

firewall | system blokowania włamań (IPS) | serwer VPN
system antywirusowy | system antyspamowy | filtr URL



U6000

UTM NETASQ U6000 jest urządzeniem integrującym w jednej obudowie podstawowe elementy niezbędne do kompletnego zabezpieczenia i monitorowania sieci lokalnej, zaprojektowanym z myślą o dużych korporacjach. Zawiera firewall, system wykrywania i blokowania włamań IPS (Intrusion Prevention System), serwer VPN, system antywirusowy, system antyspamowy oraz system filtrowania dostępu do stron internetowych (filtr URL).

Firewall - NETASQ U6000 wyposażony jest w wysokiej klasy stateful inspection firewall. Dzięki intuicyjnej konsoli konfiguracyjnej oraz analizatorowi reguł pozwalającemu na wychyczenie ewentualnych błędów i sprzeczności, definiowanie reguł jest zadaniem stosunkowo prostym. Administrator ma możliwość zdefiniowania wielu różnych zestawów reguł określających, jaki ruch powinien być przez firewall przepuszczany, a jaki blokowany, obowiązujących w różnych przedziałach czasowych. Pozwala także na ustalenie innych zasad filtrowania ruchu w godzinach pracy, innych w godzinach popołudniowych, a jeszcze innych w dni wolne od pracy.

Intrusion Prevention System (IPS) - system Intrusion Prevention w urządzeniach NETASQ wykorzystuje unikalną, stworzoną w laboratoriach firmy NETASQ technologię wykrywania i blokowania ataków ASQ. Analizie w poszukiwaniu zagrożeń i ataków poddawany jest cały ruch sieciowy od trzeciej do siódmej warstwy modelu OSI. Stosowane są trzy podstawowe metody: analiza protokołów, analiza heurystyczna oraz sygnatury kontekstowe.

Technologia ASQ (Active Security Qualification) - technologia bazuje na tzw. kontekstowej analizie ruchu przechodzącego przez urządzenie, która dokonywana jest bezpośrednio w jądrze systemu operacyjnego (kernel mode), a nie jak to jest w przypadku innych urządzeń UTM w trybie proxy (proxy mode). Możliwość prowadzenia analizy w trybie kernel pozwala osiągnąć niespotykaną w innych urządzeniach UTM szybkość działania, niezależną od liczby uruchomionych serwisów czy zdefiniowanych w danym momencie reguł.

Virtual Private Networks (VPN) - urządzenie posiada wbudowany serwer VPN, który pozwala na tworzenie bezpiecznych połączeń, tzw. kanałów VPN. Kanały VPN mogą być tworzone pomiędzy użytkownikami pracującymi w terenie, a siedzibą firmy (połączenia client-to-site) lub pomiędzy centralą a oddziałami firmy (połączenia site-to-site). Kanały VPN budowane są w oparciu o protokół IPsec lub SSL. Dostępność kanałów VPN w czasie może być ściśle nadzorowana - administrator systemu decyduje w jakie dni i w jakich godzinach jest możliwe otwarcie danego kanału VPN.

SEISMO - moduł dodatkowy umożliwiający administratorowi wykrywanie słabych punktów sieci firmowej poprzez wyszukiwanie nieaktualnych wersji oprogramowania na stacjach roboczych i wykrywania niedozwolonego typu ruchu wewnątrz sieci. W przypadku zidentyfikowania nieprawidłowości SEISMO automatycznie informuje o nich administratora, wskazuje zagrożone stacje oraz sugeruje administratorowi źródła, z których może on pobrać odpowiednie poprawki.

Ochrona antywirusowa – U6000 posiada wbudowany system ochrony antywirusowej ClamAV. Pod kątem obecności wirusów sprawdzana jest cała poczta przychodząca i wychodząca. Wiadomości zawierające wirusy są automatycznie usuwane, a o zdarzeniu powiadamiany jest odbiorca poczty. Sprawdzane są też wszystkie odwiedzane przez użytkowników strony internetowe oraz zbiory pobierane z Internetu. Dodatkowo, opcjonalnie dostępny jest skaner antywirusowy Kaspersky AV. Filtr ochrony antywirusowej może pracować w trybie proxy lub bridge. W przypadku zastosowania trybu bridge ochrona antywirusowa jest „przezroczysta” dla ruchu sieciowego i nie wymaga żadnych zmian w konfiguracji sieci.

