I-ZP.271.7.2025 Radzyń Podlaski,1.07.2025 r.

**Załącznik nr 5 - Szczegółowy opis przedmiotu zamówienia**

Spis treści

[1. UTM (Unified Threat Management)- 1 szt 3](#_Toc201586061)

[2. Firewall sieciowy-3 szt. 12](#_Toc201586062)

[3. UPS - Zasilacz awaryjny do NAS-3 szt. 13](#_Toc201586063)

[4. Network Attached Storage (NAS) - Dysk sieciowy wraz z 2 dyskami o pojemności min.2TB każdy- 2 szt. 16](#_Toc201586064)

[5. Network Attached Storage (NAS) - Dysk sieciowy w obudowie RACK wraz z 4 dyskami o pojemności min. 8TB każdy-1 szt. 20](#_Toc201586065)

[6. UPS do klastra serwerów-1 szt. 23](#_Toc201586066)

[7. UPS 3KVA-1 szt. 25](#_Toc201586067)

[8. UPS - Zasilacz awaryjny do stanowisk pracy-30 szt. 28](#_Toc201586068)

[9. Serwer - Klaster serwerów-1 szt. 29](#_Toc201586069)

[10. Macierz dyskowa do klastra-1 szt. 38](#_Toc201586070)

[11. Oprogramowanie antywirusowe-60 szt. 40](#_Toc201586071)

[12. Switch zarządzalny, co najmniej 16 portów, 10Gb 47](#_Toc201586072)

[13. Wdrożenie serwera RADIUS-1 szt. 48](#_Toc201586073)

[14. Urządzenia Access point- 3 szt. 52](#_Toc201586074)

[15. Dysk zewnętrzne o pojemności co najmniej 4TB (5 szt.) 54](#_Toc201586075)

[16. Klucze sprzętowe U2F-30 szt. 55](#_Toc201586076)

[17. Oprogramowanie do monitorowania infrastruktury informatycznej-1 szt. 56](#_Toc201586077)

[18.Switch zarządzalny, co najmniej 48 portów, typ portów Gigabit Ethernet (10/100/1000) (3 szt.) 67](#_Toc201586078)

[19.Wdrożenie( dostawa , instalacja i rozmieszczenie) oprogramowania typu SIEM do analizy logów w czasie rzeczywistym i powiadamiania o wykrytych nieprawidłowościach.( 1 szt.) 69](#_Toc201586079)

# UTM (Unified Threat Management)- 1 szt

Wymagania Ogólne

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

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

System powinien umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – rozwiązanie powinno zapewniać możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System powinien umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall powinien dysponować co najmniej 10 portami Gigabit Ethernet RJ-45.

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.

4. System wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.

4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

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

Polityki, Firewall

1. Polityka Firewall uwzględniająca: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

2. System realizujecy translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu powinna istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

5. Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

7. Element systemu realizujący funkcję Firewall integrujący się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

Połączenia VPN

1. System umożliwiający konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji powinien zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System umożliwiający konfigurację połączeń typu SSL VPN. W zakresie tej funkcji powinien zapewniać:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania powinien posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

1. Routingu statycznego.

2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.

4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.

5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.

6. BFD (Bidirectional Forwarding Detection).

7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwiający wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. SD-WAN wspierający zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwiający zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. System powinien dawać możliwość określania pasma dla poszczególnych aplikacji.

3. System powinien pozwalać na zdefiniowanie pasma dla wybranych użytkowników niezależnie od ich adresu IP.

4. System zapewniający możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwiający skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. Silnik antywirusowy zapewniający skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

3. System umożliwiający skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

4. System umożliwiający blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

5. System dysponujący sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

7. System powinien współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.

8. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opierająca się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System chroniący przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków zawierająca minimum 5000 wpisów. Aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System zapewniający wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).

7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.

8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwiająca kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji zawierająca minimum 2000 sygnatur. Aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur.

6. Możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

7. System powinien umożliwiać określanie dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzystający z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra WWW dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW powinien dostarczać kategorie stron zabronionych prawem np.: Hazard.

4. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Filtr WWW umożliwiający statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

6. Filtr WWW dający możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.

9. System pozwalający określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwiający weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. System dający możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

3. System powinien umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System współpracujący z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiający przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

5. System dający możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewall posiadający wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję Firewall umożliwiający wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania element systemu pełniący funkcję Firewall zapewniający przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów do dnia 30.06.2026 r.

4. Logowanie obejmujące zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

5. Możliwość włączenia logowania per reguła w polityce firewall.

6. System zapewnia możliwość logowania do serwera SYSLOG.

7. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen do dnia 30.06.2026 r.

b) Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów do 30.06.2026 r.

Gwarancja oraz wsparcie

System objęty serwisem gwarancyjnym producenta do dnia 30.06.2026 r., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe

System objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do dnia 30.06.2026 r.

System objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

* Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
* Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
* Doradztwo w zakresie konfiguracji.
* Zdalne wsparcie techniczne.
* Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
* Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
* Przygotowanie urządzenia do zdalnej konfiguracji.
* Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
* Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
* Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
* Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Wymagania powinny być potwierdzone dokumentami dostarczonymi przed podpisaniem umowy:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. Wymaga się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Dokument ten powinien zostać dostarczony wraz z dostawą urządzenia.

2. Wymaga się, aby został dostarczony dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. Dokument ten powinien zostać dostarczony wraz z dostawą urządzenia.

# Firewall sieciowy-3 szt.

Dostarczane urządzenia Wykonawca dostarczy we wskazane przez Zamawiającego lokalizacje:

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Lokalizacja** | **Liczba sztuk** |
| 1 | Ujęcie Wody w Białej  Biała 97B, 21-300 Radzyń Podlaski | 1 |
| 2 | Ujęcie Wody w Branicy Radzyńskiej Kol. Branica Radzyńska – Kol. 49B, 21-300 Radzyń Podlaski | 1 |
| 3 | Urząd Gminy  ul. Warszawska 32, 21-300 Radzyń Podlaski | 1 |

Minimalne wymagania:

**1. Przeznaczenie urządzenia**

Urządzenie powinno pełnić rolę zintegrowanego rozwiązania sieciowego, obejmującego funkcje bramy sieciowej, przełącznika sieciowego oraz kontrolera sieciowego. Urządzenie musi być zdolne do zarządzania ruchem sieciowym z zachowaniem wysokiego poziomu bezpieczeństwa oraz obsługi rozwiązań z zakresu zarządzania siecią lokalną (LAN) i sieciami rozległymi (WAN). Urządzenie zostanie skonfigurowane przez Wykonawcę według wytycznych zamawiającego

**2. Wymagania techniczne**

1. **Obudowa i montaż:**
   * Urządzenie w obudowie rackowej 1U.
   * Materiały obudowy: stal lub aluminium.
2. **Procesor i pamięć:**
   * Procesor minimum czterordzeniowy, o częstotliwości taktowania co najmniej 1,7 GHz.
   * Pamięć RAM: minimum 4 GB DDR4.
   * Wbudowana pamięć na system operacyjny: minimum 16 GB eMMC.
3. **Interfejsy sieciowe:**
   * Minimum 8 portów Gigabit Ethernet RJ45 dla sieci LAN.
   * Minimum 1 port 10G SFP+ dla sieci LAN.
   * Minimum 1 port Gigabit Ethernet RJ45 oraz 1 port 10G SFP+ dla sieci WAN.
   * Możliwość podłączenia zewnętrznych modułów SFP+.
4. **Zasilanie i zasilanie rezerwowe:**
   * Wbudowany zasilacz o mocy co najmniej 50W, z możliwością podłączenia zasilania rezerwowego (DC input).
   * Zakres napięcia zasilania: 100–240V AC, 50/60 Hz.
5. **Funkcje sieciowe i bezpieczeństwo:**
   * Wsparcie dla routingów z przepustowością co najmniej 3,5 Gbps przy włączonym systemie wykrywania i zapobiegania włamaniom (IDS/IPS).
   * Obsługa mechanizmów QoS z możliwością zarządzania na poziomie aplikacji, domen i krajów.
   * Wbudowany firewall z funkcjami analizy stanu połączeń oraz obsługą VLAN.
   * Wsparcie dla VPN (WireGuard, L2TP, OpenVPN) z możliwością konfiguracji polityk routingowych.
   * Obsługa redundancji WAN z przełączaniem awaryjnym i równoważeniem obciążenia.
6. **Dodatkowe funkcje:**
   * Wbudowany wyświetlacz LCD o przekątnej co najmniej 1,3 cala do podstawowej konfiguracji i monitorowania.
   * Możliwość montażu wewnętrznego dysku twardego 3.5" do przechowywania danych sieciowych.
7. **Środowisko pracy**

* Zakres temperatury pracy: od -10°C do 40°C.
* Wilgotność względna: od 5% do 95% (bez kondensacji).

1. **Certyfikaty i zgodność**

* Urządzenie musi posiadać certyfikaty CE, FCC oraz IC.

1. **Gwarancja**

* Wykonawca zapewni 24 miesiące gwarancji na urządzenie

# UPS - Zasilacz awaryjny do NAS-3 szt.

Dostarczane urządzenia Wykonawca dostarczy we wskazane przez Zamawiającego lokalizacje:

|  |  |  |
| --- | --- | --- |
| L.p. | Lokalizacja | Liczba sztuk |
| 1 | Ujęcie Wody w Białej  Biała 97B, 21-300 Radzyń Podlaski | 1 |
| 2 | Ujęcie Wody w Branicy Radzyńskiej Kol. Branica Radzyńska – Kol. 49B, 21-300 Radzyń Podlaski | 1 |
| 3 | Urząd Gminy  ul. Warszawska 32, 21-300 Radzyń Podlaski | 1 |

Minimalne wymagania:

| **Charakterystyka podstawowa** | **Parametry wymagane** |
| --- | --- |
| Technologia wykonania UPS | Line-interactive |
| Moc pozorna (VA) | minimum 1050 |
| Moc rzeczywista (W) | minimum 600 |
| Kształt fali na wyjściu(praca na baterii) | Symulowane napięcie sinusoidalne lub czysta fala sinusoidalna |
| Automatyczna regulacja napięcia (mechanizm AVR) | Wymagany |
| Ochrona przed przeciążeniem | Wymagana(minimum bezpiecznik) |
| Filtr EMI/RFI | Wymagany |
| Układ przeciwprzepięciowy (J) | Wymagany, minimum 150 |
| Nominalne napięcie wejściowe (V) | 230+/-10% |
| Obsługiwany zakres napięcia wejściowego (V) | minimum 165 - 290 |
| Częstotliwość wejściowa(Hz) | 50+/-5 ; 60+/-5 |
| Wykrywanie częstotliwości wejściowej | Wymagane automatyczne |
| Napięcie przy pracy na baterii (V) | 230+/-10% |
| Częstotliwość przy pracy baterii (Hz) | 50+/-1% ; 60+/-1% |
| Rodzaj złącza wejściowego | UniSchuko (połączenie złącza FR i Schuko) |
| Rodzaj złącza wyjściowego | FR x 4 |
| Typowy czas przełączenia na baterie (ms) | 4 ms |
| Czas podtrzymania na baterii | Wymagana, czas pracy przy pełnym obciążeniu (600W) do 1 min, przy połowie obciążenia (300W) do 4 min |
| Ładowanie baterii | Typowy czas ładowania do 6 h |
| Sygnalizacja | Wymagane alarmy dźwiękowe oraz diody LED |
| Diody LED - syngalizacja | Zasilanie włączone, Tryb liniowy, Tryb baterii, Tryb obejścia, Niski poziom baterii, Przeciążenie, Usterka UPS |
| Alarmy dźwiękowe - sygnalizacja | Tryb baterii, Niski poziom baterii, Przeciążenie, Usterka UPS |
| Port komunikacyjny USB (HID) | Wymagany |
| Dołączone oprogramowanie do zarządzania | Wymagane, obsługa platform Windows 11, Windows 10, Windows Server 2022, Windows Server 2019, Windows Server 2016,macOS 15.1.1, macOS 14, macOS 13.5.1, macOS 13.2, macOS 13.1, macOS 12 |
| Obudowa | Tower |
| Konstrukcja obudowy | Plastikowa |
| Rozmiary (szer. x wys. x gł.) (mm) | Nie większe niż 95 x 220 x 307 |
| Waga | maksimum 7 kg (urządzenie bez opakowania i akcesoriów) |
| Temperatura robocza (°C) | 0 - 40 |
| Względna wilgotność robocza (bez kondensacji) (%) | 0 - 90 |
| Rozproszenie ciepła (BTU/hr) | Nie więcej niż 27 BTU/hr |
| Pozostałe wymagane certyfikaty | CE |

