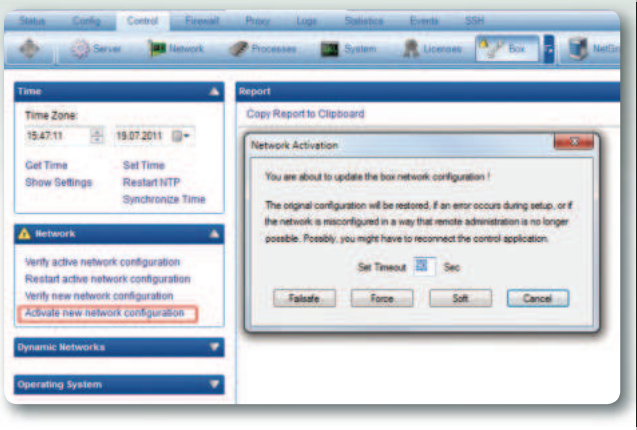
Barracuda NG Firewall F400 – test

W bogatej ofercie Barracuda Networks znajduje się m.in. rodzina urządzeń i maszyn wirtualnych Barracuda NG Firewall zaprojektowanych jako zapora następnej generacji (Next Generation) przeznaczona dla różnej wielkości przedsiębiorstw z jedną lokalizacją, jednak pełnię swoich możliwości osiąga dopiero przy wdrożeniach korporacyjnych, gdzie trzeba zadbać o połączenia i odpowiedni poziom bezpieczeństwa między odległymi oddziałami.

Jarosław Kowalski

Urządzenia zapewniające bezpieczeństwo przesyłanych danych i dostępu do zasobów sieciowych to obecnie nieodzowny element każdej infrastruktury. Nie sposób wyobrazić sobie firmowe środowisko IT, które nie byłoby, choćby w minimalnym stopniu, zabezpieczone. Nowoczesne rozwiązania tego rodzaju zawierają nie tylko funkcjonalności zapory sieciowej, ale ich zaawansowane opcje pozwalają również dokładnie określić, jaki ruch sieciowy powinien być dozwolony, a jaki zablokowany. Bez problemu potrafią rozpoznać użytkownika i aplikacje uzyskujące dostęp do sieci, aby odpowiednio zareagować według zdefiniowanych zasad.

Obecnie producenci rozwiązań zabezpieczających mają na uwadze przede wszystkim globalizację przedsiębiorstw, których oddziały niejednokrotnie znajdują się w odległych lokalizacjach, dlatego oferują urządzenia na różnym poziomie funkcjonalności i wydajności, dostosowane do potrzeb infrastruktury, w której są wdrażane. Jednym z producentów kompleksowych rozwiązań z zakresu zabezpieczeń infrastruktury i sieci jest Barracuda Networks. Dzięki swoim produktom obejmującym między innymi bezpieczeństwo sieci, poczty elektronicznej i danych, a także urządzenia filtrujące treści przetwarzane w chmurze, firma ta stała się liderem w dziedzinie urządzeń tego segmentu. Oferta Barracuda Networks jest skierowana do niewielkich firm oraz dużych korporacji, które łączy wspólna świadomość zagrożeń wynikających z przetwarzania danych oraz korzystania z sieci. Wachlarz funkcjonalny i wydajnościowy oferowanych urządzeń NG Firewall pozwala na zastosowanie nawet w bardzo małych lokalizacjach czy domowych biurach, a także w dużych centralach firm.



Activate New Network.

Barracuda NG Firewall jest rozwiązaniem, które umożliwia łatwą segmentację sieci oraz kontrolę dostępu, ochronę przed włamaniami, wirusami i spamem oraz filtrowanie WEB. Jednak na szczególne wyróżnienie zasługują funkcjonalności, które powodują, że Barracuda NG Firewall staje się prawdziwym kombajnem bezpieczeństwa sieciowego.

