Załącznik nr 1
do Zapytania ofertowego nr 1.1/FEPW1.2/SANTOS

Opis Przedmiotu Zamówienia

„Modernizacja infrastruktury teleinformatycznej”

Krościenko Wyżne, luty 2025

1 Wymagania ogólne dla urządzeń

- całość sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;
- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązania; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;
- **Minimalny okres gwarancji - 12 miesięcy** liczony od daty podpisania protokołu odbioru.
- Gwarancja producenta z pozostawieniem dysków twardych u Zamawiającego w przypadku ich uszkodzenia.

2 Miejsca montażu

Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w miejscach wskazanych przez Zamawiającego, zgodnie z poniższym zestawieniem:

A. **Siedziba Zamawiającego:** ul. Południowa 51, 38-422 Krościenko Wyżne
B. **Punkt nr 1:** ul. ks. Stanisława Staszica 16, 38-400 Krosno
C. **Punkt nr 2:** ul. Rynek 1, 38-200 Jasło
D. **Punkt nr 3:** ul. Bieszczadzka 29, 38-400 Krosno
E. **Punkt nr 4:** ul. Krakowska 20, 35-213 Rzeszów
F. **Punkt nr 5:** al. Tadeusza Rejtana 33, 35-310 Rzeszów

Lp.	Wyszczególnienie	Miejsce montażu					
		A.	B.	C.	D.	E.	F.
1.	Router brzegowy	1					
2.	Kontroler sprzętowy	1					
3.	Przełącznik zarządzalny	1	1	1	1	1	1
4.	Punkt dostępowy AP	4	2	2	2	1	1
5.	Router kliencki	1	1	1	1	1	1
6.	Modernizacja infrastruktury sieciowej	X	X	X	X	X	X
7.	Serwer	1					

3 Zestawienie pozycji

Lp.	Wyszczególnienie	Liczba	Jedn. miary	Okres gwarancji (m-ce)	Rodzaj gwarancji
1.	Router brzegowy	1	szt.	12	producenta
2.	Kontroler sprzętowy	1	szt.	12	producenta
3.	Przełącznik zarządzalny	6	szt.	12	producenta
4.	Punkt dostępowy AP	12	szt.	12	producenta
5.	Router kliencki	6	szt.	12	producenta
6.	Serwer	1	szt.	12	producenta
7.	Wdrożenie i konfiguracja i uruchomienie sieci	1	szt.	*Nie dotyczy.*	*Nie dotyczy.*
8.	Modernizacja infrastruktury sieciowej	1	szt.	12	wykonawcy
9.	Szkolenia kadry dotyczące polityki bezpieczeństwa sieci	16	godz.	*Nie dotyczy.*	*Nie dotyczy.*
10.	Szkolenia kadry dotyczące konfiguracji access pointów	8	godz.	*Nie dotyczy.*	*Nie dotyczy.*

4 Szczegółowa specyfikacja techniczna

4.1 Zakup routera brzegowego

Wymagania ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - min. 10 portami Gigabit Ethernet RJ-45.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

Parametry wydajnościowe

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 4 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.

Funkcje Systemu Bezpieczeństwa

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.

12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku, kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
3. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
4. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
5. Możliwość włączenia logowania per reguła w polityce firewall.
6. System zapewnia możliwość logowania do serwera SYSLOG.
7. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.

Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- obsługa procesu RMA u producenta,
- zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta,
- jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta,
- minimum 3 zdalne konsultacje techniczne z inżynierem posiadającym najwyższy poziom certyfikacji technicznej producenta, ****wymagana wersja PRO****
- jednorazowa usługa hardeningu konfiguracji w formie zdalnej sesji technicznej mającej na celu przegląd konfiguracji urządzenia i przedstawienie zaleceń rekonfiguracji zgodnie z „dobrymi praktykami" producenta, ****wymagana wersja PRO****
- dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.

4.2 Zakup kontrolera sprzętowego

Kontroler sprzętowy sieci

- Urządzenie wspiera jedynie kompatybilne urządzenia typu AP, switch, Gateway pochodzące od tego samego producenta. Urządzenie musi być wyposażone w min. 2 porty RJ45 o prędkości 10/100 Mb/s
- Urządzenie musi być wyposażone w dwa porty USB – 1 x USB 2.0 oraz 1 x microUSB
- Urządzenie musi mieć możliwość obsługi do 100 punktów dostępowych i do 1000 klientów jednocześnie.
- Urządzenie musi mieć możliwość zasilania poprzez standard 802.3af/at lub poprzez MicroUSB (5VDC/1A)
- Urządzenie musi posiadać min. 1GB pamięci RAM oraz min 4GB pamięci stałej
- Urządzenie musi posiadać minimum dwurdzeniowy procesor o taktowaniu nie mniejszym niż 1GHz
- Wymiary urządzenie nie mogą być większe niż: 100x100x30mm
- Urządzenie musi mieć możliwość zarządzania całą siecią (elementy składowe sieci rozumiane jako router, przełączniki oraz punkty dostępowe WiFi)
- W zakresie zarządzania punktami dostępowymi/siecią WiFi urządzenie musi spełniać następujące wymagania:
  1. Urządzenie musi umożliwiać scentralizowane zarządzanie siecią WiFi lokalnie jak i zdalnie
  2. Urządzenie musi umożliwiać konfigurację sieci WiFi i realizować następujące funkcje: MultiSSID, równoważenie obciążenia punktów dostępowych, sterowanie pasmem, ograniczenie prędkości transmisji, umożliwić utworzenie harmonogramu sieci WiFi, QoS
  3. Urządzenie musi umożliwić uwierzytelnianie użytkowników za pomocą strony powitalnej.
  4. Urządzenie musi posiadać funkcjonalność kontroli dostępu, filtrowania adresów MAC, izolacji klientów sieci bezprzewodowej, mapowania VLAN do SSID
  5. Urządzenie musi umożliwiać automatyczne wykrywanie oraz jednorodną konfigurację punktów dostępowych
  6. Wspierać funkcjonalność tworzenia strony powitalnej (tzw. Portalu) dla klientów sieci bezprzewodowej. Portal musi posiadać narzędzia umożliwiające uwierzytelnianie klientów bezprzewodowych poprzez kody jednorazowe bądź utworzone na kontrolerze konta użytkowników
- W zakresie zarządzania przełącznikami urządzenie musi spełniać następujące wymagania:

1. Umożliwiać pełną konfigurację sieci VLAN (dodanie sieci VLAN, konfiguracja portów)
2. Umożliwiać konfigurację adresacji poszczególnych urządzeń w danych sieciach VLAN
3. Generować topologię sieci wyświetlając połączenia zarządzanych urządzeń wraz z informacją o numerze portu i szybkości połączenia
4. Automatycznie wykrywać kompatybilne urządzenia znajdujące się w sieci lokalnej
5. Umożliwiać konfigurację agregacji portów zgodnie ze standardem 802.3ad

- W zakresie zarządzania routerem urządzenie musi umożliwiać wykorzystanie następujących funkcjonalności:
  1. Zarządzanie interfejsami routera wraz z tworzeniem VLAN-ów i interfejsów przypisanych do tych VLAN-ów
  2. Konfigurację VPN w zakresie serwera oraz kont klientów
  3. Wymaga się, by urządzenie obsługiwało protokoły min. IPSec oraz OpenVPN
- Urządzenie w zestawie musi posiadać kabel Ethernet
- Urządzenie musi posiadać następujące certyfikaty: CE, FCC, RoHS
- Dopuszczana temperatura pracy urządzenia musi zawierać się w przedziale od 0 do 40 stopni Celsjusza

W ramach dostawy kontrolera zamawiający wymaga dostarczenia przełącznika 10Gbit/s.

Cechy sprzętowe

- Urządzenie musi być wyposażone w min. 24 gigabitowe porty RJ45 oraz min. cztery porty SFP+. Nie są dopuszczane porty SFP+ współdzielone z portami RJ45 (tzw. „combo")
- Porty SFP+ muszą również obsługiwać moduły pracujące z prędkością 1Gbps
- Urządzenie musi posiadać port konsolowy RJ45 lub microUSB
- Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward
- Rozmiar tablicy adresów MAC urządzenia min. 16K
- Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 128 Gbps
- Min. szybkość przekierowań pakietów 95,2 Mpps
- Urządzenie musi wspierać funkcjonalność PoE zgodną ze standardem 802.3af/at, minimalny wymagany budżet dostępny dla zasilanych urządzeń to 380W
- Całkowity pobór mocy urządzenia (wliczając pełne obciążenie PoE) nie może przekraczać 490W
- Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19" oraz posiadać w zestawie odpowiednie uchwyty montażowe
- Głębokość urządzenia nie może przekraczać 450 mm

Standardy

Urządzenie musi spełniać następujące standardy:

- 802.3i
- 802.3u
- 802.3z
- 802.3ab
- 802.3ad
- 802.3ae
- 802.3af
- 802.3at
- 802.3az
- 802.3x
- 802.1ab

- 802.1d
- 802.1w
- 802.1s
- 802.1p
- 802.1q

Funkcjonalność
Wymaga się, aby urządzenie posiadało następujące funkcjonalności:

- Zarządzanie za pomocą przeglądarki poprzez interfejs http/https
- Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia
- Obsługę stosu IPv4 i IPv6
- Funkcję wykrywania pętli
- Funkcję izolacji portów
- Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji)
- Obsługę protokołu LLDP/LLDP-MED
- Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6
- Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6)
- Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP)
- Obsługę 4K identyfikatorów VLAN
- Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN)
- IGMP Snooping oraz MLD Snooping
- Obsługę min 500 grup multicastowych jednocześnie
- MVR
- Obsługę routingu statycznego i/lub dynamicznego
- Możliwość konfiguracji co najmniej 16 interfejsów IP
- Obsługę min 40 tras statycznych dla funkcji routingu statycznego
- Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+
- Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia
- Obsługę list kontroli dostępu (ACL)
- Obsługę SNMP w wersjach v1/v2c/v3
- Obsługę grup RMON 1,2,3,9)

Pozostałe wymagania:

- Urządzenie musi posiadać certyfikację CE
- Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta

4.3 Zakup przełącznika zarządzalnego

Cechy sprzętowe

- Urządzenie musi być wyposażone w min. 8 gigabitowych portów RJ45 oraz min. dwa porty SFP (nie dopuszcza się portów SFP współdzielonych z portami RJ45, tzw. portów „combo”)

- Co najmniej 8 portów musi dostarczać zasilanie PoE zgodnie ze standardami 802.3af/at z łącznym budżetem PoE min. 140W.
- Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward
- Rozmiar tablicy adresów MAC urządzenia min. 8K
- Min. szybkość przekierowań pakietów 14,88 Mpps
- Bufor pakietów min 512KB
- Pobór mocy urządzenia nie może przekraczać 180W przy maksymalnym wykorzystaniu budżetu PoE
- Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe
- Głębokość urządzenia nie może przekraczać 190 mm
- Urządzenie musi mieć możliwość pracy w trybie standalone jak również móc być centralnie zarządzanym poprzez kontroler
- Urządzenie musi posiadać zabezpieczenie przeciwprzepięciowe na portach RJ45 chroniące przed przepięciami min. 5kV

