# ASQ: ZALETY SYSTEMU IPS W NETASQ

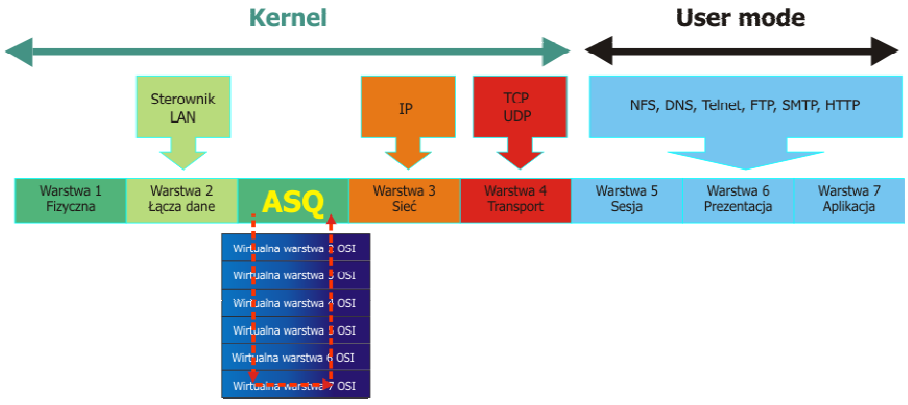
Firma NETASQ specjalizuje się w rozwiązaniach do zintegrowanego zabezpieczenia sieci komputerowych, kierując się przy tym założeniem, że ryzyko ataku jest identyczne niezależnie od rozmiarów firmy. Od początku swojej działalności za główny cel firma postawiła sobie dostarczanie rozwiązań zapewniających najwyższy poziom zabezpieczeń niezależnie od wielkości firmy korzystającej z rozwiązań. Wszystkie urządzenia UTM NETASQ wyposażone są w pełną funkcjonalność bez względu na model.

W swoich rozwiązaniach NETASQ stosuje autorską technologię ASQ (Active Security Qualification) zapewniającą skuteczną ochronę przed nowymi, jeszcze niesklasyfikowanymi zagrożeniami. **NETASQ, jako pierwszy dostawca rozwiązań do ochrony sieci, zastosował unikalną technologię integrującą system wykrywania i blokowania włamań z firewallem.** Obecnie uznawany jest za jednego z czołowych europejskich dostawców rozwiązań do zabezpieczania sieci firmowych, a jego produkty dostępne są w ponad 50 krajach na całym świecie.

## WYDAJNOŚĆ SYSTEMU ASQ

NETASQ oferuje pełną ochronę nie tylko przed znanymi zagrożeniami, ale przed wszystkim przed tymi, które jeszcze nie zostały sklasyfikowane i na które jeszcze nie opracowano sygnatur. Tym samym zapewnia kompletną proaktywną ochronę w momencie ataku na firmową sieć. Opracowany przez NETASQ Intrusion Prevention System o nazwie ASQ oferuje wysoką wydajność jednocześnie zapewniając wysoki poziom bezpieczeństwa. **Efektywność rozwiązania uzyskiwana jest dzięki analizie przesyłanych pakietów na poziomie jądra systemu operacyjnego o nazwie NETASQ Secured BSD** (NS-BSD).

Konkurencyjne rozwiązania wykorzystują system blokowania włamań dodając go do już istniejącej architektury zapory ogniowej firewall. W takich systemach IPS traktowany jest jako dedykowany moduł pośredniczący proxy, do którego kierowane są połączenia. Powoduje to konieczność ponownego analizowania pakietów przez IPS oraz tworzenia kopii zapasowych danych przesyłanych między modułami w pamięci systemu operacyjnego. Wpływa to na czas w jakim pakiety poddawane są analizie. W konsekwencji system ASQ firmy NETASQ w konfrontacji z rozwiązaniami pozostałych producentów systemów IPS uzyskuje nieporównywalną wydajność.




ASQ dokonuje analizy połączenia na poziomie jądra systemu operacyjnego.

