Załącznik nr 8 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA
(CZĘŚĆ TECHNICZNA)

Dostawa i wdrożenie infrastruktury IT oraz oprogramowania
w ramach projektu grantowego
pn. “Cyberbezpieczny Samorząd”
Priorytet II: Zaawansowane usługi cyfrowe
Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa
Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

48620000-0	Systemy operacyjne
48000000-8	Pakiety oprogramowania i systemy informatyczne
48710000-8	Pakiety oprogramowania do kopii zapasowych i odzyskiwania
48820000-2	Serwery
48821000-9	Serwery sieciowe
48823000-3	Serwery plików
72265000-0	Usługi konfiguracji oprogramowania
32428000-9	Modernizacja sieci
32420000-3	Urządzenia sieciowe
80500000-9	Usługi szkoleniowe

Zawartość:

I. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO

1. Wprowadzenie.

Celem realizowanego projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Realizacja projektu poprzez wsparcie grantowe jednostek samorządowych, będzie obejmowała:

A) wdrożenie lub aktualizację polityk bezpieczeństwa informacji (SZBI) a także przeprowadzenie w JST audytów SZBI - zadanie objęte odrębnym postępowaniem;

B) wdrożenie technologii i systemów teleinformatycznych podnoszących poziom bezpieczeństwa informacji oraz środków zwiększających odporność - zgodnie z obowiązującymi przepisami prawa (w tym z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności) a także z uwzględnieniem uznanych norm, standardów i rekomendacji w obrocie profesjonalnym;

C) podniesienie poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie - zadanie objęte odrębnym postępowaniem.

2. Zakres przedmiotu zamówienia.

Przedmiotem zamówienia jest dostawa sprzętu oraz oprogramowania IT oraz wdrożenie systemów i rozwiązań teleinformatycznych (instalacja, konfiguracja i integracja) mających na celu podniesienie poziomu Cyberbezpieczeństwa oraz zwiększenie odporności Jednostki w ramach projektu grantowego pn. „Cyberbezpieczny Samorząd" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC). Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Zakres zamówienia składa się z następujących zadań:

1. Dostawa, instalacja oraz konfiguracja urządzeń sieci WLAN i LAN w Urzędzie Gminy Miejsce Piastowe

- Punkt dostępowy 802.11be zgodny z Wi-Fi 7 – 10 szt.
- Przełącznik sieciowy 48-port typ 1 – 2 szt.
- Przełącznik sieciowy 48-port typ 2 – 2 szt.
- Przełącznik sieciowy 16-port – 2 szt.
- Kontroler sieciowy - 1 szt.

2. Dostawa oraz konfiguracja urządzeń sieci WLAN i LAN klasy Enterprise w Gminnym Ośrodku Pomocy Społecznej w Miejscu Piastowym

- Przełącznik sieciowy 24-port – 1 szt.
- Punkt dostępowy 802.11ax zgodny z Wi-Fi 6 – 2 szt.

3. Dostawa oraz konfiguracja urządzeń sieci WLAN i LAN klasy Enterprise w Szkoła Podstawowa w Głowience, Szkoła Podstawowa w Łężanach, Szkoła Podstawowa w Miejscu Piastowym, Szkoła Podstawowa w Rogach, Szkoła Podstawowa Targowiskach, Szkoła Podstawowa we Wrocance, Szkoła Podstawowa w Zalesiu.

- Przełącznik sieciowy 24-port typ 1 – 7 szt.
- Przełącznik sieciowy 24-port typ 2 – 7 szt.

- Punkt dostępowy 802.11ax zgodny z Wi-Fi 6 – 71 szt.

4. Dostawa, instalacja oraz konfiguracji urządzenia typu NGFW, implementacja mechanizmów bezpieczeństwa sieciowego w Urzędzie Gminy Miejsce Piastowe
- NGFW wraz z licencjami – 1 szt.
- Zakres prac konfiguracyjnych i wdrożeniowych.

5. Dostawa, instalacja oraz konfiguracja urządzeń typu NGFW, implementacja mechanizmów bezpieczeństwa sieciowego w Gminny Ośrodek Pomocy Społecznej w Miejscu Piastowym, Szkoła Podstawowa w Głowience, Szkoła Podstawowa w Łężanach, Szkoła Podstawowa w Miejscu Piastowym, Szkoła Podstawowa w Rogach, Szkoła Podstawowa Targowiskach, Szkoła Podstawowa we Wrocance, Szkoła Podstawowa w Zalesiu.
- Urządzenie NGFW – 8 kpl.

6. Zakup platformy serwerowej wraz z odpowiednim środowiskiem systemowym na potrzeby wdrożenia usług katalogowych i systemu zarządzania tożsamością w Urzędzie Gminy Miejsce Piastowe
- Serwer wirtualizacji typ 1 – 1 szt.
- Oprogramowanie systemowe i wirtualizacyjne – 1 kpl.
- Platforma zarządzająca urządzeniami NGFW
- Oprogramowanie do zbierania, analizowania i wizualizowania danych
- Usługi instalacji, konfiguracji, wdrożenia oraz migracji systemów

7. Zakup platformy serwerowej wraz z odpowiednim środowiskiem systemowym na potrzeby wdrożenia usług katalogowych w Gminny Ośrodek Pomocy Społecznej w Miejscu Piastowym
- Serwer typ 2 – 1 szt.
- Oprogramowanie systemowe – 1 kpl.

8. Zakup i wdrożenie dedykowanych serwerów NAS do wykonywania kopii zapasowych w Urzędzie Gminy Miejsce Piastowe.
- Serwer NAS – 1 szt.
- Dysk NAS 8TB– 8 szt.
- Polityka tworzenia i odtwarzania backup.

9. Zakup i wdrożenie dedykowanych serwerów NAS do wykonywania kopii zapasowych w Szkoła Podstawowa w Głowience, Szkoła Podstawowa w Łężanach, Szkoła Podstawowa w Miejscu Piastowym, Szkoła Podstawowa w Rogach, Szkoła Podstawowa Targowiskach, Szkoła Podstawowa we Wrocance, Szkoła Podstawowa w Zalesiu
- Serwer NAS – 7 kpl.

10. Dostawa kompleksowego rozwiązania typu antywirus – zarządzanego centralnie
- Oprogramowanie Antywirus – 100 lic.

11. Wdrożenie Systemu Centralnej Autoryzacji, AD, MFA, VPN.
- Serwer Centralnej Autoryzacji – 1 kpl.
- Karty elektroniczne dla systemu MFA – 50 szt.
- Czytniki kart elektronicznych dla systemu MFA – 45 szt.
- Zakres prac konfiguracyjnych i wdrożeniowych – 1 kpl.

12. Usługi zewnętrzne zwiększające poziom bezpieczeństwa informacji tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych – wsparcie i monitoring.

3. Ogólne wymagania Zamawiającego.

Niniejszy dokument ma celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawę oprogramowania i urządzeń, wdrożenie rozwiązań oraz zapewnienie innych usług teleinformatycznych, których podstawowym celem jest podniesienie poziomu bezpieczeństwa informacji oraz zwiększenie odporności JST, w ramach projektu „Cyberbezpieczny Samorząd". Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych i jakościowych, oraz wskazuje technologie, które muszą być wykorzystane tak aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.
Opisane w dokumencie wymagania należy traktować jako podstawowe i minimalne.
Tam, gdzie w opisie przedmiotu zamówienia został wskazany znak towarowy (marka), producent, dostawca, patent, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczone przez konkretnego Dostawcę lub nastąpiło wskazanie norm, europejskich ocen technicznych, wspólnych specyfikacji technicznych lub innych odniesień, o których mowa w art. 101 ust. 1 pkt 2 lub ust. 3 ustawy, Zamawiający zgodnie z art. 99 ust. 5 ustawy dopuszcza złożenie oferty równoważnej lub z godnie z art. 101 ust. 4 ustawy zaoferowanie rozwiązań „równoważnych" w stosunku do wskazanych w opisie przedmiotu zamówienia pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych od założonych w SWZ.
Ciężar wykazania spełnienia tych wymagań leży po stronie wykonawcy w składanej ofercie lub jeżeli ten przypadek ma miejsce w trakcie realizacji umowy – w chwili zaistnienia konieczności dokonania takiej zmiany.
- W przypadku zastosowania zasad wskazanych powyżej w trakcie realizacji umowy, mogą one wystąpić pod warunkiem, że zmiany te nie będą wpływać na oferowany w ofercie przedmiot zamówienia i efekt zakreślony niniejszym OPZ.
- W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

Wymagania ogólne dotyczące sprzętu:

1) Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane po dniu 30 czerwca 2024r.
2) Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji, nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego czy w zakresie gwarancji producenta.
3) Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.
4) Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.

5) Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów.
6) Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.
7) Serwis sprzętu będzie świadczony przez producenta lub jego autoryzowanego partnera serwisowego posiadającego wdrożoną normę min. PN-EN ISO 9001 lub równoważną.
8) Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty 24 miesięczną gwarancją i wsparciem producenta, chyba że okres i warunki gwarancji zostały dodatkowo określony w opisie szczegółowym specyfikowanego wyposażenia/sprzętu. W okresie gwarancji Wykonawca jest zobowiązany zapewnić Zamawiającemu:
    a. usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia,
    b. przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (faks lub e-mail) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy),
    c. dostęp do bezpośredniego wsparcia technicznego producenta wraz z prawem do aktualizacji oprogramowania systemowego.
9) W ramach gwarancji wymagane jest wsparcie producenta sprzętu, a czas reakcji na zgłoszenia będzie realizowany w trybie następny dzień roboczy w miejscu instalacji i zastrzeżeniem, że uszkodzone nośniki danych pozostają u Zamawiającego. Ponadto wymagane jest, aby dostarczony poziom wsparcia producenta dawał możliwość kategoryzacji zgłoszeń i w przypadku awarii krytycznych gwarantował natychmiastową pomoc telefoniczną, szybką interwencję specjalisty ds. eskalacji zgłoszeń oraz wizytę serwisanta i/lub wysyłkę uszkodzonych części.
10) Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.

Wymagania ogólne dotyczące oprogramowania:

Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1) certyfikaty licencyjne wystawione przez producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
2) nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
3) adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
4) zestawienie dostarczonych Zamawiającemu pozycji w zakresie Oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego;

5) standardowe warunki licencyjne producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
6) standardowe warunki Wsparcia technicznego producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
7) oświadczenie producenta Oprogramowania potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki Wsparcia technicznego.

Wymagania w zakresie dokumentacji technicznej:

Przed rozpoczęciem prac wdrożeniowych, Wykonawca zobowiązany jest do opracowania dokumentacji technicznej (koncepcji technicznej wdrożenia) na podstawie wcześniej przeprowadzonej analizy przedwdrożeniowej oraz z uwzględnieniem wymagań warunków zamówienia. Zakres dokumentacji technicznej powinien obejmować:

A) Projekt techniczny wdrożenia.
B) Harmonogram Wdrożenia.
C) Dokumentację Powykonawczą (po zakończeniu realizacji prac wdrożeniowych).

1) Dokumentacja powinna zawierać schematy i architekturę wdrażanych systemów i rozwiązań, konfigurację urządzeń oraz właściwości i funkcjonalności pozwalające na poprawną z punktu widzenia technicznego eksploatację.
2) Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja warunkuje rozpoczęcie prac Wykonawcy.

Pozostałe wymagania:

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.
Wykonawca zobowiązany jest do powołania zespołu zajmującego się realizacją przedmiotu zamówienia składającego się co najmniej z:

A) Kierownika Projekt ze strony Wykonawcy;
B) Zespołu inżynierów odpowiedzialnych za konkretne obszary wdrożenia.

II. SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO - UŻYTKOWE

1. Dostawa, instalacja oraz konfiguracja urządzeń sieci WLAN i LAN w Urzędzie Gminy Miejsce Piastowe.

Przed przystąpieniem do prac instalacyjno-wdrożeniowych, należy opracować koncepcję techniczną w zakresie rozbudowy i modernizacji sieci LAN/WiFi.

Koncepcja powinna obejmować:

a) część instalacyjno-montażową;
b) część aktywną związaną z zaplanowaniem architektury sieci i zakresu konfiguracji urządzeń aktywnych. Należy przygotować koncepcję wdrożenia uwzględniając hierarchiczny model projektowania i budowy sieci tj. wydzielając warstwę dystrybucyjną oraz dostępową.

1.1. Koncepcja wdrożenia.

W ramach zamówienia należy dostarczyć, zainstalować oraz skonfigurować urządzenia aktywne sieci tj. Przełączniki oraz urządzenia sieci bezprzewodowej.
Należy przygotować koncepcję wdrożenia uwzględniając hierarchiczny model projektowania i budowy sieci. Ponadto wymagana będzie segmentacja sieci w oparciu o technologię 802.1Q (VLAN) oraz konfiguracja innych mechanizmów sieciowych które przyczynią sie do poprawy bezpieczeństwa, wydajności i dostępność oraz sieci wewnętrznej LAN.

Zamówienie obejmuję dostawę, instalację oraz konfigurację kontrolera sieciowego, do którego należy podłączyć nowo dostarczane przełączniki sieciowe jednostek podległych, biorące udział w projekcie.
Dodatkowo zamówienie obejmuje dostawę, konfigurację oraz wymianę (10 szt.) istniejących punktów dostępowych na nowe w budynku Urzędu Gminy. Nowe punkty dostępowe należy skonfigurować z istniejącym kontrolerem sieci bezprzewodowej.

Zakres prac instalacyjno-wdrożeniowych powinien obejmować co najmniej:

a) Część pasywna:
   - Montaż 10 szt. urządzeń bezprzewodowych w ramach istniejącego okablowania w budynku Urzędu Gmin;
   - Instalacja przełączników sieci LAN (6 szt.).
b) Część aktywna:
   - Podłączenie urządzeń aktywnych sieci tj. Przełączniki sieciowe (16-portowe 2 szt.) oraz punkty dostępowe (10 szt.) do istniejącego kontrolera;
   - Konfiguracja nowego kontrolera sieciowego;
   - Wykonanie segmentacji wyodrębniając minimum 10 sieci zaproponowanych przez zamawiającego w oparciu o technologię 802.1Q;
   - Dostosowanie konfiguracji istniejących przełączników do nowo tworzonych vlanów;
   - Konfigurację mechanizmów STP;
   - Dodatkowo w celu ograniczenia niepożądanego ruchu w warstwie 2 wskazana jest izolacja poszczególnych komputerów (port isolation).

