Index

Numbers
3DES, 50–51, 321
802.1ae security (MACSec), 175
802.1x standard
 authentication server, 158
 authenticator, 158, 316
 ISE (Integrated Services Engine)
 and, 174
 RADIUS (Remote Authentication Dial-in User Service)
 authentication server and, 158
 TACACS+ comparison, 159
 supplicant, 158, 316
 TACACS+ (Terminal Access Controller Access Control System +), 316
 Active Directory and, 162–163
 administrative access configuration,
 160–161
 authentication server and, 158
 RADIUS comparison, 159
 router configuration, 162–163
 router connectivity, 164
ACL (access control list), 3, 6
ARP ACLs, 111–112, 311
network management and, 146–147
PACLs (port access lists), 133
router ACLs, 133
VACLs (VLAN access lists), 133–134
ACS (Access Control Server), 316
 authentication, 161–162
 authorization, 161–162
Active Directory, AAA services and, 162
Active/Standby failover, 248
Adleman, Leonard, 52
ADSM (Adaptive Security Device Manager),
configuration, initial, 250–251
AES (Advanced Encryption Standard),
51–52, 306
AH (Authentication Headers) protocol
ISAKMP (Internet Security Association),
191–192
tunnel mode, 192–193
AIC (Application Inspection Control), 325
firewalls and, 246
ALE (annual loss expectancy), 14
algorithms
 asymmetric, RSA, 52–53
 hash functions, 53
digital signatures, 55–57
HMAC (hash MAC), 55
MD5, 54
password hash values, 54
SHA-1, 54
SHA-2, 54–55
vulnerabilities, 54
polyalphabetic, 47–48
symmetric, 48–52
3DES, 50–51
AES (Advanced Encryption Standard),
51–52
AAA services
 ACS (Access Control Server), 161–162
 Active Directory and, 162
 ISE (Identity Services Engine), 161–162
 local authentication and accounting,
 160–161
 SSH and, 161
 acceptance, 15
 access ports, PortFast and, 114–115
 ACK flag, 31
 TCP SYN flood attack and, 35
block ciphers, 49, 306
DES (Digital Encryption Standard), 50
IVs (initialization vectors), 49
RC4, 52
stream-based ciphers, 50
alternate string expressions, IPS, 271
Always-On VPN, 197–198
anomaly-based detection methods, IPS, 267
anti-replay, IPsec and, 187
AnyConnect SSL VPN, 207–209, 322
application-level firewalls, 221
ARP (Address Resolution Protocol), 93
ARP ACLs, 111–112, 311
ARP broadcast, 93
ARP poisoning, 37, 93–95, 309
DAI (Dynamic ARP Inspection) and, 38
DHCP snooping and, 38
MAC address and, 94
man-in-the-middle attack, 304
ASA (Adaptive Security Appliance), 307
access policies
interface access rules, 253–254
object groups, 254–256
ASDM (Adaptive Security Device Manager), 250
configuration, initial, 250–251
default, 65
SCEP, 66–67
security levels, 251–252
viewing/adding, 65–66
ASA 9.x
firewall series
Active/Active failover, 248
Active/Standby failover, 248
AIC (Application Inspection Control), 246
Clustering, 249
deployment, 247
DHCP and, 246
IP routing, 246
IPv6 support, 246
NAT (Network Address Translation), 246
routed firewall, 247
security contexts, 249
site-to-site VPNs and, 212
transparent firewall, 247, 325
high availability implementation, 247–249
ASDM (Adaptive Security Device Manager)
clientless SSL VPN, 204–207
interface access rules, 254
assets, 6, 19
asymmetric algorithms, 305
RSA, 52–53
asymmetric encryption, 46
attacks. See also layer 2 attacks; threats
ARP poisoning, 37–38
birthday attack, 68
brute-force, 29
brute-force attack, 67
buffer overflow, 34
chosen ciphertext attack, 67
ciphertext-only attack, 67
data exfiltration, 39–40
dictionary, 29
DoS (denial-of-service), 34
exhaustive, 29
injection attacks, 270
known plaintext attack, 67
malware
spyware, 39
trojan horses, 39
viruses, 39
worms, 39
meet-in-the-middle attack, 68
MITM (man-in-the-middle), 37
motivations, 26–27
password, 29
ping of death, 35
ping scans, 30
reasons for, 26–27
reconnaissance, 30
smurf attack, 36–37
social engineering attacks
pharming, 38
phishing, 38
preventing, 38–39
TCP SYN flood, 34–35
vectors, 27–28
authentication, 321
AAA services, 160–161
ACS and, 161–162
ISE and, 161–162
key authentication, IPsec, 209–212
NTP, 150–151
authentication server
RADIUS and, 158
TACACS+, 158
AuthNoPriv mode, 145
AuthPriv mode, 145
AUX port, 142–143
AV (asset value), 14
availability, security and, 3
avoidance, 15

