

# Stručný obsah

<b>Kapitola 1</b>	<b>Úvod do zabezpečení sítě</b>	<b>1</b>
<b>Kapitola 2</b>	<b>Software a hardware jednotky Cisco PIX Firewall</b>	<b>13</b>
<b>Kapitola 3</b>	<b>Softwarový obraz Cisco PIX Firewallu a jeho aktualizace</b>	<b>27</b>
<b>Kapitola 4</b>	<b>Konfigurace PIX Firewallu</b>	<b>49</b>
<b>Kapitola 5</b>	<b>Převody adres v Cisco PIX Firewallu</b>	<b>63</b>
<b>Kapitola 6</b>	<b>Konfigurace přístupu přes Cisco PIX Firewall</b>	<b>77</b>
<b>Kapitola 7</b>	<b>Služba syslog</b>	<b>97</b>
<b>Kapitola 8</b>	<b>Konfigurace mechanismu AAA v Cisco PIX Firewallu</b>	<b>107</b>
<b>Kapitola 9</b>	<b>Pokročilá obsluha protokolů a strážce útoků v Cisco PIX Firewallu</b>	<b>143</b>
<b>Kapitola 10</b>	<b>Havarijní převzeti služeb Cisco PIX Firewallu</b>	<b>169</b>
<b>Kapitola 11</b>	<b>Konfigurace technologií IPSec na Cisco PIX Firewalllech</b>	<b>189</b>
<b>Kapitola 12</b>	<b>Kontextově závislé řízení přístupu CBAC v Cisco IOS Firewallu</b>	<b>231</b>
<b>Kapitola 13</b>	<b>Konfigurace autentizačního proxy serveru v Cisco IOS Firewallu</b>	<b>269</b>
<b>Příloha A</b>	<b>Konfigurace mechanismů detekce vniknutí v PIX Firewallu</b>	<b>285</b>
<b>Příloha B</b>	<b>Konfigurace protokolu SNMP na PIX Firewallu</b>	<b>293</b>
<b>Příloha C</b>	<b>Konfigurace protokolu DHCP na PIX Firewallu</b>	<b>299</b>
<b>Příloha D</b>	<b>Konfigurace služby SSH na PIX Firewallu</b>	<b>305</b>
<b>Příloha E</b>	<b>Zdroje informací o bezpečnosti</b>	<b>317</b>
<b>Příloha F</b>	<b>Odpovědi na otázky ke cvičení</b>	<b>323</b>

# Obsah

<b>O autorech</b>	<b>xix</b>
Odborná spolupráce	xix
<b>Věnování</b>	<b>xxi</b>
<b>Poděkování</b>	<b>xxi</b>
<b>Úvod</b>	<b>xxii</b>
O této knize	xxii
Cíle pro studium knihy	xxii
Konvence pro syntaxi příkazů	xxii
Ikony použité v knize	xxiii

## Kapitola 1

<b>Úvod do zabezpečení sítí</b>	<b>1</b>
<b>Proč je zabezpečení sítí důležité</b>	<b>2</b>
<b>Definice návrhu bezpečných sítí</b>	<b>2</b>
<b>Kategorie hrozeb síťové bezpečnosti</b>	<b>4</b>
<b>Jak dochází k prolomení bezpečnosti</b>	<b>6</b>
Útoky s obhlídkou	6
Útoky vůči přístupu	6
Útoky s odepřením služeb	8
<b>Zásady zabezpečení sítě a bezpečnostní kruh</b>	<b>8</b>
<b>Shrnutí</b>	<b>10</b>
<b>Otázky ke cvičení</b>	<b>11</b>

## Kapitola 2

<b>Software a hardware jednotky Cisco PIX Firewall</b>	<b>13</b>
<b>Typy firewallů</b>	<b>14</b>
Paketové filtry	14
Proxy filtry	16
Stavové paketové filtry	17
<b>Logika PIX Firewallu</b>	<b>17</b>

<b>Modely PIX Firewallu</b>	<b>19</b>
Ovládací prvky, konektory a prvky předního a zadního panelu	20
<b>Otázky ke cvičení</b>	<b>26</b>

