

# Jak wybrać urządzenie UTM

**BEZPIECZEŃSTWO** | Coraz większą popularność wśród produktów służących ochronie sieci lokalnej zdobywają urządzenia *Unified Threat Management* (UTM). Kompleksowo zabezpieczają one styk sieci urzędu z Internetem.

Paweł Rybczyk

Urządzenia UTM zapewniają kompletną ochronę, nadzorując ruch na obrzeżu sieci lokalnej. Oferta wytwórców takich modeli może przyprawić niejednego administratora o przysłowiowy zawrót głowy. Jakże zatem przyjąć kryteria wyboru UTM? Które z funkcji są przydatne, a które mogą okazać się jedynie zbędnym dodatkiem?

## Kluczowa kwestia – wydajność

Większość administratorów postawiona przed zadaniem wyboru rozwiązania UTM dla sieci lokalnej postępuje zgodnie z ogólnie przyjętymi zasadami logiki i wyszukuje na rynku model z możliwie największą liczbą funkcji. Szybko jednak okazuje się, że zachwalane przez handlowca urządzenie po podłączeniu do punktu styku sieci lokalnej z Internetem drastycznie obniża przepustowość sieci. W efekcie administrator zaczyna czasochłonną procedurę sprawdzania każdego elementu sieci, aby zlokalizować przyczynę spadku jej wydajności.

Jak zatem wśród wielu urządzeń wybrać to właściwe, które spełni nasze oczekiwania dotyczące utrzymania odpowiedniego poziomu bezpieczeństwa i nie obniży sprawności naszej sieci?

Producenci w opisach urządzeń UTM podają najczęściej dwa parametry: przepustowość i liczbę sesji równoległych, które dany model jest zdolny obsłużyć. O wydajności danego rozwiązania decyduje integracja podstawowych elementów UTM – zapory ogniowej z systemem wykrywania i systemem zapobiegania zagrożeniom (*Intrusion Prevention System*). Wybierając konkretne urządzenie UTM, należy więc dokładnie sprawdzić, czy jego wydajność jest taka sama dla wszystkich kluczowych funkcji.

Kolejnym elementem godnym uwagi jest system operacyjny, który zarządza

urządzeniem UTM. Ma on decydujący wpływ na wydajność urządzenia, jest też parametrem wyjściowym podczas analizy pozostałych modułów UTM. Wskazane jest, by system operacyjny producenta UTM opierał się na jądrze znanego i sprawdzonego systemu. Przykładem mogą być tu rozwiązania z rodziny BSD (Open-BSD, Free-BSD), określane często jako najbezpieczniejsze.

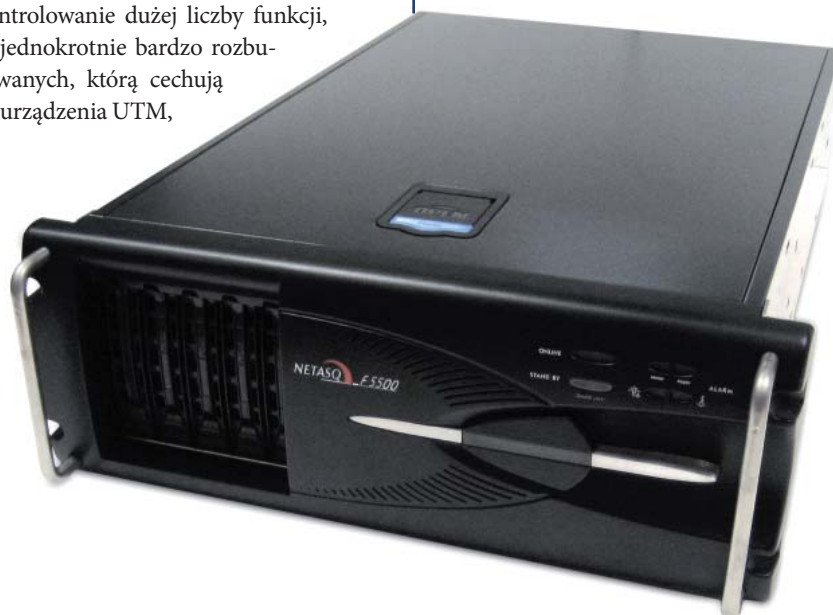
Istotną cechą urządzeń UTM jest również to, czy analiza pakietów odbywa się przez osobny moduł (*proxy mode*), czy bezpośrednio na poziomie jądra systemu (*kernel mode*). Pożądana jest jak najmniejsza liczba komunikatów wysyłanych pomiędzy odrębnymi modułami ochrony a systemem operacyjnym urządzenia. Jeśli takich komunikatów jest wiele, czas analizy znacznie się wydłuża. Najlepszym rozwiązaniem jest zatem analiza w trybie *kernel mode*, w którym moduł IPS jest skompilowany bezpośrednio w jądrze systemu.

