

Spis treści

	Przedmowa	9
Rozdział 1.	Wstęp	11
Rozdział 2.	Słabość protokołów sieciowych i związane z tym problemy	13
Rozdział 3.	SSL jako standard bezpiecznego przesyłania danych	15
	3.1. Historia i znaczenie protokołu SSL	15
	3.1.1. Przebieg nawiązania połączenia SSL	16
	3.1.2. Znaczenie zaufanego certyfikatu	17
	3.2. Generowanie certyfikatów przy użyciu programu OpenSSL	17
	3.2.1. Tworzenie własnego CA	18
	3.2.2. Tworzenie klucza prywatnego dla serwera	20
	3.2.3. Generowanie wniosku o wystawienie certyfikatu	20
	3.2.4. Wystawianie certyfikatu dla serwera	21
	3.2.5. Ściąganie hasła z klucza prywatnego serwera	22
	3.2.6. Unieważnianie certyfikatów	22
	3.2.7. Generowanie listy CRL (unieważnionych certyfikatów)	22
	3.2.8. Sprawdzenie ważności certyfikatu	23
	3.2.9. Różne formaty certyfikatów	23
	3.3. Kompilacja biblioteki OpenSSL ze źródeł	24
	3.4. Graficzne nakładki do programu OpenSSL	25
	3.5. Generowanie certyfikatów w środowisku Windows Server 2003	27
Rozdział 4.	Tunelowanie portów	33
	4.1. Program Stunnel	34
	4.1.1. stunnel.conf	37
	4.1.2. Przykład 1	39
	4.1.3. Przykład 2	41
	4.2. Tunele SSH	43
	4.2.1. Przykład 1	43
	4.2.2. Przykład 2 — SSH jako Socks Proxy	44
	4.2.3. Przykład 3 — tunele z przekazywaniem zdalnym	45
	4.2.4. Przykład 4 — tunel UDP po SSH	48
Rozdział 5.	OpenVPN — praktyczna implementacja tuneli VPN	51
	5.1. Instalacja	51
	5.1.1. Instalacja w systemie Linux Debian	52
	5.1.2. Instalacja przez kompilację źródeł programu (Linux)	52
	5.1.3. Instalacja pod systemami MS Windows	56

5.2.	Konfiguracja OpenVPN	58
5.3.	Praktyczny przykład — zdalny dostęp do zasobów firmy dla pracowników	59
5.3.1.	Generowanie certyfikatów SSL	60
5.3.2.	Konfiguracja po stronie serwera	61
5.3.3.	Uruchomienie usługi serwera OpenVPN	63
5.3.4.	Konfiguracja klienta	64
5.4.	Bardziej złożona konfiguracja z wieloma użytkownikami	67
5.4.1.	Przypisywanie stałych adresów IP użytkownikom	68
5.4.2.	Pliki ustawień użytkowników w katalogu ccd	68
5.4.3.	Tworzenie pliku dostep.txt	69
5.4.4.	Testowanie	70
5.4.5.	Logowanie zdarzeń do pliku	71
5.5.	Unieważnianie certyfikatów	72
5.6.	Łączenie oddziałów firmy	74
5.6.1.	Przykład rozwiązania z routerem	75
5.6.2.	Tunel VPN z mostkowaniem	79
5.6.3.	Tunel VPN z mostkowaniem w Windows XP	84
5.7.	OpenVPN w Windows Server z uwierzytelnianiem przez Active Directory	87
5.7.1.	Konfiguracja serwera	87
5.7.2.	Konfiguracja klienta	89
5.8.	OpenVPN w systemach Windows Mobile (PDA)	91
5.8.1.	Instalacja	91
Rozdział 6.	IPSec	95
6.1.	IPSec a translacja adresów (maskarada)	98
Rozdział 7.	IPSec w systemie Linux	101
7.1.	IPSec — przygotowanie środowiska w systemie Linux	101
7.2.	Instalacja programu OpenSWAN	102
7.3.	Praktyczny przykład — brama IPSec/VPN dla użytkowników mobilnych	104
7.3.1.	Konfiguracja bramy IPSec (Linux)	105
7.3.2.	Uruchomienie tunelu	109
7.4.	Konfiguracja klienta Windows	110
7.5.	Debugowanie połączenia	113
7.6.	Konfiguracja z uwierzytelnieniem przez certyfikaty	114
7.6.1.	Konfiguracja OpenSWAN z wykorzystaniem certyfikatów	115
7.7.	Import certyfikatów w systemie Windows	116
7.7.1.	Konfiguracja połączenia	121
7.8.	Dostęp z urządzeń PDA — Windows Mobile 2003, 2005, 2006	124
7.9.	Łączenie oddziałów firmy tunelem IPSec	125
Rozdział 8.	Cisco — łączenie oddziałów firmy. Site-to-Site IPSec Tunnel	131
8.1.	Access-listy w routerach Cisco	133
8.2.	Łączenie oddziałów firmy — praktyczny przykład	135
8.3.	Debugowanie połączenia	138
8.4.	Łączenie oddziałów firmy z tunelowaniem GRE	141
8.5.	IPSec z GRE — konfiguracja z trzema routerami	145
8.6.	Łączenie oddziałów firmy z mostkowaniem	152
8.7.	Łączenie oddziałów firmy Cisco-Linux	154
Rozdział 9.	Cisco — zdalny dostęp VPN dla pracowników	159
9.1.	Zdalny dostęp pracowników — konta przechowywane lokalnie na routerze	159
9.2.	Konfiguracja klienta VPN	163
9.3.	Zdalny dostęp pracowników — uwierzytelnianie przez RADIUS	164
9.3.1.	Instalacja MS IAS	164
9.3.2.	Konfiguracja routera	169

