

Współautorka i redaktor merytoryczny (17)

Autorzy i konsultanci (17)

Przedmowa (21)

Część I Wprowadzenie do firewalli i problemów bezpieczeństwa w sieci (23)

Rozdział 1. Wprowadzenie do problemów bezpieczeństwa informacji (25)

- Wprowadzenie (25)
- Konsekwencje braku systemu bezpieczeństwa w dobie internetu (26)
 - o Definiowanie bezpieczeństwa informacji (29)
 - o Podstawowe pojęcia związane z bezpieczeństwem (31)
 - o Wiedza to władza (32)
 - o Myśl jak złodziej (32)
 - o Blokowanie dróg, którymi można się włamać (33)
- Rodzaje zagrożeń i ataków na system (34)
 - o Fizyczne bezpieczeństwo (34)
 - o Bezpieczeństwo sieciowe (36)
 - o Motywacje włamywaczy (37)
 - o Podstawowe kategorie rozwiązań stosowanych w systemach bezpieczeństwa (40)
 - o Wracając do źródeł: standardowe porty TCP/UDP (40)
 - o Klasyfikacja różnych typów ataków (45)
- Polityki bezpieczeństwa (57)
 - o Zapobieganie celowym naruszeniom systemu bezpieczeństwa od wewnątrz (57)
 - o Ustalanie, kto powinien być odpowiedzialny za bezpieczeństwo sieci (58)
 - o Ustalanie odpowiedzialności za przygotowanie planu i polityk bezpieczeństwa (58)
 - o Projektowanie polityki bezpieczeństwa firmy (59)
 - o Określanie naszych potrzeb w zakresie bezpieczeństwa (65)
 - o Oficjalne klasyfikacje bezpieczeństwa (68)
 - o Cele, które należy uwzględnić w planie bezpieczeństwa (69)
- Tworzenie polityki bezpieczeństwa (70)
 - o Edukowanie użytkowników sieci w zakresie bezpieczeństwa (71)
- Ochrona infrastruktury systemu informatycznego (74)
 - o Poprawianie systemu bezpieczeństwa (74)
- Korzystanie z protokołu SSL i Secure Shell (76)
 - o Testowanie systemu bezpieczeństwa (77)
- Inne rozwiązania sprzętowe wykorzystywane w systemach bezpieczeństwa (79)
 - o Monitorowanie aktywności użytkowników w sieci (79)
 - o Zapobieganie atakom z zewnątrz oraz nieautoryzowanym wejściom do systemu z zewnętrznych sieci (81)
- Podsumowanie (82)

Rozdział 2. Podstawowe pojęcia związane z firewallami (83)

- Wprowadzenie (83)
- Definicja firewalla (83)
 - o Typy firewalli (85)
- Sieci i firewallle (87)
 - o Interfejsy firewalli: wewnętrzny, zewnętrzny i strefy DMZ (88)

- o Polityki firewalli (91)
 - o Tłumaczenie adresów (91)
 - o Wirtualne sieci prywatne (94)
- Popularne firewalle (96)
 - o Firewalle sprzętowe (98)
 - o Firewalle programowe (100)
- Podsumowanie (101)

Rozdział 3. Pojęcie, konstrukcja i zasady projektowania strefy DMZ (103)

- Wprowadzenie (103)
- Podstawy stref DMZ (104)
 - o Podstawowe przykłady stref DMZ (107)
 - o Pojęcia związane z przepływem danych (112)
 - o Sieci ze strefami DMZ a sieci bez nich (115)
- Podstawowe zasady projektowania stref zdemilitaryzowanych (116)
 - o Dlaczego faza projektowania jest tak ważna? (117)
 - o Projektowanie zabezpieczeń dla potrzeb bezpośredniej transmisji danych między hostami w sieci (120)
 - o Podstawowe informacje o przepływie danych w sieci i protokołach transmisji danych (121)
 - o Projektowanie ochrony w odpowiedzi na naturalne słabości protokołów TCP/IPv4 (122)
 - o Publiczne i prywatne adresy IP (123)
 - o Porty (123)
 - o Wykorzystanie firewalli do ochrony zasobów sieciowych (124)
 - o Przepływ danych a zagrożenia dla systemu bezpieczeństwa (127)
- Zagrożenia w szczególnych zastosowaniach stref DMZ (131)
 - o Połączenia z partnerami biznesowymi (131)
 - o Witryny WWW i FTP (132)
 - o Usługi e-mail (132)
- Zaawansowane strategie projektowania stref DMZ (133)
 - o Zaawansowane zagadnienia związane z projektowaniem stref DMZ (133)
 - o Dostępność strefy zdemilitaryzowanej i przejmowanie przez firewall funkcji innego firewalla (136)
- Podsumowanie (140)

Rozdział 4. Wprowadzenie do systemów wykrywania włamań (141)

