

# Obsah

Poděkování	xv
Předmluva od autorů knihy	xvii
O autorech	xix
Odborný redaktor původního vydání	xxi
Úvod	xxiii

Kapitola 1

## **Úvod do ISA Serveru** **1**

---

Co je ISA Server?	1
Proč server pro „zabezpečení a urychlení“?	2
Zabezpečení Internetu	3
Urychlení Internetu	6
Historie ISA: Microsoft Proxy Server	8
V počátcích: Proxy Server, verze 1.0	8
Zlepšuje se to: Proxy Server, verze 2.0	8
Nový název a vylepšená funkčnost: Proxy Server 3.0 (ISA Server)	10
Provedení ISA Serveru	12
Samostatný ISA Server vs. člen pole	14
Instalační režimy ISA Serveru	15
Rodina podnikových serverů Microsoft .NET	16
Role ISA Serveru v síťovém prostředí	19
Přehled architektury ISA Serveru	19
Vrstvené filtrování	30
Filtrování paketů	21
Filtrování přepínaných okruhů	22
Filtrování na úrovni aplikací	23
Typy klientů ISA Serveru	24
Ověřování na ISA Serveru	32
Základní ověřování	33
Ověřování algoritmem Digest	34
Integrované ověřování Windows	34
Ověřování na základě certifikátu klienta	35

<b>Přehled hlavních částí ISA Serveru</b>	<b>35</b>
Bezpečnostní složka (firewall)	36
Přehled součástí firewallu	36
Zpevnění systému	38
Bezpečné, integrované sítě VPN	38
Integrovaná detekce průniku	41
Prvky pro ukládání webového obsahu do mezipaměti	42
Prvky pro sdílení připojení k Internetu	43
Prvky zajišťující rozšiřitelnost platformy	46
<b>Komu je určena tato kniha a co vše v ní najdete</b>	<b>47</b>
<b>Souhrn</b>	<b>49</b>
<b>Stručný přehled</b>	<b>50</b>
Co je ISA Server?	50
Přehled hlavních částí ISA Serveru	52
Komu je určena tato kniha a co vše v ní najdete	53
<b>Často kladené otázky</b>	<b>54</b>
Kapitola 2	
<b>ISA Server v podnikovém prostředí</b>	<b>57</b>
<b>Úvod</b>	<b>57</b>
<b>Charakteristiky rozlehlých sítí</b>	<b>57</b>
Spolehlivost	58
Škálovatelnost	59
Škálování směrem nahoru	60
Podpora více procesorů	60
Proč právě symetrický multiprocessing?	61
Hierarchické a distribuované ukládání do mezipaměti	63
<b>Návrh řešení pro rozlehlé sítě</b>	<b>68</b>
Obecné principy návrhů rozlehlých sítí	69
Co vzít do úvahy při návrhu implementace ISA Serveru	75
Funkčnost ISA Serveru	80
ISA Server a vzájemná spolupráce s dalšími produkty	81
Administrativní oprávnění	83
<b>Plánování polí s více servery</b>	<b>85</b>
Správa více serverů	86
Zálohování informací o konfiguraci pole ISA Serverů	86
<b>Používáme vrstvenou zásadu</b>	<b>88</b>
<b>Plánování jednotlivých prvků zásad</b>	<b>89</b>
<b>Principy licencování ISA Serveru</b>	<b>91</b>
<b>Souhrn</b>	<b>92</b>

