

编著：
[美] Cisco公司
译：
信达工作室



CISCO IOS

网络安全

CISCO IOS

NETWORK SECURITY

Documentation from the
Cisco IOS™ Reference Library

人民邮电出版社
www.pptph.com.cn

CISCO SYSTEMS

CISCO PRESS
www.ciscopress.com

Cisco IOS 网络安全

[美] Cisco 公司 编著

信达工作室 译

人民邮电出版社

Cisco IOS 网络安全

- ◆ 编 著 [美] Cisco 公司
译 信达工作室
责任编辑 俞 彬

- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@pptph.com.cn
网址 <http://www.pptph.com.cn>
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

- ◆ 开本:787×1092 1/16
印张:28.75
字数:707千字 2001年1月第1版
印数:1-5 000册 2001年1月北京第1次印刷

著作权合同登记 图字:01-2000-2852号

ISBN 7-115-09036-X/TP·2007

定价:52.00元

内 容 提 要

本书全面介绍了在 Cisco 网络设备上如何配置 Cisco IOS 安全特性，以确保网络安全的方法、技巧和命令。全书包括五部分：身份认证、授权和统计，安全服务器协议，流量过滤，网络数据加密以及其他安全特性。第一部分详细介绍了配置身份认证、授权和统计的方法以及命令；第二部分讲述了配置 RADIUS、TACACS+、TACACS、扩展 TACACS 以及 Kerberos 的方法和命令；第三部分讨论了配置动态访问列表、反射访问列表和 TCP 截取的方法和命令；第四部分详细介绍了配置网络数据加密的方法和命令；第五部分介绍了配置口令、权限、IP 安全选项的方法以及使用的命令。

本书内容丰富，阐述详细，可作为网络管理人员的参考书或相关领域的培训教材。

版权声明

Cisco Systems, Inc: Cisco IOS Network Security
Authorized translation from English language edition published
by Cisco Press.

Copyright © 1998 by Cisco Press.

All rights reserved. For sale in Mainland China only.

本书中文简体字版由美国 Cisco Press 出版公司授权人民邮电出版社出版。未经出版者书面许可，对书的任何部分不得以任何方式复制或抄袭。

版权所有，侵权必究。

目 录

第 1 章 安全性概述	1
1.1 本书内容简介	1
1.1.1 身份认证、授权和统计	2
1.1.2 安全服务器协议	2
1.1.3 数据流过滤	3
1.1.4 网络数据加密	3
1.1.5 其他安全特性	3
1.2 创建有效的安全策略	4
1.2.1 安全策略的性质	4
1.2.2 安全策略的两个级别	5
1.2.3 开发有效的安全策略的技巧	5
1.3 认识安全危险和 Cisco IOS 解决方案	7
1.3.1 防止对网络设备的未经授权的访问	8
1.3.2 防止对网络的未经授权的访问	9
1.3.3 防止网络数据窃听	9
1.3.4 防止欺骗性路由更新	10
1.4 使用 Cisco IOS 软件创建防火墙	10
1.4.1 防火墙概述	10
1.4.2 创建防火墙	11
1.4.3 配置防火墙的其他指导原则	11
第一部分 身份认证、授权和统计 (AAA)	
第 2 章 AAA 概述	15
2.1 AAA 安全服务	15
2.1.1 使用 AAA 的益处	16
2.1.2 AAA 基本原理	16

2.1.3 方法列表	17
2.2 从何处开始	18
2.2.1 AAA 配置过程概述	18
2.2.2 启用 AAA	18
2.2.3 停用 AAA	18
2.3 下一步工作	19
第 3 章 配置认证	21
3.1 AAA 身份认证方法列表	21
3.1.1 方法列表举例	22
3.1.2 配置 AAA 身份认证的通用步骤	23
3.2 AAA 身份认证方法	23
3.2.1 使用 AAA 配置登录身份认证	23
3.2.2 使用 AAA 配置 PPP 身份认证	26
3.2.3 使用 AAA 配置 ARA 身份认证	28
3.2.4 使用 AAA 配置 NASI 身份认证	30
3.2.5 启用特权级口令保护	32
3.2.6 启用身份认证覆盖 (override)	32
3.2.7 启用双重身份认证	33
3.3 非 AAA 身份认证方法	35
3.3.1 配置线路口令保护	35
3.3.2 建立用户名身份认证	36
3.3.3 启用 CHAP 或 PAP 身份认证	36
3.3.4 配置 TACACS 和扩展 TACACS 口令保护	40
3.4 身份认证示例	40
3.4.1 RADIUS 身份认证示例	41
3.4.2 TACACS+ 身份认证示例	42
3.4.3 TACACS 和扩展 TACACS 身份认证示例	43
3.4.4 Kerberos 身份认证示例	43
3.4.5 双重身份认证配置示例	43
第 4 章 身份认证命令	51
4.1 aaa authentication arap	51
4.2 aaa authentication enable default	53
4.3 aaa authentication local-override	54
4.4 aaa authentication login	55
4.5 aaa authentication nasi	57
4.6 aaa authentication password-prompt	58
4.7 aaa authentication ppp	59
4.8 aaa authentication username-prompt	60