## Kapitola 3

## **Softwarový obraz Cisco PIX Firewallu a jeho aktualizace** **27**

<b>Rozhraní příkazového řádku PIX Firewallu</b>	<b>28</b>
<b>Údržba a testování PIX Firewallu</b>	<b>29</b>
<b>Instalace nového operačního systému na PIX Firewall</b>	<b>38</b>
Přechod na jinou verzi softwaru PIX	39
Přechod na jiný operační systém PIX v monitorovacím režimu	40
Instalace operačního systému PIX 5.0 a staršího	41
Instalace operačního systému PIX 5.1 a novějšího	42
Vytvoření zaváděcí diskety BootHelper na počítači s Windows	42
Vytvoření zaváděcí diskety BootHelper na pracovní stanici se systémem Unix, Solaris nebo Linux	43
Instalace modulu BootHelper pro PIX Firewall s disketovou jednotkou	43
<b>Obnovení hesla</b>	<b>44</b>
Obnovení hesla z diskety ve verzi PIX Classic, PIX 10 000, 510 a 520	45
Obnovení hesla s protokolem TFTP v modelu PIX 501, 506E, 515E, 525 a 535	46
<b>Otázky ke cvičení</b>	<b>47</b>

## Kapitola 4

## **Konfigurace PIX Firewallu** **49**

<b>Úrovně zabezpečení ASA</b>	<b>49</b>
<b>Šest základních příkazů pro konfiguraci Cisco PIX Firewallu</b>	<b>52</b>
Příkaz nameif	53
Příkaz interface	54
Příkaz ip address	55
Příkaz nat	56
Příkaz global	56
Příkaz route	58
<b>Otázky ke cvičení</b>	<b>61</b>

## Kapitola 5

**Převody adres v Cisco PIX Firewallu 63****Přenosové protokoly 64**

Protokol TCP 65

Protokol UDP 66

**Převody adres v PIX Firewallu 68**

Statické převody adres 69

Dynamické převody adres 71

Převody a spojení 74

**Otázky ke cvičení 75**

## Kapitola 6

**Konfigurace přístupu přes Cisco PIX Firewall 77****Konfigurace přístupu přes PIX Firewall 78****Práce s příkazy static a conduit 79**

Příkaz static 79

Příkaz conduit 80

**Další metody přístupu přes PIX Firewall 86**

Konfigurace mechanismu PAT 87

Konfigurace převodů nat 0 89

Konfigurace příkazu FIXUP Protocol 90

Podpora multimédií 91

**Konfigurace více rozhraní 92**

Příkaz name 95

**Otázky ke cvičení 95**

## Kapitola 7

**Služba syslog 97****Zprávy syslog 97****Konfigurace služby syslog 98**

Příkaz logging host 101

Příkaz logging trap 101

Příkaz logging buffered 102

Příkaz logging console 102

Příkaz logging facility 102

Příkaz logging monitor	103
Příkaz logging standby	103
Příkaz logging timestamps	103
Příkaz (no) logging message	104
Příkaz show logging	104
Příkaz clear logging	105
<b>Nové zprávy syslog podle verzí</b>	<b>105</b>
<b>Otázky ke cvičení</b>	<b>106</b>

## Kapitola 8

<b>Konfigurace mechanismu AAA v Cisco PIX Firewallu</b>	<b>107</b>
Definice mechanismu AAA	108
Činnost průřezové proxy autentizace	111
Podporované servery AAA	112
Instalace nástroje CSACS pro Windows NT	112
Přidávání uživatelů do CSACS-NT	115
<b>Konfigurace mechanismů autentizace</b>	<b>118</b>
Autentizace ostatních služeb	122
Virtuální Telnet	122
Virtuální HTTP	125
Autentizace konzolového přístupu	126
Změna časových limitů pro autentizaci	128
Změna výzvy pro autentizaci	129
<b>Konfigurace mechanismů autorizace</b>	<b>130</b>
Přidání autorizačního pravidla do CSACS-NT	132
Autorizace ostatních služeb	135
<b>Konfigurace mechanismů účtování</b>	<b>136</b>
Prohlížení účetních záznamů s CSACS-NT	138
Účtování ostatních služeb	138
<b>Ověření konfigurace</b>	<b>139</b>
<b>Otázky ke cvičení</b>	<b>141</b>

