

<<网络安全Cisco解决方案>>

图书基本信息

书名：<<网络安全Cisco解决方案>>

13位ISBN编号：9787505372924

10位ISBN编号：7505372920

出版时间：2002-1

出版时间：电子工业出版社

作者：(美)andrew g. mason mark j. newcomb

页数：362

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络安全Cisco解决方案>>

内容概要

虽然Cisco Systems公司通过推出Cisco Secure产品系列来帮助客户建立安全的网络，但到目前为止，国内尚没有使用Cisco Secure产品系列来解决因特网安全性问题的出版物，本书的出版填补了这一空白。

本书英文原版的作者都是具有高深资历的网络安全专家，其中主笔人Andrew G. Mason作为一位Cisco网络认证工程师，具有多年使用Cisco Secure产品来设计和实现

<<网络安全Cisco解决方案>>

书籍目录

第一部分 因特网安全性基础

- 第1章 因特网安全性 2
 - 1.1 因特网上的威胁 2
 - 1.2 网络服务 3
 - 1.2.1 路由器服务 3
 - 1.2.2 防火墙服务 4
 - 1.2.3 认证和授权服务 5
 - 1.2.4 网络地址转换服务 5
 - 1.2.5 加密和解密服务 6
 - 1.2.6 代理服务 7
 - 1.3 TCP/IP协议集的安全性 7
 - 1.3.1 TCP/IP概述 8
 - 1.3.2 网际协议 9
 - 1.3.3 地址解析协议 15
 - 1.3.4 因特网控制报文协议 16
 - 1.3.5 传输控制协议 18
 - 1.3.6 用户数据报协议 19
 - 1.4 拒绝服务攻击 20
 - 1.4.1 SYN洪泛攻击 20
 - 1.4.2 Ping攻击 21
 - 1.5 创建企业安全性策略 22
 - 1.6 小结 23
 - 1.7 FAQ (常见问题) 23
 - 1.8 词汇表 24
- 第2章 基本的Cisco路由器安全性 25
 - 2.1 基本的管理安全性 26
 - 2.1.1 访问列表 27
 - 2.1.2 标准访问列表 28
 - 2.1.3 扩展访问列表 33
 - 2.1.4 命名访问列表 33
 - 2.2 密码管理 34
 - 2.2.1 enable password命令 34
 - 2.2.2 enable secret命令 35
 - 2.3 物理安全性 35
 - 2.3.1 控制线路访问 36
 - 2.4 带外管理安全性 37
 - 2.5 Cisco发现协议 38
 - 2.6 超文本传输协议 (HTTP) 配置服务 38
 - 2.7 简单网络管理协议 39
 - 2.8 网络时间协议 41
 - 2.9 警示标语 43
 - 2.10 推荐的最小IOS安全性设置 43
 - 2.10.1 拒绝RFC 1918路由 44
 - 2.10.2 UDP和TCP服务器 45
 - 2.10.3 Finger服务 45

<<网络安全Cisco解决方案>>

- 2.10.4 IP Unreachable报文 45
- 2.10.5 ICMP Redirect报文 47
- 2.10.6 定向广播 48
- 2.10.7 Proxy ARP 48
- 2.10.8 IP Verify 48
- 2.10.9 IP源路由 49
- 2.11 TCP截获 50
- 2.12 小结 52
 - 2.12.1 全局命令示例配置 53
 - 2.12.2 接口命令示例配置 54
 - 2.12.3 vty命令示例配置 54
- 第二部分 Cisco Secure 产品系列
- 第3章 Cisco安全性解决方案和产品系列概述 56
 - 3.1 Cisco安全性解决方案 56
 - 3.1.1 标识 57
 - 3.1.2 周边安全性 57
 - 3.1.3 安全连接性 58
 - 3.1.4 安全性监控 58
 - 3.1.5 安全性管理 59
 - 3.2 Cisco Secure产品系列 59
 - 3.2.1 Cisco Secure PIX防火墙 59
 - 3.2.2 Cisco IOS防火墙 60
 - 3.2.3 Cisco Secure IDS 61
 - 3.2.4 Cisco Secure Scanner 63
 - 3.2.5 Cisco Secure Policy Manager 65
 - 3.2.6 Cisco Secure Access Control Server 66
 - 3.3 小结 68
 - 3.4 常见问题 68
 - 3.5 词汇表 68
 - 3.6 参考书目 69
 - 3.7 网上资源 69
- 第4章 Cisco Secure PIX防火墙 70
 - 4.1 PIX产品型号 71
 - 4.1.1 PIX 506 71
 - 4.1.2 PIX 515 72
 - 4.1.3 PIX 520/525 73
 - 4.1.4 PIX 535 73
 - 4.2 PIX防火墙功能 74
 - 4.3 PIX配置 76
 - 4.3.1 基本配置 76
 - 4.3.2 实际的配置 82
 - 4.3.3 单个DMZ配置 87
 - 4.3.4 带AAA认证的双重DMZ 94
 - 4.4 通过PPTP实现的VPN 105
 - 4.4.1 ip local pool命令 106
 - 4.4.2 vpdn命令 106
 - 4.4.3 sysopt命令 108

