拒绝服务攻击宝典

拒绝服务攻击宝典

我们所说的DoS (Denial of Service)攻击其中文含义是拒绝服务攻击，这种攻击行动使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。黑客不正当地采用标准协议或连接方法，向攻击的服务发出大量的讯息，占用及超越受攻击服务器所能处理的能力，使它当(Down)机或不能正常地为用户服务。

“拒绝服务”是如何攻击的？有什么方法和措施可以防范此类攻击？在新时代云趋势的环境下，拒绝服务攻击又会如何发展？有什么新的趋势？

本技术手册将从三个方面为您提供详细的安全策略，包括：拒绝服务攻击的原理，拒绝服务攻击的防范和拒绝攻击与云。

教你认识拒绝服务攻击

DoS即Denial Of Service，拒绝服务的缩写。DoS是指故意攻击网络协议实现的缺陷，或直接通过野蛮手段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。

“拒绝服务”是如何攻击的？有哪些攻击方式？会造成什么后果？

- ❖解析拒绝服务攻击的攻击技术
- ❖分布式拒绝服务攻击(DDoS)原理及防范（一）
- ❖分布式拒绝服务攻击(DDoS)原理及防范（二）

如何防范拒绝服务攻击

只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为这是由于网络协议本身的安全缺陷造成的，从而拒绝服务攻击也成为了攻击者的终极手法。

难道我们只能坐以待毙？没有什么方法可以防范拒绝服务攻击吗？

- ❖拒绝式服务攻击袭来　你采取防御措施了吗？
- ❖如何防御网络拒绝服务攻击
- ❖如何阻止分布式拒绝服务攻击
- ❖如何防御网站上的分布式拒绝服务攻击
- ❖四招打败僵尸网络的拒绝服务攻击

风起“云”涌中的拒绝服务攻击

拒绝服务攻击这一古老的网络犯罪在几年再次成为了数据中心运营者们的心头之患。

随着公司越来越多地使用虚拟化数据中心和云服务，企业基础架构中新的薄弱环节也就渐渐浮出了水面。与此同时，拒绝服务攻击正在把目标从野蛮的数据洪潮中转向对应用基础架构更具技术性的攻击。

当拒绝服务攻击遇到云，我门将遭遇什么？又该如何应对呢？

- ❖当拒绝服务攻击遇到云
- ❖云计算应对拒绝服务攻击的四个教训

解析拒绝服务攻击的攻击技术

DoS 即 Denial Of Service，拒绝服务的缩写。DoS 是指故意攻击网络协议实现的缺陷，或直接通过野蛮手段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。

事实上，任何事物都有一个极限，所以总能找到一个方法使请求的值大于该极限值，因此就会故意导致所提供的服务资源匮乏，导致服务资源无法满足需求的情况。所以，千万不要认为拥有了足够宽的带宽和足够快的服务器就有了一个不怕拒绝服务攻击的高性能网站，拒绝服务攻击会使所有的资源都变得非常渺小。

其实，有个形象的比喻可以深入理解 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对餐馆进行拒绝服务攻击的话，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……；相应地，计算机和网络系统是为互联网用户提供互联网资源的，如果有黑客要进行拒绝服务攻击的话，则同样有好多手段！

今天最常见的拒绝服务攻击包括对计算机网络的带宽攻击和连通性攻击。带宽攻击是指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击是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。

传统上，攻击者所面临的主要问题是网络带宽，由于较小的网络规模和较慢的网络速度限制，攻击者无法发出过多的请求。虽然类似"the 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的 UNIX 系统，但大多数的 DoS 攻击还是需要相当大带宽的，而以个人为单位的黑客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来同时对同一个目标发动大量的攻击请求，这就是 DDoS 攻击。

DDoS（Distributed Denial Of Service），分布式拒绝服务攻击，又把 DoS 向前发展了一大步，这种分布式拒绝服务攻击是黑客利用在已经侵入并已控制的不同的高带宽主机（可能是数百，甚至成千上万台）上安装大量的 DoS 服务程序，它们等待来自中央攻击控制中心的命令，中央攻击控制中心在适时将启动全体受控主机的 DoS 服务进程，让它们对一个特定目标发送尽可能多的网络访问请求，形成一股 DoS 洪流冲击目标系统，猛烈的 DoS 攻击同一个网站。在寡不敌众的力量抗衡下，被攻击的目标网站会很快失去反应而不能及时处理正常的访问甚至系统瘫痪崩溃。

可见 DDoS 与 DoS 的最大区别是人多力量大。DoS 是一台机器攻击目标，DDoS 是被中央攻击中心控制的很多台机器利用高带宽攻击目标，可更容易地将目标攻下。另外，DDoS 攻击方式较为自动化，攻击者可以将程序安装到网络中的多台机器上，所采用的这种攻击方式很难被攻击对象察觉，直到攻击者发下统一的攻击命令，这些机器才同时发起进攻。

可以说 DDoS 攻击是由黑客集中控制发动的一组 DoS 攻击的集合，现在这种方式被认为是最有效的攻击形式，并且非常难以抵挡。

无论是 DoS 攻击还是 DDoS 攻击，简单地看，都只是一种破坏网络服务的黑客方式，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）制造大流量无用数据，造成通往被攻击主机的网络拥塞，使被攻击主机无法正常和外界通信；

（2）利用被攻击主机提供服务或传输协议上处理重复连接的缺陷，反复高频地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他正常的请求；

（3）利用被攻击主机所提供服务程序或传输协议的本身缺陷，反复发送畸形的攻击数据引发系统错误地分配大量系统资源，使主机处于挂起状态甚至死机。

（作者：人民网　来源：TechTarget 中国）

分布式拒绝服务攻击(DDoS)原理及防范（一）

DDoS 攻击概念

DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等等各项性能指标不高它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了 - 目标对恶意攻击包的"消化能力"加强了不少，例如你的攻击软件每秒钟可以发送 3,000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10,000 个攻击包，这样一来攻击就不会产生什么效果。

这时侯分布式的拒绝服务攻击手段（DDoS）就应运而生了。你理解了 DoS 攻击的话，它的原理就很简单。如果说计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再能起作用的话，攻击者使用 10 台攻击机同时攻击呢？用 100 台呢？DDoS 就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。

