SIECI | CENTRUM DANYCH | KOMUNIKACJA | TESTY I PORÓWNANIA | BEZPIECZEŃSTWO | ROZWIĄZANIA DLA MSP

Networld

PRZEDRUK

MAJ 2014 (05/212) INDEKS 328820 CENA 26,90 ZŁ (W TYM 5% VAT) www.networld.pl

PAMIĘCI MASOWE

OFENSYWA UKŁADÓW NAND/FLASH

TEST

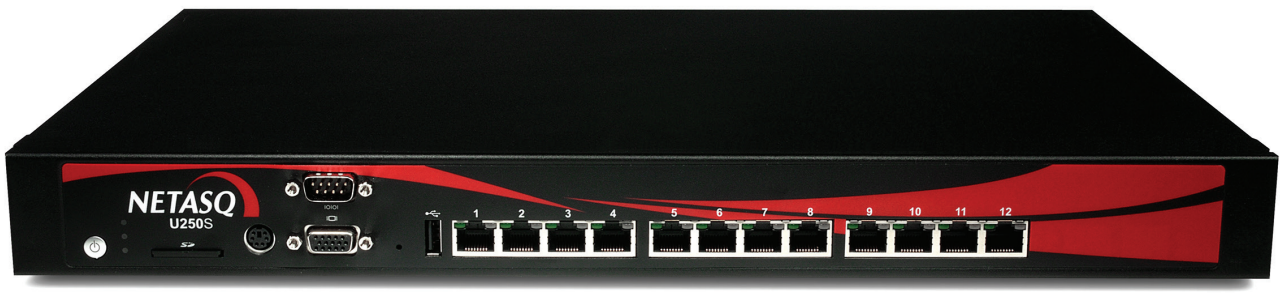
NETASQ U250S

ISSN 1232-8723

JAK CHŁODZIĆ MAŁĄ SERWEROWNIĘ
Małe środowisko IT wymaga specyficznego podejścia do planowania systemów wentylacji

FIBRE CHANNEL W ODWROCIE
Technologia Fibre Channel stopniowo traci przewagę nad Ethernetem. Czy czeka ją ostateczne wyparcie?

Bezpieczeństwo zintegrowane dla każdego



Ochrona sieci, stacji roboczych i użytkowników za pomocą jednego urządzenia? Jeszcze niedawno małe i średnie firmy nie mogły sobie pozwolić na takie rozwiązania. Dziś sytuacja zmieniła się na tyle, że wielu producentów urządzeń UTM dostosowuje swoją ofertę również do potrzeb i możliwości niewielkich przedsiębiorstw. Przykładem takiego działania jest firma Netasq i jej urządzenie U250S.

Jarosław Kowalski

Zanim przystąpiliśmy do instalacji i konfiguracji urządzenia UTM Netasq U250S, przejrzeliśmy zasoby, dostępne na stronach producenta, dotyczące wdrożenia. Bez problemu można znaleźć dokumentację techniczną, bazę wiedzy czy opis konkretnych rozwiązań. Mimo tego, iż właściwie wszystko w IT kręci się wokół języka angielskiego, miłym zaskoczeniem była dostępność dokumentacji w języku polskim.

Urządzenie UTM Netasq U250S jest niewielkich rozmiarów (1U) i mimo tego, że można je zamontować w standardowej szafie 19-calowej, z powodzeniem zmieści się na niedużej półce. Wyposażone jest w 12 gigabitowych portów, które na panelu nie są oznaczone (np. WAN, LAN, DMZ), a jedynie ponumerowane. Dodatkowo do dyspozycji jest port konsolowy oraz gniazdo monitora i klawiatury PS/2 w przypadku, gdy wykonujemy konfigurację w trybie tekstowym. Gniazda fizyczne monitora i klawiatury w urządzeniu mogą się przydać wtedy, gdy w wyniku błędnej konfiguracji korzystanie ze zdalnego połączenia stanie się niemożliwe. Na przednim panelu znajduje się również gniazdo USB, do którego można podłączyć dedykowany modem GSM (aby zapewnić redundancję połączenia internetowego) oraz gniazdo kart SD, gdyby konieczny był zapis danych urządzenia na nośniku zewnętrznym.