Zaawansowany **filtr aplikacyjny** pozwala na skuteczne egzekwowanie reguł bezpieczeństwa dzięki integracji w rdzeń silnika firewalla dla kontroli aplikacji warstwy 7. Barracuda NG Firewall identyfikuje i stosuje złożone reguły bezpieczeństwa nawet w skomplikowanych aplikacjach, które niejednokrotnie potrafią maskować swój ruch sieciowy w innych protokołach (np. http). Filtr aplikacyjny bez problemu potrafi kontrolować wszelkiego rodzaju komunikatory internetowe oraz aplikacje P2P. Warto

zaznaczyć, że przy definiowaniu reguł aplikacyjnych można sterować dostępem do poszczególnych funkcji oferowanych przy korzystaniu z danego serwisu. Wskazać tu można choćby blokadę pojedynczych funkcji portali społecznościowych, jak na przykład możliwości komentowania, przeglądania zdjęć lub filmów.

Barracuda NG Firewall wyróżnia się podejściem do realizacji bezpiecznych połączeń VPN. Można na nim skonfigurować tunelowanie w konfiguracji *Client-to-site* lub *Site-to-site* zapewniając bezpieczną, szyfrowaną komunikację za pośrednictwem internetu. Bez względu na model Barracuda NG Firewall dostępna jest nieograniczona liczba licencji dla klientów VPN. Jednak w tej usłudze wart uwagi jest fakt, że do realizacji tunelowania VPN zaimplementowano autorski protokół **TINA**.

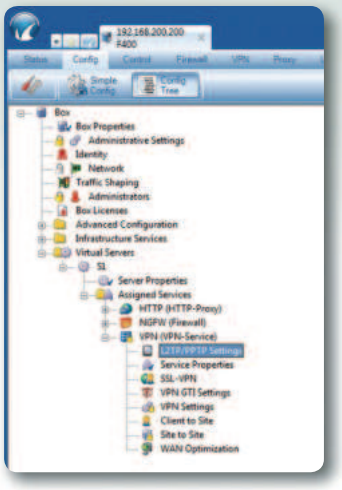
W odróżnieniu od technologii IPSEC, w której zestawiany jest dla każdego z łączy osobny tunel VPN, w TINIE w jednym dużym tunelu zestawianych jest wiele osobnych połączeń VPN. Dzięki temu w przypadku przerwania jednego z nich przy wykorzystaniu technologii Traffic Intelligence połączenie zostanie automatycznie przełączone na inny tunel bez strat w ruchu sieciowym. Przy użyciu technologii TINA w pojedynczym dużym tunelu może funkcjonować do 24 transportów (tunele wewnętrzne). Do budowania bezpiecznych połączeń między poszczególnymi lokalizacjami wykorzystuje się intuicyjne i proste w obsłudze narzędzie Graficzny Edytor Konfiguracji (GTI). Jest to unikalna funkcja zawarta w Barracuda NG Firewall, dzięki której zestawianie tuneli odbywa się za pomocą metody przeciągnij i upuść.

Reguły bezpieczeństwa wykorzystywane w Barracuda NG Firewall oprócz wskazania na aplikacje czy konkretne protokoły mogą być oparte na ID użytkownika, jego przynależności do określonych grup, lokalizacji oraz określeniu godzin dostępu do zasobów w czasie pracy biura. Dzięki temu istnieje pełna kontrola nad dostępem użytkowników i aplikacji do infrastruktury oraz internetu.

TESTOWANIE

Do redakcyjnych testów trafił model ze średniej półki, a mianowicie rozwiązanie sprzętowe Barracuda NG Firewall F400. Zanim urządzenie do nas dotarło, odbyliśmy krótką prezentację na temat funkcjonalności oraz możliwości konfiguracyjnych NG Firewall. Od samego początku można było zauważyć, że jest to rozwiązanie dość zaawansowane funkcjonalnie, a jego wdrożenie i konfiguracja nie należy do najłatwiejszych.

Model F400 jest urządzeniem o wysokości 1U przeznaczonym do montażu w szafie rackowej. Standardowo wyposażony jest w 8 portów Gigabit Ethernet, z których jeden standardowo przeznaczony jest do zarządzania. Na przednim panelu urządzenia umieszczono wszystkie gniazda Ethernet, dodatkowo port konsolowy oraz dwa porty USB do opcjonalnego użycia modemu 3G oraz wyświetlacz informacyjny, dzięki czemu możliwy jest łatwy dostęp do wszystkich złączy po jednej stronie.



