NETASQ

ZINTEGROWANY SYSTEM OCHRONY SIECI

U30S

U70S

U150S

U250S

U500S

U800S

W STANDARDZIE:

FIREWALL ZINTEGROWANY Z IPS | FILTR URL DEDYKOWANY NA POLSKI RYNEK | ANTYWIRUS
ZARZĄDZANIE I DWA MODUŁY RAPORTUJĄCE W JĘZYKU POLSKIM | POŁĄCZENIA VPN | SSL PROXY
POLSKIE WSPARCIE TECHNICZNE | KONTROLA APLIKACJI I URZĄDZEŃ MOBILNYCH

UTM
Unified Threat Management

SERIA US:NG
U30S | U70S | U150S | U250S | U500S | U800S | NG 1000-A | NG 5000-A

NETASQ
we secure IT

NATO, Uniwersytet Cambridge, Europejska Agencja Obrony, Sekretariat Generalny Rady Unii Europejskiej to tylko niektórzy klienci korzystający z NETASQ.

NATO OTAN

VPN, firewall oraz ochrona poczty elektronicznej spełniają normy poufności NATO

Wszystkie urządzenia NETASQ UTM zapewniają te same funkcjonalności oraz możliwości. Skuteczność produktów firmy NETASQ doceniają zarówno małe, jak i duże firmy oraz międzynarodowe korporacje i instytucje m.in. Europejski Organ Nadzoru Globalnego Systemu Nawigacji Satelitarnej, NATO, Dyrekcja ds. Personelu i Administracji Komisji Europejskiej czy Uniwersytet Cambridge.

UNIKATOWA ARCHITEKTURA SYSTEMU

Elementem wyróżniającym rozwiązania UTM firmy NETASQ jest integracja zapory sieciowej (Stateful Inspection Firewall) z modułem IPS (Intrusion Prevention System) na poziomie jądra. Tak głęboka integracja dwóch kluczowych modułów urządzeń NETASQ pozwala na uzyskanie wysokiej wydajności podczas analizy całego pakietu, a więc jego nagłówka i zawartości. W ten sposób rozwiązania NETASQ spełniają dwa najważniejsze oczekiwania klientów wobec tego typu urządzeń - skutecznie eliminują niebezpieczny ruch oraz zapewniają wysoką szybkość skanowania.

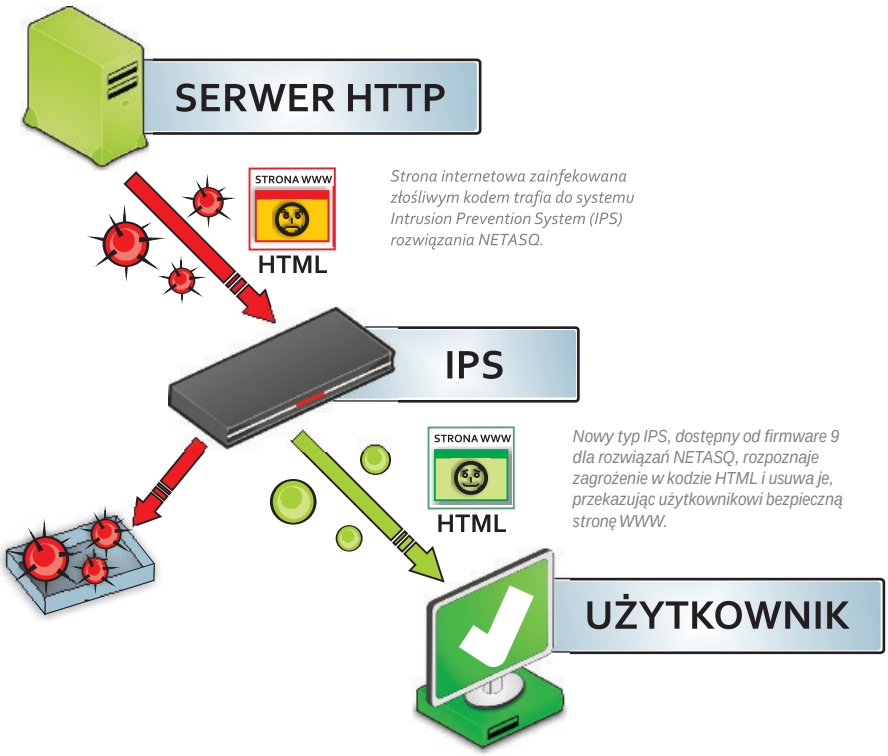
OPATENTOWANA TECHNOLOGIA WYKRYWANIA ZAGROŻEŃ

