TEST: Barracuda Next Generation Firewall s. 54

Zarządzanie procesami w systemach Linux s. 49

9
2013

Miesięcznik informatyków i menedżerów IT

www.it-professional.pl

IT professional

Nr 9 (22) wrzesień 2013 Cena 29,00 zł (w tym 5% VAT)

SYSTEMY KONTROLI DOSTĘPU s. 12

- **Uwierzytelnianie za pomocą Smart Card**
  Stosowanie kart inteligentnych w środowisku Active Directory
- **Virtual Smart Card**
  Nowe mechanizmy bezpieczeństwa zaimplementowane w Windows 8
- **Biometria na co dzień**
  Darmowy system pracy grupowej. Możliwości platformy, sposoby zarządzania
- **Biometria zgodna z prawem**
  Prawne aspekty dotyczące gromadzenia i przetwarzania danych biometrycznych

s. 67

Storage dla wirtualizacji

Projektowanie infrastruktury pamięci masowej dla środowisk wirtualnych

s. 27

Zainstaluj się sam!

Automatyczna instalacja systemów z rodziny GNU/Linux

s. 45

Rekomendacje NIST 800-115

Metody audytowania. Testowanie zabezpieczeń zgodnie z zaleceniami NIST

ISSN 2083-9588

Serwery ▪ Stacje robocze ▪ Bezpieczeństwo ▪ Infrastruktura i sieci ▪ Zarządzanie i prawo IT ▪ Technologie mobilne

W świecie IT na dobre zadomowiły się UTM-y. Sprawdzamy, jakie cechy oferują urządzenia firmy Barracuda Networks.

Baracuda NG Firewall

09/2013 REKOMENDACJA REDAKCJI IT professional

Zabezpieczenia w Barracudach

Artur Cieślik

Firmy i ich zdalne lokalizacje wykorzystują dostęp do internetu, aby skorzystać z zasobów serwerów WWW czy poczty. Potrzebują również wglądu do danych znajdujących się w bazach danych na serwerach w centrali oraz możliwości edycji tych informacji. Administrator w takim przypadku może stanąć przed dylematem, jak zabezpieczyć zdalną sieć, jednocześnie nie rezygnując z wymaganych możliwości np. routera, antywirusa czy wymuszania polityk bezpieczeństwa dla hostów użytkowników. Każda dodatkowa funkcja to w końcu czas potrzebny na jej konfigurację i utrzymanie. Te dwa składniki są niebagatelną częścią budżetu IT i rozwiązaniem idealnym byłoby stosowanie zabezpieczeń bez kompromisów wynikających z kosztów utrzymania. Rozwiązanie idealne powinno oferować zaawansowane funkcje, jednocześnie wymagając minimalnych nakładów czasu administratora na konfigurację i utrzymanie infrastruktury firewall oraz VPN.

Do testów otrzymaliśmy trzy najważniejsze składniki będące częścią rozwiązania Barracuda NG Firewall. Barracuda NG Firewall F400 jest średniej wielkości urządzeniem typu firewall do zastosowania w większym biurze lub centrali firmy. Barracuda NG Firewall F10 to niewielki UTM do zastosowania w małym biurze lub lokalizacji home office. Ostatnią częścią układanki był wirtualny serwer zarządzania, czyli Barracuda Control Center. Test był wykonany pod kątem funkcjonalnym, wygody i skuteczności zarządzania taką infrastrukturą. Jednocześnie ocenione zostały funkcje bezpieczeństwa oferowane przez NG Firewall.

> TESTOWANE URZĄDZENIA

Rodzina urządzeń Barracuda NG Firewall składa się z appliance różnej wielkości i wydajności. Testowany model F400 plasuje się mniej więcej pośrodku stawki. Większymi są urządzenia F600, F800, F900. Model F10 jest natomiast najmniejszym urządzeniem z tej rodziny. Oprócz fizycznych urządzeń UTM-y występują również w postaci maszyny wirtualnej. Nie jest to wyjątek – wielu producentów oferuje obecnie tego typu rozwiązania.

