

Numerics

- 3DES (triple DES), 367
- 802.11 security enhancements, 429
- 802.11 Task Group, 429
- 802.11 WEP, 427, 431
- 802.1x, 205
 - deployment models, 345
 - identity design guidelines, 339
 - mobile access rights, 346

A

- AAA (authentication, authorization, and accounting), 6
 - distributed AAA server synchronization, 337
 - identity, 324
 - server
 - design guidelines, 330
 - high-end resilient campus security design, 564
 - medium network campus security design, 553
 - network resiliency considerations, 336
 - requirements, 338
 - scalability, 335
 - summary, 338
- acceptable use policy (AUP), 32
- access
 - as a result of attacks, 63
 - control (IPsec), 376
 - e-mail access control, 302
 - physical access, 195, 326
 - access control lists. *See* ACLs
- access layer
 - security role, 463
- access point hardening, 425
- accounting management, 592
- ACK, 673
- ACLs (access control lists), 6, 181, 238, 673
 - IPsec deployment, 396
 - manual ACL trace back, 253
- active mode (FTP), 316
- addressing (IP), design considerations, 224, 227–232
- AES (Advanced Encryption Standard), 673
- analyzing security risks, 39
- anomaly based NIDS, 153–154
- antivirus guidelines, 709–710
- antivirus mail layer, 301
- APNIC (Asia Pacific Network Information Center), 673
- appliance-based network services, 190
- application-based extranets, 529
- application-based security devices, 272–274
- applications
 - flooding, 102–103
 - gateways, 147
 - hardening, 189–190
 - identity, 323
 - manipulation attacks, 79–81
 - security, 299
 - application evaluation, 318
 - DNS, 304–309
 - e-mail, 299–301
 - e-mail, access control, 302
 - e-mail, design recommendations, 303
 - FTP, 315
 - HTTP/SSL, 311–314
 - instant messaging (IM), 316

- APs (rogue), 425
- ARP, 215–216
 - inspection, 217
 - spoofing, 84
- ASICs (application-specific integrated circuits), 273
- asymmetric routing, 247–248
- ATM clouds, 354
- attacker elite, 59
- attacks
 - application manipulation attacks, 79–81
 - ARP, 218
 - attacker elite, 59
 - attacker types, 57
 - CAM tables, 211
 - campus networks, 537–538
 - composite attacks, 108–115
 - crackers, 59
 - creative VLAN hopping, 214
 - cross-site scripting, 82
 - data scavenging, 70
 - DDoS, 62, 98
 - DDoS trace back, 253
 - DHCP snooping, 219
 - direct access attacks, 77
 - DoS attacks
 - ICMP unreachable DoS
 - considerations, 262
 - network flooding design
 - considerations, 251–254, 257–259
 - TCP SYN flooding design
 - considerations, 260
 - flooding attacks
 - MAC flooding, 94–95
 - network flooding, 95–96, 100–103
 - high-end resilient campus design, 566
 - increased access, 63
 - medium network campus design, 555
 - network edge, 483–484
 - network manipulation attacks, 78
 - preparing for, 13
 - probing and scanning, 66, 71
 - process, 56
 - rating scale, 68
 - read attacks, 69
 - redirection attacks, 103–107
 - results, 63
 - rogue devices, 92
 - rogue DHCP servers, 220
 - routing infrastructures, 240
 - script kiddies, 58
 - sniffer attacks, 75
 - spoofing attacks, 82
 - IP spoofing, 84–92
 - MAC spoofing, 83
 - taxonomies, 64–68
 - VLAN hopping, 214
 - war dialing/driving, 73
 - weapons, 14
- AUP (acceptable use policy), 32
- authentication, 155
 - EIGRP authentication, 247
 - factors in identity, 328
 - gateway-based network authentication, 346
 - hardware VPN device authentication, 580
 - IPsec, 364, 367
 - digital signatures, 365
 - Mode Config and Xauth, 366
 - presared keys, 364
 - OSPF MD5 authentication, 245
 - PEAP, 429
 - routing protocol message authentication, 242
 - settings (routers), 175–176
 - line access, 176
 - setting up usernames, 177
 - SSH, 178

authentication, authorization, and accounting.

