Test: sieci przemysłowe UTM Stormshield SNi40 s. 48

Konteneryzacja – Docker a bezpieczeństwo s. 26

5
2018

Miesięcznik informatyków i menedżerów IT

www.it-professional.pl

IT professional

Nr 5 (78) maj 2018 — Cena 33,00 zł (w tym 5% VAT)

TELEKONFERENCJE I WIZUALIZACJA INFORMACJI

s. 10

Zdalna komunikacja w firmie. Systemy do konferencji online i strumieniowania wideo – funkcjonalność, usługi i rodzaje systemów konferencyjnych. Prezentacja i wyświetlanie danych jako istotny aspekt komunikacji. Przegląd narzędzi Business Intelligence do wizualizacji danych

s. 38

Zarządzanie aktualizacjami systemów i oprogramowania

Procesy wdrażania aktualizacji a cyberbezpieczeństwo organizacji

s. 56

Polityka prywatności dla usługi IT zgodnie z rodo

Ochrona danych osobowych. Zakres i cele przetwarzania

s. 62

Automatyzacja i orkiestracja w Linuksie

Open SaltStack – darmowe rozwiązanie open source

ISSN 2083-9588

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

DOSTĘPNE E-WYDANIE

Rozwiązania klasy UTM firmy Stormshield były już dwukrotnie obiektami naszych testów i przyznane zostały im nagrody w plebiscycie na produkt roku. Tym razem postanowiliśmy przyjrzeć się nowości w portfolio producenta – rozwiązaniu dedykowanemu do pracy w trudnych warunkach, a więc przeznaczonemu do zabezpieczenia ruchu w sieciach przemysłowych.

