Miesięcznik informatyków i menedżerów IT

it-professional.pl

12
2022

# Test: Stormshield SN-M-Series 720 s. 64

# Introspekcja i mapy maszyn wirtualnych s. 48

# IT professional

Nr 12 (133) grudzień 2022

PRODUKT ROKU 2022

## Analiza awarii w OVHcloud s. 27

**Stan wiedzy po 18 miesiącach od incydentu**

## Wazuh – monitorowanie bezpieczeństwa hostów s. 40

**Otwartoźródłowy system wykrywania włamań do urządzeń podłączonych do sieci**


## KSIĄŻKA GRATIS

**Funkcje bezpieczeństwa Microsoft Office 365**

Cena 41,00 zł (w tym 8% VAT)
ISSN 2083-9588

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

Kompletny system bezpieczeństwa zapewniający ochronę na brzegu sieci to rozwiązanie obejmujące wiele obszarów, takich jak IPS, filtrowanie stron internetowych, antywirus, antyspam, VPN czy analiza podatności. Tym razem testujemy UTM firmy Stormshield – SN-M-Series 720.

12/2022 REKOMENDACJA REDAKCJI IT professional

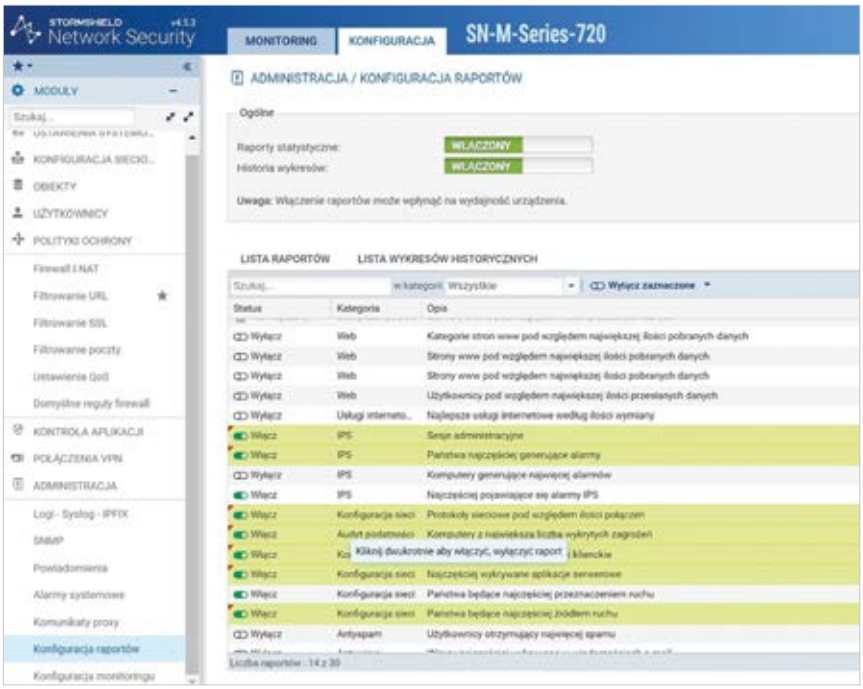
ZABEZPIECZENIA UTM

# Stormshield SN-M-Series 720, czyli kompleksowa ochrona

**Piotr Maziakowski**

Model SN-M-Series 720 to nowy produkt w ofercie zapór ogniowych Stormshielda, wprowadzony na rynek w połowie bieżącego roku. Urządzenie przeznaczone jest dla średnich i dużych organizacji. Stormshield ulokował w jednym narzędziu wiele usług zabezpieczających, m.in. wbudowany antywirus, firewall/IPS/IDS, filtrowanie stron internetowych, filtrowanie adresów URL, wykrywanie aplikacji i zarządzanie nimi, antyspam i antyphishing oparte na reputacji, deszyfrowanie SSL (HTTP, SMTP, POP3, FTP). Opcja dodatkowa to możliwość uruchomienia zaawansowanego silnika antywirusowego oraz sandboxu w chmurze Stormshield hostowanej w Europie. Dzięki zastosowanym technologiom otrzymujemy ochronę przed takimi zagrożeniami jak wirusy, próby nieautoryzowanego dostępu, kontrolę aplikacji, zarządzanie lukami w zabezpieczeniach, blokowanie hostów na podstawie reputacji czy geolokalizacji.

