Test: Stormshield SN-L-Series-2200 – wszechstronna zapora s. 50

IAM Identity Center s. 23

2
2025

Miesięcznik informatyków i menedżerów IT

itprofessional.pl

IT professional

Nr 2 (159) luty 2025

HURTOWNIA DANYCH W CHMURZE s. 8

Przegląd możliwości Redshifta – usługi analitycznej w ramach Amazon Web Services – proces konfiguracji, zaawansowane funkcje, zarządzanie kosztami oraz skalowalnością, dobre praktyki, a także zestawienie najistotniejszych plusów i minusów rozwiązania.

AI w decyzjach organów nadzorczych s. 54

Przetwarzanie danych przez modele sztucznej inteligencji w zderzeniu z przepisami rodo

Systemy gaszenia w centrum danych s. 64

Zapobieganie oraz tłumienie pożarów w data center

Ataki typu buffer overflow w testach bezpieczeństwa s. 68

Omówienie podatności na przepełnienie bufora w kontekście pracy współczesnego pentestera

Cena 48,00 zł (w tym 8% VAT)
ISSN 2083-9588
9 772083 958004

DOSTĘPNE E-WYDANIE

Zunifikowane zarządzanie zagrożeniami oraz zapory sieciowe następnej generacji były swego czasu chwytliwymi hasłami marketingowymi, które miały przyciągnąć klienta. Obecnie ta technologia to powszechnie panujący standard. Sprawdzamy, co w jego obrębie ma do zaoferowania Stormshield.

02/2025 REKOMENDACJA REDAKCJI IT professional

UNIFIED THREAT MANAGEMENT

Stormshield SN-L-Series-2200 – wszechstronna zapora

Marcin Jurczyk

Rozwiązania typu Unified Threat Management firmy Stormshield po raz pierwszy pojawiły się na naszym redakcyjnym stole testowym niespełna 10 lat temu. Sama marka była wtedy dość mało znana, choć czerpała technologicznie z produktów znanych pod nazwą Netasq. Na przestrzeni czasu rozpoznawalność nieco wzrosła, a portfolio rozwiązań francuskiego producenta zostało wyraźnie rozszerzone. Poza UTM-ami, pracującymi głównie na brzegu tradycyjnych sieci, pojawiły się także produkty chroniące sieci przemysłowe. Obecnie Stormshield oferuje kilkanaście modeli zapór sprzętowych przeznaczonych do ochrony sieci różnych rozmiarów. W katalogu znajdziemy zarówno małe UTM-y zamknięte w obudowie typu desktop i przeznaczone do ochrony małych biur zdalnych, w których pracuje od kilku do kilkudziesięciu użytkowników, a także wydajne, pełnowymiarowe zapory, mogące chronić ruch sieciowy tysięcy użytkowników z przepustowością kilkudziesięciu gigabajtów na sekundę. Model dostarczony do testów to jedno z bardziej wydajnych pudełek w ofercie, przeznaczone do ochrony środowisk wyskalowanych na około tysiąc użytkowników końcowych.

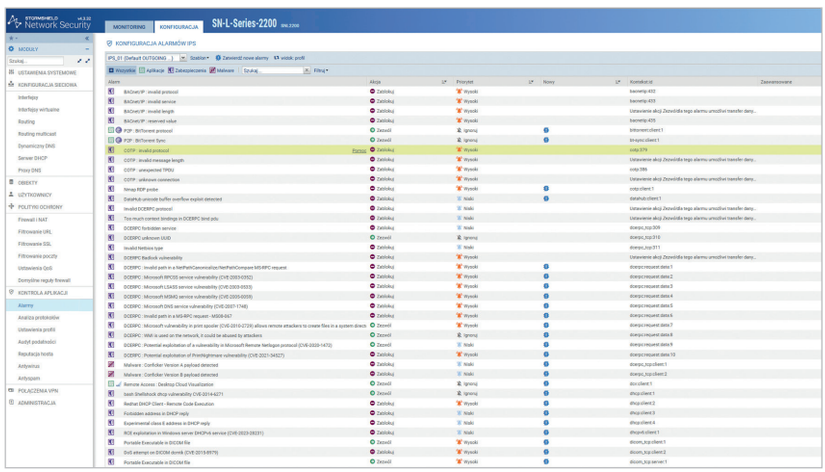
> ARCHITEKTURA I WYDAJNOŚĆ

Testowana zapora klasy NGFW to jeden z dwóch reprezentantów serii L, czyli dużych firewalli klasy korporacyjnej przeznaczonych do ochrony brzegu sieci w największych przedsiębiorstwach. Nomenklatura nazewnicza firmy Stormshield pozwala łatwo nawigować pomiędzy różnymi rodzajami produktów. Serie urządzeń oznaczono dobrze znanymi identyfikatorami typu: XS, S, M, L oraz XL. Osobna kategoria to zapory przeznaczone do ochrony środowisk OT.

