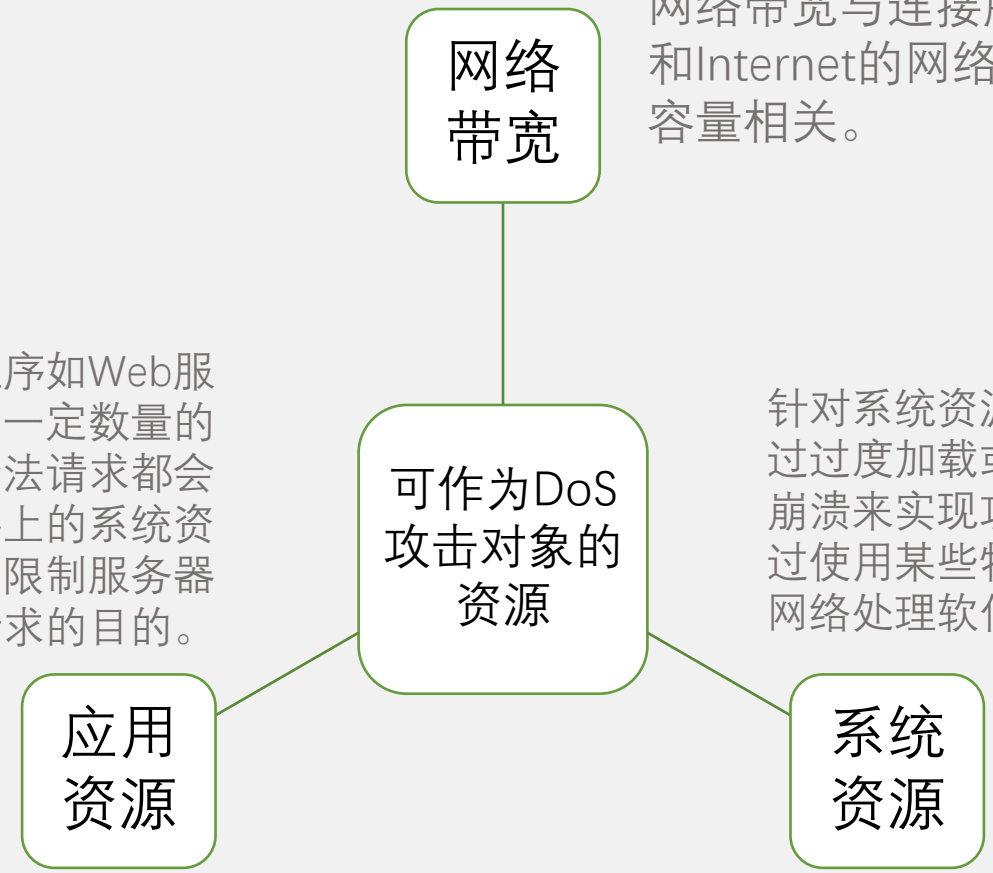
第七章 拒绝服务攻击

- 7.1 拒绝服务攻击
- 7.2 洪泛攻击
- 7.3 分布式拒绝服务攻击
- 7.4 基于应用的带宽攻击
- 7.5 反射攻击与放大攻击
- 7.6 拒绝服务攻击防范
- 7.7 对拒绝服务攻击的响应

7.1.1 拒绝服务攻击的本质

- 拒绝服务（Denial-of-Service，DoS）攻击是一种针对某些服务可用性的攻击。在计算机和通信安全的背景下，DoS攻击一般攻击目标系统的网络服务，通过攻击其网络连接来实现。这种针对服务可用性的攻击不同于其他传统意义上的不可抗力产生的攻击，它是通过造成IT基础设施的损害或毁坏而导致服务能力的丧失。
- NISTSP 800-61计算机安全事故处理指南（NIST Computer Security Incident Handling Guide）[CICH12]中对DoS攻击给出的定义如下：拒绝服务（DoS）是一种通过耗尽CPU、内存、带宽以及磁盘空间等系统资源，来阻止或削弱对网络、系统或应用程序的授权使用的行为。

7.1.1 拒绝服务攻击的本质



7.1.1 拒绝服务攻击的本质

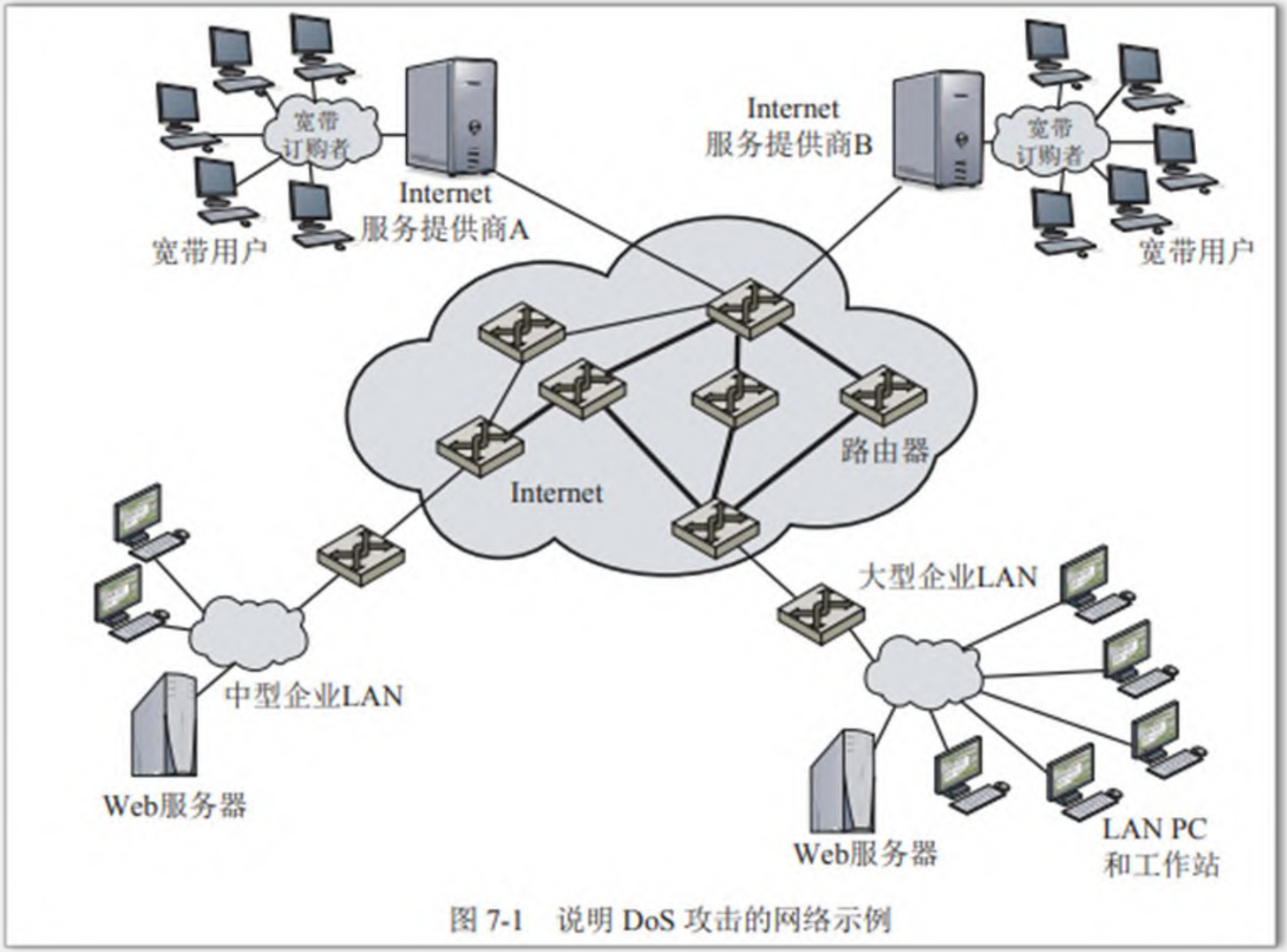


图 7-1　说明 DoS 攻击的网络示例

7.1.2 经典的拒绝服务攻击

- 对于一个组织，最简单的经典DoS攻击就是洪泛攻击（flooding attack）。
- 洪泛攻击的目标就是占据所有到目标组织的网络连接的容量。如果攻击者能够访问具有大容量网络连接的系统，那么这个系统可能会产生比目标连接容量大得多的通信流量。
- 在经典的ping洪泛攻击中，ICMP回送请求数据包的源地址使用的是攻击者的真实IP地址，攻击的源很容易被识别。
  ① 由于攻击源很容易被明确地识别，那么被发现和受到法律追究的可能性大大增加。
  ② 目标系统会尽可能地响应请求。每当服务器接受到一个ICMP回送请求数据包，就会发送一个ICMP回送响应数据包直接给攻击者，这会将攻击反射给攻击源。

7.1.3 源地址欺骗

- 在很多类型的DoS攻击中，所使用数据包的一个共同特征是采用伪造的源地址，也就是所谓的源地址欺骗(source address spoofing)。
- 这往往是通过许多操作系统上的原始套接字接口（raw socket interface）来实现。
- 攻击者可以制造出大量的目的地址指向目标系统的数据包，但这些数据包的源地址是随机选择的，通常各不相同。
- 拥塞将发生在连接到最终的低容量链路的路由器上。
- 使用带有伪造源地址的数据包也会使得发现攻击者很困难。
- 为什么Internet中允许如此容易地伪造源地址?

