

# Obsah

Předmluva .....	6
Poděkování .....	24
Úvod .....	25
Kdo by si měl koupit tuto knihu .....	25
Jak je tato kniha uspořádána .....	26
Část 1: Zabezpečení systému .....	26
Kapitola 1: Základy zabezpečení Linuxu .....	26
Kapitola 2: Instalace a nastavení systému .....	26
Kapitola 3: Sledování a audit systému .....	27
Část 2: Zabezpečení sítě .....	27
Kapitola 4: Nastavení síťových služeb .....	27
Kapitola 5: Sledování a auditování sítě .....	27
Část 3: Zabezpečení aplikací .....	27
Kapitola 6: Elektronická pošta .....	27
Kapitola 7: Služby HTTP .....	27
Kapitola 8: Zabezpečení služby Samba .....	28
Část 4: Zabezpečení perimetru .....	28
Kapitola 9: Firewally na úrovni síťové vrstvy .....	28
Kapitola 10: Firewally na úrovni transportní vrstvy .....	28
Kapitola 11: Firewally na úrovni aplikační vrstvy .....	28
Část 5: Vzdálený přístup a ověřování .....	28
Kapitola 12: Virtuální privátní sítě .....	28
Kapitola 13: Silné ověřování uživatelů .....	29
Přílohy .....	29
Příloha A: Další zdroje informací .....	29
Příloha B: Moduly PAM .....	29
Konvence .....	29
Pomozte nám pomoci vám .....	30
Část 1. Zabezpečení systému .....	31
1. Základy zabezpečení Linuxu .....	33
Základy zabezpečení informací .....	33
Terminologie zabezpečení .....	33
Bašta (Bastion host) .....	34
DMZ (Demilitarizovaná zóna) .....	34

Extranet .....	35
Firewall .....	36
Intranet .....	36
Paketový filtr .....	37
Server proxy .....	37
Zabezpečení pomocí skrývání .....	37
<b>Proces zabezpečení informací .....</b>	<b>37</b>
Vývoj zásad zabezpečení – tvorba bezpečnostní politiky .....	38
Verze .....	38
Úvod .....	38
Schéma sítě .....	38
Fyzické zabezpečení .....	39
Služby intranetu a extranetu .....	39
Vzdálený přístup .....	39
Nastavení firewallu .....	39
Zásady uživatelských účtů .....	39
Zásady používání dat .....	39
Audit, sledování a prosazování zásad .....	40
Oficiální souhlas .....	40
Implementace mechanismu zabezpečení .....	40
Fyzické zabezpečení .....	40
Služby intranetu a extranetu .....	40
Vzdálený přístup .....	41
Zásady uživatelských účtů .....	41
Zásady používání dat .....	41
Auditování, sledování a prosazování zásad .....	41
Periodické úpravy zásad a audit zabezpečení .....	41
<b>Cíle zabezpečení informací .....</b>	<b>42</b>
<b>Utajení dat .....</b>	<b>42</b>
Šifrování pomocí privátního klíče .....	43
Šifrování pomocí veřejného klíče .....	43
<b>Integrita dat .....</b>	<b>43</b>
<b>Ověřování uživatelů a řízení přístupu .....</b>	<b>44</b>
<b>Dostupnost dat a služeb .....</b>	<b>45</b>
<b>Zabezpečení Linuxu .....</b>	<b>45</b>
<b>Druhy útočníků .....</b>	<b>45</b>
Výtržníci .....	46
Členové kultu .....	46
Vyzvědači .....	46
Zasvěcenci .....	46