Standardy
Urządzenie musi spełniać następujące standardy:

- 802.3i
- 802.3u
- 802.3ab
- 802.3ad
- 802.3af
- 802.3at
- 802.3az
- 802.3x
- 802.1ab
- 802.1D
- 802.1s
- 802.1p
- 802.1q
- 802.1w

Funkcjonalność
Wymaga się, aby urządzenie posiadało następujące funkcjonalności:

- Zarządzanie poprzez interfejs graficzny dostępny zarówno poprzez połączenie http jak i https
- Zarządzanie poprzez CLI (Telnet, SSH), z poziomu CLI musi być możliwa konfiguracja wszystkich funkcji urządzenia
- Obsługę stosu IPv4 i IPv6
- Funkcję wykrywania pętli
- Funkcję izolacji portów
- Funkcję agregacji portów z wykorzystaniem protokołu LACP
- Obsługę protokołu LLDP/LLDP-MED
- Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6
- Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6)
- Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP)
- Obsługę 4K identyfikatorów VLAN

- Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN)
- IGMP Snooping oraz MLD Snooping
- MVR
- Obsługę routingu statycznego i/lub dynamicznego IPv4 jak i IPv6
- Możliwość konfiguracji co najmniej 30 interfejsów IP
- Obsługę min 30 tras statycznych dla funkcji routingu statycznego
- Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+
- Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia
- Obsługę list kontroli dostępu (ACL)
- Obsługę SNMP w wersjach v1/v2c/v3
- Obsługę grup RMON 1,2,3,9

Pozostałe wymagania:

- Urządzenie musi posiadać certyfikację CE
- Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta
- wydajność przełączania 20 Gb/s

4.4 Zakup punktów dostępowych AP

- Urządzenie musi być wyposażone w min. 1 port RJ45 pracujący z prędkością 1Gb/s obsługujący standard PoE 802.3at
- Urządzenie musi być wyposażone w gniazdo umożliwiające zasilanie urządzenia bezpośrednio z wykorzystaniem zewnętrznego zasilacza lub injectora pasywnego PoE 48V
- Urządzenie musi być wyposażone w przycisk przywracania ustawień fabrycznych
- Urządzenie musi być wyposażone w min. 2 anteny wewnętrzne dookólne o zysku min 4dBi dla sieci 2,4GHz oraz min 5dBi dla sieci 5GHz
- Urządzenie musi wspierać standardy IEEE 802.11a/b/g/n/ac/ax oraz częstotliwości pracy 2,4 oraz 5GHz
- Łączna prędkość modułów radiowych musi wynosić min. 1733 Mbps
- Maksymalny pobór mocy urządzenia nie może być większy niż 13W
- Urządzenie powinno być dostosowane do montażu na ścianie lub suficie oraz posiadać dołączony zestaw montażowy
- Urządzenie musi pracować zarówno jako urządzenie typu stand-alone lub w trybie podłączonym do kontrolera sieci bezprzewodowej
- Kontroler sieci bezprzewodowej realizowany musi być jako oprogramowanie przeznaczone do instalacji na systemach operacyjnych Windows/Linux lub kontroler sprzętowy – oddzielne urządzenie
- Oprogramowanie kontrolera sieci bezprzewodowych musi być realizowane jako oprogramowanie bezpłatne, bez dodatkowych opłat licencyjnych
- Urządzenie musi posiadać funkcjonalność tworzenia wielu sieci WiFi – min. 14 SSID
- Urządzenie musi posiadać funkcjonalność: wyłącznik sieci bezprzewodowej, automatyczny wybór kanału, kontrola mocy transmisji, QoS (WMM), sterowanie pasmem, równoważenie obciążenia pasma, kontrola przepustowości, harmonogram resetu oraz harmonogram sieci bezprzewodowej.
- Urządzenie musi posiadać możliwość utworzenia strony powitalnej
- Urządzenie musi posiadać możliwość mapowania SSID do VLAN oraz tworzenia sieci dla gości

- Urządzenie musi posiadać możliwość wyłączenia diody LED na obudowie
- Urządzenie musi być zarządzane z poziomu przeglądarki internetowej, oraz obsługiwać zarządzanie poprzez HTTPS
- Urządzenie musi posiadać obsługę SNMP v1/v2c, v3
- Urządzenie musi posiadać certyfikat CE, FCC oraz RoHS
- W zestawie z urządzeniem powinien być dostarczony zestaw montażowy
- Dopuszczalna temperatura pracy powinna zawierać się w przedziale od 0 do 40 stopni Celsjusza.

