Załącznik Nr 1
do Zapytania ofertowego

(pieczęć wykonawcy)

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

„Zakup i dostarczenie routerów Fortigate wraz wdrożeniem i szkoleniem dla Wojewódzkiego Funduszu Ochrony Środowiska i Gospodarki Wodnej w Warszawie".

1. Zakup jednego urządzenia klasy UTM – Fortigate 100D dla Centrali WFOŚiGW w Warszawie wraz z roczną subskrypcją i serwisem obejmującymi:
   a) pomoc techniczną producenta i gwarancję z czasem reakcji 8x5,
   b) sygnatury AV, IPS, Spam, App, Web filter,
   c) nowe wersje oprogramowania,
   d) serwis AHB gwarantujący wymianę urządzenia w następny dzień roboczy (w przypadku wystąpienia awarii)
   o parametrach nie niższych niż:
   - przepustowość firewall – 2,5 Gbps,
   - maksymalna liczba jednoczesnych sesji – 3 miliony,
   - maksymalna liczna nowych sesji na sekundę - 22 tysiące,
   - przepustowość IPS – 950 Mbps,
   - przepustowość Antywirus – 300 Mbps w trybie Proxy i 650 Mbps w trybie Flow,
   - wysokość – 1U;
2. Zakup pięciu urządzeń klasy UTM – Fortigate 60D dla pięciu Wydziałów Zamiejscowych WFOŚiGW w Warszawie wraz z roczną subskrypcją obejmującą:
   a) pomoc techniczną producenta i gwarancję z czasem reakcji 8x5,
   b) sygnatury AV, IPS, Spam, App, Web filter,
   c) nowe wersje oprogramowania,
   o parametrach nie niższych niż:
   - przepustowość firewall – 1,5 Gbps,
   - maksymalna liczba jednoczesnych sesji – 500 tysięcy,
   - maksymalna liczna nowych sesji na sekundę - 4000 tysiące,
   - przepustowość IPS –200 Mbps,
   - przepustowość Antywirus – 35 Mbps w trybie Proxy i 50 Mbps w trybie Flow,
   - wysokość – 1U;
3. Wdrożenie obejmujące:
   a) przygotowanie projektu wykonawczego konfiguracji urządzeń w zakresie integracji z siecią zamawiającego oraz konfiguracji sieci, routingu, polityk, profili AV, Web filtering, VPN Site-to-Site,
   b) konfigurację sieci, routingu, polityk i profili AV i Web filtering na urządzeniach 100D oraz 60D (zgodnie z projektem wykonawczym),
   c) konfigurację VPN site-to-site pomiędzy urządzeniem 100D a urządzeniami 60D,
   d) konfigurację VPN SSL na urządzeniu 100D,
   e) doradztwo w zakresie wdrożenie i integracji urządzeń 100D oraz 60D w sieciach Zamawiającego do 15 godzin roboczych.

4. Jeden voucher na autoryzowane szkolenie Fortigate 201 gwarantujące zdobycie praktycznych umiejętności potrzebnych do samodzielnej konfiguracji podstawowych funkcjonalności dostępnych w urządzeniu FortiGate obejmujące następujące zagadnienia:
   a) Wstęp do UTM;
      - rozwiązania firmy Fortinet,
      - FortiGuard Subscription Services,
      - podstawowa konfiguracja urządzenia FortiGate
   b) Logowanie i monitoring
      - konfiguracja logowania dla zdarzeń systemowych,
      - konfiguracja protokołu Syslog i SNMP,
      - konfiguracja alertów mailowych
   c) Konfiguracja firewalla
      - zasada działania firewalla stanowego,
      - reguły uwierzytelniające użytkowników,
      - polityki bazujące na urządzeniach,
      - NAT,
      - tworzenie obiektów dla reguł zapory ogniowej,
      - ochrona przed zagrożeniami – konfiguracja UTM,
      - traffic shaping
   d) Lokalne uwierzytelnianie użytkowników
      - metody uwierzytelniania,
      - obiekty użytkowników i grup,
      - dwuskładnikowe uwierzytelnianie -- FortiToken
   e) SSL-VPN
      - koncepcja sieci VPN,
      - dostępne technologie,
      - architektura SSL VPN,
      - tryby działania SSL- VPN,
      - konfiguracja SSL-VPN
   f) IPSec-VPN
      - Architektura,
      - topologie i konfiguracja IPSec VPN,
      - tryby pracy: route-based i policy-based,
      - konfiguracja tuneli VPN
   g) Skanowanie antywirusowe
      - conserve Mode,
      - skanowanie Proxy-Based,
      - skanowanie Flow-Based,
      - kwarantanna,
      - globalne ustawienia modułu AV
   h) Filtracja Antyspamowa
      - metody filtrowania spamu,
      - FortiGuard Email Filtering,
      - obsługa nagłówków MIME,
      - konfiguracja czarnych i białych list,
      - DNS Blackholling i Open Relay Database
   i) Filtr stron WWW
      - metody filtrowania stron WWW,
      - kolejność filtrowania,
      - konfiguracja lokalnego filtra stron WWW,
      - filtrowanie po zawartości stron,
      - FortiGuard Web Filtering - filtrowanie po kategoriach tematycznych

