

Check Point SecurePlatform

Platforma zabezpieczeń Firewall do zastosowań w systemach o podwyższonych wymaganiach bezpieczeństwa

Technologie informatyczne są niezbędne do prawidłowego funkcjonowania większości firm i instytucji. Często zależy od nich realizacja zadań biznesowych. Dla banków i sklepów internetowych oraz wielu innych firm zakłócenia w pracy systemu informatycznego bezpośrednio oznaczają utratę dochodów. Utrzymanie bezpieczeństwa systemu i dostępności jego zasobów stały się koniecznością. Wraz z rozwojem systemów informatycznych ich ochrona jest coraz trudniejsza. Systemy funkcjonują, bowiem w rozbudowanych i nietrywialnych do kontrolowania środowiskach sieciowych jak Internet, intranet i ekstranet. Środki ochrony zawarte w systemach operacyjnych, bazach danych i aplikacjach nie są już wystarczające. Kluczowe zadania bezpieczeństwa pełnią dedykowane zabezpieczenia sieciowe.

Najczęściej stosowane obecnie w korporacjach zabezpieczenia sieciowe oparte są na produktach izraelskiej firmy Check Point Software Technologies (wg analizy rynku Gartner Inc.). Flagowym produktem Check Point jest system zaporowy VPN-1/FireWall-1. Zabezpieczenia VPN-1/FireWall-1 dostarczane są w specjalizowanych urządzeniach jak Crossbeam X40S i Nortel ASF, bądź instalowane na sprzęcie i systemach operacyjnych ogólnego przeznaczenia (m.in. Linux, SUN Solaris, czy Windows NT/2000). Dostępne są także liczne rozwiązania określane nazwą Firewall Appliance lub Security Appliance, gdzie oprogramowanie Check Point zainstalowane jest przez dostawcę urządzeń także na zwykłym sprzęcie klasy PC i systemach operacyjnych ogólnego przeznaczenia (najczęściej Linux i FreeBSD).

Z punktu widzenia bezpieczeństwa chronionych zasobów informatycznych przedsiębiorstwa oraz samego systemu zabezpieczeń platforma Firewall i oprogramowanie VPN-1/FireWall-1 stanowią jedną całość. Na nic się nie zda zaawansowana technologia inspekcji ruchu sieciowego, jeżeli intruz np. poprzez Telnet, czy HTTP uzyska dostęp do platformy Firewall i wyłączy moduły zabezpieczeń. Największe zagrożenie w tym zakresie stwarzają słabo przygotowane rozwiązania Firewall Appliance. Instalując oprogramowanie Check Point na Windows NT/2000, SUN Solaris, czy Linux większość ludzi zdaje sobie sprawę z konieczności wcześniejszego przygotowania systemu operacyjnego (m.in. usunięcia zbędnych protokołów i usług). Szczegółowe instrukcje do tego dostarczane są przez Check Point i jej partnerów, m.in.: <http://www.checkpoint.pl/html/cps.html>

Wdrażając zabezpieczenia Check Point na sprzęcie typu Firewall Appliance często pochopnie zakłada się, że platforma Firewall została odpowiednio przygotowana przez jej dostawcę. W praktyce jednak często producenci Firewall Appliance w pierwszej kolejności koncentrują się na stworzeniu odpowiedniej obudowy dla swoich urządzeń oraz ukrywaniu prawdziwej nazwy zastosowanego systemu operacyjnego i rodzaju procesora, aby sprawić wrażenie dostarczania urządzeń dedykowanych i mieć wytłumaczenie ich „kosmicznej” ceny. W wielu rozwiązaniach Firewall Appliance obserwuje się także świadome rozbudowywanie i komplikowanie narzędzi administracyjnych (np. narzędzi zarządzania przez przeglądarkę WWW). Stwarza to niebezpieczeństwo popełnienia błędów przez administratorów, jeżeli nie odbyli oni z tego odpowiednich szkoleń, a firma nie wykupiła u dostawcy sprzętu usług pomocy technicznej.



Każde wdrożenie systemu zabezpieczeń Check Point VPN-1/FireWall-1, niezależnie od tego czy odbywa na platformie systemu operacyjnego ogólnego przeznaczenia czy urządzenia o nazwie Firewall Appliance, powinno zawierać kompletną analizę bezpieczeństwa. Analiza obejmuje ochronę zasobów systemu informatycznego oraz samego systemu zabezpieczeń, który także może stać się obiektem ataku.

