

# NETASQ Virtual Appliance

**Ochrona klasy UTM w formie wirtualnej maszyny, pracującej w środowiskach VMware lub Citrix, zapewniająca wszystkie funkcjonalności znane z fizycznych urządzeń NETASQ.**

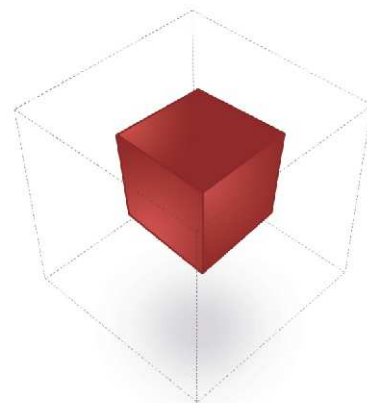
Korzyści płynące z wirtualizacji są oczywiste: redukcja kosztów, optymalizacja zasobów, łatwiejsze uruchamianie i zarządzanie usługami, jak również szybsze odzyskiwanie danych.

W środowiskach zwirtualizowanych wiele maszyn wirtualnych zlokalizowanych jest na jednej platformie sprzętowej. Serwery pocztowe i www, tradycyjnie zlokalizowane w strefie DMZ, mogą się zatem znajdować w tym samym środowisku, co serwery produkcyjne, potencjalnie zwiększając dostępność tych ostatnich. Przy przejściu ze środowiska fizycznego do

wirtualnego konieczne jest utrzymanie pożądanego poziomu ochrony również w ruchu pomiędzy wirtualnymi serwerami znajdującymi się na jednym serwerze fizycznym. Taką rolę najlepiej spełnia wirtualne urządzenie zabezpieczające – wtedy ruch nie musi być już wyprowadzany ze środowiska wirtualnego na firewall fizyczne. Dodatkowo wirtualne urządzenie zabezpieczające umożliwia korzystanie w pełni z ogólnych zalet wirtualizacji m.in. równoważenia obciążenia, możliwości przenoszenia i szybkiego odzyskiwania danych.

## OCHRONA SIECI DZIĘKI WIRTUALNYM ROZWIĄZANIOM NETASQ

Zintegrowany na poziomie jądra systemu operacyjnego firewall wraz z systemem wykrywania włamań (IDS/IPS) dnia zerowego



stanowi podstawę wszystkich urządzeń wirtualnych NETASQ. Dzięki analizie protokołów i aplikacji sieci silnik NETASQ wykrywa i blokuje zagrożenia, zdecydowanie zmniejszając ryzyko fałszywego alarmu dzięki analizie behawioralnej połączonej z szeregiem baz sygnatur kontekstowych. Wirtualne rozwiązania NETASQ pozwalają również na ochronę przed wirusami, spamem oraz zagrożeniami płynącymi z Internetu, dzięki wyposażeniu w filtr URL. NETASQ seria V zapewnia także ochronę dla ruchu VoIP i wspiera tunele IPsec i SSL VPN, gwarantując pełną ochronę dla komunikacji sieciowej.

## NETASQ SERIA V:

- FIREWALL
- IDS/IPS
- VPN IPSEC, SSL
- AUTORYZACJA (AD, LDAP)
- SEISMO
- QoS
- ANTYWIRUS
- ANTYSZPAM
- FILTR URL
- RAPORTOWANIE ZDARZEŃ
- MONITORING SIECI

## NETASQ SERIA V do ochrony stacji roboczych:

GŁÓWNE CECHY	V50	V100	V200	V500	VU
Chronione adresy IP	50	100	200	500	unlimited
Jednoczesne połączenia	100.000	200.000	400.000	600.000	3.000.000
802.1Q VLAN (max)	32	128	128	128	512
Tunele IPSEC VPN (max)	100	500	1000	1000	10.000
Jednoczesna liczba klientów SSL VPN	50	256	512	512	2.048

## NETASQ SERIA VS do ochrony serwerów:

GŁÓWNE CECHY	V55	VS10
Ilość chronionych maszyn wirtualnych	5	10
SEISMO – pasywny skaner wnętrza sieci	TAK	TAK
Jednoczesne połączenia	100.000.000	200.000.000
802.1Q VLAN (max)	512	512
Tunele IPSEC VPN (max)	10.000	10.000
Jednoczesna liczba Klientów SSL VPN	2.048	2.048



### FIREWALL/AUTORYZACJA

- autoryzacja w oparciu o zewnętrzne usługi katalogowe: LDAP, Active Directory, Radius, NTLM
- Transparentna autoryzacja: Microsoft SPNEGO - certyfikaty SSL

### UTM/WIELOFUNKCYJNY

#### FIREWALL

- proxy: SMTP, POP3, HTTP, FTP
- antywirus, antyspyware, antyspam w oparciu o listy reputacyjne (DNS RBL) oraz zaawansowaną analizę heurystyczną
- IPSEC VPN
- SSL VPN