# Network Attached Storage (NAS) - Dysk sieciowy wraz z 2 dyskami o pojemności min.2TB każdy- 2 szt.

Dostarczane urządzenia Wykonawca dostarczy we wskazane przez Zamawiającego lokalizacje:

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Lokalizacja** | **Liczba sztuk** |
| 1 | Ujęcie Wody w Białej  Biała 97B, 21-300 Radzyń Podlaski | 1 |
| 2 | Ujęcie Wody w Branicy Radzyńskiej Kol. Branica Radzyńska – Kol. 49B, 21-300 Radzyń Podlaski | 1 |

Minimalne wymagania:

| **Element** | **Minimalne wymagania** |
| --- | --- |
| Obudowa | Tower |
| Procesor | Czterordzeniowy procesor o taktowaniu 2.0 GHz (maksymalnie 2,7 GHz z przyspieszeniem) osiągający w teście PassMark co najmniej 2950 punktów  Załącznik zawierający obowiązującą tabelę wyników testu PassMark znajduje się w załączniku nr 5.1 do SWZ |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) |
| Pamięć RAM | min. 2 GB pamięci non-ECC SODIMM z możliwością rozszerzenia do min. 6 GB |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 2 kieszenie na dyski twarde typu hot-swap. Obsługiwane dyski 3.5” oraz 2.5”. |
| Pamięć masowa | Zainstalowane dyski:  Min. 2 zainstalowane dyski HDD 3,5“ 2 TB 5400 obr./min SATA III 6 Gb/s.  Zamawiający dopuszcza możliwość instalacji dysków przez Wykonawcę na etapie dostawy.  Dyski muszą znajdować się na oficjalnej liście kompatybilności dysków dla oferowanego urządzenia przygotowanej przez producenta urządzenia. |
| Porty zewnętrzne | Minimum:  •    2 porty USB 3.2.1 |
| Porty sieciowe | Minimum:  • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |
| Funkcja Wake on LAN/WAN | Tak |
| Wentylator obudowy | Min. 1 wentylator 92 mm x 92 mm |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS  Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:  •         Wewnętrzny: Btrfs, ext4  •         Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| Zarządzanie pamięcią masową | •         Maksymalny rozmiar pojedynczego wolumenu: 108 TB  •         Minimalny liczba wewnętrznych wolumenów: 64  •         Minimalny liczba obiektów iSCSI Target: 128  •         Minimalny liczba jednostek iSCSI LUN: 256  •         Obsługa klonowania/migawek jednostek iSCSI LUN |
| Obsługiwane typy macierzy RAID | Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0, RAID 1 |
| Funkcja udostępniania plików | •       Minimalna liczba kont użytkowników: 2 048  •       Minimalna liczba grup użytkowników: 256  •       Minimalna liczba folderów współdzielonych: 256  •       Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 500  • Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 1 500 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| Usługa katalogowa | Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| Bezpieczeństwo | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie  SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| Obsługiwane systemy klienckie | Windows i MacOS wersje wspierane przez producentów |
| Obsługiwane przeglądarki | Chrome, Firefox, Microsoft Edge, Safari 13 i nowsze  Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android 11.0 i nowsze) na tabletach |
| Zasilanie | Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 60 W |
| Oprogramowanie | •   Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych  •   Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów  •   Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.  •       Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| Gwarancja | Wykonawca udzieli gwarancji:  • 2 lat na urządzenia główne z możliwością przedłużenia do 4 lat za pomocą dodatkowego pakietu gwarancyjnego |
| Dodatkowe wymagania | W ramach dostawy Wykonawca powinien skonfigurować urządzenia według wytycznych Zamawiającego |

# Network Attached Storage (NAS) - Dysk sieciowy w obudowie RACK wraz z 4 dyskami o pojemności min. 8TB każdy-1 szt.

Minimalne wymagania:

|  |  |  |
| --- | --- | --- |
| **Element** | **Parametry wymagane** | |
| Obudowa | Rack 1U | |
| Procesor | Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark co najmniej 4 630 punktów  Załącznik zawierający obowiązującą tabelę wyników testu PassMark znajduje się w załączniku nr 5.1 do SWZ | |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) | |
| Pamięć  RAM | min. 32 GB pamięci ECC SODIMM | |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA. | |
| Pamięć masowa | Zainstalowane dyski:  Min. 4 zainstalowane dyski HDD 3,5“ 8 TB 7200 obr./min SATA III 6 Gb/s. Dyski muszą znajdować się na oficjalnej liście kompatybilności dysków dla oferowanego urządzenia przygotowanej przez producenta urządzenia.  Zamawiający dopuszcza możliwość instalacji dysków przez Wykonawcę na etapie dostawy | |
| Porty zewnętrzne | Minimum:  •         2 porty USB 3.2.1  •         1 port eSATA (jako gniazdo rozszerzenia) | |
| Porty sieciowe | Minimum:  • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) | |
| Funkcja Wake on LAN/WAN | Tak | |
| Gniazdo rozszerzeń PCIe 2.0 | Min. 1x 4-liniowe gniazdo x8 gen. 3 | |
| Dodatkowa karta rozszerzeń | Dwuportowa karta rozszerzeń 10 GbE SFP+  Karta rozszerzeń musi znajdować się na oficjalnej liście kompatybilności kart sieciowych dla oferowanego urządzenia przygotowanej przez producenta urządzenia.  Zamawiający dopuszcza możliwość instalacji karty przez Wykonawcę na etapie dostawy | |
| Wentylator obudowy | Min. 2 wentylatory (40 × 40 × 20 mm) | |
| Obsługiwane protokoły sieciowe | Min. SMB (CIFS) NFSv3, NFSv4, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP | |
| Obsługiwane systemy plików | Min.:  •         Wewnętrzny: Btrfs, ext4  •         Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT | |
| Zarządzanie pamięcią masową | •         Maksymalny rozmiar pojedynczego wolumenu: 108 TB  •         Minimalny liczba wewnętrznych wolumenów: 64  •         Minimalny liczba obiektów iSCSI Target: 128  •         Minimalny liczba jednostek iSCSI LUN: 256  •         Obsługa klonowania/migawek jednostek iSCSI LUN | |
| Obsługiwane typy macierzy RAID | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | |
| Funkcja udostępniania plików | •         Minimalna liczba kont użytkowników: 2 048  •         Minimalna liczba grup użytkowników: 256  •         Minimalna liczba folderów współdzielonych: 512  •         Minimalna liczba jednoczesnych połączeń  CIFS/AFP/NFS/FTP: 500\*  *\*Liczba jednoczesnych połączeń może zostać zwiększona do 2 000 po zainstalowaniu co najmniej 8 GB pamięci RAM.* | |
| Uprawnienia | Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji | |
| Wirtualizacja | Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack® | |
| Usługa katalogowa | Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP | |
| Bezpieczeństwo | Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) | |
| Obsługiwane przeglądarki | Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach | |
| Oprogramowanie | •   Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych  •   Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów  •   Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.  •   Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. | |
| Konserwacja | • | Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack |
| Zasilanie | • | Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz. |
| Gwarancja | •  • | 3 lata na urządzenia główne  1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack |
| Dodatkowe wymagania |  | W ramach dostawy Wykonawca powinien skonfigurować urządzenia według wytycznych Zamawiającego |

# UPS do klastra serwerów-1 szt.

Minimalne wymagania:

| **Charakterystyka podstawowa** | **Parametry wymagane** |
| --- | --- |
| Fazy | Trójfazowe |
| Technologia wykonania UPS | Podwójna konwersja online |
| Możliwość rozbudowy o kolejne UPS (praca równoległa) | Wymagana |
| Moc pozorna (VA) | 10000 |
| Moc rzeczywista (W) | 10000 |
| Kształt fali na wyjściu(praca na baterii) | Czysta fala sinusoidalna |
| Kompatybilność z zasilaczami z aktywnym PFC | Wymagana |
| Ochrona przed przeciążeniem | Wymagana(minimum bezpiecznik i wewnętrzny ogranicznik prądu) |
| Filtr EMI/RFI | Wymagany |
| Nominalne napięcie wejściowe (V) | Faza – zero (L-N):220, 230, 240 Vac, Faza – faza (L-L):380, 400, 415 Vac |
| Zakres napięcia wejściowego (V) | Faza – zero (L-N) 132 ~ 276 Vac  Faza – faza (L-L): 228 ~ 478 Vac |
| Konfigurowalny zakres napięcia ( Vac ) | Faza – zero (L-N) 220 ~ 250 Vac  Faza – faza (L-L): 380 ~ 435 Vac |
| Częstotliwość wejściowa(Hz) | 50 ± 3  60 ± 3 |
| Zakres częstotliwości wejściowej ( Hz ) | 40 ~ 70 |
| Współczynnik mocy wejściowej | 0.99 |
| Kompatybilność z generatorem | Wymagana |
| Dwa źródła zasilania | Wymagane |
| Tolerancja napięcia wyjściowego ( % ) | 1.5 % |
| Współczynnik mocy | 1 |
| Ochrona przed przeciążeniem (tryb liniowy) | 105~110% obciążenia przez 60 min, 110~125% obciążenia przez 10 min, 125~150% obciążenia przez 1 min, >150% obciążenia od razu |
| Ochrona przed przeciążeniem (tryb baterii) | 105~110% obciążenia przez 60 min, 110~125% obciążenia przez 10 min, 125~150% obciążenia przez 1 min, >150% obciążenia od razu |
| Współczynnik szczytu | 03:01 |
| Zniekształcenia harmoniczne (obciążenie liniowe) | THD＜1% |
| Zniekształcenia harmoniczne (obciążenie nieliniowe) | THD＜5% |
| Rodzaj złącza wejściowego | Złącze typu kostka zaciskowa do łączenia przewodów |
| Rodzaj złącza wyjściowego | Złącze typu kostka zaciskowa do łączenia przewodów |
| Typowy czas przełączenia na baterie (ms) | 0 ms |
| Bateria | Wymagana praca z zewnętrznymi modułami baterii, możliwość zastosowania zewnętrznych modułów |
| Czas podtrzymania | Dla połowy obciążenia (5000W) minimum 20 minut |
| Sygnalizacja | Wymagane alarmy dźwiękowe oraz wyświetlacz LCD |
| Alarmy dźwiękowe | minimum Tryb baterii, Niski poziom baterii, Przeciążenie, Przeładowanie, Przegrzanie, Usterka UPS, Wymień baterię |
| Konfiguracja wybranych parametrów | Przez wyświetlacz LCD, minimum ustawienia trybu pracy, baterii, ustawienia wejścia-wyjścia |
| Dołączone oprogramowanie do zarządzania | Wymagane, obsługa platform Windows, Linux, Vmware |
| Zarządzanie przez sieć | Zainstalowana karta zarządzająca HTTP/SNMP |
| Port szeregowy | RS232 x 1 + RS485 x 1 |
| Obudowa | Wymagana możliwość instalacji w szafie RACK |
| Konstrukcja obudowy | Metalowa |
| Szyny/uchwyty rack | Wymagane |
| Rozmiary (szer. x wys. x gł.) (mm) | Nie większe niż 6U |
| Temperatura robocza (°C) | 0 ~ 40 |
| Względna wilgotność robocza (bez kondensacji) (%) | 0 ~ 90 |
| Certyfikaty | CE, IEC62040-1, IEC62040-2 |
| Na urządzenie | minimum 2 lata |

