

Rozwiązania Cyberoam zapewniają kompleksową ochronę sieci: firewall, IPS, kontrola dostępu do www i aplikacji, antywirus, antyspam, VPN, zarządzanie łączem, raportowanie, 3G/4G, WAF.

### 5 powodów do zakupu urządzeń Cyberoam UTM:

- Najwyższa wydajność w swojej klasie urządzeń
- Atrakcyjna cena
- Intuicyjne zarządzanie
- Wbudowany moduł raportowania (bezpłatny)
- Samoobsługowa kwarantanna antyspamowa

W Polsce dotychczas zaufały nam jednostki administracji publicznej m.in. urzędy miast, urzędy gmin, starostwa powiatowe, uczelnie wyższe, szpitale, spółki energetyczne oraz firmy z różnych obszarów gospodarki m.in. produkcyjne, farmaceutyczne, ubezpieczeniowe, transportowe, telekomunikacyjne.

**Administratorze, zabezpiecz swoją sieć już dziś - zapraszamy do bezpłatnych testów rozwiązań**



### Urządzenia serii NG

**Seria NG:** 15iNG, 25iNG/6P, 35iNG, 50iNG, 100iNG, 200iNG/XP, 300iNG/XP, 500iNG/XP, 750iNG/XP

**Seria bezprzewodowa NG:** 15wiNG, 25wiNG, 25wiNG-6P, 35wiNG



## Funkcjonalności

### Zapora sieciowa

- zapora warstwy 8 (User – Identity Firewall)
- obsługa wielu stref (Zone Based Firewall)
- kryteria kontroli dostępu: tożsamość użytkownika, strefa źródłowa i docelowa, adresy MAC oraz IP, rodzaj usługi sieciowej
- polityki UTM: IPS, filtr Web, filtr aplikacji, Anti-Virus, Anti-Spam, zarządzanie pasmem
- kontrola i podgląd aplikacji na poziomie warstwy 7
- ograniczanie dostępu bazie harmonogramu (Access Scheduling)
- translacja adresów sieciowych (NAT) w oparciu o polityki
- H.323, SIP NAT Traversal
- wsparcie dla VLAN zgodnie z 802.1q
- ochrona przed atakami DoS i DDoS
- filtrowanie adresów MAC, IP, ochrona przed ich Spoofingiem

### Ochrona Anti-Virus i Anti-Spyware

- wykrywanie i usuwanie złośliwego oprogramowania w postaci wirusów, robaków i koni trojańskich
- ochrona przed phishingiem oraz oprogramowaniem typu Spyware i Malware
- automatyczna aktualizacja bazy sygnatur zagrożeń
- skanowanie ruchu HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IM, VPN
- indywidualne skanowanie użytkownika
- skanowanie na podstawie rozmiaru pliku
- skanowanie na podstawie rodzaju pliku
- dodawanie treści takich jak podpis lub disclaimer

### Ochrona Anti-Spam

- skanowanie ruchu przychodzącego (inbound) lub ruchu wychodzącego (outbound)
- ochrona przed spamem na podstawie RBL (Real-time Blacklist), analiza nagłówka MIME
- filtrowanie oparte o treść nagłówka, rozmiar, adres nadawcy, adres odbiorcy
- oznaczenie wiadomości w linii tematu
- możliwość skierowania podejrzanej wiadomości na dedykowany adres email
- filtrowanie obrazów w oparciu o RPD (Recurrent Pattern Detection)
- ochrona w trybie Zero Hour Virus Outbreak Protection
- wydzielona strefa kwarantanny z możliwością obsługi przez użytkownika
- filtrowanie spamu na podstawie reputacji adresu IP, białych lub czarnych list
- informowanie i zarządzanie wiadomościami przez mechanizm spam digest

### Ochrona IPS

- ponad 4500 gotowych sygnatur zagrożeń, możliwość definiowania własnych sygnatur
- możliwość tworzenia indywidualnych lub zbiorowych polityk IPS
- kreowanie polityk per użytkownik
- automatyczna aktualizacja sygnatur z sieci CRProtect
- wykrywanie anomalii w protokołach sieciowych
- ochrona przed atakami typu DDoS

### Filtrowanie Web

- wbudowana baza kategorii stron Web
- filtrowanie na bazie adresów URL, słów kluczowych, plików
- ponad 82 kategorie, możliwość definiowania własnych kategorii stron
- filtrowanie ruchu HTTP i HTTPS
- blokowanie adresów zagrożonych Malware, Phishing, Pharming
- priorytetyzowanie i przydział pasma na podstawie kategorii
- kontrola dostępu na podstawie harmonogramu
- blokada apletów Java, Cookies, Active X
- zgodność z CIPA
- ochrona przed wyciekaniem danych przez HTTP i HTTPS

