

# Obsah:

<b>Předmluva</b>	<b>xiii</b>
<b>Úvodem</b>	<b>xvii</b>
<b>Část 1: Síťová bezpečnost</b>	<b>1</b>
<b>Kapitola 1: Proč internetové firewally?</b>	<b>3</b>
Co se pokoušíte chránit?	4
Proti čemu se pokoušíte bránit?	7
Jak můžete chránit vaši síť?	13
Co je internetový firewall?	17
<b>Kapitola 2: Služby na Internetu</b>	<b>25</b>
Elektronická pošta	26
Přenos souborů	28
Usenet News	31
World Wide Web	32
Další informační služby	34
Informace o lidech	35
Real-time konferenční služby	37
Name služby	38
Služby řízení sítě	39
Time služby	40
Síťový systém souborů	41
Window systémy	42
Tiskové systémy	42
<b>Kapitola 3: Bezpečnostní strategie</b>	<b>45</b>
Nejmenší privilegium	45
Obrana do hloubky	47
Škrťící bod	48
Nejslabší článek	48
Postoj bezpečného selhání	49
Všeobecná účast	52
Rozmanitost obrany	53
Jednoduchost	54

<b>Část II: Výstavba firewallů</b>	<b>55</b>
<b>Kapitola 4: Návrh firewallů</b>	<b>57</b>
Některé definice firewallů	57
Architektury firewallů	63
Variace na architektury firewallů	71
Interní firewally	82
Co přinese budoucnost	88
<b>Kapitola 5: Bastion hostitelé</b>	<b>91</b>
Obecné principy	92
Speciální druhy bastion hostitelů	93
Výběr počítače	94
Výběr fyzického umístění	98
Umístění bastion hostitele v síti	99
Výběr služeb poskytovaných bastion hostitelem	100
Nedovolte, aby byly na bastion hostiteli uživatelské účty!	102
Vybudování bastion hostitele	103
Obsluha bastion hostitele	126
Ochrana stanice záloh	128
<b>Kapitola 6: Filtrování paketů</b>	<b>131</b>
Proč filtrování paketů?	132
Konfigurace směrovače pro filtrování paketů	136
Jak vypadá paket	138
Co provádí směrovač s pakety?	154
Konvence pro pravidla filtrování paketů	158
Filtrování podle adresy	161
Filtrování podle služby	164
Volba směrovače pro filtrování paketů	168
Měl by umět zaznamenávat přijaté a odmítnuté pakety	179
Kde provádět filtrování paketů	180
Spojení všeho dohromady	182
<b>Kapitola 7: Proxy-systémy</b>	<b>189</b>
Proč proxy?	190
Jak proxy-systém pracuje	193
Terminologie - proxy servery	195
Použití proxy u služeb Internetu	197
Proxy provoz bez proxy serveru	199
Použití SOCKS při proxy provozu	200
TIS Internet Firewall Toolkit - použití pro proxy	202
Co dělat, když nemůžete použít proxy?	204

<b>Kapitola 8: Konfigurace internetových služeb</b>	<b>207</b>
Elektronická pošta	209
Přenos souborů	222
Terminálový přístup	238
Vzdálené provádění příkazů	240
NNTP (Network News Transfer Protocol)	245
World Wide Web (WWW) a HTTP	250
Další informační služby	260
Vyhledávací informační služby	266
Služby zajišťující konference v reálném čase	270
DNS (Domain Name System)	278
Služby pro správu sítě	297
NTP (Network Time Protocol)	306
NFS (Network File System)	309
NIS/YP (Network Information Service/Yellow Pages)	312
Window Systems X11	313
Tiskové protokoly (lpr a lp)	317
Analýza jiných protokolů	319
<b>Kapitola 9: Dva ukázkové firewally</b>	<b>321</b>
Stíněná subsíťová architektura	321
Stíněná hostitelská architektura	340
<b>Kapitola 10: Autentifikace a příchozí služby</b>	<b>351</b>
Mechanismy autentifikace	359
Systémy pro úplnou autentifikaci	365
Šifrování na úrovni sítě	370
Terminálové servery a modemové banky	374
<b>Část III: Udržování bezpečnosti vašeho systému</b>	<b>377</b>
<b>Kapitola 11: Bezpečnostní politiky</b>	<b>379</b>
Vaše bezpečnostní politika	380
Budování bezpečnostní politiky	386
Dosažení strategických a politických rozhodnutí	389
Co když nedokážete bezpečnostní politiku vytvořit?	394
<b>Kapitola 12: Údržba firewallu</b>	<b>395</b>
Průběžná péče	395
Monitorování systému	398
Údržba aktuálnosti	407
Kolik času to zabere?	410
Kdy začít znovu?	411

<b><i>Kapitola 13: Reakce na „bezpečnostní události“</i></b>	<b>413</b>
Reakce na událost	413
Co dělat po vzniku události	421
Sledování a zachycení vetřelce	422
Plánování reakce	425
Být připraven	434
<b><i>Část IV: Dodatky</i></b>	<b>441</b>
<b><i>Dodatek A: Zdroje</i></b>	<b>443</b>
WWW-stránky	443
FTP	444
Poštovní seznamy	444
Skupiny News (News groups)	446
Response Teams a jiné organizace	447
Konference	450
Články	452
Knihy	454
<b><i>Dodatek B: Nástroje</i></b>	<b>457</b>
Nástroje pro ověření totožnosti	458
Analyzační nástroje	459
Nástroje pro filtrování paketů	461
Nástroje pro proxy-systémy	462
Démoni	462
Utility	463
<b><i>Dodatek C: Základy TZP/IP</i></b>	<b>465</b>
Úvod do TZP/IP	465
Architektura protokolu TZP/IP	469
Vrstva přístupu k síti	470
Internetová vrstva	472
Přenosová vrstva	477
Aplikační vrstva	481
Adresování, směrování a multiplexing	483
IP-adresa	485
Směrovací architektura Internetu	491
Směrovací tabulka	493
Protokoly, porty a sokety	496
<b><i>Rejstřík</i></b>	<b>503</b>