安全+ SECURITY
2013/12 总第023
技术版 与安全人士分享技术心得 Share technique experience with security professionals

# DDo_S 放大攻击原理及防护方法

绿盟科技安全研究部　洪海

**摘要：**DDoS 放大攻击是一种历史悠久而又威力强大的攻击技术。最早的放大拒绝服务攻击可以追溯到古老的 smurf 攻击。现代的 DDoS 放大攻击能够对被攻击目标造成极大影响，甚至拖慢局部互联网的访问速度。本文将对各种 DDoS 放大攻击的原理和 DDoS 放大攻击的防护方法进行简单的介绍。

**关键词：** DDoS 反射攻击、DDoS 放大攻击、DDoS 防护

## 一、 概念

在介绍其具体技术之前，我们先对几个概念进行简要的说明。

### (一) 针对网络带宽资源的 DDoS 攻击

按照 DDoS 攻击所针对的攻击目标和所属的层次，可以将 DDoS 攻击大体分为三类，即：针对网络带宽资源的 DDoS 攻击（网络层）、针对连接资源的 DDoS 攻击（传输层）以及针对计算资源的攻击（应用层）。针对网络带宽的 DDoS 攻击是最古老而常见的一种 DDoS 攻击方式。

无论是服务器的网络接口带宽，还是路由器、交换机等互联网基础设施的数据包处理能力，都是存在着事实上的上限的。当到达或通过的网络数据包数量超过了这个上限时，就会出现网络拥堵、响应缓慢的情况。针对网络带宽资源的 DDoS 攻击就是根据该原理，利用广泛分布的僵尸主机发送大量的网络数据包，占满被攻击目标的全部带宽，从而使正常的请求无法得到及时有效的响应，造成拒绝服务。

### (二) DDoS 反射攻击

攻击者可以使用 Ping Flood、UDP Flood 等方式直接对被攻击目标展开针对网络带宽资源的 DDoS 攻击，但这种方式不仅低效，还很容易被查到攻击的源头。虽然攻击者可以使用伪造源 IP 地址的方式进行隐藏，但更好的方式是使用 DDoS 反射攻击技术。