Do wykrywania i blokowania włamań rozwiązania NETASQ wykorzystują unikatową technologię Active Security Qualification (ASQ), która dzięki analizie protokołowej połączonej z zaawansowaną heurystyką pozwala na wykrywanie zagrożeń niezależnie od sygnatur (ochrona proaktywna). W ten sposób sieć jest chroniona przed najnowszymi zagrożeniami, dla których sygnatury jeszcze nie powstały, gwarantując pełną ochronę komunikacji internetowej.

OBSŁUGA KART SD

Wszystkie urządzenia NETASQ US mają możliwość bezpośredniego zapisywania logów na karty SD. Obsługiwane nośniki to standardowe karty SD oraz SDHC o maksymalnej pojemności 32 GB. Jest to szczególnie przydatne dla klientów korzystających z najmniejszych modeli U30S i U70S nie wyposażonych w dyski twarde.

JAK DZIAŁA SYSTEM IPS W NETASQ



Nowy typ IPS, dostępny w urządzeniach NETASQ, rozpoznaje zagrożenia w kodzie HTML, usuwa je i przekazuje użytkownikowi bezpieczną stronę WWW. Standardowy IPS potrafi jedynie zablokować stronę z zagrożeniem i odciąć od niej użytkownika.

KONTROLA RUCHU SZYFROWANEGO SSL

Urządzenia NETASQ pozwalają na kontrolę ruchu szyfrowanego SSL. Rozwiązanie działa jak serwer proxy SSL i umożliwia sprawdzanie ruchu HTTPS, zarówno przychodzącego, jak i wychodzącego. Sprawdzanie zakodowanych w SSL danych odbywa się po rozkodowaniu pakietu. Jeśli przesyłane informacje są bezpieczne, zapora ponownie szyfruje pakiet, podpisuje go własnym certyfikatem zgodności i przesyła dalej do użytkownika.

BEZPIECZNA KOMUNIKACJA VPN

Wszystkie urządzenia NETASQ pozwalają na szyfrowanie komunikacji pomiędzy lokalizacjami oraz zabezpieczanie zdalnego dostępu do zasobów firmy, protokołami IPSec oraz SSL. Dla klientów wymagających zabezpieczenia ciągłości komunikacji na wypadek awarii łącza, każde urządzenie wyposażono w funkcję VPN failover, dzięki której drugi tunel automatycznie zestawi się na zapasowym łączu, gwarantując nieprzerwaną komunikację.

DWA FILTRY URL

Filtr URL jest standardowym wyposażeniem każdego urządzenia NETASQ UTM. Pozwala on blokować użytkownikom dostęp do wybranych stron internetowych, w tym również do stron HTTPS. Dzięki ścisłej współpracy firmy NETASQ z polskim dystrybutorem powstał jedyny filtr URL dedykowany na polski rynek – baza filtrowanych stron internetowych została stworzona na podstawie analizy nawyków pracowników polskich firm. Filtr ten dostarcza ponad 50 kategorii tematycznych, według których klasyfikowane są strony. Jeśli jakiejś strony brakuje w klasyfikacji można ją dodać za pomocą specjalnie przygotowanej zakładki na stronie NETASQ.PL. Zgłoszona w ten sposób strona zostanie sprawdzona i dodana do 24h od zgłoszenia. Drugą opcja filtrowania jest rozszerzony filtr URL w chmurze zawierający 65 kategorii, w tym 8 skierowanych na bezpieczeństwo – razem ponad 100 mln adresów URL.

