21 BEIJING HOPE

21世纪网络工程师设计宝典丛书 2

Cisco Network Security

网络核心技术内幕

Cisco 网络安全解决方案

上册

本书配套光盘内容包括：
与本书配套的电子书

〔美〕 Cisco Systems公司 著
希望图书创作室 译

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

21世纪网络工程师设计宝典丛书 2

Cisco Network Security

网络核心技术内幕

Cisco 网络安全解决方案

上册

本书配套光盘内容包括
与本书配套的电子书

〔美〕 Cisco Systems公司 著
希望图书创作室 译

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn
2000

21 世纪网络工程师设计宝典丛书 2

Cisco Network Security

网络核心技术内幕

Cisco 网络安全解决方案

下册

本书配套光盘内容包括：
与本书配套的电子书

〔美〕 Cisco Systems公司 著
希望图书创作室 译

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn
2000

内 容 提 要

本书是 21 世纪网络工程师设计宝典系列之一，全面介绍了如何针对 Cisco 网络设备配置 Cisco IOS 安全特性。通过 Cisco IOS 安全特性的配置，使我们的网络能够避免有意和无意的攻击，避免由于合法用户的误操作造成的数据丢失或泄露，从而保护网络系统的安全。全书共分六部分：认证、授权及记帐（AAA）、安全服务器协议、流量过滤和防火墙、IP 安全和加密技术、其它安全特性和附录。认证提供了识别用户的方法，它在允许用户访问网络以及网络资源之前确认用户的身份；授权提供了远程访问控制的方法，它包括一次性授权和对每个服务进行授权；记帐提供了收集和发送帐单信息、审计信息以及报告信息的手段。安全服务器协议部分讲述了配置 RADIUS、Kerberos、TACACS+、TACACS 和扩展 TACACS 的方法、命令和过程。流量过滤和防火墙部分讲述了如何配置网络设备进行流量过滤以及如何把网络设备配置成精细入微的防火墙。IP 安全与加密部分讲述配置 Cisco 加密技术、配置 IPSec、配置证书认证机构（CA）的互操作能力以及配置 Internet 密钥交换的方法。其它安全特性部分讲述了进一步加强网络安全的其它技术与措施。

本书内容极为丰富，技术新、指导性和实用性强，不但是从事网络规划和设计的广大工程人员、系统分析人员和网管人员的重要学习指导书，同时也是高等院校相关专业师生重要的自学、教学参考用书和社会相关领域培训班教材。

本书配套光盘内容包括与本书配套的电子书。

版 权 声 明

系　列　书：21 世纪网络工程师设计宝典系列（2）
书　　名：网络核心技术内幕——Cisco 网络安全解决方案（上）
文本著作者：〔美〕Cisco Systems公司 著　希望图书创作室 译
责任编辑：周凤明
CD 制作者：希望多媒体开发中心
CD 测试者：希望多媒体测试部
出版、发行者：北京希望电子出版社
地　　址：北京海淀路 82 号，100080
网址: www.bhp.com.cn
E-mail: lwm@hope.com.cn
电话: 010-62562329,62541992,62637101,62637102,62633308,62633309
（发行和技术支持）
010-62613322-215（门市）　010-62531267（编辑部）
经　　销：各地新华书店、软件连锁店
排　　版：希望图书输出中心
CD 生 产 者：文录激光科技有限公司
文本印刷者：北京双青印刷厂
开本 / 规格：787×1092　16 开本　43.5 印张　861 千字
版次 / 印次：2000 年 2 月第 1 版　2000 年 2 月第 1 次印刷
印　　数：0001-5000 册
本 版 号：ISBN7-900031-71-5/TP・71
定　　价：78.00 元（1CD，含配套书，上下册）

