Link do produktu: https://sklep.ps.com.pl/firewall-atp700-eu102f-atp-12gigabit-user-2xsfp-2xusb-1y-bundle-p-238658.html



Firewall ATP700-EU102F ATP 12Gigabit User 2xSFP 2xUSB 1Y Bundle

Cena brutto	**8 268,99 zł**
Cena netto	**6 722,76 zł**
Numer katalogowy	**NUZYXBFPLB00031**
Kod producenta	**ATP700-EU0102F**
Kod EAN	**4718937610525**
Gwarancja	**12 mc.**
Funkcje (zapory sieciowe)	**Firewall**
Przepustowość zapory	**6000**
Przepustowość VPN	**1200**
Maks. ilość sesji	**1600000**
Porty we/wy (sieciówka drobna)	**2 x USB 3.0 Type A**
Waga	**3.3**
Wymiary	**Szerokość produktu - 430 mm Głębokość produktu - 250 mm Wysokość produktu - 44 mm**
Pozostałe parametry	**Zarządzanie energią Napięcie wejściowe AC 100-240 V Częstotliwość wejściowa AC 50/60 Hz Prąd wejściowy 2.5 A Maksymalne zużycie mocy 46 W Warunki zewnętrzne Zakres temperatur (eksploatacja) 0 - 40 °C Zakres temperatur (przechowywanie) -30 - 70 °**
Kolor (wyliczeniowy)	**Srebrny**

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.

Bezpieczne WiFi gwarantuje bezpieczeństwo w zdalnych miejscach pracy

- Wraz z rosnącą liczbą urządzeń priorytetem staje się równowaga między wydajnością a bezpieczeństwem. Niezależnie od tego, czy jest to urządzenie przewodowe, bezprzewodowe, czy IoT, usługa Secure WiFi służy do budowy bezpiecznego tunelu L2 dla użytkownika Work-From-Home, aby łatwo i bezpiecznie rozszerzyć środowisko pracy, tak jakbyś był w biurze z bezpieczeństwo zarówno uwierzytelniania dwuskładnikowego, jak i bezpiecznego tunelu, co zwiększa produktywność i ułatwia obsługę IT. Usługa Secure WiFi odblokowuje również maksymalną liczbę zarządzanych punktów dostępu dla zapory ATP.