

Inhaltsverzeichnis

Netzwerksicherheit: Ein Überblick	23
Teil I: Routing Grundlagen	51
1 AAA: Ein Überblick	53
1.1 Die Sicherheitsdienste des AAA	53
1.1.1 Die Vorteile des AAA	55
1.1.2 Die Philosophie des AAA	55
1.1.3 Die Methodenlisten	56
1.2 Die ersten Schritte	56
1.2.1 Ein Überblick über den Konfigurationsprozess des AAA	56
1.2.2 Die Aktivierung des AAA	57
1.2.3 Die Deaktivierung des AAA	57
1.3 Die nächsten Schritte	58
2 Die Konfiguration der Authentifizierung	61
2.1 Die Methodenlisten der AAA-Authentifizierung	61
2.1.1 Beispiele zu Methodenlisten	62
2.1.2 Das allgemeine Konfigurationsverfahren für die AAA-Authentifizierung	64
2.2 Die AAA-Authentifizierungsmethoden	64
2.2.1 Die Konfiguration der Login-Authentifizierung unter AAA	65
2.2.2 Die Konfiguration der PPP-Authentifizierung unter AAA	69
2.2.3 Die Konfiguration der AAA Skalierbarkeit für PPP-Anfragen	72
2.2.4 Die Konfiguration der ARA-Authentifizierung unter AAA	73
2.2.5 Die Konfiguration der NASI-Authentifizierung unter AAA	76
2.2.6 Das Festlegen einer Zeitdauer für die Login-Eingabe	78
2.2.7 Die Aktivierung des Passwort-Schutzes für den privilegierten Level	79
2.2.8 Die Aktivierung einer Authentifizierungsüberstimmung	80
2.2.9 Die Änderung des bei der Passworteingabe angezeigten Textes	80
2.2.10 Die Konfiguration persönlicher Login-Meldungen für die AAA-Authentifizierung	80

2.2.11	Die Aktivierung der doppelten Authentifizierung	82
2.2.12	Die Aktivierung der automatisierten doppelten Authentifizierung	85
2.3	Die Nicht-AAA-Authentifizierungsmethoden	88
2.3.1	Die Konfiguration des line-Passwortschutzes	89
2.3.2	Die Einrichtung einer Benutzernamen-Authentifizierung	90
2.3.3	Die Aktivierung der CHAP- oder PAP-Authentifizierung	91
2.3.4	Die Verwendung des MS-CHAP	96
2.3.5	Die Konfiguration des TACACS- und des erweiterten TACACS-Passwortschutzes	98
2.4	Authentifizierungsbeispiele	99
2.4.1	RADIUS-Authentifizierungsbeispiele	99
2.4.2	TACACS+-Authentifizierungsbeispiele	101
2.4.3	TACACS and Extended TACACS-Authentifizierungsbeispiele	102
2.4.4	Kerberos-Authentifizierungsbeispiele	103
2.4.5	Ein AAA-Skalierungsbeispiel	103
2.4.6	Konfigurationsbeispiele für Login- und abgelehnte Login-Meldungen	105
2.4.7	Konfigurationsbeispiele zur doppelten Authentifizierung	105
2.4.8	Ein Konfigurationsbeispiel für die automatisierte doppelte Authentifizierung	112
2.4.9	Ein MS-CHAP-Konfigurationsbeispiel	114
3	Die Authentifizierungsbefehle	117
3.1	aaa authentication arap	117
3.2	aaa authentication banner	120
3.3	aaa authentication enable default	121
3.4	aaa authentication fail-message	123
3.5	aaa authentication local-override	125
3.6	aaa authentication login	126
3.7	aaa authentication nasi	128
3.8	aaa authentication password-prompt	130
3.9	aaa authentication ppp	132
3.10	aaa authentication username-prompt	134
3.11	aaa new-model	135
3.12	aaa processes	136
3.13	access-profile	137
3.14	arap authentication	141
3.15	clear ip trigger-authentication	143
3.16	ip trigger-authentication (globale Konfiguration)	144
3.17	ip trigger-authentication (Interface-Konfiguration)	145
3.18	login authentication	147
3.19	login tacacs	148
3.20	nasi authentication	149
3.21	ppp authentication	150
3.22	ppp chap hostname	153
3.23	ppp chap password	154
3.24	ppp chap refuse	156

