文章编号:1000 - 582X(2004)06 - 0013 - 04

状态防火墙受攻击导致状态表溢出故障的解决*

杨 劲
(重庆工商大学 计算机工程与信息科学学院,重庆 400020)

摘 要:网络防火墙的状态检测就是针对连接请求的数据包,检查连接实体其是否符合 TCP/IP 协议的状态转换规则,相符则接收数据。DoS/DDoS 攻击通过在短时间内发送大量短小的数据包给防火墙,造成状态表被填满而拒绝接收新的连接,导致产生拒绝服务攻击。传统的解决方案往往增加防火墙的负担。针对网络上常见的流量型 DoS/DDoS 攻击造成的状态防火墙状态表溢出故障提供一种应急解决方案。

关键词:网络安全;状态防火墙;DoS/DDoS 攻击
中图分类号:TP309.2 **文献标识码**:A

由于 TCP/IPv4 协议族本身不足以保障计算机网络的信息安全[1],因此在网络工程实践中普遍采用附加措施,以求得在一定程度上小范围的自我保护。防火墙是目前重要而且关键的技术之一。在早期应用环境中,防火墙的计算能力一般远高于通信线路对计算的需求,常规技术下的防火墙能够很好地工作。但是随着通信技术和市场的发展,计算机网络带宽不断增长,应用也趋于多样化,防火墙越来越成为网络出口的瓶颈。在这样的形势下对防火墙新技术新体系结构的研究逐渐成为计算机网络安全中的一个重要研究课题。

从总体上看防火墙可分为两大类包过滤防火墙和应用级防火墙[2-3]。包过滤防火墙效率高,但功能受限,技术成熟稳定。应用级防火墙特指防火墙要在应用级如 http, telnet 对数据进行过滤,效率一直是应用级防火墙的瓶颈。代理服务器是应用级防火墙之一,但通用性不好,效率较低,高端防火墙一般不采用代理服务器方案。基于状态检测的包过滤防火墙(简称状态防火墙)是对包过滤防火墙的扩展和优化。

DoS(Denial of Service 拒绝服务)和 DDoS(Distributed Denial of Service 分布式拒绝服务)攻击是大型网站和网络服务器的安全威胁之一。此类攻击利用合理的服务请求占用过多的服务资源,从而使合法用户无法得到服务响应的网络攻击行为。例如典型的 DoS/DDoS 攻击 SYN Flood 就是利用 TCP 协议缺陷造成资源耗尽和资源过载,而当一个对资源的合理请求大大超过资源的支付能力时,合法的访问者将无法享用合理的服务。DoS/DdoS 除了攻击网络主机以外,还可能对于网络上的所有网络设备构成威胁。其中,由于防火墙往往处于要保护的网络资源的外围,因此最容易受到攻击。目前,比较常见的 DoS/DDoS 攻击主要还有 UDP Flood、ICMP Flood、Crikey CRC Flood 及其变种攻击等。

1 状态防火墙的工作原理

1.1 状态防火墙工作流程

包过滤防火墙对数据包头信息进行解析,并与规则库中的安全规则进行匹配决定,数据被丢弃还是放行。为了对这一机制进行进一步的优化,CheckPoint® 首先提出了基于状态检测的包过滤防火墙的改进技

* 收稿日期:2004 - 01 - 03
基 金 目:国家自然科学基金资助项目(60372101)
作者简介:杨劲(1968 -),男,重庆人,重庆工商大学讲师,主要从事多媒体网络技术研究。

术。开发状态检测功能是为了让规则能够运用到会话发起过程,从而提高防火墙的强度。

状态防火墙基于这样一个基本事实:网络中大部分数据是通过面向连接的TCP协议传输的,只要控制了连接建立过程,那么可以认为整个通信过程是可信的[4-5]。状态检测防火墙查看包头后,根据规则集作出决定。阻挡或允许访问的决定适用于该会话后来的所有包(会话则由来源、目标地址、协议和时间因素确定)。基于状态检测的包过滤防火墙数据处理流程如图1所示。

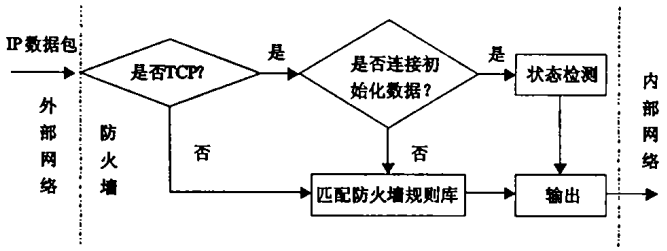

图1 状态防火墙数据处理流程

从图1中可以看出,通信中的很大一部分数据能够绕过运算复杂的规则库匹配过程。对于取而代之的状态检查,因此这是一个简洁高效的处理过程。

1.2 状态防火墙工作机制

笔者以对象的方式描述和管理连接实体,每个实体是一个对象,对象有生命周期属性和方法。

实体的产生:每一次Client和Server之间连接的3次握手(Three-way Handshake)过程,构成一个实体的生成过程。这是一个临时过程,如果连接成功,则防火墙生成一个完整实体;如果连接失败,则释放本次连接占用的资源。建立过程中的实体称为未成熟实体。

