SYN 代理防御 syn-flood 攻击的原理及实现①

龙 恒

(茂名职业技术学院 实训中心，茂名 525000)

摘 要：syn-flood 是拒绝服务攻击中较为常见的一种，它利用建立 TCP 连接需要进行三次握手的特点，向被攻击者发送大量非法的第一次握手数据包，导致被攻击者建立了大量的处于 SYN_RCVD 状态的 TCP 连接，使得被攻击者无法建立正常的 TCP 连接。首先介绍了 TCP 连接的建立过程，提出了一种代理三次握手的方法来解决被攻击者的资源被大量消耗的问题，经过测试证明，该办法能够较为有效地降低 syn-flood 攻击造成的危害。

关键词：DDoS；syn-flood；三次握手；syn-cookies；SYN 代理

Principle and Realization of SYN Proxy for Defensing Syn-Flood Attack

LONG Heng

(Training Center, Maoming Vocational Technical College, Maoming 525000, China)

Abstract: syn-flood is a common denial of service attack. It uses the characteristics that it requires three-way handshake to establish TCP connection to send a large number of illegal first handshake packet to the target, leading to establish a large number of TCP connections of SYN_RCVD state on the target.So the target cannot establish normal TCP connection. This paper firstly describes the process of establishing a TCP connection,and then proposes a way that agency three-way handshake to solve the problem of over-consumption of resources. It is proved that it can reduce the harm of the syn-flood attack.

Keywords: DDoS; syn-flood; three-way handshake; syn-cookies; syn-proxy

1 引言

拒绝服务攻击(Denial of Service，简称 DoS)是指攻击者使用某种方式对目标计算机或者网络进行攻击，导致目标不能正常提供服务。分布式拒绝服务(Distributed Denial of Service，简称 DDoS)攻击是在 DoS 的基础上发展起来的，攻击者使用多台计算机对目标进行攻击，攻击者通常拥有更多的资源(充足运算能力及带宽)，其破坏力远大于 DoS 攻击，而且比 DoS 攻击更难防范。洪水(flood)攻击是 DDoS 攻击中比较常见的一种，其原理就是向攻击目标发送大量的非法数据包，消耗目标的大量资源，由于它的原理比较简单，攻击者不需要掌握很深专业知识既可发动攻击，使得这种攻击在互联网中比较泛滥。syn-flood 是洪水攻击中破坏力较强的一种，它利用了 TCP 协议的弱点，向攻击目标发送大量非法的第一次握手数据包，导致正常的访问者不能与攻击目标建立 TCP 连接。这种攻击通常比单纯消耗网络带宽的攻击更有杀伤力。

2 TCP连接的建立过程

为了描述方便，把请求建立 TCP 连接的一端称为客户端，把接受请求的那一端称为服务器。TCP 连接建立之前需要进行一个称为三次握手的过程，图 1 显示了这个过程和相关状态的变化：

TCP 首部中含有 6 个比特的控制标志[1]，其中跟三次握手有关的是 SYN 和 ACK 这两个标志。客户端向服务器发送一个 SYN 标志设置为 1 的数据包，客户端进入 SYN_SEND 状态，服务器收到这个 SYN 标志设置为 1 的数据包后进入 SYN_RCVD 状态，这一步称为第一次握手；服务器向客户端发回一个 SYN 和 ACK 标志都设置为 1 的数据包，客户端接收到后进入

① 收稿时间:2010-07-09;收到修改稿时间:2010-07-30

ESTABLISHED 状态，这一步称为第二次握手；客户端向服务器发送一个 ACK 标志设置为 1 的数据包，服务器接收到这个数据包后进入 ESTABLISHED 状态，这一步称为第三次握手，三次握手完成后一个 TCP 连接就成功建立了[2]。