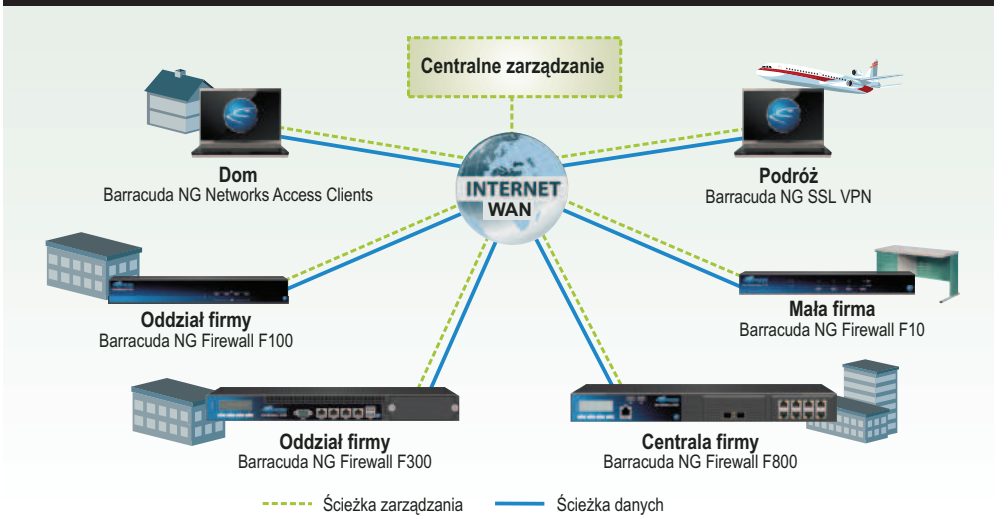
Drzewo ustawień w trybie advanced config.

Przed uruchomieniem postanowiliśmy zapoznać się z dokumentacją techniczną, a przede wszystkim znaleźć dokumenty niezbędne do podstawowego uruchomienia urządzenia. Firma Barracuda Networks na swoich stronach wykazuje pełną dokumentacje techniczną serii NG Firewall. Podstawowe informacje i instrukcje dostępne są jako pliki PDF, natomiast dodatkowe, zaawansowane informacje jako materiały online w bibliotece technicznej.

Pierwszego uruchomienia dokonaliśmy w naszym pokoju redakcyjnym. Jednak dość głośna praca urządzenia zmusiła nas do przeniesienia go w docelowe miejsce, czyli serwerowni. Tam się okazało, że wśród kilkunastu serwerów NG Firewall F400 wyróżnia się poziomem emitowanego hałasu.

Do połączenia z urządzeniem, administracji i konfiguracji wykorzystuje się aplikację **NG Admin**, którą można

Zastosowanie urządzeń Barracudy w różnych typach sieci



uruchomić bez instalacji bezpośrednio z pliku exe. Po użyciu domyślnych wartości i zatwierdzeniu klucza certyfikatu zestawiane jest połączenie szyfrowane z urządzeniem. W podstawowym oknie, po logowaniu, udostępnione są najważniejsze informacje i parametry pracy systemu. Pierwsze logowanie uruchamia również łatwy w obsłudze i intuicyjny kreator konfiguracji, jednak zrezygnowaliśmy z niego na rzecz ręcznego wprowadzania ustawień.

Na szczęście konfiguracja poszczególnych funkcjonalności jest bardzo dobrze i z najdrobniejszymi szczegółami opisana w dokumentacji technicznej, a ponadto na bieżąco w każdym oknie konfiguracyjnym wyświetlana jest legenda opisująca wyświetlane opcje, co jest niezmiernie pomocne w przypadku wątpliwości, czego dotyczy modyfikowane ustawienie. Dlatego też bez większych problemów udało nam się uruchomić funkcje routera, podstawowy *firewall*, *proxy* oraz serwer VPN. Chcąc włączyć i skonfigurować poszczególne funkcjonalności Barracuda NG Firewall, należy najpierw utworzyć wirtualny serwer, który będzie świadczył te usługi i dopiero na nim dokonywać właściwej konfiguracji. Jest to bardzo dobre rozwiązanie, szczególnie przy planowaniu uruchomienia High Availability, gdyż wirtualizacja usług pozwala szybko i bezstratnie przełączać ruch pomiędzy urządzeniami w klastrze.