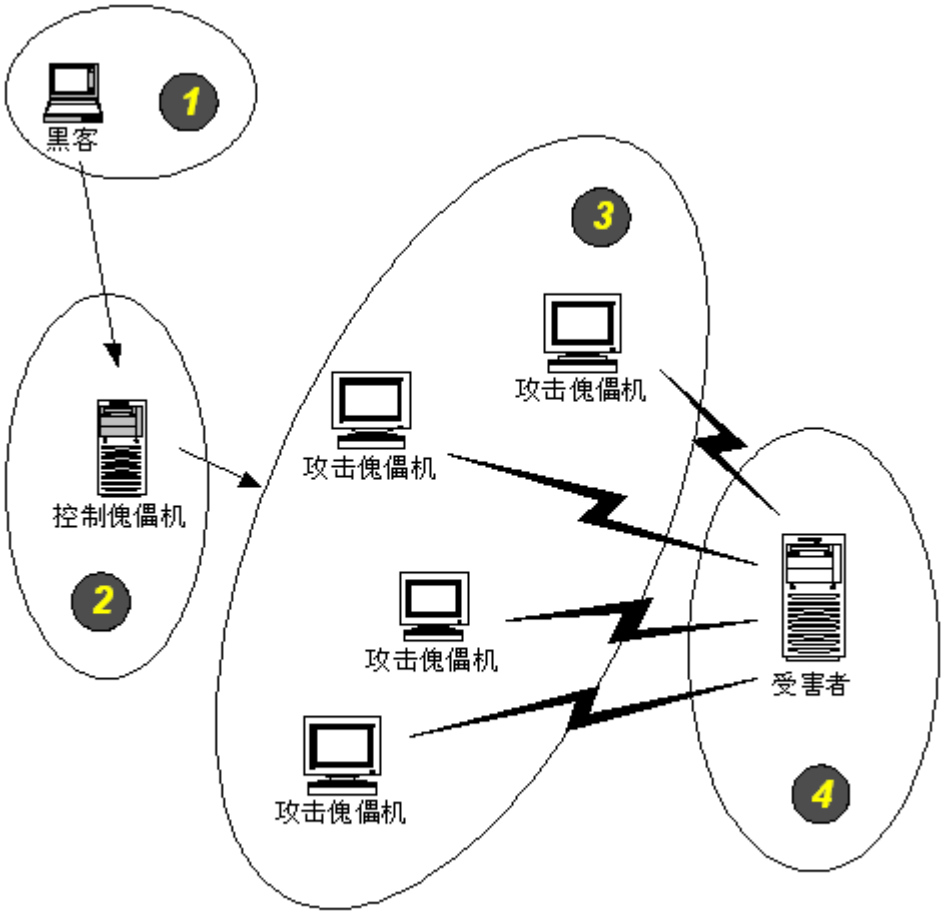
高速广泛连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5G 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

被 DDoS 攻击时的现象

- 被攻击主机上有大量等待的 TCP 连接
- 网络中充斥着大量的无用的数据包，源地址为假
- 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯
- 利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求

- 严重时会造成系统死机

攻击运行原理



图一　分布式拒绝服务攻击体系结构

如图一，一个比较完善的 DDoS 攻击体系分成四大部分，先来看一下最重要的第 2 和第 3 部分：它们分别用做控制和实际发起攻击。请注意控制机与攻击机的区别，对第 4 部分的受害者来说，DDoS 的实际攻击包是从第 3 部分攻击傀儡机上发出的，第 2 部分的控制机只发布命令而不参与实际的攻击。对第 2 和第 3 部分计算机，黑客有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击傀儡机就成为害人者去发起攻击了。

有的朋友也许会问道："为什么黑客不直接去控制攻击傀儡机，而要从控制傀儡机上转一下呢？"。这就是导致 DDoS 攻击难以追查的原因之一了。做为攻击者的角度来说，肯定不愿意被捉到（我在小时候向别人家的鸡窝扔石头的时候也晓得在第一时间逃掉，呵呵），而攻击者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台机器后，高水平的攻击者会首先做两件事：1. 考虑如何留好后门（我以后还要回来的哦）！2. 如何清理日志。这就是擦掉脚印，不让自己做的事被别人查觉到。比较不敬业的黑客会不管三七二十一把日志全都删掉，但这样的话网管员发现日志都没了就会知道有人干了坏事了，顶多无法再从日志发现是谁干的而已。相反，真正的好手会挑有关自己的日志项目删掉，让人看不到异常的情况。这样可以长时间地利用傀儡机。

但是在第 3 部分攻击傀儡机上清理日志实在是一项庞大的工程，即使在有很好的日志清理工具的帮助下，黑客也是对这个任务很头痛的。这就导致了有些攻击机弄得不是很干净，通过它上面的线索找到了控制它的上一级计算机，这上级的计算机如果是黑客自己的机器，那么他就会被揪出来了。但如果这是控制用的傀儡机的话，黑客自身还是安全的。控制傀儡机的数目相对很少，一般一台就可以控制几十台攻击机，清理一台计算机的日志对黑客来讲就轻松多了，这样从控制机再找到黑客的可能性也大大降低。

黑客是如何组织一次 DDoS 攻击的？

这里用"组织"这个词，是因为 DDoS 并不象入侵一台主机那样简单。一般来说，黑客进行 DDoS 攻击时会经过这样的步骤：

1. 搜集了解目标的情况

下列情况是黑客非常关心的情报：

- 被攻击目标主机数目、地址情况
- 目标主机的配置、性能
- 目标的带宽

对于 DDoS 攻击者来说，攻击互联网上的某个站点，如 http://www.mytarget.com，有一个重点就是确定到底有多少台主机在支持这个站点，一个大的网站可能有很多台主机利用负载均衡技术提供同一个网站的 www 服务。以 yahoo 为例，一般会有下列地址都是提供 http://www.yahoo.com 服务的：

66.218.71.87

66.218.71.88

66.218.71.89

66.218.71.80

66.218.71.81

66.218.71.83

66.218.71.84

66.218.71.86

如果要进行 DDoS 攻击的话，应该攻击哪一个地址呢？使 66.218.71.87 这台机器瘫掉，但其他的主机还是能向外提供 www 服务，所以想让别人访问不到 http://www.yahoo.com 的话，要所有这些 IP 地址的机器都瘫掉才行。在实际的应用中，一个 IP 地址往往还代表着数台机器：网站维护者使用了四层或七层交换机来做负载均衡，把对一个 IP 地址的访问以特定的算法分配到下属的每个主机上去。这时对于 DDoS 攻击者来说情况就更复杂了，他面对的任务可能是让几十台主机的服务都不正常。

所以说事先搜集情报对 DDoS 攻击者来说是非常重要的，这关系到使用多少台傀儡机才能达到效果的问题。简单地考虑一下，在相同的条件下，攻击同一站点的 2 台主机需要 2 台傀儡机的话，攻击 5 台主机可能就需要 5 台以上的傀儡机。有人说做攻击的傀儡机越多越好，不管你有多少台主机我都用尽量多的傀儡机来攻就是了，反正傀儡机超过了时候效果更好。

但在实际过程中，有很多黑客并不进行情报的搜集而直接进行 DDoS 的攻击，这时候攻击的盲目性就很大了，效果如何也要靠运气。其实做黑客也象网管员一样，是不能偷懒的。一件事做得好与坏，态度最重要，水平还在其次。

2. 占领傀儡机

黑客最感兴趣的是有下列情况的主机：

- 链路状态好的主机
- 性能好的主机
- 安全管理水平差的主机

这一部分实际上是使用了另一大类的攻击手段：利用形攻击。这是和 DDoS 并列的攻击方式。简单地说，就是占领和控制被攻击的主机。取得最高的管理权限，或者至少得到一个有权限完成 DDoS 攻击任务的帐号。对于一个 DDoS 攻击者来说，准备好一定数量的傀儡机是一个必要的条件，下面说一下他是如何攻击并占领它们的。