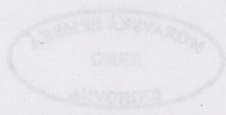
Firewall pro dvě sítě: veřejné a privátní adresy .....	269
Firewall pro tři sítě s demilitarizovanou zónou .....	272
Ochrana proti známým útokům .....	275
Falšování adres (Address Spoofing) .....	275
Útok Smurf .....	275
Útok Syn-Flood .....	276
Útok skenováním portů .....	276
Útok Ping smrti .....	276
Překlad síťových adres .....	276
NAPT (Network Address Port Translation) .....	277
Statický NAT .....	277
LSNAT (Load-Sharing Network Address Translation) .....	278
Konfigurace NAT pomocí iptables .....	278
Shrnutí .....	279
<b>10. Firewally na úrovni transportní vrstvy .....</b>	<b>281</b>
<b>    Servery proxy .....</b>	<b>281</b>
Servery proxy na úrovni transportní vrstvy .....	282
Servery proxy na úrovni aplikační vrstvy .....	282
<b>    Protokol SOCKS .....</b>	<b>282</b>
<b>    SOCKS4 vs. SOCKS5 .....</b>	<b>283</b>
<b>    Potřebujete SOCKS? .....</b>	<b>283</b>
<b>    Server proxy NEC SOCKS5 .....</b>	<b>284</b>
Pro jednu síť .....	284
Pro dvě sítě .....	284
<b>    Instalace SOCKS5 z RPM .....</b>	<b>284</b>
<b>    Kompilace nejnovější verze SOCKS5 .....</b>	<b>285</b>
Parametry kompilace pro Linux .....	288
Software, který SOCKS5 neobsahuje .....	293
Ověřování Kerberos5 (--with-krb5[=path]) .....	293
Ident (--with-ident[=path]) .....	293
Sestavování spustitelného souboru serveru SOCKS5 .....	293
<b>    Konfigurace serveru SOCKS5 .....</b>	<b>294</b>
Direktiva ban .....	294
Syntaxe .....	294
Příklady .....	295
Direktiva auth .....	295
Syntaxe .....	295
Příklady .....	295

Direktiva interface .....	296
Syntaxe .....	296
Příklady .....	296
Direktivy proxy-type .....	297
Syntaxe .....	297
Příklady .....	298
Direktiva permit/deny .....	298
Syntaxe .....	298
Příklady .....	299
Direktiva set .....	299
Syntaxe .....	299
Příklady .....	299
Pochopení hledání vzorků v socks5.conf .....	300
Vzorky hostitelů .....	300
Vzorky portů .....	302
Vzorky ověřování .....	302
Vzorky příkazů .....	303
<b>Soubor s hesly pro SOCKS5 .....</b>	<b>303</b>
<b>Spouštění a zastavování serveru SOCKS5 .....</b>	<b>304</b>
Samostatný .....	304
Předem spuštěné podprocesy .....	304
inetd .....	304
S vlákny .....	304
<b>Skript runsocks .....</b>	<b>307</b>
<b>Konfigurace sdílené knihovny SOCKS5 .....</b>	<b>308</b>
<b>Konfigurace klientů SOCKS5 se systémy Windows .....</b>	<b>309</b>
<b>Překladač IPv4-to-IPv6 v SOCKS5 .....</b>	<b>311</b>
<b>Shrnutí .....</b>	<b>312</b>
<b>11. Firewally na úrovni aplikační vrstvy .....</b>	<b>313</b>
<b>FWTK: TIS Firewall Toolkit .....</b>	<b>313</b>
Instalace FWTK Firewall Toolkit .....	314
<b>Architektura FWTK .....</b>	<b>319</b>
Proxy firewally pro jednu síť .....	319
Proxy firewall pro dvě sítě .....	320
<b>Konfigurace FWTK Firewall Toolkit .....</b>	<b>320</b>
<b>Pravidla NetACL .....</b>	<b>321</b>



