Test: Stormshield SN210W – zabezpieczenia klasy UTM s. 49

Splunk – zarządzanie zdarzeniami s. 44

9
2017

Miesięcznik informatyków i menedżerów IT

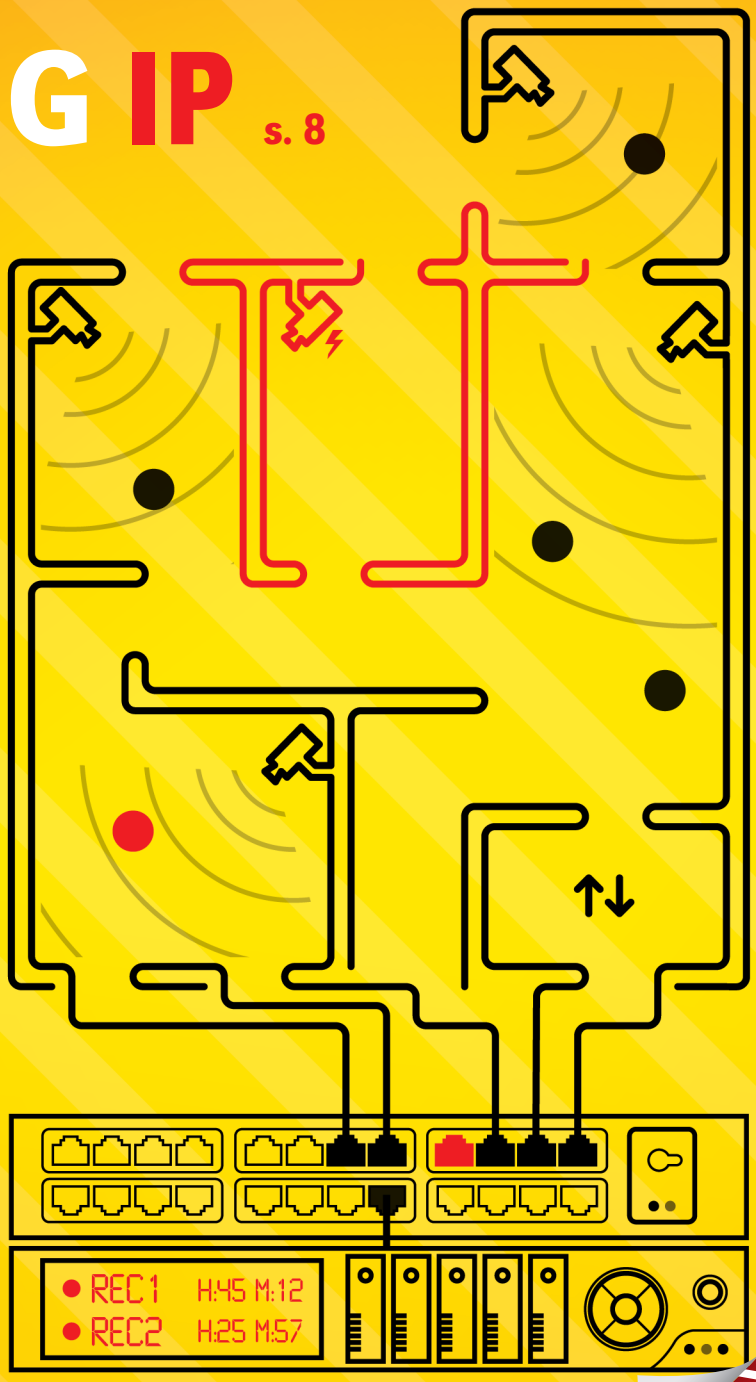
www.it-professional.pl

IT professional

Nr 9 (70) wrzesień 2017 — Cena 33,00 zł (w tym 5% VAT)

