

## Magiczne pudełko, czy siła technologii?



Podłączając interfejs sieciowy naszych komputerów, czy to kablowy, czy bezprzewodowy, nie zastanawiamy się nad tym, w jaki sposób jesteśmy chronieni przez wszelkim złem czyhającym na nas w sieci.

Podświadomie wmawiamy sobie, że osobisty firewall – a w komplecie z nim program antywirusowy – zapewniają nam bezpieczne rozmowy przy użyciu komunikatorów, przeglądanie stron WWW, wykonywanie przelewów bankowych czy korzystanie z poczty elektronicznej.

W niewielkich sieciach jest jeszcze możliwe obarczenie użytkownika końcowego problemami związanymi z bezpieczeństwem jego obecności w sieci.

W większych infrastrukturach, w sieciach firm czy instytucji, bezpieczeństwo jest kluczowym elementem komunikacji, więc bardzo często wykorzystuje się do jego zapewnienia różne rozwiązania chroniące przed atakami na poziomie sieci. W celu zadbania o bezpieczeństwo w takich przypadkach, stosuje się coraz częściej zintegrowane systemy zabezpieczeń. Takie specjalistyczne rozwiązania (ang. Unified Threat Management – UTM) to prawdziwe kombajny, będące w stanie zadbać o kilka płaszczyzn bezpieczeństwa jednocześnie. Na rynku dostępne są liczne rozwiązania różnych producentów – ja chciałbym przybliżyć urządzenie FortiGate 310B firmy Fortinet.

Cechą charakterystyczną rodziny urządzeń FortiGate jest zastosowanie układów ASIC (ang. Application Specific Integrated Circuit), realizujących najważniejsze zadania urządzenia w dedykowanych układach krzemowych.

Układy FortiASIC to rodzina specjalizowanych, wysokowydajnych procesorów do analizy ruchu sieciowego oraz zawartości (ang. *content*), stworzona na potrzeby właśnie takich urządzeń jak Unified Threat Management w celu nadania im maksymalnego możliwego przyspieszenia

wykonywanych operacji. Fortinet FortiOS to utwardzona wersja systemu operacyjnego obsługująca urządzenie. Steruje ona właściwą pracą poszczególnych modułów oraz pozwala na łatwą administrację za pomocą interfejsu webowego.

Sam system operacyjny, jak i zawarte w nim funkcjonalności firewall i VPN, aktualizowane są przez administratora na podstawie aktywnego serwisu FortiCare, natomiast silniki wspierające funkcje bezpieczeństwa (AV, IPS, WEB, AS) są dynamicznie aktualizowane poprzez specjalną sieć Fortinet FortiGuard Center, co zapewnia zawsze aktualne wersje baz sygnatur oraz najświeższe aktualizacje bezpieczeństwa.

FortiOS jest systemem wielopoziomowym, zapewniającym zoptymalizowane wydajnościowo działanie urządzenia przy maksymalnym wykorzystaniu jego możliwości obliczeniowych.

Urządzenia klasy UTM wymagają ogromnych mocy obliczeniowych do wykonywania swoich zadań. Układ FortiASIC wykorzystuje specjalny język Content Pattern Recognition Language (CPRL), który został zaprojektowany tak aby zmaksymalizować wydajność zarówno dla pojedynczych usług, jak i dla całego pakietu ochrony oferowanego przez UTM Fortinet.

W urządzeniu kryje się sporo ciekawych rozwiązań, a najbardziej interesujące z nich to dwa specjalizowane wysokowydajne procesory FortiASIC.

Pierwszy z nich, oznaczony indeksem CP (ang. Content Processor) zbudowany jest z dwóch procesorów, zaszytych w jednym chipie. Content Processor oraz Key Exchange Processor zawarte w układzie bardzo znacząco wpływają na obniżenie opóźnień związanych ze skanowaniem antywirusowym, szyfrowaniem VPN czy przetwarzaniem danych uwierzytelniających.

Ten układ bardzo mocno podnosi wydajność urządzenia podczas przetwarzania zawartości.

