

# NETWORLD

## Firewalle nowej generacji

17 lutego 2011 13:03

*Józef Muszyński, IDG News Service*

**Tradycyjne zapory ogniowe dla przedsiębiorstw, których działanie jest głównie oparte na blokowaniu portów, powoli są wypierane przez nową generację urządzeń - szybsze i inteligentniejsze "firewalle aplikacyjne", określane jako NGFW (next-generation firewalls). Wymagają one zupełnie innego sposobu myślenia o zadaniach ochronnych zapór ogniowych.**

Przedsiębiorstwa planujące przejście z tradycyjnych zapór ogniowych na firewalle nowej generacji powinny zaczynać od przestawienia się na zdecydowanie inny sposób myślenia o zadaniach bezpieczeństwa przypisanych do zapory, zwłaszcza w zakresie ustanawiania kontroli aplikacji używanych przez pracowników korzystających z dostępu do internetu - witryn WWW i portali społecznościowych. Stary sposób myślenia o tradycyjnych zaporach bazujących na portach, z administratorami systemu posługującymi się "językiem protokołów", obecnie okazuje się już nieadekwatny do potrzeb. Firmy muszą przystosować się do używania bardziej "biznesowego" słownika, związanego z używanymi aplikacjami i zrozumiałego na szczeblu zarządu.

**Zapory nowej generacji są zorientowane na aplikacje**, umożliwiając przedsiębiorstwom wymuszanie na pracownikach stosowanie się do reguł polityk używania aplikacji, opartych na tożsamości.

**NGFW (next-generation firewalls)** mogą oferować także funkcje VPN, możliwość wykonywania analiz ruchu pod kątem zapobiegania włamaniom; mogą również wykorzystywać techniki filtrowania według reputacji i integrują się z usługami katalogowymi w obszarze zarządzania tożsamością i politykami. Taka definicja została zaproponowana przez firmę Gartner, a dostawcy rozwiązań do ochrony sieci (m.in. Palo Alto Networks, McAfee, Check Point, Fortinet, Sonic Wall) zaczęli tym terminem określać swoje niektóre produkty.

Ile czasu potrzeba, żeby termin NGFW znalazł się w powszechnym użyciu? Za pierwszego dostawcę, który zawarł funkcje NGFW w swoich produktach, uważa się firmę Palo Alto Networks z kalifornijskiej Doliny Krzemowej (założoną przez Nir Zuka, współtwórcę pierwszych firewalli z technologią *stateful inspection*, wcześniej pracownika m.in. Check Point), która w 2007 r. zaoferowała serię pionierskich urządzeń typu NGFW. Inni dostawcy, m.in. Fortinet, Cisco, Check Point, McAfee, rozszerzyli funkcje swoich produktów w tym kierunku. Również firmy specjalizujące się w IPS (np. Sourcefire) zapowiadają na ten rok aplikacyjne zapory ogniowe, choć różniące się nieco funkcjonalnie od urządzeń Palo Alto Networks. Jednakże wykorzystanie zaawansowanych firewalli jest obecnie ciągle niewielkie. Choć termin NGFW funkcjonuje od co najmniej 3 lat, to według danych Gartnera, ich rzeczywiste wykorzystanie obecnie jest bardzo niewielkie - poniżej 1%. Jednocześnie analitycy Gartnera patrzą w przyszłość optymistycznie i przewidują, że w 2014 r. ich wykorzystanie wzrośnie do 35%. Dostawcy ciągle rozwijają swoje oferty i przewiduje się, że w niezbyt odległej perspektywie czasowej NGFW powinna stać się zaporą podstawową.

Jednym z czynników zwiększających zainteresowanie NGFW jest potrzeba bardziej wnikliwego przyglądania się działaniom w sieci i konsumpcji pasma. Za pośrednictwem NGFW przedsiębiorstwa mogą utrzymywać lepszą kontrolę aplikacji, związaną z zapotrzebowaniem na pasmo i nadawaniem priorytetów dla określonego ruchu aplikacyjnego. Ponadto niektóre NGFW (np. Check Point czy SonicWall) mogą działać podobnie jak narzędzia DLP (*data-loss prevention*), blokując wycieki na podstawie słów kluczowych czy innych definicji.

Pojęcie NGFW obejmuje zapory ogniowe dla przedsiębiorstw zapewniające efektywną realizację funkcji zapobiegania włamaniom w odniesieniu do ruchu, jak również mające baczenie na przechodzący przez zaporę ruch aplikacyjny - w celu egzekwowania reguł polityki określających dopuszczalne korzystanie z aplikacji (na podstawie tożsamości użytkownika). Zapora taka ma też mieć możliwość wykorzystywania takich informacji, jak analiza reputacji internetowej - w celu wspomaganie filtrowania malware, lub integracji z Active Directory.

Jednak według niektórych dostawców, przyszłość NGFW nadal jest niepewna. Wskazują oni na brak testów przeprowadzonych przez niezależne laboratorium - ICSA Labs rozważa możliwość przeprowadzenia testów różnych produktów, ale problemem jest klarowna definicja, czym właściwie jest NGFW? Gartner, lansując własną definicję, zauważa, że niektórzy dostawcy oferują kontrolę aplikacji, a inni tylko bardziej zaawansowane IPS. Większość producentów zapór dla przedsiębiorstw jest jeszcze na wczesnym etapie dochodzenia do pełnego modelu NGFW.

Zamieszanie wprowadza też określenie Unified Threat Management (UTM) - analitycy firmy badawczej IDC uważają, że UTM ma z grubsza to samo znaczenie co NGFW. Jednak według Gartnera termin UTM powinien być stosowany do rozwiązań bezpieczeństwa używanych w małym lub średnim biznesie, podczas gdy NGFW jest przeznaczona do dużych przedsiębiorstw (za takie firma uważa organizacje zatrudniające powyżej tysiąca pracowników).

W opinii wielu specjalistów, nie warto konsolidować wszystkiego w jednej skrzynce w ochronie bardziej rozbudowanych sieci. Pozostaje także pytanie o rolę NGFW, gdy użytkownicy nie działają za zaporą ogniową - podróżując z laptopem lub używając urządzeń mobilnych? Tutaj rozwiązaniem może być funkcja VPN wbudowana w zaporę nowej generacji.

<http://www.networld.pl/news/367236/Firewalle.nowej.generacji.html>