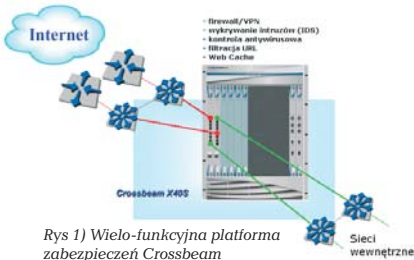


Crossbeam – nowa generacja platformy zabezpieczeń

Systemy zabezpieczeń sieciowych wiodących producentów (m.in. Check Point, Radware¹) rozwijane są w zakresie szczegółowej kontroli aplikacyjnej. W praktyce sprowadza się to do integracji zabezpieczeń firewall i IDS. Wykonywanie tych zadań w sposób skuteczny i jednocześnie wydajny wymaga zastosowania „mocnej” platformy sprzętowej. Sprzęt ogólnego przeznaczenia (np. serwery Intel/SPARC) jak również urządzenia określone jako appliance (tzn. urządzenia o architekturze PC z pre-instalowanym oprogramowaniem zabezpieczeń) nie pozwalają na swobodne stosowanie zabezpieczeń w sieciach wewnętrznych firm, ani też operatorów telekomunikacyjnych.

Producenci zabezpieczeń sieciowych stosują trzy podstawowe techniki podwyższenia wydajności – równoleglenie przetwarzania, specjalizowane układy ASIC² oraz procesory sieciowe (Network Processor). Np. układy ASIC umożliwiają działanie Radware DefensePro (in-line IDS) z przepływnością rzędu 3 Gbps. Zastosowanie specjalnej architektury sprzętowej i procesorów sieciowych w urządzeniach Crossbeam zapewnia wysoką wydajność działania kontroli aplikacyjnej najnowszej wersji zabezpieczeń Check Point NG with Application Intelligence. Oprócz firewall/VPN na jednej platformie Crossbeam mogą pracować inne zabezpieczenia jak system wykrywania intruzów IDS, czy system kontroli zawartości i filtracji URL (patrz rysunek 1).



Rys 1) Wielo-funkcyjna platforma zabezpieczeń Crossbeam

Modele urządzeń i wspierane aplikacje

Urządzenia Crossbeam dostępne są w serii X, dedykowanej dla central sieci korporacyjnych, centrów danych i sieci operatorów telekomunikacyjnych oraz serii C przeznaczonej dla sieci firmowych (patrz rysunek 2).

Na jednym urządzeniu Crossbeam może funkcjonować wiele aplikacji zabezpieczeń. Intencją firmy jest wspieranie produktów sieciowych i zabezpieczeń, posiadających najwyższe w swojej klasie referencje na rynku. Obecnie obsługiwane są m.in. następujące rozwiązania (w zależności od modelu):



Rys 2) Modele urządzeń Crossbeam

- systemy zabezpieczeń Check Point Firewall-1/VPN-1, VSX, GX,
- system bramki bezpieczeństwa Check Point Interspect
- systemy kontroli zawartości: Aladdin eSafe, Trend Micro InterScan VirusWall/IMSS/IWSS,
- systemy filtracji URL: Websense EIM
- systemy wykrywania intruzów: Check Point Interspect, Snort NIDS, ISS RealSecure,
- system Web Cache: Squid Proxy,
- system obsługi logów: Argus Flow Monitor.

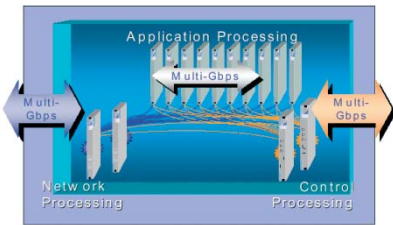
Architektura i moduły wewnętrzne

Urządzenia Crossbeam należą do nowej generacji platform zabezpieczeń. Zastosowano w nich architekturę sprzętową X-Stream umożliwiającą osiągnięcie bardzo wysokiej wydajności i niezawodności funkcjonowania zabezpieczeń sieciowych. Architektura Crossbeam składa się z następujących, zintegrowanych ze sobą komponentów (patrz rysunek 3):

- moduły przetwarzania ruchu sieciowego NPM (Network Processing Modules), odbierające pakiety z sieci i rozdzielające je do odpowiednich modułów przetwarzania aplikacji APM (Application Processing Modules), wykonujące przy tym ich równoważenie obciążenia (load balancing),
- moduły przetwarzania aplikacji APM, na których działają różne aplikacje zabezpieczeń jak firewall/VPN, IPS/IDS, systemy antywirusowe i filtracji URL,

- moduł kontrolny CPM (Control Processing Modules) odpowiedzialny za monitorowanie i analizę stanu komponentów urządzenia Crossbeam oraz funkcje ochrony przed awariami (m.in. wykrywanie awarii i automatyczne przełączenie uszkodzonych modułów),
- szyna połączeniowa (backplane) dla modułów NPM i APM o przepustowości wielo-gigabitowej (dwa łącza 1.6 Gbps do każdego APM, 3.2 Gbps per blade, 200 Mbps do zarządzania), posiadająca dwie redundancyjne ścieżki transmisji danych.

Moduły NPM sterowane są za pomocą systemu operacyjnego czasu rzeczywistego VxWorks. Moduły APM i CPM działają na bazie systemu operacyjnego Crossbeam X-Series Operating System (XOS), opartego na jądrze Linux. System operacyjny został dostosowany do obsługi architektury X-Stream. Zachowuje



Rys 3) Architektura Crossbeam X-Stream

jednak zgodność z bibliotekami Linux tak, aby możliwa była bezproblemowa instalacja oprogramowania rozwijanego przez producentów zabezpieczeń. Wszystkie ww. moduły urządzenia Crossbeam (NPM, APM i CPM) mogą być montowane w dwóch egzemplarzach w celu zapewnienia odporności na awarie. Crossbeam umożliwia wdrożenie systemu zabezpieczeń odpornego na awarie w zakresie elementów sprzętowych Crossbeam, modułów zabezpieczeń (firewall, IPS/IDS, itd.) oraz otaczającego środowiska sieciowego. Urządzenia sieciowe jak przełączniki L2/L3 mogą zostać podłączone do dwóch modułów NPM tak, aby w razie awarii jednego przełącznika komunikacja była kontynuowana przez ścieżkę zapasową.

Autoryzowanym dystrybutorem rozwiązań Crossbeam Systems w Polsce oraz Europie Centralnej i Wschodniej jest CLICO Sp. z o.o.
<http://www.clico.pl/hardware/crossbeam/>

¹Raport Gartner, Magic Quadrant for Enterprise Firewalls, 19 czerwca 2003.

²Implementacja algorytmów zabezpieczeń w specjalizowanych układach scalonych ASIC (Application-Specific Integrated Circuit). Praktyczna implementacja koncepcji zabezpieczeń sprzętowych.