Test: Barracuda CloudGen Firewall F600 s. 49

Pester – testowanie kodu w PowerShellu s. 28

7
2018

Miesięcznik informatyków i menedżerów IT

www.it-professional.pl

IT professional

Nr 7 (80) lipiec 2018 — Cena 33,00 zł (w tym 5% VAT)

MONITOROWANIE – NAGIOS s. 10

Cele i korzyści monitoringu. Przegląd narzędzi do monitorowania infrastruktury sieciowo-serwerowej. Nagios jako standard open source do nadzorowania systemów IT przedsiębiorstwa – możliwości, podstawy wdrożenia, zalety wersji komercyjnej

s. 64

Ansible w służbie NOC

Automatyzacja zadań w centrach operacyjnych

s. 68

Konfiguracja serwera na potrzeby SQL Server

Optymalizacja sprzętu i systemu operacyjnego

s. 40

Cryptojacking – nowe cyberzagrożenie

Wykorzystywanie komputerów użytkowników do kopania kryptowalut

ISSN 2083-9588

Serwery ▪ Stacje robocze ▪ Bezpieczeństwo ▪ Infrastruktura i sieci ▪ Zarządzanie i prawo IT ▪ Techn

DOSTĘPNE E-WYDANIE

Przez redakcyjne laboratorium testowe przewinęło się już sporo różnego rodzaju zapór sieciowych, które mniej lub bardziej zasługiwały na dopisek NextGen w nazwie. Tym razem testujemy wydajnego firewalla amerykańskiej firmy Barracuda Networks.

7/2018 REKOMENDACJA REDAKCJI IT professional

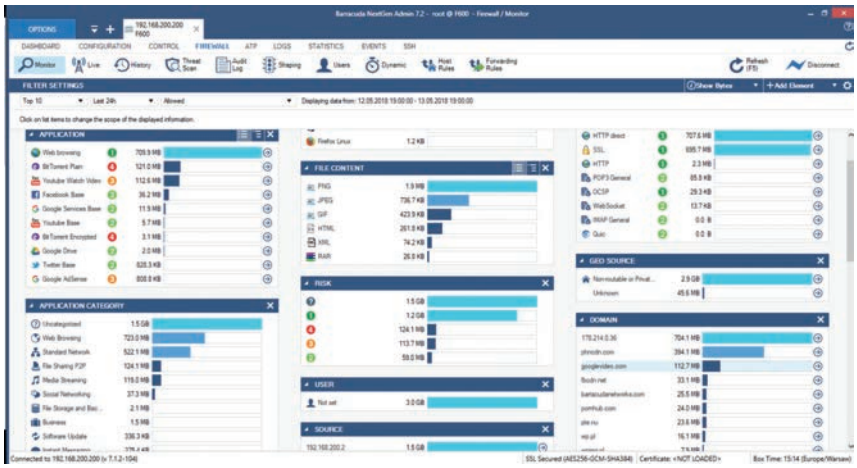
ZAPORY SIECIOWE NGFW

Barracuda CloudGen Firewall F600

Marcin Jurczyk

Przy każdej możliwej okazji podkreślamy, jak ważne jest bezpieczeństwo infrastruktury sieciowo-serwerowej każdego przedsiębiorstwa. W momencie publikacji tekstu odmieniane ostatnio przez wszystkie przypadki GDPR i rodo będą już aktem obowiązującym, a wzmożoną aktywność we wszystkich obszarach związanych z zapewnieniem bezpieczeństwa, nie tylko dotyczących danych osobowych, zauważył na pewno każdy. Na przestrzeni ostatniego dziesięciolecia dostarczane zapory sieciowe ewoluowały i poza prostym filtrowaniem ruchu w oparciu o 3 i 4 warstwę modelu OSI, potrafią także kontrolować ruch sieciowy na podstawie warstw wyższych, aż do poziomu warstwy aplikacji włącznie. Obecnie sprzedawane firewalle to najczęściej wielozadaniowe kombajny, będące w stanie filtrować strumień danych w oparciu o wiele czynników, a poszczególni producenci prześcigają się w liczbie mechanizmów bezpieczeństwa, które mogą zaoferować w ramach pojedynczego produktu.