<b>Pravidla brány .....</b>	<b>323</b>
tn-gw: Telnet Proxy .....	323
ftp-gw: FTP Proxy .....	326
http-gw: HTTP Proxy .....	328
plug-gw: TCP Proxy obecného účelu .....	330
smap: poštovní proxy pro SMTP .....	331
<b>Používání silného ověřování v FWTK .....</b>	<b>332</b>
authsrv .....	332
Uživatel .....	332
Skupina uživatelů .....	332
Plné jméno .....	333
Poslední úspěšné přihlášení k serveru proxy .....	333
Mechanismus ověřování, který se má použít pro tohoto uživatele .....	333
<b>Shrnutí .....</b>	<b>337</b>
<b>Část 5. Vzdálený přístup a ověřování .....</b>	<b>339</b>
<b>12. VPN (Virtual Private Networking) .....</b>	<b>341</b>
<b>Slabikář VPN .....</b>	<b>341</b>
Náklady nezávislé na vzdálenosti připojení .....	343
Náklady nezávislé na topologii připojení .....	343
Znovupoužití stávajících připojení k internetu .....	343
<b>Protokol IPSec (IP Security) .....</b>	<b>344</b>
<b>Ověřovací hlavička IP (Authentication Header) .....</b>	<b>345</b>
<b>Zapouzdření obsahu pomocí IP ESP (Encapsulating Security Payload) ...</b>	<b>346</b>
Transportní režim ESP .....	346
Tunelový režim ESP .....	347
<b>FreeS/WAN .....</b>	<b>347</b>
<b>Získání FreeS/WAN .....</b>	<b>348</b>
<b>Instalace FreeS/WAN .....</b>	<b>349</b>
<b>Konfigurace FreeS/WAN .....</b>	<b>351</b>
<b>Úpravy souboru ipsec.secrets .....</b>	<b>352</b>
<b>Úpravy souboru ipsec.conf .....</b>	<b>355</b>
<b>Testování konfigurace .....</b>	<b>358</b>
<b>Protokol PPTP (Point-to-Point Tunneling Protocol) .....</b>	<b>359</b>
Ověřování .....	359
Důvěřnost .....	360

PopTop .....	361
Stažení PopTop .....	361
Konfigurace PopTop .....	361
Spouštění PopTop .....	362
Konfigurace klienta PPTP ve Windows 2000 .....	363
SSH (Secure Shell) .....	364
Jak SSH pracuje .....	365
OpenSSH .....	366
Získání OpenSSH .....	366
Konfigurace OpenSSH .....	367
Pár slov o ověřování RSA .....	370
Používání OpenSSH .....	371
Shrnutí .....	373
<b>13. Silné ověřování uživatele .....</b>	<b>375</b>
<b>Kerberos .....</b>	<b>375</b>
Entita .....	376
KDC (Key Distribution Center) .....	376
Řídící klíč .....	376
Přihlašovací údaje .....	376
Tiket .....	377
TGT (Ticket-Granting Tiket) .....	377
Oblast .....	377
KDC (Key Distribution Center) .....	377
Služby upravené pro Kerberos .....	377
Klienti upravení pro Kerberos .....	377
Důvěrnost .....	379
Pohodlí .....	379
<b>Konfigurace KDC (Kerberos Domain Controller).....</b>	<b>379</b>
Konfigurační soubor KDC (kdc.conf) .....	381
Nástroj kdb5_util .....	383
Soubor kadm5.acl .....	383
Nástroj kadmind.local .....	385
Zaplňování databáze KDC .....	386
Konfigurace serverů používajících Kerberos .....	387
ftpd .....	389
telnetd .....	390
kshd .....	390
klogind .....	391