<b>Kapitola 3 – Pojmy a zásady zabezpečení</b>	<b>721</b>
Přehled zabezpečení	721
Vymezení základních pojmů zabezpečení	721
Cíle zabezpečení	721
Kdo a jak může ohrozit zabezpečení sítě	722
Členění bezpečnostních nástrojů	723
Návrh souhrnného plánu zabezpečení	724
Začlenění ISA Serveru do plánu zabezpečení	724
<b>Kapitola 4 – Plánování a návrh rozmístění ISA Serverů do sítě</b>	<b>725</b>
Rozmístění ISA Serverů: sporné body při jeho plánování a návrhu	725
Implementace služby Active Directory	726
Faktory zajišťující nepřetržitou dostupnost služeb	726
<b>Kapitola 5 – Instalace ISA Serveru</b>	<b>727</b>
Instalace ISA Serveru na systém Windows 2000 Server	727
Vlastní průběh instalace	728
Přechod z Microsoft Proxy Serveru 2.0	728
<b>Kapitola 6 – Správa ISA Serveru</b>	<b>729</b>
Integrovaná správa	729
Obecné úlohy správy ISA Serveru	730
Používání funkcí pro monitorování, zasilání varovných zpráv, protokolování a tvorbu sestav	730
Vzdálená správa	730
<b>Kapitola 7 – Architektura ISA a konfigurace klientů</b>	<b>731</b>
Architektura ISA Serveru	731
Instalace a konfigurace klientů ISA Serveru	732
<b>Kapitola 8 – Konfigurace ISA Serveru pro přístup z podnikové sítě do Internetu</b>	<b>733</b>
Konfigurace serveru pro odchozí síťový provoz	733
Nastavení sítě v uzlu Network Configuration	733
Vytvoření bezpečné zásady odchozího provozu	734
Konfigurace filtrů aplikací, které ovlivní odchozí síťový provoz	734
Mezipaměť webové proxy a její nastavení	735
<b>Kapitola 9 – Konfigurace ISA Serveru pro přístup zvenčí do podnikové sítě</b>	<b>735</b>
Konfigurace filtrování paketů na ISA Serveru	735
Filtry aplikací, které ovlivňují příchozí přístup	735
Návrh uspořádání demilitarizované zóny	736
<b>Kapitola 10 – Publikování serverů do Internetu</b>	<b>736</b>
Typy publikování	736
Publikování webového serveru	736
Publikování služeb	737
Služba Gatekeeper H.323	738
Virtuální privátní sítě	738

<b>Kapitola 11 – Optimalizace, přizpůsobení, integrace a zálohování ISA Serveru</b>	<b>738</b>
Optimalizace výkonu ISA Serveru	738
Jak si ISA Server přizpůsobit „na míru“ svým potřebám	739
Integrace ISA Serveru s dalšími službami	740
Zálohování a obnova konfigurace ISA Serveru	741
<b>Kapitola 12 – Hledání a odstraňování chyb</b>	<b>741</b>
Základní principy hledání a odstraňování chyb	741
Řešení problémů při instalaci a konfiguraci ISA Serveru	742
Řešení problémů s ověřováním totožnosti a právy přístupu	742
Řešení problémů s klienty ISA	743
Řešení problémů v oblasti ukládání do mezipaměti, publikování a práce služeb	744
 <b>Rejstřík</b>	 <b>745</b>

---

<b>Stručný přehled</b>	<b>94</b>
Charakteristiky rozlehlých sítí	94
Návrh řešení pro rozlehlé sítě	95
Plánování polí s více servery	96
Problematika licencí ISA Serveru	96
<b>Často kladené otázky</b>	<b>97</b>
 Kapitola 3	
<b>Pojmy a zásady zabezpečení</b>	<b>99</b>
<b>Úvod</b>	<b>99</b>
<b>Přehled zabezpečení</b>	<b>100</b>
Vymezení základních pojmů zabezpečení	100
Bezpečnostní terminologie	103
<b>Cíle zabezpečení</b>	<b>106</b>
Řízení fyzického přístupu k počítačům a sítí	106
Souhrn problematiky fyzického zabezpečení	114
Prevence náhodné kompromitace dat	114
Prevence proti záměrným porušením bezpečnosti uvnitř podniku	116
Jak zamezit úmyslným interním porušením bezpečnosti	119
Jak zamezit neautorizovaným průnikům a útokům zvenčí	120
Externí vetřelci s možností interního přístupu	120
Taktické plánování	120
<b>Kdo a jak může ohrozit zabezpečení sítě</b>	<b>121</b>
Motivace vetřelců	121
Klasifikace určitých typů útoků	124
Útoky typu odepření služby (Denial-of-Service)	125
Skenování a spoofing	132
Útok pomocí zdrojového směrování	135
Zneužití jiných protokolů	135
Zneužití systému a softwaru	136
Trojské koně, viry a červi	136
<b>Členění prostředků pro zabezpečení</b>	<b>138</b>
Hardwarové prostředky pro zabezpečení	138
Softwarové prostředky pro zabezpečení	139
<b>Návrh souhrnného plánu zabezpečení</b>	<b>140</b>
Zhodnocení bezpečnostních potřeb	141
Hodnocení úrovně zabezpečení	143
Právní hlediska	144
Návrh zodpovědnosti za zabezpečení sítě	144
Bezpečnostní školení uživatelů sítě	149
<b>Začlenění ISA Serveru do plánu zabezpečení</b>	<b>150</b>
Role ISA Serveru při detekci průniků	150