#### IPS/KONTROLA APLIKACJI

- analizator spójności reguł
- graficzny harmonogram dla polityk bezpieczeństwa
- automatyczna kwarantanna w przypadku ataku
- ochrona przed atakami typu flooding
- ochrona przed wyciekiem danych

- zaawansowany system zarządzania fragmentacją pakietów
- ochrona przed atakami SQL injections
- ochrona przed Cross Site Scripting (XSS)
- wykrywanie koni trojańskich
- ochrona przed uprowadzeniem sesji
- kontrola poprawności protokołów aplikacji z wykorzystaniem pluginów: IP, TCP, UDP, HTTP, FTP, SIP, RTP/RTCP, H323, DNS, SMTP, POP3, IMAP4, NNTP, SSL, MGCP, Edonkey, SSH, Telnet itd.

#### USŁUGI SIECIOWE

- DHCP client and server
- NTP client
- DNS cache proxy
- tryby pracy: transparentny, router, hybrydowy
- translacja adresów (NAT, PAT, split)
- routing statyczny
- Policy Based Routing
- routing dynamiczny

- Quality of Service (QoS)
- Load balancing

#### ZARZĄDZANIE

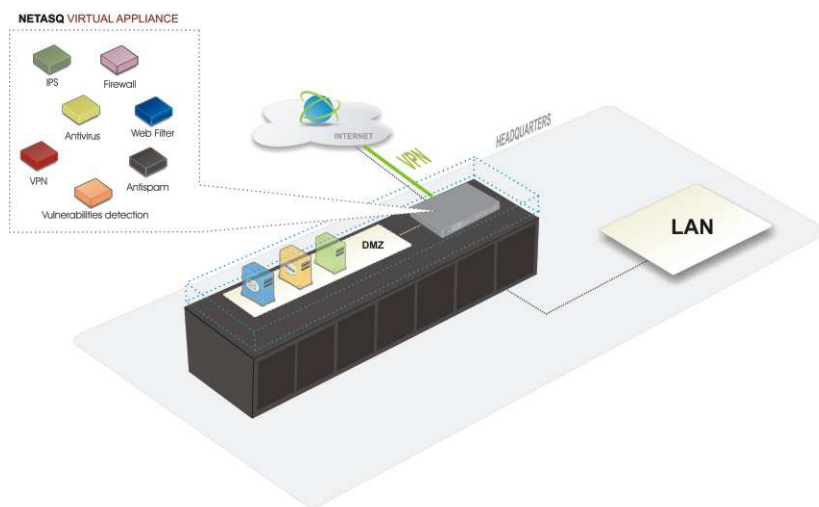
- możliwość zarządzania przez wielu administratorów
- różne uprawnienia dla administratorów
- NETASQ UNIFIED MANAGER
- NETASQ REAL-TIME MONITOR
- NETASQ EVENT REPORTER
- ssh v2
- zarządzanie przez port SERIAL

#### MONITORING I RAPORTOWANIE

- Logowanie do wielu serwerów Syslog
- powiadamianie o zdarzeniach za pośrednictwem e-maila
- automatyczne generowanie raportów
- SNMP v1, v2, v3 (DES, AES) agent

#### OPCJE

- NETASQ SEISMO - pasywny skaner wnętrza sieci



### PRZYKŁADOWE ZASTOSOWANIE

#### Sieci wirtualne wymagają takiej samej ochrony jak sieci fizyczne

NETASQ Virtual Appliances zapewniają sieci wirtualnej taki sam poziom ochrony jak jej fizycznemu odpowiednikowi. Seria V rozwiązań NETASQ potrafi zagwarantować ochronę ruchu zarówno pomiędzy maszynami wirtualnymi, jak i ruchu w całej sieci wirtualnej i fizycznej. Dzięki temu wirtualizacja pozwala na oszczędności i równocześnie nie powoduje obniżenia dotychczasowego poziomu ochrony. Urządzeniami NETASQ - zarówno wirtualnymi jak i fizycznymi - można zarządzać za pomocą jednej aplikacji.

#### NA TEMAT NETASQ:

Firma NETASQ została założona w 1998 i obecnie jest europejskim liderem wśród dostawców rozwiązań bezpieczeństwa IT dedykowanych dla firm. NETASQ oferuje rozwiązania klasy Unified Threat Management (UTM) oparte na unikalnej architekturze ASQ, które wyposażono w zapórę sieciową, filtr zawartości, antyspyware, antywirus oraz antyspam. UTM firmy NETASQ posiadają również filtr URL, wirtualną sieć prywatną (VPN) – IPsec, SSL (Secure Socket Layer) oraz własny wbudowany system zapobiegania włamaniom (IPS). Dystrybutorem urządzeń firmy NETASQ w Polsce jest spółka DAGMA, posiadająca w swoim portfolio szeroki wachlarz rozwiązań bezpieczeństwa IT.