- Wprowadzenie (141)
- Na czym polega wykrywanie włamań? (142)
 - o Sieciowe systemy IDS (144)
 - o Systemy IDS dla hostów (145)
 - o Rozproszone systemy IDS (146)
- Jak rozpoznać włamanie? (147)
- Dlaczego systemy wykrywania włamań są tak ważne? (148)
 - o Dlaczego atakujący interesują się właśnie mną? (149)
 - o Jak dopasować system IDS do naszego planu bezpieczeństwa? (149)
 - o Czy firewall nie może służyć jako system IDS? (150)
 - o Jak jeszcze można poszukiwać śladów włamań? (151)

- Co jeszcze można zrobić za pomocą systemów wykrywania włamań? (153)
 - o Monitorowanie dostępu do baz danych (153)
 - o Monitorowanie funkcji serwerów DNS (154)
 - o Ochrona serwerów poczty elektronicznej (154)
 - o Wykorzystywanie systemu IDS do monitorowania przestrzegania polityki bezpieczeństwa firmy (155)
- Podsumowanie (155)

Część II Firewallle systemów Linux i Solaris (157)

Rozdział 5. Firewallle iptables (159)

- Wprowadzenie (159)
- Potrzeba stosowania zapór sieciowych (160)
- Wybór komputera pełniącego rolę zapory sieciowej (161)
- Podstawy działania zapory iptables (162)
- Konfiguracja zapory iptables za pomocą tekstowej konsoli systemu Linux (164)
 - o Czyszczenie tablic i łańcuchów przetwarzania pakietów (164)
 - o Zerowanie liczników łańcuchów (165)
 - o Wyświetlanie listy reguł (166)
 - o Ustalanie domyślnej reguły przetwarzania pakietów (167)
 - o Tworzenie i niszczenie własnych łańcuchów przetwarzania pakietów (168)
 - o Modyfikowanie listy reguł przetwarzania pakietów (168)
- Opcje tworzące definicję reguły (169)
- Przykłady konfiguracji zapory iptables (169)
 - o Generalizowanie adresów IP i nazw interfejsów (169)
 - o Schemat filtrującej zapory sieciowej (171)
 - o Blokowanie wybranych adresów IP (171)
 - o Limitowanie ruchu ICMP (172)
 - o Udostępnianie połączenia internetowego (173)
 - o Przezroczyste pośrednictwo w połączeniu (174)
 - o Przekierowywanie portu do wnętrza sieci (176)
 - o Monitorowanie połączeń sieciowych (176)
- Zarządzanie zaporą iptables za pomocą graficznego interfejsu użytkownika (177)
- Podsumowanie (181)

Rozdział 6. Zarządzanie firewallami o otwartym kodzie źródłowym (183)

- Wprowadzenie (183)
- Testowanie firewalli (184)
 - o Fałszowanie adresów IP (185)
 - o Otwarte porty (uruchomione usługi) (185)
 - o Monitorowanie dysków twardych, pamięci RAM i pracy procesorów (186)
 - o Podejrzani użytkownicy, nietypowe dane uwierzytelniające i czas logowania (186)
 - o Weryfikacja bazy danych reguł (187)
 - o Sprawdzenie możliwości zestawiania połączeń (187)
 - o Skanowanie portów (188)
- Wykorzystanie aplikacji Telnet, Ipchains, Netcat i SendIP do badania firewalla (189)
 - o Ipchains (189)
 - o Telnet (189)

- o Netcat (190)
 - o SendIP - fałszerz pakietów (195)
- Dzienniki pracy oraz opcje blokowania ruchu i generowania komunikatów (198)
 - o Firewall Log Daemon (198)
 - o Program fwlogwatch (204)
 - o Automatyzacja pracy programu fwlogwatch (208)
 - o Wykorzystanie aplikacji fwlogwatch i skryptów CGI (215)
- Dodatkowe narzędzia analizy zdarzeń firewalla (220)
- Podsumowanie (222)

Rozdział 7. System Solaris jako bezpieczny router i firewall (223)

- Wprowadzenie (223)
- System Solaris jako bezpieczny router (224)
 - o Uzasadnienie wyboru systemu Solaris (224)
 - o Warunki uruchomienia funkcji routingu (225)
 - o Konfiguracja routingu (227)
 - o Zwiększanie poziomu zabezpieczeń (231)
 - o Wymogi bezpieczeństwa (231)
 - o Wyłączenie funkcji routingu (233)
- Routing pakietów protokołu IP wersji 6. (235)
 - o Pliki konfiguracyjne (235)
 - o Programy IPv6 (239)
 - o Procedura uruchomienia routera IPv6 (241)
 - o Wyłączenie funkcji routingu IPv6 (242)
- Stacje korzystające z protokołu IP w wersji 6. (244)
 - o Automatyczna konfiguracja (244)
 - o Ręczna konfiguracja (244)
 - o System Solaris jako bezpieczna brama (246)
- System Solaris jako firewall (246)
 - o Teoria firewalli (247)
 - o Ogólny projekt firewalla (248)
 - o SunScreen Lite (249)
 - o IP Filter (250)
 - o Wykorzystanie mechanizmu NAT (250)
- Podsumowanie (251)