### Filtrowanie aplikacji

- wbudowana baza kategorii aplikacji
- 20 kategorii np.: gry, komunikatory, P2P, media streamingowe, proxy
- kontrola dostępu na podstawie harmonogramu
- szczegółowa kontrola aplikacji:
  - zezwolenia na dodawanie obrazów i wideo, zablokowanie gier i aplikacji na portalu Facebook
  - anonimowych serwerów proxy np. TOR, JAP
  - keyloggerów
- podgląd aplikacji w warstwie 7, podgląd użytkowników w warstwie 8

### Web Application Firewall (WAF)

- model ochrony: Positive Protection
- unikalna technologia Intuitive Website Flow Detector
- ochrona przed: SQL injections, Cross-site Scripting (XSS), Session Hijacking, URL Tampering, Cookie Poisoning itp.
- wsparcie dla HTTP 0.9/1.0/1.1
- zakres ochrony: od 5 do 200 serwerów aplikacji

### Wirtualne sieci prywatne VPN

- wsparcie dla IPSec, L2TP, PPTP
- szyfrowanie: DES/3DES, AES, Twofish, Blowfish, Serpent
- obsługa algorytmów haszujących: MD5, SHA-1
- uwierzytelnianie przez współdzielony klucz (PSK) lub z użyciem certyfikatów cyfrowych
- IPSec NAT Traversal
- wsparcie dla funkcji Dead Peer Detection i Perfect Forward Secrecy
- obsługa grup Diffie Hellmann: 1,2,5,14,15,16
- wsparcie dla zewnętrznych centrów certyfikacji (CA)
- eksport konfiguracji dla pracowników mobilnych
- obsługa nazw domenowych
- redundancja tuneli VPN
- obsługa sieci z nakładającą się adresacją IP
- wsparcie dla połączeń typu hub & spoke

### SSL VPN

- tunelowanie ruchu TCP oraz UDP
- uwierzytelnianie w oparciu o: Active Directory, LDAP, RADIUS, lokalna baza
- wielowarstwowe uwierzytelnianie klienta poprzez certyfikat, nazwę użytkownika oraz hasło
- polityki dostępu dla użytkowników i grup użytkowników
- obsługa połączeń tunelowych: split lub full
- możliwość zestawiania połączenia przez portal bez użycia klienta (z użyciem przeglądarki internetowej)
- możliwość zestawiania połączenia z użyciem lekkiego klienta programowego
- granularna kontrola dostępu do wewnętrznych zasobów sieciowych
- kontrola administracyjna: session time out, Dead Peer Detection, możliwość aranżacji wyglądu portalu web
- dostęp do aplikacji na bazie protokołów HTTP, HTTPS, RDP, TELNET, SSH

### Zarządzanie komunikatorami Instant Messaging

- kontrola komunikatorów Yahoo oraz Windows Live Messenger
- skanowanie ruchu pod kątem obecności wirusów
- zezwalanie/blokada: logowania użytkownika, transferu plików, strumieniowania obrazu wideo, chat
- filtrowanie treści
- możliwość zapisywania aktywności komunikatorów w logach systemowych
- wychwytywanie transferu plików archiwów
- konfiguracja własnych alertów

### Wireless WAN

- wbudowany port USB dla obsługi modemów 3G/4G/WiMAX
- możliwość ustalenia priorytetu (Primary/Backup)

### Zarządzanie pasmem

- regulowanie pasma dla aplikacji i użytkowników
- polity w trybie gwarancji pasma lub w trybie burst
- wykrywanie obciążenia per aplikacja lub per użytkownik
- raportowanie obciążenia dla interfejsów WAN
- restrykcje dla kategorii stron i aplikacji

### Tożsamość i kontrola użytkownika

- ograniczanie czasu dostępu
- kwotowe restrykcje czasu lub ilości danych
- zarządzanie dostępnym pasmem w oparciu o harmonogram
- restrykcje dla aplikacji P2P i IM

### Sieć

- ochrona przed utratą łączności (Multi-WAN failover) w tym wykorzystanie modemu 3G/4G/WiMAX
- równoważenie obciążenia (load balancing) na bazie WRR
- Policy Based Routing per aplikacja lub per użytkownik
- wsparcie dla HTTP Proxy
- routing dynamiczny: RIPv1, RIPv2, OSPF, BGP, Multicast Forwarding
- Parent Proxy z FQDN
- IPv6 Ready

