

# IT professional

Nr 8 (45) sierpień 2015      Cena 33,00 zł (w tym 5% VAT)

## OPTIMALIZACJA PAMIĘCI MASOWYCH s. 10

▶ Technologie EMC FastCache i FastVP, wykorzystujące dyski SSD do zwiększania wydajności macierzy dyskowych, oraz zastosowanie Oracle ZFS Appliance i protokołu direct NFS. Możliwości mechanizmów, architektura, wdrażanie

### s. 29 Systemd – więcej niż init

Nowa koncepcja, rozszerzony zakres zadań, bezpieczeństwo, zarządzanie usługami

### s. 34 Citrix Provisioning Services

Dostarczanie zwirtualizowanych aplikacji i desktopów. Wdrażanie, licencjonowanie

### s. 43 Automatyczne wykrywanie oszustw

Praktyczne aspekty uczenia maszynowego i algorytmów eksploracji danych



Unified Threat Management to określenie charakteryzujące zapory sieciowe integrujące w ramach pojedynczego „pudełka” wiele mechanizmów chroniących przed zagrożeniami sieciowymi, w tym IPS, antywirus, antyspam itp. Sprawdziliśmy, jakie funkcje oferuje mało znany na polskim rynku Stormshield SN900.



## BEZPIECZEŃSTWO SIECI

# Stormshield SN900 – skuteczny UTM

**Marcin Jurczyk**

**S**tormshield to stosunkowo nowa marka rozwiązań z segmentu security, która pojawiła się na rynku zabezpieczeń sieciowych w 2014 roku. O ile sama marka nie zdążyła jeszcze przebić się do świadomości wielu użytkowników, o tyle całe zaplecze stojące za rozwiązaniem jest już dobrze znane. Mamy bowiem do czynienia z kontynuacją doskonale znanych produktów, występujących dotychczas pod nazwą Netasq. Skąd więc zmiana nazwy i wprowadzenie na rynek nowej marki? Historia francuskiej firmy Netasq sięga 1998 roku, a profil działalności od samego początku dotyczył zabezpieczeń sieciowych w postaci zintegrowanych zapór sieciowych. W 2012 roku firma stała się częścią grupy EADS (European Aeronautic Defence and Space Company), znanej obecnie jako grupa Airbus (powszechnie rozpoznawalny koncern lotniczo-zbrojeniowy).

W 2014 roku Airbus połączył się z firmą Arkoon Network Security, w efekcie czego powstała właśnie marka Stormshield Network Security. Co ważne, klienci mający już doświadczenie z produktami Netasq nie mają się czego obawiać – nowa seria urządzeń Stormshield to naturalna kontynuacja dobrze znanych rozwiązań Netasq, a każda kolejna wersja oprogramowania systemowego to ewolucja przetestowanych przez tysiące użytkowników wydań.

### > SPRZĘT I WYDAJNOŚĆ

Produkty Stormshield to rozwiązania klasy UTM zaprojektowane z myślą o zróżnicowanej grupie odbiorców. Dostępne modele zostały sklasyfikowane ze względu na wielkość biznesu i liczbę komputerów działających w chronionej sieci. Najmniejsze rozwiązania dedykowane są dla sieci obsługujących od 10 do maksymalnie 70 komputerów (modele: SN150/200/300). Kolejny

przedział to rozwiązania dla sieci średnich i dużych organizacji – mogą zabezpieczać od 71 do 500 stacji roboczych (modele: SN500/700/900/910). W portfolio znajdują się również UTM-y dla klientów korporacyjnych i data center, mogące obsłużyć do 15 tys. komputerów (SN2000/3000/6000). Ponadto Stormshield występuje również w formie maszyny wirtualnej.

Dużą zaletą Stormshield SN900 jest dostosowanie rozwiązania do polskich realiów, zarówno pod względem polonizacji interfejsu i dokumentacji, jak też stworzenia dedykowanego zestawu kategorii filtra URL.



