dos攻击

[锁定](https://baike.baidu.com/view/10812319.htm)

本词条由[“科普中国”百科科学词条编写与应用工作项目](http://www.cast.org.cn/) 审核 。

DoS是Denial of Service的简称，即拒绝服务，造成DoS的攻击行为被称为DoS攻击，其目的是使计算机或网络无法提供正常的服务。最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。[1]

DoS攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。这种攻击会导致资源的匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快都无法避免这种攻击带来的后果。[1]

**中文名**

dos攻击

**外文名**

Denial of Service

**含    义**

拒绝服务

**目    的**

使计算机或网络无法提供正常服务

**例    子**

计算机网络带宽攻击和连通性攻击

目录

1. 1 [综述](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#1)
2. ▪ [概念理解](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#1_1)
3. ▪ [攻击流程](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#1_2)
4. ▪ [攻击手段](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#1_3)
5. ▪ [攻击方法](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#1_4)
6. ▪ [攻击程序](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#1_5)
7. 2 [防范](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2)
8. ▪ [SYN Flood攻击](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2_1)
9. ▪ [Smurf攻击：](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2_2)
10. ▪ [Ping of Death](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2_3)
11. ▪ [泪滴攻击](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2_4)
12. ▪ [DRDOS](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2_5)
13. ▪ [退让策略](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2_6)
14. ▪ [防火墙](https://baike.baidu.com/item/dos%E6%94%BB%E5%87%BB/3792374?fr=aladdin#2_7)

综述

概念理解

DoS到底是什么？接触PC机较早的同志会直接想到微软磁盘操作系统的DOS--DiskOperationSystem？不，此DoS非彼DOS也，DoS即DenialOfService，拒绝服务的缩写。[1] 

作个形象的比喻来理解DoS。街头的餐馆是为大众提供餐饮服务，如果一群地痞流氓要DoS餐馆的话，手段会很多，比如霸占着餐桌不结账，堵住餐馆的大门不让路，骚扰餐馆的服务员或厨子不能干活，甚至更恶劣……相应的计算机和网络系统则是为[Internet](https://baike.baidu.com/item/Internet)用户提供互联网资源的，如果有[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)要进行DoS攻击的话，可以想象同样有好多手段！今天最常见的DoS攻击有对计算机网络的带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用[网络资源](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E8%B5%84%E6%BA%90)都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击指用大量的连接请求冲击计算机，使得所有可用的[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。[1]

传统上，攻击者所面临的主要问题是[网络带宽](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B8%A6%E5%AE%BD)，由于较小的网络规模和较慢的[网络速度](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E9%80%9F%E5%BA%A6)的[限制](https://baike.baidu.com/item/%E9%99%90%E5%88%B6)，攻击者无法发出过多的请求。虽然类似“the [ping](https://baike.baidu.com/item/ping) of death”的攻击类型只需要较少量的包就可以摧毁一个没有打过[补丁](https://baike.baidu.com/item/%E8%A1%A5%E4%B8%81)的UNIX系统，但大多数的DoS攻击还是需要相当大的带宽的，而以个人为单位的[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)们很难使用高带宽的资源。为了克服这个缺点，DoS攻击者开发了分布式的攻击。攻击者简单利用工具集合许多的[网络带宽](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B8%A6%E5%AE%BD)来同时对同一个目标发动大量的攻击请求，这就是[DDoS](https://baike.baidu.com/item/DDoS)(Distributed Denial of Service)攻击。[1]

无论是DoS攻击还是DDoS攻击，简单的看，都只是一种破坏网络服务的[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)方式，虽然具体的实现方式千变万化，但都有一个共同点，就是其根本目的是使受害[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)或网络无法及时接收并处理外界请求，或无法及时回应外界请求。其具体表现方式有以下几种：[1]

1，制造大[流量](https://baike.baidu.com/item/%E6%B5%81%E9%87%8F)无用数据，造成通往被攻击[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)的[网络拥塞](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%8B%A5%E5%A1%9E)，使被攻击主机无法正常和外界通信。[1]

2，利用被攻击[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)提供服务或[传输协议](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE)上处理重复连接的[缺陷](https://baike.baidu.com/item/%E7%BC%BA%E9%99%B7)，反复高频的发出攻击性的重复服务请求，使被攻击主机无法及时处理其它正常的请求。[1]

3，利用被攻击[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)所提供服务[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)或[传输协议](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE)的本身实现[缺陷](https://baike.baidu.com/item/%E7%BC%BA%E9%99%B7)，反复发送畸形的攻击数据引发系统错误的分配大量[系统资源](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E8%B5%84%E6%BA%90)，使主机处于[挂起状态](https://baike.baidu.com/item/%E6%8C%82%E8%B5%B7%E7%8A%B6%E6%80%81)甚至死机。[1]

使用僵尸电脑进行DOS攻击

僵尸电脑（Zombie computer），简称“僵尸（zombie）”，有些人称之为“肉鸡”，接入互联网的电脑被病毒感染后，受控于黑客，可以随时按照黑客的指令展开拒绝服务（DoS）攻击或发送垃圾信息。通常，一部被侵占的电脑只是僵尸网络里面众多中的一环，而且会被用来去运行一连串的或远端控制的恶意程序。很多“僵尸电脑的拥有者”都没有察觉到自己的系统已经被“僵尸化”，就仿佛是没有自主意识的僵尸一般。[1]

攻击流程

要理解dos攻击，首先要理解TCP连接的[三次握手](https://baike.baidu.com/item/%E4%B8%89%E6%AC%A1%E6%8F%A1%E6%89%8B)过程(Three-wayhandshake)。在[TCP/IP协议](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE)中，TCP协议提供可靠的连接服务，采用三次握手建立一个连接。[1]

第一次握手:建立连接时，[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)发送SYN包((SYN=i)到服务器，并进入SYN SEND状态，等待服务器确认;

第二次握手:服务器收到SYN包，必须确认客户的SYN (ACK=i+1 )，同时自己也发送一个SYN包((SYN=j)}即SYN+ACK包，此时服务器进入SYN\_RECV状态;[1]

第三次握手:客户端收到服务器的SYN+ACK包，向服务器发送确认包ACK(ACK=j+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手，客户端与服务器开始传送数据。[1]

