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
- oznaczanie 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 wyciekiem 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
- Imożliwość 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
- polisy 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
- Parrent Proxy z FQDN
- IPv6 Ready

Wysoka dostępność
- Active-Active
- Active-Passive z synchronizacją stanu
- Stateful Failover
- alerty o zmianie status 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: zapory, 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 PFD, 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

Interfejsy

Liczba wbudowanych portów GE	10
Port konsolowy (RJ-45)	1
Port USB	2
Hardware Bypass	2
Konfigurowalne porty Internal/DMZ/WAN	Tak

Wydajność systemu

Przepustowość Firewall dla ruchu UDP (Mbps)	12,000
Przepustowość Firewall dla ruchu TCP (Mbps)	9,500
Liczba nowych sesji na sekundę	85,000
Liczba równoczesnych sesji	2,000,000
Przepustowość IPSec VPN (Mbps)	3,000
Liczba tuneli IPSec VPN	500
Przepustowość SSL VPN (Mbps)	500
Przepustowość WAF(Mbps)	850
Przepustowość Anti-Virus (Mbps)	2,600
Przepustowość IPS (Mbps)	2,400
Przepustowość UTM/NGFW (Mbps)	1,500
Uwierzytelnieni użytkownicy/węzły	Nieograniczona

Wymiary (cm)

W x Sz x G	4.4 x 43.9 x 30.1
Waga (Kg)	5.1 kg

Zasilanie

Napięcie wejściowe	100-240VAC
Pobór mocy (W)	137W
Emisja ciepła (BTU)	467
Dodatkowy zasilacz	-

Konsorcjum FEN Sp. z o.o.
ul. Dąbrowskiego 273A
60-406 Poznań
sales@fen.pl

Cyberoam
Unified Threat Management

Funkcjonalności - szczegóły

Typ systemu
- dedykowane rozwiązanie sprzętowe
- obsługa w ramach jednego urządzenia poniższych funkcjonalności podstawowych: firewall, IPS, antywirus, antyspam, kontrola treści (web i aplikacji), poufność danych
– IPSec VPN oraz SSL VPN, z uwzględnieniem identyfikacji poszczególnych użytkowników lub grup użytkowników

Zapora sieciowa (firewall)
- tryby pracy: routing (z funkcją NAT), bridge (transparent) i hybrydowy (część jako router, część jako bridge)
- tworzenie wydzielonych stref bezpieczeństwa firewall np. WAN, LAN, DMZ
- obsługa 802.1q VLAN (tworzenie do 4096 interfejsów wirtualnych definiowanych jako VLAN)
- analiza ruchu szyfrowanego protokołem SSL

Antywirus
- skanowanie następujących protokołów: SMTP, POP3, IMAP, FTP, HTTP, HTTPS
- możliwość skanowania ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach np. FTP na porcie 2021
- automatyczna aktualizacja bazy sygnatur (szczepionek) antywirusowych oraz możliwość ręcznej aktualizacji
- wbudowany moduł kwarantanny z możliwością samoobsługi przez użytkowników

Antyspam
- skanowanie protokołów: SMTP, POP3, IMAP
- wbudowany moduł kwarantanny z możliwością samoobsługi przez użytkowników

IPS
- możliwość włączenia/wyłączanie poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów
- automatyczne pobieranie aktualizacje sygnatur ataków

Filtrowanie URL (Web)
- blokowanie anonimowych proxy działających poprzez HTTP i HTTPS
- wyświetlanie komunikatu o przyczynie zablokowania dostępu do strony www. Administrator może edytować treść komunikatu i dodania logo organizacji
- stały dostęp do globalnej bazy zasilającej filtr URL

Filtrowanie aplikacji
- identyfikacja i kontrola aplikacji na podstawie głębokiej analizy pakietów, niezależnie od wykorzystywanego portu TCP/IP, protokołu, szyfrowania
- szczegółowa kontrola dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo
- automatyczna aktualizacja sygnatur aplikacji

VPN
- tworzenie połączeń VPN: IPsec (Site-to-site, Client-to-site), L2TP i PPTP
- wbudowany moduł SSL VPN, podłączanie jednocześnie 100 użytkowników SSL VPN (maksymalnie 500)
- skanowanie antywirusowe tuneli VPN (IPsec/L2TP/PPTP)
- monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności

Load balancing
- load balancing i failover dla łącz internetowych
- przełączania na inne łącze w przypadku awarii podstawowego łącza.
- wykrycie awarii łącza możliwe przy użyciu protokołów ICMP, TCP i UDP
- wysyłanie powiadomień do administratora o zmianie statusu urządzenia (w postaci wiadomości e-mail)
- wsparcie dla modemów 3G/4G podłączanych poprzez port USB

Zarządzanie
- tworzenie kont administracyjnych o różnych uprawnieniach
- automatyczne wylogowanie administratora po określonym czasie bezczynności
- definiowanie polityk hasłowych dla administratorów
- zarządzanie poprzez bezpieczny kanał komunikacji: HTTPS, SSH i konsolę
- monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, obciążenie interfejsów sieciowych)
- przechowywanie przynajmniej dwóch wersji firmware
- automatyczne wykonywanie kopii zapasowej konfiguracji systemu

Logowanie oraz raportowanie
- generowanie raportów, które powiążą poszczególne zdarzenia z nazwami użytkowników
- generowanie raportów dotyczące wszystkich blokowanych połączeń z uwzględnieniem użytkowników i adresu IP
- generowanie raportów dotyczących transferu danych w oparciu o aplikację, użytkowników i adres IP
- logowanie na serwerze syslog zdarzeń związanych z: antywirus, antyspam, filtrowanie treści, IPS, firewall
- wbudowany lokalny dysk o pojemności minimum 250 GB na potrzeby logowania i raportowania

Konsorcjum FEN Sp. z o.o.
ul. Dąbrowskiego 273A
60-406 Poznań
sales@fen.pl

Cyberoam
Unified Threat Management