1.1.1. Punkt dostępowy 802.11be zgodny z Wi-Fi 7 – 10 szt.

Wymagania ogólne:

Parametr lub warunek	Minimalne wymagania
Wymagania Ogólne	Sufitowy, trzy-zakresowy punkt dostępowy pracujący w standardzie 802.11a/b/g/n/ac/ax/be zgodny z Wi-Fi 7. Zasilane przez PoE 802.3at
Port LAN	1 x 1/2.5 GbE RJ45
Antena	2.4 GHz 4 dBi 5 GHz 6 dBi 6 GHz 5.8 dBi
Zgodność z Hotspot 2.0	tak
Zasilanie	802.3at PoE+
Pobór mocy	21W
Moc nadawania 2,4GHz	22 dBm
Moc nadawania 5GHz	26 dBm
Moc nadawania 6GHz	23 dBm
Pasmo	802.11a/b/g/n/ac/ax/be
Ilość SSID	8 per radio
Temperatura pracy	-30 to 60° C (-22 to 140° F)
Wilgotność pracy	od 5 do 90% niekondensująca
Certyfikaty	CE, FCC, IC
Obsługa VLAN	802.1Q
Klienci równoczesni	300+
Prędkość	802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b 1, 2, 5.5, 11 Mbps 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n 6.5 Mbps do 300 Mbps (MCS0 - MCS15, HT 20/40) 802.11ac (WiFi 5) 6.5 Mbps do 1.7 Gbps (MCS0 - MCS9 NSS1/2, VHT 20/40/80/160) 802.11ax (WiFi 6/6E) 7.3 Mbps do 2.4 Gbps (MCS0 - MCS11 NSS1/2, HE 20/40/80/160) 802.11be (WiFi 7) 7.3 Mbps do 5.7 Gbps (MCS0 - MCS13 NSS1/2, EHT 20/40/80/160/240/320)
Zarządzanie	zarządzanie i konfigurowanie przez kontroler sieciowy
Funkcjonalność	802.1x oraz URL redirect (guest)
Gwarancja	Urządzenie dostarczone z minimum 24 msc gwarancji i wsparcia producenta lub wykonawcy

1.1.2. Przełącznik sieciowy 48-port typ 1 – 2 szt.

Wymagania ogólne:

- Typ i liczba portów - 48x 10/100/1000 RJ45, 4x 10Gigabit Ethernet SFP+
- Obudowa 1U, rackmount (dostarczone uchwyty montażowe)
- Możliwość stackowania przełączników – do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym Link Aggregation i port mirroring

1. Zarządzenie energią:
   - Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)
   - Możliwość wyłączenia diod LED w celu oszczędzania energii
2. Parametry wydajnościowe:
   - Przełącznik line-rate zapewniający pracę z pełną wydajnością wszystkich interfejsów
   - Pamięć DRAM – 1GB
   - Pamięć Flash – 512MB
   - Wielkość bufora pakietów – 1.5MB
   - Obsługa 4000 sieci VLAN
   - 16.000 adresów MAC
   - Wire-speed IPv4 routing – 990 tras statycznych; 128 interfejsów IP
   - Obsługa ramek jumbo – do 9000 bajtów
   - 2000 IGMP group
   - 8 połączeń zagregowanych typu „port channel”
   - Ilość wpisów w listach kontroli dostępu Security ACL – 1000
3. Obsługa protokołu SNTP
4. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
5. Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   - IEEE 802.1w Rapid Spanning Tree
   - IEEE 802.1s Multi-Instance Spanning Tree
   - Per-VLAN Rapid Spanning Tree (PVRST+)
   - Obsługa 126 instancji protokołu STP
7. Obsługa protokołu LLDP i LLDP-MED
8. Obsługa Q-in-Q oraz Selective Q-in-Q
9. Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)
10. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
11. Możliwość uruchomienia funkcji serwera DHCP
12. Mechanizmy związane z bezpieczeństwem sieci:
    - Wiele poziomów dostępu administracyjnego poprzez konsolę
    - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    - Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard
    - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
    - Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community

- Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priorty, TCP flag. Obsługa czasowych list ACL
- Obsługa mechanizmów zapewaniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]
- Bezpieczny proces bootowania urządzenia
- Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika

13. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    - Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
    - Kontrola sztormów dla ruchu broadcast/multicast/unicast
    - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
    - Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu
14. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN z możliwością konfiguracji do 4 sesji monitorujących
15. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
16. Obsługa protokołu sFlow
17. Zarządzanie:
    - Port konsoli – USB typu C i RJ45
    - Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia
    - Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP
    - Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami
    - Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
    - Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu
18. Zasilacz AC 230V
19. Praca w szerokim zakresie temperatur: -5^{o}C – 50^{o}C
20. Głębokość urządzenia nie przekracza 35cm

1.1.3. Przełącznik sieciowy 48-port typ 2 – 2 szt.

Wymagania ogólne:

- Typ i liczba portów - 48x 10/100/1000 POE+ RJ45, 4x 10Gigabit Ethernet SFP+
- Budżet mocy dla POE – 370W
- Obudowa 1U, rackmount (dostarczone uchwyty montażowe)
- Możliwość stackowania przełączników – do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym Link Aggregation i port mirroring

Zarządzenie energią:

- Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)
- Zasilanie PoE można włączać i wyłączać w oparciu o harmonogram zdefiniowany przez użytkownika w celu oszczędzania energii (modele z obsługą POE)
- Zapewnia zasilanie PoE podczas restartu urządzenia (modele z obsługą POE)
- Możliwość wyłączenia diod LED w celu oszczędzania energii

Parametry wydajnościowe:

- Przełącznik line-rate zapewniający pracę z pełną wydajnością wszystkich interfejsów
- Pamięć DRAM – 1GB
- Pamięć Flash – 512MB
- Wydajność przełączania – 176 Gbps i 130 Mpps
- Wielkość bufora pakietów – 1.5MB
- Obsługa 4000 sieci VLAN
- 16.000 adresów MAC
- Wire-speed IPv4 routing – 990 tras statycznych; 128 interfejsów IP
- Obsługa ramek jumbo – do 9000 bajtów
- 2000 IGMP group
- 8 połączeń zagregowanych typu „port channel”
- Ilość wpisów w listach kontroli dostępu Security ACL – 1000

Obsługa protokołu SNTP
Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2.
Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

- IEEE 802.1w Rapid Spanning Tree
- IEEE 802.1s Multi-Instance Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- Obsługa 126 instancji protokołu STP

Obsługa protokołu LLDP i LLDP-MED
Obsługa Q-in-Q oraz Selective Q-in-Q
Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)
Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
Możliwość uruchomienia funkcji serwera DHCP
Mechanizmy związane z bezpieczeństwem sieci:

- Wiele poziomów dostępu administracyjnego poprzez konsolę
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard

- Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
- Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community
- Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priorty, TCP flag. Obsługa czasowych list ACL
- Obsługa mechanizmów zapewaniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]
- Bezpieczny proces bootowania urządzenia
- Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika

Mechanizmy związane z zapewnieniem jakości usług w sieci:

- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
- Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek
- Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
- Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu

Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN z możliwością konfiguracji do 4 sesji monitorujących.
Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
Obsługa protokołu sFlow.
Zarządzanie:

- Port konsoli – USB typu C i RJ45
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia
- Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP
- Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
- Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu

Zasilacz AC 230V.
Praca w szerokim zakresie temperatur: 0^{o}C – 50^{o}C.
Głębokość urządzenia nie przekracza 35cm.

1.1.4. Przełącznik sieciowy 16-port – 2 szt.

Wymagania ogólne:

Materiał obudowy	Stal SGCC
Interfejs zarządzania	Ethernet In-Band
Interfejs sieciowy	(16) portów GbE RJ45 (2) porty 1G SFP
Interfejs PoE	(8) PoE/PoE+ (Piny 1, 2+; 3, 6-)
Całkowita przepustowość bezblokująca	Min. 18 Gbps
Pojemność przełączania	Min. 36 Gbps
Wskaźnik przekazywania	Min. 26,78 Mpps
Metoda zasilania	Uniwersalne wejście, 100–240V AC, 50/60 Hz
Zasilanie	AC/DC, wewnętrzne, 60W
Obsługiwany zakres napięcia	100–240V AC
Maks. pobór mocy	Min. 18W (Bez wyjścia PoE)
Całkowita dostępna moc PoE	Min. 2W
Maks. moc PoE na port według PSE	PoE+: 32W
Zakres napięcia trybu PoE	PoE: 44–57V PoE+: 50–57V
Ochrona ESD/EMP	Powietrze: ± 16kV, kontakt: ± 12kV
Wyświetlacz LCM	(1) dotykowy 1,3"
Przycisk	Resetowanie fabryczne
Wstrząsy i wibracje	Standard ETSI300-019-1.4
Temperatura pracy otoczenia	-5 do 40° C (23 do 104° F)
Wilgotność pracy otoczenia	10 do 90% bez kondensacji
Certyfikacje	CE, FCC, IC
Min. Funkcje warstwy 2	Miksowanie IGMP STP / RSTP z priorytetami i wyłączaniem na poziomie portu Izolacja portu Kontrola burzowa VLAN głosowa Lustro portu Agregacja portu LACP Ograniczenie szybkości multicast / broadcast Blokada adresu MAC Kontrola przepływu Kontrola 802.1X Ramki Jumbo Ochrona pętli własnej Miksowanie DHCP / ochrona Limit prędkości egress LLDP-MED Port ograniczony przez MAC Izolacja urządzenia za pomocą list ACL
Funkcje warstwy 3	–
Diody LED	
System	Status
Ethernet	PoE Prędkość/link/aktywność
SFP	Link/aktywność
Wymiary	442 x 200 x 44 mm (17,4 x 7,9 x 1,7")
Waga	Bez uchwytów montażowych: 2,8 kg (6,2 funta) Z uchwytami montażowymi: 2,9 kg (6,4 funta)
Gwarancja	Urządzenie dostarczone z minimum 24 msc gwarancji i wsparcia producenta lub wykonawcy

1.1.5. Kontroler sieciowy - 1 szt.

Wymagania ogólne:

Obsługiwana liczba urządzeń	500
Standardy	802.1x
Zarządzanie, monitorowanie, konfiguracja	• Automatyczne wykrywanie urządzeń • Konfiguracje grupowe • Grupowe aktualizacje firmware'ów • Inteligentne monitorowanie stanu sieci • Ostrzeżenia o nietypowych zdarzeniach • Ujednolicony proces konfiguracji • Harmonogram restartu • Spersonalizowana strona logowania do sieci
Porty we/wy	• 2 x 10/100/1000 Mbit/s • 1 x USB 3.0
Wymagania środowiskowe	• Dopuszczalna temperatura pracy: 0~50 st. C • Dopuszczalna temperatura przechowywania: -40~70 st. C • Dopuszczalna wilgotność powietrza: 10%~90%, bez kondensacji • Dopuszczalna temperatura przechowywania: 5%~90%, bez kondensacji
Zasilanie	100-240 V~50/60 Hz, 0,6 A
Akcesoria w zestawie	• Kontroler sprzętowy Omada OC300 • Instrukcja szybkiej konfiguracji • Kabel Ethernet • Przewód zasilający • Zestaw do montażu w szafie rack
Kolor	Czarny
Wymiary	294 × 180 × 44 mm
Pozostałe parametry	• Dostęp do chmury • Zarządzanie L3 • Zarządzanie multi-site

2. Dostawa oraz konfiguracja urządzeń sieci WLAN i LAN klasy Enterprise w Gminnym Ośrodku Pomocy Społecznej w Miejscu Piastowym.

Przed przystąpieniem do prac instalacyjno-wdrożeniowych, należy opracować koncepcję techniczną w zakresie rozbudowy i modernizacji sieci LAN/WiFi.

2.1. Koncepcja wdrożenia.

W ramach zamówienia należy dostarczyć oraz skonfigurować urządzenia aktywne sieci tj. Przełącznik oraz urządzenia sieci bezprzewodowej.
Należy przygotować koncepcję wdrożenia uwzględniając hierarchiczny model projektowania i budowy sieci. Ponadto wymagana będzie segmentacja sieci w oparciu o technologię 802.1Q (VLAN) oraz konfiguracja innych mechanizmów sieciowych które przyczynią sie do poprawy bezpieczeństwa, wydajności i dostępność oraz sieci wewnętrznej LAN.

Zamówienie obejmuję dostawę, instalację oraz konfigurację Przełącznika sieciowego, który należy podłączyć do nowo dostarczanego kontrolera sieciowego zlokalizowanego w Urzędzie Gminy Miejsce Piastowe.
Dodatkowo zamówienie obejmuje dostawę oraz konfigurację (2 szt.) punktów dostępowych. Nowe punkty dostępowe należy skonfigurować z istniejącym kontrolerem sieci bezprzewodowej zlokalizowanym w Urzędzie Gminy Miejsce Piastowe.

Zakres prac instalacyjno-wdrożeniowych powinien obejmować co najmniej:

a) Część pasywna:
- Instalacja przełączników sieci LAN;

b) Część aktywna:
- Podłączenie urządzeń aktywnych sieci tj. Przełączniki oraz punkty dostępowe do kontrolerów zlokalizowanych w Urzędzie Gminy Miejsce Piastowe;
- wykonanie segmentacji sieci (serwery, peryferia, stacje robocze) w oparciu o technologię 802.1Q;
- Dostosowanie konfiguracji istniejących przełączników do nowo tworzonych vlanów;
- konfigurację mechanizmów STP;
- dodatkowo w celu ograniczenia niepożądanego ruchu w warstwie 2 wskazana jest izolacja poszczególnych komputerów (port isolation).

2.1.1. Przełącznik sieciowy 24 - port – 1 szt.

Wymagania ogólne:

Klasa przełącznika	Zarządzalny
Zastosowanie	Średnie i duże firmy
Architektura sieci	GigabitEthernet
Liczba portów 10/100/1000 Mbps	24
Liczba portów SFP+	4
Port konsoli	Tak
Przepustowość	128 Gb/s
Prędkość przekazywania	95.23 Mpps
Rozmiar tablicy adresów MAC	16
Obsługa ramek Jumbo	Tak
Rozmiar ramki Jumbo	9 KB
Bezpieczeństwo	• Izolacja portów • Bezpieczne zarządzanie siecią przez HTTPS z SSLv3 / TLS 1.2 • Zarządzanie bezpiecznym interfejsem wiersza poleceń (CLI) z SSHv1 / SSHv2 • Kontrola dostępu oparta na IP / Port / MAC
Zarządzanie, monitorowanie, konfiguracja	• Automatyczna instalacja DHCP • Podwójny obraz, podwójna konfiguracja • Monitorowanie procesora • Diagnostyka kabli • EEE • Odzyskiwanie hasła • SNTP • Dziennik systemu
Typ obudowy	Desktop
Wentylator	Nie
Zasilacz	Zewnętrzny
Pobór mocy	23.6 W
Akcesoria w zestawie	• Przełącznik • Przewód zasilający • Skrócona instrukcja instalacji • Zestaw do montażu w racku • Gumowe nóżki
Zasilanie	100-240 V AC ~ 50/60 Hz
Wymiary	440 × 180 × 44 mm

2.1.2. Punkt dostępowy 802.11ax zgodny z Wi-Fi 6 – 2 szt.

Wymagania ogólne:

Parametr lub warunek	Minimalne wymagania
Wymagania Ogólne	Sufitowy, dwu-zakresowy punkt dostępowy pracujący w standardzie 802.11a/b/g/n/ac/ax zgodny z Wi-Fi 6. Zasilane przez PoE 802.3af/at lub paswyne PoE 48V.
Port LAN	1 x GbE RJ45 port
Antena	2.4 GHz 4 dBi 5 GHz 6 dBi
Zgodność z Hotspot 2.0	tak
Zasilanie	802.3af PoE, passive PoE (48V)
Pobór mocy	13W
Moc nadawania 2,4GHz	22 dBm
Moc nadawania 5GHz	26 dBm
Pasmo	802.11a/b/g/n/ac/ax
Ilość SSID	8 per radio
Temperatura pracy	-30 to 60° C (-22 to 140° F)
Wilgotność pracy	od 5 do 90% niekondensująca
Certyfikaty	CE, FCC, IC
Obsługa VLAN	802.1Q
Klienci równoczesni	300+
Prędkość	802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b 1, 2, 5.5, 11 Mbps 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n 6.5 Mbps do 600 Mbps (MCS0 - MCS31, HT 20/40) 802.11ac 6.5 Mbps do 3.4 Gbps (MCS0 - MCS9 NSS1/2/3/4, VHT 20/40/80/160) 802.11ax 7.3 Mbps do 4.8 Gbps (MCS0 - MCS11 NSS1/2/3/4, HE 20/40/80/160)
Zarządzanie	zarządzanie i konfigurowanie przez kontroler
Funkcjonalność	802.1x oraz URL redirect (guest)
Gwarancja	Urządzenie dostarczone z minimum 24 msc gwarancji i wsparcia producenta lub wykonawcy

3. Dostawa oraz konfiguracja urządzeń sieci WLAN i LAN klasy Enterprise w Szkoła Podstawowa w Głowience, Szkoła Podstawowa w Łężanach, Szkoła Podstawowa w Miejscu Piastowym, Szkoła Podstawowa w Rogach, Szkoła Podstawowa Targowiskach, Szkoła Podstawowa we Wrocance, Szkoła Podstawowa w Zalesiu.