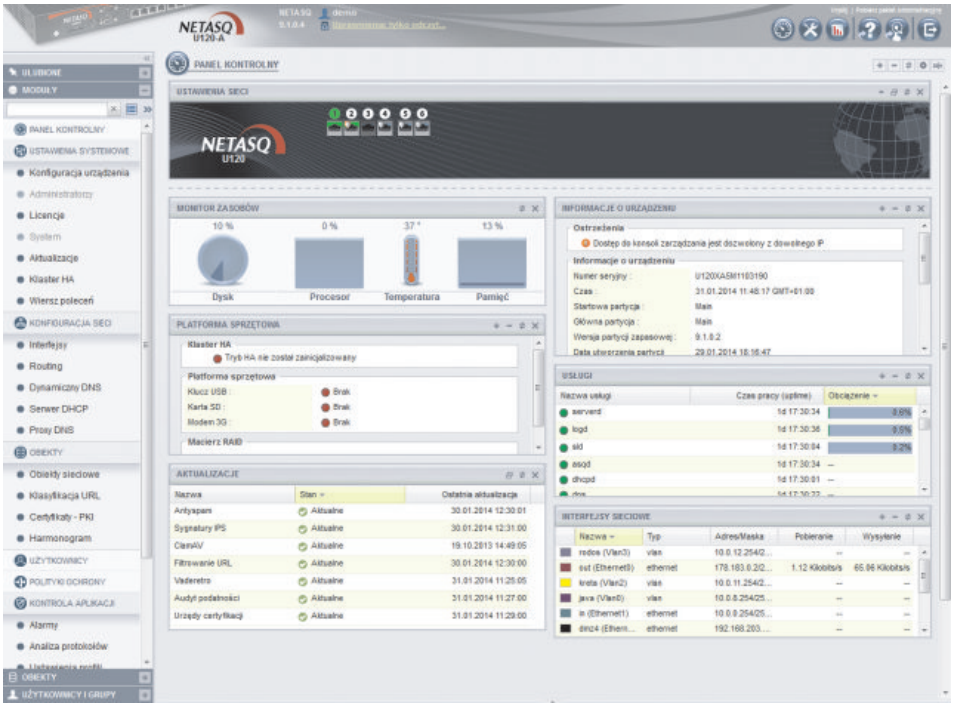
Dedykowany na polski rynek filtr URL – baza stron internetowych została stworzona na podstawie analizy nawyków pracowników polskich firm.

Dla najbardziej wymagających administratorów opcja rozszerzonego filteringu zawierająca 100 mln adresów w chmurze.

AIRBUS DEFENCE & SPACE

NETASQ należy do grupy Airbusa europejskiej korporacji zajmującej się problematyką bezpieczeństwa

NETASQ
we secure IT



Konsola zarządzająca urządzeniami NETASQ dostępna jest z poziomu przeglądarki WWW również w języku polskim. Wyświetlane treści można dowolnie organizować, ponieważ wszystkie okna, wyświetlające poszczególne funkcjonalności, mogą być przemieszczane przy zastosowaniu techniki przeciągnij i upuść. Ta sama technika pozwala na szybką konfigurację zestawu reguł dla firewalla.

NETASQ umożliwia administratorowi kontrolę wybranych aplikacji sieciowych, takich jak komunikator Skype, programy P2P, a także aplikacje dostępne w serwisie Facebook.

ZARZĄDZANIE W JĘZYKU POLSKIM

Każde urządzenie NETASQ konfigurowane jest z poziomu graficznej konsoli administracyjnej dostępnej poprzez przeglądarkę internetową. Konsolę można również obsługiwać w języku polskim za pomocą urządzeń mobilnych.

POLITYKI BEZPIECZEŃSTWA W ZALEŻNOŚCI OD UŻYTKOWNIKÓW

Dzięki możliwości integracji każdego urządzenia z bazami użytkowników Active Directory lub LDAP, każde urządzenie NETASQ umożliwia tworzenie osobnych polityk bezpieczeństwa dla poszczególnych użytkowników. Jeśli w sieci nie ma jeszcze bazy użytkowników, można ją stworzyć z wykorzystaniem rozwiązania NETASQ.

KONTROLA APLIKACJI I BYOD

Urządzenia NETASQ umożliwiają administratorowi kontrolę i zarządzanie aplikacjami sieciowymi.

