Wprowadzenie 17

Rozdział 1. Bezpieczeństwo sieci 27
- Słabe punkty **27**
- Typy ataków **28**
  - Ataki rozpoznawcze **29**
  - Ataki dostępu **29**
  - Ataki odmowy usług (DoS) **30**
- Reguły bezpieczeństwa sieci **31**
  - Etap 1. Zabezpiecz **32**
  - Etap 2. Monitoruj **32**
  - Etap 3. Przetestuj **33**
  - Etap 4. Ulepszaj **33**
- AVVID i SAFE **33**
  - Co to jest AVVID? **33**
  - Co to jest SAFE? **34**
- Pytania kontrolne **35**

Rozdział 2. Technologie ścian ogniowych i ściany ogniowe Cisco PIX 37
- Korzystanie z informacji zawartych w tym rozdziale **37**
- Sprawdzian „Czy już to wiem?” **37**
- Zagadnienia podstawowe **38**
- Technologie ścian ogniowych **38**
  - Filtrowanie pakietów **38**
  - Proxy **39**
  - Inspekcja stanu **40**
- Ściana ogniowa Cisco PIX **40**
  - Zabezpieczenia systemu czasu rzeczywistego **40**
  - Algorytm ASA **41**
  - Proxy z przycinaniem **41**
  - Nadmiarowość **41**
- Podsumowanie **41**
- Pytania kontrolne **42**

Rozdział 3. Bezpieczna ściana ogniowa Cisco PIX 43
- Korzystanie z informacji zawartych w tym rozdziale **43**
- Sprawdzian „Czy już to wiem?” **43**
- Zagadnienia podstawowe **44**
- Przegląd ścian ogniowych Cisco PIX **44**
  - Adaptacyjny algorytm bezpieczeństwa ASA **44**
  - Proxy z przycinaniem **46**
- Modele ścian ogniowych PIX i ich cechy **47**
  - Ochrona przed intruzami **47**
  - Wykorzystanie AAA **48**
  - Obsługa certyfikatu X.509 **48**
  - Translacja adresów sieciowych i adresów portów **48**
  - Zarządzanie ścianą ogniową **49**
  - Simple Network Management Protocol (SNMP) **49**
  - Współpraca z Syslog **49**
  - Wirtualne sieci prywatne (VPN) **50**
  - Cisco Secure PIX 501 **50**
  - Cisco Secure PIX 506 **51**
  - Cisco Secure PIX 515 **52**
  - Cisco Secure PIX 520 **54**
  - Cisco Secure PIX 525 **57**
  - Cisco Secure PIX 535 **59**
- Podsumowanie **61**
- Pytania kontrolne **62**

Rozdział 4. Obsługa systemu 65
Korzystanie z informacji zawartych w tym rozdziale **65**
Sprawdzian „Czy już to wiem?” **65**
Zagadnienia podstawowe 66
Dostęp do ściany ogniowej Cisco PIX **66**
Dostęp do ściany ogniowej Cisco PIX poprzez Telnet **66**
Dostęp do ściany ogniowej Cisco PIX za pomocą protokołu SSH (Secure Shell) **67**
Instalacja nowego systemu operacyjnego **68**
Uaktualnianie klucza aktywacyjnego **70**
Uaktualnianie systemu operacyjnego Cisco PIX **72**
Uaktualnianie systemu operacyjnego poleceniem copy tftp flash **72**
Uaktualnianie systemu operacyjnego w trybie monitora **73**
Uaktualnianie systemu operacyjnego za pomocą klienta HTTP **75**
Tworzenie dyskietki pomocniczej na komputerze PC z systemem Windows **75**
Obsługa funkcji Auto Update **77**
Odzyskiwanie hasła **77**
Odzyskiwanie hasła – wstęp **78**
Odzyskiwanie hasła do ściany ogniowej PIX ze stacją dyskietek (PIX 520) **78**
Odzyskiwanie hasła do ściany ogniowej PIX bez stacji dyskietek (PIX 501, 506, 515, 525 i 535) **79**
Podsumowanie **80**
Pytania kontrolne **80**