首先，黑客做的工作一般是扫描，随机地或者是有针对性地利用扫描器去发现互联网上那些有漏洞的机器，象程序的溢出漏洞、cgi、Unicode、ftp、数据库漏洞…(简直举不胜举啊)，都是黑客希望看到的扫描结果。随后就是尝试入侵了，具体的手段就不在这里多说了，感兴趣的话网上有很多关于这些内容的文章。

总之黑客现在占领了一台傀儡机了！然后他做什么呢？除了上面说过留后门擦脚印这些基本工作之外，他会把 DDoS 攻击用的程序上载过去，一般是利用 ftp。在攻击机上，会有一个 DDoS 的发包程序，黑客就是利用它来向受害目标发送恶意攻击包的。

3. 实际攻击

经过前 2 个阶段的精心准备之后，黑客就开始瞄准目标准备发射了。前面的准备做得好的话，实际攻击过程反而是比较简单的。就象图示里的那样，黑客登录到做为控制台的傀儡机，向所有的攻击机发出命令："预备~ ，瞄准~，开火!"。这时候埋伏在攻击机中的 DDoS 攻击程序就会响应控制台的命令，一起向受害主机以高速度发送大量的数据包，导致它死机或是无法响应正常的请求。黑客一般会以远远超出受害方处理能力的速度进行攻击，他们不会"怜香惜玉"。

老到的攻击者一边攻击，还会用各种手段来监视攻击的效果，在需要的时候进行一些调整。简单些就是开个窗口不断地 ping 目标主机，在能接到回应的时候就再加大一些流量或是再命令更多的傀儡机来加入攻击。

(作者：徐一丁　来源：TechTarget 中国)

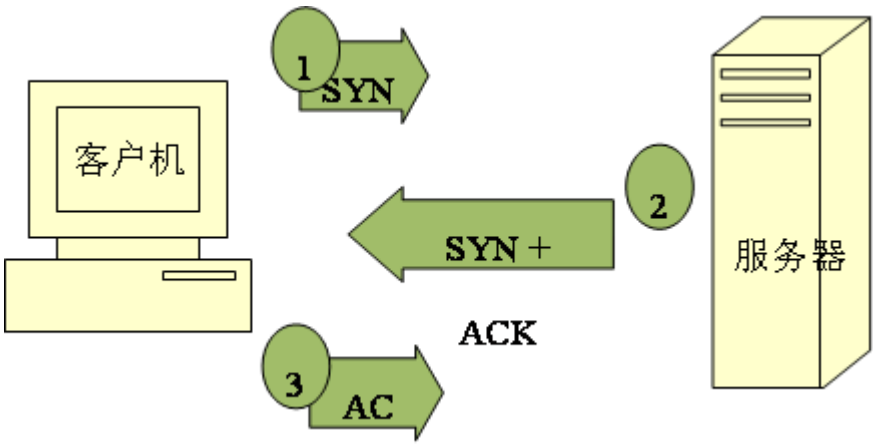
分布式拒绝服务攻击(DDoS)原理及防范（二）

DDoS 攻击实例 - SYN Flood 攻击

Syn Flood 原理 - 三次握手

Syn Flood 利用了 TCP/IP 协议的固有漏洞。面向连接的 TCP 三次握手是 Syn Flood 存在的基础。

TCP 连接的三次握手



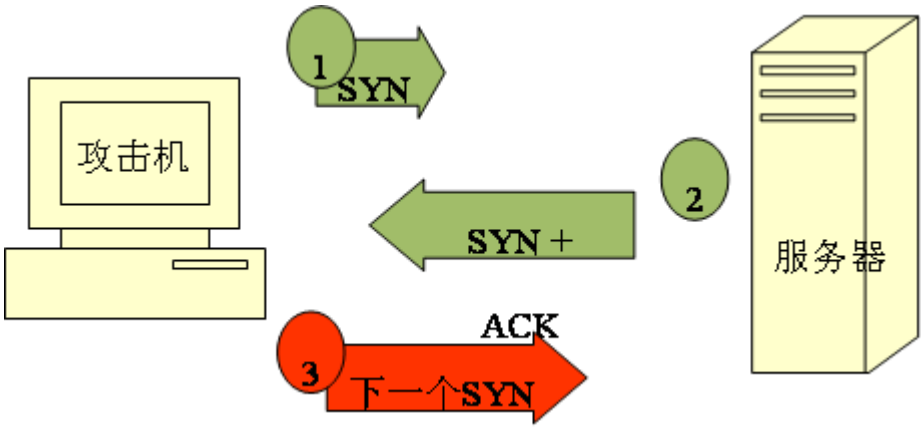
图二 TCP 三次握手

如图二，在第一步中，客户端向服务端提出连接请求。这时 TCP SYN 标志置位。客户端告诉服务端序列号区域合法，需要检查。客户端在 TCP 报头的序列号区中插入自己的 ISN。服务端收到该 TCP 分段后，在第二步以自己的 ISN 回应(SYN 标志置位)，同时确认收到客户端的第一个 TCP 分段(ACK 标志置位)。在第三步中，客户端确认收到服务端的 ISN(ACK 标志置位)。到此为止建立完整的 TCP 连接，开始全双工模式的数据传输过程。

Syn Flood 攻击者不会完成三次握手

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，这种情况我们称做：服务器端受到了 SYN Flood 攻击（SYN 洪水攻击）。



图三 Syn Flood 恶意地不完成三次握手

下面是我在实验室中模拟的一次 Syn Flood 攻击的实际过程

这一个局域网环境，只有一台攻击机（PIII667/128/mandrake），被攻击的是一台 Solaris 8.0 (spark)的主机，网络设备是 Cisco 的百兆交换机。这是在攻击并未进行之前，在 Solaris 上进行 snoop 的记录，snoop 与 tcpdump 等网络监听工具一样，也是一个很好的网络抓包与分析的工具。可以看到攻击之前，目标主机上接到的基本上都是一些普通的网络包。

```
……          ? ->
(broadcast)  ETHER Type=886F (Unknown),
size = 1510 bytes          ? ->
(broadcast)  ETHER Type=886F (Unknown),
size = 1510 bytes          ? ->
```

(multicast) ETHER Type=0000 (LLC/802.3),

size = 52 bytes ? ->

(broadcast) ETHER Type=886F (Unknown),

size = 1510 bytes192.168.0.66 ->

192.168.0.255 NBT Datagram Service

Type=17 Source=GU[0]192.168.0.210 ->

192.168.0.255 NBT Datagram Service Type=17

Source=ROOTDC[20]192.168.0.247 ->

192.168.0.255 NBT Datagram Service Type=17

Source=TSC[0] ? ->

(broadcast) ETHER Type=886F (Unknown),

size = 1510 bytes192.168.0.200 ->

(broadcast) ARP C Who is 192.168.0.102, 192.168.0.102 ?

