Załącznik nr 1 do SWZ

Nr sprawy: ZP/TP/23/2024

Zamawiający:
Szpital Specjalistyczny im. A. Falkiewicza we Wrocławiu

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
DLA PROJEKTU:

„Modernizacja sieci IT razem z założeniem sieci wifi oraz zabezpieczeniem sieci informatycznej w tym: zakup urządzeń infrastruktury sieciowej."

I. Krótki opis stanu obecnego.

Szpital posiada obecnie sieć przewodową, która była instalowana wiele lat temu i wymaga modernizacji, w tym założenia sieci bezprzewodowej.

II. Opis stanu docelowego

Przedmiotem zamówienia jest modernizacja sieci IT razem z założeniem sieci wifi oraz zabezpieczeniem sieci informatycznej w tym: zakup urządzeń infrastruktury sieciowej dla Szpitala Specjalistycznego im. A. Falkiewicza we Wrocławiu.

W szczególności, w zakres zamówienia wchodzi: modernizacja istniejącej sieci LAN, zaprojektowanie, dostawa, montaż, uruchomienie sieci wifi, na terenie Szpitala Specjalistycznego im. A. Falkiewicza we Wrocławiu wraz z przeprowadzeniem szkolenia personelu IT Szpitala z obsługi wdrożonych rozwiązań sieciowych.

Cel główny projektu to dostosowanie szpitala do wymogów w zakresie przetwarzania elektronicznej dokumentacji medycznej oraz poprawa dostępności, jakości i efektywności usług świadczonych przez Szpital Specjalistyczny im. A. Falkiewicza we Wrocławiu poprzez wdrożenie nowoczesnych rozwiązań, wykorzystujących zaawansowane technologie informacyjno-komunikacyjne. Osiągnięcie celu głównego możliwe będzie dzięki zrealizowaniu działań odpowiadających na określone potrzeby pacjentów i personelu medycznego.

Stan docelowy, zostanie osiągnięty poprzez doposażenie i zmodernizowanie obecnie wykorzystywanej infrastruktury zgodnie z poniższym opisem:

1) Dokumentacja projektowa infrastruktury sieciowej pasywnej światłowodowej oraz kablowej miedzianej, urządzeń aktywnych oraz sieci bezprzewodowej wraz z usługą planowania sieci bezprzewodowej Site Survey.
2) Rozbudowa istniejącej sieci LAN okablowaniem kat. 6A o dodatkowych 75 punktów logicznych 2xRJ45 w istniejących lub nowych trasach kablowych
3) Rozbudowa istniejącej sieci LAN okablowaniem kat. 6A o dodatkowych min 83 punktów logicznych 1xRJ45 na potrzeby sieci bezprzewodowej w istniejących lub nowych trasach kablowych
4) Dostawa, instalacja oraz konfiguracja urządzeń aktywnych
5) Usługa rekonfiguracji istniejącej sieci wraz z wdrożeniem nowego zakresu VLANów, routingu oraz mechanizmów wysokiej dostępności oraz innych niezbędnych wytycznych po wykonaniu dokumentacji projektowej

III. Dokumentacja projektowa modernizacji infrastruktury sieciowej

Obowiązkiem przyszłego Wykonawcy po rozstrzygnięciu postępowania przetargowego jest przygotowanie kompletnej dokumentacji projektowej obejmującej wszystkie branże dla zadań opisanych w niniejszym OPZ z uwzględnieniem następujących wytycznych:

1) W projektach wykonawczych Wykonawca powinien wyszczególnić wszystkie niezbędne roboty budowlane i instalacyjne oraz normy branżowe), dotyczące niniejszego projektu.
2) Dokumentacja projektowa powinna umożliwiać etapową realizację prac, pozwalając w trakcie tych prac na bezpieczne użytkowanie istniejącego sprzętu informatycznego.
3) Zabezpieczenia, o których mowa w niniejszym dokumencie, powinny uwzględniać ochronę przed czynnikami losowymi oraz przed nieumyślnym i umyślnym działaniem człowieka. W dokumentacjach projektowych należy więc założyć współdziałanie systemów infrastruktury, systemów informatycznych i procedur administracyjnych.
4) Dokumentację projektową należy przygotować w 3 egzemplarzach w wersji papierowej oraz 1 wersji elektronicznej w formacie pdf i dwg.
5) Wszystkie projekty muszą być opracowywane w porozumieniu z Zamawiającym i przez niego zatwierdzone oraz pisemnie dopuszczone do realizacji.

