

Spis treści

O autorze (17)

Rozdział 1. Wprowadzenie do architektury Microsoft Forefront Security (19)

- 1.1. Wstęp (19)
- 1.2. Bezpieczeństwo punktów styku z Internetem oraz innymi sieciami (20)
 - 1.2.1. Microsoft Internet Security and Acceleration (ISA) Server 2006 (20)
 - 1.2.2. Intelligent Application Gateway 2007 (22)
 - 1.2.3. Forefront Threat Management Gateway - MBE (wersja Medium Business Edition) (22)
 - 1.2.4. Forefront Threat Management Gateway 2010 (27)
- 1.3. Bezpieczeństwo stacji roboczych i serwerów ogólnego przeznaczenia (27)
 - 1.3.1. Microsoft Forefront Client Security (28)
- 1.4. Bezpieczeństwo serwerów specjalistycznych: Exchange, SharePoint oraz Office Communications Server 2007 (30)
 - 1.4.1. Forefront Security for Exchange Server 2007 (30)
 - 1.4.2. Forefront Security for SharePoint (33)
 - 1.4.3. Microsoft Forefront Security for Office Communications Server (35)
 - 1.4.4. Forefront Server Security Management Console (37)
- 1.5. Szkolenia i certyfikacje (39)

Rozdział 2. Infrastruktura klucza publicznego oraz mechanizmy automatycznej aktualizacji systemów i oprogramowania (41)

- 2.1. Wstęp (41)
- 2.2. Zagadnienia infrastruktury klucza publicznego (42)
 - 2.2.1. Kryptografia symetryczna (42)
 - 2.2.2. Kryptografia asymetryczna (42)
 - 2.2.3. Funkcje skrótu (43)
 - 2.2.4. Komponenty infrastruktury klucza publicznego (43)
 - 2.2.5. Jednostka certyfikująca (44)
 - 2.2.6. Hierarchia jednostek certyfikujących (44)
 - 2.2.7. Certyfikaty (47)
- 2.3. Wdrożenie 2-poziomowej hierarchii jednostek certyfikujących Standalone Root CA, Enterprise Subordinate (53)
 - 2.3.1. Plik CAPolicy.inf oraz Policy.inf (54)
 - 2.3.2. Identyfikatory OID (55)
 - 2.3.3. Manualna publikacja certyfikatu i listy CRL (57)
 - 2.3.4. Instalacja jednostki Standalone Root CA na Windows Server 2003 (59)
 - 2.3.5. Instalacja jednostki Enterprise Subordinate CA na Windows Server 2003 (68)
 - 2.3.6. Weryfikacja poprawności działania infrastruktury PKI przedsiębiorstwa (73)
 - 2.3.7. Instalacja jednostki Stand Alone Root CA w Windows Server 2008 (76)
 - 2.3.8. Instalacja jednostki Enterprise Subordinate w Windows Server 2008 (84)
- 2.4. WSUS - Windows System Update Services (91)
 - 2.4.1. Proces instalacji dla systemu Windows Server 2003 (91)
 - 2.4.2. Konsola zarządzania serwerem WSUS (99)
 - 2.4.3. Rekonfiguracja serwera WSUS (101)
 - 2.4.4. Raportowanie (110)
 - 2.4.5. Synchronizacja ze stroną Windows Update (110)

- 2.4.6. Serwery downstream (111)
- 2.4.7. Zarządzanie klientami serwera WSUS (111)
- 2.4.8. Zarządzanie klientami z wykorzystaniem polis domenowych (113)
- 2.4.9. Zarządzanie aktualizacjami (114)
- 2.4.10. Instalacja serwera WSUS w Windows Server 2008 (117)
- 2.4.11. Zestawienie ustawień polis dla funkcjonalności Windows Update (121)
- 2.5. Pobieranie aktualizacji offline (130)
- 2.6. Podsumowanie (132)

Rozdział 3. Bezpieczeństwo Windows Server 2003 oraz 2008 (133)

- 3.1. Wstęp (133)
- 3.2. Zagadnienia bezpieczeństwa Windows Server 2008 (133)
 - 3.2.1. Konfiguracja zabezpieczeń z poziomu Menedżera serwera (134)
 - 3.2.2. Konfiguracja zwiększonych zabezpieczeń programu Internet Explorer (134)
 - 3.2.3. Polisa lokalna i polisy domenowe (137)
- 3.3. Polisy w środowisku Windows 2008 oraz Vista (138)
 - 3.3.1. Zasady konta - Account Policies (139)
 - 3.3.2. Zasady haseł - Password Policy (140)
 - 3.3.3. Zasady blokady konta - Account Lockout Policy (142)
 - 3.3.4. Zasady protokołu Kerberos - Kerberos Policy (143)
 - 3.3.5. Zasady lokalne - Local Policies (145)
 - 3.3.6. Zasady inspekcji - Audit Policy (145)
 - 3.3.7. Opcje zabezpieczeń - Security Options (161)
- 3.4. Kreator konfiguracji zabezpieczeń - Security Configuration Wizard (200)
 - 3.4.1. Security Compliance Management Toolkit Series (212)
 - 3.4.2. Dodanie rozszerzeń do Kreatora konfiguracji zabezpieczeń (213)
- 3.5. Podsumowanie (213)

Rozdział 4. Instalacja i konfiguracja wstępna ISA Server 2006 wersja Standard Edition (215)