? -> (broadcast) ETHER Type=886F (Unknown),

size = 1510 bytes ? ->

(broadcast) ETHER Type=886F (Unknown),

size = 1510 bytes192.168.0.66 ->

192.168.0.255 NBT Datagram Service Type=17

Source=GU[0]192.168.0.66 ->

192.168.0.255 NBT Datagram Service Type=17

Source=GU[0]192.168.0.210 ->

192.168.0.255 NBT Datagram Service Type=17 Source=ROOTDC[20]

? -> (multicast)

ETHER Type=0000 (LLC/802.3),

size = 52 bytes ? -> (broadcast)

ETHER Type=886F (Unknown), size = 1510 bytes ? ->

(broadcast) ETHER Type=886F (Unknown),

size = 1510 bytes……

接着，攻击机开始发包，DDoS 开始了…，突然间 sun 主机上的 snoop 窗口开始飞速地翻屏，显示出接到数量巨大的 Syn 请求。这时的屏幕就好象是时速 300 公里的列车上的一扇车窗。这是在 Syn Flood 攻击时的 snoop 输出结果：

…… 127.0.0.178 ->

lab183.lab.net AUTH C port=1352 127.0.0.178 ->

lab183.lab.net TCP D=114 S=1352 Syn Seq=674711609

Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=115 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net UUCP-PATH C port=1352 127.0.0.178 ->

lab183.lab.net TCP D=118 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net NNTP C port=1352 127.0.0.178 ->

lab183.lab.net TCP D=121 S=1352 Syn

Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=122 S=1352 Syn

Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=124 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=125 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=126 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=128 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=130 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=131 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=133 S=1352

Syn Seq=674711609 Len=0 Win=65535 127.0.0.178 ->

lab183.lab.net TCP D=135 S=1352 Syn

Seq=674711609 Len=0 Win=65535……

这时候内容完全不同了，再也收不到刚才那些正常的网络包，只有 DDoS 包。大家注意一下，这里所有的 Syn Flood 攻击包的源地址都是伪造的，给追查工作带来很大困难。这时在被攻击主机上积累了多少 Syn 的半连接呢？我们用 netstat 来看一下：

netstat -an | grep SYN ……192.168.0.183.9　　127.0.0.79.1801

0　　0 24656

0 SYN_RCVD192.168.0.183.13

127.0.0.79.1801

0　　0 24656

0 SYN_RCVD192.168.0.183.19

127.0.0.79.1801 0

0 24656 0 SYN_RCVD192.168.0.183.21

127.0.0.79.1801 0

0 24656 0 SYN_RCVD192.168.0.183.22

127.0.0.79.1801 0

0 24656 0 SYN_RCVD192.168.0.183.23

127.0.0.79.1801 0

0 24656 0 SYN_RCVD192.168.0.183.25

127.0.0.79.1801 0

0 24656 0 SYN_RCVD192.168.0.183.37

127.0.0.79.1801 0

0 24656 0 SYN_RCVD192.168.0.183.53

127.0.0.79.1801 0

0 24656 0 SYN_RCVD……

其中 SYN_RCVD 表示当前未完成的 TCP SYN 队列，统计一下：

netstat -an | grep SYN | wc -l

5273

netstat -an | grep SYN | wc -l

5154

netstat -an | grep SYN | wc -l

5267

…

共有五千多个 Syn 的半连接存储在内存中。这时候被攻击机已经不能响应新的服务请求了，系统运行非常慢，也无法 ping 通。

这是在攻击发起后仅仅 70 秒钟左右时的情况。

DDoS 的防范

到目前为止，进行 DDoS 攻击的防御还是比较困难的。首先，这种攻击的特点是它利用了 TCP/IP 协议的漏洞，除非你不用 TCP/IP，才有可能完全抵御住 DDoS 攻击。一位资深的安全专家给了个形象的比喻：DDoS 就好象有 1,000 个人同时给你家里打电话，这时候你的朋友还打得进来吗？

不过即使它难于防范，也不是说我们就应该逆来顺受，实际上防止 DDoS 并不是绝对不可行的事情。互联网的使用者是各种各样的，与 DDoS 做斗争，不同的角色有不同的任务。我们以下面几种角色为例：

- 企业网管理员
- ISP、ICP 管理员
- 骨干网络运营商
- 企业网管理员

网管员做为一个企业内部网的管理者，往往也是安全员、守护神。在他维护的网络中有一些服务器需要向外提供 WWW 服务，因而不可避免地成为 DDoS 的攻击目标，他该如何做呢？可以从主机与网络设备两个角度去考虑。

主机上的设置

几乎所有的主机平台都有抵御 DoS 的设置，总结一下，基本的有几种：

- 关闭不必要的服务
- 限制同时打开的 Syn 半连接数目
- 缩短 Syn 半连接的 time out 时间
- 及时更新系统补丁

网络设备上的设置

企业网的网络设备可以从防火墙与路由器上考虑。这两个设备是到外界的接口设备，在进行防 DDoS 设置的同时，要注意一下这是以多大的效率牺牲为代价的，对你来说是否值得。

1. 防火墙

- 禁止对主机的非开放服务的访问
- 限制同时打开的 SYN 最大连接数
- 限制特定 IP 地址的访问
- 启用防火墙的防 DDoS 的属性
- 严格限制对外开放的服务器的向外访问
- 第五项主要是防止自己的服务器被当做工具去害人。

2. 路由器

以 Cisco 路由器为例

- Cisco Express Forwarding（CEF）
- 使用 unicast reverse-path
- 访问控制列表（ACL）过滤
- 设置 SYN 数据包流量速率
- 升级版本过低的 ISO
- 为路由器建立 log server

其中使用 CEF 和 Unicast 设置时要特别注意，使用不当会造成路由器工作效率严重下降，升级 IOS 也应谨慎。路由器是网络的核心设备，与大家分享一下进行设置修改时的小经验，就是先不保存。Cisco 路由器有两份配置 startup config 和 running config，修改的时候改变的是 running config，可以让这个配置先跑一段时间（三五天的就随意啦），觉得可行后再保存配置到 startup config；而如果不满意想恢复原来的配置，用 copy start run 就行了。

ISP / ICP 管理员

ISP / ICP 为很多中小型企业提供了各种规模的主机托管业务，所以在防 DDoS 时，除了与企业网管理员一样的手段外，还要特别注意自己管理范围内的客户托管主机不要成为傀儡机。客观上说，这些托管主机的安全性普遍是很差的，有的连基本的补丁都没有打就赤膊上阵了，成为黑客最喜欢的"肉鸡"，因为不管这台机器黑客怎么用都不会有被发现的危险，它的安全管理太差了；还不必说托管的主机都是高性能、高带宽的-简直就是为 DDoS 定制的。而做为 ISP 的管理员，对托管主机是没有直接管理的权力的，只能通知让客户来处理。在实际情况时，有很多客户与自己的托管主机服务商配合得不是很好，造成 ISP 管理员明知自己负责的一台托管主机成为了傀儡机，却没有什么办法的局面。而托管业务又是买方市场，ISP 还不敢得罪客户，怎么办？咱们管理员和客户搞好关系吧，没办法，谁让人家是上帝呢？呵呵，客户多配合一些，ISP 的主机更安全一些，被别人告状的可能性也小一些。

骨干网络运营商

他们提供了互联网存在的物理基础。如果骨干网络运营商可以很好地合作的话，DDoS 攻击可以很好地被预防。在 2000 年 yahoo 等知名网站被攻击后，美国的网络安全研究机构提出了骨干运营商联手来解决 DDoS 攻击的方案。其实方法很简单，就是每家运营商在自己的出口路由器上进行源 IP 地址的验证，如果在自己的路由表中没有到这个数据包源 IP 的路由，就丢掉这个包。这种方法可以阻止黑客利用伪造的源 IP 来进行 DDoS 攻击。不过同样，这样做会降低路由器的效率，这也是骨干运营商非常关注的问题，所以这种做法真正采用起来还很困难。