Wymaga się zaprojektowania systemu, w którym funkcjonalność i wydajność są niezmienne przez cały okres użytkowania, oraz systemu otwartego, w którym Użytkownik może samodzielnie dokonywać podłączeń, przełączeń oraz zmian w konfiguracji bez utraty wymaganej gwarancji 25-letniej producenta okablowania.

Dokumentacja projektowa musi zawierać:

- Wytyczne oraz ustalenia z Zamawiającym,
- Założenia przyjęte przez Projektanta (koncepcje po konsultacjach z Zamawiającym),
- Opis zadań, przyjętej idei i architektury połączeń
- Opis wydajności, funkcjonalności i cech użytkowych systemu (funkcje - korzyści dla Zamawiającego)
- Opis konkretnych elementów (budowa, parametry, wymagania dot. parametrów oraz wskazówki instalacyjne),
- Zasady prowadzenia tras, mocowania kabli, budowy przepustów, promienie gięcia, zapasy kabli, etc,
- Rysunki schematyczne (poglądowe), rysunki szczegółów
- Schematy ideowe, rysunki wyposażenia szaf, podkłady z trasami i punktami końcowymi zakończeń światłowodowych.
- Oznaczenia portów i administracja – propozycja lub wg wymagań Zamawiającego,
- Procedury pomiarowe - dokładnie opisane włącznie z ustawieniem przykładowego miernika, wskazanymi do pomiarów wymaganymi normami, a w przypadku połączeń światłowodowych - wymóg pomiarów reflektometrycznych,
- Odbiór i certyfikacja wykonanej instalacji – opis wymagań,
- Alternatywne propozycje (warunki dla rozwiązań zamiennych),
- Szczegółowy opis zakresu wdrożenia urządzeń aktywnych – konfiguracja, adresacja, podział na podsieci VLAN, Routing, SSID, politykę bezpieczeństwa sieci Wifi etc.
- STWiOR - Specyfikacja Techniczna Wykonania i Odbioru Robót
- KOSZTORYS na kwotę nie wyższą niż kwota ofertowa Wykonawcy
- Specyfikację materiałową wraz z ilościami.
- Zamawiający wymaga od Wykonawcy wykonania aktualnej dokumentacji sieci komputerowej - punktów PL (punkt logiczny), dla wszystkich punktów PL istniejących

w Szpitalu, także tych nieobjętych przedmiotem niniejszego OPZ w formie plików pdf i dwg.

IV. Rozbudowa szkieletu sieci światłowodowej

Zgodnie z przygotowaną dokumentacją projektową należy na terenie Szpitala wykonać kompleksową rozbudowę instalacji okablowania światłowodowego. Przyjęto, że należy rozbudować szkielet sieci światłowodowej o min. 11 nowych budynkowych punktów dystrybucyjnych BPD połączonych w topologii gwiazdy z obecną serwerownią min. 12 włóknowym kablem światłowodowym jednomodowym. Kabel należy prowadzić w istniejących lub nowo wybudowanych trasach światłowodowych. Światłowody należy zaspawać i wykonać wymagane pomiary reflektometryczne. Należy zastosować szafy wiszące 19 cali o wymiarach min. 9U wraz z kompletnym wyposażeniem w panele światłowodowe oraz panele krosowe. Wszystkie szafy należy zasilić z lokalnych punktów zasilania na odpowiednich i niezależnych zabezpieczeniach oraz uziemić. Wszelkie pozostałe wytyczne dotyczące rozbudowy okablowania światłowodowego oraz punktów dystrybucyjnych muszą być zawarte w dokumentacji projektowej.