3.25	ppp chap wait	157
3.26	ppp pap sent-username	158
3.27	ppp use-tacacs	160
3.28	show ip trigger-authentication	161
3.29	show ppp queues	163
3.30	timeout login response	164
4	Die Konfiguration der Autorisierung	167
4.1	Die AAA-Autorisierungsarten	168
4.2	Bezeichnete Methodenlisten für die Autorisierung	168
4.3	Die AAA-Autorisierungsmethoden	170
4.4	Die vorbereitenden Maßnahmen für die AAA-Autorisierung	170
4.5	Die Konfiguration der AAA-Autorisierung	171
4.6	Die Konfiguration der Autorisierung	171
4.6.1	TACACS+-Autorisierung	172
4.6.2	if-Authenticated-Autorisierung	172
4.6.3	none-Autorisierung	172
4.6.4	Local-Autorisierung	172
4.6.5	RADIUS-Autorisierung	173
4.6.6	Kerberos-Autorisierung	173
4.7	Die Konfiguration der AAA-Autorisierung mit bezeichneten Methodenlisten	173
4.7.1	Die Autorisierungsarten	174
4.7.2	Die Autorisierungsmethoden	174
4.8	Die Deaktivierung der Autorisierung für globale Konfigurationsbefehle	175
4.9	Die Autorisierung für das rückwärtige (Reverse) Telnet	175
4.10	Die Attribut-Value-Paare der Autorisierung	177
4.11	Konfigurationsbeispiele zur Autorisierung	177
4.11.1	Ein Konfigurationsbeispiel mit einer bezeichneten Methodenliste	177
4.11.2	TACACS+-Autorisierungsbeispiele	179
4.11.3	Ein RADIUS-Autorisierungsbeispiel	180
4.11.4	Beispiele zum Kerberos-Instanzen-Vergleich	181
4.11.5	Autorisierungsbeispiele für das reverse Telnet	181
5	Die Autorisierungsbefehle	185
5.1	aaa authorization	185
5.2	aaa authorization config-commands	189
5.3	aaa authorization reverse-access	191
5.4	aaa new-model	194
5.5	authorization	196
5.6	ppp authorization	197
6	Die Konfiguration des Accountings	199
6.1	Bezeichnete Methodenlisten für das Accounting	199
6.2	Die AAA-Accountingarten	201
6.2.1	Das Netzwerk-Accounting	201
6.2.2	Das Verbindungs-Accounting	204

6.2.3	Das EXEC-Accounting	206
6.2.4	Das System-Accounting	208
6.2.5	Das Befehls-Accounting	208
6.3	Die vorbereitenden Maßnahmen für das AAA-Accounting	209
6.4	Die Aufgabenliste zur Konfiguration des AAA-Accountings	209
6.4.1	Die Konfiguration des Accountings mit bezeichneten Methodenlisten	210
6.4.2	Die Aktivierung des Accountings	211
6.4.3	Die Überwachung des Accountings	213
6.5	Die Attribut-Value-Paare des Accountings	213
6.6	Konfigurationsbeispiele für das Accounting	214
6.6.1	Ein Accounting-Konfigurationsbeispiel	214
6.6.2	Ein Konfigurationsbeispiel mit einer bezeichneten Methodenliste	215
7	Die Accountingbefehle	217
7.1	aaa accounting	217
7.2	aaa accounting suppress null-username	221
7.3	aaa accounting update	222
7.4	accounting	223
7.5	ppp accounting	225
7.6	show accounting	226
Teil II: Sicherheits-Server-Protokolle		229
8	Die Konfiguration des RADIUS	231
8.1	RADIUS-Überblick	231
8.2	Die Arbeitsweise des RADIUS	233
8.3	Die schrittweise Konfiguration des RADIUS	234
8.3.1	Die Konfiguration des Routers für die RADIUS-Server-Kommunikation	235
8.3.2	Die Konfiguration des Routers für die Verwendung herstellereigener RADIUS-Attribute	236
8.3.3	Konfiguration des Routers für hersteller-proprietary RADIUS-Server-Kommunikation	237
8.3.4	Die Konfiguration des Routers für die Abfrage des RADIUS-Servers nach statischen Routen und IP-Adressen	238
8.3.5	Konfiguration des Routers für die erweiterten Port-Informationen eines Netzwerk-Access-Servers	238
8.3.6	Konfiguration der RADIUS-Authentifizierung	240
8.3.7	Konfiguration der RADIUS-Autorisierung	240
8.3.8	Konfiguration des RADIUS-Accountings	240
8.3.9	RADIUS-Attribute	240
8.3.10	Beispiele zur RADIUS-Konfiguration	241
9	RADIUS-Befehle	245
9.1	aaa nas-port extended	245
9.2	ip radius source-interface	247
9.3	radius-server attribute nas-port extended	248
9.4	radius-server configure-nas	249