Stormshield SNi40

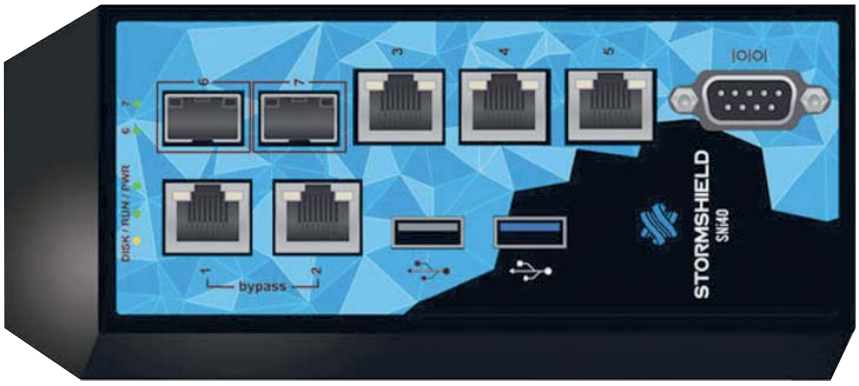
UTM dla sieci przemysłowych

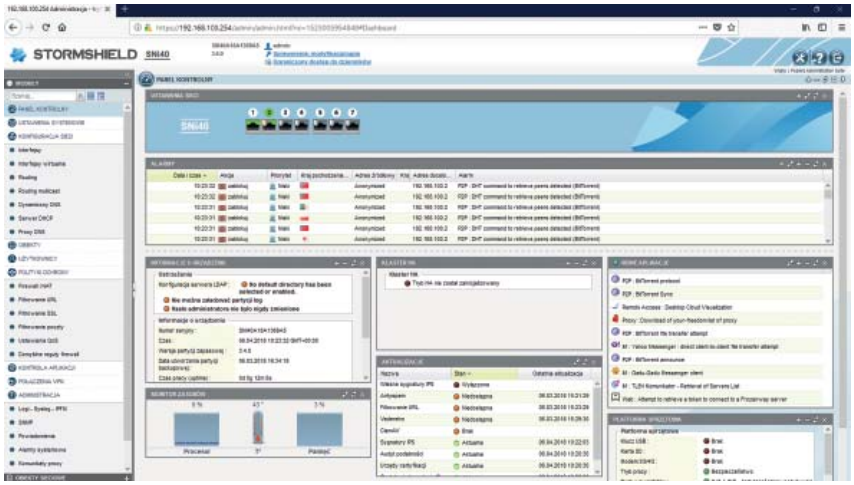
Marcin Jurczyk

UTM i sieci przemysłowe to tandem, który jeszcze do niedawna ciężko sobie było wyobrazić. O ile tradycyjne środowiska IT od wielu lat są zabezpieczane na poziomie zróżnicowanych urządzeń filtrujących ruch i kontrolujących dostęp do zasobów, o tyle w świecie OT (Operational Technology) rządziły zgoła inne prawa i reguły gry. Chyba nikomu nie trzeba tłumaczyć, jak istotne z punktu widzenia rachunku zysków i strat, jest utrzymanie ciągłości działania linii produkcyjnej. Warto też pamiętać, że automatyczne sterowanie produkcją może dotyczyć zarówno niewielkiej fabryki cukierków, jak i elektrowni o strategicznym znaczeniu na poziomie całego kraju. Oczywiście w każdym przypadku mamy do czynienia z nieco innym ciężarem gatunkowym, a co za tym idzie, inną architekturą systemu. W obu przypadkach istnieje jednak wspólny mianownik w postaci sieci przemysłowej, której stabilne działanie odgrywa kluczową rolę.

Szeroko rozumiane bezpieczeństwo sieci przemysłowej to od pewnego czasu coraz bardziej nośny temat. Próby ataków i kompromitacja zabezpieczeń wydawałoby się strategicznych obiektów w różnych zakątkach świata to coraz częstsze motywy przewodnie w serwisach informacyjnych. Do grona producentów rozwiązań bezpieczeństwa dla środowisk OT w ostatnim czasie dołączył Stormshield – francuski producent systemów bezpieczeństwa, dotychczas kojarzony głównie z tradycyjnymi produktami dla IT. Testowany model SNi40 to na razie jedyne rozwiązanie Stormshielda przystosowane do pracy w sieciach przemysłowych, charakteryzujących się nie tylko specyficznym zestawem protokołów sterowania, ale także dużo bardziej wymagającymi warunkami środowiskowymi, jak zapylenie, wilgoć czy dużo szerszy zakres temperatur. Jest to na tyle nowe rozwiązanie, że póki co lista referencyjna dotyczy głównie wdrożeń we Francji. Postanowiliśmy zatem sami sprawdzić, czego można się spodziewać po najnowszym produkcie Stormshielda.

SNi40 nie posiada żadnych elementów mechanicznych, takich jak wentylatory czy tradycyjny dysk twardy, co zmniejsza ryzyko wystąpienia ewentualnych awarii, a zakres temperatur, w jakich może pracować, jest charakterystyczny dla środowisk przemysłowych (od -40 do +70 stopni C). Relatywna wilgotność operacyjna to zakres od 0 do 90%.





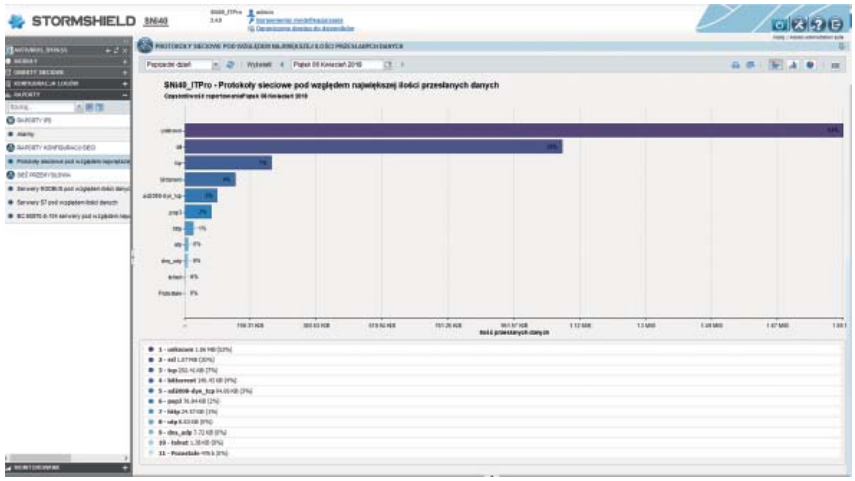
Panel kontrolny to centralny punkt informacji o statusie pracy urządzenia. Podobnie jak reszta webGUI jest identyczny jak dashboardy w pozostałych UTM-ach firmy Stormshield.