实体的状态:实体记录连接的当前状态(例如双方连接序号、已确认数据、半连接状态等信息),并随通信的进行,不断更新实体状态。实体状态分为两类:一类是经过确认的状态,另一类为临时状态。当收到数据时,实体先进入临时状态,收到接收端确认信息后再将临时状态修正为确认状态,这一措施可避免实体状态同通信双方不同步问题。

实体的方法:对于非连接请求数据包,如果它不属于任何实体,则被直接丢弃。对属于某一实体的数据包,实体检查其是否符合TCP/IP协议的状态转换规则[6-7],相符则接收数据,否则丢弃。

这样,系统每接收到数据包,则在实体集中匹配所属实体,如果匹配成功,数据包被转交给所属实体做进一步处理。实体的功能决定了防火墙过滤功能的强度,匹配算法的效率决定了防火墙的整体效率。

2 DoS/DdoS攻击

2.1 DoS/DDoS攻击原理

DoS/DDoS攻击通过伪造超过服务器处理能力的访问数据耗尽系统资源而造成服务器响应阻塞,使目标计算机无法提供正常的服务。系统资源包括网络带宽、文件系统空间容量、开放的进程或者允许的连接等。

从攻击类型来看,DoS/DDoS攻击主要分为针对一切网络设备的流量型攻击(这是目前主要的DoS/DDoS攻击形式)、针对主机的堆栈突破型攻击和针对系统漏洞的特定型攻击。典型流量型攻击方法有SYN Flood、ACK Flood、UDP Flood、ICMP Flood和MStream Flood等,而堆栈突破型攻击包括Winnnuke、Jolt、Teardrop等。

流量型攻击之所以很难预防,在于它利用了TCP协议本身的弱点。以SYN Flood为例,攻击者在TCP连接实体产生(3次握手)过程中,假造向服务器发送了SYN报文后突然死机或掉线,使服务器在发出SSYN+ACK应答报文后是无法收到客户端的ACK报文的(第3次握手无法完成),形成大量的未成熟实体(半连接),而消耗非常多的资源,最后导致服务器失去响应。

而基于非连接的ICMP/UDP Flood攻击的原理更简单,攻击者采用大量经过伪造的小包攻击,降低目标主机和网络的处理能力,如果调动多台攻击机,甚至可造成直接的带宽阻塞。

对于防火墙而言,同样要对网络上的连接请求进行判断和处理,因此对于服务器可以进行有效攻击的DoS/DdoS工具往往也可以用于防火墙上。这种攻击对于处理速度非常快的包过滤防火墙而言可能不太奏效,但是对于基于状态检测的防火墙可能就会造成防火墙的瘫痪。

2.2 DoS/DdoS对于状态防火墙的攻击

目前常见的大多数状态防火墙产品都使用状态表判断是否获得的包属于两个主机间已经存在的会话,当防火墙遇到包匹配规则库但不匹配当前定义的状态时,状态表中会增加一条新的会话条目。防火墙根据

不同原因会从状态表中移去相关条目，这些原因包括会话 time - out 值过期，检测到 TCP FIN 或者 TCP、RST 包等。

如果新的状态条目增加速度超过防火墙删除条目的速度，远程攻击者将可以利用此缺陷填满所有状态表缓冲区，导致产生拒绝服务攻击。

攻击者可以发送短小的，大量匹配规则库的包给防火墙，这样新的条目增加就可能超过防火墙删除的速度，状态表就可以很容易的被填满，导致许多防火墙实现对那些不匹配已经存在会话状态的包拒绝接受，而新的连接也将不能建立，使得产生拒绝服务攻击。

攻击者可以利用下面几种方法进行攻击：

1) TCP SYN Flood

为了建立 TCP 连接，客户端和服务器端必须参与 3 次握手。客户端系统通过发送 SYN 消息给服务器，然后服务器通过发送 SYN - ACK 消息应答 SYN 消息给客户端。客户端最后通过应答 ACK 消息完成建立连接，然后进行数据传输。

在 SYN FLOOD 攻击中，攻击者可以发送伪造 IP 源地址的 SYN 包，使得这些通信看起来来自多个客户端。假如这些包匹配防火墙规则，就会建立状态表跟踪这些连接。由于客户端地址是伪造的，发送给客户端的 SYN - ACK 消息将被丢弃，大量此类通信可导致防火墙装条表被伪造条目填满，产生拒绝服务攻击。

2) UDP Flood

在 UDP FLOOD 攻击中，攻击者可发送大量伪造源 IP 地址的小 UDP 包。但是，由于 UDP 协议是无连接性的，没有一些会话状态指示信息（SYN、SYN - ACK、ACK、FIN 或 RST）帮助防火墙检测不正常的协议状态。结果，基于状态的防火墙必须依靠源和目的地址建立状态表条目和设置会话超时值。大量此类信息填充状态表可导致防火墙产生拒绝服务攻击。