Część III Firewalle PIX (253)

Rozdział 8. Wprowadzenie do firewalli PIX (255)

- Wstęp (255)
- Ogólna charakterystyka zapór PIX (256)
 - o Wbudowany system operacyjny (256)
 - o Algorytm ASA (257)
 - o Zaawansowana obsługa protokołów (266)
 - o Obsługa sieci VPN (266)
 - o Filtracja adresów URL (267)
 - o Translacja NAT i PAT (268)
 - o Ciągłość dostępu (269)
- Platformy sprzętowe PIX-a (270)

- o Modele (270)
 - o Port konsoli (274)
- Licencje i uaktualnianie oprogramowania (275)
 - o Licencje (276)
 - o Uaktualnianie oprogramowania (277)
 - o Resetowanie haseł (278)
- Korzystanie z wiersza poleceń (280)
 - o Konfiguracje domyślne (280)
 - o Tryby administracji (281)
 - o Podstawowe polecenia (283)
 - o Zarządzanie konfiguracjami (287)
 - o Restartowanie systemu (289)
- Podsumowanie (290)

Rozdział 9. Kontrola ruchu sieciowego (293)

- Wprowadzenie (293)
- Obsługa ruchu wychodzącego (293)
 - o Dynamiczna translacja adresów (294)
 - o Blokowanie ruchu wychodzącego (299)
- Obsługa ruchu przychodzącego (307)
 - o Statyczna translacja adresów (308)
 - o Listy dostępu (309)
 - o Ścieżki (309)
 - o Obsługa komunikatów ICMP (310)
 - o Przekierowywanie portów (310)
- Kompilowane listy dostępu - TurboACL (312)
- Grupowanie obiektów (312)
 - o Konfiguracja i wykorzystanie grup obiektów (313)
- Studium przypadku (316)
 - o Listy dostępu (318)
 - o Listy outbound i ścieżki (320)
- Podsumowanie (322)

Rozdział 10. Zaawansowane funkcje firewalli PIX (323)

- Wprowadzenie (323)
- Obsługa protokołów o wyższym stopniu złożoności (323)
 - o FTP (327)
 - o DNS (331)
 - o SMTP (333)
 - o HTTP (335)
 - o Polecenia "r" (335)
 - o RPC (336)
 - o RTSP, NetShow i VDO Live (338)
 - o SQL*Net (341)
 - o Protokoły VoIP (342)
 - o SCCP (344)
 - o SIP (345)
 - o ILS i LDAP (347)

- Filtrowanie ruchu sieci WWW (347)
 - o Filtrowanie adresów URL (348)
 - o Filtrowanie wykonywalnej zawartości stron WWW (353)
- Obsługa DHCP (355)
 - o Firewall PIX jako klient DHCP (356)
 - o Firewall PIX jako serwer DHCP (357)
- Inne zaawansowane funkcje (361)
 - o Kontrola fragmentacji - FragGuard (361)
 - o AAA Floodguard (363)
 - o SYN Floodguard (363)
 - o Sprawdzanie trasy odwrotnej (365)
 - o Routing w trybie unicast (367)
 - o Częściowy routing rozsyłania grupowego (371)
 - o PPPoE (376)
- Podsumowanie (378)

Rozdział 11. Rozwiązywanie problemów i monitorowanie wydajności (381)

- Wprowadzenie (381)
- Rozwiązywanie problemów ze sprzętem i okablowaniem (382)
 - o Rozwiązywanie problemów ze sprzętem (383)
 - o Rozwiązywanie problemów z okablowaniem (392)
- Rozwiązywanie problemów z komunikacją (395)
 - o Weryfikacja adresowania (396)
 - o Weryfikacja trasowania (397)
 - o Weryfikacja translacji adresów (402)
 - o Weryfikacja dostępu (405)
- Rozwiązywanie problemów z IPsec (409)
 - o ISAKMP (411)
 - o IPsec (414)
- Przechwytywanie ruchu sieciowego (417)
 - o Wyświetlanie wyników przechwytywania (418)
 - o Przesyłanie wyników przechwytywania (419)
- Monitorowanie i rozwiązywanie problemów z wydajnością (421)
 - o Monitorowanie wydajności procesora (422)
 - o Monitorowanie stanu pamięci (426)
 - o Monitorowanie wydajności sieci (428)
 - o Wydajność firewalla PIX a protokół ident (429)
- Podsumowanie (430)

Część IV Check Point NG i urządzenia Nokia IP Series (433)

Rozdział 12. Instalowanie i konfigurowanie firewalla VPN-1/FireWall-1 Next Generation (435)

