文章编号：2096-1472(2019)-03-29-03
DOI:10.19644/j.cnki.issn2096-1472.2019.03.009

SYN Flood攻击的原理及防御

张文川
(兰州石化职业技术学院，甘肃 兰州 730060)

摘　要：SYN-Flood攻击是当前网络上最为常见的DDoS攻击，也是最为经典的拒绝服务攻击，它利用了TCP协议实现上的一个缺陷，通过向网络服务所在端口发送大量的伪造源地址的攻击报文，就可能造成目标服务器中的半开连接队列被占满，从而阻止其他合法用户进行访问。为了有效防范这种攻击，在分析攻击原理的基础上，发现可以使用TCP代理防御及TCP源探测防御方法来解决这个问题，经过测试证明，该办法能够有效降低SYN Flood攻击造成的危害。

关键词：DDoS攻击；STN Flood攻击；TCP代理防御；TCP源探测防御
中图分类号：TP399　**文献标识码**：A

The Principle and Defense of SYN Flood Attack

ZHANG Wenchuan
(*Lanzhou Petrochemical College of Vocational Technology*,*Lanzhou* 730060,*China*)

Abstract:SYN-Flood attack is the most common DDoS attack and the most classic denial-of-service attack on the current network.It takes advantage of a flaw in TCP protocol implementation and sends a large number of attack packets of forged source addresses to the port where the network service is located,which may cause the semi-open connection queue in the target server to be occupied,thus preventing other legal users from accessing.In order to effectively prevent this attack,on the basis of analyzing the attack principle,it is found that TCP proxy defense and TCP source detection defense methods can be used to solve this problem.Testsprove that this method can effectively reduce the harm caused by SYN Flood attack.

Keywords: DdoSattack;STN Flood attack;TCP proxy defense;TCP source detection defense

1 引言(Introduction)

过去，攻击者所面临的主要问题是网络宽带不足，受限于较慢的网络速度，攻击者无法发出过多的请求。虽然类似“Ping of Death”的攻击只需要较少量的报文就可以摧毁一个没有打过补丁的操作系统，但大多数的DoS攻击还是需要相当大的带宽，而以个人为单位的攻击者很难拥有大量的带宽资源，这个时候就出现了分布式拒绝服务攻击DDoS(Distributed Denial of Service)。DDoS攻击是指攻击者通过控制大量的僵尸主机(俗称“肉鸡”)，向被攻击目标发送大量精心构造的攻击报文，造成被攻击者所在网络的链路拥塞、系统资源耗尽，从而使被攻击者产生拒绝向正常用户的请求提供服务的效果。如图1所示。

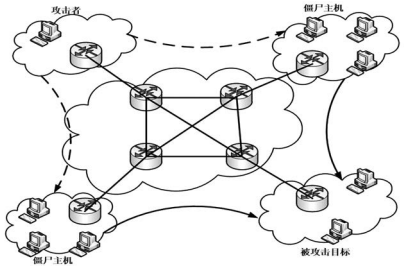

图1 DDoS攻击示意图

Fig.1 DDoS attack schematic

2 SYN Flood攻击原理(Principle of SYN Flood attack)

单从字面上看，SYN Food攻击[1]与TCP协议中的SYN

基金项目：全国工业和信息化职业教育教学指导委员会工信行指委“基于校企合作人才培养模式的信息化教学的研究与实践”项目编号：【2018】20号.

报文有关，在了解SYN Food攻击原理之前，我们先来熟悉一下TCP三次握手的过程，如图2所示。第一次握手：客户端向服务器端发送一个SYN(Synchronize)报文。第二次握手：服务器收到客户端的SYN报文后，将返回一个SYN+ACK的报文，表示客户端的请求被接受，ACK即表示确认(Acknowledgment)。第三次握手：客户端收到服务器的SYN+ACK包，向服务器发送ACK报文进行确认，ACK报文发送完毕，三次握手建立成功。

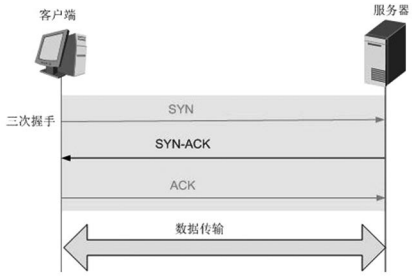

图2 三次握手机制

Fig.2 Three-time handshake mechanism

SYN Flood攻击正是利用了TCP三次握手的这种机制。如图3所示，攻击者向目标服务器发送大量的SYN报文请求，这些SYN报文的源地址一般都是不存在或不可达的。当服务器回复SYN+ACK报文后，不会收到ACK回应报文，导致服务器上建立大量的半连接。这样，服务器的资源会被这些半连接耗尽，导致无法回应正常的请求。防火墙防御SYN Flood攻击时，一般会采用TCP代理和TCP源探测两种方式。