在上述过程中，还有一些重要的概念:[1]

半连接:收到SYN包而还未收到ACK包时的连接状态称为半连接，即尚未完全完成三次握手的TCP连接。

半连接队列:在三次握手协议中，服务器维护一个半连接队列，该队列为每个客户端的SYN包(SYN=i )开设一个条目，该条目表明服务器已收到SYN包，并向客户发出确认，正在等待客户的确认包。这些条目所标识的连接在服务器处于SYN\_ RECV状态，当服务器收到客户的确认包时，删除该条目，服务器进入ESTABLISHED状态。

Backlog参数:表示半连接队列的最大容纳数目。[1]

SYN-ACK重传次数:服务器发送完SYN-ACK包，如果未收到客户确认包，服务器进行首次重传，等待一段时间仍未收到客户确认包，进行第二次重传，如果重传次数超过系统规定的最大重传次数，系统将该连接信息、从半连接队列中删除。注意，每次重传等待的时间不一定相同。[1]

半连接存活时间:是指半连接队列的条目存活的最长时间，也即服务从收到SYN包到确认这个报文无效的最长时间，该时间值是所有重传请求包的最长等待时间总和。有时也称半连接存活时间为Timeout时间、SYN\_RECV存活时间。[1]

上面三个参数对系统的TCP连接状况有很大影响。[1]

SYN洪水攻击属于DoS攻击的一种，它利用TCP协议缺陷，通过发送大量的半连接请求，耗费CPU和内存资源。SYN攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统，事实上SYN攻击并不管目标是什么系统，只要这些系统打开TCP服务就可以实施。从图4-3可看到，服务器接收到连接请求(SYN=i )将此信息加入未连接队列，并发送请求包给客户端( SYN=j,ACK=i+1 )，此时进入SYN\_RECV状态。当服务器未收到客户端的确认包时，重发请求包，一直到超时，才将此条目从未连接队列删除。配合IP欺骗，SYN攻击能达到很好的效果，通常，客户端在短时间内伪造大量不存在的IP地址，向服务器不断地发送SYN包，服务器回复确认包，并等待客户的确认，由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造的SYN包将长时间占用未连接队列，正常的SYN 请求[1]

被丢弃，目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。过程如下:[1]

攻击主机C(地址伪装后为C&apos;)-----大量SYN包---->被攻击主机[1]

C&apos;<-------SYN/ACK包----被攻击主机[1]

由于C’地址不可达，被攻击主机等待SYN包超时。攻击主机通过发大量SYN包填满未连接队列，导致正常SYN包被拒绝服务。另外，SYN洪水攻击还可以通过发大量ACK包进行DoS攻击。

攻击手段

[拒绝服务攻击](https://baike.baidu.com/item/%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1%E6%94%BB%E5%87%BB)是一种对网络危害巨大的恶意攻击。今天，DoS具有代表性的攻击手段包括PingofDeath

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/62667cd0781718c2a0ec9cc7?fr=lemma&ct=single)dos攻击快闪族

、TearDrop、UDPflood、SYNflood、LandAttack、IPSpoofingDoS等。看看它们又是怎么实现的。[1]

**死亡之ping (pingofdeath)DengKelen**

ICMP(InternetControlMessageProtocol，[Internet控制信息协议](https://baike.baidu.com/item/Internet%E6%8E%A7%E5%88%B6%E4%BF%A1%E6%81%AF%E5%8D%8F%E8%AE%AE))在Internet上用于错误处理和传递控制信息。最普通的ping[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)就是这个功能。而在TCP/IP的RFC文档中对包的最大尺寸都有严格限制规定，许多[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)的[TCP/IP协议](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE)栈都规定ICMP包大小为64KB，且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)。"PingofDeath"就是故意产生畸形的测试Ping（PacketInternetGroper）包，声称自己的尺寸超过ICMP上限，也就是加载的尺寸超过64KB上限，使未采取保护措施的网络系统出现[内存分配](https://baike.baidu.com/item/%E5%86%85%E5%AD%98%E5%88%86%E9%85%8D)错误，导致TCP/IP协议栈崩溃，最终接收方[宕机](https://baike.baidu.com/item/%E5%AE%95%E6%9C%BA)。[1]

**泪滴**

[泪滴攻击](https://baike.baidu.com/item/%E6%B3%AA%E6%BB%B4%E6%94%BB%E5%87%BB)利用在TCP/IP协议栈实现中信任IP碎片中的包的标题头所包含的信息来实现自己的攻击。[IP](https://baike.baidu.com/item/IP)分段含有指示该分段所包含的是原包的哪一段的信息，某些TCP/IP协议栈（例如NT在servicepack4以前）在收到含有重叠偏移的伪造分段时将崩溃。[1]

**UDP**[泛洪](https://baike.baidu.com/item/%E6%B3%9B%E6%B4%AA)

**(UDPflood)**

UDPflood攻击：如今在Internet上UDP（用户[数据包](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8C%85)协议）的应用比较广泛，很多提供WWW和Mail等服务[设备](https://baike.baidu.com/item/%E8%AE%BE%E5%A4%87)通常是使用Unix的[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)，它们默认打开一些被[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)恶意利用的UDP服务。如echo服务会显示接收到的每一个[数据包](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8C%85)，而原本作为测试功能的chargen服务会在收到每一个数据包时随机反馈一些字符。UDPflood假冒攻击就是利用这两个简单的TCP/IP服务的[漏洞](https://baike.baidu.com/item/%E6%BC%8F%E6%B4%9E)进行恶意攻击，通过伪造与某一[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)的Chargen服务之间的一次的UDP连接，回复地址指向开着Echo服务的一台主机，通过将Chargen和Echo服务互指，来回传送毫无用处且占满带宽的垃圾数据，在两台主机之间生成足够多的无用数据流，这一[拒绝服务攻击](https://baike.baidu.com/item/%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1%E6%94%BB%E5%87%BB)飞快地导致网络可用带宽耗尽。[1]