Ochrona przed spamem - ochrona antyspamowa zapewniana jest poprzez wbudowany w urządzenie system DNS Blacklisting, umożliwiający blokowanie spamu bezpośrednio u źródła. Lista serwerów rozsyłających spam jest na bieżąco aktualizowana. Administrator może tworzyć własne białe i czarne listy. W modelu U6000 stosowane są także heurystyczne metody antyspamowe oraz analiza Bayesiańska.

Filtrowanie URL - urządzenie wyposażone jest we własny, stale aktualizowany moduł filtrowania stron internetowych. Administrator może w każdej chwili uzupełnić listę stron, które powinny być dostępne lub niedostępne dla użytkowników. Filtr URL może być ustawiany dla wszystkich lub wybranych grup użytkowników definiowanych przez administratora. Jako opcja w modelu U6000 dostępny jest filtr URL firmy OPTENET.

Quality of Service (QoS)/Bandwith Management - urządzenie wyposażone jest w mechanizmy zapewniające priorytyzację ruchu sieciowego oraz zarządzanie pasmem. Do poszczególnych reguł, definiowanych na firewallu, może zostać przypisany określony priorytet lub do określonego typu ruchu (HTTP, VoIP) przydzielona zostaje minimalna i maksymalna szerokość pasma, jaką może on wykorzystać.

Load Balance - NETASQ U6000 pozwala na jednoczesne utrzymywanie i wykorzystywanie kilku połączeń z Internetem. Ruch sieciowy może być rozkładany w takim przypadku równomiernie na wszystkie aktywne połączenia. W razie awarii któregoś z połączeń, pozostałe automatycznie przejmują jego funkcję.

High Availability - istnieje możliwość zestawienia dwóch urządzeń tak, aby działały w klastrze. Dzięki takiemu rozwiązaniu w przypadku awarii urządzenia podstawowego drugie urządzenie automatycznie przejmie wszystkie jego funkcje i generuje raport o awarii przesyłany następnie do administratora. Przełączenie takie następuje na tyle szybko, że nawiązane wcześniej połączenia nie zostaną zerwane.

Monitoring w czasie rzeczywistym - każde z urządzeń firmy Netasq posiada w standardzie konsolę umożliwiającą podgląd w czasie rzeczywistym pracy zapory sieciowej, kontrolę stanu bieżącego ochrony na styku sieci, kontrolę połączeń dla poszczególnych stacji, monitoring i kontrolę komunikatów generowanych przez IPS, monitoring i kontrolę stanów kanałów VPN etc.

Raportowanie - każde urządzenie wyposażone jest w zaawansowane narzędzie do przeglądania logów oraz sporządzania graficznych raportów. Raporty takie mogą dotyczyć np. wykrytych i zablokowanych ataków, analizy aktywności w sieci, odwiedzanych stron internetowych etc. Administrator może korzystać ze zdefiniowanych przez producenta raportów oraz w zależności od potrzeb tworzyć własne, dostosowane do indywidualnych wymagań.

Podstawowe informacje o urządzeniu:

- liczba portów routowalnych 10/100/1000 Mbps – od 6 do 24
- wydajność firewalla wraz z modulem IPS (ASQ) – 5 000 Mbps
- liczba jednoczesnych połączeń TCP – 2 500 000
- liczba nowych sesji na sekundę – 40 000
- pamięć dyskowa – 2 x 74 GB RAID1
- maksymalna liczba reguł filtrujących – 32 000
- obsługa do 256 VLAN-ów
- wbudowany Dialup router (PPTP, PPPoE, L2TP, PPP)

Kanały VPN:

- obsługa protokołów IPSec, PPTP oraz SSL
- wydajność kanału VPN szyfrowanego AES - 600 Mbps
- liczba tuneli VPN – 10 000
- liczba tuneli VPN SSL – 2 048
- liczba tuneli VPN PPTP – 64
- szyfrowanie kanałów algorytmem DES, 3 DES lub AES, CAST128 oraz Blowfish
- autentykacja z wykorzystaniem SHA1 oraz MD5
- autentykacja z wykorzystaniem certyfikatów IKE
- klucz szyfrujący pre-shared, statyczny lub PKI
- VPN typu Hub & Spoke
- kanały VPN typu site-to-site
- kanały VPN typu client-to-site
- funkcja „keep alive” dla kanałów VPN
- funkcja „Dead Peer Detection”
- obsługa kanałów VPN IPSec
- NAT-Traversal (UDP 500 oraz 4500)

Wykrywanie włamań i ataków (Intrusion Prevention System):

- technologia ASQ pracująca w trybie kernel-mode
- plug-iny dynamicznie analizujące ruch (HTTP, FTP, DNS, RIP, H323, EMule, SSL, SSH, Telnet, SMTP, POP3, IMAP4, NNTP, generic, itp.)
- wielowarstwowa analiza protokołów (do warstwy aplikacji)
- blokowanie znanych i nieznanymi ataków
- ochrona przed atakami na kanały VPN
- ochrona przed atakami typu flooding (ICMP, UDP, TCP)

- ochrona przed wyciekami danych poprzez rekonstrukcję i dekodowanie ruchu
- ochrona przed trojanami i backdoorami
- ochrona przed uprowadzeniem sesji
- ochrona informacji o systemie operacyjnym
- dynamiczne czarne listy
- automatycznie aktualizowane sygnatury kontekstowe
- czasowa i stała kwarantanna
- filtry aplikacji P2P oraz Instant Messaging
- ochrona przed spyware

Funkcje sieciowe oraz filtrowanie:

- tryb pracy routera, bridge'a (transparentny) lub hybrydowy
- routing per interface
- translacja adresów (NAT, PAT i Split)
- harmonogram czasowy dla reguł
- dynamiczne zarządzanie pasmem
- priorytyzacja ruchu sieciowego (QoS)
- obsługa aliasów adresów IP

Funkcje High Availability:

- praca w trybie Active/Passive
- synchronizacja konfiguracji
- synchronizacja sesji

Funkcje antywirusowe:

- wbudowany ClamAV lub jako opcja Kaspersky AV
- transparentne skanowanie SMTP, POP3, HTTP
- automatyczne aktualizacje

Funkcje antyspamowe:

- DNS Blacklisting
- analiza heurystyczna

Autentykacja:

- obsługa Single-Sign-On
- obsługa LDAP (wewnętrzny i zewnętrzny)
- współpraca z autentykacją Windows (NT4 - NTLM, WIN2K - Kerberos)
- współpraca z Radius
- wbudowany PKI CA oraz CRL
- zgodność PKI
- funkcja „web enrollment”

Usługi dodatkowe:

- HTTP Proxy, filtrowanie URL, filtrowanie AV
- obsługa protokołu ICAP dla filtrowania Web
- SMTP Proxy
- POP3 Proxy
- usługa DynDNS
- DNS Cache Proxy
- SNMP v1, v2 oraz v3
- obsługa NTP
- wbudowany serwer DHCP
- automatyczna aktualizacja serwisów i usług
- ochrona konfiguracji kluczem na USB

Monitoring, raportowanie, powiadomienia:

- powiadomienia na e-mail
- SNMP v1, v2 oraz v3
- monitor pracujący w czasie rzeczywistym
- dziennik zdarzeń (syslog)
- raportowanie historii zdarzeń
- zapisywanie niebezpiecznych pakietów (Packet Dumping)

Zarządzanie:

- konsola administracyjna pod Windows
- monitor zdarzeń pod Windows
- narzędzie raportujące pod Windows
- konsola do centralnej administracji
- Obsługa syslog, SSHv2, konsola RS-232

Dodatkowe opcje:

- SEISMO – skaner bezpieczeństwa wnętrza sieci
- Skaner antywirusowy Kaspersky AV
- Centralna konsola zarządzająca
- OPTENET URL – poszerzona klasyfikacja URL

Wymiary fizyczne:

- Wysokość – 4U
- Wysokość x szerokość x głębokość (mm) – 178x686x483
- Waga – 36 kg

Certyfikaty:

- Common Criteria EAL 2+