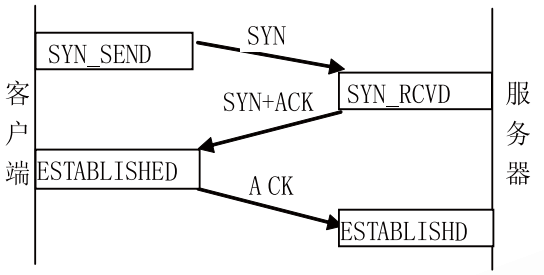

图 1 TCP 三次握手状态变迁图

在 TCP 协议通讯的过程中还有两个用于保证传输可靠性的首部字段：Sequence Number(顺序号，简称为 seq)和 Acknowledgment Number(确认号，简称为 ack)，它们都是 32 位无符号整数计数器，顺序号的初始值是一个由系统确定的整数值[3]，用来表示在当前数据包中包含的数据的第一个字节在整个连接中其中一端所发送的数据的序号，序列号达到 232-1 之后又从 0 开始计数[4]。而确认号是接收端对接收到的数据的确认，它的值是上次接收到的数据包的序列号加上该数据包包含的数据的字节数，另外如果数据包的 SYN 或 FIN 控制位被设置为 1，确认号的数值还要再增加 1，发送端也可以把确认号看作是接收端所期望接收的下一个字节的序号。

3 syn-flood攻击的原理

服务器收到第一次握手数据包后，就会在内核中新建一个处于 SYN_RCVD 状态(半开放状态)的连接，保存完连接后服务器就向客户端发送一个第二次握手的数据包，然后就等待会等待客户端发回一个确认数据包以完成第三次握手。TCP 提供的是一种保证可靠性的传输服务，如果在一定的时间间隔内没有收到客户的确认数据包，就认为是自己发送的第二次握手的数据包在传输过程中丢失了，TCP 就会重复发送第二次握手的数据包，一直到客户端发回确认或者超时为止[5]。

由于发起攻击的客户端的源 IP 地址通常都是不真实的而且攻击者也根本就没想过要给服务器发第二次握手的数据包，因此服务器不可能收到客户端对第二次握手的确认，在客户端发送的伪造的第一次握手的数据包数量非常多的时候，服务器上就会保存了大量的半开放状态的连接，当这些非法连接占完了服务器用于建立 TCP 连接的所有资源后，正常的连接就不能建立，导致服务器无法提供服务，更为严重的是如果非法数据包的数量特别巨大，服务器的处理器资源也会被耗尽，服务器就会处于瘫痪状态。

4 syn代理的原理

从 syn-flood 攻击的原理可以看出，它利用的是 TCP 在第一次握手后会建立大量的半开放状态的连接这个特点发起攻击的，如果在第一次握手的时候服务器不创建半开放状态的连接，而等收到第三次握手数据包后才创建完整的连接，这样服务器中用于建立 TCP 连接的资源就不会因为客户端发送大量非法的第一次握手数据包而耗尽。Linux 的 TCP 协议实现了一个称为 syn-cookies 的机制使用的就是这个原理，它根据第一次握手数据包的源地址、目标地址、源端口、目标端口、序列号、MSS 表的索引以及一个时间值算出一个新的序列号，将这个新的序列号放在第二次握手数据包的序列号字段发送给客户端。当接收到客户端发送的符合第三次握手特征的数据包后，将该数据包的确认号字段减一后与它的源地址、目标地址、源端口、目标端口等信息进行运算以验证合法性，如果验证通过，就认为这个数据包是一个第三次握手的数据包，此时才在内核中创建一个 ESTABLISHED 状态的连接。

syn-cookies 用来对本机进行保护是比较理想的，SYN 代理除了适用于保护本机外也适用于中间设备对目标机器的防护，本文把运行 SYN 代理的设备称为防火墙。SYN 代理的工作过程分为三个阶段，第一阶段是客户端先与防火墙进行三次握手，如图 2 所示，序列号 y 是使用 syn-cookies 算法生成的，整个过程与 syn-cookies 的工作过程相似，不同在于第二次握手是由防火墙代替服务器回应的。

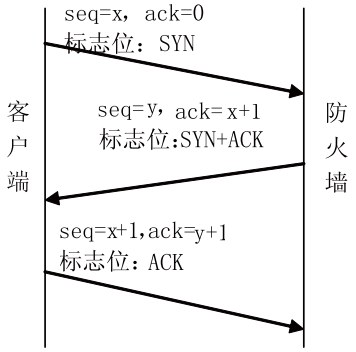

图 2 客户端与防火墙的三次握手

第二阶段是防火墙代替客户端与服务器进行三次握手，过程如图 3 所示，这是一个标准的三次握手，注意这里防火墙发给服务器的序列号的值 x 与客户端发给防火墙的是一样的，这有助于防火墙在后面调整双方序列号的值。

