

## OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ) – Część 2

na realizację zamówienia: Szkolenia specjalistyczne w zakresie FortiGate w ramach projektu pn. „Cyberbezpieczny Samorząd”

### Rozdział I – PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest świadczenie usługi polegającej na zorganizowaniu i przeprowadzeniu specjalistycznych szkoleń dla uczestników zgodnie z poniższym zestawieniem:

Lp.	Temat szkolenia	Liczba uczestników	Uczestnicy
1	FortiGate – Zaawansowana konfiguracja urządzenia	2	administratorzy IT urzędu

Szkolenia mogą być realizowane w trybie:

- online w sali narad Urzędu Miejskiego,
- online (z wykorzystaniem platformy szkoleniowej zapewnionej przez Wykonawcę lub Zamawiającego).

**Czas trwania szkolenia:** Szkolenie musi obejmować 3 dni szkoleniowe po 8 godzin każdy (łącznie 24 godziny dydaktyczne).

### Rozdział II – CEL SZKOLENIA

Celem szkolenia jest nabycie przez uczestników zaawansowanej wiedzy i umiejętności w zakresie:

- konfiguracji i administracji urządzeniami FortiGate,
- projektowania i wdrażania polityk bezpieczeństwa,
- zaawansowanej konfiguracji sieci, routingu i segmentacji,
- integracji FortiGate z usługami katalogowymi i systemami Fortinet Security Fabric,
- konfiguracji VPN (IPsec, SSL, ADVPN, VXLAN),
- diagnostyki i rozwiązywania problemów,
- konfiguracji i utrzymania klastrów HA,
- stosowania najlepszych praktyk bezpieczeństwa.

Szkolenie ma na celu podniesienie kompetencji administratorów IT oraz zwiększenie bezpieczeństwa infrastruktury sieciowej urzędu.

### Rozdział III – ZAKRES SZKOLENIA

Zakres szkolenia obejmuje zaawansowane zagadnienia administracji FortiGate, w szczególności:



## **1. Architektura urządzenia**

- Architektura sprzętowa i programowa
- Mechanizmy akceleracji (NP, CP)
- Flow-based vs Proxy-based
- Rola FortiGate w Security Fabric

## **2. VDOM – Wirtualizacja w obrębie urządzenia**

- Koncepcja Virtual Domains
- Podział zasobów i separacja konfiguracji
- Scenariusze wykorzystania VDOM
- Tryby pracy urządzenia: NAT / Transparent

## **3. Zaawansowana konfiguracja sieci i routingu**

### **3.1 Tworzenie sieci VLAN**

- Interfejsy VLAN
- Segmentacja ruchu

### **3.2 Routing dynamiczny**

- OSPF – konfiguracja, sąsiedztwo, obszary
- BGP – podstawy, polityki, filtrowanie tras

### **3.3 Policy Routing**

- Zasada działania
- Tworzenie reguł PBR

### **3.4 SD-WAN**

- Load Balancing
- Redundancja łączy internetowych
- SLA i monitorowanie jakości łączy

## **4. Uwierzytelnianie użytkowników**

- Integracja z usługami katalogowymi – FSSO
- Tworzenie reguł firewall opartych o grupy użytkowników
- Konta użytkowników gości



- Dwuskładnikowa autoryzacja – FortiToken

## **5. Identyfikacja urządzeń**

- Device Detection
- Klasyfikacja urządzeń
- Polityki oparte o typ urządzenia

## **6. Endpoint Control**

- Integracja z FortiClient
- Rejestracja urządzeń
- Wymuszanie zgodności (Compliance Enforcement)

## **7. Cooperative Security Fabric**

- Integracja urządzeń z portfolio Fortinet
- Wymiana informacji o zagrożeniach
- Automatyzacja reakcji (Automation Stitches)