MONITORING IP s. 8

Ocena skutków dla systemów monitoringu wizyjnego zgodnie z rodo oraz powiązania z regulacjami o ochronie danych osobowych. Technologie wykorzystywane w urządzeniach telewizji przemysłowej CCTV zwiększające bezpieczeństwo na monitorowanym terenie – wykorzystanie kamer HD, rejestratorów obrazu i sieci Ethernet



s. 54

Naruszenie bezpieczeństwa danych klienta

Odpowiedzialność wykonawcy i ochrona danych osobowych na podstawie uodo

s. 65

Projektowanie i instalacja wysoko dostępnego klastra vSphere

Rozwiązania VMware dla MŚP oferowane w ramach licencji Essentials Plus

s. 38

Wirtualne karty inteligentne

Uwierzytelnianie dwuskładnikowe. Zwiększenie bezpieczeństwa systemów IT

ISSN 2083-9588

DOSTĘPNE E-WYDANIE

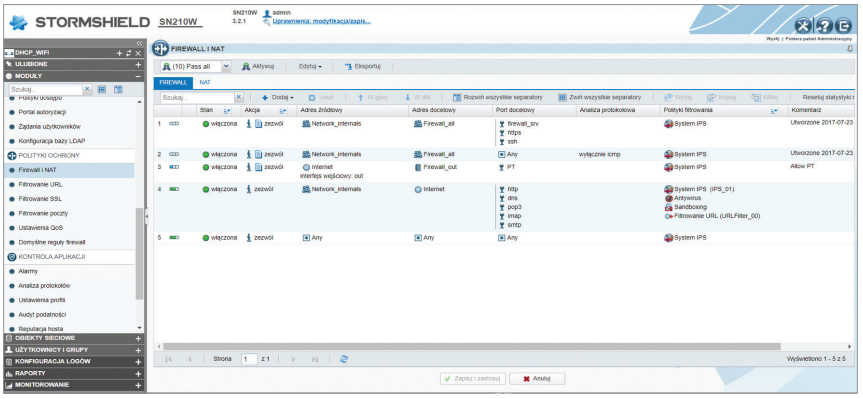
Rozwiązania klasy Unified Threat Management (UTM) to podstawowy rodzaj zabezpieczenia na brzegu sieci stosowany w większości małych i średnich przedsiębiorstw. Wybór urządzeń all-in-one jest spory, przez co wybór konkretnego modelu może nie być najłatwiejszy. Testujemy możliwości jednego z takich rozwiązań.

ZABEZPIECZENIA UNIFIED THREAT MANAGEMENT (UTM)

Stormshield SN210W – wszystko w jednym

Marcin Jurczyk

Dokładnie dwa lata temu po raz pierwszy przetestowaliśmy zaporę sieciową klasy UTM firmy Stormshield. Było to urządzenie przeznaczone dla dużych przedsiębiorstw, wyposażone w wiele portów miedzianych i charakteryzujące się dobrą wydajnością. Marka Stormshield była wtedy mało rozpoznawalna, choć sama technologia już dobrze znana. Wynikało to z faktu, że w rzeczywistości mieliśmy do czynienia z rebrandingiem popularnej na europejskim rynku marki Netasq, której doświadczenie w świecie zintegrowanych firewalli sięgało 1998 roku. Od tamtej pory sporo się zmieniło. Pojawiły się kolejne generacje oprogramowania układowego, a także nowe modele urządzeń. Tym razem otrzymaliśmy do testów reprezentanta najmniejszej serii przeznaczonej dla niewielkich firm – model SN210W.



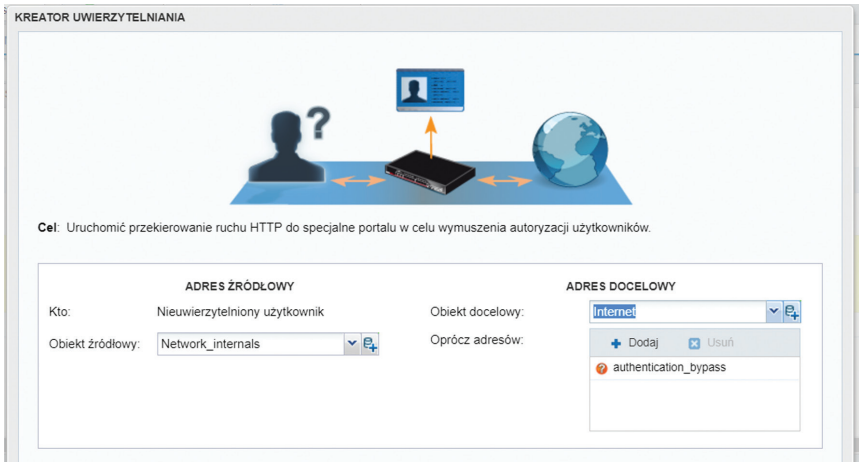
Większość mechanizmów bezpieczeństwa konfigurowana jest za pomocą reguł filtrowania.