# UPS 3KVA-1 szt.

Minimalne wymagania:

| **Charakterystyka podstawowa** | **Parametry wymagane** |
| --- | --- |
| Technologia wykonania UPS | Online podwójna konwersja |
| Moc pozorna (VA) | 3000 |
| Moc rzeczywista (W) | 2700 |
| Kształt fali na wyjściu(praca na baterii) | Czysta fala sinusoidalna |
| Kompatybilność z zasilaczami z aktywnym PFC | Wymagana |
| Ochrona przed przeciążeniem | Wymagana(minimum bezpiecznik i wewnętrzny ogranicznik prądu) |
| Filtr EMI/RFI | Wymagany |
| Nominalne napięcie wejściowe (V) | 230 ± 10% |
| Obsługiwany zakres napięcia wejściowego (V) | 190 ~ 300 |
| Częstotliwość wejściowa(Hz) | 50 ± 10, 60 ± 10 |
| Wykrywanie częstotliwości wejściowej | Wymagane automatyczne |
| Napięcie przy pracy na baterii (V) | 208 +/-1% ; 220 +/-1%; 230 +/-1%; 240 +/-1% |
| Częstotliwość przy pracy baterii (Hz) | 50+/-0.1% ; 60+/-0.1% |
| Rodzaj złącza wejściowego | IEC C20 |
| Rodzaj złącza wyjściowego | IEC C19 x 1, IEC C13 x 8 |
| Typowy czas przełączenia na baterie (ms) | 0 ms |
| Bateria | Wbudowana |
| Czas pracy przy połowie obciążenia (min.) | 14 |
| Czas pracy przy pełnym obciążeniu (min.) | 4 |
| Typowy czas ponownego ładowania (godziny) | 4 |
| Rodzaj baterii | Hermetyczna kwasowo-ołowiowa |
| Praca z zewnętrznymi kompatybilnymi modułami bateryjnymi | Wymagana |
| Ilośc możliwych do podłączenia modułów bateryjnych | 3 |
| Sygnalizacja | Wymagane alarmy dźwiękowe oraz wyświetlacz LCD |
| Alarmy dźwiękowe | minimum Tryb baterii , Niski poziom baterii , Przeciążenie , Przeładowanie , Przegrzanie, Usterka UPS, Wymień baterię |
| Konfiguracja wybranych parametrów | Przez wyświetlacz LCD. Minimum: Ustawienie trybu, Ustawienia alarmu, Wejście i wyjście, Ustawienia baterii |
| Port komunikacyjny USB | Wymagany |
| Port wyłącznika awaryjnego EPO | Wymagany |
| Dołączone oprogramowanie do zarządzania | Wymagane, obsługa platform Windows, Linux, Vmware |
| Zarządzanie przez sieć | Wymagane jest dostarczenie UPS wraz z kartą zarządzającą umożliwiającą zarządzanie HTTP/SNMP |
| Obudowa | Wymagana możliwość instalacji w szafie RACK lub ustawienia jako Tower |
| Konstrukcja obudowy | Metalowa |
| Szyny/uchwyty rack | Wymagane |
| Temperatura robocza (°C) | 0 ~ 40 |
| Względna wilgotność robocza (bez kondensacji) (%) | 20 ~ 90 |
| Pozostałe wymagane certyfikaty | CE, RoHS |
| Na urządzenie | minimum 2 lata |
| Na baterie | minimum 2 lata |
| Montaż | Wraz z dostawą urządzenia Wykonawca zamontuję UPS w szafie RACK znajdującej się w budynku Zamawiającego |

# UPS - Zasilacz awaryjny do stanowisk pracy-30 szt.

Minimalne wymagania:

| Charakterystyka podstawowa | Parametry wymagane |
| --- | --- |
| Technologia wykonania UPS | Line-interactive |
| Moc pozorna (VA) | minimum 850 |
| Moc rzeczywista (W) | minimum 425 |
| Kształt fali na wyjściu(praca na baterii) | Symulowana fala sinusoidalna |
| Automatyczna regulacja napięcia (mechanizm AVR) | Wymagany |
| Ochrona przed przeciążeniem | Wymagana(minimum bezpiecznik oraz wewnętrzny ogranicznik prądu) |
| Filtr EMI/RFI | Wymagany |
| Układ przeciwprzepięciowy (J) | Wymagany, minimum 150 |
| Nominalne napięcie wejściowe (V) | 230+/-10% |
| Obsługiwany zakres napięcia wejściowego (V) | minimum 165 - 290 |
| Częstotliwość wejściowa(Hz) | 50+/-5 ; 60+/-5 |
| Wykrywanie częstotliwości wejściowej | Wymagane automatyczne |
| Napięcie przy pracy na baterii (V) | 230+/-10% |
| Częstotliwość przy pracy baterii (Hz) | 50+/-1% ; 60+/-1% |
| Rodzaj złącza wejściowego | Schuko |
| Gniazdka | FR x 3 |
| Typowy czas przełączenia na baterie (ms) | 4 ms |
| Czas podtrzymania na baterii | Wymagana, czas pracy przy pełnym obciążeniu do 1 min, przy obciążeniu 200W do 5,5 min. |
| Ładowanie baterii | Typowy czas ładowania do 6 h |
| Sygnalizacja | Wymagane alarmy dźwiękowe oraz diody LED |
| Diody LED - syngalizacja | Zasilanie włączone, Tryb liniowy, Tryb baterii, Tryb obejścia, Niski poziom baterii, Przeciążenie, Usterka UPS |
| Alarmy dźwiękowe - sygnalizacja | Tryb baterii, Niski poziom baterii, Przeciążenie, Usterka UPS |
| Port komunikacyjny USB (HID) | Wymagany |
| Dołączone oprogramowanie do zarządzania | Wymagane, obsługa platform Windows, Linux oraz mac |
| Obudowa | Tower |
| Konstrukcja obudowy | Plastikowa |
| Rozmiary (szer. x wys. x gł.) (mm) | Nie większe niż 84 x 174 x 280 |
| Waga | maksimum 4,2 kg (urządzenie bez opakowania i akcesoriów) |
| Temperatura robocza (°C) | 0 - 40 |
| Względna wilgotność robocza (bez kondensacji) (%) | 0 - 90 |
| Rozproszenie ciepła (BTU/hr) | Nie więcej niż 34 BTU/hr |
| Pozostałe wymagane certyfikaty | CE, RoHS |
| Gwarancja | minimum 2 lata na urządzenie i baterie |

# Serwer - Klaster serwerów-1 szt.

**Dostawa, instalacja, wdrożenie klastra wysokiej niezawodności (klastra HA) oraz migracja danych z obecnego środowiska Zamawiającego wraz z organizacją systemu kopii zapasowych**

**1.**    **Dostawa komponentów klastra HA**

W ramach zamówienia należy dostarczyć następujący sprzęt wraz z oprogramowaniem i okablowaniem niezbędnym do stworzenia klastra wysokiej niezawodności. Dostarczany sprzęt musi być fabrycznie nowy, nie noszący śladów użytkowania.

* Serwer hosta platformy wirtualizacyjnej – 3 szt.
* Macierz dyskowa – 1 szt (szczegółowy opis w pkt 10.).
* Przełączniki z portami 10Gb do komunikacji wewnętrznej klastra HA wraz z kompletem wkładek i kabli DAC, patchcordów  potrzebnych do konfiguracji klastra HA – 2 szt.
* Serwer typu NAS służący jako archiwum kopi zapasowych – 1 szt. (szczegółowy opis w pkt 5)
* Przełączniki dostępowe do sieci LAN Zamawiającego min. 48 portowe z możliwością podpięcia klastra HA poprzez porty 10Gb – 2 szt. (szczegółowy opis w pkt 12)

Wyżej wymieniony sprzęt należy dostarczyć, skonfigurować i zamontować w siedzibie Zamawiającego, w serwerowni na parterze budynku, w szafach rack udostępnionych Wykonawcy po uprzednim zdemontowaniu urządzeń wskazanych przez Zamawiającego. Koszty dostawy i instalacji urządzeń powinny być wkalkulowane w ofertę, Wykonawca nie może wnosić o dodatkową zapłatę związaną z kosztami wysyłki, ubezpieczenia, instalacji sprzętu itp.

Szczegółowa specyfikacja sprzętu:

* Serwer hosta platformy wirtualizacyjnej - 3 szt.

| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| --- | --- |
| **Obudowa** | Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz każdy, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Płyta główna powinna obsługiwać CPU do 64 rdzeni. |
| **RAM** | Minimum 128GB DDR5 ECC RDIMM 4800MT/s, w minimum 4 kościach w celu zwiększenia wydajności oferowanego rozwiązania. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1.5TB pamięci RAM. |
| **Funkcjonalność pamięci RAM** | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) lub równoważne. |
| **Gniazda PCI** | - minimum 1x slot PCIe 16x generacji 4  - minimum 2x slot PCIe 8x generacji 4 |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz łącznie 8 interfejsów sieciowych 10Gb Ethernet w standardzie SFP+ (liczba portów nie może być osiągnięta poprzez zainstalowanie karty w wymaganych slotach PCIe). Dostarczone kable DAC SFP+ min. 3m 10Gb Ethernet w ilości umożliwiającej podłączenie serwerów zgodnie ze schematem poglądowym na Rysunku 1. |
| **Dyski twarde** | Zainstalowana karta wyposażona w dwa dyski M.2 NVMe o pojemności min. 480GB w konfiguracji RAID 1 oraz DWPD o wartości nie mniejszej niż 1. |
| **System operacyjny/System wirtualizacji** | Licencja na system operacyjny - wymagana kompatybilność z obecnie posiadaną infrastrukturą. Licencja na Windows Server 2025 Datacenter, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze. |
| **Wbudowane porty** | 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA |
| **Zasilacze** | Redundantne, Hot-Plug min. 700W każdy. |
| **Bezpieczeństwo** | * Moduł TPM 2.0 |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklarację CE.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows 2019, Microsoft Windows 2022. |
| **Warunki gwarancji** | 3 lata gwarancji producenta, realizowana w miejscu instalacji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

Uwaga: Serwery muszą być tego samego typu o tych samych parametrach fizycznych, procesorach, dyskach i pamięci RAM co jest funkcjonalnością wymaganą do bezproblemowej instalacji i funkcjonowania klastra HA

Do klastra Wykonawca powinien dostarczyć również 40 licencji MS WINSVR CAL 2025.