Okno aplikacji jest podzielone na kilka funkcjonalnych części, dzięki czemu można łatwo odnaleźć interesujący obszar ustawień bądź informacji. Samą konfigurację można przeprowadzać w dwóch trybach – prostym, gdzie znajdujemy funkcje pod postacią ikonek z opisem, które wybiera się z głównego okna lub aktywując tryb zaawansowany, co przełącza całe menu konfiguracyjne do postaci drzewa. Wbrew pozorom zaawansowany widok drzewa wydaje się być bardziej intuicyjny od prostego, dzięki czemu łatwo rozwinąć odpowiednią gałąź i znaleźć interesujące nas ustawienie.

Aplikację NG Admin można wykorzystać do połączenia z wieloma urządzeniami NG Firewall jednocześnie, co sposobuje otwieranie się ustawień każdego z nich w osobnej zakładce na górze okna aplikacji. Natomiast gdybyśmy chcieli scentralizować zarządzanie NG Firewall w odległych lokalizacjach, należałoby skorzystać z **Barracuda NG Control Center**, które jest instalowane jako dodatkowe urządzenie bądź wirtualny *appliance*. Dzięki temu rozwiązaniu można w łatwy sposób kontrolować kilka bądź nawet kilka tysięcy lokalizacji. Wart uwagi jest fakt, że dzięki tej centralnej konsoli zarządzania możemy wykonywać pewne czynności jednokrotnie, a następnie dystrybuować je do wszystkich lub wybranych urządzeń Barracuda NG Firewall. Jako że wszystkie rozwiązania NG Firewall zawierają zaawansowane opcje logowania i raportowania, to wykorzystanie do przeglądania tych zasobów NG Control Center pozwala zebrać informacje na temat kondycji infrastruktury oraz raportów o stanie systemu w jednym miejscu.

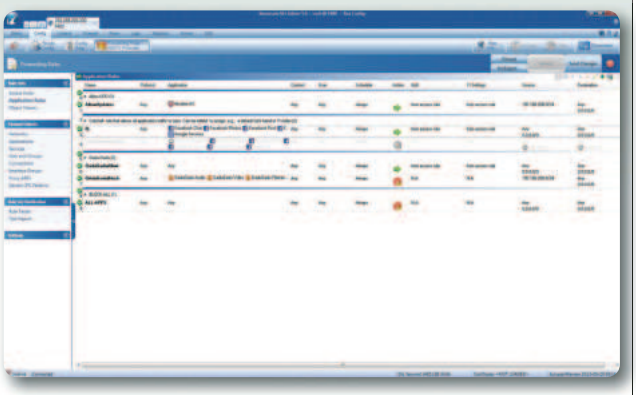
W czasie testów postanowiliśmy wziąć na warsztat jedną z wyróżnionych funkcjonalności, czyli **filtr aplikacyjny**. Utworzyliśmy reguły, które określały poziom dostępu do popularnego serwisu społecznościowego. Bez problemu można było całkowicie zablokować korzystanie z niego, ale dzięki zaawansowanym filtrom da się również wyłączyć możliwość korzystania tylko z części funkcjonalności (w naszym przypadku dostępu do materiałów wideo). Później dodatkowo wyłączyliśmy możliwość korzystania z czatu, przeglądania zdjęć czy komentowania wpisów innych użytkowników. Wykorzystując dostępne opcje bez problemu da się ustawić dostęp na poziomie *read only*.

Reguły, jakie można zdefiniować w Barracuda NG Firewall pozwalają na niezwykle zaawansowane sterowanie dostępem do zasobów sieci bądź internetu, a obszerna baza zdefiniowanych obiektów pozwala łatwo odnaleźć właściwą usługę, protokół czy zasób, który chcemy wykorzystać do realizacji polityki bezpieczeństwa. Oczywiście, na potrzeby konkretnego środowiska administratorzy mogą definiować własny zbiór obiektów wykorzystywanych później w regułach dostępowych.

