

Firewall, IPS, VPN, QoS, SEISMO
Antywirus, Filtr URL, Antyspam



UTM

Unified Threat Management



NOWY STANDARD SZYBKOŚCI

							
U30	U70	U120	U250	U450	U1100	U1500	U6000
200 Mbps	600 Mbps	700 Mbps	850 Mbps	1.000 Mbps	2.800 Mbps	3.800 Mbps	5.000 Mbps
50.000 liczba sesji równoległych	100.000 liczba sesji równoległych	200.000 liczba sesji równoległych	400.000 liczba sesji równoległych	600.000 liczba sesji równoległych	800.000 liczba sesji równoległych	1.200.000 liczba sesji równoległych	2.500.000 liczba sesji równoległych

Zarządzanie

Administracja urządzeniami NETASQ odbywa się z konsoli graficznej dostępnej z poziomu systemu Windows (Administration Suite). Uprawnienia do podglądu i konfiguracji wszystkich lub tylko wybranych modułów mogą zostać przydzielone dowolnej liczbie administratorów. Możliwe jest skorzystanie z monitora śledzącego pracę systemu w czasie rzeczywistym oraz narzędzia, służącego do gromadzenia i przeglądania logów, na podstawie których możliwe jest wygenerowanie szczegółowych raportów z pracy urządzenia oraz zdarzeń w sieci. Sporym ułatwieniem w administracji sieciami rozproszonymi w różnych lokalizacjach jest możliwość centralnego zarządzania urządzeniami NETASQ. Konsola do centralnego zarządzania - Global Administration umożliwia zarządzanie maksymalnie 5 urządzeniami w ramach podstawowej licencji. W wypadku bardziej rozbudowanych sieci konsolę należy zakupić osobno.

Firewall

UTM NETASQ wyposażony jest w wysokiej klasy stateful inspection firewall, który dzięki analizatorowi reguł jest wyjątkowo prosty w konfiguracji. Zadaniem analizatora reguł jest wychwylenie wszystkich błędów i sprzeczności logicznych podczas tworzenia nowych reguł sprawiając tym samym, że ich zdefiniowanie jest wyjątkowo proste, a same reguły są zawsze poprawne.

NETASQ umożliwia stworzenie harmonogramów, które pozwalają określić m.in. w jakich godzinach lub dniach tygodnia dany ruch powinien być przez firewall przepuszczany lub blokowany. Przykładem wykorzystania funkcji harmonogramu jest blokowanie w godzinach pracy dostępu do stron internetowych umożliwiających zakupy on-line i automatyczne odblokowywanie ich po zakończeniu pracy. Harmonogram może być stosowany zarówno dla zbioru reguł na firewallu, do filtra URL jak i do VPN lub do translacji adresów (NAT).

Intrusion Prevention System (IPS)

IPS to najważniejszy moduł urządzeń NETASQ, który odpowiada za wykrywanie i blokowanie ataków na sieć firmową. W urządzeniach NETASQ Intrusion Prevention System wykorzystuje unikalną, stworzoną w laboratoriach firmy NETASQ, technologię wykrywania i blokowania ataków ASQ (Active Security Qualification). ASQ bazuje na trzech podstawowych metodach: analizie protokołów, analizie heurystycznej oraz sygnaturach kontekstowych. Analizie w poszukiwaniu zagrożeń i ataków poddawany jest cały ruch sieciowy od trzeciej do siódmej warstwy modelu OSI. Dodatkowo, dzięki zastosowaniu technologii ASQ, moduł IPS zapewnia skuteczną ochronę nie tylko przed znanymi już zagrożeniami, ale również przed tymi, które pojawią się w przyszłości (tzw. ochrona proaktywna).