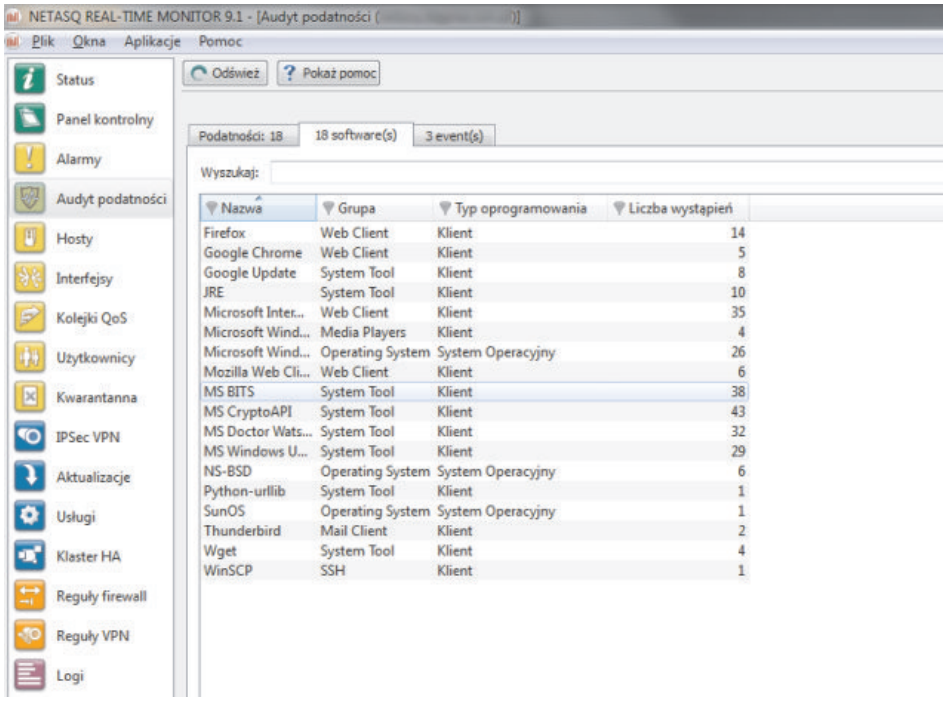
Dzięki temu możliwe jest m.in. blokowanie wybranych programów. Przykładowo, niepożądane w sieci firmowej komunikatory internetowe, takie jak Skype, czy też aplikacje obciążające łącze, np. P2P, mogą być blokowane wszystkim lub wybranym użytkownikom. Administrator ma też możliwość kontroli urządzeń mobilnych, wykorzystywanych przez pracowników (BYOD), dzięki odrębnemu modułowi do blokowania dostępu do firmowej sieci z urządzeń mobilnych, na których NETASQ automatycznie rozpoznaje oprogramowanie.

PEŁNY MONITORING SIECI

Rozwiązania NETASQ dają administratorowi możliwość pełnej kontroli chronionej sieci. Za pomocą Real Time Monitora możliwe jest kontrolowanie wszystkich zdarzeń w czasie rzeczywistym, a także śledzenie aktywności poszczególnych użytkowników sieci firmowej czy weryfikowanie ewentualnych alarmów, generowanych przez poszczególne moduły rozwiązania NETASQ.

EU RESTRICTED

Zezwolenie Rady Unii Europejskiej na ochronę informacji wrażliwych Unii za pomocą szyfrowanych sieci VPN



"Na początku podchodziliśmy z rezerwą do Audytu Podatności, ale narzędzie to bardzo szybko samo udowodniło swoją przydatność w sieci teleinformatycznej naszego urzędu i bardzo nam się spodobało."

Bogdan Gołyźniak - Powiatowy Urząd Pracy dla Powiatu Nowosądeckiego
(17 urządzeń firmy NETASQ zabezpiecza komunikację pomiędzy jednostkami powiatu).

WYKRYWANIE PODATNOŚCI

Audyt Podatności to narzędzie, które ma na celu pomóc administratorowi w kontroli aplikacji sieciowych, z których na co dzień korzystają użytkownicy sieci. Audyt Podatności pomaga także w stałym monitorowaniu wysokiego poziomu bezpieczeństwa, poprzez wykrywanie i wskazywanie nieaktualnych wersji oprogramowania, w którym wykryto luki, wrażliwości czy podatności na ataki. Audyt działa każdorazowo, gdy komputer lub serwer z sieci LAN generuje ruch, który przechodzi przez urządzenie NETASQ. Ruch taki jest sprawdzany przez firewall, a następnie przez IPS, dzięki czemu Audyt Podatności uzyskuje informacje na temat aplikacji inicjującej dany ruch. Następnie Audyt sprawdza wykrytą aplikację pod kątem wrażliwości na ataki i zagrożenia.

