网络工作组P。弗格森
请求评论：2827Cisco Systems，Inc.过时：D. Senie 2267
BCP：38Amaranth Networks Inc.
类别：最新最佳实践（2000年5月）

网络入口过滤：
击败采用IP源地址欺骗的拒绝服务攻击

该备忘录的状态

本文档指定了互联网社区的互联网最佳实践，并要求讨论和提出改进建议。

版权声明

摘要

最近事实证明，使用伪造源地址的各种拒绝服务（DoS）攻击对于互联网服务提供商和整个互联网社区来说都是一个麻烦的问题。本文讨论了一种简单，有效，简单的入口流量过滤方法禁止使用"伪造" IP地址的拒绝服务攻击从互联网服务提供商（ISP）聚合点"背后"传播。

目录

1. 引言

针对互联网中各种目标的拒绝服务攻击浪潮再起[1]，这在互联网服务提供商（ISP）和网络安全社区内部提出了新的挑战，需要寻找新的创新方法来减轻此类攻击。实现这一目标的困难很多。一些简单的工具可以限制这些攻击的有效性和范围，但尚未广泛实施。

这种攻击方法已有一段时间了。然而，捍卫它一直是一个令人担忧的问题。 BillCheswick引用[2]就是说，他在最后一刻从书中提到了"防火墙和互联网安全"[3]，因为被攻击系统的管理员无法有效防御系统。在提及该方法时，他担心会鼓励使用该方法。

虽然本文档中讨论的过滤方法绝对无法防范源自有效前缀（IP地址）的泛洪攻击，但将阻止原始网络内的攻击者使用不符合标准的伪造源地址发起此类攻击进入过滤规则。敦促所有互联网连接提供商实施本文档中描述的过滤，禁止攻击者使用伪造的源地址，这些源地址不在合法公告前缀的范围内。换句话说，如果ISP正在聚合多个下游网络的路由通告，流量过滤应用于禁止声称源自这些汇总公告之外的流量。

实施此类过滤的另一好处是，可以使发起方轻松跟踪其真实来源，因为攻击者必须使用有效且可合法到达的源地址。

2. 背景资料

下面是TCP SYN泛洪问题的简化示意图：

```
                                                        204.69.207.0/24
主机<------路由器<---互联网<------路由器<-攻击者

          TCP /同步
     <-------------------------------------------
            来源：192.168。 0.4 / 32
同步/确认
没有路线
          TCP /同步
     <-------------------------------------------
            资料来源：10.0.0.13/32
同步/确认
没有路线
          TCP /同步
     <-------------------------------------------
            来源：172.16。 0.2 / 32
同步/确认
没有路由
```

[等…]

假设：

- "主机"是目标机器。
- 攻击者位于"有效"前缀204.69.207.0/24中。
- 攻击者使用随机改变的源地址发起攻击；在此示例中，源地址从[4]中描述，通常不存在于全局互联网路由表中，因此不可达。但是，任何无法到达的前缀都可以用作攻击手段。

另外值得一提的是，伪造源地址似乎是源自于一个或多个全局路由表中的另一个合法网络。例如，使用有效网络地址的攻击者可能会通过使攻击似乎来自实际上并非发起攻击且完全无辜的组织而遭受严重破坏。在这种情况下，受到攻击的系统管理员可能会过滤来自明显攻击源的所有流量。添加此类过滤器将导致拒绝服务

合法的，非恶意的终端系统。在这种情况下，受到攻击的系统管理员会无意间成为攻击者的帮凶。

更为复杂的是，TCP SYN泛洪攻击会将SYN-ACK数据包发送到一台或多台不参与攻击但成为次要受害者的主机。这使攻击者可以一次滥用两个或多个系统。

使用UDP和ICMP泛洪攻击曾尝试过类似的攻击。前一种攻击（UDP泛洪）使用伪造数据包尝试将chargen UDP服务连接到另一端的echo UDP服务site.Systems管理员切勿允许从管理域外部发往系统诊断端口的UDP数据包到达系统。后一种攻击（ICMP泛洪）使用IP子网广播复制机制中的阴险功能。这种攻击依赖于为大型多路访问广播网络服务的路由器，将IP广播地址（例如，发往10.255.255.255的地址）帧化为第2层广播帧（对于以太网，FF：FF：FF：FF：FF：FF）。以太网NIC硬件（特别是MAC层硬件）在正常操作中仅侦听选定数量的地址。所有设备在正常操作中共同共享的一个MAC地址是媒体广播，即FF：FF：FF：FF：FF：FF。在这种情况下，设备将接收数据包并发送中断进行处理。因此，这些广播帧的泛洪将消耗终端系统上的所有可用资源[9]。也许是审慎的考虑，系统管理员应确保默认情况下不允许边界路由器转发定向广播数据包。