内 容 提 要

本书是 21 世纪网络工程师设计宝典系列之一，全面介绍了如何针对 Cisco 网络设备配置 Cisco IOS 安全特性。通过 Cisco IOS 安全特性的配置，使我们的网络能够避免有意和无意的攻击，避免由于合法用户的误操作造成的数据丢失或泄露，从而保护网络系统的安全。全书共分六部分：认证、授权及记帐（AAA）、安全服务器协议、流量过滤和防火墙、IP 安全和加密技术、其它安全特性和附录。认证提供了识别用户的方法，它在允许用户访问网络以及网络资源之前确认用户的身份；授权提供了远程访问控制的方法，它包括一次性授权和对每个服务进行授权；记帐提供了收集和发送帐单信息、审计信息以及报告信息的手段。安全服务器协议部分讲述了配置 RADIUS、Kerberos、TACACS+、TACACS 和扩展 TACACS 的方法、命令和过程。流量过滤和防火墙部分讲述了如何配置网络设备进行流量过滤以及如何把网络设备配置成精细入微的防火墙。IP 安全与加密部分讲述配置 Cisco 加密技术、配置 IPSec、配置证书认证机构（CA）的互操作能力以及配置 Internet 密钥交换的方法。其它安全特性部分讲述了进一步加强网络安全的其它技术与措施。

本书内容极为丰富，技术新、指导性和实用性强，不但是从事网络规划和设计的广大工程人员、系统分析人员和网管人员的重要学习指导书，同时也是高等院校相关专业师生重要的自学、教学参考用书和社会相关领域培训班教材。

本书配套光盘内容包括与本书配套的电子书。

版 权 声 明

系　列　书：21 世纪网络工程师设计宝典系列（2）
书　　名：**网络核心技术内幕——Cisco 网络安全解决方案（下）**
文本著作者：（美）Cisco Systems公司 著　希望图书创作室 译
责任编辑：周凤明
CD 制作者：希望多媒体开发中心
CD 测试者：希望多媒体测试部
出版、发行者：北京希望电子出版社
地　　址：北京海淀路 82 号，100080
网址: www.bhp.com.cn
E-mail: lwm@hope.com.cn
电话: 010-62562329,62541992,62637101,62637102,62633308,62633309
（发行和技术支持）
010-62613322-215（门市）　010-62531267（编辑部）
经　　销：各地新华书店、软件连锁店
排　　版：希望图书输出中心
CD 生 产 者：文录激光科技有限公司
文本印刷者：北京双青印刷厂
开本 / 规格：787×1092　16 开本　43.5 印张　861 千字
版次 / 印次：2000 年 2 月第 1 版　2000 年 2 月第 1 次印刷
印　　数：0001-5000 册
本 版 号：ISBN7-900031-71-5/TP・71
定　　价：78.00 元（1CD，含配套书，上下册）
说明：凡我社光盘配套图书若有缺页、倒页、脱页、自然破损，本社负责调换。

译 者 序

网络的普及在给我们带来便利的同时也带来了安全隐患，互联网的广泛应用使这一矛盾更加尖锐，如何最大限度地保护网络资源和数据的安全已经成为网络管理员和各部门关注的重点。网络安全涉及面广，不同的部门、不同的信息有着不同的安全要求。利用现有设备增强网络的安全性是一项投资少、见效快的可行方案。

Cisco IOS 是 Cisco 公司出品的网际操作系统，这是一个与硬件分离的软件体系结构。随着网络技术的不断发展，它可以动态地升级，以适应不断变化的技术。除了网络管理和维护外，控制网络的访问、提供访问的安全性也是该软件的基本功能之一。本书全面介绍了通过配置 Cisco IOS 让网络更加安全的操作方法、配置步骤、配置命令以及命令的详细描述，同时指出了配置过程中应该注意的一些问题。

全书由六部分组成。第一部分介绍配置 Cisco 认证、授权以及记帐（AAA）的方法，这是验证用户身份、记录用户操作的三种手段；第二部分介绍配置下述安全服务器协议的方法、命令和过程：RADIUS、Kerberos、TACACS+、TACACS 和扩展 TACACS；第三部分介绍如何配置网络设备来完成流量过滤以及如何把网络设备配置成防火墙；第四部分介绍如何通过加密的方法配置 IP 的安全性，内容包括配置 Cisco 加密技术、配置 IPSec 网络安全、配置 Internet 密钥交换安全协议；第五部分介绍配置口令和特权、邻接路由器认证和配置 IP 安全选项；第六部分是本书的附录，它完整地介绍了 RADIUS 属性和 TACACS+属性值对。