4.9	aaa new-model	61
4.10	access-profile	62
4.11	arap authentication	65
4.12	login authentication	66
4.13	login tacacs	67
4.14	nasi authentication	67
4.15	ppp authentication	68
4.16	ppp chap hostname	70
4.17	ppp chap password	71
4.18	ppp chap refuse	72
4.19	ppp chap wait	73
4.20	ppp pap sent-username	74
4.21	ppp use-tacacs	75
第 5 章	配置授权	77
5.1	AAA 授权类型	77
5.2	AAA 授权方法	78
5.3	AAA 授权前的准备工作	78
5.4	AAA 授权配置任务列表	78
5.5	配置授权	79
5.6	关闭全局配置命令授权	80
5.7	授权属性-值对 (Attribute-Value Pair)	80
5.8	授权配置示例	80
5.8.1	TACACS+ 授权示例	81
5.8.2	RADIUS 授权示例	81
5.8.3	Kerberos 实例映射示例	82
第 6 章	授权命令	83
6.1	aaa authorization	83
6.2	aaa authorization config-commands	85
6.3	aaa new-model	86
第 7 章	配置统计	89
7.1	AAA 统计类型	89
7.1.1	网络统计	90
7.1.2	连接统计	93
7.1.3	EXEC 统计	95
7.1.4	系统统计	97
7.1.5	命令统计	98
7.2	AAA 统计的准备工作	98

7.3	AAA 统计配置任务列表	98
7.4	启用 AAA 统计	99
7.4.1	禁止为用户名字符串为空的用户会话生成统计记录	99
7.4.2	生成临时统计记录	99
7.5	监视统计	100
7.6	统计属性-值对	100
7.7	统计配置示例	100
第 8 章	统计命令	103
8.1	aaa accounting	103
8.2	aaa accounting suppress null-username	105
8.3	aaa accounting update	105
8.4	show accounting	106
第二部分 安全服务器协议		
第 9 章	配置 RADIUS	111
9.1	RADIUS 概述	111
9.2	RADIUS 操作	112
9.3	RADIUS 配置任务列表	113
9.4	为 RADIUS 服务器通信配置路由器	113
9.5	为厂商专用的 RADIUS 服务器通信配置路由器	114
9.6	配置路由器以便向 RADIUS 服务器 查询静态路由和 IP 地址	115
9.7	指定 RADIUS 身份验证	115
9.8	指定 RADIUS 授权	115
9.9	指定 RADIUS 统计	115
9.10	RADIUS 属性	116
9.11	厂商专用的 RADIUS 属性	116
9.12	RADIUS 配置示例	116
9.12.1	RADIUS 身份验证和授权示例	116
9.12.2	RADIUS AAA 示例	117
9.12.3	厂商专用的 RADIUS 配置示例	118
第 10 章	RADIUS 命令	119
10.1	ip radius source-interface	119
10.2	radius-server configure-nas	120
10.3	radius-server dead-time	121
10.4	radius-server host	122
10.5	radius-server host non-standard	123
10.6	radius-server key	124