Do podstawowych wymagań w tym zakresie stawianych platformie Firewall należą:

- **bezpieczeństwo** – odporność na próby penetracji i nieupoważnionego dostępu oraz ataki destrukcyjne i destabilizujące DoS (m.in. hardening systemu operacyjnego, usunięcie niebezpiecznych narzędzi zdalnego dostępu jak Telnet, FTP, HTTP),
- **wydajność (szybkość)** – zabezpieczenia nie obniżają upoważnionym użytkownikom dostępności i jakości usług systemu informatycznego,
- **niezawodność** – odporność na awarie sprzętowe i zakłócenia pracy zabezpieczeń,
- **skalowalność** – możliwość sprawnej rozbudowy i aktualizacji sprzętu (m.in. wymiana procesora na szybszy, zwiększenie pamięci RAM, dodanie kart sieciowych),
- **elastyczność** – możliwość tworzenia architektury zabezpieczeń sieci dostosowanej do potrzeb (np. tworzenie odpowiednich stref bezpieczeństwa, rozszerzenie funkcjonalności zabezpieczeń),
- **zarządzanie i monitorowanie** – łatwe w użyciu i kompletne narzędzia do konfiguracji i monitorowania stanu systemu operacyjnego (m.in. obciążenie procesora i pamięci, zajętość systemu plików, stan modułów zabezpieczeń),
- **przystępna cena** – koszt sprzętu Firewall nie powinien pochłaniać funduszy, które można przeznaczyć na wzbogacenie funkcjonalności zabezpieczeń (np. zakup dedykowanych narzędzi do analizy i raportowania zdarzeń) oraz podniesienie kwalifikacji administratorów (np. szkolenia na stopnie specjalizacji Check Point Certified Security Administrator i Check Point Certified Security Expert).

Check Point z myślą o wdrożeniach technologii VPN-1/FireWall-1 w systemach o podwyższonych wymaganiach bezpieczeństwa (m.in. systemy bankowe, finansowe, wojskowe, rządowe) opracował i bezpłatnie dostarcza własną dystrybucję systemu operacyjnego. System ten nosi nazwę **SecurePlatform**. Umożliwia on spełnienie wyżej wymienionych wymagań - i co istotne - bez ponoszenia dużych nakładów pracy i kosztów na zakup sprzętu.



SecurePlatform to system operacyjny opracowany i dostarczany przez Check Point w ramach dystrybucji swoich produktów zabezpieczeń. SecurePlatform w rzeczywistości nie jest nową, niesprawdzoną technologią. Został opracowany na bazie istniejącego od wielu lat i najbardziej wydajnego w zakresie operacji sieciowych systemu operacyjnego Linux (jądro Red Hat). W zakresie bezpieczeństwa i wydajności platformy Firewall został dostrojony z najdrobniejszymi szczegółami. Instalacja SecurePlatform odbywa się ze specjalnie przygotowanego nośnika CD-ROM. Program instalacyjny zawsze rozpoczyna od sformatowania dysku. Następnie instalowany jest specjalnie dostrojony system operacyjny i wybrane moduły zabezpieczeń Check Point. Instalacja SecurePlatform może odbywać się także poprzez port szeregowy bez konieczności podłączania konsoli do maszyny Firewall.

Projektując SecurePlatform przyjęto słuszne założenie, że system operacyjny maszyny Firewall jest potrzebny jedynie do obsługi sprzętu. Całościowa funkcjonalność zabezpieczeń zawarta jest w oprogramowaniu Check Point. Razem z nim dostarczany jest komplet dedykowanych narzędzi do zarządzania i monitorowania zabezpieczeń, monitorowania systemu operacyjnego oraz scentralizowanego instalowania nowych wersji oprogramowania Check Point i zarządzania licencjami.

W systemach informatycznych obowiązują dwa podstawowe modele bezpieczeństwa – „allow all” i „deny all” (RFC 2196, Site Security Handbook). Model „allow all” zakłada dostępność wszystkich usług i selektywne blokowanie, tych które stwarzają zagrożenie. Model „deny all” zakłada usunięcie wszystkich usług i selektywne dodawanie tylko tych, które są potrzebne. Projektując SecurePlatform przyjęto wprowadzający mniejsze ryzyko dla bezpieczeństwa Firewall model „deny all”. Domyślna instalacja SecurePlatform zawiera pakiety ograniczone do niezbędnego minimum.