<b>Správa přihlašovacích údajů v Kerberos .....</b>	<b>392</b>
Používání Kerberos pro umožnění přístupu k vašemu účtu jiným uživatelům .....	394
<b>Používání aplikací využívajících Kerberos .....</b>	<b>394</b>
telnet .....	394
ftp .....	396
rlogin, rsh a rcp .....	397
<b>S/Key a OPIE .....</b>	<b>399</b>
<b>Instalace OPIE .....</b>	<b>400</b>
<b>Konfigurace OPIE .....</b>	<b>400</b>
<b>Použití OPIE .....</b>	<b>402</b>
<b>PAM (Pluggable Authentication Modules) .....</b>	<b>404</b>
<b>Instalace PAM .....</b>	<b>405</b>
<b>Konfigurace PAM .....</b>	<b>405</b>
<b>Příklady PAM .....</b>	<b>407</b>
pam_unix .....	408
pam_cracklib .....	408
<b>Shrnutí .....</b>	<b>409</b>
<b>Přílohy .....</b>	<b>411</b>
<b>Příloha A: Další zdroje informací .....</b>	<b>413</b>
<b>Sdružení, která se zabývají zabezpečením .....</b>	<b>413</b>
www.sans.org .....	413
www.gocsi.com .....	413
<b>WWW stránky s informacemi o Linuxu .....</b>	<b>413</b>
www.linuxsecurity.com .....	413
www.lwn.net .....	413
<b>Webové stránky dodavatelů Linuxu .....</b>	<b>413</b>
www.redhat.com/support/errata .....	413
www.calderasystems.com/support/security .....	414
www.debian.org/security .....	414
www.suse.de/security .....	414
www.turbolinux.com/security .....	414
<b>Rady o zabezpečení .....</b>	<b>414</b>
www.cert.org .....	414
csrc.nist.gov .....	414

<b>Časopisy o zabezpečení .....</b>	<b>415</b>
www.scmagazine.com .....	415
www.infosecuritymag.com .....	415
<b>E-mailové diskusní skupiny o zabezpečení .....</b>	<b>415</b>
www.cert.org/contact_cert/certmaillist.html .....	415
www.securityfocus.com/bugtraq/archive .....	415
lists.gnac.net/firewalls .....	415
www.nfr.com/mailman/listinfo/firewall-wizards .....	415
<b>České internetové adresy .....</b>	<b>416</b>
www.root.cz .....	416
www.underground.cz .....	416
www.hysteria.sk .....	416
www.linux.cz .....	416
www.linuxzone.cz, www.abclinuxu.cz .....	416
linux@linux.cz .....	416

## **Příloha B: Moduly PAM .....** **417**

<b>Přehled .....</b>	<b>417</b>
Ověřování .....	417
Účet .....	417
Heslo .....	417
Relace .....	417
<b>Modul pam_access .....</b>	<b>419</b>
<b>Modul pam_cracklib .....</b>	<b>420</b>
<b>Modul pam_deny .....</b>	<b>422</b>
<b>Modul pam_group .....</b>	<b>423</b>
<b>Modul pam_limits .....</b>	<b>424</b>
<b>Modul pam_pwdb .....</b>	<b>426</b>
Účet .....	426
Ověřování .....	426
Heslo .....	426
Relace .....	426
Účet .....	426
Ověřování .....	427
Heslo .....	427
Relace .....	428



Modul pam_rootok .....	428
Modul pam_securetty .....	428
Modul pam_unix .....	429
Účet .....	429
Ověřování .....	429
Heslo .....	429
Relace .....	430

<b>Rejstřík .....</b>	<b>433</b>
-----------------------	------------

<b>Časté útoky na linuxové servery .....</b>	<b>47</b>
Útoky na webové servery .....	47
Vniknutí přes skripty CGI .....	47
Přetečení vyrovnávací paměti .....	48
Kompromitování uživatele root .....	48
Útoky DoS (Denial of Service) .....	49
útok teardrop .....	49
útok synflood .....	49
Falšování adres .....	49
Ukradení relace .....	50
Odposlouchávání (Eavesdropping) .....	50
Trojské koně .....	50
Kryptoanalýza a útoky hrubou silou .....	52
<b>Přístup k zabezpečení informací .....</b>	<b>53</b>
Fyzické zabezpečení .....	53
Zabezpečení systému .....	54
Zabezpečení sítě .....	54
Zabezpečení aplikací .....	55
Zabezpečení perimetru .....	55
Vzdálený přístup a ověřování .....	55
Lidé a bezpečnost – lidský faktor .....	55
Shrnutí .....	56
<b>2. Instalace a nastavení systému .....</b>	<b>57</b>
Volba distribuce Linuxu .....	57
Red Hat .....	58
Caldera .....	58
SuSE .....	59
Turbolinux .....	60
Debian .....	61
A vítězem je... .....	62
Vytváření bezpečného jádra .....	63
Zabezpečení uživatelských účtů .....	65
Dobrá hesla .....	68
Stínová hesla .....	70
Xinová: další generace hesel .....	71