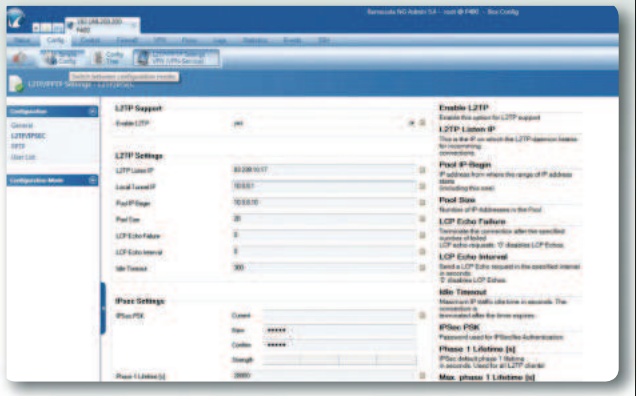
Chcąc skorzystać z bazy gotowych obiektów i sprawdzić skuteczność zdefiniowanych filtrów, uruchomiliśmy regułę blokującą zasoby sieciowe zlokalizowane w wybranym kraju. Wybór padł na Francję, po czym potwierdziliśmy poprawne działanie uruchomionego filtra, gdyż nie udało się otworzyć żadnej strony zlokalizowanej na serwerach tego kraju.

Wszelkie zmiany, czy to w zakresie konfiguracji samego urzą-

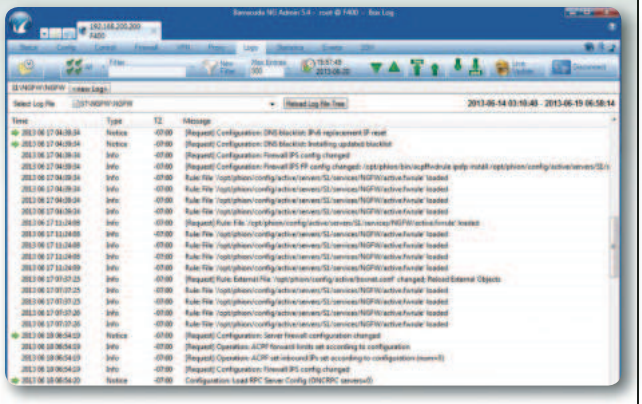
Barracuda NG Firewall F300.



Filtr aplikacyjny.



Konfiguracja serwera VPN.



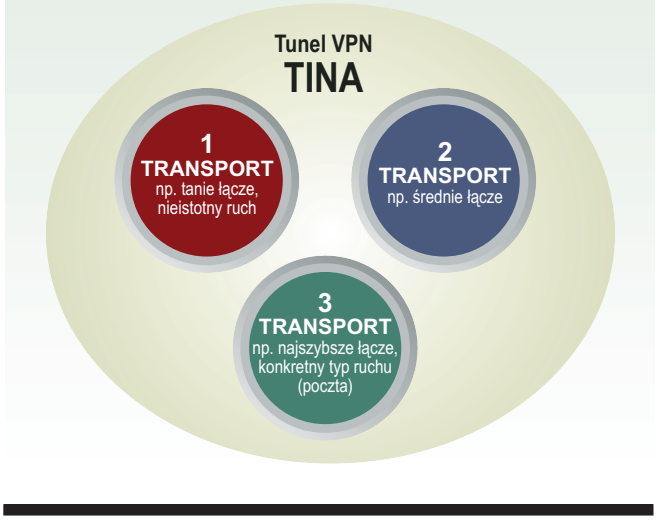
Podgląd logów NG Firewall.

dzenia, czy zapory wymagają od administratora odblokowania możliwości wprowadzania zmian (przejście w tryb Unlock), co ma na celu uniknięcie przypadkowych zmian. Następnie taką konfigurację należy „wysłać do urządzenia" oraz aktywować. Przed wprowadzeniem zmian administrator jest pytany o tryb wprowadzenia zmian. Tutaj istnieje wybór pomiędzy całkowitym, natychmiastowym zatwierdzeniem i uruchomieniem zmian oraz bezpiecznym „failsafe", gdzie w przypadku błędnej konfiguracji i zablokowaniu sobie możliwości pracy, po określonym czasie urządzenie robi krok wstecz i odwołuje zmiany (można to porównać do zmiany rozdzielczości w systemach Windows. Gdy ustawimy nieobsługiwany tryb i nie zatwierdzimy go po zmianach, po pewnym czasie następuje powrót do pierwotnych ustawień).

Obok urządzenia fizycznego udało nam się również uruchomić wirtualną wersję Barracuda NG Firewall. Włączenie rozwiązania w tej postaci jest niezwykle proste i sprowadza się do ściągnięcia odpowiedniego pliku maszyny wirtualnej (wspierane platformy to Citrix i VMware), a po uruchomieniu należy tylko w konsoli określić adresację IP do zarządzania, po czym można połączyć się aplikacją NG Admin i wykonać bardziej zaawansowaną konfigurację.