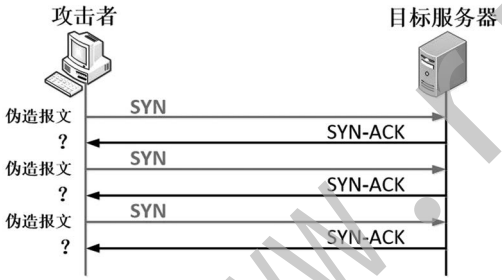

图3 SYN Flood攻击

Fig.3 SYN Flood attack

3 TCP代理防御(TCP proxy defense)

TCP代理[2,3]是指防火墙部署在客户端和服务器中间，当客户端向服务器发送的SYN报文经过防火墙时，防火墙代替服务器与客户端建立TCP三次握手。如图4所示，防火墙先对SYN报文进行统计，如果发现连续一段时间内去往同一目的地址的SYN报文超过预先设置的阈值，则启动TCP代理。启动TCP代理后，防火墙收到SYN报文，将会代替服务器回应SYN+ACK报文，接下来如果防火墙没有收到客户端回应的ACK报文，则判定此SYN报文为非正常报文，防火墙代替服务器保持半连接一定时间后，放弃此连接。如果防火墙收到了客户端回应的ACK报文，则判定此SYN报文为正常业务报文，此时防火墙会代替客户端与服务器建立TCP三次握手，该客户端的后续报文都将直接送到服务器。整个TCP代理的过程对于客户端和服务器都是透明的。TCP代理过程中，防火墙会对收到的每一个SYN报文进行代理和回应，并保持半连接，所以当SYN报文流量很大时，对防火墙的性能要求非常的高。其实，TCP代理的本质就是利用防火墙的高性能，代替服务器承受半连接带来的资源消耗，由于防火墙的性能一般比服务器高很多，所以可以有效防御这种消耗资源的攻击。

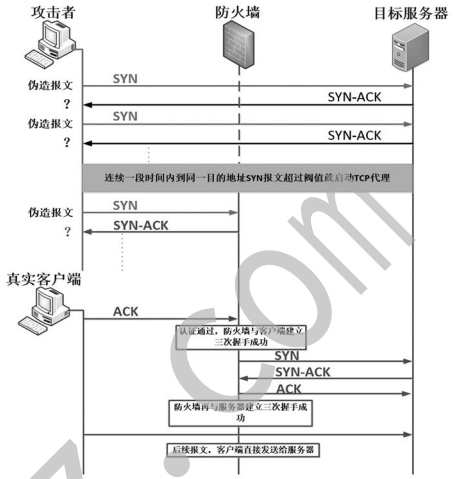

图4 TCP代理防御

Fig.4 TCP proxy defense

4 SYN Flood预防配置命令(SYN flood preventive configuration command)

如表1所示，以USG9500系列防火墙V300R001版本为例，给出了TCP代理和TCP源探测的配置命令[4,5]。

表1 TCP代理和TCP源探测配置命令

Tab.1 TCP proxy and TCP source detection configuration commands

功能	命令行
开启SYN Flood攻击防御功能	firewall defend syn-flood enable
配置基于接口的TCP代理功能	firewall defend syn-flood interface {interface-type interface-number|all} [alert-rate alert-rate-number][max-rate max-rate-number][tcp-proxy {auto|on}]
配置基于IP地址的TCP代理功能	firewall defend syn-flood i pip-address[max-rate max-rate-number] [tcp-proxy{auto|on|off}]
配置基于安全区域的TCP代理功能	firewall defend syn-flood zone zone-name[max-rate max-rate-number] [tcp-proxy{auto |on|off}]
配置TCP源探测功能	Firewallsource-ip detect interface {interface-type interface-number|all} [alert-rate alert-rate-number] [max-rate max-rate-number]