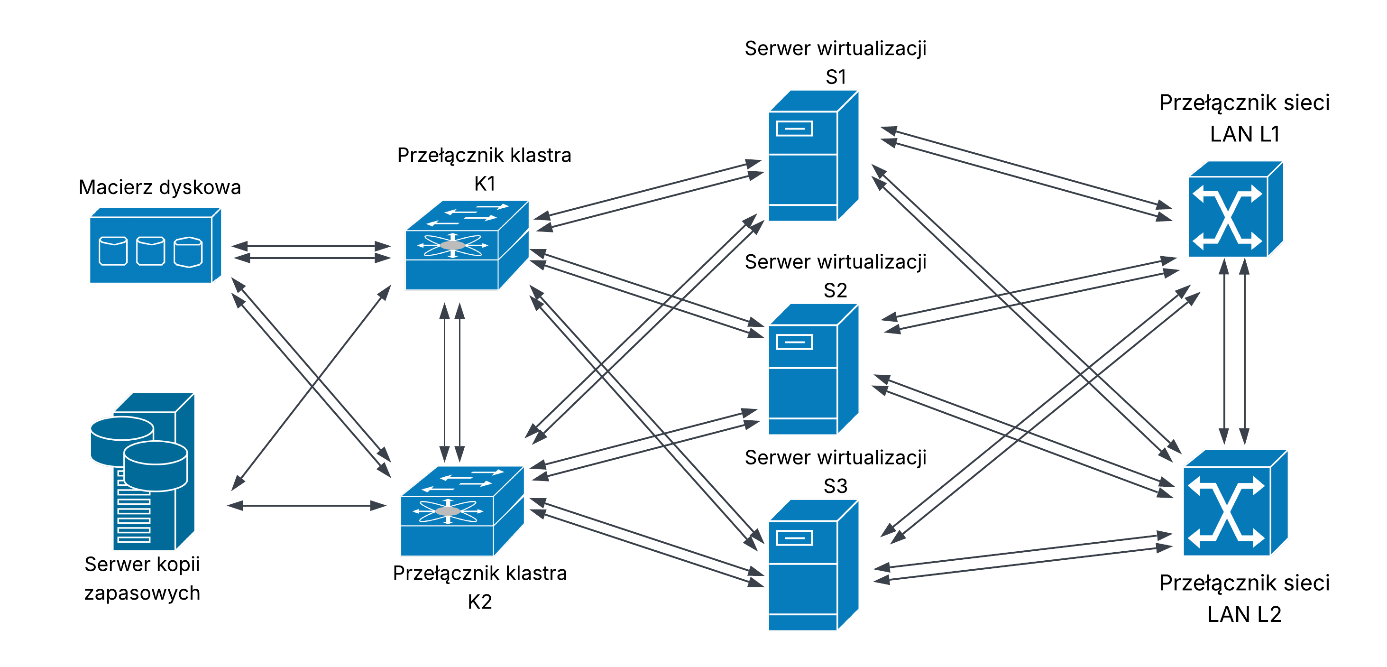
* Przełączniki do komunikacji wewnętrznej klastra HA wraz z kompletem wkładek i kabli DAC, patchkordów niezbędnych do konfiguracji klastra HA – 2 szt.

| **Komponent** | **Minimalne wymagania** |
| --- | --- |
| **Porty** | Przełącznik 1U wyposażony w porty:  - minimum 16 portów 10 Gigabit Ethernet SFP+  - 1 port konsolowy RJ45 lub USB |
| **Kable/wkładki** | Kable DAC SFP+ 10GbE min. 1m w ilości niezbędnej do podłączenia urządzeń zgodnie ze schematem poglądowym na Rysunku 1. |
| **Zasilanie** | 2 redundantne zasilacze AC |
| **RACK** | Musi zapewniać instalację w szafach 19” |
| **Pamięć** | Pamięć CPU: 256MB |
| **Wydajność** | Musi posiadać matrycę przełączającą o wydajności min. 300Gbps |
| **Chłodzenie** | Temperatura pracy w przedziale 0-40 stopni Celcjusza |
| **Funkcjonalności warstwy II** | Musi obsługiwać ramki „Jumbo” o długości min. 9000 B.  Musi obsługiwać, co najmniej 2000 VLANów.  Pamięć, dla co najmniej 32 000 adresów MAC.  Musi obsługiwać protokoły: STP, RSTP, MSTP  Musi wspierać funkcjonalność wirtualnej agregacji portów LACP  Musi być zgodny z następującymi standardami IEEE:  IEEE 802.1Q  IEEE 802.3ad  IEEE 802.1D / 802.1w / 802.1s  IEEE 802.1X  IEEE 802.3x  IEEE 802.1p |
| **Funkcjonalności warstwy III** | Wsparcie dla DHCP server i DHCP Relay |
| **Mechanizmy bezpieczeństwa i QoS** | Musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci:   * co najmniej 8 kolejek dla obsługi ruchu, * Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). * Obsługa DSCP * Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci: * Autoryzacja użytkowników/portów w oparciu o 802.1x * Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6 |
| **Mechanizmy zarządzania** | Musi wspierać następujące mechanizmy zarządzania   * Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 lub SSHv2 * Urządzenie musi posiadać port konsolowy do zarządzania typu RJ45 (konsola) |

**2. Wdrożenie klastra HA**

2.1  Projekt wykonawczy

W ramach prowadzonych prac Wykonawca przygotuje projekt budowanego klastra wysokiej dostępności i przedłoży go do akceptacji w ciągu 21 dni od podpisania umowy. Projekt ten należy przygotować zgodnie z ideą przedstawioną na Rysunek 1.



Rysunek 1 Schemat poglądowy budowy klastra.

Projekt wykonawczy wdrożenia musi zawierać szczegółowy harmonogram realizacji prac, sporządzony przez Wykonawcę, w którym uwzględnione zostaną:

* Konieczność utrzymania ciągłości usług realizowanych przy udziale środowisk wirtualnych w zasobach Zamawiającego oraz przy założeniu minimalizowania skutków czasów przerwy niezbędnych do wykonania migracji poszczególnych maszyn wirtualnych. Niezbędne czasy niedostępności poszczególnych usług muszą zostać ograniczone do czasu niezbędnego na czas potrzebny do wstrzymania pracy poszczególnych maszyn w dotychczasowym środowisku a następnie ich ponownego uruchomienia w zasobach zbudowanego centrum danych
* Konieczność realizacji prac instalacyjnych i uruchomieniowych w dni robocze Zamawiającego w godzinach od 7:00 do 15:00.

Zamawiający dokona akceptacji projektu w ciągu 5 dni roboczych od złożenia oficjalnym kanałem komunikacji.

2.2  Wdrożenie systemu klastra

* Sprzęt należy dostarczyć, zamontować w  szafach rack i podłączyć do infrastruktury Zamawiającego w siedzibie UG Radzyń Podlaski zgodnie z punktem nr 1.
* Podczas wdrożenia należy podłączyć urządzenia do sieci  LAN/SAN oraz przeprowadzić konfigurację dostarczonych rozwiązań sieciowych zgodnie z dokumentacją sieci dostarczoną przez przedstawiciela Zamawiającego ze szczególnym uwzględnieniem adresacji, VLANów, oraz mechanizmów zabezpieczeń wdrożonych już przez zamawiającego. Wszystkie nowe zagadnienia związane z wdrożeniem, a dotyczące konfiguracji sieci należy uzgodnić z Zamawiającym
* Przełączniki K1 i K2, dedykowane dla komunikacji w ramach klastra HA i macierzy, muszą zostać skonfigurowane z wykorzystaniem mechanizmu wirtualnej agregacji portów (np. MLAG, VLT, vPC lub równoważnego), umożliwiającego terminowanie agregacji EtherChannel/LACP z urządzeń zewnętrznych (serwerów, macierzy) równocześnie na obu przełącznikach przy zachowaniu niezależności ich systemów operacyjnych.
* Przełączniki L1 i L2, przeznaczone do budowy sieci LAN, mogą zostać skonfigurowane jako wirtualny stos urządzeń (stack) z wykorzystaniem najbardziej wydajnych interfejsów dostępnych w dostarczonych urządzeniach.
* Wszystkie połączenia serwerów, macierzy oraz przełączników LAN do przełączników klastra i/lub przełączników sieci LAN powinny zostać, o ile to możliwe, zrealizowane z wykorzystaniem agregacji łączy (LAG, MLAG, VLT lub równoważnej) w celu zapewnienia wysokiej dostępności oraz równoważenia obciążenia.
* Przełączniki sieciowe dostarczone w ramach wdrożenia należy skonfigurować zgodnie z zaleceniami Zamawiającego dostosowując konfigurację zgodnie z dokumentacją sieci LAN urzędu
* Należy przeprowadzić proces instalacji oprogramowania wirtualizacyjnego Proxmox lub oprogramowania równoważnego\* na dostarczonych serwerach wraz z konfiguracją RAID dysków,  połączeń sieciowych wraz z ich nadmiarowością, modułów odpowiedzialnych za monitorowanie sprawności i zarządzania poszczególnymi podzespołami maszyn.
* Wykonawca dostarczy i zainstaluje oprogramowanie do wirtualizacji w najnowszych dostępnych wersjach wraz ze wszystkimi niezbędnymi poprawkami dostępnymi na dzień podpisania protokołu odbioru.
* W następnym etapie należy wykonać synchronizację klastra HA  składającego  
   się z trzech dostarczonych serwerów.
* Na etapie wdrożenia Wykonawca podłączy do sieci  i skonfiguruje niezbędne  
   do pracy w klastrze oraz udostępniania zasobów ustawienia dostarczanej macierzy dyskowej.
* Dodatkowo należy wdrożyć i skonfigurować system kopii zapasowych oparty  
   o archiwa gromadzone na dyskach serwera  NAS wymienionego w punkcie 1.
* Serwer kopii NAS należy skonfigurować w uzgodnieniu  z Zamawiającym i zgodnie z  jego zaleceniami a także najlepszymi praktykami dotyczącymi tego zagadnienia. Serwer będzie służył jako repozytorium kopii zapasowych klastra HA. Część zasobów NAS należy wydzielić jako serwer kopii zapasowych najistotniejszych z punktu widzenia zachowania ciągłości działania firmy komputerów użytkowników.
* Wykonawca w ramach wdrożenia przeprowadzi migrację będących w zasobach Zamawiającego systemów serwerowych, wirtualnych oraz tych zlokalizowanych na fizycznych maszynach, wraz z oprogramowaniem tam zgromadzonym.
* W trakcie wykonywania migracji zasobów Zamawiającego na Klaster HA należy zaktualizować systemy operacyjne oraz oprogramowanie do najnowszych wersji (za wyjątkiem systemów gdzie oprogramowanie Zamawiającego wyraźnie wskazuje że nie będzie współpracowało z najnowszymi wersjami systemów operacyjnych, a czynności te narażały by je na utratę stabilności i awarie).
* Przed zgłoszeniem do odbioru prac Wykonawca  w obecności przedstawiciela Zamawiającego musi przeprowadzić testy niezawodności dostarczonego systemu polegające na:
  + symulacji awarii pojedynczych linków połączeniowych pomiędzy urządzeniami a przełącznikami sieciowymi,
  + symulacji awarii jednego z węzłów klastra HA.
* Wykonawca po ukończeniu prac wdrożeniowych ma obowiązek dostarczyć dokumentację powykonawczą zawierającą opis wdrożenia, schematy połączeń, adresacje urządzeń, konfigurację VLANów, karty katalogowe i certyfikaty dostarczonych urządzeń.