Nástroj sudo .....	72
Instalace sudo .....	72
Soubor sudoers .....	72
Používání sudo .....	73
Soubor sudo.log .....	73
Oprávnění souborů a adresářů .....	74
suid a sgid .....	75
Nastavení umask .....	78
Omezování velikosti výpisu paměti při havárii .....	78
Zabezpečení protokolů – syslog .....	79
Šifrování systému souborů .....	79
Kryptografický systém souborů .....	80
Instalace CFS .....	80
Konfigurace CFS .....	81
Používání CFS .....	81
PPDD (Practical Privacy Disk Driver) .....	82
Instalace PPDD .....	83
Používání PPDD .....	84
Shrnutí .....	84
<b>3. Sledování a auditování systému .....</b>	<b>87</b>
Protokolování systému pomocí nástroje syslog .....	88
Soubor syslog.conf .....	88
facility .....	89
priority .....	90
destination .....	90
action .....	90
Zabezpečení syslog serveru .....	91
Sledování protokolu systému .....	92
swatch .....	92
Instalace swatch .....	92
Konfigurace swatch .....	93
Hledání vzorků .....	93
Akce při hledání vzorků .....	93
Příklady konfiguračního souboru swatch .....	94
Spouštění swatch .....	95

<b>logcheck</b> .....	<b>96</b>
Instalace logcheck .....	96
Konfigurace logcheck .....	97
Spouštění logcheck .....	100
<b>swatch vs. logcheck</b> .....	<b>101</b>
<b>Auditování integrity souborů</b> .....	<b>101</b>
<b>tripwire</b> .....	<b>102</b>
Instalace tripwire .....	102
Konfigurace tripwire .....	103
Konfigurační soubor programu tripwire .....	104
Soubor se zásadami programu tripwire .....	105
Spouštění programu tripwire .....	108
<b>Audit hesel</b> .....	<b>109</b>
<b>John the Ripper</b> .....	<b>109</b>
Instalace programu John the Ripper .....	109
Konfigurace programu john .....	111
wordfile .....	111
idle .....	111
save .....	111
beep .....	111
Spouštění programu john .....	112
<b>Shrnutí</b> .....	<b>113</b>
<b>Část 2. Zabezpečení sítě</b> .....	<b>115</b>
<b>4. Nastavení síťových služeb</b> .....	<b>117</b>
<b>Zabezpečení síťových služeb</b> .....	<b>117</b>
<b>Spouštění internetových daemonů pomocí inetd</b> .....	<b>118</b>
<b>Konfigurace inetd pomocí /etc/inetd.conf</b> .....	<b>119</b>
Název služby .....	119
Druh socketu .....	119
Protokol .....	119
Wait/Nowait[,max] .....	119
Uživatel [,skupina] .....	120
Program serveru .....	120
Parametry programu serveru .....	120
<b>Příklady konfigurace inetd</b> .....	<b>120</b>
<b>xinetd: další generace inetd</b> .....	<b>121</b>