Przed przystąpieniem do prac instalacyjno-wdrożeniowych, należy opracować koncepcję techniczną w zakresie rozbudowy i modernizacji sieci LAN/WiFi.

3.1. Koncepcja wdrożenia.

W ramach zamówienia należy dostarczyć oraz skonfigurować urządzenia aktywne sieci tj. Przełączniki (14 szt.) oraz punkty dostępowe sieci bezprzewodowej (71 szt.). Lokalizacja urządzeń aktywnych sieci znajduje się w poniżej tabeli:

	Przełącznik Sieciowy typ 1	Przełącznik Sieciowy typ 2	Punkt dostępowy
SP im. Benedykta Wierdaka w Głowience	1	1	8
SP im. Tadeusza Kościuszki w Łężanach	1	1	7
SP im. Tytusa Trzecieskiego w Miejscu Piastowym	1	1	17
SP im. Kazimierza Wielkiego w Rogach	1	1	15
SP im. Św. Jana Kantego w Targowiskach	1	1	10
SP im. Stanisławy Grelli we Wrocance	1	1	7
SP im. Józefa Piłsudskiego w Zalesiu	1	1	7

Należy przygotować koncepcję wdrożenia uwzględniając hierarchiczny model projektowania i budowy sieci. Ponadto wymagana będzie segmentacja sieci w oparciu o technologię 802.1Q (VLAN) oraz konfiguracja innych mechanizmów sieciowych które przyczynią się do poprawy bezpieczeństwa, wydajności i dostępność oraz sieci wewnętrznej LAN.

Zamówienie obejmuję dostawę, instalację oraz konfigurację Przełączników sieciowych (14 szt.), które należy podłączyć do nowo dostarczanego kontrolera sieciowego zlokalizowanego w Urzędzie Gminy Miejsce Piastowe.
Dodatkowo zamówienie obejmuje dostawę oraz konfigurację (71 szt.) punktów dostępowych Nowe punkty dostępowe należy skonfigurować z istniejącym kontrolerem sieci bezprzewodowej zlokalizowanym w Urzędzie Gminy Miejsce Piastowe.

Zakres prac instalacyjno-wdrożeniowych powinien obejmować co najmniej:

a) Część pasywna:
- Instalacja przełączników sieci LAN;

b) Część aktywna:
- Podłączenie urządzeń aktywnych sieci tj. Przełączniki oraz punkty dostępowe do kontrolerów zlokalizowanych w Urzędzie Gminy Miejsce Piastowe;
- wykonanie segmentacji sieci (serwery, peryferia, stacje robocze) w oparciu o technologię 802.1Q;
- konfigurację mechanizmów STP;
- dodatkowo w celu ograniczenia niepożądanego ruchu w warstwie 2 wskazana jest izolacja poszczególnych komputerów (port isolation).

3.1.1. Przełącznik sieciowy 24-port typ 1 – 7 szt.

Wymagania ogólne:

Porty	• 24 Porty RJ45 10/100/1000 Mb/s • 4 Gigabitowe Sloty SFP • 1 Port konsolowy RJ45 • 1 Port konsolowy Micro-USB
Ilość wentylatorów	Bezwentylatorowy
Zasilanie	100-240 V AC~50/60 Hz
Wymiary (S x G x W)	440 × 180 × 44 mm
Montaż	Szafa Rack
Wydajność przełączania	56 Gb/s
Szybkość przekierowań pakietów	41.66 Mpps
Ramki jumbo	9 KB
Funkcja Quality of Service	• 8 kolejek priorytetów • Priorytetowanie 802.1p CoS/DSCP • Planowanie kolejki - SP (Strict Priority) - WRR (Weighted Round Robin) - SP+WRR • Kontrola przepustowości - Ograniczenie przepustowości bazując na Port/Przepływ • Płynniejsza wydajność • Action for Flows - Mirror (do wspieranego interfejsu) - Redirect (do wspieranego interfejsu) - Rate Limit - QoS Remark
Cechy przełącznika L3	• 32 interfejsy IPv4/IPv6 (V1), 128 interfejsów IPv4/IPv6 (V2) • Statyczny routing - 48 statyczne trasy • Statyczny ARP • 316 ARP wpisy • Proxy ARP • Gratuitous ARP • DHCP Serwer • DHCP Przekaźnik • DHCP L2 Przekaźnik
Funkcje L2 i L2+	• Link Aggregation - statyczna agregacja linków - 802.3ad LACP - Do 8 grup agregacji, zawierających 8 portów na grupę • Spanning Tree Protocol - 802.1d STP - 802.1w RSTP - 802.1s MSTP - STP Security: TC Protect, BPDU Filter, BPDU Protect, Root Protect, Loop Protect • Wykrywanie Pętli - Bazujące na Porcie - Bazujące na VLAN • Flow Control - 802.3x Flow Control - HOL Blocking Prevention • Mirroring - Port Mirroring - CPU Mirroring - One-to-One - Many-to-One - Tx/Rx/Both

L2 Multicast	• Wsparcie 511 (IPv4, IPv6) grup IGMP • IGMP Snooping - IGMP v1/v2/v3 Snooping - Fast Leave - IGMP Snooping Querier - IGMP Authentication • IGMP Authentication • MVR • MLD Snooping - MLD v1/v2 Snooping - Fast Leave - MLD Snooping Querier - Static Group Config - Limited IP Multicast • Multicast Filtering: 256 profili, do 16 wpisów na profil
Funkcje zaawansowane	• Automatyczne wykrywanie urządzeń • Konfiguracja Batch • Aktualizacja Firmware Batch • Inteligentne monitorowanie sieci • Ostrzeżenia o nieprzewidzianych zdarzeniach • Ujednolicona konfiguracja • Harmonogram Restartów
Sieci VLAN	• Grupy VLAN - Max Grupy 4K VLAN • 802.1Q Tagowany VLAN • MAC VLAN: 12 wpisów • Protokół VLAN: Szablon Protokołu 16, Protokół VLAN 16 • GVRP • VLAN VPN (QinQ) - QinQ bazujący na porcie - Selektywny QinQ • Głosowy VLAN
Listy kontroli dostępu	• ACL bazujący na czasie • MAC ACL - Źródłowy MAC - Docelowy MAC - VLAN ID - Priorytet użytkownika - Ether Type • IP ACL - Źródłowy IP - Docelowy IP - Fragment - Protokół IP - TCP Flag - TCP/UDP Port - DSCP/IP TOS - Priorytet użytkownika • Combined ACL • Zawartość pakietu ACL • IPv6 ACL • Polityka - Mirroring - Redirect - Rate Limit - QoS Remark • ACL aplikowane do Port/VLAN
Bezpieczeństwo transmisji	• Wiązanie IP-MAC-Port - DHCP Snooping - Inspekcja ARP - IPv4 Source Guard

	• Wiązanie IPv6-MAC-Port - DHCPv6 Snooping - Detekcja ND - IPv6 Source Guard • DoS Defend • Static/Dynamic Port Security - Do 64 adresów MAC na Port • Broadcast/Multicast/Unicast Storm Control - tryb kontroli kbps/ratio • Kontrola dostępu bazująca na IP/Port/MAC • 802.1X - autoryzacja bazująca na Porcie - autoryzacja bazująca na MAC - VLAN Assignment - MAB - VLAN Gościa - Wsparcie autoryzacji Radius • AAA (włączając TACACS+) • Izolacja Portu • Bezpieczne zarządzanie Web poprzez HTTPS z SSLv3/TLS 1.2 • Bezpieczne zarzadzanie Command Line Interface (CLI) z SSHv1/SSHv2
IPv6	• IPv6 Dual IPv4/IPv6 • Multicast Listener Discovery (MLD) Snooping • IPv6 ACL • IPv6 Interfejs • Statyczny routing IPv6 • IPv6 neighbor discovery (ND) • Wykrywanie ścieżki maximum transmission unit (MTU) • Internet Control Message Protocol (ICMP) version 6 • TCPv6/UDPv6 • IPv6 aplikacje - DHCPv6 Client - Ping6 - Tracert6 - Telnet (v6) - IPv6 SNMP - IPv6 SSH - IPv6 SSL - Http/Https - IPv6 TFTP
Funkcje panelu zarządzania	• Interfejs graficzny GUI • Interfejs linii poleceń CLI • SNMP v1/v2c/v3 - Trap/Inform - RMON (grupy 1, 2, 3, 9) • Szablon SDM • Klient DHCP/BOOTP • 802.1ab LLDP/LLDP-MED • Autoinstalacja DHCP • Dual Image, Dual Configuration • Monitorowanie zużycia procesora • Diagnostyka kabli • EEE • Odzyskiwanie hasła • SNTP • Logi systemowe
Gwarancja	Urządzenie dostarczone z minimum 24 msc gwarancji i wsparcia producenta lub wykonawcy

3.1.2. Przełącznik sieciowy 24 - port typ 2 – 7 szt.

Wymagania ogólne:

Porty	• 24× Porty RJ45 10/100/1000 Mb/s • 4× Sloty SFP+ 10G • 1× Port Konsolowy RJ45 • 1× Port Konsolowy Micro-USB
Ilość wentylatorów	2 Wentylatory
Zasilanie	100-240 V AC~50/60 Hz
Porty PoE+ (RJ45)	• Zgodność ze standardami: 802.3at/af • Porty PoE+: 24 Porty, do 30W na port • Łączne zasilanie: 384 W
Wymiary (S x G x W)	440 × 330 × 44 mm
Montaż	Szafa Rack
Wydajność przełączania	128 Gb/s
Szybkość przekierowań pakietów	95,23 Mp/s
Tablica adresów MAC	16 K
Bufor pakietów	12 Mb
Ramki jumbo	9 KB
Funkcja Quality of Service	• 8 kolejek priorytetów • Priorytetowanie 802.1p CoS/DSCP • Planowanie kolejki - SP (Strict Priority) - WRR (Weighted Round Robin) - SP+WRR • Kontrola przepustowości - Ograniczenie przepustowości bazując na Port/Przepływ • Płynniejsza wydajność • Action for Flows - Mirror (do wspieranego interfejsu) - Redirect (do wspieranego interfejsu) - Rate Limit - QoS Remark
Cechy przełącznika L3	• 128 interfejsów IPv4/IPv6 • Statyczny routing - 48 statyczne trasy • Statyczny ARP - 128 Statycznych wpisów • Proxy ARP • Gratuitous ARP • DHCP Serwer • Przekaźnik DHCP - DHCP Przekaźnik interfejsu - DHCP Przekaźnik VLAN • DHCP L2 Przekaźnik
Funkcje L2 i L2+	• Link Aggregation - statyczna agregacja linków - 802.3ad LACP - Do 8 grup agregacji, zawierających 8 portów na grupę • Spanning Tree Protocol - 802.1d STP - 802.1w RSTP - 802.1s MSTP - STP Security: TC Protect, BPDU Filter, Root Protect • Wykrywanie Pętli - Bazujące na Porcie - Bazujące na VLAN • Flow Control - 802.3x Flow Control

	- HOL Blocking Prevention • Mirroring - Port Mirroring - CPU Mirroring - One-to-One - Many-to-One - Tx/Rx/Both
L2 Multicast	• IGMP Snooping - IGMP v1/v2/v3 Snooping - Fast Leave - IGMP Snooping Querier - IGMP Authentication • IGMP Authentication • MLD Snooping - MLD v1/v2 Snooping - Fast Leave - MLD Snooping Querier - Static Group Config - Limited IP Multicast • MVR • Multicast Filtering: 256 profili i 16 wpisów na profil
Funkcje zaawansowane	• Automatyczne wykrywanie urządzeń • Konfiguracja Batch • Aktualizacja Firmware Batch • Inteligentne monitorowanie sieci • Ostrzeżenia o nieprzewidzianych zdarzeniach • Ujednolicona konfiguracja • Harmonogram Restartów
Sieci VLAN	• Grupy VLAN - Max Grupy 4K VLAN • 802.1Q Tagowany VLAN • MAC VLAN: 7 wpisów • Protokół VLAN: Szablon Protokołu 16, Protokół VLAN 16 • PrywatnyVLAN • GVRP • VLAN VPN (QinQ) - QinQ bazyjący na porcie - Selektywny QinQ • Głosowy VLAN
Listy kontroli dostępu	• ACL bazujący na czasie • MAC ACL - Źródłowy MAC - Docelowy MAC - VLAN ID - Priorytet użytkownika - Ether Type • IP ACL - Źródłowy IP - Docelowy IP - Fragment - Protokół IP - TCP Flag - TCP/UDP Port - DSCP/IP TOS - Priorytet użytkownika • Combined ACL • Zawartość pakietu ACL • IPv6 ACL • Polityka - Mirroring - Redirect