Barracuda Networks to amerykańska firma z branży zabezpieczeń IT, w której ofercie widać wyraźny podział na produkty zabezpieczające sieci, aplikacje sieciowe oraz chroniące pocztę e-mail i przetwarzane dane. Dotychczas dwukrotnie testowaliśmy rozwiązania tej firmy – w numerze 09/2013 „IT Professional" sprawdzaliśmy możliwości modeli zapór F10 oraz F400, a w numerze 12/2014 przyjrzeliśmy się rozwiązaniu do zarządzania kopiami zapasowymi Barracuda Backup. Od tamtej pory minęło już kilka lat, co w świecie IT nierzadko oznacza epokę. Pora więc zobaczyć, co poza nową nazwą linii rozwiązań oferuje Barracuda. Zwłaszcza że nazwa wygląda intrygująco – czyżby określenie CloudGen miało być następcą utartej marketingowo nazwy grupy urządzeń NextGen Firewall?

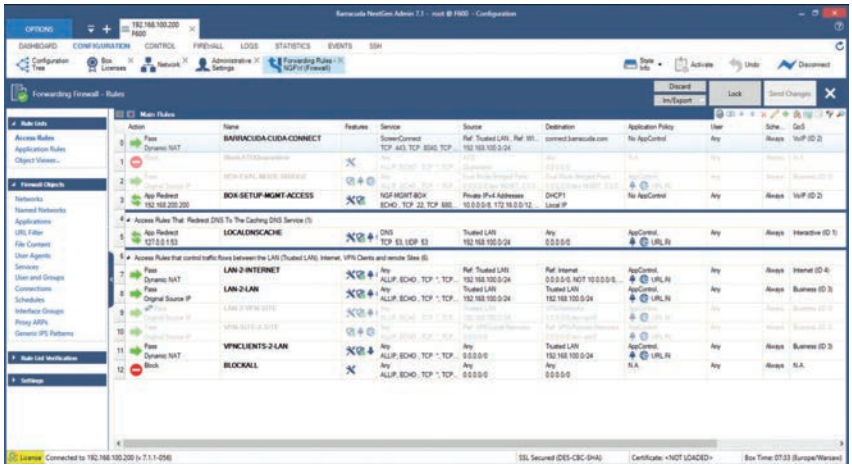


W nowoczesnym i rozbudowanym funkcjonalnie urządzeniu nie mogło zabraknąć statystyk firewalla.

> HARDWARE

W zależności od tego, czy mamy do czynienia z tradycyjnym środowiskiem IT, czy też dowolną wersją chmury obliczeniowej oraz zmianami związanymi z miejscem i sposobem filtrowania ruchu sieciowego, Barracuda Networks zastąpiła nazwę całej grupy produktów realizujących funkcję zapory ogniowej. W praktyce zamiana z NextGen Firewall na CloudGen Firewall nie oznacza żadnej rewolucji,

a sam producent w opisie produktu mówi o „firewallach następnej generacji w erze przetwarzania w chmurze". Zmiana łączy się głównie ze sposobem wdrażania tej grupy produktów i coraz bardziej rozproszoną charakterystyką infrastruktur firmowych, które należy chronić. Na potrzeby testu otrzymaliśmy tradycyjny, sprzętowy firewall ze średniej półki, oznaczony symbolem F600. Poza rozwiązaniem typu appliance dostępne są również odpowiednio licencjonowane wersje maszyn wirtualnych, a także predefiniowane, gotowe do natychmiastowego wdrożenia instancje w ramach katalogu usług dla chmur obliczeniowych AWS, Azure oraz Google Cloud Platform.



Standardowa struktura i logika budowania listy reguł firewalla.

