

Załącznik nr 1b

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ) – Część 2**Szkolenia specjalistyczne z zakresu cyberbezpieczeństwa dla 3 administratorów:
FortiOS Administrator****1. Postanowienia i wymagania ogólne**

- **Przedmiot zamówienia:** Szkolenie z zakresu administracji, konfiguracji i obsługi systemów FortiGate dla pracowników Zamawiającego - FortiOS Administrator.
- **Liczba uczestników:** 3 osoby (administratorzy sieci i systemów IT). Szkolenie musi odbyć się w dwóch turach (w jednej dwóch pracowników, w drugiej jeden).
- **Forma szkolenia:** Warsztaty online.
- **Czas trwania:** Minimum 3 dni robocze.
- **Język szkolenia:** Język polski.
- **Koszty logistyczne Wykonawcy:** Cena całkowita oferty musi uwzględniać wszelkie koszty związane z realizacją zamówienia. Zamawiający nie ponosi żadnych dodatkowych kosztów.

2. Cel szkolenia

Po zakończeniu szkolenia uczestnik powinien potrafić:

- Skonfigurować podstawowe ustawienia sieciowe FortiGate od ustawień fabrycznych,
- Skonfigurować i kontrolować dostęp administratora do FortiGate,
- Korzystać z GUI i CLI do administracji,
- Opisać metody rejestracji urządzeń,
- Wyświetlać i wyszukiwać logi na FortiGate i FortiAnalyzer,
- Konfigurować polityki firewall dla IPv4,
- Stosować przekierowanie portów, NAT źródłowy i NAT docelowy,
- Analizować tablicę routingu FortiGate,
- Konfigurować routing statyczny,
- Implementować redundancję tras i równoważenie obciążenia,
- Skonfigurować zdalne serwery uwierzytelniania LDAP i RADIUS na FortiGate,
- Monitorować użytkowników firewall z poziomu GUI FortiGate,
- Wdrażać Fortinet Single Sign-On (FSSO) zintegrowany z Microsoft Active Directory (AD),
- Opisać funkcje szyfrowania i certyfikaty,
- Opisać inspekcję SSL na FortiGate,



- Konfigurować profile bezpieczeństwa neutralizujące zagrożenia i niewłaściwe użycie, w tym wirusy, torrenty i nieodpowiednie strony WWW,
- Stosować techniki kontroli aplikacji do monitorowania i kontrolowania ruchu aplikacyjnego, również na niestandardowych portach i protokołach,
- Konfigurować tunele IPsec VPN za pomocą kreatora i metodą manualną,
- Konfigurować SD-WAN i weryfikować dystrybucję ruchu,
- Rozpoznawać zadania urządzenia głównego i zapasowego w klastrze HA,
- Identyfikować różne tryby działania HA z wykorzystaniem protokołu FGCP,
- Diagnozować i korygować typowe problemy,
- Identyfikować FortiGate VM oraz FortiGate CNF w chmurze,
- Identyfikować FortiSASE oraz jego zastosowania.

3. Wymagania wobec Wykonawcy i Trenera

- Trener prowadzący szkolenie musi posiadać aktualny certyfikat inżynierski producenta na poziomie minimum FCP (Fortinet Certified Professional), FCSS (Fortinet Certified Solution Specialist) lub wykazać się równoważnymi kompetencjami, potwierdzonymi dokumentami, w szczególności w zakresie zaawansowanej znajomości konfigurowania i administrowania urządzeniami FortiGate.
Powyższe wskazanie jest konieczne i wynika, z tego iż Zamawiający posiada i eksploatuje w swoim środowisku sprzęt firmy Fortinet (urządzenia UTM oraz switchy).
- Wykonawca zobowiązany jest dostarczyć uczestnikom komplet materiałów szkoleniowych/laboratoryjnych w formie elektronicznej (np. PDF) najpóźniej w dniu rozpoczęcia szkolenia.
- Uczestnicy szkolenia otrzymają certyfikat ukończenia szkolenia sygnowany przez Fortinet.

4. Termin organizacji szkolenia

Szkolenie musi odbyć się w dwóch turach. Termin przeprowadzenia szkoleń: IV kwartał 2026r.

Terminy przeprowadzenia szkoleń będą ustalane z Wykonawcą wybranym w niniejszym postępowaniu w zakresie niniejszej Części zamówienia.

Ny Szefidli 4y (na)