4.5 Zakup routera klienckiego

Cechy sprzętowe

- Urządzenie musi być wyposażone w min. 5 gigabitowych portów Ethernet RJ45
- Min. 3 z w/w portów muszą mieć możliwość wykorzystania jako porty WAN
- Urządzenie musi posiadać min. 1 port WAN SFP
- Urządzenie musi obsługiwać min 140000 równoczesnych sesji NAT
- Przepustowość urządzenia musi wynosić min. 290Mbps dla połączeń VPN IPSec.
- Rozmiary urządzenia nie mogą przekraczać (Szerokość x Głębokość x Wysokość) 230 × 135 × 40mm

Standardy

Urządzenie musi spełniać następujące standardy:

- 802.3
- 802.3u
- 802.3x
- 802.3q
- 802.3ab

Funkcjonalność

Wymaga się, aby urządzenie posiadało następujące funkcjonalności:

- DHCP Server/Client
- Rezerwacja adresów DHCP
- Możliwość zmiany adresu MAC na portach WAN
- Równoważenie obciążenia pasma
- Tryb łącza zapasowego
- Obsługa połączeń VPN PPTP/L2TP/IPSec/OpenVPN, dla IPSec wymagana jest obsługa trybów LAN do LAN oraz Client-Server
- Musi być dostępna funkcjonalność umożliwiająca powiązanie adresów IP i MAC
- Wbudowane narzędzia diagnostyczne Ping oraz Traceroute
- Synchronizacja czasu z serwerem NTP
- Obsługa DDNS

Inne

- Urządzenie musi posiadać certyfikaty CE oraz ROHS
- zasilacz awaryjny o mocy 650VA/360W wykonany w topologii VI (line-interactive) z baterią minimalnej pojemności 7Ah umożliwiającej podtrzymanie pracy dla 50% (180 W) obciążenia na czas nie krótszy niż 8 minut.
- **Wszystkie zasilacze musza być tego samego producenta i monitorowane/zarządzane z jednego programu zarządzającego.**

4.6 Zakup serwera

Obudowa

- Obudowa 1U serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami dedykowanymi do tego urządzenia przez producenta serwera.
- obudowa powinna posiadać dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
- Obudowa powinna posiadać możliwość instalacji panelu LCD pozwalającego jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej.
- W obudowie powinien być zainstalowany zestaw redundantnych zasilaczy mocy co najmniej 700W w standardzie Titanium każdy wymienialnych podczas pracy oraz zestaw redundantnych wentylatorów.
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Obudowa powinna posiadać możliwość instalacji interfejsu do połączenia z aplikacją zarządzającą serwerem na telefonie.
- Aplikacja zarządzająca powinna być dostępna na Android i iOS

Płyta główna

- Płyta główna obsługująca co najmniej dwa procesory i co najmniej 16 slotów na pamięć taktowaną przynajmniej z częstotliwością 3200MT/s przy użyciu odpowiednich procesorów.
- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
- Musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust),
- Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera.
- Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0

Procesor

- typu skalowalnego posiadający co najmniej 8 rdzeni dający w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 19010

Pamięć RAM

- 64 GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 3200MT/s

Dyski

- Miejsce na co najmniej 8 dysków w rozmiarze 2.5" wymienialne bez wyłączania systemu.
- Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski.
- Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,10
- W serwerze powinny być zainstalowane co najmniej cztery dyski co najmniej 480GB SSD

Karty sieciowe

- Na płycie głównej powinna być zainstalowana dwuportowa karta sieciowa 1GB BT i dwuportowa karta 10/25GB w standardzie SFP28 Karty nie mogą zajmować slotu PCIe
- W serwerze powinien być co najmniej jeden slot PCIe x16

Karta zarządzająca

Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet, umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej
- szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika
- możliwość podmontowania zdalnych wirtualnych napędów
- wirtualną konsolę z dostępem do myszy, klawiatury
- wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
- integracja z Active Directory
- możliwość obsługi przez ośmiu administratorów jednocześnie
- Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
- możliwość podłączenia lokalnego poprzez złącze RS-232.
- możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.
- Monitorowanie zużycia dysków SSD
- możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
- automatyczne zgłaszanie alertów do centrum serwisowego producenta
- automatyczne update firmware dla wszystkich komponentów serwera
- możliwość przywrócenia poprzednich wersji firmware
- możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
- możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
- automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.

Oprogramowanie zarządzające

Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:

- wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
- możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
- wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;
- możliwość oskryptowywania procesu wykrywania urządzeń;
- możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
- szczegółowy opis wykrytych systemów oraz ich komponentów;
- możliwość eksportu raportu do CSV, HTML, XLS;
- grupowanie urządzeń w oparciu o kryteria użytkownika;
- automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
- szybki podgląd stanu środowiska;
- podsumowanie stanu dla każdego urządzenia;
- szczegółowy status urządzenia/elementu/komponentu;
- generowanie alertów przy zmianie stanu urządzenia;
- filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
- integracja z service desk producenta dostarczonej platformy sprzętowej;
- możliwość przejęcia zdalnego pulpitu;
- możliwość podmontowania wirtualnego napędu;
- kreator umożliwiający dostosowanie akcji dla wybranych alertów;
- możliwość importu plików MIB;

- przesyłanie alertów „as-is" do innych konsol firm trzecich;
- aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
- możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
- możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
- moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.

Certyfikaty
Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
Serwer musi posiadać deklarację CE.

Producent serwera nie może pochodzić z kraju objętego sankcjami dowolnego członka NATO.

Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155.
Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware.

Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:
Monitoring:

- ilość podłączonych oraz rozłączonych systemów
- stan podłączonych urządzeń
- informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
- informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
- informacje o statusie gwarancji dla poszczególnych urządzeń
- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
- informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
- wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
- wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
- monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
- zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
- szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.