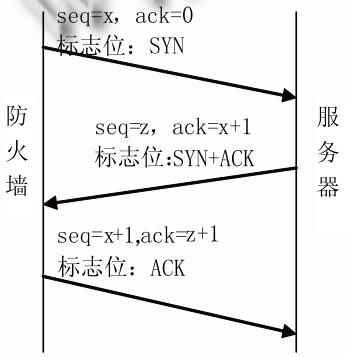

图 3 防火墙与服务器的三次握手

第三阶段就是在连接建立后调整双方在通讯过程中的序列号和确认号，在第二阶段中提到了客户端生成的序列号 x、服务器生成的序列号 z 和防火墙生成的序列号 y。为了能让客户端和服务器能正常通讯，防火墙必须负责校正双方通讯过程中的 ack 和 seq 值，为此防火墙必须保存 y-z 的差值(seq 和 ack 都是无符号整数，因此还要保存差值的正负情况)，防火墙在收到客户端发给服务器的数据包后将数据包的 ack 值修改改为 ack=ack-(y-z)，才将该数据包转发给被服务器，防火墙在收到服务器发给客户机的数据包后，将该数据包的 seq 值修改为 seq=seq+(y-z)，然后才将该数据包转发给客户端。

5 实现

在那些不支持 syn-cookies 的系统中，如果要实现 syn-cookies 就必须修改内核源代码，这在 windows 这种不开源的系统中是无法实现的。SYN 代理的原理相当简单，本文主要讨论一些设计方面的要点：

(1) 设计一个高效及准确的 syn-cookies 算法，Linux 系统中实现的 syn-cookies 算法的准确性很高，客户端发来第三次握手中的确认号几乎无法被伪造，因此在收到一个通过验证的第三次握手数据包后就可以正确地建立一个完整的 TCP 连接，使得客户端无法通过发送大量的非法的第三次握手的数据包进行攻击。但是这个算法的计算量比较大，如果用来保护本机，这种算法是理想的，但是如果作为一个保护多台机器的防火墙设备，就可能需要在准确性和性能方面折中了。

(2) 选择一种保存 TCP 连接信息的数据结构，这个数据结构主要考虑所消耗的内存以及可能保存的最大连接数，如果连接数非常多，就要使用一种在查找方面比较快速的数据结构，在同样的运行环境下进行测试，双方都保存一百万个连接，使用数据包的源地址和源端口作为关键字，哈希表的查找速度比红黑树要快五倍左右。而在连接数较少的情况下使用二叉树比较节省内存，二叉树不需要象哈希表那样预分配一个大内存块，并且在动态增加节点的时候比较方便，而哈希表在需要扩展的时候需要对已经保存的所有节点重新计算该节点在数组中的索引值，并且要调整指针的指向。

(3) 确定内存的分配方式，因为洪水攻击发送过来的数据包数量很大，因此需要使用大量的内存来生成第二次握手的数据包，如果每新建一个数据包都采用动态分配内存的方式就会造成大量的内存碎片从而导致内存的浪费，同时也会影响内存的分配速度。由于每个第二次握手的数据包的大小都是相同的，因此可以每次动态分配一个大的内存块，其大小是一个数据包所使用的内存的若干倍，每生成一个数据包就从这个内存块里为一个数据包申请内存即可，用完一块内存后再动态分配一块，所有这些内存块用链表的形式串联起来，以便于回收。这样可减少内存碎片并且可以提高内存分配的效率。同样，这种分配算法也适用于保存连接信息。

(4) 防火墙在与客户端进行三次握手成功后，客户端可能会立刻就向服务器发送数据，而此时防火墙与服务器的三次握手可能还没有成功，因此无法将数据包转发给服务器。为了避免这种情况，可以在回应客户端的第二次握手的时候将数据包的滑动窗口(Window)字段设为 0。在防火墙与服务器进行第二次握手时保存下服务器发

