

# Spis treści

Podziękowania .....	xvii
Wprowadzenie .....	xix
Konwencje wykorzystane w książce .....	xx
Wskazówki dla Czytelnika .....	xx
O zawartości płyty CD .....	xxi
Wymagania systemowe .....	xxii
Pomoc techniczna .....	xxii

## Część I Infrastruktura adresowania i przepływu pakietów

<b>1 Protokół IPv4 .....</b>	<b>3</b>
<b>Pojęcia .....</b>	<b>3</b>
Warstwy sieciowe .....	3
Adresowanie protokołu IPv4 .....	4
Prywatne adresy protokołu IPv4 .....	6
Mechanizm automatycznego nadawania prywatnych adresów IP (APIPA) .....	8
Adresy rozgłoszeniowe .....	8
Translacja adresów sieciowych .....	10
Adresowanie w warstwie 2 i w warstwie 3 .....	12
Protokoły warstwy 4: UDP i TCP .....	13
<b>Czynniki wymagające uwzględnienia podczas planowania i projektowania .....</b>	<b>14</b>
Projektowanie połączenia z siecią Internet .....	14
Tworzenie schematu adresowania protokołu IPv4 .....	15
Planowanie adresów hostów .....	17
Korzystanie z tuneli VPN .....	17
Planowanie nadmiarowości .....	19
Korzystanie z komputerów z kilkoma połączeniami sieciowymi .....	20
<b>Kroki procesu wdrożenia .....</b>	<b>21</b>
Ręczne konfigurowanie klientów pracujących z protokołem IPv4 .....	21
Konfigurowanie sposobu zachowywania się klienta w sytuacji braku dostępnego serwera DHCP .....	22
Dodawanie nowych tras do tabeli tras .....	22
<b>Bieżące zadania administracyjne .....</b>	<b>23</b>
<b>Rozwiązywanie problemów .....</b>	<b>23</b>
ARP .....	23
Ipconfig .....	24
Netstat .....	25
PathPing .....	26
Monitor wydajności .....	27
Ping .....	28
Menedżer zadań .....	29

Diagnostyka sieci systemu Windows Network Diagnostics .....	29
Podsumowanie rozdziału .....	30
Informacje dodatkowe .....	30
<b>2 Protokół IPv6 .....</b>	<b>31</b>
Pojęcia .....	31
Różnice pomiędzy protokołami IPv4 i IPv6 .....	32
Adresowanie protokołu IPv6 .....	34
Automatyczna konfiguracja protokołu IPv6 .....	40
DHCPv6 .....	42
Wykrywanie sąsiadów .....	42
Zabezpieczenia protokołu IPv6 .....	43
Technologie wspomagające przechodzenie do protokołu IPv6 .....	43
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	51
Migracja do protokołu IPv6 .....	51
Uzyskiwanie adresów IPv6 .....	52
Planowanie aktualizacji infrastruktury sieciowej .....	52
Planowanie wykorzystania technologii wspierających przechodzenie do protokołu IPv6 .....	54
Kroki procesu wdrożenia .....	55
Wyłączanie protokołu IPv6 .....	55
Ręczne konfigurowanie protokołu IPv6 .....	56
Konfigurowanie protokołu IPv6 za pomocą skryptu .....	57
Włączanie obsługi technologii ISATAP .....	57
Włączanie obsługi technologii Teredo .....	60
Konfigurowanie komputera jako routera protokołu IPv6 .....	61
Bieżące zadania administracyjne .....	65
Rozwiązywanie problemów .....	65
Netsh .....	65
Ipconfig .....	66
Nslookup .....	67
Rozwiązywanie problemów związanych z funkcjonowaniem technologii Teredo .....	68
Podsumowanie rozdziału .....	69
Informacje dodatkowe .....	69
<b>3 Protokół DHCP .....</b>	<b>71</b>
Pojęcia .....	71
Proces przydzielania adresu przez serwer DHCP .....	71
Cykl życia klienta DHCP .....	73
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	73
Serwery DHCP .....	74
Agenci przekazywania DHCP .....	75
Czas trwania dzierżawy DHCP .....	76
Projektowanie zakresów .....	77
Łączenie serwerów DHCP w klastry .....	78
Dynamiczny system DNS .....	78