**SYN**[泛洪](https://baike.baidu.com/item/%E6%B3%9B%E6%B4%AA)

**(SYNflood)**

SYNflood攻击：我们知道当用户进行一次标准的TCP（TransmissionControlProtocol）连接时，会有一个3次握手过程。首先是请求服务方发送一个SYN（SynchronizeSequenceNumber）消息，服务方收到SYN后，会向请求方回送一个SYN-ACK表示确认，当请求方收到SYN-ACK后，再次向服务方发送一个ACK消息，这样一次TCP连接建立成功。“SYNFlooding”则专门针对TCP协议栈在两台[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)间初始化连接握手的过程进行DoS攻击，其在实现过程中只进行前2个步骤：当服务方收到请求方的SYN-ACK确认消息后，请求方由于采用源地址欺骗等手段使得服务方收不到ACK回应，于是服务方会在一定时间处于等待接收请求方ACK消息的状态。而对于某台[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)来说，可用的TCP连接是有限的，因为他们只有有限的内存[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)用于创建连接，如果这一缓冲区充满了虚假连接的初始信息，该服务器就会对接下来的连接停止响应，直至缓冲区里的连接企图超时。如果恶意攻击方快速连续地发送此类连接请求，该[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)可用的TCP连接队列将很快被阻塞，系统可用资源急剧减少，网络可用带宽迅速缩小，长此下去，除了少数幸运用户的请求可以插在大量虚假请求间得到应答外，服务器将无法向用户提供正常的合法服务。[1]

**Land（LandAttack）攻击**

在[Land攻击](https://baike.baidu.com/item/Land%E6%94%BB%E5%87%BB)中，[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)利用一个特别打造的SYN包--它的原地址和目标地址都被设置成某一个服务

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/1f569482dc17c3ddf603a6c1?fr=lemma&ct=single)dos攻击

器地址进行攻击。此举将导致接受[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个[空连接](https://baike.baidu.com/item/%E7%A9%BA%E8%BF%9E%E6%8E%A5)，每一个这样的连接都将保留直到超时，在Land攻击下，许多UNIX将崩溃，NT变得极其缓慢（大约持续五分钟）。[1]

IP欺骗

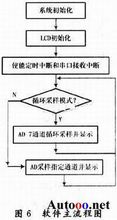
这种攻击利用[TCP协议](https://baike.baidu.com/item/TCP%E5%8D%8F%E8%AE%AE)栈的RST位来实现，使用IP欺骗，迫使[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)把合法用户的连接复位，影响合法用户的连接。假设有一个合法用户（100.100.100.100）已经同[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)建了正常的连接，攻击者构造攻击的TCP数据，伪装自己的IP为100.100.100.100，并向服务器发送一个带有RST位的TCP[数据段](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E6%AE%B5)。[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)接收到这样的数据后，认为从100.100.100.100发送的连接有错误，就会清空[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)中已建立好的连接。这时，合法用户100.100.100.100再发送合法数据，[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)就已经没有这样的连接了，该用户就被拒绝服务而只能重新开始建立新的连接。[1]

攻击方法

具体DoS攻击方法很多，但大多都可以分为以下几类：[1]

**利用**[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)实现的[缺陷](https://baike.baidu.com/item/%E7%BC%BA%E9%99%B7)

[OOB攻击](https://baike.baidu.com/item/OOB%E6%94%BB%E5%87%BB)（常用工具winnuke），teardrop攻击（常用工具teardrop.cboink.cbonk.c），lan

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/f15e2429d4e269b399250ac2?fr=lemma&ct=single)软件主流程图

d攻击，IGMP碎片包攻击，jolt攻击，Cisco2600路由器IOSversion12.0（10）[远程](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B)[拒绝服务攻击](https://baike.baidu.com/item/%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1%E6%94%BB%E5%87%BB)等等，这些攻击都是利用了被攻击[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)的实现上的[缺陷](https://baike.baidu.com/item/%E7%BC%BA%E9%99%B7)完成DoS攻击的。通常这些攻击工具向被攻击系统发送特定类型的一个或多个报文，这些攻击通常都是致命的，一般都是一击致死，而且很多攻击是可以伪造源地址的，所以即使通过IDS或者别的sniffer[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)记录到攻击报文也不能找到谁发动的攻击，而且此类型的攻击多是特定类型的几个报文，非常短暂的少量的报文，如果伪造源IP地址的话，使追查工作几乎是不可能。[1]

那么如何造成这些攻击的？通常是[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)开发过程中对某种特定类型的报文、或请求没有处理，导致软件遇到这种类型的报文运行出现异常，导致软件崩溃甚至[系统崩溃](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E5%B4%A9%E6%BA%83)。下面结合几个具体实例解释一下这种攻击的成因。[1]

1997年5月7号有人发布了一个winnuke.c。首先建立一条到Win95/NT[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)的TCP连接，然后发送TCP紧急数据，导致对端[系统崩溃](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E5%B4%A9%E6%BA%83)。139/TCP是Win95/NT系统最常见的侦听[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)，所以winnuke.c使用了该端口。之所以称呼这种攻击为[OOB攻击](https://baike.baidu.com/item/OOB%E6%94%BB%E5%87%BB)，因为MSG\_OOB标志，实际应该是TCP紧急数据攻击。[1]

原始teardrop.c只构造了两种碎片包，每次同时发送这两种UDP碎片包。如果指定发送次数，将完全重复先前所发送出去的两种碎片包。它可以伪造源ip并跨越路由器进行[远程](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B)攻击，影响的系统包括Linux/WinNT/Win95。使用的方法是：[1]

teardrop源ip目的ip[-s源端口][-d目的端口][-n次数]

比较新的一个DoS攻击是[Windows](https://baike.baidu.com/item/Windows)的SMB实现中的DoS攻击，2002年8月发布，只要允许匿名连接的[windows](https://baike.baidu.com/item/windows)系统就可以进行[远程](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B)攻击，强烈建议Windows用户打相应的[补丁](https://baike.baidu.com/item/%E8%A1%A5%E4%B8%81)。它的方法就是先和目标系统建立一个连接，然后发送一个特定的请求，目标系统就会兰屏。发布的测试工具SMBdie.exe是图形界面工具，输入目标地址NETBIOS名称即可。[1]