- 4.1. Wstęp (215)
 - 4.1.1. Nazewnictwo danych dla stosu TCP/IP (216)
 - 4.1.2. Nagłówek datagramu IPv4 (216)
 - 4.1.3. Pole Typ usługi - TOS (aktualnie DSCP) (217)
 - 4.1.4. Protokół UDP (ang. User Datagram Protocol) (218)
 - 4.1.5. Nagłówek protokołu UDP (219)
 - 4.1.6. Protokół TCP (ang. Transmission Control Protocol) (219)
 - 4.1.7. Nagłówek protokołu TCP (220)
- 4.2. Architektura serwera ISA 2006 (221)
 - 4.2.1. Reguły połączenia (ang. Connection Rules), elementy połączenia (ang. Connection Elements) i elementy tworzące (ang. Creation Elements) (224)
 - 4.2.2. Usługi działające na serwerze ISA 2006 Standard Edition (226)
- 4.3. Wersje produktu. Wymagania sprzętowe i systemowe (226)
 - 4.3.1. Szacowanie wstępne zapotrzebowania na moc obliczeniową procesora (procesorów) (227)
- 4.4. Licencjonowanie (228)
- 4.5. Porównanie różnic w stosunku do wersji poprzednich, czyli ISA 2000 i 2004 (228)
- 4.6. Proces instalacji wersji SE (229)
 - 4.6.1. ISA 2006 Service Pack 1 (234)
 - 4.6.2. Funkcjonalności oraz rozszerzenia udostępnione wraz z Service Pack 1 (235)
 - 4.6.3. Funkcjonalności rozszerzone w stosunku do wersji pierwotnej (235)

- 4.6.4. Weryfikacja poprawności instalacji i konfiguracji podstawowej. Narzędzie ISA Best Practices Analyzer Tool (236)
- 4.7. Hardening serwera (240)
 - 4.7.1. Zabezpieczanie interfejsów wewnętrznych (240)
 - 4.7.2. Zabezpieczanie interfejsu zewnętrznego (241)
 - 4.7.3. Wykorzystanie narzędzia Security Configuration Wizard (243)
- 4.8. Zaawansowane zagadnienia instalacyjne (245)
 - 4.8.1. Konfiguracja jednointerfejsowa (245)
 - 4.8.2. Instalacja nienadzorowana (246)
 - 4.8.3. Odinstalowywanie i modyfikacja zainstalowanych komponentów serwera ISA 2006 (247)
 - 4.8.4. Instalacja konsoli administracyjnej na innym serwerze lub stacji klienckiej (248)
 - 4.8.5. Logi instalacyjne serwera ISA 2006 (250)
 - 4.8.6. Delegowanie uprawnień administracyjnych dla wersji SE (250)
- 4.9. Podsumowanie (253)

Rozdział 5. ISA 2006 jako zaporę sieciową i serwer Proxy (255)

- 5.1. Wstęp (255)
- 5.2. Konsola do zarządzania - ISA Server Management Console (255)
 - 5.2.1. Gałąź Networks (258)
 - 5.2.2. Gałąź Cache (259)
 - 5.2.3. Gałąź Add-ins (259)
- 5.3. Gałąź General (260)
 - 5.3.1. Sekcja ISA Server Administration (261)
 - 5.3.2. Sekcja Global HTTP Policy Settings (267)
 - 5.3.3. Sekcja Additional Security Policy (269)
 - 5.3.4. Mechanizm Flood Mitigation (271)
- 5.4. Omówienie środowiska testowego wykorzystywanego przy omawianiu zagadnień konfiguracyjnych serwera ISA 2006 SE (275)
 - 5.4.1. Typy sieci (276)
 - 5.4.2. Właściwości sieci Internal (277)
 - 5.4.3. Właściwości sieci External (280)
 - 5.4.4. Obiekt sieciowy Local Host (281)
 - 5.4.5. Właściwości sieci VPN Clients (282)
 - 5.4.6. Właściwości sieci Quarantine VPN Clients (282)
 - 5.4.7. Obiekty sieciowe Network Sets (283)
 - 5.4.8. Network Rules - zasady sieciowe (284)
 - 5.4.9. Zakładka Web Chaining (287)
 - 5.4.10. Tworzenie nowej sieci (288)
 - 5.4.11. Automatyczna konfiguracja sieci - szablony sieciowe - Network Templates (291)
 - 5.4.12. Reguły dostępu - reguły zapory (297)
- 5.5. Gałąź Firewall Policy (298)
 - 5.5.1. Zakładka Tasks (299)
 - 5.5.2. Zakładka Toolbox (300)
 - 5.5.3. Protokoły sieciowe (Protocols) (312)
 - 5.5.4. Tworzenie reguły dostępu (Access Rule) (323)
- 5.6. Typy klientów ISA oraz sposób ich konfiguracji (329)
 - 5.6.1. Konfiguracja manualna klienta typu Web Proxy (329)

- 5.6.2. Włączenie funkcjonalności Web Proxy (334)
- 5.6.3. Automatyczna konfiguracja ustawień za pomocą Group Policy (335)
- 5.6.4. Funkcjonalność Autodiscovery (337)
- 5.6.5. Instalacja oprogramowania Firewall Client (340)
- 5.7. Polisy systemowe - podgląd i modyfikacja (346)
- 5.8. Podsumowanie (349)

Rozdział 6. Publikowanie zasobów za pomocą serwera ISA Server 2006 (351)