W przypadku modelu F600 istnieje kilka dostępnych wersji, różniących się liczbą i rodzajem portów sieciowych, zasilaniem oraz wydajnością. Testowany model to wersja E20 będąca najbardziej wydajnym modelem. Urządzenie zamknięte w metalowej obudowie o wysokości 1U przeznaczonej do instalacji w szafie rack wyposażono w 8 miedzianych portów 1 GbE oraz 2 gniazda na wkładki SFP+ 10 GbE. Dwa niezależne zasilacze wewnętrzne o mocy 300 W odpowiadają za redundancję zasilania, a wbudowany na przedniej ścianie obudowy wyświetlacz LCD wraz z 4 przyciskami pozwala na podgląd podstawowych informacji o urządzeniu oraz funkcje typu wyłączenie czy restart urządzenia. Dodatkowo z przodu obudowy znajdziemy dedykowany port RJ45 konsoli, a także 2 porty USB 2.0 (zewnętrzna pamięć flash lub modem). Producent nie chwali się wprost, z jakiego CPU korzysta. Pamięć operacyjna na poziomie 8 GB oraz wewnętrzny dysk SSD o pojemności 270 GB to jedyne parametry, jakie znajdziemy w oficjalnej specyfikacji urządzenia. Całość pozwala na pracę w trybie firewall z przepustowością 20 Gb/s (ruch UDP 1500 bajtów pomiędzy wieloma portami). W trybie IPS przepustowość spada do 8 Gb/s, a dla NGFW (IPS, kontrola aplikacji i filtr URL) do 6,4 Gb/s. Dodatkowe uruchomienie funkcji antywirusa spowolni dodatkowo F600 do 5,8 Gb/s, co oznacza 70% spadek wydajności przy maksymalnej ochronie sieci. To sporo. Producent deklaruje maksymalną liczbę otwartych sesji na poziomie 2,1 mln przy 115 000 nowych sesji na sekundę. Parametry wydajnościowe plasują model F600 jako rozwiązanie dla klientów średniej wielkości, a także większych firm. W zależności od charakterystyki ruchu sieciowego przyjmuje się, że liczba chronionych

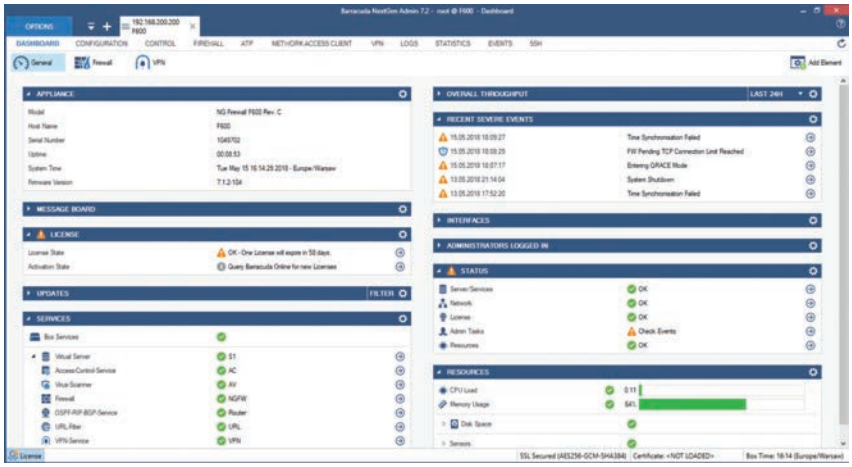
Ważną funkcją dostępną tylko w rozwiązaniach Barracuda Networks, na którą warto zwrócić uwagę, jest TINA (Transport Independent Network Architecture) VPN – autorskie rozszerzenie standardu IPSec o funkcje podnoszące kontrolę nad tunelami VPN, niezawodność i stabilność transmisji.

użytkowników mieści się w zakresie 1000–4000. Zapory fizyczne można oczywiście łączyć w klaster HA w celu podniesienia dostępności usługi.