9.5	radius-server dead-time	250
9.6	radius-server extended-portnames	251
9.7	radius-server host	252
9.8	radius-server host non-standard	253
9.9	radius-server optional passwords	255
9.10	radius-server key	255
9.11	radius-server retransmit	257
9.12	radius-server timeout	258
9.13	radius-server vsa send	259
10	Konfiguration des TACACS+	261
10.1	TACACS+-Überblick	262
10.2	Die Arbeitsweise des TACACS+	263
10.3	Die schrittweise Konfiguration des TACACS+	265
10.3.1	Das Festlegen des TACACS+-Server-Hosts	266
10.3.2	Konfiguration des TACACS+-Authentifizierungsschlüssels	267
10.3.3	Konfiguration der TACACS+-Authentifizierung	268
10.3.4	Konfiguration der TACACS+-Autorisierung	268
10.3.5	Konfiguration des TACACS+-Accountings	268
10.3.6	Die TACACS+-AV-Paare	268
10.4	Beispiele zur TACACS+-Konfiguration	268
10.4.1	Beispiele zur TACACS+-Authentifizierung	269
10.4.2	Ein TACACS+-Autorisierungsbeispiel	271
10.4.3	Ein TACACS+-Accountingbeispiel	272
10.4.4	Beispiel zur TACACS+-Dämon-Konfiguration	273
11	Konfiguration des TACACS und des erweiterten TACACS	275
11.1	Die Beschreibung des TACACS-Protokolls	276
11.2	Die schrittweise Konfiguration des TACACS und des erweiterten TACACS	277
11.2.1	Konfiguration des TACACS-Passwortschutzes auf Benutzer-Level	278
11.2.2	Deaktivierung der Passwortüberprüfung auf Benutzer-Level	278
11.2.3	Konfiguration der optionalen Passwortverifizierung	279
11.2.4	Konfiguration des TACACS-Passwortschutzes auf dem privilegierten Level	279
11.2.5	Deaktivierung der Passwortüberprüfung im privilegierten Level	280
11.2.6	Die Aktivierung der Rückmeldung bei Benutzeraktionen	280
11.2.7	Konfiguration der Authentifizierung von Benutzeraktionen	281
11.2.8	Festlegen des TACACS-Server-Hosts	282
11.2.9	Beschränkung der Login-Versuche	282
11.2.10	Aktivierung des erweiterten TACACS-Modus	282
11.2.11	Aktivierung des erweiterten TACACS für die PPP-Authentifizierung	283
11.2.12	Aktivierung des Standard-TACACS für die ARA-Authentifizierung	283
11.2.13	Aktivierung des erweiterten TACACS für die ARA-Authentifizierung	284
11.2.14	Aktivierung des TACACS zur Verwendung einer bestimmten IP-Adresse	285
11.3	Beispiele zur TACACS-Konfiguration	286
12	Befehle des TACACS, des erweiterten TACACS und des TACACS+	289
12.1.1	Vergleich der TACACS-Befehle	289

12.2	arap use-tacacs	290
12.3	enable last-resort	292
12.4	enable use-tacacs	293
12.5	ip tacacs source-interface	294
12.6	tacacs-server attempts	295
12.7	tacacs-server authenticate	296
12.8	tacacs-server directed-request	297
12.9	tacacs-server extended	298
12.10	tacacs-server host	299
12.11	tacacs-server key	301
12.12	tacacs-server last-resort	302
12.13	tacacs-server login-timeout	303
12.14	tacacs-server notify	303
12.15	tacacs-server optional-passwords	304
12.16	tacacs-server retransmit	305
12.17	tacacs-server timeout	306
13	Konfiguration des Kerberos	309
13.1	Ein Kerberos-Überblick	309
13.2	Arbeitsweise der Kerberos-Clientunterstützung	312
13.2.1	Authentifizierung gegenüber dem Grenz-Router	312
13.2.2	Erwerb eines TGT von einem KDC	312
13.2.3	Die Authentifizierung gegenüber Netzwerkdiensten	313
13.3	Die schrittweise Konfiguration des Kerberos	314
13.3.1	Konfiguration des KDC mit Kerberos-Befehlen	315
13.3.2	Konfiguration der Routers zur Verwendung des Kerberos-Protokolls	317
13.3.3	Überwachung und Betrieb des Kerberos	323
13.4	Beispiele zur Kerberos-Konfiguration	324
13.4.1	Beispiele zum Festlegen eines Kerberos-Bereichs	324
13.4.2	Ein Beispiel zum Kopieren der SRVTAB-Dateien	324
13.4.3	Nicht-Kerberos-Konfigurationsbeispiele	324
13.4.4	Ein Beispiel zur Vereinbarung einer verschlüsselten Telnet-Sitzung	335
14	Die Kerberos-Befehle	337
14.1	clear kerberos creds	337
14.2	connect	338
14.3	kerberos clients mandatory	341
14.4	kerberos credentials forward	342
14.5	kerberos instance map	343
14.6	kerberos local-realm	344
14.7	kerberos preauth	345
14.8	kerberos realm	346
14.9	kerberos server	347
14.10	kerberos srvtab entry	349
14.11	kerberos srvtab remote	350
14.12	key config-key	351