V. Rozbudowa istniejącej sieci LAN okablowaniem kat. 6A

Zgodnie z przygotowaną dokumentacją projektową należy na terenie Szpitala wykonać kompleksową instalację okablowania strukturalnego o minimalnej kat. 6A a okablowanie należy prowadzić w istniejących trasach kablowych lub wykonać niezbędne dobudowy nowych tras. Punkty logiczne należy wykonać natynkowo. Planuje się instalację min. 75 punktów logicznych 2 x RJ45. Wszelkie pozostałe wytyczne dotyczące rozbudowy okablowania muszą być zawarte w dokumentacji projektowej.

Należy dostosować wzornictwo i sposób prowadzenia budowanej sieci do rodzaju pomieszczeń w jakich będzie ona przebiegać.

Gniazda należy instalować w sposób nie kolidujący z wyposażeniem pomieszczenia.

Przez PL należy rozumieć punkt logiczny zawierający - 1 podwójne gniazdo logiczne – 2xRJ 45 (8P8C) kat. 6A.

Każde gniazdo PL musi być opisane na samym gnieździe i odpowiednio w szafie dystrybucyjnej.

VI. Rozbudowa istniejącej sieci LAN na potrzeby sieci bezprzewodowej WiFi okablowaniem kat. 6A

Zgodnie z przygotowaną dokumentacją projektową należy na terenie Szpitala wykonać kompleksową instalację okablowania strukturalnego o minimalnej kat. 6A, a okablowanie należy prowadzić w istniejących trasach kablowych lub wykonać niezbędne dobudowy nowych tras. Zgodnie z wstępnymi założeniami planuje się instalację min. **83** bezprzewodowych punktów dostępowych, dlatego należy wykonać min. **83** punktów logicznych 1 x RJ45. Bezprzewodowe punkty należy instalować na istniejących sufitach lub na sufitach

podwieszanych z wykorzystaniem niezbędnych elementów montażowych. Określenie ich lokalizacji nastąpi na bazie usługi Site Survey, która jest elementem dokumentacji projektowej. Wszelkie pozostałe wytyczne dotyczące rozbudowy okablowania muszą być zawarte w dokumentacji projektowej.

Należy dostosować wzornictwo i sposób prowadzenia budowanej sieci do rodzaju pomieszczeń w jakich będzie ona przebiegać.

Gniazda należy instalować w sposób nie kolidujący z wyposażeniem pomieszczenia.

Przez PL należy rozumieć punkt logiczny zawierający - 1 pojedyncze gniazdo logiczne – 1xRJ 45 (8P8C) kat. 6A.

Każde gniazdo PL musi być opisane na samym gnieździe i odpowiednio w szafie dystrybucyjnej.

VII. Urządzenia aktywne – przełączniki sieciowe min. 14 szt.

Przełącznik sieciowy
W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Zamawiający jest w posiadaniu rozwiązania "Fortigate, model FG-201F". W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem Fortigate, o następujących parametrach:

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Budżet mocy dla portów PoE min.: 370 W.
- Maksymalny pobór mocy bez budżetu dla PoE: 110 W.
- Minimalny zakres temperatury pracy: 0-40^{o}C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

- W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.

e) 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3

- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Centralne zarządzanie konfiguracją urządzenia
   - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   - Centralne zarządzanie sieciami VLAN.
   - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.

- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
- Automatyczna detekcja i rekomendacje konfiguracji.
- Przesyłanie logów na zewnętrzny serwer syslog.
- Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- Obsługa białych i czarnych list adresów MAC.
- Wykrywanie aplikacji komunikujących się w sieci.

2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy.

Wsparcie Wykonawcy obejmie pomoc techniczną, aktualizacje oprogramowania oraz wymianę uszkodzonego sprzętu.

Zakres Usługi

1. Wsparcie techniczne – Usługa obejmie wsparcie techniczne dostępne 24 godziny na dobę, 7 dni w tygodniu (24x7x365), w tym możliwość otwierania zgłoszeń przez portal, telefonicznie i online.

2. Aktualizacje oprogramowania – Zamawiający otrzyma dostęp do aktualizacji oprogramowania, w tym nowych funkcji oraz poprawek. Wykonawca udzieli Zamawiającemu wsparcia przy procesach aktualizacji.

3. Wymiana sprzętu – W ramach Wsparcia, Wykonawca zapewni wymianę sprzętu, z wysyłką zamiennika w następnym dniu roboczym po potwierdzeniu awarii. Montaż i demontaż sprzętu oraz koszty transportu zapewni Wykonawca.

