Załącznik Nr 5 do zapytania ofertowego

Opis Przedmiotu Zamówienia (OPZ)
(dotyczący części I i II)

Przedmiotem zamówienia jest realizacja zadań pod nazwą:

„Wzmocnienie bezpieczeństwa poprzez zakup, wdrożenie, konfigurację oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa oraz przeprowadzenie profesjonalnego szkolenia z administrowania i zarządzania urządzeniami FortiGate dla IT".

W ramach realizacji projektu grantowego „Cyberbezpieczny Samorząd" realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021- 2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

p.t. ”Wzmocnienie poziomu bezpieczeństwa w Gminie Świętajno”

Numer naboru: FERC.02.02-CS.01-001/23

Umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0007

- **Część I** zamówienia zakup, wdrożenie, konfigurację oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa.
- **Część II** zamówienia: przeprowadzenie profesjonalnego szkolenia z administrowania i zarządzania urządzeniami FortiGate dla informatyka Urzędu.

Lp.	Nazwa zamówienia	Ilość
Część I **Zakup, wdrożenie, konfigurację oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa**		
1.	FortiSwitch-148F -48 port gwarancja 2 lata	2
2.	FortiAP 231G gwarancja 2 lata	3
3.	Urządzenia do backupu - serwer plików NAS z nośnikami danych - GOPS, SDS, Szkoła	3
4.	FortiTOken Mobile - Software one-time password tokens for iOS, Android and Windows Phone mobile devices 5 users	2
5.	UPS min 600VA dla UG oraz jednostek	27
6.	Router z zabezpieczeniem antywirusowym - GOPS, SDS	2
Część II **Profesjonalne szkolenie FortiGate**		
1.	przeprowadzenie profesjonalnego szkolenia z administrowania i zarządzania urządzeniami FortiGate dla IT	1

Szczegółowe minimalne wymagania dla zamawianych urządzeń.

Część I.1.

Nazwa		Ilość
FortiSwitch-148F -48 port		2
1.	Przełącznik sieciowy	W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. Zamawiający jest w posiadaniu rozwiązania FortiGate 60F W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem Fortigate, o następujących parametrach:
2.	Parametry fizyczne platformy	- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. - Zasilanie AC 230V. - Maksymalny pobór mocy: 60 W. - Minimalny zakres temperatury pracy: 0-40°C.
3.	Interfejsy sieciowe - wymagania minimalne	1.Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 48 porty GE RJ-45. b) 4 porty 10 GE SFP+.
4.	Zarządzanie	– Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). – Wsparcie dla SNMP w wersjach 1-3 – Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. – Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. – Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. – Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). – Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. – Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. – Automatycznie wykonywane rewizje konfiguracji.
5.	Parametry wydajnościowe	– Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. – Tablica adresów MAC o pojemności co najmniej 32k wpisów. – Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6.	Wymagane funkcje	– Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. – Obsługa Jumbo Frames. – Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). – Agregacja portów zgodna ze standardem 802.3ad. – Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. – Obsługa routingu statycznego.

		– Port-mirroring. – Uwierzytelnianie 802.1x na poziomie portu. – Uwierzytelnianie 802.1x w oparciu o adres MAC. – W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). – W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. – W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. – Obsługa protokołu sFlow.
7.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	– System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. – System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
8.		– Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: – Centralne zarządzanie konfiguracją urządzenia – Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania – Centralne zarządzanie sieciami VLAN. – Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u – Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. – Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. – Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. – Automatyczna detekcja i rekomendacje konfiguracji. – Przesyłanie logów na zewnętrzny serwer syslog. – Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. – Obsługa białych i czarnych list adresów MAC. – Wykrywanie aplikacji komunikujących się w sieci. – Musi być możliwe redundantne połączenie z elementami zarządzającymi. – W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC
9.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
10.	Wdrożenie	Zamawiający posiada infrastrukturę sieciową opartą o urządzenie FortiGate 60F. Zamawiający wymaga pełnego wdrożenia systemu bezpieczeństwa w oparciu o rozwiązanie UTM oraz Switch zarządzalny i zawiera następujące elementy: -Rejestracja oraz upgrade urządzenia - Konfiguracja VLAN - Weryfikacja działania VLAN na portach Przełącznika