See AAA

AV (antivirus) management, 141

availability, loss of, 37

axioms, 5

B

backscatter DDoS trace back, 253

basic NAT, 233

basic PKI, 131–132

BCP (best common practices), 673

Berkeley Internet Name Domain (BIND), 304

best practices

 IPT deployment, 444

 Layer 2 security, 224

 NetFlow deployment, 604

 network security devices, 278

 firewalls, 279–283

 network security management, 625

 focusing on operational requirements,
 629

 monitoring critical security events,
 625

 outsourcing, 629

 separating from network management,
 627

 separating historical event data from
 critical notifications, 626

 security, 45

 SNMP deployment, 598

 Syslog deployment, 602

BGP, 246

BIND (Berkeley Internet Name Domain), 304

biometrics, 134, 328

Black Helicopter Research case study,

 650–651

 attack example, 659

 design choices, 654–656

 migration strategy, 658

 security requirements, 652–653

black holes, 240, 252

BPDU guard, 204

buffer overflow attacks, 79–80

business priorities, 8

C

CA (certificate authority), 322

cabling, security risks, 200

caching, 413–414

CAM (Content Addressable Memory) table,
 210–211

campus devices, 550

campus LAN, 450

campus networks, 450

 design considerations, 541–542

 high-end resilient campus security design

 alternatives, 566

 devices and security roles, 559

 Ethernet switches, 560

 evaluation, 565–566

 internal servers, 562

 overview, 557

 requirements, 557

 stateful firewalls, 563

 user hosts, 562

 identity, 540

 IDS, 541

 medium network campus security design

 alternatives, 555

 devices and security roles, 550

 evaluation, 554–555

 internal servers, 551

 NIDS, 553

 overview, 549

 requirements, 549

 user hosts, 552

- overview, 535
- small network campus security design, 543
 - alternatives, 547
 - Ethernet switches, 544
 - evaluation, 546
 - internal servers, 545
 - user hosts, 545
 - WLAN AP, 546
- threats, 537–539
- capabilities (TFTP/FTP/SFTP/SCP), 600
- CAR (Committed Access Rate), 96, 254–256
- case studies, 635
 - Black Helicopter Research, 650–651
 - attack example, 659
 - design choices, 654–656
 - migration strategy, 658
 - security requirements, 652–653
 - NetGamesRUs, 637
 - migration strategy, 642
 - security requirements, 638–641
 - University of Insecurity, 643
 - attack examples, 649–650
 - design choices, 646–648
 - migration strategy, 649
 - security requirements, 645
- CCMP, 429
- CDP (Cisco Discovery Protocol), 180, 206–208
- CEF (Cisco express forwarding), 232
- centralized remote access firewalls, 389
- CERT (Computer Emergency Response Team), 39, 673
- certificate authority (CA), 322, 564
- certificate revocation lists (CRLs), 365
- CGIs (Common Gateway Interfaces), 81–82
- choke points, 460, 461
- CIA (confidentiality, integrity, and availability), 673
- ciphertext, 674
- Cisco Discovery Protocol (CDP), 206
- Cisco-specific protocols, 205
 - CDP, 208
 - DTP, 206
 - ISL, 206
 - VQP, 208
 - VTP, 207
- cleartext, 91, 674
- cleartext in-band, 608–609
- CLI (command-line interface), 674
- CLI access, 606
- collapsed campus design, 452
- Committed Access Rate (CAR), 96, 254–256
- compliance checking, 48
- composite attacks, 108
 - MITM attacks, 108
 - dsniff, 109
 - Ettercap, 110
 - remote control software, 113–115
 - rootkit, 112
 - viruses, worms, and Trojan horses, 110–111
- Computer Emergency Response Time (CERT), 39
- confidentiality, 23–24
- confidentiality, integrity, and availability (CIA), 673
- configuring
 - CAR, 256
 - configuration management, 592
 - DNS, 305–307
 - EIGRP authentication, 247
 - SSH on a PIX firewall, 186
 - tools, 606
 - vulnerabilities, 62
- content
 - caching, 413–414
 - distribution and routing, 415
 - interesting traffic, 362
 - load balancing, 415

Content Addressable Memory (CAM) table, 210

content delivery networks, 260

content filtering, 146–147, 284–286

- e-mail filtering, 150–151
- web filtering, 148

contractual compliance checking, 33

cookies (SYN cookies), 261

core layer, 463–464

core, distribution, and access design model, 450

corruption of information, 63

cost

- L2 resiliency, 516
- network security, 665

CPE managed IPsec, 407

crackers, 59

CRLs (certificate revocation lists), 365

cross-site scripting, 8182

cryptography, 155, 160

- file system cryptography, 159
- identity, 325
- L2 cryptography, 156
- L5 to L7 cryptography, 158
- network layer cryptography, 157

cryptographically secure in-band

- best deployment practices, 611
- network layer, 612–615
- supported platforms, 611

D

Data Encryption Standard (DES), 367

data interception, 442

data scavenging, 69–70

databases, synchronization, 335

DDoS (distributed denial of service) attacks, 62, 98

- backscatter DDoS trace back, 253
- CAR, 254

explanation, 100

mitigating, 257

Stacheldraht, 98

DDoS trace back, 253

decreased security alternative

- high-end resilient campus security design, 567
- high-end resilient edge security design, 525
- medium network campus design, 556
- medium network edge security design, 510
- small network campus security design, 548

demilitarized zones (DMZs), 19

denial of service attacks. *See* DoS attacks

deploying

- 802.1x deployment models, 345
- identity, 348–349
- IPsec VPNs, site-to-site, 392–397, 400–406
- IPT, 443–444
- NIDS, 289–291
- security device load balancing, 421

DES (Data Encryption Standard), 367

designing

- campus networks, 541–542
 - high-end resilient campus security, 557–566
 - medium network campus security, 549–555
 - small network campus security, 543–547

CAR, 256

e-mail applications, 303

extranets, 528

- application-based, 529
- network-based, 530

ICMP, 235–236

- destination unreachable messages, 238
- filtering recommendations, 239

- message type filtering, 235
- rate limiting, 235
- time exceeded, 239
- IP addressing, 224
 - ingress/egress filtering, 227–232
 - NAT, 233
 - route summarization, 224
- load balancing
 - security, 416
 - security device load balancing, 419–422
 - SLB, 417–418
- medium network edge security, 499–501
- network edge, 486
 - branch versus head-end design, 487–488
 - design alternatives, 497–499
 - design evaluation, 496
 - high-end resilient edge security, 512–513, 516–525
 - medium network edge security, 499–510
 - public servers, 487
 - remote access alternatives, 489
 - small networks, 489–494
- network security systems, 10–12, 449
 - collapsed campus design, 452
 - core, distribution, and access design, 450–451
 - domains of trust, 457–459
 - evaluating, 473
 - management, 454
 - scalability and performance, 466
 - ten steps of design, 467–474
- routing, 240
 - asymmetric routing, 247–248
 - protocol security, 240–247
 - symmetric routing, 249
- teleworker systems, 583
 - host protections, 576
 - network-transit protections, 577
 - transport protocols, 251
 - WEP, 428
- developing security systems, 34
 - examining policy drivers, 36–37
 - life cycles, 46–49
 - policies, 40–43
 - steps to success, 40
 - system design, 44–45
- device hardening, 171
 - applications, 189
 - components of a hardening strategy, 171–173
 - host operating systems, 187
 - logging critical events, 189
 - partitioning disk space, 188
- network devices, 173
 - routers, 174–182
 - switches, 184–186
- NIDSs, 186–187
- rogue device detection, 191–192
- devices
 - high-end resilient campus security design, 559
 - medium network campus design, 550
 - rogue, 92
 - small network campus security, 544
 - threat profile, 172
- DH (Diffie-Hellman), 366
- DHCP (Dynamic Host Configuration Protocol), 218, 674
 - snooping, 219
 - VACLs, 220
- differentiated groups WLANs, 440
- Diffie-Hellman (DH), 366
- digital certificates, 328
- digital signatures, 365
- direct access attacks, 77
- direct Internet access WLANs, 439
- disabling unneeded services, 174
- disclosure of information, 63

distributed denial of service attacks. *See* DDoS attacks

distributed DNS design, 309

distributed IPsec, 374

distributed two-tier e-mail design, 301

distributed WAN considerations, 337

distributing content, 415

distribution layer, security role, 463

DMVPN (Dynamic Multipoint VPN), 406

DMZs (demilitarized zones), 19

DNS

- distributed DNS design, 309
- filtering, single local server, 308
- security, 304
 - filtering case studies, 308–309
 - protected internal DNS servers, 307
 - recursive/nonrecursive queries, 305
 - server placement, 305
 - zone transfers, 307
- spoofing, 306–307

domains, choke points, 461

domains of trust, 455–457

- affecting security levels, 462
- network design, 457–459

DoS (denial of service) attacks, 63

IPT, 443

network design considerations

- ICMP unreachable DoS considerations, 262
- network flooding, 251–254, 257–259
- TCP SYN flooding, 260

resulting from NIDS shunning, 293

WLANs, 426

dsniff, 109

DTP (Dynamic Trunking Protocol), 206

dual-horned-host e-commerce network design, 528

dual-router DMZ, 280

Dynamic Host Configuration Protocol. *See* DHCP

Dynamic Multipoint VPN (DMVPN), 406

Dynamic Trunking Protocol (DTP), 206

E

EAP, identity design guidelines, 339

echo messages (ICMP), 237

e-commerce

- filtering, 257–259
- network design, 526–528

edge (networks), 481

- design considerations, 486
 - branch versus head-end design, 487–488
 - public servers, 487
 - remote access alternatives, 489
- high-end resilient edge security
 - design alternatives, 525
 - design evaluation, 523
 - Internet edge, 516–519
 - overview, 513, 516
 - remote access edge, 520–522
 - requirements, 512
- medium network edge security
 - design alternatives, 508–510
 - design evaluation, 507–508
 - design overview, 501
 - design requirements, 499–500
 - Internet edge, 502–504
 - remote access edge, 505–506
- security
 - identity, 485–486
 - threats, 482–484
- small network edge security, 489
 - design alternatives, 497–499
 - design evaluation, 496
 - design requirements and overview, 490