从上面的讨论可以看出，这种攻击行为威力很大，而且难于[侦察](https://baike.baidu.com/item/%E4%BE%A6%E5%AF%9F)。但真实情况下它的危害仅现于[漏洞](https://baike.baidu.com/item/%E6%BC%8F%E6%B4%9E)发布后的不长的时间段内，相关厂商会很快发布[补丁](https://baike.baidu.com/item/%E8%A1%A5%E4%B8%81)修补这种漏洞。所以上面提到的几种较老的攻击在现实的环境中，通常是无效的。不过最新的攻击方法还是让我们不寒而栗，我们可以做的就是关注安全漏洞的发布，及时打上新的[补丁](https://baike.baidu.com/item/%E8%A1%A5%E4%B8%81)。如果你想偷懒的话，购买专业安全服务公司的相关服务应该是个更好的选择。[1]

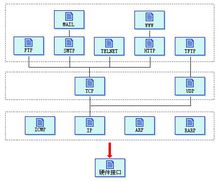
**利用协议的漏洞**

如果说上面那种漏洞危害的时间不是很长，那么这种攻击的生存能力却非常强。为了能够在网络上进行互通、互联，所有的[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)实现都必须遵循既有的协议，而如果这种协议存在漏洞的话，所有遵循此协议的软件都会受到影响。[1]

最经典的攻击是synflood攻击，它利用[TCP/IP协议](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE)的漏洞完成攻击。通常一次TCP连接的建立包括3个步骤，[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)发送SYN包给[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)端，服务器分配一定的资源给这里连接并返回SYN/ACK包，并等待连接建立的最后的ACK包，最后客户端发送ACK[报文](https://baike.baidu.com/item/%E6%8A%A5%E6%96%87)，这样两者之间的连接建立起来，并可以通过连接传送数据了。而攻击的过程就是疯狂发送SYN[报文](https://baike.baidu.com/item/%E6%8A%A5%E6%96%87)，而不返回ACK报文，[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)占用过多资源，而导致[系统资源](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E8%B5%84%E6%BA%90)占用过多，没有能力响应别的操作，或者不能响应正常的网络请求。[1]

这个攻击是经典的以小搏大的攻击，自己使用少量资源占用对方大量资源。一台P4的Linux系统大约能发到30－40M的64字节的synflood报文，而一台普通的[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)20M的流量就基本没有任何响应了（包括鼠标、键盘）。而且synflood不仅可以[远程](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B)进行，而且可以伪造源IP地址，给追查造成很大困难，要查找必须所有骨干[网络运营商](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E8%BF%90%E8%90%A5%E5%95%86)，一级一级路由器的向上查找。[1]

对于伪造源IP的synflood攻击，除非攻击者和被攻击的系统之间所有的路由器的管理者都配合查找，否

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/e865a699d61bc5456e068ccd?fr=lemma&ct=single)TCP/IP协议结构图

则很难追查。当前一些[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99)产品声称有抗DoS的能力，但通常他们能力有限，包括国外的[硬件](https://baike.baidu.com/item/%E7%A1%AC%E4%BB%B6)防火墙大多100M防火墙的抗synflood的能力只有20－30Mbps（64字节syn包），这里涉及到它们对小报文的转发能力，再大的流量甚至能把防火墙打死机。有些安全厂商认识到DoS攻击的危害，开始研发专用的抗拒绝服务产品。[1]

由于TCP/IP协议相信[报文](https://baike.baidu.com/item/%E6%8A%A5%E6%96%87)的源地址，另一种攻击方式是反射[拒绝服务攻击](https://baike.baidu.com/item/%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1%E6%94%BB%E5%87%BB)，另外可以利用还有[广播地址](https://baike.baidu.com/item/%E5%B9%BF%E6%92%AD%E5%9C%B0%E5%9D%80)，和[组播](https://baike.baidu.com/item/%E7%BB%84%E6%92%AD)协议辅助反射拒绝服务攻击效果更好。不过大多数路由器都禁止[广播地址](https://baike.baidu.com/item/%E5%B9%BF%E6%92%AD%E5%9C%B0%E5%9D%80)和[组播](https://baike.baidu.com/item/%E7%BB%84%E6%92%AD)协议的地址。[1]

另一类攻击方式是使用大量符合协议的正常服务请求，由于每个请求耗费很大[系统资源](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E8%B5%84%E6%BA%90)，导致正常服务请求不能成功。如[HTTP协议](https://baike.baidu.com/item/HTTP%E5%8D%8F%E8%AE%AE)是[无状态协议](https://baike.baidu.com/item/%E6%97%A0%E7%8A%B6%E6%80%81%E5%8D%8F%E8%AE%AE)，攻击者构造大量搜索请求，这些请求耗费大量[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)资源，导致DoS。这种方式攻击比较好处理，由于是正常请求，暴露了正常的源IP地址，禁止这些IP就可以了。[1]

**进行资源比拼**

这种攻击方式属于无赖打法，我凭借着手中的资源丰富，发送大量的垃圾数据侵占完你的资源，导致DoS。比如，ICMPflood，mstreamflood，Connectionflood。为了获得比目标系统更多资源，通常攻击者会发动DDoS（DistributedDos[分布式拒绝服务](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1)）攻击者控制多个攻击傀儡发动攻击，这样才能产生预期的效果。前两类攻击是可以伪造IP地址的，追查也是非常困难，第3种攻击由于需要建立连接，可能会暴露攻击傀儡的IP地址，通过防火墙禁止这些IP就可以了。对于难于追查，禁止的攻击行为，我们只能期望专用的抗拒绝服务产品了。[1]

攻击程序

smurf、trinoo、tfn、tfn2k以及stacheldraht是比较常见的DoS攻击[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)，本文将对它们的原理以及抵御措施进行论述，以帮助[管理员](https://baike.baidu.com/item/%E7%AE%A1%E7%90%86%E5%91%98)有效地抵御DoS风暴攻击，维护站点安全。[1]

**“smurf攻击”，如何抵御**

Smurf是一种简单但有效的DDoS攻击技术，它利用了ICMP(Internet控制信息协议）。ICMP在Internet

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/eab9044cfe1350b4d72afccf?fr=lemma&ct=single)黑客