7.1.4 SYN欺骗

- 除了基本的洪泛攻击，另一种常见的经典DoS攻击是SYN欺骗攻击。
- SYN欺骗攻击通过造成服务器上用于管理TCP连接的连接表溢出，从而攻击网络服务器响应TCP连接请求的能力。
- 这意味着以后的合法用户的TCP连接请求将得不到服务器响应，拒绝其访问服务器。
- SYN欺骗攻击是针对系统资源的DoS攻击，具体地说就是针对操作系统上网络处理程序的攻击。

7.1.4 SYN欺骗

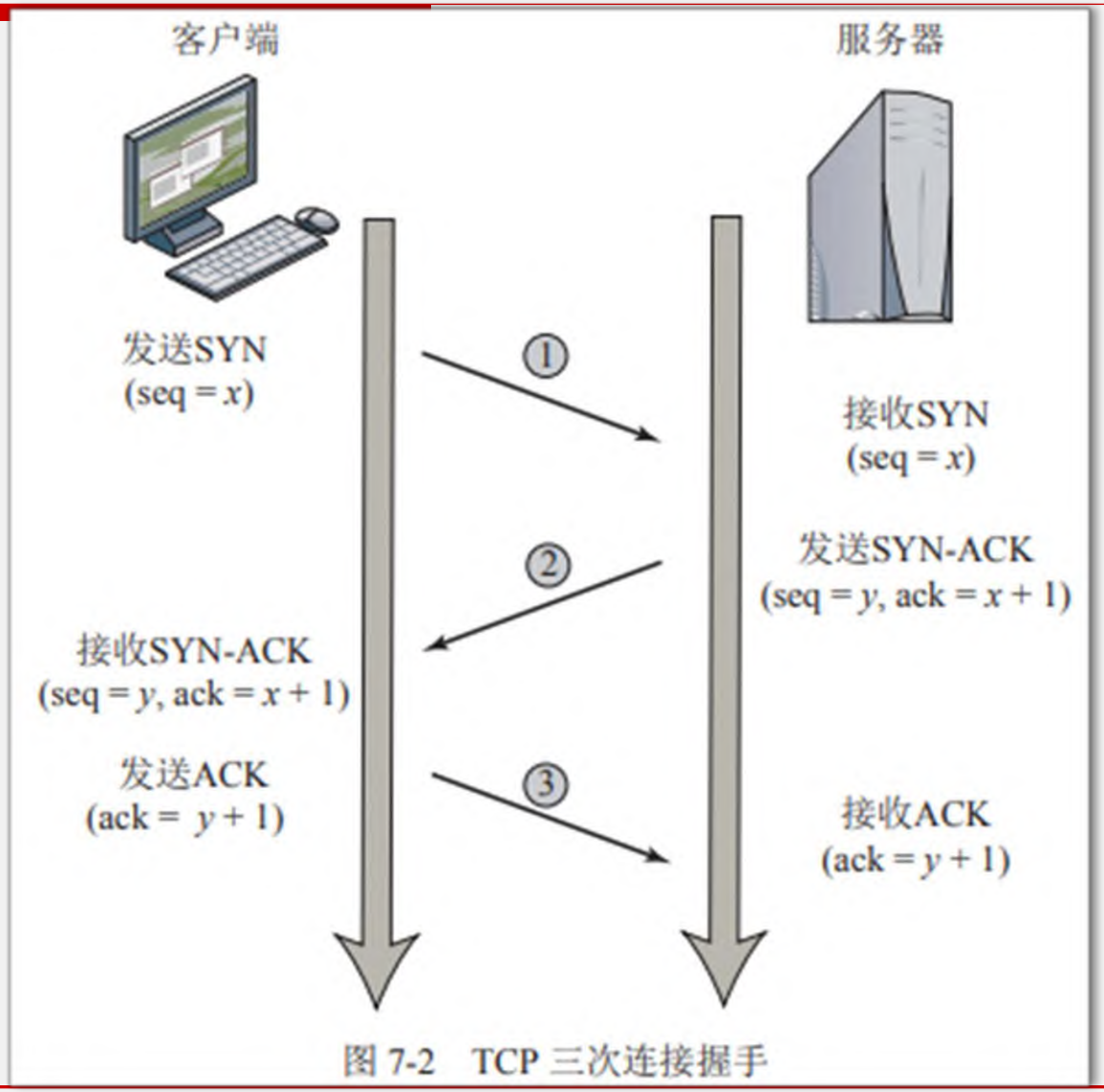


图 7-2 TCP 三次连接握手

7.1.4 SYN欺骗

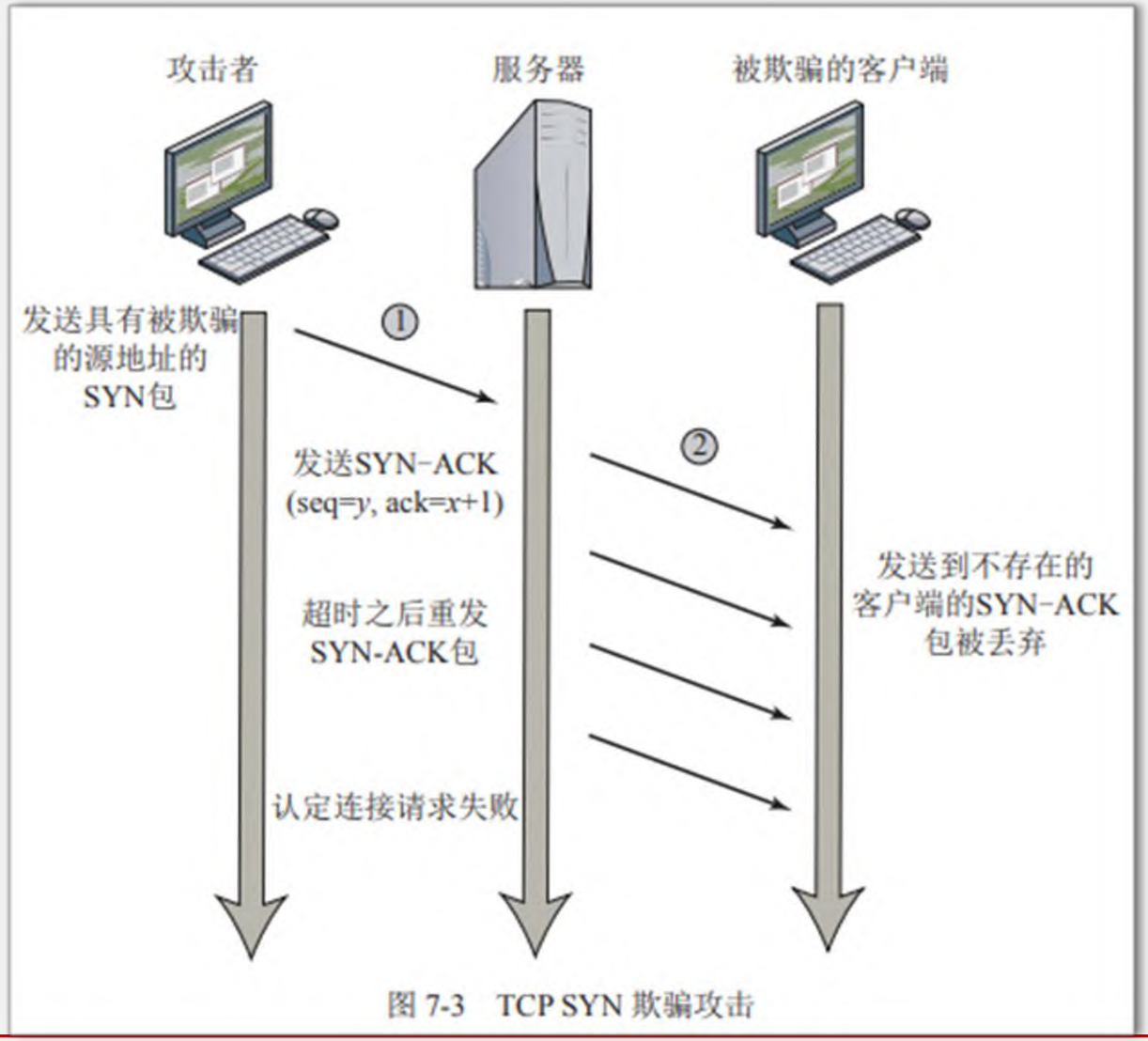


图 7-3 TCP SYN 欺骗攻击

7.2 泛洪攻击

根据攻击所使用的网络协议不同，洪泛攻击可以划分为不同类型。不管何种类型的洪泛攻击，其目的大都是使到服务器的链路超负荷。洪泛攻击的目的也可以是使服务器处理和响应网络流量的能力超负荷。

几乎任何类型的网络数据包都可以用来进行洪泛攻击。

只要数据包能够被允许流过到目标系统的链路，那么它就可以消耗到目标服务器的某个链路上的所有可用流量。实际上，数据包越大，攻击的效果就越好。通常的洪泛攻击所使用的攻击数据包类型有：

- ICMP数据包
- UDP数据包
- TCP SYN数据包

7.2 分布式拒绝服务攻击

认识到单机洪泛攻击的局限性并引入多机系统进行攻击，是DoS攻击工具的一个早期的重要发展。典型的多机系统都是受控的用户工作站或者PC机。攻击者通过操作系统上或者某些常用应用程序的一些熟知的漏洞来获得访问这些系统的权限，并在上面安装自己的程序。这些被入侵的主机系统就是所谓的僵尸机（zombie）。

为了防止自己成为DDoS攻击中的不知情参与者，最好的措施是不让自己的系统被攻击者控制。这就要求有良好的系统安全操作规范，及时打补丁，升级操作系统和应用程序到最新版本。