---

Realizace plánu pro zpevnění systému prostřednictvím ISA Serveru	151
Cíle a vodítka pro zpevnění systému	152
Jak použít tunelování a přemosťování SSL pro zabezpečenou komunikaci na webu	154
<b>Souhrn</b>	<b>157</b>
<b>Stručný přehled</b>	<b>158</b>
Přehled zabezpečení	158
Vymezení základních pojmů zabezpečení	158
Cíle zabezpečení	159
Kdo a jak může ohrozit zabezpečení sítě	159
Členění bezpečnostních nástrojů	160
Návrh souhrnného plánu zabezpečení	161
Začlenění ISA Serveru do plánu zabezpečení	161
<b>Často kladené otázky</b>	<b>162</b>
Kapitola 4	
<b>Plánování a návrh rozmístění ISA Serverů do sítě</b>	<b>165</b>
<b>Úvod</b>	<b>165</b>
<b>Rozmístění ISA Serverů: faktory jeho plánování a návrhu</b>	<b>165</b>
Zhodnocení požadavků na síť a hardware	166
<b>Implementace služby Active Directory</b>	<b>177</b>
<b>Faktory zajišťující nepřetržitou dostupnost služeb</b>	<b>178</b>
Odolnost pevných disků proti chybám	179
Odolnost sítě proti chybám	183
<b>Jak určit vhodný režim instalace ISA Serveru</b>	<b>188</b>
Instalace ve firewallovém režimu	189
Instalace v ukládacím režimu	189
Instalace v integrovaném režimu	189
Výběr samostatného serveru či pole ISA Serverů	190
Plánování konfigurace klientů ISA	191
Faktory připojení k Internetu a služby DNS	195
<b>Souhrn</b>	<b>198</b>
<b>Stručný přehled</b>	<b>199</b>
Rozmístění ISA Serverů: sporné body při jeho plánování a návrhu	199
Implementace služby Active Directory	200
Faktory zajišťující nepřetržitou dostupnost služeb	200
<b>Často kladené otázky</b>	<b>201</b>

## Kapitola 5

<b>Instalace ISA Serveru</b>	<b>205</b>
Úvod	205
Instalace ISA Serveru na systém Windows 2000 Server	205
Přípravná fáze	206
Vlastní průběh instalace	209
Instalace ISA Serveru: zkouška	210
Povýšení samostatného serveru na člena pole: zkouška	220
Změny, ke kterým dojde po instalaci ISA Serveru	230
Přechod z Microsoft Proxy Serveru 2.0	231
Co se dá převést a co ne	231
Inovace Proxy serveru 2.0 na systém Windows 2000	237
Inovace instalace Proxy Serveru 2.0 na systému Windows NT 4.0	240
Souhrn	242
Stručný přehled	243
Instalace ISA Serveru na systém Windows 2000 Server	243
Vlastní průběh instalace	243
Přechod z Microsoft Proxy Serveru 2.0	244
Často kladené otázky	245

## Kapitola 6

<b>Správa ISA Serveru</b>	<b>247</b>
Úvod	247
Integrovaná správa	248
Konzola ISA Management	248
Objekty v konzole ISA	258
Průvodci ISA	274
Obecné úlohy správy ISA Serveru	275
Konfigurace oprávnění přístupu k objektu	275
Výchozí (implicitní) oprávnění	276
Správa členství v poli serverů	278
Používání funkcí pro monitorování, zasílání varovných zpráv, protokolování a tvorbu sestav	280
Vytváříme, konfigurujeme a sledujeme výstrahy	280
Sledování relací	285
Protokolování a jeho využití	286
Generování sestav	291
Vzdálená správa	304
Vzdálená správa ISA Serveru pomocí služby Terminal Services	307

<b>Souhrn</b>	<b>311</b>
<b>Stručný přehled</b>	<b>312</b>
Integrovaná správa	312
Obecné úlohy správy ISA Serveru	313
Používání funkcí pro monitorování, zaslání varovných zpráv, protokolování a tvorbu sestav	313
Vzdálená správa	313
<b>Často kladené otázky</b>	<b>314</b>

## Kapitola 7

---

## **Architektura ISA a konfigurace klientů** **317**

<b>Úvod</b>	<b>317</b>
<b>Architektura ISA Serveru</b>	<b>318</b>
Služba firewall	320
Ovladač protokolu NAT	322
Služba plánovaného stahování obsahu (Scheduled Content Download)	323
Vzájemné interakce služeb ISA Serveru	324
Změny v konfiguraci a s nimi spojené nutné restartování služeb ISA Serveru	325
<b>Instalace a konfigurace klientů ISA Serveru</b>	<b>327</b>
Klient SecureNAT	327
Klient firewallu	333
Instalace klientů firewallu v síti	337
Klient webové proxy	359
<b>Souhrn</b>	<b>365</b>
<b>Stručný přehled</b>	<b>367</b>
Architektura ISA Serveru	367
Instalace a konfigurace klientů ISA Serveru	368
<b>Často kladené otázky</b>	<b>369</b>

