Cyberoam CR25wiNG zintegrowana ochrona dla małych firm

Jeszcze do niedawna urządzenia i systemy kompleksowego zabezpieczenia sieci były na tyle kosztowne, że pozwolić sobie na nie mogły jedynie duże firmy. Jednak rozwój technologii sieciowych i rosnąca świadomość zagrożeń wynikających z przetwarzania i udostępniania danych w sieci spowodowały, że na rynku pojawiły się urządzenia UTM skierowane również dla małych firm. Przyjrzyjmy się jednemu z nich.

Jarosław Kowalski

Niedawno firma Cyberoam zaprezentowała gigabitowe urządzenia UTM (*Unified Threat Management*) należące do nowej linii NG (*Next Generation*). Pracują pod kontrolą firmowego systemu operacyjnego CyberoamOS i są dedykowane sieciom o różnych rozmiarach. W swoich UTM producent wprowadza też coś, co nazywa „technologią warstwy 8", czyli firmową realizację polityki bezpieczeństwa przy użyciu identyfikacji użytkownika (można określać spersonalizowane reguły aktywności sieciowej w kontekście każdego użytkownika).

Do redakcyjnych testów trafił jeden z modeli nowej serii oznaczony symbolem CR25wiNG. Jest to UTM przeznaczony dla segmentu SOHO (Small Office, Home Office), dodatkowo wyposażony w interfejs sieci bezprzewodowej. Urządzenie o raczej kompaktowych wymiarach (wys. 4,4 cm, gł. 15,3 cm, szer. 23,2 cm) doskonale nadaje się do instalacji w niewielkich serwerowniach, jednak ponieważ udostępnia ono sieć bezprzewodową, to – by z niej skorzystać – powinno znajdować się raczej w pomieszczeniu biurowym.

CR25wiNG oferuje zaawansowane możliwości ochrony i zarządzania ruchem sieciowym. Wbudowany sprzętowy firewall oferuje zaawansowaną inspekcję pakietów sieciowych, aplikacji oraz operacji wykonywanych przez użytkowników, opartą na bazie tożsamości. Cyberoam UTM Firewall jest przystosowany do ochrony sieci przed atakami DoS, DDoS i IP spoofing. Intrusion Prevention System chroni przed sieciowymi atakami na poziomie aplikacji, zapewniając organizacjom ochronę przed próbami włamań, malware, trojanami, a także wykorzystaniem złośliwego kodu i zagrożeniami hybrydowymi. Dodatkowo Cyberoam Anti-Virus i Anti-Spyware oferuje aktywną ochronę e-mail i komunikatorów przed złośliwym oprogramowaniem, w tym: wirusami, robakami, spyware, atakami backdoor, trojanami i keyloggerami.

Funkcjonalność Web Filtering oferuje jedną z najbardziej rozbudowanych baz adresów URL (liczonych w milionach) pogrupowanych w ponad 82 kategoriach. Filtrowanie stron skutecznie potrafi zablokować dostęp do szkodliwych witryn, chronić przed phishingiem oraz jego bardziej niebezpieczną formą pharmingiem.

Cyberoam CR25wiNG w ramach realizacji polityk bezpieczeństwa oferuje kontrolę ruchu aplikacji w warstwie 7. Funkcja jest w stanie obsłużyć i zabezpieczyć pracę sieciową opartą na aplikacjach biznesowych typu CRM i ERP, do tego potrafi również kontrolować przepływ danych w programach typu P2P oraz serwisach społecznościowych.

Cyberoam CR25wiNG posiada także rozbudowane funkcje High Availability (HA). Niezawodność połączenia internetowego ma gwarantować obsługa wielu łączy WAN, z możliwością optymalizacji ruchu i minimalizacji obciążenia łączy. Cyberoam UTM obsługuje bezprzewodowe technologie 3G, 4G/LTE i WiMAX WAN, co pozwala na automatyczne, awaryjne przełączanie z łączy przewodowych na bezprzewodowy WAN. Wykorzystanie wielu połączeń bezprzewodowych umożliwia także wdrożenie wysokiego poziomu bezpieczeństwa w zdalnych lokalizacjach, które nie mogą mieć połączeń przewodowych.

