
Stručný obsah

Část I

Vytvoření zásad síťové bezpečnosti

Kapitola 1	Vyhodnocení hrozeb pro síťovou bezpečnost	3
Kapitola 2	Posouzení zásad zabezpečení sítě	35
Kapitola 3	Zabezpečení síťové infrastruktury	63

Část II

Bezpečnost vytáčených spojení

Kapitola 4	Bezpečnostní technologie Cisco AAA	107
Kapitola 5	Konfigurace síťového přístupového serveru se zabezpečením AAA	151
Kapitola 6	Konfigurace přístupového serveru CiscoSecure ACS a služby TACACS+/RADIUS	169

Část III

Zabezpečení internetového připojení

Kapitola 7	Konfigurace obvodového směrovače Cisco	213
Kapitola 8	Konfigurace Cisco IOS Firewallu	249

Část IV

Konfigurace CiscoSecure PIX Firewallu

Kapitola 9	Základy PIX Firewallu	279
Kapitola 10	Konfigurace přístupu přes PIX Firewall	327
Kapitola 11	Konfigurace více rozhraní a mechanismu AAA v PIX Firewallu	369
Kapitola 12	Konfigurace pokročilých funkcí PIX Firewallu	405

Část V

Konfigurace šifrovacích technologií Cisco Encryption Technology

Kapitola 13	Přehled šifrovací technologie Cisco Encryption Technology	441
Kapitola 14	Konfigurace šifrovací technologie Cisco Encryption Technology	459

Část VI

Konfigurace virtuální privátní sítě VPN s protokolem IPSec

Kapitola 15	Podpora protokolu IPSec v produktech Cisco	505
Kapitola 16	Konfigurace protokolu IPSec v Cisco IOS	551
Kapitola 17	Konfigurace podpory IPSec v PIX Firewallu	595
Kapitola 18	Škálování sítě Cisco s IPSec	629

Část VII

Přílohy

Příloha A	Scénář případové studie společnosti XYZ	669
Příloha B	Příklad zásad zabezpečení sítě ve společnosti XYZ	675
Příloha C	Konfigurace standardních a rozšířených přístupových seznamů	685
Příloha D	Odpovědi na otázky ke cvičení	719

Rejstřík

743

Obsah

O autorovi	xv
Spoluautoři	xv
Odborní korektoři	xvi
Věnování	xvii
Poděkování	xviii
Úvodní slovo	xix
Předmluva	xx
Úvod	xxi
Pro koho je kniha určena	xxi
Struktura knihy	xxi
Konvence použité v knize	xxii
Uspořádání knihy	xxii

ČÁST I

Vytvoření zásad síťové bezpečnosti

Kapitola 1

Vyhodnocení hrozeb pro síťovou bezpečnost **3**

K čemu potřebujeme zabezpečení sítě	4
Proč vznikají bezpečnostní problémy	5
Typy bezpečnostních hrozeb	12
Možnosti zabezpečení	31
Shrnutí	32
Otázky ke cvičení	32
Odkazy	33

Kapitola 2

Posouzení zásad zabezpečení sítě **35**

Význam ochrany počítačové sítě	36
Proces vyhodnocení bezpečnostních postojů	37
Zlepšení postojů vůči bezpečnosti	43

Případové studie ze zabezpečení sítí	44
Shrnutí	56
Případová studie: posouzení zásad zabezpečení sítě ve společnosti XYZ	57
Otázky ke cvičení	59
Odkazy	59

Kapitola 3

Zabezpečení síťové infrastruktury **63**

Problémy zabezpečení firemních sítí a jejich řešení	64
Zabezpečení fyzických zařízení	66
Zabezpečení administrativního rozhraní	67
Zabezpečení vzájemné komunikace mezi směrovači	83
Zabezpečení ethernetových přepínačů	93
Shrnutí	97
Případová studie: konfigurace základní síťové bezpečnosti	97
Otázky ke cvičení	102
Odkazy	102

ČÁST II

Bezpečnost vytáčených spojení

Kapitola 4

Bezpečnostní technologie Cisco AAA **107**

Zabezpečení přístupu k síti pomocí AAA	108
Metody autentizace	111
Metody autorizace	122
Metody účtování	123
Servery zabezpečení AAA	124
Shrnutí	147
Otázky ke cvičení	148
Odkazy	148