INSTALACJA I KONFIGURACJA

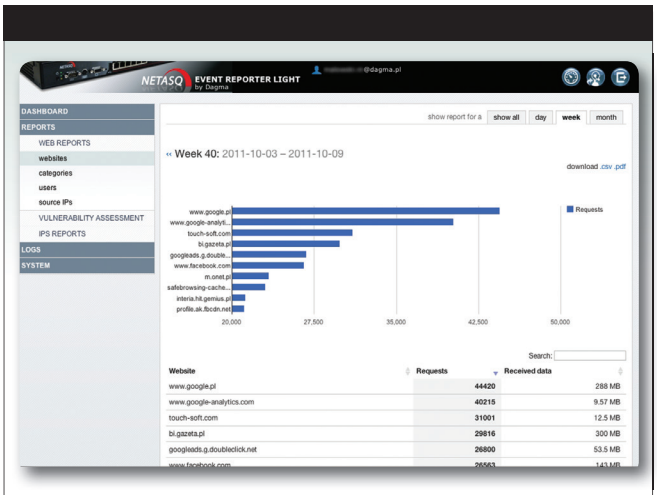
Instalację i podstawową konfigurację urządzenia można

przeprowadzić w kilku prostych krokach przy użyciu wiersza poleceń lub przeglądarki internetowej, łącząc się z fabrycznie ustalonym adresem IP. Przy pierwszym uruchomieniu można użyć kreatora konfiguracji, który pozwoli ustalić podstawowe parametry pracy (m.in. adresacje IP od strony WAN i LAN, hasło administratora) lub bezpośrednio z menu panelu webowego odnaleźć odpowiednie opcje i je skonfigurować. My wybraliśmy drugą opcję, łącząc się od razu z panelem zarządzania.

Netasq U250S może pracować w dwóch trybach – jako router umożliwiający dostęp do internetu oraz w trybie transparentnym, gdy w sieci jest już zainstalowany router i nie chcemy zmieniać bieżącej konfiguracji infrastruktury. Z uwagi na brak oznaczenia interfejsów co do ich przeznaczenia przy pierwszym podłączeniu do sieci WAN i LAN należy kierować się wskazówkami producenta (port1 – WAN, port2 – LAN). Dla zapewnienia dostępu do internetu oprócz adresacji IP na odpowiednich portach należy skonfigurować bramę, translację adresów oraz zdefiniować reguły zapory sieciowej zezwalające na wybrany ruch sieciowy.

UTM-y ze średniej półki często nie odbiegają funkcjonalnie od wersji korporacyjnych, a różnią się jedynie wydajnością. Problemem może być spadek wydajności związany z uruchomieniem wszystkich funkcji kompleksowej ochrony, jednak producenci coraz częściej implementują dodatkowe rozwiązania sprzętowe i programowe, mające na celu zapewnienie komfortu pracy bez względu na obciążenie.

Interfejs WWW, przez który wykonywaliśmy instalację i konfigurację, jest typowy dla urządzeń UTM. Ekran podzielony jest na dwie główne części funkcjonalne. Lewa kolumna zawiera menu w postaci drzewa, z pogrupowanymi opcjami. W głównym oknie oprócz informacji o pracy maszyny znajdują się szczegółowe opcje konfiguracyjne, dostępne po wskazaniu elementów z menu po lewej stronie. Ekran startowy zaraz po zalogowaniu pokazuje w głównym oknie najważniejsze dane dotyczące pracy urządzenia. Znaleźć tam można podstawowe informacje o urządzeniu, licencjach czy uruchomionych usługach. Dodatkowo widoczne są ostatnie alarmy dotyczące modułów bezpieczeństwa, konfiguracja interfejsów sieciowych oraz stan aktualizacji poszczególnych modułów. Okienka informacyjne zorganizowane są w postaci widgetów, których położenie można dostosować do własnych potrzeb lub całkowicie wyłączyć.



Event Reporter Light – przykładowy raport

O ile menu jest zorganizowane w sposób bardzo przejrzysty i intuicyjny, to główne okno może początkowo dezorientować użytkownika liczbą domyślnie uruchomionych okienek informacyjnych. Najlepiej od razu pozbyć się zbędnych elementów interfejsu. Również podczas przeglądania zawartości menu można zauważyć, że do każdego wybranego modułu funkcjonalnego dostępnych jest bardzo dużo opcji konfiguracyjnych, specyficznych wymagań środowiska IT.