DDoS 反射攻击是指利用路由器、服务器等设施对请求产生应答，从而反射攻击流量并隐藏攻击来源的一种 DDoS 技术。

DDoS 反射攻击的基本原理如下图所示。

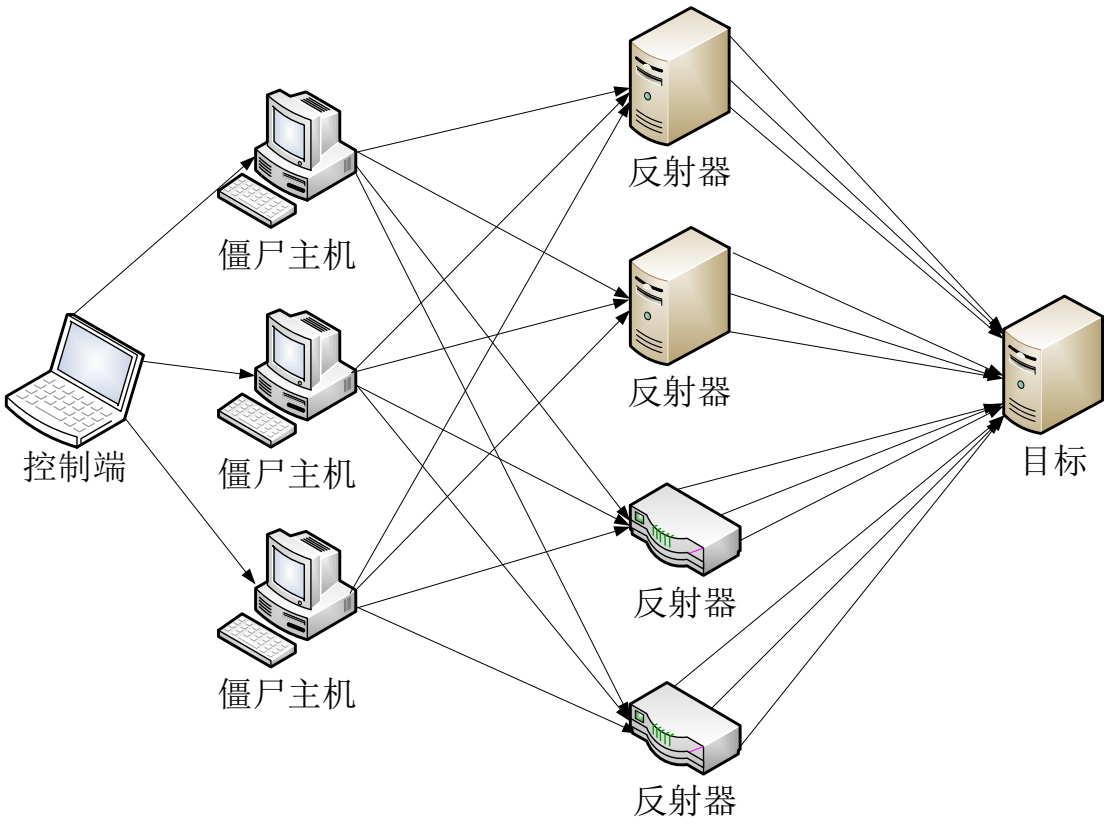


图 1 DDoS 反射攻击原理示意图

在进行 DDoS 反射攻击时，攻击者通过控制端控制大量僵尸主机发送大量的数据包。这些数据包的特别之处在于，其目的 IP 地址指向作为反射器的服务器、路由器等设施，而源 IP 地址则被伪造成被攻击目标的 IP 地址。反射器在收到数据包时，会认为该数据包是由被攻击目标所发来的请求，因此会将响应数据发送给被攻击目标。当大量的响应数据包涌向攻击目标时，就会造成拒绝服务攻击。

发动 DDoS 反射攻击需要在互联网上找到大量的反射器，对于某些种类的反射攻击，这并不难实现。例如，对于 ACK 反射攻击，只需要找到互联网上开放 TCP 端口的服务器即可，而这种服务器在互联网上的存在是非常广泛的。