Monitoring parametrów serwerów z informacją o minimum:

- Obciążeniu procesora
- Zużyciu pamięci RAM
- Temperaturze procesorów
- Temperaturze powietrza wlotowego

- Zużyciu prądu
- Zmianach w fizycznej konfiguracji serwera
- Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

Monitoring parametrów pamięci masowych z informacją o minimum:

- Opóźnieniach
- IOPS
- Przepustowości
- Utylizacji kontrolerów
  Pojemność całkowita i dostępna
- Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
- Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
- Informacje o poziomie redukcji danych
- Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
- Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
- Stanie komponentów: zasilacze, wentylatory
- Podłączonych hostach
- Ilości i statusu portów
- Utylizacji procesora
- Utylizacji poszczególnych portów
- Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

Aktualizacja firmware:

- możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania

Raporty:

- Możliwość generowania raportów dla serwerów zawierających informację o:
- Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
- Średnim obciążeniu: procesorów, pamięci RAM, IO,
- Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcji danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
- Generowanie raportów do plików CSV i PDF

Cyberbezpieczeństwo:

- Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik

bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
- Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
- Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
- Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.

Możliwość rozszerzenia funkcjonalności:
- Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.

Inne:
- Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

Aplikacja mobilna do zarządzania serwerami powinna umożliwiać:
- Monitorowanie stanu serwerów, w tym odczyt parametrów zdrowia, inwentarza i konfiguracji.
- Konfigurowanie ustawień serwera, takich jak parametry sieci, hasła administratora i kolejność urządzeń rozruchowych.
- Bezpośrednią komunikację z kontrolerem serwera za pomocą technologii bezprzewodowej.
- Zdalne zarządzanie serwerami poprzez połączenie z konsolą zarządzania.
- Pobieranie informacji o serwerach takich jak inwentarz, status, alerty oraz logi.
- Konfigurowanie serwerów zdalnie.
- Wysyłanie poleceń sterowania zasilaniem i innych poleceń.
- Otrzymywanie powiadomień o alertach z systemów zarządzania.
- Pobieranie informacji o gwarancji.
- Uruchamianie zewnętrznych aplikacji, takich jak klienci zdalnego pulpitu.
- Zabezpieczenie danych w aplikacji poprzez szyfrowanie z użyciem klucza specyficznego dla urządzenia.
- Opcjonalne zabezpieczenie dostępu do aplikacji za pomocą hasła i biometrii.
- Automatyczne wylogowanie w przypadku braku aktywności.
- Połączenie z serwerami za pomocą technologii Bluetooth Low Energy (BLE) lub Wi-Fi.
- Wyświetlanie szczegółowych informacji o serwerze oraz dzienników.
- Otrzymywanie automatycznych powiadomień z konsoli zarządzania.
- Przypisywanie adresów IP i modyfikowanie haseł.
- Konfigurowanie atrybutów BIOS.
- Wyłączanie i włączanie serwera oraz dostęp do konsoli systemowej.
- Pobieranie danych z systemów zarządzania typu "jeden do wielu".
- Wyświetlanie certyfikatu systemu w celu weryfikacji tożsamości przy pierwszym połączeniu.
- Aplikacja powinna być dostępna do pobrania w popularnych sklepach z aplikacjami.

W ramach wsparcia technicznego wymagana jest usługa polegająca na przygotowaniu i dostarczeniu spersonalizowanego panelu w chmurze.
Usługa powinna pozwalać na identyfikowanie priorytetów i potencjalnych zagrożeń technicznych sprzętu co pomoże w podejmowanie właściwych działań.

Usługa powinna spełniać następujące założenia/funkcje:
- Proaktywne zarządzanie priorytetami usług serwisowych w tym graficzną reprezentację poziomu zagrożeń.
- Możliwość personalizacji widoku przez członków zespołu do zarządzanych przez nich lokalizacji i zasobów.
- Dostęp do szczegółów dotyczących sprzętu i oprogramowania, w tym incydentów krytycznych, wsparcia technicznego, eskalacji, konserwacji na miejscu, poziomów kodu, poradników bezpieczeństwa i technicznych, zakresu wsparcia, wymiany części, łączności urządzeń i bram.

- Dostęp do danych historycznych i analiz na potrzeby planowania IT

W ramach postępowania wykonawca musi dostarczyć zasilacz awaryjny o mocy 3kVA/3kW do zabezpieczenia serwerowni głównej lokalizacji oraz stojącą szafę instalacyjną rack 19" 27U o głębokości 1000 mm.
UPS 3kVA wykonany w topologii online VI (line-interactive) umożliwiającej podtrzymanie pracy dla pełnego obciążenia na czas nie krótszy niż 7 minut. Baterie umieszczone wewnątrz UPS oraz w dedykowanym zewnętrznym module bateryjnym.

Wszystkie zasilacze musza być tego samego producenta i monitorowane/zarządzane z jednego programu zarządzającego.

4.7 Wdrożenie i konfiguracja i uruchomienie sieci

Prace wdrożeniowe mają na celu instalację, wdrożenie, uruchomienie oraz przetestowania działania stworzonej sieci urządzeń tj.:

1. Opracowanie polityki bezpieczeństwa sieci;
2. Wydzielenie podsieci;
3. Konfiguracja systemów zabezpieczeń sieciowych;
4. Konfiguracja access pointów, routera brzegowego, przełączników;
5. Nadanie praw dostępowych;
6. Uruchomienie i zaadresowanie urządzeń końcowych.