Kryteria równoważności oprogramowania wirtualizacyjnego Proxmox:

**Zarządzanie maszynami wirtualnymi:**

* Oprogramowanie musi umożliwiać uruchamianie, zarządzanie i monitorowanie maszyn wirtualnych w trybie KVM (Kernel-based Virtual Machine) lub równoważnym.
* Musi wspierać migrację maszyn wirtualnych na żywo (live migration) między różnymi hostami fizycznymi bez przerywania działania systemów.

**Zarządzanie kontenerami:**

* Wymagana jest obsługa kontenerów LXC (Linux Containers) lub równoważnych, z możliwością tworzenia, zarządzania i monitorowania kontenerów na różnych węzłach.

**Interfejs użytkownika:**

* Oprogramowanie musi oferować intuicyjny, przeglądarkowy interfejs zarządzania (GUI), umożliwiający zdalne zarządzanie zasobami, monitorowanie wydajności, a także zarządzanie uprawnieniami użytkowników.

**Wsparcie dla klastrów i HA (High Availability):**

* System powinien wspierać tworzenie klastrów z możliwością zarządzania wieloma węzłami, zapewniając wysoki poziom dostępności (High Availability) dla maszyn wirtualnych i kontenerów.

**Zarządzanie zasobami i migracją:**

* Możliwość dynamicznego przydzielania zasobów (CPU, RAM, przestrzeń dyskowa) dla maszyn wirtualnych i kontenerów.
* Obsługa migracji na żywo dla maszyn wirtualnych i kontenerów oraz obsługa redundancji zasobów.

**Zintegrowana funkcjonalność kopii zapasowych:**

* Oprogramowanie powinno oferować funkcje planowania i zarządzania kopiami zapasowymi maszyn wirtualnych i kontenerów, z możliwością przechowywania kopii na różnych mediach (dyski lokalne, sieciowe, chmura itp.).

**Wsparcie dla różnych systemów plików:**

* Musi oferować wsparcie dla popularnych systemów plików (np. ZFS, LVM, ext4, XFS) lub ich równoważników, z funkcjami zarządzania pamięcią masową i deduplikacją.

**Integracja z systemami zewnętrznymi:**

* Możliwość integracji z popularnymi systemami monitoringu i zarządzania infrastrukturą IT (np. Zabbix, Nagios, Ansible, Puppet).

**Wsparcie dla sieci wirtualnych:**

* Powinno zapewniać możliwość zarządzania sieciami wirtualnymi, w tym VLAN, bonding, routing oraz integrację z zewnętrznymi rozwiązaniami sieciowymi.

**Licencjonowanie i wsparcie:**

* Oprogramowanie powinno oferować licencjonowanie z elastycznymi opcjami dla małych i dużych wdrożeń oraz dostępnością wsparcia technicznego na różnych poziomach.

**Bezpieczeństwo:**

* Obsługa szyfrowania danych, uwierzytelniania dwuskładnikowego (2FA), oraz zgodność z aktualnymi standardami bezpieczeństwa IT.

**Otwarty kod źródłowy:**

* Oprogramowanie musi być dostępne na licencji open source, takiej jak AGPL v3 lub równoważnej, co zapewnia otwarty dostęp do kodu źródłowego, możliwość jego modyfikacji i rozpowszechniania. Oprogramowanie powinno mieć również wsparcie społeczności oraz zapewnioną transparentność w zakresie bezpieczeństwa i rozwoju.

**3.**    **Migracja zasobów , instalacja maszyn wirtualnych**

Aktualna platforma wirtualizacyjna pracuje w oparciu o wirtualizator Proxmox. Tabela 1 zawiera aktualną charakterystykę maszyn wirtualnych pracujących na zasobach Zamawiającego:

Tabela Aktualną charakterystyka maszyn wirtualnych w zasobach Zamawiającego

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **System** | **vCPU** | **Memory** | **Storage** |
| 1. | Windows Serwer 2012 | 4 | 8 GB | 120 GB |
| 2. | Windows Serwer 2022 | 2 | 4 GB | 32 GB |
| 3. | Windows Serwer 2019 | 2 | 4 GB | 385 GB |
| 4. | Windows Serwer 2019 | 4 | 16 GB | 250 GB |
| 5. | Linux  Ubuntu | 4 | 4 GB | 40 GB |
| 6. | Windows 10 | 4 | 4 GB | 32 GB |

Maszyny wirtualne należy migrować do nowo utworzonego Klastra HA z dotychczas używanego serwera wirtualizacji. Przeniesienie maszyn wirtualnych opartych na platformie Microsoft powinno odbyć się wraz z aktualizacją platform serwerowych do najnowszej możliwej wersji oprogramowania Microsoft Windows Serwer. Niektóre z kluczowych zasobów wskazanych przez Zamawiającego należy zmigrować na szereg odrębnych maszyn wirtualnych przeznaczonych do obsługi wydzielonych baz danych i aplikacji branżowych urzędu.

Dodatkowo w procesie migracji do Klastra HA wytypowane zostały zasoby fizycznego serwera użytkowanego przez Zamawiającego na którym zgromadzono szereg baz danych  
 i aplikacji branżowych.  Dane te należy migrować do klastra tworząc szereg odrębnych maszyn wirtualnych które będą obsługiwać każdą z aplikacji osobno. Maszyny wirtualne należy utworzyć jako systemy Microsoft Windows Serwer 2025 Data Center.

Zasoby serwera fizycznego:

* + około 570 GB danych,
  + system operacyjny Windows Serwer 2016,
  + kilka różnych baz danych opartych o silniki JBoss i Firebird.

Szczegóły tworzonych maszyn wirtualnych uzgodnione zostaną z Wykonawcą na etapie wdrożenia.

# Macierz dyskowa do klastra-1 szt.

Macierz dyskowa do klastra – 1 szt.

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje 12 dysków 3.5”. |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active (dual-active) posiadające łącznie minimum osiem portów LAN Ethernet o przepustowości minimum 10Gbps. Wykonawca dostarczy kable DAC SFP+ w niezbędnej liczbie do podłączenia macierzy do klastra zgodnie z zaakceptowanym projektem. |
| **Cache** | 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami. Całkowita ilość cache 32GB. |
| **Dyski** | Zainstalowane 2 dyski HDD Hot-Plug o pojemności nie mniejszej niż 12TB SAS3 12Gb 7.2k.  Zainstalowane 8 dysków SSD Hot-Plug o pojemności nie mniejszej niż 1.92TB SAS3 12Gbps.  Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych tak by uzyskać łącznie nie mniej niż 120 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. |
| **Oprogramowanie/**  **Funkcjonalności** | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.  Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków.  Możliwość wykorzystania dysków SSD jako cache macierzy.  Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 900W każdy. |
| **Diagnostyka** | Poprzez kartę zarządzającą |
| **Certyfikaty** | Macierz musi być wyprodukowana zgodnie z normą  ISO-9001:2015  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta – dokumenty potwierdzające załączyć do oferty  Musi posiadać deklaracja CE. |
| **Warunki gwarancji** | 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

# Oprogramowanie antywirusowe-60 szt.

Jeżeli Zamawiający określił w SIWZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe.

W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

Dostarczone licencje mają umożliwiać zabezpieczenie urządzeń w poszczególnych jednostkach:  
Urząd Gminy Radzyń Podlaski - 60 licencji

Dostarczone licencje mają umożliwiać korzystanie z oprogramowania od momentu aktywacji przez Zamawiającego do dnia 30.06.2026 r.

Wykonawca zapewni usługę wsparcia wdrożeniowego dla Zamawiającego w wymiarze co najmniej 4 godzin.

**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.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowsze oraz  Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 8 i 9, Ubuntu Server 20.04 i 22.04 i 24.04 LTS, System Debian 11 i 12, SUSE Linux Enterprise Server (SLES) 15, Alma Linux 8 i 9, Rocky Linux 8 i 9, Oracle Linux 8 i 9, Amazon Linux 2 i 2023.

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.

**Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku  Microsoft Windows 10/11 32-bit i 64-bit.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w  systemach macOS (FileVault).

3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie  użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także  możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

**Ochrona urządzeń mobilnych opartych o system Android**

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.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.   
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do  chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam,  dokumenty oraz inne pliki typu .jar, .reg, .msi.

4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki  muszą zostać usunięte z serwerów producenta.

5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru  przesyłanych próbek.

6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub  folderów z przesyłania.

7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich  wspieranych produktów.

8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane  do analizy.

9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji  roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie  chronione.

10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach  roboczych.

11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub  administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć  jakie pliki zostały wysłane do analizy oraz przez kogo.

12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może  zakończyć się z wynikiem:

a) Czysty,

b) Podejrzany,

c) Bardzo podejrzany,

d) Szkodliwy.

13. 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.

14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość  wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.   
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z  której administrator może przywrócić dowolne pliki oraz utworzyć dla niej  wyłączenia.

# Switch zarządzalny, co najmniej 16 portów, 10Gb

Przełączniki dostępowe do sieci LAN Zamawiającego min. 16 portowe z możliwością podpięcia klastra HA poprzez porty 10Gb wraz z kompletem wkładek oraz okablowania niezbędnych do konfiguracji klastra HA – 2 szt

W ramach dostawy Wykonawca powinien skonfigurować urządzenie według wytycznych Zamawiającego

| **Komponent** | **Minimalne wymagania** |
| --- | --- |
| **Porty** | Przełącznik 1U wyposażony w porty:  - minimum 16 portów 10 Gigabit Ethernet SFP+  - 1 port konsolowy RJ45 lub USB |
| **Kable/wkładki** | Kable DAC SFP+ 10GbE min. 1m w ilości niezbędnej do podłączenia urządzeń zgodnie ze schematem poglądowym na Rysunku 1. |
| **Zasilanie** | 2 redundantne zasilacze AC |
| **RACK** | Musi zapewniać instalację w szafach 19” |
| **Pamięć** | Pamięć CPU: 256MB |
| **Wydajność** | Musi posiadać matrycę przełączającą o wydajności min. 300Gbps |
| **Chłodzenie** | Temperatura pracy w przedziale 0-40 stopni Celcjusza |
| **Funkcjonalności warstwy II** | Musi obsługiwać ramki „Jumbo” o długości min. 9000 B.  Musi obsługiwać, co najmniej 2000 VLANów.  Pamięć, dla co najmniej 32 000 adresów MAC.  Musi obsługiwać protokoły: STP, RSTP, MSTP  Musi wspierać funkcjonalność wirtualnej agregacji portów LACP  Musi być zgodny z następującymi standardami IEEE:  IEEE 802.1Q  IEEE 802.3ad  IEEE 802.1D / 802.1w / 802.1s  IEEE 802.1X  IEEE 802.3x  IEEE 802.1p |
| **Funkcjonalności warstwy III** | Wsparcie dla DHCP server i DHCP Relay |
| **Mechanizmy bezpieczeństwa i QoS** | Musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci:   * co najmniej 8 kolejek dla obsługi ruchu, * Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). * Obsługa DSCP * Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci: * Autoryzacja użytkowników/portów w oparciu o 802.1x * Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6 |
| **Mechanizmy zarządzania** | Musi wspierać następujące mechanizmy zarządzania   * Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 lub SSHv2 * Urządzenie musi posiadać port konsolowy do zarządzania typu RJ45 (konsola) |

# Wdrożenie serwera RADIUS-1 szt.

**Minimalny zakres usługi/dostawy:**

1. **Dostarczenie oprogramowania RADIUS**:
   * Oprogramowanie RADIUS, kompatybilne z istniejącą infrastrukturą IT urzędu.
   * Oprogramowanie powinno wspierać integrację z Active Directory (AD) i być zgodne z obowiązującymi standardami bezpieczeństwa.
2. **Instalacja i konfiguracja**:
   * Instalacja oprogramowania RADIUS na serwerze udostępnionym przez zamawiającego.
   * Konfiguracja serwera RADIUS w sposób zapewniający jego pełną integrację z istniejącą infrastrukturą AD.
   * Ustawienie polityk autoryzacji, zgodnych z wymaganiami zamawiającego, dla różnych typów użytkowników (np. pracownicy, goście, zdalni użytkownicy).
3. **Testowanie i uruchomienie systemu**:
   * Przeprowadzenie testów funkcjonalnych mających na celu weryfikację poprawności działania systemu RADIUS, w tym testy uwierzytelniania użytkowników, autoryzacji oraz odpowiedzi systemu na błędne próby logowania.
   * Wdrożenie systemu do środowiska produkcyjnego po pomyślnym zakończeniu testów.
4. **Szkolenie personelu**:
   * Przeprowadzenie szkolenia dla pracowników IT urzędu w zakresie obsługi i zarządzania systemem RADIUS.
   * Dostarczenie pełnej dokumentacji technicznej oraz instrukcji użytkowania.
5. **Wsparcie powdrożeniowe**:
   * Zapewnienie wsparcia technicznego do dnia 30.06.2026 r.
   * Wsparcie powinno obejmować pomoc w rozwiązywaniu problemów, aktualizacje systemu oraz konsultacje w zakresie dalszej optymalizacji konfiguracji.