- 6.1. Wstęp (351)
- 6.2. Schemat oraz opis środowiska testowego wykorzystywanego przy omawianiu zagadnień publikacji serwerów (352)
- 6.3. Mechanizm Split-DNS (353)
 - 6.3.1. Konfiguracja serwera DNS domeny test.com na kontrolerze domeny DC (353)
 - 6.3.2. Konfiguracja serwera DNS domeny test.com na serwerze WEB-01 (354)
 - 6.3.3. Kreator publikacji serwera typu non-Web na przykładzie publikacji serwera DNS (354)
 - 6.3.4. Właściwości zaawansowane reguły publikacji serwera typu non-Web (357)
- 6.4. Zagadnienia funkcjonalności NAT (359)
 - 6.4.1. Access Rule (359)
 - 6.4.2. Publishing Rule (ustawienia domyślne) - Half-NAT (360)
 - 6.4.3. Publishing Rule w trybie Full-NAT (361)
- 6.5. Publikacja serwera FTP (361)
 - 6.5.1. Praca serwera FTP w trybie aktywnym i pasywnym (Active i Passive FTP) (362)
- 6.6. Publikowanie serwerów WWW - Web Publishing Rule (364)
 - 6.6.1. Funkcjonalności path mapping i link translation (364)
 - 6.6.2. Kreator publikacji serwera WWW (367)
 - 6.6.3. Listener (369)
 - 6.6.4. Publikacja wirtualnych serwerów WWW - przykład (376)
 - 6.6.5. Filtr aplikacyjny - HTTP (385)
- 6.7. Zabezpieczanie publikowanych serwerów WWW z wykorzystaniem protokołu HTTPS (certyfikaty SSL) (393)
 - 6.7.1. Funkcjonalność SSL Tunneling (393)
 - 6.7.2. Funkcjonalność SSL Bridging (394)
 - 6.7.3. Generowanie żądania certyfikatu oraz instalacja certyfikatu SSL na serwerze ISA (395)
 - 6.7.4. Kreator publikacji zabezpieczonego serwera WWW (400)
 - 6.7.5. Certyfikaty wieloznaczne oraz certyfikaty typu SAN (421)
 - 6.7.6. Status certyfikatów (424)
- 6.8. Mechanizmy uwierzytelniania - publikacja serwerów WWW wymagających uwierzytelniania (425)
 - 6.8.1. Uwierzytelnianie klient do serwera ISA (425)
 - 6.8.2. Uwierzytelnianie ISA do weryfikatora (425)
 - 6.8.3. Uwierzytelnianie metodą BASIC (427)
 - 6.8.4. Uwierzytelnianie Digest/Wdigest (429)
 - 6.8.5. Uwierzytelnianie Windows Integrated Authentication (431)
 - 6.8.6. Uwierzytelnianie oparte na formularzach (HTML Form-Based) (432)
 - 6.8.7. Uwierzytelnianie za pomocą certyfikatu na serwerze ISA 2006 (437)
- 6.9. Publikacja serwerów Windows SharePoint Services 3.0 oraz Microsoft Office SharePoint Server 2007 (441)

6.10. Podsumowanie (446)

Rozdział 7. Publikowanie zasobów serwera pocztowego Exchange 2003 za pomocą serwera ISA 2006 (447)

- 7.1. Wstęp (447)
- 7.2. Protokoły i porty wykorzystywane przez serwery Exchange 2003 (448)
- 7.3. Konfiguracja Exchange 2003 Front-End Back-End (448)
 - 7.3.1. Reguły zapory zapewniające komunikację pomiędzy serwerami Exchange oraz kontrolerami domeny (450)
 - 7.3.2. Zapewnienie wchodzącego i wychodzącego ruchu SMTP. Konfiguracja rekordów MX (451)
 - 7.3.3. Filtr aplikacyjny SMTP (451)
- 7.4. Kreator publikacji serwera pocztowego (452)
 - 7.4.1. Konfiguracja ruchu SMTP w obrębie organizacji Exchange 2003 pomiędzy serwerem Front-End a Back-End (455)
 - 7.4.2. Tworzenie konektora prowadzącego do i z Internetu (455)
 - 7.4.3. Konfiguracja rekordów MX dla przykładowej domeny test.com (459)
 - 7.4.4. Uwagi dotyczące konfiguracji wirtualnych serwerów SMTP na serwerach Exchange FE i BE (460)
- 7.5. Mechanizmy uwierzytelniania dla protokołu SMTP (463)
 - 7.5.1. Uwierzytelnianie AUTH PLAIN (463)
 - 7.5.2. Uwierzytelnianie AUTH LOGIN (463)
 - 7.5.3. Uwierzytelnianie NTLM (465)
 - 7.5.4. Mechanizm uwierzytelniania typu GSSAPI (466)
- 7.6. Szyfrowanie komunikacji typu serwer-serwer oraz klient-serwer (466)
 - 7.6.1. Włączenie szyfrowania po stronie serwera odbiorczego (469)
 - 7.6.2. Włączenie szyfrowania po stronie serwera nadawczego (469)
- 7.7. Komunikacja kliencka z serwerem pocztowym z wykorzystaniem protokołów SMTP/POP3/IMAP4/NNTP (471)
 - 7.7.1. Konfiguracja serwera do obsługi protokołów POP3, IMAP4, NNTP (471)
 - 7.7.2. Konfiguracja konta użytkownika od strony serwera Exchange (471)
 - 7.7.3. Kreator publikacji dostępu klienckiego dla protokołów SMTP, POP3, IMAP4 (473)
 - 7.7.4. Konfiguracja serwera POP3 (476)
 - 7.7.5. Konfiguracja serwera IMAP4 (480)
 - 7.7.6. Konfiguracja serwera NNTP (480)
- 7.8. Dostęp przez przeglądarkę internetową. Outlook Web Access - OWA (481)
 - 7.8.1. Reguła publikacji dostępu - Outlook Web Access (482)
 - 7.8.2. Uwierzytelnianie metodą Basic (486)
 - 7.8.3. Uwierzytelnianie metodą Form-Based na serwerze ISA 2006 (487)
 - 7.8.4. Uwierzytelnianie metodą Form-Based na serwerze Exchange 2003 (489)
 - 7.8.5. Przeznaczenie poszczególnych folderów wirtualnych serwera Exchange 2003 (489)
- 7.9. Konfiguracja IPsec - szyfrowanie ruchu pomiędzy serwerem Exchange Front-End a Back-End (492)
- 7.10. Mechanizm RPC over HTTPS (493)
 - 7.10.1. Rola komponentów DSAccess i DSProxy (494)
 - 7.10.2. Instalacja komponentu systemowego RPC over HTTP Proxy (496)
 - 7.10.3. Kreator publikacji dostępu RPC over HTTPS (498)

