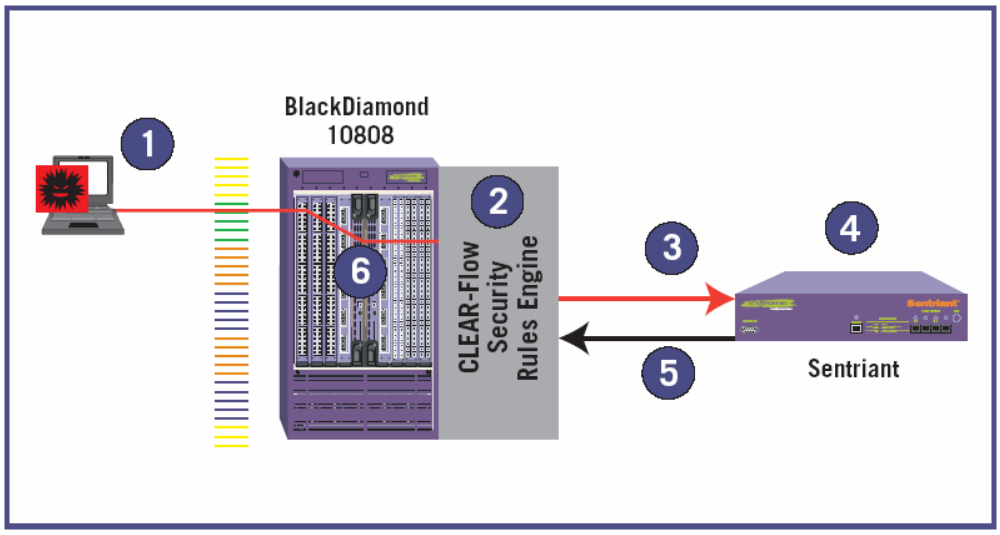
NOTKA TECHNICZNA

Extreme Networks Sentriant - monitorowanie i ochrona przed atakami w sieciach rdzeniowych (10 GB)

Skuteczna ochrona przed atakami (D)DoS oraz rozprzestrzenianiem się w sieciach robaków, spyware i innych złośliwych aplikacji (tzw. malware) wymaga zastosowania w sieci odpowiednich zabezpieczeń Intrusion Prevention System (IPS). Wprowadzenie klasycznych zabezpieczeń IPS w sieciach rdzeniowych, gdzie standardem staje się 10 GB nie jest technicznie możliwe (najbardziej wydajne urządzenia IPS osiągają przepustowość do 3 Gbps). Rozwiązaniem jest zastosowanie zabezpieczeń IPS zintegrowanych z przełącznikami rdzeniowymi. W opracowaniu została przedstawiona charakterystyka systemu zabezpieczeń Extreme Networks Sentriant, który został zaprojektowany do monitorowania i blokowania ataków w sieciach rdzeniowych 10 GB.



Rys 1). Zasady działania systemu zabezpieczeń Extreme Networks Sentriant

Urządzenie Sentriant jest podłączone do przełącznika rdzeniowego Extreme Networks BlackDiamond 10808 (10K). Sentriant nie działa w trybie in-line jak typowy IPS, przez co nie stwarza zagrożenia wprowadzania opóźnień i zakłóceń w komunikacji sieciowej. Wykrywanie ataków w tym systemie zabezpieczeń odbywa się na zasadzie analizy zachowania sieci. Nie są do tego celu wykorzystywane klasyczne techniki detekcji stosowane przez zabezpieczenia IDS/IPS, jak sygnatury i analiza heurystyczna. Urządzenia zabezpieczeń Sentriant posiadają możliwości monitorowania i ochrony komputerów w sieciach wewnętrznych bez konieczności instalacji agentów na desktop-ach. Wdrożenie zabezpieczeń Sentriant w rdzeniu sieci sprawia, że są one naturalnym uzupełnieniem występujących na styku sieci i desktop-ach zabezpieczeniach firewall i IPS.