10.7	radius-server retransmit	125
10.8	radius-server timeout	125
第 11 章	配置 TACACS+	127
11.1	TACACS+概述	127
11.2	TACACS+操作	128
11.3	TACACS+配置任务列表	129
11.4	指定 TACACS+服务器主机	130
11.5	设置 TACACS+身份验证密匙	131
11.6	指定 TACACS+身份验证	131
11.7	指定 TACACS+授权	131
11.8	指定 TACACS+统计	131
11.9	TACACS+ AV 对	132
11.10	TACACS+配置示例	132
11.10.1	TACACS+身份验证示例	132
11.10.2	TACACS+授权示例	134
11.10.3	TACACS+统计示例	134
11.10.4	TACACS+后台程序配置示例	135
第 12 章	配置 TACACS 和扩展 TACACS	137
12.1	TACACS 协议描述	137
12.2	TACACS 和扩展 TACACS 配置任务列表	139
12.3	设置用户级 TACACS 口令保护	139
12.4	关闭用户级口令核查	140
12.5	设置可选的口令验证	140
12.6	设置特权级 TACACS 口令保护	140
12.7	关闭特权级口令核查	141
12.8	设置用户操作通知	141
12.9	设置用户操作身份验证	142
12.10	建立 TACACS 服务器主机	142
12.11	限制尝试登录的次数	142
12.12	指定登录输入时间	143
12.13	启用扩展 TACACS 模式	143
12.14	为 PPP 身份验证启用扩展 TACACS	143
12.15	为 ARA 身份验证启用标准 TACACS	144
12.16	为 ARA 身份验证启用扩展 TACACS	144
12.17	启用 TACACS, 以使用特定的 IP 地址	145
12.18	TACACS 配置示例	145

第 13 章 TACACS、扩展 TACACS 和 TACACS+命令	149
13.1 TACACS 命令比较	149
13.2 arap use-tacacs	150
13.3 enable last-resort	152
13.4 enable use-tacacs	152
13.5 ip tacacs source-interface	153
13.6 tacacs-server attempts	154
13.7 tacacs-server authenticate	155
13.8 tacacs-server directed-request	156
13.9 tacacs-server extended	156
13.10 tacacs-server host	157
13.11 tacacs-server key	158
13.12 tacacs-server last-resort	159
13.13 tacacs-server login-timeout	160
13.14 tacacs-server notify	161
13.15 tacacs-server optional-passwords	161
13.16 tacacs-server retransmit	162
13.17 tacacs-server timeout	163
第 14 章 配置 Kerberos	165
14.1 Kerberos 概述	165
14.2 Kerberos 客户支持操作	166
14.2.1 向边界路由器证明身份	167
14.2.2 从 KDC 取得 TGT	167
14.2.3 向网络服务证明身份	168
14.3 Kerberos 配置任务列表	168
14.4 使用 Kerberos 命令配置 KDC	169
14.4.1 将用户加入到 KDC 数据库中	169
14.4.2 在 KDC 中创建 SRVTAB	170
14.4.3 提取 SRVTAB	170
14.5 配置路由器, 使之使用 Kerberos 协议	170
14.5.1 定义 Kerberos 域	171
14.5.2 复制 SRVTAB 文件	172
14.5.3 指定 Kerberos 身份验证	172
14.5.4 启用证书转发功能	172
14.5.5 用 Telnet 登录到路由器	173
14.5.6 建立加密的 Kerberized Telnet 会话	173
14.5.7 启用强制性 Kerberos 身份验证	174
14.5.8 启用 Kerberos 实例映射	174

14.6	监视并维护 Kerberos	175
14.7	Kerberos 配置示例	175
14.7.1	定义 Kerberos 域示例	175
14.7.2	复制 SRVTAB 文件示例	175
14.7.3	Kerberos 配置示例	175
14.7.4	指定加密 Telnet 会话示例	189
第 15 章	Kerberos 命令	191
15.1	clear kerberos creds	191
15.2	connect	192
15.3	kerberos clients mandatory	195
15.4	kerberos credentials forward	195
15.5	kerberos instance map	196
15.6	kerberos local-realm	197
15.7	kerberos preauth	198
15.8	kerberos realm	199
15.9	kerberos server	200
15.10	kerberos srvtab entry	200
15.11	kerberos srvtab remote	202
15.12	key config-key	202
15.13	show kerberos creds	203
15.14	telnet	204

第三部分 数据流过滤

第 16 章	访问控制列表：概述和指南	211
16.1	本章内容	211
16.2	关于访问控制列表	211
16.2.1	访问列表的功能	212
16.2.2	为什么要配置访问列表	212
16.2.3	何时配置访问列表	212
16.2.4	基本访问控制列表与高级访问控制列表	213
16.3	访问列表配置概述	213
16.3.1	创建访问列表	213
16.3.2	给每个访问列表指定一个唯一的名称或编号	214
16.3.3	定义转发包或阻断分组的准则	215
16.3.4	在 TFTP 服务器上创建和编辑访问列表语句	215
16.3.5	将访问列表用于接口	216
16.4	查找访问列表的完整配置和命令信息	216