14.13 show kerberos creds	352
14.14 telnet	353
Teil III: Verkehrs-Filterung und Firewalls	359
15 Access-Kontroll-Listen: Überblick und Richtlinien	361
15.1 Eine Übersicht über Access-Kontroll-Listen	361
15.1.1 Wirkung von Access-Listen	362
15.1.2 Warum Sie Access-Listen konfigurieren sollten	362
15.1.3 Unter welchen Umständen Access-Listen konfiguriert werden sollten	363
15.1.4 Einfache und erweiterte Access-Listen	364
15.2 Ein Überblick über die Konfiguration von Access-Listen	364
15.2.1 Erzeugen von Access-Listen	364
15.2.2 Zuweisung der Access-Listen zu Schnittstellen	368
15.3 Das Auffinden von vollständigen Konfigurations- und Befehls-Informationen für Access-Listen	368
16 Ein Überblick über Cisco-IOS-Firewalls	369
16.1 Ein Überblick über Firewalls	369
16.2 Die Cisco-IOS-Firewall-Lösung	370
16.2.1 Das Cisco-IOS-Firewall-Feature-Set	370
16.3 Die Errichtung eines angepassten Firewalls	371
16.4 Weitere Richtlinien für die Konfiguration Ihrer Firewall	375
17 Konfiguration der Schlüssel-Schloss-Sicherheit (Dynamische Access-Listen)	379
17.1 Über das Schlüssel-Schloss-Verfahren	379
17.1.1 Die Vorteile des Schlüssel-Schloss-Verfahrens	380
17.1.2 Unter welchen Umständen Sie das Schlüssel-Schloss-Verfahren verwenden sollten	381
17.1.3 Die Funktionsweise des Schlüssel-Schloss-Verfahrens	381
17.2 Die Kompatibilität mit Versionen vor der Cisco-IOS-Version 11.1	382
17.3 Die Spoofing-Risiken beim Schlüssel-Schloss-Verfahren	382
17.4 Der Einfluss des Schlüssel-Schloss-Verfahrens auf die Router-Performance	383
17.5 Vorbereitende Maßnahmen für die Konfiguration des Schlüssel-Schloss-Verfahrens	383
17.6 Konfiguration des Schlüssel-Schloss-Verfahrens	384
17.6.1 Konfigurationstipps zum Schlüssel-Schloss-Verfahren	385
17.7 Überprüfung der Schlüssel-Schloss-Konfiguration	388
17.8 Schlüssel-Schloss-Verwaltung	388
17.8.1 Anzeige der dynamischen Access-Listen-Einträge	389
17.8.2 Das manuelle Entfernen von dynamischen Access-Listen-Einträgen	389
17.9 Konfigurationsbeispiele zum Schlüssel-Schloss-Verfahren	389
17.9.1 Ein Beispiel des Schlüssel-Schloss-Verfahrens mit der lokalen Authentifizierung	390
17.9.2 Ein Beispiel des Schlüssel-Schloss-Verfahrens mit der TACACS+-Authentifizierung	390

18	Schlüssel-Schloss-Befehle	393
18.1	access-enable	393
18.2	access-template	394
18.3	clear access-template	396
18.4	show ip accounting	397
19	Konfiguration von IP-Sitzungsfiltern (Reflexive Access-Listen)	401
19.1	Über reflexive Access-Listen	401
19.1.1	Vorteile der reflexiven Access-Listen	402
19.1.2	Was ist eine reflexive Access-Liste?	402
19.1.3	Wie reflexive Access-Listen die Sitzungsfilterung ausführen	402
19.1.4	Wo die reflexiven Access-Listen konfiguriert werden	403
19.1.5	Wirkungsweise von reflexiven Access-Listen	403
19.1.6	Anwendungsbeschränkungen für reflexive Access-Listen	405
19.2	Vorarbeiten: Bevor Sie reflexive Access-Listen konfigurieren	405
19.2.1	Die Wahl einer Schnittstelle: Intern oder Extern	405
19.3	Die Konfiguration der reflexiven Access-Listen	406
19.3.1	Konfigurationsliste für die externe Schnittstelle	407
19.3.2	Konfigurationsliste für die interne Schnittstelle	407
19.3.3	Erstellung von reflexiven Access-Listen	408
19.3.4	Verankerung der reflexiven Access-Liste(n)	409
19.3.5	Das optionale Setzen einer globalen Zeitdauer (Timeout)	411
19.4	Konfigurationsbeispiele zu reflexiven Access-Listen	411
19.4.1	Ein Konfigurationsbeispiel für eine externe Schnittstelle	411
19.4.2	Konfigurationsbeispiel für eine interne Schnittstelle	413
20	Reflexive Access-Listen-Befehle	415
20.1	evaluate	415
20.2	ip reflexive-list timeout	417
20.3	permit (reflexive)	419
21	Konfiguration der TCP-Abfangfunktion (Schutz vor Dienstablehnungs-Attacken)	423
21.1	Über die TCP-Abfangfunktion	423
21.2	Schrittweise Konfiguration der TCP-Abfangfunktion	424
21.2.1	Aktivierung der TCP-Abfangfunktion	425
21.2.2	Die Einstellung des TCP-Abfangmodus	425
21.2.3	Einstellung des Unterbrechungsmodus der TCP-Abfangfunktion	426
21.2.4	Änderung der Zeitgeber der TCP-Abfangfunktion	426
21.2.5	Änderung der aggressiven Grenzwerte der TCP-Abfangfunktion	427
21.2.6	Überwachung und die Verwaltung der TCP-Abfangfunktion	428
21.3	Konfigurationsbeispiel zur TCP-Abfangfunktion	429
22	TCP-Abfangbefehle	431
22.1	ip tcp intercept connection-timeout	431
22.2	ip tcp intercept drop-mode	432
22.3	ip tcp intercept finrst-timeout	433