### Wysoka dostępność

- Active-Active
- Active-Passive z synchronizacją stanu
- Stateful Failover
- alerty o zmianie statusu urządzenia

### Administracja i zarządzanie

- kreator konfiguracji na bazie Web GUI
- kontrola dostępu w oparciu o role
- prosta aktualizacja oprogramowania systemowego przez Web GUI
- interfejs graficzny zgodny z Web 2.0 (HTTPS)
- możliwość zmiany motywu kolorystycznego
- obsługa z poziomu wiersza komend (CLI): port szeregowy, SSH, Telnet
- wsparcie dla SNMP (v1, v2c, v3)
- opcjonalne zarządzanie z poziomu Cyberoam Central Console
- wsparcie dla protokołu NTP
- NTP support

### Uwierzytelniania użytkowników

- wbudowana baza lokalna
- integracja z Active Directory (AD)
- wsparcie dla Windows Single Sign On
- integracja z bazą LDAP lub RADIUS
- wsparcie dla cienkich klientów (Microsoft i Citrix)
- wsparcie dla RSA SecurID
- zewnętrzne uwierzytelnianie użytkowników i administratorów
- wiązanie adresu MAC z użytkownikiem
- możliwość wykorzystania wielu serwerów uwierzytelniania

### Logowanie zdarzeń i monitoring

- prezentacja graficzna w czasie rzeczywistym
- wsparcie dla syslog
- przegląd zdarzeń dla: zapy, IPS, filtra Web, Anti-Virus, Anti-Spam, uwierzytelniania, system, admin

### Wbudowany mechanizm raportowania Cyberoam iView

- zintegrowane, oparte o Web GUI narzędzie do raportowania
- ponad 1200 wbudowanych raportów
- ponad 45 raportów zgodności
- raporty historyczne i raporty czasu rzeczywistego
- kilka dostępnych dashboard'ów
- raporty o stanie bezpieczeństwa, spamie, wirusach, ruchu sieciowym, naruszeniach polityk ochrony, VPN, słowach kluczowych w serwisach wyszukiwawczych
- zróżnicowany format raportowania: tabelaryczny, graficzny
- możliwość eksportowania do plików PDF, Excel
- automatyczne generowanie raportów zgodnie z założonym harmonogramem

### IPSec VPN Client\*\*

- wspierane platformy: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 32/64-bit
- możliwość importu pliku konfiguracyjnego

### Certyfikaty

- Common Criteria EAL4+
- ICSA Firewall – Corporate
- Checkmark UTM Level 5 Certification
- VPNC - Basic and AES interoperability

\*wydajność mierzona w oparciu o ruch HTTP zgodnie z RFC 3511

\*\*wymagany dodatkowy zakup

Specyfikacja	15iNG	25iNG/6P	35iNG	15wiNG	25wiNG/6P	35wiNG
<b>Interfejsy</b>						
Liczba wbudowanych portów GE	3	4/6	6	3	4/6	6
Port konsolowy (RJ-45)	1	1	1	1	1	1
Port USB	2	2	2	2	2	2
Hardware Bypass	-	-	-	-	-	-
Konfigurowalne porty Internal/DMZ/WAN	Tak	Tak	Tak	Tak	Tak	Tak
<b>Wydajność systemu</b>						
Przepływność Firewall dla ruchu UDP (Mbps)	1,200	1,800	3,700	1,200	1,800	3,700
Przepływność Firewall dla ruchu TCP (Mbps)	900	1,200	2,400	900	1,200	2,400
Liczba nowych sesji na sekundę	5,000	6,000	21,000	5,000	6,000	21,000
Liczba równoczesnych sesji	200,000	500,000	750,000	200,000	500,000	750,000
Przepustowość IPSec VPN (Mbps)	130	210	280	130	210	280
Liczba tuneli IPSec VPN	300	550	850	300	550	850
Przepustowość SSL VPN (Mbps)	50	75	100	50	75	100
Przepustowość WAF(Mbps)	-	100	150	-	100	150
Przepustowość Anti-Virus (Mbps)	200	350	600	200	350	600
Przepustowość IPS (Mbps)	160	240	650	160	240	650
Przepustowość UTM (Mbps)	90	125	300	90	125	300
Uwierzytelnieni użytkownicy/węzły	Nieograniczona	Nieograniczona	Nieograniczona	Nieograniczona	Nieograniczona	Nieograniczona
<b>Sieć bezprzewodowa</b>						
Standardy sieci bezprzewodowej				IEEE 802.11 a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, AES, PSK)		
Antena				Demontowana 3x3 MIMO do 8 bssid		
Punkty dostępowe				11n HT40 : +15dBm, 11b CCK: +15dBm, 11g OFDM: +15dBm		
Moc nadajnika (EIRP)				-68dBm at 300Mbps, -70dBm at 54Mbps, -88dBm at 6Mbps		
Czułość odbiornika				2.412 GHz - 2.472 GHz		
Zakres częstotliwości				5.200 GHz - 5.825 GHz		
Liczba kanałów				USA (FCC) - 11 kanałów, EU (ETSI) / Japonia (TELEC) - 13 kanałów		
Prędkość transmisji danych				802.11n: up to 450Mbps, 802.11b: 1, 2, 5, 5, 11Mbps, 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps		
<b>Wymiary (cm)</b>						
W x Sz x G	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2
Waga (Kg)	1.5 kg,	2.3 kg,	2.3 kg,	1.5 kg,	2.3 kg,	2.3 kg,
<b>Zasilanie</b>						
Napięcie wejściowe	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Zużycie energii	13.2W	33.5W	47.8W	13.2W	33.5W	47.8W
Wydzielane ciepło (BTU)	45	114	163	45	114	163
Dodatkowy zasilacz	-	-	-	-	-	-