对 DDoS 的原理与应付方法的研究一直在进行中，找到一个既有效又切实可行的方案不是一朝一夕的事情。但目前我们至少可以做到把自己的网络与主机维护好，首先让自己的主机不成为别人利用的对象去攻击别人；其次，在受到攻击的时候，要尽量地保存证据，以便事后追查，一个良好的网络和日志系统是必要的。无论 DDoS 的防御向何处发展，这都将是一个社会工程，需要 IT 界的同行们来一起关注，通力合作。

SYN-Flood 是目前最流行的 DDoS 攻击手段，早先的 DoS 的手段在向分布式这一阶段发展的时候也经历了浪里淘沙的过程。SYN-Flood 的攻击效果最好，应该是众黑客不约而同选择它的原因吧。那么我们一起来看看 SYN-Flood 的详细情况。

作者简介：徐一丁，北京玛赛网络系统有限公司方案设计部高级工程师，从事IT 工作多年。目前主要进行国内外安全产品评测与黑客攻击的研究。有丰富的网络安全设计与实施经验，并给各大电信公司如中国电信、吉通公司、联通公司等进行过系列安全培训。

（作者：徐一丁　来源：TechTarget 中国）

拒绝式服务攻击袭来　你采取防御措施了吗？

3月可谓多事之秋，诸多的网络攻击事件使这个月成为有史以来黑客攻击最为活跃的月份。到目前为止，我们看到：

- 3月3日，韩国电子商务网站及政府机构遭到DDoS攻击；
- 3月4日，Wordpress.com遭受DDoS攻击，业务受到严重扰乱；
- 3月6日，法国政府部门网络多次被黑，攻击目标指向G20相关文件；
- 3月9日，DDoS攻击服务器托管提供商Codero，并破坏Twitter网站；
- 3月9日，匿名黑客团体对BMI.com发起一起被称为"Operation Payback"的新型网络攻击，要求参与攻击的成员发动持续性的、毁灭性的攻击。

这些攻击所带的后果十分严重。鉴于此种情况，金融服务与信息服务分析中心（FS-ISAC)发布了一份建议书（2011-3-24），建议书指出所有的金融机构都有可能随时遭受拒绝式服务攻击,FS-ISAC金融服务中心通过再版《CERT安全指南》一书，帮助组织机构预防恶意攻击。

大型金融机构（各大银行）、服务提供商、政府财政监管部门、各种独立的技术基础架构以及关键基础设施（例如电力、天然气、网络服务提供商以及国家电网）都均为最有可能成为攻击目标。

为帮助上述机构更加有效地保护网络，Radware建议如下：

一、在网络边界采取防御攻击的安全措施

- 采用深度安全方案，通过反DDoS攻击的安全战略，预防和缓解所有的攻击流量，从本质上清除网络边界潜在的威胁。
- 确保解决方案能够实时检测网络周边的异常行为和入侵活动，防御所有的应用层攻击，区别合法、非法的流量，通过日志或相关系统收集详细的攻击数据并及时报告。

二、互补的安全技术必不可少

除了基本的 IPS 和防火墙保护，还需要部署多元化的安全解决方案来成功避免已知和未知的攻击威胁。具体包括以下内容：

－防 DoS/DDoS 攻击工具（网络与应用层）用来防止网络淹没攻击
－基于实时特征码技术的网络行为分析工具，使用户免受应用滥用及"零日"攻击
－通过入侵防御系统预防已知的应用漏洞威胁
－积极的应用层防御机制有效应对攻击挑战并提升响应时间
－积极的紧急反攻击策略（Smart Hands / Man-in-the-Loop 功能）

三、积极防御，随时防范攻击

- 订完善的防御计划，将专业技术人员纳入的安全事件的处理当中，以确保防御工具、警报、相关系统及解除攻击的方法，都能够正常合理的进行。
- 当系统遭到攻击，应急响应团队能立即提供支持并积极缓解攻击或进行防御。
- 积极的防御也是一种反击方式，可以消除残余的 DDoS 攻击，也可以对棘手的攻击事件进行必要的防范。

（来源：TechTarget 中国）

如何防御网络拒绝服务攻击

问：我听说在 GoDaddy.com 在 Super Bowl 期间受到了数量空前的攻击，而其他一些公司也在大型市场竞争中遇到过这种问题。如果我想要我的公司在特定的时间内可以面对强烈的攻击，我应该采取什么措施来抵挡冲击呢？

答：这是各种商业集团都需要协同合作分享信息的情况之一。例如，如果你的公司计划大型的广告活动，那么广告部的领导应该和 IT 及安全部门工作。网络流量（恶意的和合法的）可能会增加，而企业应该准备好应对各种情况。

首先，确保要有足够的带宽，不止要传输合法流量，而且要可能会有小规模的拒绝服务（DoS）攻击。我推荐在新活动开始前对 Web 架构漏洞评估和渗透测试，包括 DoS 测试。需要注意的是这些攻击可能持续几个小时、几天甚至几周。在你觉得受到了 DoS 攻击的任何时候，都应高和 ISP（Internet Service Provider，互联网服务提供商）代表即时联系。

（作者：John Strand　译者：Tina Guo　来源：TechTarget 中国）

如何阻止分布式拒绝服务攻击

分布式拒绝服务攻击，通过强迫企业系统宕机来耗费时间和金钱，对企业造成损害。本文将有助于你更好的理解分布式拒绝服务攻击的原理、它们可能造成的灾害以及如何阻止分布式拒绝服务攻击对企业服务器和系统造成伤害。

分布式拒绝服务攻击的工作原理

恶意黑客利用计算机系统（通常是网站或 Web 服务器）的缺陷或漏洞伪装成一个主系统，来执行 DDoS 攻击。当成功伪装成主系统后，黑客便可以识别其他的系统并和他们进行通讯，以便进行潜在的进一步侵害。

一旦入侵者控制了大量的傀儡系统，他/她就可以指使这些系统对某个目标系统发动一次淹没攻击，使目标系统被大量的假通信请求淹没，进而导致目标系统上的用户服务被拒绝。来自傀儡系统的大量流入信息将导致目标系统宕机，并拒绝提供服务，这样使得用户无法接受任何信息，导致用户时间和金钱的损失。

如何有效地防御分布式拒绝服务攻击（DDoS）

防御分布式拒绝服务攻击可能会很困难，因为从一堆使用相同协议和端口的通信需求中区分出某个恶意通信需求是一件相当有挑战性的事。然而，你可以采取以下几个步骤来保护系统免受分布式拒绝服务攻击。