> SPRZĘT I WYDAJNOŚĆ

Portfolio rozwiązań UTM Stormshield zostało podzielone na cztery kategorie – rozwiązania dla małych sieci ze zintegrowanym Wi-Fi (do 30 hostów), to samo bez wsparcia dla Wi-Fi (do 70 hostów), produkty dla sieci średnich i dużych firm (71–700 hostów) oraz UTM-y dla sieci korporacyjnych i centrów przetwarzania danych (do 15 tysięcy hostów). Ponadto możliwe jest również wdrożenie UTM-a w formie maszyny wirtualnej. Testowany model to jeden z dwóch dostępnych modeli ze zintegrowanym punktem dostępowym, plasujących się na samym dole portfolio producenta.

Wprowadzone ulepszenia, typu wsparcie dla wielu baz użytkowników oraz klasyfikacja ruchu z użyciem geolokalizacji i bazy reputacji, to elementy, które mogą zadecydować o wyborze SN210W spośród innych produktów.

SN210W pozycjonowany jest dla niewielkich firm i zdalnych lokalizacji, w których liczba chronionych urządzeń sieciowych nie przekracza 30 hostów. Rozwiązanie świetnie więc wpisuje się w potrzeby polskiego rynku MŚP. Producent deklaruje maksymalną wydajność firewalla na poziomie 2 Gb/s. Dołączenie ochrony IPS zmniejsza wydajność do poziomu 1,6 Gb/s dla 1518-bajtowej ramki

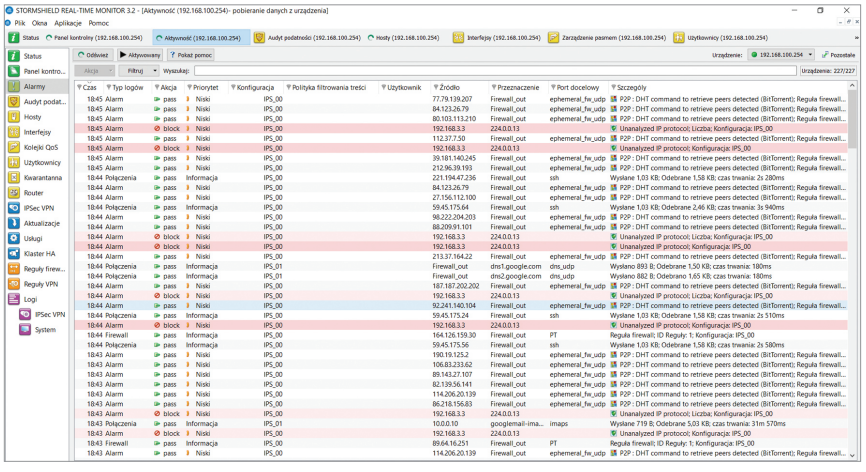


Definiowanie ustawień z wykorzystaniem kreatora.

danych. Jeśli dodatkowo zostanie uruchomiony skaner antywirusowy, spadek wydajności będzie wyraźny – w takim przypadku górny limit przepustowości dla ruchu HTTP to 300 Mb/s. Urządzenie jest w stanie obsłużyć do 200 000 równoległych sesji oraz do 15 000 nowych sesji na sekundę. Możliwe jest także zestawienie do 50 tuneli IPSec lub 20 tuneli SSL. Maksymalna przepustowość w tunelu IPSec wynosi 350 Mb/s. Dzięki wsparciu do 64 VLAN-ów możliwe jest także zdefiniowanie takiej samej liczby dostawców ISP.

