ÍNDICE

INTRODUCCIÓN **15**

CAPÍTULO 1. FUNDAMENTOS DE SEGURIDAD EN LAS REDES **23**

1.1 PRINCIPIOS DE UNA RED SEGURA 23

1.1.1 Evolución de la seguridad en redes 24

1.1.2 Claves para la protección de datos 26

1.1.3 Hacking 27

1.1.4 Organizaciones de seguridad en redes 29

1.1.5 Dominios de la seguridad en redes 30

1.1.6 Políticas de seguridad en redes 32

1.1.7 Cisco SecureX Architecture 32

1.2 VULNERABILIDADES 33

1.2.1 Virus 34

1.2.2 Gusanos 34

1.2.3 Troyanos 35

1.2.4 Mitigación de virus, gusanos y troyanos 36

1.3 METODOLOGÍAS DE ATAQUE 37

1.3.1 Ataques de reconocimiento 37

1.3.2 Ataques de acceso 38

1.3.3 Ataques de denegación de servicio 38

1.3.4 Mitigación de ataques de red 39

1.3.5 Cisco Network Foundation Protection 41

1.4 FUNDAMENTOS PARA EL EXAMEN 45

CAPÍTULO 2. SEGURIDAD EN LOS ROUTERS 47
2.1 SEGURIDAD EN EL ROUTER 47
2.1.1 Modelos de defensa 47
2.1.2 Complementos de seguridad 49
2.1.3 Acceso administrativo seguro 50
2.2 CONFIGURACIÓN DE CONTRASEÑAS 51
2.2.1 Contraseña enable secret 52
2.2.2 Contraseña de consola 53
2.2.3 Contraseña de telnet 53
2.2.4 Contraseña de auxiliar 53
2.2.5 Seguridad mejorada para conexiones virtuales 54
2.2.6 Banners 57
2.2.7 Configuración de SSH 58
2.2.8 Configuración de SSH con CCP 63
2.3 ASIGNACIÓN DE ROLES 64
2.3.1 Configuración de niveles de privilegios 64
2.3.2 Configuración de acceso a la CLI basado en roles 66
2.4 PROTECCIÓN DE ARCHIVOS Y CONTRASEÑAS 70
2.4.1 Resguardo de la configuración e imagen IOS 70
2.4.2 Recuperación de contraseñas 73
2.5 FUNDAMENTOS PARA EL EXAMEN 75

CAPÍTULO 3. MONITORIZACIÓN Y ADMINISTRACIÓN DE LA RED 77
3.1 ADMINISTRACIÓN Y REPORTES 77
3.1.1 Syslog como herramienta de registro 78
3.1.2 Configuración de Syslog 79
3.2 SNMP 82
3.3 NTP 85
3.4 AUDITORÍAS DE SEGURIDAD 89
3.4.1 Asistente de Auditoría de Seguridad 92
3.4.2 Cisco AutoSecure 94
3.4.3 One-Step Lockdown 97
3.5 FUNDAMENTOS PARA EL EXAMEN 100

CAPÍTULO 4. AAA 101
4.1 INTRODUCCIÓN A AAA 101
4.1.1 Modos de acceso AAA 102
4.1.2 Autenticación AAA 103

4.1.3 Autorización AAA 103
4.1.4 Auditoría AAA 104
4.2 CONFIGURACIÓN LOCAL DE AAA 104
4.2.1 Configuración de AAA con CLI 104
4.2.2 Configuración de AAA con CCP 105
4.3 AUTENTICACIÓN AAA BASADA EN SERVIDOR 109
4.3.1 Protocolos de autenticación AAA 109
4.3.2 Cisco Secure ACS 111
4.3.3 Instalación de ACS 112
4.3.4 Configuración de ACS 114
4.4 CONFIGURACIÓN DE AUTENTICACIÓN BASADA EN SERVIDOR 121
4.4.1 Configuración de RADIUS y TACACS+ con CLI 122
4.5 CONFIGURACIÓN DE TACACS+ CON CCP 124
4.6 RESOLUCIÓN DE FALLOS EN AAA 128
4.7 CONFIGURACIÓN DE AUTORIZACIÓN BASADA EN SERVIDOR 130
4.7.1 Configuración de autorización con CCP 132
4.8 REGISTRO DE AUDITORÍA AAA BASADA EN SERVIDOR 134
4.8.1 Configuración del registro de auditoría 134
4.9 FUNDAMENTOS PARA EL EXAMEN 136

