

# Networld

PRZEDRUK

GRUDZIEŃ 2014 (12/219) INDEKS 328820

CENA 26,90 ZŁ (W TYM 5% VAT)

[www.networld.pl](http://www.networld.pl)

MNA : tel. # 4838

BBID : qrup # 4949

BYE : vip # 9598

## NAJLEPSZĄ OBRONĄ JEST ATAK

### NARZĘDZIA DO TESTÓW PENETRACYJNYCH



**TEST**  
Netsq  
Stormshield SN500



**SIEĆ ZWIRTUALIZOWANA**

Prędzej czy później sieć podzieli los serwerów.  
Czas się przygotować

**ZABAWA W PROJEKTANTA**

Planowanie i projektowanie centrum danych  
rządzi się swoimi prawami



ISSN 1232-8723

12





# Stormshield SN500

## – kompleksowa ochrona sieci

Na rynku dostępnych jest wiele rozwiązań Unified Thread Management różnych producentów – nowością jest m.in. seria urządzeń Netasq Stormshield. Sprawdziliśmy, jak wygląda kwestia zintegrowanej ochrony infrastruktury przedsiębiorstwa, testując należący do tej serii model SN500.

Jarosław Kowalski

Seria Netasq Stormshield to 9 urządzeń przeznaczonych zarówno dla małych, jak i dużych przedsiębiorstw. Oprócz rozwiązań sprzętowych klienci mogą również wdrożyć we własnej chmurze wersje wirtualne, które funkcjonalnie nie ustępują urządzeniom fizycznym. Nowa seria oferuje między innymi pełne wsparcie protokołu IPv6, a także bezpieczny dostęp do sieci przy wykorzystaniu protokołów VPN, w tym Full SSL VPN. Rozbudowane zostały również możliwości w zakresie zarządzania

oraz raportowania. Na uwagę zasługuje wprowadzenie Microsoft Service Firewall, który na zaawansowanym poziomie pozwala filtrować ponad 50

zostały również wyposażone w możliwość agregacji interfejsów, w celu uzyskania większej niezawodności oraz przepustowości.

zamknięte w standardowej obudowie 1U do montażu w szafie 19-calowej od frontu wyposażone jest w 8 portów GbE, które tak jak we wcze-



### ► Stormshield SN500

usług Microsoft RPC. Urządzenia z najwyższej półki (SN2000, SN3000 i SN 6000)

Do naszych testów trafił model ze średniej półki oznaczony symbolem SN500. Urządzenie

śniejserii urządzeń były oznaczone jedynie kolejnymi cyframi, aby można było je

przypisać dowolnie do różnych segmentów sieci (LAN, WAN, DMZ). Urządzenie SN500 może przy tym obsłużyć do 8 łączy WAN. Obok portów sieciowych znajdują się tam również gniazda obsługujące monitor i klawiaturę do konfiguracji i instalacji w trybie tekstowym oraz port USB do wykorzystania ze specjalnym modemem GSM.

## URUCHOMIENIE URZĄDZENIA

Chcąc dowiedzieć się nieco więcej o podstawowej instalacji i konfiguracji urządzenia, sprawdziliśmy dostępność dokumentacji technicznej na stronach producenta. Bez problemu można znaleźć nie tylko niezbędne materiały do rozpoczęcia pracy z urządzeniem, ale również opisy bardziej zaawansowanych konfiguracji. Pomocą służy płyta z instrukcją użytkownika i niezbędnym oprogramowaniem dla administratorów oraz użytkowników łączących się poprzez VPN.

Pierwsze uruchomienie urządzenia nie jest zbyt skomplikowane. Korzystając z dołączonej krótkiej instrukcji bez problemu udało się połączyć z panelem webowym, który dla urządzeń Stormshield jest podstawowym narzędziem do zarządzania. Dodatkowo można wykorzystać również Stormshield Administration Suit, który stanowi pakiet programów służących do kontroli i zarządzania rozwiązaniami firmy Netasq. W jego skład wchodzi trzy podstawowe elementy. Stormshield Unified Manager służący do centralnego zarządzania większą liczbą rozwiązań Stormshield oraz Stormshield Event Reporter i Stormshield Real-Time