- devices and security roles, 491–493
- VPNs, 494
- egress filtering, 227
 - nonroutable networks, 230
 - RFC 1918, 227
 - RFC 2827, 228–229
 - uRPF, 232
- EIGRP (Enhanced Interior Gateway Routing Protocol), 247
- elite attackers, 59
- e-mail
 - filtering, 150–151
 - security, 299
 - access control example, 302
 - design recommendations, 303
 - distributed two-tier design, 301
 - two-tier design, 300
- embryonic connection, 261
- encryption, 155
 - identity, 325
 - passwords, 91, 175
- Encryption Protocol Selection, 367
- enforcement (security policies), 32–33
- ESP, 359
- Ethernet switches
 - high-end resilient campus security design, 560
 - high-end resilient edge design, 519
 - Internet edge, 504
 - medium network campus security design, 550
 - small network campus design, 544
 - small network edge security, 493
- Ettercap, 110
- evaluating
 - application security, 318
 - high-end resilient campus security design, 565
 - high-end resilient edge security design, 523

- medium network campus security design, 554
- medium network edge security design, 507–508
- security systems, 473
- small network campus design, 546
- small network edge design, 496

EXEC, 674

Extended Authentication (Xauth), 366

extranet design, 528

- application-based, 529
- network-based, 530

F

- fault management, 592
- FIB (forwarding information base), 232
- file systems
 - cryptography, 159
 - integrity checking, 136
- File Transfer Protocol (FTP), 188, 315, 599–600
- filtering
 - black holes, 252
 - content, 284–286
 - content filtering, 146–147
 - e-mail filtering, 150–151
 - web filtering, 148
- DNS
 - distributed DNS design, 309
 - single local server, 308
- e-commerce specific, 257–259
- ICMP, 235, 239, 260
- ingress/egress, 227
 - nonroutable networks, 230
 - RFC 2827, 229
 - uRPF, 232
- L3 versus L4, 541

firewalls, 142

- best practices, 283
- distributed DNS design, 310
- HA firewalls versus HA/LB firewalls, 422
- host-based, 137
- ingress/egress filtering, 229
- IPsec VPNs, 384–389
- logging, 186
- login restrictions, 185
- out-of-band management, 617
- routers with Layer 3/4 stateless ACLs, 143
- single local server DNS filtering, 308
- SSH, 186
- stateful, 144–146
 - high-end resilient campus security design, 563
 - Internet edge, 502
- three-tier web design, 314
- topology options, 279
 - dual-router DMZ, 280
 - multifirewall design, 282
 - stateful firewall DMZ design, 280
 - three-interface firewall design, 281

flash crowds, 103

flat untrusted networks, 455

flooding

- MAC, 94–95, 210–211
- network flooding, 95–96, 100–103
- stopping, 252

flow, 602

flow-based LB, 424

forward proxy caches, 414

forwarding information base (FIB), 232

fragmentation (IPsec), 381–384

fragments keyword, 236

Frame Relay, 354

FTP (File Transfer Protocol), 188, 315, 599–600

G

gateway-based network authentication, 346

gateways (security), 491

gateway-to-gateway VPNs, 355

GRE (generic route encapsulation), 106, 379

GRE + IPsec, 379

- PMTUD, 384
- site-to-site IPsec deployment, 397

GUI management tools, 606

guidelines, 42

H

HA (high availability), 390

HA firewalls versus HA/LB firewalls, 422

HA GRE hub and spoke design, 402–405

hardening (device), 171

- applications, 189–190
- components of a hardening strategy, 171–173

host operating systems, 187

- logging critical events, 189
- partitioning disk space, 188

network devices, 173

- routers, 174–182
- switches, 184–186

NIDSs, 186–187

rogue device detection, 191–192

hardware

- teleworker computers, 571, 579–582
- vulnerabilities, 61

heterogeneous networks, 665–666

HIDS, 138–139

high availability (HA), 390

high-end resilient campus security design

- alternatives, 566
- devices and security roles, 559

- Ethernet switches, 560
- evaluation, 565, 566
- internal servers, 562
- overview, 557
- requirements, 557
- stateful firewalls, 563
- user hosts, 562
- high-end resilient edge security, 516
 - design alternatives, 525
 - design evaluation, 523
 - design overview, 513, 516
 - design requirements, 512
 - Internet edge, 516
 - Ethernet switches, 519
 - Internet WAN routers, 517
 - NIDS, 518
 - public servers, 519
 - stateful firewalls, 517
 - remote access edge, 520–522
- homogenous networks, 665–666
- hopping (VLANs), 213–214
- host and application security, 136
 - HIDS, 138–139
 - host antivirus (AV), 140–141
 - host-based firewalls, 137
 - summary, 142
- host antivirus (AV), 140–141
- host AV, 546
- host-based firewalls, 137
- host operating systems, hardening, 187–189
- HTTP security, 311
 - three-tier web design, 313–314
 - two-tier web design, 311
- HTTPS (Hypertext Transfer Protocol Secure), 596, 674
- hub-and-spoke IPsec, 371
- hybrid host solutions, 161
- hybrid management design, 622
- ICMP (Internet Control Message Protocol), 235
 - design considerations, 235–236
 - destination unreachable messages, 238
 - filtering recommendations, 239
 - message type filtering, 235
 - rate limiting, 235
 - time exceeded, 239
 - echo reply, 236–237
 - echo request, 236–237
 - filtering, 260
 - unreachable DoS considerations, 262
- identity, 83, 321–322
 - 802.1x/EAP design guidelines, 339
 - AAA, 324
 - AAA server design guidelines, 330–331, 334–344
 - campus networks, 540
 - deployment, 348–349
 - device, 322
 - digital certificates, 328
 - factors, 328
 - IP addresses, 327
 - IPsec, 376
 - L4 information, 327
 - MAC addresses, 327
 - network edge, 485–486
 - network versus application, 323
 - physical access, 326
 - role in secure networking, 329
 - shared, 325
 - spoofing, 90–92
 - teleworker systems, 575
 - usernames, 328
- identity technologies, 126–127
 - basic PKI, 131–132
 - OTPs, 129–130