AUDYT PODATNOŚCI WYKRYWA SKYPE I INNE

Audyt Podatności, dostępny w NETASQ, prezentuje administratorowi szczegółową listę aplikacji sieciowych pracujących na stacjach roboczych, jak np. Google Desktop, Firefox, programy antywirusowe, itp. Kliknięcie na wskazaną przez narzędzie aplikację powoduje wyświetlenie wszystkich komputerów, na których dany program został zainstalowany, a także pozwala sprawdzić wersję konkretnej aplikacji oraz system pod jakim działa wybrana stacja.

AUDYT PODATNOŚCI - KORZYŚCI

- wykrywanie aplikacji podatnych na ataki
- kontrola aplikacji sieciowych zainstalowanych na stacjach roboczych i serwerach
- kontrola programów działających na różnych systemach operacyjnych
- podpowiadanie niezbędnych działań
- brak wpływu na wydajność systemu
- brak konieczności instalowania agentów na stacjach
- wykrywa m.in. wersje przeglądarek, klientów pocztowych, rodzaje systemów operacyjnych na stacjach roboczych

Audyt Podatności wykrywa i prezentuje szczegółową listę aplikacji sieciowych, m.in. Lotus Domino, Apple iTunes, Samba, Nessus, Apache, MySQL, Mozilla Thunderbird, Skype i wiele innych.

COMMON CRITERIA CERTIFIED EAL4+

Certyfikacja EAL4+ przyznana modułowi IPS-Firewall rozwiązań firmy NETASQ

NETASQ
we secure IT

W podstawowej cenie urządzenia NETASQ UTM administrator otrzymuje narzędzie do raportowania - Event Reporter Light.

DWA MODUŁY RAPORTUJĄCE W STANDARDZIE

W podstawowej cenie urządzenia NETASQ zawierają dostęp do zestawu podstawowych raportów z aktywności użytkowników w sieci. Jednym z nich jest dostępny z poziomu interfejsu urządzenia moduł 21 raportów typu TOP 10 tworzonych w oparciu o logi zapisywane na urządzeniu. Umożliwiają one zmianę reguł bezpośrednio na firewallu z poziomu odczytywanego raportu. Z kolei narzędzie Event Reporter Light umożliwia przeglądanie raportów nt. najczęściej przeglądanych stron internetowych (per użytkownik), najczęściej generowanych alarmów systemu IPS oraz luk w aplikacjach sieciowych. Raporty w plikach PDF i CSV dostępne są z poziomu przeglądarki WWW, a tworzone są na podstawie logów przechowywanych w bazie MySQL.

NETASQ EVENT ANALYZER

To dodatkowe narzędzie, które dostarcza komplet informacji na temat zabezpieczenia sieci, wykrytych infekcji, prób włamań do sieci, generowanego obciążenia czy identyfikacji niedozwolonych aplikacji sieciowych. Dzięki interaktywnym raportom NETASQ Event Analyzer może informować, m.in. o średnim czasie spędzonym przez pracownika na poszczególnych stronach, najczęściej wpisywanych w wyszukiwarkach frazach czy ilości pobranych danych.

PEŁNA KONTROLA SIECI

Dzięki NETASQ Event Analyzer administrator może w łatwy sposób monitorować skuteczność ustalonych polityk bezpieczeństwa i generować raporty w oparciu o 200 zdefiniowanych przez producenta wzorów. Raporty powstają na podstawie logów przechowywanych w bazie Microsoft SQL i można je udostępniać za pośrednictwem usługi RSS.

IPv6 READY

Rozwiązania firmy NETASQ zapewniają zgodność ze standardem IPv6

NETASQ VIRTUAL APPLIANCE

Rozwiązania NETASQ dostępne są zarówno w wersji sprzętowej jak i zwirtualizowanej na platformach VMware oraz Citrix. Obie wersje zapewniają chronionej sieci identycznie skuteczne zabezpieczenie.