## Stormshield SN900

## Specyfikacja

Maksymalna liczba chronionych stacji roboczych: 500

Przepustowość firewalla: 4 Gbps

Przepustowość firewalla + IPS

(ramka 1518-bajtów): 3 Gbps

Przepustowość firewalla + IPS

(pliki HTTP 1MB): 1,4 Gps

Przepustowość firewalla + IPS + AV: 300 Mbps

Przepustowość IPSec VPN: 800 Mbps

Liczba tuneli IPSec VPN: 1000

Liczba tuneli SSL VPN: 100

Maksymalna liczba sesji: 1 200 000

Liczba nowych sesji/sekundę: 25 000

Liczba VLAN-ów: 512

Liczba interfejsów: 12 100/1000 Mbps  
(+2 opcjonalne 1 Gbps fiber)

## Ceny netto

Urządzenie z najtańszą roczną opcją serwisową: 6340 euro

Urządzenie z roczną opcją serwisową Premium: 7400 euro

Audyty podatności: 770 euro

Silnik Kaspersky Antivirus: 770 euro

Obsługa kart SD: 150 euro

Rozszerzony filtr URL: 820 euro

Data źródła	Akcja	Użytkownik	Nazwa obiektu źródłowego	Nazwa obiektu docelowego	Nazwa portu doc.	Reguła	Profil konfig.	Powinno reg.	Operacja	Szczegóły
24.06.2015 0:21:51	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	POST	
24.06.2015 0:20:08	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:20:08	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:20:07	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:20:03	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:20:02	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:58	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:58	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:57	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:52	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:47	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:39	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:38	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	
24.06.2015 0:19:37	Zaczł		TPLink	54.195.242.199	http	2	01	Lokality	GET	

Podgląd zdarzeń to jeden z najważniejszych elementów każdego firewalla.

maksymalny poziom wydajnego filtrowania na poziomie 500 urządzeń w chronionej sieci. Przepustowość samego firewalla to 4 Gbps określone dla ruchu UDP 1518 bajtów. Dołączenie IPS-a wiąże się ze zmniejszeniem wydajności do 3 Gbps dla takiej samej charakterystyki sieciowej. Dla plików HTTP o rozmiarze 1 MB przepustowość spada do 1,4 Gbps. Największy wpływ na spadek wydajności filtrowania ma skaner antywirusowy – całkowita wydajność po dołączeniu modułu AV to 300 Mbps. UTM jest w stanie obsłużyć do 1,2 mln równoległych połączeń oraz do 25 tys. nowych połączeń na sekundę. Z kolei wydajność dla ruchu szyfrowanego IPSec VPN (AES128/SHA1) kształtuje się na poziomie 800 Mbps (przepustowość

oraz 1000 równoległych tuneli VPN (100 tuneli dla SSL VPN). Rozwiązanie pozwala również na konfigurację w trybie klastra wysokiej dostępności active-passive.

Za komunikację ze światem zewnętrznym odpowiada 12 interfejsów miedzianych 1 Gbps oraz opcjonalne dwa porty światłowodowe SFP o tej samej przepustowości. Producent nie zdecydował się na wydzielenie dedykowanego portu do zarządzania out-of-band. Urządzenie zamknięto w obudowę o wysokości 1U. Dokumentacja techniczna nie określa specyfikacji CPU czy ilości pamięci operacyjnej. Producent wspomina jedynie o pełnej obsłudze wielordzeniowego przetwarzania danych. Pamięć wewnętrzna SN900 to dysk twardy o pojemności 120 GB oraz opcjonalnie – karta pamięci SD (wymaga dodatkowej licencji). Na przedniej ścianie urządzenia, poza portami sieciowymi, znajdują się: przycisk włącznika, diody informujące o statusie zasilania i pracy urządzenia, slot na karty SD, a także porty umożliwiające podpięcie klawiatury i monitora (PS2, USB i VGA) oraz port szeregowy. Za pośrednictwem złącza USB można również zaktualizować urządzenie, zapisać plik konfiguracyjny i podłączyć modem. Na przednim panelu znajduje się również przycisk przywracania konfiguracji do ustawień fabrycznych.