Montaż i fizyczne uruchomienie systemu	**Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach, co najmniej w zakresie:** 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem:

	a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami. b. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN. c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1. d. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
Instalacja/ aktualizacja i konfiguracja oprogramowania	1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu. 3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). 4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych. 5. Instalacja i konfiguracja oprogramowania do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR) 6. Instalacja i konfiguracja oprogramowanie do zarzadzania infrastrukturą IT.
Konfiguracja przełączników/sieci LAN	Re/Konfiguracja przełączników w zakresie: a. Przeprowadzenie audytu obecnej topologii oraz konfiguracji. b. Dołączenie dostarczonego przełącznika do sieci LAN Zamawiajacego. c. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym). d. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy). e. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall. f. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. g. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; h. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). i. Testowanie obsługi ruchu sieciowego. j. Testowanie skuteczności zabezpieczeń.
Migracja danych	Dane (systemy dziedzinowe) muszą zostać przeniesione na nowe zasoby serwerowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych.
Instalacja i konfiguracja serwera kopii zapasowych konfiguracji	1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.: przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy.

urządzeń sieciowych	2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego). 3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie. 4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
Testowanie i modyfikacja parametrów infrastruktury sieciowej	1. Testowanie mechanizmów bezpieczeństwa 2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie mechanizmów replikacji danych. 4. Testowanie dostępu publicznego do zasobów. 5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach.
Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.** W tym czasie przedstawiciel Wykonawcy: • zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji; • dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: a) zastosowanej technologii serwerów b) zastosowanej technologii pamięci masowej c) wirtualizacji d) systemu backupu e) zastosowanych rozwiązań aplikacyjnych Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.
Opracowanie dokumentacji powykonawczej	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. 1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).

	3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów. 6. Polityki bezpieczeństwa sieci. Dokumentacja powykonawcza powinna zawierać schematy przepływu danych pomiędzy wszystkimi wdrażanymi i modyfikowanymi systemami i modułami. Dokumentacja powinna zawierać wymogi dotyczące konieczności zawarcia umów powierzenia danych osobowych na czas wdrażania i czas obsługi i wsparcia dla wdrażanych systemów. Dokumentacja powykonawcza powinna zawierać wyniki wszystkich niezależnych audytów stron internetowych i aplikacji mobilnych potwierdzające zgodność wdrożonych systemów z WCAG 2.1 oraz Ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U.2023.1440).

4.8 Modernizacja infrastruktury sieciowej

Wydatek obejmuje roboty budowlane niezbędne do przeprowadzenia modernizacji infrastruktury teleinformatycznej i podłączenia urządzeń peryferyjnych systemu zarządzania produkcją, obejmujących wykonanie infrastruktury elektrycznej i sieciowej **w 2 budynkach zakładu produkcyjnego siedziby głównej SANTOS oraz w 5 sklepach firmowych.**

Wykonanie okablowania (trasy kablowe, ułożenie okablowania, punkty logiczne) pod sieć Ethernet dla punktów dostępowych kat. 6 U/UTP.

Instalacja musi być wykonana zgodnie z wytycznymi producenta okablowania strukturalnego oraz wytycznymi norm referencyjnych w szczególności:

- EN 50174-1:2009/A1:2011 Information Technology - Cabling system installation- Part 1. Specification and quality assurance, wraz z jej polskim odpowiednikiem: PN-EN 50174-1:2010/A1:2011 Technika informatyczna - Instalacja okablowania - Część 1 - Specyfikacja i zapewnienie jakości (lub równoważne);
- EN 50174-2:2009/AB2013 Information Technology - Cabling system installation - Part 2. Installation planning and practices internal to buildings, wraz z jej polskim odpowiednikiem: PN-EN 50174-2:2010/A1:2011 Technika informatyczna - Instalacja okablowania -Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków (lub równoważne);
- EN 50174-3:2013 Information Technology - Cabling system installation - Part 3. – Industrial premises, wraz z jej polskim odpowiednikiem: PN-EN 50174-3:2014-02E Technika informatyczna - Instalacja okablowania - Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków (lub równoważne);
- EN 50310:2010 Application of equipotential bonding and earthling at premises with information technology equipment, wraz z jej polskim odpowiednikiem: PN-EN 50310:2012 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym co winno zostać potwierdzone w dokumentacji powykonawczej (lub równoważne);
- Zamawiający w odniesieniu do powyższych norm dopuszcza rozwiązania równoważne zgodne z poniższym opisem.