		Zamawiający wymaga przeprowadzenia skanów podatnościowych przez Wykonawcę. Jeśli skany wykażą podatności wszelkiego typu Wykonawca przedstawi je zamawiającemu i wskaże sposoby na zniwelowanie źródła podatności przez Zamawiającego. Na życzenie Zamawiającego Wykonawca wykona ponownie skan pokazujący zniwelowanie zagrożenia(do 60 dni od pierwszego skanu). Do skanu podatności Wykonawca dołączy raport z działania, który potwierdzi utwardzone środowisko Zamawiającego (do oferty należy dołączyć wzór raportu). Rozwiązanie, którym Wykonawca przeprowadzi wyżej wymienione skany musi spełniać podstawowe wymagania: -Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej. -Rozwiązanie umożliwia wykonywanie skanowania za pomocą dedykowanego agenta zainstalowanego na wspieranych systemach operacyjnych oraz bezagentowo na dostępnych do skanowania urządzeniach sieciowych, przy wykorzystaniu dedykowanego narzędzia instalowanego na wspieranym systemie Windows lub linux. -Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych. -Rozwiązanie posiada narzędzie lub umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet. -Rozwiązanie umożliwia wykonanie skanowania pod kątem podatności przy wykorzystaniu wszystkich dostępnych pluginów lub tylko wybranych przez administratora.
11.	Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Część I.2.

Nazwa	Ilość
FortiAP 231G	3
Access Point	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. 1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: a. Temperatura 0–50°C, b. Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington. 3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:

	a. 2.4 GHz 802.11b/g/n, b. 5 GHz 802.11a/n/ac/ax, c. 5/6 GHz 802.11a/n/ac/ax 4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. 5. Urządzenie musi być wyposażone w moduł BLE. 6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX, 7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: a. Tunnel, b. Bridge, c. Mesh. 9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST). 11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje: a. MIMO – 2x2, b. Maksymalna przepustowość dla poszczególnych modułów radiowych: i. 574 Mbps; ii. 1201 Mbps; iii. 2401 Mbps; c. Wymagana moc nadawania: i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; ii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; iii. min. 21 dBm dla pasma 6GHz z możliwością zmiany co 1dBm; d. Wsparcie dla 802.11n 20/40Mhz HT, e. Wsparcie dla kanałów 80 i 160MHz, f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz. g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, 12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512; 13. Funkcje dodatkowe: a. OFDMA UL i DL b. Spatial Reuse (BSS Coloring) c. UL-MU-MIMO d. DL-MU-MIMO e. Enhanced Target Wake Time (TWT) f. Wbudowany analizator widma g. Wbudowane mechanizmy WIPS/WIDS
Gwarancja	Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Część I.3.

Nazwa	Ilość
Urządzenia do backupu - serwer plików NAS z nośnikami danych - GOPS, SDS, Szkoła	3
Typ urządzenia	Serwer NAS
Obudowa	Tower
Procesor	Dwurdzeniowy procesor o taktowaniu 2.6 GHz (maksymalnie 3,1 GHz z

	przyspieszeniem) osiągający w teście PassMark w lutym 2023 co najmniej 3240 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	• Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 9 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA • Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej • Wbudowany slot 1x PCIe Gen3 x2 do podłączenia dodatkowej karty sieciowej 10GbE
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 porty eSATA
Porty sieciowe	Minimum: • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Wentylator obudowy	Min. 2 wentylatory 92 mm x 92 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 100 W
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić

	darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Gwarancja	Wykonawca udzieli gwarancji: • 3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dodatkowego pakietu gwarancyjnego
Dyski (4 szt)	• Wykonawca dostarczy 4 dyski będące na liście kompatybilności serwera NAS o minimalnych parametrach: Pojemność - 8000 GB Format - 3.5" Interfejs - SATA III (6.0 Gb/s) - 1 szt. Pamięć podręczna cache - 256 MB Prędkość obrotowa 7200 obr./min Prędkość odczytu (maksymalna) 210 MB/s Niezawodność MTBF 1 000 000 godz. Dodatkowe wymagania: Technologia zapisu CMR Zwiększona odporność na drgania Rescue Services (usługi odzyskiwania danych)

Część I.4.