**B**

banner messages, 147, 315
EXEC banner, 148
login banner, 148
MOTD (message of the day), 148
verification, 148
birthday attack, 68
black hat, 27
block ciphers, 49, 306
BOYD (bring your own device)
inline SGT transport, 174–175
ISE (Integrated Services Engine) and,
  172–174
AAA server, 174
authentication mechanisms, 174
COA updates, 173
dACLs, 173
MAB (MAC authentication bypass), 174
posture assessment, 173
SGAs (Security Group Access), 173
VLAN assignment, automatic, 173
WebAuth (Web authentication), 174
SGACLs (security group access lists), 176
SGFW, 176
SGT classification and, 174
SXP (SGT eXchange Protocol), 175–176
TrustSec and, 174, 176–177, 318
BPDUs (bridge protocol data units), 92
BPDU Guard, 114–115, 119, 309, 311
brute-force attacks, 29, 67
buffer overflow, 34, 304
BYOD (bring your own device), 172

**C**

CA (certificate authority), 61–63
CAM (content addressable memory),
  overflows, 96–97, 310
port security and, 113
CAN (campus area network) topology
enterprise campus, 15
enterprise core, 15–16
intranet data center, 15
CCE (Common Configuration
  Enumeration), 11
CDP (Cisco Discovery Protocol), 97–98
disabling, 310
certificates
ASA (Adaptive Security Appliance)
  default, 65
  SCEP, 66–67
  viewing/adding, 65–66
CA (certificate authority), 61–63
digital, 60
revocation, 60
uses, 61
chosen ciphertext attack, 67
chosen plaintext attack, 67
CIA triad, 2, 19, 302
availability, 3
confidentiality, 2
integrity, 3
ciphers, 46
  ROT 13 Caesar cipher, 47
  substitution ciphers, 46–47
transposition, 48
  Vigenere cipher, 47–48
ciphertext-only attack, 67
circuit-level proxies, 221, 322
Cisco Common Classification Policy
Language, 236
class maps, 236, 237
default policy, 237–238
CLI (command-line interface), role-based, 74, 77–78
clientless SSL VPN, ASDM and, 204–207
cloud-based proxies, 293
Clustering, ASA firewalls, 249, 325
CMD (Cisco MetaData) header, inline SGT transport and, 174
COA (change of authorization), ISE (Integrated Services Engine), 173, 318
collisions, 54, 306
commercial businesses, data assets and, 9–10
Common Classification Policy Language, 236, 325
community ports, PVLANS, 129
compartmentalization, 4
confidentiality, security and, 2
console ports, 145–146
context-based filtering, email, 287
control plane
control plane packets, 83
CoPP (control plane policing), 83–84
data plane packets, 82
management plane packets, 83
packets, 83, 309
services plane packets, 83
controls, 6
cost-benefit analysis, 14
qualitative risk analysis, 13–14
quantitative risk analysis, 14
CoPP (control plane policing), 83–84
cost-benefit analysis, 14
countermeasures, 6, 19
CPE (Common Platform Enumeration), 11
crackers, 27
credit card information, 40
criticality, data assets, 9
CRL (certificate revocation list), 60, 307
cryptanalysis
birthday attack, 68
brute-force attack, 67
chosen ciphertext attack, 67
chosen plaintext attack, 67
ciphertext-only attack, 67
known plaintext attack, 67
meet-in-the-middle attack, 68
cryptography. See also encryption algorithms
polyalphabetic, 47–48
symmetric, 48–52
ciphers, 46
ROT 13 Caesar cipher, 47
substitution ciphers, 46–47
transposition, 48
hash functions, 53
digital signatures, 55–57
HMAC (hash MAC), 55
MD5, 54
password hash values, 54
SHA-1, 54
SHA-2, 54–55
vulnerabilities, 54
PKCS (Public Key Cryptography Standards), 63–64
PKI standards, 63–64
PKI topologies, 64–65
public key, 56
SSH (Secure Shell), 57
Suite B cryptographic algorithms, 188, 320
CVE (Common Vulnerabilities and Exposures), 11, 303
CVSS (Common Vulnerability Scoring System)
AC (access complexity), 12
Au (Authentication), 12
AV (access vector), 12
A (Availability), 12
C (Confidentiality), 12
I (Integrity), 13
CWE (Common Weakness Enumeration), 11
dACLs (downloadable ACLs), ISE (Integrated Services Engine), 173
DAI (Dynamic ARP Inspection), 110–112, 304, 305, 311
ARP poisoning and, 38