Kroki procesu wdrożenia .....	79
Serwery DHCP .....	79
Agenci przekazywania DHCP .....	89
Konfiguracja klienta protokołu DHCP .....	90
Bieżące zadania administracyjne .....	91
Monitorowanie serwerów DHCP .....	92
Ręczne archiwizowanie i odtwarzanie serwera DHCP .....	93
Rozwiązywanie problemów .....	94
Rozwiązywanie problemów związanych z klientami protokołu DHCP .....	95
Rozwiązywanie problemów związanych z serwerami DHCP .....	95
Używanie funkcji rejestrowania inspekcji do analizy zachowania serwera DHCP .....	96
Podsumowanie rozdziału .....	97
Informacje dodatkowe .....	97
<b>4 Zapora systemu Windows z zabezpieczeniami zaawansowanymi</b> .....	<b>99</b>
Pojęcia .....	99
Filtrowanie pakietów za pomocą zapory ogniowej systemu Windows .....	100
Ochrona przesyłanych w sieci danych za pomocą protokołu IPsec .....	100
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	106
Planowanie zasad zapory ogniowej systemu Windows .....	107
Ochrona komunikacji za pomocą protokołu IPsec .....	109
Kroki procesu wdrożenia .....	117
Konfigurowanie ustawień zapory ogniowej za pomocą zasad grupy .....	117
Reguły zabezpieczeń połączeń IPsec .....	125
Bieżące zadania administracyjne .....	130
Rozwiązywanie problemów .....	132
Funkcja rejestrowania zapory ogniowej systemu Windows .....	133
Monitorowanie skójarzeń zabezpieczeń protokołu IPsec .....	136
Korzystanie z monitora sieci .....	136
Podsumowanie rozdziału .....	137
Informacje dodatkowe .....	137
<b>5 Zarządzanie mechanizmem QoS przy użyciu zasad grupy</b> .....	<b>139</b>
Pojęcia .....	139
Przyczyny problemów z wydajnością sieci .....	139
W czym może pomóc stosowanie mechanizmu QoS .....	141
Mechanizm QoS dla ruchu wychodzącego .....	142
Mechanizm QoS dla ruchu przychodzącego .....	145
Implementacja mechanizmu QoS .....	145
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	146
Określanie celów stosowania mechanizmu QoS .....	146
Planowanie wartości kodów DSCP .....	146
Planowanie dławienia ruchu .....	149
Wymagania sprzętowe i programowe .....	150
Planowanie obiektów zasad grupy oraz zasad QoS .....	151

Zasady QoS dla komputerów mobilnych pracujących z systemem Windows Vista .....	152
Kroki procesu wdrożenia .....	153
Sposób konfigurowania mechanizmów QoS za pomocą ustawień zasad grupy .....	153
Konfigurowanie ogólnosystemowych ustawień QoS .....	157
Bieżące zadania administracyjne .....	159
Usuwanie zasad QoS .....	159
Edycja zasad QoS .....	160
Monitorowanie działania mechanizmu QoS .....	160
Rozwiązywanie problemów .....	163
Analizowanie zasad QoS .....	163
Sprawdzanie zachowywania w sieci kodów DSCP .....	166
Izolowanie przyczyn problemów z wydajnością sieci .....	167
Podsumowanie rozdziału .....	168
Informacje dodatkowe .....	169
<b>6 Budowanie skalowalnych sieci .....</b>	<b>171</b>
Pojęcia .....	171
TCP Chimney Offload .....	172
Receive-Side Scaling (Skalowanie po stronie odbierającej) .....	174
NetDMA .....	176
IPsec Offload .....	177
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	178
Ocenianie skalowalnych technologii sieciowych .....	178
Testy obciążeniowe serwerów .....	180
Monitorowanie wydajności serwera .....	181
Kroki procesu wdrożenia .....	184
Konfigurowanie technologii TCP Chimney Offload .....	184
Konfigurowanie technologii Receive-Side Scaling .....	184
Konfigurowanie technologii NetDMA .....	185
Konfigurowanie technologii IPsec Offload .....	185
Bieżące zadania administracyjne .....	186
Rozwiązywanie problemów .....	186
Rozwiązywanie problemów związanych z funkcjonowaniem technologii TCP Chimney Offload .....	187
Rozwiązywanie problemów związanych z funkcjonowaniem technologii IPsec Offload .....	188
Podsumowanie rozdziału .....	189
Informacje dodatkowe .....	189