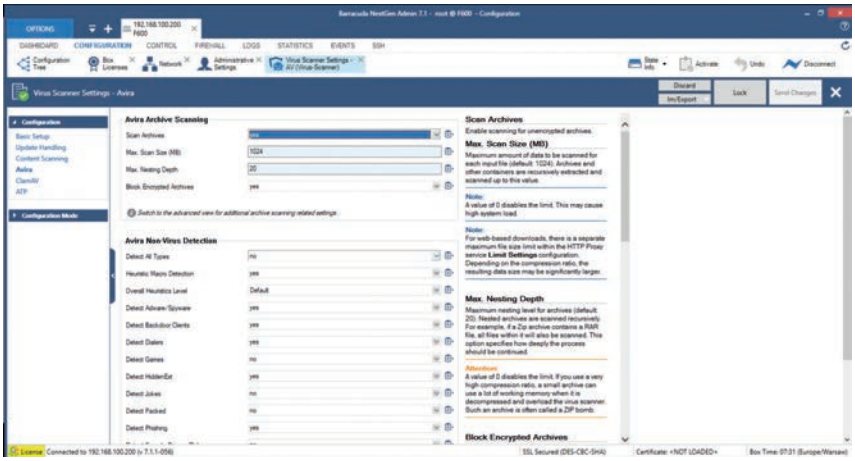
> BEZPIECZEŃSTWO W KILKU WERSJACH

Cała seria produktów CloudGen Firewall włącznie z testowanym modelem F600 zapewnia cały szereg mechanizmów bezpieczeństwa charakterystycznych dla tej klasy produktów. Zapora sieciowa, IPS, filtrowanie treści webowych, inspekcja aplikacji czy ochrona antywirusowa i antyspamowa to główne elementy ochrony sieci. Ponadto nie mogło również zabraknąć wsparcia dla bezpiecznych połączeń VPN site-to-site oraz client-to-site z wykorzystaniem najpopularniejszych protokołów oraz autorskiej implementacji IPSec – TINA. Firewalle Barracudy zapewniają także sporo dodatkowych funkcji, jak chociażby inteligentne zarządzanie ruchem czy optymalizacja WAN. Dostępnych mechanizmów ochrony jest całkiem sporo, ale niektóry z nich wymagają dodatkowej, płatnej subskrypcji.

Jedną z płatnych usług jest m.in. Advanced Threat Protection. Mechanizm ten chroni przed zagrożeniami typu malware, ransomware i 0-day, który są w stanie przedostać się przez filtry oparte na sygnaturach, takie jak chociażby IPS czy antywirus. Zasada działania, podobnie jak u konkurencji, bazuje na środowisku piaskownicy (sandbox) zlokalizowanej w chmurze producenta. Identyfikacja potencjalnie groźnych plików odbywa się dzięki porównaniu skrótu pliku z danymi w bazie, zawierającej informacje o już przeanalizowanych obiektach. Pliki, dla których skrót nie istnieje, przesyłane są do chmury, gdzie poddawane są analizie behawioralnej w pełni symulowanym środowisku, dzięki czemu możliwa jest identyfikacja nowych zagrożeń i zaawansowanych ataków ukierunkowanych. ATP wykorzystuje także wbudowany w firewall mechanizm inspekcji ruchu SSL, dzięki czemu pliki przesyłane szyfrowanym kanałem również mogą podlegać zaawansowanej analizie. Administrator ma możliwość zdefiniowania odpowiedniej polityki dla poszczególnych typów plików, w tym także może zdecydować o sposobie dostarczenia pliku do urządzenia końcowego (z wykorzystaniem kwarantanny lub natychmiast, bez czekania na wynik działania ATP). ATP to opcjonalny pakiet dostępny w formie rocznej, 3- lub 5-letniej subskrypcji. W przypadku testowanego modelu F600 licencja obejmuje sprawdzenie maksymalnie 540 tys. plików w ciągu miesiąca.



Dashboard to podstawowe źródło informacji o stanie pracy firewalla.



Rozwiązanie Barracuda pozwala na wykorzystanie dwóch silników antywirusowych jednocześnie (Avira oraz ClamAV).

Inny mechanizm ochrony wymagający dodatkowej subskrypcji to Malware Protection, którego działanie polega na analizie antywirusowej treści przesyłanych przez najpopularniejsze protokoły – HTTP(s), SMTP, POP3 oraz FTP. Dostępne są dwa silniki antywirusowe Avira oraz ClamAV, które mogą działać niezależnie dla tego samego ruchu sieciowego.