> SPRZĘT I WYDAJNOŚĆ

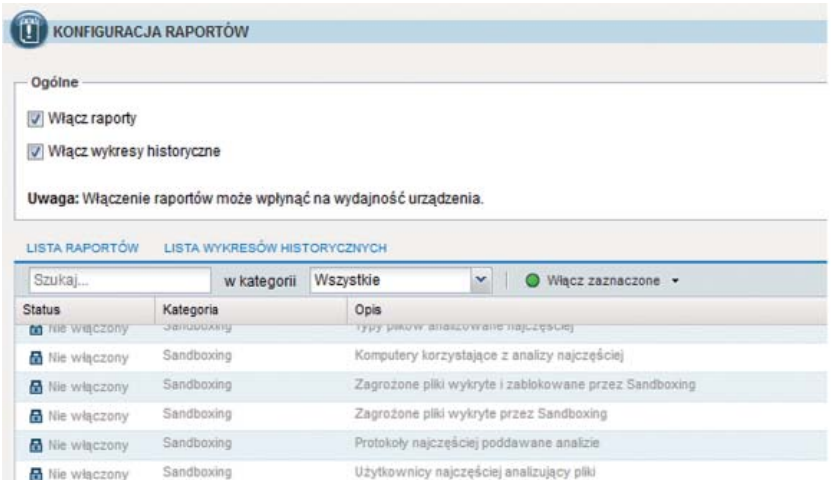
Urządzenia przeznaczone do pracy w środowiskach OT różnią się od analogicznych rozwiązań przeznaczonych dla świata IT chociażby pod względem zasilania i budowy. Nie inaczej jest też w przypadku SNi40. UTM zamknięty został w kompaktowej obudowie 1U/2U przeznaczonej do instalacji na szynie DIN. Obudowa posiada wyprowadzenie na kabel uziemienia, a sam UTM może być redundantnie zasilany. Standard zasilania to 2x 12-36 V DC 5-1,67 A, a fizyczne podłączenie zasilania realizuje się, wpinając odpowiednie przewody w oznaczone gniazda na obudowie urządzenia. Zewnętrzny zasilacz 230 V z odpowiednią przejściówką dostarczany jest opcjonalnie. Sporą część obudowy zajmuje radiator odpowiedzialny za odprowadzenie ciepła. SNi40 nie posiada żadnych elementów mechanicznych, takich jak wentylatory czy tradycyjny dysk twardy, co zmniejsza ryzyko wystąpienia ewentualnych awarii. Zakres temperatur, w jakich może pracować UTM, jest charakterystyczny dla środowisk przemysłowych – wynosi od -40 do +70 stopni Celsjusza. Relatywna wilgotność operacyjna to zakres od 0 do 90%. Producent definiuje średni czas pomiędzy awariami (MTBF) na poziomie 26,6 roku. SNi40 legitymuje się też całym szeregiem certyfikacji, zaczynając od najprostszego IP30, przez bardziej abstrakcyjne dla administratora standardowego środowiska IT certyfikaty kompatybilności elektrycznej i elektromagnetycznej CE/FCC, EN 61000-6-2:2005, certyfikaty odporności na wstrząsy i trudne warunki pracy EN 61000-6-4:2007/A1:2011 oraz IEC 6100-4-18:2006/A1:2010, a na certyfikacie do zdolności działania w ekstremalnych temperaturach IEC 60068-2 kończąc.