Tworząc SecurePlatform zwrócono uwagę na najbardziej istotne zagrożenia platformy Firewall:

- **Błędy ludzi:** System SecurePlatform nie posiada konta „root”, na które domyślnie loguje się większość administratorów i które daje im nieograniczone możliwości w systemie. W SecurePlatform administrator loguje się na konto „admin”. Konto „admin” nie jest tylko pozorną zmianą nazwy konta „root”, jak to ma miejsce w jednym z popularnych Firewall Appliance. Uprawnienia „admin” umożliwiają jedynie korzystanie z narzędzi diagnostycznych, wykonywanie kopii Backup i odtwarzanie konfiguracji systemu i zabezpieczeń za pomocą specjalnie przygotowanych narzędzi oraz konfigurowanie podstawowych parametrów urządzenia (m.in. adresy IP, ruting) oraz modułów Check Point (m.in. dodanie licencji) z użyciem specjalnie przygotowanej aplikacji „sysconfig”. Dostęp do poleceń systemu operacyjnego możliwy jest dopiero po dodatkowym uwierzytelnieniu administratora i przejściu do trybu „expert”.
- **Nieupoważniony dostęp:** W domyślnej instalacji SecurePlatform nie ma żadnych usług zdalnego dostępu, które potencjalnie stanowią zagrożenie jak Telnet, FTP, czy HTTP. Dostęp do urządzenia z sieci możliwy jest tylko poprzez szyfrowane połączenia SSH. Wynika to z faktu, że po zainstalowaniu i skonfigurowaniu Firewall zmiany w systemie operacyjnym wykonywane są bardzo rzadko, a niekiedy w ogóle się ich nie robi. Tylko zabezpieczenia Check Point są poprzez sieć zarządzane za pomocą konsoli SmartCenter. Komunikacja ta jest jednak zabezpieczona kryptograficznie (szyfrowanie sesji, uwierzytelnianie za pomocą certyfikatów X.509). Dostarczana przez Check Point konsola SmartCenter oprócz zarządzania zabezpieczeń ma także możliwości bardzo szczegółowego monitorowania systemu operacyjnego maszyny Firewall (m.in. obciążenie procesora, zajętość pamięci operacyjnej, wolne miejsce na dysku, stan procesów). Usunięcie usług zdalnego dostępu z SecurePlatform całkowicie eliminuje zagrożenie, że intruz podsłucha hasło dostępu do urządzenia przesyłane np. przez Telnet czy HTTP.
- **Podatność usług:** Platforma Firewall, zawierająca zainstalowane serwery WWW, Telnet, FTP czy też serwisy obsługujące protokoły dynamicznego rutingu, jest narażona na błędy bezpieczeństwa i podatności tych usług. Skoro takie serwisy istnieją na maszynie Firewall to poważnym zagrożeniem jest, że intruz wykorzysta je do przejścia kontroli nad Firewall (np. administrator nie zablokuje do nich dostępu w konfiguracji Check Point FireWall-1, bądź tymczasowo zostanie wyłączony moduł lub polityka FireWall-1). SecurePlatform nie posiada serwisów umożliwiających zaatakowanie maszyny Firewall, nawet przy wyłączonych zabezpieczeniach Check Point FireWall-1. Cała gama niebezpiecznych serwisów jest dostępna w wielu rozwiązaniach Firewall Appliance, gdzie np. na maszynie

Firewall jest zainstalowany serwer WWW, żeby można było konfigurować adresacje IP i ruting przez przeglądarkę WWW. W razie potrzeby na SecurePlatform dodatkowe serwisy mogą być dopiero świadomie do-instalowane przez administratora posiadającego w systemie uprawnienia „expert”.