1. Zakres prac:
   1. Wykonanie okablowania (trasy kablowe, ułożenie okablowania, punkty logiczne) pod sieć Ethernet dla punktów dostępowych kat. 6 U/UTP w miejscach wskazanych przez Zamawiającego.
   2. Roboty poinstalacyjne: uzupełnienie ubytków tynków powstałych w trakcie rozbudowy sieci, wykonanie powstałych miejscowych uzupełnień malarskich farbą emulsyjną, prace porządkowe, wywóz gruzu i zdemontowanych, złomowych elementów poinstalacyjnych.
2. Założenia podstawowe – wytyczne:
   - Wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być oznaczone nazwą lub znakiem firmowym, tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu gwarancyjnego w/w producenta;
   - Producent okablowania strukturalnego musi legitymować się ważnym certyfikatem systemu zarządzania od minimum 10 lat co gwarantuje Użytkownikowi właściwą obsługę procesów sprzedażowych i utrzymaniowych.
   - System okablowania strukturalnego zaprojektowano w wersji nieekranowanej ma posiadać wydajność klasy E zgodnie z normami referencyjnymi potwierdzoną przez uznane, niezależne laboratorium (np. 3P, GHMT) (lub równoważny).
   - Środowisko, w którym będzie instalowany osprzęt kablowy jest środowiskiem biurowym i zostało ono sklasyfikowane, jako łagodne wg skali $M_1I_1C_1E_1$
   - Podsystem okablowania poziomego w zakresie łączy miedzianych zrealizowany zostanie w oparciu o nieekranowany kabel Kategorii 6 w wersji ekranowania: U/UTP. W celu zagwarantowania niezbędnych marginesów pracy ze względu na długi okres użytkowania sieci kabel musi być przebadany w pasmie do 500 MHz. Osłona zewnętrzna musi być typu LSZH. Ze względu na gabaryty duktów przyjętych w projekcie dopuszcza się kable o średnicach zewnętrznych max. 5,4 mm W celach identyfikacyjnych wymaga się aby powłoka zewnętrzna kabla była w kolorze niebieskim.
   - Okablowanie ma być zrealizowane w oparciu o nieekranowany moduł gniazda RJ45 Kat. 6
   - Zgodnie z wymaganiami norm każdy 4–parowy kabel ma być trwale zakończony na ekranowanym module RJ45 umieszczonym w gnieździe od strony użytkownika oraz na panelu krosowym w szafie;
   - W celu zagwarantowania jak najwyższych marginesów pracy i zapasów parametrów transmisyjnych nie dopuszcza się rozwiązań złożonych z elementów różnych producentów, (tj. kabla, gniazd, kabli krosowych, itp.). Aby zagwarantować rzeczywiste i powtarzalne parametry toru oraz potwierdzić zgodność proponowanego rozwiązania z najnowszymi edycjami obowiązujących standardów międzynarodowych i niezależność od dostawcy komponentów wymagane jest na wezwanie Zamawiającego (tylko oferta wygrywająca) przedstawienie odpowiednich certyfikatów wydanych przez niezależne laboratoria uwzględniające najnowszą metodę kwalifikacji komponentów sieciowych.
3. Kable i przewody:

Okablowanie poziome ma być prowadzone nieekranowanym kablem typu: U/UTP o paśmie przenoszenia przewyższającym obowiązujące normy, min. 500 MHz w osłonie LSZH (powłoka wytwarzająca mało dymu, bezhalogenowa) o średnicy żyły: 23AWG (0,574mm), maksymalnej średnicy zewnętrznej 6,1 mm, koloru niebieskiego.

Tabela. Wymagane właściwości dla kabla miedzianego segmentu okablowania poziomego

Kategoria zgodnie z ISO11801 ed.2.2. (lub równoważny)	6
Klasyfikacja ogniowa	LSZH - IEC 60332-1; IEC 60754-2; IEC 61034
Ekranowanie	U/UTP
Klasa separacji	B
Zakres częstotliwości [MHz]	500

ø żył [AWG]	23
Max ø zewnętrzna kabla mm]	5,4
Min promień gięcia instalacja [mm]	45
Min promień gięcia użytkowanie [mm]	25
Max Waga [kg/km]	35,7
NVP	68

4. Testowanie:

Pomiary należy wykonać zgodnie z wymaganiami producenta okablowania strukturalnego oraz norm referencyjnych w szczególności:

- EN 50346:2002/A1:2007/A2:2009 Information Technology - Cabling system installation - Testing of installed cabling, wraz z jej polskim odpowiednikiem: PN-EN 50346:2004/A1:202009/A2:2010 Technika informatyczna - Instalacja okablowania - Badanie zainstalowanego okablowania (lub równoważne);
- EN 61935-1:2009 Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards, wraz z jej polskim odpowiednikiem: PN-EN 61935-1:2010E Wymagania dotyczące sprawdzania symetrycznych i współosiowych kablowych linii telekomunikacyjnych -- Część 1: Okablowanie z symetrycznych kabli telekomunikacyjnych zgodne z serią norm EN 50173 (lub równoważne);
- ISO/IEC 14763-3:2006/A1:2009 Information technology –Implementation and operation of customer premises cabling – Part 3: Testing of optical fibre cabling, wraz z jej polskim odpowiednikiem: PN-ISO/IEC 14763-3:2009/A1:2010P Technika informatyczna - Implementacja i obsługa okablowania w zabudowaniach użytkowych - Część 3: Testowanie okablowania światłowodowego (lub równoważne);

Zamawiający w odniesieniu do powyższych norm dopuszcza rozwiązania równoważne zgodne z poniższym opisem.

Mierniki użyte w procesie pomiarowym muszą uzyskać aprobatę producenta systemu okablowania

a) Testowanie statyczne powinno zostać wykonane testerem, który umożliwia sprawdzenie następujących cech poszczególnych odcinków kabli miedzianych:
   - zamiana przewodów w parze,
   - zamiana przewodów pomiędzy parami,
   - zwarcie w parze,
   - zwarcie między parami,
   - zwarcie do folii ekranującej,
   - brak połączenia.

b) Pomiary dynamiczne powinny zostać wykonane dla następujących parametrów linii:
   - mapa połączeń, ciągłość przewodów (wire map, continuity of conductors),
   - długość (Length),
   - rezystancja (DC Loop Resistance),
   - opóźnienie propagacji (Propagation Delay),
   - skośne opóźnienie propagacji (Delay Skew),
   - osłabienie sygnału częścią odbitą (Return Loss),
   - tłumienność (Attenuation),
   - przesłuch para-para na tym samym końcu kabla (Near End Crosstalk - NEXT),
   - stosunek tłumienności do przesłuchu (Attenuation to Crosstalk Ratio - ACR),
   - suma przesłuchów para-pozostałe 3 pary (Power Sum NEXT - PSNEXT),
   - równoważony przesłuch para-para na przeciwległych końcach kabla (Equal Level Far End Crosstalk – ELFEXT),
   - suma równoważonych przesłuchów para-pozostałe 3 pary na przeciwległych końcach kabla (Power Sum Equal Level Far End Crosstalk – PSELFEXT),
   - stosunek tłumienności do sumy przesłuchów (Power Sum ACR – PSACR).

c) Wyniki pomiarów dynamicznych wykonane miernikiem okablowania powinny zostać zamieszczone w formie wydruków w dokumentacji powykonawczej.