SN210W został wyposażony w 8 portów, z czego 6 to porty przełącznika, a 2 pozostałe to port WAN oraz DMZ. Wszystkie dostępne porty działają w standardzie Ethernet 10/100/1000. Bezpośrednio po wypakowaniu urządzenia i podpięciu go do sieci wszystkie porty znajdują się w trybie bridge. UTM może zostać wdrożony w trybie transparentnym lub w formie tradycyjnego routera. Za komunikację ze światem odpowiada także wbudowany punkt dostępowy, działający w standardzie 802.11 a/b/g/n, który może obsłużyć maksymalnie dwa SSID. Interfejsy bezprzewodowe to oddzielny segment sieci, z własną adresacją, których nie da się połączyć w trybie mostka w celu utworzenia jednej płaskiej podsieci. W kontekście całkiem rozsądnej w tej klasie urządzeń przepustowości poszczególnych modułów bezpieczeństwa również brak wsparcia dla standardu 802.11ac wydaje się niezrozumiały. O ile na potrzeby normalnej pracy z wykorzystaniem narzędzi biurowych czy przeglądarki łączność bezprzewodowa na poziomie ~80-100 Mb/s będzie wystarczająca, szczególnie w kontekście wąskiego gardła w postaci łącza internetowego, o tyle wykonanie kopii zapasowych czy udostępnianie większych plików będzie uciążliwe. Ciężko zatem zrozumieć decyzję producenta, tym bardziej że łączność bezprzewodowa w standardzie AC jest od dłuższego czasu czymś powszechnym także w sprzęcie do użytku domowego za około 200 zł. Funkcja punktu dostępowego posiada również dodatkowe ograniczenie – brakuje uwierzytelniania za pośrednictwem usługi RADIUS, choć nieoficjalnie udało nam się dowiedzieć, że nadchodząca wersja oprogramowania powinna rozwiązać ten problem. Innym problemem związanym z Wi-Fi, który pojawił się w trakcie testu, był brak wsparcia dla znaków specjalnych w haśle WPA2. Co ciekawe – hasło wpisane z rozpędu, zawierające znak @ i * zostało bez problemu przyjęte, jednak bez żadnego komunikatu z ciągu usunięte zostały znaki specjalne, co znacznie utrudniło diagnozę błędu.

Poza sieciowymi interfejsami do komunikacji dostępne są także 3 porty USB, z czego jeden z nich to dedykowany port konsoli. Pozostałe gniazda można wykorzystać np. w celu podłączenia modemu 3G/4G. W stosunku do poprzednich wersji firmware'u producent nie ogranicza już wsparcia tylko dla własnej wersji modemu. Obecnie podłączyć można dowolne urządzenie, dzięki czemu udało się wyeliminować limit przepustowości na poziomie 7,2 Mb/s, związany z możliwościami wcześniej wspieranego sprzętu. Niestety, SN210W nie ma wbudowanej pamięci stałej, w której można by zapisywać chociażby logi. W tym celu na przedniej ściance kompaktowej obudowy zainstalowano slot na kartę SD (oddzielnie licencjonowane!).



Real-Time Monitor to jeden z desktopowych programów do monitoringu dostępnych za darmo w ramach pakietu administracyjnego.

> FUNKCJE BEZPIECZEŃSTWA

Testowany Stormshield to rozwiązanie UTM w pełnym tego słowa znaczeniu. Zgodnie z oczekiwaniami mamy do czynienia z urządzeniem integrującym niemal wszystkie mechanizmy bezpieczeństwa w ramach jednego rozwiązania instalowanego najczęściej na brzegu sieci. Zapora ogniowa, IPS (Intrusion Prevention System), filtr antyspamowy oraz antywirusowy, głęboka inspekcja pakietów ze szczegółowym rozbiciem na aplikacje, filtrowanie adresów URL, kategoryzowanie ruchu w oparciu o geolokalizację i bazy reputacji czy w końcu mechanizm piaskownicy w chmurze, kontrola użytkowników i pasywny skaner podatności – to rozwiązania dostępne we wszystkich modelach UTM Stormshield, również w testowanym SN210W. Za fizyczną realizację mechanizmów bezpieczeństwa odpowiada specjalizowany system operacyjny NETASQ Secured BSD (NS-BSD). Testowane urządzenie pracowało pod kontrolą NS-BSD w wersji 3.2.1. W porównaniu do poprzednio testowanego modelu SN900 mamy do czynienia z przeskokiem z wersji 2.1.0, a więc z kolejną pełną rewizją oprogramowania układowego. Fundamenty systemu pozostały niezmienione – wydajność platformy w dalszym ciągu opiera się na opatentowanej technologii proaktywnego wykrywania ataków o nazwie ASQ (Active Security Qualification). W praktyce sprowadza się to do integracji funkcji firewalla z IPS na poziomie jądra systemu operacyjnego, dzięki czemu ograniczono liczbę operacji koniecznych do przeanalizowania każdego pakietu, częściowo eliminując wielokrotną analizę tych samych danych przez poszczególne moduły bezpieczeństwa.