SecurePlatform został oparty na bazie najbardziej wydajnego pod względem obsługi sieci jądra systemu operacyjnego Linux. System został dodatkowo dostrojony przez producenta zabezpieczeń w zakresie wydajności Firewall i VPN. Dzięki temu zainstalowany na standardowym sprzęcie o architekturze Intel osiąga wydajność ponad 3.0 Gb/s. Ze wszystkich dostępnych dla Check Point rozwiązań sprzętowych wydajność tego rzędu mogą osiągnąć tylko specjalizowane urządzenia dwóch firm: Crossbeam i Nortel. Kompletne informacje na ten temat znajdują się na stronie producenta:

http://www.checkpoint.com/products/choice/platforms/platforms_matrix.html

Wydajność systemu zabezpieczeń VPN-1/FireWall-1 na SecurePlatform może zostać dodatkowo podniesiona przez moduł Check Point Performance Pack oraz sprzętowe karty szyfrujące (DES, 3DES). Z użyciem modułu Check Point ClusterXL możliwe jest także budowanie klastrów Firewall, gdzie ruch sieciowy równoważony jest pomiędzy wiele maszyn pracujących w klastrze. Wysoka wydajność zabezpieczeń Check Point VPN-1/FireWall-1 NG funkcjonujących na SecurePlatform została potwierdzona przez niezależną instytucję Tolly Group (sierpień, 2002). Wyniki testów dostępne są na stronie:

<http://www.checkpoint.com/products/connect/tollyreport.html>

Istotne jest także, że koszt sprzętu użytego przez Tolly Group do instalacji SecurePlatform był mniejszy niż 5.000 USD. Poprzednie testy wydajności zabezpieczeń Check Point wykonane przez Tolly Group (marzec, 2002) na sprzęcie typu Firewall Appliance, którego koszt wynosi prawie 50.000 USD były wręcz kompromitujące. Pomimo oficjalnych informacji od producenta Firewall Appliance o wydajności swojego rozwiązania 2.0 Gb/s w rzeczywistych testach Tolly Group nie przekroczył 180 Mb/s (testy dla pakietów 64-bajty), a przy większej liczbie sesji wydajność spadła poniżej 120 Mb/s. Należy także wspomnieć, że producent tego Firewall Appliance zaimplementował własny odpowiednik Check Point Performance Pack, w którym podwyższenie wydajności osiągnięto kosztem obniżenia bezpieczeństwa FireWall-1 (m.in. wyłączono mechanizm TCP Sequence Validator).



Zapewnienie stałej dostępności usług systemu informatycznego jest ważnym kryterium bezpieczeństwa, mającym w wielu instytucjach duże znacznie, często bardziej istotne od pozostałych kryteriów: poufności, autentyczności, integralności, rozliczalności, czy niezaprzeczalności działania. W takich systemach konieczne jest, aby zabezpieczenia sieciowe posiadały środki chroniące je przed awariami sprzętowymi i programowymi. Konfiguracje systemów zabezpieczeń sieci zawierających mechanizmy ochrony przed awariami określane są terminem High Availability (HA). Z uwagi na specyfikę swojego funkcjonowania typowy problem ochrony zabezpieczeń sieci przed awariami dotyczy systemów Firewall (awaria Firewall powoduje zwykle zablokowanie dostępu do wszystkich elementów sieci chronionej).

W konfiguracji HA system Firewall składa się z dwóch lub więcej maszyn inspekcyjnych, które kontrolują się wzajemnie i w razie wystąpienia awarii przejmują zadania uszkodzonej maszyny bez utraty otwartych połączeń sieciowych. Wchodzące w skład HA maszyny Firewall są odpowiednio ze sobą zsynchronizowane oraz w większości konfiguracji posiadają także mechanizmy wykrywania awarii i automatycznego przejmowania zadań uszkodzonej maszyny. Synchronizacja polega na współdzieleniu przez maszyny Firewall tablic stanu połączeń tak, aby każdy Firewall wiedział, jakie połączenia sieciowe przechodzą przez pozostałe maszyny i jaki jest ich stan.