22.4	ip tcp intercept list	434
22.5	ip tcp intercept max-incomplete high	435
22.6	ip tcp intercept max-incomplete low	437
22.7	ip tcp intercept mode	438
22.8	ip tcp intercept one-minute high	439
22.9	ip tcp intercept one-minute low	441
22.10	ip tcp intercept watch-timeout	442
22.11	show tcp intercept connections	443
22.12	show tcp intercept statistics	444
23	Konfiguration der kontext-basierten Access-Kontrolle (CBAC)	447
23.1	Ein CBAC-Überblick	447
23.1.1	Was die CBAC bewirkt	448
23.1.2	Was die CBAC nicht bietet	448
23.1.3	Funktionsweise der CBAC	449
23.1.4	Wann und wo die CBAC konfiguriert werden sollte	451
23.1.5	Der CBAC-Prozess	452
23.1.6	Unterstützten Protokolle	453
23.1.7	Einschränkungen	454
23.1.8	Auswirkungen auf Arbeitsspeicher und Performance	455
23.2	Schrittweise Konfiguration der CBAC	455
23.2.1	Auswahl einer Schnittstelle: Intern oder Extern	456
23.2.2	Konfiguration der IP-Access-Listen auf der Schnittstelle	457
23.2.3	Konfiguration von globalen Zeitlimits und Grenzwerten	459
23.2.4	Erstellung einer Überprüfungsregel	461
23.2.5	Anwendung der Überprüfungsregel auf eine Schnittstelle	465
23.2.6	Anzeige der Konfiguration, des Zustands und der Statistiken für die kontext-basierte Access-Kontrolle	466
23.2.7	Fehlersuche (das Debugging) bei der kontext-basierten Access-Kontrolle	466
23.2.8	Das Verstehen der durch die kontext-basierten Access-Kontrolle erzeugten Syslog- und Konsolenmeldungen	468
23.2.9	Das Abschalten der CBAC	470
23.3	Ein CBAC-Konfigurationsbeispiel	470
24	Befehle der kontext-basierten Access-Kontrolle (CBAC)	475
24.1	ip inspect audit trail	475
24.2	ip inspect dns-timeout	476
24.3	ip inspect (Interface-Konfiguration)	477
24.4	ip inspect max-incomplete high	479
24.5	ip inspect max-incomplete low	480
24.6	ip inspect name (globale Konfiguration)	482
24.7	ip inspect one-minute high	487
24.8	ip inspect one-minute low	488
24.9	ip inspect tcp finwait-time	490
24.10	ip inspect tcp idle-time	491
24.11	ip inspect tcp max-incomplete host	492

24.12	ip inspect tcp synwait-time	494
24.13	ip inspect udp idle-time	495
24.14	no ip inspect	496
24.15	show ip inspect	497
Teil IV: IP-Security und Verschlüsselung		501
25	Ein Überblick über IP-Sicherheit und Verschlüsselung	503
25.1	Cisco-Verschlüsselungstechnologie (CET)	503
25.2	IPSec-Netzwerksicherheit	503
25.2.1	Vergleich von IPSec und Cisco-Verschlüsselungstechnologie	504
25.3	Das Internet-Key-Exchange-Sicherheitsprotokoll	507
25.4	Die Zusammenarbeit mit Zertifizierungsautoritäten	508
26	Konfiguration der Cisco-Verschlüsselungstechnologie	509
26.1	Wozu dient die Verschlüsselung?	510
26.2	Ausführung der Cisco-Verschlüsselung	511
26.2.1	Was wird verschlüsselt?	511
26.2.2	Wo im Netzwerk werden Pakete verschlüsselt und entschlüsselt?	511
26.2.3	Unter welchen Umständen können verschlüsselte Pakete ausgetauscht werden?	512
26.2.4	Wie erkennt ein Verschlüsselungs-Router andere gegenüberliegende Verschlüsselungs-Router?	512
26.2.5	Welche Standards werden in der Cisco-Verschlüsselung ausgeführt?	512
26.2.6	Wie funktioniert die Cisco-Verschlüsselung?	513
26.3	Zusätzliche Informationsquellen	517
26.4	Vorbereitungen: Bevor Sie die Verschlüsselung konfigurieren	517
26.4.1	Adressierung der Peer-Router	517
26.4.2	Berücksichtigung Ihrer Netzwerktopologie	518
26.4.3	Adressierung der Crypto-Maschinen in jedem Peer-Router	518
26.4.4	Beschreibung der Anwendungseigenschaften und Beschränkungen	520
26.5	Konfiguration der Verschlüsselung	522
26.5.1	Erzeugen von öffentlichen/geheimen DSS-Schlüsseln	523
26.5.2	Austausch der öffentlichen DSS-Schlüssel	525
26.5.3	Aktivierung des DES-Verschlüsselungsalgorithmus	528
26.5.4	Erstellung von Verschlüsselungskarten und deren Zuordnung zu Schnittstellen	529
26.5.5	Die Sicherung Ihrer Konfiguration	533
26.6	Konfiguration der Verschlüsselung mit GRE-Tunnels	533
26.6.1	Verschlüsselung des reinen GRE-Tunnelverkehrs	534
26.6.2	Verschlüsselung von GRE-Tunnelverkehr und anderem Verkehr	534
26.7	Konfiguration der Verschlüsselung mit einem ESA in einem VIP2	535
26.7.1	Zurücksetzen des ESA	535
26.7.2	Ausführung der zusätzlichen Verschlüsselungskonfiguration	536
26.8	Konfiguration der Verschlüsselung mit einem ESA in einem Cisco-Router der Serie 7200	537
26.8.1	Erforderliche Schritte	537