Nie dotyczy

Specyfikacja	50iNG	100iNG	200iNG/XP	300iNG/XP	500iNG-XP	750iNG-XP
<b>Interfejsy</b>						
Liczba wbudowanych portów GE	8	8	10 / 6	10 / 6	8	8
Opcjonalne porty Flexi Port** (GbE Copper / GbE Fiber / 10GbE Fiber)	-	-	8 / 8 / 4	8 / 8 / 4	8 / 8 / 4	8 / 8 / 4
Port konsolowy (RJ-45)	1	1	1	1	1	1
Port USB	2	2	2	2	2	2
Hardware Bypass	2	2	2	2	2	2
Konfigurowalne porty Internal/DMZ/WAN	Tak	Tak	Tak	Tak	Tak	Tak
<b>Wydajność systemu</b>						
Przepustowość Firewall dla ruchu UDP (Mbps)	6,500	8,000	10,000/14,000	12,000/21,000	25,000	28,500
Przepustowość Firewall dla ruchu TCP (Mbps)	4,000	5,000	8,000	9,500/10,500	18,000	20,000
Liczba nowych sesji na sekundę	45,000	60,000	85,000	100,000	180,000	200,000
Liczba równoczesnych sesji	1,000,000	3,000,000	3,200,000	3,200,000	4,500,000	6,400,000
Przepustowość IPSec VPN (Mbps)	850	1,050	1,150	1,300	3,200	4,200
Liczba tuneli IPSec VPN	2,000	4,000	4,500	5,000	6,250	7,250
Przepustowość SSL VPN (Mbps)	300	400	450	500	650	750
Przepustowość WAF(Mbps)	450	700	1,000	1,250	1,500	1,750
Przepustowość Anti-Virus (Mbps)	1,500	2,200	2,600	2,900	4,300	5,500
Przepustowość IPS (Mbps)	1,600	2,500	3,000	4,000	7,000	8,500
Przepustowość UTM/NGFW (Mbps)	850	1,050	1,400	1,700	3,750	5,000
Uwierzytelnieni użytkownicy/węzły	Nieograniczona	Nieograniczona	Nieograniczona	Nieograniczona	Nieograniczona	Nieograniczona
<b>Wymiary (cm)</b>						
W x Sz x G	4.4 X 37.2 X 44	4.4 X 37.2 X 44	4.4 x 43.9 x 30.1	4.4 x 43.9 x 30.1	4.4 x 43.3 x 47.62	4.4 x 43.3 x 47.62
Waga (Kg)	5 kg	5 kg	5.1 kg	5.1 kg	5.1 kg	5.1 kg
<b>Zasilanie</b>						
Napięcie wejściowe	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Pobór mocy (W)	99W	99W	137W	137W	208W	208W
Emisja ciepła (BTU)	338	338	467	467	345	345
Dodatkowy zasilacz	-	-	-	-	-	Tak

\*Jeśli włączone, ruch w sieci zostanie przekierowany w przypadku awarii zasilania.  
\*\*Wydajność antywirusa, IPS oraz UTM mierzona jest w oparciu o ruch HTTP, zgodnie ze wskazaniami RFC 3511. Rzeczywista wydajność może się zmieniać, w zależności od rzeczywistego środowiska sieciowego. Wartości dla oprogramowania Cyberoam OS 10.6.2. i wyższe.

