications/detail/sp/800-119/final

Beginner's Guide to Brute Force & DDoS Attacks, WHAT TO DO WHEN THE BARBARIANS ARE AT YOUR DOOR, Alienvault, Available @ https://www.alienvault.com/resource-center/white-papers/beginners-guide-to-brute-force-and-DDoS-attacks

DDoS Quick Guide, The Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center, January 2014, Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls. http://www.us-cert.gov/tlp,

Available @ https://www.us-cert.gov/security-publications/DDoS-Quick-Guide

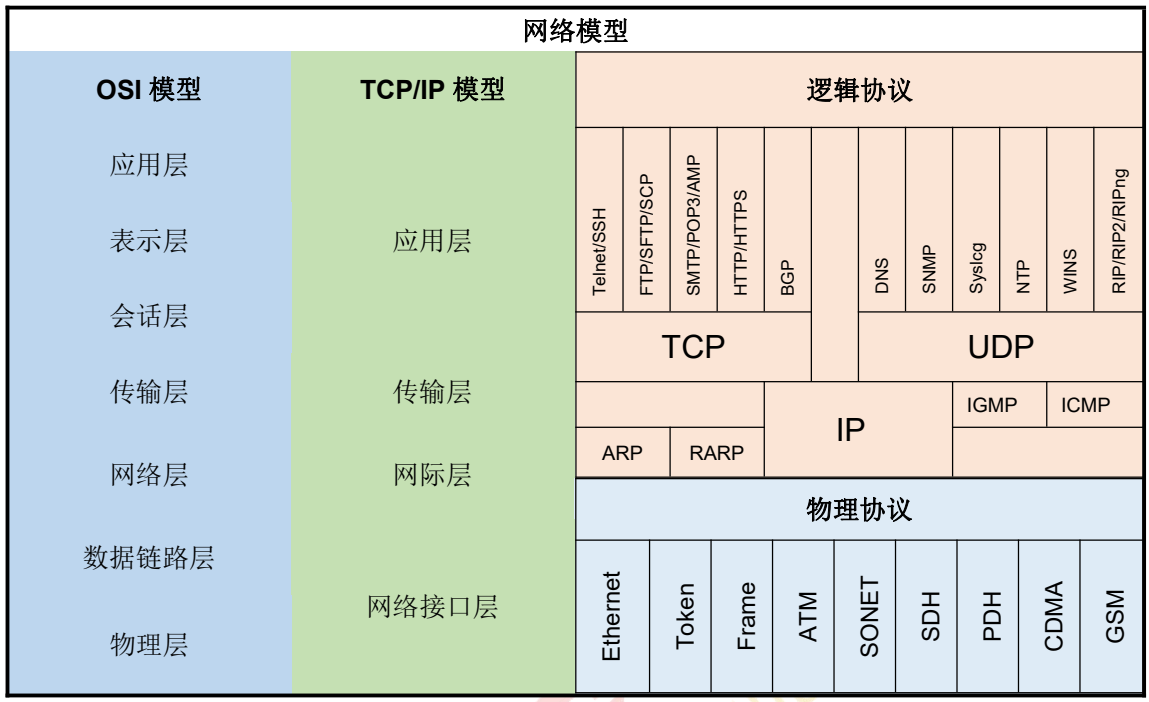
Cybersecurity Framework DDoS and Botnet Prevention and Mitigation Profile(s), Coalition for Cybersecurity Policy & Law, February 2018, Available @ https://www.cybersecuritycoalition.org/botnet-framework

Scalable Cloud Defenses for Detection, Analysis and Mitigation of DDoS Attacks

Towards the Future Internet, G. Tselentis et al. (Eds.), IOS Press, 2010, Available @

https://pdfs.semanticscholar.org/d44f/98844c5bfc38f6c867edbeab3f0957f913d0.pdf

附录 1：OSI 与 TCP/IP 的层次结构及逻辑协议



参考：https://www.inetdaemon.com/tutorials/basic_concepts/network_models/comparison.shtm

OSI 和 TCP/IP 的相似点包括了：

- 均采用层次结构。
- 均包含应用层，尽管它们在该层所包含的服务有着很大的差异。
- 均包含对应的传输层和网络层。
- 均需要被网络专业人士所了解。
- 均假设数据包是可交换的。这意味着各个数据包可以通过不同的路径到达相同的目的地。这与所有包都走相同路径的电路交换网络有所不同。

OSI 和 TCP/IP 的不同点包括了：

- TCP/IP 将会话层和表示层的问题归并到它的应用层。
- TCP/IP 将 OSI 的数据链路和物理层归并到它的网络接口层中。
- TCP / IP 看起来更简单，因为它的层数更少。
- TCP/IP 协议是互联网发展的标准，因此 TCP/IP 模型因其协议而获得认可。 相反，网络通常不被构建在 OSI 协议上的，即使 OSI 模型被用作指导。

参考：http://basicitnetworking.blogspot.com/2009/11/osi-layers-peer-to-peer-communications.html