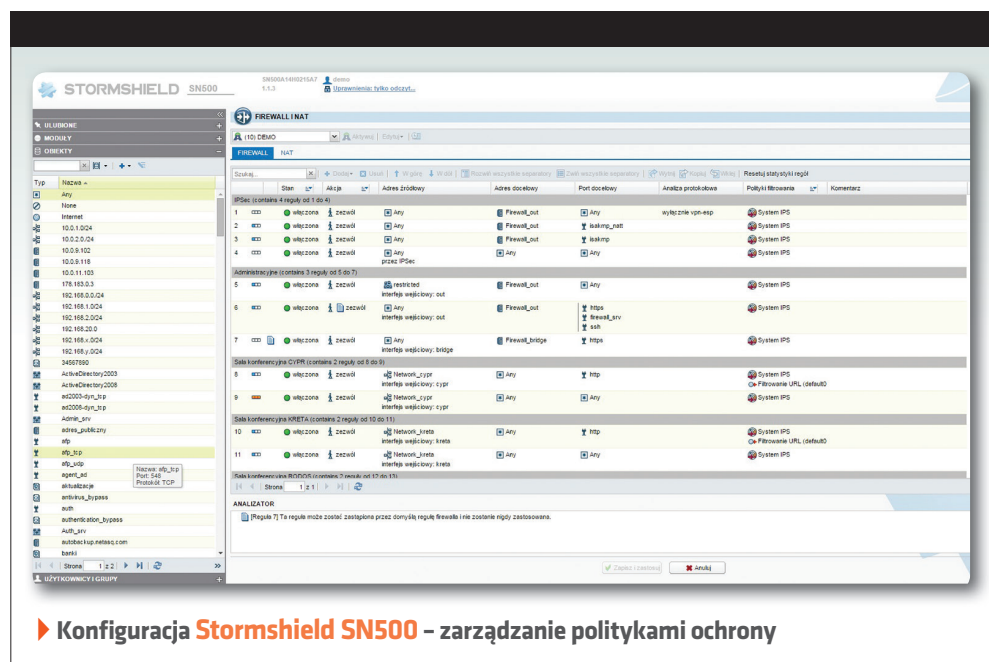
Monitor, o których wspomnieliśmy przy okazji raportowania i monitorowania.

Najważniejszą konfigurację urządzenia można wykonać dość szybko w kilku krokach. Rozpocząć należy od poprawnej konfiguracji interfejsów sieciowych. Trzeba zaznaczyć, że urządzenie firmy Netasq może pracować

z odpowiedniego ruchu, aby umożliwić dostęp do internetu z wewnątrz sieci.

Interfejs webowy, którym się posłużyliśmy jest skonstruowany przejrzysto, więc odnalezienie interesujących opcji konfiguracyjnych nie sprawiało żadnego problemu. Jest on podzielony w standardowy dla tych urządzeń spo-

moduły funkcjonalne. Ich nazwy są czytelne dla użytkownika, a kliknięcie w wybrany element pokazuje zaawansowane opcje, jakie można skonfigurować w ramach danego obszaru. Pośrodku znajduje się największe okno, gdzie domyślnie po zalogowaniu pojawiają się informacje panelu głównego,



► Konfiguracja Stormshield SN500 – zarządzanie politykami ochrony

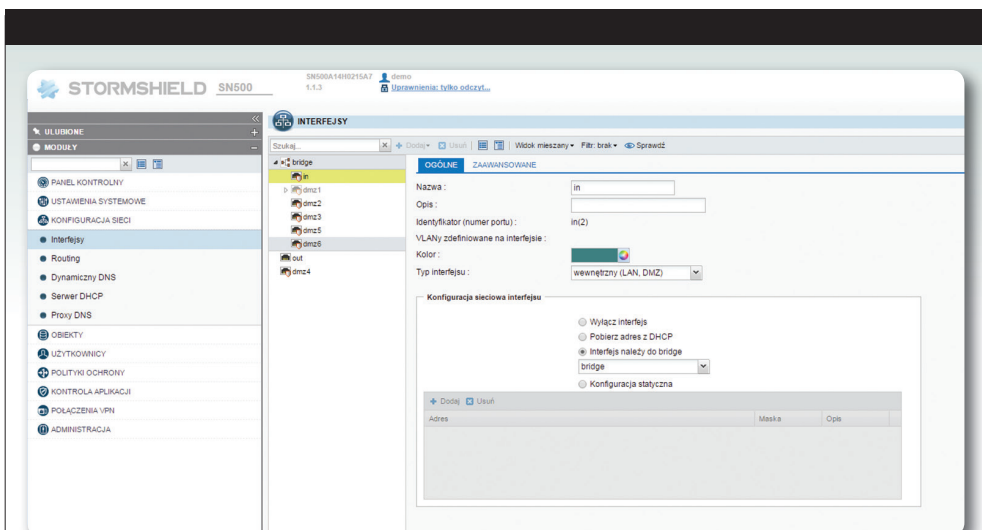
zarówno w trybie transparentnym, jak i jako router umożliwiający dostęp do internetu. W pierwszym przypadku konfiguracja nie wymaga żadnych modyfikacji w sieci firmowej. Urządzenie po prostu wpina się między aktualny router a sieć wewnętrzną, po czy należy skonfigurować niezbędne funkcje bezpieczeństwa. W drugim przypadku trzeba poprawnie skonfigurować interfejsy sieciowe w zakresie adresacji IP, określić podstawową bramę dostępu do internetu oraz zdefiniować polityki routing i dopusz-