Urządzenia zabezpieczeń Sentriant posiadają największą funkcjonalność, działając w integracji z CLEAR-Flow[1] m.in. potrafią blokować ataki (D)DoS oraz ataki robaków sieciowych jak Sasser, Welchia, MyDoom, Blaster czy SQL Slammer. CLEAR-Flow to

[1] CLEAR-Flow (Continuous Learning, Examination, Action and Reporting of Flows)

funkcjonalność wbudowana w system operacyjny przełączników Extremeware XOS, dedykowana do monitorowania ruchu sieciowego i selektywnego blokowania (ACL) niedozwolonych porcji danych. Dla przykładu CLEAR-Flow może wykrywać ataki SYN Flood poprzez monitorowanie proporcji pomiędzy liczbą pakietów TCP SYN i TCP ACK. Całość systemu zabezpieczeń (Sentriant, BlackDiamond CLEAR-Flow) jest administrowana z centralnego systemu zarządzania EPICenter.

Typowy proces działania systemu zabezpieczeń Sentriant przebiega w następujący sposób (patrz rysunek 1):

1. Intruz lub robak inicjuje atak.
2. Przełącznik BlackDiamond za pomocą mechanizmów CLEAR-Flow wykrywa "podejrzany" ruch.
3. Przełącznik BlackDiamond przekierowuje "podejrzaną" komunikację do urządzenia zabezpieczeń Sentriant.
4. Ruch sieciowy jest poddawany kontroli przez Sentriant w zakresie wykrywania ataków.
5. W razie potrzeby Sentriant dynamicznie tworzy nowe ustawienia ACL na przełączniku BlackDiamond 10K i zmiania kryteria analizy ruchu. W efekcie otrzymuje kolejne porcje "podejrzanego" ruchu. Równocześnie zabezpieczenia Sentriant wykrywają niedozwolony ruch (np. ataki DoS) i wysyłają instrukcje zablokowania ataków do EPICenter i BlackDiamond 10K. EPICenter działając w środowisku Extreme Secure Switch Infrastructure (tzn. zarządzanych przełączników rdzeniowych i brzegowych Extreme) blokuje niedozwolony ruch.

W systemie zabezpieczeń Sentriant zostały zaimplementowane następujące techniki ochrony:

1. *Virtually In-line Operation* – urządzenia zabezpieczeń Sentriant są podłączone do przełącznika sieci na zasadzie sniffera. Działając w integracji z przełącznikiem mają możliwość blokowania ataków i izolowania zainfekowanych komputerów.
2. *Hyper Detection* – system zabezpieczeń Sentriant wykorzystuje prywatne adresy IP, które nie są używane w sieciach wewnętrznych do tworzenia wirtualnych zasobów systemu informatycznego. Jest to forma „honeypot” mająca na celu zbudowanie systemu wczesnego ostrzegania. Intruzi i robaki internetowe identyfikowane są już w momencie wykonywania przez nie rekonesansu systemu informatycznego (np. skanowania sieci i portów).
3. *Active Deception* – system zabezpieczeń Sentriant w razie wykrycia prób połączeń z wirtualnymi zasobami (*Hyper Detection*) odpowiada na te zapytania specjalnie spreparowanymi pakietami TCP, UDP i ICMP. W rezultacie stanowi to utrudnienie dla robaków i intruzów, które rozpoznają zasoby systemu informatycznego i daje czas systemowi zabezpieczeń na ich zablokowanie. Mechanizm ten skutecznie chroni także przed technikami rozpoznawania systemów operacyjnych typu „fingerprint”.
4. *Surgical Defense* – ochrona przed atakami odbywa się poprzez przekierowanie ruchu od intruza/robaka do urządzenia zabezpieczeń Sentriant. Urządzenie Sentriant analizuje całość podejrzanego ruchu i selektywnie blokuje niedozwolone porcje danych.

Więcej informacji nt. rozwiązań Extreme Networks można znaleźć na serwerze Web producenta oraz polskich stronach http://www.clico.pl/hardware/extreme/