<<网络安全Cisco解决方案>>

- 4.5 使用IPSec和手工密钥的VPN 108
 - 4.5.1 crypto map命令 110
 - 4.5.2 crypto ipsec命令 111
- 4.6 使用预共享密钥的VPN 113
 - 4.6.1 isakmp命令 114
 - 4.6.2 对使用预共享密钥的VPN的解释 114
- 4.7 获得证书授权机构证书 115
- 4.8 PIX到PIX的配置 116
 - 4.8.1 使用相同内部IP地址的PIX到PIX配置 118
- 4.9 小结 119
- 第5章 Cisco IOS防火墙 120
 - 5.1 访问列表 120
 - 5.2 动态访问列表 120
 - 5.3 基于时间的访问列表 123
 - 5.4 反射访问列表 124
 - 5.4.1 Null Route命令 128
 - 5.5 Cisco IOS防火墙特性 129
 - 5.5.1 端口应用程序映射 (PAM) 129
 - 5.6 CBAC如何工作 131
 - 5.6.1 CBAC工作方式 132
 - 5.6.2 CBAC事件发生顺序 134
 - 5.6.3 CBAC所支持的协议 134
 - 5.6.4 与Cisco加密技术 (CET) 以及IPSec的兼容性 135
 - 5.7 配置CBAC 136
 - 5.7.1 选择一个接口 136
 - 5.7.2 在接口上配置IP访问列表 137
 - 5.7.3 配置全局超时值和门限值 138
 - 5.7.4 定义检查规则 139
 - 5.7.5 配置记录和审核追踪 141
 - 5.7.6 CBAC配置示例 141
 - 5.8 小结 143
- 第6章 入侵检测系统 144
 - 6.1 入侵检测概述 144
 - 6.1.1 基于主机的入侵检测系统 145
 - 6.1.2 基于网络的入侵检测系统 146
 - 6.2 入侵检测系统 147
 - 6.3 Cisco Secure入侵检测系统 (CSIDS) 147
 - 6.3.1 CSIDS部件概述 148
 - 6.3.2 CSIDS感应器 149
 - 6.3.3 CSIDS邮局协议 153
 - 6.3.4 CSIDS管理器 154
 - 6.3.5 签名 156
 - 6.3.6 对警报进行响应 159
 - 6.3.7 截获日志 161
 - 6.4 Cisco IOS防火墙IDS 162
 - 6.5 Cisco Secure PIX防火墙IDS 163
 - 6.6 Cisco IDS配置 167

<<网络安全Cisco解决方案>>

- 6.6.1 Cisco IOS防火墙IDS配置 167
- 6.6.2 Cisco Secure PIX防火墙IDS配置 169
- 6.7 小结 172
- 6.8 常见问题 173
- 6.9 词汇表 173
- 第7章 Cisco Secure Scanner 174
 - 7.1 Cisco Secure Scanner的功能 175
 - 7.1.1 第1步：网络映射 175
 - 7.1.2 第2步：数据收集 178
 - 7.1.3 第3步：数据分析 180
 - 7.1.4 第4步：安全性弱点确认 180
 - 7.1.5 第5步：数据表达和导航 182
 - 7.1.6 第6步：报告 186
 - 7.2 Cisco Secure Scanner安装 187
 - 7.3 Cisco Secure Scanner的配置 187
 - 7.3.1 第1步：运行Cisco Secure Scanner 187
 - 7.3.2 第2步：创建一个会话来捕获数据 188
 - 7.3.3 第3步：截获所收集的数据 191
 - 7.3.4 第4步：对所收集的数据进行报告 192
 - 7.4 小结 192
 - 7.5 常见问题 193
 - 7.6 词汇表 193
 - 7.7 URL 193
- 第8章 Cisco Secure Policy Manager (CSPM) 194
 - 8.1 CSPM的功能 194
 - 8.2 CSPM的安装 196
 - 8.2.1 硬件需求 196
 - 8.2.2 软件需求 197
 - 8.2.3 规划安装 197
 - 8.2.4 安装过程 202
 - 8.3 配置示例 206
 - 8.3.1 配置网络拓扑 207
 - 8.3.2 配置安全性策略 219
 - 8.3.3 生成并发布和特定设备相关的命令集 221
 - 8.4 小结 223
 - 8.5 常见问题 223
 - 8.6 词汇表 223
 - 8.7 URL 224
- 第9章 Cisco Secure ACS 225
 - 9.1 Cisco Secure ACS的功能 225
 - 9.2 认证、授权和记账 (AAA) 概述 226
 - 9.2.1 认证 227
 - 9.2.2 授权 227
 - 9.2.3 记账 227
 - 9.3 RADIUS和TACACS+ 228
 - 9.3.1 RADIUS 229
 - 9.3.2 TACACS+ 229