sób, na trzy części. Na górze zlokalizowany jest banner, na którym znajdują się odnośniki do panelu głównego, konfiguracji pomocy technicznej oraz panelu monitora aktywności. Tutaj także pokazana jest nazwa obecnie zalogowanego użytkownika wraz z możliwością obniżenia lub podniesienia uprawnień podczas korzystania z panelu. Jest to przydatna opcja, która może uchronić użytkownika z uprawnieniami administracyjnymi przed przypadkową zmianą ustawień.

Po lewej znajduje się menu rozwijalne podzielone na

a po kliknięciu odnośnika z menu pokazuje się zaawansowana konfiguracja wybranych opcji. Dodatkowo jest możliwość ustawienia najczęściej używanych elementów menu, do których będzie natychmiastowy dostęp przez kliknięcie odnośnika *Ulubione*.

Panel Kontrolny, który dostępny jest zaraz po zalogowaniu, dostarcza podstawowych informacji o pracy urządzenia wliczając w to bieżące obciążenie, alarmy, uruchomione usługi i stan interfejsów. Wybór konkretnych okien informacyjnych oraz



► Konfiguracja Stormshield SN500 – interfejsy sieciowe

ich ułożenie można bez problemu dostosować przez dodawanie i zmianę kolejności.

Konfigurując urządzenie jako router mieliśmy możliwość ustawienia trasowania na kilka sposobów. Oprócz routingu statycznego dokładnie określającego ruch pomiędzy sieciami istnieje opcja ustawień Policy Routing, gdzie w zależności od źródła lub celu ruchu sieciowego bądź jego rodzaju można wymusić korzystanie z wybranej bramy internetowej. Da się to wykorzystać do rozdzielania różnych usług między dostępne łącza, tak aby nie obciążać jednego z nich całym ruchem sieciowym.

Konfiguracja Netasq Stormshield z użyciem wielu dostawców internetu pozwala również na konfigurację równoważenia obciążenia sieciowego oraz na zapewnienie niezawodności w dostępie do internetu. Wystarczy poprawnie skonfigurować interfejsy WAN i wskazać odpowiednie bramy biorące udział w równoważeniu obciążenia lub za-

pewieniu niezawodności. Badanie dostępności bramy odbywa się przez ustawienie polecenia ping na wskazany adres zewnętrzny.