## **8. Wirtualne sieci prywatne – VPN**

### **8.1 IPsec VPN**

- Site-to-site
- Client-to-site

### **8.2 VXLAN**

- Koncepcja i zastosowania
- Tworzenie tuneli VXLAN

### **8.3 ADVPN**

- Dynamiczne VPN
- Konfiguracja hub-and-spoke

## **9. Diagnostyka i rozwiązywanie problemów**

- diag debug flow
- diag sniffer packet
- Packet Capture
- Diagnostyka VPN, routingu, polityk



- Typowe błędy konfiguracyjne

## 10. Konfiguracja urządzeń do pracy w klastrze HA

### 10.1 Tryby pracy klastra

- Active-Passive
- Active-Active
- Session pickup

### 10.2 Topologia i konfiguracja

- Wymagania sprzętowe i sieciowe
- Konfiguracja HA krok po kroku
- Synchronizacja konfiguracji
- Testowanie failover i failback

## Rozdział IV – WYMAGANIA WOBEC WYKONAWCY

Wykonawca zobowiązany jest do:

1. wykazania, że w okresie ostatnich 5 lat zrealizował co najmniej 3 usługi szkoleniowe z zakresu administracji urządzeniami Fortinet,
2. wykazania, że dysponuje min. 1 trenerem z min. 5-letnim doświadczeniem w dziedzinie bezpieczeństwa IT, który:
  - zrealizował co najmniej 3 szkolenia Fortinet,
  - posiada certyfikat **Fortinet Certified Expert Cybersecurity**,
3. przygotowania materiałów szkoleniowych w formie elektronicznej (PDF),
4. zapewnienia środowiska laboratoryjnego umożliwiającego wykonywanie ćwiczeń,
5. przeprowadzenia szkolenia zgodnie z zaakceptowanym programem,
6. przygotowania ankiet ewaluacyjnych i raportu końcowego.
7. zapewnienie 1 godziny konsultacji z trenerem w okresie do 60 dni po zakończeniu szkolenia po wcześniejszym uzgodnieniu terminu konsultacji.

## Rozdział V – WYMAGANIA ORGANIZACYJNE

Po stronie Wykonawcy:

- prowadzący szkolenie,
- materiały szkoleniowe,
- certyfikaty ukończenia,

- ankiety i raport końcowy,
- środowisko labowe.

**Po stronie Zamawiającego:**

- sala narad (jeśli szkolenie realizowane lokalnie online),
- sprzęt multimedialny,
- dostęp do Internetu,
- osoba do kontaktu z Wykonawcą.

**Rozdział VI – REZULTATY SZKOLENIA**

Po zakończeniu szkolenia uczestnicy powinni:

- konfigurować i zarządzać zaawansowanymi funkcjami FortiGate,
- projektować i wdrażać polityki bezpieczeństwa,
- konfigurować i diagnozować VPN, IPS, UTM, SD-WAN,
- analizować logi i reagować na incydenty,
- stosować najlepsze praktyki bezpieczeństwa i hardeningu,
- utrzymywać stabilne i bezpieczne środowisko sieciowe.

**Rozdział VII – KRYTERIA ODBIORU**

Szkolenie zostanie uznane za wykonane prawidłowo, jeśli:

1. zostanie przeprowadzone zgodnie z programem,
2. Wykonawca dostarczy materiały i certyfikaty,
3. zostaną przeprowadzone ankiety ewaluacyjne,
4. co najmniej 80% uczestników oceni szkolenie pozytywnie,
5. raport końcowy zostanie dostarczony w terminie.

**Rozdział VIII – HARMONOGRAM**

- Termin realizacji szkolenia: **szkolenia muszą być zrealizowane do dnia 30 kwietnia 2026 roku.**
- Szkolenie dla administratorów zostanie przeprowadzone **w dwóch oddzielnych terminach**, tak aby każdy administrator mógł uczestniczyć w zajęciach bez ryzyka zakłócenia pracy urzędu.
- Podział terminów dla uczestników zostanie uzgodniony z Zamawiającym przed rozpoczęciem szkolenia.

**Pozostałe terminy:**

- Materiały szkoleniowe: **min. 3 dni przed pierwszym terminem,**
- Raport końcowy: **do 7 dni po zakończeniu szkolenia drugiej grupy.**