O jakości systemu ochrony zabezpieczeń Firewall i VPN przed awariami sprzętowymi i programowymi decydują następujące własności:

- **Utrzymanie sesji w czasie awarii:** Moduł VPN-1/FireWall-1 bez konieczności instalacji dodatkowego oprogramowania posiada wbudowane mechanizmy synchronizacji wewnętrznych tabel stanu. Dzięki temu każda maszyna Firewall w klastrze otrzymuje na bieżąco informacje, jakie sesje przechodzą przez pozostałe maszyny i w razie awarii połączenia sieciowe mogą zostać utrzymane na innej sprawnej maszynie. Dla większości protokołów i usług awaria Firewall w ogóle nie zostanie zauważona przez użytkowników.
- **Wykrywanie awarii i przełączanie klastra:** Skuteczny system ochrony zabezpieczeń Firewall przed awariami realizuje testy sprzętu i stanu systemu operacyjnego oraz co w praktyce okazuje się najbardziej istotne wykonuje kompletne monitorowanie zabezpieczeń (m.in. kontroluje, czy moduł VPN-1/FireWall-1 funkcjonuje poprawnie, czy z jakiegoś powodu zabezpieczenia nie zostały wyłączone, czy nie uległy zablokowaniu procesy Security Servers, czy jest zainstalowana polityka bezpieczeństwa Firewall, itp.). Spełnienie tych wymagań jest możliwe po zastosowaniu dedykowanego modułu HA, dostarczanego przez Check Point (ClusterXL) lub partnerów OPSEC.

SecurePlatform z wykorzystaniem modułu Check Point ClusterXL umożliwia tworzenie klastrów Firewall spełniających powyższe wymagania skutecznej ochrony przed awariami sprzętowymi i programowymi. Zbudowane na SecurePlatform klastry Firewall mogą funkcjonować w konfiguracji Hot Stand-by (tzw. aktywna rezerwa) oraz Load Sharing (tzn. rozdzielanie obciążenia pomiędzy maszyny Firewall). W odróżnieniu od SecurePlatform urządzenia Firewall Appliance, na których nie można uruchomić modułu ClusterXL lub innego dedykowanego modułu HA funkcjonującego na poziomie zabezpieczeń (np. StoneBeat FullCluster, Rainfinity RainWall) w rzeczywistości w ogóle nie pozwalają na wdrożenie wiarygodnej ochrony zabezpieczeń Firewall przed awariami. Zewnętrzne urządzenia typu Load Balancer, protokoły rutowania (np. VRRP) czy mechanizmy klasteringu dostępne w systemie operacyjnym nie są w stanie wykryć awarii zabezpieczeń, a jedynie poważne awarie sprzętu.



Projektowanie zabezpieczeń sieci w sposób profesjonalny odbywa się zgodnie z wcześniej przeprowadzoną specyfikacją wymagań bezpieczeństwa i analizą ryzyka. Od technologii zabezpieczeń wymaga się skalowalności i elastyczności. System zabezpieczeń powinien bowiem obsługiwać istniejące oraz planowane protokoły komunikacyjne i usługi sieciowe. Szybki rozwój środowiska informatycznego wymaga od projektowanych zabezpieczeń wysokiej skalowalności i elastyczności, umożliwiających w przyszłości sprawne dokonywanie zmian w środowisku sieciowym, aplikacyjnym i usługowym.

SecurePlatform instalowane jest na standardowym sprzęcie o architekturze Intel. Zalecane jest jedynie aby wybrać markowy sprzęt serwerowy, a nie tzw. „składak”. Nie ma więc żadnych problemów z rozbudową i modernizacją SecurePlatform. Niezaprzeczalnym faktem jest, że systemy zabezpieczeń Firewall wykonują coraz bardziej szczegółową kontrolę aplikacji sieciowych i aby odbywało się to wydajnie sprzęt Firewall musi posiadać coraz szybsze procesory i więcej pamięci operacyjnej (np. Check Point wprowadził niedawno system wykrywania intruzów SmartDefence wbudowany w moduł FireWall-1). Kupując jako platformę zabezpieczeń VPN-1/FireWall-1 zamknięte urządzenie typu Firewall Appliance, które nie jest oparte na ogólnie dostępnym, markowym sprzęcie komputerowym (np. HP/Compaq, IBM i Siemens) przez wiele lat skazani będziemy na jego używanie bez możliwości rozbudowy (np. wymiany płyty głównej, wymiany procesora na szybszy, zamontowania większego dysku), a potem pozostanie nam jedynie wyrzucić ten sprzęt i zakupić nowy model Firewall Appliance.

