防范分布式拒绝服务 (DDoS) 攻击的策略

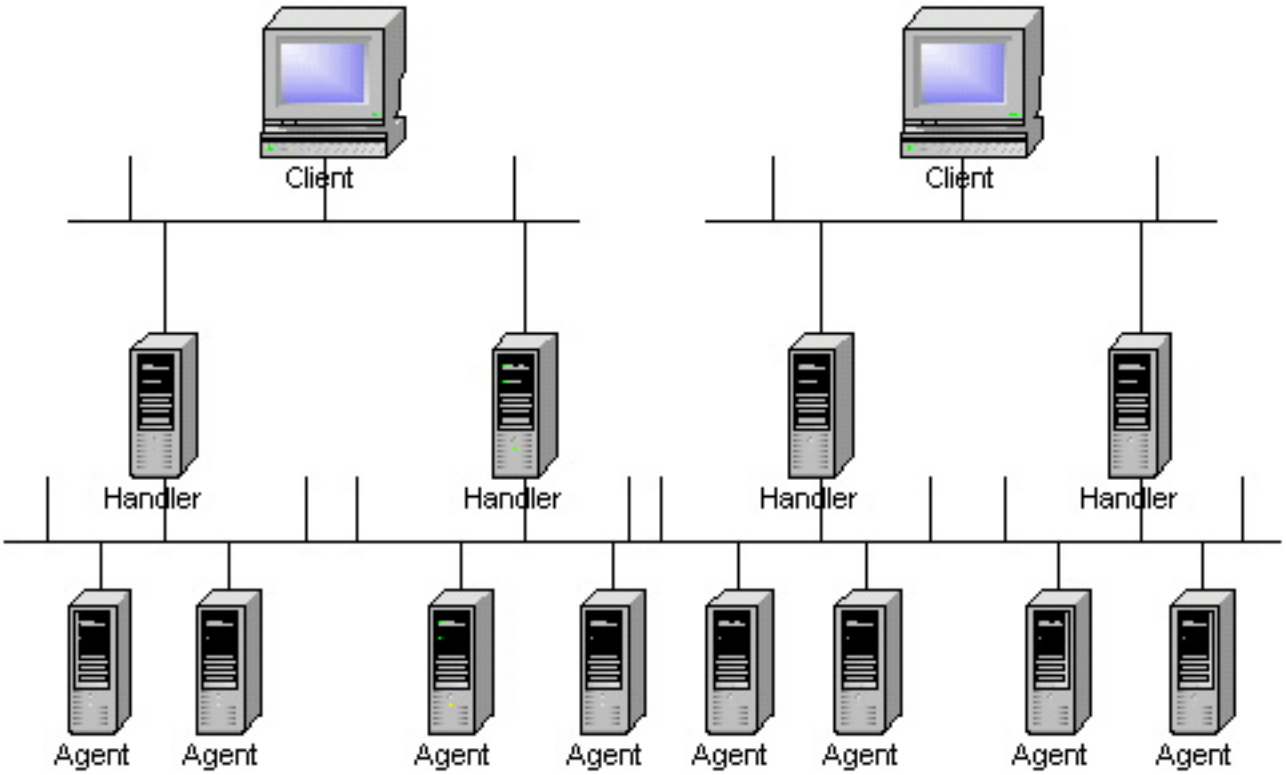
目录

简介

此白皮书中包含的信息有助于您了解分布式拒绝服务 (DDoS) 攻击是如何形成的、识别用于帮助 DDoS 攻击的程序、运用相关措施防止攻击、收集您怀疑存在攻击时的辩论信息以及了解更多有关主机安全的信息。

了解 DDoS 攻击的基础

请参阅以下图示：



客户端后是发动攻击的人。**处理器**是有特殊程序正在其上运行的漏洞主机。每个处理器均能控制多个代理。**代理**是运行特殊程序的漏洞主机。每个代理程序负责生成直接指向目标受害者的数据包流。