- 7.10.4. Zmiany w konfiguracji profilu Outlook związane z włączeniem komunikacji RPC-HTTP (500)
- 7.11. Publikacja dostępu OMA - Outlook Mobile Access (503)
- 7.12. Podsumowanie (506)

Rozdział 8. Współpraca organizacji Exchange 2007 SP1 (na serwerze Windows 2008) z serwerem ISA 2006 (507)

- 8.1. Wstęp (507)
- 8.2. Role serwerów w organizacji Exchange 2007 (507)
- 8.3. Zarządzanie rolami i funkcjonalnościami serwera Windows Server 2008 (509)
- 8.4. Konsola zarządzania - Exchange Management Console (509)
- 8.5. Konfiguracja serwerów wirtualnych IIS 7.0 (512)
- 8.6. Właściwości serwerów wirtualnych POP3 i IMAP4 (512)
 - 8.6.1. Konfiguracja serwera wirtualnego IMAP4 (516)
- 8.7. Zarządzanie metodą dostępu klienckiego (516)
- 8.8. Exchange 2007 - POP3 i certyfikaty SSL (517)
 - 8.8.1. Procedura generowania żądania i instalacji certyfikatu (518)
- 8.9. Dostęp przez OWA - Outlook Web Access (522)
 - 8.9.1. Kreator publikacji Exchange 2007 OWA (524)
- 8.10. Outlook Anywhere (530)
 - 8.10.1. Publikacja dostępu Outlook Anywhere (534)
 - 8.10.2. Rola Web Service'ów (535)
 - 8.10.3. Funkcjonalność AutoDiscover (535)
- 8.11. Rola konektorów (539)
 - 8.11.1. Konektory odbiorcze (540)
 - 8.11.2. Właściwości konektora odbierającego SMTP - Default (540)
 - 8.11.3. Właściwości konektora odbierającego SMTP - Client (541)
 - 8.11.4. Konektor wysyłający SMTP (543)
 - 8.11.5. Reguły zapory dla protokołu SMTP (547)
- 8.12. Exchange Active Sync (548)
 - 8.12.1. Exchange Active Sync w Exchange 2003 (548)
 - 8.12.2. Exchange Active Sync w Exchange 2007 (549)
- 8.13. Implementacja wysokiej dostępności - klastrowanie serwerów pełniących role Hub Transport i Client Access. Publikacja farmy serwerów (551)
 - 8.13.1. Omówienie środowiska testowego (552)
 - 8.13.2. Instalacja i konfiguracja klastra NLB w Windows Server 2008 (552)
 - 8.13.3. Publikacja farmy serwerów WWW (559)
 - 8.13.4. Problemy publikacji Outlook Anywhere przy rozkładaniu obciążenia metodą NLB (565)
- 8.14. Rola serwera Edge (566)
 - 8.14.1. Omówienie środowiska testowego (567)
 - 8.14.2. Sufiks domeny (568)
 - 8.14.3. Konsola zarządzania serwerem Edge (568)
 - 8.14.4. Implementacja serwera Edge Transport (568)
 - 8.14.5. Mechanizm Edge Synchronization. Wymuszanie synchronizacji (569)
 - 8.14.6. Rozwiązywanie nazw przez serwer Edge (569)
 - 8.14.7. Generowanie pliku konfiguracyjnego subskrypcji (569)
 - 8.14.8. Reguły zapory zapewniające komunikację pomiędzy serwerami Hub Transport a Edge dla celów subskrypcji (572)

8.14.9. Konektory zapewniające komunikację pomiędzy serwerami Hub Transport a Edge (573)

8.14.10. Reguły zapory zapewniające komunikację pomiędzy Internetem a serwerami Edge (574)

8.15. Podsumowanie (575)

Rozdział 9. Konfiguracja dostępu VPN za pomocą serwera ISA 2006 (577)