## Kapitola 8

---

## **Konfigurace ISA Serveru pro přístup z podnikové sítě do Internetu** **373**

<b>Úvod</b>	<b>373</b>
<b>Konfigurace serveru pro odchozí síťový provoz</b>	<b>374</b>
Konfigurace posluchačů, přijímajících odchozí webové požadavky	374
Výkonnost serveru	377
<b>Nastavení sítě v uzlu Network Configuration</b>	<b>377</b>
Řetězení firewallů: Směrování požadavků klientů SecureNAT a firewallu	378
Směrování požadavků klientů webové proxy	382

Konfigurace řetězení webové proxy u ISA Serverů	391
Odchozí požadavky protokolu PPTP	395
Tabulka místních adres	397
<b>Vytvoření bezpečné zásady odchozího provozu</b>	<b>403</b>
Vytváření a konfigurace prvků zásad	405
Vytváření pravidel z jednotlivých prvků zásad	424
Pravidla šířky pásma	425
Pravidla webu a obsahu	431
Pravidla protokolu	438
Pakety filtrů IP	445
<b>Konfigurace filtrů aplikací, které ovlivní odchozí síťový provoz</b>	<b>449</b>
Filtr pro přístup FTP	449
Filtr HTTP Redirector	451
Filtr SOCKS	454
<b>Mezipaměť webové proxy a její nastavení</b>	<b>457</b>
Prvky konfigurace webové mezipaměti	458
Služba plánovaného stahování obsahu	465
<b>Souhrn</b>	<b>469</b>
<b>Stručný přehled</b>	<b>470</b>
Konfigurace serveru pro odchozí síťový provoz	470
Nastavení sítě v uzlu Network Configuration	470
Vytvoření bezpečné zásady odchozího provozu	471
Konfigurace filtrů aplikací, které ovlivní odchozí síťový provoz	471
Mezipaměť webové proxy a její nastavení	471
<b>Často kladené otázky</b>	<b>472</b>
Kapitola 9	
<b>Konfigurace ISA Serveru pro přístup zvenčí do podnikové sítě</b>	<b>473</b>
<b>Úvod</b>	<b>473</b>
<b>Konfigurace filtrování paketů na ISA Serveru</b>	<b>473</b>
Princip činnosti filtrů paketů	474
Jak zapnout filtrování paketů	476
Vytvoření nových filtrů paketů	477
Správa filtrů paketů	483
Podpora dalších aplikací na ISA Serveru	484
Využití filtrů paketů pro publikování (zveřejnění) služeb na počítačích demilitarizované zóny	487
Volby pro filtrování paketů	487
<b>Filtry aplikací, které ovlivňují příchozí přístup</b>	<b>493</b>
Filtr detekce průniku službou DNS	493
Nastavení filtru H.323	494

Filtr detekce průniku protokolem POP	495
Filtr RPC	496
Filtr SMTP	496
Konfigurace doplňku SMTP Message Screener	499
<b>Návrh uspořádání demilitarizované zóny</b>	<b>506</b>
Omezení demilitarizovaných zón	506
Konfigurace demilitarizované zóny	507
Demilitarizovaná zóna a třídový ISA Server	509
Publikování služeb spuštěných v demilitarizované zóně	511
Faktory ovlivňující konfiguraci předstunutého počítače	513
<b>Souhrn</b>	<b>516</b>
<b>Stručný přehled</b>	<b>516</b>
Konfigurace filtrování paketů na ISA Serveru	516
Filtry aplikací, které ovlivňují příchozí přístup	517
Návrh uspořádání demilitarizované zóny	517
<b>Často kladené otázky</b>	<b>517</b>
Kapitola 10	
<b>Publikování serverů do Internetu</b>	<b>519</b>
<b>Úvod</b>	<b>519</b>
<b>Typy publikování</b>	<b>519</b>
Publikování webu	520
Publikování serveru	520
Publikování služeb v demilitarizované zóně	521
<b>Publikování webového serveru</b>	<b>522</b>
Příprava na publikování	522
Shrnutí postupu pro publikování webu – základní publikování	532
Publikování webu umístěného přímo na ISA Serveru	536
Publikování webu prostřednictvím přeměrování protokolu	543
Kreativní publikování, využívající sady cílů	545
Zabezpečené publikování webů	549
<b>Publikování služeb</b>	<b>558</b>
Omezení pravidel publikování serveru	559
Přípravné fáze publikování serveru	561
Shrnutí postupu pro publikování serveru – základní publikování	562
Zabezpečené publikování poštovního serveru	566
Publikování terminálového serveru	572
Publikování webového serveru prostřednictvím publikování serveru	575
<b>Služba Gatekeeper H.323</b>	<b>577</b>
Volání gatekeeper-to-gatekeeper	580
Servery ILS	582
Klienti NetMeetingu na Internetu	583