Testowany SN-L-Series-2200 to modułowy firewall zamknięty w obudowie rozmiaru 1U, który został wyposażony w redundantne zasilacze i wentylatory hot-swap, a także trzy zatoki do montażu modułów sieciowych. W konfiguracji standardowej dostępne są dwa miedziane porty o przepustowości do 2,5 Gbps, oznaczone jako MGMT1 oraz MGMT2. W praktyce nie są to jednak interfejsy zarządzania typu out-of-band, odseparowane od regularnych portów sieciowych. Po wyjęciu urządzenia z pudełka oba porty ustawione

są jako bridge, na poziomie którego skonfigurowano domyślny adres IP do wykonania wstępnej konfiguracji. Po odpowiednim zaadresowaniu i rekonfiguracji można je z powodzeniem wykorzystać jako regularne porty do obsługi ruchu chronionego i tak też zrobiliśmy na potrzeby naszych testów. Z oczywistych względów w środowisku produkcyjnym warto byłoby jednak doposażyć zaporę w moduły sieciowe przeznaczone do obsługi regularnego ruchu, a porty typu MGMT pozostawić do celów administracyjnych.

Karty rozszerzeń pozwalają na zwiększenie liczby portów w standardzie 2,5 Gbps do 26. Oczywiście dostępne są także moduły w standardzie 10 (miedź lub światłowód) oraz 40 Gbps. Wszystkie wspierane zestawienia można znaleźć w dokumentacji producenta. Wybrane moduły wyposażone w porty miedziane oferują także funkcję bypassu pozwalającą na przekazywanie ruchu nawet wtedy, gdy dojdzie do awarii zapory. Dobierając moduły sieciowe, warto brać pod uwagę także maksymalną wydajność z uwzględnieniem uruchomionych funkcji ochrony. W trybie zapory teoretyczna wydajność dla segmentów UDP o rozmiarze 1518 bajtów sięga 85 Gbps, a po włączeniu IPS-a odpowiednio 52 Gbps. Dla charakterystyki ruchu IMIX wartość ta spada do 30 Gbps w trybie samej zapory. Producent podaje również wydajność IPS-a dla ruchu HTTP 1 MB na poziomie 24 Gbps. Uruchomienie skanera antywirusowego skutkuje degradacją wydajności do poziomu 8 Gbps. Specyfikacja wydajnościowa zawiera sporo dodatkowych parametrów, jak chociażby maksymalna liczba tuneli IPSec zdefiniowana na poziomie 5000 oraz do 2400 równoczesnych sesji klienckich SSL VPN. Urealniona przepustowość IPSec (IMIX) to 7,7 Gbps. SN-L-Series-2200 powinien także poradzić sobie z 5 milionami równoległych połączeń oraz 200 tysiącami nowych połączeń na sekundę. Listing suchych danych wydajnościowych uzupełnia rekomendowana maksymalna liczba reguł na poziomie 16 tysięcy oraz do 1336 interfejsów logicznych.



IPS wraz z głęboką analizą pakietów pozwalają na szczegółową kontrolę ruchu.

Weryfikując nieco głębiej – z poziomu konsoli – architekturę sprzętową, okazuje się, że mamy do czynienia z platformą x86 wyspecjalizowaną pod kątem wysokowydajnej obsługi ruchu sieciowego z zapewnieniem wspominanej już nadmiarowości na poziomie zasilania i chłodzenia, jak również przestrzeni dyskowej (2 × SSD 240 GB RAID1). Za wydajność odpowiada procesor Intel Core i9-13900E, czyli 24-rdzeniowa jednostka wyposażona w osiem rdzeni typu performance oraz 16 rdzeni efficient, taktowanych odpowiednio do 5,2 lub 4 GHz. Na pokładzie znajdziemy też 64 GB RAM-u.