	- Rate Limit - QoS Remark • ACL aplikowane do Port/VLAN
Bezpieczeństwo transmisji	• IP-MAC-Port Binding - 512 wpisy - DHCP Snooping - ARP Inspection - IPv4 Source Guard: 100 wpisów • IPv6-MAC-Port Binding - 512 wpisy - DHCPv6 Snooping - ND Detection - IPv6 Source Guard: 100 wpisów • DoS Defend • Static/Dynamic Port Security - Do 64 adresów MAC na Port • Broadcast/Multicast/Unicast Storm Control - tryb kontroli kbps/ratio • 802.1X - autoryzacja bazująca na Porcie - autoryzacja bazująca na MAC - VLAN Assignment - MAB - Guest VLAN - Wsparcie autoryzacji Radius • AAA (włączając TACACS+) • Port Isolation • Bezpieczne zarządzanie Web poprzez HTTPS z SSLv3/TLS 1.2 • Bezpieczne zarzadzanie Command Line Interface (CLI) z SSHv1/SSHv2 • Kontrola dostępu bazująca na IP/Port/MAC
IPv6	• IPv6 Dual IPv4/IPv6 • Multicast Listener Discovery (MLD) Snooping • IPv6 ACL • IPv6 Interfejs • Statyczny routing IPv6 • IPv6 neighbor discovery (ND) • Wykrywanie ścieżki maximum transmission unit (MTU) • Internet Control Message Protocol (ICMP) wersja 6 • TCPv6/UDPv6 • IPv6 aplikacje - DHCPv6 Client - Ping6 - Tracert6 - Telnet (v6) - IPv6 SNMP - IPv6 SSH - IPv6 SSL - Http/Https - IPv6 TFTP
Funkcje panelu zarządzania	• Interfejs graficzny GUI • Interfejs linii poleceń CLI • SNMP v1/v2c/v3 - Trap/Inform - RMON (grupy 1, 2, 3, 9) • Szablon SDM • Klient DHCP/BOOTP • 802.1ab LLDP/LLDP-MED • Autoinstalacja DHCP • Dual Image, Dual Configuration

	• Monitorowanie zużycia procesora • Diagnostyka kabli • EEE • Odzyskiwanie hasła • SNTP • Logi systemowe
Środowisko pracy	• Dopuszczalna temperatura pracy: 0–45 ℃ (32–113 ℉); • Dopuszczalna temperatura przechowywania: -40–70 ℃ (-40–158 ℉) • Dopuszczalna wilgotność powietrza: 10–90% RH bez kondensacji • Dopuszczalna wilgotność przechowywania: 5–90% RH bez kondensacji
Gwarancja	Urządzenie dostarczone z minimum 24 msc gwarancji i wsparcia producenta lub wykonawcy

3.1.3. Punkt dostępowy 802.11ax zgodny z Wi-Fi 6 – 71 szt.

Wymagania ogólne:

Parametr lub warunek	Minimalne wymagania
Wymagania Ogólne	Sufitowy, dwu-zakresowy punkt dostępowy pracujący w standardzie 802.11a/b/g/n/ac/ax zgodny z Wi-Fi 6. Zasilane przez PoE 802.3af/at lub paswyne PoE 48V.
Port LAN	1 x GbE RJ45 por
Antena	2.4 GHz 4 dBi 5 GHz 6 dBi
Zgodność z Hotspot 2.0	tak
Zasilanie	802.3af PoE, passive PoE (48V
Pobór mocy	13W
Moc nadawania 2,4GHz	22 dBm
Moc nadawania 5GHz	26 dBm
Pasmo	802.11a/b/g/n/ac/ax
Ilość SSID	8 per radio
Temperatura pracy	-30 to 60° C (-22 to 140° F)
Wilgotność pracy	od 5 do 90% niekondensująca
Certyfikaty	CE, FCC, IC
Obsługa VLAN	802.1Q
Klienci równoczesni	300+
Prędkość	802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b 1, 2, 5.5, 11 Mbps 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n 6.5 Mbps do 600 Mbps (MCS0 - MCS31, HT 20/40) 802.11ac 6.5 Mbps do 3.4 Gbps (MCS0 - MCS9 NSS1/2/3/4, VHT 20/40/80/160) 802.11ax 7.3 Mbps do 4.8 Gbps (MCS0 - MCS11 NSS1/2/3/4, HE 20/40/80/160)
Zarządzanie	zarządzanie i konfigurowanie przez kontroler sieciowy
Funkcjonalność	802.1x oraz URL redirect (guest)
Gwarancja	Urządzenie dostarczone z minimum 24 msc gwarancji i wsparcia producenta lub wykonawcy

4. Dostawa, instalacja oraz konfiguracji urządzenia typu NGFW, implementacja mechanizmów bezpieczeństwa sieciowego w Urzędzie Gminy Miejsce Piastowe.

4.1. Koncepcja wdrożenia.

Należy dostarczyć urządzenie next-generation firewall wraz z niezbędnymi licencjami na okres nie krótrzy niż 24 miesiące (4.1.1). Należy wdrożyć zaawansowane mechanizmy bezpieczeństwa sieciowego zgodnie z opisem w punkcie 4.2.

4.1.1. NGFW wraz z licencjami – 1 szt.

Wymagania ogólne:

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
4. Urządzenie jest zasilanie prądem przemiennym 230V.
5. Możliwość montażu w szafie rack 19".
6. Urządzenie wyposażone w 8 wbudowanych portów GbE RJ45.
7. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – 60 interfejsów VLAN.
8. Interfejsy fizyczne mogą pracować jak interfejsy przełącznika sieciowego ze sprzętowym wsparciem dla funkcjonalności L2.
9. Urządzenie wyposażone w port USB 3.0.
10. Wysokość urządzenia 1RU.
11. Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 6 Gbps dla pakietów wielkości 1024B.
12. Urządzenie osiąga powyższe parametry wydajnościowe również wraz z uruchomionym silnikiem IPS.
13. 200 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 35 000 nowych połączeń na sekundę.
14. Możliwość połączeń VPN do 200 urządzeń z maksymalną sumaryczną przepustowością 5 Gbps dla pakietów 1024B.
15. Przepustowość dekrypcji ruchu szyfrowanego (deszyfrowanie sprzętowe) wynosi przynajmniej 1 Gbps..
16. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
17. Możliwość uruchomienia urządzenia w trybie firewall'a L2 oraz L3.
18. Urządzenie obsługuje routing statyczny oraz dynamiczny: RIP, OSPF, OSPFv3, BGP.
19. Możliwość monitorowania dostępności „next hop" w trasach statycznych i automatycznego wyłączania trasy, gdy jest niedostępny.
20. Urządzenie obsługuje ruch multicastowy oraz protokoły IGMP, PIM-SM oraz bidirectional PIM.
21. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
22. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT).
23. Urządzenie może pracować jako serwer DHCP lub DHCP relay oraz zapewnia usługę DDNS.
24. Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby.
25. Urządzanie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN).
26. Dla RA VPN urządzenie zapewnia integrację z systemami Multi-Factor Authentication MFA.
27. Urządzenie zapewnia możliwość zestawienia dostępu ZTNA dla aplikacji HTTPS do sieci wewnętrznych poprzez wykorzystanie zewnętrznego SAML Identity Provider (IdP), umożliwiając

w ten sposób osobną autoryzację do każdej z aplikacji. System współpracuje m.in. z takimi IdP jak Azure AD, Octa, Duo.

28. Urządzenie zapewnia możliwość konfiguracji połączeń VPN typu Site-to-Site w następujących topologiach:
    a. Point to Point
    b. Hub and Spoke
    c. Full Mesh
29. Urządzenie zapewnia możliwość konfiguracji połączeń VPN typu Site-to-Site za pomocą interfejsów tunelowych (VTI) zarówno statycznych jak i dynamicznych dla zapewnienia metody route-based w topologii hub and spoke.
30. Urządzenie pozwala na utworzenie interfejsu logicznego (software'owego) loopback, których stan nie jest powiązany z żadnym interfejsem logicznym. Interfejs taki można wykorzystać m.in. do: statycznych i dynamicznych tuneli VTI, BGP, SSH, Syslog, AAA, ICMP.
31. Urządzenie pozwala na uruchomienie dynamicznych następujących protokołów routingu na tunelach VTI:
    a. BGP
    b. OSPFv3/v3
    c. EIGRP
32. Urządzenie zapewnia możliwość ograniczenia pasma w konkretnym kierunku – upload i download dla:
    a. Źródłowych i docelowych stref NGFW
    b. Źródłowych i docelowych adresów IP oraz portów
    c. Aplikacji
    d. Użytkowników
    e. URLi zdefiniowanych przez administratora
33. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System może stworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelenienie
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu
    c. Wiedza o urządzeniach mobilnych, load balancerach, urządzeniach NAT
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta
    e. Wiedza o podatnościach
    f. Wiedza o bieżących zagrożeniach
34. System posiada otwarte API dla współpracy z systemami zewnętrznymi.
35. Rozwiązanie współpracuje z systemami SIEM.
36. System umożliwia wykrycie co najmniej 5000 aplikacji.
37. System posiada wbudowany moduł wykrywania aplikacji AVC na podstawie sygnatur, który współpracuje z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.
38. System posiada wbudowany moduł wykrywania aplikacji w ruchu zaszyfrowanym, który umożliwia:
    a. Wykrywanie aplikacji bez odszyfrowywania ruchu na podstawie analizy informacji zawartej w pakiecie TLS Client Hello (tzw. fingerprinting) oraz korelowania tego z docelowym adresem IP, portem, z domeną
    b. Wartość procentową, wskazującą na trafność prawidłowego określenia aplikacji
    c. Możliwość tworzenia reguł w polityce dostępu, które zablokują w ten sposób wykrytą aplikację
39. Rozwiązanie umożliwia integrację z chmurową konsolą korelacji informacji o zagrożeniach z różnych rozwiązań bezpieczeństwa tego samego producenta.
40. Urządzenie może być zarządzane lokalnie lub przez scentralizowaną konsolę zarządzającą.
41. System umożliwia zdefiniowanie różnych wartości czasu wygaśnięcia sesji dla takich protokołów jak: ARP, SIP, H.323, H225, ICMP, UDP oraz dla sesji translacji PAT i sesji pół-otwartych.
42. System umożliwia zdefiniowanie następujących podstawowych zabezpieczeń dla połączeń:
    a. Randomizacja TCP sequence number

   b. Ograniczenie ilości wszystkich połączeń globalnie oraz do jednego hosta
   c. Ograniczenie ilości połączeń pół-otwartych globalnie oraz do jednego hosta
   d. Detekcja wygasłych połączeń, poprzez sprawdzanie czy dwie strony sesji są nadal aktywne
43. Urządzenie umożliwia wybór następujących metod kompilacji reguł polityki dostępu w przypadku użycia obiektów (np. grupy adresów IP, portów):
   a. Rozłożenie jednej skonfigurowanej reguły na reguły szczegółowe będące wszystkimi możliwymi kombinacjami wszystkich elementów zawartych w obiektach w celu monitorowania każdej z tych reguł z osobna (np. ilość dopasowani połączeń hit-counts) kosztem większego wykorzystania pamięci
   b. Dopasowanie ruchu do głównej reguły na podstawie zdefiniowanych obiektów bez tworzenia wszytkich możliwych kombinacji obiektów w celu zmniejszenia wykorzystania pamięci przez szczegółowe reguły.
44. Urządzenie zapewnia możliwość przypisania do reguł czasu jej aktywności. Istnieje możliwość zdefiniowania czasu całkowitego oraz zaplanowania interwałów czasowych.
45. System IPS zapewniający:
   a. możliwość pracy w trybie in-line
   b. możliwość pracy w trybie pasywnym (IDS)
   c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
      i. złośliwe oprogramowanie
      ii. skanowanie sieci
      iii. ataki na usługę VoIP
      iv. próby przepełnienia bufora
      v. ataki na aplikacje P2P
      vi. zagrożenia dnia zerowego, itp.
   d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)
   e. wiele sposobów wykrywania zagrożeń w tym:
      i. sygnatury ataków opartych na exploitach
      ii. reguły oparte na zagrożeniach
      iii. mechanizm wykrywania anomalii w protokołach
      iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
   f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
   g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives)
   h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
   i. wiele możliwości reakcji na zdarzenia w tym takie, jak:
      i. tylko monitorowanie
      ii. blokowanie ruchu zawierającego zagrożenia
      iii. zapisywanie pakietów
   j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
   k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
      i. systemach operacyjnych
      ii. serwisach
      iii. otwartych portach, aplikacjach
      iv. zagrożeniach
   l. możliwość pasywnego gromadzenia informacji go przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych
   m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.

n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
r. obsługę reguł Snort
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)
u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa, na podstawie danych kontekstowych

46. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe
    b. pliki graficzne
    c. pliki PDF
    d. pliki wykonywalne
    e. pliki multimedialne
    f. pliki pakietu Office
    g. pliki skompresowane
47. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.
48. System umożliwia zdefiniowanie osobnej polityki IPS dla ruchu klasyfikowanego na podstawie aplikacji i wymagającego wymiany kilku pakietów w celu poprawnego wykrycia aplikacji.
49. System pozwala na budowanie polityk w oparciu o nazwy DNS z możliwością przekierowania zapytań do tzw. „sinkhole”.
50. System pozwala na przypisanie innych polityk IPS do różnych reguł polityki dostępu.
51. System zbiera dane kontekstowe, na podstawie których buduje profil każdego hosta. Profil taki zawiera informacje o systemie operacyjnym i jego wersji, aplikacjach i ich wersjach, protokołach.
52. Wyżej wymienione dane kontekstowe są mapowane do wbudowanej bazy podatności na zagrożenia. Mapowanie pozwala na trafne określenie wpływu zagrożenia na zaatakowany system (jeżeli jest podatność system jest skompromitowany, jeżeli nie było podatności to system nie został skompromitowany).
53. System pozwala na wstrzykiwanie tagów usług Azure i AWS, tagów z Vmware oraz atrybutów Office365 i i użycie ich w polityce bezpieczeństwa. System automatycznie reaguje na zmianę tych tagów i atrybutów bez konieczności aktualizowania polityki.
54. System pozwala na odszyfrowywanie ruchu TLS 1.3 natywnie, tzn. bez wymuszenia obniżenia sesji TLS do wersji 1.2.
55. System umożliwia identyfikację URL w TLS 1.3 bez deszyfracji całego ruchu a jedynie przez deszyfrację samego certyfikatu, dzięki czemu nie ma potrzeby deszyfracji całego ruchu przy wykorzystywaniu jedynie URL filteringu.
56. Wymagane licencje upoważniające do korzystania z funkcjonalności SSL VPN na okres nie krótszy niż 24 miesiące.

4.2. Zakres prac konfiguracyjnych i wdrożeniowych.

Przed rozpoczęciem prac wdrożeniowych należy opracować ogólne założenia polityki bezpieczeństwa oraz koncepcję techniczną, która powinna zostać zatwierdzona przez Zamawiającego.

Zakres prac wdrożeniowych powinien obejmować co najmniej:

- Przygotowanie polityki bezpieczeństwa komunikacji z Internetem,
- Aktualizacja oprogramowania urządzeń do najnowszej wersji stabilnej, zalecanej przez producenta,
- Uruchomienie komunikacji w sieci LAN oraz na styku z Internetem,
- Konfiguracja zapasowego dostępu do Internetu z automatycznym przepięciem w razie awarii podstawowego łącza,
- Konfiguracja interfejsów VLAN – segmentacja sieci LAN,
- Konfiguracja środowiska zarządzania w szczególności: ustawienie wszystkich parametrów związanych z adresacją i routingiem IP, ograniczenie zdalnego dostępu do urządzeń, konfiguracja autentykacji użytkowników, zapewnienie możliwości zarządzania poprzez protokoły SSH i HTTPS,
- Konfiguracja autentykacji użytkowników w zakresie dostępu do poszczególnych usług (aplikacji) w oparciu o usługi katalogowe AD,
- Konfiguracja inspekcji ruchu pod katem programów złośliwych, wirusów itp.,
- Wdrożenie usług VPN w oparciu o certyfikaty i centralny system autoryzacji,
- Konfiguracja mechanizmów zabezpieczających przed znanymi atakami w sieci typu DoS, Spoofing, Sniffing itp.,
- Konfiguracja systemu raportowania oraz rejestru zdarzeń,
- Testy poprawności konfiguracji,
- Przygotowanie instrukcji wykonywania kopii konfiguracji urządzenia i odtwarzania w przypadku awarii.