26.8.2	Optionale Schritte	537
26.8.3	Zurücksetzen des ESA	537
26.8.4	Ausführung der zusätzlichen Verschlüsselungskonfiguration	539
26.8.5	Aktivierung des ESA	540
26.8.6	Auswahl einer Crypto-Maschine	540
26.8.7	Löschen von DSS-Schlüsseln	542
26.9	Individuelle Einstellung der Verschlüsselung (Konfigurationsoptionen)	543
26.9.1	Einstellung der Zeitdauer von verschlüsselten Sitzungen	543
26.9.2	Verkürzung der Sitzungsaufbauzeiten durch zuvor erzeugte DH-Nummern	544
26.9.3	Änderung der Verschlüsselung-Access-Listen-Limits	544
26.10	Abschaltung der Verschlüsselung	546
26.11	Testlauf und Fehlersuche bei der Verschlüsselung	547
26.11.1	Testen der Verschlüsselungskonfiguration	547
26.11.2	Diagnose von Verbindungsproblemen	548
26.11.3	Diagnose bei verschiedenen anderen Problemen	548
26.11.4	Anwendung der Debug-Befehle	551
26.12	Beispiele zur Verschlüsselungskonfiguration	551
26.12.1	Beispiel zur Erzeugung von öffentlichen/geheimen DSS-Schlüsseln	551
26.12.2	Beispiel für den Austausch von öffentlichen DSS-Schlüsseln	552
26.12.3	Beispiel zur Aktivierung der DES-Verschlüsselungsalgorithmen	554
26.12.4	Beispiele zur Erstellung von Verschlüsselungs-Access-Listen, zur Erzeugung von Verschlüsselungskarten und zur Zuordnung der Verschlüsselungskarten zu Schnittstellen	555
26.12.5	Beispiel für die Veränderung der Verschlüsselungs-Access-Listen-Limits	560
26.12.6	Beispiele zur Konfiguration der Verschlüsselung mit GRE-Tunnels	560
26.12.7	Beispiele zur Konfiguration der ESA-spezifischen Verschlüsselung	563
26.12.8	Beispiele zum Löschen der DSS-Schlüssel	564
26.12.9	Beispiel zum Testen der Verschlüsselungsverbindung	567
27	Befehle der Cisco-Verschlüsselungstechnologie	569
27.1	access-list (Verschlüsselung)	569
27.2	clear crypto connection	578
27.3	crypto algorithm 40-bit-des	580
27.4	crypto algorithm des	580
27.5	crypto card	580
27.6	crypto card clear-latch	582
27.7	crypto cisco algorithm 40-bit-des	583
27.8	crypto cisco algorithm des	585
27.9	crypto cisco connections	587
27.10	crypto cisco entities	589
27.11	crypto cisco key-timeout	591
27.12	crypto cisco pregen-dh-pairs	593
27.13	crypto clear-latch	595
27.14	crypto esa	595
27.15	crypto gen-signature-keys	595
27.16	crypto key-exchange	595

16 Network Security

27.17	crypto key exchange dss	595
27.18	crypto key exchange dss passive	597
27.19	crypto key-exchange passive	599
27.20	crypto key generate dss	599
27.21	crypto key pubkey-chain dss	602
27.22	crypto key-timeout	604
27.23	crypto key zeroize dss	604
27.24	crypto map (globale Konfiguration)	606
27.25	crypto map (Interface-Konfiguration)	609
27.26	crypto pregen-dh-pairs	611
27.27	crypto public-key	611
27.28	crypto sdu connections	611
27.29	crypto sdu entities	611
27.30	crypto zeroize	611
27.31	deny	611
27.32	ip access-list extended (Verschlüsselung)	617
27.33	match address	618
27.34	permit	620
27.35	set algorithm 40-bit-des	626
27.36	set algorithm des	627
27.37	set peer	629
27.38	show crypto algorithms	630
27.39	show crypto card	630
27.40	show crypto cisco algorithms	631
27.41	show crypto cisco connections	632
27.42	show crypto cisco key-timeout	634
27.43	show crypto cisco pregen-dh-pairs	634
27.44	show crypto connections	636
27.45	show crypto engine brief	636
27.46	show crypto engine configuration	638
27.47	show crypto engine connections active	639
27.48	show crypto engine connections dropped-packets	641
27.49	show crypto key mypubkey dss	642
27.50	show crypto key pubkey-chain dss	643
27.51	show crypto key-timeout	644
27.52	show crypto map	645
27.53	show crypto mypubkey	648
27.54	show crypto pregen-dh-pairs	648
27.55	show crypto pubkey	648
27.56	show crypto pubkey name	648
27.57	show crypto pubkey serial	648
27.58	test crypto initiate-session	648
28	Konfiguration der IPSec-Netzwerksicherheit	651
28.1	IPSec-Überblick	652
28.1.1	Unterstützte Standards	652