F400B ma osiem portów 10/100/1000 MBit RJ45 z możliwością dodania modułów SFP o prędkości 1 GbE oraz 10 GbE. Platforma jest oparta na procesorze Intel Dual Core i 2 GB RAM. Pojemność wbudowanego dysku wynosi 80 GB SSD. Obudowa mieści tylko jeden zasilacz i nie ma możliwości dodania kolejnego w celu osiągnięcia redundancji. W specyfikacji producenta podano, że wydajność firewalla wynosi maksymalnie 3,9 Gbps, po uruchomieniu IPS prędkość może osiągnąć 950 Mbps, natomiast poprzez połączenia IPSec VPN urządzenie potrafi przesyłać dane z prędkością maksymalną 700 Mbps. Barracuda może obsłużyć 300 tysięcy jednoczesnych sesji oraz 16 tysięcy nowych połączeń na sekundę. Jest to wystarczająca wydajność dla średnich sieci korzystających z zasobów internetu. Ograniczenia

nie dotyczą ilości obsługiwanych użytkowników, ponieważ licencja pozwala na obsługę nieograniczonej liczby hostów, również tych łączących się poprzez VPN.

W przypadku korzystania z NG Firewalla w większych organizacjach lub gdyby okazało się konieczne kontrolowanie za pomocą UTM-a także ruchu wewnętrznego, powinniśmy zdecydować się na zakup wydajniejszych modeli. Urządzenie o oznaczeniu F900 dysponuje wydajnością 21 Gbps dla firewalla, w przypadku kontroli ruchu za pomocą modułu IPS potrafi kontrolować pakiety z prędkością 3780 Mbps. Maksymalna ilość obsługiwanych sesji jednoczesnych to 1 000 000, a kolejnych nowych w jednej sekundzie 100 tysięcy.

Wersja sprzętowa F10 oferuje przepustowość firewalla na poziomie 300 Mbps, więc całkiem nieźle. Obsługuje połączenia VPN z maksymalną prędkością 85 Mbps, a z włączonym IPS osiąga prędkość 60 Mbps. Obsługiwana liczba sesji jednoczesnych to 2000, a przyrost w jednej sekundzie to 1000 sesji.

W Barracuda NG Firewall technologia TINA (Traffic Intelligence) zapewnia większą stabilność połączeń niż w przypadku tuneli IPSec. TINA pozwala na stworzenie głównego tunelu VPN, w którym możemy skonfigurować wiele transportów, będących de facto osobnymi tunelami VPN.

> SOFTWARE

Oprogramowanie w urządzeniach NG Firewall pozwala na zarządzanie rozproszonymi środowiskami firewall. Szczególny nacisk położono na ułatwienie zarządzania zdalnymi lokalizacjami oraz kanałami site-2-site. Najważniejsze funkcje to oczywiście firewall, IPS, VPN, kontrola aplikacji, filtr webowy, antywirus, antyspam oraz integracja kontroli dostępu do sieci. Uzupełnieniem jest Control Center, które pozwala monitorować urządzenia oraz egzekwować polityki bezpieczeństwa na wielu urządzeniach jednocześnie. Centrum kontroli Barracuda występuje w wersji wirtualnej maszyny oraz w postaci fizycznych urządzeń.

> SPRZĘT I URUCHOMIENIE

Obydwa UTM-y posiadają obudowę metalową, ale tylko w F400B możliwy jest montaż w szafie teleinformatycznej 19". Producent umieścił na przednim panelu urządzenia diody sygnalizacyjne określające statusy pracy ośmiu niezależnych portów 10/100/1000 GBit RJ45. Dziewiąty port RJ45 służy do podłączenia kabla konsolowego. Ponadto na przodzie F4001B znajdują się dwa porty USB do obsługi opcjonalnych połączeń 3G WAN poprzez modem oraz pendrive, na których możemy zapisywać konfigurację. Za pomocą pendrive możemy uruchamiać urządzenia z gotowych konfiguracji, które po przygotowaniu kopiujemy wraz z obrazem na pendrive. Na przednim panelu znajduje się również wyświetlacz LCD prezentujący najważniejsze informacje podczas pracy urządzenia, z drugiej strony natomiast gniazdo zasilania do pojedynczego zasilacza.

W pudełku, razem z urządzeniem, znajdują się dwa kable Ethernet z końcówkami RJ45 potrzebnymi do podłączenia urządzenia do sieci. W konfiguracji domyślnej urządzenie zgłasza się pod adresem 192.168.200.200 na porcie nr 1. Aby rozpocząć konfigurację, wystarczy podłączyć komputer do portu przełącznika i ustawić adres z tej samej podsieci. Następnie uruchamiamy aplikację Barracuda NG Admin, służącą do zarządzania firewallami, oraz Control Center. W oknie logowania mamy do wyboru dwa tryby działania: Box oraz Control Center. Aby dostać się do konfiguracji F400B, wybieramy Box, wpisując wcześniej domyślne hasło dla użytkownika root.