## **Część III Infrastruktura rozwiązywania nazw**

<b>7 Usługa DNS .....</b>	<b>193</b>
Pojęcia .....	193
Hierarchia systemu DNS .....	193
Strefy systemu DNS .....	194

Rekordy systemu DNS .....	194
Dynamiczne aktualizacje DNS .....	195
Tłumaczenie nazw przez system DNS .....	196
<b>Czynniki wymagające uwzględnienia podczas planowania i projektowania</b>	<b>197</b>
Strefy DNS .....	198
Rozmieszczenie serwerów DNS .....	199
Replikacja stref DNS .....	201
Zabezpieczenia systemu DNS .....	202
Strefa GlobalNames .....	204
<b>Kroki procesu wdrożenia</b> .....	<b>205</b>
Konfigurowanie serwera DNS .....	205
Konfigurowanie serwera DHCP .....	217
Konfigurowanie klientów usługi DNS .....	219
Konfigurowanie nadmiarowych serwerów DNS .....	220
<b>Bieżące zadania administracyjne</b> .....	<b>221</b>
Dodawanie zasobów rekordów .....	221
Administrowanie strefami .....	222
Automatyczne monitorowanie .....	222
Promowanie strefy pomocniczej na strefą podstawową .....	225
<b>Rozwiązywanie problemów</b> .....	<b>226</b>
Dzienniki zdarzeń .....	226
Korzystanie z programu Nslookup .....	227
Rejestrowanie w trybie Debug po stronie serwera .....	229
Korzystanie z programu DNSLint .....	230
Korzystanie z programu DCdiag .....	231
Korzystanie z monitora sieci .....	233
<b>Podsumowanie rozdziału</b> .....	<b>233</b>
<b>Informacje dodatkowe</b> .....	<b>234</b>
<b>8 Usługa WINS</b> .....	<b>235</b>
<b>Pojęcia</b> .....	<b>235</b>
Historia .....	235
Nazwy systemu NetBIOS .....	236
Tłumaczenie nazw przez usługę WINS .....	237
Rejestracje klientów WINS .....	238
<b>Czynniki wymagające uwzględnienia podczas planowania i projektowania</b>	<b>239</b>
Rozmieszczenie serwerów WINS .....	239
Replikacja WINS .....	240
<b>Kroki procesu wdrożenia</b> .....	<b>242</b>
Konfigurowanie serwera WINS .....	242
Konfigurowanie replikacji WINS .....	242
Konfigurowanie klientów usługi WINS .....	243
<b>Bieżące zadania administracyjne</b> .....	<b>245</b>
Wykonywanie kopii zapasowej bazy danych serwera WINS .....	246
Kompaktowanie bazy danych serwera WINS .....	246
Sprawdzanie spójności bazy danych .....	247
Monitorowanie serwera WINS .....	248

Dodawanie statycznych rekordów WINS .....	249
Usuwanie rekordów WINS .....	251
Rozwiązywanie problemów .....	252
Rozwiązywanie problemów związanych z serwerami WINS .....	252
Rozwiązywanie problemów związanych z klientami serwera WINS .....	254
Podsumowanie rozdziału .....	258
Informacje dodatkowe .....	258