28.1.2	Eine Liste von Begriffen	654
28.1.3	Gemeinsamer Betrieb von IPSec mit anderen Cisco-IOS-Softwarefunktionen	656
28.1.4	Unterstützte Hardware, Switching-Pfade und Einkapselung	656
28.1.5	Einschränkungen	656
28.1.6	Überblick über die Funktionsweise von IPSec	657
28.1.7	Verschachtelung des IPSec-Verkehrs über mehrere Peer-Geräte	659
28.1.8	Vorbereitungen	659
28.2	Schrittweise Konfiguration von IPSec	660
28.2.1	Überprüfung der Access-Listen auf ihre Kompatibilität mit IPSec	660
28.2.2	Einstellung der globalen Laufzeiten für die IPSec-Sicherheitsassoziationen	660
28.2.3	Erzeugung von Verschlüsselungs-Access-Listen	662
28.2.4	Erstellen von Transformationssets	668
28.2.5	Erzeugung von Verschlüsselungskarten-Einträgen	670
28.2.6	Zuordnung der Verschlüsselungskartensätze zu Schnittstellen	680
28.2.7	Überwachung und Verwaltung IPSec	681
28.3	IPSec-Konfigurationsbeispiel	683
29	Befehle der IPSec-Netzwerksicherheit	685
29.1	clear crypto sa	685
29.2	crypto dynamic-map	688
29.3	crypto ipsec security-association lifetime	691
29.4	crypto ipsec transform-set	694
29.5	crypto map (globale Konfiguration)	699
29.6	crypto map (Interface-Konfiguration)	704
29.7	crypto map local-address	706
29.8	initialization-vector size	708
29.9	match address	709
29.10	mode	711
29.11	set peer	713
29.12	set pfs	715
29.13	set security-association level per-host	717
29.14	set security-association lifetime	719
29.15	set session-key	722
29.16	set transform-set	725
29.17	show crypto ipsec sa	727
29.18	show crypto ipsec security-association lifetime	730
29.19	show crypto ipsec transform-set	730
29.20	show crypto dynamic-map	731
29.21	show crypto map	733
30	Konfiguration der Zusammenarbeit mit Zertifizierungsautoritäten (CAs)	737
30.1	Überblick über die CA-Zusammenarbeit	737
30.1.1	Unterstützte Standards	737
30.1.2	Einschränkungen	738
30.1.3	Vorbereitungen	739

30.2	Ein Überblick über Zertifizierungsautoritäten	739
30.2.1	Zweck der CAs	739
30.2.2	Durchführung der IPSec ohne CAs	740
30.2.3	Durchführung von IPSec mit CAs	742
30.2.4	Wie CA-Zertifikate von IPSec-Geräte eingesetzt werden	742
30.2.5	Registrierungsautoritäten	743
30.3	Schrittweise Konfiguration der CA-Zusammenarbeit	743
30.3.1	Verwaltung der NVRAM-Nutzung (optional)	744
30.3.2	Konfiguration des Host-Namens und IP-Domänennamens Ihres Routers	745
30.3.3	Erzeugung eines RSA-Schlüsselpaares	745
30.3.4	Adressierung einer CA	746
30.3.5	Authentifizierung der CA	747
30.3.6	Beantragen von eigenen Zertifikaten	747
30.3.7	Die Speicherung Ihrer Konfiguration	748
30.3.8	Überwachung und Verwaltung der Zusammenarbeit mit der Zertifizierungsautorität (optional)	748
30.4	Was als Nächstes zu tun ist	751
30.5	Konfigurationsbeispiele zur CA-Zusammenarbeit	751
31	Befehle für die Zusammenarbeit mit Zertifizierungsautoritäten	755
31.1	certificate	755
31.2	crl optional	757
31.3	crypto ca authenticate	758
31.4	crypto ca certificate chain	760
31.5	crypto ca certificate query	761
31.6	crypto ca crl request	762
31.7	crypto ca enroll	763
31.8	crypto ca identity	766
31.9	crypto key generate rsa	768
31.10	crypto key zeroize rsa	771
31.11	enrollment mode ra	772
31.12	enrollment retry-count	773
31.13	enrollment retry-period	774
31.14	enrollment url	776
31.15	query url	777
31.16	show crypto ca certificates	778
32	Konfiguration des Internet-Key-Exchange-Sicherheitsprotokolls	781
32.1	IKE-Überblick	781
32.1.1	Unterstützte Standards	782
32.1.2	Eine Liste von Begriffen	783
32.2	Schrittweise Konfiguration des IKE	784
32.2.1	Aktivierung oder Deaktivierung des IKE	785
32.2.2	Stellen Sie sicher, dass die Access-Listen mit dem IKE kompatibel sind	786
32.2.3	Erzeugung von IKE-Verfahren	786
32.2.4	Manuelle Konfiguration der RSA-Schlüssel	792