Przede wszystkim możemy zdefiniować dowolny zestaw reguł określających, jaki ruch powinien być przez firewall przepuszczany, a jaki blokowany. Testowane urządzenie wyposażono w moduł QOS pozwalający na zapewnienie gwarantowanej przepustowości lub ograniczenie przepustowości dla




Stormshield w swojej zaporze zapewnia duże możliwości raportowania. Do dyspozycji mamy 30 predefiniowanych raportów gotowych do użycia.

każdej reguły filtrowania zdefiniowanej na firewallu. Priorytety można również przypisać do określonego typu ruchu wraz z rezerwacją przepustowości. SN-M-Series 720 pozwala na jednoczesne utrzymywanie i wykorzystywanie kilku połączeń z internetem. Komunikacja może być dzielona równomiernie na wszystkie aktywne połączenia, które w razie awarii jednego z łączy automatycznie przejmują jego funkcję. Gdy ulegnie zerwaniu podstawowe połączenie z internetem, jako jedno z łączy zapasowych można wykorzystać modem GSM podłączany do portu USB. Zapewnienie wysokiej dostępności realizuje funkcja high availability (HA). Wybrany ruch sieciowy wymagający wysokiej dostępności będzie przechodzić przez łącza HA, nie możemy

np. podczas tworzenia interfejsu VLAN wskazać interfejsów HA. Klaster urządzeń Stormshield działa w trybie aktywny–pasywny. W przypadku gdy jeden UTM z klastra ulegnie awarii, drugi (pasywny) przejmie jego funkcję i stanie się aktywny. Korzystając z dwóch dostawców łącz internetowych, do dyspozycji mamy funkcję load balancingu, gdzie równoważenie obciążenia odbywa się na podstawie adresu źródłowego lub rodzaju połączenia. Definiując dwie bramy do internetu, możemy na bieżąco weryfikować za pomocą pinga wysyłanego do wskazanej grupy hostów dostępność danej bramy, tak aby ruch był kierowany zawsze do tej aktywnej.

## > BUDOWA I SPECYFIKACJA

Model SN-M-Series-720 ma metalową obudowę o wysokości 1U i jest przystosowany do montażu w szafie rack 19''. Panel przedni wyposażono w następujące elementy:

- port szeregowy umożliwiający dostęp do urządzenia w trybie konsoli poprzez podłączenie bezpośrednio z komputerem;
- dwa porty USB 3.0, których można użyć do konfiguracji lub aktualizacji, a także do podłączenia klucza USB, klawiatury USB lub modemu USB;
- przycisk służący do resetowania urządzenia do ustawień fabrycznych (Defaultconfig);
- przycisk Reset służący do resetu zasilania urządzenia;
- port USB-C umożliwiający dostęp do produktu w trybie konsoli;
- dwa porty światłowodowe SFP+ z obsługą 10 GbE;
- osiem portów z obsługą 2,5 GbE;
- kieszeń na instalację modułu rozszerzeń – w tym modelu można dodać jeden moduł rozszerzający z RJ-45 (1 Gb lub 10 Gb) lub portem światłowodowym (1 Gb lub 10 Gb).

W tylnej części mamy dwa wewnętrzne zasilacze zapewniające redundantne zasilanie. Model SN-M-Series-720 przeznaczony jest dla średnich firm do 300 użytkowników, ale wraz z rozwojem firmy istnieje możliwość zwiększenia liczby użytkowników np. do 500. Taka skalowalność wynika z tego, iż modele SN-M-Series-720 i SN-M-Series-920 mają wspólny hardware i w zależności od posiadanej licencji platforma SN-M-Series (fizyczny sprzęt) może być modelem SNM-Series-720 lub SN-M-Series-920. Aktualizacji do modelu SN-M-Series-920 dokonujemy poprzez instalację nowej licencji.