CAPÍTULO 5. SEGURIDAD DE CAPA 2 137
5.1 SEGURIDAD DE LAN 137
5.1.1 Seguridad en los dispositivos finales 138
5.1.2 Dispositivos Cisco de seguridad para terminales 138
5.2 SEGURIDAD EN CAPA 2 140
5.2.1 Ataques comunes de capa 2 140
5.3 SEGURIDAD DE PUERTOS DE CAPA 2 142
5.3.1 Configuración de seguridad de puertos 142
5.3.2 Verificación de la seguridad de puertos 145
5.4 CONTROL DE TORMENTAS 147
5.4.1 Configuración de control de tormentas 147
5.5 PROTECCIÓN DE LAS TOPOLOGÍAS STP 148
5.5.1 Configuración de BPDU Guard 149
5.5.2 Configuración de BPDU Filter 150
5.5.3 Configuración de Root Guard 150
5.6 SEGURIDAD EN VLAN 151
5.6.1 Seguridad del enlace troncal 151
5.6.2 Configuración de un enlace troncal seguro 152

5.6.3 VLAN Access Lists 152
5.6.4 Private VLAN 153
5.6.5 Private VLAN Edge 155
5.6.6 Switched Port Analyzer 156
5.7 FUNDAMENTOS PARA EL EXAMEN 157

CAPÍTULO 6. LISTAS DE CONTROL DE ACCESO 159
6.1 INTRODUCCIÓN A ACL 159
6.1.1 Funcionamiento de las ACL 159
6.1.2 Mitigación de ataques con ACL 161
6.1.3 Tipos de lista de acceso 161
6.2 UBICACIÓN DE LAS ACL 162
6.2.1 Lista de acceso entrante 163
6.2.2 Lista de acceso saliente 163
6.3 RECOMENDACIONES EN EL DISEÑO DE LAS ACL 164
6.4 CONFIGURACIÓN DE ACL NUMERADA 165
6.4.1 Configuración de ACL estándar 166
6.4.2 Configuración de ACL extendida 167
6.4.3 Asociación de las ACL a una interfaz 168
6.4.4 Aplicación de una ACL a la línea de telnet 169
6.5 LISTAS DE ACCESO CON NOMBRE 169
6.5.1 Configuración de ACL nombrada 170
6.6 MENSAJES DE REGISTRO EN LAS ACL 170
6.7 CONFIGURACIÓN DE ACL CON CCP 171
6.8 LISTAS DE ACCESO REFLEXIVAS 175
6.9 LISTAS DE ACCESO DINÁMICAS 178
6.10 LISTAS DE ACCESO BASADAS EN TIEMPO 180
6.11 VERIFICACIÓN DE LISTAS DE ACCESO 182
6.12 LISTAS DE ACCESO IPV6 184
6.13 OBJECT GROUP 185
6.13.1 Características de los object group 186
6.13.2 Configuración de los object group 186
6.14 FUNDAMENTOS PARA EL EXAMEN 190

CAPÍTULO 7. FIREWALLS 191
7.1 REDES SEGURAS CON FIREWALLS 191
7.1.1 Características de los firewalls 192
7.1.2 Tipos de firewall 193