Zgodnie z deklaracją producenta ruch na styku sieci lokalnej i WAN-u analizowany jest na trzy sposoby. Najpierw pakiety podlegają ocenie heurystycznej, następnie przeprowadzana jest analiza protokołów i ich zgodności z RFC, a na końcu ruch poddawany jest analizie względem sygnatur kontekstowych. Zintegrowany system IPS to w zasadzie podstawowa i najskuteczniejsza broń Stormshielda. Obecnie dostępnych jest 1941 sygnatur/alarmów IPS, które zostały skategoryzowane w ramach grup: Aplikacje, Zabezpieczenia oraz Malware. Dzięki temu w prosty sposób można zdefiniować akcję (zezwól/zablokuj) oraz priorytet (niski/wysoki/ignoruj) dla każdej sygnatury. W praktyce jednym kliknięciem myszy można zablokować np. dostęp do gier dostępnych na Facebooku, pozostawiając dostęp do komunikatora czy opcji polubień. W stosunku do możliwości sprzed dwóch lat przybyło ponad 500 nowych sygnatur, co świadczy z jednej strony o większej liczbie zagrożeń, z drugiej zaś o ciągłym rozwoju platformy systemowej Stormshield. Wśród nowości dostępnych od wersji 3.0 oprogramowania są filtrowanie ruchu w oparciu o geolokację oraz reputację adresów IP.

W pierwszym przypadku bez większego wysiłku możemy stworzyć regułę filtrującą na podstawie kontynentu lub kraju. Dzięki temu łatwo można ograniczyć

LICENCJONOWANIE

Zakup SN210W z najtańszym pakietem serwisowym na 1 rok to koszt od 1014 euro netto. Zakup urządzenia z najdroższym pakietem serwisowym na 1 rok to koszt od 1217 euro netto. Klient, kupując testowane urządzenie Stormshield (koszt samego sprzętu to 845 euro netto), dokupuje do niego pakiet serwisowy na okres od jednego roku do trzech lat, który gwarantuje dostęp do aktualizacji, wsparcie techniczne ze strony dystrybutora, wymianę urządzenia w ciągu 14 dni w przypadku awarii sprzętowej oraz dostęp do newslettera Stormshield. Producent oferuje trzy rodzaje pakietów serwisowych:

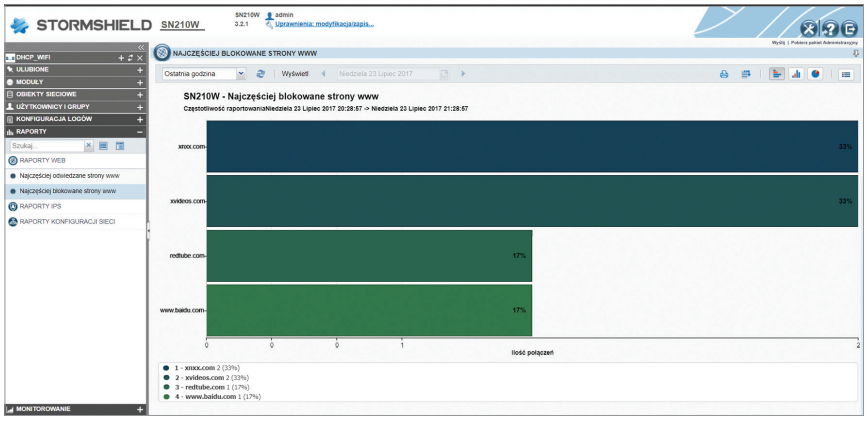
- **Remote Office Security Pack** (169 euro netto na 1 rok) – najtańsza opcja serwisowa obejmuje Next Generation Firewall zintegrowany z IPS na poziomie jądra systemowego oraz IPSec + SSL VPN;
- **UTM Security Pack** (194 euro netto na 1 rok) – najpopularniejszy wśród klientów serwisu oakiet, który łączy w sobie wszystkie opcje: Next Generation Firewall zintegrowany z IPS na poziomie jądra systemowego oraz IPSec + SSL VPN, antywirus ClamAV, polski filtr URL (stworzony przy współpracy z polskim dystrybutorem oraz administratorami polskich firm na podstawie wyników badań preferencji ruchu webowego pracowników);
- **Premium UTM Security Pack** (372 euro netto na 1 rok) – najdroższy spośród serwisów, który oprócz wspomnianego wcześniej Next Generation Firewalla, zintegrowanego z IPS na poziomie jądra systemowego oraz IPSec + SSL VPN, antywirusa ClamAV, polskiego filtra URL, zawiera silnik antywirusowy Kaspersky Lab i opcje: **audyt podatności**, **rozszerzony filtr URL** i obsługę kart SD.

Każdy z serwisów można rozszerzyć o dodatkowe opcje:

- **audyt podatności** (pasywny skaner sieci, identyfikujący aplikacje łączące się z siecią, wskazując nieaktualne wersje programów) – 118 euro netto dla rocznej opcji serwisowej;
- **silnik antywirusowy Kaspersky Lab** – 127 euro netto dla rocznej opcji serwisowej;
- **Breach Fighter piaskownica w chmurze** (sandbox) – 127 euro netto dla rocznej opcji serwisowej (wymaga aktywnego silnika antywirusowego Kaspersky lub aktywnego serwisu Premium UTM Security Pack);
- **rozszerzony filtr URL** (65 kategorii) – 144 euro dla rocznej opcji serwisowej.

Istnieje również możliwość zakupienia usługi Support Premium w jednej z trzech wersji (4, 8 i 12 godzin zdalnego administrowania), która oprócz bardzo szybkiej reakcji na zgłoszenie serwisowe pozwala korzystać z umiejętności certyfikowanych inżynierów Stormshield podczas konfiguracji funkcji lub rekonfiguracji działającego już urządzenia.

komunikację do lokalizacji geograficznych, z którymi kontakt jest niezbędny bez zagłębiania się w analizę prefiksów sieciowych. W drugim przypadku producent dostarcza predefiniowane kategorie reputacji IP, rozróżniające m.in. adresy: IP botnetów, serwerów spamerskich czy węzłów brzegowych sieci TOR. Reguły można tworzyć zarówno w kontekście adresów źródłowych, jak i docelowych.



Predefiniowane grupy tematyczne filtrów URL pozwalają na blokowanie zabronionych treści.

Dostępny jest również mechanizm oceny reputacji hostów wewnątrz sieci lokalnej. Administrator ma możliwość zdefiniowania własnej, punktowej skali oceny ryzyka w oparciu o analizę monitorowanych hostów. Na tej podstawie możliwe jest w dalszym kroku zdefiniowanie reguł filtrowania. W kontekście kontroli stanu hostów w sieci wewnętrznej warto wspomnieć także o funkcji audytu podatności. UTM jest w stanie zidentyfikować aplikacje sieciowe działające na hostach w sieci lokalnej, gdy tylko zostanie wygenerowany ruch przechodzący przez zaporę. Na tej podstawie zbierane są informacje o aplikacjach, ich wersjach, podatnościach i wykorzystaniu. Funkcja ta wymaga zakupu osobnej licencji.