Instalace xinetd .....	122
Konfigurace xinetd pomocí <i>/etc/xinetd.conf</i> .....	122
disable .....	123
socket_type .....	123
protocol .....	123
wait .....	123
user .....	123
group .....	123
instances .....	123
server .....	123
server_args .....	124
only_from .....	124
no_access .....	124
access_times .....	124
log_on_type .....	124
log_on_success .....	124
log_on_failure .....	125
bind .....	125
redirect .....	125
Příklady konfigurace xinetd .....	125
Spouštění síťových služeb z <i>/etc/rc.d</i> .....	127
Další aspekty zabezpečení sítě .....	131
Vypnutí ověřování rhosts .....	132
Daemon portmap a služby RPC .....	132
Spouštění síťových služeb jako chroot .....	133
TCP Wrappers .....	133
Instalace TCP Wrappers .....	134
Konfigurace TCP Wrappers .....	134
Příklady konfigurace balíčku TCP Wrappers .....	136
Testování konfigurace vašeho balíčku TCP Wrappers .....	137
<i>/usr/sbin/tcpd</i> .....	137
<i>/usr/sbin/safe-finger</i> .....	137
Použití <i>tcpdchk</i> .....	137
Použití <i>tcpdmatch</i> .....	138
Protokolování událostí TCP Wrappers .....	139
Soubor <i>/etc/services</i> .....	139
Příkaz <i>netstat</i> .....	141
Shrnutí .....	142

<b>5. Sledování a audit sítě .....</b>	<b>143</b>
<b>Audit sítě .....</b>	<b>143</b>
<b>Nástroje pro audit ze sítě .....</b>	<b>143</b>
Nessus .....	144
Instalace programu Nessus .....	146
GTK .....	147
Nmap .....	147
Konfigurace serveru Nessus .....	147
Spouštění daemonu Nessus .....	150
Konfigurace a spouštění klienta Nessus .....	151
Nmap .....	156
Instalace programu Nmap .....	157
Používání Nmap .....	157
<b>Nástroje pro audit z hostitele .....</b>	<b>159</b>
TARA .....	160
Instalace programu TARA .....	160
Konfigurace programu TARA .....	161
Používání programu TARA .....	162
<b>Sledování sítě .....</b>	<b>164</b>
PortSentry .....	165
Instalace PortSentry .....	165
Konfigurace PortSentry .....	165
Používání PortSentry .....	166
Ethereal .....	167
Instalace programu Ethereal .....	168
Použití programu Ethereal .....	168
<b>Shrnutí .....</b>	<b>169</b>
<b>Část 3. Zabezpečení aplikací .....</b>	<b>171</b>
<b>6. Elektronická pošta .....</b>	<b>173</b>
Sendmail .....	173
Bezpečné předávání pošty skrze ověřování SMTP .....	174
SMTP přes TLS .....	175
Použití STARTTLS .....	178
Qmail .....	179
Postfix .....	180



Princip nejmenších práv .....	180
Izolace procesu .....	180
Vlastnictví procesu .....	181
Setuid .....	181
Velké vstupy .....	181
<b>Protokol POP v. 3 (Post Office Protocol) .....</b>	<b>181</b>
<b>APOP .....</b>	<b>182</b>
<b>Instalace software Qpopper .....</b>	<b>183</b>
<b>Konfigurace programu Qpopper .....</b>	<b>183</b>
<b>Použití programu Qpopper .....</b>	<b>185</b>
<b>IMAP .....</b>	<b>185</b>
<b>Instalace software serveru IMAP .....</b>	<b>186</b>
<b>Konfigurace bezpečného serveru IMAP .....</b>	<b>186</b>
<b>Použití zabezpečeného serveru IMAP .....</b>	<b>188</b>
<b>PGP a GnuPG .....</b>	<b>190</b>
PGP (komerční) .....	190
PGPi .....	191
GnuPG .....	191
<b>Instalace GnuPG .....</b>	<b>191</b>
<b>Konfigurace GnuPG .....</b>	<b>192</b>
<b>Používání GnuPG .....</b>	<b>193</b>
Příklady .....	194
<b>Shrnutí .....</b>	<b>195</b>
<b>7. Služby HTTP .....</b>	<b>197</b>
<b>Server HTTP Apache .....</b>	<b>197</b>
<b>Konfigurace zabezpečení serveru Apache .....</b>	<b>198</b>
httpd.conf .....	198
sm.conf .....	198
access.conf .....	199
<b>Ověřování .....</b>	<b>199</b>
mod_auth .....	199
mod_auth_dbm .....	203
mod_auth_db .....	205
mod_auth_digest .....	206
<b>Řízení přístupu .....</b>	<b>208</b>