上用于错误处理和传递控制信息。它的功能之一是与主机联系，通过发送一个“回音请求”（echorequest）信息包看看主机是否“活着”。最普通的ping[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)就使用了这个功能。Smurf是用一个偷来的帐号安装到一个计算机上的，然后用一个伪造的源地址连续ping一个或多个[计算机网络](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C)，这就导致所有计算机所响应的那个计算机并不是实际发送这个信息包的那个计算机。这个伪造的源地址，实际上就是攻击的目标，它将被极大数量的响应信息量所淹没。对这个伪造信息包做出响应的计算机网络就成为攻击的不知情的[同谋](https://baike.baidu.com/item/%E5%90%8C%E8%B0%8B)。[1]

下面是SmurfDDoS攻击的基本特性以及建议采用的抵御策略：[1]

1、Smurf的攻击[平台](https://baike.baidu.com/item/%E5%B9%B3%E5%8F%B0)：smurf为了能工作，必须要找到攻击平台，这个平台就是：其[路由器](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8)上启动了IP广播功能。这个功能允许smurf发送一个伪造的ping信息包，然后将它传播到整个计算机网络中。[1]

2、为防止系统成为smurf攻击的平台，要将所有路由器上IP的广播功能都禁止。一般来讲，IP广播功能并不需要。[1]

3、攻击者也有可能从LAN内部发动一个smurf攻击，在这种情况下，禁止路由器上的IP广播功能就没有用了。为了避免这样一个攻击，许多[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)都提供了相应设置，防止计算机对IP广播请求做出响应。[1]

4、如果攻击者要成功地利用你成为攻击平台，你的路由器必须要允许[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)以不是从你的内网中产生的源地址离开网络。配置路由器，让它将不是由你的内网中生成的信息包过滤出去，这是有可能做到的。这就是所谓的网络出口过滤器功能。[1]

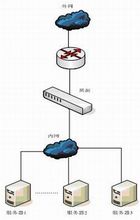
5、ISP则应使用网络入口[过滤器](https://baike.baidu.com/item/%E8%BF%87%E6%BB%A4%E5%99%A8)，以丢掉那些不是来自一个已知范围内IP地址的[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)。[1]

6、挫败一个smurf攻击的最简单方法对边界路由器的回音应答（echoreply）[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)进行过滤，然后丢弃它们，这样就能阻止“命中”Web[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)和内网。对于那些使用Cisco路由器的人，另一个选择是CAR(CommittedAccessRate，承诺访问速率）。[1]

丢弃所有的回音应答[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)能使网络避免被淹没，但是它不能防止来自上游供应者通道的交通堵塞。如果你成为了攻击的目标，就要请求ISP对回音应答[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)进行过滤并丢弃。如果不想完全禁止回音应答，那么可以有选择地丢弃那些指向你的公用Web[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)的回音应答[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)。CAR技术由Cisco开发，它能够规定出各种[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)类型使用的[带宽](https://baike.baidu.com/item/%E5%B8%A6%E5%AE%BD)的最大值。例如，使用CAR，我们就可以精确地规定回音应答[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)所使用的[带宽](https://baike.baidu.com/item/%E5%B8%A6%E5%AE%BD)的最大值。[1]

**“trinoo”，如何抵御**

trinoo是复杂的DDoS攻击[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)，它使用“master”程序对实际实施攻击的任何数量的“代理”

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/b7bc4c66ef088069ab184cc8?fr=lemma&ct=single)牵引流量技术在DOS攻击中应用

[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)实现自动控制。攻击者连接到安装了master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)的计算机，启动master程序，然后根据一个IP地址的列表，由master程序负责启动所有的代理程序。接着，代理程序用UDP信息包冲击网络，从而攻击目标。在攻击之前，侵入者为了安装[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)，已经控制了装有master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)的计算机和所有装有代理[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)的计算机。[1]

下面是trinooDDoS攻击的基本特性以及建议采用的抵御策略：

1、在master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)与代理[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)的所有通讯中，trinoo都使用了UDP协议。[入侵检测](https://baike.baidu.com/item/%E5%85%A5%E4%BE%B5%E6%A3%80%E6%B5%8B)[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)能够寻找使用UDP协议的数据流（类型17）。[1]

2、Trinoomaster程序的监听[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)是27655，攻击者一般借助telnet通过TCP连接到master程序所在计算机。[入侵检测](https://baike.baidu.com/item/%E5%85%A5%E4%BE%B5%E6%A3%80%E6%B5%8B)[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)能够搜索到使用TCP（类型6）并连接到[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)27655的[数据流](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E6%B5%81)。[1]

3、所有从master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)到代理程序的通讯都包含字符串“l44”，并且被引导到代理的UDP[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)27444。[入侵检测](https://baike.baidu.com/item/%E5%85%A5%E4%BE%B5%E6%A3%80%E6%B5%8B)[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)检查到UDP[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)27444的连接，如果有包含字符串l44的信息包被发送过去，那么接受这个信息包的计算机可能就是DDoS代理。[1]

4、Master和代理之间通讯受到口令的保护，但是[口令](https://baike.baidu.com/item/%E5%8F%A3%E4%BB%A4)不是以加密格式发送的，因此它可以被“[嗅探](https://baike.baidu.com/item/%E5%97%85%E6%8E%A2)”到并被检测出来。使用这个口令以及来自DaveDittrich的trinot[脚本](https://baike.baidu.com/item/%E8%84%9A%E6%9C%AC)，要准确地验证出trinoo代理的存在是很可能的。

一旦一个代理被准确地识别出来，trinoo网络就可以安装如下步骤被拆除：[1]

·在代理daemon上使用"strings"命令，将master的IP地址暴露出来。

·与所有作为trinoomaster的机器管理者联系，通知它们这一事件。

·在master计算机上，识别含有代理IP地址列表的文件（默认名“...”），得到这些计算机的IP地址列表。

·向代理发送一个伪造“trinoo”命令来禁止代理。通过crontab文件（在UNIX系统中）的一个条目，代理可以有规律地重新启动，因此，代理计算机需要一遍一遍地被关闭，直到代理系统的管理者修复了crontab文件为止。

·检查master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)的活动TCP连接，这能显示攻击者与trinoomaster程序之间存在的实时连接。

