
Tabla de contenido

<i>Prólogo</i>	<i>xvii</i>
<i>Prefacio</i>	<i>xxi</i>
<i>I: Seguridad en redes</i>	<i>1</i>
<i>1: Por qué firewalls para Internet</i>	<i>3</i>
Qué intenta proteger	4
Contra qué intenta protegerse	7
Cómo puede proteger su sitio	13
Qué es un firewall para Internet	17
<i>2: Servicios de Internet</i>	<i>25</i>
Correo electrónico	26
Transferencia de archivos	28
Acceso de terminal remota y ejecución de comandos	30
Noticias de Usenet	31
World Wide Web	32
Otros servicios de información	34
Información sobre personas	35
Servicios de conferencias en tiempo real	37
Servicio de nombres	38
Servicios para administración de redes	39
Servicio de hora	40
Sistemas de archivos de red (NFS)	41

Sistemas de ventanas	42
Sistemas de impresión	42
3: Estrategias de seguridad	45
Menor privilegio	45
Defensa a fondo	47
Punto de choque	48
Eslabón más débil	48
Postura de falla segura	49
Participación universal	52
Diversificación de defensa	53
Simplicidad	54
II: Construcción de firewalls	55
4: Diseño de firewalls	57
Algunas definiciones de firewall	57
Arquitecturas de firewalls	63
Variaciones en las arquitecturas de firewalls	71
Firewalls internos	82
Qué depara el futuro	88
5: Anfitriones bastión	91
Principios generales	92
Tipos especiales de anfitriones bastión	93
Cómo seleccionar una máquina	94
Cómo seleccionar una ubicación física	98
Cómo ubicar al anfitrión bastión en la red	99
Cómo seleccionar los servicios proporcionados por el anfitrión bastión	100
No permita cuentas de usuario en el anfitrión bastión	102
Cómo construir un anfitrión bastión	103
Cómo operar el anfitrión bastión	126
Cómo proteger la máquina y las copias de respaldo	128
6: Filtrado de paquetes	131
Por qué filtrado de paquetes	132
Cómo configurar un enrutador con filtrado de paquetes	136

Cómo es un paquete	138
Qué hace el enrutador con los paquetes	154
Convenciones para las reglas de filtrado de paquetes	158
Filtrado por dirección	161
Filtrado por servicio	164
Elección de un enrutador con filtrado de paquetes	168
Dónde hacer filtrado de paquetes	180
Síntesis	182
7: <i>Sistemas proxy</i>	189
Por qué utilizar un proxy	190
Cómo funciona un proxy	193
Terminología para servidores proxy	195
Uso de un proxy con servicios de Internet	197
Uso de un proxy sin un servidor proxy	199
Uso de SOCKS para proxy	200
Uso del juego de herramientas TIS Internet Firewall para proxy	202
Qué pasa si no puede utilizar un proxy	204
8: <i>Cómo configurar servicios de Internet</i>	207
Correo electrónico	209
Protocolo Simple de Transferencia de Correo (SMTP o Simple Mail Transfer Protocol)	211
Protocolo de Oficina Postal (POP o Post Office Protocol)	218
Extensiones Multimedia de Correo de Internet (MIME o Multimedia Internet Mail Extensions)	221
Transferencia de archivos	222
Protocolo para Transferencia de Archivos (FTP o File Transfer Protocol)	223
Protocolo Trivial de Transferencia de Archivos (TFTP o Trivial File Transfer Protocol)	234
Protocolo de Servicio de Archivos (FSP o File Service Protocol)	235
Protocolo para Copia Unix a Unix (UUCP o UNIX-to-UNIX Copy Protocol)	236
Acceso de terminal (Telnet)	238
Características de Telnet para filtrado de paquetes	239
Características de Telnet para usarlo con proxy	240
Resumen de recomendaciones para Telnet	240
Ejecución remota de comandos	240
Comandos 'r' de BSD	240