Rozdział 5. Połączenia i translacje w ścianach Cisco PIX 83
Korzystanie z informacji zawartych w tym rozdziale **83**
Sprawdzian „Czy już to wiem?” **83**
Zagadnienia podstawowe **84**
Jak ściana ogniowa PIX obsługuje ruch sieciowy **84**
Poziomy bezpieczeństwa interfejsów i domyślne reguły bezpieczeństwa **84**
Protokoły transportowe **85**
Translacja adresów **89**
Polecenia translacji **90**
Translacja adresów sieciowych (NAT) **91**
Translacja adresów portów (PAT) **92**
Translacja statyczna **93**
Zastosowanie polecenia static do przekierowania portów **94**
Konfigurowanie wielu typów translacji w ścianie ogniowej Cisco PIX **95**
Dwukierunkowa translacja adresów sieciowych **97**
Translacje a połączenia **97**
Konfiguracja obsługi DNS **100**
Podsumowanie **100**
Pytania kontrolne **103**

Rozdział 6. Zaczynamy pracę ze ścianą ogniową Cisco PIX 105
Sprawdzian „Czy już to wiem?” **105**
Zagadnienia podstawowe **106**
Tryby dostępu **106**
Konfiguracja ściany ogniowej PIX **107**
Polecenie interface **108**
Polecenie nameif **109**
Polecenie ip address **109**
Polecenie nat **110**
Polecenie global **111**
Polecenie route **112**
RIP **113**
Testowanie konfiguracji **114**
Zapisywanie konfiguracji **114**
Konfigurowanie DHCP w ścianie ogniowej Cisco PIX **115**
Użycie serwera DHCP w ścianie PIX **115**
Konfiguracja klienta DHCP na ścianie ogniowej Cisco PIX **116**
Konfigurowanie ustawienia czasu na ścianie ogniowej Cisco PIX **117**
Protokół czasu (NTP) **117**

Zegar systemowy ściany ogniowej PIX **119**
Przykładowa konfiguracja PIX **120**
Podsumowanie **122**
Pytania i odpowiedzi **122**

Rozdział 7. Konfigurowanie dostępu 125
Sprawdzian „Czy już to wiem?” **125**
Zagadnienia podstawowe **126**
Konfigurowanie dostępu wewnętrznego przez ścianę ogniową PIX **126**
Statyczna translacja adresów sieciowych **126**
Statyczna translacja adresów portu **128**
Funkcja przechwytywania TCP **129**
Polecenie nat 0 **129**
Listy dostępu **130**
TurboACL **133**
Konfigurowanie indywidualnego TurboACL **133**
Globalne konfigurowanie TurboACL **134**
Grupowanie obiektów **134**
network typ_obiektu **134**
protocol typ-obiektu **136**
service typ-obiektu **136**
icmp-type typ-obiektu **136**
Zagnieżdżanie grup obiektów **137**
Użycie polecenia fixup **137**
Zaawansowana obsługa protokołów **139**
Protokół transferu plików (FTP) **139**
Obsługa multimediów **140**
Podsumowanie **140**
Pytania kontrolne **141**

Rozdział 8. Syslog 143
Sprawdzian „Czy już to wiem?” **143**
Podstawowe zagadnienia **144**
Jak działa syslog **144**
Urządzenia zapisu dziennika **145**
Poziomy dziennika **146**
Konfigurowanie syslog na ścianie ogniowej Cisco PIX **146**
Konfigurowanie menedżera urządzeń PIX do przeglądania dziennika **147**
Konfigurowanie komunikatów syslog na konsoli **148**
Przeglądanie komunikatów w sesji konsoli Telnet **149**
Konfigurowanie wysyłania komunikatów syslog na serwer dziennika **149**
Konfigurowanie serwera syslogd **150**
PIX Firewall Syslog Server (PFSS) **151**
Konfigurowanie pułapek SNMP i żądań SNMP **151**
Organizacja komunikatów zapisu dziennika **152**
Jak czytać komunikaty System Log **152**
Wyłączanie komunikatów syslog **153**
Podsumowanie **153**
Pytania kontrolne **154**

Rozdział 9. Funkcja failover na ścianie Cisco PIX 157
Sprawdzian „Czy już to wiem?” **157**
Zagadnienia podstawowe **158**
Co jest przyczyną zdarzenia failover? **158**
Wymagania konfiguracji failover **159**
Monitorowanie failover **159**
Replikacja konfiguracji **161**
Tryb stateful failover **161**
Failover oparte na LAN **162**
Konfiguracja failover **163**
Podsumowanie **168**
Pytania kontrolne **169**