## OCHRONA PROAKTYWNA

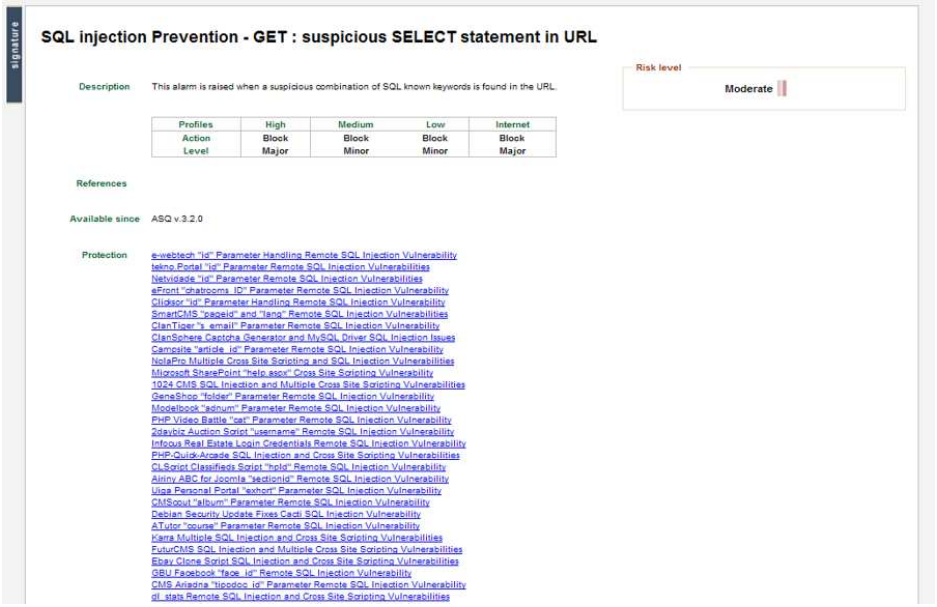
Silnik IPS zapewnia wysoką skuteczność w wykrywaniu zagrożeń dla firmowej sieci. Cały ruch na styku sieci lokalnej z siecią WAN skanowany jest przy pomocy trzech metod analizy.

Pierwszą z nich jest **analiza protokołu** w odniesieniu do standardów takich jak RFC. Ten mechanizm pozwala na odrzucenie komunikacji niezgodnej z normami. Przykładem skuteczności analizy protokołu może być wykrywanie połączeń przechodzących przez port 80. System IPS dokonując analizy ruchu przechodzącego przez port 80 potrafi wykryć czy komunikacja ta jest typowa dla połączeń http. Próba połączenia peer-to-peer poprzez port 80 (co jest niezgodne ze standardami wyznaczonymi przez RFC) spowoduje, że system ASQ odrzuci połączenie.

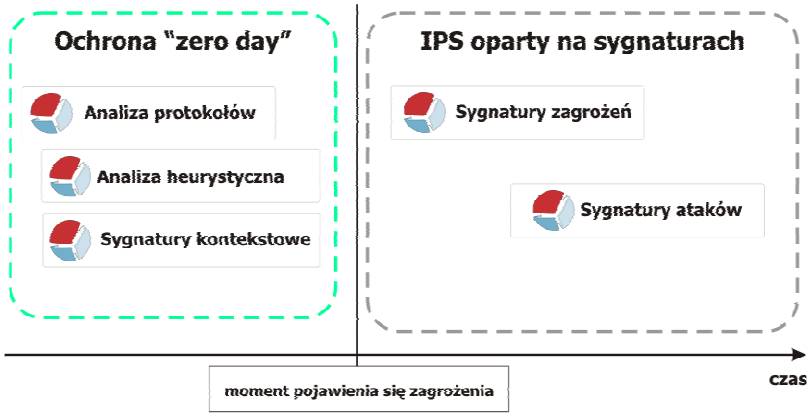
Kolejnym elementem ochrony jest **analiza heurystyczna**. Pozwala ona określić czy przechodząca przez urządzenie NETASQ komunikacja posiada cechy ataku czy też jest jedynie niegroźnym, a dopuszczalnym odchyleniem od typowego ruchu sieciowego. Analiza heurystyczna służy również do wykrywania niepożądanego zachowania w sieci, czego przykładem może być skanowanie portów, flooding czy ataki typu DDoS

Kolejnym narzędziem zastosowanym w NETASQ są regularnie aktualizowane **sygnatury kontekstowe**. Ich przewaga nad tradycyjnymi sygnaturami polega na uwzględnianiu kontekstu połączenia podczas jego analizy. Oznacza to, że ASQ bierze pod uwagę rodzaj połączenia, typ wykorzystywanych protokołów oraz portów, przez które przebiega komunikacja. Po rozpoznaniu określonego typu połączenia, silnik IPS uruchamia wtyczki programowe (tzw. plug-iny) wyspecjalizowane w ochronie danego protokołu. Dla przykładu, gdy wykryta zostanie transmisja FTP, ASQ uruchamia plug-in FTP i porównuje ten ruch z posiadanymi w bazie sygnaturami kontekstowymi. Mechanizm korzystający z sygnatur kontekstowych pozwala na szybszą analizę ruchu, która nie wymaga

porównywania z wszystkimi tradycyjnymi sygnaturami z bazy. Poza tym wystąpienie sygnatury ataku w niewłaściwym dla niej kontekście (rodzaj połączenia, protokół, port) nie pociąga za sobą blokowania ruchu. Takie rozwiązanie przekłada się na wysoką skuteczność w wykrywaniu prób ataku i zachowanie niskiego poziomu omyłkowych wskazań poprawnego połączenia (tzw. „false positive").
Na poniższym przykładzie - jednej sygnaturze kontekstowej firmy NETASQ przeciwko tzw. SQL injections odpowiada ponad 1540 sygnatur ataków zastosowanych w innych rozwiązaniach.