rexec	243
rex	244
Protocolo de la Transferencia de Noticias de Red (NNTP o Network News Transfer Protocol)	245
Características de NNTP para filtrado de paquetes	245
Características de NNTP para usarlo con proxy	246
Formas peligrosas de instalar NNTP en un ambiente de firewall	247
Formas correctas de configurar NNTP en un ambiente de firewall	249
Uso del filtrado de paquetes con NNTP	250
Resumen de recomendaciones para NNTP	250
World Wide Web (WWW) y HTTP	250
Características de HTTP para filtrado de paquetes	251
Características de HTTP para usarlo con proxy	253
Preocupaciones de la seguridad de HTTP	254
HTTP protegido	259
Resumen de recomendaciones para WWW	259
Otros servicios de información	260
Gopher	260
Servidores de Información de Área Amplia	262
Archie	264
Servicios para búsqueda de información	266
finger	267
whois	268
Servicios para conferencias en tiempo real	270
talk	270
Internet Relay Chat (IRC)	272
Multicast Backbone (MBONE)	275
Sistema de nomenclatura de dominios (DNS o Domain Name System)	278
Características de DNS para filtrado de paquetes	279
Características de DNS para usarlo con proxy	281
Datos DNS	282
Problemas de seguridad de DNS	284
Configure DNS para ocultar información	286
Configuración de DNS sin ocultar información	294
Resumen de recomendaciones para DNS	296
syslog	296
Características de syslog para filtrado de paquetes	297
Características de syslog para usarlo con proxy	297

Resumen de recomendaciones para syslog	297
Servicios para administración de redes	297
Protocolo Simple para Administración de Redes (SNMP o Simple Network Management Protocol)	297
Protocolo de Información de Enrutamiento (RIP)	300
ping	301
traceroute	302
Otros paquetes ICMP	304
Características de ICMP para filtrado de paquetes	305
Protocolo de hora de Red (NTP o Network Time Protocol)	306
Características de NTP para filtrado de paquetes	306
Características de NTP para usarlo con proxy	307
Configuración de NTP para trabajar con un firewall	307
Resumen de recomendaciones para NTP	308
Sistema de archivos de red (NFS o Network File System)	309
Características de NFS para filtrado de paquetes	311
Características de NFS para usarlo con proxy	312
Resumen de recomendaciones para NFS	312
Servicio de Información de Redes/Páginas Amarillas (NIS/YP o Network Information Service/Yellow Pages)	312
Características de NIS/YP para filtrado de paquetes	313
Características de NIS/YP para usarlo con proxy	313
Resumen de recomendaciones para NIS/YP	313
Sistema de ventanas X11	313
Características de X11 para filtrado de paquetes	315
Resumen de recomendaciones para X11	317
Protocolos de impresión (lpr y lp)	317
Características de lpr para filtrado de paquetes	318
Características de lpr para usarlo con proxy	318
Características de lp para filtrado de paquetes y proxy	319
Resumen de recomendaciones para protocolos de impresión	319
Análisis de otros protocolos	319
9: Dos ejemplos de firewalls	321
Arquitectura de subred de protección	321
Arquitectura de anfitrión de protección	340

10: Autenticación y servicios de entrada	351
Riesgos de utilizar servicios de entrada	352
Qué es autenticación	356
Mecanismos de autenticación	359
Sistemas de autenticación completa	365
Encriptación a nivel de red	370
Servidores de terminal y grupos de módems	374
III: Cómo mantener su sitio seguro	377
11: Políticas de seguridad	379
Su política de seguridad	380
Cómo conformar una política de seguridad	386
Toma de decisiones sobre estrategia y política	389
Qué pasa si no puede lograr una política de seguridad	394
12: Mantenimiento de firewalls	395
Mantenimiento	395
Monitoreo de su sistema	398
Cómo mantenerse actualizado	407
Cuánto tiempo toma	410
Cuándo debe volver a empezar	411
13: Cómo responder a los incidentes de seguridad	413
Cómo responder a un incidente	413
Qué hacer después de un incidente	421
Persecución y captura del intruso	422
Planifique su respuesta	425
Estar preparados	434
IV: Apéndices	441
A: Recursos	443
Páginas WWW	443
Sitios FTP	444
Listas de distribución de correo	444

Grupos de noticias	446
Equipos de respuesta y otras organizaciones	447
Conferencias	450
Documentos	452
Libros	454
<i>B: Herramientas</i>	457
Herramientas de autenticación	458
Herramientas de análisis	459
Herramientas para filtrado de paquetes	461
Herramientas para sistemas proxy	462
Daemons	462
Utilerías	463
<i>C: Principios básicos de TCP/IP</i>	465
Introducción a TCP/IP	465
Un modelo de comunicación de datos	466
Arquitectura de TCP/IP	469
Nivel de acceso	470
Nivel de Internet	472
Nivel de transporte	477
Nivel de aplicación	481
Direccionamiento, enrutamiento y multiplexaje	483
Dirección IP	485
Arquitectura de enrutamiento de Internet	491
Tabla de enrutamiento	493
Protocolos, puertos y sockets	496
<i>Índice</i>	503