Załącznik nr 1 do 1/ZO/WŁ/2026

Opis przedmiotu zamówienia

Dostawa systemu bezpieczeństwa sieci teleinformatycznej oraz infrastruktury pamięci masowej

Przedmiotem zamówienia jest dostawa elementów systemu zabezpieczeń sieci teleinformatycznej Zamawiającego oraz infrastruktury pamięci masowej, wraz z wymaganymi licencjami, subskrypcjami oraz nośnikami danych.

Zamówienie obejmuje w dostawę:

1. Rozszerzenie subskrypcji dla zapory sieciowej SonicWall NSA 2800 do wersji Advanced, obejmujące okres 36 miesięcy, wraz z zapewnieniem wsparcia producenta typu CSE (Customer Support Engineer) przez okres co najmniej 12 miesięcy.
2. Dostawę dwóch urządzeń zapory sieciowej klasy Next Generation Firewall równoważnych do SonicWall NSA 2800, skonfigurowanych w trybie wysokiej dostępności (High Availability), zapewniającym ciągłość pracy systemu w przypadku awarii jednego z urządzeń.
3. Dostawę licencji umożliwiającej jednoczesny dostęp zdalny dla co najmniej 50 użytkowników w technologii SSL VPN, zintegrowanej z dostarczonym systemem zapory sieciowej.
4. Dostawę licencji systemu ochrony punktów końcowych klasy EDR/Endpoint Protection równoważnego do SonicWall Capture Client Advanced, obejmującej 50 stanowisk roboczych, na okres 36 miesięcy.
5. Dostawa serwera plików typu NAS klasy biznesowej, równoważnego do QNAP TS-435XeU-4G, wyposażonego w minimum 16 GB pamięci RAM, przeznaczonego do pracy w szafie rack 19”.
6. Dostawa czterech dysków twardych klasy serwerowej, równoważnych do WD Red Pro, o pojemności co najmniej 8 TB każdy, przeznaczonych do pracy ciągłej w środowisku NAS.
7. Dostawa dwóch nośników półprzewodnikowych M.2 PCIe NVMe klasy enterprise, równoważnych do SanDisk Red SN700, o pojemności co najmniej 500 GB każdy, przeznaczonych do pracy jako pamięć cache.

Wymagania funkcjonalne i techniczne

Dostarczony system zabezpieczeń musi spełniać co najmniej następujące wymagania:

1. Zapora sieciowa powinna zapewniać funkcjonalność klasy Next Generation Firewall, w tym w szczególności:

- ochronę przed włamaniami (IPS/IDS),
- ochronę antywirusową i antymalware,
- kontrolę aplikacji i użytkowników,
- filtrowanie treści internetowych,
- analizę ruchu szyfrowanego SSL/TLS,
- obsługę tuneli VPN,
- zarządzanie pasmem oraz ruchem sieciowym.

2. System High Availability musi zapewniać:
   - automatyczne przełączanie pracy w przypadku awarii,
   - synchronizację konfiguracji i sesji,
   - brak konieczności ręcznej interwencji administratora przy przełączaniu,
   - możliwość monitorowania stanu pracy obu urządzeń.
3. System zdalnego dostępu SSL VPN musi:
   - umożliwiać bezpieczny dostęp do zasobów sieciowych,
   - obsługiwać jednoczesną pracę co najmniej 50 użytkowników,
   - wspierać uwierzytelnianie wieloskładnikowe,
   - integrować się z infrastrukturą katalogową Zamawiającego.
4. System ochrony punktów końcowych musi:
   - zapewniać ochronę przed zagrożeniami typu malware, ransomware i phishing,
   - umożliwiać centralne zarządzanie politykami bezpieczeństwa,
   - oferować funkcjonalność wykrywania i reagowania na incydenty (EDR),
   - umożliwiać raportowanie zdarzeń bezpieczeństwa.

Wymagania formalne

1. Oferowane rozwiązania muszą pochodzić z oficjalnej dystrybucji producenta.
2. Licencje muszą być przypisane do Zamawiającego.
3. Wsparcie producenta musi obejmować dostęp do aktualizacji oprogramowania i baz sygnatur.
4. Dopuszcza się oferowanie rozwiązań równoważnych, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych i technicznych określonych w niniejszym OPZ.

5. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowych urządzeń oraz niewykorzystywanych wcześniej licencji,
6. W przypadku zaoferowania rozwiązań równoważnych Wykonawca zobowiązany jest do wykazania ich równoważności.

Warunki realizacji dostawy

1. Dostawa zostanie zrealizowana do siedziby Zamawiającego w terminie określonym w SWZ.
2. Koszty transportu, ubezpieczenia oraz rozładunku ponosi Wykonawca.