DANE TECHNICZNE

Model	F10	F100	F200	F300	F400	F600	F800	F900
Obudowa	desktop mini	desktop	desktop	1U	1U	1U	1U	2U
Waga [kg]	2	3,5	3,6	4,5	5,4	5,8	13	18
Miedziane łącza Ethernet NIC	4× 1GbE	4× 1GbE	4× 1GbE	4 × 10/100+ +4 × 1GbE	8 × 1GbE	10 × 1GbE+ +1 × 10/100	12/20× 1GbE	0/24×1GbE+ +10/100/1000
Zasilacz	pojed./zewn.	pojed./zewn.	pojed./zewn.	pojed./wewn.	pojed./wewn.	pojed./wewn.	podw./wewn.	podw./wewn.
Maksymalny pobór prądu [A]	1,6	1,6	1,6	1,6	1,4	5	5	5
Przepustowość fw. [Gbps]	0,3	0,3	0,4	0,55	3,9	4,7	10	21
Przepustowość VPN [Mbps]	85	85	120	160	700	950	2200	3780
Przepustowość IPS [Mbps]	60	60	80	90	950	1316	3100	4650
Liczba jednoczesnych sesji	2 000	2 000	35 000	70 000	300 000	300 000	500 000	1 000 000
Nowe sesje [liczba sesji/s]	1 000	1 500	2 500	2 500	16 000	16 000	35 000	100 000

> OPROGRAMOWANIE I FUNKCJE

Po zalogowaniu się do urządzenia F400B w trybie Box pojawia się interfejs, który swoją budową trochę zaskakuje. Pierwszy ekran prezentuje najważniejsze informacje o urządzeniu – tutaj nie napotkamy niespodzianek. Na górze ekranu znajdziemy następujące elementy menu: Status (pierwszy ekran po zalogowaniu), Config, Control, Firewall, VPN, Logs, Statistics, Events oraz SSH. Na początku można czuć się zagubionym w interfejsie, w którym wybrano wyraźny podział na grupy funkcjonalne. Podział ten wynika raczej z potrzeb dostępu do właściwych funkcji podczas administracji urządzeniem i jest nieco odmienny niż w innych znanych rozwiązaniach. Jednak do tak posegregowanych opcji można się przyzwyczaić. Przykładem jest Config, po kliknięciu którego mamy do wyboru dwie formy prezentacji, simple oraz Full. Pierwszy widok pozwala na dostęp do najważniejszych funkcji. Dopiero po wyborze opcji Full Config otwiera się okno z całym drzewem szczegółowych parametrów urządzenia. Natomiast w Firewall mamy dostęp do opcji monitorujących stan sesji czy wykrytych zagrożeń, a jednocześnie możemy wybrać konfigurację reguł filtrujących. Klikając Proxy, można oczekiwać listy funkcji pozwalających nie tylko monitorować stan pracy tego modułu, lecz, podobnie jak w przypadku Firewall, konfigurować jego parametry. Jednak w tym miejscu producent zdecydował tylko umieścić tabelkę ze statusem obsługiwanych w danym momencie sesji. Odmienność zarządzania tym rozwiązaniem może się z początku wydawać niektórym administratorom uciążliwa. Jednak po pewnym czasie można się przekonać, że takie ułożenie funkcji bywa bardzo przydatne.