## FUNKCJE BEZPIECZEŃSTWA

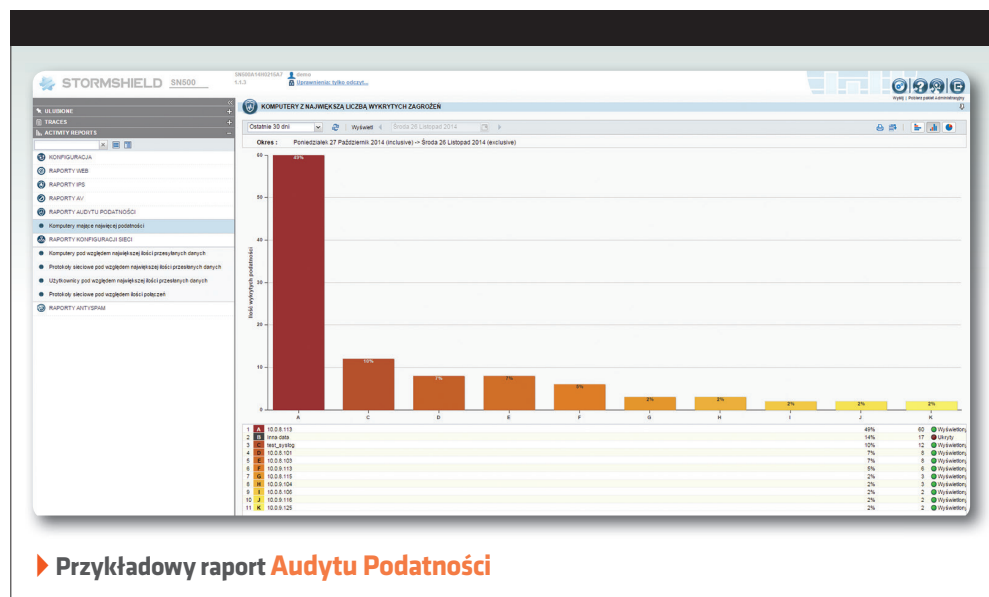
Cała konfiguracja urządzenia Stormshield SN500 opiera się na obiektach. Definiując całe

sieci, adresy IP, interfejsy, protokoły, porty czy użytkowników i ich grupy jako obiekty, o wiele łatwiej tworzyć reguły bezpieczeństwa wskazując wcześniej utworzony element. Urządzenia firmy Netasq domyślnie zawierają już obiekty najbardziej znanych elementów sieci, jakimi są protokoły, porty

czy aplikacje, jednak każdy użytkownik może zdefiniować własne, dostosowując konfigurację do wymogów bezpieczeństwa firmowej infrastruktury.

Podstawowymi funkcjami odpowiedzialnymi za realizację polityki bezpieczeństwa w przedsiębiorstwie jest zapora sieciowa oraz system zapobiegający włamaniom (IPS). W urządzeniach Stormshield elementy te działają już na poziomie jądra systemu przez wykorzystanie opatentowanej technologii ASQ (Active Security Qualification), która odpowiada za wykrywanie i blokowanie ataków. Rozwiązanie to pozwala chronić sieci nie tylko przed znanymi atakami, ale również dbać o bezpieczeństwo związane z pojawianiem się nowych zagrożeń.

Konfiguracja firewalla jest dość prosta. W module Polityki Ochrony zdefiniowane są podstawowe obszary konfiguracyjne odpowiedzialne za realizację funkcji zabezpieczających. Użytkownik ma do wyboru 10 zdefiniowanych



► Przykładowy raport Audytu Podatności



zestawów reguł zwanych słotami, które można konfigurować zgodnie z firmowymi politykami bezpieczeństwa. W ramach konfiguracji slotu określa się sposób filtrowania ruchu na poziomie zapory sieciowej, sposób filtrowania przez system IPS oraz dodatkowe moduły bezpieczeństwa sieciowego.

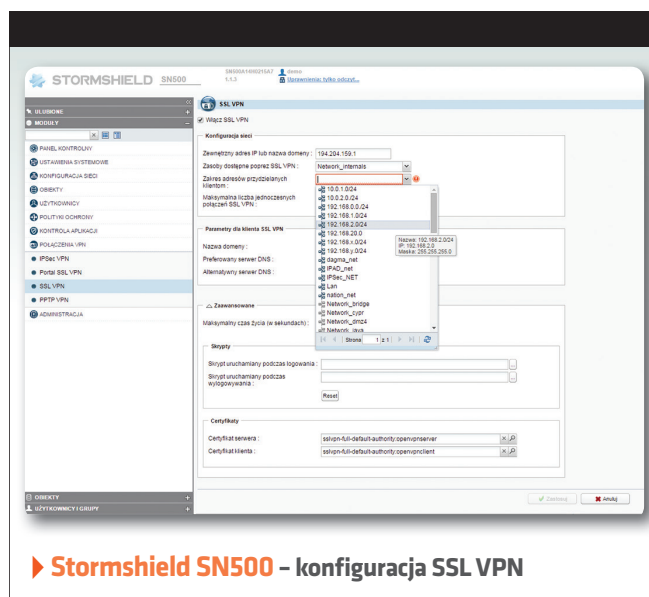
Producent wyposażył funkcje firewalla w zestaw własnych reguł, które nie mogą zostać zmodyfikowane przez użytkownika. Ma to na celu między innymi zabezpieczenie przed przypadkowym odcięciem dostępu do konfiguracji urządzenia przez niewłaściwie zdefiniowaną regułę.

