基于网络测量系统的SYN Flooding攻击防御机制

仇小锋，陈 鸣

(解放军理工大学指挥自动化学院 南京 210007)

【摘要】探索了SYN Flooding攻击的特征，提出了判断攻击发生的关键指标。介绍了网络测量系统的架构，详细阐述了具有服务保护与攻击消除功能的检测方法、攻击源追踪方法。最后分别给出了验证检测机制和追踪机制的实验与结果。

关 键 词 拒绝服务； SYN Flooding攻击； 网络测量； 地址追踪

中图分类号 TP393 文献标识码 A

A Mechanism of Defending SYN Flooding Attack Based on Network Measurement System

Qiu Xiaofeng，Chen Ming

(Institute of Command Automation, PLA University of Science & Technology Nanjing 210007)

Abstract In this paper, the characteristics of SYN flooding attack are explored, some key metrics of judging this kind of attack are proposed. Thereafter, an introduction of the architecture of network measurement system is introduced. Then the detecting method with the features of service-protected and attack-removed, the method of tracing the source of attack are expatiated in detail. Finally, the experiments for validating the mechanisms of detecting and tracing attacks are given.

Key words denial of service; SYN Flooding attack; network measurement; IP traceback

1 SYN Flooding攻击

SYN Flooding攻击是针对TCP连接的三次握手进行的，其原理是使被攻击主机上维持过多的半开连接，耗尽所有的相关资源，致使正常的用户请求因分不到资源而无法响应[1]。通常，此类攻击具有如下的特征：

1) 攻击时，攻击主机发送TCP连接请求的频度会大大超过L / T(L：服务器的最大半开连接数，T：半开连接的超时)。即攻击发生时，在服务器附近的链路上必定充斥着高强度的TCP连接请求报文；2) 攻击者如此高频度的发送会持续相当一段时间，并且持续的时间越长，其攻击产生的影响就越严重，但随之被追踪到的可能性也越大；3) 攻击者必须伪造请求报文的源地址。这些攻击报文可能不停的变换伪造地址，也可能使用同一个伪造地址。但这些地址必须是无法路由到目的地的无效地址或者非活动的有效地址，否则被伪造主机会发送RST报文释放半开连接，导致攻击失败。特征1和特征2是攻击发生的必要条件，特征3是攻击发生的充分条件，同时满足三个特征则是攻击发生的充要条件。因此，在攻击检测工具的实现中则成为判断攻击是否发生的关键指标。

2 网络测量系统

网络测量系统是一个基于被动测量技术对网络业务流进行实时监视，并分析和评估网络性能的网络被

收稿日期：2003 – 10 – 09
基金项目：国家高技术研究发展计划基金资助项目(2001AA112090)
作者简介：仇小锋(1976 –)，男，博士生，讲师，主要从事网络安全和网络测量方面的研究.

动测量系统，其系统配置如图1所示。

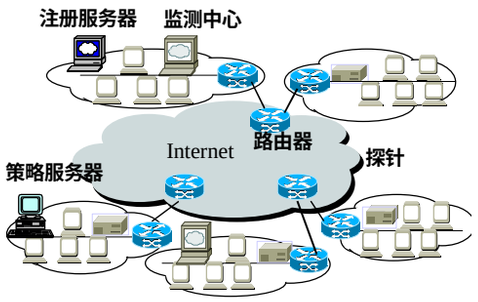

图1 网络测量系统配置图

探针分布在各级网络中的监测点上，是测量操作的实际执行者，其上驻留有多个网络测量工具。根据监测中心用策略语言描述的测量请求，组合调度各种网络测量功能，收集、缓冲和提炼测量数据，并根据需要将结果传回监测中心。

监测中心是测量任务的发起点，也是测量结果的汇集点。根据网络测量策略的语义，在特定事件(状态)发生时向探针(组)发出测量请求，并将探针返回的测量结果进行分析和显示。

注册服务器提供一些公共服务，如组件信息服务、系统时钟服务、组件注册和管理服务等。

策略服务器提供策略的解释和存储。策略(policy)定义了系统需要完成的行为或期望达到的状态 [2]。它把行为的控制和行为的执行分割开来，即定义了什么行为什么时候必须执行，但没有定义该行为包括什么具体动作。所以只要修改策略，就可以在不中断系统服务的情况下改变系统的行为和属性而无需重新编程实现。

3 攻击检测与追踪

根据对SYN Flooding攻击的分析，在网络测量平台上开发了检测和追踪SYN Flooding攻击的两个组件DetSYN和TraceSYN，并且和其他测量工具一样，位于探针上。监测中心通过策略系统调用远程探针上的检测工具监视特定的服务器；如果出现异常，则加强检测，同时采取积极的保护自救措施；一旦确认攻击，立即向监测中心告警；监测中心再根据告警向可疑用户网中的探针(组)发布追踪任务；探针执行完追踪任务后返回追踪结果；监测中心汇总生成攻击追踪报告，确认一个或多个可能的攻击源(网络)；最后，针对这些攻击源采取一些主动防御措施，在源头遏制攻击的发生。