Nazwa	Ilość
FortiTOken Mobile - Software one-time password tokens for iOS, Android and Windows Phone mobile devices 5 users	2
Opis	Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów programowych. 1.W ramach postępowania powinno zostać dostarczonych co najmniej 5 tokenów programowych współpracujących z posiadanym przez Zamawiającego urządzeniem FortiGate, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site. 2.Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.

	3.Dla tokenów na system iOS i Android wymaga się: a) aktywacji z systemu firewall FortiGate b) generowania kodu (cyfr) co 30 lub 60 sekund, c) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), d) ochrony dostępu poprzez konfigurowalny kod PIN,

Część I.5.

Nazwa	Ilość
UPS min 600VA dla UG oraz jednostek	27
Moc (VA)	900
Moc (W)	540
Topologia UPS	Line-interactive
Kształt fali przy pracy baterii	Czysta fala sinusoidalna
Obudowa	TOWER
Faza	Jednofazowe
Nominalne napięcie wejściowe (Vac)	230
Zgodne z HID porty USB	Wymagane, minimum 1
Uruchomienie przy pracy baterii	Wymagane
Kompatybilność z aktywnym PFC	Wymagane
Zakres napięcia wejściowego (Vac)	170 ~ 270
Częstotliwość wejściowa (Hz)	50 ± 3, 60 ± 3
Rodzaj złącza wejściowego	IEC C14
Automatyczna regulacja napięcia (AVR)	Wymagane
Ochrona przed przeciążeniem	Wymagane
Liczba gniazd	6
Rodzaj gniazd	Schuko
Czas pracy przy pełnym obciążeniu (min)	1
Typowy czas transferu (ms)	4
Typowy czas ponownego ładowania (Godziny)	8
Rodzaj baterii	Hermetyczna kwasowo-ołowiowa
Panel LCD	Wymagane
Informacje na panelu LCD	Rodzaj działania, Stan zasilania, Stan baterii, Stan obciążenia, Usterka i ostrzeżenie, Pozostałe informacje, Zdarzenia i rejestr
Alarmy dźwiękowe	Wymagane
Typy alarmów dzwiękowych	Tryb baterii, Niski poziom baterii, Przeciążenie, Usterka UPS
Okres gwarancji na produkt	2 lata
Okres gwarancji na baterie	2 lata

Część I.6.