5 TCP源探测防御(TCP source detection defense)

TCP代理过程中，防火墙会对收到的每一个SYN报文进行代理和回应，并保持半连接，所以当SYN报文流量很大时，对防火墙的性能要求非常的高。通常情况下，使用TCP代理[6]可以防御SYN Flood攻击，但是在报文来回路径不一致的网络环境中，TCP代理就会出现问题。因为客户端访问服务器的报文会经过防火墙，而服务器回应给客户端的报文不会经过防火墙。这种情况下，防火墙向服务器发送SYN报文建立TCP三次握手时，服务器回应的SYN+ACK报文不会经过防火墙，TCP代理功能不会成功。所以在报文来回路径不一致的网络环境中，不能使用TCP代理防御SYN Flood攻击。可是在现网中，报文来回路径不一致的场景也是很常见的，那这种情况下如果发生了SYN Flood攻击，防火墙要怎么防御呢?这就是我们所说的第二个防御方法:TCP源探测[7,8]。TCP源探测是防火墙防御SYN Flood攻击的另一种方式，在报文来回路径不一致的场景中也能使用，所以它的应用更加普遍。如图5所示，防火墙先对SYN报文进行统计，如果发现连续一段时间内去往同一目的地址的SYN报文超过预先设置的阈值，则启动TCP源探测。启动TCP源探测后，防火墙收到SYN报文，将会回应一个带有错误确认号的SYN+ACK报文，接下来如果防火墙没有收到客户端回应的RST报文，则判定此SYN报文为非正常报文，客户端为虚假源。如果防火墙收到了客户端回应的RST报文，则判定此SYN报文为正常报文,客户端为真实源。防火墙将该客户端的IP地址加入白名单，在白名单老花前，在这个客户端发出的报文都被认为是合法的报文。

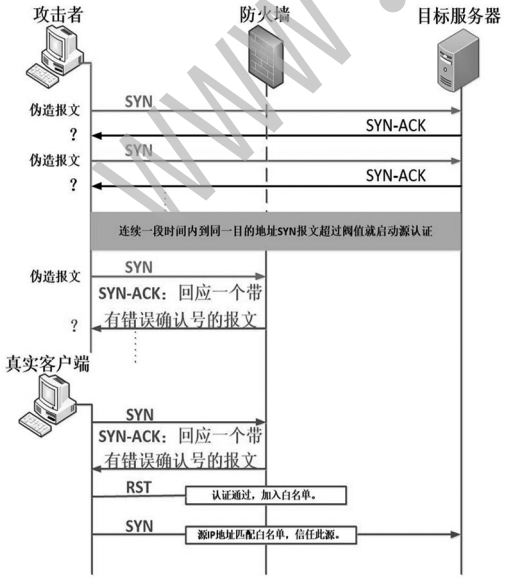

图5 TCP源探测防御方式

Fig.5 TCP source detection defense

6 结论(Conclusion)

STN Flood攻击属于技术含量很高的“高大上”，称霸DDoS攻击领域很久，但是通过分析DDoS攻击原理、SYN Flood攻击原理，我们就可以利用TCP代理防御及TCP源探测防御方法来解决这个问题。TCP代理的本质就是利用防火墙的高性能，代替服务器承受半连接带来的资源消耗，由于防火墙的性能一般比服务器高很多，所以可以有效防御这种消耗资源的攻击。

参考文献(References)

[1] Kumar P,TripathiM,NehraA,et al.SAFETY:Early Detection and Mitigation of TCP SYN Flood Utilizing Entropy in SDN[J].IEEE Transactions on Network & Service Management,2018(99):1.

[2] Zhou J X,LuoK,Wang X C,et al.Ore genesis of the FulePbZn deposit and its relationship with the Emeishan Large Igneous Province:Evidence from mineralogy,bulk COS and in situ SPb isotopes[J].Gondwana Research,2018(54):161-179.

[3] BroichM,Tulbure M G,VerbesseltJ,et al.Quantifying Australia's dryland vegetation response to flooding and drought at sub-continental scale[J].Remote Sensing of Environment,2018(212):60-78.

[4] Shin Seung-won,Kim Ri-young,Jang Jong-song.Analysis of TCP SYN Traffic:An Empirical Study[J].IEEE Trans.on Information Theory,2006,45(8):54-63.

[5] 李馥娟,王群.GPS欺骗攻击检测与防御方法研究[J].警察技术,2018(1):45-48.

[6] 徐书欣,赵景.ARP欺骗攻击与防御策略探究[J].现代电子技术,2018(8):78-82.

[7] 佚名.基于WinPcap的校园网ARP病毒检测防御系统设计与实现[J].测控技术,2018,37(8):46-52.

[8] 张滨,袁捷,乔喆,等.高级持续性威胁分析与防护[J].电信工程技术与标准化,2018(2):48-51.

作者简介：

张文川(1981-)，男，硕士，副教授.研究领域：计算机网络技术.