Konfigurace gatekeeperu	584
Pravidla směrování volání (Call Routing Rules)	587
Správa gatekeeperu	593
<b>Virtuální privátní síť</b>	<b>595</b>
<b>Souhrn</b>	<b>605</b>
<b>Stručný přehled</b>	
Typy publikování	607
Publikování webového serveru	607
Publikování služeb	608
Služba Gatekeeper H.323	608
Virtuální privátní síť	609
<b>Často kladené otázky</b>	<b>609</b>

## Kapitola 11

## **Optimalizace, přizpůsobení, integrace a zálohování ISA Serveru** **613**

<b>Úvod</b>	<b>613</b>
<b>Optimalizace výkonu ISA Serveru</b>	<b>614</b>
Stanovení výchozích hodnot a monitorování výkonu	615
Běžné problémy v oblasti výkonu ISA Serveru a jejich řešení	638
<b>Jak si ISA Server přizpůsobit „na míru“ svým potřebám</b>	<b>650</b>
Jak použít SDK (ISA Server Software Developer's Kit)	650
Jak použít doplňky jiných výrobců	653
<b>Integrace ISA Serveru s dalšími službami</b>	<b>655</b>
Spolupráce se službou Active Directory	656
Spolupráce se službou Směrování a vzdáleného přístupu	657
Spolupráce se serverem IIS (Internet Information Server)	658
Spolupráce s protokolem IPSec	659
Integrace ISA Serveru do domény Windows NT 4.0	662
<b>Zálohování a obnova konfigurace ISA Serveru</b>	<b>663</b>
Zásady zálohování	663
Zálohování a obnova konfigurace samostatných serverů	663
Zálohování a obnova konfigurace pole a rozlehlé sítě	665
<b>Souhrn</b>	<b>667</b>
<b>Stručný přehled</b>	<b>668</b>
Optimalizace výkonu ISA Serveru	668
Jak si ISA Server přizpůsobit „na míru“ svým potřebám	669
Integrace ISA Serveru s dalšími službami	670
Zálohování a obnova konfigurace ISA Serveru	671
<b>Často kladené otázky</b>	<b>671</b>

Kapitola 12

---

<b>Hledání a odstraňování chyb</b>	<b>673</b>
Úvod	673
<b>Základní principy hledání a odstraňování chyb</b>	<b>674</b>
Vodítka pro řešení problémů	675
<b>Řešení problémů při instalaci a konfiguraci ISA Serveru</b>	<b>690</b>
Problémy s neslučitelností hardwaru a softwaru	691
Potíže s úvodní konfigurací ISA Serveru	692
<b>Řešení problémů s ověřováním totožnosti a právy přístupu</b>	<b>695</b>
Problém s přístupem	697
Problémy s telefonickým připojením a sítěmi VPN	700
<b>Řešení problémů s klienty ISA</b>	<b>701</b>
Problémy s výkonem klientů	701
Problémy s připojením klientů	703
<b>Řešení problémů v oblasti ukládání do mezipaměti, publikování a práce služeb</b>	<b>706</b>
Problémy s ukládáním do mezipaměti	706
Problém při publikování	707
<b>Souhrn</b>	<b>710</b>
<b>Stručný přehled</b>	<b>710</b>
Základní principy hledání a odstraňování chyb	710
Řešení problémů při instalaci a konfiguraci ISA Serveru	711
Řešení problémů s ověřováním totožnosti a právy přístupu	712
Řešení problémů s klienty ISA	712
Řešení problémů v oblasti ukládání do mezipaměti, publikování a práce služeb	713
<b>Často kladené otázky</b>	<b>713</b>
Dodatek	
<b>Stručný přehled ISA Serveru 2000</b>	<b>715</b>
<b>Kapitola 1 – Úvod do ISA Serveru</b>	<b>715</b>
Co je ISA Server?	715
Přehled hlavních částí ISA Serveru	717
Komu je určena tato kniha a co vše v ní najdete	718
<b>Kapitola 2 – ISA Server v podnikovém prostředí</b>	<b>718</b>
Charakteristiky rozlehlých sítí	718
Návrh řešení pro rozlehlé sítě	719
Plánování polí s více servery	720
Problematika licencí ISA Serveru	721