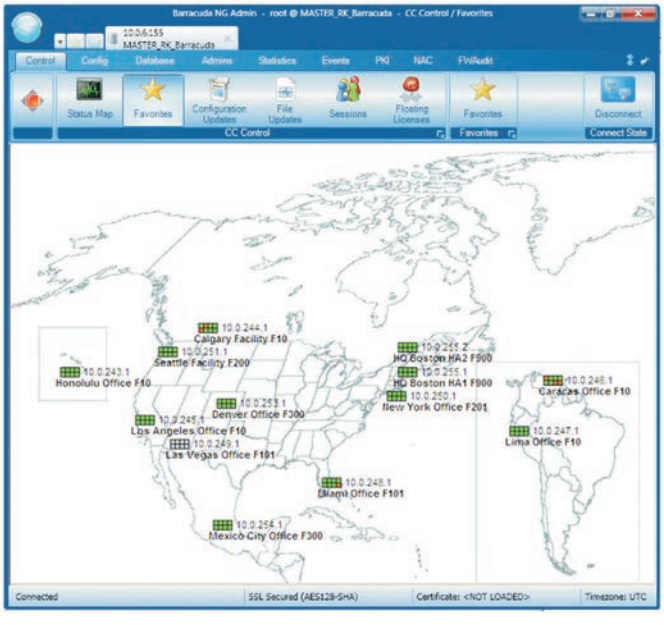
Oprogramowanie Barracuda NG Firewall pozwala na zarządzanie bezpośrednie „pudełkiem", jak również umożliwia sterowanie z poziomu Barracuda Control Center. W tym drugim przypadku postawiono na niezawodność sterowania dużą liczbą firewalli rozrzuconych po całym globie. BCC potrafi w widoku 3D przedstawić wszystkie lokalizacje, w których znajdują się kontrolowane Barracudy. Ponadto prezentuje całą sieć połączeń VPN pomiędzy urządzeniami i pozwala monitorować ewentualne problemy. W tym miejscu warto wspomnieć o innej ciekawej funkcji: podczas zarządzania Barracuda Control Center korzysta z dedykowanego kanału VPN, który działa niezależnie od pozostałej konfiguracji urządzenia. Pozwala to utrzymać łączność ze zdalnym firewallem, nawet w razie zerwania kanału site-2-site.

Konfiguracja poszczególnych funkcji została przemyślana w taki sposób, aby wielu administratorów miało możliwość jednoczesnej konfiguracji urządzenia. Pozwala na to opcja Lock, którą administrator wykorzystuje do zablokowania edycji określonej funkcji dla pozostałych administratorów. Po wprowadzeniu zmian wystarczy kliknąć opcję Send Changes, co zaktywuje nową konfigurację na urządzeniu. Wprowadzenie nowej konfiguracji może odbywać się w sposób bezpieczny. Przykładem jest zmiana adresacji IP interfejsów. Po ustawieniu nowych IP wysyłamy konfigurację i aktywujemy zmiany, jednak urządzenie wróci do poprzedniej konfiguracji, jeżeli nie nawiąże ponownie połączenia z Control Center. Bywa to szczególnie przydatne, gdy firewall znajduje się w odległości paru tysięcy kilometrów od naszego biurka…

> NAJWAŻNIEJSZE FUNKCJE

Wśród możliwości urządzenia znajdziemy obiektowego firewalla z IPS, VPN z obsługą IPSec, SSL oraz autorskiego protokołu TINA. Ponadto Barracuda NG Firewall pozwala na kształtowanie ruchu za pomocą polis routingu oraz protokołu Quality of Service. W zakresie zabezpieczeń końcówek oferuje możliwości filtrowania WWW, ochronę przeciwko malware, a także kontrolowanie ruchu poprzez identyfikację ponad 1200 aplikacji.

Ciekawym rozwiązaniem jest wspomniany protokół TINA. Technologia Traffic Intelligence pozwala na zapewnienie większej stabilności połączeń niż w przypadku tuneli IPSec. Cechą TINA jest możliwość tworzenia jednego dużego tunelu VPN, w którym możemy skonfigurować wiele transportów, będących de facto osobnymi tunelami VPN, w ramach tunelu głównego. Transporty mogą być podzielone na różnego rodzaju ruch sieciowy kierowany za pomocą zdefiniowanych reguł przez administratora. W przypadku przerwania jednego z tuneli podrzędnych (transportów) Traffic Intelligence przełącza ruch na inny działający transport,



Barracuda NG Firewall Control Center zapewnia centralny monitoring w czasie rzeczywistym wszystkich firewalli w obrębie firmy.

PODSUMOWANIE

Barracuda NG Firewall to zaawansowane rozwiązania, których moc możemy zaobserwować szczególnie w dużych i rozproszonych strukturach. Oferują nie tylko funkcje znane z innych rozwiązań, ale też wiele unikatowych opcji. Czasami nowe pomysły jednak idą w parze ze zbyt zawiłą konfiguracją w ramach interfejsu GUI, co może stanowić pewien problem dla administratorów. Urządzenia wydają się stworzone dla rozległych sieci VPN z centralizacją zarządzania. Protokół TINA, który potrafi grupować transporty i warunkować przesyłanie danych za pomocą różnych łączy, w tym zestawianych za pomocą połączeń komórkowych, jest jedną z najważniejszych funkcji tych rozwiązań. Barracuda pozwala również dopasować wydajność urządzenia do potrzeb lokalizacji bez znaczącej straty na funkcjonalności. Warto zauważyć, że nawet najmniejsze urządzenie ma większość ważnych funkcji, w tym tunele VPN zestawiane przez TINA. Pomimo miejscami trudnego GUI oferuje wiele ułatwień. Jednymi z nich są graficzne kreatory połączeń VPN oraz kształtowania ruchu. Urządzenia polecamy do zastosowania w średnich i dużych organizacjach. Zalety rozwiązania ujawnią się szczególnie w firmach posiadających wiele lokalizacji.