Zgłaszanie Awarii

Kanały zgłoszeń – Zgłoszenia awarii będzie można dokonywać przez portal wsparcia, pocztą elektroniczną oraz telefonicznie.

Czas reakcji – Czas reakcji (maksymalny czas przyjęcia zgłoszenia przez Wykonawcę) na zgłoszenie awarii wyniesie 1 godzinę.

Usługi RMA (Return Material Authorization)

1. Wymiana sprzętu – W przypadku awarii sprzętu, Wykonawca zapewni wymianę urządzenia następnego dnia roboczego na swój koszt.

2. Zwrot wadliwego sprzętu – Zamawiający zobowiązany będzie do zwrotu wadliwego sprzętu w ciągu 30 dni od otrzymania zamiennika na koszt Wykonawcy.

Obowiązki Zamawiającego

1. Zamawiający zobowiązuje się do terminowego aktualizowania zgłoszeń otwartych w systemie wsparcia.

2. Zamawiający zapewni dostępność aktualnych kopii zapasowych konfiguracji urządzeń w celu przywrócenia ich w przypadku awarii.

3. W przypadku wymiany, Zamawiający zobowiązany jest do zwrotu uszkodzonego urządzenia wraz ze wszystkimi komponentami na koszt Wykonawcy.

Opisy do wymagań ogólnych

Przełaczniki mają być połączone przez 10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots

VIII. Urządzenia aktywne – bezprzewodowe punkty dostępowe wewnętrzne min. 77 sztuk

Access Point - wewnętrzny

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -20 – 45°C,
    b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac.
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w jeden interfejs 10/100/1000 Base-TX.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel,
    b. Bridge,
    c. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2,
    b. Maksymalna przepustowość dla poszczególnych modułów radiowych:
        i. 400 Mbps;

ii. 867 Mbps;

c. Wymagana moc nadawania:
   i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
   ii. min. 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
d. Wsparcie dla 802.11n 20/40Mhz HT,
e. Wsparcie dla kanałów 80MHz,
f. Anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
h. Maksymalna deklarowana liczba klientów per moduł radiowy:
   i. 512;
   ii. 512;

12. Funkcje dodatkowe:
   a. 802.11ac MU-MIMO Wave 2
   b. Transmit Beam Forming (TxBF)
   c. Low-Density Parity Check (LDPC) Encoding
   d. Maximum Likelihood Demodulation (MLD)
   e. Maximum Ratio Combining (MRC)
   f. A-MPDU and A-MSDU Packet Aggregation

IX. Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy.

Wsparcie Wykonawcy obejmie pomoc techniczną, aktualizacje oprogramowania oraz wymianę uszkodzonego sprzętu.

Zakres Usługi

1. Wsparcie techniczne – Usługa obejmie wsparcie techniczne dostępne 24 godziny na dobę, 7 dni w tygodniu (24x7x365), w tym możliwość otwierania zgłoszeń przez portal, telefonicznie i online.

2. Aktualizacje oprogramowania – Zamawiający otrzyma dostęp do aktualizacji oprogramowania, w tym nowych funkcji oraz poprawek. Wykonawca udzieli Zamawiającemu wsparcia przy procesach aktualizacji.

3. Wymiana sprzętu – W ramach Wsparcia, Wykonawca zapewni wymianę sprzętu, z wysyłką zamiennika w następnym dniu roboczym po potwierdzeniu awarii. Montaż i demontaż sprzętu oraz koszty transportu zapewni Wykonawca.

Zgłaszanie Awarii

Kanały zgłoszeń – Zgłoszenia awarii będzie można dokonywać przez portal wsparcia, pocztą elektroniczną oraz telefonicznie.

Czas reakcji – Czas reakcji (maksymalny czas przyjęcia zgłoszenia przez Wykonawcę) na zgłoszenie awarii wyniesie 1 godzinę.

Usługi RMA (Return Material Authorization)

1. Wymiana sprzętu – W przypadku awarii sprzętu, Wykonawca zapewni wymianę urządzenia następnego dnia roboczego na swój koszt.