Listę wymienionych mechanizmów bezpieczeństwa uzupełnia funkcja filtra adresów URL. Standardowo dostępna jest wbudowana lista z podziałem na najpopularniejsze kategorie tematyczne. Za dodatkową opłatą można dokupić subskrypcję na rozszerzone filtrowanie z wykorzystaniem bazy w chmurze producenta. W tej opcji ponad 100 milionów adresów URL zostało podzielonych na 65 kategorii. Na szczególną uwagę zasługuje jednak opcja wbudowanej bazy adresów URL przygotowanej specjalnie dla polskiego rynku, w której stworzeniu pomagali administratorzy i użytkownicy pracujący w rodzimych przedsiębiorstwach. 56 kategorii, wśród których znaleźć można komunikatory, portale plotkarskie i ogłoszenia, obejmuje najpopularniejsze portale występujące na lokalnym rynku. W przypadku filtrowania adresów URL, a także innego rodzaju ruchu zaszyfrowanego w ramach protokołu SSL, dostępne jest oczywiście proxy SSL, dzięki któremu ruch jest odszyfrowywany w celu dalszej analizy. Korzystając z tego mechanizmu (odpowiednia reguła deszyfrowania poprzedzająca regułę związaną z konkretną analizą), trzeba mieć świadomość, że przeanalizowany ruch zostanie zaszyfrowany kluczem urządzenia i przesłany do odbiorcy, co trzeba odpowiednio obsłużyć na hoście klienckim, na którym przeglądarka zgłosi błąd certyfikatu.

Mechanizm proxy SSL może być również przydatny w celu analizy antywirusowej zaszyfrowanych pakietów. Standardowo Stormshield dostępny jest z silnikiem antywirusowym ClamAV. Za dodatkową opłatą dostępna jest także analiza z wykorzystaniem silnika Kaspersky Lab. Płatny antywirus jest też wymogiem koniecznym do uruchomienia również płatnego mechanizmu piaskownicy (sandbox) w chmurze o nazwie Breach Fighter. W tym przypadku analiza behawioralna i wykrywanie niepożądanych działań odbywają się w odizolowanym środowisku wirtualnym w chmurze. Dzięki temu sieć urządzeń Stormshield jest w stanie współdzielić informacje o zagrożeniach zero-day niemal w czasie rzeczywistym. Jak przystało na urządzenie tego typu, możliwe jest także skonfigurowanie bezpiecznych tuneli VPN – do wyboru są trzy protokoły – IPSec, SSL oraz PPTP. Mowa tu oczywiście zarówno o tunelach site-to-site, jak również client-to-site.

> POZOSTAŁE FUNKCJE

Podobnie jak pozostałe modele z portfolio producenta, SN210W to prawdziwy kombajn. Testowany model zalicza się do najmniejszych rozwiązań, przez co nie jest możliwe zestawienie klastra wysokiej wydajności w trybie active-passive. Poza tym możliwości SN210W nie różnią się od tego, co oferują więksi bracia. Jedną z nowości w wersji 3 oprogramowania jest integracja z wieloma bazami użytkowników Active Directory lub LDAP. Poza bazą wbudowaną oprogramowanie wspiera dodatkowo cztery bazy zewnętrzne, dzięki czemu można dopasować polityki dostępu dla zróżnicowanych grup użytkowników. Ponadto możliwe jest także definiowanie kont tymczasowych, dzięki którym łatwiej można zarządzać dostępem dla gości.

Dla administratorów posiadających nieco większe niż standardowe wymagania co do zarządzania siecią i trasowania pakietów przydatne może okazać się wsparcie dla dynamicznych protokołów routingu za pośrednictwem aplikacji Bird. Administrator może także bez problemu skonfigurować trasy powrotne czy wskazywać, przez którą bramę ma wychodzić określony ruch (realizowane jest to na poziomie reguł filtrowania). Dostępne są również funkcje kształtowania ruchu QoS.

> ZARZĄDZANIE

Głównym interfejsem zarządzania jest GUI dostępne z poziomu przeglądarki WWW. W stosunku do poprzedniej wersji NS-BSD pojawiło się kilka nowych możliwości, z których najważniejszą jest możliwość monitorowania w czasie rzeczywistym informacji o połączeniach sieciowych, parametrach pracy urządzenia i zalogowanych użytkownikach. Ponadto zmiany są raczej kosmetyczne.