### Producent

**FORTINET**  
UNIFIED THREAT MANAGEMENT SOLUTIONS

### System

UTM dla przedsiębiorstw

### Typ

Fortinet FortiGate

### Strona producenta

<http://www.fortinet.com>

### Recenzent

Grzegorz Błoński

### OCENA



## MAGICZNE PUDEŁKO, CZY SIŁA TECHNOLOGII?

Układ FortiASIC CP podczas przetwarzania zawartości plików jest wspierany przez drugi układ, oznaczony jako NP. Network Processor zajmuje się przyspieszaniem sesji niewymagających skanowania aplikacyjnego. Porty wyposażone w Network Processor działają z przepustowością kabla. Ma to ogromny wpływ na poprawę wydajności sieci.

NP to także firewall o bardzo wysokiej wydajności z akceleracją szyfrowania dla protokołu IPSec, obsługą domen wirtualnych, QoS oraz kształtowaniem ruchu.

Biorąc pod uwagę fakt, iż układy FortiASIC nowej generacji wspomagają wykrywanie zagrożeń aż w pięciu warstwach sieci według modelu ISO/OSI (od warstwy 3 do 7, co widać na Rysunku 1), FortiASIC Network Processor może podnosić przepustowość sieci między innymi:

- dla ruchu z małymi pakietami danych, na przykład VoIP,
- dla ruchu wrażliwego na opóźnienia, takiego jak przesyłanie strumieni multimedialnych,
- dla ruchu z bardzo długimi sesjami, na przykład FTP,
- dla ruchu IPSec VPN,
- dla ruchu P2P.

Właściwy dla przetwarzania przez FortiASIC ruch jest kierowany właśnie do niego, a pozostały ruch przetwarzany jest przez główny procesor urządzenia FG-310B.

Urządzeniem możemy administrować poprzez dwa rodzaje interfejsów – pierwszy z nich (Web-Based) jest oparty o przeglądarkę internetową, drugi – bardziej tradycyjny – jest typowo konsolowy (CLI – ang. Command Line Interface). Obie metody administracji mają zbliżone możliwości, jednak należy zaznaczyć, że panel administracyjny w przeglądarce jest o wiele wygodniejszy w użytkowaniu, bardziej przejrzysty i czytelny praktycznie dla każdego. Dla większych wdrożeń producent sugeruje wykorzystanie dedykowanych do tego urządzeń FortiManager.

Ogólna zasada działania FortiASIC-CP pokazana jest na Rysunku 2.

Teraz pora na kilka słów o fizyczności urządzenia, które widać na Rysunku 3. Rozmiar 1U powoduje, że urządzenie świetnie nadaje się do montażu w szafach typu Rack – po dokładne rozmiary odsyłam na stronę producenta. Spośród 10 portów wbudowanego w urządzenie koncentratora tylko 8 jest obsługiwanych przez FortiASIC-NP.

Porty USB mogą służyć między innymi do wykonywania kopii zapasowych firmware urządzenia lub do też podłączenia modemu jako łącza zapasowego. Istnieje także możliwość podłączenia modułu AMC – tylko jednego, jednak w przypadku urządzenia tej klasy jest to zupełnie wystarczające. Karty AMC (ang. Advanced Mezzanine Card) mogą obsługiwać cztery dodatkowe porty

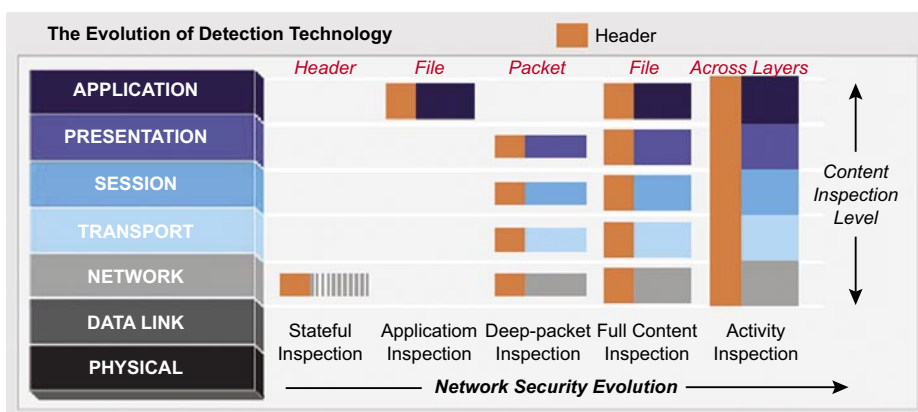
Gigabit Ethernet lub dysk twardy o pojemności 80 GB.

Widać więc, że urządzenie można łatwo rozbudować, poszerzając jego możliwości.