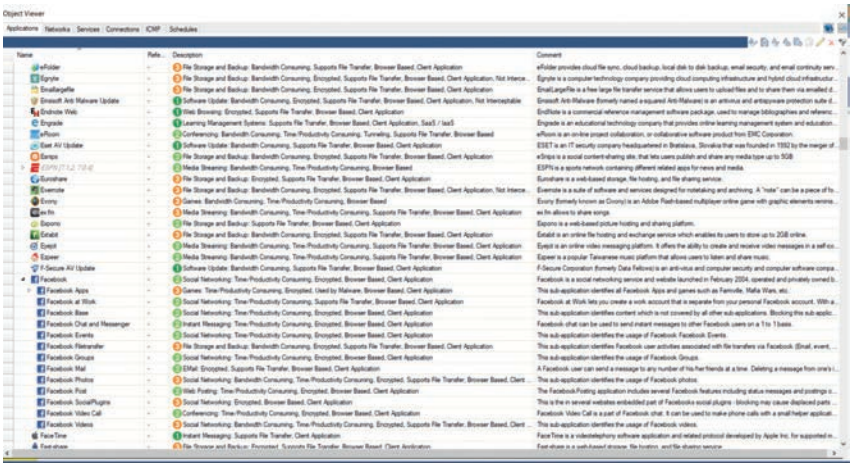
Ostatnią dodatkowo płatną i istotną z punktu widzenia funkcjonalności firewalla opcją jest Advanced Remote Access. Subskrypcja ta rozszerza funkcjonalność VPN o możliwość uruchomienia dostępu SSL VPN w oparciu o konfigurowalny portal, z poziomu którego użytkownicy zdalni mogą uzyskać

dostęp do wybranych aplikacji czy zasobów sieciowych znajdujących się w sieci lokalnej. Zakup licencji to także wsparcie dla aplikacji klienta VPN CudaLaunch, który dedykowany jest szczególnie dla firm działających w modelu BYOD oraz użytkowników platform mobilnych. Aplikacja dostępna jest dla systemów Windows, MacOS, iOS oraz Android. Advanced Remote Access to także rozszerzenie funkcjonalności firewalla o moduł NAC (Network Access Control). Za pośrednictwem klienta dedykowanego dla platform Windows, MacOS oraz Linux możliwa jest bardziej szczegółowa kontrola stanu bezpieczeństwa platformy klienckiej, z wykorzystaniem chociażby indywidualnej zapory sieciowej i polityk dostępu do sieci firmowej. Pozostałe funkcje bezpieczeństwa dostępne są w ramach licencji podstawowej z zastrzeżeniem, że aby mieć dostęp do aktualizacji sygnatur IP, bazy danych o aplikacjach, reguł filtra URL czy po prostu nowej wersji firmware'u, konieczne jest wykupienie subskrypcji Energy Updates, która zapewnia także dostęp do wsparcia technicznego.

Spośród podstawowych funkcji najbardziej przydatne okazuje się filtrowanie ruchu w oparciu o wzorce aplikacji. Application Control daje możliwość budowania reguł i polityk dostępu, wskazując bezpośrednio aplikacje dozwolone i zabronione, z uwzględnieniem szczegółowego harmonogramu czy konkretnego użytkownika. Aplikacje typu instant messaging, P2P czy wybrane funkcje Facebooka mogą być odpowiednio filtrowane. Co więcej – poza standardowymi akcjami typu zezwól/blokuj możliwe jest także zdefiniowanie innych akcji, jak chociażby wskazanie trasy przez innego dostawcę (jeśli oczywiście korzystamy z więcej niż jednego ISP) czy na przykład ograniczenie pasma do zadanej wielkości (QoS). Oczywiście dane statystyczne na temat ruchu związanego z każdą aplikacją i podgląd takich informacji na żywo wraz z identyfikacją potencjalnego ryzyka to funkcje, których nie mogło zabraknąć w nowym firewallu.

