Zapory ogniowe realizuje się nie tylko programowo

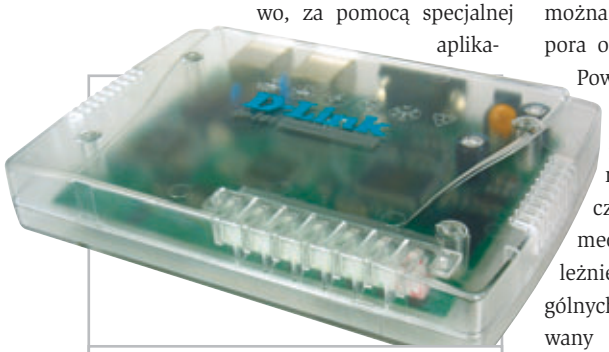
Potęga żelastwa

Nieco ponad 500 zł trzeba wydać, by sprzętowo chronić komputery podpięte do sieci globalnej. Jakich zabezpieczeń możemy się spodziewać za takie pieniądze?

Jerzy Michalczyk

Zapora ogniowa to podstawowy środek ochrony sieci prywatnych przed infiltracją ze strony osób niepowołanych. W większości przypadków chroniony jest dostęp do mocy obliczeniowej sieci oraz i udostępnianych przez nią zasobów. Firewall jest oprogramowaniem komputerowym lub urządzeniem instalowanym na styku sieci lokalnej (LAN) i rozległej (WAN, np. Internet). Dzięki skoncentrowaniu w jednym punkcie całego ruchu przechodzącego między nimi możliwa jest kontrola wszystkich informacji przesyłanych w obie strony i eliminowanie prób nielegalnego dostępu do określonych zasobów.

Przywykliśmy już do tego, że ścianę ogniową realizuje się najczęściej programowo, za pomocą specjalnej aplikacji lub wykorzystując możliwości systemu operacyjnego. Na rynku istnieją jednak alternatywne rozwiązania sprzętowe, których jedynym celem jest obrona sieci lokalnej przed niepowołanym dostępem z zewnątrz. Urządzenia tego typu przeznaczone są w zasadzie do ochrony średnich i dużych sieci, choć w ofercie większości producentów osprzętu sieciowego znajdują się też tańsze, mniej zaawansowane rozwiązania dla małych grup.



Jeden z NAJTAŃSZYCH FIREWALLI D-link DI-701 kosztuje zaledwie 730 złotych.

Co może zapora?

Mimo że sposoby ochrony danych są coraz doskonalsze, nadal możemy być pewni jednego – nie ma zabezpieczenia, którego nie można by pokonać. Pod tym względem zapora ogniowa nie jest żadnym wyjątkiem.

Powinniśmy jednak zdać sobie sprawę, że zazwyczaj najsłabszym ogniwem systemu zabezpieczeń nie jest ani maszyna, ani oprogramowanie, lecz... człowiek. Dlatego dzięki centralizacji mechanizmów ochrony oraz ich uniezależnieniu od beztroskich działań poszczególnych użytkowników dobrze skonfigurowany firewall istotnie podnosi bezpieczeństwo sieci lokalnej. Zapora ogniowa filtruje wszystkie przesyłane pakiety, przepuszczając tylko te, które nie naruszają zasad polityki bezpieczeństwa określonych przez administratora. To zadanie podstawowe. Ponadto firewall może realizować wiele dodatkowych funkcji – począwszy od translacji adresów, poprzez rejestrowanie i śledzenie wszelkich przepływających pakietów, na zdalnym zarządzaniu, buforowaniu czy szyfrowaniu danych skończywszy.

Chroń siebie...

Bardziej zaawansowane urządzenia zapewniają ochronę przed tzw. atakami Denial of Service (DoS), których celem jest unieruchomienie wybranej usługi sieciowej. Z pewnością w niejednej firmie zablokowanie serwera WWW lub poczty elektronicznej mogłoby na wiele godzin sparaliżować jej pracę. Firewall powinien być odporny na takie ataki, jak Ping of Death (przesłanie pakietu przekraczającego maksymalną dozwoloną długość), SYN Flood („zalanie" komputera setkami żądań nawiązania połączenia), LAND Attack (przesłanie pakietu z takim samym adresem i portem nadawcy oraz odbiorcy), IP Spoofing (przesyłanie pakietów ze sfałszowanym adresem nadawcy) czy Teardrop (atak wykorzystujący błąd w systemach Windows 95/NT, powodujący zawieszenie się komputera).

Ile potrzeba urządzeń, by podłączyć do Internetu i zabezpieczyć małą sieć? Wystarczy NETQOM DSL 4100 będący jednocześnie modemem ISDN, firewallem i czteroportowym przełącznikiem.