给防火墙的数据包的 Window 字段的值，假设这个值为 w。然后防火墙在向服务器发送第三次握手数据包的时候同时向客户端发送一个 Window 字段的值为 w 的数据包，根据 TCP 的工作原理可知，客户端在收到这个数据包后才会与服务器进行正常的通讯。

(5) 由于客户端不正常断开连接或者由于 syn-cookies 算法的误判会造成某些 TCP 连接无效，随着防火墙的长期运行，这种无效的连接会越来越多，因此必须设计一种连接节点的回收算法，使得在节点分配到一定的数量后重新利用那些旧的节点，回收最不经常使用的节点是一种选择。

(6) 如果网卡不支持硬件计算校验和，防火墙修改了双方数据包的序列号或确认号后必须要重算数据包的校验和，为了提高效率，防火墙不应该完整地重算整个数据包的校验和，而应该采用 RFC1141 中提出的修改数据包 TTL 值后重算校验和的算法部分重算数据包的校验和[6]。

6 测试

本文用来测试的 SYN 代理是一个笔者开发的软件防火墙中的一个模块，该防火墙是在微软的 passthru 架构的基础上开发的，passthru 是一个工作在内核中的中间层驱动程序，在 TCP/IP 的五层结构中，它工作在链路层和网络层之间。该模块的实现情况是：

① 使用了一个较为高效的但是准确率稍低的 syncookies 算法。

② 使用红黑树来保存 TCP 连接信息。

③ 使用了预分配内存的方法。

④ 回收算法是最不经常使用的节点最先被回收

⑤ 自动检测网卡是否支持计算硬件校验和，如果支持就让网卡重算校验和，如果不支持，就是使用 RFC1141 中的算法重算校验和。

防火墙运行在服务器上，为服务器提供保护，服务器的配置如下：

操作系统：windows 2003R2

CPU：Pentium Dual-Core E5200 @ 2500GHZ

内存：DDR2 1.00G

网卡：Realtek RTL8168C(P)/8111C(P) 千兆以太网卡

使用两台客户机向服务器发起攻击，客户机的配置与服务器相同。

在客户机上向服务器发送大量伪造的第一次握手的数据包，服务器上没有启用 SYN 代理，测试数据如表 1 所示：

表 1 服务器没有开启 SYN 代理的测试数据

数据包数量	CPU 占用率	网络连通情况	网站访问
100000	25%	正常	访问很慢
130000	30%	丢包	无法访问
200000	42%	不通	无法访问

在服务器上启用 SYN 代理后，测试数据如表 2 所示：

表 2 服务器开启 SYN 代理的测试数据

数据包数量	CPU 占用率	网络连通情况	网站访问
100000	10%	正常	访问正常
130000	12%	正常	访问正常
200000	22%	正常	访问正常

本文的提到的数据包数量是从交换机上观察得到的，取的是五分钟内的平均值，在千位上做了四舍五入。从测试数据可以看出，SYN 代理可以有效地防御 syn-flood 的攻击并且可以显著降低攻击造成的 CPU 占用率。

7 结语

只要攻击者拥有足够的资源，DDoS 攻击几乎是无法防范的，而且如果攻击的流量太大，超过了服务器所在的网络容量，所有的防御措施也就失去了意义。本文中对 syn-flood 的攻击的防御是在攻击的流量没有超过服务器的接入带宽的前提下，达到减少服务器的资源消耗的目的，使得服务器能够正常提供服务。SYN 代理原理简单，实践证明其可以有效缓解 syn-flood 攻击造成的影响。

参考文献

1 Information Sciences Institute University of Southern California.RFC793 transmission control protocol. [1981-9-1]. http://tools. ietf.org/html/rfc0793.

2 Comer DE.用 TCP/IP 进行网际互连:原理、协议与结构.北京:电子工业出版社,2004.164－168.

3 Stevens WR.TCP/IP 详解(卷 1:协议).北京:机械工业出版社,2000.174－186.

4 Forouzan BA, Fegan SC. TCP/IP 协议族.北京:清华大学出版社,2006.242－250.

5 李德全.拒绝服务攻击.北京:电子工业出版社,2007.57－86.

6 Mallory T, Kullberg A. RFC1141 Incremental Updating of the Internet Checksum. [1990-1-1]. http://www.ietf.org/rfc/rfc1141. txt