·如果网络正在遭受trinoo攻击，那么系统就会被UDP信息包所淹没。Trinoo从同一源地址向目标[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)上的任意[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)发送信息包。[探测](https://baike.baidu.com/item/%E6%8E%A2%E6%B5%8B)trinoo就是要找到多个UDP信息包，它们使用同一来源IP地址、同一目的IP地址、同一[源端口](https://baike.baidu.com/item/%E6%BA%90%E7%AB%AF%E5%8F%A3)，但是不同的目的端口。[1]

·在美国[FBI](https://baike.baidu.com/item/FBI)网站上有一个检测和根除trinoo的自动[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)。

**“TribalFloodNetwork”和“TFN2K”，如何抵御**

TribeFloodNetwork与trinoo一样，使用一个master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)与位于多个网络上的攻击代理进行通讯。TFN可以并行发动数不胜数的DoS攻击，[类型](https://baike.baidu.com/item/%E7%B1%BB%E5%9E%8B)多种多样，而且还可建立带有伪装源IP地址的信息包。可以由TFN发动的攻击包括：UDP冲击、TCPSYN冲击、ICMP回音请求冲击以及ICMP广播。[1]

以下是TFNDDoS攻击的基本特性以及建议的抵御策略：

1、发动TFN时，攻击者要访问master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)并向它发送一个或多个目标IP地址，然后Master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)继续与所有代理程序通讯，指示它们发动攻击。[1]

TFNMaster程序与代理程序之间的通讯使用ICMP回音应答信息包，实际要执行的指示以[二进制](https://baike.baidu.com/item/%E4%BA%8C%E8%BF%9B%E5%88%B6)形式包含在16位ID域中。ICMP(Internet控制信息协议）使信息包协议过滤成为可能。通过配置路由器或[入侵检测系统](https://baike.baidu.com/item/%E5%85%A5%E4%BE%B5%E6%A3%80%E6%B5%8B%E7%B3%BB%E7%BB%9F)，不允许所有的ICMP回音或回音应答信息包进入网络，就可以达到挫败TFN代理的目的。但是这样会影响所有使用这些功能的Internet[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)，比如ping。

TFNMaster[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)读取一个IP地址列表，其中包含代理程序的位置。这个列表可能使用如“Blowfish”的[加密程序](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86%E7%A8%8B%E5%BA%8F)进行了加密。如果没有加密的话，就可以从这个列表方便地识别出代理信息。

2、用于发现系统上TFN代理[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)的程序是td，发现系统上master程序的程序是tfn。TFN代理并不查看ICMP回音应答信息包来自哪里，因此使用伪装ICMP信息包冲刷掉这些过程是可能的。

TFN2K是TFN的一个更高级的版本，它“修复”了TFN的某些缺点：

1、在TFN2K下，Master与代理之间的通讯可以使用许多协议，例如TCP、UDP或ICMP，这使得协议过滤不可能实现。[1]

2、TFN2K能够发送破坏信息包，从而导致系统瘫痪或不稳定。

3、TFN2K伪造IP源地址，让信息包看起来好像是从LAN上的一个临近机器来的，这样就可以挫败出口过滤和入口过滤。

4、由于TFN2K是被识破的，因此还没有一项研究能够发现它的明显弱点。

在人们能够对TFN2K进行更完全的分析之前，最好的抵御方法是：

·加固系统和网络，以防系统被当做DDoS主机。

·在[边界路由器](https://baike.baidu.com/item/%E8%BE%B9%E7%95%8C%E8%B7%AF%E7%94%B1%E5%99%A8)上设置出口过滤，这样做的原因是或许不是所有的TFN2K源地址都用内部[网络地址](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%9C%B0%E5%9D%80)进行伪装。

·请求上游供应商配置入口过滤。

**“stacheldraht”，如何防范**

Stacheldraht也是基于TFN和trinoo一样的客户机/[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)模式，其中Master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)与潜在的成千个代理程序进行通讯。在发动攻击时，侵入者与master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)进行连接。Stacheldraht增加了以下新功能：攻击者与master程序之间的通讯是加密的，以及使用rcp(remotecopy，[远程](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B)复制）技术对代理程序进行更新。

Stacheldraht同TFN一样，可以并行发动数不胜数的DoS攻击，类型多种多样，而且还可建立带有伪装源IP地址的信息包。Stacheldraht所发动的攻击包括UDP冲击、TCPSYN冲击、ICMP回音应答冲击以及ICMP播放。

以下是StacheldrahtDDoS攻击的基本特征以及建议采取的防御措施：

1、在发动Stacheldraht攻击时，攻击者访问master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)，向它发送一个或多个攻击目标的IP地址。Master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)再继续与所有代理程序进行通讯，指示它们发动攻击。

Stacheldrahtmaster程序与代理程序之间的通讯主要是由ICMP回音和回音应答信息包来完成的。配置路由器或入侵检测系统，不允许一切ICMP回音和回音应答信息包进入网络，这样可以挫败Stacheldraht代理。但是这样会影响所有要使用这些功能的Internet[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)，例如ping。

2、代理[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)要读取一个包含有效master程序的IP地址列表。这个地址列表使用了Blowfish[加密程序](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86%E7%A8%8B%E5%BA%8F)进行加密。代理会试图与列表上所有的master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)进行联系。如果联系成功，代理[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)就会进行一个测试，以确定它被安装到的系统是否会允许它改变"伪造"信息包的源地址。通过配置入侵检测系统或使用[嗅探器](https://baike.baidu.com/item/%E5%97%85%E6%8E%A2%E5%99%A8)来搜寻它们的签名信息，可以[探测](https://baike.baidu.com/item/%E6%8E%A2%E6%B5%8B)出这两个行为。

代理会向每个master发送一个ICMP回音应答信息包，其中有一个ID域包含值666，一个数据域包含字符串“skillz”。如果master收到了这个信息包，它会以一个包含值667的ID域和一个包含[字符串](https://baike.baidu.com/item/%E5%AD%97%E7%AC%A6%E4%B8%B2)“ficken”的数据域来应答。代理和master通过交换这些信息包来实现周期性的基本接触。通过对这些信息包的监控，可以[探测](https://baike.baidu.com/item/%E6%8E%A2%E6%B5%8B)出Stacheldraht。