Do zarządzania działaniem urządzenia może też służyć udostępnione przez producenta dodatkowe, bezpłatne oprogramowanie Netasq Administration Suite. Jest to zestaw trzech programów, w którego skład wchodzi narzędzie do centralnego zarządzania wieloma urządzeniami UTM – Netasq Unified Manager (do 5 urządzeń bezpłatnie), Event Reporter Light służący do raportowania o zdarzeniach oraz Netasq Real-Time Monitor, pozwalający na śledzenie stanu sieci w czasie rzeczywistym.

FUNKCJONALNOŚĆ

Netasq U250S integruje najważniejsze moduły do zapewnienia bezpiecznego ruchu pomiędzy odrębnymi segmentami sieci wewnętrznej oraz nieprzerwanego dostępu do internetu. Konfiguracja opiera się w głównej mierze na obiektach oraz użytkownikach, biorących udział w działaniu modułów UTM-a i będących podstawą realizacji polityk dostępu. Obiektami mogą być

elementy sieciowe (adres lub przedział IP, cała sieć, protokół lub port), a także pojedyncze i pogrupowane adresy URL lub certyfikaty bezpieczeństwa. Jako obiekty definiuje się również harmonogramy, wykorzystywane następnie do określenia czasu obowiązywania polityk zabezpieczeń.

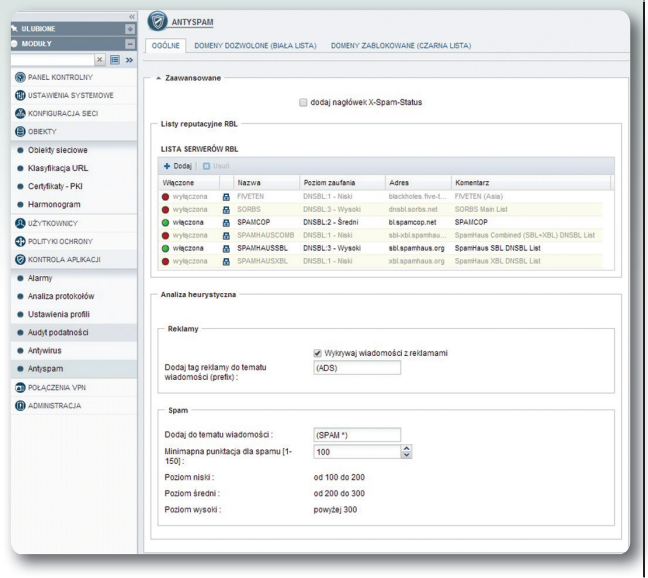
Podstawową konfiguracją UTM-a przy wykorzystaniu w charakterze bramy internetowej jest routing. Trasowanie pakietów można skonfigurować na kilka sposobów. Oprócz routingu statycznego określającego ruch między sieciami dostępnymi na poszczególnych interfejsach, można ustalić *Policy Routing*, gdzie w zależności od adresu źródłowego lub docelowego bądź rodzaju usługi (serwis, port) można przekierować ruch przez wybraną, zdefiniowaną bramę internetową. Przykładem może być rozdzielenie ruchu http od usług pocztowych (POP3, SMTP).

W wypadku konfiguracji urządzenia z dwoma niezależnymi łączami WAN, dostępne opcje routingu pozwalają także na włączenie równoważenia obciążenia połączenia internetowego. Można określić, czy ma się ono odbywać według adresów źródłowych lub adresu źródłowego i docelowego. W ramach równoważenia połączenia sieciowego wykorzystywany jest mechanizm Round Robin, gdzie każde następne połączenie kierowane jest do kolejnej bramy.

IPS I ZAPORA

Nieodłącznymi elementami każdego urządzenia UTM jest zapora sieciowa oraz system zapobiegający włamaniom (IPS). W rozwiązaniach Netasq zintegrowano te moduły na poziomie jądra systemu w ramach opatentowanej technologii proaktywnego wykrywania i blokowania ataków – Active Security Qualification. Dzięki niej firmowa sieć ma być chroniona przed najnowszymi zagrożeniami, dla których sygnatury jeszcze nie powstały. Ponadto technologia jest w stanie eliminować złośliwy kod zanim zostanie on wykonany przez przeglądarkę. Standardowy system IPS w momencie wykrycia podejrzanego kodu HTML blokuje całą stronę internetową, natomiast rozwiązanie zastosowane w urządzeniu Netasq izoluje i blokuje podejrzany element HTML, po czym „wycina" go z kodu strony, a oczyszczona wersja strony zostaje wysłana do przeglądarki.