9.1. Wstęp (577)

9.2. Konfiguracja VPN Client Access (577)

9.2.1. Faza konfiguracyjna I (577)

9.2.2. Faza II - Enable VPN Client Access (580)

9.2.3. Konfiguracja stacji klienckiej do połączeń VPN na przykładzie Windows XP (583)

9.2.4. Schemat konfiguracji Client Access VPN (591)

9.3. Budowa protokołu PPTP (592)

9.3.1. Uwierzytelnianie protokołami EAP (593)

9.3.2. Uwierzytelnianie certyfikatem klienckim (595)

9.4. Połączenia VPN realizowane za pomocą protokołu L2TP (599)

9.4.1. L2TP/IPSec. Uwierzytelnianie komputera kluczem wspólnym (600)

9.4.2. Uwierzytelnianie użytkownika protokołami EAP (602)

9.4.3. Uwierzytelnianie komputera certyfikatem IPSec (603)

9.4.4. Monitorowanie stanu pracy protokołu IPSec (607)

9.5. Konfiguracja sieci VPN Remote Sites (sieci zdalne) (609)

9.5.1. Schemat przykładowej konfiguracji VPN Remote Sites (610)

9.5.2. Kreator konfiguracji połączenia z odległą lokalizacją (610)

9.5.3. Właściwości połączenia Site-to-Site VPN (613)

9.5.4. Właściwości usługi RRAS (616)

9.5.5. Połączenia Site-to-Site VPN realizowane w oparciu o protokół L2TP/IPSec (618)

9.5.6. Konfiguracja VPN Site-to-Site oparta na czystym protokole IPSec (619)

9.6. Podsumowanie (624)

Rozdział 10. ISA 2006 - wersja Enterprise Edition (625)

10.1. Wstęp (625)

10.2. Proces instalacji wersji Enterprise Edition (625)

10.3. Środowisko testowe dla ISA 2006 Enterprise Edition (627)

10.4. Instalacja serwera Configuration Storage Server (627)

10.4.1. Instalacja repliki serwera Configuration Storage Server (629)

10.5. Usługi uruchamiane na serwerach ISA EE (631)

10.6. Konsola zarządzania serwerem ISA 2006 EE (632)

10.6.1. Właściwości poszczególnych komponentów konsoli zarządzania (633)

10.6.2. Nadawanie ról administracyjnych na poziomie organizacji EE (633)

10.6.3. Ustawienia dodatkowe na poziomie organizacji EE (634)

10.7. Sieci korporacyjne - Enterprise Network (636)

10.7.1. Tworzenie nowej sieci klasy Enterprise (636)

10.7.2. Obiekty sieciowe - Enterprise Network Sets (638)

10.7.3. Reguły sieciowe o zasięgu korporacyjnym (638)

10.8. Polisy klasy Enterprise (638)

10.8.1. Właściwości polisy klasy Enterprise (640)

10.8.2. Dodawanie ról administracyjnych do danej polisy (640)

- 10.9. Zagadnienia dodatkowe związane z serwerem CSS (641)
- 10.10. Macierze - Arrays (643)
 - 10.10.1. Kreator tworzenia i konfiguracji macierzy (643)
 - 10.10.2. Właściwości zaawansowane macierzy (645)
 - 10.10.3. Nadawanie ról administracyjnych w obrębie macierzy (647)
 - 10.10.4. Instalacja serwerów ISA mających wchodzić w skład danej macierzy (648)
 - 10.10.5. Wybór metody uwierzytelniania w obrębie danej macierzy (649)
 - 10.10.6. Właściwości serwerów wchodzących w skład danej macierzy (651)
 - 10.10.7. Tworzenie sieci wchodzących w skład danej macierzy (653)
 - 10.10.8. Reguły sieciowe (Network Rules) na poziomie macierzy (653)
- 10.11. Włączenie funkcjonalności NLB w obrębie danej macierzy (655)
 - 10.11.1. Kreator konfiguracji funkcjonalności NLB (655)
 - 10.11.2. Modyfikacja ustawień sieci po konfiguracji funkcjonalności NLB (657)
 - 10.11.3. Zarządzanie funkcjonalnością NLB (657)
- 10.12. Porty i protokoły wykorzystywane przez komponenty infrastruktury organizacji ISA 2006 EE (660)
- 10.13. Konfiguracja macierzy Back-Array oraz Front-Array (660)
 - 10.13.1. Konfiguracja serwera ISA Front-End (661)
 - 10.13.2. Konfiguracja reguł zapory na macierzy Back-Array (661)
 - 10.13.3. Konfiguracja tabeli routingu na serwerach w macierzy Front-Array (663)
 - 10.13.4. Generowanie certyfikatu dla serwera CSS (663)
 - 10.13.5. Modyfikacja konfiguracji serwera CSS (664)
 - 10.13.6. Instalacja serwerów ISA wchodzących w skład macierzy Front Array (667)
 - 10.13.7. Uprawnienia do zarządzania serwerami wchodzącymi w skład macierzy Front-Array (668)
 - 10.13.8. Podsumowanie konfiguracji (670)
 - 10.13.9. Uwaga dotycząca protokołu HTTP (filtru aplikacyjnego Web Proxy) na macierzy Back-Array (670)
- 10.14. Publikacja i dostęp do zasobów strefy DMZ (672)
- 10.15. Zagadnienia dostępu uwierzytelnionego (672)
 - 10.15.1. Instalacja serwera RADIUS (672)
 - 10.15.2. Konsola zarządzania serwerem RADIUS (IAS) (673)
 - 10.15.3. Dodawanie klienta RADIUS (674)
 - 10.15.4. Konfiguracja serwera ISA jako klienta serwera RADIUS (675)
 - 10.15.5. Tworzenie nowej polityki zdalnego dostępu (676)
 - 10.15.6. Zmiana weryfikatora z Windows (Active Directory) na RADIUS (681)
 - 10.15.7. Uwierzytelnianie dostępu VPN - poprzez serwer RADIUS (681)
- 10.16. Podsumowanie (684)

Rozdział 11. ISA 2006 - zagadnienia dodatkowe (687)

- 11.1. Wstęp (687)
- 11.2. Przepływ poświadczeń (687)
- 11.3. Środowisko testowe - przykładowe metody przekazywania poświadczeń i ich wykorzystanie (690)
 - 11.3.1. Uwierzytelnienie w trybie Basic na docelowym serwerze WWW (691)
 - 11.3.2. Uwierzytelnianie typu Windows Integrated na serwerze WWW (693)
 - 11.3.3. Uwierzytelnianie Basic na serwerze ISA. Uwierzytelnianie metodą NTLM na serwerze WWW (695)

