

Spis treści

ROZDZIAŁ 1. Wprowadzenie	11
1.1. O co chodzi z tym ruchem wychodzącym?	12
1.2. Czym jest tunel lub tunelowanie portów	13
1.3. Dlaczego tunelowanie może być niebezpieczne?	14
1.4. Tunelowanie TCP po ICMP	14
1.5. Tunelowanie TCP po zapytaniach DNS	16
1.6. Tunel OpenVPN przez serwer proxy	19
1.7. Co robić, jak żyć?	20
ROZDZIAŁ 2. Blokada ruchu wychodzącego — o co w tym chodzi?	23
2.1. Instalacja i konfiguracja routera linuksowego	24
2.2. Konfiguracja sieci w routerze linuksowym	25
2.3. iptables — linuksowy filtr pakietów	26
2.4. Przełączanie konfiguracji	32
2.5. Konfiguracja serwera DHCP	34
2.6. Problem z podwójnym NAT-owaniem	35
Podsumowanie	37
ROZDZIAŁ 3. Instalacja i konfiguracja serwera proxy Squid	39
3.1. Problem z szyfrowanymi stronami (TLS/SSL)	39
3.2. Instalacja programu Squid	45
3.3. Konfiguracja Squida	48
3.3.1. Generujemy certyfikat dla Squida	48
3.4. Pierwsze uruchomienie	51
3.5. Import certyfikatu do przeglądarek	53
3.6. Zabezpieczanie serwera Squid	56
3.6.1. Blokada wybranych typów rozszerzeń plików na podstawie adresu URL	58
3.6.2. Blokada wybranych typów plików na podstawie nagłówków odpowiedzi serwera (Content-Type oraz Content-Disposition)	59
3.6.3. Blokada pobrań niektórych plików na podstawie wyrażenia regularnego adresu URL	61
3.6.4. Blokada domen ze znakami narodowymi IDN	62
3.6.5. Blokada stron na podstawie ich adresu URL	63
3.6.6. Zaawansowana filtracja z wykorzystaniem serwera ICAP i programu antywirusowego ClamAV	64

3.7.	Wracamy do firewalla	68
3.7.1.	Zmiana polityki ruchu wychodzącego na blokuj	68
3.7.2.	Problem z aktualizacją wpisów dla zmiennych adresów IP	69
3.7.3.	Adresy, które powinniśmy odblokować	70
3.7.4.	Tryb transparentny serwera proxy	71
3.7.5.	Blokada ruchu wychodzącego na serwerach	72
3.8.	Graficzna reprezentacja logów	73
	Podsumowanie	73
ROZDZIAŁ 4.	E2Guardian jako dedykowany serwer proxy oraz serwer ICAP dla Squida	75
4.1.	Trochę o historii powstania DansGuardiana i jego odnogi E2Guardiana	75
4.2.	Instalacja programu E2Guardian	76
4.3.	Konfiguracja programu E2Guardian	76
4.4.	E2Guardian jako serwer ICAP	86
4.5.	E2Guardian w trybie transparentnym	88
4.6.	Żart primaaprilisowy — obracanie użytkownikom obrazków na stronach	89
	Podsumowanie	91
ROZDZIAŁ 5.	Bezpieczny DNS z wykorzystaniem programu Pi-hole	93
5.1.	Instalacja programu	94
5.2.	Konfiguracja Pi-hole	98
5.3.	Aktualizacja i pobieranie list	99
5.4.	Obsługa wyjątków	101
5.5.	Pi-hole jako serwer DHCP	102
5.6.	Dodawanie lokalnych wpisów DNS	102
	Podsumowanie	104
ROZDZIAŁ 6.	Diladele Web Safety	105
6.1.	Instalacja Web Safety	105
6.2.	Konfiguracja sieci — nadanie statycznego adresu IP	108
6.3.	Logowanie do panelu administracyjnego	108
6.4.	Import lub tworzenie certyfikatu rootCA	110
6.5.	Konfiguracja zasad filtracji połączeń	112
6.6.	Testujemy skonfigurowane ograniczenia	115
6.7.	Dostrajanie filtrów i konfiguracja wyjątków	116
6.8.	Konfigurujemy i testujemy dodatek YouTube Guard	119
6.9.	Konfigurujemy tryb transparentny	122
	Podsumowanie	124
ROZDZIAŁ 7.	OPNsense — zintegrowany firewall	125
7.1.	Instalacja systemu	125
7.2.	Pierwsze logowanie do GUI — kreator postinstalacyjny	127
7.3.	Testowanie połączenia	130
7.4.	Konfiguracja serwera DHCP	130
7.5.	Aktualizacja do najnowszej wersji	131