### **Część III.....Infrastruktura dostępu do sieci**

<b>9 Infrastruktura uwierzytelniania.....</b>	<b>261</b>
Pojęcia .....	261
Usługa katalogowa domeny Active Directory .....	261
Infrastruktura klucza publicznego .....	265
Zasady grupy.....	271
RADIUS.....	275
Czynniki wymagające uwzględnienia podczas planowania i projektowania.....	280
Usługa katalogowa Active Directory .....	281
Infrastruktura PKI .....	282
Zasady grupy.....	284
Serwer RADIUS .....	285
Kroki procesu wdrożenia .....	295
Wdrażanie usługi katalogowej Active Directory .....	295
Wdrażanie infrastruktury PKI.....	296
Zasady grupy.....	306
Serwery RADIUS .....	307
Stosowanie serwerów proxy protokołu RADIUS do uwierzytelniania pomiędzy domenami .....	316
Stosowanie serwerów proxy protokołu RADIUS do skalowania infrastruktury uwierzytelniania .....	324
Bieżące zadania administracyjne .....	329
Usługa Active Directory .....	329
Infrastruktura PKI .....	330
Zasady grupy.....	330
Serwery RADIUS .....	330
Narzędzia służące do rozwiązywania problemów.....	332
Usługa Active Directory .....	332
Infrastruktura PKI .....	332
Zasady grupy.....	333
Serwery RADIUS .....	333
Podsumowanie rozdziału .....	335
Informacje dodatkowe .....	335
<b>10 Sieci bezprzewodowe IEEE 802.11 .....</b>	<b>339</b>
Pojęcia .....	339
Obsługa standardów IEEE 802.11.....	340
Zabezpieczenia sieci bezprzewodowej.....	343

Składniki bezprzewodowych sieci typu 802.11 .....	349
<b>Czynniki wymagające uwzględnienia podczas planowania i projektowania</b>	<b>350</b>
Technologie zabezpieczeń bezprzewodowych .....	350
Tryby uwierzytelniania bezprzewodowego.....	353
Infrastruktura sieci intranetowej.....	354
Rozmieszczenie bezprzewodowych punktów dostępowych .....	356
Infrastruktura uwierzytelniania .....	361
Klienci bezprzewodowi .....	363
Infrastruktura PKI .....	376
Narzucanie 802.1X i platforma NAP .....	380
<b>Wdrażanie chronionego dostępu do sieci bezprzewodowej</b> .....	<b>380</b>
Wdrażanie certyfikatów .....	381
Konfigurowanie kont i grup usługi katalogowej Active Directory .....	383
Konfigurowanie serwerów NPS .....	383
Wdrażanie bezprzewodowych punktów dostępowych .....	385
Konfigurowanie klientów bezprzewodowych .....	389
<b>Bieżące zadania administracyjne</b> .....	<b>396</b>
Zarządzanie kontami użytkowników i komputerów.....	396
Zarządzanie bezprzewodowymi punktami dostępowymi.....	396
Aktualizowanie profili bezprzewodowych w formacie XML .....	397
<b>Rozwiązywanie problemów</b> .....	<b>398</b>
Narzędzia systemu Windows służące do rozwiązywania problemów związanych z sieciami bezprzewodowymi.....	398
Rozwiązywanie problemów na bezprzewodowym kliencie z systemem Windows .....	407
Rozwiązywanie problemów związanych z bezprzewodowymi punktami dostępowymi .....	409
Rozwiązywanie problemów związanych z funkcjonowaniem infrastruktury uwierzytelniania .....	415
<b>Podsumowanie rozdziału</b> .....	<b>422</b>
<b>Informacje dodatkowe</b> .....	<b>422</b>
<b>11 Uwierzytelnianie IEEE 802.1X w sieciach przewodowych</b> .....	<b>425</b>
<b>Pojęcia</b> .....	<b>425</b>
Składniki przewodowej sieci z uwierzytelnianiem 802.1X.....	426
<b>Czynniki wymagające uwzględnienia podczas planowania i projektowania</b>	<b>427</b>
Metody uwierzytelniania połączeń przewodowych .....	427
Tryby uwierzytelniania połączeń przewodowych.....	431
Infrastruktura uwierzytelniania .....	433
Klienci przewodowi .....	434
Infrastruktura PKI .....	441
Narzucanie 802.1X i platforma NAP .....	444
<b>Wdrażanie dostępu do sieci przewodowej z uwierzytelnianiem 802.1X</b> .....	<b>445</b>
Wdrażanie certyfikatów .....	445
Konfigurowanie kont i grup usługi katalogowej Active Directory .....	448
Konfigurowanie serwerów NPS .....	448
Konfigurowanie przełączników sieciowych z obsługą standardu 802.1X	450