5. Dostawa, instalacja oraz konfiguracja urządzeń typu NGFW, implementacja mechanizmów bezpieczeństwa sieciowego w Gminny Ośrodek Pomocy Społecznej w Miejscu Piastowym, Szkoła Podstawowa w Głowience, Szkoła Podstawowa w Łężanach, Szkoła Podstawowa w Miejscu Piastowym, Szkoła Podstawowa w Rogach, Szkoła Podstawowa Targowiskach, Szkoła Podstawowa we Wrocance, Szkoła Podstawowa w Zalesiu.

Przed rozpoczęciem prac instalacyjno-wdrożeniowych należy opracować ogólne założenia polityki bezpieczeństwa oraz koncepcję techniczną, która powinna zostać zatwierdzona przez Zamawiającego.

5.1. Koncepcja wdrożenia.

W ramach zamówienia należy dostarczyć zainstalować oraz skonfigurować urządzenia typu NGFW (8 szt.) wraz z niezbędnymi licencjami. Lokalizacja urządzeń NGFW znajduje się w poniżej tabeli:

	NGFW (szt.)
Gminny Ośrodek Pomocy Społecznej w Miejscu Piastowym	1
SP im. Benedykta Wierdaka w Głowience	1
SP im. Tadeusza Kościuszki w Łężanach	1
SP im. Tytusa Trzecieskiego w Miejscu Piastowym	1
SP im. Kazimierza Wielkiego w Rogach	1
SP im. Św. Jana Kantego w Targowiskach	1
SP im. Stanisławy Grelli we Wrocance	1
SP im. Józefa Piłsudskiego w Zalesiu	1

Zakres prac wdrożeniowych powinien obejmować co najmniej:

- Przygotowanie polityk bezpieczeństwa komunikacji z Internetem,
- Aktualizacja oprogramowania urządzeń do najnowszej wersji stabilnej, zalecanej przez producenta,
- Instalacja urządzeń w szafach dystrybucyjnych, podłączenie okablowania i uruchomienie komunikacji w sieci LAN oraz na styku z Internetem,
- Podłączenie do środowiskiem zarządzania, w Urzędzie Gminy Miejsce Piastowe
- Ustawienie wszystkich parametrów związanych z adresacją i routingiem IP, ograniczenie zdalnego dostępu do urządzeń, konfiguracja autentykacji użytkowników, zapewnienie możliwości zarządzania poprzez protokoły SSH i HTTPS,
- Konfiguracja tuneli SSL VPN,
- Konfiguracja tuneli IPSec do urządzenia brzegowego w Urzędzie Gminy,
- Konfiguracja systemu raportowania oraz rejestru zdarzeń,
- Testy poprawności konfiguracji.

5.1.1. Urządzenie NGFW – 8 kpl.

Wymagania ogólne:

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band .
4. Urządzenie jest zasilanie prądem przemiennym 230V.
5. Możliwość montażu w szafie rack 19".
6. Urządzenie wyposażone w 8 wbudowanych portów GbE RJ45 w tym 2 porty PoE+.
7. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – 60 interfejsów VLAN.
8. Interfejsy fizyczne mogą pracować jak interfejsy przełącznika sieciowego ze sprzętowym wsparciem dla funkcjonalności L2.
9. Urządzenie wyposażone w port USB 3.0.
10. Wysokość urządzenia 1RU.
11. Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 880 Mbps dla pakietów wielkości 1024B.
12. Urządzenie osiąga powyższe parametry wydajnościowe również wraz z uruchomionym silnikiem IPS.
13. 100 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 6 000 nowych połączeń na sekundę.
14. Możliwość połączeń VPN do 75 urządzeń z maksymalną sumaryczną przepustowością 400 Mbps dla pakietów 1024B.
15. Przepustowość dekrypcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi przynajmniej 195 Mbps.
16. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
17. Możliwość uruchomienia urządzenia w trybie firewall'a L2 oraz L3.
18. Urządzenie obsługuje routing statyczny oraz dynamiczny: RIP, OSPF, OSPFv3, BGP.
19. Możliwość monitorowania dostępności „next hop" w trasach statycznych i automatycznego wyłączania trasy, gdy jest niedostępny.
20. Urządzenie obsługuje ruch multicastowy oraz protokoły IGMP, PIM-SM oraz bidirectional PIM.
21. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
22. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT).
23. Urządzenie może pracować jako serwer DHCP lub DHCP relay oraz zapewnia usługę DDNS.
24. Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standb.
25. Urządzanie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN).
26. Dla RA VPN urządzenie zapewnia integrację z systemami Multi-Factor Authentication MFA.
27. Urządzenie zapewnia możliwość zestawienia dostępu ZTNA dla aplikacji HTTPS do sieci wewnętrznych poprzez wykorzystanie zewnętrznego SAML Identity Provider (IdP), umożliwiając w ten sposób osobną autoryzację do każdej z aplikacji. System współpracuje m.in. z takimi IdP jak Azure AD, Octa, Duo.
28. Urządzenie zapewnia możliwość konfiguracji połączeń VPN typu Site-to-Site w następujących topologiach:
    a. Point to Point
    b. Hub and Spoke
    c. Full Mesh
29. Urządzenie zapewnia możliwość konfiguracji połączeń VPN typu Site-to-Site za pomocą interfejsów tunelowych (VTI) zarówno statycznych jak i dynamicznych dla zapewnienia metody route-based w topologii hub and spoke.

30. Urządzenie pozwala na utworzenie interfejsu logicznego (software'owego) loopback, których stan nie jest powiązany z żadnym interfejsem logicznym. Interfejs taki można wykorzystać m.in. do: statycznych i dynamicznych tuneli VTI, BGP, SSH, Syslog, AAA, ICMP.
31. Urządzenie pozwala na uruchomienie dynamicznych następujących protokołów routingu na tunelach VTI:
    a. BGP
    b. OSPFv3/v3
    c. EIGRP
32. Urządzenie zapewnia możliwość ograniczenia pasma w konkretnym kierunku – upload i download dla:
    a. Źródłowych i docelowych stref NGFW
    b. Źródłowych i docelowych adresów IP oraz portów
    c. Aplikacji
    d. Użytkowników
    e. URLi zdefiniowanych przez administratora
33. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System może stworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelenienie
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu
    c. Wiedza o urządzeniach mobilnych, load balancerach, urządzeniach NAT
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta
    e. Wiedza o podatnościach
    f. Wiedza o bieżących zagrożeniach
34. System posiada otwarte API dla współpracy z systemami zewnętrznymi.
35. Rozwiązanie współpracuje z systemami SIEM.
36. System umożliwia wykrycie co najmniej 5000 aplikacji.
37. System posiada wbudowany moduł wykrywania aplikacji AVC na podstawie sygnatur, który współpracuje z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.
38. System posiada wbudowany moduł wykrywania aplikacji w ruchu zaszyfrowanym, który umożliwia:
    a. Wykrywanie aplikacji bez odszyfrowywania ruchu na podstawie analizy informacji zawartej w pakiecie TLS Client Hello (tzw. fingerprinting) oraz korelowania tego z docelowym adresem IP, portem, z domeną
    b. Wartość procentową, wskazującą na trafność prawidłowego określenia aplikacji
    c. Możliwość tworzenia reguł w polityce dostępu, które zablokują w ten sposób wykrytą aplikację
39. Rozwiązanie umożliwia integrację z chmurową konsolą korelacji informacji o zagrożeniach z różnych rozwiązań bezpieczeństwa tego samego producenta.
40. Urządzenie może być zarządzane lokalnie lub przez scentralizowaną konsolę zarządzającą
41. System umożliwia zdefiniowanie różnych wartości czasu wygaśnięcia sesji dla takich protokołów. jak: ARP, SIP, H.323, H225, ICMP, UDP oraz dla sesji translacji PAT i sesji pół-otwartych.
42. System umożliwia zdefiniowanie następujących podstawowych zabezpieczeń dla połączeń:
    a. Randomizacja TCP sequence number
    b. Ograniczenie ilości wszystkich połączeń globalnie oraz do jednego hosta
    c. Ograniczenie ilości połączeń pół-otwartych globalnie oraz do jednego hosta
    d. Detekcja wygasłych połączeń, poprzez sprawdzanie czy dwie strony sesji są nadal aktywne
43. Urządzenie umożliwia wybór następujących metod kompilacji reguł polityki dostępu w przypadku użycia obiektów (np. grupy adresów IP, portów):
    a. Rozłożenie jednej skonfigurowanej reguły na reguły szczegółowe będące wszystkimi możliwymi kombinacjami wszystkich elementów zawartych w obiektach w celu monitorowania każdej z tych reguł z osobna (np. ilość dopasowani połączeń hit-counts) kosztem większego wykorzystania pamięci

b. Dopasowanie ruchu do głównej reguły na podstawie zdefiniowanych obiektów bez tworzenia wszytkich możliwych kombinacji obiektów w celu zmniejszenia wykorzystania pamięci przez szczegółowe reguły.

44. Urządzenie zapewnia możliwość przypisania do reguł czasu jej aktywności. Istnieje możliwość zdefiniowania czasu całkowitego oraz zaplanowania interwałów czasowych.

6. Zakup platformy serwerowej wraz z odpowiednim środowiskiem systemowym na potrzeby wdrożenia usług katalogowych i systemu zarządzania tożsamością w Urzędzie Gminy Miejsce Piastowe.

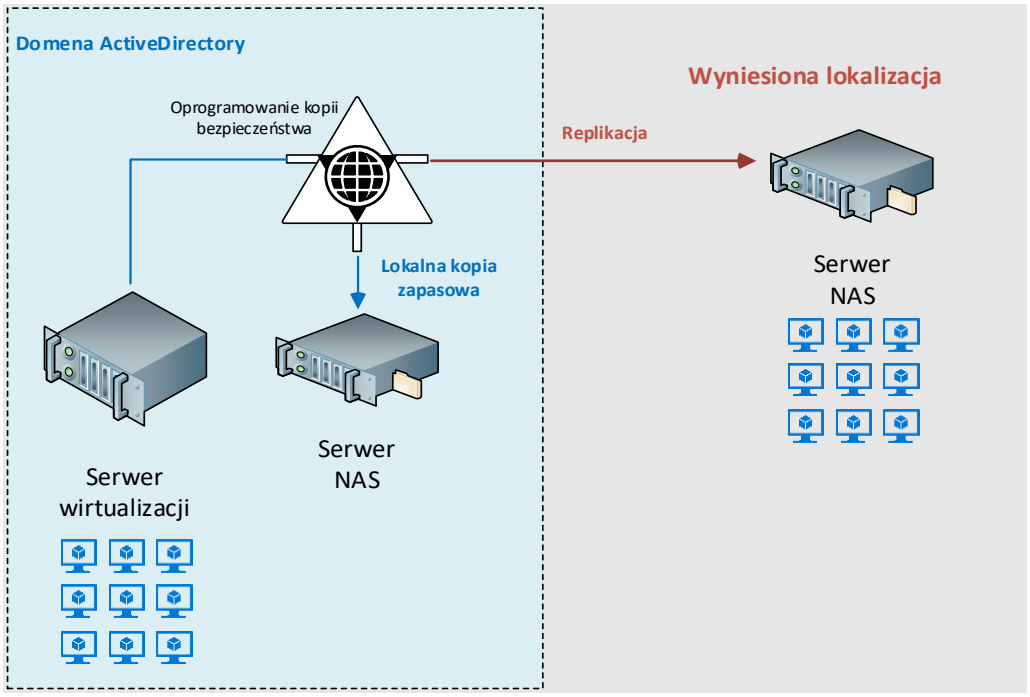
6.1. Koncepcja wdrożenia.

Serwer wirtualizacji należy skonfigurować i podłączyć do sieci zamawiającego. W ramach jego zasobów należy wdrożyć usługi:

1) Podstawowy kontroler domeny, usługi katalogowe LDAP.
2) Centralny System Autoryzacji.
3) Dodatkowe usługi domenowe DHCP, WSUS, PrintServer, Serwer Plików, Centrum certyfikatów.
4) Platforma zarządzająca urządzeniami NGFW
5) Oprogramowanie do zbierania, analizowania i wizualizowania danych
6) Wirtualna przystawka do zarządzania infrastrukturą backup'ową.

Dostosowanie konfiguracji na posiadanym przez zamawiającego serwerze DELL PE R550 do nowo wdrażanej usługi AD.

Kopie serwera powinny być wykonywane w ramach istniejącego oprogramowania Zamawiającego i zapisywane na istniejącym serwerze NAS wskazanym przez Zamawiającego. Poniżej przedstawiono ogólny schemat docelowego rozwiązania, obejmujący zasoby własne (istniejący serwer NAS wraz z zasobami dyskowymi) oraz planowany/projektowany do wdrożenia system serwerowy, który poza kopią lokalną będzie replikowany do wyniesionej lokalizacji, wskazajnej przez Zamawiającego:



Projektowane rozwiązanie obejmuje następujące elementy infrastruktury serwerowej:

- serwer wirtualizacji,

- oprogramowanie systemowe oraz oprogramowanie do wykonywania kopii bezpieczeństwa z uwzględnieniem dodatkowej lokalizacji (replika danych do wymiesionej lokalizacji),
- Centralny System Autoryzacji.

Dostawa oraz wdrożenie wszystkich wskazanych wyżej elementów infrastruktury odpowiada na zdiagnozowane potrzeby w ramach przeprowadzonej inwentaryzacji i wypełnia sugestie i zalecenia programowe w zakresie zwiększenia odporności i możliwości reagowania na zagrożenia.
Projektowane rozwiązanie powinno również spełnić wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych. Zgodnie bowiem z zapisami §20 ust. 2 (KRI) system powinien spełniać wymagania w zakresie:

- minimalizacji ryzyka utraty informacji w wyniku awarii,
- zapewnienia bezpieczeństwa przechowywanych plików systemowych oraz innych,
- zapewnienia możliwości regularnej aktualizacji oprogramowania (nowy system będzie posiadał wsparcie techniczne producenta w okresie eksploatacji).

Szczegółowe wymagania w zakresie parametrów technicznych i funkcjonalnych poszczególnych elementów infrastruktury zostały określone w dalszej części dokumentu.