Oprogramowanie zarządzające udostępnia niekiedy jeszcze bardziej rozbudowany system kontroli wykorzystania Internetu przez użytkowników sieci lokalnej. Na przykład w przypadku urządzeń serii OfficeConnect firmy 3Com, korzystając ze specjalnego internetowego katalogu klasyfikującego treści dostępne w ogólnoświatowej Sieci, można zablokować dostęp do stron WWW, serwerów FTP i grup dyskusyjnych, zawierających np. materiały pornograficzne lub propagujących przemoc. Firewall automatycznie łączy się z odpowiednim adresem i co pewien czas aktualizuje katalog. Usługa ta dostępna jest bezpłatnie przez pierwszy miesiąc od zarejestrowania urządzenia.

Zestawienie wybranych sprzętowych firewalli

● – jest; ❍ – nie ma; b.l. – bez limitu;
1) – liczba sesji zależna od wykupionego oprogramowania;
2) urządzenie jeszcze nie jest sprzedawane;
NAT – moduł translacji adresów, DHCP – serwer nazw adresów IP, VPN – prywatna sieć wirtualna, RAS – serwer zdalnego dostępu, IDS – system detekcji intruzów, DMZ – strefa zdemilitaryzowana, DOS – blokowanie serwisów;
ceny z dnia 4.02.2002 r.

Model	Porty	Maks. użytkown.	zarządzanie: WWW	Klient Windows	Port RS-232C	Telnet	SNMP i inne	NAT	Serwer DHCP	Serwer DNS	DMZ	VPN	Detekcja DoS	IDS	RAS	DNS Proxy	Data Proxy	Router	Przełącznik	Detekcja wirusów	Cena
Nokia IP 51	10/100 Mbit/s LANx4, WAN, 1xRS-232C	50	●	●	●	●	●	●	●	❍	❍	❍	●	●	❍	❍	❍	❍	●	❍	3420
3Com OfficeConnect IF DMZ	10 Mbit/s LAN, WAN	100	●	❍	❍	❍	❍	●	●	❍	❍	●	●	●	❍	❍	❍	❍	❍	❍	7750
3Com OfficeConnect IF 25	10 Mbit/s LAN, WAN, DMZ	25	●	❍	❍	❍	❍	●	●	❍	●	●	●	●	❍	❍	❍	❍	❍	❍	3080
SonicWall TELE3	10/100 Mbit/s LAN, WAN, RS-232C	5	●	❍	●	●	●	●	●	❍	❍	●	●	❍	❍	❍	❍	❍	❍	●	2900
SonicWall SOHO3	10/100 Mbit/s LAN, WAN, RS-232C	10/50	●	❍	●	●	●	●	●	❍	❍	●	●	❍	❍	❍	❍	❍	❍	●	2900 [1]
SonicWall PRO 100	10/100 Mbit/s LAN, WAN, DMZ, RS-232C	b.l.	●	❍	●	●	●	●	●	❍	●	●	●	❍	❍	❍	❍	❍	❍	●	10500
Lucent SuperpPipe 155	10/100 Mpbs LAN, ISDNx2/T1 WAN, ISDN OUT, RS-232C	b.l.	●	●	●	●	●	●	●	❍	❍	●	❍	❍	●	❍	❍	❍	❍	❍	9300
D-link DI-701	10/100 Mbit/s LAN, 10 Mbit/s WAN, RS-232C	128	❍	●	●	●	❍	●	❍	❍	❍	●	❍	❍	❍	❍	❍	❍	❍	❍	760
D-link DI-804	10/100 Mbit/s LANx4, 10 Mbit/s WAN, RS-232C	253	●	❍	●	❍	❍	●	●	❍	●	●	❍	❍	❍	❍	❍	❍	●	❍	920
D-link DI-704	10/100 Mbit/s LANx4, 10 Mbit/s WAN, RS-232C	253	●	❍	●	❍	❍	●	●	❍	●	●	❍	❍	❍	❍	❍	❍	●	❍	1080
D-link DI-707	10/100 Mbit/s LANx7, 10 Mbit/s WAN, RS-232C	253	●	❍	●	❍	❍	●	●	❍	●	●	❍	❍	❍	❍	❍	❍	●	❍	1470
D-link DRE-I304	10/100 Mbit/s LANx4, 10 Mbit/s lub ISDN WAN, RS-232C	b.l.	●	●	❍	●	❍	●	●	●	●	❍	❍	❍	●	●	❍	●	●	❍	2770
D-link DFL-300	10/100 Mbit/s LAN, WAN i DMZ	b.l.	●	❍	❍	❍	❍	●	●	❍	●	●	●	●	❍	●	❍	❍	❍	❍	ok. 2850
Surecom EP-4501	10/100 Mbit/s LAN, 10 Mbit/s WAN, RS-232C	64	●	❍	●	●	❍	●	❍	❍	●	❍	❍	❍	❍	●	❍	❍	❍	❍	650
Surecom EP-4504	10/100 Mbit/s LANx4, 10 Mbit/s WAN, RS-232C	64	●	❍	●	●	❍	●	❍	❍	●	❍	❍	❍	❍	●	❍	❍	●	❍	850
Surecom EP-4508	10/100 Mbit/s LANx8, 10 Mbit/s WAN, RS-232C	64	●	❍	●	●	❍	●	❍	❍	●	❍	❍	❍	❍	●	❍	❍	●	❍	1000
Surecom EP-4705VX-V	10/100 Mbit/s LANx5 i WAN, RS-232C	b.l.	●	❍	●	●	❍	●	❍	❍	❍	●	❍	❍	❍	●	❍	❍	●	❍	b.d. [2]
Surecom EP-3501 (do SDI)	2xRS232C (WAN+zarz.), 10/100 Mbit/s LAN	b.l.	●	❍	●	●	❍	●	❍	❍	❍	❍	❍	❍	❍	●	❍	❍	●	❍	480