7.1.3 Diseño de redes con firewalls 195
7.2 CONTROL DE ACCESO BASADO EN EL CONTEXTO 197
7.2.1 Funcionamiento de CBAC 199
7.2.2 Configuración de CBAC 200
7.2.3 Verificación de CBAC 204
7.3 FIREWALL BASADO EN ZONAS 207
7.3.1 Funcionamiento del firewall basado en zonas 208
7.3.2 Configuración del firewall basado en zonas 212
7.3.3 Configuración del firewall basado en zonas con CCP 214
7.3.4 Configuración manual del firewall basado en zonas con CCP 218
7.4 RESOLUCIÓN DE PROBLEMAS EN EL FIREWALL BASADO EN ZONAS 226
7.5 CISCO ADAPTIVE SECURITY APPLIANCE 228
7.5.1 Características del Cisco ASA 231
7.5.2 Configuración básica del firewall Cisco ASA 232
7.5.3 Configuración del firewall Cisco ASA con ASDM 238
7.6 CONFIGURACIÓN AVANZADA DEL FIREWALL CISCO ASA 245
7.6.1 Configuración de object groups 245
7.6.2 Configuración de ACL 251
7.6.3 Configuración de NAT 255
7.6.4 Configuración de control de acceso 261
7.6.5 Configuración de políticas 264
7.6.6 Configuración de acceso remoto y VPN 266
7.7 FUNDAMENTOS PARA EL EXAMEN 276

CAPÍTULO 8. CISCO IPS 277
8.1 CARACTERÍSTICAS DE LOS IDS E IPS 277
8.1.1 Implementaciones IPS basadas en red 279
8.2 FIRMAS IPS 282
8.2.1 Tipos de firmas 282
8.2.2 Alarmas de firmas 283
8.2.3 Acciones de firmas 286
8.2.4 Administración y monitorización IPS 287
8.3 CONFIGURACIÓN DE CISCO IOS IPS 288
8.3.1 Configuración de IPS con CLI 288
8.3.2 Configuración de IPS con CCP 294
8.3.3 Modificación de las firmas 299
8.3.4 Verificación y monitorización de Cisco IOS IPS 300
8.4 FUNDAMENTOS PARA EL EXAMEN 303

CAPÍTULO 9. TECNOLOGÍAS VPN 305
9.1 REDES PRIVADAS VIRTUALES 305
9.2 TÚNELES GRE 306
9.2.1 Configuración básica de túneles GRE 307
9.3 IPSEC 309
9.3.1 Características de IPsec 309
9.3.2 Modos de IPsec 311
9.3.3 Cabeceras IPsec 312
9.4 PROTOCOLOS DE IPSEC 312
9.4.1 IKE 312
9.4.2 ESP 312
9.4.3 AH 313
9.4.4 Autenticación de vecinos 314
9.5 INTERNET KEY EXCHANGE 314
9.5.1 Protocolos IKE 315
9.5.2 Fases IKE 315
9.5.3 Modos IKE 315
9.5.4 Funciones adicionales IKE 316
9.6 ALGORITMOS DE ENCRIPTACIÓN 317
9.6.1 Encriptación simétrica 317
9.6.2 Encriptación asimétrica 318
9.7 PUBLIC KEY INFRASTRUCTURE 319
9.8 CONFIGURACIÓN DE VPN SITE-TO-SITE 320
9.8.1 Configuración de la política ISAKMP 321
9.8.2 Configuración de los IPsec transform sets 322
9.8.3 Configuración de la Crypto ACL 325
9.8.4 Configuración del Crypto Map 325
9.8.5 Aplicación del Crypto Map a una interfaz 326
9.8.6 Configuración de ACL en una interfaz 327
9.9 VERIFICACIÓN 328
9.10 CONFIGURACIÓN DE IPSEC CON CCP 330
9.11 VPN DE ACCESO REMOTO 339
9.11.1 SSL VPN 339
9.11.2 Cisco Easy VPN 342
9.11.3 Servidor Cisco Easy VPN 344
9.12 FUNDAMENTOS PARA EL EXAMEN 351

ANEXO 1. INTRODUCCIÓN A IPV6 353
DIRECCIONAMIENTO IPV6 353
Formato del direccionamiento IPv6 355
Tipos de comunicación IPv6 356

ANEXO 2. CUESTIONARIO 357
PREPARATIVOS PARA EL EXAMEN 357
Recomendaciones para la presentación al examen 357
CUESTIONARIO TEMÁTICO 358

ÍNDICE ALFABÉTICO 397