一旦代理找到了一个有效master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)，它会向master发送一个ICMP信息包，其中有一个伪造的源地址，这是在执行一个伪造测试。这个假地址是“3.3.3.3”。如果master收到了这个伪造地址，在它的应答中，用ICMP信息包数据域中的“spoofworks”字符串来确认伪造的源地址是奏效的。通过[监控](https://baike.baidu.com/item/%E7%9B%91%E6%8E%A7)这些值，也可以将Stacheldraht检测出来。

3、Stacheldraht代理并不检查ICMP回音应答信息包来自哪里，因此就有可能伪造ICMP信息包将其排除。

4、Stacheldraht代理[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)与TFN和trinoo一样，都可以用一个C程序来[探测](https://baike.baidu.com/item/%E6%8E%A2%E6%B5%8B)。

防范

DoS攻击几乎是从[互联网](https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91)络的诞生以来，就伴随着互联网络的发展而一直存在也不断发展和升级。值得一提的是，要找DoS的工具一点不难，[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)群居的[网络社区](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%A4%BE%E5%8C%BA)都有共享黑客[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)的传统，并会在一起交流攻击的心得经验，你可以很轻松的从Internet上获得这些工具，像以上提到的这些DoS攻击软件都是可以从网上随意

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/f7426d8dc057b05fb31bbacb?fr=lemma&ct=single)dos攻击

找到的公开软件。所以任何一个上网者都可能构成网络安全的潜在威胁。DoS攻击给飞速发展的互联网络安全带来重大的威胁。

要避免系统免受DoS攻击，从前两点来看，[网络管理员](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E5%91%98)要积极谨慎地维护系统，确保无安全隐患和[漏洞](https://baike.baidu.com/item/%E6%BC%8F%E6%B4%9E)；而针对第三点的恶意攻击方式则需要安装防火墙等安全[设备](https://baike.baidu.com/item/%E8%AE%BE%E5%A4%87)过滤DoS攻击，同时强烈建议网络管理员应当定期查看安全[设备](https://baike.baidu.com/item/%E8%AE%BE%E5%A4%87)的日志，及时发现对系统的安全威胁行为。

Internet支持工具就是其中的主要解决方案之一，包括SuperStack3Firewall、WebCache以及ServerLoadBalancer。不但作为[安全网关](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E7%BD%91%E5%85%B3)设备的3ComSuperStack3防火墙在缺省预配置下可[探测](https://baike.baidu.com/item/%E6%8E%A2%E6%B5%8B)和防止“拒绝服务”（DoS）以及“分布式拒绝服务”（DDoS）等[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)侵袭，强有力的保护您的网络，使您免遭未经授权访问和其他来自Internet的外部威胁和侵袭；而且3ComSuperStack3ServerLoadBalancer在为多[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)提供硬件线速的4-7层负载均衡的同时，还能保护所有服务器免受“拒绝服务”（DoS）攻击；同样3ComSuperStack3WebCache在为企业提供高效的[本地缓存](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%BC%93%E5%AD%98)的同时，也能保证自身免受“拒绝服务”（DoS）攻击。

**常见攻击与防范**

SYN Flood攻击

**原理：**问题就出在TCP连接的三次握手中，假设一个用户向服务器发送了SYN报文后突然死机或掉线，那么服务器在发出SYN+ACK应答报文后是无法收到客户端的ACK报文的（第三次握手无法完成），这 种情况下服务器端一般会重试（再次发送SYN+ACK给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为SYN Timeout，一般来说这个时间是分钟的数量级（大约为30秒 -2分钟）；一个用户出现异常导致服务器的一个线程等待1分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常 多的资源----数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的CPU时间和内存，何况还要不断对这个列表中的IP进行SYN+ACK的重试。实际上如果服务器的TCP/IP栈不够强大，最 后的结果往往是堆栈溢出崩溃---即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的TCP连接请求而无暇理睬客户的正常请求（毕竟客户端的正常请求比率非常之小），此时从 正常客户的角度看来，服务器失去响应，这种情况我们称作：服务器端受到了SYN Flood攻击（SYN洪水攻击）。  
　　**防范：**第一种是缩短SYN Timeout时间  
　　第二种方法是设置SYN Cookie，就是给每一个请求连接的IP地址分配一个Cookie，如果短时间内连续受到某个IP的重复SYN报文，就认定是受到了攻击，以后从这个IP地址来的包会被一概丢弃。  
　　>netstat -n -p tcp >result.txt

Smurf攻击：

**原理：**发送伪装的ICMP数据包，目的地址设为某个网络的广播地址，源地址设为要攻击的目的主机，使所有收到此ICMP数据包的主机都将对目的主机发出一个回应，使被攻击主机在某一段时间内收到 成千上万的数据包  
　　**防范：**在cisco路由器上配置如下可以防止将包传递到广播地址上:  
　　Router(config-if)# no ip directed-broadcast

Ping of Death

**原理：**"ping of death"攻击就是我们常说的"死亡Ping"  
　　这种攻击通过发送大于65536字节的ICMP包使操作系统崩溃；通常不可能发送大于65536个字节的ICMP包，但可以把报文分割成片段，然后在目标主机上重组；最终会导致被攻击目标缓冲区溢 出，引起拒绝服务攻击。有些时候导致telne和http服务停止，有些时候路由器重启。

泪滴攻击

**原理：**对于一些大的IP数据包，往往需要对其进行拆分传送，这是为了迎合链路层的MTU（最大传输单元）的要求。比如，一个6 000字节的IP包，在MTU为2 000的链路上传输的时候，就需要分成3个IP 包。在IP报头中有一个偏移字段和一个拆分标志（MF）。如果MF标志设置为1，则表示这个IP包是一个大IP包的片段，其中偏移字段指出了这个片段在整个IP包中的位置。例如，对一个6 000字 节的IP包进行拆分（MTU为2 000），则3个片段中偏移字段的值依次为0，2 000，4 000。这样接收端在全部接收完IP数据包后，就可以根据这些信息重新组装这几个分次接收的拆分IP包。在这 里就有一个安全漏洞可以利用了，就是如果黑客们在截取IP数据包后，把偏移字段设置成不正确的值，这样接收端在收到这些分拆的数据包后，就不能按数据包中的偏移字段值正确组合这些拆 分的数据包，但接收端会不断尝试，这样就可能致使目标计算机操作系统因资源耗尽而崩溃。