Wspomniane wcześniej budowanie reguł pod kątem użytkowników dostępne jest dzięki wsparciu praktycznie wszystkich popularnych metod uwierzytelniania, takich jak chociażby MS AD, RADIUS, LDAP/S czy po prostu wewnętrzna baza użytkowników. Uzupełnieniem dla Application Control jest filtr URL Barracuda Web Filter, bazujący na podzielonej na kategorie bazie online. Dostępna jest także funkcja NG Web Filter, korzystająca z bazy lokalnej. Wersja NG nie jest jednak kompatybilna z Application Control i wymaga uruchomienia HTTP proxy.

Ostatnią, choć nie mniej ważną funkcją dostępną tylko w rozwiązaniach Barracuda Networks, na którą warto zwrócić uwagę, jest TINA (Transport Independent Network Architecture) VPN. W praktyce jest to autorskie rozszerzenie standardu IPSec o funkcje podnoszące kontrolę nad tunelami VPN, niezawodność i stabilność transmisji. Wśród usprawnień znaleźć można chociażby wsparcie dla wielu fizycznych ścieżek wewnątrz pojedynczego logicznego tunelu czy wielu tuneli pomiędzy dwoma lokalizacjami. Pierwsza opcja pozwala na natychmiastowe przełączenie ścieżek w ramach pojedynczego, logicznego tunelu VPN, bez wpływu na ciągłość transmisji danych. Możliwa jest konfiguracja maksymalnie 24 takich niezależnych subtuneli w ramach jednego, logicznego kanału VPN. Ponadto funkcja Traffic Intelligence pozwala na zarządzanie przepustowością tuneli i wykorzystanie ich przez konkretne aplikacje sieciowe. Kompresja i buforowanie ruchu szyfrowanego to kolejne mechanizmy optymalizacji w ramach protokołu TINA.



Bogata baza rozpoznawanych aplikacji dla filtrowania w warstwie siódmej (warstwa aplikacji).

> WDROŻENIE I ZARZĄDZANIE

O ile w kontekście mechanizmów bezpieczeństwa i kontroli ruchu można co najwyżej czepiać się szczegółów, o tyle w kontekście wdrożenia i zarządzania zaporą F600 trzeba przygotować się na nieco nietypowe podejście, niż w przypadku innych popularnych rozwiązań dostępnych na rynku. Zmiana podejścia wynika poniekąd ze sposobu przetwarzania ruchu przechodzącego przez urządzenie i organizacji usług realizowanych w ramach zapory. W konsekwencji nie da się skutecznie wdrożyć rozwiązania z marszu bez lektury dokumentacji, no chyba że dysponujemy czasem na szczegółowe testy lub wdrożenie dotyczy pojedynczej lokalizacji z ograniczoną listą funkcji. Rozwiązania Barracudy zaprojektowane zostały jednak do łączenia i zabezpieczania rozproszonych środowisk IT i dopiero w takim scenariuszu można dostrzec wszystkie ich zalety.

W przypadku modelu F600 i wszystkich wyższych modeli konfiguracja odbywa się za pośrednictwem aplikacji NextGen Admin przeznaczonej dla systemów Windows. Program ten to GUI, za pośrednictwem którego można się podłączyć do pojedynczego urządzenia lub serwera centralnego zarządzania Control Center, który może być użyty jako alternatywny sposób zarządzania urządzeniami Barracuda Networks. Ostatni sposób wymaga bezpośredniego dostępu do konsoli za pośrednictwem protokołu SSH lub dedykowanego portu. Kreator konfiguracji dostępny po pierwszym zalogowaniu pozwala na wstępną konfigurację zapory dla standardowego wdrożenia lub w trybie transparent bridge w celach testowych. Pierwsza niespodzianka pojawia się w momencie próby konfiguracji statycznego adresu dla portu WAN i trasy domyślnej. Intuicja podpowiada, że należałoby znaleźć odpowiedni port w opcjach sieciowych, a następnie wyedytować jego konfigurację. Nic bardziej mylnego – już na tym etapie trzeba sięgnąć do dokumentacji, gdzie co prawda znajdziemy opis, jak to zrobić, ale trudno nazwać ten proces intuicyjnym. Problem wynika ze specyficznej architektury CloudGen Firewalla, która bazuje na trzech warstwach: Box Layer, Virtual Server Layer oraz Service Layer. Pierwsza warstwa jest zarazem najniższą i realizuje podstawowe funkcje, takie jak logowanie zdarzeń oraz konfiguracja urządzenia wraz z podsystemem sieciowym odpowiedzialnym za realizację funkcji zarządzania. Warstwa Virtual Server to, jak wynika z nazwy, poziom logiczny realizujący komunikację IP dla wszystkich usług dostępnych w ramach firewalla. Z kolei warstwa usług Service Layer to już konkretne serwisy, takie jak firewall, serwer VPN czy usługa DHCP uruchamiane na poziomie wirtualnego serwera, zapewniającego wewnętrzną komunikację pomiędzy każdym z serwisów.