<<网络安全Cisco解决方案>>

- 9.3.3 RADIUS和TACACS+之间的差异 230
 - 9.4 Cisco Secure ACS的安装 231
 - 9.4.1 Windows NT和Windows 2000版本的安装 231
 - 9.4.2 UNIX版本的安装 232
 - 9.5 Cisco Secure ACS的配置 233
 - 9.5.1 基于Web的配置和ACS Admin站点 233
 - 9.5.2 User Setup和Group Setup配置选项 234
 - 9.5.3 Network Configuration配置选项 236
 - 9.5.4 System Configuration配置选项 238
 - 9.5.5 Interface Configuration配置选项 240
 - 9.5.6 Administration Control配置选项 241
 - 9.5.7 External User Databases配置选项 243
 - 9.5.8 Reports and Activity配置选项 245
 - 9.5.9 Online Documentation配置选项 247
 - 9.6 网络访问服务器的配置 248
 - 9.6.1 AAA配置概述 248
 - 9.7 配置示例 253
 - 9.7.1 案例假设 253
 - 9.7.2 技术方面 253
 - 9.7.3 潜在的风险 254
 - 9.7.4 配置 254
 - 9.7.5 ACS服务器的配置 254
 - 9.7.6 NAS配置 255
 - 9.7.7 认证配置 256
 - 9.7.8 授权配置 257
 - 9.7.9 记账配置 258
 - 9.8 小结 259
 - 9.9 常见问题 259
 - 9.10 词汇表 259
 - 9.11 书目 260
 - 9.12 URL 260
- 第三部分 因特网安全性环境
- 第10章 保护企业网的安全 262
- 10.1 拨号连接的安全性 262
 - 10.2 拨号用户认证、授权和记账 (AAA) 264
 - 10.3 使用TACACS+和RADIUS的AAA认证设置 266
 - 10.3.1 初始配置 267
 - 10.3.2 创建一个方法列表 268
 - 10.3.3 将列表应用到接口 270
 - 10.3.4 调整配置 271
 - 10.4 AAA授权设置 272
 - 10.5 AAA记账设置 273
 - 10.6 同时使用所有的AAA服务 274
 - 10.7 虚拟专用网 (VPN) 275
 - 10.7.1 L2F 275
 - 10.7.2 L2TP 276
 - 10.7.3 GRE隧道 276

<<网络安全Cisco解决方案>>

- 10.7.4 加密 276
- 10.7.5 IPSec配置 276
- 10.8 小结 278
- 第11章 提供到因特网的安全访问 279
- 11.1 因特网服务 280
- 11.2 要常见的因特网安全性威胁 280
 - 11.2.1 网络入侵 281
 - 11.2.2 拒绝服务 (DoS) 攻击 282
- 11.3 因特网服务安全性示例 284
 - 11.3.1 在因特网服务安全性示例中的最初问题和威胁 284
 - 11.3.2 对因特网服务安全性示例的建议修改 286
 - 11.3.3 在因特网服务安全性示例修改后的问题和威胁 289
- 11.4 Web服务 290
 - 11.4.1 针对Web服务器的威胁 290
 - 11.4.2 针对Web服务器所受威胁的解决方案 290
 - 11.4.3 针对Web服务器的配置建议 291
- 11.5 文件传输协议 (FTP) 服务 291
 - 11.5.1 针对FTP服务器的威胁 291
 - 11.5.2 针对FTP服务器所受威胁的解决方案 292
 - 11.5.3 针对FTP服务器的配置建议 292
- 11.6 因特网电子邮件服务器 (SMTP/POP3/IMAP4) 292
 - 11.6.1 针对因特网电子邮件服务器的威胁 293
 - 11.6.2 针对因特网电子邮件服务器所受威胁的解决方案 294
 - 11.6.3 针对因特网电子邮件服务器的配置推荐 294
- 11.7 域名系统 (DNS) 服务器 294
 - 11.7.1 针对DNS服务器的威胁 295
 - 11.7.2 针对DNS服务器所受威胁的解决方案 295
 - 11.7.3 针对DNS服务器的配置建议 295
- 11.8 后端服务器 295
 - 11.8.1 针对后端服务器的威胁 296
 - 11.8.2 针对后端服务器所受威胁的解决方案 296
- 11.9 小结 296
- 11.10 常见问题 297
- 11.11 词汇表 297
- 第四部分 附录
- 附录A Cisco SAFE : 针对企业网的安全性蓝图 300
 - A.1 本附录的作者 300
 - A.2 概述 300
 - A.3 本附录的读者 301
 - A.4 忠告 301
 - A.5 体系结构概述 302
 - A.6 模块概念 302
 - A.7 企业模块 309
 - A.8 企业网园区模块 309
 - A.9 企业网边缘模块 320
 - A.10 移植策略 334
 - A.11 附件A : 确认实验室 335

<<网络安全Cisco解决方案>>

- A.12 附件B：网络安全性入门 352
- A.13 附件C：体系结构分类学 359
- A.14 RFC 360
- A.15 其他参考 361
- A.16 其他公司产品参考 361
- A.17 致谢 362

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>