SN-M-Series-720 wyposażono w wielordzeniowy procesor, co zapewnia wysoką moc obliczeniową:

- wydajność firewalla: 18 Gb/s,
- wydajność IPS (1518 byte UDP): 10 Gb/s,
- wydajność IPS (1 Mbyte HTTP files): 5 Gb/s,
- wydajność antywirusa: 3 Gb/s,
- wydajność VPN IPSec: 4 Gb/s,
- liczba tuneli VPN: 1000,
- liczba klientów SSL VPN (portal mode) – 300,
- liczba jednoczesnych połączeń VPN – 300.

Co ciekawe, wraz z aktualizacją licencji do wersji SN-M-Series-920 uzyskamy dwukrotne zwiększenie wydajności niemalże w każdym parametrze.

## > PANEL STEROWANIA I FUNKCJE

Urządzeniem możemy zarządzać z poziomu przeglądarki internetowej lub konsoli znakowej. Zaletą jest to, że UTM ma obsługę w języku polskim, jednak nie przetłumaczono wszystkich komunikatów, np. szczegółów błędów, co powoduje, że czasem wygodniej przełączyć się na język angielski, aby nazwy funkcji i interfejsów w widoku były takie same jak w komunikatach błędów. Warto podkreślić, że obsługa błędów jest bardzo pomocna i z samych komunikatów można bez kłopotu wywnioskować, jakie ustawienie powoduje problem. Opcje w menu pogrupowano i umieszczono po lewej stronie interfejsu. Z menu głównego dostępne są grupy: Ustawienia systemowe, Konfiguracja sieciowa, Obiekty, Użytkownicy, Polityki ochrony, Kontrola aplikacji, Połączenia VPN i Administracja. Interfejs jest przejrzysty, a poszczególne funkcje umieszczono logicznie, co pozwala po krótkim zapoznaniu sprawnie nawigować.

**Testowane urządzenie wyposażono w moduł QOS pozwalający na zapewnienie gwarantowanej przepustowości lub ograniczenie przepustowości dla każdej reguły filtrowania zdefiniowanej na firewallu.**

Z poziomu ustawień systemowych mamy dostęp do informacji o systemie, aktualizacjach czy ustawień sposobu uwierzytelnienia do interfejsu zarządzania oraz definiowania uprawnień do zarządzania urządzeniem. Można definiować uprawnienia pełne lub tylko do odczytu w zakresie wszystkich podstawowych funkcji urządzenia, jak firewall i NAT, VPN, logi, IPS, filtry treści, interfejsy.

Z poziomu menu Konfiguracja sieciowa możemy zarządzać interfejsami sieciowymi, dodawać je, edytować lub usuwać. Do dyspozycji mamy:

- Bridge interface – logiczny interfejs łączący kilka interfejsów fizycznych lub VLAN;
- Ethernet interface – fizyczny interfejs wbudowany w urządzenie lub moduł rozszerzający;
- VLAN interface – segment sieci;
- Aggregate – umożliwia włączenie funkcji LACP, która pomaga poprawić przepustowość zapory sieciowej, gdyby łącze główne w agregacji przestało odpowiadać;
- GRETAP – pozwala na enkapsulację ruchu na warstwie drugiej modelu ISO/OSI, funkcji można użyć do łączenia witryn współdzielących ten sam zakres adresów IP z wykorzystaniem protokołu GRE;
- PPPoE/PPTP modem interface – umożliwia obsługę połączeń typu PPPoE, PPP, PPTP i 3G;

- USB/ethernet interface – pozwala na podłączenie modemu USB bezpośrednio do UTM.