9.4. Uprawnienia do zasobów w sieci wewnętrznej	170
9.4.1. Ruch przechodzący przez tunel VPN (split tunneling)	171
9.4.2. Filtracja ruchu w tunelu VPN	172
Rozdział 10. Cisco ASA	175
10.1. ASA jako brama VPN dla pracowników	176
10.2. ASA jako brama SSL-VPN (WEB-VPN)	181
10.2.1. Konfiguracja SSL-VPN w ASA przez SDM	181
10.2.2. Połączenie testowe	185
Rozdział 11. Windows Server jako brama VPN	189
11.1. Konfiguracja usługi Routing i dostęp zdalny	191
11.2. Konfiguracja klienta	197
11.3. Dostęp do VPN na podstawie członkostwa w grupie w Windows 2003	200
11.4. Dostęp do VPN na podstawie członkostwa w grupie w Windows 2008	205
11.5. Tablica routingu po stronie klienta	208
11.6. Firewall — filtrowanie ruchu wewnątrz tunelu VPN	211
11.6.1. Postępowanie w systemie Windows 2003	211
11.6.2. Postępowanie w systemie Windows 2008	212
11.6.3. Dodawanie nowej reguły filtru	213
11.7. SSTP — nowy protokół dostępu VPN	214
Rozdział 12. Łączenie oddziałów firmy z wykorzystaniem systemów Windows Server 2003	215
12.1. Konfiguracja lokalizacji 1 — Gliwice	216
12.2. Konfiguracja lokalizacji 2 — Bytom	220
12.3. Konfiguracja zabezpieczeń IPSec	221
12.4. Debugowanie połączenia	222
Rozdział 13. Połączenia VPN w systemach Windows Mobile	223
13.1. Konfiguracja Windows Mobile z uwierzytelnianiem przez klucz współdzielony (PSK)	223
13.2. Konfiguracja Windows Mobile z certyfikatami	224
Rozdział 14. Konfiguracja połączenia IPSec w routerach Linksys.....	227
14.1. Połączenie typu Site-to-Site.....	228
14.1.1. Współpraca z innymi urządzeniami	229
14.2. Zdalny dostęp dla pracowników	230
Rozdział 15. Podsumowanie	233
15.1. Przydatne linki.....	234
Skorowidz	237