本书由张长富、宋斌、黄石海、张建安、栾开春、马向群、刘民、陈玉婷等翻译，最后由张长富统稿。参加翻译、录入、材料整理与校对工作的还有：崔立模、陈聪、陈孟英、彭涛、李匀、黄中敏、张兵、龚楚奇、尹兰、郝晓伟、夏桂娟、王志宏、王锋、李鹰、王丰、冯桂林、欧阳志、苏春波、柴少飞、李林等。翻译过程中得到了享受政府特殊津贴的专家张福林先生的热情指导和帮助，在此深表感谢。由于译者水平所限，欢迎读者批评指正。

张长富

2000.1

致　谢

Cisco IOS 参考库（Cisco IOS Reference Library）是众多 Cisco 专业作家和编辑数年齐心协力的成果。随着 Cisco IOS 组网特性和功能的不断增加，这套丛书也在不断地发掘和集成展示这些特性和功能的用户文档。

目前 Cisco IOS 专业作家和编辑小组包括：Katherine Anderson、Hugh Bussell、Melanie Cheng、Christy Choate、Sue Cross、Meredith Fisher、Tina Fox、Sheryl Kelly、Marsha Kinnear、Doug MacBeth、Lavanya Mandavilli、Mary Mangone、Andy Mann、Bob Marburg、Greg McMillan、Madhu Mitra、Vicki Payne、Jeremy Pollock、Patricia Rohrs、Teresa Oliver Schick、Wink Schuetz、Grace Tai、Brian Taylor、Jamianne Von-Prudelle、Amanda Worthington。

编著小组对参与评审原稿，并在绝大多数情况下为本书编著提供原始材料的众多工程师、客户支持人员以及市场营销专家深表感谢。

目　录

（上）

引论：安全性概览 1
关于本书 1
建立有效的安全策略 4
识别网络风险以及 Cisco IOS 解决方案 7
关于 Cisco IOS 12.0 参考库 10
使用 Cisco IOS 软件 14

第一部分
认证　授权及记帐　AAA

第 1 章 AAA 概要 23
AAA 安全服务 23
从哪里开始 25
下面做什么 26
第 2 章　认证配置 27
AAA 认证方法列表 27
AAA 认证方法 29
非 AAA 认证方法 45
认证示例 51
第 3 章　认证命令 68
aaa authentication arap 68
aaa authentication banner 70
aaa authentication enable default 71
aaa authentication fail-message 72
aaa authentication local-override 74
aaa authentication login 75
aaa authentication nasi 76
aaa authentication password-prompt 78
aaa authentication ppp 79
aaa authentication username-prompt 80
aaa new-model 81
aaa processes 82
access-profile 83
arap authentication 86
clear ip trigger-authentication 87
ip trigger-authentication
(global configuration) 88
ip trigger-authentication
(interface configuration) 89
login authentication 90
login tacacs 91
nasi authentication 91
ppp authetication 92
ppp chap hostname 94
ppp chap password 95
ppp chap refuse 96
ppp chap wait 97
ppp pap sent-username 98
ppp use-tacacs 99
show ip trigger-authentication 100
show ppp queues 101
timeout login response 103
第 4 章　授权配置 104
AAA 授权类型 104
授权的命名方法列表 104
AAA 授权方法 106
AAA 授权先决条件 106
AAA 授权配置 106

授权配置 107
使用命名方法列表配置 AAA 授权 108
关闭全局配置命令授权 109
反向 Telnet 授权 110
授权属性值对（Attribute-Value Pair） 110
授权配置示例 111
第 5 章 授权命令 116
aaa authorization 116
aaa authorization config-commands 119
aaa authorization reverse-access 120
aaa new-model 123
authorization 123
ppp authorization 125
第 6 章 记帐配置 126
记帐的命名方法列表 126
AAA 记帐类型 127
AAA 记帐先决条件 133
AAA 记帐配置任务列表 133
使用命名方法列表配置 AAA 记帐 134
开放记帐 135
监督记帐 136
记帐属性值对（Attribute-Value Pair） 136
记帐配置示例 136
第 7 章 记帐命令 139
aaa accounting 139
aaa accounting suppress null-username 142
aaa accounting update 142
accounting 144
ppp accounting 145
show accounting 146