SEISMO – wewnętrzny audyt sieci

Uzupełnieniem proaktywnej ochrony realizowanej w oparciu o system IPS jest SEISMO - moduł skanujący wnętrze sieci w poszukiwaniu jej słabych punktów oraz potencjalnych zagrożeń. SEISMO umożliwia administratorowi zidentyfikowanie słabych punktów sieci firmowej poprzez wyszukiwanie nieaktualnych wersji oprogramowania na stacjach roboczych i wykrywanie niedozwolonego typu ruchu wewnątrz sieci. W przypadku zidentyfikowania nieprawidłowości SEISMO automatycznie informuje o nich administratora, wskazując równocześnie zagrożone stacje i sugerując źródła, z których należy pobrać odpowiednie poprawki likwidujące wykryte luki.

VPN - wirtualne sieci prywatne

Urządzenia NETASQ posiadają wbudowany serwer VPN, który umożliwia tworzenie bezpiecznych połączeń tzw. kanałów VPN.

Kanały te mogą być tworzone pomiędzy użytkownikami pracującymi w terenie, a siedzibą firmy (połączenia client-to-site) lub pomiędzy centralą firmy, a jej oddziałami (połączenia site-to-site).

Kanały VPN budowane są w oparciu o protokół IPSec lub SSL i mogą być szyfrowane z wykorzystaniem algorytmów DES, 3DES lub AES. Dostępność kanałów VPN może być ściśle nadzorowana w czasie - administrator systemu decyduje, w jakie dni i w jakich godzinach możliwe jest otwarcie wybranego kanału VPN.

Autoryzacja użytkowników

Dzięki obsłudze baz użytkowników każde urządzenie NETASQ umożliwia zdefiniowanie polityk bezpieczeństwa dla każdego użytkownika z osobna. Jeśli w sieci jest już taka baza to istnieje możliwość integracji urządzenia z serwerem LDAP lub AD (Active Directory). Jeśli takiej bazy nie ma można ją stworzyć na każdym urządzeniu. NETASQ współpracuje również z bazami RADIUS, Kerberos oraz NTLM Server.

Ochrona antywirusowa

Urządzenia NETASQ posiadają wbudowany system ochrony antywirusowej ClamAV, który sprawdza pocztę przychodzącą i wychodzącą (protokoły POP3 i SMTP). Wiadomości zawierające wirusy są automatycznie usuwane, a o zdarzeniu powiadamiany jest odbiorca poczty. Pod kątem obecności wirusów sprawdzane są także wszystkie strony internetowe odwiedzane przez użytkowników oraz zbiory pobierane z Internetu (ruch HTTP) oraz ruch FTP (od wersji firmware 8). Filtr antywirusowy może pracować w trybie proxy lub bridge. W przypadku zastosowania trybu bridge ochrona antywirusowa jest "przezroczysta" dla ruchu sieciowego i nie wymaga wprowadzania żadnych zmian w konfiguracji sieci. Jako opcja dostępny jest skaner antywirusowy Kaspersky AV.

Ochrona przed spamem

Wszystkie urządzenia NETASQ wykorzystują technologię wykrywania spamu firmy Vade Retro, która integruje w sobie metodę heurystyczną z analizą Bayesa. W skład technologii Vade Retro wchodzi 7 podstawowych metod:

- analiza z wykorzystaniem reguł empirycznych,
- analiza semantyczna,
- reguły reakcji zwrotnej (counter-reaction),
- analiza kodu HTML,
- analiza zestawów znaków,
- wykrywanie scamu,
- analiza raportów o braku możliwości dostarczenia poczty.

Ochrona przed spamem zapewniana jest również poprzez wbudowany w urządzenie system DNS Blacklisting, znany jako RBL (Real Time Blackhole). System ten umożliwia blokowanie spamu bezpośrednio u źródła, dzięki stale aktualizowanej liście serwerów rozsyłających spam. Administrator może tworzyć własne białe i czarne listy domen.

Wiadomości, które zostaną sklasyfikowane jako spam mogą zostać oznaczone poprzez dołączenie stosowanego ciągu znaków w temacie maila (np. SPAMx, gdzie x oznacza poziom ufności od 1 do 3 z jakim dana wiadomość została rozpoznana jako spam). Najnowszy firmware 8 dla urządzeń NETASQ umożliwia również blokowanie niechcianych wiadomości.