Nazwa	Ilość
Router z zabezpieczeniem antywirusowym - GOPS, SDS	2
Przeznaczenie:	xDSL
Wejście na kartę SIM:	Nie
Wi-Fi Mesh:	Tak
Tryb pracy:	Access Point, Bridge, Repeater, Router
Rodzaj urządzenia:	Router przewodowy
Przeznaczenie:	xDSL
Złącza:	1 x RJ-11, 1 x RJ-45 2.5 Gigabit (LAN/WAN), 1 x USB 2.0, 1 x USB 3.2 Gen. 1, 1 x Złącze zasilania, 3 x Złącze anteny zewnętrznej, 4 x RJ-45 10/100/1000 (LAN)
Obsługiwane standardy:	Wi-Fi 6 (802.11 a/b/g/n/ac/ax)
Częstotliwość pracy:	2.4/5 Ghz (DualBand)
Antena:	Wewnętrzna - 1 szt., Zewnętrzna - 3 szt.
Maksymalna prędkość transmisji bezprzewodowej [Mb/s]:	5665
Maksymalna prędkość transmisji bezprzewodowej w paśmie 5 GHz [Mb/s]:	4804
Maksymalna prędkość transmisji bezprzewodowej w paśmie 2.4 GHz [Mb/s]:	861
Zabezpieczenia transmisji bezprzewodowej:	WPA Enterprise, WPA-Personal, WPA2 Enterprise, WPA2-Personal, WPA3-Personal, WPS
Zarządzanie i konfiguracja:	Amazon Alexa, Aplikacja
Dodatkowe informacje:	1GB pamięci RAM, Czterordzeniowy procesor 2.0 GHz, Diody LED, Obsługa WPS, Pamięć flash: 256MB, Przycisk On/Off, Przycisk Reset
Wi-Fi Mesh:	Tak
Wejście na kartę SIM:	Nie
Router mobilny:	Nie
Ochrona:	AiProtection Pro, Blokowanie złośliwych stron, Dwukierunkowy IPS, Filtrowanie adresów MAC, Firewall, Zapobieganie i blokowanie zainfekowanych urządzeń
LAN:	IPTV, Link aggregation, Ręczne przypisanie adresu IP, Serwer DHCP, Wake on LAN
WAN:	3G/4G LTE dongle, Agregacja WAN, Android tethering, Automatyczne IP, DDNS, DMZ, DNS over TLS, Dual WAN, L2TP, Let's Encrypt, Port triggering, PPPoE, PPTP, Przekierowanie portów, Przekierowywanie NAT, Safe browsing, Statyczne IP
Sieć Wi-Fi:	Airtime fairness, Beamforming, IPv4, IPv6, Klient RADIUS, MU-MIMO, OFDMA, Sieć gościnna, UTF-8 SSID, Wireless scheduler
USB:	AiCloud, AiDisk, Bezpieczne usuwanie dysku, Download master, ext2, ext3, ext4, HFS+, NTFS, Serwer FTP, Serwer mediów, Serwer Samba, Shared Folder privileges
VPN (Virtual Private Network):	Instant Guard, Klient VPN L2TP, Klient VPN OVPN, Klient VPN PPTP, Klient VPN WireGuard, Serwer VPN IPSec, Serwer VPN OVPN, Serwer VPN WireGuard, VPN Fusion
Dołączone akcesoria:	Instrukcja szybkiej instalacji, Kabel RJ-45, Zasilacz
Gwarancja:	Nie mniej niż 24 miesiące

Część II.1.

Nazwa	Ilość osób
przeprowadzenie profesjonalnego szkolenia z administrowania i zarządzania urządzeniami FortiGate	1

dla IT	
Forma szkolenia:	Szkolenie zdalne-dlerning
Firma szkoleniowa:	Firma szkoleniowa powinna posiadać autoryzację edukacyjną firmy Fortinet w Polsce.
Prowadzący:	Certyfikowany trener Fortinet - Fortinet Certified Trainer (FCT)
Język szkolenia	polski
Plan szkolenia:	• System and Network Settings • Firewall Policies and NAT • Routing • Firewall Authentication • Fortinet Single Sign-On (FSSO) • Certificate Operations • Antivirus • Web Filtering • Intrusion Prevention and Application Control • SSL VPN • IPsec VPN • SD-WAN Configuration and Monitoring • Security Fabric • High Availability • Diagnostics and Troubleshooting
W ramach szkolenia uczestnik powinien uzyskać następujące kompetencje:	• Configure FortiGate basic networking from factory default settings • Configure and control administrator access to FortiGate • Use the GUI and CLI for administration • Control network access to configured networks using firewall policies • Apply port forwarding, source NAT, and destination NAT • Analyze a FortiGate route table • Route packets using policy-based and static routes for multi-path and load-balanced deployments • Authenticate users using firewall policies • Monitor firewall users from the FortiGate GUI • Offer Fortinet Single Sign-On (FSSO) access to network services, integrated with Microsoft Active Directory (AD) • Understand encryption functions and certificates • Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies • Configure security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites • Apply application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports • Offer an SSL VPN for secure access to your private network • Establish an IPsec VPN tunnel between two FortiGate devices • Configure static routing • Configure SD-WAN underlay, overlay, and, local breakout • Identify the characteristics of the Fortinet Security Fabric • Deploy FortiGate devices as an HA cluster for fault tolerance and high performance • Diagnose and correct common problems
Materiały szkoleniowe	Uczestnik szkolenia otrzyma autoryzowane materiały szkoleniowe Fortinet
Certyfikat ukończenia szkolenia	Uczestnik szkolenia otrzyma certyfikat potwierdzający zrealizowanie szkolenia sygnowany przez Fortinet.
Termin szkolenia	Szkolenie zostanie zrealizowane w terminie do 20.12.2024