- RADIUS and TACACS+, 128
 - summary, 134
- IDSs (intrusion detection systems), 5, 67, 541
- IETF (Internet Engineering Task Force), 675
- IGRP (Interior Gateway Routing Protocol), 246
- IKE (Internet Key Exchange), 158, 358, 675
 - IKE IPsec, 367
 - IKE phase 1, 362
 - IKE quick mode, 363
- IM (instant messaging), 316
- increased security alternative
 - high-end resilient campus security design, 566
 - medium network campus design, 555
 - medium network edge security design, 510
 - small network campus security design, 548
- increased VPN requirements alternative
 - (medium network edge security design), 509
- Information Technology (IT), 10
- INFOSEC (Information Security), 30
- InfoSec acceptable use policy
 - e-mail, 704
 - general use and ownership, 700
 - overview, 699
 - security and proprietary information, 701
 - system and network activities, 702
- ingress filtering, 227
 - nonroutable networks, 230
 - RFC 1918, 227
 - RFC 2827, 228–229
 - uRPF, 232
- inside NIDS, 162
- instant messaging (IM), 316
- integrity, 155
- integrity checking (file systems), 136
- Internet edge, 516
 - high-end resilient edge design
 - Ethernet switches, 519
 - Internet WAN routers, 517
 - NIDS, 518
 - public servers, 519
- interesting traffic, 362
- Interior Gateway Routing Protocol (IGRP), 246
- internal servers
 - high-end resilient campus security design, 562
 - medium network campus security design, 551
 - small network campus design, 545
- internal user aggregation, 285
- Internet Control Message Protocol. *See* ICMP
- Internet edge, 502
 - Ethernet switches, 504
 - high-end resilient edge design, 517
 - NIDS, 503
 - public servers, 504
 - stateful firewalls, 502
- Internet Key Exchange. *See* IKE
- Internet Protocol Security. *See* IPsec
- interoperability (IPsec), 392
- interswitch linking (ISL), 206
- intrusion-detection systems (IDSs), 5, 67, 541
- IOS (Internet Operating System), 675
- IP addressing
 - design considerations, 224
 - ingress/egress filtering, 227–232
 - NAT, 233
 - route summarization, 224
 - identity, 327
 - IPsec considerations, 381
 - security design effects, 464–465
 - static translation, 233
- IP redirection attacks, 105

- IP spoofing, 84–89
 - identity spoofing, 90–92
 - transport spoofing, 86
 - IP telephony. *See* IPT
 - IPsec (Internet Protocol Security), 20, 432–436
 - access control, 376
 - elements of, 358
 - ESP, 359
 - identity, 376
 - IKE, 358
 - interoperability, 392
 - Layer 3 considerations, 376
 - GRE, 379
 - IP addressing, 381
 - routing, 377
 - NAT, 377
 - outsourcing, 407
 - PMTUD, 381–384
 - SA establishment, 362
 - phase 1, 362
 - phase 2, 363
 - security
 - authentication methods, 364–366
 - DH, 366
 - Encryption Protocol Selection, 367
 - PFS, 366
 - split tunneling, 368, 371
 - transport mode, 360
 - tunnel mode, 360
 - IPsec VPNs, 354–356
 - firewall and NIDS placement, 384–389
 - HA, 390
 - outsourcing, 407
 - platform options
 - remote user, 376
 - site-to-site, 375
 - QoS, 391
 - site-to-site deployment examples, 392
 - ACLs, 396
 - basic IPsec, 394–396
 - DMVPN, 406
 - GRE + IPsec, 397, 400–401
 - HA GRE hub and spoke design, 402–405
 - site-to-site VPNs, 355
 - topologies
 - centralized remote access firewall, 389
 - choices, 371–374
 - semitrusted, 388
 - trusted topology, 385
 - IPT (IP telephony), 441
 - data interception, 442
 - deployment options, 443
 - firewalls, 444
 - IPv6, 668, 669
 - ISL (interswitch linking), 206
 - IT (Information Technology), 10
- ## J–L
-
- key card access, 197
 - L2 cryptography, 156
 - L2 redirection attacks
 - ARP redirection/spoofing, 103
 - STP redirection, 104
 - L2 resiliency, 516
 - L3+ cryptography, 431
 - IPsec, 434
 - SSH/SSL, 436
 - L5 to L7 cryptography, 158
 - LAN-to-LAN VPNs, 355
 - Layer 2
 - redundancy, 250
 - security, 201
 - 802.1x, 205
 - ARP, 215–217

- best practices, 224
- Cisco-specific protocols, 205–208
- DHCP, 218–220
- MAC flooding, 210–211
- protocols, 202
- PVLANs, 222
- STP, 203, 204
- VLAN hopping, 213–214
- VLANs, 223
- Layer 3, IPsec considerations, 376
 - GRE, 379
 - IP addressing, 381
 - routing, 377
- Layer 4, identity, 327
- LB NIDS, 424
- legislation, 666–667
- life cycles (security systems), 46–49
- line access (routers), 176
- Linux, 272
- load balancing, 249, 415
 - security, 416
 - security device load balancing, 419–422
 - SLB, 417–418
- lock-and-key access, 196
- logging
 - critical events, 189
 - PIX firewalls, 186
- login banners, 176

M

- MAC addresses, identity, 327
- MAC flooding, 94–95, 210–211
- MAC spoofing, 83
- maintenance (security systems), 47
- management access (routers), 178–180
 - ACL options, 181
 - SNMP, 179

- managing, 591. *See also* network security
 - management; secure network management
 - goals of management, 591–592
 - network security, 454
 - security troubleshooting, 663–664
- man-in-the-middle (MITM) attacks, 63
- manipulation attacks
 - application manipulation attacks, 79–81
 - network manipulation attacks, 78
 - spoofing attacks, 82–83
- manual ACL trace back, 253
- MD5
 - digest authentication, 242–243
 - OSPF MD5 authentication, 245
- mean time between failures (MTBF), 274
- medium network campus security design
 - alternatives, 555
 - devices and security roles, 550
 - evaluation, 554–555
 - internal servers, 551
 - NIDS devices and security roles, 553
 - overview, 549
 - requirements, 549
 - user hosts, 552
- medium network edge security, 499–501
 - design alternatives
 - increased security, 510
 - increased VPN requirements, 508
 - design evaluation, 507–508
 - Internet edge, 502
 - Ethernet switches, 504
 - NIDS, 503
 - public servers, 504
 - stateful firewalls, 502
 - remote access edge, 505
 - VPNs, 505
 - WANs, 506
- message authentication, 242
- middleware AAA topology, 332