Filtr URL

Wszystkie urządzenia NETASQ wyposażono we własny moduł filtrowania stron internetowych, którego lista stron może być dowolnie modyfikowana przez administratora. Dodatkowo filtr URL może swoim działaniem obejmować wszystkich lub wybranych użytkowników zdefiniowanych przez administratora.

Określone filtry mogą działać tylko w wyznaczonych godzinach, dzięki czemu użytkownicy mogą np. w godzinach popołudniowych mieć zapewniony szerszy dostęp do Internetu niż w czasie godzin pracy. Jako opcja dostępny jest filtr URL firmy OPTENET (dla modeli wyposażonych w twarde dyski). Istnieje także możliwość przekierowania ruchu do skanowania na zewnętrznym serwerze URL, takim jak X-Stop lub WebSense.

Monitoring i raportowanie

Każde z urządzeń firmy NETASQ pozwala na zaawansowany monitoring oraz kontrolę sieci firmowej bez dodatkowych opłat. Już w podstawowej cenie urządzenia, administrator otrzymuje dostęp do monitora śledzącego pracę systemu w czasie rzeczywistym - Real Time Monitor. W konsoli tej możliwe jest sprawdzenie m.in. jakie w danym momencie alarmy generuje IPS, który użytkownik jaką stronę przegląda, czy też kto otrzymuje najwięcej wiadomości spamowych. Do sprawdzania historii zdarzeń w sieci służy konsola NETASQ Event Reporter, która umożliwi przeglądanie logów oraz generowanie raportów. Logi przechowywane są w bazie danych (PostgreSQL) dzięki czemu administrator może tworzyć raporty w zależności od tego jakie zdarzenia, użytkownicy oraz jaki okres go interesują. Do dyspozycji administratora NETASQ oddaje gotowe, zdefiniowane raporty, które mogą być automatycznie przesyłane na wybrany serwer plików, serwer FTP lub pod wskazany przez administratora adres e-mail.

Quality of Service (QoS)

Wszystkie urządzenia wyposażone są w mechanizmy zapewniające priorytyzację ruchu sieciowego oraz zarządzanie pasmem. Istnieje możliwość przypisania do poszczególnych reguł, definiowanych na firewallu, określonego priorytetu lub przydzielenie określonemu typowi ruchu (HTTP, VoIP) minimalnej i maksymalnej szerokości pasma, jaką może on wykorzystać.

High Availability - wysoka dostępność

Wszystkie wersje urządzeń (poza U30) mogą pracować w układzie High Availability, co umożliwia skuteczne zabezpieczenie sieci na wypadek awarii jednego z urządzeń.

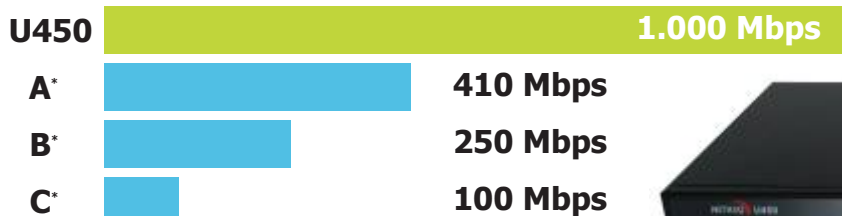
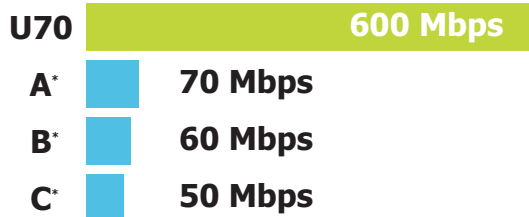
Load Balance - równoważenie obciążenia łącza

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

NETASQ UTM vs. konkurencja

Przepustowość firewalla z włączonym IPS

* A, B, C - urządzenia konkurencyjne w danej kategorii cenowej, dane na dzień 15.10.2008 wg materiałów producentów