- 11.3.4. Uwierzytelnianie Basic na serwerze ISA. Uwierzytelnianie metodą Kerberos Constrained Delegation na serwerze WWW (696)
- 11.4. Kompresja protokołu HTTP (699)
- 11.5. Buforowanie treści dla protokołów HTTP, HTTPS oraz FTP (701)
 - 11.5.1. Tworzenie reguły buforowania (703)
- 11.6. Kształtowanie ruchu HTTP i zarządzanie nim (706)
 - 11.6.1. Kreator konfiguracji zarządzania ruchem HTTP (707)
- 11.7. Monitorowanie serwera i środowiska (710)
 - 11.7.1. Dashboard (710)
 - 11.7.2. Alerty (710)
 - 11.7.3. Sesje (717)
 - 11.7.4. Serwisy (719)
 - 11.7.5. Raporty (720)
 - 11.7.6. Connectivity Verifiers - weryfikator połączeń (729)
 - 11.7.7. Logging (732)
 - 11.7.8. Change Tracking (734)
- 11.8. Gałąź Troubleshooting (736)
 - 11.8.1. Gałąź Troubleshooting - zakładka Traffic Simulator (737)
 - 11.8.2. Gałąź Troubleshooting - zakładka Diagnostic Logging (739)
- 11.9. Archiwizacja i odtwarzanie (740)
 - 11.9.1. Kreator archiwizacji konfiguracji globalnej (740)
 - 11.9.2. Kreator odtwarzania konfiguracji globalnej (741)
 - 11.9.3. Archiwizacja i odtwarzanie na innych poziomach konfiguracji (743)
- 11.10. Microsoft Internet Security and Acceleration (ISA) Server 2006 Software Development Kit (SDK) (746)
- 11.11. Podsumowanie (746)

Rozdział 12. Mechanizmy antywirusowe i antyspamowe. Antigen for Exchange 2003 (747)

- 12.1. Wstęp (747)
- 12.2. Podejście historyczne (747)
- 12.3. Microsoft Antigen 9.0 SP1 for Exchange 2003 (748)
 - 12.3.1. Wymagania systemowe dla serwera i konsoli zarządzania Antigen (749)
 - 12.3.2. Proces instalacji oprogramowania Antigen for Exchange (749)
 - 12.3.3. Usługi instalowane z produktu Antigen 9.0 (754)
- 12.4. Antigen SPAM Manager (754)
 - 12.4.1. Wymagania sprzętowe dla serwera i konsoli zarządzania (754)
 - 12.4.2. Proces instalacji oprogramowania Antigen for SMTP oraz Antigen with SPAM Manager (755)
 - 12.4.3. Usługi instalowane z produktu Antigen 9.X. SPAM Manager (756)
- 12.5. Mechanizmy antyspamowe wbudowane w serwer Exchange 2003 SP2 (756)
 - 12.5.1. Poziomy działania mechanizmów antyspamowych (757)
 - 12.5.2. Kolejność przetwarzania odebranej wiadomości w środowisku Exchange 2003 (757)
 - 12.5.3. Włączanie funkcji antyspamowych na wirtualnym serwerze SMTP w Exchange 2003 SP2 (758)
 - 12.5.4. Opcje sender oraz recipient filtering (759)
 - 12.5.5. Opcja connection filtering (762)
 - 12.5.6. Mechanizm Sender ID Filtering (764)
 - 12.5.7. Mechanizm Intelligent Message Filtering (766)

- 12.6. Mechanizmy antyspamowe wbudowane w Exchange 2007 (769)
 - 12.6.1. Kolejność przetwarzania odebranej wiadomości w środowisku Exchange 2007 (770)
 - 12.6.2. Rola agentów transportowych (771)
 - 12.6.3. Instalacja agentów antyspamowych na serwerze pełniącym rolę Hub Transport (773)
 - 12.6.4. Opcje konfiguracyjne na poziomie serwera Hub Transport (774)
 - 12.6.5. Opcje konfiguracyjne na poziomie organizacji Exchange (776)
- 12.7. Podsumowanie (784)

Rozdział 13. Forefront Server Security for Exchange 2007 (787)

- 13.1. Wstęp (787)
- 13.2. Wymagania sprzętowe i systemowe (787)
- 13.3. Proces instalacyjny (788)
- 13.4. Licencjonowanie (792)
- 13.5. Usługi na serwerze FSE (793)
 - 13.5.1. Agenci transportowi (793)
 - 13.5.2. Rola poszczególnych serwisów (794)
- 13.6. Forefront - konsola zarządzania (795)
 - 13.6.1. Zakładka SETTINGS (795)
 - 13.6.2. Zakładka FILTERING (815)
 - 13.6.3. Zakładka REPORT (827)
 - 13.6.4. Narzędzia linii poleceń (837)
- 13.7. Klucze rejestru związane z konfiguracją FSE (841)
- 13.8. Klucze rejestru związane z uaktualnieniami silników antywirusowych FSE (845)
- 13.9. Lista typów plików (845)
- 13.10. Podsumowanie (845)

Rozdział 14. Forefront Security for SharePoint Server 2007 (847)