Nazwa	Typ	Adresy IPv4	Adres IPv6	Pobieranie	Wysyłanie
VLAN Port (Ethernet)	Ethernet	192.168.200.254/255.255.255.224		0.07 KioB/s	1.01 KioB/s
LAN1 (Ethernet)	Ethernet	192.168.200.254/255.255.255.0		1.48 KioB/s	1.79 KioB/s
dmz1 (Ethernet)	Ethernet	192.168.200.254/255.255.255.0		---	---
dmz2 (Ethernet)	Ethernet	192.168.200.254/255.255.255.0		---	---
dmz3 (Ethernet)	Ethernet	192.168.200.254/255.255.255.0		---	---

Panel kontrolny umożliwia podgląd najważniejszych zdarzeń oraz ustawień konfiguracyjnych UTM-a. Jego wygląd można zmieniać i personalizować.

W SN900 zamontowano wbudowany zasilacz, którego gniazdo znajduje się z tyłu obudowy. Znaleźć tam można również dwa dodatkowe porty USB (funkcjonalność analogiczna do portu na przednim panelu) oraz wyloty dwóch wentylatorów. W zestawie znajdziemy też uchwyty ułatwiające montaż w szafie oraz zestaw kabli.

## > FUNKCJE BEZPIECZEŃSTWA

Silą rozwiązań Netasq, a teraz również Stormshield, jest integracja funkcjonalności tradycyjnej zapory ogniowej z systemem IPS na poziomie jądra systemu operacyjnego. Technologia ta nosi nazwę ASQ – Active Security Qualification, a system operacyjny – Netasq Secured BSD (NS-BSD). Dzięki takiemu podejściu wyeliminowano potrzebę wielokrotnego przetwarzania tego samego ruchu sieciowego przez wiele modułów, przez co skrócono czas filtrowania ruchu i poprawiono ogólną wydajność systemu. Ruch sieciowy można filtrować, wykorzystując trzy polityki: klasyczny firewall, moduł IPS lub moduł IDS. Ostatnia opcja jest szczególnie przydatna na etapie wdrażania rozwiązania Stormshield w działającej sieci. Automatyczna detekcja pozwala scharakteryzować profil sieciowy, a następnie zdefiniować politykę filtrowania odpowiadającą specyfice konkretnego środowiska sieciowego.

Naturalnym rozszerzeniem IPS jest mechanizm głębszej inspekcji pakietów, pozwalający rozpoznać rodzaj aplikacji sieciowej przechodzącej przez UTM. Dzięki temu administrator ma możliwość filtrowania ruchu na podstawie ustawień dla konkretnych aplikacji, co pozwala w precyzyjny sposób kontrolować dostęp do internetu. Testowane urządzenie jest w stanie zidentyfikować prawie 400 różnego rodzaju aplikacji sieciowych z ponad 1400 predefiniowanych schematów (wzorców alertów) dostępnych w formie sygnatur kontekstowych. Filtrowanie poszczególnych elementów Facebooka czy aplikacji P2P do wymiany danych to najpopularniejsze scenariusze dostępne dzięki

rozpoznawaniu aplikacji na podstawie głębokiej inspekcji pakietów. Inną cechą systemu IPS działającego na urządzeniach Stormshield jest selektywne blokowanie złośliwego kodu wywołanej strony WWW – w odróżnieniu od standardowej akcji blokowania takiej witryny UTM jest w stanie wyizolować szkodliwą część kodu, przepuszczając jedynie niegroźną część żądania do przeglądarki użytkownika.

Stormshield, poza klasyczną zaporą ogniową oraz IPS-em oferuje również cały zestaw funkcji zwiększających poziom bezpieczeństwa sieci. Na uwagę zasługuje pasywny skaner wnętrza sieci, umożliwiający zidentyfikowanie luk i podatności oprogramowania zainstalowanego na komputerach w chronionej sieci. Urządzenie potrafi zidentyfikować oprogramowanie źródłowe na podstawie ruchu generowanego

[illegible]

Real-time Monitor to dodatkowa konsola umożliwiająca szybki podgląd działania UTM-a.

przez aplikacje, a następnie wskazać ewentualne podatności z nim związane i zasugerować aktualizację oprogramowania podatnego na ataki. Część producentów rozwiązań UTM oferuje podobną funkcjonalność, jednak realizuje to za pośrednictwem aplikacji agenta, dedykowanej dla konkretnej wersji systemu operacyjnego hosta.