verifying, 117–118
data assets
commercial business classifications, 9–10
criticality, 8–9
government classifications, 10
ISO/IEC, 10
military classifications, 10
NISCC, 10
sensitivity, 8–9
TLP, 10
data center topology, 16
data classification, 9
data exfiltration
credit card information, 40
IP (intellectual property), 39–40, 305
PII (personally identifiable information), 40
data plane packets, 82
DDoS (distributed DoS) attack, 36
reflected, 36–37, 305
defense-in-depth security strategy, 4, 303
email threats, 286–287
firewalls and, 221–222
DES (Digital Encryption Standard)
3DES, 50–51
CBC (Cipher Block Chaining), 50–51
ECB (Electronic Code book), 50–51
symmetric algorithms and, 50
DHCP (Dynamic Host Configuration Protocol), 99–101, 311
DHCP snooping
ARP snooping and, 38, 304
configuration, 108–110
verifying, 116–117
DHCP spoofing, 99–101
DoS attacks, 100
firewalls and, 246
peer-to-peer attacks, 100
DHCPACK response packet, 108
DHCPNACK response packet, 108
DHCPPOFFER response packet, 108
dictionary attacks, 29
Diffie-Hellman key exchange, 187, 320
digital certificates, 60
digital signatures, 55–57, 306
DSA (Digital Security Algorithm), 57
DSS (Digital Signature Standard), 57
ECDSA (Elliptic Curve DSA), 57
direct DoS attack, 36
DLP (data loss prevention), email, 287, 328
DMZ (demilitarized zone), 17–18, 303
IPS positioning, 277
DoS (denial-of-service) attack, 34
DDoS (distributed DoS) attack, 36
reflected, 36–37, 305
DHCP and, 100
direct DoS attack, 36
double tagging, 99, 310, 312
DSA (Digital Security Algorithm), 57
DSS (Digital Signature Standard), 57
DTP (Dynamic Trunking Protocol), 98–99
disabling, 116, 312
switch ports, 310
verifying, 120

E

EAP-TLS, ISE authorization and, 177–178
ECB (Electronic Code Book), 50, 306
ECDHE-ECDSA (Elliptical Curve Diffie-Hellman Elliptical Curve Digital signature standard), 188, 320
ECDSA (Elliptic Curve DSA), 57
EF (exposure factor), 14, 303
EIGRP routing update authentication, 82, 308
email
anti-malware filtering, 287
blacklisting, 288
context-based filtering, 287
DLP (data loss prevention)
endpoint, 287
imprecise methods, 287
network, 287
precise methods, 287
encryption, 288
ESA (Email Security Appliance)
AMP (Advanced Malware Protection), 289, 329
anti-malware, 288–289
antivirus signatures, 289
context-based filtering, 288
DLP, 289
message flow, 290
outbound scanning, 289
outbreak filters, 288–289
reputation-based filtering, 288, 328
sandboxing, 290
viruses, 288–289
spam filtering, 286–287
spoofing, 29
encryption. See also cryptography
asymmetric algorithms, 46
RSA, 52–53
certificates
CA (certificate authority), 61–63
digital, 60
revocation, 60
SSL/TLS and, 61
uses, 61
email, 288
PKCS (Public Key Cryptography Standards), 63–64
PKI standards, 63–64
symmetric algorithms, 46, 48–49
3DES, 50–51
AES (Advanced Encryption Standard), 51–52
block ciphers, 49, 306
DES (Digital Encryption Standard), 50
IVs (initialization encryption vectors), 49
private-key, 49
RC4, 52
secret-key, 49
session keys, 49
shared-key, 49
single-key, 49
stream-based ciphers, 49, 50
endpoints
endpoint posture assessment,
AnyConnect SSL VPN, 209
threats
anti-malware, 294
antivirus, 294
encryption of local data, 294
HIPS (host-based IPS) and, 295
ISE (Identity Services Engine), 294
personal firewall, 294
ESA (Email Security Appliance), 286, 287
AMP (Advanced Malware Protection)
file reputation, 289, 329
file retrospection, 289
sandboxing, 290
anti-malware, 288–289
antivirus signatures, 289
cost-based filtering, 288
DLP (data loss prevention), PII
(personally identifiable information), 289
message flow, 290
outbound scanning, 289
outbreak filters, 288–289
reputation-based filtering, 288, 328
viruses, 288–289
ESP (Encrypting Security Payload), 319
ISAKMP (Internet Security Association), 192
tunnel mode, 193, 320
EXEC banner, 148
exhaustive attacks, 29
exposure, 6, 19
extranets, 18