Dopełnieniem rozbudowanej funkcjonalności urządzenia jest również obsługa VPN SSL i IPSec, zarządzanie przepustowością

łącza, zaawansowane możliwości logowania i raportowania (z wykorzystaniem aplikacji iView) oraz obsługa protokołu IPv6.

INSTALACJA I KONFIGURACJA

Podłączenie do sieci i podstawowa konfiguracja urządzenia nie powinno sprawić większych problemów nawet mniej doświadczonym użytkownikom. Dołączona do zestawu krótka instrukcja wystarczy, aby szybko ustawić podstawowe funkcje i podłączyć sieć LAN do internetu. O ile jednak standardowa konfiguracja jest dostępna w cenie zakupu, to zaawansowane funkcjonalności – m.in. IPS, Antyspam, antywirus, Web and Application Filter czy Web Application Firewall – są dostępne jako dodatkowe subskrypcje.

Uruchomienie i instalację tradycyjnie rozpoczęliśmy od zapoznania się z dokumentacją techniczną, jednak otrzymany zestaw zawierał jedynie kilkustronicową instrukcję podłączenia i podstawowej konfiguracji urządzenia. Dodatkowe pliki opisujące zaawansowane opcje konfiguracyjne są dostępne do pobrania na stronie producenta. Po zarejestrowaniu urządzenia i utworzeniu konta na stronie Cyberoam.com użytkownik otrzymuje możliwość podglądu aktywnych subskrypcji, możliwych sposobów wsparcia technicznego, a także funkcji generowania ticketów serwisowych i podglądu ich statusów.

Tylny panel CR25wiING ma cztery gigabitowe porty Ethernet. Choć są one oznaczone jako WAN, LAN czy DMZ, to nie są skonfigurowane w odpowiadającej im roli i dlatego nie ma konieczności stosowania się do tych oznaczeń. Wykorzystanie portów zależy od tego, jak połączenia fizyczne zostaną zaplanowane lub jakie są wymogi konfiguracyjne. Dostępne są również dwa porty USB, które mogą posłużyć do podłączenia zewnętrznego modemu GSM, w celu zapewnienia redundancji dostępu do internetu oraz dodatkowy port konsolowy, do realizacji bezpośrednich połączeń przez RS232. Na tylnym panelu znajdują się również trzy gniazda antenowe sieci bezprzewodowej, realizowanej w tym urządzeniu w technologii 3x3 MIMO (trzy strumienie danych w obie strony).

CR25wiNG najwygodniej zarządzać przez panel webowy, choć oczywiście można oprzeć się na konsoli tekstowej dostępnej przez Telnet, SSH czy wspomniany wcześniej port konsolowy. Przy pierwszym uruchomieniu dostęp odbywa się poprzez zdefiniowany wcześniej przez producenta adres IP portu LAN. Połączenie WAN jest skonfigurowane do uzyskania adresu przez DHCP. Po zalogowaniu wyświetla się panel zarządzania podzielony w tradycyjny dla takich urządzeń sposób, czyli w układzie dwukolumnowym. Po lewej znajduje się funkcjonalnie podzielone menu, a po prawej

Poruszanie się po menu panelu zarządzania nie jest żadnym problemem. Opcje zebrane pod postacią funkcjonalnych przycisków są ułożone metodycznie w odpowiadających im tematycznych sekcjach.

Dashboard z najważniejszymi informacjami odnośnie do pracy systemu. Jego stałym elementem jest ramka zawierająca komunikaty systemowe. Inne elementy, tj. status systemu, zużycie zasobów, wykryte zagrożenia w różnych obszarach czy informacja na temat licencji są zawarte w ramkach, które można ustawiać w dowolnej kolejności lub po prostu wyłączać.