## Kapitola 9

## **Pokročilá obsluha protokolů a stráže útoků v Cisco PIX Firewallu 143**

<b>K čemu je potřeba pokročilé zpracování protokolů</b>	<b>144</b>
Standardní režim FTP	145
Pasivní režim FTP	146
Příkaz fixup protocol FTP	148
Vzdálený shell rsh	149
Protokol SQL*Net	151
<b>Podpora multimédií</b>	<b>153</b>
Protokol RTSP	153
Protokol H.323	157
<b>Stráže útoků</b>	<b>159</b>
Stráž pošty MailGuard	159
Stráž DNS Guard	160
Stráž fragmentačních útoků	161
Stráž záplavy AAA	162
Stráž záplavy SYN	163
<b>Shrnutí</b>	<b>167</b>
<b>Otázky ke cvičení</b>	<b>167</b>

## Kapitola 10

## **Havarijní převzetí služeb Cisco PIX Firewallu 169**

<b>Činnost havarijního převzetí</b>	<b>171</b>
Kabel pro havarijní převzetí	171
Replikace aktivní konfigurace	172
Monitorování havarijního převzetí	173
Zpětné převzetí služeb	177
<b>Konfigurace havarijního převzetí</b>	<b>177</b>
<b>Praktické cvičení</b>	<b>181</b>
Úkol 1: Konfigurace havarijního předání služeb směrem k sekundárnímu PIX Firewallu na primárním PIX Firewallu	182
Úkol 2: Jak může primární PIX Firewall opět přejít do aktivního stavu	184
Úkol 3: Konfigurace stavového předání služeb na primárním PIX Firewallu	185
<b>Otázky ke cvičení</b>	<b>187</b>

## Kapitola 11

# Konfigurace technologií IPSec na Cisco PIX Firewallch

189

<b>Cisco Secure PIX Firewall umožňuje činnost bezpečné virtuální sítě VPN</b>	<b>190</b>
PIX Firewall, virtuální sítě VPN a protokoly IPSec	191
Standardy IPSec	193
Výměna klíčů IKE	193
Bezpečnostní asociace SA	193
Šifrování DES	194
Šifrování 3DES	194
Šifrování AES	194
Algoritmus Diffie-Hellman	194
Algoritmus MD5	194
Algoritmus SHA-1	195
Podpisy RSA	195
Certifikační autority	195
<b>Konfigurace podpory IPSec v PIX Firewallu</b>	<b>195</b>
Úkol 1: Příprava na protokol IPSec	196
Úkol 2: Konfigurace IKE a výměny předem sdílených klíčů	197
Úkol 3: Konfigurace IPSec	202
Úkol 4: Testování a kontrola celkové konfigurace protokolu IPSec	218
<b>Škálování sítě VPN s PIX Firewallem</b>	<b>219</b>
PIX Firewall a zápis u certifikační autority	220
<b>Případová studie 1: Konfigurace IPSec v PIX Firewallu pro dvoubodové spojení hostitelů s předem sdílenými klíči</b>	<b>220</b>
Zásady zabezpečení sítě	221
Příklad konfigurace PIX Firewallu 1	221
Příklad konfigurace PIX Firewallu 2	223
<b>Případová studie 2: Tunely IPSec v síti s úplným grafem nad třemi pracovišti a s předem sdílenými klíči</b>	<b>224</b>
Zásady zabezpečení sítě	225
Příklad konfigurace PIX Firewallů pro Portland, Seattle a San Jose	225
<b>Shrnutí</b>	<b>228</b>
<b>Otázky ke cvičení</b>	<b>229</b>
<b>Odkazy</b>	<b>229</b>