Zarówno wersja sprzętowa, jak i wirtualna (Virtual Appliance) mogą być administrowane z poziomu jednej konsoli, umożliwiającej przenoszenie konfiguracji pomiędzy tymi wersjami. NETASQ Virtual Appliance obsługuje następujące wersje platform wirtualnych:

- VMware VSphere 4.0,4.1, 5.0, 5.1 oraz 5.5
- Citrix XenServer 5.0, 5.5, 5.6, 6.0, 6.1 oraz 6.2

NETASQ Virtual Appliance to identyczne rozwiązanie jak wersja sprzętowa NETASQ UTM. Zapewnia skuteczną ochronę zarówno pomiędzy maszynami wirtualnymi, jak i w fizycznej części sieci.

NETASQ SERIA VS 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	1 000	1 000	10 000
Jednoczesna liczba klientów SSL VPN	50	256	512	512	2 048

NETASQ SERIA VS do ochrony serwerów

GŁÓWNE CECHY	VS5	VS10
Ilość chronionych maszyn wirtualnych	5	10
Audyt Podatności	TAK	TAK
Jednoczesne połączenia	1 000 000	2 000 000
802.1Q VLAN (max)	512	512
Tunele IPSEC VPN (max)	10 000	10 000
Jednoczesna liczba klientów SSL VPN	2.048	2.048

Pozostałe certyfikaty uzyskane przez NETASQ

AUTORYZOWANE CENTRUM POMOCY TECHNICZNEJ

Użytkownicy rozwiązań firmy NETASQ mogą bezpłatnie korzystać z pomocy technicznej w języku polskim. Pomoc świadczą wykwalifikowani inżynierowie techniczni, z którymi można kontaktować się w dni robocze, w godzinach 8-18, telefonicznie 32 259 11 89 lub pisząc na adres pomoc@netasq.pl.

AUTORYZOWANE CENTRUM SZKOLENIOWE

O specyfice i możliwościach rozwiązań NETASQ można dowiedzieć się podczas szkoleń organizowanych przez Autoryzowane Centrum Szkoleniowe DAGMA. Wszystkie szkolenia prowadzone są metodami warsztatowymi przez doświadczonych trenerów. Ich kwalifikacje potwierdzają liczne certyfikacje przyznane przez firmę NETASQ. Dzięki dużemu naciskowi położonemu na część praktyczną, uczestnicy szkoleń bardzo szybko zdobywają nowe umiejętności obsługi rozwiązań NETASQ.

O FIRMIE NETASQ

Firma NETASQ zostala zalozona w 1998r. i obecnie jest europejskim liderem wsród dostawców rozwiazan bezpieczenstwa IT dedykowanych dla firm. NETASQ nalezy do grupy Cassidian CyberSecurity, która jest czescia koncernu EADS - wlasciciela Eurocoptera i Airbusa. NETASQ oferuje rozwiazania klasy Unified Threat Management (UTM), które potrafia nie tylko blokowac niebezpieczny ruch, ale równiez usuwac szkodliwa zawartosc z kodu HTML i dostarczac uzytkownikowi bezpieczna witryne. Rozwiazania NETASQ chronia przed zagrozeniami oraz spamem, a takze umozliwiaja zdalna komunikacje za pomoca bezpiecznych tuneli VPN. Pozwalaja na filtrowanie stron internetowych oraz zarzadzanie pasmem (QoS). Produkty NETASQ posiadaja w standardzie rozszerzony filtr URL zawierajacy klasyfikacje stron w okolo 50 kategoriach tematycznych, ze szczególnym naciskiem na polskie serwisy internetowe. Dodatkowo male i srednie firmy moga korzystac z narzedzia do raportowania w jezyku polskim, dostepnego w podstawowej cenie urzadzenia.