Sama konfiguracja zapory składa się z dwóch etapów.

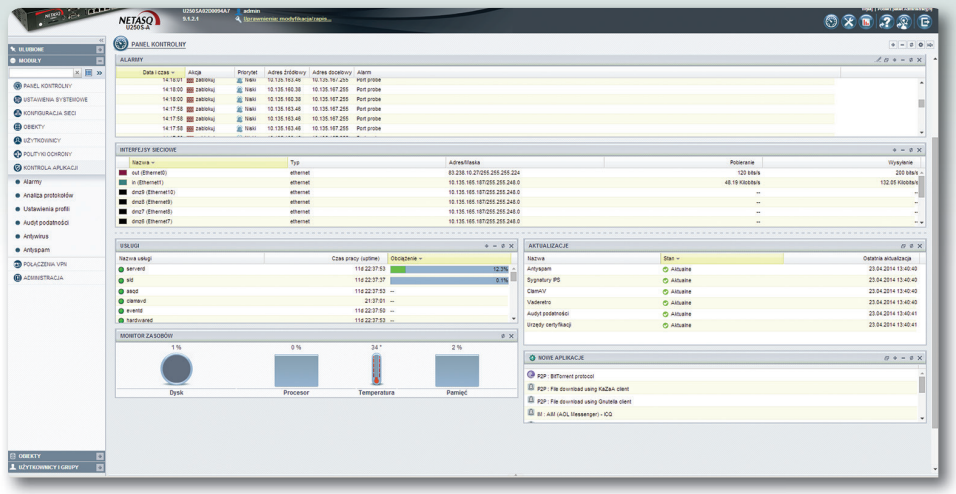


Konfiguracja filtra antyspamowego

W pierwszym reguły są domyślne definiowane przez producenta; mają na celu zapewnienie komunikacji z urządzeniem nawet w przypadku, gdy zostanie uruchomiona reguła *Block All* lub administrator wprost nie stworzy reguły zezwalającej na podłączenie się do urządzenia. Nie można sprawdzić składni fabrycznie zdefiniowanych reguł – co najwyżej podejrzeć ich działanie w przystawce *Real Time Monitor*.

Dodatkową metodą konfiguracji, na którą użytkownik ma większy wpływ są lokalne polityki ochrony. Administrator ma do wyboru 10 zdefiniowanych zestawów reguł (zwanych slotami), które może konfigurować zgodnie z założonymi politykami bezpieczeństwa.

W ramach ustawień slotu określa się sposób filtrowania ruchu na poziomie firewalla,



Główny Panel Kontrolny urządzenia Netasq U250S

sposób filtrowania przez system IPS oraz inne dodatkowe moduły bezpieczeństwa sieciowego (Qos). Okno konfiguracji reguł składa się z dwóch części. W górnej zarządza się Slotami oraz regułami firewalla, natomiast dolna pozwala na definiowanie poszczególnych wpisów zapory, czyli ustalanie warunków, jakie musi spełnić ruch, aby zostać uwzględniony w czasie analizowania i realizacji polityk. Poruszanie się po panelu zarządzania regułami firewalla oraz definiowanie wpisów jest łatwe i nie powinno sprawić żadnych problemów dzięki przejrzystości i prostocie nawigowania między elementami interfejsu.

W rozwiązaniach Netasq zintegrowano zaporę sieciową i IPS na poziomie jądra systemu w ramach opatentowanej technologii proaktywnego wykrywania i blokowania ataków – Active Security Qualification. Dzięki niej firmowa sieć ma być chroniona przed najnowszymi zagrożeniami, dla których sygnatury jeszcze nie powstały. Ponadto technologia jest w stanie eliminować złośliwy kod zanim zostanie on wykonany przez przeglądarkę.

Modem 3G Netasq

Zapora jest w urządzeniu Netasq U250S elementem integrującym wszystkie moduły bezpieczeństwa. Definiując regułę filtrowania i wybierając odpowiednią opcję w kolumnie *Polityka filtrowania* administrator aktywuje bądź wyłącza poszczególne elementy ochrony. Uruchamiając system zapobiegania atakom (IPS) lub jedynie ich wykrywania (IDS) można również wybrać jeden z dziesięciu zdefiniowanych przez producenta profili systemu ASQ.