## > FILTROWANIE POŁĄCZEŃ

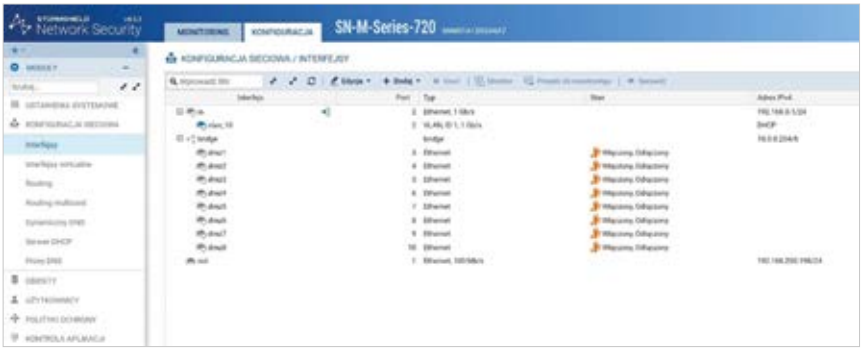
Jeśli chodzi o konfigurację zapory, do dyspozycji mamy zestaw reguł domyślnych (ang. implicit rules) zdefiniowanych na urządzeniu oraz możliwość konfigurowania własnych polityk. Reguły domyślne umożliwiają komunikację z UTM-em nawet w sytuacji, gdy zdefiniowane przez administratora polityki zablokują taką komunikację, dzięki czemu nie traci się łączności z urządzeniem. Reguły domyślne możemy włączyć i wyłączyć, ale nie da się ich edytować. Analiza pakietów w pierwszej kolejności realizowana jest przez reguły domyślne, następnie pakiet dopasowywany jest do reguł zdefiniowanych przez administratora.

W ramach zdefiniowanych profili mamy pięć pozycji ze wstępnie zdefiniowanymi zasadami ochrony i pięć do indywidualnego zdefiniowania:

- blokuj wszystkie 01 – domyślnie włączone w ustawieniach fabrycznych, gdzie otwarte będą tylko porty używane do zarządzania firewallem (1300/TCP i 443/TCP), a wszystkie inne połączenia są blokowane;
- wysokie 02 – dozwolony jest tylko ruch sieciowy e-mail i FTP oraz ping z wewnętrznych interfejsów na zewnątrz;
- średnie 03 – ochrona obejmuje połączenia wychodzące na podstawie domyślnej definicji protokołów na urządzeniu, np. dla portu 80 zezwolony będzie tylko ruch HTTP, w przypadku innego połączenia niż HTTP na porcie 80 zostanie ono zablokowane; akceptowane są w tym profilu wszystkie połączenia, których nie zdefiniowano na liście protokołów;
- niskie 04 – wymuszona jest analiza protokołu dla połączeń wychodzących;
- filtr w pozycji 05–09 – to puste zasady;
- przepuszczaj wszystko – zezwolony jest cały ruch sieciowy na wszystkich portach.

Wykorzystanie profili z domyślnym zestawem oraz możliwość zdefiniowania pięciu własnych zestawów reguł ułatwiają wdrożenie oraz wprowadzanie i testowanie zmian. Bez dotykania reguł w profilu produkcyjnym możemy wprowadzać zmiany w innych profilach, a do testów podmieniać tylko profil. Użyteczną funkcją z poziomu reguł firewalla jest możliwość wyszukiwania w logach oraz monitoringu. Wyszukaj w logach prowadzi do menu Logi z aktywnym filtrem wyświetlającym wpisy dla tylko zaznaczonej reguły firewall, natomiast Wyszukaj w monitoringu prowadzi do menu Monitorowanie, gdzie od razu mamy wyświetlone aktywne połączenia odnoszące się do zaznaczonej reguły.