相比于直接伪造源地址的 DDoS 攻击，DDoS 反射攻击由于增加了一层反射步骤，更加难以追溯攻击来源。

**(三) DDoS 放大攻击**

DDoS 放大攻击是 DDoS 反射攻击的一种特殊形式。简单的说，当使用的反射器对网络流量具有放大作用时，DDoS 反射攻击就变成了 DDoS 放大攻击。

针对网络带宽资源的 DDoS 攻击、DDoS 反射攻击和 DDoS 放大攻击的关系见下图。

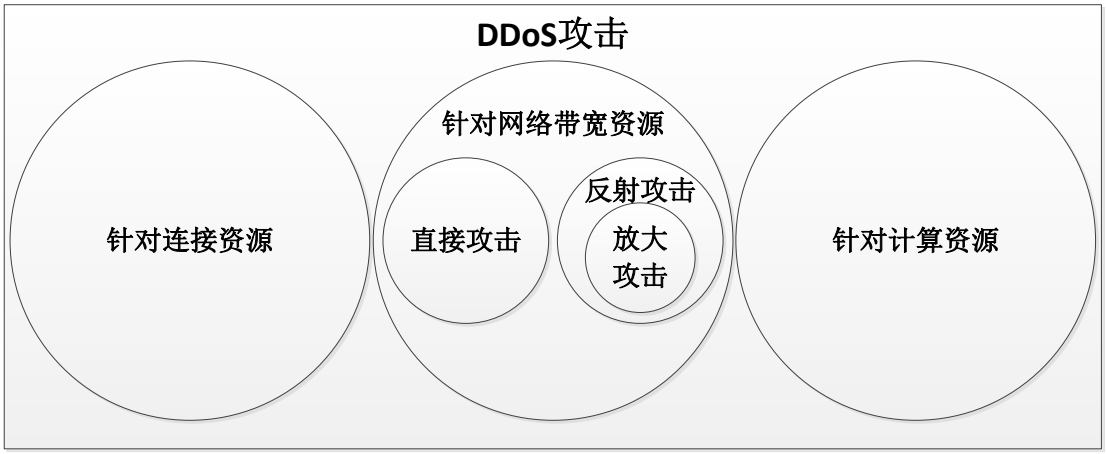


图 2 流量式攻击、反射攻击和放大攻击的关系

本文后面会对 DDoS 放大攻击的技术原理进行详细的介绍。

## 二、 DDoS 放大攻击的技术原理

### (一) DDoS 放大攻击的特点

前面已经提到，DDoS 放大攻击是一种特殊的 DDoS 反射攻击，其特殊之处在于反射器对于网络流量具有放大作用，因此我们也可以将这种反射器称为放大器。进行 DDoS 放大攻击的方式与 DDoS 反射攻击的方式也是基本一致的，不同之处在于反射器（放大器）所提供的网络服务需要满足一定条件。

首先，在反射器提供的网络服务协议中，需要存在请求和响应数据量不对称的情况，响应数据量需要大于请求数据量。响应数据量与请求数据量的比值越大，放大器的放大倍数也就越大，进行 DDoS 放大攻击的效果也就越明显。

其次，进行 DDoS 放大攻击通常会使用无需认证或握手的协议。DDoS 放大攻击需要将请求数据的源 IP 地址伪造成被攻击目标的 IP 地址，如果使用的协议需要进行认证或者握手，则该认证或握手过程没有办法完成，也就不能进行下一步的攻击。因此，绝大多数的 DDoS 放大攻击都是用基于 UDP 协议的网络服务进行攻击。

最后，放大器使用网络服务部署的广泛性决定了该 DDoS 放大攻击的规模和严重程度。如果存在某些网络服务，不需要进行认证并且放大效果非常好，但是在互联网上部署的数量很少，那么利用该网络服务进行放大也不能打出很大的流量，达不到 DDoS 攻击的效果，这种网络服务也就不具备作为 DDoS 放大攻击放大器的价值。

以上三点就是 DDoS 放大攻击中放大器所开放的网络服务具有的特点，之后介绍的 DNS 放大攻击、SNMP 放大攻击都满足这些特点。同时我们也可以说，满足以上三个特点的网络服务协议都能够用于 DDoS 放大攻击。

**(二) DNS 放大攻击**

DNS 是域名系统（Domain Name System）的缩写，是因特网的一项核心服务。它作为可以将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。DNS 使用的 TCP 与 UDP 端口号都是 53，主要使用 UDP 协议。

通常，DNS 响应数据包会比查询数据包大，攻击者利用普通的 DNS 查询请求就能够将攻击流量放大 2 到 10 倍。但更有效的方法是使用 RFC 2671 中定义的 DNS 扩展机制 EDNS0。

在没有 EDNS0 以前，对 DNS 查询的响应数据包被限制在 512 字节以内。当需要应答的数据包超过 512 字节时，根据 DNS 服务实现的不同，可能会丢弃超过 512 字节的部分，也可能会使用 TCP 协议建立连接并重新发送。无论是哪种方式，都不利于进行 DNS 放大攻击。

在 EDNS0 中，扩展了 DNS 数据包的结构，增加了 OPT RR 字段。在 OPT RR 字段中，包含了客户端能够处理的最大 UDP 报文大小的信息。服务端在响应 DNS 请求时，解析并记录下客户端能够处理的最大 UDP 报文的大小，并根据该大小生成响应的报文。