Rozdział 10. Wirtualne sieci prywatne - VPN 173
Korzystanie z informacji zawartych w tym rozdziale **173**
Sprawdzian „Czy już to wiem?" **174**
Przegląd technologii VPN **174**
Bezpieczeństwo IP (IPSec) **175**
Internetowa wymiana kluczy (IKE) **178**
Instytucje certyfikacyjne (CA) **180**
Konfigurowanie ściany ogniowej PIX jako bramki VPN **181**
Wybieranie konfiguracji **181**
Konfigurowanie IKE **182**
Konfigurowanie IPSec **186**
Usuwanie błędów z połączenia VPN **194**
Klient Cisco VPN **199**
Grupy VPN **200**
Protokoły tunelowania PPTP i L2PT **200**
Konfigurowanie ściany PIX dla skalowalnych VPN **202**
Obsługa PPPoE **203**
Podsumowanie **203**
Pytania kontrolne **204**
Scenariusz **205**
Konfiguracja VPN **205**
Konfiguracja Los Angeles **212**
Konfiguracja Bostonu **213**
Konfiguracja w Atlancie **213**
Kompletne konfiguracje PIX **214**
Jak oddziałują na siebie wiersze konfiguracji **220**

Rozdział 11. PIX Device Manager 223
Sprawdzian „Czy już to wiem?" **223**
Zagadnienia podstawowe **224**
Przegląd PDM **224**
Warunki uruchomienia PDM w PIX Firewall **226**
Wymagania systemowe PDM **227**
Wymagania dotyczące przeglądarki **227**
Wymagania dotyczące Windows NT/2000 **227**
Wymagania dotyczące systemu Sun Solaris **227**
Wymagania dotyczące systemu Linux **228**
Instalacja i konfiguracja PDM **228**
Wykorzystanie PDM do konfiguracji PIX **229**
Korzystanie z PDM przy konfiguracji VPN **240**
Wykorzystanie PDM do kreowania międzylokalizacyjnego VPN **240**
Użycie PDM do kreowania VPN o zdalnym dostępie **244**
Podsumowanie **252**
Pytania i odpowiedzi **253**

Rozdział 12. Filtrowanie zawartości za pomocą ściany Cisco PIX 257
Sprawdzian „Czy już to wiem?" **257**
Filtrowanie apletów Javy **258**
Filtrowanie obiektów ActiveX **260**
Filtrowanie adresów URL **260**
Identyfikowanie serwera filtrowania **260**
Konfigurowanie reguł filtrowania **261**
Filtrowanie długich adresów URL **263**
Przeglądanie statystyk filtrowania i konfiguracji **263**
Podsumowanie **265**
Pytania kontrolne **265**

Rozdział 13. Przegląd AAA i Cisco PIX Firewall 269
Jak najlepiej wykorzystać ten rozdział **269**
Sprawdzian „Czy już to wiem?" **270**
Zagadnienia podstawowe **270**
Przegląd AAA i Cisco PIX Firewall **270**

Definicja AAA **271**
AAA i Cisco PIX Firewall **271**
Proxy z przycinaniem **272**
Obsługiwane typy serwerów AAA **273**
Cisco Secure Access Control Server (CSACS) **274**
Minimalne wymagania CSACS ľ sprzętowe oraz dotyczące systemu operacyjnego **274**
Instalacja CSACS w środowisku Windows 2000/NT Server **275**
Podsumowanie **281**
Pytania kontrolne **281**

Rozdział 14. Konfiguracja AAA w jednostce PIX 283
Korzystanie z informacji zawartych w tym rozdziale **283**
Sprawdzian „Czy już to wiem?" **284**
Zagadnienia podstawowe **285**
Definiowanie serwerów AAA **285**
Konfiguracja AAA na ścianie ogniowej PIX **286**
Etap 1. Identyfikacja serwera AAA i sieciowego serwera dostępowego **286**
Etap 2. Konfigurowanie uwierzytelniania **289**
Etap 3. Konfigurowanie autoryzacji **297**
Etap 4. Konfigurowanie rozliczania **305**
Cisco Secure i konfiguracja proxy z przycinaniem **310**
Konfigurowanie ładowalnych list kontroli dostępu **310**
Wykrywanie błędów w ustawieniach AAA **312**
Sprawdzanie ściany ogniowej PIX **312**
Sprawdzanie CSACS **316**
Podsumowanie **316**
Pytania kontrolne **318**