<b>Zabezpečování serveru Apache .....</b>	<b>210</b>
Uživatel Apache .....	211
Vlastnictví a práva pro strom obsahu .....	211
Skrývání obsahu adresáře .....	211
Skripty CGI .....	212
Server Side Includes .....	212
<b>Protokoly aplikace .....</b>	<b>212</b>
error_log .....	213
<b>mod_ssl .....</b>	<b>213</b>
<b>Instalace mod_ssl .....</b>	<b>214</b>
<b>Konfigurace mod_ssl .....</b>	<b>215</b>
Vytvoření certifikační autority .....	215
Použití sebou podepsaného certifikátu .....	219
<b>Apache-SSL .....</b>	<b>223</b>
<b>Shrnutí .....</b>	<b>224</b>
<b>8. Zabezpečení serveru Samba .....</b>	<b>225</b>
<b>Server Samba .....</b>	<b>225</b>
<b>Instalace serveru Samba .....</b>	<b>228</b>
<b>Správa Samby pomocí SWAT .....</b>	<b>229</b>
SWAT-SSL .....	231
<b>Zabezpečení Samby .....</b>	<b>232</b>
Ověřování uživatelů .....	232
User .....	233
UID .....	233
LAN-Manager-password .....	233
NT-password .....	234
account-flags .....	234
update-time .....	234
Řízení přístupu .....	234
Režim share .....	234
Režim user .....	235
Režim server .....	236
Režim domain .....	236
Jiné funkce řízení přístupu .....	237
Direktiva [homes] .....	238



Důvěrnost komunikace se Sambou .....	238
Vytváření certifikační autority pro Samba-SSL .....	239
Konfigurace Samby pro podporu SSL .....	240
Stahování a Instalace SSL Proxy .....	241
<b>Použití Samby jako primárního řadiče domény Windows NT .....</b>	<b>244</b>
Nastavení Samby jako PDC .....	244
<b>Shrnutí .....</b>	<b>246</b>

## **Část 4. Zabezpečení perimetru .....** **249**

### **9. Firewally na úrovni síťové vrstvy .....** **251**

<b>Firewally: přehled .....</b>	<b>251</b>
Firewally na úrovni síťové vrstvy .....	251
Firewally na úrovni transportní vrstvy .....	251
Firewally na úrovni aplikační vrstvy .....	252
<b>Linux jako platforma pro firewall .....</b>	<b>253</b>
Jednotná správa .....	253
Spotřební hardware .....	253
Robustní filtrování založené na jádře .....	253
Ověřená platforma .....	253
Výkon .....	253
Cena .....	254
Podpora .....	254
Rozšiřující aplikace Application Bundling .....	254
<b>Filtrování paketů .....</b>	<b>254</b>
<b>Minulost: ipfwadm a ipchains .....</b>	<b>255</b>
<b>Použití ipchains .....</b>	<b>255</b>
Řetězec Input (vstup) .....	256
Řetězec Output (výstup) .....	256
Řetězec Forward (předávání) .....	256
<b>Příklady Ipchains .....</b>	<b>258</b>
<b>Přítomnost: Netfilter .....</b>	<b>259</b>
<b>Konfigurace systému Netfilter .....</b>	<b>261</b>
iptables .....	262
Použití iptables .....	263
Specifikace pravidel iptables .....	265
<b>Vzorové scénáře firewallů .....</b>	<b>268</b>
<b>Server pro vytáčená připojení s jedním rozhraním .....</b>	<b>268</b>