Na pojedynczym urządzeniu możliwe jest utworzenie kilku instancji Virtual Servera. To właśnie na poziomie tej warstwy dodawany jest nasz publiczny adres do komunikacji ze światem zewnętrznym. Domyślnie tworzona jest instancja S1 nasłuchująca na adresie pętli zwrotnej 127.0.0.9. Dopiero z poziomu Virtual Servera możliwe jest uruchomienie poszczególnych usług, co również może doprowadzić do nieporozumień przy pierwszym kontakcie z rozwiązaniami Barracuda. Bez zajrzenia w dokumentację np. trudno doszukać się powodu, dla którego nigdzie z poziomu NG Admina nie można dotrzeć do sekcji poświęconej konfiguracji VPN. Dopiero uruchomienie usługi z odpowiedniego poziomu drzewa konfiguracji uruchamia dodatkowe elementy menu. Kiedy już potencjalny administrator oswoi się z logiką i architekturą zapory, kolejne czynności konfiguracyjne przychodzą z większą łatwością i sam interfejs NG Admina staje się logiczny i uporządkowany, włączając w to nie tylko czystą konfigurację, ale także podgląd działania zapory na żywo wraz z informacjami o potencjalnych zagrożeniach. IT

Autor jest architektem w międzynarodowej firmie z branży IT. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

PODSUMOWANIE

Barracuda CloudGen Firewall F600, podobnie jak pozostałe zapory serii F, jest kompleksowym rozwiązaniem odpowiedzialnym za wielowektorowe zabezpieczenie styku sieci. Obserwując raporty Gartnera (Magic Quadrant) dotyczące tej klasy produktów, trudno zrozumieć, dlaczego Barracuda Networks wciąż nie może opuścić grupy graczy niszowych. Kompletność testowanego CloudGena to główna zaleta rozwiązania, co w połączeniu z wydajnością zmieniającą się wraz z wyborem większego pudełka stanowi o sile produktu. Faktem jest także stosunkowo nieszablonowe podejście do funkcji zarządzania. Same narzędzia, jak NG Admin, są funkcjonalne i dopracowane, ale w związku ze specyficzną architekturą systemu trzeba liczyć się z nieco dłuższym czasem wdrożenia w porównaniu z większością konkurencyjnych rozwiązań. Na szczęście producent dostarcza świetną, szczegółową dokumentację na stronie **campus.barracuda.com**, co również pozytywnie wyróżnia go na tle konkurencji, także tej o wiele bardziej znanej i utytułowanej.

Werdykt

Barracuda CloudGen Firewall F600

Zalety

- ⊕ Wydajność
- ⊕ Kompleksowe podejście do ochrony użytkowników
- ⊕ Wysoka odporność na awarie
- ⊕ Świetna dokumentacja
- ⊕ Protokół TINA (rozszerzenie standardu IPSec)
- ⊕ Narzędzia do zarządzania

Wady

- ⊖ Specyficzna architektura systemowa

Cena

Urządzenie: 15 749 euro + obowiązkowy serwis 2 834 euro netto/rok

Energy Updates – 2834/7244 euro (za rok/3 lata)

ATP - 4147/10 552 euro (za rok/3 lata)

Ocena **9**/10