当使用无法到达的源地址发起TCPSYN攻击时，目标主机会尝试预留资源等待响应，攻击者会反复更改发送的每个新数据包的虚假源地址，耗尽更多主机资源。

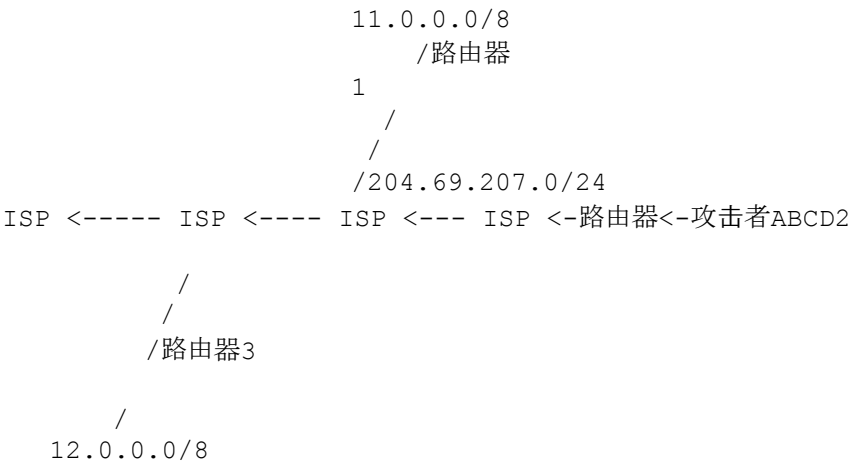
或者，如果攻击者使用他人的有效主机地址作为源地址，则被攻击系统将发送一封大量SYN /ACK数据包被认为是连接建立序列的发起者。这样，攻击者就会损坏两个系统：目标系统和实际在全局路由系统中使用欺骗地址的系统。

两种攻击方法的结果都是性能极度下降，或更糟糕的是，系统崩溃。

针对这种威胁，大多数操作系统供应商都对其软件进行了修改，使目标服务器能够以极高的连接尝试率抵御攻击。这是解决问题的欢迎和必要部分。入口过滤将需要大量时间全面实施和完全有效，但可以快速实施操作系统扩展。这种组合应该证明对防止源地址欺骗有效。有关供应商和平台软件升级的信息，请参见[1]。

3. 限制伪造流量

此类攻击遇到的问题很多，涉及主机软件实现，路由方法和TCP /IP协议本身的缺点。但是，通过限制源自下游网络的传输流量为已知的（有意为目标的）前缀（es），在这种攻击情况下，可以消除源地址欺骗问题。



在上面的示例中，攻击者位于204.69.207.0/24（由ISP D提供互联网连接）。"路由器2"的入口（输入）链路上的输入流量过滤器提供了与攻击者网络的连接限制，流量仅允许源于204.69.207.0/24前缀内的源地址的流量，并禁止攻击者使用前缀范围外的"无效"源地址。

换句话说，上面"路由器2"上的入口过滤器将检查：IFpacket的源地址来自204.69.207.0/24 然后酌情转发

IFpacket的源地址为"否"数据包网络管理员应记录有关丢弃数据包的信息。这样就为监控任何可疑活动提供了基础。

4. 网络设备的其他可能功能

将来的平台实现应考虑其他功能。值得注意的是：

- o在远程访问服务器上实施自动过滤。
  在大多数情况下，拨入访问服务器的用户是单个计算机上的单个用户。源自该PC的数据包的唯一有效源IP地址是ISP分配的地址（静态或动态分配）。远程访问服务器可以检查入口处的每个数据包，确保用户不会欺骗其发起数据包的源地址。显然，对于客户合法地通过远程路由器连接网络或子网的情况，也需要做出规定，但可以将其作为可选参数实现。我们已经收到报告，一些供应商和一些ISP已经开始实现此功能。

我们考虑过建议路由器也按照[8]中的建议验证发送方的源IP地址，但这种方法在当今的真实网络中无法很好地运行。建议的方法是查找源地址，查看到该地址的返回路径将与数据包到达的接口流出同一接口。鉴于互联网中不对称路由的数量，这显然是有问题的。