Konfigurowanie klientów przewodowych.....	452
Bieżące zadania administracyjne.....	456
Zarządzanie kontami użytkowników i komputerów.....	456
Zarządzanie przełącznikami sieciowymi z obsługą standardu 802.1X ....	457
Aktualizowanie profili przewodowych w formacie XML.....	457
Rozwiązywanie problemów.....	458
Narzędzia systemu Windows, służące do rozwiązywania problemów związanych z sieciami przewodowymi.....	458
Rozwiązywanie problemów na przewodowym kliencie z systemem Windows.....	464
Rozwiązywanie problemów związanych z przełącznikami sieciowymi, obsługującymi standard 802.1X.....	466
Rozwiązywanie problemów związanych z funkcjonowaniem infrastruktury uwierzytelniania.....	470
Podsumowanie rozdziału.....	477
Informacje dodatkowe.....	478
<b>12 Zdalny dostęp poprzez połączenia VPN.....</b>	<b>481</b>
Pojęcia.....	481
Składniki opartego na systemie Windows, zdalnego dostępu za pośrednictwem połączeń VPN.....	484
Czynniki wymagające uwzględnienia podczas planowania i projektowania.....	486
Protokoły połączeń VPN.....	486
Metody uwierzytelniania.....	491
Serwery VPN.....	494
Infrastruktura sieci Internet.....	498
Infrastruktura sieci Intranet.....	500
Jednoczesność dostępu dla klientów VPN do sieci Internet oraz do sieci intranetowej.....	505
Infrastruktura uwierzytelniania.....	507
Klienci VPN.....	509
Infrastruktura PKI.....	513
Narzucanie VPN i platforma NAP.....	518
Dodatkowe kwestie związane z bezpieczeństwem.....	518
Silne szyfrowanie łączy.....	519
Filtrowanie pakietów połączenia VPN na serwerze VPN.....	519
Filtrowanie przez zaporę ogniową pakietów połączeń VPN.....	519
Wykorzystywanie serwerów VPN do różnych celów.....	532
Blokowanie ruchu trasowanego przez klientów VPN.....	534
Jednoczesność dostępu.....	535
Nieużywane protokoły VPN.....	536
Wdrażanie zdalnego dostępu do sieci opartego na połączeniach VPN.....	536
Wdrażanie certyfikatów.....	536
Konfigurowanie infrastruktury dostępu do sieci Internet.....	541
Konfigurowanie kont użytkowników i grup usługi katalogowej Active Directory.....	542
Konfigurowanie serwerów RADIUS.....	542