- 确保公司的互联网连接有多余的网络带宽：这是最容易的防御分布式拒绝服务攻击的方法，但同时它也是昂贵的。只要有足够的带宽来处理通信请求，就可以有效的防止小规模的分布式拒绝服务攻击（DDoS）。同时，企业拥有的网络带宽越大，攻击者就越难去阻塞它的连接。
- 请务必使用入侵检测系统（IDS）。如今有的一些入侵检测系统通过核查连接的方法和阻止某些请求到达公司服务器的方法，已经拥有了保护系统免受 DDoS 攻击的技术。
- 使用分布式拒绝服务攻击（DDoS）防御产品。许多厂商提供 DDoS 防护以及防御装置用来专门应对 DDoS 的攻击。

- 设置 DoS 响应。节流和速限技术可以降低 DDoS 攻击的损害。
- 为重要用户提供一个使用单独 IP 地址池的备份互联网连接。当主要线路被大量恶意请求淹没时，这将提供一条备用链路。

(作者：SearchSecurity.com Staff 译者：Lily 来源：TechTarget 中国)

如何防御网站上的分布式拒绝服务攻击

问：防止我们的网站受到分布式拒绝服务攻击的最好方法是什么？

答：在分布式拒绝服务攻击（distributed denial-of-service，DDoS）中，攻击者在不同的互联网位置使用大量系统向服务器发送洪水般的伪造流量请求淹没服务器。由于攻击流量和合法的 Web 请求之间的相似性，这些攻击很难防御。

但是仍然有些方法可以自我保护。以下是一些基本建议：

- 确保在互联网连接上有合适的带宽。只需简单地使用足够的带宽（和处理能力）来支持请求服务就可以避免低程度的 DDoS。
- 在网络上配置入侵防御系统。有些（但不是所有）DDoS 攻击都有可识别的签名，可以被 IPS 检测到，并用于防御这些请求进入 Web 服务器。
- 使用 DDoS 防御工具，包括思科的 Cisco Guard 产品。它是特别为识别和防御分布式拒绝服务攻击而设计的。
- 为重要用户使用独立的 IP 地址，来进行备份互联网连接。当你不能把所有的网站访问转换到备份的连接上（攻击会同时转移！）时，你可以在原来的路径充满了伪造请求地事后，向重要用户提供网站的另一个途径。

这些技巧可以帮你建造坚固的 Web 基础架构，可以最好的在 DDoS 攻击中存活。祝你好运。

（作者：Mike Chapple　译者：Tina Guo　来源：TechTarget 中国）

四招打败僵尸网络的拒绝服务攻击

也许很多人还没有注意到，据 Arbor Networks 的统计，2008 年僵尸网络的拒绝服务攻击超过了每秒 40GB 的限度。这也就是说，当前的僵尸网络的攻击规模已经达到一个僵尸网络有 190 万台僵尸电脑的程度，而僵尸网络的拒绝服务攻击是最难防御的攻击之一。因此，这也是拒绝服务攻击成为勒索者试图把在线商家作为人质获取赎金的常用手段的原因。这对于犯罪分子来说是一笔大买卖，而且这个生意很兴隆。

下面这种情况就很常见：犯罪分子利用一个僵尸网络大军渗透和消除对于你有价值的服务。攻击目标的范围包括仅用一个拒绝服务攻击使你的一台重要服务器达到饱和或者使你的互联网连接达到饱和，有效地中断你的全部互联网服务。在某些情况下，这些坏蛋首先发起攻击，中断网络服务，然后要求支付赎金。有时候，这些坏蛋仅仅发出赎金的要求，并且威胁说如果不在某日之前满足他们的要求，他们将中断攻击目标的网站。

当然，这些可能对我们来说已经不是什么新鲜事了。但是，如果你遭到过僵尸网络的拒绝服务攻击或者遭到过多次这种攻击，你是否想过你和你的公司应该采取什么措施吗?你如何准备应对这种类型的攻击?许多公司(包括大企业和小企业)都这样对待这个问题，他们解释说"我们没有黑客要的东西"或者"我们是小目标，不值得这样麻烦"。在某些情况下，这种事情是非常真实的，就是拒绝服务攻击的风险不值得安全投资。但是，在许多情况下，这种想法是一种危险的错误。这种风险实际上比想象的要大。如果我从一个坏蛋的角度考虑这个问题，我在追求一二样东西，金钱或者名誉。如果你能够提供其中任何一样东西，你就有机会成为攻击目标。

因此，现在我们就来解决这个问题。你如何能够打败一个僵尸网络的拒绝服务攻击?这个答案取决于你遇到的拒绝服务攻击的类型、你的网络基础设施、你拥有的安全工具和其它变量。尽管在你的独特的环境中你如何防御拒绝服务攻击有许多变量，但是，强调一些最流行的策略是有价值的。

下面是打败拒绝服务攻击的一些技巧。其中有些方法过去在防御拒绝服务攻击中取得了成功。有些方法是全新的，但是，提供了一种非常令人心动的解决方案。

由 ISP 提供的拒绝服务攻击防御产品或者拒绝服务攻击服务

这种防御策略是通常是最有效的，当然也是最昂贵的。许多 ISP(互联网服务提供商)为你的互联网链路提供某种方式的云计算拒绝服务攻击保护。这个想法是 ISP 在允许通讯进入你的互联网线路之前先清理你的通讯。由于这种防御是在云计算中完成的，你的互联网链路不会被拒绝服务攻击阻塞。不被阻塞至少是这个防御的目标。再说一次，没有一劳永逸的高明办法。这种服务也可以由第三方在云计算拒绝服务攻击防御服务中提供。在发生拒绝服务攻击时，他们把你的通讯转移到他们那里。他们清理你的通讯然后再把这些通讯发回给你。这一切都是在云计算中发生的，因此，你的互联网线路不会被阻塞。ISP 提供的拒绝服务攻击服务的例子包括 AT&T 的互联网保护服务和 Verizon Business 提供的拒绝服务攻击防御减轻服务。

RFC3704 过滤

基本的访问控制列表(ACL)过滤器。RFC3704 的主要前提是数据包应该来自于合法的、分配的地址段、与结构和空间分配一致。要达到这个目的，有一个全部没有使用的或者保留的 IP 地址的列表。这些地址是你从互联网中永远看不到的。如果你确实看到了这些地址，那么，它肯定是一个欺骗的源 IP 地址，应该丢弃。这个列表的名称是 Bogon 列表，你应该咨询一下你的 ISP，看他们是否能在这个欺骗的通讯进入你的互联网链路之前在云计算中为你管理这种过滤。Bogon 列表大约每个月修改一次。因此，如果 ISP 没有为你做这个事情，那么，你必须自己管理你的 Bogon 访问控制列表规则(或者找另一家 ISP)。

黑洞过滤

这是一个非常有效的常见的技术。一般来说，这需要与你的 ISP 一起做。RTBH(远程触发黑洞)过滤是一种能够提供在不理想的通讯进入一个保护的网络之前放弃这种通讯的能力的技术。这种技术使用 BGP(边界网关协议)主机路由把发往受害者服务器的通讯转接到下一跳的一个 null0 接口。RTBH 有许多变体，但是，其中一个变态值得特别关注。与你的 ISP 一起试试 RTBH 过滤，让他们为你在云计算中放弃那种通讯，从而防止拒绝服务攻击进入你的通讯线路。