## Kapitola 12

## **Kontextově závislé řízení přístupu CBAC v Cisco IOS Firewallu** **231**

<b>Úvod do Cisco IOS Firewallu</b>	<b>232</b>
Kontextově závislé řízení přístupu CBAC	232
Autentizační proxy server	233
Detekce vniknutí	234
Činnost kontextově závislého řízení přístupu CBAC	242
Základní konfigurace mechanismu CBAC	246
Konfigurace inspekčních pravidel CBAC	254
Aplikace inspekčních pravidel a přístupových seznamů na jednotlivá rozhraní směrovače	260
Testování, ověřování a monitorování CBAC	265
<b>Otázky ke cvičení</b>	<b>266</b>

## Kapitola 13

## **Konfigurace autentizačního proxy serveru v Cisco IOS Firewallu** **269**

<b>Úvod do autentizačního proxy serveru v systému IOS</b>	<b>270</b>
<b>Úkoly spojené s konfigurací autentizačního proxy serveru</b>	<b>272</b>
Konfigurace serveru AAA	273
Konfigurace mechanismu AAA	276
Konfigurace autentizačního proxy serveru	279
Přezkoušení a ověření konfigurace	281
Příklad konfigurace proxy autentizačních služeb	282
<b>Otázky ke cvičení</b>	<b>284</b>

## Příloha A

## **Konfigurace mechanismů detekce vniknutí v PIX Firewallu** **285**

<b>Úvod do detekce vniknutí IDS v PIX Firewallu</b>	<b>286</b>
Prvky konfigurace mechanismů detekce vniknutí	286
Příklady konfigurace IDS v PIX Firewallu	289
Projevy vniknutí IDS v PIX	291
<b>Časté otázky</b>	<b>291</b>
<b>Doporučená literatura</b>	<b>292</b>



## Příloha B

**Konfigurace protokolu SNMP na PIX Firewallu    293**

Podpora protokolu SNMP v PIX Firewallu    294

Načítání dat SNMP z PIX Firewallu    294

Prohlížeč MIB Browser    295

Zachycené události SNMP    295

Konfigurace procházení MIB a odesílání událostí syslog v PIX Firewallu    295

Databáze zařízení SNMP v1 MIB-II    296

Webové zdroje informací o SNMP    297

## Příloha C

**Konfigurace protokolu DHCP na PIX Firewallu    299**

Základy DHCP    300

Server DHCP    300

Klient DHCP    301

Příklady konfigurací    302

PIX 506 jako server DHCP: statická definice vnější adresy    302

PIX 506 jako klient DHCP: dynamické přidělování vnější adresy    302

Zdroje informací o DHCP v síti WWW    303

## Příloha D

**Konfigurace služby SSH na PIX Firewallu    305**

Úvod do bezpečného shellu SSH    306

Povolení služby SSH v konfiguraci PIX Firewallu    306

Povolení příjmu spojení SSH v PIX Firewallu    306

Konfigurace klienta SSH pro připojení k jednotce PIX    308

Řešení problémů s klientským spojením SSH    313

Jak získat klienta SSH pro určitou platformu    315

## Příloha E

**Zdroje informací o bezpečnosti    317**

Příloha F

<b>Odpovědi na otázky ke cvičení</b>	<b>323</b>
Odpovědi na otázky ke cvičení z kapitoly 1	323
Odpovědi na otázky ke cvičení z kapitoly 2	324
Odpovědi na otázky ke cvičení z kapitoly 3	325
Odpovědi na otázky ke cvičení z kapitoly 4	325
Odpovědi na otázky ke cvičení z kapitoly 5	326
Odpovědi na otázky ke cvičení z kapitoly 6	327
Odpovědi na otázky ke cvičení z kapitoly 7	328
Odpovědi na otázky ke cvičení z kapitoly 8	328
Odpovědi na otázky ke cvičení z kapitoly 9	330
Odpovědi na otázky ke cvičení z kapitoly 10	330
Odpovědi na otázky ke cvičení z kapitoly 11	332
Odpovědi na otázky ke cvičení z kapitoly 12	333
Odpovědi na otázky ke cvičení z kapitoly 13	334
<b>Rejstřík</b>	<b>337</b>