W systemach o podwyższonych wymaganiach bezpieczeństwa (np. systemy bankowe, finansowe, rządowe, wojskowe) zabezpieczenia sieci powinny zapewniać precyzyjne monitorowanie funkcjonowania systemu Firewall, stref DMZ oraz innych wydzielonych stref bezpieczeństwa, ruterów, a także łączy dostępowych do sieci zewnętrznych w celu generowania odpowiednich alarmów. Nie jest zalecane w takich systemach oparcie bezpieczeństwa na jednej, wielo-funkcyjnej maszynie Firewall (np. Firewall na ruterze WAN). W takiej konfiguracji nie ma bowiem możliwości monitorowania łączy do sieci zewnętrznej przez dedykowane urządzenie IDS (tzn. zwykle nie ma technicznej możliwości podłączenia urządzenia IDS bezpośrednio do łączy WAN). Zalecane jest rozdzielenie zadań ochrony systemu informatycznego od zadań sterowania transferem danych w sieci i ochrony dostępności łączy (m.in. ruting dynamiczny). Zadania te powinny być realizowane przez dedykowane do tego celu systemy i urządzenia (m.in. kontrola dostępu i monitorowanie komunikacji to zadanie systemu Firewall, sterowanie ruchem w sieci to zadanie ruterów). Taki podział jest wskazany także z uwagi na łatwiejsze zarządzanie, diagnozowanie problemów i utrzymanie całości systemu.

Poszukując odpowiedniej platformy do wdrożenia zabezpieczeń VPN-1/FireWall-1 rozsądne jest wybrać platformę, na którą nowe wersje oprogramowania Check Point tworzone są bez opóźnień. Można to łatwo zweryfikować analizując, kiedy na poszczególne platformy pojawiła się najnowsza wersja produktu - Next Generation (NG). Linux i oparte na nim SecurePlatform to systemy operacyjne, na które nowe wersje oprogramowania Check Point i nowe rodzaje modułów zabezpieczeń pojawiają się w pierwszej kolejności. Szczególnie SecurePlatform jako system operacyjny dostarczany bezpośrednio przez Check Point wspiera bardzo szeroki zakres modułów zabezpieczeń, m.in.: VPN-1/FireWall-1 SmallOffice, VPN-1 Net, VPN-1 Pro, VPN-1 XL (Performance Pack), FireWall-1, FireWall-1 XL (Performance Pack), FloodGate-1, ClusterXL, SmartView Monitor, VPN-1/FireWall-1 VSX, User Authority Server oraz VPN-1 SecureClient Policy Server.



Bezpieczeństwa nie można kupić jako produktu. Bezpieczeństwo to stan, który uzyskuje się z użyciem środków technicznych (np. Firewall, VPN, IDS), organizacyjnych (np. procedury i kontrola) oraz prawnych (np. ubezpieczenie). Utrzymanie wysokiego poziomu bezpieczeństwa oraz prawidłowego funkcjonowania systemu zabezpieczeń wymaga jego właściwego zarządzania i monitorowania. Obecnie w coraz bardziej skomplikowanych i rozbudowanych środowiskach sieciowych kluczową rolę odgrywa zarządzanie bezpieczeństwem.

Od platformy Firewall wymaga się, aby posiadała łatwe w użyciu i kompletne narzędzia do konfiguracji i monitorowania stanu systemu operacyjnego i procesów zabezpieczeń. SecurePlatform zawiera specjalnie przygotowaną aplikację „sysconfig” do konfiguracji interfejsów sieciowych, routingu IP, nazwy hosta i domeny, DNS, czasu i daty systemowej oraz modułów zabezpieczeń (cpconfig). Graficzna konsola zabezpieczeń Check Point (SmartView) posiada możliwości bardzo szczegółowego monitorowania systemu operacyjnego maszyny Firewall (m.in. obciążenie procesora, zajętość pamięci operacyjnej, wolne miejsce na dysku, stan procesów). Z użyciem SmartUpdate z centralnej konsoli zarządzania Firewall instalowanie są nowe wersje i poprawki do oprogramowania Check Point i samego systemu SecurePlatform. Za pomocą SmartUpdate odbywa się także scentralizowane zarządzanie licencjami produktu.