对于DDoS攻击的目标来讲，其对攻击的响应与对任何的洪泛攻击的响应一样，只是响应量更多、更复杂。

7.2 分布式拒绝服务攻击

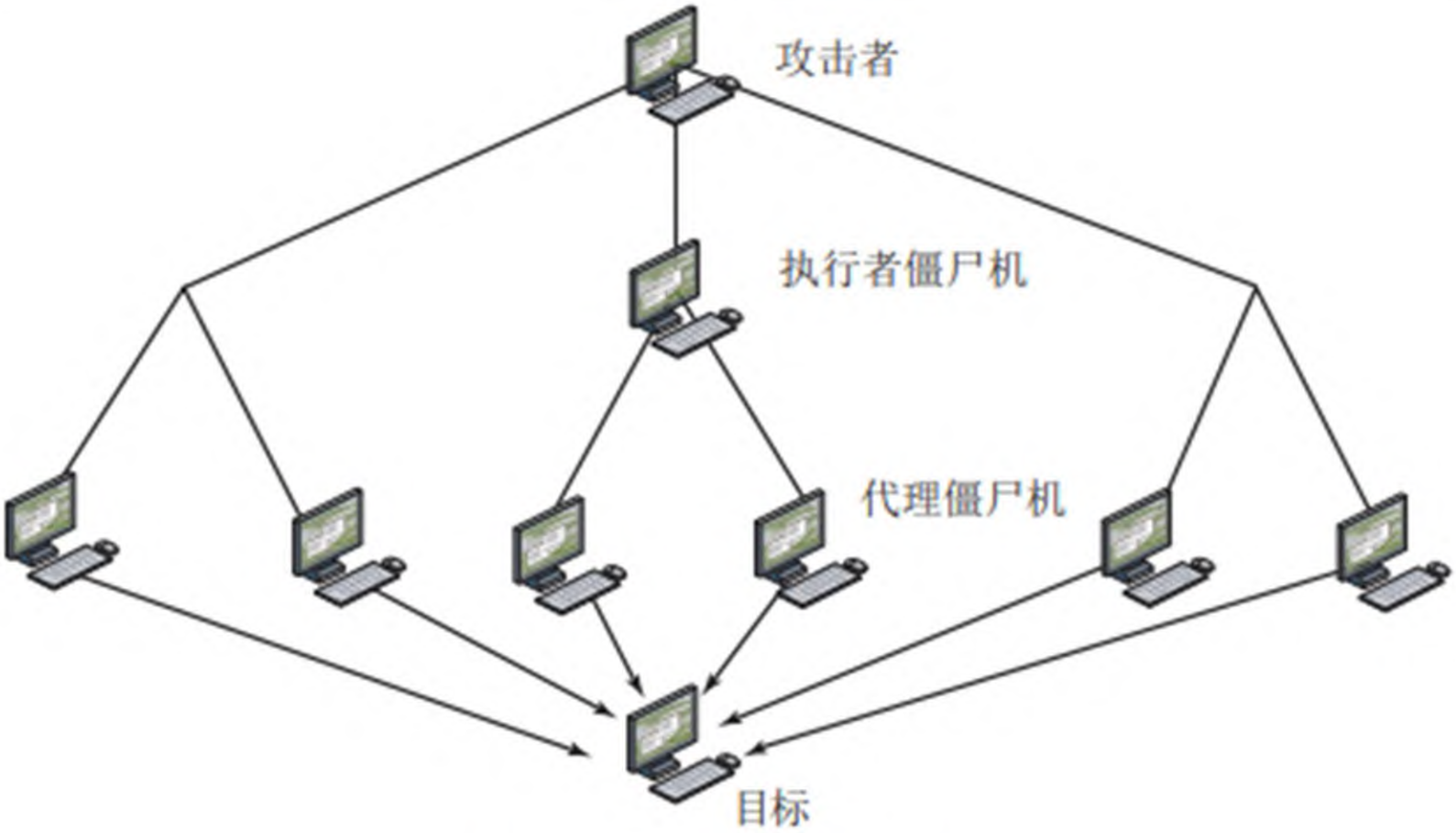


图 7-4　DDoS 攻击体系结构

7.4.1 SIP洪泛

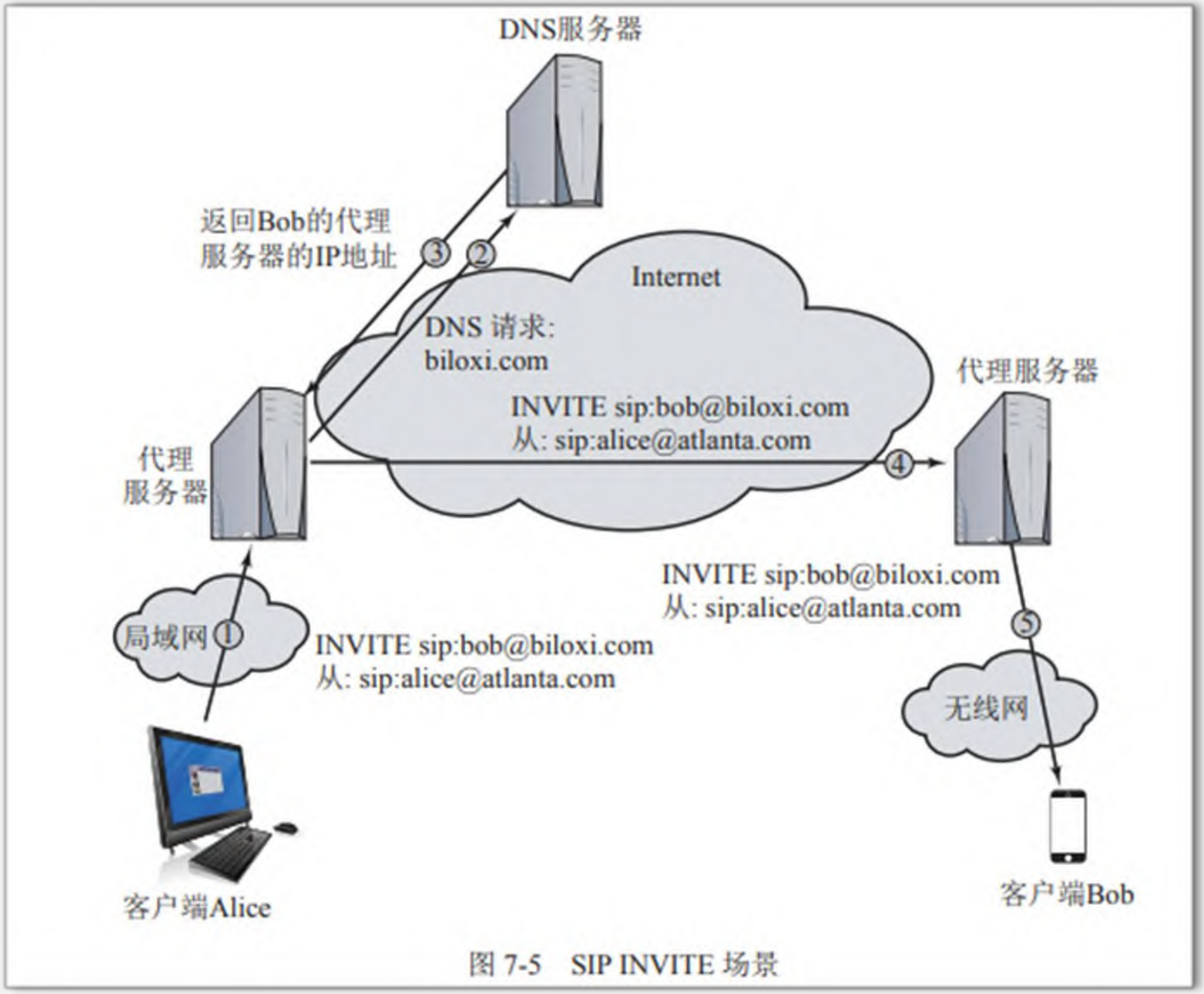


图 7-5　SIP INVITE 场景

7.4.2 基于HTTP的攻击

HTTP洪泛攻击

- HTTP洪泛攻击指的是利用HTTP请求攻击Web服务器。
- 这是一种DDoS攻击，HTTP请求来自许多不同的bots。
- 这些请求可以被预设为消耗相当大的资源的形式 。
- 此类攻击的一个变种被称为递归HTTP洪泛：bots从给定的HTTP链接出发，通过递归方式遍历给定Web服务器的所有链接。这种攻击也被称为爬虫。

SLOWLORIS

- 有一种被称为Slowloris[SOUR12]的HTTP攻击形式，它十分有趣却又非正常[DAMO12]。
- Slowloris利用多线程支持多个到同一服务器应用程序的请求技术进行攻击。
- 它通过向Web服务器不停地发送不完整的HTTP请求，试图独占所有可用的请求处理线程。
- 由于每个请求都需要消耗一个线程，所以Slowloris攻击最终能耗尽所有Web服务器的连接能力，从而有效地拒绝合法用户的访问请求。
- Slowloris与典型拒绝服务攻击不同之处在于，Slowloris利用合法的HTTP流量。
- 现有依赖特征检测的入侵检测和入侵防护手段无法识别出Slowloris。

7.5 反射攻击与放大攻击

- DDoS攻击中，中间媒介是运行攻击者程序的受控系统。与DDoS攻击不同，反射攻击和放大攻击通常利用的是网络服务系统的正常功能。
- 攻击者发送带有虚假源地址的数据包给某些网络服务系统上的服务。网络服务器为了响应这些数据包，会发送一个响应包给攻击包所指向的源地址，而这个地址正是攻击者想要攻击的目标系统。
- 如果攻击者发送一定数量的拥有同样源地址的请求包给一定数量的提供同样服务的服务器，那么这些服务所产生的响应数据包将会几乎全部占据目标系统的网络链路。这些服务器系统实际上成为了DDoS攻击的中间媒介（intermediary），而且它们对数据包的处理看上去也是正常的。
- 这种攻击有两种基本的变种：简单反射攻击（simple reflection attack）和放大攻击（amplification attack）。

7.5.1 反射攻击

- 反射攻击是上述攻击的一种直接实现。攻击者将其想攻击的目标系统地址作为数据包的源地址，并将这些数据包发送给中间媒介上的已知网络服务。当中间媒介响应时，大量的响应数据包会被发送给源地址所指向的目标系统。
- 攻击者希望，他们所利用的网络服务是一个用较小请求就可以产生较大响应数据包的服务。
- 作为反射攻击的中间系统往往是拥有较高系统性能的网络服务器或者良好网络连接性能的路由器。
- 另一种类型的反射攻击利用TCP SYN数据包和建立TCP连接的三次握手进行攻击。攻击者发送一些带有虚假源地址的SYN数据包给选定的中间媒介。作为回应，中间媒介会回应一个SYN-ACK数据包给这个数据包中的源地址所指向的主机，这是真正的目标系统。攻击者利用一定数量的中间媒介来形成大量的SYN-ACK数据包。
- 任何常用的TCP服务都可以被用来进行这类反射攻击。