3) Crikey CRC Flood

2002 年美国的研究者 Stephen Gill 报告了一种新的攻击基于状态防火墙的方法，他称为 Crikey CRC Flood（C2 Flood）。CRC 校验在每个网络层中计算，并用来判断传输中是否数据有破坏。C2 Flood 是一种包含传输层（TCP，UDP）非法检验和的包，由于传输层的检查不经过防火墙操作，多种实现选择了通过忽略这些校验来优化性能，因此如果 C2 Flood 类型的包匹配防火墙规则，就会在防火墙中建立会话表条目，并传递非法数据包到目的地址。

但是与防火墙不同，目的主机必须对接收到的包进行校验操作，由于接收到的是非法数据包，因此主机就会简单的丢弃 C2 Flood 包，由于没有对源主机进行应答因此源主机也不会进行重传操作。这就导致防火墙由于没有接收到任何目的地址反馈，而不能进行有效的调整状态表，导致产生状态表被填满，拒绝接收新的连接。

3　问题的解决

3.1　现有解决方案的缺陷

DoS/DDoS 的攻击原理和源代码早已公布，但基于同样原理的攻击依然频繁发生而目前却鲜有完全有效的解决方法。

研究人员想出了一切应对 DoS 攻击的方法：在人们熟知的防火墙、IDS、VPN 甚至杀毒软件中，增加了预防 DoS/DDoS 攻击的技术，如设置诸如 Random Drop、SYN Cookie、带宽限制之类的防护算法。或者让 IDS 与防火墙联动，在 IDS 通过旁路检测到 DoS 攻击后，立即给防火墙发布指令，抛弃无效的连接或半连接。这些措施（例如 Syn Cookie/Syn gate 技术）往往是为了保护服务器，而加重了防火墙的负担，往往造成防火墙的迅速瘫痪，并造成受保护主机无法与外界通讯，正好实现了拒绝服务攻击的效果。

3.2　应急解决方案

既然现在还没有完善的防止 DoS/DDoS 攻击的解决方案，那么临时解决方案往往是遭遇攻击时网络管理者首先选择的措施：

1) 使用防火墙功能检测和阻挡淹没通信

目前有不少防火墙产品已经提供了检测和阻挡 UDP 和 TCP SYN Flood 攻击功能。虽然效果有好有坏，建议管理员使用这些防火墙功能。

2) 使用动态更改状态表大小

状态表使用动态分配可以动态的调整状态条目，在需要的时候增加防火墙用于存储状态表缓存的容量，可以一定程度上增加攻击者利用这个漏洞的难度。

3) 对初始会话使用分离的 Time - out 值

对初始化和已建立会话维护分离不同的会话超时值，允许攻击通信产生的条目快速删除，不过仍旧维护状态表中的合法条目。

4) 使用动态调整会话时间（Aggressive Aging）

会话超时值减少的情况下,攻击者必须增加攻击强度以确保新建立的条目能快于防火墙删除这些条目的速度。通过使用动态会话时间,可以减低状态表收敛的时间,使攻击难度增加。

5) 允许连接跟踪关闭

对部分协议关闭连接跟踪功能,可以增加攻击难度。

4 结束语

针对网上常见的 DoS/DdoS 流量类攻击对于状态防火墙的影响进行了分析和探讨,并提供了一些应急处理措施,由于网络上的 DoS/DdoS 攻击类型数量繁多,各有特点,并不断的发展,因此只能对大多数的目前的 DoS/DdoS 流量类攻击有作用,要彻底解决 DoS/DdoS 的影响,目前的技术条件还无法实现。

参考文献:

[1] STEVEN M BELLOVIN. Security problems in the TCP/IP protocol suite[J]. Computer Communications Review, 1989, 19(3):10 - 19.

[2] STEVEN M BELLOVIN, CHESWICK WR. Network firewalls[J]. IEEE Communications Magazine, 1994, 32(9): 50 - 56.

[3] GB/T 18019 - 1999, GB/T18020 - 1999, GB/T17900 - 1999, 防火墙国家标准[S].

[4] CheckPoint Software Technologies Ltd. Stateful Inspection Technology[R], 1996.

[5] RFC791, Internet Protocol[S], 1981.

[6] RFC793, Transmission Control Protocol[S], 1981.

Solution of Stateful Firewall's Iptables Overflow Caused by Attack

YANG Jin

(Computer College, Chongqing Technology Business University, Chongqing 400020, China)

Abstract: The intensity and efficiency are two centrally technical indicator of the firewall. The function of state checking of network's fire wall is to check the coming data pack, to judge if those connected entities are accordant with the rule of TCP/IP exchange. Attacks of DoS/DDoS send large numbers of short data packs to firewall in a short time. Those attacks may make firewall's iptables overflow and refuse new connection. The traditional solutions often increase the burden of the firewall. This paper puts a new temporary way to solution this problem in emergent state.

Key words: network security; stateful firewall; attack of DoS/DDoS

(编辑 张小强)