SN-L-Series-2200 to wydajne rozwiązanie mogące chronić środowiska IT i OT. Dla lokalnych firm zaletą będzie fakt, że rozwiązania Stormshielda tworzone są w Europie i uwzględniają wymogi prawne stawiane na gruncie UE.

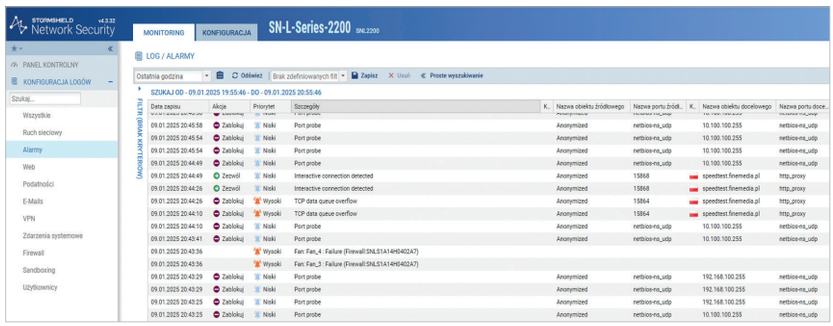
Za realizację mechanizmów bezpieczeństwa po stronie oprogramowania odpowiada wyspecjalizowany system operacyjny NETASQ Secured BSD (NS-BSD) w najnowszej odsłonie 4.8.5, bazujący na jądrze FreeBSD 11.3. Fundamenty OS-u pozostały niezmienione – wydajność platformy w dalszym ciągu opiera się na opatentowanej technologii proaktywnego wykrywania ataków o nazwie ASQ (Active Security Qualification), o której coraz mniej można znaleźć na oficjalnej stronie Stormshielda. W praktyce sprowadza się to do integracji funkcji firewalla z IPS-em 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.

> BEZPIECZEŃSTWO

Testowana zapora, podobnie jak pozostałe modele w ofercie producenta, to pełnokrwiste rozwiązania klasy UTM/NGFW. Funkcje bezpieczeństwa realizowane są na wielu płaszczyznach – zaczynając od standardowej zapory sieciowej typu stateful, poprzez funkcje IDS/IPS, Deep Packet Inspection na antywirusie czy antyspamie kończąc. Dostępne jest również filtrowanie adresów URL, a także

zaawansowana ochrona AV z funkcją sandboxingu w chmurze dostawcy, wymagająca jednak zakupu dodatkowej licencji. W standardzie dostajemy silnik ClamAV. W analogiczny sposób można rozszerzyć możliwości klasyfikacji adresów URL za pośrednictwem opcjonalnej bazy Bitdefendera.

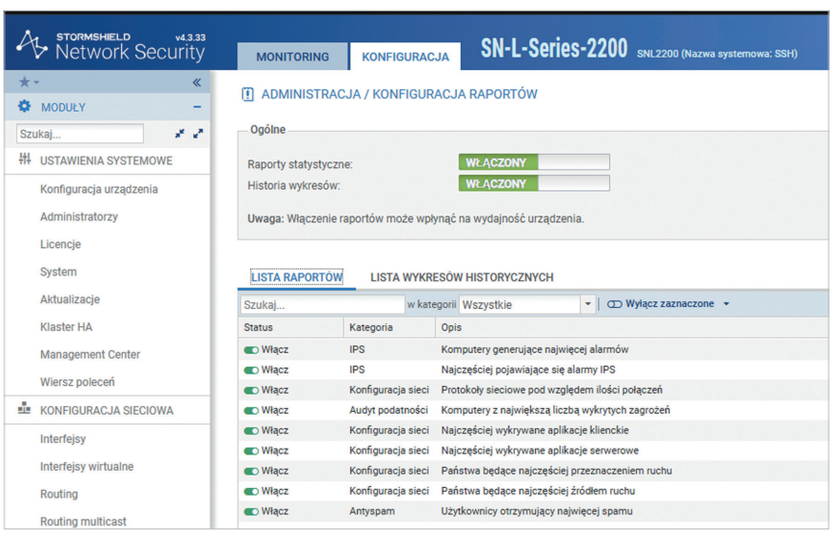
Osobnej licencji wymaga również ochrona ruchu dla protokołów działających w sieciach przemysłowych. Mowa tu o ponad 10 protokołach, jak chociażby Modbus, S7 czy PROFI-NET, dla których dostępne są mechanizmy głębokiej inspekcji pakietów w ramach IPS-a. Nasza testowa zapora pozbawiona była licencji tego typu, a więcej na temat ochrony sieci OT od Stormshielda można znaleźć w teście zapory SNi40 („IT Professional" 5/2018, s. 48). Innym mechanizmem kontroli dostępu spełniającym definicję ZTNA (Zero Trust Network Access) jest możliwość weryfikacji wybranych ustawień bezpieczeństwa dla hostów uzyskujących połączenie do zasobów firmowych za pośrednictwem SSL VPN. Dostępne jest także wieloskładnikowe uwierzytelnianie użytkowników.