7.5.1 反射攻击

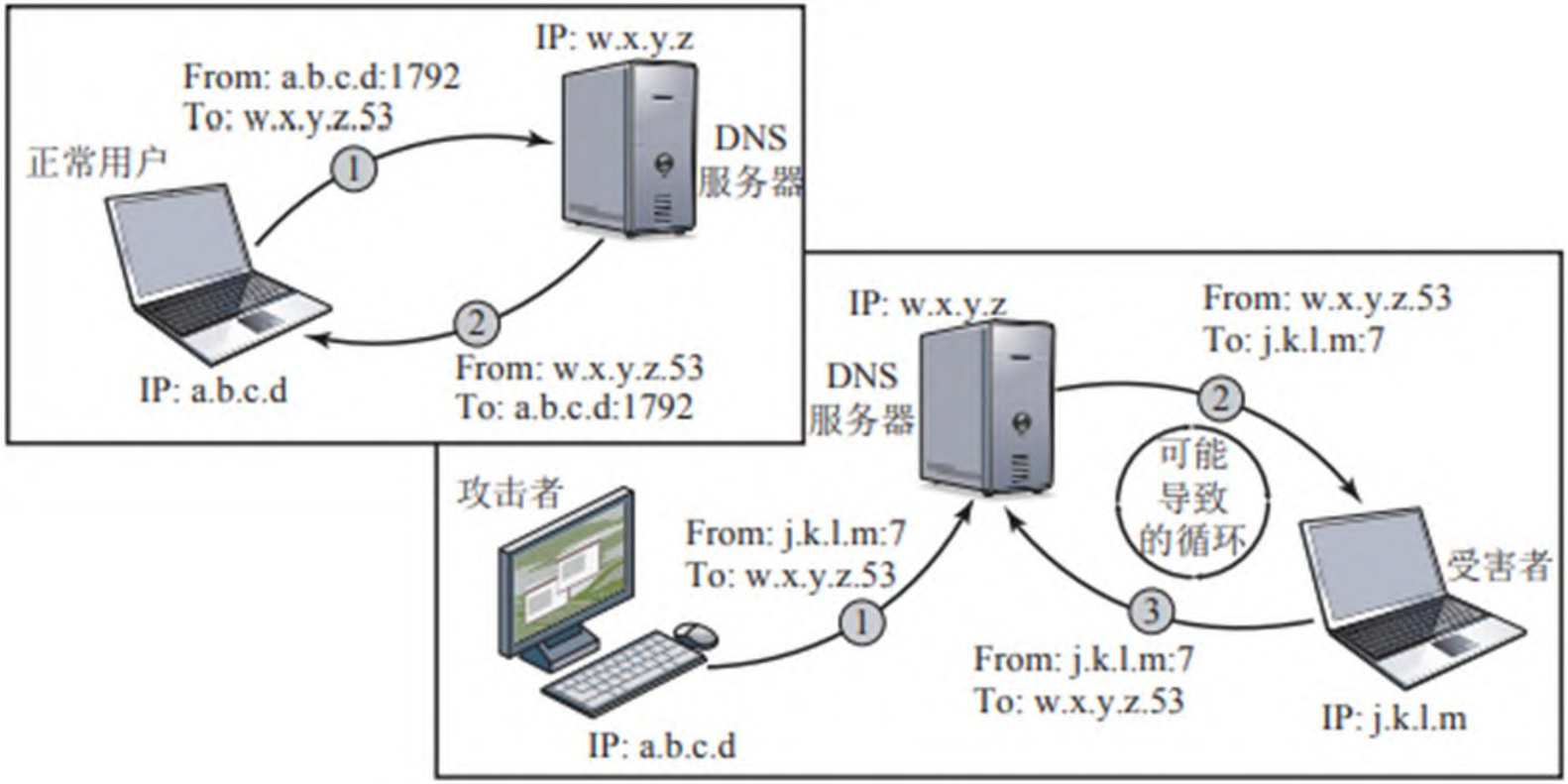


图 7-6 DNS 反射攻击

7.5.2 放大攻击

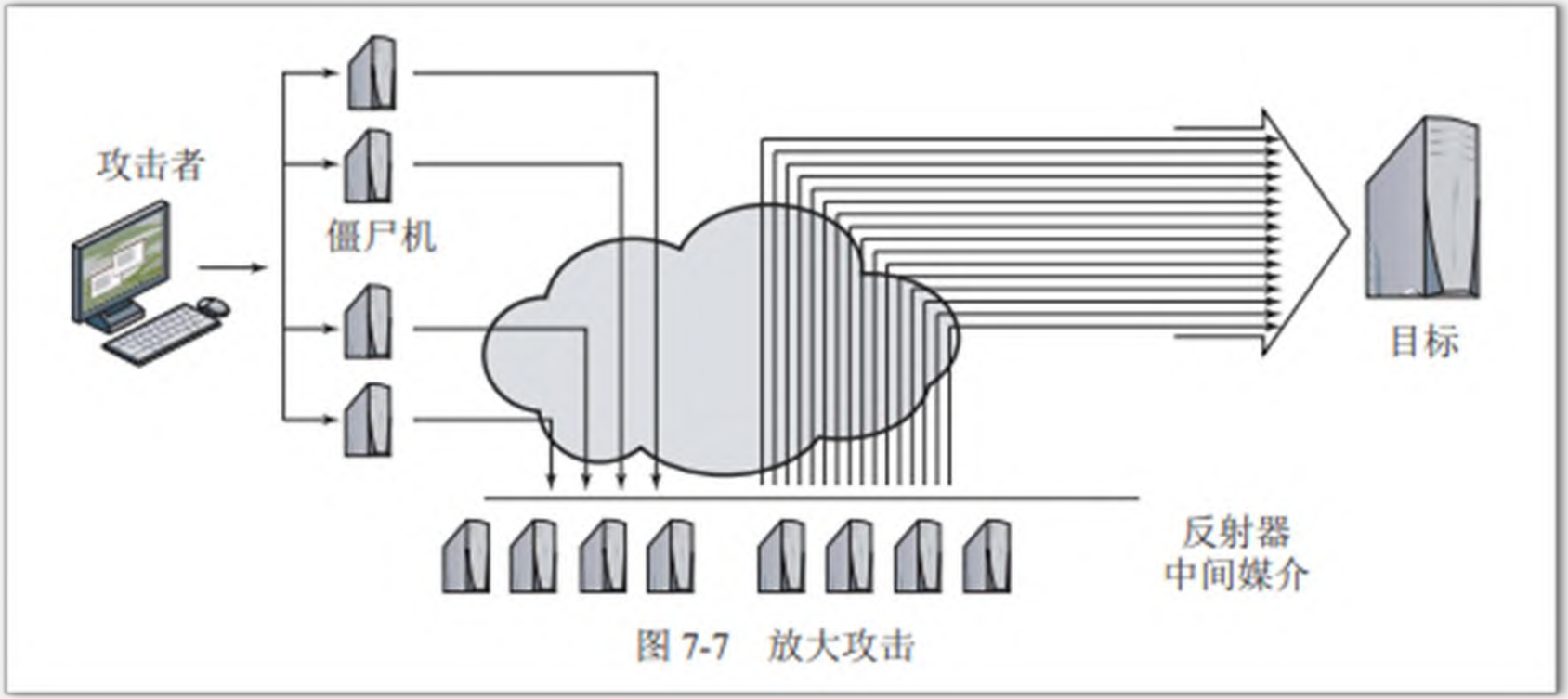


图 7-7　放大攻击

7.5.3 DNS放大攻击

- 反射或放大攻击的另一个变种将DNS服务器作为中间媒介系统，使用了直接指向合法DNS服务器的数据包进行攻击。
- 攻击者利用DNS协议将较小的请求数据包转化为较大的响应数据包而达到攻击效果。
- 这种类型的放大攻击与传统的利用多个主机产生大量的响应数据包的放大攻击有着明显的不同。利用标准的DNS协议，一个60字节的UDP请求数据包可以很容易地生成一个512字节（传统网络上一个数据包所允许的最大字节数）的UDP响应包。而仅仅需要一个有着足够大数量的DNS记录的域名服务器就可以完成其攻击过程。
- 在DNS放大攻击中，攻击者常常选择那些网络连接性能良好的DNS服务器。
- 对付所有基于反射机制的攻击的基本方法是防止使用虚假地址。DNS服务器的正确配置，尤其是限定仅对内部客户系统提供递归响应，如RFC5358中描述的那样，可以很好地限制这类攻击的一些变种。

补充：典型拒绝服务攻击技术

- 6.2.1 Ping of Death
- 6.2.2 泪滴（Teardrop）
- 6.2.3 IP欺骗DoS攻击
- 6.2.4 UDP洪水
- 6.2.5 SYN洪水
- 6.2.6 Land攻击
- 6.2.7 Smurf攻击
- 6.2.8 Fraggle攻击
- 6.2.9 电子邮件炸弹
- 6.2.10 畸形消息攻击
- 6.2.11 Slashdot effect

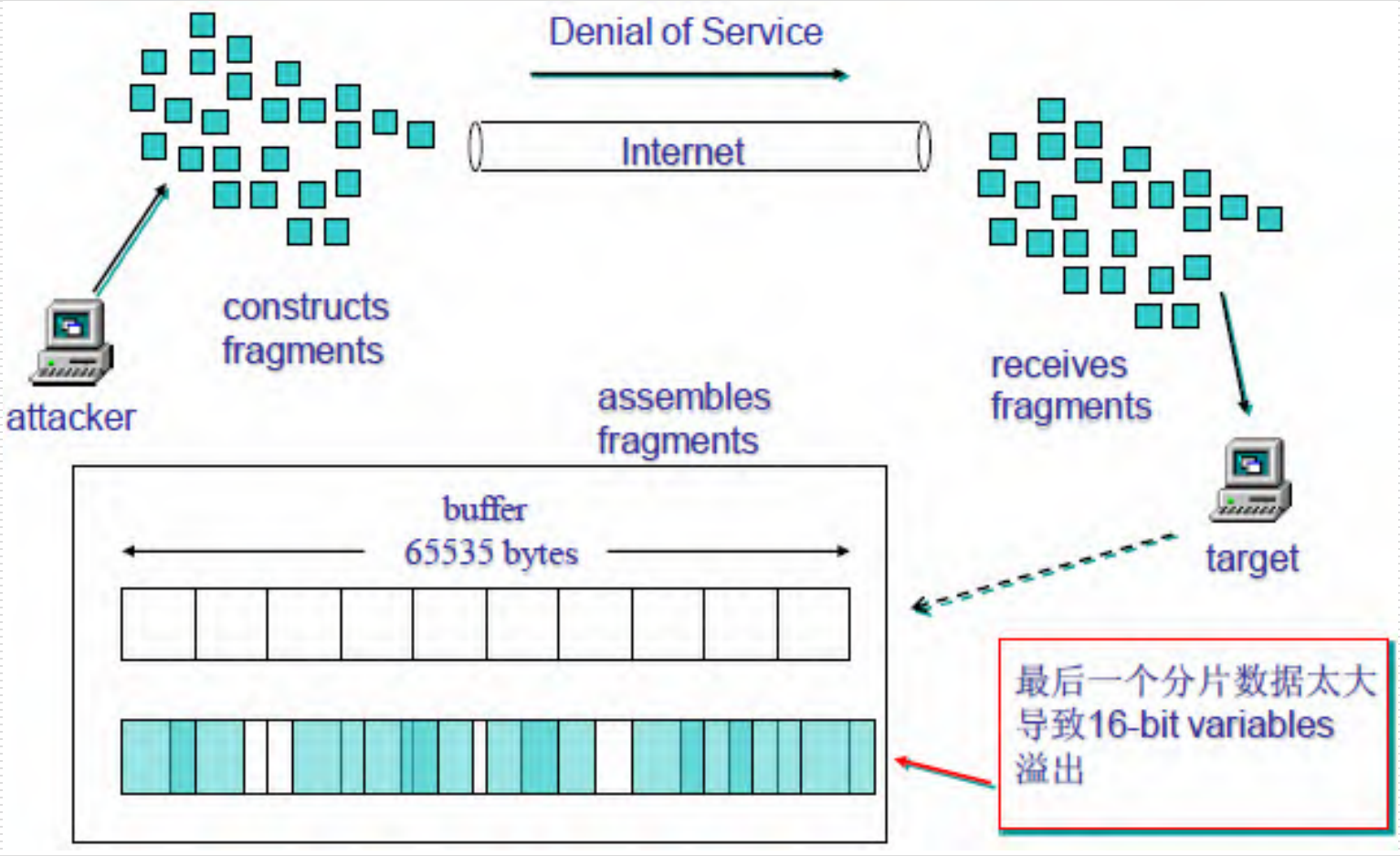
补充：Ping of Death

- Ping是一个非常著名的程序，这个程序的目的是为了测试另一台主机是否可达。现在所有的操作系统上几乎都有这个程序，它已经成为系统的一部分。
- Ping程序的目的是为了查看网络上的主机是否处于活动状态。
- 通过发送一份ICMP回显请求报文给目的主机，并等待返回ICMP回显应答，根据回显应答的内容判断目的主机的状况。

补充： Ping of Death

- Ping之所以会造成伤害是源于早期操作系统在处理ICMP协议数据包存在漏洞。
- ICMP协议的报文长度是固定的，大小为64KB，早期很多操作系统在接收ICMP数据报文的时候，只开辟64KB的缓存区用于存放接收到的数据包。
- 一旦发送过来的ICMP数据包的实际尺寸超过64KB(65536B)，操作系统将收到的数据报文向缓存区填写时，报文长度大于64KB，就会产生一个缓存溢出，结果将导致TCP/IP协议堆栈的崩溃，造成主机的重启动或是死机。

补充： Ping of Death



补充： Ping of Death

- Ping程序有一个“-l”参数可指定发送数据包的尺寸，因此，使用Ping这个常用小程序就可以简单地实现这种攻击。例如通过这样一个命令：

  Ping -l 65540 192.168.1.140

- 如果对方主机存在这样一个漏洞，就会形成一次拒绝服务攻击。这种攻击被称为“死亡之Ping”。

补充： Ping of Death

- 现在的操作系统都已对这一漏洞进行了修补。对可发送的数据包大小进行了限制。
- 在**Windows xp sp2**操作系统中输入这样的命令：

  Ping -l 65535 192.168.1.140

  系统返回这样的信息：

  Bad value for option -l, valid range is from 0 to 65500.