F

file transfer, SCP (Secure Copy Protocol)
and, 151
FIN flag, 31
FIN scan, 31–32
fingerprinting, 30
OS fingerprinting, 33
FireSIGHT, 327
acting, 271
adapting, 271
AMP (Advanced Malware Protection), 272, 329
blacklisting, 272
deployment
inline, 275
passive mode, 273
SPAN port, 274
tap mode, 274
detection, 271
discovery and awareness, 273
dynamic file analysis, 273
FirePOWER, 272
learning, 271
Snort technology, 272
firewalls
AIC (Application Inspection Control), 246
application-level, 221
ASA firewalls
Active/Active failover, 248
Active/Standby failover, 248
Clustering, 249
deployment, 247
security contexts, 249
site-to-site VPNs and, 212
defense in depth and, 221–222
DHCP and, 246
host, 221
IP routing, 246
IPv6 support, 246
Kaspersky Internet Security, 221
NAT (Network Address Translation), 246
packet filtering, 322
personal, 221–222, 323
proxy, 220
circuit-level proxies, 221
kernel proxy, 221, 322
SOCKS firewall, 221
stateful
ACK flag, 222
operation, 222–223
state table, 223
SYN flag, 222
Zone Alarm Pro Firewall, 221
zone-based, 230
Cisco Common Classification Policy, 236
class maps, 236
self-zone, 238
zone-to-zone access, 239
flags
ACK, 31
FIN, 31
PSH, 31
RST, 31
scans, 30–31
state table, 223
SYN, 31
URG, 31
foreign governments, 26

government data asset classification, 10
gratuitous ARP, 94
DAI (Dynamic ARP Inspection) and, 111
gray hat, 27

hackers, 27
hacktivists, 27, 304
hairpinning, VPNs and, 195–196, 320
hash functions, 53
digital signatures, 55–57
HMAC (hash MAC), 55
MD5, 54
password hash values, 54
SHA-1, 54
SHA-2, 54–55
vulnerabilities, 54
HMAC (hash MAC), 55, 306
IPsec and, 187
host firewalls, 221, 323
HTTP
disable server, 315
proxy firewalls and, 221
HTTPS connections
disable server, 315
in-band connections, 142, 144
human threat agents, 27