6.1.1. Serwer wirtualizacji typ 1 – 1 szt.

Parametr lub warunek	**Minimalne wymagania techniczne i funkcjonalne**
Obudowa	Typu RACK, wysokość 2U Szyny umożliwiające wysunięcie serwera z szafy stelażowej z możliwością instalacji ramienia do zarządzania kablami Możliwość zainstalowania min. 12 dysków twardych hot plug 3,5”, Wszystkie dyski muszą być obsługiwane przez pojedynczy zainstalowany kontroler RAID,
Płyta główna	Dwuprocesorowa Wyprodukowana i zaprojektowana przez producenta serwera Możliwość instalacji procesorów 64-rdzeniowych Min. 3 złącza PCI Express generacji 4 w tym: - 1 fizyczne złącze o prędkości x16 Min. 1 złącze OCP 3.0 na potrzeby instalacji karty sieciowej Min. 32 gniazda pamięci RAM Wsparcie dla technologii: SDDC, ADDDC, ECC, Memory Mirroring Wbudowany wewnętrzny slot na kartę Micro SD
Procesor	Procesor 16-rdzeniowy, taktowanie bazowe 2GHz, architektura x86_64, maksymalny TDP 150W Osiągający w teście SPEC CPU 2017 Floating Point wynik min. 383 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera
Ilość procesorów	2
Pamięć	512 GB RAM DDR5 Registered 5600MHz Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność Możliwość rozbudowy do 8TB RAM
Dyski twarde	4 szt. dysków SATA Hot-Plug 1,92TB SSD Mixed Use 4 szt. dysków SATA 4TB HDD Hot-Plug 7200 RPM Możliwość instalacji na płycie głównej 2 dysków M.2 zabezpieczonych sprzętowym Raid (dyski nie mogą zajmować złączy PCI Express, ani klatek dla dyski hot plug)

Kontrolery I/O	Kontroler SAS RAID 12Gb dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania
Kontrolery LAN	4x 1Gbit Base-T RJ45, 2x 10Gbit Base-T RJ45 Karta nie może zajmować żadnego ze slotów PCIe
Porty	Z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA Wewnątrz obudowy: 1x USB 3.2, slot na kartę Micro SD Z tyłu obudowy: 3x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem, możliwość instalacji portu DB9 Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera Możliwość instalacji dodatkowego redundantnego portu RJ45 służącego do zarządzania, w slocie OCP zamiast karty sieciowej
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania posiadający swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 Update systemowego firmware Monitoring i możliwość ograniczenia poboru prądu Zdalne włączanie/wyłączanie/restart Zapis video zdalnych sesji Podmontowanie lokalnych mediów z wykorzystaniem Java client Przekierowanie konsoli szeregowej przez IPMI Zrzut ekranu w momencie zawieszenia systemu Możliwość przejęcia zdalnego ekranu Możliwość zdalnej instalacji systemu operacyjnego Alerty Syslog Przekierowanie konsoli szeregowej przez SSH Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera Możliwość mapowania obrazów ISO z lokalnego dysku operatora Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.

	Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, Producent serwera ponadto powinien zapewniać narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.

Bezpieczeństwo	Zainstalowany moduł TPM 2.0
Wspierane OS	Wspierane systemy operacyjne: Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 22.04 LTS
Zasilanie, chłodzenie	Redundantne zasilacze hot plug o mocy min. 1100W z certyfikatem min. Titanium; Redundantne wentylatory hot plug, zainstalowane nadmiarowo min. N+1
Gwarancja	3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym czasem reakcji do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej. Możliwość wykupienia dodatkowego serwisu zapewniającego gwarantowany czas naprawy serwera w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagania powyżej maszyny
Dokumentacja, inne	Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

6.1.2. Oprogramowanie systemowe i wirtualizacyjne – 1 kpl.

Wymagana jest dostawa najnowszej wersji wieczystej licencji uprawniającej zgodnie z zasadami licencjonowania określonymi przez producenta do zainstalowania i użytkowania na oferowanym serwerze w środowisku fizycznym, lub min. czterech wirtualnych uruchomień serwerowego systemu operacyjnego posiadającego następujące, wbudowane cechy:

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 16 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL)

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f. Szyfrowanie plików i folderów.
g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i. Serwis udostępniania stron WWW.
j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
k. Wsparcie dla algorytmów Suite B (RFC 4869),
l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
    i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    iii. Obsługi 4-KB sektorów dysków
    iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
    v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Możliwość uruchomienia czterech maszyn wirtualnych.

Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

6.2. Platforma zarządzająca urządzeniami NGFW.

Wymagana jest dostawa oprogramowania z wieczystą licencją uprawniającą zgodnie z zasadami licencjonowania określonymi przez producenta do podłączenia minimum 10 urządzeń, wraz ze wsparciem producenta na okres nie krótszy niż 24 miesiące. Oprogramowanie musi spełniać następujące wymagania:

Platforma zarządzająca urządzeniami NGFW oparta na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym. Platforma zarządzająca w postaci maszyny wirtualnej działająca pod kontrolą VMware ESXi lub Hyper-V i spełniającą następujące wymagania:

a. umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym,
b. jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego,
c. zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności admnistrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria,
d. ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm,
e. ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami,
f. zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany,
g. zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS,
h. zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją,
i. ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci,
j. daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta,
k. ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora,
l. zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS,
m. ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej,
n. zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania,
o. zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu,
p. zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP,
q. zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze,
r. zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika,
s. zapewnia informowanie o zagrożeniach poprzez,
i. wysłanie e-maila,
ii. wyslanie trap SNMP,
iii. przesłanie informacji do serwera Syslog,

iv. uruchomienie skryptu użytkownika,
v. wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane połączenie,
t. posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy,
i. aktualnego stanu danego urządzenia,
ii. podglądu historii dostępnych zasobów,
iii. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing),
u. ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym,
v. ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
i. dozwolone porty i protokoły
ii. dozwolone aplikacje według różnych kategorii
iii. dozwolone kategorie stron internetowych (URL filtering)
iv. dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej
v. sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne,
w. w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia,
x. pozwala na łatwą nawigację pomiędzy obiektami. Pozwala podejrzeć, w którym innym obiekcie jest on zagnieżdżony lub w której polityce jest użyty,
y. posiada narzedzie do monitorowania połączeń, które zostały sklasyfikowne do odpowiedniej reguły („hit count”). Narzędzie pozwala na monitorowanie jak dużo połączeń zachodzi dla konkretnych reguł w określonej jednostce czasu oraz pozwala na szybkie wyszukanie reguł niepotrzebnych, do których przez zadany okres nie trafił żaden ruch,
z. pozwala na wysłanie na sensor tylko wybranych elementów modyfikowanej konfiguracji,
aa. określa przewidywany czas implementacji polityki na sensor przed implementacją,
bb. pozwala przed rekonfiguracją na przegląd implementowanych zmian w porównaniu do aktualnych ustawień urządzenia zarządzalnego.

6.3. Oprogramowanie do zbierania, analizowania i wizualizowania danych.

Należy wdrożyć oprogramowanie do monitorowania wydajności, które umożliwia zbieranie i analizowanie danych z różnych systemów i aplikacji. Jego główne funkcjonalności obejmują:

Monitorowanie wydajności: Śledzi wydajność serwerów, aplikacji, baz danych i urządzeń sieciowych w czasie rzeczywistym.
Powiadomienia: Wysyła automatyczne powiadomienia o awariach lub przekroczeniach ustalonych progów, co pozwala na szybką reakcję.
Wizualizacja danych: Oferuje różnorodne opcje wizualizacji, takie jak wykresy, mapy i dashboardy, co ułatwia analizę danych.
Zarządzanie zdarzeniami: Umożliwia klasyfikację zdarzeń, co wspiera proces rozwiązywania problemów.
Rozszerzalność: Obsługuje integracje i dodatki, co pozwala na dostosowanie funkcjonalności do specyficznych potrzeb użytkowników.
Automatyzacja pracy: możliwość automatyzacji zadań poprzez rozbudowany system triggerów, skryptów i reguł automatycznego reagowania na problemy.
Integracja: z wieloma narzędziami i systemami zewnętrznymi, umożliwiając łatwe zarządzanie różnorodnymi środowiskami IT.
Wsparcie dla protokołu SNMP (Simple Network Management Protocol), co umożliwia łatwe zbieranie danych z urządzeń sieciowych, m.in., obciążenie CPU, wykorzystanie pamięci oraz status interfejsów.
Wsparcie do korzysta z agentów, które są instalowane na monitorowanych urządzeniach. Agenci zbierają lokalne dane i przesyłają je do centralnego serwera monitorującego. Umożliwia to dokładniejsze śledzenie stanu systemu oraz identyfikację problemów w czasie rzeczywistym.

Zakres prac wdrożeniowych oprogramowania powinien obejmować co najmniej:

- Przygotowanie szablonów do urządzeń klienta
- Przygotowanie dynamicznych wykresów do wizualizacji danych o wydajności systemów i sieci w czasie rzeczywistym.
- Przygotowanie templatów do gromadzenia informacje o sprzęcie, takie jak producent, model i numer seryjny, pomagając w zarządzaniu zasobami.
- Monitorowanie interfejsów sieciowych hostów, zbieranie danych o przepustowości, opóźnieniach i błędach.
- Monitorowanie usług działających na hostach, takich jak serwery czy bazy danych, informując o ich stanie.
- Monitorowanie urządzeń takich jak UPS, Monitoring Wizyjny, HotSpoty
- Przygotowanie alertów na podstawie ustalonych progów lub zdarzeń, takich jak awarie sprzętu lub przekroczenie wykorzystania zasobów.
- Utworzenie atomatycznych powiadamian użytkowników o krytycznych zdarzeniach za pomocą e-maila, lub komunikatorów.
- Utworzenie interaktywnych map sieciowych, które wizualizują połączenia i stan monitorowanych urządzeń.
- Przygotowanie raportów o stanie sieci, wydajności hostów i wykorzystaniu zasobów, ułatwiając analizę długoterminową.

6.4. Usługi instalacji, konfiguracji, wdrożenia oraz migracji systemów.

Dostarczony serwer należy zamontować oraz skonfigurować w celu wdrożenia usług, o których mowa w punkcie 11.1.4

7. Zakup platformy serwerowej wraz z odpowiednim środowiskiem systemowym na potrzeby wdrożenia usług katalogowych w Gminnym Ośrodeku Pomocy Społecznej w Miejscu Piastowym.

7.1. Koncepcja wdrożenia.

Serwer wirtualizacji należy skonfigurować i podłączyć do sieci zamawiającego. W ramach jego zasobów należy wdrożyć usługi katalogowe, jako serwer domenowy tylko do odczytu powiązany z głównym serwerem AD w Urzędzie Gminy.

Szczegółowe wymagania w zakresie parametrów technicznych i funkcjonalnych poszczególnych elementów infrastruktury zostały określone w dalszej części dokumentu.

7.1.1. Serwer typ 2 – 1 szt.

Parametr lub warunek	Minimalne wymagania techniczne i funkcjonalne
Obudowa	Typu Tower z możliwością konwersji do RACK, wysokość do 4U Możliwość zainstalowania min. 4 dysków twardych hot plug 3,5”, lub rekonfiguracji do 16 dysków 2,5”
Płyta główna	Wyprodukowana i zaprojektowana przez producenta serwera Możliwość instalacji procesorów 64-rdzeniowych Min. 4 złącza PCI Express w tym: - 1 fizyczne złącze generacji 4 Min. 4 gniazda pamięci RAM Wsparcie dla technologii: ECC
Procesor	Procesor 6-rdzeniowy, taktowanie bazowe 2.9GHz, architektura x86_64, maksymalny TDP 65W Osiągający w teście SPEC CPU 2017 Floating Point wynik min. 50 pkt Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera
Pamięć	32 GB RAM DDR4 3200MHz Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność Możliwość rozbudowy do 128GB RAM
Dyski twarde	3 szt. dysków SATA Hot-Plug 480GB SSD Read Intensive
Kontrolery I/O	Kontroler SAS RAID 12Gb dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10,5
Kontrolery LAN	4x 1Gbit Base-T RJ45
Porty	Z przodu obudowy: 1x USB 3.2, 1x USB 2.0 Wewnątrz obudowy: 1x USB 3.0 Z tyłu obudowy: 4x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem, port DB9
Diagnostyka	Możliwość przewidywania awarii min. dla pamięci i dysków wewnętrznych Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania umożliwiający: Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.

	Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 Update systemowego firmware Monitoring i możliwość ograniczenia poboru prądu Zdalne włączanie/wyłączanie/restart Zapis video zdalnych sesji Podmontowanie lokalnych mediów z wykorzystaniem Java client Przekierowanie konsoli szeregowej przez IPMI Zrzut ekranu w momencie zawieszenia systemu Możliwość przejęcia zdalnego ekranu Możliwość zdalnej instalacji systemu operacyjnego Alerty Syslog Przekierowanie konsoli szeregowej przez SSH Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera Możliwość mapowania obrazów ISO z lokalnego dysku operatora Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników

	-blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, Producent serwera ponadto powinien zapewniać narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
Bezpieczeństwo	Zainstalowany moduł TPM 2.0 Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz oraz czujnika otwarcia obudowy
Wspierane OS	Wspierane systemy operacyjne: Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 VMware ESXi, 7, 8.0
Zasilanie, chłodzenie	Redundantne zasilacze hot plug o mocy min. 750W z certyfikatem min. Titanium
Gwarancja	3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym czasem reakcji do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej. Możliwość wykupienia dodatkowego serwisu zapewniającego gwarantowany czas naprawy serwera w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagania powyżej maszyny
Dokumentacja, inne	Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

7.1.2. Oprogramowanie systemowe – 1 kpl.

Wymagana jest dostawa najnowszej wersji wieczystej licencji uprawniającej zgodnie z zasadami licencjonowania określonymi przez producenta do zainstalowania i użytkowania na oferowanym serwerze w środowisku fizycznym, lub min. dwóch wirtualnych uruchomień serwerowego systemu operacyjnego posiadającego wbudowane cechy określone w pkt. 6.1.2

8. Zakup i wdrożenie dedykowanego serwera NAS do wykonywania kopii zapasowych w Urzędzie Gminy Miejsce Piastowe.

8.1. Koncepcja wdrożenia.

Usługa backupu i archiwizacji danych powinna zostać wdrożona w taki sposób, aby był zgodny z zasadą 3-2-1. Jest to to standard tworzenia kopii zapasowych, który polega na tworzeniu trzech niezależnych kopii danych na dwóch różnych nośnikach z jedną wyniesioną poza lokalizację jednostki. Należy przyjąć że:

- Pierwsza kopia będzie przechowywana lokalnie na wewnętrznych dyskach twardych serwera backupowego,
- Druga kopia będzie przechowywana na nowo dostarczonym i uruchomionym serwerze NAS (pkt. 8.1.1),
- Trzecia kopia danych będzie wyniesiona do zewnentrznej, wskazanej przez zamawiającego lokalizacji, na posiadanym przez zamawiającego serwerze NAS.

Celem wdrożenia tworzenia kopii zapasowych 3-2-1 jest zmniejszenie potencjalnego wpływu „pojedynczego punktu podatności na awarię". Oznacza to, że jeśli jedno z urządzeń ulegnie awarii i znajdująca się na nim kopia danych zostanie utracona, do dyspozycji są jeszcze pozostałe dwie kopie danych. Wyniesienie dodatkowej kopii poza budynek jednostki, umożliwia natomiast odzyskanie kluczowych danych Zamawiającego w przypadku awarii dużych rozmiarów bądź fizycznego zniszczenia siedziby Zamawiającego (pożar, wybuch, działania terrorystyczne, klęski żywiołowe).