**3. Wymagania techniczne**

1. **Zgodność z Active Directory**:
   * Oprogramowanie musi wspierać pełną integrację z AD, umożliwiając centralne zarządzanie użytkownikami, grupami oraz politykami dostępu.
2. **Wysoki poziom bezpieczeństwa**:
   * RADIUS musi zapewniać szyfrowanie przesyłanych danych (np. poprzez zastosowanie protokołu EAP-TLS) oraz wspierać dwuetapowe uwierzytelnianie (2FA).
   * System powinien umożliwiać audyt logów w celu monitorowania aktywności użytkowników.
3. **Skalowalność**:
   * System musi być skalowalny i umożliwiać łatwe rozszerzenie funkcjonalności w przyszłości, wraz z rozwojem infrastruktury IT urzędu.
4. **Wydajność**:
   * Oprogramowanie powinno być zoptymalizowane pod kątem wydajności, umożliwiając obsługę co najmniej 500 równoczesnych połączeń bez zauważalnego spadku wydajności.

**4. Harmonogram realizacji**

1. **Etap 1: Dostawa oprogramowania**
2. **Etap 2: Instalacja i konfiguracja**
3. **Etap 3: Testowanie i uruchomienie**
4. **Etap 4: Szkolenie personelu**

**5. Wymagania dotyczące konfiguracji i polityk autoryzacji**

**5.1. Konfiguracja serwera RADIUS**

1. **Podstawowa konfiguracja serwera**:
   * Serwer RADIUS powinien być zainstalowany na dedykowanym serwerze fizycznym lub wirtualnym, z systemem operacyjnym wspieranym przez dostawcę oprogramowania.
   * Serwer powinien być zabezpieczony za pomocą najnowszych poprawek bezpieczeństwa oraz ograniczony do niezbędnych funkcji i usług.
   * Oprogramowanie RADIUS powinno być skonfigurowane do komunikacji z Active Directory (AD) w celu uwierzytelniania użytkowników.
2. **Konfiguracja połączenia z Active Directory**:
   * Serwer RADIUS musi być skonfigurowany do korzystania z LDAP lub LDAPS (LDAP Secure) w celu komunikacji z Active Directory.
   * Serwer RADIUS powinien mieć zdefiniowane co najmniej jedno konto serwisowe w AD z odpowiednimi uprawnieniami do odczytu danych użytkowników i grup.
   * W przypadku korzystania z LDAPS, certyfikaty SSL/TLS muszą być poprawnie zainstalowane i skonfigurowane, aby zapewnić bezpieczne połączenie.
3. **Uwierzytelnianie wieloskładnikowe (MFA)**:
   * RADIUS musi wspierać uwierzytelnianie wieloskładnikowe (MFA) dla wszystkich użytkowników zdalnych (np. korzystających z VPN).
   * Wdrożone rozwiązanie MFA powinno być zintegrowane z serwerem RADIUS i wspierać popularne metody takie jak aplikacje mobilne (Google Authenticator, Microsoft Authenticator), SMS lub tokeny sprzętowe.
4. **Konfiguracja logów**:
   * Serwer RADIUS powinien być skonfigurowany do generowania szczegółowych logów dotyczących prób uwierzytelniania, autoryzacji i błędów.
   * Logi powinny być automatycznie archiwizowane i przechowywane przez okres co najmniej 12 miesięcy.
   * W celu zapewnienia zgodności z RODO, logi muszą być chronione przed nieautoryzowanym dostępem i szyfrowane, jeśli są przechowywane na zewnętrznych nośnikach.

**5.2. Polityki autoryzacji**

1. **Polityki dostępu dla pracowników**:
   * Użytkownicy wewnętrzni (pracownicy urzędu) muszą być autoryzowani na podstawie członkostwa w odpowiednich grupach Active Directory.
   * Polityki dostępu powinny być oparte na zasadzie minimalnych uprawnień, zapewniając dostęp tylko do zasobów niezbędnych do wykonywania obowiązków służbowych.
   * Dla krytycznych zasobów (np. systemy finansowe) wymagane jest uwierzytelnianie dwuskładnikowe (2FA).
2. **Polityki dostępu dla gości**:
   * Goście uzyskujący dostęp do sieci Wi-Fi urzędu muszą być autoryzowani za pomocą tymczasowych kont użytkowników, które automatycznie wygasają po określonym czasie (np. 24 godziny).
   * Polityki dostępu dla gości powinny zapewniać izolację sieciową, umożliwiając jedynie dostęp do Internetu i zasobów publicznych (np. strony internetowe urzędu).
3. **Polityki dostępu dla zdalnych użytkowników (VPN)**:
   * Użytkownicy łączący się z siecią urzędu za pośrednictwem VPN muszą być autoryzowani za pomocą członkostwa w grupach Active Directory oraz uwierzytelniani wieloskładnikowo (MFA).
   * Dostęp zdalny powinien być ograniczony do zaufanych urządzeń, spełniających określone kryteria bezpieczeństwa (np. zainstalowane aktualizacje, aktywne oprogramowanie antywirusowe).
   * Sesje VPN powinny być automatycznie przerywane po określonym czasie bezczynności (np. 30 minut) oraz po upływie maksymalnego czasu trwania sesji (np. 8 godzin).
4. **Polityki dostępu dla urządzeń sieciowych**:
   * Urządzenia sieciowe, takie jak przełączniki, routery, punkty dostępowe, muszą być autoryzowane przez serwer RADIUS przed uzyskaniem dostępu do sieci wewnętrznej.
   * Polityki dostępu powinny być oparte na adresach MAC urządzeń oraz przypisanych im rolach (np. dostęp do VLANów).
5. **Zarządzanie politykami na poziomie centralnym**:
   * Wszystkie polityki autoryzacji muszą być zarządzane centralnie, z możliwością szybkiej aktualizacji w odpowiedzi na nowe zagrożenia lub zmiany organizacyjne.
   * Zmiany w politykach dostępu muszą być automatycznie dokumentowane i audytowane, aby zapewnić zgodność z wewnętrznymi regulacjami oraz wymaganiami prawnymi.

**5.3. Zabezpieczenia i zgodność z przepisami**

1. **Bezpieczeństwo połączeń RADIUS**:
   * Połączenia między klientami RADIUS (np. punkty dostępowe, VPN) a serwerem RADIUS muszą być zabezpieczone za pomocą kluczy współdzielonych (shared secret) oraz szyfrowane.
   * Należy zapewnić ochronę przed atakami typu brute-force poprzez skonfigurowanie ograniczeń dotyczących liczby nieudanych prób logowania.
2. **Zgodność z przepisami**:
   * Wdrożone rozwiązania muszą być zgodne z obowiązującymi przepisami dotyczącymi ochrony danych osobowych (RODO) oraz bezpieczeństwa IT.
   * Serwer RADIUS musi umożliwiać realizację audytów zgodności, w tym przechowywanie i udostępnianie logów dla celów audytowych.

# Urządzenia Access point- 3 szt.

Minimalne Wymagania Techniczne:

Dostawa obejmuje 3 szt urządzeń typu access point.

W ramach dostawy Wykonawca powinien skonfigurować urządzenia według wytycznych Zamawiającego

|  |  |
| --- | --- |
| Kategoria | Wymagania Minimalne |
| Interfejs sieciowy | Minimum 1 port 2.5 GbE RJ45 |
| Metoda zasilania | Power over Ethernet (PoE+), zgodnie z 802.3at |
| Maksymalne zużycie energii | 22 W |
| Standardy WiFi | 802.11a/b/g/n/ac/ax (WiFi 6/6E) |
| Tryby pracy | tryb pracy jako punkt dostępowy (access point) |
| Przestrzenie antenowe | 2.4 GHz: 2x2 MU-MIMO  5 GHz: 4x4 MU-MIMO  6 GHz: 4x4 MU-MIMO |
| Minimalna prędkość danych | 2.4 GHz: do 573.5 Mbps (BW40)  5 GHz: do 4.8 Gbps (BW160)  6 GHz: do 4.8 Gbps (BW160) |
| Maksymalna liczba klientów | Ponad 600 jednoczesnych połączeń |
| Standardy bezpieczeństwa | WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3) |
| Bezpieczeństwo | Zaawansowane mechanizmy bezpieczeństwa, takie jak ochrona przed atakami typu DoS (Denial of Service) oraz wykrywanie i zapobieganie atakom typu brute force.  Przynajmniej jeden rodzaj uwierzytelniania, RADIUS lub LDAP, zapewniając bezpieczeństwo i kontrolę dostępu do sieci. |
| Certyfikaty | CE, FCC, IC |
| Temperatura pracy | od -30°C do 60°C |
| Wilgotność pracy | od 5% do 95% (bez kondensacji) |
| Interfejs zarządzania | Ethernet, Bluetooth |
| Aplikacja zarządzająca | Możliwość zarządzania za pomocą dedykowanej aplikacji sieciowej  Aplikacja powinna umożliwiać zaawansowane opcje konfiguracji sieciowej, takie jak zarządzanie pasmem, priorytetyzacja ruchu oraz kontrola dostępu do sieci. Ponadto bsługiwać automatyczne aktualizacje oprogramowania, zapewniając tym samym, że urządzenie będzie zawsze wyposażone w najnowsze poprawki bezpieczeństwa i funkcjonalności oraz oferować funkcje monitorowania sieci w czasie rzeczywistym, umożliwiając administratorom natychmiastową reakcję na wszelkie problemy. |
| Obsługa VLAN | 802.1Q |
| Zaawansowane QoS | Ograniczanie prędkości dla użytkowników  Funkcje analizy spektrum, umożliwiając administratorom identyfikację źródeł zakłóceń w paśmie radiowym.  integracja z systemami zarządzania siecią, umożliwiająca scentralizowane zarządzanie wieloma punktami dostępowymi. |
| Izolacja ruchu gości | Sprzęt powinien oferować wsparcie dla sieci gościnnych, umożliwiając tworzenie oddzielnych sieci dla gości z izolacją od sieci wewnętrznej. |
| Możliwość montażu | Montaż na ścianie lub suficie |
| Max. Moc nadawania | 2.4 GHz: 22 dBm  5 GHz: 26 dBm  6 GHz: 26 dBm |
| Zysk anteny | 2.4 GHz: 3.2 dBi  5 GHz: 5.3 dBi  6 GHz: 6 dBi |
| Oprogramowanie | Obsługa do 8 SSID na radio  Mechanizm izolacji ruchu gości  Aktualizacje oprogramowania zarządzane centralnie  Obsługa trybu zerowego oczekiwania DFS (Dynamic Frequency Selection)  Wsparcie dla mesh networking, umożliwiając tworzenie rozszerzalnych i samonaprawiających się sieci bezprzewodowych. |
| Elementy montażowe | Zamawiający wymaga dostarczenia wraz z urządzeniem dedykowanego uchwytu oraz elementów montażowych. |

# Dysk zewnętrzne o pojemności co najmniej 4TB (5 szt.)

**Minimalne wymagania:**

**Przeznaczenie urządzenia**

Urządzenie ma służyć jako zewnętrzny nośnik danych o wysokiej pojemności, dedykowany do przechowywania i transportu dużych ilości danych w trudnych warunkach środowiskowych. Dysk powinien być odporny na wstrząsy, kurz i wodę, a także zapewniać szybki transfer danych przez interfejs USB 3.1.