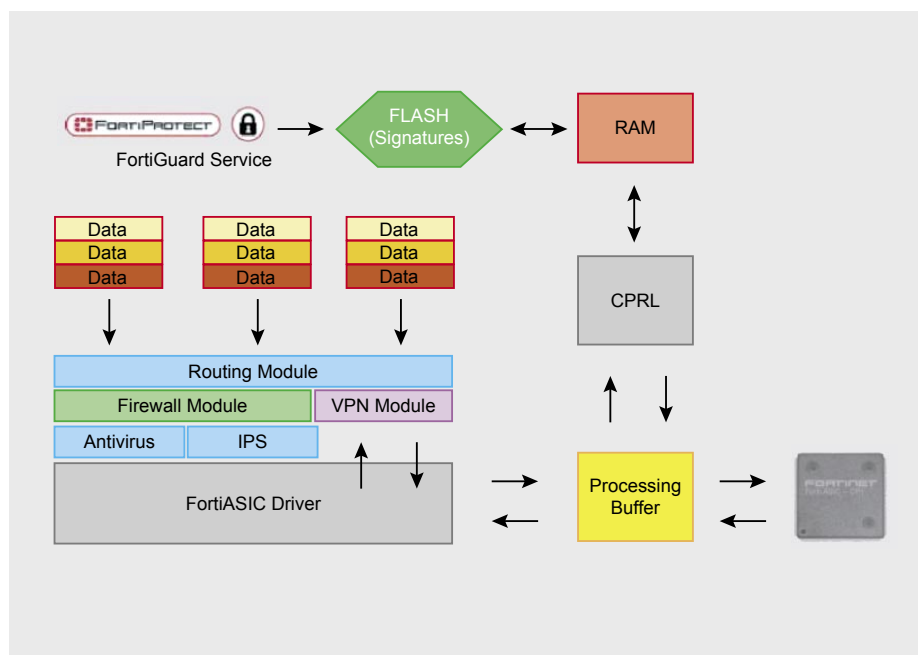
Możliwość skonfigurowania urządzenia do pracy w trybie wysokiej dostępności (HA) pozwala na budowanie klastrów opartych o takie urządzenia.

Urządzenie podczas pracy emituje hałas na pewnym poziomie, który jest spowodowany pracą układów chłodzenia. Muszą one zapewniać odpowiednią temperaturę pracy układów nawet przy maksymalnym obciążeniu urządzenia.

FG-310B może pracować jako typowy router, zapewniający translację adresów w trybie NAT/Route oraz w trybie transparent, w którym jest



Rysunek 1. FortiASIC działa aż na 5 warstwach modelu ISO/OSI



Rysunek 2. FortiASIC-CP – zasada działania

# NARZĘDZIA

niewidoczny w sieci. Tryb pracy urządzenia nie ma wpływu na jego wydajność i nie utrudnia w żaden sposób komunikacji. Użytkownicy sieci nie odczuwają żadnych problemów związanych z jego pracą. Wraz z urządzeniem dostarczane jest oprogramowanie klienckie – FortiClient.

Stanowi ono uzupełnienie sprzętowej ochrony sieci o program pozwalający na bardzo elastyczne konfigurowanie polityki bezpieczeństwa na pojedynczym komputerze.

Na Rysunku 4. prezentującym konsolę zarządzania, widać mnogość zakładek oraz opcji, na które może mieć wpływ użytkownik tego oprogramowania. Połączenie programu antywirusowego, antyspamowego, osobistego firewalla, filtra treści stron WWW z mechanizmem szyfrowania sieci VPN pozwala na dużo wygodniejsze zarządzanie bezpieczeństwem.

FG-310B obsługuje nielimitowaną ilość użytkowników. Urządzenie ma sporo zalet, które należałoby podkreślić:

- pełny system narzędzi umożliwi sprawne zarządzanie bezpieczeństwem,
- kompleksowa ochrona zasobów powoduje obniżenie kosztów ich utrzymania,
- duży wachlarz modeli urządzeń umożliwi dobranie właściwego rozwiązania dla swoich potrzeb,
- nowoczesna technologia ASIC zapewnia ochronę zasobów bez utraty wysokiej przepustowości,
- autorskie technologie dają pewność obsługi i gwarancję użytych zabezpieczeń,
- duża wydajność urządzeń zapewni obsługę największych sieci telekomunikacyjnych,
- obsługa całej gamy protokołów

- sieciowych pozwala na realizację dodatkowych usług,
- spójny, pojedynczy interfejs zarządzania ułatwia administrację systemem,
- tryb transparentny ułatwia testy i implementację w istniejącej sieci bez narażania na przerwy w dostępie do usług sieciowych,
- zintegrowanie wielu funkcji w jednym urządzeniu upraszcza strukturę całej sieci.