Kapitola 5

Konfigurace síťového přístupového serveru se zabezpečením AAA **151**

Problém zabezpečení vzdáleného přístupu a jeho řešení	152
Proces konfigurace AAA v přístupovém serveru	153

Shrnutí	163
Případová studie: konfigurace přístupového serveru se zabezpečením AAA	164
Otázky ke cvičení	167
Odkazy	168

Kapitola 6

Konfigurace přístupového serveru CiscoSecure ACS a služby TACACS+/RADIUS 169

Balík CiscoSecure ACS pro systémy Windows NT a Unix	170
CiscoSecure ACS for Windows NT	171
CiscoSecure ACS for Unix	188
Konfigurace služby TACACS+ v CiscoSecure ACS	190
Konfigurace služby RADIUS v CiscoSecure ACS	197
Zdvojená autentizace	202
Shrnutí	204
Případová studie: konfigurace CSNT	205
Otázky ke cvičení	209
Odkazy	210

ČÁST III

Zabezpečení internetového připojení

Kapitola 7

Konfigurace obvodového směrovače Cisco 213

Systémy obvodového zabezpečení Cisco	214
Řízení služeb TCP/IP	220
Prevence proti útokům s přesměrováním	222
Řízení přístupu	224
Ochrana proti útoku odepřením služeb	228
Šifrování v síťové vrstvě	231
Mapování adres IP s mechanismy NAT a PAT	233
Záznam událostí obvodového směrovače	237
Shrnutí	238
Případová studie: konfigurace obvodového směrovače Cisco	239
Otázky ke cvičení	245
Odkazy	245

Kapitola 8**Konfigurace Cisco IOS Firewallu** **249**

Bezpečnostní problémy a jejich řešení s Cisco IOS Firewallem	250
Konfigurace Cisco IOS Firewallu	251
Plánování Cisco IOS Firewallu	254
Konfigurace kontextově závislého řízení přístupu CBAC	257
Správa Cisco IOS Firewallu	268
Shrnutí	270
Případová studie: konfigurace Cisco IOS Firewallu	270
Otázky ke cvičení	275
Odkazy	275

Část IV**Konfigurace CiscoSecure PIX Firewallu****Kapitola 9****Základy PIX Firewallu** **279**

Co je to PIX Firewall?	280
Co a jak se přes PIX Firewall dostane z vnější sítě	282
Modely PIX Firewallu a jeho komponenty	291
Modely PIX Firewallu a jeho komponenty	292
Konfigurace PIX Firewallu	301
Příklad konfigurace PIX Firewallu	321
Shrnutí	322
Případová studie: konfigurace mechanismu NAT v PIX Firewallu při ochraně identity vnitřní sítě	323
Otázky ke cvičení	325
Odkazy	325

Kapitola 10**Konfigurace přístupu přes PIX Firewall** **327**

Konfigurace řízení přístupu v odchozím provozu	328
Řízení přístupu k hostitelům vnitřní sítě	343
Shrnutí	363
Případová studie: konfigurace CiscoSecure PIX Firewallu s jedinou interní sítí	364
Otázky ke cvičení	366
Odkazy	367

Kapitola 11

Konfigurace více rozhraní a mechanismu AAA v PIX Firewallu

369

Konfigurace přístupu k více rozhraním	370
Konfigurace autentizace uživatelů	392
Shrnutí	397
Případová studie: konfigurace více rozhraní a mechanismu AAA v PIX Firewallu	398
Otázky ke cvičení	402
Odkazy	403

Kapitola 12

Konfigurace pokročilých funkcí PIX Firewallu

405

Pokročilé převody síťových adres: NAT 0	406
Řízení přístupu v odchozím provozu	408
Konfigurace blokování javových appletů a filtrování adres URL	411
Konfigurace záznamu adres FTP a URL	414
Konfigurace protokolu SNMP	417
Konfigurace havarijního převzetí služeb PIX Firewallu	419
Konfigurace funkcí virtuálních sítí VPN	423
Nástroj CiscoSecure Policy Manager	428
Údržba PIX Firewallu	428
Shrnutí	432
Případová studie: konfigurace pokročilých funkcí PIX Firewallu	433
Otázky ke cvičení	437
Odkazy	437