Ponadto można stworzyć listę słów kluczowych, których wystąpienie w adresie strony WWW uniemożliwi jej pobieranie.

...i serwery swoje

Jak wspomniałem, firewalle mogą oferować wiele dodatkowych usług, które pomagają zabezpieczyć sieć bądź przyśpieszyć w niej pracę. Część urządzeń wyposażona jest nie w jedno, ale kilka (co najmniej dwa) gniazd sieciowych. Do jednego z nich dołączamy komputery z sieci lokalnej, drugie natomiast służy do podpięcia serwerów, co pozwala na odseparowanie od siebie tych dwóch części komputerowej infrastruktury. Umieszczone osobno serwery znajdują się w tak zwanej strefie zdemilitaryzowanej (DMZ – de-militarized zone), zwanej też siecią graniczną o ograniczonym bezpieczeństwie. Dzięki temu, mimo włamania się do widocznego na zewnątrz serwera, dane w sieci lokalnej są wciąż chronione.

Wśród ciekawych opcji na szczególne wyróżnienie zasługują Proxy Cache Services. Usługa ta umożliwia zoptymalizowanie ruchu na łączu WAN poprzez przechowywanie informacji (stron WWW), do których często odwołują się użytkownicy sieci. Niestety, rozwiązanie to dostępne jest jedynie w droższych urządzeniach, tańsze zapewniają np. buforowanie zapytań kierowanych do serwerów nazw domenowych (DNS – Domain Name Servers).

Jeśli zależy nam na wysokim poziomie zabezpieczeń, postawmy na rozwiązania profesjonalne, np. Nokię IP51.

Sieć z firewalli

Wiele firm, które potrzebują ciągłej wymiany informacji, staje przed dużym problemem – jak połączyć sieci lokalne kilku oddziałów oddalonych od siebie o setki, a nawet tysiące kilometrów. Wykupienie łącza dzierżawionego jest bardzo drogie, a czasem wręcz niemożliwe. Jedynym wyjściem staje się podłączenie wszystkich filii do sieci globalnej, takiej jak Internet. Virtual Private Network to usługa pozwalająca łączyć kilka sieci prywatnych „tunelami", przez które przenoszone są tylko informacje zaszyfrowane. Szyfrowanie całych pakietów znacznie zwiększa bezpieczeństwo połączenia, ponieważ ukrywa numery połączeń i przesyłane dane.

Urządzenia z VPN umożliwiają sieciom pracującym z innymi protokołami bądź z adresami IP, które nie są unikatowe, korzystanie z sieci globalnej. Dają możliwość całemu systemowi na używanie jednego adresu IP, który również może być przydzielany dynamicznie. Pozwala to firmie korzystającej np. z protokołu IPX na podłączenie do Internetu za pomocą modemu u dostawcy dynamicznie przydzielającego adresy. Dodatkową zaletą zwiększającą bezpieczeństwo jest ukrycie adresów lokalnych systemu.

Nie samym firewallem...

Przedstawiona charakterystyka urządzeń zabezpieczających to zaledwie czubek góry lodowej. Rynek obfituje w rozwiązania o mniejszym lub większym stopniu komplikacji. Urządzenia różnią się szczegółami – poziomem zabezpieczeń, liczbą obsługiwanych protokołów, sposobem zarządzania, możliwościami wymiany oprogramowania i rozbudowy.

Poza sprzętem oferującym jedynie podstawowe możliwości często dostępne są też urządzenia wielofunkcyjne. Przykładowo: duża liczba firewalli to jednocześnie kilku- lub kilkunastoportowe przełączniki, eliminujące w przypadku małych sieci konieczność stosowania koncentratorów bądź dodatkowych switchy. Część urządzeń pełni jednocześnie funkcję rutera szerokopasmowego bądź ISDN, a niektóre łączą w sobie wszystkie te funkcje... Przykładowe rozwiązania zebraliśmy w tabeli powyżej, przed decyzją o zakupie warto zawsze przejrzeć oferty kilkunastu producentów i przeszukać zasoby Internetu. ■

INFO

Producenci rozwiązań sprzętowych
http://www.dlink.com/
http://www.surecom.com.tw/
http://www.nokia.com/
http://www.lucent.com/
http://www.sonicwall.com/

Oprogramowanie do obsługi firewalli
http://www.checkpoint.pl/