第二部分 安全服务器协议

第 8 章 配置 RADIUS 151
RADIUS 概览 151
RADIUS 操作 152
RADIUS 配置任务表 153
第 9 章 RADIUS 命令 160
aaa nas-port extended 160
ip radius source-interface 161
radius-server attribute nas-port extended 162
radius-server configure-nas 163
radius-server dead-time 164
radius-server extended-portnames 164
radius-server host 165
radius-server host non-standard 166
radius-server optional passwords 167
radius-server key 168
radius-server retransmit 169
radius-server timeout 169
radius-server vsa send 170
第 10 章 配置 TACACS+ 172
TACACS+概览 172
TACACS+操作 173
TACACS+配置任务列表 174
TACACS+配置示例 176
第 11 章 配置 TACACS 和扩展 TACACS . 181
TACACS 协议描述 181
TACACS 和扩展 TACACS 配置任务列表 .. 182
TACACS 配置示例 188
第 12 章 TACACS、扩展 TACACS 和 TACACS+命令 190
TACACS 命令比较 190
arap use-tacacs 190
enable last-resort 191
enable use-tacacs 192
ip tacacs source-interface 193
tacacs-server attempts 194
tacacs-server authenticate 194
tacacs-server directed-request 195
tacacs-server extended 196
tacacs-server host 197
tacacs-server key 198
tacacs-server last-resort 199
tacacs-server login-timeout 200
tacacs-server notify 200
tacacs-server optional-passwords 201
tacacs-server retransmit 202

tacacs-server timeout 202
第 13 章 配置 Kerberos 204
Kerberos 概览 204
Kerberos 客户机支持的操作 206
Kerberos 配置任务列表 207
Kerberos 配置示例 213
第 14 章 kerberos 命令 225
clear kerberos creds 225
connect 226
kerberos clients mandatory 228
kerberos credentials forward 229
kerberos instance map 230
kerberos local-realm 231
kerberos preauth 232
kerberos realm 233
kerberos server 233
kerberos srvtab entry 234
kerberos srvtab remote 236
key config-key 236
show kerberos creds 237
telnet 238

第三部分 流量过滤与防火墙

第 15 章 访问控制列表：概述与指导 . 245
关于访问控制列表 245
访问列表配置概述 247
查找访问列表的完整配置和命令信息 249
第 16 章 Cisco IOS 防火墙概述 250
防火墙概述 250
Cisco IOS 防火墙解决方案 250
创建专用的防火墙 251
配制防火墙的其它指导原则 253
第 17 章 配置锁定和密钥的安全性（动态访问列表） 255
关于锁定和密钥 255
Cisco IOS 版本 11.1 与早期版本的兼容性 256
地址欺诈对锁定和密钥的威胁 257
使用锁定和密钥对路由器性能的影响 257
配置锁定和密钥的前提条件 258
配置锁定和密钥 258
检验锁定和密钥配置 260
锁定和密钥的维护 261
配置锁定和密钥示例 261
第 18 章 锁定和密钥命令 263
access-enable 263
access-template 264
clear access-template 265
show ip accounting 266
第 19 章 配置 IP 会话过滤（反射访问列表） 269
关于反射访问列表 269
配置反射访问列表前的准备工作 271
配置反射访问列表 272
配置反射访问列表示例 275
第 20 章 反射访问列表命令 279
evaluate 279
ip reflexive-list timeout 280
permit (reflexive) 281
第 21 章 配置 TCP 截取（防止拒绝服务攻击） 284
关于 TCP 截取 284
TCP 截取的配置任务列表 285
TCP 截取的配置范例 287
第 22 章 TCP 截取命令 288
ip tcp intercept connection-timeout 288
ip tcp intercept drop-mode 288
ip tcp intercept finrst-timeout 289
ip tcp intercept list 290
ip tcp intercept max-incomplete high 291
ip tcp intercept max-incomplete low 292
ip tcp intercept mode 293
ip tcp intercept one-minute high 294
ip tcp intercept one-minute low 295
ip tcp intercept watch-timeout 296
show tcp intercept connections 297
show tcp intercept statistics 298