- MITM (man-in-the-middle) attacks, 63, 108
 - dsniff, 109
 - Ettercap, 110
 - remote control software, 113–115
 - rootkit, 112
 - viruses, worms, and Trojan horses, 110–111
- mixed AAA topology, 333
- mobile worker security concerns, 370
- monitoring
 - NIDS, 290
 - security systems, 47
- MTBF (mean time between failures), 274
- multifirewall design, 282
- multisegment NIDS, 295

N

- n* squared problem, 364
- NAS (network access server), 675
- NAT (Network Address Translation), 22, 224, 233
 - IPsec, 377
 - manipulating flows, 250
- NBMA (Nonbroadcast Multiaccess), 406
- NetFlow, 603–604
- NetGamesRUs.com case study, 637
 - migration strategy, 642
 - security requirements, 638
 - design choices, 640–641
 - edge security, 639
- NETOPS (network operations), 593
- network access server (NAS), 675
- network-based extranets, 530
- network-based managed IPsec, 407
- network devices, hardening, 173
 - routers, 174–182
 - switches, 184–186
- network flooding, 95–96
 - application flooding, 102–103
 - smurf attacks, 96
 - TCP SYN flooding, 100–101
- network identity, 323
- network-integrated security functions, 274–276
- network layer
 - cryptographically secure in-band, 612–615
 - cryptology, 157
- network manipulation attacks, 78
- network security
 - cost, 665
 - IPv6, 668–669
 - legislation, 666–667
 - systematic nature of, 669
- network security axioms (NSA), 5
- network security management, 591
 - best practices, 625
 - focusing on operational requirements, 629
 - monitoring critical security events, 625
 - outsourcing, 629
 - separating from network management, 627
 - separating historical event data from critical notifications, 626
 - cleartext in-band, 608–609
 - cryptographically secure in-band
 - best deployment practices, 611
 - network layer, 612–615
 - supported platforms, 611
 - hybrid management design, 622
 - organizational realities, 593
 - out-of-band (OOB) management, 616–621

- protocol capabilities
 - HTTP/HTTPS, 596
 - NetFlow, 603–604
 - SNMP, 597–598
 - Syslog, 601–602
 - Telnet/SSH, 594
 - TFTP/FTP/SFTP/SCP, 599–600
- tools
 - configuration/provisioning tools, 605
 - GUI, 606
 - security monitoring tools, 607
- network security platforms
 - application-based security devices, 272–274
 - general-purpose OS security devices
 - advantages, 269
 - disadvantages, 270
 - software options, 270–271
 - network-integrated security functions, 274–276
 - recommendations, 277
- network security systems, 6
 - operational simplicity, 15–16
 - predictability, 19–20
- Network Time Protocol (NTP), 181
- networks
 - campus. *See* campus networks
 - e-commerce, 526–528
 - edge, 481
 - branch versus head-end design, 487–488
 - design alternatives, 497–499
 - design considerations, 486
 - design evaluation, 496
 - high-end resilient edge security, 512–513, 516–525
 - identity, 485–486
 - ISP router, 486
 - medium network edge security, 499–510
 - public servers, 487
 - small network security, 489–494
 - threats, 482–484
 - extranets, 528
 - application-based, 529
 - network-based, 530
 - heterogeneous, 666
 - homogenous, 666
 - identity, 321, 322
 - 802.1x/EAP design guidelines, 339
 - AAA, 324
 - AAA server design guidelines, 330–344
 - deployment, 348–349
 - device, 322
 - digital certificates, 328
 - factors, 328
 - IP addresses, 327
 - L4 information, 327
 - MAC addresses, 327
 - network versus application, 323
 - physical access, 326
 - role in secure networking, 329
 - shared, 325
 - usernames, 328
 - loss of availability, 37
 - remote access alternatives, 489
 - security
 - as a system, 6
 - avoiding security through obscurity, 21–22
 - Black Helicopter Research, 650–659
 - business priorities, 8
 - confidentiality, 23–24
 - content filtering, 146–151, 284–286
 - cryptography, 155–160
 - device best practices, 278–283
 - difficulties of, 121–125
 - emerging technologies, 161
 - firewalls, 142–146
 - good network design, 10–12

- hybrid host solutions, 161
- inside NIDS, 162
- NetGamesRUs case study, 637–643
- NIDS, 151–154, 287–295
- operational simplicity, 15–16
- policies, 31–33
- predictability, 19–20
- proxy servers, 284–286
- system design, 44–45, 449
- system development and operation,
 - 34–37, 40–43
- system life cycles, 46–49
- technologies, 126
- University of Insecurity, 643–650
- vendors, 30
- weapons, 14
- teleworker computers, 571
- NIDS, 151–152, 186–187
 - alerts, 290
 - anomaly based NIDS, 153–154
 - attack response, 292
 - best practices, 289
 - deployment, 289–291
 - high-end resilient edge design, 518
 - inside NIDS, 162
 - Internet edge, 503
 - IPsec VPN placement, 384–389
 - medium network campus security design,
 - 553
 - multisegment NIDS, 295
 - placement, 287
 - signature-based NIDS, 152
 - stick LB NIDS design, 423
 - TCP resets, 294
- Nmap Ping sweep, 72
- no ip directed-broadcast command, 96
- Nonbroadcast Multiaccess (NBMA), 406
- nonrecursive queries, 305
- nontechnical compliance checking, 33

- NSA (network security axioms), 5
- NTP (Network Time Protocol), 181

O

- obfuscation, 82
- one-time password (OTP), 91
- one-to-one NAT, 233
- OOB (out of band) management, 616–617
 - best deployment uses, 621
 - example, 620
 - multisite considerations, 619
 - supported platforms, 619
- open source software
 - disadvantages, 272
 - OSs and security, 271
- operational simplicity, 15–16
- OSPF (Open Shortest Path First), 245
- OSs
 - network security, 269–271
 - security, 268
- OTP (one-time password), 91, 129–130, 135
- out-of-band (OOB) management, 616–617
- outsourcing
 - IPsec, 407
 - network security management best practices, 629

P

- paging, 625
- partial mesh IPsec, 372
- partitioning disk space, 188
- passive mode (FTP), 316
- passive technology-assisted compliance
 - checking, 32
- passphrases, 708