2. Zwrot wadliwego sprzętu – Zamawiający zobowiązany będzie do zwrotu wadliwego sprzętu w ciągu 30 dni od otrzymania zamiennika na koszt Wykonawcy.

Obowiązki Zamawiającego

1. Zamawiający zobowiązuje się do terminowego aktualizowania zgłoszeń otwartych w systemie wsparcia.

2. Zamawiający zapewni dostępność aktualnych kopii zapasowych konfiguracji urządzeń w celu przywrócenia ich w przypadku awarii.

3. W przypadku wymiany, Zamawiający zobowiązany jest do zwrotu uszkodzonego urządzenia wraz ze wszystkimi komponentami na koszt Wykonawcy.

X. System centralnego zarządzania

System centralnego zarządzenia urządzeniami bezpieczeństwa oraz logowania.
W ramach postępowania wymaganym jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego (np. NGFW).

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Interfejsy, Dyski:

1. System musi dysponować co najmniej:
   - 4 portami Gigabit Ethernet RJ-45.

oraz portem konsoli szeregowej.

2. Powierzchnia dyskowa min. 8 TB.
3. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0,1
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. System musi umożliwiać zarządzenie co najmniej 30 systemami bezpieczeństwa.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 30 systemów.
3. System musi być w stanie przyjmować minimum 2 GB logów na dzień.

Funkcje systemu centralnego zarządzania
W ramach centralnego systemu zarządzenia muszą być realizowane co najmniej poniższe funkcje:

1. System musi posiadać system zarządzenia zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).
2. System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
3. System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).
4. System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.

5. System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
6. System musi umożliwiać zarządzenie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania.
7. System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.
8. System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).
9. System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.
10. System musi pozwalać na zapisywanie i zdalne wykonywanie skryptów na urządzeniach.
11. System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).
12. System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mash.
13. System musi umożliwiać Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

Funkcje logowania

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów, do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

Funkcja raportowania

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Funkcje korelacji

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.

2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System powinien korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI.

2. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów.
3. System musi posiadać API które umożliwia zarządzenie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.
4. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

W ramach postępowania przetargowego Wykonawca gwarantuje autoryzowane szkolenie producenta rozwiązania - dla jednej osoby ze strony Zamawiającego.

XI. Access Point – 8 sztuk – zewnętrzny

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na słupie lub ścianie na zewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
   a. Temperatura -40 – 60°C,
   b. Wilgotność 10–90%.
2. Obudowa musi spełniać normę IP67.
3. Urządzenie musi być dostarczone z elementami mocującymi oraz zasilaczem.
4. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.

5. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac/ax,
    c. Skaner 2.4GHz i 5GHz.
6. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
7. Urządzenie musi być wyposażone w moduł BLE.
8. Liczba interfejsów:
   Co najmniej 2 w standardzie 10/100/1000 Base-TX
9. Urządzenie powinno być zasilane poprzez interfejs ETH zgodnie ze standardem 802.3at oraz być zgodne ze standardem 802.3az.
10. Urządzenie musi posiadać wbudowane zabezpieczenie przeciwprzepięciowe.
11. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel,
    b. Bridge,
    c. Mesh.
12. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
13. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3 PSK, WPA3-Enterprise, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
14. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2,
    b. Maksymalna przepustowość dla poszczególnych modułów radiowych:
        i. 2.4GHz 574 Mbps;
        ii. 5GHz 1200 Mbps;
    c. Wymagana moc nadawania:
        i. min. 27 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
        ii. min. 25 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
    d. Wsparcie dla 802.11n 20/40Mhz HT,
    e. Wsparcie dla kanału 80 MHz,
    f. Anteny – wbudowane anteny o zysku min. 10dBi
    g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
    h. Maksymalna deklarowana liczba klientów dla poszczególnych modułów radiowych:
        i. 512;
        ii. 512;
15. Funkcje dodatkowe:
    a. OFDMA UL i DL
    b. Spatial Reuse (BSS Coloring)
    c. UL-MU-MIMO 802.11ax
    d. DL-MU-MIMO
    e. Enhanced Target Wake Time (TWT)
16. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance oraz posiadać certyfikację DFS.

XII. Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy.

Wsparcie Wykonawcy obejmie pomoc techniczną, aktualizacje oprogramowania oraz wymianę uszkodzonego sprzętu.