**Wymagania techniczne**

1. **Pojemność**:
   * Dysk musi mieć pojemność nominalną 4 TB.
2. **Interfejs**:
   * USB 3.2 Gen 1 (kompatybilny wstecz z USB 2.0).
3. **Wytrzymałość i ochrona**:
   * Urządzenie musi być odporne na wodę i kurz zgodnie z normą IP68 (testowany przez 60 minut w zanurzeniu na głębokości 2 metrów).
   * Powinno spełniać wymogi normy wojskowej MIL-STD-810G 516.6 w zakresie odporności na upadki z wysokości 1,5 metra.
   * Konstrukcja trójwarstwowa: silikonowa powłoka ochronna, amortyzująca warstwa buforowa, twarda obudowa z tworzywa sztucznego.
4. **Temperatura pracy**:
   * Zakres temperatury pracy: od 5°C do 50°C.
5. **Zasilanie**:
   * Zasilanie z portu USB
6. **Kompatybilność**:
   * Systemy operacyjne: Windows 7 / 8 / 8.1 / 10 / 11, macOS X 10.6 lub nowszy, Linux Kernel 2.6 lub nowszy.
7. **Dodatkowe funkcje**:
   * Technologia wykrywania wstrząsów, która zatrzymuje działanie dysku w przypadku wykrycia wstrząsu i wznawia je po zakończeniu wibracji.
   * Zintegrowany system zarządzania kablem USB w obudowie urządzenia.
8. **Gwarancja**:
   * Minimum 3-letnia gwarancja producenta.

**Certyfikaty i zgodność**

* Urządzenie musi spełniać normy IP68 oraz MIL-STD-810G 516.6.

# Klucze sprzętowe U2F-30 szt.

**Minimalne wymagania:**

**Przeznaczenie urządzenia**

Urządzenie ma służyć jako bezpieczny klucz do uwierzytelniania użytkowników w systemach informatycznych, zapewniając wieloskładnikowe uwierzytelnianie (MFA) zgodne z najnowszymi standardami bezpieczeństwa. Klucz powinien obsługiwać protokoły FIDO2 oraz U2F, a także być zgodny z szeroką gamą aplikacji i usług online.

Urządzenia zostaną skonfigurowane przez Wykonawcę według wytycznych zamawiającego.

**Wymagania techniczne**

1. **Interfejsy komunikacyjne**:
   * USB 2.0 typu A.
   * Obsługa NFC (Near Field Communication) dla urządzeń mobilnych.
2. **Wymiary i waga**:
   * Wymiary: nie większe niż 18 mm x 45 mm x 3,35 mm.
   * Waga: nie więcej niż 4,5 g.
3. **Funkcje bezpieczeństwa**:
   * Obsługa FIDO2 CTAP1, CTAP2, CTAP2.1 oraz Universal 2nd Factor (U2F).
   * Możliwość przechowywania do 100 wykrywalnych poświadczeń FIDO2.
   * Wsparcie dla kluczy kryptograficznych RSA (do 4096-bitów) oraz ECC (P256, P384).
   * Ochrona przed phishingiem i innymi atakami na tożsamość.
4. **Wytrzymałość**:
   * Odporność na wodę i kurz zgodnie z normą IP68.
   * Odporność na zgniatanie.
5. **Zakres temperatur pracy**:
   * Temperatura pracy: od 0°C do 40°C.
   * Temperatura przechowywania: od -20°C do 85°C.
6. **Zgodność**:
   * Urządzenie musi być zgodne z systemami operacyjnymi takimi jak Windows, macOS, Linux, Android, iOS oraz z popularnymi przeglądarkami internetowymi.
   * Wsparcie dla popularnych usług chmurowych i aplikacji do zarządzania hasłami.

**Certyfikaty i zgodność**

* Urządzenie musi posiadać certyfikaty FIDO U2F, FIDO L1 oraz być zgodne z normą IP68.

# Oprogramowanie do monitorowania infrastruktury informatycznej-1 szt.

Opis minimalnych wymagań technicznych dla kompleksowego rozwiązanie do zarządzania, inwentaryzacji, monitorowania i zapewnienia bezpieczeństwa IT. Oprogramowanie powinno wspierać kluczowe procesy w organizacji oraz stanowić kompleksowe wsparcie dla działu IT.

 Oprogramowanie powinno posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program powinien umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz zapewniać pomoc w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12), dzięki czemu nie powinien być objęty limitem ilości danych; baza danych powinna być rozwiązaniem darmowym, niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wymagać 64-bitowego systemu operacyjnego Windows.

Dane dotyczące działań pracownika na komputerze, takie jak historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych, tj. informacji o stacji roboczej. Powinny one być również grupowane w osobnym, dedykowanym oknie, co powinno umożliwiać, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów – program powinien umożliwiać nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator powinien mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną, np. powinien móc wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów.

Działania administratorów powinny być logowane, co oznacza, że program powinien posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie, w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów powinny być również automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, powinna być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS. Program powinien umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli, co powinno pozwalać na określenie minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad.

Program powinien zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny powinien być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA powinno być możliwe skonfigurowanie okresu, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania powinna być możliwa do pominięcia tylko w lokalnej konsoli serwera.

**MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO)** powinno obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

* wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping;
* wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU);
* wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci;
* wizualizacji urządzeń na mapach z funkcją siatki, która powinna umożliwiać korygowanie pozycji ikon na mapie do najbliższej linii siatki;
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła;
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków, np. schematu rozmieszczenia pomieszczeń w budynku;
* wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze;
* wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie;
* wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie, zarówno w sposób manualny, jak i automatyczny;
* blokowania mapy urządzeń przed przypadkową edycją;
* monitorowania serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych, wraz z możliwością definiowania własnych serwisów, monitorując czas ich odpowiedzi i procent utraconych pakietów.

Program powinien również umożliwiać monitorowanie serwerów pocztowych poprzez:

* monitorowanie czasu logowania do serwisu odbierającego oraz czasu wysyłania poczty;
* monitorowanie stanu systemów i wysyłanie powiadomień (e-mail, SMS i inne) w razie, gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem);
* wykonywanie operacji testowych;
* wysyłanie powiadomień, jeśli serwer pocztowy nie działa.

Dodatkowo, oprogramowanie powinno umożliwiać:

* monitorowanie serwerów WWW i adresów URL;
* cykliczne monitorowanie czasu ładowania strony internetowej, zmian treści na stronie internetowej i statusu protokołu HTTPS;
* obsługę szyfrowania SSL/TLS w powiadomieniach e-mail;
* obsługę urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID;
* obsługę komunikatów syslog i pułapek SNMP oraz ewidencjonowanie odebranych z nich danych.

Monitorowanie routerów i przełączników powinno obejmować:

* monitorowanie zmian stanu interfejsów sieciowych;
* monitorowanie ruchu sieciowego;
* monitorowanie podłączonych stacji roboczych z graficzną prezentacją panelu switcha;
* monitorowanie ruchu generowanego przez podłączone do portów stacje robocze.
* W zakresie monitorowania serwisów Windows, program powinien alarmować, gdy serwis przestanie działać, oraz umożliwiać jego uruchomienie, zatrzymanie lub zrestartowanie.
* wyświetlanie statystyk przy każdym urządzeniu na mapie, takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu;
* monitorowanie stanu maszyn wirtualnych Vmware, wskazując, czy maszyna działa, nie działa, czy jest wstrzymana;
* zarządzanie stanem maszyn wirtualnych Vmware poprzez wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny;
* monitorowanie wydajności systemów Windows, obejmujące obciążenie CPU, pamięci, zajętość dysków oraz transfer sieciowy.

Oprogramowanie powinno zawierać Inteligentne Mapy i Oddziały, które powinny służyć do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz umożliwiać tworzenie dynamicznych map według własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania powinny dotyczyć m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP oraz danych z inwentaryzacji urządzenia.

Program powinien również oferować funkcję kompilatora plików MIB, która powinna umożliwiać dodawanie definicji dla modułów SNMP. Dodatkowo, oprogramowanie powinno umożliwiać nakładanie na urządzenia liczników wydajności WMI oraz SNMP według szablonów oraz definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, takich jak:

* wysyłanie komunikatu pulpitowego,
* wysyłanie wiadomości e-mail,
* wysyłanie SMS,
* wysyłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl,
* wysyłanie wiadomości przez Microsoft Teams oraz Slack,
* uruchomienie programu,
* wysyłanie pułapki SNMP,
* wysyłanie pakietu Wake-On-LAN,
* zatrzymanie/restart usługi Windows,
* wyłączenie/restart komputera.

Alarmy powinny być konfigurowane przez administratora z wykorzystaniem ciągu przyczynowo-skutkowego. Oznacza to, że administrator powinien mieć możliwość wskazania dowolnego zdarzenia z listy, którego wykrycie wzbudzi alarm, oraz dowolnej liczby akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów powinno być konfigurowalne do automatycznego uruchomienia po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie, np. co 5 minut. Możliwość nałożenia ograniczenia czasowego na akcje, np. "nie wykonuj między 8:00-16:00", powinna być dostępna.

Alarmy powinny również pozwalać na priorytetyzację urządzeń oraz grupowanie według ważności i typu urządzenia. Oprogramowanie powinno umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z autoryzacją OAuth 2.0.

Program powinien mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP)

**W ZAKRESIE INWENTARYZACJI** program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Powinien prezentować szczegóły dotyczące sprzętu, takie jak model, procesor, pamięć, płyta główna, napędy, karty itp.
2. Powinien umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Powinien obejmować m.in. zestawienie posiadanych konfiguracji sprzętowych, informacje o wolnym miejscu na dyskach, średnim wykorzystaniu pamięci oraz dane pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Powinien informować o zainstalowanych aplikacjach oraz aktualizacjach Windows, co powinno bezpośrednio umożliwiać audytowanie i weryfikację użytkowania licencji w organizacji.
5. Powinien zbierać informacje o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej, takich jak instalacja/deinstalacja aplikacji, zmiany adresu IP itd.
6. Powinien posiadać możliwość wysyłania powiadomień, np. e-mailem, w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Powinien umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
8. Powinien umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Powinien umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Powinien umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie, wraz z wykrywaniem metadanych plików użytkownika, takich jak obrazy (wymiary obrazka), wideo (długość filmu), audio (długość nagrania), archiwa (liczba plików w środku, rozmiar po wypakowaniu).
11. Powinien umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików, a działania administratorów wykonywane w tej funkcji powinny być logowane.