UTM wyposażony został w 5 miedzianych interfejsów Ethernet 10/100/1000 oraz 2 gniazda na wkładki światłowodowe 1 Gbps. Co istotne – dwa pierwsze porty mogą działać w trybie bypass. Umożliwia to ciągłość komunikacji nawet w przypadku awarii zasilania. W naszym środowisku testowym odpięcie zasilania powodowało utratę komunikacji na poziomie 2 sekund. Aby skorzystać z opcji bypassu, konieczne jest włączenie w odpowiedniej sekcji ustawień systemowych UTM-a tak zwanego trybu bezpiecznego. Poza portami komunikacji sieciowej dostępne są także 2 porty USB – 2.0 i 3.0, do których podłączyć można dysk USB lub modem 3G/4G. Producent zadbał także o wyprowadzenie dedykowanego portu szeregowego. Pamięć wewnętrzną zrealizowano w oparciu o dysk SSD o pojemności 32 GB. Producent deklaruje maksymalną wydajność UTM-a w trybie zapory sieciowej na poziomie 4,8 Gb/s. Rozszerzenie funkcji zapory o funkcję IPS powoduje degradację wydajności do poziomu 2,9 Gb/s dla 1518-bajtowej ramki danych UDP i do 1,8 Gb/s dla plików ściąganych za pośrednictwem protokołu HTTP o pojemności 1 MB.

W przypadku ochrony sieci przemysłowej to właśnie mechanizmy ochrony, wykorzystujące reguły zapory i systemu IPS, stanowią o ochronie przed potencjalnymi atakami. Podobnie jak



Administrator ma możliwość wyboru spośród predefiniowanych raportów.



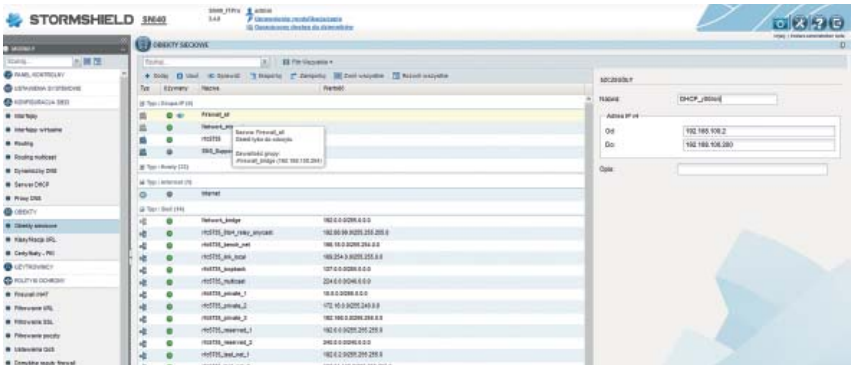
Wśród dostępnych raportów można znaleźć również te dedykowane dla protokołów sieci przemysłowych.

w przypadku pozostałych urządzeń firmy Stormshield, SNi40 potrafi także terminować tunele VPN w oparciu o IPSec oraz SSL. W pierwszym przypadku obsługiwanych jest do 500 tuneli działających z przepustowością do 1,1 Gb/s (dla AES 128). W przypadku SSL VPN możliwe jest utworzenie do 100 tuneli lub obsługa do 75 klientów za pośrednictwem portalu. Parametry te są dość imponujące, choć ciężko sobie wyobrazić aż takie zapotrzebowanie na bezpieczne tunele VPN terminowane na urządzeniu UTM przeznaczonym do ochrony sieci OT. Bardziej przydatna z pewnością okaże się duża liczba wspieranych równolegle sesji na poziomie 500 000 oraz wsparcie dla 20 000 nowych sesji na sekundę. Przy systemach automatyki kontrolujących niezliczoną liczbę czujników, detektorów czy innego rodzaju elementów kluczowych dla kontroli procesu produkcyjnego ten parametr akurat może okazać się istotny. Wspierane protokoły przemysłowe to: Modbus, S7 200-300-400, EtherNet/IP, OPC UA, OPC DA oraz IEC-60870-5-104. W odróżnieniu od UTM-ów Stormshield przeznaczonych do ochrony sieci IT (a więc głównie serwerów i użytkowników) producent skaluje swoje urządzenie nie ze względu na liczbę użytkowników, ale na liczbę chronionych programowalnych sterowników logicznych PLC, która w przypadku SNi40 wynosi 15.