32.2.5 Konfiguration der zuvor mitgeteilten Schlüssel	794
32.2.6 Aufheben der IKE-Verbindungen	795
32.2.7 Fehlersuche beim IKE	796
32.3 Was als Nächstes zu tun ist	796
32.4 IKE-Konfigurationsbeispiel	796
33 Die Befehle des Internet-Key-Exchange-Sicherheitsprotokolls	799
33.1 address	799
33.2 addressed-key	801
33.3 authentication (IKE-Verfahren)	803
33.4 clear crypto isakmp	804
33.5 crypto isakmp enable	805
33.6 crypto isakmp identity	806
33.7 crypto isakmp key	808
33.8 crypto isakmp policy	810
33.9 crypto key generate rsa	812
33.10 crypto key pubkey-chain rsa	815
33.11 encryption (IKE-Verfahren)	817
33.12 group (IKE-Verfahren)	818
33.13 hash (IKE-Verfahren)	819
33.14 key-string	820
33.15 lifetime (IKE-Verfahren)	822
33.16 named-key	823
33.17 show crypto isakmp policy	825
33.18 show crypto isakmp sa	826
33.19 show crypto key mypubkey rsa	828
33.20 show crypto key pubkey-chain rsa	829
Teil V: Weitere Sicherheitsfunktionen	833
34 Konfiguration der Passwörter und Privilegien	835
34.1 Zugangsbeschränkung zu privilegierten EXEC-Befehlen	835
34.1.1 Setzen oder Ändern eines statischen Enable-Passworts	836
34.1.2 Schutz der Passwörter mit den Befehlen enable password und enable secret	836
34.1.3 Setzen oder Ändern eines Line-Passworts	837
34.1.4 Aktivierung des TACACS-Passwortschutzes für den privilegierten EXEC-Modus	838
34.2 Die Verschlüsselung von Passwörtern	838
34.3 Konfiguration von mehreren privilegierten Levels	839
34.3.1 Setzen des privilegierten Levels für einen Befehl	840
34.3.2 Änderung des privilegierten Standardlevels für Verbindungen	840
34.3.3 Anzeige der aktuellen privilegierten Levels	840
34.3.4 Das Einloggen in einen privilegierten Level	840
34.4 Wiederherstellung eines verlorenen Enable-Passworts	841
34.4.1 Prozess der Passwortwiederherstellung	842
34.4.2 Prozedur 1 zur Passwortwiederherstellung	842

34.4.3	Prozedur 2 zur Passwortwiederherstellung	845
34.5	Wiederherstellung eines verlorenen Line-Passworts	847
34.6	Konfiguration der Identifizierungsunterstützung	849
34.7	Konfigurationsbeispiele zu Passwörtern und Privilegien	849
34.7.1	Beispiele über mehrere privilegierte Levels	849
34.7.2	Beispiele zu Benutzernamen	850
35	Befehle zu Passwörtern und Privilegien	853
35.1	enable	853
35.2	enable password	854
35.3	enable secret	857
35.4	ip identd	859
35.5	password	860
35.6	privilege level (global)	861
35.7	privilege level (Line)	863
35.8	service password-encryption	864
35.9	show privilege	865
35.10	username	866
36	Authentifizierung der Nachbar-Router: Überblick und Richtlinien	871
36.1	Vorteile der Nachbarauthentifizierung	871
36.2	Protokolle, die die Nachbarauthentifizierung einsetzen	872
36.3	Unter welchen Umständen die Nachbarauthentifizierung konfiguriert werden sollte	872
36.4	Funktionsweise der Nachbarauthentifizierung	872
36.4.1	Klartextauthentifizierung	873
36.4.2	MD5-Authentifizierung	874
36.5	Schlüsselverwaltung (von Schlüsselketten)	874
37	Konfiguration der IP-Sicherheitsoptionen	877
37.1	Konfiguration der einfachen IP-Sicherheitsoptionen	877
37.1.1	Aktivierung der IPSO und das Setzen der Sicherheitsklassifizierungen	878
37.1.2	Festlegung, wie die IP-Sicherheitsoptionen ausgeführt werden sollen	878
37.2	Konfiguration der erweiterten IP-Sicherheitsoptionen	880
37.2.1	Konfiguration der globalen Standardeinstellungen	881
37.2.2	Zuweisung der ESOs zu einer Schnittstelle	881
37.2.3	Die Zuweisung der AESOs zu einer Schnittstelle	881
37.3	Konfiguration der DNSIX-Verfolgungsspurfunktion	881
37.3.1	Aktivierung der DNSIX-Verfolgungsspurfunktion	882
37.3.2	Angabe des Hosts, der die Verfolgungsspurmeldungen empfangen soll	882
37.3.3	Einstellung der Übertragungsparameter	883
37.4	Konfigurationsbeispiele zur IPSO	883
37.4.1	Beispiel 1	883
37.4.2	Beispiel 2	884
37.4.3	Beispiel 3	884

38	Befehle der IP-Sicherheitsoptionen	885
38.1	dnsix-dmdp retries	885
38.2	dnsix-nat authorized-redirection	886
38.3	dnsix-nat primary	887
38.4	dnsix-nat secondary	888
38.5	dnsix-nat source	889
38.6	dnsix-nat transmit-count	890
38.7	ip security add	891
38.8	ip security aeso	892
38.9	ip security dedicated	893
38.10	ip security eso-info	895
38.11	ip security eso-max	896
38.12	ip security eso-min	897
38.13	ip security extended-allowed	899
38.14	ip security first	900
38.15	ip security ignore-authorities	901
38.16	ip security implicit-labelling	902
38.17	ip security multiLevel	903
38.18	ip security reserved-allowed	905
38.19	ip security strip	906
38.20	show dnsix	907
Teil VI: Anhänge		909
Anhang A: RADIUS-Attribute		911
A.1	Die unterstützten RADIUS-Attribute	911
A.2	Eine Liste zur Beschreibung der RADIUS-Attribute	917
Anhang B: TACACS+-Attribut-Werte-Paare		941
B.1	Die TACACS+-AV-Paare	941
B.2	TACACS+-Accounting-AV-Paare	949
Stichwortverzeichnis		955