

## Zagrożenia są wszędzie

Opisujemy najnowsze metody ataku na serwer WWW poprzez wstrzyknięcie kodu > 38

## Na ratunek drukarkom sieciowym

Jak szybko poradzić sobie z awariami maszyn i kłopotami z wydrukami > 40

# Co potrafi polski serwer

**SPRZĘT** | Głównym zamysłem twórców ethernet 2 było stworzenie produktu, który będzie łączył w sobie przyjazny interfejs z rozbudowanymi funkcjami sieciowymi Linuksa. Czy taki mariaż jest możliwy?

Krzysztof Kamiński

**A**nalizie poddaliśmy model ethernet 2 smb, rekomendowany dla grupy roboczej, która składa się z 25–50 komputerów. Jest on oparty na chipsecie Q965 i wyposażony w procesor Intel Xeon 3040 (1,86 GHz). Z powodu korzystania z funkcji wirtualizacyjnych podstawowa konfiguracja została rozszerzona z 2 GB do 4 GB pamięci RAM. Produkt wyróżnia się zgrabną obudową i kieszeniami na 3 dyski SATA. Sprzętu nie musimy instalować. Po rozpakowaniu jest gotowy do pracy. Panel konfiguracyjny został udostępniony przez producenta na predefiniowanym adresie IP i porcie. Przed uruchomieniem warto przeczytać instrukcję obsługi, która bardzo szczegółowo opisuje wszystkie funkcje serwera.

### Konfiguracja dysków

Dla danych użytkownika przeznaczone są trzy hotswappable kieszenie SATA obsługujące – wg producenta – dyski o pojemności do 1TB. W modelu nie znaleźliśmy kontrolera wspierającego sprzętowo funkcje RAID, stąd też obsługa macierzy odbywa się programowo. Dane możemy przechowywać w konfiguracji RAID 0, RAID 1 i RAID 5.

Pliki systemowe i konfiguracyjne znajdują się na dysku, który jest niedostępny z zewnątrz obudowy. Jego awaria może unieruchomić serwer, jednak producent zapewnia, że taka sytuacja jeszcze nie miała miejsca.



### Brama internetowa

Dużą zaletą systemu są 3 interfejsy sieciowe – wszystkie o prędkości 1 Gb/s. Dzięki temu możliwa jest obsługa dwóch niezależnych łączy WAN lub ustawienia jednego z nich jako łącza do strefy DMZ. Co więcej, w przypadku konfiguracji z dwoma łączami WAN ethernet 2 monitoruje ich dostępność – gdy jeden z nich ulega awarii, wtedy ruch sieciowy przełączany jest na sprawne łącze. Możliwe jest również przypisywanie typu ruchu do konkretnego interfejsu.

Kolejną interesującą opcją jest transparentne proxy sieciowe z autorskim filtrem zawartości. Nie ogranicza się ono do analizy adresów URL czy też

**Serwer ethernet 2**, zbudowany na podstawie chipsetu Q965 i procesora Intel Xeon 3040 (1,86GHz) stanowi zintegrowaną architekturę dla całej organizacji. Urządzenie łączy w sobie funkcje systemów linuksowych z prostym w obsłudze interfejsem.

tworzenia białych i czarnych list, które obecnie stają się coraz mniej skuteczne. Filtr za pomocą bazy słów dostarczanej przez producenta używa systemu analizy treści poszczególnych części strony. Dzięki temu możemy sprawdzić zawartość witryn dokładniej oraz w łatwy sposób dostosować serwer do potrzeb konkretnej instytucji. Ponadto możliwe jest stworzenie listy stron, które nie mają podlegać sprawdzeniu. Firma Embedos

domyślnie umożliwia blokowanie stron o tematyce pornograficznej, hackingu, rozrywkowej (czat, gry online, humor, wideo). Warto wspomnieć, że ethernus 2 udostępnia przejrzyste logi i wykresy przedstawiające sposób wykorzystania łącza przez użytkowników.

Funkcjonalnością, którą szczególnie docenią instytucje posiadające kilka oddziałów, jest VPN. Usługa ta udostępniania jest przy użyciu oprogramowania openVPN. Jest to aplikacja, której konfiguracja w pierwotnej wersji była skomplikowana. Na szczęście w przypadku ethernusa 2 wszystkie czynności związane z ustawieniami i generowaniem certyfikatów wykonywane są z poziomu interfejsu WWW.

Do wyboru mamy dwa tryby pracy: LAN-to-LAN oraz RoadWarrior. Pierwszy służy do łączenia sieci wewnętrznych, natomiast drugi przeznaczony jest dla użytkowników zewnętrznych. Tryby te różnią się generowanymi plikami konfiguracyjnymi w sekcji dotyczącej routingu i dostępu do sieci.

Serwer ethernus 2 obsługuje też podstawowe usługi sieciowe takie jak: DHCP, DNS forwarding, FTP oraz WWW. Co ważne, serwer stron internetowych umożliwia szyfrowanie danych (SSL) za pomocą certyfikatu, który był wygenerowany lokalnie lub został dostarczony przez firmę certyfikacyjną. Możliwe jest również uruchamianie aplikacji napisanych w języku PHP.