Elementem pomocnym podczas definiowania reguł firewalla jest *Analizator Reguł*, który na bieżąco sprawdza poprawność konfiguracji pod względem użytych obiektów i metod skanowania ruchu. W przypadku wykrycia nieprawidłowości analizator zawiadomi o problemie oraz zaznaczy odpowiednią regułę, której on dotyczy.

ANTYWIRUS I ANTYSPAM

Konfigurację ochrony antywirusowej oraz antyspamowej można wykonać w ramach *Kontroli Aplikacji*. Standardowo dołączony do urządzenia skaner antywirusowy oparty jest na silniku ClamAV, który skanuje całą pocztę przychodzącą (POP3) i wychodzącą (SMTP). Dzięki temu wirusy przenoszone w załącznikach są automatycznie usuwane, a odbiorca wiadomości jest informowany o eliminacji zagrożenia. Dodatkowo na obecność wirusów sprawdzane są także protokoły HTTP oraz FTP. W ramach rozszerzonej, płatnej licencji można wyposażyć urządzenie w skaner antywirusowy oparty na rozwiązaniach firmy Kaspersky.

Ochrona antyspamowa, która wykorzystuje heurystyki rozwijane w technologii ASQ, stanowi podstawę obrony przed niepożądanymi wiadomościami. W zależności od polityki bezpieczeństwa firmy, administrator może skonfigurować filtr antyspamowy tak, aby oznaczał wiadomości jako spam i przepuszczał dalej do adresata lub je całkowicie blokował. W konfiguracji filtra antyspamowego dla zaufanych nadawców można utworzyć białą listę, aby e-maile od nich były zawsze zaufane, natomiast czarna lista skutecznie blokuje wskazanych nadawców spamu.

FILTROWANIE ADRESÓW I KONTROLA APLIKACJI

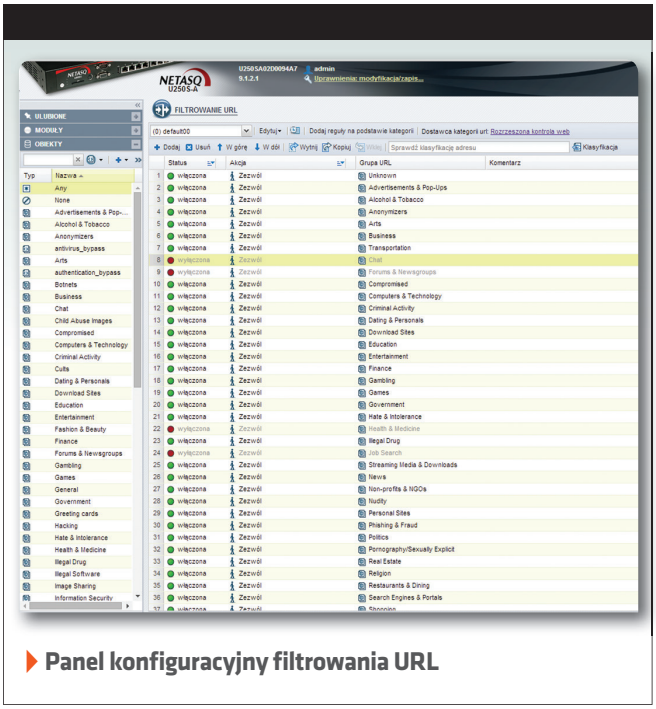
Moduł filtrowania adresów URL dostępny jest z poziomu menu *Polityki Ochrony*. Administrator może zdefiniować aż dziesięć zestawów

filtrowania URL, które da się dowolnie modyfikować w zakresie zezwolenia lub blokowania grup tematycznych czy pojedynczych adresów. Przy określaniu polityki filtrowania administrator korzysta z gotowej, dostarczonej przez producenta, klasyfikacji adresów URL. W konfiguracji podstawowej urządzenia, Netasq udostępnia bazę polskich adresów internetowych. Filtr ten umożliwia identyfikację 53 kategorii tematycznych, według których określa się polityki dostępu.