DRDOS

**原理：**攻击时，攻击者巧妙的利用了反弹服务器群来将洪水数据包反弹给目标主机 反弹服务是指某些服务器在收到一个请求数据报后就会产生一个回应数据报。所有的 Web 服务器、DNS 服务器及路 由器都是反弹服务器，他们会对 SYN 报文或其他 TCP 报文回应 SYNACKs 或 RST 报文， 以及对一些 IP 报文回应 ICMP 数据报超时或目的地不可达消息的数据 报。任何用于普通目的 TCP 连 接许可的网络服务器都可以用做数据包反射服务器

**配置路由器、防火墙和入侵检测系统来抵御常见DDoS攻击**

**Smurf**

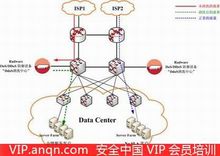
·确定你是否成为了攻击平台：对不是来自于你的内部网络的[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)进行[监控](https://baike.baidu.com/item/%E7%9B%91%E6%8E%A7)；监控大容量的回音请求和回音应答信息包。

·避免被当做一个攻击平台：在所有路由器上禁止IP广播功能；将不是来自于内部网络的信息[包过滤](https://baike.baidu.com/item/%E5%8C%85%E8%BF%87%E6%BB%A4)掉。

·减轻攻击的危害：在边界路由器对回音应答信息包进行过滤，并丢弃；对于Cisco路由器，使用CAR来规定回音应答信息包可以使用的带宽最大值。

**trinoo**

·确定你是否成为攻击平台：在master[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)和代理程序之间的通讯都是使用UDP协议，因此对使用UDP

[](https://baike.baidu.com/pic/dos%E6%94%BB%E5%87%BB/3792374/0/a583631ee73987b91bd576d4?fr=lemma&ct=single)dos攻击

协议（类别17）进行过滤；攻击者用TCP[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)27655与master[程序连接](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F%E8%BF%9E%E6%8E%A5)，因此对使用TCP（类别6）端口27655连接的流进行过滤；master与代理之间的通讯必须要包含字符串“l44”，并被引导到代理的UDP端口27444，因此对与UDP端口27444连接且包含字符串l44的数据流进行过滤。

·避免被用作攻击平台：将不是来自于你的内部网络的[信息包](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%8C%85)[过滤](https://baike.baidu.com/item/%E8%BF%87%E6%BB%A4)掉。

·减轻攻击的危害：从理论上说，可以对有相同源IP地址的、相同目的IP地址的、相同[源端口](https://baike.baidu.com/item/%E6%BA%90%E7%AB%AF%E5%8F%A3)的、不通目的端口的UDP信息包序列进行过滤，并丢弃它们。

**TFN**

·确定你是否成为攻击平台：对不是来自于内部网络的信息包进行监控。

·避免被用作攻击平台：不允许一切到你的网络上的ICMP回音和回音应答信息包，当然这会影响所有要使用这些功能的Internet[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)；将不是来源于内部网络的信息包过滤掉。

Stacheldraht

·确定你是否成为攻击平台：对ID域中包含值666、数据域中包含字符串“skillz”或ID域中包含值667、数据域中包含字符串“ficken”的ICMP回音应答信息包进行过滤；对源地址为“3.3.3.3”的ICMP信息包和ICMP信息包数据域中包含字符串“spoofworks”的数据流进行过滤。

·手工防护

一般而言手工方式防护DDOS主要通过两种形式：

[系统优化](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E4%BC%98%E5%8C%96)――主要通过优化被攻击系统的核心参数，提高系统本身对DDoS攻击的响应能力。但是这种做法只能针对小规模的DDOS进行防护。

[网络追查](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E8%BF%BD%E6%9F%A5)――遭受DDoS攻击的系统的管理人员一般第一反应是询问上一级网络运营商，这有可能是ISP、IDC等，目的就是为了弄清楚攻击源头。

退让策略

为了抵抗DDOS攻击，DengKelen客户可能会通过购买硬件的方式来提高系统抗DDOS的能力。但是这种退让策略的效果并不好，一方面由于这种方式的性价比过低，另一方面，[黑客](https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2)提高供给流量之后，这种方法往往失效，所以不能从根本意义上防护DDoS攻击。

防火墙

[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99)几乎是最常用的安全产品，但是防火墙设计原理中并没有考虑针对DDOS攻击的防护，在某些情况下，防火墙甚至成为DDOS攻击的目标而导致整个网络的拒绝服务。

首先是防火墙缺乏DDOS攻击检测的能力。通常，防火墙作为三层包转发[设备](https://baike.baidu.com/item/%E8%AE%BE%E5%A4%87)部署在网络中，一方面在保护内部网络的同时，它也为内部需要提供外部[Internet服务](https://baike.baidu.com/item/Internet%E6%9C%8D%E5%8A%A1)的设备提供了通路，如果DDOS攻击采用了这些[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)允许的合法协议对内部系统进行攻击，防火墙对此就无能为力，无法精确的从背景流量中区分出攻击流量。虽然有些防火墙内置了某些模块能够对攻击进行检测，但是这些检测机制一般都是基于特征规则，DDOS攻击者只要对攻击[数据包](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8C%85)稍加变化，防火墙就无法应对，对DDOS攻击的检测必须依赖于行为模式的算法。

第二个原因就是传统防火墙计算能力的限制，传统的防火墙是以高强度的检查为代价，检查的强度越高，计算的代价越大。而DDOS攻击中的海量流量会造成防火墙性能急剧下降，不能有效地完成包转发的任务。最好防火墙的部署位置也影响了其防护DDOS攻击的能力。传统防火墙一般都是部署在网络入口位置，虽然某种意义上保护了网络内部的所有资源，但是其往往也成为[DDOS](https://baike.baidu.com/item/DDOS)攻击的目标，攻击者一旦发起DDOS攻击，往往造成网络性能的整体下降，导致用户正常请求被拒绝。