- passwords
 - cracking, 91
 - encryption, 91, 175
 - MD5, 243
 - OTPs, 129
 - reusable, 127
 - sample policy
 - application development standards, 708
 - guidelines, 706
 - overview, 705
 - passphrases, 708
 - protection standards, 707
- PAT (port address translation), 233
- patch management systems, 189
- path maximum transmission unit discovery (PMTUD), 381–384
- PCs, security, 269
- PEAP, 429
- perfect forward secrecy (PFS), 366
- performance
 - managing, 591
 - network security system design, 466
 - PC platform security, 270
 - split tunneling, 369
- perimeter security, 491
- PFS (perfect forward secrecy), 366
- PGP (Pretty Good Privacy), 304
- physical access
 - identity, 326
- physical security, 195
 - cable plant issues, 200
 - data centers, 198
 - electromagnetic radiation concerns, 200
 - facilities
 - key card access, 197
 - keycard with turnstile, 197
 - lock-and-key access, 196
 - single-factor identity factor, 198
 - identity mechanisms for insecure locations, 199
 - PC threats, 201
 - preventing password recovery at insecure locations, 199
- PIN-code readers, 198
- Ping utility, 72
- PKI (Public Key Infrastructure), 360
 - basic PKI, 131
 - types of, 132
 - usage basics, 347
- plaintext password authentication, 242
- PMTUD (path maximum transmission unit discovery), 381–384
- policies, 42
 - comparing with current network operation, 469
 - development, 40–41
 - enforcement, 32–33
 - examining drivers, 36–37
 - examples
 - antivirus guidelines, 709–710
 - INFOSEC acceptable use policy, 699–704
 - passwords, 705–708
 - overview, 31
 - policy teams, 43
 - reviewing documents, 468
 - security, 29
 - system development and operation, 34
 - vulnerabilities, 62
- port address translation (PAT), 233
- port command, 145
- port scanning, 71
- port security, 212
- predictability, 19–20

- pre-shared keys, IPsec peer authentication, 364
- Pretty Good Privacy (PGP), 304
- probing and scanning attacks, 66, 71
- protocols
 - ICMP, design considerations, 235
 - Layer 2 protocols, 202
 - Layer 2 security
 - 802.1x, 205
 - ARP, 215–217
 - best practices, 224
 - Cisco-specific protocols, 205–208
 - DHCP, 218–220
 - MAC flooding, 210–211
 - PVLANs, 222
 - STP, 202–204
 - VLANs, 223
 - security, Cisco-specific, 205
- provisioning tools, 606
- proxy servers, 147, 284
 - DMZ proxy design, 286
 - firewall-enforced user aggregation, 285
 - internal user aggregation, 285
 - RADIUS, 676
- PSTN dial-up
 - high-end resilient edge security, 523
 - medium network edge security, 507
- PSTNs (Public Switched Telephone Networks), 356
- Public Key Infrastructure. *See* PKI
- public servers
 - high-end resilient edge design, 519
 - Internet edge, 504
 - small network edge security, 494
- Public Switched Telephone Networks (PSTNs), 356
- PVLANs, 222–223
 - out-of-band management, 617
 - security, 223

Q–R

- QoS (IPsec VPNs), 391
- RADIUS, 128
- rate limiting (ICMP), 235
- read attacks, 69
- real-time technology enforcement, 32
- reconnaissance (recon) attacks, 69
- recursive queries, 305
- redirection attacks
 - IP redirection attacks, 105
 - L2 redirection attacks, 103
 - STP redirection attacks, 104
 - transport redirection attacks, 106–107
- redundancy (Layer 2), 250
- regional Internet registries (RIRs), 230
- remote access edge, 505
 - design evaluation, 508
 - high-end resilient edge security, 520
 - VPNs, 521
 - WANs, 522
 - VPNs, 505
 - WANs, 506
- remote control software attacks, 113–115
- remote user IPsec platforms, 376
- remote user-store access, 334
- remote user VPNs, 356
- reverse proxy caches, 414
- RFC 1918, 227
- RFC 2827, 228–229
- RFC 3330, 231
- RIP (Routing Information Protocol), 244
- RIPv2, 244
- RIRs (regional Internet registries), 230
- risk analysis, 38–39
- rogue APs, 425

- rogue devices, 92
 - campus networks, 542
 - detection, 191–192
 - Root guard, 205
 - rootkit, 112
 - route summarization (IP addressing), 224
 - router/switch software integrated security functions, 274
 - routers
 - ACLs, 238
 - authentication settings, 175–178
 - hardening options, 182
 - hardening settings, 174–175
 - Layer 3/4 stateless ACLs, 143
 - management access, 178–180
 - ACL options, 181
 - SNMP, 179
 - network edge security, 491
 - routing
 - black holes, 240
 - content, 415
 - design considerations, 240
 - asymmetric routing, 247–248
 - protocol security, 240–247
 - symmetric routing, 249
 - IPsec Layer 3 considerations, 377
 - manipulating flows, 250
 - security design effects, 464
 - sinkhole routing, 252
 - Routing Information Protocol (RIP), 244
 - RSA (Rivest-Shamir-Adleman), 676
 - sandwich security device load balancing, 421
 - scalability
 - AAA server, 335
 - network security system design, 466
 - SCP, 599–600
 - script kiddies, 58
 - scripting, 82
 - SECOPS (security operations), 593
 - Secure FTP (SFTP), 315
 - Secure Hash Algorithm (SHA), 367
 - secure network management, 591
 - cleartext in-band, 608–609
 - cryptographically secure in-band
 - best deployment practices, 611
 - network layer, 612–615
 - supported platforms, 611
 - hybrid management design, 622
 - optional components, 623
 - organizational realities, 593
 - out-of-band (OOB) management, 616–621
 - protocol capabilities
 - HTTP/HTTPS, 596
 - NetFlow, 603–604
 - SNMP, 597–598
 - Syslog, 601–602
 - Telnet/SSH, 594
 - TFTP/FTP/SFTP/SCP, 599
 - tool capabilities, 605–607
 - troubleshooting, 663–664
 - secure networking legislation, 666–667
 - Secure Shell (SSH), 178
 - Secure Socket Layer (SSL), 677
 - Secure Socket Layer (SSL) offload, 417
-
- S**
- S/MIME (Secure Multipurpose Internet Mail Extensions), 304
 - SA establishment (IPsec), 362–363

- security, 30
 - affect on routing and IP addressing, 464–465
 - application-based security devices, 272–274
 - applications, 299
 - DNS, 304–309
 - e-mail, 299–301
 - e-mail, access control, 302
 - e-mail, design recommendations, 303
 - evaluation, 318
 - FTP, 315
 - HTTP/SSL, 311–314
 - instant messaging (IM), 316
 - as a system, 6
 - attacks
 - application manipulation attacks, 79–81
 - attacker elite, 59
 - attacker types, 57
 - composite attacks, 108–115
 - crackers, 59
 - data scavenging, 70
 - direct access attacks, 77
 - flooding attacks, 94–96
 - application flooding, 102–103
 - TCP SYN flooding, 100–101
 - network manipulation attacks, 78
 - probing and scanning, 66, 71
 - process, 56
 - rating scale, 68
 - read attacks, 69
 - redirection attacks, 103–107
 - results, 63
 - rogue devices, 92
 - script kiddies, 58
 - sniffer attacks, 75
 - spoofing attacks, 82–92
 - taxonomies, 64–68
 - war dialing/driving, 73
 - avoiding security through obscurity, 21–22
 - best practices (firewalls), 45, 278–283
 - Black Helicopter Research case study, 650–651
 - attack example, 659
 - design choices, 654–656
 - migration strategy, 658
 - security requirements, 652–653
 - business priorities, 8
 - caching, 414
 - campus, 535
 - design considerations, 541–542
 - high-end resilient campus security design, 557–566
 - medium network campus security design, 549–555
 - small network campus security design, 543–547
 - threats, 537–539
 - choke points, 460–461
 - compliance checking, 48
 - confidentiality, 23–24
 - content filtering, 146–147, 284–286
 - e-mail filtering, 150–151
 - web filtering, 148
 - cost, 665
 - cryptography, 155
 - file system cryptography, 159
 - L2 cryptography, 156
 - L5 to L7 cryptography, 158
 - Network layer cryptography, 157
 - cryptography, 160
 - difficulties of, 121–125
 - disabling unneeded services, 174
 - domains of trust, 455–459
 - DoS attacks
 - ICMP unreachable DoS considerations, 262