Oprócz obsługi zwykłego protokołu HTTP, filtr URL pozwala również na blokowanie stron w ruchu szyfrowanym (HTTPS). Jeżeli moduł nie uwzględnia danego serwisu, w prosty i szybki sposób można zgłosić dystrybutorowi rozwiązań Netasq, firmie Dagma, konieczność dodania strony do klasyfikacji, przy gwarancji uwzględnienia serwisu w ciągu jednego dnia roboczego od zgłoszenia.

Rozszerzony filtr URL dostępny jest jako dodatkowa, płatna opcja bazująca na definicjach ponad 65 kategorii dostępnych (ponad 100 milionów adresów URL) w chmurze, z czego osiem bezpośrednio dotyczy bezpieczeństwa. W tym przypadku filtrowanie adresów polega na wysyłaniu zapytań dotyczących klasyfikacji URL do chmury, dzięki czemu urządzenie nie jest obciążone przez utrzymywanie wszystkich definicji adresów w pamięci wewnętrznej.

Netasq U250S pozwala administratorom zdecydować, z których aplikacji dostępnych przez sieć mogą korzystać użytkownicy. Dzięki głębokiej inspekcji pakietów urządzenie potrafi w czasie rzeczywistym określić, jaka aplikacja łączy się z internetem i sprawdzić szczegóły tego połączenia. Dzięki temu system IPS, wzmocniony systemem ASQ, wykrywa i blokuje aplikacje, które łącząc się z sieciami zewnętrznymi mogą powodować infekcję sieci lokalnej lub jej nadmierne obciążenie.



Panel konfiguracyjny filtrowania URL

ZDALNY DOSTĘP

Jak większość urządzeń UTM, Netasq U250S zapewnia również możliwość dostępu do zasobów wewnętrznych przez tworzenie bezpiecznych kanałów VPN. Dzięki serwerowi VPN wbudowanemu w Netasq można tworzyć bezpieczne połączenia między odległymi od siebie oddziałami firmy (Site-to-Site), a także między firmą a pracownikami zdalnymi (Client-to-Site). Zestawiane kanały VPN budowane są na bazie jednego z protokołu IPSec, SSL lub PPTP. Producent wyposażył urządzenie w sprzętową akcelerację ASIC (Application Specific Integrated Circuit) odpowiadającą za szyfrowanie tuneli IPSec, dzięki czemu potrafi ono utrzymać wysoką wydajność mimo opóźnień wynikających z szyfrowania zdalnych połączeń.

Dodatkowo, dzięki funkcji VPN Failover można zapewnić ciągłość ruchu przesyłanego tunelami IPSec VPN poprzez automatyczne zestawianie zapasowego tunelu VPN w przypadku awarii podstawowego. Realizacja tunelowania jest ułatwiona dzięki temu, że Netasq zapewnia możliwość tworzenia połączeń z urządzeniami innych firm oraz aplikacjami klienckimi przy wykorzystaniu dowolnego produktu obsługującego standard VPN w protokole IPSec.

Netasq U250S

PASYWNY SKANER WNĘTRZA SIECI

Funkcją, o której warto wspomnieć, jest też audyt podatności,

realizowany przez pasywny skaner wnętrza sieci. Skaner wychwytuje luki bezpieczeństwa w chronionym środowisku sieciowym i działa każdorazowo, gdy komputer lub serwer z sieci LAN generuje ruch przechodzący przez urządzenie Netasq. Przesyłane pakiety są wtedy analizowane przez firewall oraz IPS i dzięki temu system uzyskuje informacje na temat aplikacji inicjującej ruch oraz jej podatności na ataki i zagrożenia. Po zakończeniu audytu administrator dostaje zestawienie aplikacji sieciowych, pracujących na stacjach roboczych w firmie. Kliknięcie wskazanej aplikacji wyświetla komputery, na których dany program został zainstalowany, podaje wersję programu i system, pod jakim działa wybrana wersja aplikacji.

