定义防止 TCP SYN 拒绝服务攻击的策略

目录

摘要

有潜在拒绝服务攻击在该的网络服务提供商(ISP)目标网络设备。

- **TCP SYN 攻击**：发送方传输大量不能完成的连接。这将造成连接队列填满的情况，从而拒绝合法 TCP 用户的服务。

本文包含了潜在 TCP SYN 攻击如何发生，以及如何使用 Cisco IOS 软件防止这种攻击的建议方法的技术说明。

注意： Cisco IOS 11.3 软件有一项功能，可主动防御 TCP 拒绝服务攻击。此功能在文档配置 TCP 拦截（防御拒绝服务攻击）中介绍。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题说明

TCP SYN 攻击

当正常 TCP 连接开始时，目的地主机将收到源主机发出的 SYN(synchronize/start) 数据包，并发回同步应答(同步确认)。连接建立之前，目的地主机必须监听 SYN ACK 的 ACK（确认）。这称为“TCP 三次握手”。

等待同步应答（SYN ACK）的确认（ACK）时，目的地主机上的大小有限的连接队列将记录等待完成的连接。因为 ACK 预计在同步应答后几毫秒内到达，此队列通常迅速倒空。

TCP SYN 攻击利用了此设计，由攻击源主机（相对于受害主机）生成带有随机源地址的 TCP 同步数据包。受害目标主机向随机源地址发送同步确认，并且在连接队列中添加新条目。因为同步应答指定用于不正确或不存在的主机，因此“三方握手”的最后一部分永远不会完成，并且条目保留在连接队列中，直到计时器到期，保留时间通常为一分钟。通过从随机 IP 地址快速生成欺骗性 TCP 同步数据包，有可能将连接队列填满，从而拒绝合法用户请求的 TCP 服务（例如电子邮件、文件传输或 WWW）。

由于来源 IP 地址是伪造的，因此很难追踪到攻击者。

问题的外部表现包括：无法获得电子邮件、无法收到 WWW 的或 FTP 服务连接，或者主机上存在大量处于 SYN_RCVD 状态的 TCP 连接。

保护网络设备免受攻击

在防火墙后面的设备

TCP SYN 攻击的特征是 SYN 数据包从随机源 IP 地址汇集而来。终止入局同步数据包的防火墙后面的所有设备，已经能够免受此攻击方式，并且不需要采取进一步措施。防火墙示例包括 Cisco 专用互联网交换 (PIX) 防火墙或配有访问列表的 Cisco 路由器。欲知如何在 Cisco 路由器上设置访问控制列表的示例，请参见“增强 IP 网络安全”文件。

提供公开可用的服务（邮件服务器、公共 Web 服务器）的设备

由于您可以使用访问控制列表，将入站访问明确限制为少量精选 IP 地址，因此防止防火墙后面的设备受到随机 IP 地址的 SYN 攻击则相对简单。然而，公共 Web 服务器或邮件服务器面对互联网时，则没有办法确定哪些流入 IP 源地址是友好的而哪些是不友好的。因此，无法明确地防御来自随机 IP 地址的攻击。主机有几个可用的选项：

- 增大连接队列（SYN ACK 队列）的大小。
- 缩短三方握手的超时等待时间。
- 利用供应商软件补丁程序来检测和避免此问题（如果有）。

您应该联系您的主机供应商，查看他们是否创建特定补丁程序解决 TCP 同步应答攻击。

注意： 在服务器上过滤 IP 地址无效，是因为攻击者可能改变他的 IP 地址，并且其地址有可能与合法主机的地址相同。

防止网络无意地充当攻击者

由于此拒绝服务攻击的主要机制是生成随机 IP 地址发出的数据流，因此我们建议过滤指定到互联网的流量。当它们进入互联网时，基本概念是丢掉带有无效源 IP 地址的数据包。这不能阻止您网络上的拒绝服务攻击，但是可以帮助被攻击当事人排除您的位置为攻击者的来源。此外，它使您的网络受到此类攻击的可能性有所降低。

防止无效的 IP 地址传输

在把您的网络连接到互联网的路由器上过滤数据包，您只可以允许带有有效源 IP 地址的数据包离开您的网络，进入互联网。

例如，如果您的网络包括网络 172.16.0.0，而您的路由器使用某个串行 0/1 接口连接到您的 ISP，您可以按如下方式运用访问控制列表：

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

注意： 访问控制列表的最后一行确定是否有任何无效源地址的数据流输入互联网。它对此线路不重要，但有助于查找可能的攻击来源。

防止接收无效的 IP 地址

对于向终端网络提供服务的 ISP，我们强烈建议从您的客户端验证流入数据包。这可以通过在边界路由器上使用流入数据包过滤器来实现。

例如，如果您的客户端具有通过名为“串行 1/0”的串行接口连接到您的路由器的以下网络编号，您便可以建立以下访问控制列表：

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

注意： 访问控制列表最后一行确定是否有任何带无效源地址的数据流进入互联网。它对此线路不重要，但有助于查找可能的攻击来源。

此主题的某些细节在 NANOG [北美网络操作员第一组]邮件列表中讨论。列表存档位于：http://www.merit.edu/mail.archives/nanog/index.html

有关 TCP SYN 拒绝服务攻击和 IP 欺骗的详细说明，请参阅：http://www.cert.org/advisories/CA-1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

相关信息

- 技术支持 - Cisco Systems