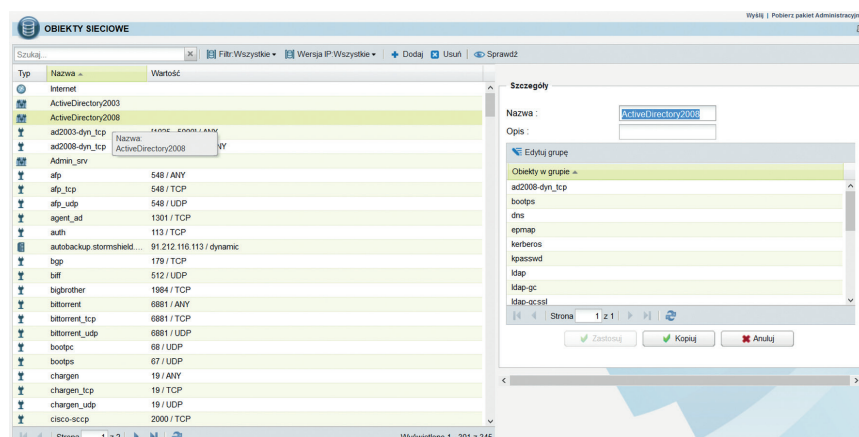
Możliwości filtrowania dostępu do potencjalnie niepożądanych zasobów internetu rozszerza funkcja filtra URL. Domyślnie producent udostępnia

podzieloną na kategorie bazę adresów URL. Na uwagę zasługuje jednak zestaw filtrów specyficznych dla profilu polskiego użytkownika, przygotowany przez polskiego dystrybutora – 53 kategorie adresów HTTP oraz HTTPS, a także możliwość zgłaszania nowych adresów z gwarantowanym czasem dodania wpisu do bazy w ciągu jednego dnia roboczego. Opcjonalnie dostępny jest również bardziej rozbudowany URL filtering wykorzystujący technologie chmurowe (przeszukiwanie bazy URL poza urządzeniem). Płatna opcja dotyczy ponad 100 mln adresów URL podzielonych na 65 kategorii tematycznych. To dużo.

Wśród mechanizmów bezpieczeństwa nie mogło również zabraknąć funkcji skanera antywirusowego oraz antyspamowego. Ochrona przeciwwirusowa realizowana jest z użyciem jed-







Obiekt to podstawowy element ułatwiający konfigurację UTM-ów Stormshield.

W obszarze zabezpieczenia przeciwko niechcianym wiadomościom e-mail Stormshield oferuje kilka mechanizmów obronnych, w tym powszechne czarne i białe listy oraz synchronizację z najpopularniejszymi serwerami reputacyjnymi RBL (Realtime Blackhole List). Ponadto dostępny jest mechanizm analizy heurystycznej, potrafiący rozpoznawać niechcianą korespondencję między innymi na podstawie analizy semantycznej, analizy kodu HTML i typu wiadomości delivery failure notification.

SN900 jako typowy UTM pozwala również na terminowanie połączeń VPN. Do wyboru mamy trzy protokoły: IPSec, SSL lub PPTP. Szyfrowanie IPSec wspierane jest sprzętowo za

pomocą dedykowanego układu ASIC. W zależności od potrzeb możliwe jest też zestawienie tuneli site-to-site lub client-to-site, za pośrednictwem dedykowanej aplikacji klienta VPN.