5. Termin realizacji:
   a) Powyższe czynności należy wykonać w okresie realizacji Zamówienia, po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym.
   b) Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w siedzibie Zamawiającego w pierwszym dniu roboczym następującym po pracach wdrożeniowo-instalacyjnych w godzinach od 7.00 do 15.00.

6. Opracowanie dokumentacji powykonawczej:
   a. Po zakończeniu robót Wykonawca zobowiązany jest przedłożyć Zamawiającemu dokumentację powykonawczą zawierającą mapy w skali 1:100 z dołączonymi pomiarami i testami sieci komputerowej oraz instalacji elektrycznej oraz opisem wykonanej instalacji. Dokumentacja powykonawcza powinna zawierać projekt sieci komputerowej, instalacji elektrycznej, z naniesionymi punktami dostępowymi wraz z przebiegiem trasy kablowej w pomieszczeniach Zamawiającego; powinna zawierać również zestawienie materiałów użytych do jej wykonania.
   b. Wymagana jest forma papierowa i elektroniczna dokumentacji, zatwierdzona przez osoby z odpowiednimi uprawnieniami (uprawnienia producenta okablowania do projektowania okablowania strukturalnego).
   c. Dokumentacja powinna zawierać konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania, które nie umożliwiają wyeksportowanie konfiguracji do pliku tekstowego bądź posiadają rozproszoną konfigurację).
   d. Dokumentacja powinna zawierać pliki pomiarów komputerowych, które muszą być nieprzetworzonymi plikami pobranymi bezpośrednio z miernika pomiarowego.
   e. Certyfikat producenta okablowania strukturalnego dla projektowanej kategorii/klasy, wyniki pomiarów dla wszystkich linii okablowania (wydruk z miernika), certyfikaty dopuszczenia do obrotu na użyte komponenty w instalacji (dostarcza producent lub przedstawiciel regionalny).

7. Gwarancja

Całość rozwiązania ma być objęta jednolitą, spójną 12-miesięczną gwarancją systemową, obejmującą całą część transmisyjną wraz z kablami krosowymi i innymi elementami dodatkowymi. Gwarancja ma być udzielona bezpośrednio klientowi końcowemu. Gwarancja systemowa ma być bezpłatną usługą serwisową oferowaną użytkownikowi końcowemu (inwestorowi) przez producenta okablowania. Musi obejmować ona swoim zakresem całość systemu okablowania od głównego punktu dystrybucyjnego do gniazda użytkownika i zawierać, podsystem okablowania szkieletowego i poziomego.
W celu uzyskania tego rodzaju gwarancji cały system musi być zainstalowany przez firmę instalacyjną posiadającą odpowiedni status uprawniający do udzielenia gwarancji producenta. Wniosek o udzielenie gwarancji składany przez firmę instalacyjną do producenta ma zawierać: listę zainstalowanych elementów systemu, wyciąg z dokumentacji powykonawczej podpisany przez projektanta oraz instalatora, wyniki pomiarów dynamicznych typu Permanent Link wszystkich torów transmisyjnych według norm ISO/IEC 11801 ed. 2.2 lub EN 50173-1 (lub równoważnych).

4.9 Szkolenia kadry dotyczące polityki bezpieczeństwa sieci

Zamawiający wymaga przeprowadzenia szkolenia / instruktażu stanowiskowego dla pracowników Zamawiającego, zgodnie z poniższymi założeniami.

Forma szkolenia	Szkolenie online
Czas trwania szkolenia	8 godz. dydaktycznych (1 dzień)
Język szkolenia	Polski
Liczba osób	Max. 5

Program szkolenia / podstawowe kwestie poruszone na szkoleniu	• Podstawy bezpieczeństwa sieciowego
	• Zabezpieczenia techniczne sieci internetowych
	• Monitoring i detekcja sieci
	• Zarządzanie bezpieczeństwem sieciowym
	  ○ Monitoring i detekcja
	  ○ Procedury operacyjne
	  ○ Ciągłość działania
	  ○ Audyt i zgodność
	• Zasady korzystania z sieci

Dokumenty	Zaświadczenie o ukończeniu szkolenia

4.10 Szkolenia kadry dotyczące konfiguracji access pointów

Zamawiający wymaga przeprowadzenia szkolenia / instruktażu stanowiskowego dla pracowników Zamawiającego, zgodnie z poniższymi założeniami.

Forma szkolenia	Szkolenie online
Czas trwania szkolenia	8 godz. dydaktycznych (1 dzień)
Język szkolenia	Polski
Liczba osób	Max. 5
Program szkolenia / podstawowe kwestie poruszone na szkoleniu	• Możliwości techniczne dostarczonego rozwiązania, w tym AP • Zasady konfiguracji sieci WiFi • Zasady tworzenia VLAN • Możliwości zarządzania siecią z wykorzystaniem kontrolera i oferowanych rozwiązań • Zasady konfiguracji AP i przełączników w zakresie VLAN • Konfiguracja zabezpieczeń AP i VLAN • Optymalizacja sieci bezprzewodowej
Dokumenty	Zaświadczenie o ukończeniu szkolenia