## Ochrona, monitoring, logowanie

Zanim przystąpimy do analizy funkcji poszczególnych rozwiązań UTM, powinniśmy rozpatrzyć jeszcze aspekt zarządzania. Kontrolowanie dużej liczby funkcji, niejednokrotnie bardzo rozbudowanych, którą cechują się urządzenia UTM,

nie powinno sprawiać nam kłopotów. Pomocą dla administratora powinna być przejrzysta i intuicyjna w obsłudze konsola zarządzająca. Oczywiście weryfikacja stopnia intuicyjności konsoli jest bardzo trudna, jednak sprawdzenie pozostałych elementów – monitoringu i funkcji zarządzania logami – pozwala szybko ocenić czytelność i przejrzystość konsoli. Ważne jest, aby umożliwiała ona kontrolowanie stanu połączeń dla każdej stacji w obrębie sieci lokalnej, pozwalała weryfikować poprawność działania wszystkich usług i aktualizacji systemu oraz monitorowała ruch przechodzący przez urządzenie. Najlepsze rozwiązania typu UTM umożliwiają administratorowi przeprowadzenie takiego monitoringu już za pomocą swoich podstawowych funkcji. Dodatkową usługą jest zarządzanie logami. Niektóre modele wyposażone są w „nadobowiązkowo-

Firewall, system wykrywania i blokowania włamań IPS, serwer VPN, system antywirusowy i antyspamowy oraz system filtrowania dostępu do stron internetowych (filtr URL) to funkcje UTM F5500 firmy NETASQ.



we” a ułatwiający pracę funkcjonalności, np. rozbudowany system przechowywania logów w bazie SQL z opcją generowania automatycznych raportów.

Nowością wśród funkcji urządzeń UTM jest oferowany przez firmę NETASQ audyt bezpieczeństwa sieci lokalnej w odniesieniu do stacji klienckich. Taki system monitoruje sieć komputerową firmy czy urzędu i w razie potrzeby wskazuje potencjalne źródła ataku oraz informuje administratora o konieczności instalacji odpowiedniej aktualizacji. Tego typu skaner nie powinien przy tym generować dodatkowego ruchu w sieci lokalnej.

Można zatem pokusić się o wniosek, że podstawowymi parametrami, które należy brać pod uwagę, wybierając rozwiązanie UTM, są: wysoki poziom bezpieczeństwa przy równoczesnym zachowaniu wysokiej wydajności urządzenia oraz rozbudowana administracja.

### UTM – zintegrowana ochrona sieci

Oprócz podstawowych modułów firewall i IPS UTM-y dysponują również ochroną antywirusową (proxy dla http, smtp, pop3) oraz antyspamową (proxy dla smtp, pop3). Pożądanym uzupełnieniem zabezpieczeń antywirusowych jest funkcjonalność filtrowania stron internetowych (*URL Filtering*), która znacznie obniża prawdopodobieństwo zainfekowania sieci groźnym wirusem przez blokowanie podejrzanych stron zawierających m.in. treści pornograficzne, pirackie wersje oprogramowania, cracki itp. Producent urządzenia zaopatrzonego w taką usługę powinien udostępniać gotową klasyfikację adresów URL oraz umożliwiać administratorowi tworzenie własnej.

UTM pozwalają także zabezpieczać dostęp do sieci lokalnej ze zdalnej lokalizacji oraz umożliwiają zadanej grupie użytkowników dostęp do serwerów znajdujących się w strefie zdemilitaryzowanej (DMZ). Takie możliwości daje VPN (*Virtual Private Network*), dzięki której użytkownicy sieci korporacyjnej korzystający z jej zasobów poza godzinami pracy (np. w domu) są odpowiednio zabezpieczani m.in. dzięki szyfrowanemu połączeniu. Funkcjonalność VPN w rozwiązaniach typu UTM można podzielić na dwie grupy:

- budowanie tuneli VPN między lokalizacjami firmy (*Site-To-Site*),

### Cechy dobrego urządzenia UTM

Skuteczny UTM w podstawowej konfiguracji powinien zapewniać:

- firewall,
- Intrusion Prevention System,
- serwer VPN,
- serwer LDAP (lub możliwość integracji z istniejącą bazą),
- usługę zarządzanie logami,
- filtrowanie URL (klasyfikacja producenta, klasyfikacja administratora),
- kształtowanie pasma,
- ochronę antywirusową (protokoły http, smtp, pop3),
- ochronę antyspamową (protokoły smtp, pop3).