3.1 攻击检测与保护

DetSYN组件具有两个基本功能：半开连接队列的记录与维护以及报文源地址的验证功能。

半开连接队列的记录与维护功能是指对特定服务器的半开连接队列进行监视，使得探针上维护的队列与服务器上实际的半开连接队列尽量相似。主要的操作包括队列的增加、删除和更新。

报文源地址的验证功能是指对报文源地址的有效性和活动性进行验证。首先判断报文源地址是否属于无效地址，如保留地址或广播地址等；其次，进一步验证有效地址的活动性，即源主机是否处于开机状态并与互联网保持物理连接。一旦检测到一定数量的无效地址或非活动地址，则可确认发生了攻击。

近年来，大量的研究表明网络流量呈现自相似性[3]，即具有突发的特性。而网络中95%的流量是采用TCP协议传输的。因此，当网络中某一时刻出现大量TCP连接请求时，并不能武断的认为发生了DoS攻击，而应该尽快的检测，同时启动一些自救措施，保护服务的可用性，称之为服务保护(检测出攻击前)和攻击消除(检测出攻击后)。

服务保护功能是指在检测出攻击前对服务器响应新服务请求所实行的一种“快速通道”机制。服务器允许保持的最大连接数远远大于最大半开连接数，因此，在半开连接队长超过某个阈值M(小于最大半开连接数)后，有选择的允许一定数量(N)的连接请求经过半开连接队列快速进入连接建立状态；而对于超过N部分的请求则拒绝连接，使其快速释放所占的半开连接资源。

攻击消除功能是指在检测出攻击后阻止攻击请求占用服务器资源而满足部分非攻击请求的措施。类似于服务保护，对于攻击请求，使其尽快释放占用的资源；而对于其他请求，则有选择的通过“快速通道”使其进入连接状态，接受服务，如果这些连接在一段时间内没有收到第三次握手，则由探针执行拆链操作，释放占用的TCP连接资源。

3.2 攻击追踪

在攻击发生后，仅仅依靠服务保护和攻击消除，只能减轻被攻击服务器的受灾程度，为少量合法用户继续提供服务，并不能有效的阻止正在发生的攻击。要完全阻断攻击，必须找出攻击源或者攻击源所在的

网络，从源头上彻底遏制攻击行为的发生。

DetSYN检测到攻击后，向监测中心报告攻击信息；监测中心根据报告的内容及相关策略，组织新的追踪任务，并向适当的探针集合发布，或者向其他监测中心发送协同追踪请求。探针接到追踪任务后，立即启动TraceSYN工具并读取执行参数，包括被攻击主机地址和端口、攻击类型、攻击发生的时间、攻击追踪的有效期TTL以及告警阈值M等。接着探针开始过滤附近经过的流数据，记录具有攻击特征(发往被攻击主机的特定端口)的流数量。如果流数量超过了告警阈值M，或者执行时间超过了追踪有效期，则向监测中心返回追踪结果。监测中心汇总所有的追踪结果，形成最终的攻击追踪报告。

在攻击追踪中，攻击追踪报告的可信度直接取决于如何选取适当的追踪探针集合。如果选取的追踪探针集合覆盖了攻击源所在的网络或者攻击流经的网络，那么最后的攻击追踪报告就是可信的；反之结果就不可信。由于探针通常部署在每个本地网的出口点，所以可以选取被攻击服务器所在自治域的每个出口点(边界路由器)附近的探针作为首次执行追踪任务的探针集合。

4　实验与分析

4.1　攻击检测实验

1) 构建如图2所示的攻击检测环境。为了降低实验复杂性，网络测量系统只包含探针和监测中心，一些策略和指令在监测中心上通过手工进行加载；服务器(PⅣ, Win2000 Server)提供Web服务；攻击源(PⅢ, Linux)能够伪造源IP地址和端口，向服务器发送指定频率的SYN Flooding攻击分组流。发送攻击分组时，采用依次递增的源端口号，以便用源端口号表示分组发送的先后次序。2) 对服务器的半开连接性能进行测试。测得其半开连接最大队长约为46，超时约为21 s。即在21 s内如果服务器连续收到超过46个TCP连接请求，并且这些请求都没有成功建立连接，则没有竞争到半开连接队列的请求将被拒绝服务。3) 分别产生4 分组/s和40 分组/s的攻击分组流，对服务器进行攻击，并分别使用常规的统计检测方法和DetSYN方法检测攻击。常规的统计检测方法通常只是简单的依据TCP连接请求到达服务器的速率来判断攻击，而不考虑这些请求有无实际占用半开连接队列。实验中，记录每个超时内到达的TCP连接请求数，如果请求数超过半开连接最大队长，则认为有攻击发生，尽管这些请求中可能包含了少量的合法请求。DetSYN方法中，设置启动快速通道的阈值M为40；设置每次快速通道启动后，准入的最大请求数N为1 000；设置源地址验证的超时时间为1.5 s。