Podstawowej konfiguracji na potrzeby infrastruktury można dokonać na dwa sposoby, za pomocą wygodnego kreatora lub ręcznie. Kreator przeprowadza jedynie przez podstawowe opcje – najpierw należy określić tryb pracy (Gateway lub Bridge), później konfigurację interfejsów WAN i LAN, powiadomienia e-mailowe o zdarzeniach systemowych, a na końcu ustawienia daty i czasu. W przypadku ręcznej konfiguracji należy skorzystać z dwóch obszarów menu, *SYSTEM* i *NETWORK*, gdzie odpowiednie opcje pozwolą zdefiniować te same parametry.

Urządzenie o raczej kompaktowych wymiarach (wys. 4,4 cm, gł. 15,3 cm, szer. 23,2 cm) doskonale nadaje się do instalacji w niewielkich serwerowniach, jednak ponieważ udostępnia ono sieć bezprzewodową, to – by z niej skorzystać – raczej powinno znajdować się w pomieszczeniu biurowym.

Poruszanie się po menu nie jest żadnym problemem. Opcje zebrane pod postacią funkcjonalnych przycisków początkowo mogą wydawać się trudne do opanowania, jednak są ułożone metodycznie w odpowiadających im tematycznych sekcjach.

W sekcji ***SYSTEM*** dostępne są wszystkie (oprócz sieciowych) ustawienia administracyjne urządzenia. Wśród ustawień dostępu do zarządzania, można określić zasady logowania przez SSL VPN oraz zarządzać certyfikatami na urządzeniu. Przy czym można skorzystać z zewnętrznego certyfikatu lub wygenerować go we własnym zakresie.

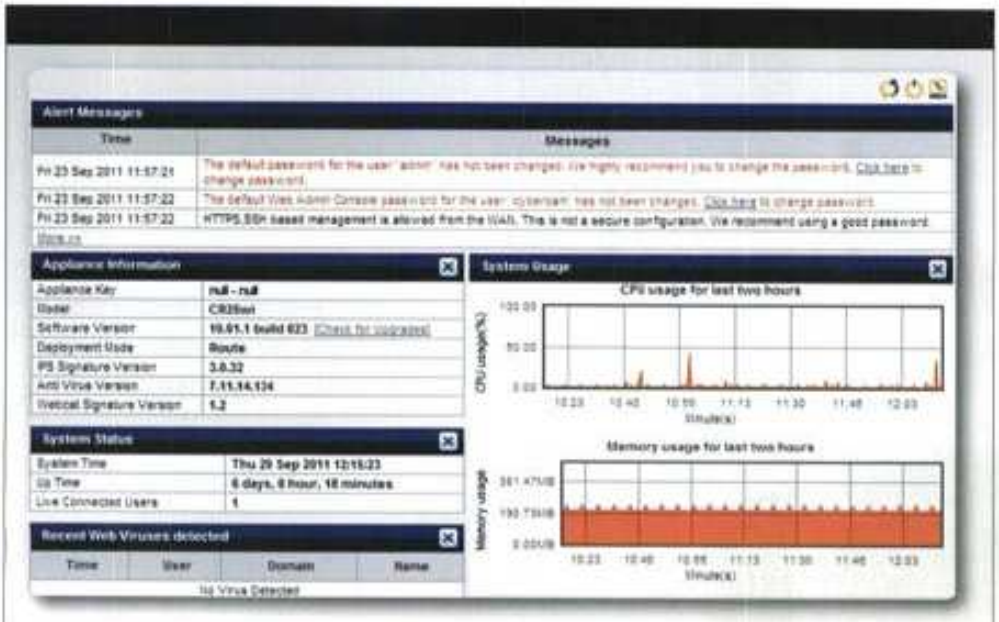
OBJECTS pozwala zdefiniować elementy systemu, które później są wykorzystane przy definiowaniu reguł zabezpieczeń i dostępu. Obiektami mogą być hosty określone po adresie MAC lub IP, całe sieci, zakresy IP, a także serwisy w kombinacji wykorzystywanych portów i protokołów, certyfikaty oraz różne rodzaje plików.