- Wprowadzenie (435)
- Zanim rozpoczniesz (435)
 - o Uzyskiwanie licencji (437)
 - o Zabezpieczanie komputera (438)
 - o Konfigurowanie interfejsów sieciowych (440)
 - o Konfigurowanie DNS (442)

- o Przygotowanie do instalacji produktu VPN-1/FireWall-1 NG (442)
 - o Aktualizowanie wcześniejszej wersji (447)
- Instalowanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Windows (448)
 - o Instalowanie z płyty CD (449)
 - o Konfigurowanie produktu Check Point VPN-1/FireWall-1 NG w systemie Windows (458)
- Usuwanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Windows (471)
 - o Usuwanie produktu VPN-1 & FireWall-1 (471)
 - o Usuwanie pakietu SVN Foundation (473)
 - o Usuwanie klientów zarządzających (474)
- Instalowanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Solaris (475)
 - o Instalowanie z płyty CD (476)
 - o Konfigurowanie produktu Check Point VPN-1/FireWall-1 NG w systemie Solaris (481)
- Usuwanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Solaris (493)
 - o Usuwanie produktu VPN-1 & FireWall-1 (493)
 - o Usuwanie pakietu SVN Foundation (496)
 - o Usuwanie klientów zarządzających (497)
- Instalowanie produktu Check Point VPN-1 /FireWall-1 NG na platformie Nokia (498)
 - o Instalowanie pakietu VPN-1/FireWall-1 NG (499)
 - o Konfigurowanie produktu VPN-1/FireWall-1 NG na platformie Nokia (503)
- Podsumowanie (504)

Rozdział 13. Graficzny interfejs użytkownika (507)

- Wprowadzenie (507)
- Zarządzanie obiektami (507)
 - o Obiekty sieciowe (509)
 - o Usługi (522)
 - o Zasoby (527)
 - o Aplikacje OPSEC (528)
 - o Serwery (528)
 - o Użytkownicy wewnętrzni (531)
 - o Czas (532)
 - o Łącze wirtualne (533)
- Dodawanie reguł (534)
 - o Reguły (534)
- Właściwości globalne (537)
 - o Niejawne reguły FW-1 (537)
 - o Panel Security Server (539)
 - o Panel Authentication (539)
 - o Panel VPN-1 (539)
 - o Panel Desktop Security (540)
 - o Panel Visual Policy Editor (540)
 - o Panel Gateway High Availability (540)
 - o Panel Management High Availability (540)
 - o Panel Stateful Inspection (540)
 - o Panel LDAP Account Management (540)
 - o Panel Network Address Translation (540)

- o Panel ConnectControl (540)
 - o Panel Open Security Extension (541)
 - o Panel Log and Alert (541)
- Narzędzie SecureUpdate (541)
- Narzędzie Log Viewer (543)
 - o Wybór kolumn (545)
- Narzędzie System Status (545)
- Podsumowanie (546)

Rozdział 14. Tworzenie zasad bezpieczeństwa (549)

- Wprowadzenie (549)
- Przyczyny tworzenia polityki bezpieczeństwa (549)
- Sposób tworzenia polityki bezpieczeństwa (550)
 - o Projekt zabezpieczeń (552)
 - o Architektura firewalla (553)
 - o Tworzenie polityki (553)
- Wdrażanie polityki bezpieczeństwa (557)
 - o Zasady domyślne i wstępne (557)
 - o Przekształcanie polityki bezpieczeństwa do postaci reguł (558)
 - o Manipulowanie regułami (569)
 - o Opcje polityki (571)
- Instalowanie polityki bezpieczeństwa (573)
- Pliki polityki bezpieczeństwa (574)
- Podsumowanie (575)

Rozdział 15. Konfiguracje zaawansowane (577)

- Wprowadzenie (577)
- Moduł Check Point High Availability (CPHA) (578)
 - o Zapewnienie wysokiej dostępności (578)
 - o Przełączanie awaryjne (580)
 - o Synchronizacja firewalla (581)
- Konfiguracja z pojedynczym punktem wejściowym VPN (583)
 - o Konfigurowanie bramy (584)
 - o Konfigurowanie zasad polityki bezpieczeństwa (588)
- Konfiguracja z wieloma punktami wejściowymi VPN (589)
 - o Pokrywające domeny VPN (590)
 - o Konfigurowanie bramy (592)
 - o Pokrywanie domen VPN (593)
- Inne metody zapewniania wysokiej dostępności (596)
 - o Awaryjne przełączanie funkcji trasowania (596)
 - o Opcje sprzętowe (597)
- Podsumowanie (598)

Rozdział 16. Konfigurowanie prywatnych sieci wirtualnych (599)

- Wprowadzenie (599)
- Schematy szyfrowania (600)
 - o Algorytmy szyfrowania; kryptografia symetryczna i asymetryczna (600)