Partnerstwo technologiczne z firmami Siemens i Schneider pozwala na ciągłe udoskonalanie produktu. Różnica pomiędzy SNi40 a pozostałymi rozwiązaniami UTM Stormshielda kończy się w zasadzie na warstwie sprzętowej. Pozostałe właściwości, takie jak firmware, konsola zarządzania, sygnatury IPS czy wsparcie dla wspólnej platformy zarządzania Stormshield Management Center i Visibility Center, pozostają wspólne dla produktów IT oraz OT.

> FUNKCJE BEZPIECZEŃSTWA

Poza wyżej opisanymi zmianami w architekturze sprzętowej, SNi40 to regularny UTM nieodbiegający znacznie funkcjonalnością od pozostałych modeli dostępnych w ofercie producenta. Charakterystyka środowiska przemysłowego dyktuje jednak nieco inne priorytety w kontekście bezpieczeństwa sieci – to nie użytkownik wraz z całą listą aplikacji i usług jest głównym podmiotem dla systemu zabezpieczeń, a system sterowania produkcją. W związku z powyższym w przypadku SNi40 nie znajdziemy funkcji takich jak ochrona antywirusowa, antyspamowa czy filtrowanie na podstawie adresów URL. Cały model licencyjny bazuje na dwóch poziomach zabezpieczeń – Industrial Security Pack oraz Industrial Plus Security Pack. W pierwszym przypadku mamy do czynienia z zabezpieczeniem w oparciu o NG firewall oraz IPS. Pakiet „Plus" to dodatkowo funkcja audytu podatności. Oba pakiety zawierają także licencję na tunele VPN IPSec oraz SSL. Kupując SNi40, należy zatem liczyć się z kosztem samego urządzenia na poziomie 2000 euro oraz wybranej opcji serwisowej. Do wyboru pozostaje długość subskrypcji – 1, 3 lub 5 lat. Podobnie jak inne rozwiązania Stormshielda, również SNi40 może pracować w klastrze wysokiej dostępności active-passive. W takim przypadku należy liczyć się z podwójnym kosztem za samo urządzenie oraz dodatkową opłatą za podstawowy pakiet serwisowy HA, gdyż oba urządzenia muszą działać w oparciu o tę samą wersję firmware'u wraz z aktualnymi sygnaturami.



Obiektowe podejście do definiowania reguł to element charakterystyczny dla rozwiązań Stormshield.