ICMP packets, ping of death and, 35
ID repository
ACS (Access Control Server) and, 162
ISE (Identity Services Engine) and, 162
IKE v1 protocol
aggressive mode, 190
automatic key generation and, 189
automatic key refresh and, 189
main mode, 189–190
phase 1, 189
phase 2, 190
SA (security association) negotiation, 189
IKE v2 protocol, 190–191
in-band connections, 142, 314
HTTPS connections, 144
SNMP, 144–146
VTY ports, 143–144
informs, 144
injection attacks, IPS, 270
inline SGT transport, 174–175
integrity, 303
security and, 3
interface access rules, ASA access policies, 253–254
interfaces command, 77
intranets, 18, 19
IOS
privilege levels, 76–77
resilient configuration, 79–80
role-based CLI, 77–78
IP (intellectual property), 26, 39–40, 305
IP addresses
NAT (Network Address Translation) and, 230
spoofing, 28, 304
state tables, 223
ip command, 77
IP protocol, state tables, 223
IP routing, firewalls and, 246
IPS (Intrusion Prevention System) actions
block, 265
drops, 265
reset, 265
shun, 265
alternate string expressions, 271
assessment terms, 277–278
detection methods
anomaly based, 267
signature based, 267
DMZ positioning, 276
evasion techniques, 267–271
exploit, 328
HIPS (host-based IPS), 266
injection attacks, 270
inside positioning, 277
NIPS (network-based IPS), 266
outside positioning, 275–276
packet fragmentation, 267–269
promiscuous mode, 266
risk, 264
threats, 264
vulnerability, 265
zero-day threat, 265, 327
IPsec, 319, 320
delivery modes, 192
transport mode, 193–194
tunnel mode, 192–193
HMAC and, 187
IPV6, 194
protocols
AH, 191–192
ESP, 192
IKE v1, 189–190
IKE v2, 190–191
ISAKMP, 191
security services, 186
anti-replay, 187
confidentiality, 187
data integrity, 187
key management, 187–188
origin authentication, 187
Suite B cryptographic standard, 188–189
site-to-site VPNs, preshared key authentication, 209–212
IPv6
extension headers, 321
firewalls and, 246
IPsec and, 194
IS (information systems) infrastructure, 4
ISAKMP (Internet Security Association)
AH (Authentication Headers) protocol, 191–192
ESP (Encrypting Security Payload), 192
ISAKMP (Internet Security Association Key Management Protocol), 191
ISE (Integrated Services Engine), 318
authentication, 161–162
authorization, 161–162
BYOD (bring your own device) and, 172–174
mobile device management, 177–178
isolated ports, PVLANs, 129
IT infrastructure, 4
IVs (initialization vectors), 49

J
job rotation, security and, 5

K
Kaspersky Internet Security, 221
kernel proxy firewall, 221, 322
key authentication, IPsec, site-to-site VPNs and, 209–212
key management, IPsec and, 187
keychains, 80–82, 308
known plaintext attack, 67

L
layer 2 attacks
ARP poisoning attacks, 93–95
CAM overflows, 96–97
CDP/LLDP reconnaissance, 97–98
DHCP spoofing, 99–101
MAC attacks, 95–96
mitigating
DAI (Dynamic ARP Inspection), 110–112
DHCP snooping and, 108–110
DTP, disabling, 116
port security, 112–114
STP security features, 114–116
verification, 116–120
STP (Spanning Tree Protocol) attacks, 92–93
VLAN hopping
double tagging, 99
switch spoofing and, 98–99
least privilege principle, 3–4, 302
line console 0 command, 145–146
LLDP (Link Layer Discovery Protocol), 97–98
disabling, 310
local proxies, 293
login banner, 148
Loop Guard, 115–116, 119–120

M
MAB (MAC authentication bypass), ISE (Integrated Services Engine), 174
MAC addresses
attacks, 309
port security and, 113
spoofing, 28
MAC spoofing, 95–96, 305, 309
macof tool, 96–97
MACSec (802.1ae security), 175, 319
malware attacks
   spyware, 39
   trojan horses, 39
   viruses, 39
   worms, 39
management plane packets, 83
masquerading, 28–29
MD5 algorithm, 54, 308, 315
meet-in-the-middle attack, 68
military data asset classification, 10
mitigation, 15, 303
MITM (man-in-the-middle) attack, 37, 304
mobile device management, ISE (Integrated Services Engine), authorization and, 177–178
MOTD (message of the day), 148
MPF (Modular Policy Framework), 246, 326
class maps, 256
configuration, 256–257
policy maps, 256
service policies, 256
MQC (Modular QoS CLI)
class maps, 84
policy maps, 84
service policies, 84
MTU (maximum transmission unit), 267–269