- budowanie tuneli VPN między użytkownikami mobilnymi a firmą (*Client-To-Site*).

Najczęściej spotykanymi protokołami wykorzystywanymi do tworzenia wirtualnej sieci prywatnej (VPN) są SSL, IPSec oraz PPTP. Najbardziej pożądana jest sytuacja, w której producent oferuje w ramach danego rozwiązania możliwość wykorzystania wszystkich trzech wymienionych protokołów. Dodatkowym atutem jest możliwość wyboru klienta VPN, czyli oprogramowania, które zapewnia szyfrowane połączenie z centralą firmy. W przypadku PPTP klient ten jest zainstalowany wraz z systemem Windows, dla IPSec – jest dostarczany przez producenta, a klientem dla SSL jest przeglądarka internetowa.


Kolejną funkcją urządzeń UTM zalecaną przy korzystaniu z VPN jest tzw. serwer usług katalogowych. Chodzi tu o możliwość stworzenia bazy użytkowników w celu ustawienia polityki bezpieczeństwa dla każdego z osobna (*per user*). W przypadku urządzeń UTM ważna jest możliwość integracji urządzenia z istniejącym serwerem LDAP, AD (*Active Directory*) lub uruchomienie takiej usługi bezpośrednio na urządzeniu. Dzięki takiemu rozwiązaniu reguły na firewallu są tworzone dla konkretnej uwiarygodnionej osoby (grupy osób), niezależnie od tego, z której stacji (z którego IP) osoba ta korzysta.

Przydatną funkcją jest możliwość tworzenia kalendarzy, które pozwalają określić m.in. w jakich godzinach lub dniach powinien działać konkretny zestaw reguł. Może on odnosić się do zbioru reguł na firewallu,

filtra URL lub do translacji adresów (NAT) czy VPN. Przykładem wykorzystania funkcji kalendarzy jest blokowanie w godzinach pracy stron internetowych umożliwiających zakupy on-line i odblokowywanie ich po zakończeniu pracy. Powiązanie zbiorów reguł z kalendarzami może być wykorzystywane również przy kształtowaniu pasma (*Traffic Shaping*). W wyniku tego kontrola obciążenia pasma może odbywać się przez urządzenia automatycznie z różnymi rygorami w zależności od dnia tygodnia i godziny. Rozwiązanie to umożliwia określanie limitu dla danego ruchu w postaci wartości dyskretnych np. przy użyciu wartości procentowych. Pozwala to na zastosowanie bardzo elastycznej polityki dotyczącej regulacji ruchu pakietów w sieci.

Często pomijaną funkcjonalnością UTM jest możliwość zapewnienia ciągłości połączenia w przypadku awarii któregoś z łączy ISP. Innymi słowy – chodzi o konfigurację łącza zapasowego, które zostaje uruchomione, gdy łącze główne staje się niedostępne. Taka funkcjonalność umożliwia także równoważenie łączy przy jednoczesnym korzystaniu z usług dwóch lub większej liczby dostawców.

### Kompleksowa analiza

Produkty zabezpieczające typu UTM z pewnością spełnią oczekiwania nawet najbardziej wymagających administratorów. Ważne, aby podczas kompleksowego badania wszystkich parametrów UTM, zwrócić szczególną uwagę, czy funkcja zarządzania logami jest dostarczana przez producenta wraz z podstawową licencją na urządzenie, oraz najważniejsze – na jakich warunkach wytwórca udziela gwarancji na swój produkt. Podczas zakupu warto również sprawdzić, czy dystrybutor zapewnia lub umożliwia uczestnictwo w szkoleniach na temat danego rozwiązania w autoryzowanym centrum treningowym. 

Autor jest inżynierem systemowym w firmie DAGMA sp. z o.o., zajmującej się bezpieczeństwem IT. Absolwent informatyki Uniwersytetu Śląskiego w Katowicach oraz Jyväskylä Politechnic w Finlandii. Specjalizuje się w tematyce zapewniania bezpieczeństwa danych, ochronie sieci przed atakami z zewnątrz oraz zintegrowanych rozwiązaniach typu UTM.