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\think>ping -l 65540
Bad value for option -l, valid range is from 0 to 65500.
```

补充： Ping of Death

- **Ping Of Death攻击的攻击特征、检测方法和反攻击方法总结如下：**
  - 攻击特征：该攻击数据包大于65535个字节。由于部分操作系统接收到长度大于65535字节的数据包时，就会造成内存溢出、系统崩溃、重启、内核失败等后果，从而达到攻击的目的。
  - 检测方法：判断数据包的大小是否大于65535个字节。
  - 反攻击方法：使用新的补丁程序，当收到大于65535个字节的数据包时，丢弃该数据包，并进行系统审计。

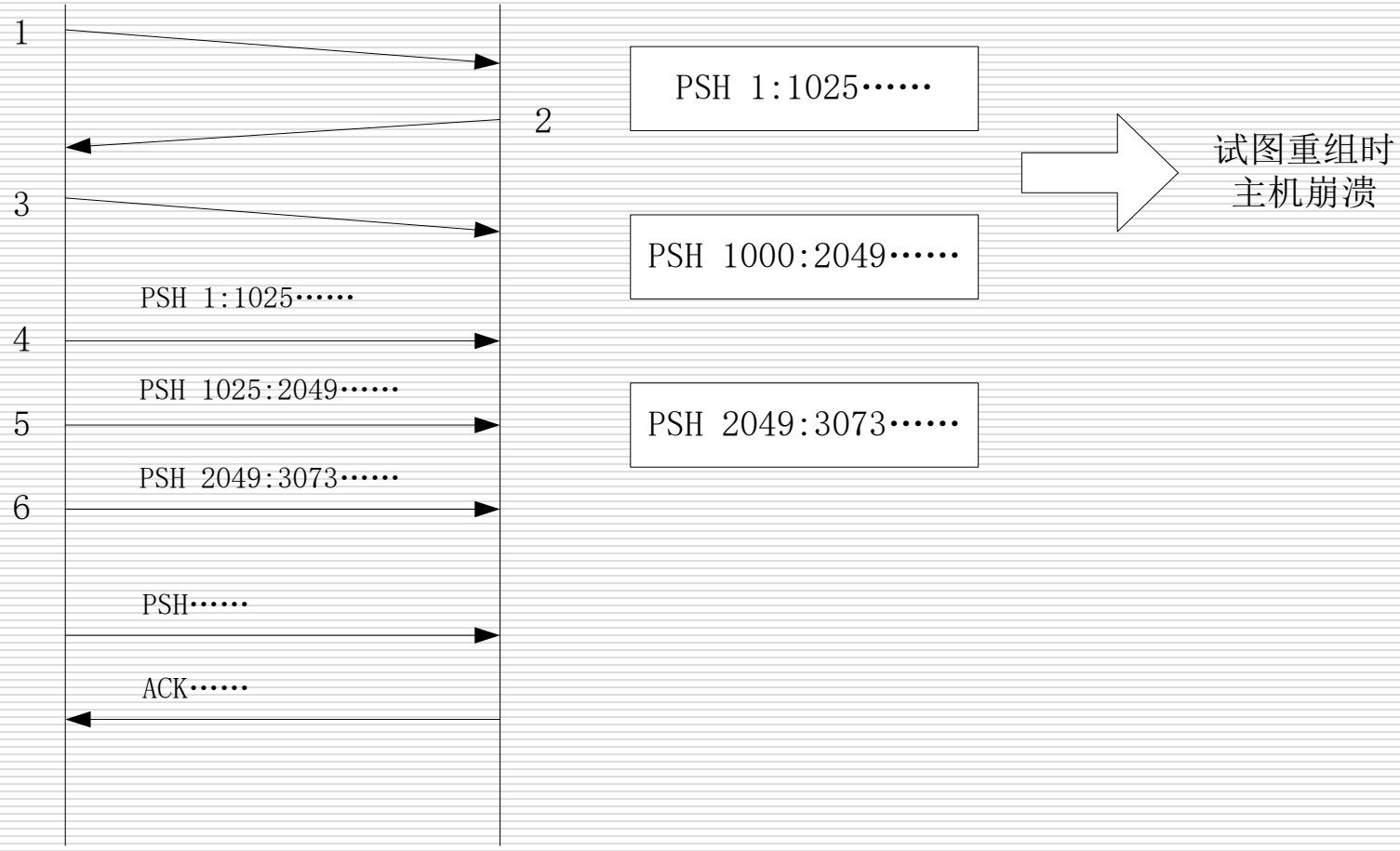
补充：泪滴（Teardrop）

- “泪滴”也被称为分片攻击，它是一种典型的利用**TCP/IP**协议的问题进行拒绝服务攻击的方式，由于第一个实现这种攻击的程序名称为**Teardrop**，所以这种攻击也被称为“泪滴”。

补充： 泪滴（Teardrop）

- 两台计算机在进行通信时，如果传输的数据量较大，无法在一个数据报文中传输完成，就会将数据拆分成多个分片，传送到目的计算机后再到堆栈中进行重组，这一过程称为“分片”。
- 为了能在到达目标主机后进行数据重组，IP包的TCP首部中包含有信息（分片识别号、偏移量、数据长度、标志位）说明该分段是原数据的哪一段，这样，目标主机在收到数据后，就能根据首部中的信息将各分片重新组合还原为数据。

补充：例子


1
2
3
PSH 1:1025……
4
PSH 1025:2049……
5
PSH 2049:3073……
6
PSH……
ACK……
PSH 1:1025……
PSH 1000:2049……
PSH 2049:3073……
试图重组时
主机崩溃

补充：例子

- 如上图所示，从客户机向服务器发送一个数据报文无法发送完成的数据，这些数据会被分片发送。
- 报文1、2、3是TCP连接的三次握手过程，接着4、5、6客户机向服务器发送三个报文，在这三个数据报文首部信息中，有每个报文的分片信息。

补充：例子

- 这就是报文重组的信息：
  - PSH 1:1025(1024) ack 1, win 4096
  - PSH 1025:2049(1024) ack 1, win 4096
  - PSH 2049:3073(1024) ack 1, win 4096
- 在这个报文中，可以看到在第**4**、**5**、**6**这三个报文中，第**4**个发送的数据报文中是原数据的第**1**～**1025**字节内容，第**5**个发送的报文包含的是第**1025**～**2048**字节，第**6**个数据报文是第**2049**～**3073**个字节，接着后面是继续发送的分片和服务器的确认。当这些分片数据被发送到目标主机后，目标主机就能够根据报文中的信息将分片重组，还原出数据。

补充：例子

- 如果入侵者伪造数据报文，向服务器发送含有重叠偏移信息的分段包到目标主机，例如如下所列的分片信息：
  - PSH 1:1025(1024) ack1, win4096
  - PSH 1000:2049(1024) ack1, win4096
  - PSH 2049:3073(1024) ack1, win4096
- 这样的信息被目的主机收到后，在堆栈中重组时，由于畸形分片的存在，会导致重组出错，这个错误并不仅仅是影响到重组的数据，由于协议重组算法，会导致内存错误，引起协议栈的崩溃。

补充： 泪滴（teardrop）

- 泪滴攻击的攻击特征、检测方法和反攻击方法总结如下：
  - 攻击特征：Teardrop工作原理是向被攻击者发送多个分片的IP包，某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。
  - 检测方法：对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。
  - 反攻击方法：添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。

补充： IP欺骗DoS攻击

- 这种攻击利用RST位来实现。
- 假设现在有一个合法用户(61.61.61.61)已经同服务器建立了正常的连接，攻击者构造攻击的TCP数据，伪装自己的IP为61.61.61.61，并向服务器发送一个带有RST位的TCP数据段。服务器接收到这样的数据后，认为61.61.61.61发送的连接有错误，就会清空缓冲区中建立好的连接。
- 这时，如果合法用户61.61.61.61再发送合法数据，服务器就已经没有这样的连接了，该用户就必须重新开始建立连接。

补充： IP欺骗DoS攻击

- 攻击时，攻击者会伪造大量的IP地址，向目标发送RST数据，使服务器不对合法用户服务，从而实现了对受害服务器的拒绝服务攻击。

补充：UDP洪水

- UDP洪水（UDP flood）主要是利用主机能自动进行回复的服务（例如使用UDP协议的chargen服务和echo服务）来进行攻击。