N

NAT (Network Address Translation), 230, 324
ASA 9.x implementation
   auto NAT, 231
dynamic NAT, 230, 232
manual NAT, 231
manual NAT after auto NAT, 231
object-oriented approach, 230
PAT (Port Address Translation), 230, 233
Policy NAT, 233–234
static NAT, 230, 231–232
Twice NAT, 233–234
configuration viewing, 235
firewalls and, 246
NAT traversal, VPNs and, 198–199
show nat command, 235
translation viewing, 235
xlate command, 235
xlate detail command, 235
natural threat agents, 27
need-to-know principle, 3–4
network management
   ACLs and, 146–147
   banner messages, 147
   EXEC banner, 148
   login banner, 148
   MOTD (message of the day), 148
   verification, 148
   HTTP and, 146
   HTTPS and, 146
   NTP authentication and, 150–151
   SNMPv3 and, 147, 149
   SSH and, 146
NISCC (National Infrastructure Security Coordination Centre), 10, 303
NIST SP 800-30, 7, 11
Nmap, 30–31, 305
   FIN scan, 31–32
   NULL scan, 31
   XMAS scan, 33
noAuthNoPriv mode, 145
NTP authentication, 315
   network management and, 150–151
NULL scan, 31

O

OIDs, 144
operational threat agents, 27
organized crime, 26
origin authentication, IPsec and, 187
OS fingerprinting, 33
OSPF routing update, authentication, 80–82, 308
out-of-band connections, 142
console port, 145–146

P
packet filtering firewalls, 220, 322
packet fragmentation, IPS, 267–269
packets
  control plane, 83, 309
data plane, 82
management plane, 83
services plane, 83
PACLs (port access lists), 133
parser views, 77
password attacks, 29
passwords, VTY ports, 144
peer-to-peer attacks, DHCP and, 100
personal firewalls, 221–222, 323
PGP (Pretty Good Privacy), email encryption, 288
pharming, 38, 305
phishing, 38
physical threat agents, 27
PII (personally identifiable information), 40
ping of death, 35, 305
ping scans, 30
PKCS (Public Key Cryptography Standards), 63–64
PKI (public key infrastructure), 57–58
policy maps, 236
polyalphabetic algorithms, 47–48
port scans, 30–31, 304
port security, 112
  CAM overflows and, 113
  MAC addresses visible, 113
  verifying, 118
PortFast, 114–115
ports
  community, 129
  isolated, 129
  promiscuous, 129, 313
  protected, 131–132
  state tables, 223
  trunk ports, 98, 310
private keys, 306
private-key cryptography, 49
privilege levels, 76–77, 307
promiscuous mode, IPS, 267
promiscuous ports, 313
PVLANs, 129
protected ports, PVLAN Edge, 131–132
protocols, IPsec process
  IKE v1, 189–190
  IKE v2, 190–191
  ISAKMP, 191–192
proxies
  cloud-based, 293
  local, 293
  proxy attacks, PVLANs, 132–133
  proxy firewalls, 220
    circuit-level proxies, 221
    kernel proxy, 221
    SOCKS firewall, 221
  proxy servers, web caching and, 221
PSH flag, 31
public key cryptography, 56, 306
private keys, 58–59
public keys, 58–59
PVLAN Edge, 131–132, 313, 314
PVLANs (private VLANs), 128–129
ports
  community, 129
  isolated, 129
  promiscuous, 129
  proxy attacks, 132–133, 314
  set up, 129–131

Q
qualitative risk analysis, 13–14
quantitative risk analysis
  ALE (annual loss expectancy), 14
  SLE (single loss expectancy), 14
  AV (asset value), 14
  EF (exposure factor), 14
RA (registration authority), 61, 307
RADIUS (Remote Authentication Dial-in User Service), 316
authentication server and, 158
TACACS+ comparison, 159
RC4 algorithms, 52
reconnaissance attacks, 30
reflected DDoS (distributed DoS) attack, 36–37, 30
resilient configuration, 79–80
risk, 6, 19, 303
acceptance, 15
avoidance, 15
mitigation, 15
transfer, 15
risk management, 7, 302
acceptance, 15
asset classification, 8
assets, data assets, 8–10
avoidance, 15
controls
qualitative risk analysis, 13–14
quantitative risk analysis, 14
cost-benefit analysis, 14
mitigation, 15
transfer, 15
vulnerabilities, CVSS, 11–13
Rivest, Ron, 52
role-based CLI, 77–78
Root Guard, 115, 119
root view, 77–78
ROT 13 Caesar cipher, 47
routed firewalls, 247
router ospf command, 78
router security
control plane, 83
CoPP (control plane policing), 83–84
data plane packets, 82
management plane packets, 83
services plane packets, 83
EIGRGP routing update authentication, 82
IOS privilege levels, 76–77
OSPF routing update, authentication, 80–82
resilient configuration, 79–80
role-based CLI, 77–78
SSH access, 74–76
routers, TACACS+ and, 164
RSA asymmetric algorithm, 52–53, 306
RST flag, 31