a połączenie tunelem głównym pozostaje nietknięte. Przełączenie jest na tyle szybkie, że nie powinno prowadzić do opóźnień pakietów. W jednym tunelu TINA pozwala umieścić maksymalnie 24 transporty. Ponadto technologia ta umożliwia przełączanie transportów w ramach jednego głównego tunelu VPN, a także pozwala nadawać priorytety różnym rodzajom przesyłanych danych za pomocą QoS w ramach tunelu, np. SMTP, VoIP, WWW. W celu zaoszczędzenia pasma możemy również kompresować przesyłany ruch w tunelu.

Reguły firewall w Barracuda NG Firewall definiujemy jako polityki dla wskazanego ruchu, w których wybieramy zdefiniowane profile IPS oraz kontroli aplikacji. Natomiast nie znajdziemy możliwości dodania odpowiednich profili filtrowania dostępu do kategorii WWW oraz usuwania malware'u. Tę część konfiguracji musimy przeprowadzać osobno, definiując dodatkowo ACL dla poszczególnych użytkowników czy adresów IP. Jednocześnie warto zauważyć, że konfiguracja usługi proxy jest w tym rozwiązaniu dosyć skomplikowana i czasochłonna, a brak powiązania reguł firewall z proxy zwiększa, niestety, liczbę działań potrzebnych do skonfigurowania urządzenia.

Ciekawym elementem reguł firewall są tzw. kaskady. Możemy je tworzyć na regułach typu Forward, czyli filtrujących ruch przechodzący przez firewall. Reguła Cascade jest przekierowaniem do osobnego zestawu reguł, z którego możemy wrócić lub przejść do dowolnego innego zestawu reguł za pomocą zdefiniowanego warunku kaskady powrotnej. Łatwiej to zrozumieć, porównując to rozwiązanie do łańcuchów IPTABLES znanych z Linuksa. Barracuda NG Firewall posiada reguły typu Host oraz Forwarding. W regułach Host znajdziemy łańcuchy, na których możemy filtrować ruch hosta typu inbound oraz outbound. Reguły Forwarding są odpowiednikiem łańcucha Forward w IPTABLES, a zestawy reguł definiowane przez użytkownika są opcjonalnymi łańcuchami, do których kierujemy pakiety na podstawie zdefiniowanych warunków.

> PRZYDATNE OPCJE

Barracuda NG Firewall posiada również inne przydatne funkcje. Oprogramowanie testowanego rozwiązania pozwala również na integrację z serwerami uwierzytelniającymi, w tym Active Directory. Funkcja jest oparta na agencie, co znacznie ułatwia implementację i uniezależnia od schematu Active Directory. Warto również wspomnieć o usłudze niezbędnej szczególnie w większych środowiskach, a mianowicie o zarządzaniu zmianami w konfiguracjach urządzeń. W Barracudzie zastosowano natywnie RCS, czyli Revision Control System, który działa w zakresie całego urządzenia. RCS umożliwia dokładne śledzenie wprowadzonych zmian w każdym z modułów, a także przywracanie ich w przypadku zaistnienia takiej potrzeby do wybranej wersji poprzedniej. IT

Autor specjalizuje się w realizacji audytów bezpieczeństwa informacji, danych osobowych i zabezpieczeń sieci informatycznych. Był wieloletnim menedżerem Działu Integracji Systemów. Prowadzi szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych oraz audytów zabezpieczeń systemów informatycznych.

Werdykt

Barracuda NG Firewall

Zalety

- ⊕ Skalowalność
- ⊕ Autorski VPN
- ⊕ Zarządzanie zmianami w konfiguracji
- ⊕ Graficzne kreatory połączeń

Wady

- ⊖ Nieco skomplikowana konfiguracja
- ⊖ Osobne ACL dla proxy oraz firewalla

Ocena 9/10