Szczegółowe logowanie zdarzeń i prosty podgląd ułatwiają analizę ruchu.

NOWOŚCI

Wśród nowinek, które pojawiły się z najnowszą odsłoną platformy systemowej, znajdziemy również wsparcie dla kluczy współdzielonych spełniających wymagania post-quantum (PPK) dla protokołu IKEv2, dynamiczny routing multicast, a także wersję drugą BIRD-a – silnika realizującego funkcje routingu. Testowany model ma także wbudowany pasywny skaner podatności. Oznacza to, że dzięki analizie ruchu pochodzącego z urządzeń w sieci lokalnej możliwe jest wykrycie podatności konkretnych programów. Urządzenie potrafi zidentyfikować oprogramowanie źródłowe na podstawie ruchu generowanego przez aplikacje, a następnie wskazać ewentualne podatności z nim związane i zasugerować aktualizację oprogramowania zagrożonego atakami. Część producentów rozwiązań UTM oferuje podobną funkcjonalność, jednak realizuje to za pośrednictwem aplikacji agenta przeznaczonej dla konkretnej wersji systemu operacyjnego hosta.



Wbudowana lista raportów ułatwia analizę statystyk i alertów.

FILTROWANIE RUCHU

Samo filtrowanie ruchu, a co za tym idzie budowa zestawu reguł, opiera się na politykach. Producent standardowo dostarcza 10 profili, które mogą realizować różne scenariusze ochrony. W analogiczny sposób definiuje się choćby polityki filtrowania URL, SMTP oraz SSL. Sama reguła filtrowania ruchu poza podstawowymi informacjami, takimi jak adres źródłowy, docelowy czy akcja, zawiera również cały zestaw dodatkowych funkcji. Zdefiniować tu można chociażby parametry logowania zdarzeń, harmonogram obowiązywania reguły czy wybór bramy. Z tego samego poziomu zdefiniujemy także kolejki QoS. W kontekście źródła i miejsca docelowego ruchu możliwa jest również kategoryzacja ze względu na predefiniowaną usługę webową oraz reputację adresu IP, a także na podstawie położenia geograficznego. W ten sposób można chociażby zdefiniować regułę dla ruchu do/z chmury AWS-u, z uwzględnieniem regionu, względem którego można zablokować ruch. W prosty sposób odetniemy także połączenie z określonego kraju czy regionu geograficznego. Oczywiście reguły można tworzyć względem konkretnych użytkowników i sposobu ich uwierzytelnienia. Z poziomu wyboru mechanizmu inspekcji określimy, czy dane będą analizowane

tylko na poziomie firewalla, IDS-a oraz IPS-a, decydując się również na jedną spośród wcześniej zdefiniowanych polityk. Na tym etapie podejmujemy też decyzję w kwestii dodatkowych mechanizmów inspekcji, jak antywirus, sandboxing, funkcje antyspamowe, filtrowanie URL, SMTP, FTP i SSL. Oczywiście odpowiednia analiza ruchu szyfrowanego będzie wymagała uprzedniego stworzenia reguł deszyfrujących. Firewall nie omieszka nas o tym poinformować.