第 17 章 配置锁定和密钥安全性（动态访问列表）	217
17.1 本章内容	217
17.2 关于锁定和密钥	217
17.2.1 锁定和密钥优点	218
17.2.2 何时使用锁定和密钥	218
17.2.3 锁定和密钥的工作原理	218
17.3 Cisco IOS Release 11.1 与早期版本的兼容性	219
17.4 电子欺骗对锁定和密钥的威胁	219
17.5 锁定和密钥对路由器性能的影响	220
17.6 配置锁定和密钥前的准备工作	220
17.7 配置锁定和密钥	220
17.7.1 锁定和密钥配置的注意事项	221
17.8 验证锁定和密钥配置	222
17.9 锁定和密钥的维护	223
17.9.1 显示动态访问列表条目	223
17.9.2 手工删除动态访问列表条目	223
17.10 锁定和密钥配置示例	224
17.10.1 使用本地身份验证的锁定和密钥示例	224
17.10.2 使用 TACACS+ 身份验证的锁定和密钥示例	224
第 18 章 锁定和密钥命令	227
18.1 access-enable	227
18.2 access-template	228
18.3 clear access-template	229
18.4 show ip accounting	230
第 19 章 配置 IP 会话过滤（反射访问列表）	233
19.1 本章的内容	233
19.2 关于反射访问列表	233
19.2.1 反射访问列表的优点	234
19.2.2 什么是反射访问列表	234
19.2.3 反射访问列表如何实现会话过滤	234
19.2.4 在何处配置反射访问列表	235
19.2.5 反射访问列表的工作原理	235
19.2.6 使用反射访问列表的限制	236
19.3 配置反射访问列表前的准备工作	236
19.3.1 选择内部接口还是外部接口	236
19.4 配置反射访问列表	237
19.4.1 外部接口配置任务列表	237

19.4.2	内部接口配置任务列表	237
19.4.3	定义反射访问列表	238
19.4.4	嵌套反射访问列表	239
19.4.5	设置全局超时值 (可选)	239
19.5	反射访问列表配置示例	240
19.5.1	外部接口配置示例	240
19.5.2	内部接口配置示例	242
第 20 章	反射访问列表命令	243
20.1	evaluate	243
20.2	ip reflexive-list timeout	244
20.3	permit (reflexive)	245
第 21 章	配置 TCP 截取 (防止拒绝服务攻击)	249
21.1	本章内容	249
21.2	关于 TCP 截取	249
21.3	TCP 截取配置任务列表	250
21.4	启用 TCP 截取	250
21.5	设置 TCP 截取模式	251
21.6	设置 TCP 截取删除模式	251
21.7	更改 TCP 截取定时器	251
21.8	更改 TCP 截取主动阈值	252
21.9	监视和维护 TCP 截取	253
21.10	TCP 截取配置范例	253
第 22 章	TCP 截取命令	255
22.1	ip tcp intercept connection-timeout	255
22.2	ip tcp intercept drop-mode	256
22.3	ip tcp intercept finrst-timeout	257
22.4	ip tcp intercept list	257
22.5	ip tcp intercept max-incomplete high	258
22.6	ip tcp intercept max-incomplete low	259
22.7	ip tcp intercept mode	260
22.8	ip tcp intercept one-minute high	261
22.9	ip tcp intercept one-minute low	262
22.10	ip tcp intercept watch-timeout	263
22.11	show tcp intercept connections	264
22.12	show tcp intercept statistics	265

