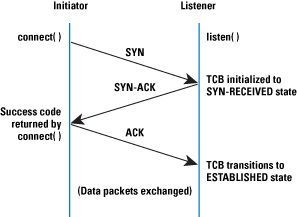
**SYN Flood攻击及防御方法**

1. **为什么Syn Flood会造成危害**

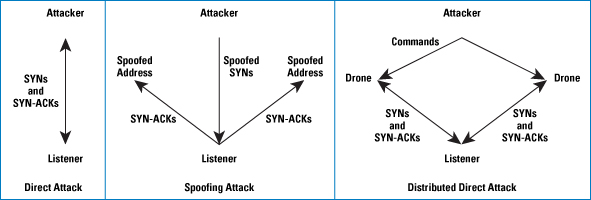
这要从计算机网络的TCP/IP协议栈的实现说起。当开放了一个TCP端口后，该端口就处于Listening状态，不停地监视发到该端口的SYN报文，一旦接收到Client发来的SYN报文，就需要为该请求分配一个TCB（Transmission Control Block），通常一个TCB至少需要280个字节，在某些操作系统中TCB甚至需要1300个字节，并返回一个SYN ACK报文，立即转为SYN-RECEIVED即半开连接状态，而某些操作系统在SOCKT的实现上最多可开启512个半开连接（如Linux2.4.20 内核）。这种过程如下图所示：



从以上过程可以看到，如果恶意的向某个服务器端口发送大量的SYN包，则可以使服务器打开大量的半开连接，分配TCB，从而消耗大量的服务器资源，同时也使得正常的连接请求无法被相应。而攻击发起方的资源消耗相比较可忽略不计。

1. **如何防御Syn Flood攻击**

我们先来看一下Syn Flood有哪些种类，如下图所示：



1．Direct Attack 攻击方使用固定的源地址发起攻击，这种方法对攻击方的消耗最小2．Spoofing Attack 攻击方使用变化的源地址发起攻击，这种方法需要攻击方不停地修改源地址，实际上消耗也不大

3．Distributed Direct Attack 这种攻击主要是使用僵尸网络进行固定源地址的攻击

对于第一种攻击的防范可以使用比较简单的方法，即对SYN包进行监视，如果发现某个IP发起了较多的攻击报文，直接将这个IP列入黑名单即可。当然下述的方法也可以对其进行防范。对于源地址不停变化的攻击使用上述方法则不行，首先从某一个被伪装的IP过来的Syn报文可能不会太多，达不到被拒绝的阈值，其次从这个被伪装的IP（真实的）的请求会被拒绝掉。因此必须使用其他的方法进行处理。

1.无效连接监视释放

这种方法不停监视系统的半开连接和不活动连接，当达到一定阈值时拆除这些连接，从而释放系统资源。这种方法对于所有的连接一视同仁，而且由于SYN Flood造成的半开连接数量很大，正常连接请求也被淹没在其中被这种方式误释放掉，因此这种方法属于入门级的SYN Flood方法。

2.延缓TCB分配方法

从前面SYN Flood原理可以看到，消耗服务器资源主要是因为当SYN数据报文一到达，系统立即分配TCB，从而占用了资源。而SYN Flood由于很难建立起正常连接，因此，当正常连接建立起来后再分配TCB则可以有效地减轻服务器资源的消耗。常见的方法是使用SYN Cache和SYN Cookie技术。

SYN Cache技术：

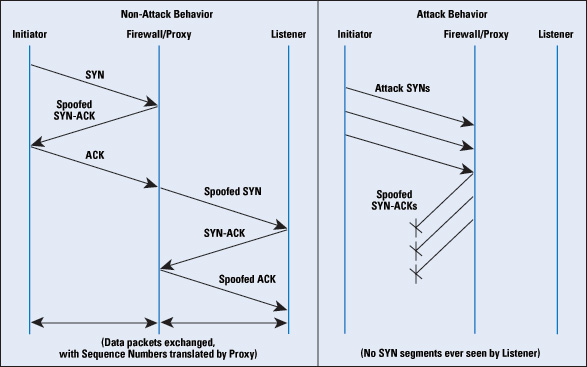
这种技术是在收到SYN数据报文时不急于去分配TCB，而是先回应一个SYN ACK报文，并在一个专用HASH表（Cache）中保存这种半开连接信息，直到收到正确的回应ACK报文再分配TCB。在FreeBSD系统中这种 Cache每个半开连接只需使用160字节，远小于TCB所需的736个字节。在发送的SYN ACK中需要使用一个己方的Sequence Number，这个数字不能被对方猜到，否则对于某些稍微智能一点的SYN Flood攻击软件来说，它们在发送SYN报文后会发送一个ACK报文，如果己方的Sequence Number被对方猜测到，则会被其建立起真正的连接。因此一般采用一些加密算法生成难于预测的Sequence Number。