第 23 章　配置基于上下文的访问控制 . 300
CBAC 概述 300
CBAC 配置的任务 305
CBAC 配置示例 316
第 24 章　基于上下文的访问控制命令 . 322
ip inspect audit trail 322
ip inspect dns-timeout 323
ip inspect (interface configuration) 324
ip inspect max-incomplete high 324
ip inspect max-incomplete low 326
ip inspect name (global cofiguration) 327
ip inspect one-minute high 331
ip inspect one-minute low 332
ip inspect tcp finwait-time 333
ip inspect tcp idle-time 334
ip inspect tcp max-incomplete host 335
ip inspect tcp synwait-time 336
ip inspect udp idle-time 337
no ip inspect 338
show ip inspect 338

目　录

（下）

第四部分　IP安全和加密技术

第 25 章　IP 安全和加密技术概述 343

Cisco 加密技术 343
IPSec 网络安全性 343
Internet 密钥交换安全性协议 346
身份认证互操作性 346

第 26 章　配置 Cisco 加密技术 347

为什么要加密 347
Cisco 加密的实现 348
补充信息来源 352
准备工作：在配置加密之前 353
配置加密 356
GRE 隧道加密配置 363
VIP2 中 ESA 加密配置 364
对 Cisco 7200 系列路由器上的 ESA
进行加密配置 365
定制加密（配置选项） 369
关闭加密 371
加密测试和故障排除 371
加密配置示例 374

第 27 章　Cisco 加密技术命令 390

access-list（encryption） 390
clear crypto connection 396
crypto algorithm 40-bit-des 398
crypto algorithm des 398
crypto card 398
crypto card clear-latch 399
crypto cisco algorithm 40-bit-des 400
crypto cisco algorithm des 402
crypto cisco connections 403
crypto cisco entities 405
crypto cisco key-timeout 406
crypto cisco pregen-dh-pairs 407
crypto clear-latch 409
crypto esa 409
crypto gen-signature-keys 409
crypto key-exchange 409
crypto key exchange dss 409
crypto key exchange dss passive 411
crypto key-exchange passive 412
crypto key generate dss 412
crypto key pubkey-chain dss 415
crypto key-timeout 416
crypto key zeroize dss 417
crypto map(global configuraion) 418
crypto map(interface configuration) 421
crypto pregen-dh-pairs 422
crypto public-key 422
crypto sdu connections 422
crypto sdu entities 422
crypto zeroize 422
deny 422
ip access-list extended(encryption) 427
match address 428
permit 430
set algorithm 40-bit-des 434

set algorithm des 435
set peer 436
show crypto algorithms 437
show crypto card 437
show crypto cisco algorithms 438
show crypto cisco connections 439
show crypto cisco key-timeout 440
show crypto cisco pregen-dh-pairs 441
show crypto connections 442
show crypto engine brief 442
show crypto engine configuration 444
show crypto engine connections active 445
show crypto engine connections dropped-packets 447
show crypto key mypubkey dss 448
show crypto key pubkey-chain dss 448
show crypto key-timeout 450
show crypto map 450
show crypto mypubkey 452
show crypto pregen-dh-pairs 452
show crypto pubkey 453
show crypto pubkey name 453
show crypto pubkey serial 453
test crypto initiate-session 453
第 28 章 配置 IPSec 网络安全 456
IPSec 概述 456
IPSec 配置任务列表 461
IPSec 配置示例 476
第 29 章 IPSec 网络安全性命令 478
clear crypto sa 478
crypto dynamic-map 479
crypto ipsec security-association lifetime 482
crypto ipsec transform-set 484
crypto map（global configuration） 487
crypto map（interface configuration） 491
crypto map local-address 492
initialization-vector size 493
match address 494
mode 496
set peer 497
set pfs 499
set security-association level per-host 500
set security-association lifetime 501
set session-key 503
set transform-set 506
show crypto ipsec sa 507
show crypto ipsec security-association lifetime 510
show crypto ipsec transform-set 510
show crypto dynamic-map 511
show crypto map 512
第 30 章 配置身份认证互操作性 515
CA 互操作性概述 515
认证机构概述 516
CA 互操作性配置任务列表 519
下面要做什么 524
CA 互操作性配置示例 524
第 31 章 身份认证互操作性命令 528
certificate 528
crl optional 529
crypto ca authenticate 530
crypto ca certificate chain 531
crypto ca certificate query 532
crypto ca crl request 533
crypto ca enroll 534
crypto ca identity 536
crypto key generate rsa 538
crypto key zeroize rsa 540
enrollment mode ra 541
enrollment retry-count 542
enrollment retry-period 543
enrollment url 544
query url 545
show crypto ca certificates 546
第 32 章 配置 Internet 密钥交换安全协议 549
IKE 概要 549
IKE 配置任务列表 551