Z uwagi na to, że konfiguracja jednej z flagowych funkcjonalności Barracuda NG Firewall, autorskiego protokołu VPN wymagała zaawansowanej wiedzy administracyjnej wsparliśmy się doświadczeniem technika na co dzień wdrażającego rozwiązania firmy Barracuda Networks. Pokazał on, jak za pomocą NG Control Center skonfigurować oraz zestawiać połączenia VPN.

Idea działania protokołu VPN TINA

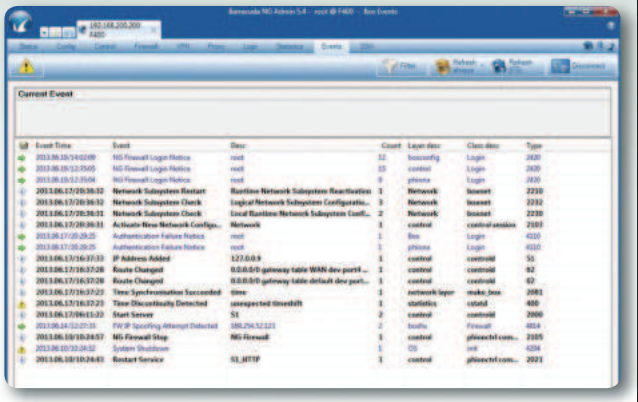


Po skonfigurowaniu odpowiednich opcji uruchamiających usługę VPN należy jedynie – korzystając z interfejsu graficznego (GTI) i mapy lokalizacji urządzeń – zestawić tunel przeciągając kursor myszy między wybranymi obiektami.

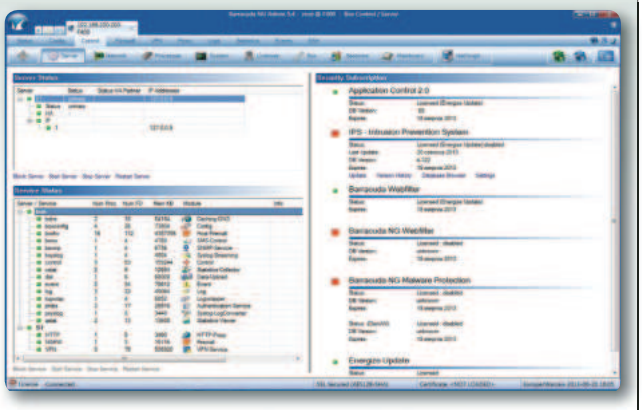
Oczywiście rozwiązania tej klasy wspierają także konfiguracje niezawodnościowe. Począwszy od możliwości wykorzystania modemów 3G do zapewnienia redundancji łącza, po konfiguracje klastrowe wielu urządzeń. Jednak taka funkcjonalność jest obostrzona pewnymi warunkami. Nie da się wykonać konfiguracji HA między rozwiązaniem wirtualnym oraz rozwiązaniem sprzętowym, a także między dwoma różnymi modelami urządzeń fizycznych (np. F100 i F200)

PODSUMOWANIE

Barracuda NG firewall jest z pewnością rozwiązaniem godnym polecenia. Zaawansowane opcje pozwalają dostosować reguły pracy do niemal każdego środowiska. Natomiast pełny wachlarz wersji sprawia, że mogą sobie na niego pozwolić również mniejsze przedsiębiorstwa. Szczególnie warto zwrócić uwagę na to rozwiązanie ze względu na wyróżniające je funkcjonalności (autorski VPN, filtr aplikacyjny czy inspekcję SSL) oraz na unikalne podejście do centralnego zarządzania, które ma na celu minimalizację nakładu pracy administratorów, a co za tym idzie – zmniejszenie kosztów zatrudnienia technika w każdej placówce, gdzie zainstalowany jest NG Firewall. Zaawansowane funkcje urządzenia idą w parze z liczbą opcji, które ze względu na ich mnogość niejednokrotnie trudno odszukać.



Podgląd zdarzeń w aplikacji NG Admin.



Status serwera wirtualnego.