- network flooding design
 - considerations, 251–259
- TCP SYN flooding design
 - considerations, 260
- events, 46
- extranets, 529
- firewalls, 142
 - routers with Layer 3/4 stateless ACLs, 143
 - stateful, 144–46
- good network design, 10–12
- identity, 321–322
 - 802.1x/EAP design guidelines, 339
 - AAA, 324
 - AAA server design guidelines, 330–331, 334–344
 - deployment, 348–349
 - device, 322
 - digital certificates, 328
 - factors, 328
 - IP addresses, 327
 - L4 information, 327
 - MAC addresses, 327
 - network versus application, 323
 - physical access, 326
 - role in secure networking, 329
 - shared, 325
 - usernames, 328
- incident response, 49
- IPsec
 - authentication methods, 364–366
 - DH, 366
 - Encryption Protocol Selection, 367
 - PFS, 366
 - split tunneling, 370
- IPT, 441
 - data interception, 442
 - deployment options, 443
 - firewalls, 444
- IPv6, 668–669
- Layer 2, 201
 - 802.1x, 205
 - ARP, 215–217
 - best practices, 224
 - Cisco-specific protocols, 205–208
 - DHCP, 218–220
 - MAC flooding, 210–211
 - protocols, 202
 - PVLANS, 222
 - STP, 202–204
 - VLAN hopping, 213–214
 - VLANs, 223
- layer roles, 463–464
- legislation, 666–667
- load balancing, 415–416
 - security device load balancing, 419–422
 - SLB, 417–418
- NetGamesRUs.com case study, 637
 - migration strategy, 642
 - security requirements, 638–641
- network-integrated security functions, 274–276
- NIDS, 151
 - alerts, 290
 - anomaly based NIDS, 153–154
 - attack response, 292
 - best practices, 289
 - deployment, 289–291
 - multisegment NIDS, 295
 - placement, 287
 - signature-based NIDS, 152
 - TCP resets, 294
- operational simplicity, 15–16
- OS network security devices, 269–271
- OSs, 268
- passphrases, 708
- physical, 195
 - cable plant issues, 200

- data centers, 198
- electromagnetic radiation concerns, 200
- identity mechanisms for insecure locations, 199
- key card access, 197
- keycard with turnstile, 197
- lock-and-key access, 196
- PC threats, 201
- preventing password recovery at insecure locations, 199
- single-factor identity problem, 198
- policies, 29
 - antivirus guidelines, 709–710
 - enforcement, 32–33
 - INFOSEC example, 699–704
 - overview, 31
 - passwords, 705–708
- predictability, 19–20
- proxy servers, 284
 - DMZ proxy design, 286
 - firewall-enforced user aggregation, 285
- risks, 38–39
- routing protocols, 240
 - asymmetric routing, 247–248
 - message authentication, 242
 - specific protocol options, 244–247
 - symmetric routing, 249
- software deployment, 667
- stateless security features, 250
- system design, 449
 - collapsed campus design, 452
 - core distribution, and access design model, 450, 451
 - management, 454
 - ten steps to design, 467–474
 - system development and operations, 34
 - examining policy drivers, 36–37
 - policy development, 40–43
 - steps to success, 40
 - system design, 44–45
 - system life cycles, 46–49
 - system rough drafts, 470
 - system scalability and performance, 466
- technologies, 126
 - host and application security, 136–142
 - identity technologies, 126–134
- teleworker, 571
 - design evaluations, 583
 - hardware-based design, 579–582
 - host protections, 576
 - identity, 575
 - network-transit protections, 577
 - software-based design, 578
 - threats, 572–575
- transport protocols, 251
- University of Insecurity case study, 643
 - attack examples, 649–650
 - design choices, 646–648
 - migration strategy, 649
 - security requirements, 645
- vendors, 30
- versus access, 43
- vulnerabilities, 12–13, 60
 - configuration, 62
 - hardware, 61
 - policy, 62
 - software, 60
 - usage, 62
- weapons, 14
- WLANs

- 802.11 security enhancements, 429
- 802.11 WEP, 427, 431
- access point hardening, 425
- differentiated groups WLANs, 440
- direct Internet access WLANs, 439
- DoS attacks, 426
- L3+ cryptography, 431, 434–436
- recommendations, 438
- rogue APs, 425
- security device load balancing, 419–420
 - HA firewall versus HA/LB firewall, 422
 - sandwich model, 421
 - stick model, 423
- security management, 592
- security policy database (SPD), 362
- selecting technologies for network security design, 469
- semitrusted IPsec topology, 386–388
- Sendmail, 303
- Server Load Balancing (SLB), 417
- servers
 - DNS configuration, 305
 - proxy, 676
- SFTP (Secure FTP), 315, 599–600
- SHA (Secure Hash Algorithm), 367
- shared identity, 325
- signature-based NIDS, 152
- Simple Network Management Protocol. *See* SNMP
- single sign-on (SSO), 331
- sinkhole routing, 252
- site-to-site IPsec platforms, 375
- site-to-site IPsec VPN deployment examples, 392–406
- site-to-site VPNs, 355
 - remote access edge, 505
- Slashdot effect, 103
- SLB (Server Load Balancing), 417
- small network campus security design, 543
 - alternatives, 547
 - Ethernet switches, 544
 - evaluation, 546
 - internal servers, 545
 - user hosts, 545
 - WLAN AP, 546
- small network edge security design, 489
 - alternatives, 497
 - decreased security small network design, 499
 - increased security small network design, 498
 - design requirements and overview, 490
 - devices and security roles
 - Ethernet switches, 493
 - optional WAN routers, 492
 - public servers, 493
 - router/security gateways, 491
 - evaluation, 496
 - VPNs, 494
- smurf attacks, 95–96
- sniffer attacks, 75
- sniffers (WLANs), 426
- SNMP (Simple Network Management Protocol), 179
 - deployment best practices, 598
 - security considerations, 597
 - use of, 597
- SOCKS, 286
- software
 - open source, 272
 - OS-based network security, 270–271
 - security legislation, 667
 - teleworker computers, design considerations, 578
 - vulnerabilities, 60
- SPD (security policy database), 362
- split tunneling (IPsec), 368–371

