

Obsah

Část I – Základy bezpečnosti9

Kapitola 1

Základy obvodového zabezpečení11

Důležité pojmy	12
Hlubková obrana	15
Případová studie hlubkové obrany	25
Shrnutí	26

Kapitola 2

Filtrování paketů27

Abeceda TCP/IP: jak funguje filtrování paketů	27
Směrovače Cisco jako paketové filtry	29
Jak účinně využívat zařízení pro filtrování paketů	32
Problémy s paketovými filtry	43
Dynamické filtrování paketů a reflexivní přístupové seznamy	50
Shrnutí	54
Odkazy	54

Kapitola 3

Stavové firewally55

Jak funguje stavový firewall	55
Co je to stav	56
Stavové filtrování a stavová inspekce	66
Shrnutí	78
Odkazy	79

Kapitola 4

Proxy firewally81

Základy	81
Typy proxy firewallů	84
Proxy neboli aplikační bránové firewally	86
Problémy s protokoly a proxy firewally	88
Nástroje pro proxy komunikaci	90
Shrnutí	94
Odkazy	94

Kapitola 5

Zásady zabezpečení	95
Firewally tvoří zásady zabezpečení	95
Jak vytvořit zásady	103
Otázky obvodu sítě	110
Shrnutí	113
Odkazy	113

Část II – Rozšíření obvodu **115****Kapitola 6**

Úloha směrovače	117
Směrovač jako zařízení zabezpečovacího obvodu	117
Směrovač jako bezpečnostní zařízení	122
Zodolnění směrovače	132
Shrnutí	146
Odkazy	147

Kapitola 7

Detekce síťového narušení	149
Základní fakta o detekci síťového narušení	149
Úloha síťového IDS v ochranném obvodu	157
Umístění senzoru IDS	161
Případové studie	166
Shrnutí	171

Kapitola 8

Virtuální privátní síť	173
Základní fakta o VPN	173
Výhody a nevýhody tunelů VPN	177
Základní informace o protokolu IPSec	182
Další protokoly VPN: PPTP a L2TP	206
Shrnutí	211
Odkazy	212

Kapitola 9

Zodolnění hostitelského počítače	213
Úrovně zodolnění	213
Úroveň 1: Zodolnění proti místním útokům	215
Úroveň 2: Zodolnění proti síťovým útokům	221
Úroveň 3: Posílení proti útokům na aplikace	227
Návod na dodatečné zodolnění	230
Shrnutí	231

Kapitola 10

Součásti obrany hostitelského systému233
Hostitelské systémy a obvod sítě	233
Antivirový software	238
Hostitelsky orientované firewally	242
Hostitelská detekce vniknutí	257
Úskalí komponent hostitelské obrany	265
Shrnutí	267
Odkazy	268

Část III – Návrh koncepce zabezpečení sítě . . .271

Kapitola 11

Základy návrhu sítě273
Sběr požadavků na návrh	274
Součásti návrhu	285
Shrnutí	293
Odkazy	293

Kapitola 12

Oddělení prostředků295
Bezpečnostní zóny	295
Obvyklé prvky návrhu	303
Oddělení se sítí VLAN	315
Shrnutí	318
Odkazy	319

Kapitola 13

Softwarová architektura321
Softwarová architektura a obrana sítě	321
Jak softwarová architektura ovlivňuje způsob obrany sítě	323
Umístění softwarových komponent	327
Jak rozpoznat možné problémy softwarové architektury	330
Testování softwaru	332
Doporučení pro návrh obrany sítě	333
Případová studie: systém péče o zákazníky	334
Případová studie: webově orientovaná fakturační aplikace	336
Shrnutí	338
Odkazy	338

Kapitola 14

Integrace sítě VPN339
Služba SSH	339

Vrstva SSL	343
Řešení se vzdálenou plochou	347
Protokol IPSec	351
Ostatní úvahy k sítím VPN	354
Případová studie návrhu VPN	355
Shrnutí	359

Kapitola 15

Vyladění výkonu navržené sítě361

Výkonnost a bezpečnost	361
Které prvky návrhu zabezpečení sítě mají vliv na její výkonnost	364
Dopady šifrování	373
Zvýšení výkonu pomocí vyrovnávání zátěže	379
Shrnutí	382
Odkazy	382

Kapitola 16

Ukázky návrhů383

Přehled kritérií bezpečnostního návrhu	383
Případové studie	385
Shrnutí	403

Část IV – Zhodnocení obvodu405

Kapitola 17

Údržba bezpečnostního obvodu407

Sledování systému a sítě	407
Reakce na incidenty	422
Jak přizpůsobit prostředí změnám	426
Shrnutí	432
Odkazy	433

Kapitola 18

Analýza síťových záznamových souborů435

Význam záznamových souborů sítě	435
Základy analýzy záznamových souborů	441
Analýza záznamových souborů směrovače	447
Analýza záznamových souborů síťového firewallu	449
Analýza záznamových souborů hostitelsky centralizovaného firewallu a systému IDS	452
Shrnutí	456

Kapitola 19

Řešení problémů s ochrannými komponentami	457
Postup při hledání a odstraňování závady	457
Několik postřehů pro odhalování a odstraňování závad	460
Sada nástrojů užitečných při odhalování a odstraňování závad	462
Shrnutí	484
Odkazy	484

Kapitola 20

Techniky zhodnocení návrhu	485
Externí zhodnocení	485
Interní zhodnocení	502
Shrnutí	509
Odkazy	510

Kapitola 21

Sít' pod palbou	511
Přístup hackerů k útoku na síť	511
Zkoumání metod narušitele	512
GIAC GCFW praktické návrhy sítí vytvořené studenty	514
Shrnutí	538
Odkazy	539

Kapitola 22

Význam hloubkové ochrany	541
Hrady: příklad architektury s hloubkovou obranou	541
Pohlcující bariéry	550
Hloubková obrana aplikovaná na informace	554
Shrnutí	556

Část V – Přílohy **559** |

Příloha A

Úkázkové konfigurace přístupových seznamů Cisco ..	561
Úplný přístupový seznam pro čistě privátní síť	561
Úplný přístupový seznam pro chráněnou podsít, která umožňuje přístup k veřejným serverům z Internetu	564

Příloha B

Několik slov ke kryptografii571
Šifrovací algoritmy	571
Shrnutí	575
Odkazy	575

Příloha C

Systémy NAG pro fyzické oddělení577
Jak vypadá fyzické oddělení	577
Co jsou to systémy NAG	578
Fyzické oddělení NAG ve spojení s firewally	580
Implementace zařízení NAG	580
Shrnutí	581
Rejstřík583