To konkretne rozwiązanie FG-310B pozwala na realizację wielu funkcji ochronnych w jednym urządzeniu, ochronę informacji w czasie rzeczywistym i budowę wysokowydajnych systemów bezpieczeństwa nowej generacji. Systemy Fortinet skutecznie ochronią przesyłane w sieci i przez Internet informacje oraz pozwolą na sprawne zarządzanie bezpieczeństwem IT.

Dodatkowym faktem potwierdzającym przydatność takich rozwiązań są certyfikaty przyznawane firmie. Jednym z najbardziej cenionych certyfikatów jest Common Criteria EAL4+ (<http://www.cse-cst.gc.ca>) – reprezentujący najwyższy w branży bezpieczeństwa IT poziom certyfikatu.

Tych certyfikatów i firma, i urządzenie otrzymały znacznie więcej – zainteresowanych szczegółami odsyłam na stronę producenta.

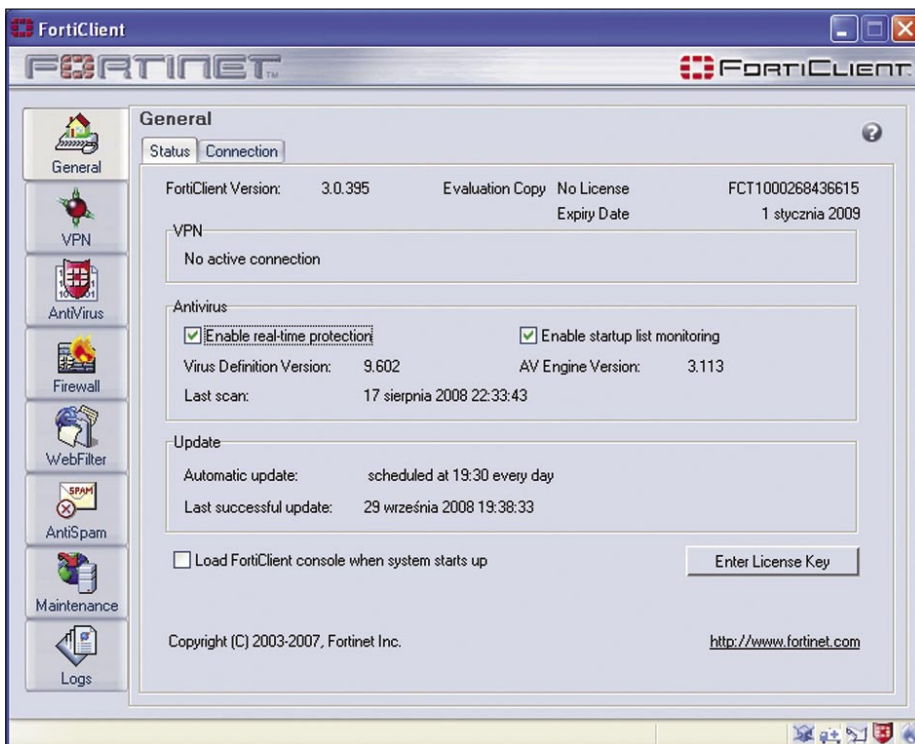
Podsumowując w kilku słowach całokształt możliwości oferowanych przez FG-310B, spokojnie można użyć stwierdzenia, iż pudełeczko jest magiczne – jednak dzieje się to za sprawą upakowanej w jego wnętrzu technologii.

Można odnieść wrażenie, że to wręcz niemożliwe, iż wszystkie opisane rozwiązania mieszczą się w tak małym urządzeniu.

Rozwiązania tej klasy powinny znaleźć się w sferach zainteresowania (ale nie tylko) firm pragnących za sprawą jednego urządzenia znacznie podnieść poziom bezpieczeństwa sieciowego we własnej firmie, przy jednoczesnym zapewnieniu łatwości zarządzania zasobami sieci oraz możliwości szybkiego reagowania na incydenty.



Rysunek 3. Wygląd urządzenia Fortinet FG 310-B



Rysunek 4. Interfejs zarządzania zabezpieczeniem hostów - FortiClient