7.6.	Utworzenie lub import urzędu CA	131
7.7.	Konfiguracja serwera proxy (Squid)	131
7.8.	Instalacja i integracja skanera antywirusowego Clam-AV z serwerem proxy	134
7.9.	Zewnętrzne listy dostępu w serwerze proxy	137
7.10.	Włączenie dostępu przez SSH	137
7.11.	Dodajemy kolejne blokady	138
7.12.	Instalacja wtyczki Zenarmor — dodajemy firewall warstwy aplikacyjnej	140
7.13.	Konfiguracja wtyczki Zenarmor — tworzymy zasadę bezpieczeństwa	141
7.14.	System IDS i pozostałe funkcje	146
7.14.1.	IDS — tworzenie własnych reguł	147
7.15.	Dodatek Geo-IP do firewalla	149
	Podsumowanie	149
ROZDZIAŁ 8.	UTM na przykładzie FortiGate 60F	151
8.1.	Czym UTM różni się od zwykłego routera — zasada działania	152
8.2.	Wstępna konfiguracja urządzenia	155
8.3.	Zaczynamy zabawę z firewallem	159
8.4.	Włączamy profile zabezpieczeń w regule firewalla	162
8.4.1.	Weryfikacja działania skanera antywirusowego	162
8.4.2.	Włączamy SSL Deep Inspection, czyli rozszywamy protokół TLS	163
8.4.3.	Import własnego certyfikatu root CA	166
8.4.4.	Blokowanie programów wg kategorii	169
8.4.5.	Web Filter — blokowanie stron na podstawie kategorii	170
8.4.6.	Web Filter — blokowanie stron na podstawie adresu URL lub wyrażenia regularnego	172
8.4.7.	Tryb inspekcji flow-based vs proxy-based	174
8.4.8.	DNS filter, czyli filtracja w warstwie zapytań DNS	175
8.4.9.	File Filter — blokowanie pobrań wybranych typów plików	176
8.4.10.	System IPS — włączanie ochrony oraz tworzenie własnych sygnatur	177
8.4.11.	Sygnatury aplikacji	181
8.5.	Praktyczne przykłady z życia	182
8.5.1.	Chcemy zablokować Facebooka dla wszystkich z wyjątkiem działu marketingu	182
8.5.2.	Chcemy zablokować pobieranie plików EXE ze wszystkich stron z wyjątkiem zaufanych stron typu Microsoft itp.	184
8.5.3.	Dodajemy listę domen zaufanych instytucji do wyjątków inspekcji SSL	185
8.5.4.	Geo-IP, czyli blokujemy klasy z krajów potencjalnie niebezpiecznych	186
8.5.5.	Odblokowujemy wybrane programy w określonych godzinach i dniach tygodnia	187
8.5.6.	Blokujemy domeny zawierające znaki narodowe w nazwie (IDN)	189

8.6.	Podgląd logów	190
8.6.1.	Wysyłka logów do centralnego serwera Syslog	191
8.7.	FortiGate jako Web Application Firewall	192
8.7.1.	Przygotowanie reguły firewalla i profilu inspekcji SSL dla WAF	193
8.7.2.	Testujemy działanie WAF	195
8.8.	Analiza pakietów dochodzących do routera	196
8.9.	Polecenia dostępne w systemie FortiOS	196
	Podsumowanie	200
ROZDZIAŁ 9.	Konfiguracja przeglądarek do współpracy z serwerem proxy	203
9.1.	Ręczna konfiguracja proxy w przeglądarce	204
9.2.	Konfiguracja ustawień proxy za pomocą zasad grupy w środowisku Active Directory	206
9.3.	Ustawianie serwera proxy poprzez wpis rejestru	210
9.4.	Ustawianie serwera proxy poprzez plik autokonfiguracji (PAC)	211
9.5.	Ustawienia proxy dla lokalnego konta systemowego	215
9.6.	Import zaufanego urzędu certyfikacji (tzw. Root CA) w komputerach użytkowników	215
	Podsumowanie	219
ROZDZIAŁ 10.	Podsumowanie	221
10.1.	Bądź na bieżąco	221
10.2.	Uświadamiaj użytkowników	221
10.3.	Przygotuj regulamin korzystania ze służbowego komputera oraz sieci ..	221
10.4.	Sprawdzaj stan programów antywirusowych	222
10.5.	Ogranicz dostęp użytkownikom po VPN-ie	222
10.6.	Rozważ wymuszenie całego ruchu przez VPN	222
10.7.	Odseparuj Wi-Fi od sieci LAN	223
10.8.	Monitoruj połączenia VPN regułkami firewalla	223
10.9.	Rozważ przełączenie użytkowników z połączenia kablowego na Wi-Fi + VPN	224
10.10.	Dodaj 2FA (weryfikacja dwuskładnikowa) do połączeń VPN	224
10.11.	Podziel sieć na VLAN-y	224
10.12.	Zabezpiecz serwer plików	225
10.13.	Skonfiguruj Zasady ograniczeń oprogramowania w GPO	226
10.14.	Zablokuj możliwość pobierania plików	226
10.15.	Problem z Dropboxem (i z innymi dostawcami)	226
10.16.	Rób backupy ☺	227
10.17.	Blokuj aplikacje zdalnego dostępu	227
10.18.	Monitoruj obciążenie łącza i innych parametrów	227
10.19.	Sprawdzaj cyklicznie reguły firewalla	228
10.20.	Nie zezwalaj na podłączanie swoich prywatnych laptopów/urządzeń do sieci wewnętrznej	228
10.21.	Usuwać konta byłych pracowników	228
10.22.	Postaw centralny serwer logów	228
10.23.	Monitoruj liczbę sesji połączeń użytkownika	228

DODATEK A	OpenSSL — przydatne polecenia	229
	Przykład utworzenia urzędu głównego i pośredniego	232
DODATEK B	Filtry programu Wireshark oraz tcpdump	235
DODATEK C	Przelicznik maski podsięci	237
DODATEK D	Monitoring na ESP	239