Sama nawigacja i administracja wymaga chwili przyzwyczajenia. Przesiadka z rozwiązań UTM innych producentów wymaga zmiany sposobu myślenia, chociażby ze względu na brak definicji stref bezpieczeństwa, pomiędzy którymi definiowane są polityki bezpieczeństwa. Zdecydowana większość czynności administracyjnych odbywa się z poziomu menu Polityki ochrony | Firewall i NAT. Na poziomie pojedynczej reguły definiuje się nie tylko adres źródłowy i docelowy wraz z wybranymi portami czy aplikacjami podlegającymi filtrowaniu, ale również cały szereg funkcji dodatkowych, takich jak deszyfrowanie SSL, generowanie alarmów, przypisywanie polityk QoS, policy-based routing czy ustawienie harmonogramu. Sama organizacja menu jest dość standardowa, z rozwijanym menu funkcjonalnym po lewej stronie okna i odpowiednim panelem konfiguracyjnym w centrum strony przeglądarki. Na pochwałę zasługuje bardzo dobra polonizacja interfejsu, co wyróżnia produkty Stormshield na tle konkurencji. O ile w przypadku większości testów urządzeń pozostajemy przy angielskiej wersji językowej celem uniknięcia trudów związanych z interpretacją niektórych tłumaczeń, o tyle w przypadku Stormshielda praca w ojczystym języku nie przysparza żadnych trudności. Innym interfejsem użytkownika jest konsola CLI. W niektórych przypadkach, jak chociażby ustawienie polskiej wersji filtra URL, konieczne jest skorzystanie z ręcznej edycji plików konfiguracyjnych i wywołanie aktualizacji. W większości jednak webGUI okazuje się wystarczające.

Ciekawą opcją jest centralne zarządzanie wieloma geograficznie rozproszonymi UTM-ami za pomocą oprogramowania Stormshield Management Center. W ten sposób można centralnie definiować reguły zapory, NAT i VPN. Sama konfiguracja VPN pomiędzy wieloma urządzeniami za pośrednictwem SMC jest maksymalnie uproszczona dzięki zastosowaniu intuicyjnego kreatora. Scentralizowane jest również tworzenie i zarządzanie obiektami sieciowymi. Interfejs użytkownika dostępny z poziomu przeglądarki jest niemalże identyczny do dostępnego bezpośrednio z poziomu urządzenia. Stormshield Management Center dystrybuowany jest w formie prekonfigurowanej maszyny wirtualnej, a obsługa do pięciu urządzeń UTM jest darmowa. IT

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

PODSUMOWANIE

W kategorii rozwiązań UTM dedykowanych dla najmniejszych środowisk SN210W oferuje wysoką wydajność i bogactwo funkcji podnoszących bezpieczeństwo na styku sieci. Liczba opcji dostępnych w podstawowym pakiecie serwisowym może nie jest imponująca, ale już za niewiele większą opłatę roczną można zyskać pakiet funkcji, który znacznie podwyższy poziom bezpieczeństwa oferowanego przez urządzenie. Dopracowania wymagają opcje związane z obsługą sieci bezprzewodowej – w tym zakresie pojawiło się najwięcej niedomagań w trakcie testu. Wprowadzone w najnowszej wersji oprogramowania ulepszenia, typu wsparcie dla wielu baz użytkowników czy klasyfikacja ruchu w oparciu o geolokalizację i bazę reputacji oraz funkcja sandboxingu w chmurze producenta, to elementy, które mogą zadecydować o wyborze SN210W spośród innych produktów dostępnych na rynku. Zgodnie z informacjami otrzymanymi od producenta, już we wrześniu br. usunięty zostanie problem używania znaków specjalnych w hasłach dla sieci bezprzewodowych (wersja 3.3 firmware dla Stormshield SN210W). Producent również pracuje nad wsparciem dla RADIUS w urządzeniach serii W, tj. SN210W i SN160W.

Werdykt

Stormshield SN210W

Zalety

- świetnie spolszczony, intuicyjny interfejs WebGUI
- wysoka wydajność w tej klasie
- reguły w oparciu o geolokację
- wyczerpująca analiza aplikacji
- pasywny skaner zagrożeń

Wady

- brak wsparcia dla 802.11ac
- brak obsługi uwierzytelniania RADIUS dla Wi-Fi
- miejscami zagmatwana organizacja menu

Ocena **8**/10