Lokalne polityki ochrony definiujemy w opcji Firewall i NAT w ramach profili. W danym momencie wykorzystywany może być tylko jeden profil z zestawem reguł. Każdy profil umożliwia zdefiniowanie zasad i sposobu filtrowania ruchu sieciowego. Wykorzystywane są m.in. firewall/IPS/IDS, firewall aplikacyjny, filtrowanie Microsoft Services, jako opcja przemysłowy firewall/IPS/IDS, wykrywanie i kontrola wykorzystywanych urządzeń mobilnych, filtrowanie oparte na geolokacji (kraje, kontynenty), dynamiczna reputacja hosta, filtrowanie adresów URL na podstawie wbudowanego filtra lub bazy danych adresów w chmurze, a także istnieje możliwość podpięcia polskiej bazy dresów blokowanych. Filtrowanie opiera się na porównaniu odebranego pakietu IP z kryteriami zawartymi w regułach aktywnej polityki. Użyteczną funkcją jest możliwość sprawdzenia zasad firewalla, który pilnuje, czy utworzona reguła nie blokuje innej lub czy w samej regule nie ma błędu – wówczas ostrzega przed jej zatwierdzeniem.




Menu – interfejsy sieciowe.

## > INTRUSION PREVENTION

Stworzony przez Stormshielda system zapobiegania włamaniom (ang. Intrusion Prevention System, IPS) wykorzystuje technologię wykrywania i blokowania ataków ASQ (ang. Active Security Qualification). W procesie poszukiwania zagrożeń i ataków analizie poddawany jest cały ruch sieciowy od warstwy L3 (ang. network layer) do warstwy L7 (ang. application layer) modelu ISO/OSI. IPS bazuje na analizie heurystycznej, analizie protokołów oraz analizie na podstawie sygnatur kontekstowych.

Analiza heurystyczna na podstawie statystyk i zachowań określa, czy dany ruch powinien być zezwolony, czy zablokowany jako potencjalny atak. Analiza protokołów kontroluje zgodność ruchu sieciowego przechodzącego przez urządzenie ze standardami RFC i tylko ruch zgodny ze standardem jest zezwalany. Kontrola protokołów obejmuje zarówno pakiety, jak i sesje. Stormshield dynamicznie dostosowuje ochronę do typu protokołu poprzez dedykowane pluginy, które po wykryciu rodzaju protokołu (np. HTTP, FTP, SMTP, DNS) odpowiadają za jego ochronę. Sygnatury kontekstowe, systematycznie aktualizowane, umożliwiają wykrycie znanych już ataków, jakie zostały sklasyfikowane i dla

których opracowano odpowiednie sygnatury. Blokowanie na podstawie sygnatur kontekstowych bierze pod uwagę, gdzie wykryto atak, tzn. rodzaj połączenia, protokół i port. Wystąpienie sygnatury ataku w niewłaściwym dla niego kontekście nie powoduje reakcji IPS-a, co eliminuje liczbę fałszywych alarmów.

Konfiguracja IPS-a zawiera podobnie jak konfiguracja firewalla 10 predefiniowanych profili, które dowolnie konfigurujemy. Jednocześnie możemy wybierać różne profile IPS dla ruchu przychodzącego i wychodzącego.

Stormshield pozwala na analizowanie ruchu HTTPS w celu ochrony aplikacji z wykorzystaniem systemu antywirusowego, opcjonalnie sandboxa w chmurze Stormshield. Aby włączyć na urządzeniu filtrowanie i analizę połączeń HTTPS, wymagane jest skonfigurowanie serwera proxy SSL. Dla wybranych serwisów internetowych istnieje możliwość włączenia funkcji bypass_ssl, co spowoduje pominięcie tych adresów (funkcja często wykorzystywana przy połączeniach z serwisami bankowości internetowej).