攻击者通常使用以下四种程序发起 DDoS 攻击：

1. Trinoo
2. TFN
3. TFN2K
4. Stacheldraht

为帮助 DDoS，攻击者需要有数百至数千台漏洞主机。主机通常是 Linux 和 SUN 计算机；但是，工具也可以被移植到其他平台。攻陷主机和安装工具的过程是自动的。该过程可划分成以下几个步骤，在这些步骤中攻击者：

1. "起动扫描阶段，对大量主机(100,000或更多)的已知弱点进行探测。"
2. 攻陷易受攻击主机，获取访问权。
3. 在每台主机上安装工具。
4. 对漏洞主机进行进一步扫描和破坏。

由于使用了自动化进程，攻击者在 5 秒钟内即可攻陷一台主机并在其上安装工具。换句话说，在不到一小时的时间内即可攻陷数千台主机。

用于帮助攻击的常用程序的特征

以下是黑客用于帮助分布式拒绝服务攻击的普通程序：

- Trinoo客户端、处理器和代理之间的通信使用以下端口：`1524 tcp`
  `27665 tcp`
  `27444 udp`
  `31335 udp`**注意：** 以上所列端口是此工具的*默认端口*。仅将这些端口用作导向和示例，因为可以轻易更改端口号。
- TFN客户端、处理器和代理之间的通信使用 ICMP ECHO 和 ICMP ECHO REPLY 数据包。
- Stacheldraht客户端、处理器和代理之间的通信使用以下端口：`16660 tcp`
  `65000 tcp`
  `ICMP ECHO`
  `ICMP ECHO REPLY`**注意：** 以上所列端口是此工具的默认端口。仅将这些端口用作导向和示例，因为可以轻易更改端口号。
- TFN2K客户端、处理器和代理之间的通信不使用任何特定端口，例如，可以在运行时提供或者通过程序随机选择，但它是 UDP、ICMP 和 TCP 数据包的组合。有关 DDoS 程序的详细分析，请参阅以下条款。