攻击者能够利用 dig（Domain Information Groper）和 EDNS0 进行高效的 DNS 放大攻击。

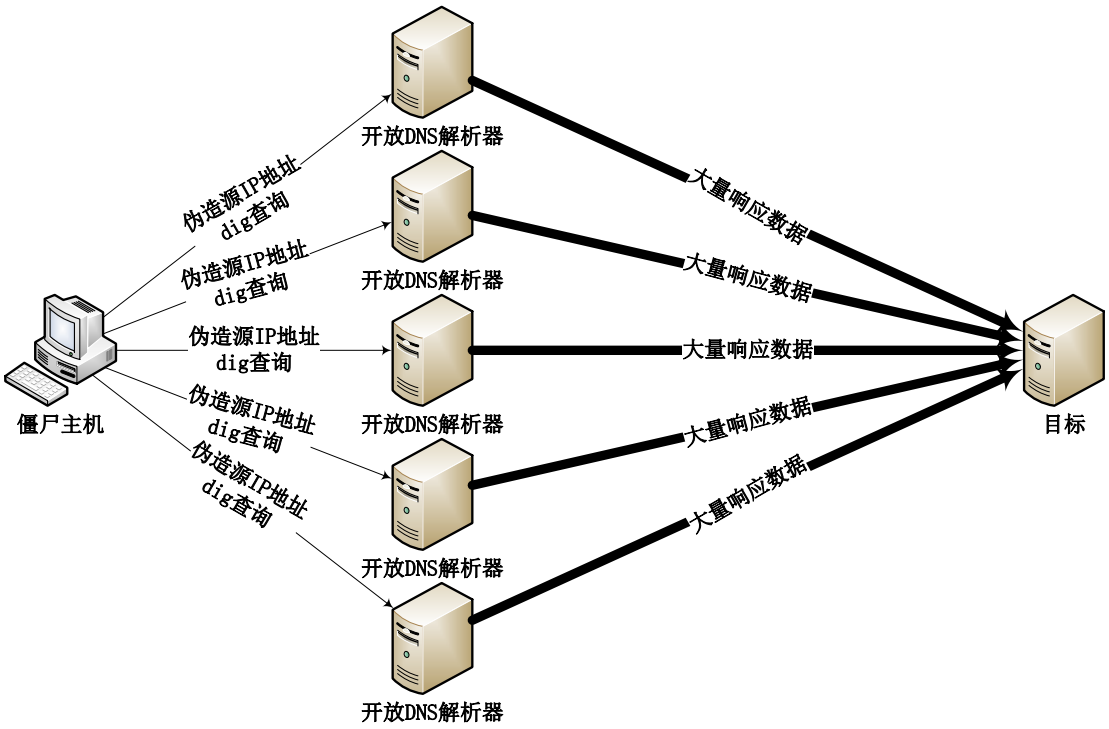


图 3 DNS 反射攻击示意图

攻击者向广泛存在的开放 DNS 解析器发送 dig 查询，将 OPT RR 字段中的 UDP 报文大小设置为很大的值（如 4096），并将请求的源 IP 地址伪造成被攻击目标的 IP 地址。DNS 解析器收到查询请求后，会将解析的结果发送给被攻击目标。当大量的解析结果涌向目标时，就会导致目标网络拥堵和缓慢，造成拒绝服务攻击。

攻击者发送的 DNS 查询请求数据包大小一般为 60 字节左右，而查询返回结果的数据包大小通常为 3000 字节以上，因此，使用该方式进行放大攻击能够达到 50 倍以上的放大效果。极端情况下，36 字节的查询请求能够产生 3k～4k 字节的应答，也就是说，能够对攻击流量进行一百倍放大。

在 2013 年 3 月对 Spamhaus 的 DDoS 攻击中，主要就是用了 DNS 放大攻击技术，使得攻击流量达到了史无前例的 300Gbps，甚至拖慢了局部互联网的响应速度。

**(三) SNMP 放大攻击**

SNMP 是简单网络管理协议（Simple Network Management Protocol）的缩写，该协议是目前 UDP/IP 网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维护互联网设备。SNMP 协议使用 UDP 161 端口进行通信。

由于 SNMP 的效果很好，网络硬件厂商开始把 SNMP 加入到它们制造的每一台设备。今天，各种网络设备上都可以看到默认启用的 SNMP 服务，从交换机到路由器，从防火墙到网络打印机，无一例外。同时，许多厂商安装的 SNMP 都采用了默认的通信字符串