Nie ma logicznego uzasadnienia, aby w systemie operacyjnym maszyny Firewall tworzyć dodatkowe narzędzia zdalnego zarządzania, jeżeli są one dostępne w konsoli Check Point. Sytuacja jaka ma miejsce w niektórych rozwiązaniach Firewall Appliance, gdzie instaluje się serwer WWW do konfigurowania systemu operacyjnego poprzez przeglądarkę WWW, niepotrzebnie stwarza zagrożenia dla bezpieczeństwa i stabilności platformy Firewall oraz obniża wydajność systemu (każdy proces, a szczególnie serwer WWW w systemie operacyjnym, obciążą dodatkowo pamięć operacyjną i procesor).



Każda firma posiada ograniczony budżet jaki może przeznaczyć na zabezpieczenia systemu informatycznego. Statystycznie nakłady na bezpieczeństwo wynoszą ok. 5 procent całościowych nakładów na informatykę. Koszt sprzętu Firewall nie powinien pochłaniać funduszy, które można przeznaczyć na wzbogacenie funkcjonalności zabezpieczeń (np. zakup dedykowanych narzędzi do analizy i raportowania zdarzeń) oraz podniesienie kwalifikacji administratorów (tzn. szkolenia na stopnie specjalizacji Check Point Certified Security Administrator i Check Point Certified Security Expert).

SecurePlatform instalowane na standardowym, markowym sprzęcie komputerowym, którego koszt nie przekracza 5.000 USD może osiągnąć bardzo wysoką wydajność zabezpieczeń Firewall i VPN. Sprzęt ten może być w trakcie eksploatacji Firewall swobodnie rozbudowywany i modernizowany. SecurePlatform zostało zbudowane na bazie oprogramowania *open-source* (jądro Linux) i także jest produktem, za który Check Point nie pobiera opłaty.

Planując zakup sprzętu dla zabezpieczeń Check Point należy bardzo dokładnie przyrzeć się przedstawionej przez dostawcę ofercie. Szczególną uwagę należy zwracać na oferty Firewall Appliance. Niekiedy bowiem cena takiego sprzętu znacznie przekracza koszt oprogramowania zabezpieczeń i zawiera koszty ukryte (np. instalacja nowej wersji oprogramowania Check Point wymaga instalacji nowej wersji systemu operacyjnego tego Firewall Appliance). Wiele rozwiązań Firewall Appliance opartych na systemie zabezpieczeń Check Point zostało tak zaprojektowane, aby sprawiać wrażenie urządzeń dedykowanych (np. została zmieniona prawdziwa nazwa zastosowanego systemu operacyjnego, stosowane są nietypowe płyty główne i procesory).

Dodanie do komputera PC dodatkowych kart LAN/WAN, protokołów dynamicznego routingu czy konsoli zarządzania przez przeglądarkę WWW nie tworzy z niego dedykowanego urządzenia Firewall. W rzeczywistości oferowany poziom bezpieczeństwa i wydajność tych rozwiązań są nieporównywalnie niższe od SecurePlatform. Co także się niestety zdarza, sprzedawcy niektórych rozwiązań Firewall Appliance zachęcają do zakupu swoich urządzeń podając nieprawdziwe informacje, że licencje Check Point na ten sprzęt są tańsze. Obniżone zyski ze sprzedaży licencji Check Point są wtedy rekompensowane przez zyski ze sprzedaży kosztownego sprzętu.

Krzywdzące byłoby generalizowanie i określenie wszystkich dostępnych na rynku rozwiązań Firewall Appliance jako niebezpieczne i oparte na słabej jakości sprzęcie. Dobrej klasy rozwiązania Firewall Appliance dostarczane są m.in. przez producentów markowego sprzętu komputerowego jak HP/Compaq, IBM i Siemens.

Decyzja o wyborze technologii zabezpieczeń i platformy Firewall należy zwykle do integratorów. Ponoszą oni za to pełną odpowiedzialność. SecurePlatform jest tylko jedną z dostępnych opcji. Stanowi ona jednak prawdziwe wyzwanie dla integratorów, aby z roli dostawcy sprzętu i oprogramowania stać się dostawcą rozwiązań bezpieczeństwa.

□ Mariusz Stawowski

O autorze:

Autor od wielu lat zawodowo zajmuje się bezpieczeństwem systemów informatycznych. Posiada w tym zakresie liczne stopnie specjalizacji m.in. ekspert zabezpieczeń Check Point, konsultant Entrust. Jest autorem dwóch książek i wielu publikacji w prasie informatycznej. Od 1996 roku zajmuje się produktami zabezpieczeń Check Point.