To, na co warto zwrócić uwagę w rozwiązaniach Stormshield to sposób działania modułu IPS, który w odróżnieniu od innych systemów tego typu w momencie wykrycia podejrzanego kodu HTML, wycina go, a oczyszczona wersja strony zostaje przepuszczona do użytkownika.

Zapora w urządzeniu Netas jest elementem integrującym wszystkie moduły bezpieczeństwa. Definiując regułę filtrowania, administrator może włączyć lub wyłączyć poszczególne elementy ochrony, w tym system zapobiegania atakom IPS lub jedynie ich wykrywania IDS. Poprawność definiowanych reguł bezpieczeństwa zapewniona jest przez wykorzystany w urządzeniach Stormshield Analizator Reguł, który na bieżąco sprawdza użyte obiekty oraz metody skanowania ruchu i w przypadku nieprawidłowości użytkownik zostanie powiadomiony wraz ze wskazaniem błędnego wpisu.

Z poziomu obszaru Polityki Ochrony dostępny jest także moduł filtrowania adresów URL, gdzie administrator może łatwo określić polityki filtrowania w postaci zestawów adresów URL, do których dostęp jest dozwolony lub zabroniony z uwagi na określone grupy tematyczne. Oczywiście blokowaniu mogą podlegać również pojedyncze adresy bezpośrednio wskazane w polityce przez administratora.

Określając polityki filtrowania URL administrator korzysta z klasyfikacji tematycznej dostarczonej przez producenta. Należy zaznaczyć, że oprócz globalnej bazy dostępna jest również baza polskich stron, które zostały sklasyfikowane na potrzeby krajowych firm. Prócz obsługi zwykłego protokołu HTTP urządzenie jest w stanie filtrować ruch szyfrowany HTTPS. Ruch rozszyfrowywany jest na poziomie jądra systemowego, zatem sam proces dekodowania jest w pełni bezpieczny, gdyż nie można go podejrzyc z zewnątrz. Jeśli



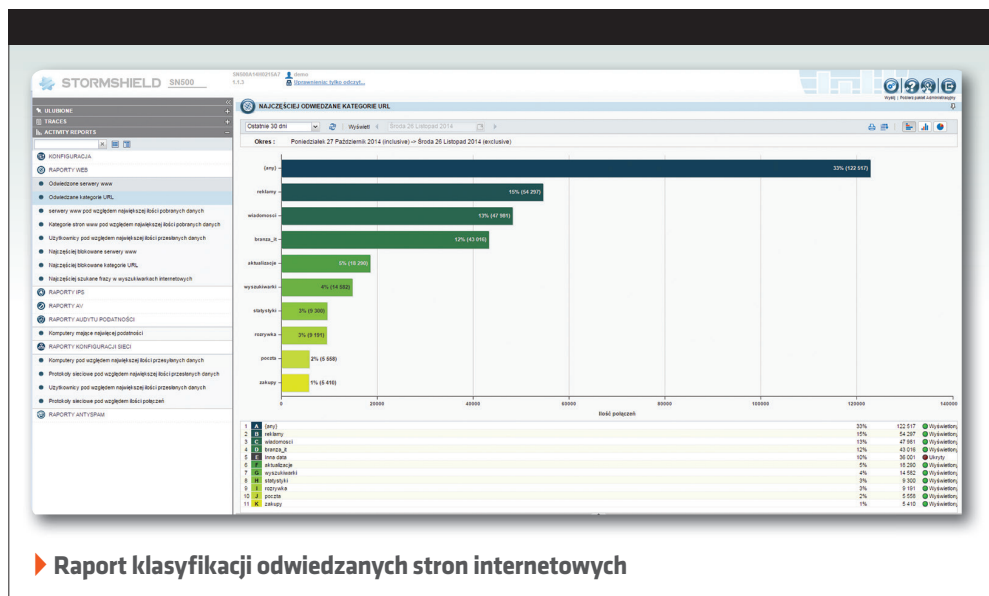
## ► Stormshield SN500 – konfiguracja SSL VPN

jest to ruch poprawny, urządzenie Stormshield szyfruje go ponownie i przesyła dalej do odbiorcy.