- spoofing attacks, 82
 - DNS, 306–307
 - IP spoofing, 84–92
 - MAC spoofing, 83
- SQL (Structured Query Language), 676
- SSH (Secure Shell), 178, 676
 - deployment, 595
 - firewalls, 186
 - use of, 594
- SSH/SSL, 436
- SSL (Secure Socket Layer), 311, 677
- SSL (Secure Socket Layer) offload, 417
- SSO (single sign-on), 331
- Stacheldraht, 98
- standards, 42
- stateful firewalls, 144–146
 - DMZ design, 280
 - high-end resilient campus security design, 563
 - high-end resilient edge design, 517
 - Internet edge, 502
- stateless security features, 250
- state-sharing security devices, 249
- static translation, 233
- stick model of security device load balancing, 423
- STP, 202–204
- support (open source software), 272
- switches, hardening, 184–186
- symmetric routing, 249
- SYN cookies, 261
- Syslog, 601, 677
 - deployment best practices, 602
 - security considerations, 601
- Syslog, 180

T

- TACACS+, 128
- taxonomies
 - attacks, 64–68
 - application manipulation attacks, 79–81
 - composite attacks, 108–115
 - direct access attacks, 77
 - flooding attacks, 94–96, 100–103
 - network manipulation attacks, 78
 - read attacks, 69
 - redirection attacks, 103–107
 - sniffer attacks, 75
 - spoofing attacks, 82–92
- TCN (Topology Change Notification), 211
- TCP (Transmission Control Protocol), 79, 251
- TCP Intercept, 261
- TCP resets, 294
- TCP spoofing, 87
- TCP SYN flooding, 100–101, 260
- technologies (security), 126
 - content filtering, 146–151
 - cryptography, 155–160
 - emerging technologies, 161
 - firewalls, 142–146
 - host and application security, 136–142
 - hybrid host systems, 161
 - identity technologies, 126–134
 - inside NIDS, 162
 - NIDS, 152–154
- teleworker security, 571
 - design evaluations, 583
 - hardware-based design, 579–582
 - host protections, 576

- identity, 575
- network-transit protections, 577
- software-based design, 578
- threats, 572–575
- Telnet
 - deployment, 595
 - use of, 594
- TFTP, 599–600
- theft of service, 63
- threat profile, 172
- threats
 - campus networks, 537–539
 - network edge, 482–484
 - OOB management, 620
 - teleworker systems, 572–575
 - traffic assessment, 664
- three-domain security design, choke points, 461
- three-interface firewall design, 281
- three-tier e-commerce network design, 526
- three-tier web design, 313–314
- TKIP, 429
- TLS (Transport Layer Security), 24, 677
- topologies
 - IPsec, split tunneling, 368, 371
 - IPsec VPNs, 371–374
 - centralized remote access firewall, 389
 - semitrusted, 386–388
 - trusted, 385
- Topology Change Notification (TCN), 211
- traffic
 - flow, 602
 - management, 454
- Transmission Control Protocol (TCP), 79, 251
- transparent caches, 414
- transport mode (IPsec), 360

- transport protocols, design considerations, 251
- transport redirection attacks, 106–107
- transport spoofing, 86
- triple DES (3DES), 367
- Trojan horses, 110–111
- troubleshooting
 - flooding, 252
 - preparing for attacks, 13
 - secure network management, 663–664
- trust, 455
 - choke points, 460
 - identities, 323
- trusted IPsec topology, 386
- tuning NIDS, 290
- tunnel mode (IPsec), 360
- tunneling (GRE), 379
- two-tier e-mail design, 300
- two-tier web design, 311

U

- UDP, 251
- UDP spoofing, 86–87
- University of Insecurity case study, 643
 - attack examples, 649–650
 - design choices, 646–648
 - migration strategy, 649
 - security requirements, 645
- uRPF (unicast reverse path forwarding), 232, 486
- usage vulnerabilities, 62
- user hosts
 - high-end resilient campus security design, 562
 - medium network campus security design, 552
 - small network campus design, 545

usernames
 identity, 328
 setup, 177

V

VACLs
 DHCP, 220
 warning, 221
van Eck freaking, 200
vendors, 30
virtual private networks. *See* VPNs
viruses, 110–111
VLAN Query Protocol (VQP), 208
VLAN Trunking Protocol (VTP), 207
VLANs
 DHCP snooping, 219
 hopping, 213–214
 PVLANS, 222–223
VPNs (virtual private networks), 353, 494
 core, distribution, and access design model,
 451
 high-end resilient edge security, 521
 IPsec
 firewall and NIDS placement,
 384–389
 platform options, 375–376
 topology choices, 371–374
 IPsec VPNs
 outsourcing, 407
 site-to-site deployment examples,
 392–406
 medium network remote access edge,
 505
 mobile worker concerns, 370
 overview, 353
 remote user VPNs, 356
 site-to-site VPNs, 355

VQP (VLAN Query Protocol), 208
VTP (VLAN Trunking Protocol), 207
vulnerabilities, 12–13, 60
 configuration, 62
 hardware, 61
 policy, 62
 scanning, 71
 software, 60
 usage, 62

W

WANs
 branch versus head-end design, 487
 core, distribution, and access design model,
 451
 distributed WAN considerations, 337
 high-end resilient edge security, 522
 medium network edge security, 506
 routers, small network edge security,
 492
war dialing/driving, 73
WCCP (Web Cache Control Protocol),
414
weapons, 14
web applications, 313–314
 attacks, 81
 two-tier web design, 311
Web Cache Control Protocol (WCCP),
414
web filtering, 148
WEP (Wired Equivalent Privacy), 46
 designing, 428
 WPA, 430
Wi-Fi Protected Access (WPA), 430
WLAN AP
 high-end resilient campus security
 design, 565

- medium network campus security
 - design, 553
- small network campus design, 546
- WLANs, 424
 - 802.11 security enhancements, 429
 - 802.11 WEP, 427, 431
 - access point hardening, 425
 - DoS attacks, 426
 - IPsec, 432
 - L3+ cryptography, 431
 - IPsec, 434
 - SSH/SSL, 436
 - rogue APs, 425
 - security, 46
 - differentiated groups WLANs, 440

- direct Internet access WLANs, 439
 - recomendations, 438
 - sniffers, 426
- worms, 110, 111
- WPA (Wi-Fi Protected Access), 430

X-Z

- Xauth (Extended Authentication), 366
- zone transfers (DNS servers), 307