注意： Theaw 链路指向不由 Cisco Systems 维护的外部网站。

DoS 项目的“trinoo”分布式拒绝服务攻击工具

“Tribe Flood Network”分布式拒绝服务攻击工具

“stacheldraht”分布式拒绝服务攻击工具

有关 DDoS 工具及其变体的详细信息，请参阅 Packet Storm 网站上的分布式攻击工具索引。

预防

以下是用于防止分布式拒绝服务攻击的建议方法。

1. 在连接上行末端的路由器输入接口上使用 ip verify unicast reverse-path interface 命令。此功能检查该接口上作为输入接收的每个数据包。如果源 IP 地址在指回数据包所到达同一接口的 CEF 表中没有路由，则路由器会丢弃数据包。单播 RPF 的作用是，它将在 ISP 的 POP（租用和拨号）处终止 SMURF 攻击（及其他取决于源 IP 地址伪装的攻击）。这保护了您的网络和客户，也保护了互联网的其他部分。要使用单播 RPF，请在路由器中启用“CEF 交换”或“CEF 分布式交换”。无需为 CEF 交换配置输入接口。只要 CEF 在路由器上运行，就可以将各接口配置为其他交换模式。RPF 是一种在接口或子接口上启用的输入端功能，并用于对路由器收到的数据包进行处理。在路由器上开启 CEF 至关重要。没有 CEF，RPF 将不会工作。单播 RPF 在任何 11.2 或 11.3 镜像均不受支持。单播 RPF 包括在支持 CEF 的平台 12.0 中，其中包括 AS5800。因此，单播 RFP 可以配置在 AS5800 的 PSTN/ISDN 拨号接口上。
2. 使用访问控制列表 (ACL) 过滤所有 RFC-1918 地址空间。参阅以下示例：
```
access-list 101
deny ip 10.0.0.0    0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0  0.15.255.255 any
access-list 101 permit ip any any

interface xy
   ip access-group 101 in
```
有关可被过滤的专用 IPv4 地址空间的另一信息源是现在已过期的 IETF 草案“记录已向 IANA 登记的专用 IPv4 地址块。”
3. 通过使用 ACL 应用入口和出口过滤（参阅 RFC-2267 ）。参阅以下示例：
```
{ ISP Core } -- ISP Edge Router -- Customer Edge Router -- { Customer network }
```
ISP 边缘路由器应仅接收源地址属于客户网络的流量。客户网络应仅接收源地址不属于客户网络块的流量。这是 ISP 边缘路由器的示例 ACL ：
```
access-list 190 permit ip {customer network} {customer network mask} any
access-list 190 deny ip any any [log]

interface {ingress interface} {interface #}
ip access-group 190 in
```
这是用户边缘路由器的示例 ACL ：
```
access-list 187 deny ip {customer network} {customer network mask} any
access-list 187 permit ip any any

access-list 188 permit ip {customer network} {customer network mask} any
access-list 188 deny ip any any

interface {egress interface} {interface #}
ip access-group 187 in
ip access-group 188 out
```
如果您能打开 Cisco 快速转发 (CEF)，则可通过启用单播反向路径转发大幅减少 ACL 的长度，从而提高性能。总的来说，要支持单播反向路径转发，您只需能够在路由器上启用 CEF；启用功能的接口不需要成为CEF的交换接口。
4. 使用 CAR 限制 ICMP 数据包的速率。参阅以下示例：
```
interface xy
 rate-limit output access-group 2020 3000000 512000 786000 conform-action transmit exceed-action drop access-list 2020 permit icmp any any echo-reply
```
5. 为 SYN 数据包配置速率限制。参阅以下示例：
```
access-list 152 permit tcp any host eq www
access-list 153 permit tcp any host eq www established

interface {int}
rate-limit output access-group 153 45000000 100000 100000
conform-action transmit exceed-action drop
 rate-limit output access-group 152 1000000 100000 100000
conform-action transmit exceed-action drop
```
在前一个示例中，请：用最大链接带宽替换 **45000000**用介于 50% 到 30% 的 SYN 溢出率的值替换 **1000000**用准确值替换*突发流量正常*和*突发流量最大*速率注意，如果您将突发速率设置为大于 30%，则许多合法 SYN 可能被丢弃。要明确设置突发速率的位置，请使用 show interfaces rate-limit 命令，以显示接口的一致速率和超出速率。您的目标是尽量少限制SYN的速率，使事情重新运作起来。**警告：** 我们建议

您首先在正常状态期间(在攻击发生之前）测量相当数量的同步信息包，并使用那些值进行限制。在您部署此测量前，请仔细审查编号。如果 SYN 攻击瞄准特定主机，请考虑在该主机上安装 IP 过滤程序包。其中一个此类程序包为 IP Filter。 有关实施细节，请参阅 IP Filter 示例。

捕获证据和联系执法

如果可能，请获取一个攻击流量示例，以进行后续分析（一般称为“数据包捕获”）。请使用有足够处理能力的 Solaris 或 Linux 工作站，以便跟上数据包流。要获取此类数据包捕获，请使用 tcpdump 程序（适用于 Windows、Solaris 和 Linux 操作系统）或 snoop 程序（仅适用于 Solaris OS）。 以下是如何使用这些程序的一个基本示例：

```
tcpdump -i interface -s 1500 -w capture_file
  snoop -d interface -o capture_file -s 1500
```

本示例中的 MTU 大小是 1500；如果 MTU 大于 1500，请更改此参数。

如果您想付诸法律，并且您位于美国境内，请联系您当地的 FBI 现场办事处。有关详细信息，可从国家基础设施保护中心网站获取。如果您位于欧洲，则不存在任何单一联络点。请联系您当地的执法机构，并请求他们予以帮助。

CISCO 不能代表您与执法机构联系。一旦您与执法取得初步联系，Cisco PSIRT 团队就可与该执法展开合作。

有关常用主机安全材料，请访问 CERT/CC 网页。

相关信息

- **使用 Cisco 路由器确定数据包泛洪的特征并加以跟踪**
- **蠕虫病毒缓解技术详细资料**
- **改善 Cisco 路由器的安全性**
- **Cisco 产品安全事件响应**
- **安全 @ Cisco**
- **技术支持和文档 - Cisco Systems**