Wdrażanie serwerów VPN .....	544
Konfigurowanie infrastruktury sieci intranetowej.....	549
Wdrażanie klientów VPN .....	552
Bieżące zadania administracyjne .....	559
Zarządzanie kontami użytkowników .....	559
Zarządzanie serwerami VPN .....	559
Aktualizowanie profili menedżera połączeń .....	562
Rozwiązywanie problemów .....	562
Narzędzia służące do rozwiązywania problemów .....	562
Rozwiązywanie problemów związanych ze zdalnym dostępem za pomocą połączeń VPN .....	567
Podsumowanie rozdziału .....	575
Informacje dodatkowe .....	575
<b>13 Połączenia VPN pomiędzy lokalizacjami .....</b>	<b>577</b>
Pojęcia .....	577
Omówienie funkcji trasowania z wybieraniem numeru na żądanie .....	578
Składniki opartych na systemie Windows połączeń VPN pomiędzy dwoma lokalizacjami .....	584
Czynniki wymagające uwzględnienia podczas planowania i projektowania.....	585
Protokoły VPN .....	585
Metody uwierzytelniania .....	588
Routery VPN .....	592
Infrastruktura sieci Internet .....	597
Infrastruktura wewnętrznej sieci w łączonych lokalizacjach .....	600
Infrastruktura uwierzytelniania .....	603
Infrastruktura PKI .....	605
Wdrażanie połączeń VPN pomiędzy lokalizacjami .....	609
Wdrażanie certyfikatów .....	609
Konfigurowanie infrastruktury dostępu do sieci Internet .....	614
Konfigurowanie kont użytkowników i grup usługi katalogowej Active Directory .....	615
Konfigurowanie serwerów RADIUS .....	616
Wdrażanie routerów odbierających .....	618
Wdrażanie routerów wywołujących .....	625
Konfigurowanie infrastruktury sieci wewnętrznej.....	632
Konfigurowanie infrastruktury sieciowej znajdującej się pomiędzy lokalizacjami .....	635
Bieżące zadania administracyjne .....	637
Zarządzanie kontami użytkowników .....	637
Zarządzanie routerami VPN .....	638
Rozwiązywanie problemów .....	640
Narzędzia służące do rozwiązywania problemów .....	640
Rozwiązywanie problemów związanych z połączeniami VPN łączącymi dwie lokalizacje .....	641
Podsumowanie rozdziału .....	651
Informacje dodatkowe .....	652

## Część IV .....Infrastruktura ochrony dostępu do sieci

<b>14 Omówienie mechanizmu ochrony dostępu do sieci</b> .....	657
Potrzeba stosowania ochrony dostępu do sieci.....	657
Złośliwe oprogramowanie i jego wpływ na stosowanie komputerów w przedsiębiorstwie .....	657
Ochrona przez złośliwym oprogramowaniem w sieciach korporacyjnych	659
Rola platformy NAP .....	664
Korzyści biznesowe ze stosowania platformy NAP .....	667
Składniki platformy NAP .....	668
Agenci kondycji systemu oraz składniki weryfikujące kondycję systemu	671
Klienci i serwery narzucania .....	672
Serwery NPS.....	672
Metody narzucania .....	673
Narzucanie IPsec.....	674
Narzucanie 802.1X.....	674
Narzucanie VPN.....	675
Narzucanie DHCP .....	675
Sposób działania platformy NAP .....	676
Sposób działania narzucania IPsec .....	677
Sposób działania narzucania 802.1X .....	678
Sposób działania narzucania VPN .....	679
Sposób działania narzucania DHCP .....	680
Podsumowanie rozdziału .....	682
Informacje dodatkowe .....	682
<b>15 Przygotowanie mechanizmów ochrony dostępu do sieci</b> .....	685
Ocena aktualnej infrastruktury sieciowej .....	685
Komputery intranetowe.....	686
Pomocnicza infrastruktura sieciowa .....	688
Serwery zasad kondycji NAP .....	690
Czynniki wymagające uwzględnienia podczas planowania i projektowania	690
Kroki procesu wdrożenia .....	693
Bieżące zadania administracyjne .....	694
Konfiguracja zasad wymogów kondycji .....	695
Składniki zasad wymogów kondycji .....	695
Sposób przeprowadzania oceny kondycji klienta NAP.....	704
Czynniki wymagające uwzględnienia podczas planowania i projektowania zasad wymogów kondycji .....	709
Serwery naprawcze .....	710
Serwery naprawcze a metody narzucania NAP .....	712
Czynniki wymagające uwzględnienia w procesie planowania i projektowania serwerów naprawczych.....	713
Podsumowanie rozdziału .....	714
Informacje dodatkowe .....	715
<b>16 Narzucanie IPsec</b> .....	717