附录 2：OSI 和 TCP/IP 各层次的 DDoS 攻击

OSI 层	7	6	5	4	3	2	1
TCP/IP 层	4			3	2	1	
DDoS 攻击类型名称	应用层	表示层	会话层	传输层	网络层	数据链路层	物理层
Smurf 攻击			不适用		X	不适用	不适用
ICMP 泛洪攻击			不适用		X	不适用	不适用
IP/ICMP 分片攻击			不适用		X	不适用	不适用
SYN 泛洪攻击			不适用	X		不适用	不适用
UDP 泛洪攻击			不适用	X		不适用	不适用
其他 TCP 泛洪攻击（Spoof/Non）			不适用	X		不适用	不适用
TCP 连接耗尽攻击			不适用	X		不适用	不适用
IPSec 泛洪攻击 IKE/ISAKMP 相关			不适用	X		不适用	不适用
满传输速率攻击			不适用	X		不适用	不适用
长连接 TCP 会话攻击			不适用	X		不适用	不适用
其他连接泛洪			不适用	X		不适用	不适用
SSL 耗尽攻击		X	不适用			不适用	不适用
伪造证书攻击		X	不适用			不适用	不适用
中间人攻击		X	不适用			不适用	不适用
反射/放大攻击（DNS、NTP……）	X		不适用			不适用	不适用

应用请求泛洪攻击	X		不适用			不适用	不适用
其他泛洪攻击（SMTP、DNS、 SNMP、 FTP、SIP 等）	X		不适用			不适用	不适用
针对性的应用攻击	X		不适用			不适用	不适用
数据库连接池资源耗尽攻击	X		不适用			不适用	不适用
资源耗尽攻击	X		不适用			不适用	不适用
HTTP POST 请求耗尽攻击	X		不适用			不适用	不适用
HTTP Get 请求耗尽攻击	X		不适用			不适用	不适用
模拟用户访问攻击	X		不适用			不适用	不适用
Slow read 攻击	X		不适用			不适用	不适用
Slow POST 攻击	X		不适用			不适用	不适用
Slow loris 攻击	X		不适用			不适用	不适用

参考：http://resources.arbornetworks.com/wp-content/uploads/INFO_DDoSAttackTypes_EN.pdf

附录 3：DDoS 及其他攻击方式的监控地图

以下是 2 种主要用于追踪 DDoS 活动的监控地图：

1. Digital Attack Map - https://www.digitalattackmap.com/about/
   a. 每日更新
2. A10 - https://threats.a10networks.com/
   a. 实时更新

以下是 9 种可用于跟踪包含 DDoS 攻击在内的各种攻击活动的监控地图：

1. Security Incidents - https://www.ibm.com/security/resources/xforce/xfisi/

a. 自 2018 年 1 月开始更新（每年更新一次）

2. Checkpoint – https://threatmap.checkpoint.com/ThreatPortal/livemap.html

a. 每日更新

3. Kaspersky - https://cybermap.kaspersky.com/

a. 实时更新

4. Fortinet - https://threatmap.fortiguard.com/

a. 不定期更新

5. FireEye - https://www.fireeye.com/cyber-map/threat-map.html

a. 不定期更新

6. Bitdefender - https://threatmap.bitdefender.com/

a. 实时更新

7. Threatbutt - https://threatbutt.com/map/

a. 实时更新

8. Deteque - https://www.deteque.com/live-threat-map/

a. 实时更新

9. Akami - https://www.akamai.com/us/en/resources/visualizing-akamai/real-time-webmonitor.jsp

a. 实时更新

附录 4：最大规模的 DDoS 攻击

日期	攻击目标	攻击流量强度（TB/秒）	被攻击的设备	设备漏洞触发点	攻击手段
2018 年 3 月 [14]	US SP	1.7	Memcached 服务器	访问认证	“反射放大型”DDoS
2018 年 2 月 [15]	Github	1.3	Memcached 服务器	访问认证	“反射放大型”DDoS
2016 年 10 月 [16, 17]	Dyn DNS	1.2	数百万 IoT 设备	认证	TCP、UDP 洪攻击

Memcached 服务器[18, 19]

Memcached 服务器允许需要从外部数据库访问大量数据的应用程序将某些数据缓存在内存中，使得应用程序的访问速度比其外出从数据库中获取重要数据时更快。

这些服务器应该部署于受信任的网络内因为它们默认在 TCP 上使用 UDP（端口 11211）通信，无需身份认证。 但是，在刚刚爆发两轮最大规模的攻击之后的 2018 年 3 月 8 日据估计大约有 50000[20]台 Memcached 服务器被公开暴露。

至少有以下 3 种措施可缓解该漏洞的危害：将服务器移至受信任的网络、安装默认禁用 UDP 协议的新版 Memcached，最后是关闭端口 11211。

目前，仍大约有 31000 个 Memcached 服务器对外开放[21]。

[14] https://www.theregister.co.uk/2018/03/05/worlds_biggest_DDoS_attack_record_broken_after_just_ five_days/

[15] https://www.theregister.co.uk/2018/03/05/worlds_biggest_DDoS_attack_record_broken_after_just_ five_days/

[16] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[17] See Page 7, Infrastructure attacks SYN “TCP” floods and Syn “UDP” Floods

[18]https://www.globaldots.com/memecached-servers-DDoS-attacks-complete-analysis/

[19]https://www.geekwire.com/2018/memcached-servers-used-launch-record-setting-DDoS-attacks/

[20]https://memcachedscan.shadowserver.org/stats/ 21 https://memcachedscan.shadowserver.org/stats/