SYN Cookie技术：

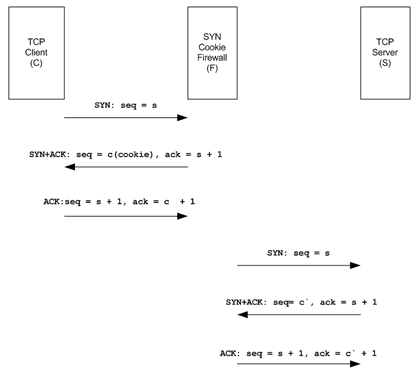
对于SYN攻击，SYN Cache虽然不分配TCB，但是为了判断后续对方发来的ACK报文中的Sequence Number的正确性，还是需要使用一些空间去保存己方生成的Sequence Number等信息，也造成了一些资源的浪费。Syn Cookie技术则完全不使用任何存储资源，这种方法比较巧妙，它使用一种特殊的算法生成Sequence Number，这种算法考虑到了对方的IP、端口、己方IP、端口的固定信息，以及对方无法知道而己方比较固定的一些信息，如MSS、时间等，在收到对方 的ACK报文后，重新计算一遍，看其是否与对方回应报文中的（Sequence Number-1）相同，从而决定是否分配TCB资源。

3．使用SYN Proxy防火墙

SYN Cache技术和SYN Cookie技术总的来说是一种主机保护技术，需要系统的TCP/IP协议栈的支持，而目前并非所有的操作系统支持这些技术。因此很多防火墙中都提供一种 SYN代理的功能，其主要原理是对试图穿越的SYN请求进行验证后才放行，下图描述了这种过程：



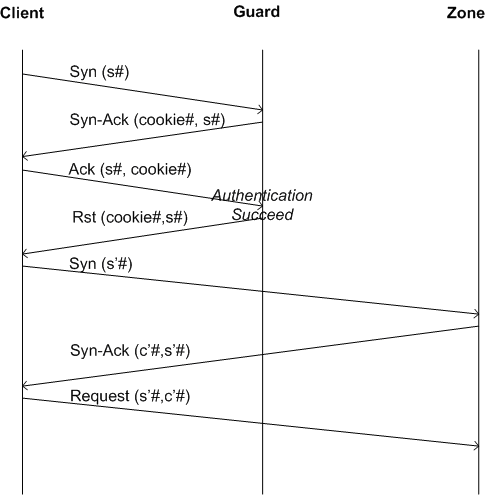
从上图（左图）中可以看出，防火墙在确认了连接的有效性后，才向内部的服务器（Listener）发起SYN请求，在右图中，所有的无效连接均无法到达内 部的服务器。而防火墙采用的验证连接有效性的方法则可以是SYN Cookie或SYN Cache等其他技术。采用这种方式进行防范需要注意的一点就是防火墙需要对整个有效连接的过程发生的数据包进行代理，如下图所示：



因为防火墙代替发出的SYN ACK包中使用的序列号为c，而服务器真正的回应包中序列号为c’，这其中有一个差值|c-c’|，在每个相关数据报文经过防火墙的时候进行序列号的修改。

TCP Safe Reset技术：

这也是防火墙SYN代理的一种方式，其工作过程如下图所示：



这种方法在验证了连接之后立即发出一个Safe Reset命令包，从而使得Client重新进行连接，这时出现的Syn报文防火墙就直接放行。在这种方式中，防火墙就不需要对通过防火墙的数据报文进行 序列号的修改了。这需要客户端的TCP协议栈支持RFC 793中的相关约定，同时由于Client需要两次握手过程，连接建立的时间将有所延长。