SPECYFIKACJA URZĄDZEŃ NETASQ UTM DLA v.9.1

PARAMETRY	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
Przepustowość firewalla z włączonym IPS	400 Mb/s	800 Mb/s	1 Gb/s	1,8 Gb/s	2,4 Gb/s	3,5 Gb/s	10,8 Gbp/s	17,5 Gbps
Przepustowość IPSec VPN AES	100 Mb/s	200 Mb/s	250 Mb/s	350 Mb/s	450 Mb/s	550 Mb/s	1,5 Gb/s	3 Gb/s
Liczba portów 10/100/1000	5*	8	8	12	12	12	8-14	16-22
Interfejsy światłowodowe	-	-	-	-	opcja	opcja	opcja	opcja
Równoległe sesje	75 000	150 000	250 000	600 000	1 200 000	1 500 000	1 200 000	3 000 000
Nowe sesje/sekundę	5 000	8 000	10 000	12 000	16 000	22 000	75 000	100 000
Nielimitowana liczba użytkowników	✓	✓	✓	✓	✓	✓	✓	✓
SPECYFIKACJA SIECIOWA	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
VLAN 802.1Q	64	64	256	512	512	512	256	512
Liczba tuneli IPSec VPN	50	100	500	1 000	1 000	2 000	5 000	10 000
Liczba tuneli SSL VPN	20	50	75	150	300	500	1 024	2 048
Policy Routing	✓	✓	✓	✓	✓	✓	✓	✓
FIREWALL - IPS/IDS	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
ASQ - system zapobiegania włamaniom	✓	✓	✓	✓	✓	✓	✓	✓
Analiza protokołów	✓	✓	✓	✓	✓	✓	✓	✓
Sygnatury kontekstowe	✓	✓	✓	✓	✓	✓	✓	✓
Wykrywanie i monitoring aplikacji	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona VoIP	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona ruchu SSL	✓	✓	✓	✓	✓	✓	✓	✓
Audyt podatności	opcja	opcja	opcja	opcja	opcja	opcja	opcja	opcja
ANTYWIRUS - ANTYSPAM	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
Wbudowany antywirus (ClamAV)	✓	✓	✓	✓	✓	✓	✓	✓
Kaspersky AV	opcja	opcja	opcja	opcja	opcja	opcja	opcja	opcja
Ochrona dla SMTP, POP3, HTTP, FTP	✓	✓	✓	✓	✓	✓	✓	✓
Analiza w oparciu o serwery DNS RBL	✓	✓	✓	✓	✓	✓	✓	✓
Analiza heurystyczna	✓	✓	✓	✓	✓	✓	✓	✓
FILTROWANIE URL	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
Liczba kategorii tematycznych dedykowanych dla Polski	50+	50+	50+	50+	50+	50+	50+	50+
Opcjonalny URL filtering w chmurze	65	65	65	65	65	65	65	65
UŻYTKOWNICY	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
LDAP (wewnętrzny lub zewnętrzny), Active Directory	✓	✓	✓	✓	✓	✓	✓	✓
Transparentne uwierzytelnianie	✓	✓	✓	✓	✓	✓	✓	✓
Integracja z PKI	✓	✓	✓	✓	✓	✓	✓	✓
ZAPEWNIENIE CIĄGŁOŚCI PRACY	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
Praca w klastrze (High Availability)	-	✓	✓	✓	✓	✓	✓	✓
Zapasowa partycja systemowa	✓	✓	✓	✓	✓	✓	✓	✓
Redundantna macierz dyskowa (RAID)	-	-	-	-	-	-	opcja	✓
Redundantne zasilanie sieciowe	-	-	-	-	-	-	✓	✓
Wykrywanie awarii sprzętu w klastrze HA	-	< 1 sekundy	< 1 sekundy	< 1 sekundy	< 1 sekundy	< 1 sekundy	< 1 sekundy	< 1 sekundy
Synchronizacja sesji w klastrze HA	-	✓	✓	✓	✓	✓	✓	✓
RAPORTOWANIE	U30S	U70S	U150S	U250S	U500S	U800S	NG 1000-A	NG 5000-A
Dysk twardy	-	-	120 GB	120 GB	120 GB	120 GB	70GB	70GB
Obsługa kart SD	opcja	opcja	opcja	opcja	opcja	opcja	-	-
Syslog	✓	✓	✓	✓	✓	✓	✓	✓
Klient SNMP (v1-3, DES-AES)	✓	✓	✓	✓	✓	✓	✓	✓

* w tym dwa dwuportowe switche

www.netasq.pl

Dystrybucja w Polsce: DAGMA Biuro Bezpieczenstwa IT, ul. Bazantów 4/2, 40-668 Katowice, tel. 32 793 11 00, faks 32 793 11 90, www.dagma.com.pl