j) Kontrola aplikacji
- zasada działania i możliwości,
- konfiguracja listy kontrolowanych aplikacji

5. Jeden voucher na autoryzowane szkolenie Fortigate 301 gwarantujące zdobycie wiedzy i nabycie praktycznych umiejętności potrzebnych do implementacji rozwiązań bezpieczeństwa w sieciach o różnych topologiach i rozmiarach

a) Konfiguracja Routingu
- routing statyczny,
- Policy Routing,
- Blackhole Routes,
- Reverse Path Forwarding – RPF,
- routing dynamiczny (RIP, OSPF, BGP, ISIS),
- diagnostyka

b) Wirtualne Sieci Lokalne (VLAN) oraz Wirtualne domeny (VDOM)
- tworzenie VLAN-ów na urządzeniu Fortigate,
- konfiguracja VDOM'ów,
- połączenia typu Inter-VDOM

c) Transparentny tryb pracy urządzenia
- różnice pomiędzy trybem pracy NAT/Route i Transparent,
- VLAN-y w trybie transparentnym,
- domeny broadcastowe,
- port pairing,
- Spanning Tree Protocol i agregacji łączy

d) High Availability
- tryby pracy klastra Active-Pasive oraz Active-Active,
- konfiguracja HA Master,
- konfiguracja HA Slave,
- zasada działania klastra,
- failover,
- konfiguracja wirtualnych klastrów - Virtual Clusters

e) Zaawansowana konfiguracja IPSec VPN
- architektura, topologie i konfiguracja IPSec VPN,
- konfiguracja tuneli redundantnych,
- monitorowanie i debuggowanie połączeń VPN

f) Intrusion Prevention System – IPS
- możliwości systemu IPS dostępne na urządzeniu FortiGate,
- tworzenie własnych sygnatur IPS,
- konfiguracja sensora IPS,
- konfiguracja sensora DOS

g) FSSO - Fortinet Single Sign On
- zaawansowane uwierzytelnianie użytkowników,
- współpraca z Windows Active Directory,
- Fortinet Single Sign On,
- tryby pracy FSSO

h) Operacje oparte na certyfikatach
- wprowadzenie do kryptografii,
- zarządzanie certyfikatami na urządzeniu Fortigate,
- SSL Content Inspection

i) Zaawansowana konfiguracja modułu Application Control
- komunikatory sieciowe,
- zaawansowane możliwości dla komunikatorów MSN, Yahoo, ICQ and AIM,
- konfiguracja polityk typu Instant Messenger,

- traffic shaping – dla aplikacji,
- monitorowanie i diagnostyka systemu FortiOS

j) Ochrona przed wyciekiem danych – DLP
- metody inspekcji DLP,
- filtrowanie po typie lub po nazwie plików,
- konfiguracja filtrów DLP,
- konfiguracja sensora DLP

k) Wszystko razem
- konfiguracja poznanych funkcjonalności według przykładowego scenariusza