- 很多提供WWW和Mail等服务设备通常是使用Unix的服务器，它们默认打开一些被黑客恶意利用的UDP服务。如echo服务会显示接收到的每一个数据包，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。

补充：UDP洪水

- 当我们向**echo**服务的端口发送一个数据时，**echo**服务会将同样的数据返回给发送方，而**chargen**服务则会随机返回字符。
- 当两个或两个以上系统存在这样的服务时，攻击者利用其中一台主机向另一台主机的**echo**或者**chargen**服务端口发送数据，**echo**和**chargen**服务会自动进行回复，这样开启**echo**和**chargen**服务的主机就会相互回复数据。
- 由于这种做法使一方的输出成为另一方的输入，两台主机间会形成大量的**UDP**数据包。当多个系统之间互相产生**UDP**数据包时，最终将导致整个网络瘫痪。

补充： SYN洪水

- SYN Flood是当前最流行的拒绝服务攻击方式之一，这是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，使被攻击方资源耗尽(CPU满负荷或内存不足)的攻击方式。
- SYN Flood是利用TCP连接的三次握手过程的特性实现的。

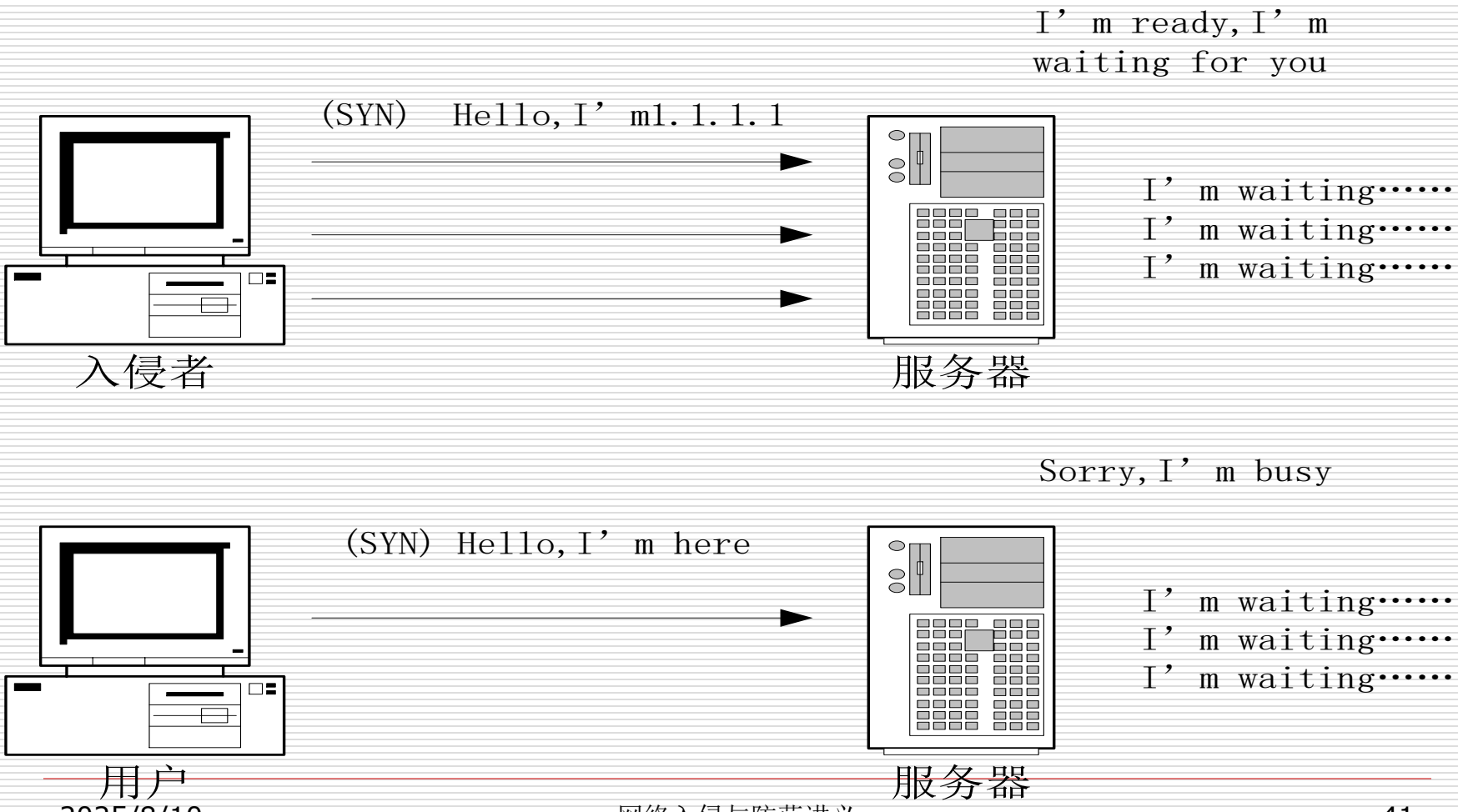
补充：SYN洪水

- 在TCP连接的三次握手过程中，假设一个客户端向服务器发送了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，这种情况下服务器端一般会重试，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。
- 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(伪造IP地址)，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。

补充： SYN洪水

- 即使是简单的保存并遍历半连接列表也会消耗非常多的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——既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，此时从正常客户的角度看来，服务器失去响应，这种情况就称作：服务器端受到了SYN Flood攻击(SYN洪水攻击)。

补充：SYN“洪水”攻击示意图



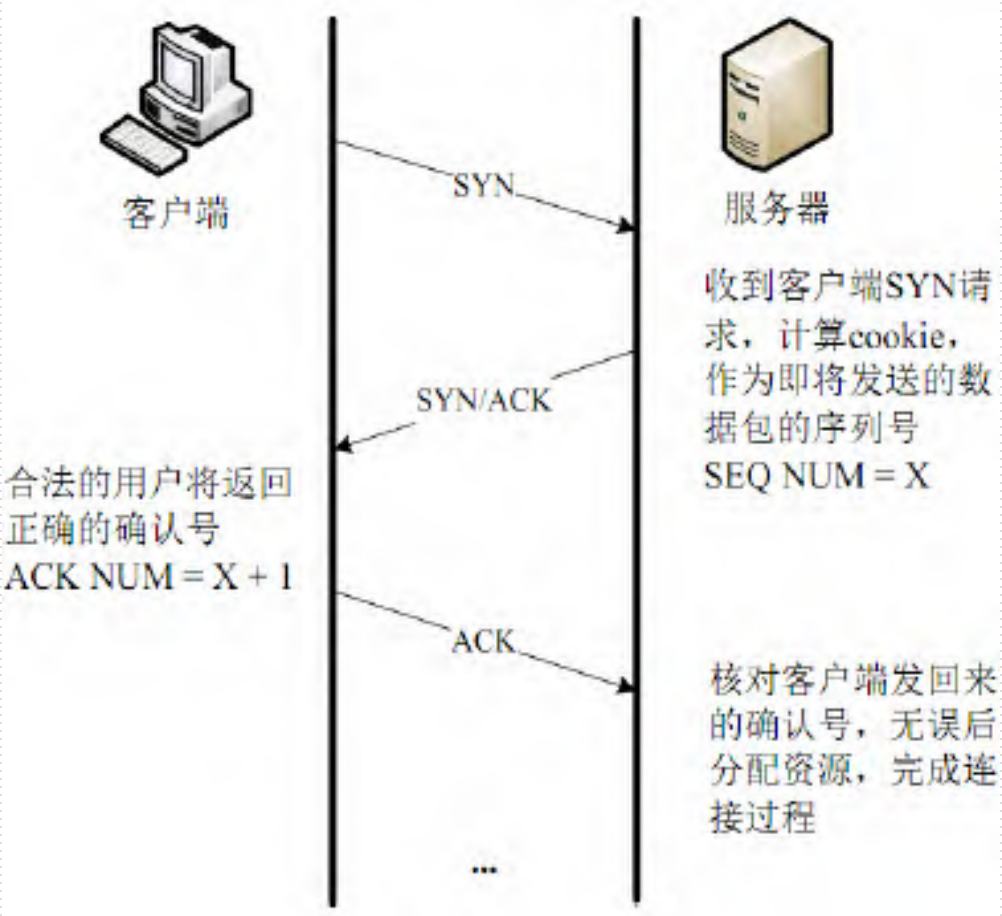
补充：SYN“洪水”的防御

- **SYN洪水攻击比较难以防御，以下是几种解决方法：**
  - 缩短SYN Timeout时间
  - 设置SYN Cookie
  - 负反馈策略
  - 退让策略
  - 分布式DNS负载均衡
  - 防火墙

补充：缩短SYN Timeout时间

- 由于SYN Flood攻击的效果取决于服务器上保持的SYN半连接数，这个值=SYN攻击的频度 x SYN Timeout，所以通过缩短从接收到SYN报文到确定这个报文无效并丢弃该连接的时间，可以成倍的降低服务器的负荷。

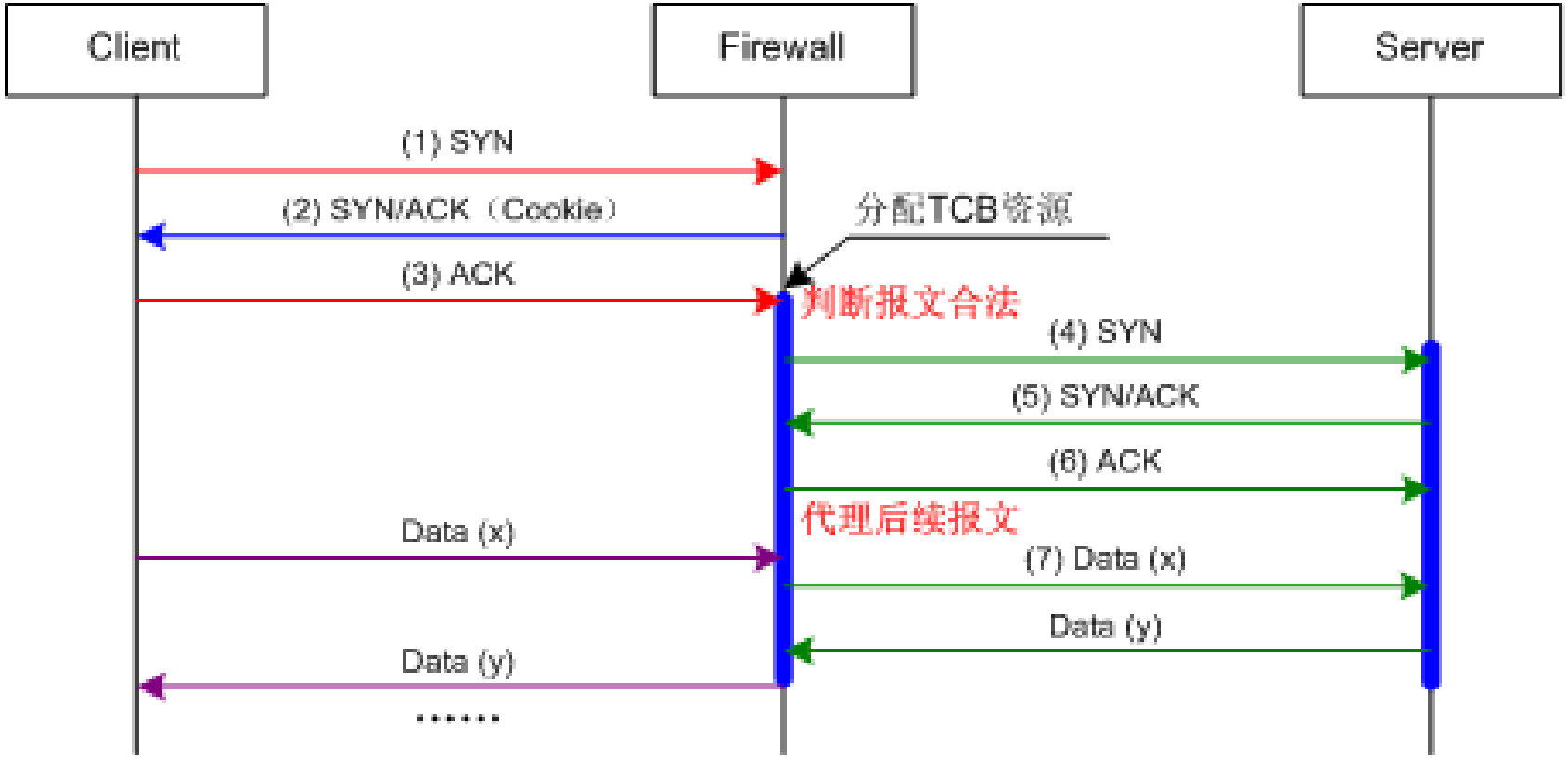
补充：设置SYN Cookie



补充：设置SYN Cookie

- 当服务器S接收到一个SYN包时，返回SYN/ACK包，其ACK序列号是经过加密的，由源地址，源端口，目标地址，目标端口和一个加密种子计算得出。然后服务器释放所有的状态。
- 如果一个ACK包从客户端C返回，服务器将重新计算来判断它是不是上个SYN/ACK的返回包。如果是，S就可以直接进入TCP连接状态并打开连接，否则直接丢弃。这样，S就可以避免守侯半开放连接了。

补充：设置SYN Cookie



防火墙使用SYN Cookie防范SYN Flood

补充：设置SYN Cookie

- 防火墙的**SYN Cookie**技术利用**SYN/ACK**报文携带的认证信息，对握手协商的**ACK**报文进行了认证，从而避免了防火墙过早分配**TCB**资源，可以有效防范**SYN Flood**攻击。
- 在防范**SYN Flood**攻击的过程中，防火墙作为虚拟的服务器与客户端交互，同时也作为虚拟的客户端与服务器交互，在为服务器过滤掉恶意连接报文的同时保证了常规业务的正常运行。

补充：负反馈策略

- 正常情况下，**OS**对**TCP**连接的一些重要参数有一个常规的设置：**SYN Timeout**时间、**SYN-ACK**的重试次数、**SYN**报文从路由器到系统再到**Winsock**的延时等等。
- 这个常规设置针对系统优化，可以给用户提供方便快捷的服务；一旦服务器受到攻击，**SYN Half link** 的数量超过系统中**TCP**活动**Half link**最大连接数的设置，系统将会认为自己受到了**SYN Flood**攻击，并将根据攻击的判断情况作出反应：减短**SYN Timeout**时间、减少**SYN-ACK**的重试次数、自动对缓冲区中的报文进行延时等等措施，力图将攻击危害减到最低。

补充：退让策略

- 退让策略是基于**SYN Flood**攻击代码的一个缺陷：**SYN Flood**一旦攻击开始，将不会再进行域名解析。