第四部分 网络数据加密

第 23 章 配置网络数据加密	269
23.1 为什么要加密	269
23.2 Cisco 的加密实现	270
23.2.1 什么被加密了	270
23.2.2 分组在网络的什么地方被加密和解密	270
23.2.3 加密分组何时被交换	271
23.2.4 加密路由器如何识别其他对等加密路由器	271
23.2.5 Cisco 加密实现了哪些标准	271
23.2.6 Cisco 加密如何工作	271
23.3 配置加密前的准备工作	274
23.3.1 确定对等路由器	274
23.3.2 考虑网络拓扑结构	275
23.3.3 确定每个对等路由器中的加密引擎	275
23.3.4 理解实现要点和局限性	276
23.4 配置加密	277
23.4.1 生成 DSS 公钥/私钥	277
23.4.2 交换 DSS 公钥	278
23.4.3 启用 DES 加密算法	279
23.4.4 定义加密映射表, 并将它们指定给接口	281
23.4.5 备份配置	283
23.5 GRE 隧道加密配置	283
23.5.1 只对 GRE 隧道通信进行加密	283
23.5.2 对 GRE 隧道通信和其他通信都进行加密	283
23.6 VIP2 中 ESA 加密配置	284
23.6.1 重置 ESA	284
23.6.2 执行其他的加密配置	285
23.7 对 Cisco 7200 系列路由器上的 ESA 进行加密配置	286
23.7.1 必须完成的任务	286
23.7.2 可选任务	286
23.7.3 重置 ESA	286
23.7.4 执行其他加密配置	287
23.7.5 启用 ESA	288
23.7.6 选择加密引擎	288
23.7.7 删除 DSS 密钥	289
23.8 定制加密 (配置选项)	290
23.8.1 定义加密会话的持续时间	290
23.8.2 通过预先生成 DH 编号缩短会话的建立时间	290

23.8.3 修改加密访问列表的限制	291
23.9 关闭加密	292
23.10 加密测试和故障排除	292
23.10.1 测试加密配置	293
23.10.2 诊断连接故障	293
23.10.3 使用调试命令	295
23.11 加密配置示例	295
23.11.1 生成 DSS 公钥/私钥示例	296
23.11.2 交换 DSS 密钥示例	296
23.11.3 启用 DES 加密算法示例	298
23.11.4 建立加密访问列表、定义加密映射表并将它用于接口的示例	299
23.11.5 修改加密访问列表限制示例	303
23.11.6 GRE 隧道加密配置示例	304
23.11.7 ESA 特有加密配置任务示例	306
23.11.8 删除 DSS 密钥示例	308
23.11.9 测试加密连接示例	311
第 24 章 网络数据加密命令	313
24.1 access-list (encryption)	313
24.2 clear crypto connection	320
24.3 crypto algorithm 40-bit-des	321
24.4 crypto algorithm des	323
24.5 crypto clear-latch	324
24.6 crypto esa	325
24.7 crypto gen-signature-keys	326
24.8 crypto key-exchange	328
24.9 crypto key-exchange passive	330
24.10 crypto key-timeout	331
24.11 crypto map(global configuration)	332
24.12 crypto map(interface configuration)	334
24.13 crypto pregen-dh-pairs	335
24.14 crypto public-key	336
24.15 crypto sdu connections	337
24.16 crypto sdu entities	339
24.17 crypto zeroize	341
24.18 deny	342
24.19 ip access-list extended(encryption)	346
24.20 match address	347
24.21 permit	348
24.22 set algorithm 40-bit-des	353

24.23	set algorithm des	354
24.24	set peer	355
24.25	show crypto algorithms	355
24.26	show crypto card	356
24.27	show crypto connections	357
24.28	show crypto engine brief	358
24.29	show crypto engine configuration	359
24.30	show crypto engine connections active	361
24.31	show crypto engine connections dropped-packets	362
24.32	show crypto key-timeout	363
24.33	show crypto map	363
24.34	show crypto map interface	366
24.35	show crypto map tag	367
24.36	show crypto mypubkey	369
24.37	show crypto pregen-dh-pairs	369
24.38	show crypto pubkey	370
24.39	show crypto pubkey name	371
24.40	show crypto pubkey serial	372
24.41	test crypto initiate-session	373

第五部分 其他安全特性

第 25 章	配置口令和权限	377
25.1	保护对特权 EXEC 命令的访问	377
25.1.1	设置或修改静态有效口令	377
25.1.2	使用有效口令和有效密钥保护口令	378
25.1.3	设置或修改线路口令	378
25.1.4	为特权 EXEC 模式设置 TACACS 口令保护	379
25.2	加密口令	379
25.3	配置多重权限级别	380
25.3.1	设置命令的权限级别	380
25.3.2	修改线路的默认权限级别	380
25.3.3	显示当前的权限级别	380
25.3.4	登录到某个权限级别	381
25.4	恢复丢失的有效口令	381
25.4.1	恢复口令的步骤	382
25.4.2	第一种口令恢复方法	382
25.4.3	第二种口令恢复方法	383
25.5	恢复丢失的线路口令	385
25.6	配置标识支持	386