思科 IPS 7.0 源 IP 声誉过滤

思科最近发布了 IPS 7.0 代码更新。这个升级包括一个名为全球关联的功能。简言之，全球关联功能检查它看到的每一个源 IP 地址的声誉得分。如果这个来源的声誉不好，入侵防御系统(IPS)的传感器就可以放弃这个通讯或者提高一个点击的风险级别值。下面是思科对全球关联功能的解释：

IPS 7.0 包含一个名为"思科全球关联"的新的安全功能。这个功能利用了我们在过去的许多年里收集的大量的安全情报。思科 IPS 将定期从思科 SensorBase 网络接收威胁更新信

息。这个更新的信息包括互联网上已知的威胁的详细信息，包括连续攻击者、僵尸网络收获者、恶意爆发和黑网(dark nets)等。IPS 使用这个信息在恶意攻击者有机会攻击重要资产之前过滤掉这些攻击者。IPS 然后把全球威胁数据结合到自己的系统中以便更早地检测和防御恶意活动。

当然，你可以设置全球关联，这样的话，你的传感器就能够知道有恶意活动声誉的网络设备，并且能够对这种设备采取行动。

思科调整 SensorBase 的方法之一是接收来自思科 7.0 IPS 传感器的信息。企业可以选择使用这个程序，也可以选择不适用这个程序。思科 IPS 使用的 SensorBase 有不同的威胁种类。其中两种是僵尸网络收获者和以前的拒绝服务攻击实施者。因此，当你遭到僵尸网络拒绝服务攻击的时候，这个传感器将放弃所有的来至声誉不良的来源的通讯。这个过程在使用这种特征之前就开始了，对于传感器资源(处理器、背板等)来说是非常便宜的。这使它成为在拒绝服务攻击期间使用的一个理想的方法。这也是思科 IPS 在处理 IPS 特征之前检查 SensorBase 的原因。

许多僵尸网络拒绝服务攻击使用通向你的网络服务器的 SSL(安全套接字层)。这有助于攻击者隐藏其负载，防止你可能拥有的检测引擎的检查。然而，考虑到全球关联仅使用源 IP 地址的声誉得分做出决定，防御 SSL 分布式拒绝服务攻击是没有问题的。没有任何其它厂商为自己的 IPS 解决方案增加基于声誉的检查功能，因此，它们不能防御任何形式的 SSL 分布式拒绝服务攻击。一些 IPS 厂商确实能够能通过解密传输中的数据打开和查看 SSL 数据包内部。然而，这个过程在 IPS 资源(处理器、背板、内存等)方面太昂贵，不能用于分布式拒绝服务攻击。它会迅速消除传感器本身的通讯瓶颈。

当然，如果这个分布式拒绝服务攻击阻塞了你的链路，这个策略可能就不起作用。但是，如果分布式拒绝服务攻击仅仅阻塞了部分服务器，而没有阻塞整个网络，那就表明这个防御措施的作用很好。全球关联不是一个妙方，而是你的工具箱中的另一个工具。

IP 源防护

这个问题不是五大主要问题的一部分，不过，这个问题仍然值得一提。这个技巧是打开你的交换机中的 IP 源防护功能。这个功能可以阻止主机在变成僵尸电脑的时候发出欺骗性的数据包。这不是一个防御工具，而是一个守法公民工具，尽管它能够阻止内部的欺骗性的分布式拒绝服务攻击。如果每一家公司都打开 IP 源防护功能，它就能够帮助减少我们遇到的欺骗性分布式拒绝服务攻击的数量。启用 IP 源防护功能的一项增加的好处是能够帮助你找到你的网络中已经成为僵尸网络一部分的主机。当这个恶意软件发动欺骗性攻击的时候，这个交换机端

口能够自动锁死，并且向你的安全监视站点报告这个事件。或者你报告这个事件并且保持打开这个端口，但是，除了真正的IP地址源通讯之外，放弃所有的通讯。

（作者：秦老　来源：TechTarget中国）

当拒绝服务攻击遇到云

拒绝服务攻击这一古老的网络犯罪在几年再次成为了数据中心运营者们的心头之患。

随着公司越来越多地使用虚拟化数据中心和云服务，企业基础架构中新的薄弱环节也就渐渐浮出了水面。与此同时，拒绝服务攻击正在把目标从野蛮的数据洪潮中转向对应用基础架构更具技术性的攻击。

对于把关键商业数据存储在外部设备和业务依赖于持续通讯的企业而言，这样的威胁日趋严重。另外，随着多租户服务的普及，拒绝服务已经把攻势瞄准了那些可能对其它协同定位公司的服务产生重大影响的公司，即便两者并处于同一行业。

"企业依然把安全和有效性列为接受云计算的头等障碍，"Frost & Sullivan 的信息安全研究全球项目经理 Rob Ayoub 在一份声明中称，"今天的主机和其他数据中心经营者必须有能力在不中断对用户服务的同时从容地应对这些攻击。"

最明显的攻击将继续像数据的洪水一般侵袭受害者的网络，干扰公司与其上游供应商的联系。网络基础架构公司 VeriSign（VRSN）在最新的域名行业简报中指出，暴力的拒绝服务攻击的势头猛增，这些可以在迅速增加的域名查找中看出来。

分布式拒绝服务攻击"可能会在我们的通信流量中占有几个百分点，"VeriSign 的首席技术官 Ken Silva 说。"这对于我们而言不过是一个很小的污染问题，但是对于受害者而言就很成问题了。"

最好的解决办法是追捕到攻击者，可是在僵尸网络和匿名代理的世界里，这又谈何容易。不过，专家说还是有办法的。以下列出四个关于新旧世界中分布式拒绝服务攻击（DDoS）的经验之谈，供大家借鉴。

1. 分布式拒绝服务攻击非常简单

过去，在分布式拒绝服务攻击中的计算机一般会受到一个单一病毒的攻击。当病毒从足够多的系统中清除出去，攻击者就能够继续覆没一个网络。然而，随着僵尸网络的兴起，还有将这些网络租赁给攻击者和犯罪分子，受害者的网络安全就受到了严重的威胁。除此以外，仅仅控制一个网络连接变得十分简单，特别是通过显著增加带宽进行的分布式拒绝服务攻击，Prolexic 网络防护服务首席技术官 Paul Sop 说。

"人们不了解攻击者用增加带宽来击败你有多么轻而易举，"Sop 说。

在 2005 年，受害者在受到攻击时所监测到的信息流量高达到 3.5Gbps。在 2006 年，这个数字甚至超过了 10Gbps，在很多情况下还受到网络主干线能力的限制。在 2009 年，Arbor Networks 监测到有超过 2700 起袭击事件中的信息流量超过 10Gbps。

2. 具体的应用程序成为目标

今天，拒绝服务攻击的危险越来越集中在公司基础架构中资源密集型的部分，之后使关键服务器和服务中断。攻击者使用低带宽攻击特定的应用程序，以此来攻击受害者的在线服务。

比如，滥用安全 HTTP 请求可能会让公司的服务器和路由器瘫痪，或者开放大量账户创建请求，以此来牵制很多应用程序，Sop 说。

"这些人在过去学会了如何用泰森式的拳头来击败受害者，但是在最近的三年里，我们也看到了很多人面对这样的攻击如何做出漂亮的回应，"他说，"真正的攻击者只攻击应用程序本身。"