- o Metody wymiany kluczy - tunelowanie i szyfrowanie w miejscu (602)
 - o Funkcja skrótu i podpisy cyfrowe (603)
 - o Certyfikaty i ośrodki certyfikacji (604)
 - o Typy sieci VPN (604)
 - o Domeny VPN (604)
- Konfigurowanie sieci VPN z użyciem FWZ (605)
 - o Definiowanie obiektów (605)
 - o Dodawanie reguł VPN (607)
 - o Ograniczenia FWZ (608)
- Konfigurowanie sieci VPN z użyciem IKE (609)
 - o Definiowanie obiektów (609)
 - o Dodawanie reguł VPN (610)
 - o Testowanie sieci VPN (613)
 - o Uwagi dotyczące sieci zewnętrznych (616)
- Konfigurowanie sieci VPN z użyciem SecuRemote (616)
 - o Obiekt bramy lokalnej (616)
 - o Właściwości szyfrowania użytkownika (617)
 - o Reguły szyfrowania klienta (619)
- Instalowanie oprogramowania klienckiego SecuRemote (620)
- Użycie oprogramowania klienckiego SecuRemote (622)
 - o Dokonanie trwałych zmian w pliku objects_5_0.C (623)
 - o Funkcja Secure Domain Login (624)
- Podsumowanie (625)

Rozdział 17. Przegląd platformy Nokia Security Platform (627)

- Wprowadzenie (627)
- Przedstawienie urządzeń Nokia IP Series (628)
 - o Modele korporacyjne (628)
- Proste administrowanie systemem (635)
- Podsumowanie (638)

Rozdział 18. Konfigurowanie firewalla Check Point (639)

- Wprowadzenie (639)
- Przygotowanie do konfiguracji (639)
 - o Uzyskiwanie licencji (640)
 - o Konfigurowanie nazwy komputera (641)
 - o Opcje produktu FireWall-1 (641)
- Konfigurowanie firewalla (643)
 - o Instalowanie pakietów (644)
 - o Włączanie pakietów (645)
 - o Przekazywanie IP i polityki firewalla (647)
 - o Uruchomienie narzędzia cpconfig (650)
- Testowanie konfiguracji (659)
 - o Testowanie dostępu klientów GUI (660)
 - o Przesyłanie i pobieranie polityki (663)
- Aktualizowanie firewalla (667)
 - o Aktualizowanie z wersji 4.1 SP6 do wersji NG FP2 (668)
 - o Aktualizowanie z wersji NG FP2 do wersji NG FP3 (670)

- o Cofnięcie aktualizacji produktu 4.1 do wersji NG (671)
- Podsumowanie (671)

Rozdział 19. Przedstawienie interfejsu Voyager (673)

- Wprowadzenie (673)
- Podstawowa konfiguracja systemu (673)
 - o Ekran początkowy (674)
 - o Konfigurowanie podstawowych danych interfejsu sieciowego (676)
 - o Dodawanie bramy domyślnej (682)
 - o Konfigurowanie czasu, daty i strefy czasowej (684)
 - o Konfigurowanie DNS i wpisów komputerów (687)
 - o Konfigurowanie przekazywania poczty (690)
 - o Konfigurowanie powiadomień o zdarzeniach systemowych (691)
- Konfigurowanie systemu w zakresie bezpieczeństwa (691)
 - o Włączanie dostępu poprzez SSH (692)
 - o Wyłączenie dostępu poprzez Telnet (695)
 - o Alternatywa dla protokołu FTP (695)
 - o Zabezpieczanie protokołu FTP (696)
 - o Konfigurowanie protokołu SSL (698)
- Opcje konfiguracyjne (701)
 - o Interface Configuration (701)
 - o System Configuration (702)
 - o SNMP (703)
 - o IPv6 (703)
 - o Reboot, Shut Down System (703)
 - o Security and Access Configuration (703)
 - o Fault Management Configuration (704)
 - o Routing Configuration (704)
 - o Traffic Management (705)
 - o Router Services (706)
- Podsumowanie (707)

Rozdział 20. Administrowanie systemem w zakresie podstawowym (709)

- Wprowadzenie (709)
- Restartowanie systemu (709)
- Zarządzanie pakietami (711)
 - o Instalowanie pakietów (711)
 - o Włączanie i wyłączanie pakietów (715)
 - o Usuwanie pakietów (717)
- Zarządzanie obrazami IPSO (717)
 - o Aktualizacja do nowszej wersji obrazu IPSO (718)
 - o Usuwanie obrazów IPSO (721)
- Zarządzanie użytkownikami i grupami (721)
 - o Użytkownicy (722)
 - o Grupy (725)
- Konfigurowanie tras statycznych (727)
- Archiwizacja i odtwarzanie systemu (728)
 - o Zestawy konfiguracji (729)