Bardziej wymagającym klientom oferowany jest dostęp do bazy sklasyfikowanych adresów URL w chmurze producenta, co odciąża urządzenie od przetrzymywania bazy w pamięci podręcznej. W przypadku spraw-

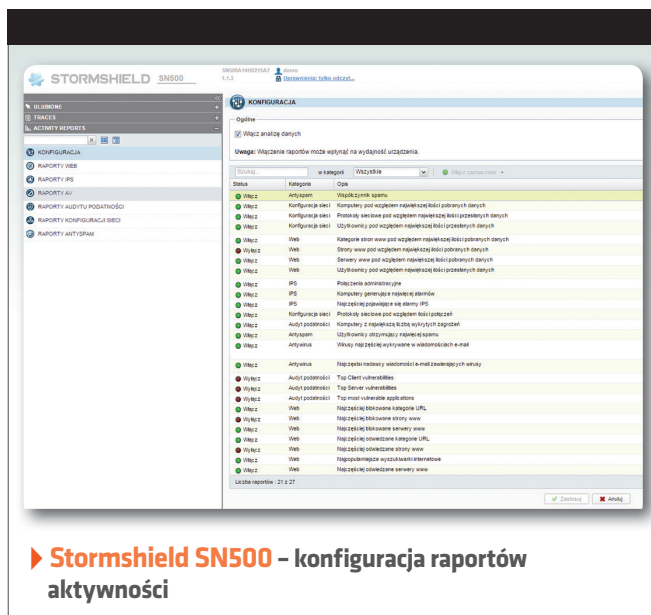
dzania adresów w takiej bazie urządzenie Netasq Stormshield nie sięga do niej za każdym razem, kiedy zaistnieje potrzeba sklasyfikowania tego samego obiektu URL. UTM pamięta ten adres przez około pół godziny, po czym następuje ponowne sprawdzenie.

Dzięki bardzo szczegółowej  
i głębokiej inspekcji pakietów



Stormshield SN500 potrafi w czasie rzeczywistym sprawdzić i określić, jaka aplikacja nawiązuje połącze-

z określeniem urządzeń, z których dana osoba może uzyskać dostęp do sieci, a także w jakich dniach lub godzinach.



► **Stormshield SN500 – konfiguracja raportów aktywności**

nie z internetem, dzięki czemu systemy IPS i ASQ są w stanie zablokować dostęp serwisom, które w niekontrolowany sposób mogłyby zainfekować sieć lokalną lub zbyt nią obciążyć.

Rozwiązanie Netasq bardzo dobrze radzi sobie również w zakresie kontroli użytkowników mających dostęp do sieci. Administrator łatwo może utworzyć i przypisać reguły określające możliwości działania poszczególnych użytkowników lub całych grup. Dzięki elastycznym politykom bezpieczeństwa można blokować ruch na poziomie użytkowników, a także monitorować i analizować poczynania pracowników.

Mechanizmy autoryzacji wykorzystywane w urządzeniach Stormshield dają bardzo duże możliwości kreowania uprawnień wybranych użytkowników, włącznie

Oprócz możliwości zbudowania zwykłej wewnętrznej bazy użytkowników, każde urządzenie daje możliwość uruchomienia własnej bazy LDAP. Dodatkowo Netasq współpracuje również z Active Directory, RADIUS oraz Kerberos.

Kolejnym elementem, o którym trzeba wspomnieć przy okazji testowania urządzenia Netasq Stormshield jest Pasywny Skaner Wnętrza Sieci. Wykonuje on Audyt Podatności polegający na wykrywaniu luk bezpieczeństwa w chronionym środowisku. Działa on za każdym razem, kiedy dowolne urządzenie generuje w sieci ruch przechodzący przez urządzenie Stormshield. Podczas kontroli ustalane są informacje o aplikacji, która wygenerowała ruch, a następnie jest ona sprawdzana pod kątem podatności na ataki.

Audyt podatności wyszukuje nieaktualne wersje oprogramowania na stacjach roboczych i serwerach, przy czym wykrywa również niedozwolony ruch w sieci. W przypadku nieprawidłowości wskazuje zagrożone urządzenie oraz sugeruje rozwiązanie poprzez wskazanie odpowiednich poprawek do aplikacji i systemów.