SACLs (security group ACLs), 174
safeguards, 6
ScanLine, 30
scans
FIN scan, 31–32
flags, 30–31
NULL scan, 31
ping scans, 30
port scans, 30–31
XMAS, 33
SCAP (Security Content Automation Protocol), 11, 302
SCEP (Simple Certificate Enrollment Protocol), 66–67
SCP (Secure Copy Protocol), file transfer and, 151
secret-key cryptography, 49
secure boot-config command, 79
secure bootset, 79, 308
security
assets, 6
availability, 3
CIA triad, 2
confidentiality, 2
controls, 6
countermeasures, 6
defense-in-depth, 4
exposure, 6
goals, 2
guiding principles, 3–6
integrity, 3
job rotation, 5
least privilege, 3–4
need-to-know, 3–4
no access default, 4
risk, 6
safeguards, 6
separation of duties, 4–5
threat, 6
threat agent, 6
vacations, mandatory, 5–6
vulnerability, 6
security contexts, firewalls, 249
security levels, ASA interfaces, 251–252
security zones
DMZ (demilitarized zone), 17–18
extranets, 18
intranets, 18
private, 18
public, 18
self-zone in zone-based firewalls, 238
sensitivity, 302
data assets, 8–9
separation of duties, 4–5
service policies, 236
services plane packets, 83
SGACLs (security group access lists), 319
BOYD (bring your own device) and, 176
SGAs (Security Group Access), ISE
(Integrated Services Engine), 173, 318
SGFW, 319
BOYD (bring your own device) and, 176
SGT (security group tag)
SGAs (Security Group Access) and ISE, 173
SGT classification
BYOD (bring your own device) and, 174
dynamic tagging and, 174
static tagging and, 174
SHA-1 algorithm, 54
SHA-2 algorithm, 54–55, 306
Shamir, Adi, 52
shared-key cryptography, 49
signature-based detection methods, IPS, 267
single-key cryptography, 49
site-to-site VPNs, IPsec, preshared key authentication, 209–212
SLE (single loss expectancy), 14, 303
smurf attack, 36–37
SNMP (Simple Network Management Protocol)
in-band connections, 142, 144–146
OIDs, 144
SNMPv3, network management and, 147, 149
social engineering attacks
pharming, 38
phishing, 38
preventing, 38–39
SOCKS firewall, 221
SOHO (small office/home office) topology, 17
spam filtering, 286–287
SPF (Sender Policy Framework), 29, 305
split tunneling, VPNs and, 196–197, 321
spoofing, 28
DHCP, 99–101
e-mail, 29
IP address spoofing, 28, 304
MAC address spoofing, 28–29
switch spoofing, 98–99
spyware, 39
SSH (Secure Shell), 57
AAA services and, 161
configuration, 74–76
network management and, 146
VTY ports and, 146
SSL/TLS, 205–206
state sponsors, 26
stateful firewalls
ACK flag, 222
operation, 222–223
state table, 223
SYN flag, 222
STP (Spanning Tree Protocol) attacks, 92–93
BPDU Guard and, 114–115, 119
Loop Guard, 115–116, 119–120
Root Guard, 115, 119
verifying, 118–120
stream-based ciphers, 49, 306
substitution ciphers, 46–47
Suite B cryptographic algorithms, 320
ECDHE-ECDSA (Elliptical Curve Diffie-Hellman Elliptical Curve Digital signature standard), 188, 320
SuperScan, 30
SVI (switched virtual interfaces), router
  switches
    ACLs
      PACLS, 133
      VACLs, 133–134
    switch spoofing, 98–99
SXP (SGT eXchange Protocol), 319
BOYD (bring your own device) and,
  175–176
TrustSec and, 174, 318
symmetric algorithms, 48–49, 305–306
  3DES, 50–51
  AES (Advanced Encryption Standard),
    51–52
  block ciphers, 49, 306
DES (Digital Encryption Standard), 50
  IVs (initialization vectors), 49
private-key, 49
RC4, 52
secret-key, 49
session keys, 49
shared-key, 49
single-key, 49
stream-based ciphers, 49, 50
symmetric encryption, 46
SYN flag, 31

