



antivirus

IPS

antispam

VPN

firewall

**Unified
Threat
Management**

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

F200



UTM (Unified Threat Management) NETASQ F200 jest urządzeniem integrującym w jednej obudowie wszystkie elementy niezbędne do kompletnego zabezpieczenia sieci lokalnej, odpowiednim dla dużych firm. NETASQ F200 wykorzystuje unikalną technologię ASQ (Active Security Qualification), która zapewnia skuteczną ochronę nie tylko przed znanymi już zagrożeniami, ale także tymi, które dopiero pojawiają się w przyszłości (tzw. ochrona proaktywna lub zero-day threat protection). Zastosowanie technologii ASQ pozwala uzyskać bardzo wysoki stopień bezpieczeństwa przy zachowaniu niespotykanej w innych urządzeniach UTM szybkości działania.

Firewall. NETASQ F200 wyposażony jest w wysokiej klasy stateful inspection firewall. Dzięki intuicyjnej konsoli konfiguracyjnej oraz analizatorowi reguł pozwalającemu na wychwycenie 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 (Active Security Qualification). Analizie w poszukiwaniu zagrożeń i ataków poddawany jest cały ruch sieciowy od trzeciej (Network Layer) do siódmej (Application Layer) 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 mode pozwala osiągnąć niespotykaną w innych urządzeniach UTM szybkość działania, niezależną od liczby uruchomionych serwisów czy zdefiniowanych w danym momencie reguł. Analizie w poszukiwaniu zagrożeń i ataków poddawany jest cały ruch sieciowy od trzeciej (Network Layer) do siódmej (Application Layer) warstwy modelu OSI. Stosowane są trzy podstawowe metody: analiza protokołów, analiza heurystyczna oraz sygnatury kontekstowe.

Virtual Private Networks (VPN). Urządzenie posiada wbudowany serwer VPN, pozwalający na tworzenie bezpiecznych połączeń, tzw. kanałów VPN. Kanały VPN mogą być tworzone pomiędzy użytkownikami pracującymi w terenie (tzw. zdalnymi użytkownikami), 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 i mogą być szyfrowane z wykorzystaniem algorytmów DES, 3DES lub AES. Możliwe jest otwarcie kanałów VPN client-to-site z wykorzystaniem protokołu SSL. Na zdalnym komputerze nie musi być wtedy zainstalowany klient VPN - do uzyskania połączenia wykorzystywana jest przeglądarka internetowa. 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.

Ochrona antywirusowa. F200 posiada wbudowany system ochrony antywirusowej ClamAV. Na obecność wirusów sprawdzana jest cała poczta przychodząca i wychodząca (protokoły POP3 oraz SMTP). Wiadomości zawierające wirusy są automatycznie usuwane, a o zdarzeniu powiadamiany jest odbiorca poczty. Na obecność wirusów sprawdzane są też wszystkie odwiedzane przez użytkowników strony internetowe oraz zbiory pobierane z Internetu (ruch HTTP). Dodatkowo, opcjonalnie dostępny jest skaner antywirusowy Kaspersky AV. Filtr ochrony antywirusowej może pracować w trybie proxy mode lub bridge mode. W przypadku zastosowania trybu bridge mode ochrona antywirusowa jest „przezroczysta” dla ruchu sieciowego i nie wymaga żadnych zmian w konfiguracji sieci.



antivirus

IPS

antispam

VPN

firewall

**Unified
Threat
Management**

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 F200 dodatkowo stosowane są także heurystyczne metody antyspamowe oraz analiza Bayesianska.

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. Dodatkowo 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 w modelu F200 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) minimalna i maksymalna szerokość pasma, jaką może on wykorzystać.

Load Balance/High Availability. NETASQ F200 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. Istnieje możliwość podłączenia drugiego urządzenia High Availability.

Podstawowe informacje

- wydajność firewall wraz z modułem IPS (ASQ) - 192 Mbps
- wydajność kanału VPN szyfrowanego AES - 33 Mbps
- liczba jednoczesnych połączeń TCP - 65.000
- maksymalna liczba reguł filtrujących - 4.096
- maksymalna liczba kanałów VPN IPSec - 1.000
- liczba portów routowalnych 10/100 Mbps - 4
- pamięć - 40 GB HDD
- liczba portów szeregowy RS-232 C - 1
- port USB - 1
- nieograniczona liczba użytkowników

Funkcje sieciowe oraz filtrowanie

- tryb pracy routera, bridge'a (transparentny) lub hybrydowy
- routing per interface
- obsługa do 64 VLAN-ów
- wbudowany Dialup router (PPTP, PPPoE, PPP)
- translacja adresów (NAT, 1 to PAT, PAT i Split)
- harmonogram czasowy dla reguł
- analizator spójności reguł (dla NAT, reguły firewalla, URL)
- xDSL High Availability oraz Load Balance
- obsługa do 8 modemów xDSL lub Dialup
- dynamiczne zarządzanie pasmem
- priorytyzacja ruchu sieciowego (QoS)
- obsługa aliasów adresów IP

Wykrywanie włamań i ataków (IPS)

- 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 nieznanych 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
- ochrona przed skanowaniem podatności systemu (vulnerability scanning)

Kanały VPN

- obsługa protokołów IPSec oraz PPTP
- możliwość otwarcia do 1.000 kanałów VPN IPSec
- możliwość otwarcia do 32 kanałów VPN PPTP
- szyfrowanie kanałów algorytmem DES, 3 DES lub AES, CAST128 oraz Blowfish
- ESP
- 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 SSL
- VPN SSL Web Mode oraz Full Mode
- NAT-Traversal (UDP 500 oraz 4500)

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
- filtr bayesianski

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 ICAP dla filtrowania URL
- 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 dla 5 urządzeń
- syslog, SSHv2, konsola RS-232

Dodatkowe opcje

- Kaspersky AV
- centralna konsola zarządzająca (wersja nielimitowana)
- OPTENET URL

Wymiary fizyczne

- waga - 5 kg
- szerokość x głębokość x wysokość (mm) - 450 x 231 x 44

Certyfikaty

- Common Criteria EAL 2+
- ICASA Labs