Wzór – Załącznik Nr 9 do SWZ

SPECYFIKACJA WYKONANIA SERWEROWNI

Przedmiotem prac inwestycji pn. ***„Remont pomieszczeń budynku Gminnego Ośrodka Kultury w Smołdzinie wraz z aranżacją wnętrz"*** jest również wykonanie sieci teleinformatycznej oraz wyposażenie serwerowni w urządzenia wymienione poniżej, w tym również UTM, jako zabezpieczenie sieci lokalnej na styku z internetem.

Przewiduje się wykonanie sieci strukturalnej – komputerowej, telefonicznej oraz wydzielonego zasilania prądowego.

Założenia:

1. sieć położona ma być podtynkowo i w peszlach,
2. Internet, za pomocą światłowodu, będzie doprowadzony przez instalatorów ORANGE, jednak wykonawca ma zapewnić jego przeciągnięcie w dyskretnym korytku tak, by była możliwość wymiany, albo dołożenia innych przewodów przez operatorów w przyszłości,
3. sieć komputerowa oraz telefoniczna wykonana ma być w tej samej - 6 kategorii, z uwzględnieniem gniazd RJ45, a wszystko w celu naprzemiennego wykorzystania sieci w zależności od bieżących potrzeb pracowników GOK – telefon, komputer, drukarka,
4. we wskazanych pomieszczeniach zamontowane mają być gniazda w których należy uwzględnić podwójne gniazdo 230V oraz **2** podwójna gniazda RJ45,
5. pomieszczenie, w którym planowana jest serwerownia znajduje się w „magazynie" usytuowanym na piętrze budynku GOK,
6. urządzenia oraz inne elementu wyposażenia, które będą zainstalowane w serwerowni:
    a) szafka 15U, z zastrzeżeniem, że dopiero po wyremontowaniu owego pomieszczenia i adaptacji zgodnie z projektem, możliwe będzie doprecyzowanie ostateczne jej wielkości,
    b) switch 24 portowy, 1 Gigabit – rakowy,
    c) UTM,
    d) patch panel 24 porty - rakowy
    e) listwa zasilająca rakowa
    f) UPS – 1500 VA
    g) organizer kabli,
    h) przewody patchcordy – w zależności od potrzeb,
    i) dwie półki rakowe.
7. instalacja 230 V winna być wykonana wg następujących założeń:
    a) dla instalacji komputerowej należy wykonać przyłącze w oddzielnej szafce,
    b) instalacja zasilana ma być z oddzielnej fazy,

Zadanie współfinansowane ze środków Rządowego Funduszu Inwestycji Lokalnych

c) wykonanie instalacji winno być zrealizowane z zachowaniem obowiązujących norm i przepisów,

d) należy przewidzieć na jednym obwodzie obciążenie z uwzględnieniem nadmiarowym z uwagi na fakt, że w przyszłości mogą zaistnieć okoliczności wymuszające dołożenie urządzeń – by potem nie rozbudowywać instalacji,

e) serwerownia winna być zasilona oddzielnym zabezpieczeniem,

8. Należy uwzględnić 8 zespołów gniazd [1 gniazdo-2x230V, 2 gniazda–4xRJ45], przewiduje się, że będą one zainstalowane w pomieszczeniach oddalonych max o 30-40 m od serwerowni w zależności od sposobu i trasy prowadzenia przewodów – zatem średnio, do wyceny można przyjąć po 80 mb na jedno przyłącze, czyli po około 20 mb do jednego gniazda. Ostateczne umiejscowienie gniazd zostanie doprecyzowane w trakcie prac remontowych.

Wymagania wobec urządzenia

1. Zgodność z certyfikatami CB, CE, FCC Class A, IC, VCCI, RCM, UL, CCC
2. **Wydajność**
   a) Przepustowość firewalla
   b) Min. 7 Gbps
   c) Przepustowość VPN SSL
   d) Min. 1.2 Gbps
   e) Przepustowość IPS
   f) Min. 1,2 Gbps
   g) Przepustowość w trybie NGFW
   h) Min. 1,0 Gbps
   i) Liczba jednoczesnych połączeń
   j) Min. 6.000.000
   k) Liczba nowych połączeń/sekundę
   l) Min. 32.000
   m) Liczba licencji użytkowników
   n) Nieograniczona

3. **Interfejsy fizyczne**
   a) Pamięć masowa
   b) SSD nie mniejszy niż 64GB
   c) Interfejsy (wymienialne)
   d) 8 x GE RJ45, 1 x SFP
   e) Porty wejścia/wyjścia
   f) 2 x USB 2.0 (tył), 1 x COM (RJ45),

4. **Parametry techniczne**
   a) Dysk - SSD nie mniejszy niż 64GB
   b) Memory - Min. 4Gb DDR4
   c) Processor - Min. Dual-Core 1,5GHz

5. **Gwarancja na urządzenie – min** 3 lata

Zadanie współfinansowane ze środków Rządowego Funduszu Inwestycji Lokalnych

Wymagania wobec funkcjonalności urządzenia:

Ochrona sieci:

1. komponent musi posiadać technologię wykrycia i blokady ruchu wychodzącego, który mógłby przejąć kontrolę nad zdalnym hostem,
2. komponent Konfigurowalny IPS (Intrusion Protection System) oraz ochrona przed atakami DoS,
3. komponent musi zawierać protokoły IPsec oraz SSL musi pozwalać elastycznie tworzyć i zarządzać bezpiecznymi tunelami VPN

Ochrona poczty e-mail:

1. komponent winien posiadać,:
   a) infrastrukturę szyfrowania wiadomości e-mail, opartą na politykach skanowanie DLP w celu ochrony danych,
   b) umożliwić użytkownikom zarządzanie własną skrzynką e-mail oraz spamu oraz przeglądać logi wiadomości,
   c) warunki w pkt a) i b) nie są bezwzględnymi, choć mile widzianymi w funkcjonalności proponowanego urządzenia,
2. komponent musi mieć możliwość blokowania zainfekowanych wiadomości przed wysłaniem ich ze skrzynki pocztowej oraz musi chronić korespondencję przed nielegalnym dostępem

Ochrona Web:

1. komponent musi mieć łatwe tworzenie polityk opartych o URL oraz o wymuszenie pewnych ograniczeń związanych z czasem i treścią przeglądanych stron WWW dla poszczególnych użytkowników i grup,
2. komponent ma mieć możliwość ustawienia ograniczeń przepustowości dla niechcianych aplikacji zwiększając przy tym priorytet dla aplikacji biznesowych,
3. komponent musi pozwolić na połączenie silnika antywirusowego i urządzenia UTM dla pełnej ochrony treści WWW

Ochrona aplikacji:

1. Komponent musi dostarczyć dodatkową warstwę ochrony dla najczęściej używanych aplikacji,
2. komponent musi zapobiegać atakom typu SQL Injection, Cross-Site Scripting, Directory Traversal, manipulacji plikami Cookie

Dodatkowo licencja powinna zawierać komponent, który dostarczany jest w chmurze i zapewnia ochronę przed atakami ukierunkowanymi. Komponent musi posiadać analizę poprzez wykrywanie, blokowanie i reagowanie na nieznane zagrożenia.

Zadanie współfinansowane ze środków Rządowego Funduszu Inwestycji Lokalnych