ČÁST V

Konfigurace šifrovacích technologií Cisco Encryption Technology

Kapitola 13

Přehled šifrovací technologie Cisco Encryption Technology

441

Řešení mechanismu šifrování	442
Přehled šifrovacího systému Cisco IOS	449

Shrnutí	457
Otázky ke cvičení	457
Odkazy	458

Kapitola 14

Konfigurace šifrovací technologie Cisco Encryption Technology 459

Základy šifrovací technologie Cisco Encryption Technology	460
Konfigurace šifrovací technologie CET	468
Diagnostika a řešení problémů v technologii CET	492
Úvahy k implementaci šifrování	494
Exportní politika pro šifrovací algoritmy	497
Pomůcka pro přípravu činností spojených se šifrováním	497
Pomůcka pro konfigurační postupy	498
Shrnutí	500
Otázky ke cvičení	500
Odkazy	501

ČÁST VI

Konfigurace virtuální privátní sítě VPN s protokolem IPSec

Kapitola 15

Podpora protokolu IPSec v produktech Cisco 505

Vytvoření zabezpečené virtuální sítě VPN s protokolem IPSec	506
Co je to IPSec?	507
Jak protokol IPSec funguje	509
Technologie použité v protokolu IPSec	514
Infrastruktura veřejného klíče a podpora certifikačních autorit	535
Toky IKE a IPSec v systémovém softwaru Cisco IOS	539
Přehled konfigurace protokolu IPSec	541
Shrnutí	547
Otázky ke cvičení	548
Odkazy	548

Kapitola 16

Konfigurace protokolu IPSec v Cisco IOS 551

Konfigurace IPSec v Cisco IOS s autentizací podle předem sdílených klíčů	552
Konfigurace IPSec v Cisco IOS s autentizací podle náhodných výrazů šifrovaných v RSA	579
Shrnutí	587
Případová studie: konfigurace IPSec v Cisco IOS s předem sdílenými klíči	588
Otázky ke cvičení	591
Odkazy	592

Kapitola 17

Konfigurace podpory IPSec v PIX Firewallu 595

Úkol 1: Příprava na protokol IPSec	597
Úkol 2: Konfigurace IKE a výměny předem sdílených klíčů	597
Úkol 3: Konfigurace IPSec	603
Úkol 4: Testování a kontrola celkové konfigurace protokolu IPSec	619
Shrnutí	621
Případová studie: konfigurace IPSec v PIX Firewallu s předem sdílenými klíči	622
Otázky ke cvičení	625
Odkazy	627

Kapitola 18

Škálování sítě Cisco s IPSec 629

Konfigurace podpory certifikační autority ve směrovačích Cisco a PIX Firewallu	630
Škálování virtuálních privátních sítí Cisco VPN	656
Shrnutí	663
Otázky ke cvičení	664
Odkazy	664

ČÁST VII
Přílohy

Příloha A

Scénář případové studie společnosti XYZ 669

Základní informace o společnosti XYZ	670
Firemní oddělení zapojená do projektu	672
Cíl zabezpečení sítě ve společnosti XYZ	673

Příloha B**Příklad zásad zabezpečení sítě
ve společnosti XYZ****675**

Formulace pravomocí a rozsahu pravidel	676
Zásady přípustného používání	678
Zásady identifikace a autentizace	679
Zásady přístupu k Internetu	679
Zásady přístupu k firemní síti	680
Zásady vzdáleného přístupu	680
Postupy při vzniku bezpečnostního incidentu	682

Příloha C**Konfigurace standardních
a rozšířených přístupových seznamů****685**

Adresování v protokolu IP a obecné principy přístupových seznamů	687
Konfigurace standardních přístupových seznamů IP	694
Konfigurace rozšířených přístupových seznamů IP	701
Ověření konfigurace přístupových seznamů	713
Pojmenované přístupové seznamy IP	714
Shrnutí	717
Odkazy	717

Příloha D**Odpovědi na otázky ke cvičení****719****Rejstřík****743**