- o Tworzenie kopii zapasowej (730)
 - o Odtwarzanie z kopii zapasowej (733)
- Protokołowanie (734)
 - o Protokołowanie lokalne (734)
 - o Protokołowanie zdalne (735)
 - o Dzienniki kontroli (736)
- Planowanie zadań cron (736)
- Podsumowanie (738)

Rozdział 21. Wysoka dostępność i klastry (741)

- Wprowadzenie (741)
- Projektowanie klastra (741)
 - o Dlaczego klastry? (741)
 - o Wysoka dostępność czy podział obciążenia? (742)
 - o Obsługa klastrów w produktach Check Point (743)
 - o Łączenie klastra z siecią - przełączniki czy koncentratory? (746)
 - o Funkcje FireWall-1, pojedyncze bramy i klastry - podobieństwa i różnice (747)
- Instalowanie produktu FireWall-1 NG FP3 (749)
 - o Sprawdzenie wymagań wstępnych instalacji (749)
 - o Opcje instalacji (750)
 - o Procedura instalacji (750)
- Check Point ClusterXL (754)
 - o Konfigurowanie produktu ClusterXL w trybie HA New mode (754)
 - o Testowanie produktu ClusterXL w trybie HA New mode (770)
 - o Sposób działania produktu ClusterXL w trybie HA New mode (774)
 - o Specjalne uwagi dla produktu ClusterXL w trybie HA New mode (780)
 - o Konfigurowanie produktu ClusterXL w trybie HA Legacy mode (783)
 - o Konfigurowanie produktu ClusterXL w trybie podziału obciążenia (784)
 - o Testowanie produktu ClusterXL w trybie podziału obciążenia (785)
 - o Sposób działania produktu ClusterXL w trybie podziału obciążenia (789)
 - o Specjalne uwagi dla produktu ClusterXL w trybie podziału obciążenia (792)
- Klastry w systemie Nokia IPSO (793)
 - o Konfigurowanie klastra Nokia (793)
 - o Konfiguracja produktu Check Point FireWall-1 dla klastra Nokia (795)
 - o Konfigurowanie klastra Nokia w interfejsie Voyager (800)
 - o Testowanie klastra Nokia (804)
 - o Sposób działania klastrów Nokia (810)
 - o Specjalne uwagi dla klastrów Nokia (814)
- Klastry VRRP w systemie Nokia IPSO (815)
 - o Konfigurowanie klastra Nokia VRRP (815)
 - o Konfigurowanie klastra Nokia VRRP w interfejsie Voyager (817)
 - o Testowanie klastra Nokia VRRP (822)
 - o Sposób działania klastrów VRRP (824)
 - o Specjalne uwagi dla klastrów Nokia VRRP (827)
 - o Rozwiązania klastrowe innych firm (827)
- Klastry i strojenie wydajności funkcji wysokiej dostępności (828)
 - o Przepustowość danych i duża liczba połączeń (828)
- Podsumowanie (836)

Część V Serwer ISA (839)

Rozdział 22. Planowanie i projektowanie wdrożenia serwera ISA (841)

- Wprowadzenie (841)
- Wdrożenie serwera ISA - zagadnienia dotyczące planowania i projektowania (841)
 - o Szacowanie wymagań sieciowych i sprzętowych (842)
 - o Wymagania systemowe (842)
 - o Wymagania programowe (843)
 - o Wymagania sprzętowe (843)
- Zastosowanie usługi Active Directory (853)
- Zagadnienia o krytycznym znaczeniu (854)
 - o Odporność na uszkodzenia dysków twardych (854)
- Planowanie właściwego trybu instalacji (863)
 - o Instalacja w trybie firewalla (864)
 - o Instalacja w trybie bufora (864)
 - o Instalacja w trybie zintegrowanym (865)
 - o Konfiguracja samodzielna a macierzowa (865)
 - o Planowanie konfiguracji klientów ISA (866)
 - o Łączność z internetem oraz zagadnienia związane z systemem DNS (871)
- Podsumowanie (874)

Rozdział 23. Instalacja programu ISA Server (875)

- Wprowadzenie (875)
- Organizacja planu instalacji (875)
 - o Pliki instalacyjne i uprawnienia (876)
 - o Klucz produktu oraz licencja produktu (876)
 - o Uwagi dotyczące Active Directory (877)
 - o Tryb serwera (877)
 - o Lokalizacja plików programu ISA Server na dysku (877)
 - o Identyfikatory występujące w sieci wewnętrznej a tabela adresów lokalnych (878)
 - o Instalacja dodatkowych funkcji programu ISA Server (878)
- Przebieg instalacji (879)
 - o Instalacja programu ISA Server - krok po kroku (879)
 - o Rozszerzenie serwera samodzielnego do elementu macierzy - krok po kroku (889)
 - o Zmiany wprowadzone na skutek instalacji programu ISA Server (897)
- Migracja z programu Microsoft Proxy Server 2.0 (898)
 - o Co podlega przeniesieniu, a co nie? (898)
 - o Uaktualnienie programu Proxy Server 2.0 na platformie Windows 2000 (903)
 - o Uaktualnienie programu Proxy Server 2.0 na platformie Windows NT (906)
- Podsumowanie (908)