Rozdział 15. Ochrona przed atakami i obsługa multimediów 321
Sprawdzian „Czy już to wiem?" **321**
Zagadnienia podstawowe **322**
Obsługa multimediów w jednostce PIX **322**
Protokół RSTP **323**
H.323 **323**
Ochrona przed atakami **325**
Nadzorowanie fragmentacji i wirtualne składanie **326**
Nadzorowanie systemu nazw domen (DNS Guard) **326**
Nadzorowanie poczty elektronicznej (Mail Guard) **327**
Obrona przed zalewem **328**
Zabezpieczenia przed zalewem AAA **329**
Mechanizm wykrywania intruzów w ścianie ogniowej PIX **329**
Konfiguracja mechanizmu wykrywania intruzów **330**
Omijanie dynamiczne **332**
Polecenie ip verify reverse-path **333**
Podsumowanie **334**
Pytania kontrolne **335**

Dodatek A. Odpowiedzi na pytania 337
Rozdział 1 **337**
Pytania kontrolne **339**
Rozdział 2 **340**
Sprawdzian „Czy to już wiem?" **340**
Pytania kontrolne **341**
Rozdział 3 **342**
Sprawdzian „Czy to już wiem?" **342**
Pytania kontrolne **343**
Rozdział 4 **344**
Sprawdzian „Czy to już wiem?" **344**
Pytania kontrolne **345**
Rozdział 5 **347**
Sprawdzian „Czy to już wiem?" **347**
Pytania kontrolne **348**

Rozdział 6 **350**
Sprawdzian „Czy to już wiem?” **350**
Pytania kontrolne **351**
Rozdział 7 **353**
Sprawdzian „Czy to już wiem?” **353**
Pytania kontrolne **354**
Rozdział 8 **356**
Sprawdzian „Czy to już wiem?” **356**
Pytania kontrolne **357**
Rozdział 9 **358**
Sprawdzian „Czy to już wiem?” **358**
Pytania kontrolne **359**
Rozdział 10 **361**
Sprawdzian „Czy to już wiem?” **361**
Pytania kontrolne **363**
Rozdział 11 **363**
Sprawdzian „Czy to już wiem?” **363**
Pytania kontrolne **365**
Rozdział 12 **367**
Sprawdzian „Czy to już wiem?” **367**
Pytania kontrolne **368**
Rozdział 13 **370**
Sprawdzian „Czy to już wiem?” **370**
Pytania kontrolne **371**
Rozdział 14 **372**
Sprawdzian „Czy to już wiem?” **372**
Pytania kontrolne **374**
Rozdział 15 **376**
Sprawdzian „Czy to już wiem?” **376**
Pytania kontrolne **377**
Dodatek B **380**

Dodatek B. Zadania problemowe i przykładowe konfiguracje 387
Zadanie 1. Konfiguracja podstawowa ściany ogniowej PIX **387**
Informacja o podstawowej konfiguracji jednostki PIX w centrali **387**
Informacja o podstawowej konfiguracji jednostki PIX w Minneapolis **390**
Informacja o podstawowej konfiguracji jednostki PIX w Houston **391**
Zadanie 2. Konfiguracja zasad dostępu do centrali **393**
Zadanie 3. Konfiguracja uwierzytelniania **394**
Zadanie 4. Konfiguracja logowania **394**
Zadanie 5. Konfiguracja VPN **395**
Konfiguracja tunelowa VPN centralnej jednostki HQ_PIX **395**
Konfiguracja tunelowa VPN ściany ogniowej w Houston, HOU_PIX **399**
Konfiguracja tunelowa VPN ściany ogniowej w Minneapolis, MN_PIX **402**
Weryfikacja i wykrywanie błędów **405**
Zadanie 6. Konfiguracja przełączania awaryjnego **406**
Co tu działa nieprawidłowo? **407**

Słowniczek 419

Skorowidz 433