Omówienie metod narzucania IPsec .....	717
Sieci logiczne tworzone przez metody narzucania IPsec .....	719
Procesy zachodzące podczas inicjowania komunikacji objętej metodami narzucania IPsec .....	720
Reguły zabezpieczeń połączeń dla metod narzucania IPsec .....	723
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	726
Usługa katalogowa Active Directory .....	726
Infrastruktura PKI .....	727
Urzędy rejestrowania kondycji .....	734
Zasady protokołu IPsec .....	742
Klienci NAP .....	743
Wdrażanie metod narzucania IPsec .....	744
Konfigurowanie usługi Active Directory .....	745
Konfigurowanie infrastruktury PKI .....	745
Konfigurowanie urzędów rejestrowania kondycji .....	750
Konfigurowanie serwerów zasad kondycji NAP .....	758
Konfigurowanie serwerów naprawczych w sieci granicznej .....	763
Konfigurowanie klientów NAP .....	763
Punkt kontrolny dla procesu wdrażania metod narzucania IPsec w trybie raportowania .....	767
Konfigurowanie i stosowanie zasad protokołu IPsec .....	768
Bieżące zadania administracyjne .....	775
Dodawanie nowego klienta NAP .....	776
Dodawanie nowych agentów SHA oraz nowych modułów SHV .....	776
Zarządzanie urzędami certyfikacji platformy NAP .....	776
Zarządzanie urzędami rejestrowania kondycji .....	778
Rozwiązywanie problemów .....	780
Narzędzia służące do rozwiązywania problemów .....	780
Rozwiązywanie problemów związanych z metodami narzucania IPsec .....	784
Podsumowanie rozdziału .....	792
Informacje dodatkowe .....	792
<b>17 Narzucanie 802.1X .....</b>	<b>795</b>
Omówienie metod narzucania 802.1X .....	795
Stosowanie list ACL .....	798
Stosowanie sieci VLAN .....	800
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	801
Grupa zabezpieczeń dla wykluczania NAP .....	801
Metody uwierzytelniania 802.1X .....	801
Typ narzucania 802.1X .....	802
Punkty dostępowe 802.1X .....	802
Klienci NAP .....	803
Wdrażanie metod narzucania 802.1X .....	805
Konfigurowanie usługi Active Directory .....	806
Konfigurowanie metody uwierzytelniania opartej na protokole PEAP .....	806
Konfigurowanie punktów dostępowych 802.1X .....	808
Konfigurowanie serwerów naprawczych w sieci z ograniczeniami .....	809