下面做什么 558
IKE 配置示例 559
第 33 章 Internet 密钥交换安全协议命令 560
address 560
addressed-key 561
authentication(IKE policy) 563
clear crypto isakmp 564
crypto isakmp enable 565
crypto isakmp identity 566
crypto isakmp key 567
crypto isakmp policy 569
crypto key generate rsa 571
crypto key pubkey-chain rsa 573
encryption(IKE policy) 574
group(IKE policy) 575
hash(IKE policy) 576
key-string 577
lifetime(IKE policy) 578
named-key 579
show crypto isakmp policy 581
show crypto isakmp sa 582
show crypto key mypubkey rsa 583
show crypto key pubkey-chain rsa 584
第五部分 其它安全特性
第 34 章 配置口令和特权 589
保护到特权 EXEC 命令的访问 589
加密口令 591
配置多重特权级别 591
恢复丢失的有效口令 592
恢复丢失的线路口令 597
配置标识支持 598
口令和特权配置示例 598
第 35 章 口令和特权命令 601
enable 601
enable password 602
enable secret 603
ip identd 605
password 606
privilege level (global) 607
privilege level (line) 608
service password-encryption 609
show privilege 610
username 611
第 36 章 邻接路由器认证：概要及方略 615
邻接认证的优点 615
使用邻接认证的协议 615
何时配置邻接认证 616
邻接认证工作原理 616
密钥管理（密钥链） 617
第 37 章 配置 IP 安全选项 618
配置基本 IP 安全选项 618
配置扩展 IP 安全选项 619
配置 DNSIX 审计跟踪功能 621
IPSO 配置示例 622
第 38 章 IP 安全选项命令 624
dnsix-dmdp retries 624
dnsix-nat authorized-redirection 625
dnsix-nat primary 625
dnsix-nat secondary 626
dnsix-nat source 626
dnsix-nat transmit-count 627
ip security add 628
ip security aeso 629
ip security dedicated 629
ip security eso-info 631
ip security eso-max 632
ip security eso-min 633
ip security extended-allowed 634
ip security first 635
ip security ignore-authorities 635
ip security implicit-labelling 636
ip security multilevel 637
ip security reserved-allowed 639
ip security strip 640
show dnsix 641

第六部分 附 录

附录 A RADIUS 属性 645
所支持的 RADIUS 属性 645
RADIUS 属性完整列表 651
附录 B TACACS+属性值对 670
TACACS+属性值（AV）对 670
TACACS+记帐属性值（AV）对 676

引论

安全性概览

该章包括下述各节：

- 关于本书——概要叙述本指南各主题。
- 建立有效的安全策略——学会为自己的组织机构建立安全策略的技巧和手段。安全策略应该最后确定，并且，在配置安全特性之前，安全策略应该是最新的安全策略。
- 识别安全风险和所采用的 Cisco 解决方案——找出网络中可能存在的共同风险，并使用 Cisco IOS 安全特性避免安全漏洞。

关于本书

本书讲述了如何为 Cisco 网络设备配置 Cisco IOS 安全特性。这些安全特性能够保护网络，避免网络退化或失效，避免来自有目的的攻击或合法用户的误操作而造成的数据丢失或泄密。