W ramach zamówienia należy dostarczyć, zainstalować oraz skonfigurować serwer NAS wraz z dyskami do wykonywania kopii zapasowych.

8.1.1. Serwer NAS – 1 szt.

Parametr lub warunek	Minimalne wymagania techniczne i funkcjonalne
Procesor	Procesor 4-rdzeniowy, taktowanie bazowe 2.2GHz, architektura x86_64, maksymalny TDP 25W Osiągający w teście Average CPU Mark Multithread rating wynik min. 5400 pkt (wynik musi być opublikowany na stronie https://www.cpubenchmark.net
Wbudowana pamięć RAM	Min. 4 GB
Maks. wielkość pamięci	32 GB
Rodzaj pamięci	DDR4
Liczba gniazd pamięci	4
Maks. liczba dysków	8
Format szerokości	2,5" (SFF) 3,5" (LFF)
Interfejs dysku	SATA
Obsługa hot-swap dysków	Tak
RAID	Tak
Poziomy RAID	0, 1, 10 (1+0), 5, 6, JBOD
Protokoły sieciowe	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN, L2TP).
Architektura sieci	GigabitEthernet
Interfejs sieciowy	4 x 10/100/1000 Mbit/s
Gniazda we/wy	1 x eSATA 4 x RJ-45 LAN 2 x USB 3.0
Liczba wentylatorów	Min. 2

Wentylator	8 cm
Obudowa	Rack 2U
Gniazda rozszerzeń	1 x PCIe 3.0 x 8
Zasilanie	100 - 240 V (prąd zmienny) 50 / 60 Hz, jednofazowo
Akcesoria w zestawie	Przewody zasilania prądem przemiennym x2 /1 zwykły przewód i 1 przewód C13 do C14
Pozostałe parametry	Wspornik do montażu szafy: • Szafa typu rack 19" z 2 słupkami (montaż bezpośredni) • Szafa typu rack 19" z 4 słupkami

8.1.2. Dysk NAS 8TB – 8 szt.

Wymagania ogólne:

Rodzaj urządzenia:	Dysk twardy - wewnętrzny
Pojemność:	Min. 8 TB
Rodzaj obudowy:	3,5"
Interfejs:	SATA 6Gb/s
Wielkość bufora:	256 MB
Cechy:	Technologia Advanced Format, technologia NASware, ciągła praca 24x7, Balans Dwupłaszczyznowy, Konwencjonalne nagrywanie magnetyczne (CMR)
Szerokość:	101.6 mm
Głębokość:	147 mm
Wysokość:	26.1 mm
Waga:	715 g
Szybkość transmisji urządzenia:	600 MBps (zewnętrzna)
Szybkość wewnętrzna danych:	215 MBps
Prędkość obrotowa:	Min. 5640 obr/min
MTBF:	Min. 1 000 000 godziny
Praca 24x7:	Tak
Błędy nienaprawialne:	1 na 10^14
Cykl z obciążeniem / bez obciążenia:	Min. 600,000
Interfejsy:	1 x SATA 6 Gb/s
Kompatybilna Wnęka:	3,5"
Zużycie energii:	Max. 5.2 wat (odczyt) Max. 5.2 wat (zapis) Max. 3.1 wat (bezczynność) Max. 0.3 wat (stan uśpienia)
Zgodność z normami:	UL, TUV, BSMI, ICES-003, FCC, KC, Directive 2011/65/EU, RCM, Directive 2015/863, UKCA, CB Scheme, Maghreb
Obsługa i wsparcie:	Gwarancja – Min 3 lata
inimalna temperatura pracy:	0 °C
Maksymalna temperatura pracy:	65 °C
Min. temperatura przechowywania:	-40 °C
Maks. temperatura przechowywania:	70 °C
Odporność na wstrząsy (podczas pracy):	70 g @ 2 ms
Odporność na wstrząsy (w stanie spoczynku):	250 g @ 2 ms
Emisja dźwięku:	24 dBA

8.2. Polityka tworzenia i odtwarzania backup.

Wykonawca odpowiedzialny jest za opracowanie polityki tworzenia kopii zapasowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.
Zakres wdrożenia:

1. Dostawa serwera.
2. Montaż serwera, konfiguracja serwera do pracy w infrastrukturze Zamawiającego, uruchomienie; aktualizacja firmware serwerów; konfiguracja maszyny wirtualnej dla systemu backupu; instalacja serwera/konsoli zarządzającej kopiami zapasowymi.
3. Opracowanie Harmonogramu tworzenia kopii zapasowych z podziałem na maszyny fizyczne/wirtualne; określeniem: częstotliwości tworzenia kopii pełnych, częstotliwości tworzenia kopii przyrostowych, częstotliwości tworzenia kopii na nośnikach wymiennych, częstotliwości weryfikacji poprawności tworzonych kopii zapasowych, częstotliwości i zakresu przeprowadzania testów odtworzeniowych. Na podstawie Harmonogramu Wykonawca skonfiguruje zadania backupowe na insteniejącym oprogramowaniu. Uruchomi tworzenie kopii zapasowych na serwerze backupowym oraz na serwerach NAS (lokalnym oraz w wwyniesionej lokalizacji).
4. Począwszy od dnia uruchomienia tworzenia kopii zapasowych, Wykonawca będzie zobowiązany do monitorowania pracy systemu backupowego przez min. 7 dni. Nadzór będzie miał na celu potwierdzenie prawidłowości wykonywanych kopii na serwerze oraz nośnikach wymiennych; potwierdzenie tworzenia kopii zgodnie z Harmonogramem.
5. Po zakończeniu pełnego cyklu tygodniowego tworzenia kopii zapasowych zgodnie z Harmonogramem, przeprowadzi testy odtworzenia maszyn wirtualnych. Testy odtworzeniowe będą przeprowadzone przy udziale administratora Zamawiającego.
6. Po okresie monitorowania, na podstawie potwierdzenia przez Zamawiającego zgodności wykonywanych kopii zgodnie z Harmonogramem oraz na podstawie zakończonych sukcesem testów odtworzeniowych, Wykonawca przeprowadzi instruktaż z zakresu:
   - bieżącej obsługi systemu, podstaw administracji,
   - modyfikacji Harmonogramu i zadań backupowych,
   - czynności sprawdzania prawidłowości wykonywanych kopii zapasowych na serwerze oraz nośnikach wymiennych,
   - procedury i czynności przeprowadzania testów odtworzeniowych.

9. Zakup i wdrożenie dedykowanych serwerów NAS do wykonywania kopii zapasowych w Szkoła Podstawowa w Głowience, Szkoła Podstawowa w Łężanach, Szkoła Podstawowa w Miejscu Piastowym, Szkoła Podstawowa w Rogach, Szkoła Podstawowa Targowiskach, Szkoła Podstawowa we Wrocance, Szkoła Podstawowa w Zalesiu.

9.1. Koncepcja wdrożenia.

W ramach zamówienia należy dostarczyć, zainstalować oraz skonfigurować serwery NAS wraz z dyskami do wykonywania lokalnych kopii zapasowych. Konfiguracja replikacji wybranych danych na nowo dostarczany serwer NAS w Urzędzie Gminy (pkt. 8.1.1)
Lokalizacja serwerów NAS oraz dysków znajduje się w poniżej tabeli:

	Serwer NAS	Dysk 2TB
SP im. Benedykta Wierdaka w Głowience	1	2
SP im. Tadeusza Kościuszki w Łężanach	1	2
SP im. Tytusa Trzecieskiego w Miejscu Piastowym	1	2
SP im. Kazimierza Wielkiego w Rogach	1	2
SP im. Św. Jana Kantego w Targowiskach	1	2
SP im. Stanisławy Grelli we Wrocance	1	2
SP im. Józefa Piłsudskiego w Zalesiu	1	2

9.1.1. Serwer NAS – 7 kpl.

Parametr lub warunek	Minimalne wymagania techniczne i funkcjonalne
Procesor	Procesor 4-rdzeniowy, taktowanie bazowe 2GHz, architektura x86_64, maksymalny TDP 10W Osiągający w teście Average CPU Mark Multithread rating wynik min. 2900 pkt (wynik musi być opublikowany na stronie https://www.cpubenchmark.net
Wbudowana pamięć RAM	Min. 2 GB
Maks. wielkość pamięci	6 GB
Rodzaj pamięci	DDR4
Maks. liczba dysków	2
Typ dysku	HDD, SSD
Format szerokości	2,5" (SFF) 3,5" (LFF)
Interfejs dysku	SATA
Obsługa hot-swap dysków	Tak
RAID	Tak
Poziomy RAID	0, 1, JBOD
Protokoły sieciowe	SMB/AFP/NFS/FTP/WebDAV
Architektura sieci	GigabitEthernet
Interfejs sieciowy	2 x 10/100/1000 Mbit/s
Gniazda we/wy	2 x RJ-45 LAN 2 x USB 3.0
Liczba wentylatorów	Min. 1
Wentylator	9.2 cm
Akcesoria w zestawie	Zainstalowane 2szt dysków 2TB SATA 6Gb/s 256GB Cache Hot-Plug, technologia NASware, praca 24x7
Obudowa	Desktop
Zasilanie	100 V do 240 V AC

Wymiary	Max. 165 x 110 x 235 mm

10. Dostawa kompleksowego rozwiązania typu antywirus – zarządzanego centralnie.

10.1. Koncepcja wdrożenia.

W ramach zamówienia należy dostarczyć 100 szt. licencji antywirus.
Lokalizacja licencji znajduje się w poniżej tabeli:

	Lic. Antywirus
Gminny Ośrodek Pomocy Społecznej w Miejscu Piastowym	10
SP im. Benedykta Wierdaka w Głowience	12
SP im. Tadeusza Kościuszki w Łężanach	12
SP im. Tytusa Trzecieskiego w Miejscu Piastowym	14
SP im. Kazimierza Wielkiego w Rogach	14
SP im. Św. Jana Kantego w Targowiskach	14
SP im. Stanisławy Grelli we Wrocance	12
SP im. Józefa Piłsudskiego w Zalesiu	12

10.1.1. Oprogramowanie Antywirus – 100 lic.

W ramach licencji wieczystej lub subskrypcji oprogramowania na okres nie krótszy niż 24 miesiące oprogramowanie musi spełniać następujące wymagania:

Administracja zdalna w chmurze
1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych
1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania

wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

<u>Ochrona serwera</u>

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

<u>Ochrona urządzeń mobilnych opartych o system Android</u>

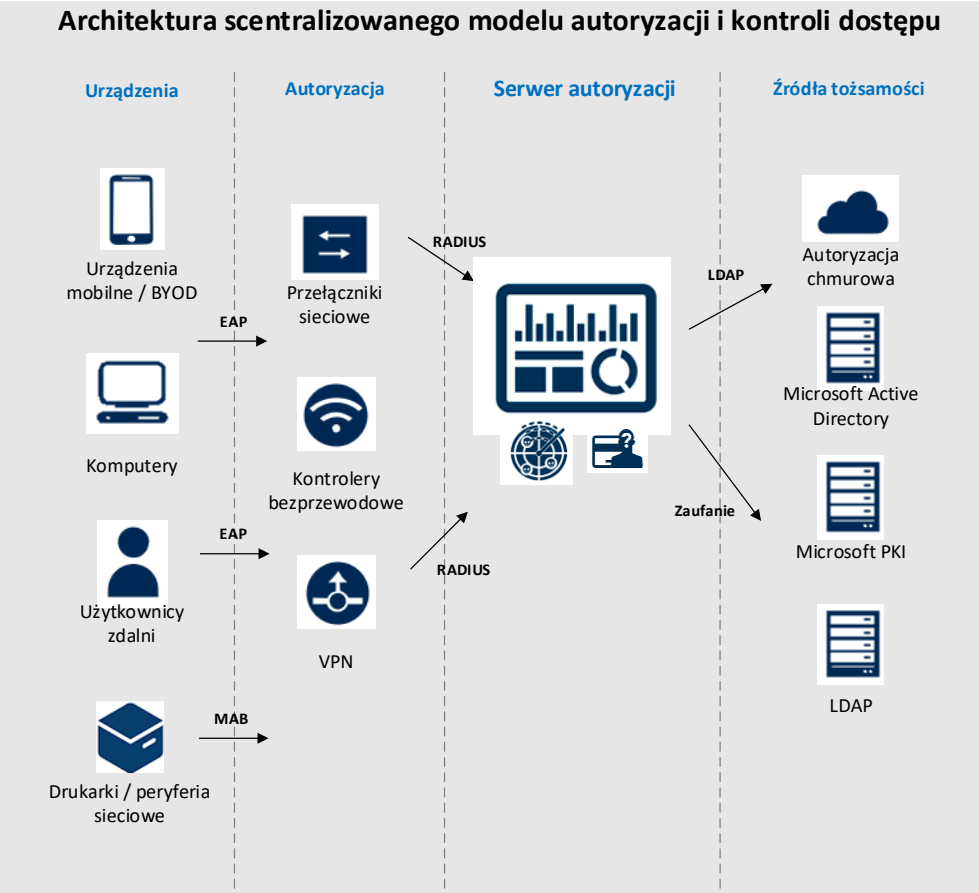
1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
a. usunięcie zawartości urządzenia,
b. przywrócenie urządzenie do ustawień fabrycznych,
c. zablokowania urządzenia,
d. uruchomienie sygnału dźwiękowego,
e. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
a. nazwę aplikacji,
b. nazwę pakietu,
c. kategorię sklepu Google Play,
d. uprawnienia aplikacji,
e. pochodzenie aplikacji z nieznanego źródła.

11. Wdrożenie Systemu Centralnej Autoryzacji, AD, MFA, VPN.

11.1. Koncepcja techniczna systemu.

Budowa Centralnego Systemu Autoryzacji obejmuje instalację oraz integrację kilku systemów (AD, MFA, VPN), które powinny tworzyć jednolitą architekturę bezpiecznego uwierzytelniania użytkowników i urządzeń w sieci jednostki. Rozwiązanie powinno zapewnić:

a) Centralną Autentykację i autoryzację z integracją ze środowiskiem Active Directory,
b) Możliwość zastosowania uwierzytelniania dwuskładnikowego MFA (np. SMS, tokeny, aplikacje mobilne) w dostępie zdalnym lub do lokalnych zasobów (usługi, urządzenia),
c) Możliwość zapewnienia profiling'u dla użytkowników przy współpracy z Active Directory,
d) Możliwość tworzenia reguł dostępu opartych na tożsamości użytkowników z AD, ich lokalizacji, ról oraz innych atrybutów (np. dział, grupa, urządzenie),
e) Możliwość identyfikacji typu urządzeń łączących się z siecią (laptopy, smartfony, drukarki itp.), co pozwoli na stosowanie różnych polityk bezpieczeństwa,
f) Wdrożenie dla wszystkich użytkowników mechanizmu Active Directory na ich komputerach,
g) Narzędzia do prostego zarządzania mechanizmami autoryzacji użytkowników oraz możliwość monitorowania ich aktywności w środowisku informatycznym.



Koncepcyjny schemat systemu przedstawia powyższy rysunek. Podstawą jego funkcjonowania jest źródło tożsamości, stąd konieczność wdrożenia usług Active Directory. Kompleksowe wdrożenie zapewni bezpieczny i kontrolowany dostęp do urządzeń WLAN, LAN, WAN, komputerom, serwerom oraz innym urządzeniom podłączonym do infrastruktury Urzędu Gminy.

