

因特网防火墙技术



[因特网防火墙技术_下载链接1](#)

著者:刘渊

出版者:机械工业出版社

出版时间:1998-08

装帧:平装

isbn:9787111066408

作者介绍:

目录: 目录

前言

第1章 概论

1.1 因特网的特点

1.2 因特网将成为信息战的战略目标

1.3 如何保护因特网的站点

1.3.1 无安全防卫

1.3.2 模糊安全防卫

1.3.3 主机安全防卫

1.3.4 网络安全防卫

1.4 防火墙

第2章 因特网的安全与保安策略

2.1 因特网服务的安全隐患

2.1.1 电子邮件

2.1.2 文件传输 (FTP)

2.1.3 远程登录 (Telnet)

2.1.4 用户新闻 (UsenetNews)

- 2.1.5万维网 (WWW)
- 2.1.6其他的网络信息服务
- 2.1.7网络文件系统 (NFS)
- 2.2 因特网的安全问题及其原因
 - 2.2.1薄弱的认证环节
 - 2.2.2系统的易被监视性
 - 2.2.3易欺骗性
 - 2.2.4有缺陷的局域网服务和相互信任的主机
 - 2.2.5复杂的设置和控制
 - 2.2.6无法估计主机的安全性
- 2.3因特网上站点的脆弱性
- 2.4 因特网的保安措施
 - 2.4.1最小特权
 - 2.4.2纵深防御
 - 2.4.3阻塞点
 - 2.4.4最弱连接
 - 2.4.5失败时的保安策略
 - 2.4.6全体参与
- 第3章 建立防火墙
 - 3.1一些有关的定义
 - 3.1.1 包过滤
 - 3.1.2代理服务
 - 3.1.3多种技术的混合使用
 - 3.2防火墙结构
 - 3.2.1双宿主主机结构
 - 3.2.2主机过滤结构
 - 3.2.3子网过滤结构
 - 3.3 防火墙的各种变化和组合
 - 3.3.1使用多堡垒主机
 - 3.3.2合并内外部路由器
 - 3.3.3合并堡垒主机和外部路由器
 - 3.3.4慎用将堡垒主机与内部路由器合并
 - 3.3.5慎用多内部路由器结构
 - 3.3.6使用多外部路由器
 - 3.3.7多参数网络结构
 - 3.3.8双宿主主机加子网过滤
 - 3.4 内部防火墙
 - 3.4.1试验网络
 - 3.4.2低保密度网络
 - 3.4.3高保密度网络
 - 3.4.4 联合防火墙
 - 3.4.5共享参数网络
 - 3.4.6内部防火墙的堡垒主机之选择
 - 3.5防火墙的未来
- 第4章 堡垒主机
 - 4.1建立堡垒主机的一般原则
 - 4.2特殊的堡垒主机
 - 4.2.1无路由双宿主主机
 - 4.2.2牺牲主机
 - 4.2.3内部堡垒主机
 - 4.3堡垒主机的选择
 - 4.3.1堡垒主机操作系统的选择
 - 4.3.2堡垒主机速度的选择

4.3.3如何配置堡垒主机的硬件

4.4 堡垒主机的物理位置

4.4.1位置要安全

4.4.2堡垒主机在网络上的位置

4.5 堡垒主机提供服务的选择

4.6建立堡垒主机

4.6.1系统日志的建立方法

4.6.2关闭所有不需要的服务

4.6.3如何关闭服务

4.6.4哪些服务需要被保留

4.6.5堡垒主机的重新配置

4.6.6进行安全分析

4.7堡垒主机的监测

4.7.1监测堡垒主机的运行

4.7.2自动监测堡垒主机

4.8对堡垒主机的保护与备份

第5章 包过滤

5.1包过滤是如何工作的

5.1.1包过滤的优点

5.1.2包过滤的缺点

5.2包过滤路由器的配置

5.2.1协议总是双向的

5.2.2准确理解“往内”与“往外”的语义

5.2.3准确设置“默认允许”与“默认拒绝”