- 切入点：假设一台服务器在受到**SYN Flood**攻击后迅速更换自己的**IP**地址，那么攻击者仍在不断攻击的只是一个空的**IP**地址，并没有任何主机，而防御方只要将**DNS**解析更改到新的**IP**地址就能在很短的时间内恢复用户通过域名进行的正常访问。
- 为了迷惑攻击者，我们甚至可以放置一台“牺牲”服务器让攻击者满足于攻击的“效果”。

补充：分布式DNS负载均衡

- 在众多的负载均衡架构中，基于DNS解析的负载均衡本身就拥有对SYN Flood的免疫力。
- 基于DNS解析的负载均衡能将用户的请求分配到不同IP的服务器主机上，攻击者攻击的永远只是其中一台服务器，一来这样增加了攻击者的成本，二来过多的DNS请求可以帮助我们追查攻击者的真正踪迹。

补充： Land攻击

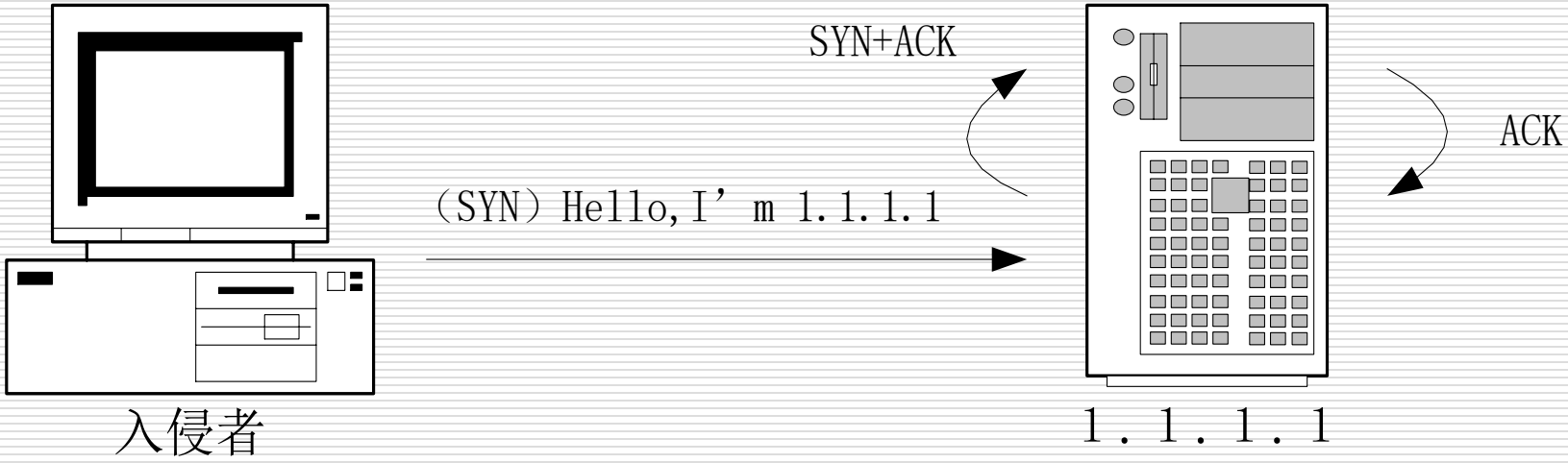
- Land是因特网上最常见的拒绝服务攻击类型，它是由著名黑客组织rootshell发现的。
- 原理很简单，向目标机发送大量的源地址和目标地址相同的包，造成目标机解析Land包时占用大量的系统资源，从而使网络功能完全瘫痪。

补充：Land攻击

- Land攻击也是利用TCP的三次握手过程的缺陷进行攻击。
- Land攻击是向目标主机发送一个特殊的SYN包，包中的源地址和目标地址都是目标主机的地址。目标主机收到这样的连接请求时会向自己发送SYN/ACK数据包，结果导致目标主机向自己发回ACK数据包并创建一个连接。
- 大量的这样的数据包将使目标主机建立很多无效的连接，系统资源被大量的占用。

补充： Land攻击

- Land攻击示意图：



补充： Land攻击

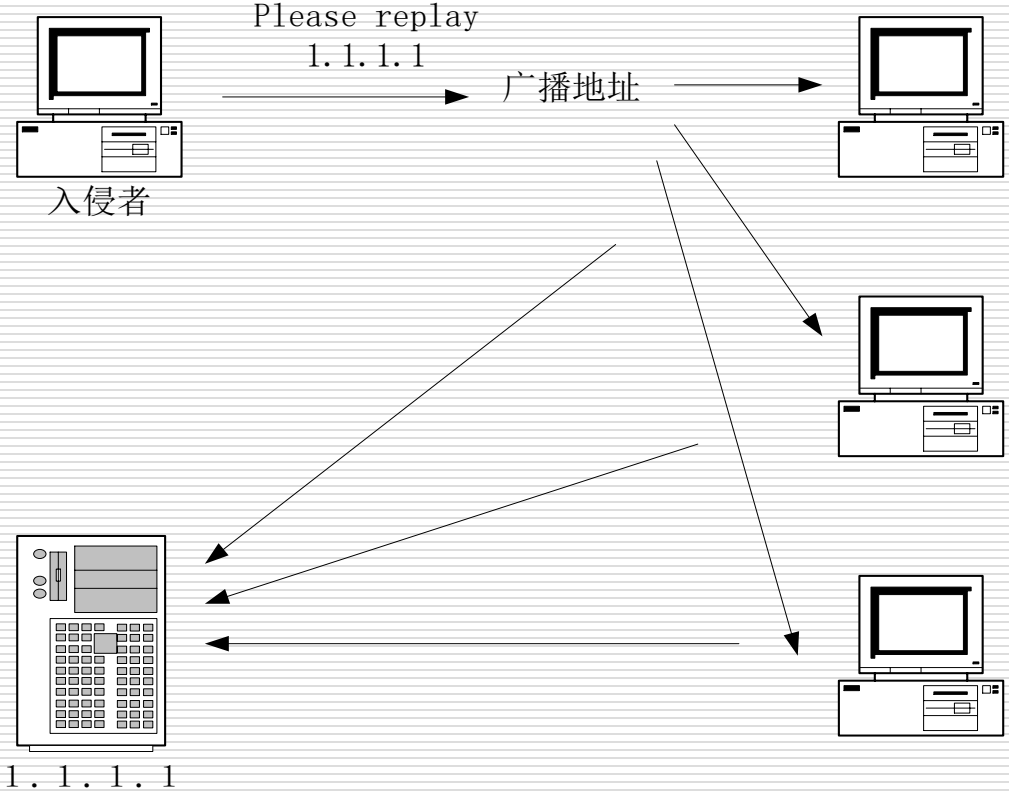
- **Land攻击可简要概括如下：**
  - 攻击特征：用于Land攻击的数据包中的源地址和目标地址是相同的。操作系统接收到这类数据包时，不知道该如何处理堆栈中的这种情况，或者循环发送和接收该数据包，消耗大量的系统资源，从而有可能造成系统崩溃或死机等现象。
  - 检测方法：判断网络数据包的源/目标地址是否相同。
  - 反攻击方法：适当配置防火墙设备或过滤路由器的过滤规则可以防止这种攻击行为，并对这种攻击进行审计。

补充：Smurf攻击

- Smurf攻击是利用IP欺骗和ICMP回应包引起目标主机网络阻塞，实现DoS攻击。
- Smurf攻击原理：在构造数据包时将源地址设置为被攻击主机的地址，而将目的地址设置为广播地址，于是，大量的ICMP echo回应包被发送给被攻击主机，使其因网络阻塞而无法提供服务。
- 比Ping of Death洪水的流量高出1或2个数量级。

补充： Smurf攻击

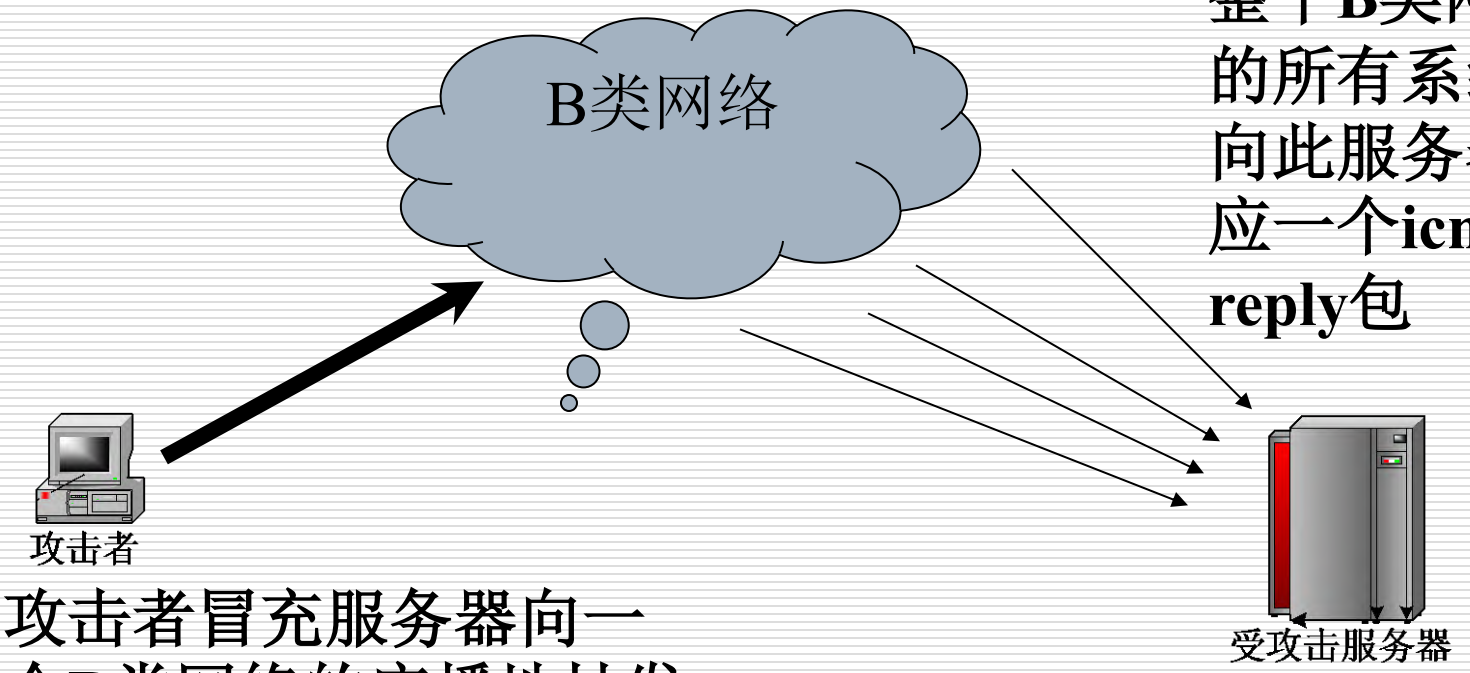
- Smurf攻击示意图：



补充： Smurf攻击

- 如上例所示，入侵者的主机发送了一个数据包，而目标主机就收到了三个回复数据包。
- 如果目标网络是一个很大的以太网，有200台主机，那么在这种情况下，入侵者每发送一个ICMP数据包，目标主机就会收到200个数据包，因此目标主机很快就会被大量的回复信息吞没，无法处理其他的任何网络传输。
- 这种攻击不仅影响目标主机，还能影响目标主机的整个网络系统。

补充： Smurf攻击例子



整个B类网络的所有系统都向此服务器回应一个icmp reply包

攻击者冒充服务器向一个B类网络的广播地址发送ICMP echo包

补充：Fraggle攻击

- Fraggle攻击原理与Smurf一样，也是采用向广播地址发送数据包，利用广播地址的特性将攻击放大以使目标主机拒绝服务。
- 不同的是，**Fraggle使用的是UDP应答消息而非ICMP**。

补充： 电子邮件炸弹

- 电子邮件炸弹是最古老的匿名攻击之一，由于这种攻击方式简单易用，互联网上也很容易找到这些发送匿名邮件的工具，并且入侵者只需要知道对方的电子邮件地址就可以进行攻击了。
- 传统的电子邮件炸弹只是简单的往你的邮箱里发送大量的邮件，入侵者的目的是要用垃圾邮件填满你的邮箱后，正常的邮件就会因空间不够而被服务器拒收。

补充： 电子邮件炸弹

- 如果用户的邮箱使用空间不受限制，那么电子邮件炸弹攻击就有可能影响到服务器的正常工作了。
- 最有可能的情况是入侵者不断发送大量的电子邮件，由于用户的邮箱空间不受限制，服务器会接收全部的邮件并保存在硬盘上。大量到来的邮件将不断吞噬服务器上的硬盘空间，最终将耗尽服务器上的所有硬盘空间，使得服务器无法再对外服务。
- 还有一种可能是通过设置一台机器不断地大量向同一地址发送电子邮件，入侵者能够耗尽接收者网络的带宽。

补充： 电子邮件炸弹

- 电子邮件是通过**SMTP**协议进行发送的，最初的**SMTP**协议服务是不需要进行身份认证的，在发送电子邮件的过程中不对用户进行身份认证。
- **SMTP**不会进行认证，邮件的发送人可以伪造任何邮件地址，甚至可以不写发件人的信息。这就是能发送匿名邮件的原因。
- 针对**SMTP**的问题，新的**SMTP**协议规范新增了**2**个命令，对发送邮件的发件人进行身份认证，在一定程度上降低了匿名电子邮件的风险。

补充： 畸形消息攻击

- 畸形消息攻击是一种有针对性的攻击方式，它利用目标主机或者特定服务存在的安全漏洞进行攻击。