11.1.1. Komputery klienckie w sieci powinny zostać podłączone do domeny z konfiguracją zgodną z najlepszymi praktykami i akceptowaną przez Zamawiającego

oraz z zachowaniem istotnych ustawień użytkowników **Serwer Centralnej Autoryzacji – 1 kpl.**

System powinien zapewniać pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu. System realizuje wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń. System może obejmować kontrolą dostęp wszystkich urządzeń podłączonych do sieci IP w tym terminali, komputerów PC, smartfonów i tabletów, telefonii IP, terminali video i innych podłączonych urządzeń.
System pracujący w modelu HA zainstalowany w ramach dostarczonej platformy wirtualizacyjnej.

a) System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
b) System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
c) System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
d) System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
e) System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
f) System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
g) System musi umożliwiać obsługę co najmniej 200 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
h) Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
i) System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
j) System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    - VM – min. VMWare ESXi, Hyper-V, Proxmox, KVM
    - Maszyny fizyczne - serwery wspierane przez producenta.
k) System musi posiadać funkcjonalność serwerów:
    - serwera RADIUS dla infrastruktury sieciowej,
    - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    - serwera SYSLOG,
    - serwera TACACS+,
    - serwera Monitoringu,
    - serwera DHCP,
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
l) System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
m) System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
n) System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
o) System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów

(min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.

p) Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
q) System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
r) System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
s) System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
t) System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
u) System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
v) System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
w) Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
x) System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
y) System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
z) System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
aa) System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
bb) System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
cc) Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
dd) System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
ee) System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
ff) System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
gg) System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
hh) System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
ii) System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
jj) System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
kk) System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.

ll) System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
mm) System musi posiadać funkcję personalizacji strony gościnnej.
nn) Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
oo) Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
pp) Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
qq) Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
rr) Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
ss) Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
tt) Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
uu) Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
vv) Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
ww) Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
xx) Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
yy) System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
zz) System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
aaa) System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
bbb) System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
ccc) System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
ddd) System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
eee) System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM
fff) System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS,.
ggg) System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:

- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
- Czy włączony jest firewall
- Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
- Czy jest włączone szyfrowanie dysku systemowego
- Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
- Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
- Czy w systemie są uruchomione procesy wskazane przez administratora
- Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności

- Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
  - Wartości klucza rejestru
  - Typu wartości: Number, String, Version

hhh) System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.

iii) System musi współpracować z serwerem tokenów.

jjj) System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:

- Microsoft Windows
- Mac OS
- iOS
- Android

kkk) System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).

lll) System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

a) System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.

b) System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:

- MAC,
- PAP/ASCII,
- CHAP,
- SNMP,
- 802.1X.

c) wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.

d) System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.

e) System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.

f) System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).

g) System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:

- Tożsamość/Urządzenie końcowe,
- Grupa tożsamości/urządzeń końcowych,
- Parametry urządzeń końcowych, min: system operacyjny, wersja,
- Atrybuty Active Directory,
- Jednostka organizacyjna tożsamości/urządzeń końcowych,
- Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
- Grupy urządzeń sieciowych,
- Porty urządzeń sieciowych,
- Grupy portów urządzeń sieciowych,
- Jednostka organizacyjna portów,
- Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
- Data, czas ważności polityki,
- Wewnętrzny Captive Portal,
- Metoda autoryzacji.

h) System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących

producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.

i) System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
j) System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
k) System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
l) System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
m) System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
n) System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
o) System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
p) System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
q) System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
r) System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
s) System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
t) System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1) System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2) Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
    - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1) System musi posiadać funkcję zintegrowanego serwera DHCP.
2) System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3) System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
    - Uruchamianie usługi dla wybranych podsieci,
    - Przypisanie ustalonego adresu IP dla adresu MAC.
    - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
    - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,

- Możliwość określania braku dostępu dla wybranych adresów MAC,
- Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
- Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
- Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
- Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
- Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1) System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2) System musi umożliwiać tworzenia haseł administratorom.
3) System musi umożliwiać tworzenie listy komend uprawnień dla administratorów.
4) System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5) System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6) System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7) System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8) System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1) Monitoring autoryzacji.
2) Monitoring dla zdarzeń systemowych.
3) Monitoring dla zdarzeń DHCP.
4) Monitoring dla tożsamości.
5) Monitoring dla urządzeń końcowych.
6) Monitoring dla urządzeń sieciowych.
7) Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8) Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9) Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10) Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11) System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12) System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13) System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14) System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15) System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.

16) System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17) Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18) Raport zdarzeń Microsoft Active Directory, minimum:
    - Logowania, wylogowania z system w tym błędne logowania,
    - Logowania do sieci 802.1X.

Alarmy

1) System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    - wiadomości e-mail,
    - Syslog,
    - notyfikacji systemowych.
2) Alarmy mogą być generowane w sytuacjach, min:
    - Ilości obsługiwanych transakcji RADIUS,
    - Opóźnienie obsługi transkacji RADIUS,
    - Statusu krytycznego modułów.
3) System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
    - badanie łączności IP za pomocą ping, traceroute,
    - tcpdump protokołów RADIUS, TACACS+,
    - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
        – nazwy użytkownika,
        – adresu MAC,
        – statusu uwierzytelnienia (udana lub nieudana),
        – powodu, jeżeli uwierzytelnienie nieudane,
        – zakresu czasowego, co do dnia, godziny i minuty,
    - wykonanie zdalnego polecenia na urządzeniu sieciowym.

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 24 miesięczną licencje na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC.
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.

Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

11.1.2. Karty elektroniczne dla systemu MFA – 50 szt.

W ramach zamówienia należy dostarczyć 50 szt. kart elektronicznych. Karty należy skonfigurować do logowania do domeny na wskazanych przez zamawiającego stacjach roboczych.

Wymagania ogólne:

Pamięć	do 64 kB
Podpisywanie i szyfrowanie RSA	klucze do 2048 bitów
Podpisywanie ECC GF(p)	klucze 256 bitów (wkrótce), 384, 512, 521 bitów na życzenie
Wspierane algorytmy	RSA, ECC, DES/3DES, AES, SHA1 (ograniczone) SHA-256, SHA-384
Wsparcie dla Secure Messaging	Tak
Generowanie kluczy	na karcie (RSA,ECC)
Protokoły	T=0
API	PKCS#11, MS CAPI/CSP/CNG, miniDriver, PC/SC
Certyfikat bezpieczeństwa aplikacji podpisu kwalifikowanego (QSCD)	CC EAL 4+
Certyfikat platformy sprzętowej	CC EAL 5+
Wsparcie dla systemów operacyjnych	Windows 8, 8.1, 10 (obsługa systemów operacyjnych 32/64bit), Linux (via PKCS#11), MacOSX (PKCS#11) oraz ograniczone wsparcie dla Windows 7
Część zbliżeniowa	MIFARE Classic 1k (13,56 Mhz)
Inne	wsparcie dla usług Terminal Services

11.1.3. Czytniki kart elektronicznych dla systemu MFA – 45 szt.

W ramach zamówienia należy dostarczyć 45 szt. czytników do kart stykowych elektronicznych, inteligentnych. Czytniki mają współpracować z kartami (pkt. 11.1.2)

Wymagania ogólne:

Obsługiwane układy scalone Tag IC	Obsługa wszystkich głównych układów scalonych kart inteligentnych zgodnych z normą ISO/IEC 7816
Obsługiwane normy	• ISO/IEC 7816 Część 1 do 4 • EMV 2011 Wersja 4.3 Poziom 1
Protokół karty inteligentnej	T=0, T=1
Prędkość interfejsu karty inteligentnej	• Do 600 kbps (w zależności od karty) • TA1=97
Częstotliwość zegara karty inteligentnej	Zgodny z normą ISO/IEC 7816; Działa do 16 MHz
Typ styku	• 8-stykowe gniazdo styków przesuwnych ID-1 • Obsługa C4/C8 • Przełącznik wykrywania karty
Wskaźnik stanu	LED
Interface	USB 2.0 Full Speed (12 Mbps)
Złącze	1,5 m kabel USB ze złączem USB typu A
MTBF	~7M hours
Pobór mocy	<6 mA bez karty; 25 mA z kartą
Sterownik PC/SC	Specyfikacja PC/SC wer. 2.01.14 dla: • Windows® 7/8/10 (32 i 64 bity); Windows® Server 2003/2008/2012 • MacOS 10.9.x, 10.10.x, 10.11.x • Linux 2.6.x, 3.x (32 i 64 bity)

11.1.4. Zakres prac konfiguracyjnych i wdrożeniowych – 1 kpl.

W ramach zamówienia w obrębie Urzędu Gminy Miejsce Piastowe mają zostać wykonane następujące zadania:

- Wdrożenie Systemu Centralnej Autoryzacji (integracja z domeną).
- Wdrożenie usług katalogowych wraz z migracją użytkowników sieci do domeny.
- Wdrożenie zasad GPO i dystrybucja podstawowego oprogramowania.
- Wdrożenie Centrum certyfikacji typu Enterprise.
- Wdrożenie protokołu 802.1x dla przełączników sieciowych oraz urządzeń sieci WLAN (w obrębie Urzędu Gminy Miejsce Piastowe).
- Wdrożenie autoryzacji dwuskładnikowej (MFA) z wykorzystaniem dostarczonych kart
- Wdrożenie platformy zarządzającej (pkt 6.2) wszystkimi dostarczanymi urządzeniami NGFW.
- Wdrożenie oprogramowanie do zbierania, analizowania i wizualizowania danych sieci.

12. Usługi zewnętrzne zwiększające poziom bezpieczeństwa informacji tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych – wsparcie i monitoring.

Usługa wsparcia i opieki serwisowej obejmująca wdrożone rozwiązania i systemy w następującym zakresie:

Monitorowanie
- bieżące monitorowanie i wykrywanie zdarzeń w trybie 24/h

Reagowanie
- bieżące reagowanie na zdarzenia i awarie
- zapobieganie i usuwanie zagrożeń, ograniczenie skutków zdarzeń
- zapewnienie urządzeń zastępczych w razie konieczności

Zarządzanie
- aktualizacja oprogramowania urządzeń, w tym aktualizacja firmware'ów, oraz wykonywanie upgrade'ów i update'ów urządzeń aktywnych zgodnie z zaleceniami TAC producenta
- dokonywanie niezbędnych rekonfiguracji
- regularne wykonywanie kopii zapasowych w modelu 3+2+1
- tworzenie kopii zapasowych środowisk wirtualnych
- kontrola wykorzystywania zasobów
- przeprowadzanie regularnych audytów i analizy ryzyka (co najmniej raz w roku)

Raportowanie
- zapisywanie zdarzeń systemowych (logowanie zdarzeń i ich rozliczalność)
- analizowanie logów systemowych oraz działań użytkowników
- archiwizacja plików systemowych, plików konfiguracyjnych oraz firmware'ów urządzeń w zewnętrznej lokalizacji DC

Wymagania organizacyjne i operacyjne:
- Wykonawca zapewni świadczenie usług wsparcia i serwisu zgodnie z określonym poziomem SLA:

Czas Reakcji Serwisowej (CRS)	W DNI robocze w godzinach 8.00 – 20.00	W pozostałym czasie
Maksymalny Czas Podjęcia Reakcji Serwisowej	1 h	2 h
Maksymalny czas Usunięcia Awarii krytycznych	8 h	NBD (następny dzień roboczy)

- Zapewnienie wszelkich zasobów (inżynierskich, służb technicznych itp.) potrzebnych do kompleksowej realizacji usługi.
- Uruchomienie telefonicznego centrum serwisowego dla Zamawiającego, działającego w godzinach od 8.00 – do 20.00 w dni robocze – na potrzeby zgłaszania incydentów/awarii oraz wszelkich nieprawidłowości w funkcjonowaniu infrastruktury.
- Prowadzenie elektronicznej ewidencji incydentów/awarii oraz zgłoszeń serwisowych.
- Wypełnianie w imieniu Zamawiającego obowiązków wynikających z przepisów Prawa, w szczególności ustawy o Krajowym Systemie Cyberbezpieczeństwa.
- W sytuacjach szczególnych zagrożeń, podejmowania niezwłocznie działań w celu zapobieżenia lub ograniczenia ich skutków.

- Zachowanie w tajemnicy wszelkich informacji związanych z realizacją umowy, z wyłączeniem tych informacji, których obowiązek udostępnienia wynika z obowiązujących przepisów prawa.

III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ PRZEKAZANIA DO EKSPLOATACJI.

1. Pozostałe wymagania od Wykonawcy.

1) Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii uwzględniając warunki ich wykonania.
2) Wykonawca powinien ponadto uwzględnić w cenie w ramach kosztów dodatkowych:
   - koszty dostawy sprzętu na miejsce instalacji,
   - koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania prac,
   - koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego,
   - koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac,
   - koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane,
   - koszty opracowania dokumentacji powykonawczej,
   - koszty uporządkowania oraz przywrócenia obiektu po wykonanych robotach do stanu pierwotnego wraz z naprawą ewentualnych szkód użytkownikowi lub osobom trzecim.
3) Wykonawca zobowiązany jest do:

- dokonywania z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji,
- stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego,
- udzielania na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.

Uwaga!

1) Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Rozwiązania muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem.
1) Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:
   - zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,
   - redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   - zapewnienia bezpieczeństwa plików,

- dbałość o aktualizację oprogramowania.

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).
Konieczność zapewnienia tej funkcjonalności wynika z:

§21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej),

Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa.

Wdrożone rozwiązania powinny spełniając wymagania przywołanych aktów prawnych oraz standardów rynkowych.

2. Przeszkolenie dla przedstawicieli Zamawiającego.

Wykonawca jest zobowiązany do przeszkolenia przedstawicieli Zamawiającego z wdrożonych w ramach projektu systemów i rozwiązań. Szkolenie powinno być przeprowadzone w formie prezentacji z możliwością zalogowania się na konsole urządzeń w trybie do odczytu z możliwością analizy dokonanej konfiguracji i włączenia mechanizmów monitorowania. Przeszkolenie powinno być ukierunkowane na wskazanie roli i funkcji danego elementu systemu w kontekście podniesienia odporności i możliwości zapobiegania incydentom (funkcji podniesienia poziomu cyberbezpieczeństwa). Powinno również obejmować ogólne zasady zarządzania i monitorowania urządzeń.

- Przeszkolenie dla min 2 przedstawicieli zamawiającego,
- Forma: zdalne lub stacjonarne (do ustalenia z Zamawiającym),
- Czas trwania: min. 6 godzin szkoleniowych,
- Materiały szkoleniowe – nie będą wymagane.

3. Odbiór końcowy.

Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji. Odbiory będą odbywać się zgodnie z zapisami w Umowie na realizację zamówienia. Przed przystąpieniem do odbioru końcowego Wykonawca przygotuje następujące dokumenty:

- Protokoły z pomiarów i testów – jeśli dotyczy.
- Odpowiednie atesty i certyfikaty - jeśli są wymagane.
- Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta.
- Protokoły odbiorów częściowych.

Spis treści