## BEZPIECZNY DOSTĘP Z ZEWNĄTRZ

Konfiguracja urządzeń Stormshield pozwala również na zabezpieczenie komunikacji z odległymi lokalizacjami oraz pracę użytkowników zewnętrznych zgodną z regułami polityk security. Kanaly zdalnych połączeń można zestawiać przy wykorzystaniu protokołów IPSec, SSL lub PPTP, przy czym ostatni wskazany jest bardziej do celów testowych niż produkcyjnych.

Dla dostępu realizowanego przez SSL VPN możliwe jest uruchomienie portalu, który

będzie zawierał listę niezbędnych aplikacji możliwych do uruchomienia w ramach połączenia tunelowanego lub korzystając z dowolnego klienta OpenVPN uzyskać pełen dostęp do sieci wewnętrznej firmy. Wysoka wydajność szyfrowanych połączeń VPN uzyskiwana jest dzięki sprzętowej akceleracji ASIC (Application Specific Integrated Circuit), która odpowiada za szyfrowanie tuneli IPSec.

Natomiast ciągłość ruchu dla połączeń tunelowanych zapewniona jest przez funkcję VPN Failover, która w przypadku awarii tunelu podstawowego zestawia automatycznie zapasowy kontynuując możliwość komunikacji między stronami połączenia.

Co ważne, do zestawienia połączeń Site-to-Site nie ma konieczności użycia wyłącznie urządzeń firmy Netasq. Do poprawnej konfiguracji wystarczy z drugiej strony użyć sprzętu, który obsługuje

## Netasq Stormshield SN500 Specyfikacja techniczna

### WYDAJNOŚĆ

Firewall	1 Gb/s
Firewall + IPS	1 Gb/s

### ŁĄCZNOŚĆ SIECIOWA

Liczba jednoczesnych sesji	250 000
Nowe sesje na sekundę	20 000
802.1Q VLAN (maks.)	256
Liczba ISP (maks.)	8

### VPN

Przepustowość IPSec	500 Mb/s
Maks. liczba tuneli IPSec	500 Mb/s
Maks. liczba tuneli SSL	25

### ANTYWIRUS

Przepustowość HTTP	200 Mb/s
--------------------	----------

poprawnie komunikację VPN w standardzie IPsec.

## MONITOROWANIE I LOGOWANIE

Dane niezbędne do analizy pracy urządzenia lub elementów sieci obsługiwanych przez Stormshield SN500 zapisywane są na wewnętrznym dysku sieciowym (dla tego modelu jest to 120 GB) lub karcie SD.

Narzędziem, które pozwala na bieżąco śledzić pracę systemu jest Real Time Monitor. Umożliwia on sprawdzanie najważniejszych parametrów sieci, aktywności użytkowników oraz procesów samego urządzenia. Jest to element pakietu Stormshield Administration Suite, który dostępny jest w cenie urządzenia.

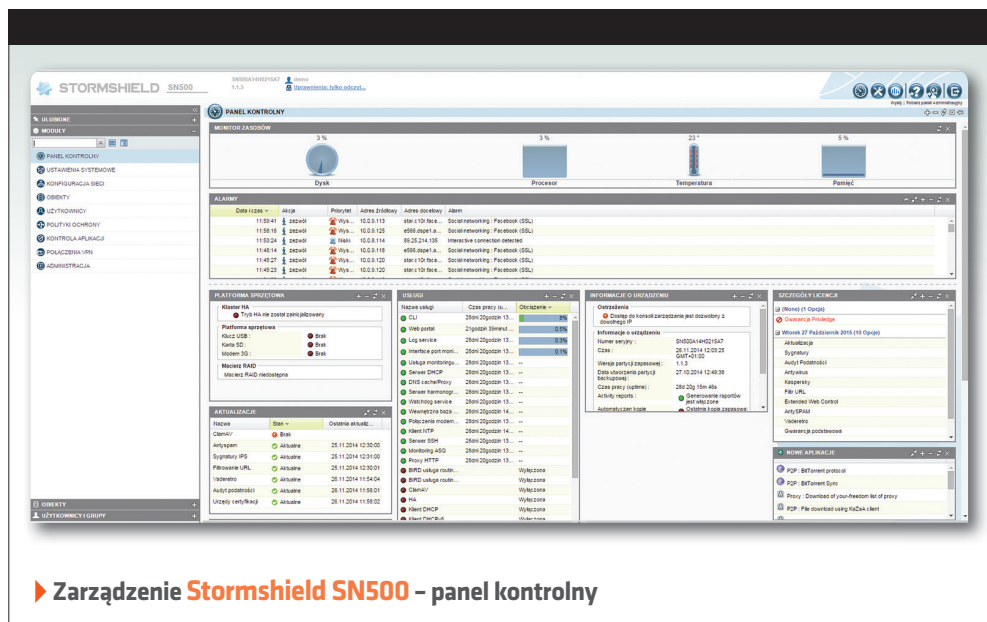
Bezpłatnym narzędziem analitycznym dla administratorów wykorzystujących urządzenia firmy Netasq jest również Stormshield Event Reporter Light. Zawiera ono listę najpotrzebniejszych szablonów raportów dotyczących najważniejszych modułów funkcyjnych urządzenia Stormshield SN500. Potrafi generować raporty na podstawie danych z filtra WWW, systemu IPS oraz Audytu Podatności, które zawierają informacje o użytkownikach i odwiedzanych przez nich stronach, lukach w aplikacjach sieciowych oraz alarmach generowanych przez system IPS. Raporty generowane są w postaci plików PDF oraz CSV i dostępne z poziomu konsoli WWW.