3. 了解主机代管的现实

在云中，公司不仅仅需要担心针对他们资源的攻击，而且需要留意他们协同定位的租户。当然，使用协同定位服务的公司必须确保他们的设备受到妥善的保护。物理服务器可能控制着大多用户的虚拟机，供应商也应该采取不同的措施来确保虚拟机之间的安全。

"那些供应商在共享平台上托管很多客户，"Sop 说。事实上，公司不太可能了解他们到底拥有怎样的邻居，所以审核他们数据中心房东的防御体系应该是他们所做的第一步。了解你对于安全问题所需要担负的责任也非常重要，因为有时候，这不属于你的协同定位供应商的职责范围。

4. 期待云来帮助云

虽然向云计算的运动已经凸现了企业基础架构中的弱点，并且增加了公司连接到网络的危险性，但是，不可否认，云计算能够迅速提供资源并且能够快速收集关键领域专业信息的能力可以缓解这样的威胁，Silva 说。

"你可以拥有世界上最棒的数据中心，但是你只能在每个数据中心里安置一定数量的带宽，"他说。

相反，公司应该与一家带宽即服务的供应商达成协议，无论是内容分发网络比如 Akamai 或者是像 VeriSign 提供的更为纯粹的基础架构支持，他补充道。

"我认为 CIO 们需要不断地学习和汲取经验教训才是在云中减少拒绝服务攻击唯一真正的出路，不论这个云是帮你自己创建的还是你购买的，"Silva 说。

对于每一个数据中心的运营者而言，真正的教训是，如果这样的袭击已经干预了你的网络与互联网之间的联系，那么，就太迟了。

"受害者所能做的最坏的打算就是在自己的家门口进行防御之战，"Sop 说。

(译者：哲婷　来源：TechTarget 中国)

云计算应对拒绝服务攻击的四个教训

拒绝服务攻击这种老套的网络犯罪如今成为了数据中心管理人员所需面临的新威胁。

随着越来越多的公司开始使用虚拟化数据中心和云服务，企业基础设施出现了新的弱点。与此同时，拒绝服务攻击也开始由原来利用大量数据流进行暴力式攻击转变为针对基础应用程序的技术性攻击。

云安全缺失了什么?

企业云安全 在线服务应该具备五大特征

云安全：多方谋攻拨云安全迷雾

拒绝服务攻击正对那些将重要业务数据放置在公司以外的公司构成越来越大的威胁，因为他们的业务依赖于持续的通讯。此外，随着多租户的普及，针对一个公司的攻击可能会影响到另外一些虽然没有联系的，但也采用主机托管的公司的服务。

Frost & Sullivan 公司信息安全研究部全球项目总监 Rob Ayoub 称："在部署云计算中，企业一直将安全性和可获得性作为重中之重。考虑到这些因素，托管和其他的数据中心管理人员必须具备在不中断客户服务的情况下缓解攻击的能力。"

效果最明显的攻击仍然是发送大量的数据包，这将重创受害者的网络，堵塞公司与上游服务提供商之间的连接。暴力式拒绝服务攻击正在大幅增长，这导致互联网基础设施公司 VeriSign 在他们最新一期"域名行业简报"(Domain Name Industry Brief)中对这一趋势进行了评论。

VeriSign 公司首席技术官 Ken Silva 称："分布式拒绝服务攻击可能在我们信息中占一定比例。对于我们来说这是一个很小的问题，但是对于受害者来说这却是一个重大问题。"

最佳的解决方案是抓获攻击者，但是由于全球僵尸网络泛滥和大量的匿名代理导致这非常困难。不过专家表示，除此之外还是有一些其它的解决办法。以是是四则关于 DDoS 攻击的教训。

1. 发动 DDoS 攻击很容易

过去，黑客发动拒绝服务攻击通常是通过一个蠕虫病毒。当蠕虫病毒在整个系统中被清除后，黑客瘫痪整个网络的能力也将随之终止。

网络保护服务公司 Prolexic 公司首席技术官 Paul Sop 称，随着极难根除的僵尸网络的出现，以及向攻击者出租这些僵尸网络的营生的出现，犯罪分子可以随意的用数据包淹没受害者的网络。并且堵塞单一的网络连接变得更为容易，特别是在 DDoS 攻击带宽大幅增加后。

Sop 称："人们不明白攻击者怎么那么容易就可以的增加他们的带宽以实施攻击。"

统计信息显示，在 2005 年，攻击数量达到顶峰时的带宽为 3.5 Gbps。到了 2006 年，这一数值超过了 10 Gbps，并且在很多情况下受到了互联网骨干连接能力的限制。Arbor 网络的调查显示，在 2009 年，带宽超过 10 Gbps 的情况下发生了 2700 多起攻击事件。

2. 以特殊应用为目标

尽管目前拒绝服务攻击的风险正在增大，过去这些攻击主要将目标锁定为公司基础设施中的资源密集部分，但是现在关键服务器与服务成为了攻击目标。攻击者利用低带宽对特殊应用进行攻击即可瘫痪受害者的在线服务。

Prolexic 公司的 Sop 举例称，滥用安全 HTTP 请求会导致公司服务器和路由器堵塞，大量的帐户创建请求也会堵死许多应用。

他称："这些坏家伙在过去学会了如何用泰森的拳法暴打受害者，然而在过去三年里，我们发现这些家伙开始转战网络，对网站进行攻击。不过，真正的攻击者攻击的目标是应用自身。"

3. 熟悉主机托管

在云计算中，公司需要担心的不仅仅是对他们资源的攻击，还需要担心对主机托管租户的攻击。使用主机托管服务的公司必须确保设施获得了充分的保护。物理服务器可以支持多个客户的虚拟机，提供商采取不同的措施以确保虚拟机间的安全距离，为受管制行业中的客户处理相关的管制问题。Sop 称："这些提供商在共享平台上托管着大量的客户。"

尽管公司不太可能知道他们的邻居是谁，但是审查他们租用的数据中心的防御措施是第一步。熟悉自己需要承担哪些安全负责，托管提供商无需承担哪些安全责任也是非常重要的。

4. 用云计算帮助云计算

尽管云计算的普及正在为公司的基础设施带来一些新弱点，增加了公司与互联网连接的重要性，但是云计算可以快速提供资源、汇聚重要领域内的专家的特点也可帮助缓解威胁。

Sop 称："你能够拥有世界上最好的数据中心，但是对于每个数据中心，你只能拥有不多的带宽。"

相反，公司应当与带宽即服务提供商签订合同，无论其服务是类似 Akamai 公司的内容分发网络还是类似 VeriSign 公司那样的纯粹基础设施服务。

Silva 称："我认为，对于首席信息官来说能够真正并且有效缓解拒绝服务攻击的方法正是云计算，无论这个云是你自己创建的还是你购买的。"

Sop 指出，每位数据中心管理人员需要吸收的教训是，如果攻击到达了连接互联网的网络连接，那么一切都为时已晚。他称："对于受害者来说，最糟糕的事情就是在家门口与攻击者作战。"

（作者：网界网　来源：TechTarget 中国）