Link do produktu: https://sklep.ps.com.pl/firewall-usgflex700-eu0102f-12gbe-2xsfp-2xusb-1y-utm-bundle-p-238659.html

Firewall USGFLEX700-EU0102F 12GbE 2xSFP 2xUSB 1Y UTM Bundle

Cena brutto	**8 264,99 zł**
Cena netto	**6 719,50 zł**
Numer katalogowy	**NUZYXBFPLB00032**
Kod producenta	**USGFLEX700-EU0102F**
Kod EAN	**4718937614851**
Kolor (wyliczeniowy)	**Szary**
Wymiary	**Szerokość produktu 430 mm Głębokość produktu 250 mm Wysokość produktu 44 mm**
Porty we/wy (sieciówka drobna)	**2 x SFP**
Przepustowość VPN	**1100**
Funkcje (zapory sieciowe)	**Firewall**
Filtrowanie danych	**Ochrona Szyfrowanie / bezpieczeństwo HTTPS,IPSec,SSL/TLS Obsługuje VPN IKEv2, IPSec, SSL, L2TP/IPSec**
Uwaga	**CE+WEEE**
Pozostałe parametry	**Praca Emisja ciepła 120,1 BTU/h Certyfikaty FCC 15 (A), CE EMC (A), C-Tick (A), BSMI Łączność Technologia łączności Przewodowa Ilość portów USB 3.2 Gen 1 (3.1 Gen 1) Typu-A 2 Ilość portów Ethernet LAN (RJ-45) 12 Prędkość transferu danych przez E**
Waga	**4.8**
Maks. ilość sesji	**1600000**
Przepustowość zapory	**5400**
Funkcje VPN	**Sieć komputerowa Liczba tuneli vpn 500 Liczba użytkowników 150 użyt. Liczba VLANs 128**
Gwarancja	**12 mc.**

Opis produktu

Zaawansowana ochrona przed ewoluującymi zagrożeniami

- Dzisiejsze cyberataki mnożą się w dużych ilościach wraz z bardziej zróżnicowanymi formami zagrożeń, w tym kradzieżą kryptowalut, złośliwym oprogramowaniem, rosnącymi wariantami oprogramowania ransomware i wieloma

innymi! Zapora ogniowa ZyWALL ATP jest wyposażona w inteligentną inteligencję w chmurze, która zapewnia bezproblemową ochronę przed wszystkimi zaawansowanymi trwałymi zagrożeniami, zapewniając najwyższą dogłębną ochronę przed przyszłymi nieznanymi atakami.

Uczenie maszynowe w chmurze

- Inteligencja Zyxel Cloud identyfikuje nieznane pliki ze wszystkich zapór ATP, gromadzi wyniki w bazie danych i zapewnia codzienną aktualizację wszystkim ATP, skutecznie przekształcając każde nowe zagrożenie w nowy element inteligencji i stale rozwijając się dzięki samorozwoju ekosystemu bezpieczeństwa, który dostosowuje się do nowych zaawansowanych ataków na cały czas.

Piaskownica

- Sandboxing to izolowane środowisko chmurowe, które zawiera nieznane pliki w celu identyfikacji nowych typów złośliwego oprogramowania, których konwencjonalny statyczny mechanizm bezpieczeństwa nie jest w stanie wykryć, zapewniając ochronę przed atakami typu zero-day.

Filtr reputacji Wywłaszczająca ochrona IP/DNS/URL

- Filtr reputacji, składający się z funkcji IP Reputation, DNS Threat Filter i URL Threat Filter, dopasowuje adresy IP/domeny/adresy URL do zawsze aktualnej bazy danych reputacji w chmurze i określa, czy adres jest wiarygodny, czy nie. Poprawia to skuteczność blokowania, ogranicza dostęp do złośliwego adresu IP/domeny/URL i blokuje dostęp z zaatakowanych źródeł, zapewniając w ten sposób szczegółową ochronę przed stale ewoluującymi cyberzagrożeniami.

Wyprzedź zagrożenia dzięki CDR

- Collaborative Detection & Response (CDR) służy do identyfikowania zagrożeń i ryzyka w bardziej złożonej organizacji pracowników, obciążenia pracą i miejsca pracy. Zapora ATP zapewnia administratorom sieci zasady bezpieczeństwa oparte na regułach. Zapory sieciowe wykrywają zagrożenie na dowolnym z podłączonych klientów, a następnie automatycznie reagują na zagrożenia cybernetyczne i zabezpieczają urządzenia na obrzeżach sieci (bezprzewodowy punkt dostępu). Jest to idealne rozwiązanie dla IT, aby sprostać wymaganiom zdecentralizowanej infrastruktury sieciowej i zapewnić automatyczną ochronę.