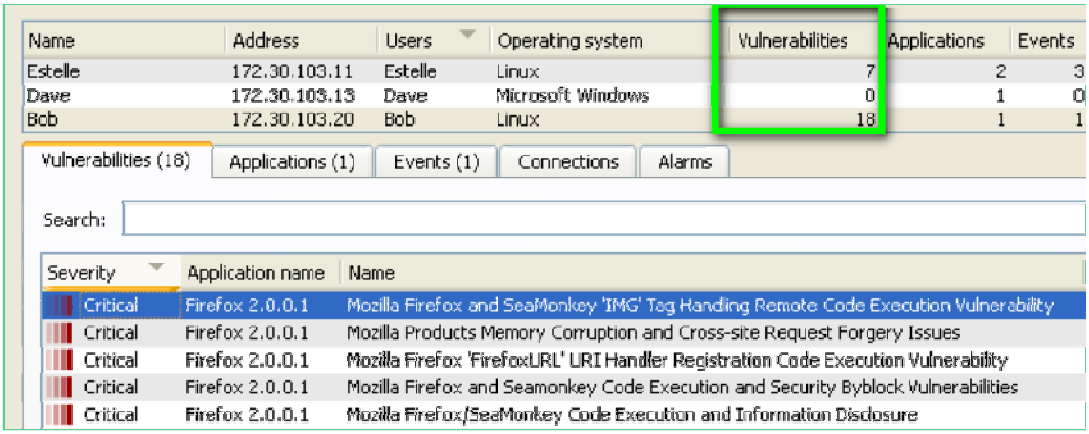



Połączenie trzech omówionych wyżej metod analizy w rozwiązaniach NETASQ zapewnia pełną ochronę „dnia zerowego". Poniższy wykres prezentuje architekturę system ASQ firmy NETASQ, która zapewnia ochronę w chwili pojawienia się zagrożenia. Konkurencyjne rozwiązania IPS oparte na sygnaturach są zależne od szybkości wydania wzorca ataku (pattern) przez producenta.




## SEISMO: skaner wnętrza sieci

Uzupełnieniem ochrony w czasie rzeczywistym jest pasywny skaner wnętrza sieci. Unikalny silnik o nazwie SEISMO skanuje cały ruch przechodzący przez ASQ, pochodzący z różnych segmentów sieci, w poszukiwaniu aplikacji podatnych na ataki. Informacje zebrane w czasie skanowania ruchu przez SEISMO służą do oceny ryzyka ataku dla każdej monitorowanej stacji roboczej. SEISMO zbiera informacje dotyczące słabych punktów i luk w nieaktualnych wersjach aplikacji łączących się z Internetem. Dzięki niemu można uzyskać szczegółowy raport o podatności sieci na ataki wraz z wyszczególnieniem potencjalnych źródeł zagrożeń. SEISMO nie generuje żadnego dodatkowego ruchu, dzięki czemu nie ma wpływu obciążenie sieci. Administrator otrzymuje informacje o lukach wraz z propozycjami ewentualnego rozwiązania, które pozwolą zmniejszyć ryzyko (np. poprzez aktualizację aplikacji).



## Podsumowanie

Technologia NETASQ to modelowe rozwiązanie w dziedzinie zabezpieczania tradycyjnej jak i wirtualnej architektury sieciowej, oparte na zasadzie „zero tolerancji". Wszystkie metody analizy składające się na system IPS są automatycznie aktywne od momentu instalacji produktu. W przeciwieństwie do większości rozwiązań konkurencyjnych, które dodały oprogramowanie IPS do istniejącego już rozwiązania firewallowego, technologia NETASQ od początku opierała się na systemie IPS zintegrowanym z zaporą ogniową. Oprócz tego NETASQ jest jedynym producentem zabezpieczeń, który oferuje wykrywanie luk i skanowanie sieci w czasie rzeczywistym jako integralną część swoich urządzeń. Technologia ASQ firmy NETASQ zastosowana jest w rozwiązania sprzętowych oraz wirtualnych, kompatybilnych z platformami wirtualizacji VMware i Citrix.