Rozdział 24. Administrowanie serwerem ISA (911)

- Wprowadzenie (911)
- Koncepcja administracji zintegrowanej (911)
 - o Konsola ISA Management (912)
 - o Kreatory ISA (935)

- Wykonywanie typowych zadań administracyjnych (936)
 - o Konfiguracja uprawnień do obiektów (937)
 - o Administrowanie macierzą (939)
- Korzystanie z funkcji monitorowania, alarmowania, rejestracji oraz raportowania (941)
 - o Tworzenie, konfiguracja i monitorowanie alarmów (941)
 - o Sesje monitorowania (946)
 - o Korzystanie z rejestracji (948)
 - o Generowanie raportów (953)
- Koncepcja administracji zdalnej (964)
 - o Instalacja konsoli ISA Management (964)
 - o Zdalne administrowanie serwerem ISA z wykorzystaniem usług Terminal Services (966)
- Podsumowanie (971)

Rozdział 25. Optymalizacja, dostosowywanie, integracja oraz tworzenie kopii bezpieczeństwa serwera ISA (973)

- Wprowadzenie (973)
- Optymalizacja wydajności serwera ISA (973)
 - o Ustalanie linii odniesienia i monitorowanie wydajności (975)
 - o Postępowanie z typowymi problemami z wydajnością (997)
- Dostosowywanie programu ISA Server do własnych potrzeb (1008)
 - o Korzystanie z pakietu ISA Server SDK (1009)
 - o Korzystanie z dodatków niezależnych firm (1012)
- Integracja programu ISA Server z innymi usługami (1014)
 - o Współpraca z Active Directory (1014)
 - o Współpraca z usługami Routing and Remote Access (1016)
 - o Współpraca z usługą IIS (1017)
 - o Współpraca z protokołem IPSecurity (1018)
 - o Integracja programu ISA Server z domeną Windows NT 4.0 (1021)
- Tworzenie kopii zapasowych i przywracanie konfiguracji serwera ISA (1021)
 - o Zasady tworzenia kopii zapasowych (1022)
 - o Tworzenie kopii zapasowej i przywracanie konfiguracji serwerów samodzielnych (1022)
 - o Tworzenie kopii zapasowej i przywracanie konfiguracji macierzy i przedsiębiorstwa (1024)
- Podsumowanie (1026)

Rozdział 26. Rozwiązywanie problemów z serwerem ISA (1027)

- Wprowadzenie (1027)
- Wskazówki dotyczące rozwiązywania problemów (1027)
 - o Pięć kroków rozwiązywania problemu (1028)
- Rozwiązywanie problemów z instalacją i konfiguracją programu ISA Server (1040)
 - o Problemy ze zgodnością sprzętową i programową (1040)
 - o Problemy związane z konfiguracją początkową (1041)
- Rozwiązywanie problemów z uwierzytelnianiem i dostępem (1044)
 - o Problemy z uwierzytelnianiem (1044)
 - o Problemy z dostępem (1047)

- o Problemy z połączeniami komutowanymi i połączeniami typu VPN (1049)
- Rozwiązywanie problemów klientów serwera ISA (1051)
 - o Problemy wydajnościowe klientów (1051)
 - o Problemy klientów z połączeniami (1052)
- Rozwiązywanie problemów z buforowaniem i udostępnianiem (1055)
 - o Problemy z buforowaniem (1055)
 - o Problemy z udostępnianiem (1056)
- Podsumowanie (1058)

Rozdział 27. Zaawansowane udostępnianie serwerów przy użyciu serwera ISA (1061)

- Wprowadzenie (1061)
- Wyłączanie mechanizmu puli gniazd (1065)
 - o Wyłączanie puli gniazd usług WWW oraz FTP (1066)
 - o Wyłączanie puli gniazd usług SMTP oraz NNTP (1068)
 - o Wyłączanie usług IIS na serwerze ISA (1069)
- Udostępnianie serwera (1070)
 - o Udostępnianie usług terminalowych działających w sieci wewnętrznej (1070)
 - o Udostępnianie usług terminalowych na serwerze ISA (1075)
 - o Jednoczesne udostępnianie usług terminalowych na serwerze ISA oraz w sieci wewnętrznej (1078)
 - o Udostępnianie witryn TSAC (1079)
 - o Udostępnianie serwerów FTP znajdujących się w sieci wewnętrznej (1089)
 - o Udostępnianie serwerów FTP umieszczonych na serwerze ISA (1100)
 - o Zastosowanie reguł udostępniania treści WWW w celu umożliwienia bezpiecznego dostępu FTP (1108)
 - o Udostępnianie serwerów HTTP oraz HTTPS (SSL) przy użyciu reguł udostępniania serwerów (1113)
 - o Udostępnianie hosta pcAnywhere umieszczonego w sieci wewnętrznej (1117)
- Publikacja treści WWW (1120)
 - o Moduły nasłuchujące Incoming Web Requests (1121)
 - o Zestawy miejsc docelowych (1122)
 - o Wpisy w publicznym systemie DNS (1123)
 - o Wpisy w prywatnym systemie DNS (1123)
 - o Zakończenie połączenia SSL na serwerze ISA (1125)
 - o Mostkowanie połączeń SSL (1142)
 - o Bezpieczne połączenia FTP wykorzystujące protokół SSL (1151)
 - o Udostępnianie serwera certyfikatów (1153)
- Podsumowanie (1156)