W kontekście pozostałych aspektów działania SNi40 osoby zainteresowane zakupem można w zasadzie odesłać do testu modelu SN210W („IT Professional" 09/2017, s. 49), a czytając test, wystarczy pamiętać o braku wyżej wymienionych funkcji. Za fizyczną realizację mechanizmów bezpieczeństwa odpowiada w dalszym ciągu specjalizowany system operacyjny NETASQ Secured BSD (NS-BSD). Testowane urządzenie pracowało pod kontrolą najnowszego NS-BSD w wersji 3.2.4, a więc trzon funkcjonalności był zbliżony do poprzednio testowanego przez nas modelu, który działał w oparciu o wersję 3.2.1. Fundamenty wydajności i funkcjonalności systemu pozostały bez zmian – wydajność platformy w dalszym ciągu opiera się na opatentowanej technologii proaktywnego wykrywania ataków o nazwie ASQ (Active Security Qualification), co w praktyce sprowadza się do integracji funkcji firewalla z IPS na poziomie jądra systemu operacyjnego, dzięki czemu ograniczona zostaje liczba operacji koniecznych do przeanalizowania każdego pakietu oraz częściowo wyeliminowana wielokrotna analiza tych samych danych przez poszczególne moduły bezpieczeństwa. Jak już wspomniano, zapora ogniowa i IPS to elementy kluczowe z punktu widzenia zabezpieczenia sterowników sieci przemysłowej i właśnie na tym poziomie odbywa się blokowanie potencjalnie niebezpiecznego ruchu w kierunku systemu sterowania produkcją. Na poziomie reguł zapory definiowanych dla konkretnych użytkowników realizowane mogą być polityki dostępu do elementów infrastruktury OT. Z kolei dedykowane dla ochrony protokołów przemysłowych sygnatury IPS mają za zadanie odfiltrować potencjalne ataki i zagrożenia. W obecnej wersji oprogramowania pojawiło się około 150 sygnatur więcej w stosunku do rewizji 3.2.1, w której znaleźć można było 1941 pozycji, również tych przeznaczonych dla protokołów przemysłowych (dedykowane 52 sygnatury w najnowszej wersji). Do nowości w wersji 3 NS-BSD, na które zwróciliśmy uwagę w teście modelu SN210W, warto zaliczyć budowanie reguł w oparciu o geolokację oraz reputację adresów IP. Choć funkcja ta dostępna jest również na SNi40, prawdopodobnie okaże się mało przydatna w dość mocno izolowanych od ruchu globalnego sieciach przemysłowych.

Funkcja audytu podatności, dostępna w pakiecie serwisowym Plus, pozwala 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 i podatnościach związanych z korzystaniem z nich. Może to okazać się przydatne w kontekście identyfikacji potencjalnych zagrożeń na stacjach sterowania i w nastawniach. IT

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

PODSUMOWANIE

SNi40 to jak na razie pierwsze i jedyne rozwiązanie w portfolio produktów Stormshielda specjalizowane do ochrony sieci przemysłowych. Tematyka bezpieczeństwa to ostatnimi czasy temat nośny, wymagający sporo uwagi i chyba właśnie te elementy przesądziły o zaistnieniu na rynku rozwiązań dla środowisk OT. Administratorzy mający dotychczas do czynienia z produktami UTM tego producenta z pewnością docenią interfejs webGUI uniwersalny dla całej linii UTM-ów. Dzięki temu czas wdrożenia jest znacznie krótszy, a prawdopodobieństwo popełnienia błędu podczas konfiguracji mniejsze. Parametry wydajnościowe w zestawieniu z ceną rozwiązania również zasługują na uwagę i mogą być elementem decydującym podczas wyboru dostawcy zabezpieczeń dla sieci przemysłowej. Na ile debiut Stormshielda na rynku OT okaże się sukcesem, czas pokaże. Z racji tego, że jest to nowość, brakuje na razie referencji z polskiego rynku. Coraz większa świadomość branży pozwala jednak wierzyć w sukces.

Werdykt

Stormshield SNi40

Zalety

- świetnie spolszczony, intuicyjny interfejs WebGUI
- identyczny interfejs dla wszystkich produktów
- duża wydajność
- zgodność z certyfikatami przemysłowymi
- cena
- proste zasady licencjonowania

Wady

- ograniczony wybór – jedyny produkt OT w ofercie producenta

Cena

Urządzenie – 2000 euro

Industrial Security Pack (FW+IPS, VPN) – 320 euro (1 rok)

Industrial Plus Security Pack (FW+IPS, VPN, audyt podatności) – 500 euro (1 rok)

Ocena **8**/10