Dlatego aby skrócić czas wdrożenia i docelowej konfiguracji, należałoby odbyć szkolenie w zakresie obsługi i konfiguracji Barracuda NG firewall, a dodatkowo już na starcie posiadać odpowiednią wiedzę z zakresu usług i protokołów sieciowych. Na pewno nie jest to urządzenie do samodzielnej konfiguracji przez administratorów, którzy takiej wiedzy nie mają mimo tego, że nic nie możemy zarzucić udostępnionej przez producenta dokumentacji technicznej.

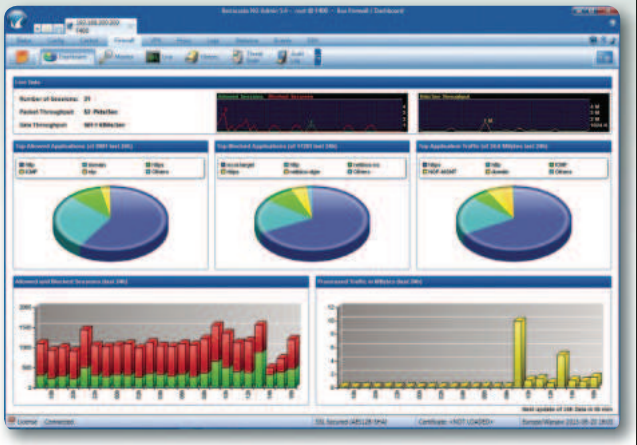
Jedynym minusem, jaki udało nam się zaobserwować, jest niezwykle głośna praca urządzenia fizycznego.

Jeśli chodzi o wsparcie oraz ceny, to każdy klient kupujący rozwiązanie Barracuda NG firewall musi jednocześnie wykupić przynajmniej na rok serwis **Energize Updates**, który na tym poziomie zapewnia subskrypcję aktualizacji, dostęp do najnowszych wersji firmware, wsparcie e-mailowe producenta i dystrybutora oraz wsparcie telefoniczne 5 dni roboczych w tygodniu. Do tego każde urządzenie objęte jest roczną gwarancją producenta. Pozostałe dostępne poziomy serwisowe to **Instant Replacement** (przedłuża gwarancję, przyspiesza wymianę uszkodzonego urządzenia oraz zapewnia wsparcie techniczne 24/7) oraz **Premium Support**, który jest najwyższym poziomem serwisu i wsparcia technicznego z przydzielonym opiekunem prowadzącym zgłoszenia – wyceniane indywidualnie. Należy również wspomnieć, że między innymi ze względu na zaawansowanie funkcjonalne, poziom szyfrowania oraz autorskie rozwiązania Barracuda NG Firewall zostało zakwalifikowane jako urządzenie o znaczeniu strategicznym i może być wdrażane również przez instytucje wojskowe. Skutkuje to tym, że każdy zakup oraz testy (również w naszym przypadku) muszą zostać zgłoszone do Agencji Bezpieczeństwa Wewnętrznego.

Dodatkowym atutem w przypadku zakupu odpowiednich poziomów wsparcia jest możliwość wymiany urządzenia na nowe po czterech latach korzystania. Klient otrzymuje wtedy w ramach supportu nowy odpowiednik obecnie używanego rozwiązania. Jeśli chodzi o ceny, to testowany model (F400 rev. B) na obecnie kosztuje 4999 euro, dla porównania model Barracuda NG Firewall F10 to koszt 599 euro. Natomiast wsparcie techniczne na podstawowym poziomie to wydatek 899 euro dla F400 oraz 99 euro dla F10. Oczywiście wyższe poziomy wsparcia są odpowiednio droższe.

W odróżnieniu od bazowych funkcji dostępnych w cenie urządzenia, również dodatkowe moduły są licencjonowane oddzielnie. Zakup NG Malware Protection to wydatek rzędu 699 euro/rok, a SSL VPN i Network Access Control – 499 euro.

Jak widać, ceny kompletnego rozwiązania, do którego trzeba doliczyć NG Control Center w przypadku architektury rozproszonej, nie należą do najniższych, ale Barracuda NG Firewall bez względu na wersję i funkcjonalność warta swojej ceny, szczególnie obecnie, gdy skuteczna ochrona dostępu do danych i przepływu informacji jest tak trudna do utrzymania.



Statystyki firewalla.

Dodatkowe informacje:

- *www.barracuda.com*
- *www.barracuda.com.pl*