Rozdział 28. Ochrona usług pocztowych przy użyciu serwera ISA (1157)

- Wprowadzenie (1157)
- Konfiguracja usług pocztowych na serwerze ISA (1158)
 - o Udostępnianie usługi IIS SMTP na serwerze ISA (1159)
 - o Program Message Screener na serwerze ISA (1166)
 - o Udostępnianie serwera Exchange na serwerze ISA (1170)
 - o Udostępnianie usługi Outlook Web Access na serwerze ISA (1197)
 - o Program Message Screener na serwerze ISA oraz Exchange (1207)
- Konfiguracja usług pocztowych w sieci wewnętrznej (1213)

- o Udostępnianie serwera Exchange umieszczonego w sieci wewnętrznej (1214)
 - o Udostępnianie usługi RPC serwera Exchange (1216)
 - o Udostępnianie witryny Outlook Web Access uruchomionej na wewnętrznym serwerze Exchange (1223)
 - o Program Message Screener na wewnętrznym serwerze Exchange (1225)
- Oprogramowanie MailSecurity oraz MailEssentials firmy GFI przeznaczone dla serwerów SMTP (1228)
 - o Wersje programu MailSecurity (1230)
 - o Instalacja programu MailSecurity dla bram SMTP (1230)
 - o Konfiguracja programu MailSecurity (1233)
- Podsumowanie (1239)

Część VI Wykrywanie włamań (1241)

Rozdział 29. Snort - wprowadzenie (1243)

- Wprowadzenie (1243)
- Do czego służy aplikacja Snort? (1244)
- Wymagania systemowe aplikacji Snort (1246)
 - o Wymagania sprzętowe (1246)
- Funkcje aplikacji Snort (1248)
 - o Monitor pakietów (1249)
 - o Preprocesor (1249)
 - o Mechanizm detekcji włamań (1250)
 - o Moduł rejestracji danych i generowania komunikatów alarmowych (1251)
- Wykorzystanie aplikacji Snort w sieci (1252)
 - o Zastosowanie aplikacji Snort (1254)
 - o Program Snort a architektura sieci (1259)
 - o Wady programu Snort (1262)
- Bezpieczeństwo aplikacji Snort (1264)
 - o Snort jest aplikacją podatną na ataki (1264)
 - o Zabezpieczanie systemu Snort (1265)
- Podsumowanie (1266)

Rozdział 30. Instalacja programu Snort (1267)

- Wprowadzenie (1267)
- Krótki opis dystrybucji systemu Linux (1268)
 - o Debian (1268)
 - o Slackware (1268)
 - o Gentoo (1269)
- Instalacja biblioteki PCAP (1270)
 - o Instalacja biblioteki libcap z plików źródłowych (1271)
 - o Instalacja biblioteki libcap z pakietu RPM (1274)
- Instalacja programu Snort (1275)
 - o Instalacja programu Snort z plików źródłowych (1275)
 - o Konfigurowanie aplikacji Snort - edycja pliku snort.conf (1276)
 - o Instalacja pakietu RPM programu Snort (1279)
 - o Instalacja programu Snort w systemie Windows (1281)
 - o Instalacja najnowszych wersji programu Snort (1284)
- Podsumowanie (1284)

Rozdział 31. Łączenie firewalli i systemów IDS (1287)

- Wprowadzenie (1287)
- Systemy IDS o określonej polityce działania (1287)
 - o Definiowanie polityki działania systemów IDS (1289)
 - o Przykład konfiguracji systemu (1293)
 - o Wdrażanie systemów IDS o określonej polityce działania (1297)
- Aktywne systemy IDS (1300)
 - o Powstanie aktywnego systemu IDS w projekcie Snort (1301)
 - o Instalacja programu Snort w trybie aktywnym (1301)
 - o Wykorzystanie aktywnego systemu IDS do ochrony sieci (1313)
- Funkcje IDS w firewallu PIX (1316)
 - o Sygnatury (1316)
 - o Konfigurowanie pracy firewalli PIX z systemami IDS (1319)
 - o Konfiguracja wykluczeń (1322)
- Podsumowanie (1323)

Dodatki (1325)

Skorowidz (1327)