Opcje pod przyciskiem ***NETWORK*** pozwalają określić wszystkie niezbędne do pracy ustawienia sieciowe. Oprócz osobnej konfiguracji każdego z portów można dodatkowo zdefiniować strefy (*zones*) logiczne w obszarach LAN i DMZ do określania polityk dostępu. Część stref jest zdefiniowana na stałe i przypisana do wybranych portów Ethernet. W tej sekcji można dokonać również konfiguracji sieci bezprzewodowej. Obsługuje ona podstawowe metody zabezpieczeń (WEP, WPA, WPA2, 802.11i, TKIP, AES, PSK, 802.1x EAP). W ustawieniach sieci bezprzewodowej na uwagę zasługuje fakt, że można ją skonfigurować w zupełnie innej adresacji niż fizyczny interfejs LAN i dzięki temu przy użyciu jednego urządzenia posiadać dwie odrębne sieci wewnętrzne.

Opcją, która standardowo nie jest widoczna w panelu WEB jest WIRELESS WAN, czyli dostęp do sieci internet przez podłączony do portu USB modem GSM. Aby była ona widoczna należy z poziomu konsoli tekstowej, aktywować ją odpowiednim poleceniem. Dbając o wysoką dostępność połączenia internetowego warto skorzystać z tej możliwości i ustawić bezprzewodowe połączenie WAN jako backupowy dostęp do internetu.

Podstawowe polityki bezpieczeństwa opierają się głownie na identyfikacji przez adres IP. Sekcja ***IDENTITY*** pomaga zarządzać polisami, dostępem i ruchem sieciowym poprzez identyfikację użytkownika. Bazę użytkowników można zbudować opierając się na serwerze autoryzacyjnym (Radius lub Active Directory) lub na wewnętrznej bazie użytkowników. Integracja z serwerem Active Directory jest stosunkowo prosta i nie powinna sprawić większych problemów. Natomiast obsługa użytkowników zdefiniowanych w wewnętrznej bazie opiera się na konieczności logowania do urządzenia Cyberoam. Realizowane jest to za pomocą aplikacji klienckiej instalowanej na komputerach. Producent udostępnił aplikację do współpracy z CR25wiNG, przeznaczoną na platformy mobilne z systemem Android, umożliwiającą przede wszystkim połączenie urządzeń mobilnych z internetem, ale także dającą dostęp do kwarantanny oraz statystyk użytkownika. Jest to szczególnie przydatne, gdy chcemy wymusić realizację polityk dostępowych dla wszystkich użytkowników internetu w naszej sieci. Dzięki identyfikacji użytkowników można śledzić ich aktywność w ruchu sieciowym oraz określać spersonalizowane polityki dostępu.

Producent udostępnił aplikację do współpracy z CR25wiNG, przeznaczoną na platformy mobilne z systemem Android, umożliwiającą przede wszystkim połączenie urządzeń mobilnych z internetem, ale także dającą dostęp do kwarantanny oraz statystyk użytkownika.



Dashboard – jego stałym elementem jest ramka zawierająca komunikaty systemowe. Inne elementy, tj. status systemu, zużycie zasobów, wykryte zagrożenia w różnych obszarach czy informacja na temat licencji są zawarte w ramkach, które można ustawiać w dowolnej kolejności lub po prostu wyłączać.

FIREWALL udostępnia opcje pozwalające określić zaawansowane reguły dostępu do sieci oparte na adresach źródłowych i docelowych lub wykorzystywane serwisy. Można przy tym określić filtry webowe oraz aplikacyjne, a także skanowanie antywirusowe i spamu dla wielu protokołów sieciowych.

WEB FILTER oraz *APPLICATION FILTER* pozwalają zarządzać pracą aplikacji w sieci oraz dostępem do stron internetowych. Można skorzystać z bazy kilkudziesięciu prekonfigurowanych opcji, opierając się na konkretnych domenach i słowach kluczowych służących do filtrowania oraz gotowych definicji aplikacji. Administratorzy mogą wykorzystać te kategorie do zdefiniowania elastycznych reguł dostępowych przypisanych nie tylko konkretnym hostom, ale także pojedynczym użytkownikom.