## > ZARZĄDZANIE UŻYTKOWNIKAMI

Urządzenie umożliwia integrację z wieloma bazami użytkowników typu LDAP, jak Active Directory, OpenLDAP, SPNEGO, czy też wykorzystanie wewnętrznej bazy LDAP przechowującej profile użytkowników oraz powiązany certyfikat X.509. Dzięki możliwościom integracji reguły na firewallu mogą być tworzone dla zalogowanego lub niezalogowanego użytkownika. Każdorazowo login uwierzytelnionego użytkownika jest łączony z hostem, z którego nastąpiło logowanie, a wszystkie pakiety generowane przez użytkownika są oznaczone jego identyfikatorem i zapisane zgodnie z przyjętą przez administratora polityką retencji.

Możemy również zdefiniować konta tymczasowe, które będą automatycznie blokowane po zadanym okresie, co jest bardzo pomocne w przypadku tworzenia kont dla dostawców zewnętrznych, np. na czas realizacji umowy. Urządzenie pozwala na tworzenie kanałów VPN wraz z automatycznie konfigurowanym klientem SSL VPN na Windows oraz wsparciem dla Android/iPhone IPSec VPN. Do wyboru są: IPsec VPN – w trybie client-to-site oraz site-to-site, SSL VPN – w trybie client-to-site, SSL VPN – w trybie client-to-site (portal), PPTP VPN – w trybie client-to-site.

## PODSUMOWANIE

Model SN-M-Series-720 to propozycja zaawansowanej ochrony infrastruktury. Konfiguracja jest bezproblemowa, a uruchomienie podstawowej ochrony dzięki predefiniowanym profilom nie powinno sprawić kłopotu również mniej doświadczonym administratorom. Urządzenie pozwala na dynamiczne zarządzanie łączami i rozbudowę sieci dzięki wielu elastycznym opcjom konfiguracji, a także rozszerzenie licencji na 500 użytkowników czy dołożenie dodatkowego modułu interfejsów miedzianych lub światłowodowych 1 GbE lub 10 GbE. Warto też zauważyć, że Stormshield umożliwia rozbudowę ochrony poprzez opcje dodatkowe wymagające rozszerzonej licencji. Możemy dozbroić sprzęt w takie funkcje jak: audyt podatności, czyli pasywny skaner zagrożeń (SEISMO); zaawansowany skaner antywirusowy (HTTP, POP3, SMTP, FTP, SSL); rozszerzone filtrowanie stron WWW (HTTP, HTTPS) w chmurze Stormshield; Stormshield Breach Fighter, czyli sandboxing bazujący na chmurze; obsługa protokołów przemysłowych (BACnet/IP, CIP, EtherNet/IP, IEC-60870-5-104, Modbus, OPC UA, OPC (DA/HDA/AE), PROFINET IO/RT, UMAS, S7 200-300-400). Testowany model polecamy nawet mniej doświadczonym administratorom ze względu na bogatą dokumentację z przykładami użycia również w języku polskim, a także instrukcje obsługi dostępne w formie wideo. Urządzenie oferuje wysoki poziom wydajności oraz ochrony, zabezpiecza brzeg sieci i kontrolę dostępu użytkowników. Brakuje natomiast centralnej funkcji zarządzania siecią bezprzewodową, która sprawiłaby, że rozwiązanie stałoby się jeszcze bardziej kompletne.

Autor od 2004 r. związany z branżą IT i nowych technologii w obszarze administrowania systemami klasy ERP. Specjalizuje się w realizacji wdrożeń i audytów bezpieczeństwa informacji.

## Werdykt

### Stormshield SN-M-Series 720

**Zalety**

- personalizowany Intrusion Prevention System/Intrusion Detection System (IPS/IDS)
- integracja z LDAP
- kształtowanie pasma (QoS)
- funkcje HA
- filtrowanie stron WWW (HTTP, HTTPS)
- logowanie zdarzeń i raportowanie
- personalizowany VPN
- upgrade licencji do SN-M-Series 920
- możliwości rozbudowy
- rozszerzenia dodatkowe

**Wady**

- brak zarządzania WLAN

Ocena **9**/10