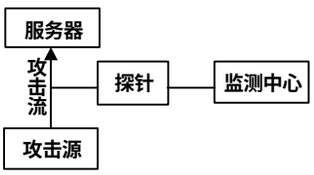

图2　攻击检测的实验环境

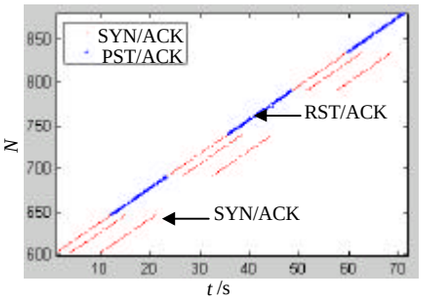

图3　攻击时服务器的响应情况

DetSYN方法与统计检测方法的比较如表1所示。攻击时服务器的响应情况如图3所示，由图中可知，当服务器遭到攻击时，呈现出较明显的周期性拒绝服务，服务器在一段时间内持续的拒绝所有的服务请求，而在随后的一段时间内可能接受某些服务请求。实验中我们用拒绝服务持续的时间占整个周期的比重来粗略的表示拒绝服务的比率。经过多次实验得到的结果数据如表1所示。

由实验结果可知，虽然使用DetSYN方法可能导致检测攻击的时延略有增加，但对用户而言，其服务请求都不会遭到拒绝，充分保证了服务的可用性；用DetSYN方法检测攻击需要的最小攻击分组数较统计检测方法要低，提高了检测工具的灵敏度；实际的拒绝服务的比率要大于表1中的数值，这是因为当半开连接队列溢出时所有请求都被拒绝服务，但当半开连接队列未满时用户的请求未必一定被接收，它需要和攻击请求竞争有限的半开连接资源，这些资源随着队列中的半开连接不断超时而逐渐被释放。

表1 DetSYN方法与统计检测方法的比较

主体	性能	攻击速率/分组·s^{-1}	统计检测方法	DetSYN方法
服务器	服务器拒绝服务的时延	4	11.339 s	No DoS
		40	1.176 s	No DoS
攻击者	攻击所需最小攻击分组数	4	47	∞
		40	47	∞
检测工具	检测所需的最小攻击分组数	4	47	41
		40	47	41
	检测攻击的时延	4	11.339 s	11.631 s
		40	1.176 s	2.774 s
客户	拒绝服务的比率	4	>52.92%	0
		40	>94.43%	0

4.2 攻击追踪实验

首先，搭建了如图4所示的攻击追踪实验网络，用路由器连接四个网段构建了一个简单的广域网环境。然后从攻击主机向服务器发起强度为20 分组/s的攻击流，并从用户主机通过多线程下载工具下载服务器上的文件。接着在监测中心上手工加载策略：

SchPolicy = { (10001, M1, when(now), {P2，P3，P4}, START,
T10001, TraceSYN, {192.9.201.65, 80, SYN Flooding, 45, 90 }) }

该策略包含一条标识为10001的策略规则。其含义是监测中心M1立即在探针组{ P2，P3，P4}上加载攻击追踪(TraceSYN)任务T10001，其中目的主机的地址是192.9.201.65，端口为80，攻击类型为SYN Flooding，追踪有效期*TTL*为45 s，告警阈值*M*为90。

最后监测中心经过一段时间(略大于追踪有效期)收到所有追踪探针返回的追踪结果，经过汇总得到最后的攻击报告，如表2所示。在追踪有效期(45 s)内，192.9.203.0网络收集到了6个发往服务器(192.9.201.65:80)的流，192.9.204.0网络没有发现这样的流，而192.9.202.0网络在4.593 s内就收集到了90个攻击流。由此，可以断定攻击来自192.9.202.0网络的可能性最大，来自192.9.204.0网络的可能性最小。

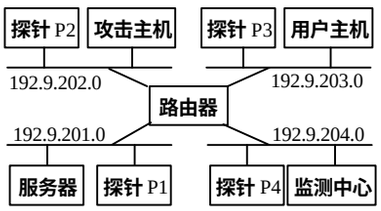

图4 攻击追踪实验的网络环境

表2 攻击追踪报告

攻击192.9.201.65:80的追踪报告 *M*=90, *TTL*=45 s			
探针所在网络	流数量/个	耗时/s	疑似度
192.9.202.0	90	4.593	高
192.9.203.0	6	45	中
192.9.204.0	0	45	低

5 小 结

本文提出的SYN Flooding攻击防御机制能在及时有效地检测攻击的同时保护正常的服务，并能快速协同地追踪出攻击源网络。下一步作者将研究如何扩展该防御机制以适应其他的DoS和DDoS攻击。

参 考 文 献

[1] 颜学雄, 王清贤, 李梅林. SYN Flooding攻击原理及预防方法[J]. 计算机应用, 2000, 20(8): 41-43

[2] Lupu E. A Role-based framework for distributed system management[D]. London: University of London, 1998

[3] Paxson V, Floyd S. Wide area traffic: the failure of Poisson modeling[J]. IEEE/ACM Transactions on Networking, 1995, 3(3): 226-24

编 辑 漆 蓉