（community string），这些通信字符串是程序获取设备信息和修改配置必不可少的。最常见的默认通信字符串是 public 和 private，除此之外还有许多厂商私有的默认通信字符串。几乎所有运行 SNMP 的网络设备上，都可以找到某种形式的默认通信字符串。

在 SNMPv1 中定义的 Get 请求可以尝试一次获取多个 MIB 对象，但响应消息的大小受到设备处理能力的限制。如果设备不能返回全部请求的响应，则会返回一条错误信息。在 SNMPv2 中，添加了 GetBulk 请求，该请求会通知设备返回尽可能多的数据，这使得管理程序能够通过发送一次请求就获得大段的检索信息。

利用默认通信字符串和 GetBulk 请求，攻击者能够开展有效的 SNMP 放大攻击。

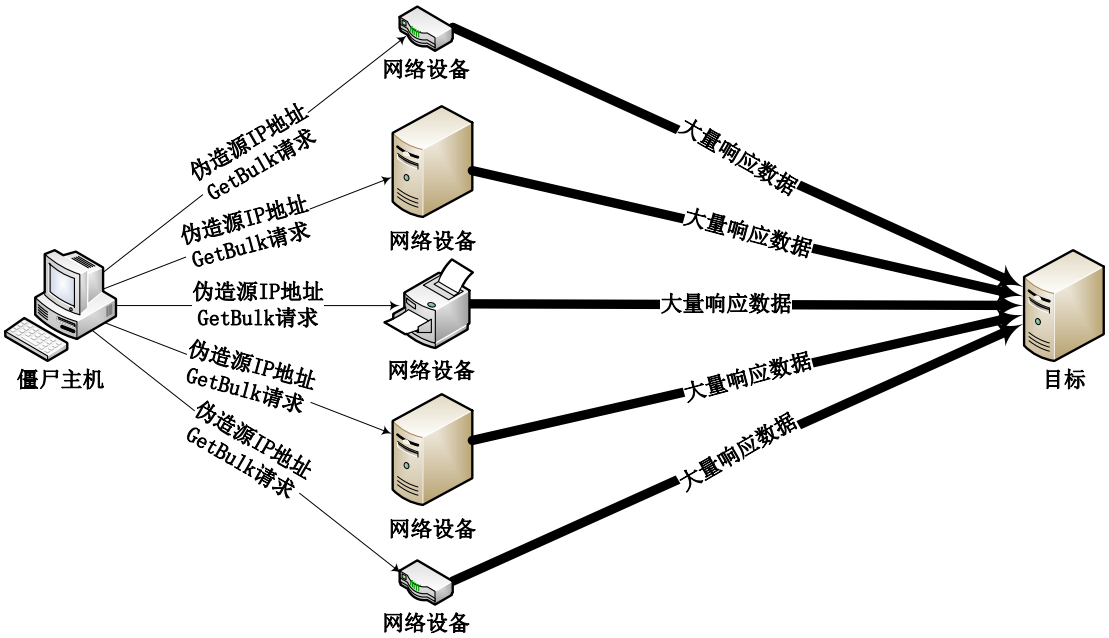


图 4 SNMP 反射攻击示意图

攻击者向广泛存在并开启了 SNMP 服务的网络设备发送 GetBulk 请求，使用默认通信字符串作为认证凭据，并将源 IP 地址伪造成被攻击目标的 IP 地址。设备收到 GetBulk 请求后，会将响应结果发送给被攻击目标。当大量的响应结果涌向目标时，就会导致目标网络拥堵和缓慢，造成拒绝服务攻击。

攻击者发送的 GetBulk 请求数据包约为 60 字节左右，而请求的响应数据能够达到 1500 字节以上，因此，使用该方式进行放大攻击能够达到 20 倍以上的放大效果。

**(四) 其他放大攻击**

前面详细介绍了 DNS 放大攻击和 SNMP 放大攻击的原理。除了这两种协议以外，还有一些协议和网络服务可以用于 DDoS 放大攻击。

在 NTP 协议中，monlist 请求可以获取与目标 NTP 服务器进行过同步的最后 600 个客户端的 IP 地址。发送一个很小的请求包，就能获取到大量的活动 IP 地址组成的连续 UDP 包。通过伪造 IP 地址并发送 monlist 请求，可以将攻击流量放大 500 倍以上。