Zakres Usługi
1. Wsparcie techniczne – Usługa obejmie wsparcie techniczne dostępne 24 godziny na dobę, 7 dni w tygodniu (24x7x365), w tym możliwość otwierania zgłoszeń przez portal, telefonicznie i online.
2. Aktualizacje oprogramowania – Zamawiający otrzyma dostęp do aktualizacji oprogramowania, w tym nowych funkcji oraz poprawek. Wykonawca udzieli Zamawiającemu wsparcia przy procesach aktualizacji.
3. Wymiana sprzętu – W ramach Wsparcia, Wykonawca zapewni wymianę sprzętu, z wysyłką zamiennika w następnym dniu roboczym po potwierdzeniu awarii. Montaż i demontaż sprzętu oraz koszty transportu zapewni Wykonawca.

Zgłaszanie Awarii
Kanały zgłoszeń – Zgłoszenia awarii będzie można dokonywać przez portal wsparcia, pocztą elektroniczną oraz telefonicznie.

Czas reakcji – Czas reakcji (maksymalny czas przyjęcia zgłoszenia przez Wykonawcę) na zgłoszenie awarii wyniesie 1 godzinę.

Usługi RMA (Return Material Authorization)
1. Wymiana sprzętu – W przypadku awarii sprzętu, Wykonawca zapewni wymianę urządzenia następnego dnia roboczego na swój koszt.
2. Zwrot wadliwego sprzętu – Zamawiający zobowiązany będzie do zwrotu wadliwego sprzętu w ciągu 30 dni od otrzymania zamiennika na koszt Wykonawcy.

Obowiązki Zamawiającego
1. Zamawiający zobowiązuje się do terminowego aktualizowania zgłoszeń otwartych w systemie wsparcia.
2. Zamawiający zapewni dostępność aktualnych kopii zapasowych konfiguracji urządzeń w celu przywrócenia ich w przypadku awarii.
3. W przypadku wymiany, Zamawiający zobowiązany jest do zwrotu uszkodzonego urządzenia wraz ze wszystkimi komponentami na koszt Wykonawcy.

XIII. Informacje dodatkowe

Zakres obowiązków Wykonawcy obejmuje również:

- Wypakowanie i utylizacja opakowań.
- Montaż w miejscu przeznaczenia używania (odpowiednie szafy RACK).
- Podłączenie do istniejącej infrastruktury sieci LAN i zasilania.
- Aktualizacja oprogramowania wewnętrznego.

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji realizacji każdego Zadania. Dokumentacja ma być przechowywana przez cały okres realizacji projektu.

Wszystkie urządzenia oraz materiały stanowiące przedmiot zamówienia powinny być fabrycznie nowe i mieć datę produkcji nie większą, niż 12 miesięcy wstecz od daty podpisania Umowy na wykonanie przedmiotu zamówienia.

Uszczelnienia przeciwpożarowe.

Przejścia przez elementy oddzielenia przeciwpożarowego uszczelnić ogniochronnie o klasie odporności ogniowej, takiej jak klasa odporności ogniowej oddzielenia, w którym zlokalizowano przepust. Zastosować piankę ogniochronną Hilti CFS-F FX (lub równoważną). Przez przegrody ogniowe przeprowadzić należy sam kabel - bez rury osłonowej.

W ramach zamówienia Wykonawca zobowiązuje się do przeszkolenia personelu Działu Informatyki Zamawiającego (3 osoby), które umożliwi ww. personelowi obsługę wszystkich nowo dostarczonych rozwiązań oraz bezpieczne administrowanie siecią lan/wifi.

XIV. Dokumentacja powykonawcza

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego. Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresie dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu.

Hasła muszą zostać dostarczone w zamkniętej kopercie i przekazane muszą być protokolarnie wyznaczonemu przedstawicielowi Zamawiającego.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania – w wersji elektronicznej.

Dokumentacja musi być sporządzona w języku polskim.

XV. Załączniki:

Zamawiający udostępnia posiadane rzuty budynków oraz schematy instalacji elektrycznych i logicznych stanowią załącznik nr 1a do SWZ i są spakowane do pliku zip.