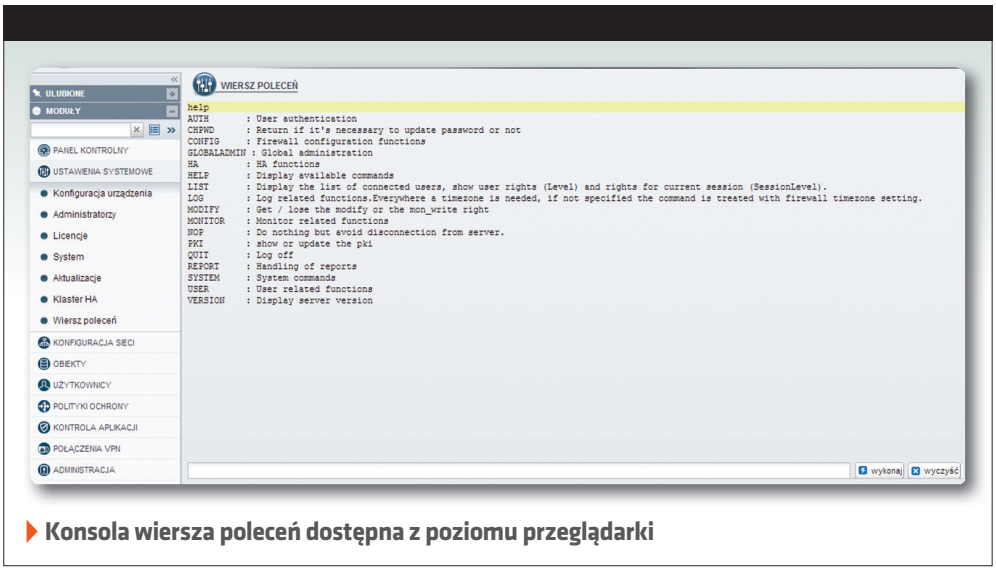
Skaner potrafi również wyszukać nieaktualne wersje oprogramowania na stacjach roboczych i serwerach, a dodatkowo wykrywa niedozwolony ruch wewnątrz sieci. W przypadku zidentyfikowania nieprawidłowości system powiadamia o nich automatycznie, wskazując zagrożone stacje robocze. Sugeruje także źródła, z których można pobrać odpowiednie poprawki i aktualizacje, które przywrócą optymalny poziom bezpieczeństwa.

PODSUMOWANIE

Urządzenie U250S ze względu na swoją wydajność, prostotę obsługi oraz zastosowane technologie z pewnością wyróżnia się wśród urządzeń typu UTM. Tym bardziej że bez względu na model klient otrzymuje pakiet funkcjonalności, które u innych producentów zwykle są dodatkowo licencjonowane, a rzeczywistym ograniczeniem są tylko parametry techniczne sprzętu. Jedynie zaawansowane opcje wymagają wykupienia dodatkowych licencji. Testowany model przeznaczony jest dla średnich firm lub oddziałów większych przedsiębiorstw (według zaleceń producenta – do obsługi do 250 stacji roboczych) i z pewnością będzie tam doskonale spełniał swoją rolę. Natomiast jeżeli klient woli wykorzystać rozwiązania firmy Netasq w chmurze prywatnej, może nabyć jedno z rozwiązań UTM w postaci maszyny wirtualnej.

Zakup Netasq U250S to koszt 3250 euro. Dodatkowe 748 euro kosztuje roczny serwis podstawowy (aktualizacje, pomoc techniczna w języku polskim, zestaw Netasq Administration Suite). Klient może zainwestować 1430 euro w roczny serwis Premium UTM Security Pack, który zawiera serwis podstawowy, a oprócz tego dodatkową ochronę antywirusową Kaspersky, audyt podatności, rozszerzony filtr URL oraz obsługę kart SD. Serwis podstawowy oraz Premium UTM Security można nabyć na okres od roku do pięciu lat, przy czym wygaśnięcie serwisu nie oznacza zaprzestania pracy urządzenia, a jedynie utratę prawa do pomocy technicznej czy aktualizacji.

Firma Netasq od wielu lat specjalizuje się w tworzeniu rozwiązań zintegrowanego bezpieczeństwa, a jej produkty zostały z powodzeniem wdrożone również w polskich przedsiębiorstwach i instytucjach publicznych. U250S pozwoli firmie wzmocnić pozycję wśród uznanych producentów rozwiązań Unified Thread Management.



Konsola wiersza poleceń dostępna z poziomu przeglądarki

PARAMETRY TECHNICZNE NETASQ U250S

Przepustowość zapory sieciowej z włączonym IPS	1,8 Gb/s
Przepustowość IPSec VPN AES	350 Mb/s
Liczba równoległych sesji	600 000
Liczba nowych sesji	12 000/s
Liczba tuneli IPSec VPN	1000
Liczba tuneli SSL VPN	150
Liczna obsługiwanych użytkowników	bez limitu