IM (*Instant Messaging*) pozwala na konfigurację i zarządzanie ograniczeniami dla komunikatorów Yahoo oraz MSN. Ruch przychodzący z sieci w postaci plików oraz sam czat jest objęty różnymi zasadami i strategiami filtrowania treści. Konfigurując reguły, można dodać kontakt czatu lub grupy kontaktów, wykorzystując je do konfigurowania zasad. Szkoda, że ta funkcjonalność standardowo nie obsługuje najbardziej popularnych komunikatorów wykorzystywanych w polskich firmach.

Dopełnieniem w zakresie bezpieczeństwa jest skanowanie ruchu sieciowego w zakresie ochrony antywirusowej oraz antyspamowej, konfigurowanej w sekcjach *ANTIVIRUS* i *ANTISPAM*. W ustalaniu parametrów ochrony antywirusowej należy określić odpowiednie opcje dla protokołów mail, http oraz FTP, reguły skanowania antywirusowego oraz pożądane wyjątki. Konfiguracja ochrony antyspamowej opiera się między innymi na ustawieniu filtrowaniu nagłówków, rozmiarze wiadomości, adresie nadawcy. Wykorzystuje także aktualne listy RBL oraz czarne i białe listy adresów IP. Wsparciem dla realizacji polityki bezpieczeństwa jest z pewnością także automatyczna aktualizacja sygnatur wirusów. W ochronie antywirusowej i antyspamowej wykryte zagrożenia mogą zostać przekazane do kwarantanny, do której dostęp realizowany jest na bieżąco.

Inne funkcje urządzenia Cyberoam CR25wiNG, które pomagają w zarządzaniu infrastrukturą IT, to *TRAFFIC DISCOVERY*, która na bieżąco monitoruje połączenia sieciowe. Przeglądając je można skorzystać z filtrowania po aplikacji, użytkowniku oraz adresie IP.

Kolejna sekcja dotyczy logowania i raportowania (LOGS & REPORTS), gdzie administrator ma możliwość skonfigurowania logowania praktycznie każdego aspektu działania CR25wiNG, wybierając spośród kilkudziesięciu opcji. Do tego dochodzą zaawansowane opcje raportowania przy wykorzystaniu zintegrowanej aplikacji webowej iView, gdzie jest możliwość podglądu zaawansowanych informacji dotyczących wykorzystywania każdej funkcjonalności oraz statystyk generowanych podczas monitorowania i skanowania ruchu sieciowego.

Cena Cyberoam CR25wiNG w podstawowej funkcjonalności wynosi 780 USD, do tego dochodzi koszt subskrypcji kompletu modułów zabezpieczających z rocznym wsparciem i gwarancją w cenie 319 USD. Koszt zakupu nie należy do najniższych, ale funkcjonalność, prostota obsługi i przejrzysty, intuicyjny model zarządzania sprawiają, że urządzenie jest warte swojej ceny.

PODSUMOWANIE

Liczba dostępnych opcji Cyberoam CR25wiNG sprawia, że jest to urządzenie godne uwagi wszędzie tam, gdzie bezpieczeństwo infrastruktury i danych stawiane jest na pierwszym miejscu. Choć przeznaczeniem tego modelu są małe biura, to z pewnością sprawdzi się także w średniej wielkości firmach, nawet w tych, które posiadają odległe lokalizacje, gdyż producent przewidując taką konfigurację umożliwił centralne zarządzanie wieloma urządzeniami tego typu poprzez aplikację w chmurze (Cyberoam on-Cloud Management Service – CCMS.)

Dla zainteresowanych producent umieścił na swoich stronach internetowych demo aplikacji, gdzie można przejrzeć dostępne opcje konfiguracyjne i ewentualnie zadecydować, czy taka funkcjonalność jest satysfakcjonująca.

Szczegółowy raport użycia stron internetowych.