- 14.1. Wstęp (847)
- 14.2. Wymagania sprzętowe i systemowe (847)
- 14.3. Proces instalacyjny (848)
- 14.4. Licencjonowanie (852)
- 14.5. Usługi na serwerze FSSP (852)
- 14.6. Forefront - konsola zarządzania (852)
 - 14.6.1. Zakładka SETTINGS (852)
 - 14.6.2. Zakładka FILTERING (865)
 - 14.6.3. Zakładka OPERATE (868)
 - 14.6.4. Zakładka REPORT (869)
 - 14.6.5. Narzędzia linii poleceń (877)
- 14.7. Klucze rejestru związane z konfiguracją FSSP (880)
- 14.8. Klucze w rejestrze związane z uaktualnieniami silników antywirusowych FSSP (882)
- 14.9. Lista typów plików (883)
- 14.10. Podsumowanie (883)

Rozdział 15. Forefront Security for Office Communications Server 2007 (885)

- 15.1. Wstęp (885)
- 15.2. Wymagania sprzętowe i systemowe (885)
- 15.3. Proces instalacyjny (886)
- 15.4. Licencjonowanie (890)
- 15.5. Usługi na serwerze FSOCS (890)

- 15.6. Forefront - konsola zarządzania (891)
 - 15.6.1. Zakładka SETTINGS (891)
 - 15.6.2. Zakładka FILTERING (903)
 - 15.6.3. Zakładka OPERATE (907)
 - 15.6.4. Zakładka REPORT (907)
 - 15.6.5 Narzędzia linii poleceń (913)
- 15.7. Klucze rejestru związane z konfiguracją Forefront Security for Office Communications Server 2007 (917)
- 15.8. Klucze w rejestrze związane z uaktualnieniami silników antywirusowych FSOCS (920)
- 15.9. Listy typów plików (920)
- 15.10. Podsumowanie (920)

Rozdział 16. Forefront Server Security Management Console (921)

- 16.1. Wstęp (921)
- 16.2. Wspierane technologie (921)
- 16.3. Wymagania sprzętowe i systemowe (921)
- 16.4. Instalacja Forefront Security Console (922)
- 16.5. Instalowane narzędzia dodatkowe związane z obsługą FSSMC (924)
- 16.6. Konsola - widok ogólny (924)
- 16.7. Konfiguracja globalna (925)
 - 16.7.1. Zakładka SMTP Server (925)
 - 16.7.2. Zakładka Statistics Polling (926)
 - 16.7.3. Zakładka Download Configuration (926)
- 16.8. Zarządzanie użytkownikami (927)
 - 16.8.1. Proces dodawania użytkownika (927)
- 16.9. Serwery (928)
 - 16.9.1. Dodawanie nowych serwerów (928)
 - 16.9.2. Instalacja agenta zarządzania (930)
 - 16.9.3. Grupy serwerów (931)
- 16.10. Zarządzanie zadaniami - Job Management (935)
 - 16.10.1. Zadanie Signature Redistribution Jobs (935)
 - 16.10.2. Kopiowanie (duplikowanie zadania) (938)
 - 16.10.3. Kasowanie zadania (938)
 - 16.10.4. Uruchomienie zadania (938)
 - 16.10.5. Zadania operacyjne - Operations Job (939)
 - 16.10.6. Zadanie aktywacji serwerów Forefront lub Antigen (942)
 - 16.10.7. Zadanie modyfikacji ustawień generalnych produktów Forefront SP1 (Exchange lub SharePoint) (943)
 - 16.10.8. Manual Scan Jobs (944)
 - 16.10.9. Schedule Report Job (944)
 - 16.10.10. Remote Log Retrieval Job (946)
 - 16.10.11. Packages - zarządzanie instalacją pakietów oprogramowania (946)
- 16.11. Quarantine Manager (950)
- 16.12. Reports (950)
 - 16.12.1. Engine and Signature (951)
 - 16.12.2. Detection (952)
 - 16.12.3. SMTP Traffic (954)
 - 16.12.4. New Servers (954)
- 16.13. Auto Discovery dla serwerów Exchange (956)

- 16.13.1. Dodawanie wykrytego serwera Exchange do konsoli FSSMC (956)
- 16.14. Alerty (956)
 - 16.14.1. Konfigurowanie alertów: Virus, Spam, Filter oraz File Filter (na przykładzie Virus Alerts) (957)
 - 16.14.2. Konfiguracja - Signature Update Alerts (958)
- 16.15. Event Logs - Alert Logs (959)
 - 16.15.1. Czyszczenie wpisów w Alert Logs (959)
- 16.16. Event Logs - Notification Logs (960)
- 16.17. Wsparcie dla Cluster Continuous Replication (CCR) (961)
- 16.18. Redundancja środowiska zarządzania za pomocą FSSMC (961)
- 16.19. Podsumowanie (962)

Rozdział 17. Forefront Client Security (963)