### > USŁUGI DODATKOWE

SN900 to nie tylko zintegrowana zapora sieciowa. Urządzenie oferuje również szereg funkcji dodatkowych, rozszerzających możliwości standardowego firewalla. Na uwagę zasługują chociażby opcje konfiguracji routingu. Trasowanie można zrealizować na kilka sposobów, z routingiem statycznym na czele, poprzez trasowanie na podstawie zasad (adres źródłowy, docelowy, port, użytkownik), a na routingu dynamicznym (moduł

Bird) kończąc (RIP, BGP, OSPF). W najnowszej wersji oprogramowania systemowej konfiguracja routingu dynamicznego została również udostępniona w konsoli webGUI (dotychczas konfiguracja zaawansowanego routingu wymagała zalogowania do CLI). Możliwe jest również skonfigurowanie load balancingu dla wielu dostawców ISP według adresów źródłowych lub połączenia.

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 umożliwia definiowanie polityk dla grup lub pojedynczych użytkowników.

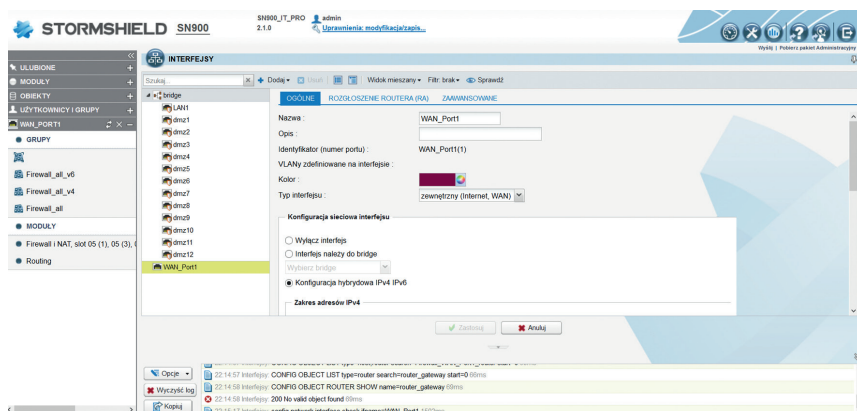
### > ZARZĄDZANIE I MONITORING

Uruchomienie i konfiguracja SN900 podobnie jak pozostałych UTM-ów Stormshield może odbywać się na dwa sposoby – z wykorzystaniem interfejsu WebGUI lub za pośrednictwem CLI. Dodatkowo na płycie DVD dostarczonej wraz z urządzeniem znajduje się pakiet Administration Suite, zawierający aplikacje do konfiguracji urządzenia, monitoringu w czasie rzeczywistym oraz przeglądania logów UTM-a (są to odpowiednio pakiety: Global Administration, Realtime Monitor oraz Event Reporter, którego pełna wersja wymaga zakupu dodatkowej licencji). Podstawowym interfejsem konfiguracyjnym jest jednak GUI dostępne z poziomu przeglądarki internetowej (oficjalnie wspierane są Internet Explorer 7 i nowsze oraz Firefox od wersji 3.6). Podczas pierwszego podłączenia do UTM-a należy pamiętać o wyborze odpowiedniego portu.

Domyślnie pierwszy port skonfigurowany jest jako interfejs typu OUT

## PODSUMOWANIE

SN900 to przedstawiciel nowej linii produktów Stormshield, będącej następcą znanej serii urządzeń Netasq. Zgodnie z oczekiwaniami nowe urządzenia oferują większe możliwości w porównaniu z dobrze znanymi na rynku rozwiązaniami klasy UTM francuskiego producenta. Testowany model SN900 jest urządzeniem o wydajności wystarczającej do zabezpieczenia całkiem sporej sieci. Oferowane mechanizmy bezpieczeństwa, wraz ze wsparciem technicznym oferowanym przez polskiego dystrybutora, powinny zaspokoić nawet najbardziej wymagających klientów. Dużą zaletą jest dostosowanie rozwiązania do polskich realiów, zarówno pod względem polonizacji interfejsu i dokumentacji, jak też stworzenia dedykowanego zestawu kategorii filtra URL. Cena urządzenia nie należy do najniższych, jednak biorąc pod uwagę możliwości zabezpieczenia styku sieci oraz szereg oferowanych funkcji dodatkowych, warto poważnie rozważyć zakup produktów marki Stormshield.