Możliwe jest również użycie bardziej rozbudowanego, ale za to płatnego narzędzia przeznaczonego głównie dla dużych firm. Jest to Stormshield Event Analyzer, który za pośrednictwem interak-

tywnych raportów, generowanych na podstawie danych urządzenia przechowywanych w bazie MS SQL dostarcza dokładnych informacji na temat odwiedzanych przez pracowników stron, ilości ściąganych danych oraz fra-

zmytnych raportów, generowanych na podstawie danych urządzenia przechowywanych w bazie MS SQL dostarcza dokładnych informacji na temat odwiedzanych przez pracowników stron, ilości ściąganych danych oraz fra-

zmytnych raportów, generowanych na podstawie danych urządzenia przechowywanych w bazie MS SQL dostarcza dokładnych informacji na temat odwiedzanych przez pracowników stron, ilości ściąganych danych oraz fra-



► Zarządzenie Stormshield SN500 – panel kontrolny

tywnych raportów, generowanych na podstawie danych urządzenia przechowywanych w bazie MS SQL dostarcza dokładnych informacji na temat odwiedzanych przez pracowników stron, ilości ściąganych danych oraz fra-

## PODSUMOWANIE

Możliwości, jakie dają urządzenia firmy Netasq sprawiają, że każdy, kto poważnie myśli o zabezpieczeniu sieci firmowej przed zagrożeniami, dbając przy tym o prostotę instalacji i obsługi oraz utrzymanie wysokiej wydajności połączeń sieciowych powinien rozważyć jego zakup. Dostępne różno-

kazała, że są to elementy zabezpieczenia z najwyższej półki, ale testy modelu z serii Stormshield potwierdziły nas w przekonaniu, że każdy, kto dokona wyboru urządzenia Stormshield z pewnością będzie spał spokojnie bez obawy o bezpieczeństwo własnej sieci.

Testowany model Stormshield SN 500 wraz z rocznym wsparciem technicznym to koszt rzędu 2700 euro netto. Dla porównania, najniższy model z całej serii – SN150 można nabyć za mniej niż 500 euro netto. Jeśli chodzi o dostępny serwis to wraz z pojawieniem się serii Stormshield powiększyła się też liczba opcji licencyjnych. Dwie podstawowe opcje,

Security Pack, który przeznaczony jest dla dwóch najmniejszych modeli – SN150 oraz SN200 – i pozwala korzystać jedynie z funkcji firewall, IPS, a także VPN. Ostatnią opcją licencyjną jest Enterprise Security Pack, który w odróżnieniu od Remote Office Security Pack został dodatkowo wyposażony w Audyt Podatności. Wsparcie techniczne zawarte jest w cenie pakietu licencyjnego. Każdy klient, bez względu na to, jaką opcję wybierze, otrzymuje wsparcie telefoniczne oraz drogą e-mailową. Dodatkowo klienci mogą skorzystać z autoryzowanych przez producenta szkoleń dotyczących produktów Stormshield. ■