- 17.1. Wstęp (963)
- 17.2. Architektura środowiska Forefront Client Security (964)
 - 17.2.1. Role serwerów środowiska FCS (964)
- 17.3. Topologie wdrożenia serwerów FCS (967)
 - 17.3.1. Wdrożenie w małych organizacjach (967)
 - 17.3.2. Wdrożenie w średnich i dużych organizacjach (970)
 - 17.3.3. Kolejność wdrażania poszczególnych ról serwerów FCS (974)
 - 17.3.4. Zgodność z systemami operacyjnymi - serwer FCS (974)
- 17.4. Procedura instalacyjna serwera Forefront Client Security (975)
 - 17.4.1. Instalacja topologii dwuserwerowej (976)
 - 17.4.2. Instalacja serwera dystrybucyjnego (981)
 - 17.4.3. Komponenty serwera FCS (983)
 - 17.4.4. Pierwsze uruchomienie konsoli zarządzania (985)
 - 17.4.5. Usługi działające na serwerach FCS (988)
 - 17.4.6. Rozwiązywanie problemów z instalacją serwera FCS. Logi instalacyjne (988)
- 17.5. Forefront Client Security - klient (989)
 - 17.5.1. Wymagania sprzętowe dla klienta (989)
 - 17.5.2. Zgodność i niezgodność z systemami operacyjnymi (990)
 - 17.5.3. Proces instalacji (990)
 - 17.5.4. Rozwiązywanie problemów z instalacją klienta FCS. Logi instalacyjne (991)
 - 17.5.5. Wymagania co do wdrożenia FCS w Active Directory (992)
 - 17.5.6. Wymagania Active Directory co do polityki FCS (992)
 - 17.5.7. Metody wdrożenia klienta (992)
- 17.6. Interfejs użytkownika (993)
 - 17.6.1. Konsola zarządzania klientem FCS. Opcja Scan (994)
 - 17.6.2. Konsola zarządzania klientem FCS. Opcja History (995)
 - 17.6.3. Konsola zarządzania klientem FCS. Opcja Tools (996)
 - 17.6.4. Skanowanie automatyczne (998)
 - 17.6.5. Akcja domyślna (998)
 - 17.6.6. Poziom alertowania (999)
 - 17.6.7. Nadpisywanie konfiguracji w oparciu o poziom zagrożenia (Severity) (1001)
 - 17.6.8. Nadpisywanie konfiguracji w oparciu o kategorię zagrożenia (1001)
 - 17.6.9. Nadpisywanie konfiguracji w oparciu o nazwę wykrytego oprogramowania typu malware (1002)
 - 17.6.10. Skanowanie w trybie Real-time (1003)
 - 17.6.11. Stan ikon sygnalizujących pracę klienta FCS (1005)

- 17.6.12. Zaawansowane opcje konfiguracyjne - wykluczenia (1005)
- 17.6.13. Opcje administratora (1006)
- 17.6.14. SpyNet community (1007)
- 17.6.15. Kwarantanna (1008)
- 17.6.16. Software Explorer (1008)
- 17.6.17. Allowed items (1010)
- 17.6.18. Wykrycie zagrożenia (1011)
- 17.6.19. Przeznaczenie plików wykonywalnych oraz bibliotek typu dll klienta FCS (1011)
- 17.6.20. Usługi działające po stronie klienta (1012)
- 17.7. FCS Enterprise Dashboard (1013)
 - 17.7.1. Polisa FCS (1016)
 - 17.7.2. Role administratorów (1016)
 - 17.7.3. Tworzenie polisy (1016)
 - 17.7.4. Wdrażanie polisy (1022)
 - 17.7.5. Wygląd polisy FCS w konsoli GPMC (1025)
- 17.8. Security State Assessment (1025)
 - 17.8.1. Konfiguracja ustawień SSA w polisie FCS (1026)
 - 17.8.2. Architektura SSA (1026)
 - 17.8.3. SSA Security Checks (1028)
- 17.9. Raportowanie i monitorowanie (1031)
 - 17.9.1. Architektura MOM Reporting (1031)
 - 17.9.2. Lista predefiniowanych raportów (1031)
- 17.10. Alerty (1034)
 - 17.10.1. FCS - poziomy alertów (1034)
 - 17.10.2. Przeglądanie alertów (1036)
 - 17.10.3. Funkcjonalność Automatic Alert Resolution (1037)
 - 17.10.4. Zagrożenia typu Flood (1037)
- 17.11. Podsumowanie (1038)

Rozdział 18. Forefront Threat Management Gateway Medium Business Edition (1039)

- 18.1. Wstęp (1039)
- 18.2. Wymagania sprzętowe i systemowe (1039)
- 18.3. Dodatkowe uwagi instalacyjne (1040)
- 18.4. Proces instalacji (1040)
- 18.5. Kreator konfiguracji (1042)
 - 18.5.1. Faza I (1043)
 - 18.5.2. Faza II (1046)
 - 18.5.3. Faza III (1047)
- 18.6. Konsola Forefront TMG (1049)
 - 18.6.1. Widok z poziomu Forefront TMG (1050)
- 18.7. Gałąź Firewall Policy (1055)
 - 18.7.1. Zakładka Tasks (1055)
 - 18.7.2. Konfiguracja dostępu klienckiego - Configure Client Access (1057)
- 18.8. Gałąź Web Access Policy (1060)
 - 18.8.1. Kreator ogólnej polisy dostępu do serwerów WWW - Configure Web Access Policy (1061)
 - 18.8.2. Konfiguracja wykrywania szkodliwego oprogramowania - Configure Malware Inspection (1063)

18.8.3. Konfiguracja serwera Web Proxy - Configure Web Proxy	(1067)
18.8.4. Konfiguracja buforowania - Configure Web Caching	(1067)
18.9. Gałąź Update Center	(1067)
18.9.1. Konfiguracja ustawień Update Center	(1068)
18.9.2. Pobieranie aktualizacji oraz licencjonowanie	(1069)
18.10. Gałąź Virtual Private Networking	(1069)
18.11. Usługi na serwerze Forefront TMG	(1071)
18.12. Narzędzie IsaMgmt.exe	(1071)
18.12.1. Lista wspieranych typów węzłów UI	(1072)
18.12.2. Lista wspieranych kreatorów	(1073)
18.12.3. Argumenty kreatora Web Access	(1073)
18.13. Podsumowanie	(1074)
Skorowidz	(1075)