- 目前无论是**Windows**、**Unix**、**Linux**等各类操作系统上的许多服务都存在安全漏洞，由于这些服务在处理信息之前没有进行适当正确的错误校验，所以一旦收到畸形的信息就有可能会崩溃。

补充： 畸形消息攻击

- 例如，在**IIS 5**没有安装相应的修补包以及没有相应的安全措施时，向**IIS 5**服务器递交如下的**URL**会导致**IIS 5**停止服务：
  http://testIP/...[25kb of '.']...ida
  而向**IIS 5**递交如下的**HTTP**请求会导致**IIS**系统的崩溃，需要重启动才能恢复：
  "GET /.....[3k]..... .htr HTTP/1.0"
- 这两者都是向服务器提交正常情况下不会出现的请求，导致服务器处理错误而崩溃，是典型的畸形消息攻击。

补充：Slashdot effect

- **Slashdot effect**来自**Slashdot.org**这个网站，这曾是十分知名而且浏览人数十分庞大的**IT**、电子、娱乐网站，也是**blog**网站的开宗始祖之一。由于**Slashdot.org**的知名度和浏览人数的影响，在**Slashdot.org**上的文章中放入的网站链接，有可能一瞬间被点入上千次，甚至上万次，造成这个被链接的网站承受不住突然增加的连接请求，出现响应变慢、崩溃、拒绝服务。这种现象就称为**Slashdot effect**，这种瞬间产生的大量进入某网站的动作，也称作**Slashdotting**。

补充：Slashdot effect

- 这种攻击手法使web服务器或其他类型的服务器由于大量的网络传输而过载，一般这些网络流量是针对某一个页面或一个链接而产生的。
- 当然这种现象也会在访问量较大的网站上正常的发生，但一定要把这些正常现象和攻击区分开来。
- 如果您的服务器突然变得拥挤不堪，甚至无法响应再多的请求时，您应当仔细检查一下这个资源匮乏的现象，确认在10000次点击里全都是合法用户进行的，还是由5000个合法用户和一个点击了5000次的攻击者进行的。

7.6 拒绝服务攻击防范

- 需要明确的是，我们不可能完全预防DoS攻击。
- 如果攻击者可以构造足够大的合法流量到达你的系统，那么这个流量就很有可能会淹没你的系统网络连接，从而限制其他想连接到你的系统的合法网络请求。
- 典型地，在著名的Slashdot新闻聚合站点发布一条新闻经常会导致其所引用的服务器系统超负荷。
- 一般地，抵御DDoS攻击有下面四条防线[PENG07,CHAN02]：
  ① 攻击预防和先发制人机制（攻击前）
  ② 攻击检测和过滤（攻击时）
  ③ 攻击源回溯和识别（攻击时和攻击后）
  ④ 攻击反应（攻击后）

7.6 拒绝服务攻击防范

- 很多的DoS攻击的关键性内容是使用虚假的源地址。这既可以掩盖直接或分布式DoS攻击的攻击者，也可用来将反射或放大的网络通信流量涌向目标系统。
- 因此，根本的、长期有效的抵御DoS攻击的方法是限制主机系统发送带有虚假源地址数据包的能力。
  1. 过滤器应该尽可能地接近数据包源头，放在可以获得输入数据包的有效地址范围的路由器或网关附近。
  2. 也可以用过滤器来确认源地址所指向的返回路径是否是当前数据包发送过来所使用的路径。
  3. 过滤器应该被应用于网络流量离开其ISP网络之前，或者甚至要在其网络的入口点。
  4. 可以使用改进版本的TCP连接处理程序来专门抵御SYN欺骗攻击。

7.6 拒绝服务攻击防范

- 抵御广播放大攻击的最好措施是屏蔽IP定向广播的使用。这可以由ISP或者那些被利用作为中间媒介的组织来实现。
  1. 限制或阻塞流向可疑服务、源端口和目的端口组合的网络流量
  2. 抵御以应用程序资源为攻击目标的DoS攻击一般要求修改作为目标的应用程序
  3. 应用程序也可以限制某种类型的交互的速率以持续提供某种类型的服务
  4. 除了这些直接抵御DoS攻击的措施外，完整的良好系统安全实践也是必须的。这样做的目的是不让自己的主机被攻击者控制成为僵尸机。
  5. 一个基于网络服务的组织应该配置镜像，在多个站点上复制出多个同样的、具有多条网络连接的服务器。

7.7 对拒绝服务攻击的响应

- 为了成功地响应DoS攻击，一个良好的偶然事件响应计划是必须的。
  - 如何联系你的Internet服务提供商的技术人员。
  - DoS攻击，尤其是洪泛攻击，所产生的流量数据包只能在你的服务器的上行流量中被过滤掉。
  - 这个响应计划也要包括对于攻击的具体响应措施。
  - 组织人员和ISP方面的责任划分的依据是组织的可用资源和技术能力。
- 对于组织内部：
  - 应该已经实施了或安装了标准的反欺骗、定向广播和速率限制过滤器，
  - 理想状态下，还应该装有某种形式的网络自动监视和入侵检测系统，从而在遇到异常数据时，可以很快地检测到。

7.7 对拒绝服务攻击的响应

- 当检测到一次DoS攻击，我们首先要做的事情是判定出这次攻击的类型，并选择一个最佳的方法来抵御这次攻击。通常这个过程应该包括：
  ① 数据包的捕获
  ② 数据包的分析
  ③ 寻找常见的攻击数据包类型
- 组织可能也希望ISP能够追踪攻击数据包流而确定这些包的源。
- 如果攻击是来自大量的分布式或反射系统的扩展的、协同的、洪泛的攻击，那么要想过滤掉足够的数据包从而保证网络连接的连通性几乎是不可能。
- 除了快速地对这种类型的攻击进行响应外，组织的事故响应策略应该确定用来响应类似的意外情况的进一步措施。