5. 负债

这种性质的过滤有可能破坏某些类型的"特殊"服务。提供这些类型的特殊服务的互联网服务提供商（ISP）最大利益是考虑采用其他方法实施这些服务，以避免受到入口流量过滤的影响。

[6]中定义的移动IP受到入口流量过滤的具体影响。如所指定的，到移动节点的流量是通过隧道传输的，但不从移动节点的流量是通过隧道传输的。这样会导致来自移动节点的数据包的源地址与连接站点的网络不匹配。为适应入口过滤和其他问题，移动IP工作组开发了一种"反向隧道"方法，在[7]中指定。这为移动节点传输的数据在传输到互联网之前先传输到本地代理提供了一种方法。反向隧道传输协议还有其他好处，包括更好地处理多播流量。鼓励那些实施移动IP系统的人实施这种反向隧道方法。

如前所述，尽管入口流量过滤大大降低了源地址欺骗的成功率，但并不排除攻击者使用允许前缀过滤范围内的另一台主机的伪造源地址。但是，它可以确保在确实发生此类攻击时，网络管理员可以确保该攻击实际上源自已知的已知前缀。这样可以简化对罪魁祸首的跟踪，最糟糕的是，管理员可以在问题解决之前阻止一系列源地址。

如果在使用DHCP或BOOTP的环境中使用入口过滤，则建议网络管理员确保允许源地址为0.0.0.0且目的地为255.255.255.255的数据包到达路由器中的中继代理。定向广播复制的范围应受到控制，但不得随意转发。

6. 总结

互联网连接网络外围的入口流量过滤将降低源地址欺骗拒绝服务攻击的有效性。网络服务提供商和管理员已经开始在外围路由器上实施这种类型的过滤，建议所有服务提供商尽快这样做。除了帮助整个互联网社区击败这种攻击方法之外，如果服务提供商可以明确证明其网络已经在客户链路上建立了入口过滤，还可以帮助服务提供商定位攻击源。

公司网络管理员应实施过滤，确保其公司网络不是此类问题的根源。确实，可以在组织内部使用过滤，以确保通过将系统不正确地连接到错误的网络来确保用户不会造成问题。
实际上，过滤还可能阻止心怀不满的员工免受匿名攻击。

所有网络管理员都有责任确保自己不会成为此类攻击的不明来源。

7. 安全注意事项

本文档的主要目的是从本质上提高整个互联网社区的安全实践和认识；随着越来越多的互联网提供商和企业网络管理员实施入口过滤，攻击者利用伪造源地址作为攻击方法的机会将大大减少。当来源更可能为"有效"时，简化追踪攻击源的方式。通过减少整个互联网的攻击次数和频率，将有更多资源追踪最终发生的攻击。

8. 致谢

北美网络运营商小组（NANOG）[5]作为一个整体，在公开讨论这些问题并积极寻求可能的解决方案时，应受到特别赞扬。另外，还要感谢Justin Newton（Priori网络）和Steve Bielagus（IronBridge网络）的评论和贡献。

9. 参考文献

[1] CERT咨询CA-96.21； TCP SYN泛洪和IP欺骗攻击； 1996年9月24日。

[2] B.齐格勒，" Hacker Tangles
Panix网站"，《华尔街日报》，1996年9月12日。

[3] "防火墙和互联网安全：击退狡猾的黑客"；威廉·R·切斯威克和史蒂文·贝洛文，Addison-Wesley出版公司，1994年； ISBN 0-201-63357-4。

[4] Rekhter，Y.，Moskowitz，R.，Karrenberg，D.，de Groot，G.和E. Lear，"专用互联网的地址分配"，1996年2月。RFC 1918

[5] 北美网络运营商组； 。http://www.nanog.org

[6] Perkins，C，" IP移动性支持"，1996年10月。RFC 2002

[7] 黑山共和国，“移动IP反向隧道”，1998年5月。RFC 2344

[8] Baker，F，“ IP版本4路由器的要求”，1995年6月。RFC 1812

[9] 感谢：Craig Huegen；请参阅：。http://www.quadrunner.com/~chuegen/smurf.txt

10.作者致辞

Paul Ferguson
Cisco Systems, Inc.
13625 Dulles Technology
Dr.Herndon, Virginia 20170
USA

电子邮件：ferguson@cisco.com

DanielSenie
Amaranth Networks
Inc.324 Still River
Road Bolton, MA
01740 USA

电子邮件：dts@senie.com

11. 完整的版权声明

致谢

RFC编辑器功能的资金目前由互联网协会提供。