本指南由五部分组成：

- 认证、授权及记帐（AAA，Authentication、Authorization、Accounting）
- 安全服务器协议
- 流量过滤和防火墙
- IP 安全和加密技术
- 其它安全特性

下面概要叙述各部分的内容。

认证、授权及记帐（AAA）

本部分讲述如何配置 Cisco 认证、授权及记帐（AAA）范式。AAA 是一种以一致的、模块化方式配置三项独立安全功能的体系结构。

- 认证（Authentication）——认证提供了识别用户的方法，它包括登录和口令对话框、质询与回应、消息报告、以及根据所选择的安全协议而采用的加密方法。认证是在允许用户访问网络以及网络资源之前确认用户身份的方法。通过定义认证方法的命名列表，然后在各种接口中运用这一列表的方法配置 AAA 认证。
- 授权（Authorization）——授权提供了远程访问控制的方法，它包括一次性授权或对每个服务授权、每个用户的帐户列表以及个性配置、用户组支持以及 IP、IPX、ARA、Telnet 支持。

远程安全服务器——比如 RADIUS 或 TACACS+——通过分配一对相关的属性值（AV）对，向用户授予特定权限。属性值对（Attribute-Value Pairs）定义了相应用户的权限。AAA 授权通过把描述用户能够执行的权限的属性位组合起来的方法进行授权。这些属性与保存在数据库中的特定用户的权限信息相比较，结果返回给 AAA，以此确定用户的实际能力和限制。

- 记帐（Accounting）——记帐提供了收集和发送安全服务器信息的方法，这些信息包括帐单、审记以及报告等，比如用户身份、启动和停止时间、执行的命令（比如 PPP）、包的数量、字节数等。通过记帐我们可以跟踪用户访问的服务以及他们所耗用的网络资源数量。

注意 可以在 AAA 之外配置认证。但是，如果要使用 RADIUS、Kerberos 或 TACACS+，或者如果希望配置一种备份的认证方法，那么就必须配置 AAA。

安全服务器协议

在许多环境下，AAA 使用安全协议完成其安全功能。如果你的路由器或访问服务器作为网络访问服务器来使用，AAA 就是在网络访问服务器与 RADIUS、Kerberos 或 TACACS+安全服务器之间建立通讯的手段。

这一部分的各章介绍了如何配置下述安全服务器协议：

- RADIUS——这是一个分布式客户/服务器系统，它通过 AAA 实现安全网络，避免非授权访问。在 Cisco 的 RADIUS 实现中，RADIUS 的客户端运行在 Cisco 路由器上，并向包含所有用户认证和网络服务访问信息的中心 RADIUS 服务器发送认证请求。
- Kerberos——这是一个密钥网络认证协议，它通过使用数据加密标准（DES，Data Encryption Standard）加密算法进行加密和认证的 AAA 来实现。以前，Kerberos 设计用于认证对网络资源的请求。现在，Kerberos 基于完成用户和服务安全验证的可信任第三方的概念。Kerberos 的主要用途是验证用户和他们所使用的网络服务与其所声明的用户和服务相同。为完成这一任务，可信任 Kerberos 服务器向用户发放门票（Ticket）。这些门票具有有限的使用期限，它们被保存在用户的信任缓冲区中，并在需要使用标准的用户名-口令认证机制的场所使用。
- TACACS+ ——这是一个实现了 AAA 的安全应用程序，它提供了用户访问路由器或网络访问服务器时的集中化验证。TACACS+服务保存在运行 TACACS+守护程序的数据库中，典型情况下，它们在 UNIX 或 Windows NT 工作站上运行。TACACS+提供了独立的和模块化的 AAA 工具。
- TACACS 和扩展 TACACS——TACACS 是一种比较古老的访问协议，它与新型的 TACACS+协议不兼容。TACACS 协议提供了口令检查和认证，并提供了用于安全与记帐目的的用户动作通知。扩展 TACACS 是对古老的 TACACS 协议的扩充，它在 TACACS 协议的基础上提供了一些附加功能。