在 CHARGEN 协议中，每当服务器收到客户端的一个 UDP 数据包，这个数据包中的内容将被丢弃，而服务器将发送一个数据包到客户端，其中包含长度为 0～512 字节之间随机值的任意字符。利用该协议可以将攻击流量放大 2～10 倍。

需要说明的是，由于这些协议在互联网上部署的范围不够广泛，因此他们不能作为 DDoS 放大攻击的主要手段和产生攻击流量的主要部分，只能作为辅助手段增大攻击流量。

## 三、 DDoS 放大攻击的防护方法

对于 DDoS 放大攻击，可以从三个方面进行防护。

### (一) 对开放 DNS、SNMP 服务的设备进行防护

首先，应确认设备上的 DNS、SNMP 服务是否是必要的，如非必要，则应该关闭这些服务。

如果必须开放 DNS、SNMP 服务，则应加强对这些服务请求的鉴权和认证。例如，DNS 服务不应对互联网上的任意计算机都提供域名解析服务，而只应该响应该 ISP 或该网络内部的 DNS 解析请求；SNMP 要使用非默认的独特的通信字符串，并尽可能升级到 SNMPv3 版本，以提高安全性。

最后，还应该限制 DNS、SNMP 响应数据包大小的阈值，直接丢弃超大的响应数据包。

只要对开放 DNS、SNMP 服务的设备等放大器进行有效防护，就能从根源上杜绝 DDoS 放大攻击的产生。

### (二) ISP 对伪造源 IP 地址的数据包进行过滤

攻击者能够发送伪造源 IP 地址的数据包，这是针对网络带宽资源的 DDoS 攻击能够产生的根本原因。通过伪造源 IP 地址，不仅能够发动反射 DDoS 反射攻击和 DDoS 放大攻击，还能够有效的隐藏攻击来源，降低攻击者面临的风险。如果 ISP 能够对伪造源 IP 地址的数据包进行过滤，使其不能进入到互联网中，就能够从根本上解决针对网络带宽资源的 DDoS 攻击问题。

在 RFC 2827/BCP 38 中高度建议使用入口过滤，以阻止伪造源 IP 地址的网络攻击。遗憾的是，只有少数的公司和 ISP 遵守了这些建议，而只有当所有接入互联网的设备都遵守该规则时，才能彻底阻止伪造源 IP 地址的网络攻击。

### (三) 使用 Anycast 技术对攻击流量进行稀释和清洗

利用 DDoS 放大攻击技术，能够打出很大的流量。对这种规模的攻击，需要对攻击流量在多个清洗中心进行分布式清洗，将攻击流量扩散和稀释，之后在每个清洗中心进行精细的清洗。

使用 Anycast 技术进行防护是一种可行的方案。通过使用 Anycast 技术，可以有效的将攻击流量有效分散到不同地点的清洗中心进行清洗。在正常环境下，这种方式能够保证用户的请求数据被路由到最近的清洗中心；当发生 DDoS 攻击时，这种方式能够将攻击流量有效的稀释到防护方的网络设施中。此外，每一个清洗中心都声明了相同的 IP 地址，攻击流量不会向单一位置聚集，攻击情况从多对一转变为多对多，网络中就不会出现单点瓶颈。在攻击流量被稀释之后，清洗中心对流量进行常规的清洗和阻断就变得相对容易了。

## 四、 总结

DDoS 放大攻击是一种针对网络带宽资源的分布式拒绝服务攻击形式，通常利用网络协议请求与响应数据的不对称、网络服务无需认证以及网络服务部署的广泛性来达到放大攻击流量的效果。

常见的 DDoS 放大攻击技术包括 DNS 放大攻击和 SNMP 放大攻击等，其他一些协议和网络服务也能够作为辅助手段增加 DDoS 放大攻击的流量。

对 DDoS 放大攻击的防护，需要从攻击源头、放大器、被攻击目标三个方面进行防护，才能达到最有效的防护效果。