PODSUMOWANIE

Testowana zapora to wydajne rozwiązanie mogące chronić zarówno środowiska IT, jak i OT. Szeroki wachlarz dostępnych mechanizmów ochrony sieci pozycjonuje produkty Stormshielda jako ciekawą i konkurencyjną alternatywę dla największych graczy na rynku tego typu rozwiązań. Dla niektórych przedsiębiorstw z europejską metryką, podlegających lokalnym wymogom bezpieczeństwa, zaletą będzie fakt, iż rozwiązania firmy Stormshield tworzone są w Europie i z uwzględnieniem wymogów prawnych stawianych na gruncie lokalnym. Najnowsza wersja oprogramowania to kontynuacja dobrze znanej platformy. W stosunku do naszych testów sprzed niemal 10 lat również sposób zarządzania i obsługa interfejsu niewiele się zmieniły, a dzięki tej konsekwencji użytkownicy, którzy mieli już wcześniej do czynienia z produktami tego producenta, odnajdą się szybko w konfiguracji. Wydajność SN-L-Series-2200 powinna zaspokoić wymagania dużych środowisk, choć warto zaznaczyć, iż poziom ochrony jest niemal identyczny bez względu na model zapory, a także jej wersję w formie maszyny wirtualnej, przeznaczonej również na popularne platformy chmurowe. Przydałoby się nieco uprościć licencjonowanie – sekcja z dostępnymi funkcjami w panelu WebGUI zawiera mnóstwo pozycji, które trudno odpowiednio sklasyfikować względem wymaganej licencji.

> ZARZĄDZANIE I OPCJE DODATKOWE

Podstawowym interfejsem administratora jest WebGUI. Umożliwia on wybranie języka polskiego, a samo spolszczenie jest na wysokim poziomie, szczególnie jeśli porównać je z próbami innych producentów. Oczywiście w celu uniknięcia błędnej interpretacji niektórych opcji najbezpieczniej będzie korzystać z wersji angielskiej. Sposób zarządzania poszczególnymi funkcjami nie zmienił się zbytnio na przestrzeni lat. Sam UI nie wygląda może szczególnie atrakcyjnie, ale jest za to dość intuicyjny i bardzo responsywny. Niektóre opcje obsługi, jak chociażby przeciągnij i upuść oraz skróty klawiaturowe typu kopiuj/wklej, miło zaskakują, ułatwiając czynności administracyjne. Innym sposobem zarządzania jest interfejs linii komend. Opcja ta przeznaczona jest jednak przede wszystkim dla inżynierów wsparcia technicznego lub zaawansowanych użytkowników. Oczywiście możliwe jest również centralne zarządzanie wieloma zaporami za pośrednictwem Stormshield Management Center – serwera dostępnego w formie maszyny wirtualnej. W ten sposób z pojedynczej konsoli można ustanowić bezpieczne połączenie z wieloma rozproszonymi geograficznie zaporami chroniącymi wiele lokalizacji w celu zarządzania, monitorowania i zbierania logów.

Urządzenie oferuje również szereg funkcji dodatkowych, które rozszerzają możliwości standardowego firewalla. Na uwagę zasługują chociażby opcje konfiguracji routingu. Trasowanie można zrealizować na kilka sposobów: z routingiem statycznym na czele, jak również na podstawie zasad (adres źródłowy, docelowy, port, użytkownik) czy przy wykorzystaniu routingu dynamicznego (moduł Bird v2, RIP, BGP, OSPF). Od wersji 4.8 dostępny jest również routing multicast. Zapora z powodzeniem sprawdzi się także jako serwer DHCP oraz DNS cache proxy.

Stormshield pozwala również na kształtowanie pasma (QoS). Decyzje o zapewnieniu odpowiedniej przepustowości czy ograniczeniu zasobów mogą być podejmowane na poziomie pojedynczych reguł zapory sieciowej. Reglamentowanie dostępu do internetu można również definiować na podstawie ram czasowych. Odpowiednie profile filtrowania mogą obowiązywać w standardowych godzinach pracy, a inne w porze ograniczonej aktywności. Integracja z bazami LDAP pozwala na definiowanie polityk dla grup lub pojedynczych użytkowników.

Autor pracuje jako architekt IT w firmie Kyndryl. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

Werdykt

Stormshield SN-L-Series-2200

Zalety

- wydajność
- rozbudowane mechanizmy ochrony
- spolszczenie WebGUI na wysokim poziomie
- ZTNA dla SSL VPN
- QoS
- HA
- pasywny skaner podatności

Wady

- drobne błędy w oprogramowaniu
- złożone licencjonowanie

Ocena **9**/10