Specyfikacja urządzeń NETASQ

PARAMETRY	U30	U70	U120	U250	U450	U1100	U1500	U6000
Przepustowość firewalla z włączonym IPS (Mbps)	200	600	700	850	1.000	2.800	3.800	5.000
Przepustowość IPsec VPN (AES) (Mbps)	80	120	160	190	225	450	600	800
Interfejsy 10/100/1000	-	6	6	6	15	8	10	6-24
Interfejsy 10/100	2	-	-	-	-	-	-	-
Sesje równoległe	50.000	100.000	200.000	400.000	600.000	800.000	1.200.000	2.500.000
Nowe sesje/sekundę	4.000	6.000	6.500	8.500	10.500	20.000	25.000	40.000
SPECYFIKACJA SIECIOWA	U30	U70	U120	U250	U450	U1100	U1500	U6000
VLAN 802.1Q	32	32	128	128	128	256	256	512
Liczba tuneli IPsec VPN	50	100	500	1.000	1.000	4.000	6.000	10.000
Liczba tuneli SSL VPN	-	50	256	512	512	1.024	1.024	2.048
Maksymalna liczba reguł filtrowania	1.000	2.000	8.000	8.000	8.000	16.000	16.000	32.000
Liczba równoległych połączeń PPTP	48	48	96	96	96	192	192	192
Obsługa redundantnych łączy WAN	4	4	8	8	8	12	12	12
Policy Routing	✓	✓	✓	✓	✓	✓	✓	✓
FIREWALL - IPS	U30	U70	U120	U250	U450	U1100	U1500	U6000
System zapobiegania włamaniom ASQ	✓	✓	✓	✓	✓	✓	✓	✓
Analiza protokołów	✓	✓	✓	✓	✓	✓	✓	✓
Sygnatury kontekstowe	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona VoIP	✓	✓	✓	✓	✓	✓	✓	✓
SEISMO - wewnętrzny audyt sieci	opcja	opcja	opcja	opcja	opcja	opcja	opcja	opcja
ANTYWIRUS - ANTYSZPAM	U30	U70	U120	U250	U450	U1100	U1500	U6000
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	U30	U70	U120	U250	U450	U1100	U1500	U6000
Klasyfikacja NETASQ (15 kategorii)	✓	✓	✓	✓	✓	✓	✓	✓
Klasyfikacja Optenet (>50 kategorii)	-	-	opcja	opcja	opcja	opcja	opcja	opcja
UŻYTKOWNICY	U30	U70	U120	U250	U450	U1100	U1500	U6000
LDAP (wewnętrzny lub zewnętrzny), Active Directory	✓	✓	✓	✓	✓	✓	✓	✓
Transparentne uwierzytelnianie	✓	✓	✓	✓	✓	✓	✓	✓
Integracja z PKI	-	-	✓	✓	✓	✓	✓	✓
ZAPEWNIENIE CIĄGŁOŚCI PRACY	U30	U70	U120	U250	U450	U1100	U1500	U6000
Praca w klastrze (High Availability)	-	✓	✓	✓	✓	✓	✓	✓
Zapasowa partycja systemowa	✓	✓	✓	✓	✓	✓	✓	✓
Redundantna macierz dyskowa (RAID)	-	-	-	-	-	-	-	Power-RAID
RAPORTOWANIE	U30	U70	U120	U250	U450	U1100	U1500	U6000
Logi bezpośrednio z urządzenia	-	-	70GB	70GB	70GB	70GB	70GB	70GB
Syslog	✓	✓	✓	✓	✓	✓	✓	✓
Klient SNMP (v1-3, DES-AES)	✓	✓	✓	✓	✓	✓	✓	✓
Klient i serwer DHCP	✓	✓	✓	✓	✓	✓	✓	✓
NTP - Klient DynDNS	✓	✓	✓	✓	✓	✓	✓	✓
DNS relay oraz cache	✓	✓	✓	✓	✓	✓	✓	✓