T

  tableaus, polyalphabetic ciphers, 47
TACACS+ (Terminal Access Controller
  Access Control System +), 316, 317
Active Directory and, 162–163
  administrative access configuration, 160–161
  authentication server and, 158
  RADIUS comparison, 159
  router configuration, 162–163
  router connectivity, 164
TCP SYN flood attack, 34–35
technical threat agents, 27
terrorist groups, 26
threats, 6, 19, 302
  actors, 26
  agents, 6, 19

human, 27
natural, 27
operational, 27
physical, 27
technical, 27
black hat, 27
crackers, 27
gray hat, 27
hackers, 27
hacktivists, 27
thrill hackers, 27
white hat, 27
thrill hackers, 27
timeouts, state table, 223
TLP (Traffic Light Protocol) classifications,
  10, 302, 303
TLS (Transport Layer Security)
  AnyConnect SSL VPN, 205
  clientless SSL VPN, 205
topologies, 18
  CAN (campus area network), 15–16
  data center, 16
  SOHO (small office/home office), 17
  virtual, 17
  WAN (wide area network), 16
transfer, 15
transparent firewall, 247, 325
transport mode, IPsec
  AH protocol, 193
  ESP, 194
transposition ciphers, 48
trap messages, informs, 144
trojan horses, 39
trunk ports, 310
double tagging and, 99
VLANs and, 98
TrustSec, 318
  BOYD (bring your own device) and, 176–177
  BYOD (bring your own device) and, 174
  SACLs (security group ACLs) and, 174
  SXP (SGT eXchange Protocol) and, 174
TTL (time-to-live) value, 270
tunnel mode, IPsec
  AH protocol, 192–193
  ESP, 193, 320
URG flag, 31

VeriSign certificates, 61, 307
Vigenere cipher, 47–48
virtual topology, 17
viruses, 39, 304
VLANs (virtual local area networks), 18–19, 303. See also PVLANs (private VLANs)
ACLs
  PACLs (port access lists), 133
  router ACLs, 133
  VACLs (VLAN access lists), 133–134
attack mitigation, 128
double tagging, 99, 310, 312
ISE (Integrated Services Engine),
  automatic assignment, 173
native, 128
VLAN hopping, 98–99, 310
VMware, FireSIGHT and, 271
VPNs (virtual private network)
  Always-On VPN, 197–198
  hairpinning, 195–196, 320
  IPsec and, 186
  NAT traversal, 198–199
remote access
  AnyConnect SSL, 207–209, 322
  clientless SSI, 204–207
  site-to-site, IPsec, 209–212
  split tunneling, 196–197, 321
VTY ports, 314
  SSH and, 146
VTY (virtual terminal) ports, 143–144
  in-band connections, 142
vulnerability, 6, 19, 303
controls
  qualitative risk analysis, 13–14
  quantitative risk analysis, 14
CVSS (Common Vulnerability Scoring System), 11–13

WAN (wide area network), 16
web caching, proxy servers and, 221
WebAuth (Web authentication), ISE (Integrated Services Engine), 174, 318
web-based threats
  web proxies and, 292–293
WSA (Web Security Appliance), 293–294
  AVC (Application Visibility and Control), 293–294
blacklisting, 293
malware scanning, 293
TLS/SSL decryption, 294
URL categorization, 293
URL filtering, 293
white hat, 27
worms, 39
write-view, 147
WSA (Web Security Appliance)
  AVC (Application Visibility and Control), 293–294
blacklisting, 293
malware scanning, 293, 329
TLS/SSL decryption, 294
URL categorization, 293
URL filtering, 293

X-Y-Z
X.509 standard, 307
PKIs and, 58
XMAS scan, 33, 305

Zone Alarm Pro Firewall, 221
zone-based firewalls, 230
  Cisco Common Classification Policy
    Language, 236
class maps, 236
self-zone, 238
zone-to-zone access, 239