Konfigurowanie serwerów zasad kondycji NAP .....	809
Konfigurowanie klientów NAP .....	819
Punkt kontrolny dla procesu wdrażania metod narzucania 802.1X w trybie raportowania .....	823
Testowanie ograniczania dostępu do sieci .....	823
Konfigurowanie zasad sieci dla niezgodnych klientów NAP do pracy w trybie odroczonego narzucania .....	825
Konfigurowanie zasady sieciowej do pracy w trybie narzucania .....	826
Bieżące zadania administracyjne .....	828
Dodawanie nowego klienta NAP .....	828
Dodawanie nowych agentów SHA oraz nowych modułów SHV .....	828
Zarządzanie punktami dostępowymi 802.1X .....	829
Rozwiązywanie problemów .....	829
Narzędzia służące do rozwiązywania problemów .....	829
Rozwiązywanie problemów związanych z metodami narzucania 802.1X .....	832
Podsumowanie rozdziału .....	836
Informacje dodatkowe .....	836
<b>18 Narzucanie VPN .....</b>	<b>839</b>
Omówienie metod narzucania VPN .....	839
Czynniki wymagające uwzględnienia podczas planowania i projektowania .....	843
Stosowanie składnika Network Access Quarantine Control .....	843
Grupa zabezpieczeń dla wykluczania NAP .....	845
Rodzaje filtrowania pakietów .....	845
Metody uwierzytelniania połączeń VPN .....	846
Serwery VPN .....	847
Klienci NAP .....	847
Wdrażanie metod narzucania VPN .....	850
Konfigurowanie usługi Active Directory .....	851
Konfigurowanie serwerów VPN .....	851
Konfigurowanie metody uwierzytelniania opartej na protokole PEAP .....	852
Konfigurowanie serwerów naprawczych .....	852
Konfigurowanie serwerów zasad kondycji NAP .....	853
Konfigurowanie klientów NAP .....	861
Punkt kontrolny dla procesu wdrażania metod narzucania VPN w trybie raportowania .....	864
Testowanie ograniczania dostępu do sieci .....	864
Konfigurowanie trybu odroczonego narzucania .....	866
Konfigurowanie zasady sieciowej do pracy w trybie narzucania .....	867
Bieżące zadania administracyjne .....	869
Dodawanie nowego klienta NAP .....	869
Dodawanie nowych agentów SHA oraz nowych modułów SHV .....	869
Rozwiązywanie problemów .....	870
Narzędzia służące do rozwiązywania problemów .....	870
Rozwiązywanie problemów związanych z metodami narzucania VPN .....	873
Podsumowanie rozdziału .....	877
Informacje dodatkowe .....	877

<b>19 Narzucanie DHCP</b> .....	879
<b>Omówienie metod narzucania DHCP</b> .....	879
<b>Czynniki wymagające uwzględnienia podczas planowania i projektowania</b>	882
<b>Grupa zabezpieczeń dla wykluczania NAP</b> .....	882
<b>Serwery DHCP</b> .....	883
<b>Serwery zasad kondycji NAP</b> .....	884
<b>Zasady wymogów kondycji dla określonych zakresów DHCP</b> .....	884
<b>Opcje DHCP dla klientów NAP</b> .....	885
<b>Sposób zachowywania się metod narzucania DHCP w przypadku braku</b>	
<b>dostępności serwera zasad kondycji NAP</b> .....	885
<b>Klienci NAP</b> .....	885
<b>Wdrażanie metod narzucania DHCP</b> .....	887
<b>Konfigurowanie serwerów naprawczych</b> .....	887
<b>Konfigurowanie serwerów zasad kondycji NAP</b> .....	888
<b>Konfigurowanie klientów NAP</b> .....	893
<b>Konfigurowanie serwerów DHCP</b> .....	895
<b>Punkt kontrolny dla procesu wdrażania metod narzucania DHCP</b>	
<b>w trybie raportowania</b> .....	900
<b>Testowanie ograniczania dostępu do sieci</b> .....	901
<b>Konfigurowanie trybu odroczonego narzucania</b> .....	903
<b>Konfigurowanie zasady sieciowej do pracy w trybie narzucania</b> .....	903
<b>Bieżące zadania administracyjne</b> .....	905
<b>Dodawanie nowego klienta NAP</b> .....	905
<b>Dodawanie nowych agentów SHA oraz nowych modułów SHV</b> .....	905
<b>Rozwiązywanie problemów</b> .....	906
<b>Narzędzia służące do rozwiązywania problemów</b> .....	906
<b>Rozwiązywanie problemów związanych z metodami narzucania DHCP</b>	909
<b>Podsumowanie rozdziału</b> .....	912
<b>Informacje dodatkowe</b> .....	913
<b>Indeks</b> .....	931