5.3包的基本构造

5.4 在协议各层上包的传输

5.4.1TCP/IP以太网的例子

5.4.2IP层以上各层的情况

5.4.3IP层以下各层的情况

5.4.4应用层协议

5.4.5Non-IP协议（非IP协议）

5.5路由器对包的操作

5.5.1日志记录

5.5.2返回ICMP错误码

5.6设定包过滤规则

5.7依据地址进行过滤

5.8依据服务进行过滤

5.8.1 往外的Telnet服务

5.8.2往内的Telnet服务

5.8.3有关Telnet的总结

5.8.4不要仅依据源端口来过滤

5.9包过滤路由器的选择

5.9.1包过滤路由器的速度

5.9.2用通用计算机做路由器

5.9.3包过滤规则

5.9.4包过滤规则的次序

5.9.5对进入和离开网络的包分别制定规则

5.10应该对放行与拒绝的包建立日志

5.11设置包过滤的物理位置

5.12 包过滤系统的集成

5.13一些因特网服务的包过滤特性

- 5.13.1电子邮件
- 5.13.2简单邮件传输协议 (SMTP)
- 5.13.3邮政管理协议 (POP)
- 5.13.4文件传输
- 5.13.5远程登录 (Telnet)
- 5.13.6网络新闻传输协议 (NNTP)
- 5.13.7WWW
- 5.13.8域名系统 (DNS)
- 第6章 代理系统
 - 6.1为什么要进行代理
 - 6.2代理的优点
 - 6.3代理的缺点
 - 6.4 代理是如何工作的
 - 6.4.1使用定制客户软件进行代理
 - 6.4.2使用定制用户过程进行代理
 - 6.5代理服务器
 - 6.5.1应用级与回路级代理
 - 6.5.2公共与专用代理服务器
 - 6.5.3智能代理服务器
 - 6.6 在因特网服务中使用代理
 - 6.6.1TCP与其他协议
 - 6.6.2单向与多向连接
 - 6.7 不使用代理服务器的代理
 - 6.8使用SOCKS进行代理
 - 6.9 使用TIS因特网防火墙工具包进行代理
 - 6.10 使用TISFW TK的FTP代理
 - 6.10.1 使用TISFWTK的Telnet和rlogin代理
 - 6.10.2使用TISFWTK的公共代理
 - 6.10.3其他的TISFWTK代理
 - 6.11如果不能代理怎么办
 - 6.11.1没有代理服务器
 - 6.11.2 代理无法保证服务的安全
 - 6.11.3无法修改客户程序或过程
 - 6.12 一些因特网服务代理的特性
 - 6.12.1电子邮件
 - 6.12.2文件传输
 - 6.12.3Telnet
 - 6.12.4NNTP
 - 6.12.5WWW
 - 6.12.6DNS
- 第7章 因特网服务在防火墙中的配置及实例
 - 7.1在防火墙中配置因特网服务
 - 7.1.1电子邮件
 - 7.1.2文件传输
 - 7.1.3远程登录Telnet服务配置的注意事项
 - 7.1.4 新闻传输协议NNTP配置的注意事项
 - 7.1.5 HTTP和WWW的配置注意事项
 - 7.1.6DNS配置的注意事项
 - 7.2防火墙实例

7.2.1子网过滤结构的防火墙
7.2.2 主机过滤结构的防火墙
第8章 系统的安全保障和防火墙的维护
8.1使用往内服务的安全隐患
8.2什么是认证
8.3认证机制的实例
8.4 安全规定的内容
8.4.1安全规定应包含的内容
8.4.2 在安全规定中不应被提及内容
8.5如何制订安全规定
8.6防火墙的维护
8.7安全事故的处理
附录A 有关防火墙的资源
附录B 防火墙工具和软件
附录C TCP/IP的内部结构
附录D 有关网络安全和防火墙的书籍
• • • • • ([收起](#))

[因特网防火墙技术_下载链接1](#)

标签

防火墙

网络通信

网络安全

评论

[因特网防火墙技术_下载链接1](#)

[因特网防火墙技术_下载链接1](#)