### Serwer plików i drukarek

Udostępnianie plików i drukarek odbywa się za pomocą pakietu samba. Dzięki niemu mamy możliwość nadawania praw do całych udziałów poszczególnym użytkownikom i grupom lub tworzyć udziały publiczne. Niestety brakuje opcji nadawania praw dostępu do katalogów i plików – z udostępniania wyłączone są katalogi robocze baz danych, poczty itp. Wszystkie zasoby sieciowe można udostępnić przez usługi WWW i ftp. Ethernus 2 ma również funkcję serwera wydruku dla urządzeń podłączanych przez interfejs USB i LPT.

### Poczta elektroniczna

Urządzenie może pełnić funkcję bezpiecznego serwera poczty elektronicznej. Mechanizmy takie jak greylisting, bia-

łe i czarne listy, rozbudowany filtr bayesowski czy możliwość użycia serwerów DNSBL chronią pracowników instytucji przed wszechobecnym spamem. Oczywiście każdą z tych opcji da się osobno skonfigurować i w razie potrzeby wyłączyć.

Zdalny dostęp do poczty możliwy jest przez klienta typu Webmail. Na poziomie użytkownika dostępne jest samodzielne definiowanie przekierowań, filtrów oraz autoodpowiedzi. Nie zapomniano również o przejrzystych logach, z których może korzystać administrator systemu.

### Bazy danych

Na serwerze ethernus 2 mamy dostęp do baz danych MySQL, PostgreSQL oraz Firebird. Niektóre z nich zainstalowane są od razu, inne trzeba pobrać ze strony producenta. Nie wynika to bynajmniej z ograniczonej ilości miejsca na dysku, ale z postanowień licencyjnych producentów odpowiedzialnych za silniki wspomnianych baz.

Konfiguracja serwerów baz danych ogranicza się do wskazania miejsca przechowywania plików i ustalenia hasła administratora. Odpowiednie wyjątki generowane są w zaporze sieciowej automatycznie. Należy jednak zwrócić uwagę, iż w przypadku gdy baza danych ma służyć jedynie aplikacji uruchomionej w urządzeniu ethernus 2 można – poprzez usunięcie wyjątku – zabronić do niej dostępu z zewnątrz.

### Wirtualizacja

Często zdarza się, że dany program – wykorzystywany w pracy przez wszystkich użytkowników – jest kompatybilny wyłącznie z systemami rodziny Windows. Jeśli takie oprogramowanie nie wymaga zbyt dużych zasobów, wtedy możemy pokusić się o konsolidację serwerów w jednej maszynie – ethernus 2. Dzięki temu nie ma konieczności utrzymywania osobnego serwera, który oprócz generowania kosztów związanych z energią elektryczną wymaga również prac konserwacyjnych i serwisu.

Konfiguracja usług wirtualizacyjnych – podobnie jak jest to w przypadku innych funkcji ethernusa 2 – dokonywana jest z poziomu przeglądarki WWW. Już po kilku kliknięciach możliwe jest podłączenie się do przygotowanej maszyny wirtualnej za pomocą udostępnionego oprogramowa-


nia firmy VMWare. Firma ta jest również producentem silnika, na którym oparto usługę. Dlatego też te osoby, które używały wcześniej produktów typu VMWare Server, nie będą miały problemów z instalacją wirtualnego systemu operacyjnego.

### Bezpieczeństwo danych

Prócz konfiguracji macierzy dyskowej nad bezpieczeństwem danych przechowywanych na serwerze czuwa rozbudowany system tworzenia i odzyskiwania kopii bezpieczeństwa. Do wyboru mamy kopie pełne, przyrostowe i różnicowe. Zadania archiwizacji mogą przebiegać zgodnie z harmonogramem bądź też można je uruchamiać na żądanie. W przypadku zasobów plikowych mamy możliwość wyłączenia pojedynczych katalogów i plików. Proces tworzenia kopii bezpieczeństwa dostępny jest również w przypadku baz danych i poczty elektronicznej. Oprócz kopii danych użytkowników warto zrobić także duplikat ustawień systemu, który w razie awarii będziemy w stanie łatwo przenieść na inną maszynę ethernus 2. Nośnikiem do archiwizacji może być zewnętrzna nagrywarka oraz np. dysk USB.

Ciekawą opcją – którą znajdziemy w menu *Grupy i użytkownicy* – jest *zgodność z GIODO*. Funkcja ta narzuca tworzenie nowych haseł co 30 dni oraz wymusza ich odpowiednią długość i historię.

Do funkcji zapewniających bezpieczeństwo danych należy również dołączyć możliwość współpracy z szeroką gamą urządzeń UPS. Dzięki niej w przypadku wyczerpywania się baterii system zostanie automatycznie wyłączony, zapobiegając tym samym potencjalnej utracie danych.

Tym, co odróżnia produkt firmy Embodos od konkurencji, są kompletne rozwiązania (sprzęt, system operacyjny, wsparcie), które w razie problemów serwisujemy u jednego producenta. Ponadto w ofercie znajdziemy szerokie pakiety wsparcia technicznego. Serwisy i aktualizacje mogą być dokonywane zarówno zdalnie (VPN), jak i podczas wizyt serwisanta w urządzeniu, w którym działa serwer. 

Autor jest analitykiem systemu w sektorze publicznym oraz specjalistą ds. IT w IPTI, specjalizuje się w bezpieczeństwie sieci teleinformatycznych i aplikacji.