12 portów miedzianych i 2 światłowodowe – wszystkie w pełni konfigurowalne.

należący do strefy niezaufanej, przez co nie jest możliwe uzyskanie dostępu do urządzenia. Po pierwszym zalogowaniu do urządzenia (standardowo <https://10.0.0.254>) należy przeprowadzić wstępną konfigurację urządzenia wraz z aktywacją pakietu serwisowego. W przeglądarce wyświetlony zostanie Panel kontrolny, będący zbiorem widżetów wyświetlających informacje na temat pracy głównych modułów firewalla. Z lewej strony okna znajdziemy menu funkcjonalne UTM-a, zawierające wszystkie opcje konfiguracyjne z podziałem na bloki funkcyjne, takie jak: Ustawienia systemowe, Konfiguracja sieci, Polityki ochrony i Kontrola aplikacji. W zależności od wybranej sekcji wyświetlone zostaje rozwijane podmenu, zawierające wszystkie dostępne moduły konfiguracyjne. Wybór interesującej nas opcji skutkuje wyświetleniem widoku konfiguracji w centralnej części przeglądarki. Na górnej belce znajdują się ikony menu odpowiadającego za konfigurację samego środowiska WebGUI, odwołanie do pomocy kontekstowej i link pozwalający na wywołanie raportów aktywności (Activity Reports to wbudowana przeglądarka zdarzeń logowanych przez UTM-a, dostępna w formie dodatkowej zakładki w IE lub Firefoksie). Generalnie środowisko graficzne dostępne z poziomu WWW jest przejrzyste i intuicyjne. Na szczególną

uwagę zasługuje świetna polonizacja – w odróżnieniu od większości tego typu produktów dostępnych na rynku w przypadku Stormshielda bez obaw można korzystać z polskiego tłumaczenia. Nazwy wszystkich opcji zostały przetłumaczone w przemyślany sposób, dzięki czemu nie trzeba się zastanawiać, co autor tłumaczenia miał na myśli. Polski dystrybutor udostępnia również własną wersję podręcznika użytkownika, w której w przystępny sposób opisano poszczególne kroki konfiguracyjne (w odróżnieniu od oryginalnego manuala, w którym omawiane są poszczególne funkcjonalności UTM-a).

Sama konfiguracja poszczególnych modułów to proces, który nie powinien przysporzyć trudności nawet początkującym użytkownikom. Większość elementów można zdefiniować intuicyjnie bez zaglądania do jakiegokolwiek dokumentacji. Wspomniane wcześniej darmowe oprogramowanie uzupełnia podstawową funkcjonalność UTM-a. Realtime Monitor to typowe narzędzie do monitorowania szczegółów pracy urządzenia i stanu zabezpieczenia sieci w czasie rzeczywistym. Możliwy jest tu podgląd praktycznie wszystkich elementów, a szczególny nacisk położono na alarmy sieciowe. Event Reporter umożliwia przegląd historycznych danych zapisywanych w formie logów na lokalnym dysku urządzenia.

Zebrane informacje kategoryzowane są w formie raportów aktywności dla poszczególnych bloków funkcjonalnych UTM-a.

Bardziej wymagający użytkownicy mogą sięgnąć po oprogramowanie Virtual Log Appliance, dostarczane przez producenta w formie maszyny wirtualnej w formacie ova. Poza standardową funkcją kolektora zdarzeń (wykorzystuje syslog) NGVirtual Log Appliance oferuje rozbudowane widoki (podzielone na kategorie) oraz możliwość śledzenia wskaźników bezpieczeństwa sieci. Wirtualna maszyna bazuje na systemie Ubuntu. Za graficzno-analityczną część odpowiada pakiet elasticsearch + kibana.

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

## Werdykt

### Stormshield SN900

#### Zalety

- + świetnie spolszczony, intuicyjny interfejs WebGUI
- + wysoka wydajność
- + obsługa BGP i OSPF
- + rozbudowane narzędzia do monitoringu
- + pasywny skaner zagrożeń
- + stosunek cena/jakość

#### Wady

- brak portu zarządzania out-of-band

Ocena

9/10