**SYN-cookie和地址状态监控**

SYN Flood攻击给互联网造成重大影响后，针对如何防御SYN Flood攻击出现了几种比较有效的技术。

1．SYN－cookie技术

一般情况下，当服务器收到一个TCP SYN报文后，马上为该连接请求分配缓冲区，然后返回一个SYN＋ACK报文，这时形成一个半连接。SYN Flood正是利用了这一点，发送大量的伪造源地址的SYN连接请求，而不完成连接。这样就大量的消耗的服务器的资源。

SYN－cookie技术针对标准TCP连接建立过程资源分配上的这一缺陷，改变了资源分配的策略。当服务器收到一个SYN报文后，不立即分配缓冲区，而是利用连接的信息生成一个cookie，并将这个cookie作为将要返回的SYN＋ACK报文的初始序列号。当客户端返回一个ACK报文时，根据包头信息计算cookie，与返回的确认序列号（初始的序列号＋1）的前24位进行对比，如果相同，则是一个正常连接，然后，分配资源，建立连接。

该技术的巧妙之点在于避免了在连接信息未完全到达前进行资源分配，使SYN Flood攻击的资源消耗失效。实现的关键之处在于cookie的计算。cookie的计算应该做到包含本次连接的状态信息，使攻击者不能伪造cookie。cookie的计算过程如下：

1）服务器收到一个SYN包后，计算一个消息摘要mac： mac = MAC（A，k）； MAC是密码学中的一个消息认证码函数，也就是满足某种安全性质的带密钥的hash函数，它能够提供cookie计算中需要的安全性。

A为客户和服务器双方的IP地址和端口号以及参数t的串联组合：

A = SOURCE\_IP || SOURCE\_PORT || DST\_IP || DST\_PORT || t

K为服务器独有的密钥；

时间参数t为32比特长的时间计数器，每64秒加1；

2）生成cookie：

cookie = mac（0:24）：表示取mac值的第0到24比特位；

3）设置将要返回的SYN+ACK报文的初始序列号，设置过程如下：

i.  高24位用cookie代替；

ii.  接下来的3比特位用客户要求的最大报文长度MMS代替；

iii.  最后5比特位为t mod 32。

客户端收到来自服务器SYN+ACK报文后，返回一个ACK报文，这个ACK报文将带一个cookie（确认号为服务器发送过来的SYN ACK报文的初始序列号加1，所以不影响高24位），在服务器端重新计算cookie，与确认号的前24位比较，如果相同，则说明未被修改，连接合法，然后，服务器完成连接的建立过程。

SYN-cookie技术由于在连接建立过程中不需要在服务器端保存任何信息，实现了无状态的三次握手，从而有效的防御了SYN Flood攻击。但是该方法也存在一些弱点。由于cookie的计算只涉及了包头的部分信心，在连接建立过程中不在服务器端保存任何信息，所以失去了协议的许多功能，比如，超时重传。此外，由于计算cookie有一定的运算量，增加了连接建立的延迟时间，因此，SYN-cookie技术不能作为高性能服务器的防御手段。通常采用动态资源分配机制，当分配了一定的资源后再采用cookie技术，Linux就是这样实现的。还有一个问题是，当我们避免了SYN Flood攻击的同时，同时也提供了另一种拒绝服务攻击方式，攻击者发送大量的ACK报文，使服务器忙于计算验证。尽管如此，在预防SYN Flood攻击方面，SYN-cookie技术仍然是一种有效的技术。

 2．地址状态监控

地址状态监控的解决方法是利用监控工具对网络中的有关TCP连接的数据包进行监控，并对监听到的数据包进行处理。处理的主要依据是连接请求的源地址。

每个源地址都有一个状态与之对应，总共有四种状态：

初态：任何源地址刚开始的状态；

NEW状态：第一次出现或出现多次也不能断定存在的源地址的状态；

GOOD状态：断定存在的源地址所处的状态；

BAD状态：源地址不存在或不可达时所处的状态；

具体的动作和状态转换根据TCP头中的位码值决定。

1）监听到SYN包，如果源地址是第一次出现，则置该源地址的状态为NEW状态；如果是NEW状态或BAD状态；则将该包的RST位置1然后重新发出去，如果是GOOD状态不作任何处理。

2）监听到ACK或RST包，如果源地址的状态为NEW状态，则转为GOOD状态；如果是GOOD状态则不变；如果是BAD状态则转为NEW状态；如果是BAD状态则转为NEW状态。

3）监听到从服务器来的SYN ACK报文（目的地址为addr），表明服务器已经为从addr发来的连接请求建立了一个半连接，为防止建立的半连接过多，向服务器发送一个ACK包，建立连接，同时，开始计时，如果超时，还未收到ACK报文，证明addr不可达，如果此时addr的状态为GOOD则转为NEW状态；如果addr的状态为NEW状态则转为BAD状态；如果为addr的状态为BAD状态则不变。

下面分析一下基于地址状态监控的方法如何能够防御SYN Flood攻击。

1）对于一个伪造源地址的SYN报文，若源地址第一次出现，则源地址的状态为NEW状态，当监听到服务器的SYN+ACK报文，表明服务器已经为该源地址的连接请求建立了半连接。此时，监控程序代源地址发送一个ACK报文完成连接。这样，半连接队列中的半连接数不是很多。计时器开始计时，由于源地址是伪造的，所以不会收到ACK报文，超时后，监控程序发送RST数据包，服务器释放该连接，该源地址的状态转为BAD状态。之后，对于每一个来自该源地址的SYN报文，监控程序都会主动发送一个RST报文。

2）对于一个合法的SYN报文，若源地址第一次出现，则源地址的状态为NEW状态，服务器响应请求，发送SYN＋ACK报文，监控程序发送ACK报文，连接建立完毕。之后，来自客户端的ACK很快会到达，该源地址的状态转为GOOD状态。服务器可以很好的处理重复到达的ACK包。

从以上分析可以看出，基于监控的方法可以很好的防御SYN Flood攻击，而不影响正常用户的连接。

3. 小结

　　本文介绍了SYN Flood攻击的基本原理，然后详细描述了两种比较有效和方便实施的防御方法：SYN-cookie技术和基于监控的源地址状态技术。SYN-cookie技术实现了无状态的握手，避免了SYN Flood的资源消耗。基于监控的源地址状态技术能够对每一个连接服务器的IP地址的状态进行监控，主动采取措施避免SYN Flood攻击的影响。这两种技术是目前所有的防御SYN Flood攻击的最为成熟和可行的技术。