Moduł inwentaryzacji zasobów powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i oprogramowania, w tym:

* przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatyczne aktualizowanie zgromadzonych informacji;
* przydzielanie dostępu administratorów do zasobów na podstawie praw do oddziałów;
* tworzenie powiązań między zasobami a urządzeniami;
* tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory) oraz wskazywanie osób odpowiedzialnych;
* wskazywanie osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy;
* definiowanie własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania powinna istnieć możliwość dodawania dodatkowych informacji, takich jak numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej lub własny komentarz;
* określenie atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów;
* określenie atrybutów dodatkowych tylko dla wybranych typów zasobów.
* masową edycję atrybutów zasobów;
* definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie;
* import danych z zewnętrznego źródła (.CSV);
* przechowywanie dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), takich jak skan faktury zakupu, gwarancji, dowolnego dokumentu itp.;
* tworzenie powiązań między zasobami a dokumentami w relacji 1:N
* oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.;
* ewidencjonowanie czynności wykonywanych na zasobach, takich jak aktualizacja, naprawa w serwisie, konserwacja itp., wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności;
* generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania;
* przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów, wraz z konfigurowalną sekcją zawierającą dane i logo organizacji;
* konfigurację stylu automatycznego numerowania dodawanych zasobów według zdefiniowanego wzorca;
* konfigurację stylu automatycznego numerowania dodawanych dokumentów i protokołów według zdefiniowanego wzorca;
* archiwizację i porównywanie audytów zasobów;
* tworzenie kodów kreskowych dla zasobów;
* drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy;
* inwentaryzację zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android, która powinna umożliwiać wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych oraz drukowanie etykiet;
* możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android;
* inwentaryzację stacji roboczych niepodłączonych do sieci (bez instalacji Agenta) poprzez manualne wykonanie skanów inwentaryzacji offline;
* definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji, w tym:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych oraz skanowanie archiwów ZIP;
2. Dostarczanie informacji o aplikacjach używanych w organizacji;
3. Tworzenie własnych wzorców aplikacji;
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.;
5. Dostarczanie informacji o komputerach, na których aplikacja została wykryta;
6. Zarządzanie posiadanymi licencjami;
7. Wskazywanie osób odpowiedzialnych za licencję;
8. Wskazywanie użytkowników licencji.
9. Tworzenie powiązań między licencjami a dokumentami w relacji 1:N
10. Konfigurowalne scenariusze zarządzania licencjami, które powinny obejmować: przypisywanie licencji do użytkownika, przypisywanie licencji do wielu komputerów tego samego użytkownika, przypisywanie licencji według numerów seryjnych oraz przypisywanie licencji według różnych wersji aplikacji na jednym urządzeniu.
11. Przeprowadzanie audytów legalności oprogramowania oraz powiadamianie tylko w przypadku przekroczenia liczby posiadanych licencji, z możliwością wykonania aktualnych raportów audytowych w każdej chwili.
12. Zarządzanie posiadanymi licencjami poprzez generowanie raportów zgodności licencji.
13. Przypisywanie do programów numerów seryjnych, wartości itp., z możliwością filtrowania elementów per oddział w oknach audytowych.

**W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW** program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez:

* monitorowanie faktycznego czasu aktywności, w tym dokładnego czasu pracy z godziną rozpoczęcia i zakończenia pracy;
* monitorowanie procesów, gdzie każdy proces powinien mieć określony całkowity czas działania oraz czas aktywności użytkownika, wraz z informacją o uruchomieniu na podwyższonych uprawnieniach;
* monitorowanie rzeczywistego użytkowania programów, w tym procentowej wartości wykorzystania aplikacji, obrazującej czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona, wraz z informacją, na którym komputerze wykonano daną aktywność;
* zbieranie informacji o edytowanych przez użytkownika dokumentach;
* rejestrowanie historii pracy za pomocą cyklicznych zrzutów ekranowych;
* monitorowanie listy odwiedzanych stron WWW, w tym tytułów, adresów, liczby i czasu wizyt;
* monitorowanie transferu sieciowego użytkowników, w tym ruchu lokalnego i transferu internetowego generowanego przez użytkownika;
* monitorowanie wydruków, obejmujące informacje o dacie wydruku, wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany) oraz zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), z możliwością "grupowania" drukarek poprzez identyfikację drukarek oraz monitorowanie kosztów wydruków;
* monitorowanie nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Dodatkowo, program powinien umożliwiać:

* wykrywanie podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy;
* zdefiniowanie czasu (min. 15 minut), gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury;
* wyszczególnienie podejrzanej aktywności w raportach;
* generowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności;
* automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności;
* blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen powinny być tworzone dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami;
* integrację list stron w formie plików .TXT z dowolnego adresu zewnętrznego, np. CERT;
* korzystanie z wbudowanej listy stron sklasyfikowanych jako zagrożenia;
* automatyczne odświeżanie list stron zintegrowanych z adresów zewnętrznych;
* blokowanie ruchu na wskazanych portach TCP/IP;
* blokowanie pobierania przez przeglądarki internetowe plików z określonym rozszerzeniem;
* prowadzenie rejestru naruszeń blokad;
* wysyłanie powiadomień, gdy użytkownik odwiedzi stronę z określonej grupy domen, pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internecie, wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady;
* przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu, który może być dołączony np. do akt pracownika;
* definiowanie godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone;
* generowanie raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie;
* blokowanie uruchamiania aplikacji według maski nazwy oraz lokalizacji pliku, z regułami w postaci listy blokowanych plików lub lokalizacji tworzonymi dla użytkownika lub grupy użytkowników, które mogą być kopiowane pomiędzy grupami lub kontami.

Program powinien zawierać funkcje Grupy użytkowników oraz Grupy Inteligentne, które powinny służyć do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

**Program powinien umożliwiać realizację zdalnej pomocy użytkownikom**. W ramach kontroli stacji użytkownika powinien być dostępny podgląd pulpitu użytkownika oraz możliwość przejęcia nad nim kontroli, z możliwością zdefiniowania, czy użytkownik powinien zostać zapytany o zgodę na połączenie oraz opcją odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego zarówno użytkownik, jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy i klawiatury dla użytkownika. Funkcja zdalnego dostępu powinna umożliwiać równoczesne podłączenie do tego samego komputera kilku administratorom.

Moduł powinien zawierać bazę zgłoszeń, która powinna umożliwiać użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, którzy otrzymują automatyczne powiadomienie o przypisanym im problemie. Oprogramowanie powinno umożliwiać integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł powinien również umożliwiać przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawierać dokumenty prawne dotyczące ochrony sygnalistów, w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę.

Program powinien umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również wymianę informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System powinien umożliwiać użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.

Moduł ten powinien zawierać komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat powinien pozwalać na:

* zarządzanie dostępem do czatu na 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej;
* prowadzenie rozmów między „zwykłymi” użytkownikami;
* przesyłanie plików między rozmówcami w trybie online;
* tworzenie pokojów tematycznych oraz rozmów grupowych;
* oznaczanie kontaktów jako „ulubionych” na liście kontaktów;
* uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW helpdesku;
* wyświetlanie w trybie jasnym lub ciemnym.

Moduł powinien zawierać również bazę wiedzy, która ma pomóc użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy, z możliwością nadawania artykułom jednego z 3 statusów (opublikowany, wewnętrzny, szkic). Program powinien umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik powinien mieć możliwość przeglądania historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta, a administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów.

Dostęp do systemu zgłoszeń oraz bazy wiedzy powinien być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, który powinien być wyświetlany w trybie jasnym lub ciemnym.

Moduł zdalnej pomocy powinien również umożliwiać uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Moduł pomocy zdalnej powinien umożliwiać również:

* pobieranie listy użytkowników z Active Directory;
* wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym;
* zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont;
* zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń;
* zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń;
* zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy;
* tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO;
* automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników;
* definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji;
* przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii;
* procesowanie zgłoszeń użytkowników z wiadomości e-mail;
* eksportowanie listy zgłoszeń do plików CSV i XLSX;
* integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0;
* tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń;
* wykonywanie operacji na wielu zgłoszeniach równocześnie;
* dołączanie załączników do zgłoszeń;
* rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy;
* szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników;
* wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia;
* zrzuty ekranowe (podgląd pulpitu);
* zdalną modyfikację rejestrów;
* dystrybucję oprogramowania przez Agenty;
* definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami;
* przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników;
* dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI);
* kolejkowanie zadań dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji;
* możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu;
* możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy;
* planowanie nieobecności pracowników helpdesk;
* obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem;
* generowanie raportów obsługi helpdesk;
* zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie/edycja konta lokalnego użytkownika systemu);
* zarządzanie procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami);
* wymianę plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

 Oprogramowanie powinno obejmować poniższe elementy z sieci lokalnej Zamawiającego:

* (1x) Urządzenie klasy UTM (dostarczane w ramach tego postępowania)
* (1x) Firewall Sieciowy (dostarczane w ramach tego postępowania)
* (3x) Urządzenia Access point (dostarczane w ramach tego postępowania)
* (1x) Macierz dyskowa (dostarczana w ramach tego postępowania)
* (5x) NAS oraz dostarczane w ramach tego postępowania
* (3x) Przełączniki zarządzalne firmy HP
* (2x) Przełączniki zarządzalne firmy Ubiquiti
* (5x) Przełączniki zarządzalne dostarczane w ramach tego postępowania
* (4x) Serwery Windows oraz dostarczane w ramach tego postępowania
* (1x) Serwery Linux
* (4x) Serwer wirtualizacji Proxmox oraz dostarczane w ramach tego postępowania
* (60x) stacji roboczych Windows 10 i 11
* (1x) Rejestrator wideo
* (20x) Drukarki

W ramach dostawy powyższego oprogramowania Zamawiający powinien otrzymać:

- licencję wieczystą na oprogramowanie

- wsparcie serwisowe (aktualizacje i pomoc techniczną) do dnia 30.06.2026 r.

- Możliwość przedłużenia wsparcia serwisowego o 12 miesięcy

- Możliwość dokupienia modułów (rozszerzenia funkcjonalności) oraz zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie.

# 18.Switch zarządzalny, co najmniej 48 portów, typ portów Gigabit Ethernet (10/100/1000) (3 szt.)

Wymagane minimalne parametry techniczne

|  |  |
| --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne |
| Typ | Przełącznik sieciowy Ethernet Smart Management rack 1Gbit. |
| Porty | a) Minimum 48 porty 1G RJ45 10/100/1000BASE-T      b) Minimum 4 porty SFP+ z możliwością pracy 1G/10G  Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX |
| Parametry fizyczne | Wysokość maksymalnie 1U, montowany w szafie typu rack 19’’ |
| Pamięć | Co najmniej 512 MB SDRAM  Co najmniej 256 MB pamięci flash  Bufor pakietów co najmniej 1.5 MB |
| Procesor | min 1-rdzeniowy, o taktowaniu min 800MHz |
| Wielkość tablicy adresów MAC | Co najmniej 16000 |
| Ilość obsługiwanych sieci VLAN | Co najmniej 256 |
| Wydajność | • Przepustowość przełączania: min. 176  Gbit/s      • Przełączanie dla pakietów: min. 130.95 Mpps.      • Opóźnienie:  < 4.5 uSec dla 100 Mb  < 2.2 uSec dla 1000 Mb  <1.2 uSec dla 10 Gbps |
| Obsługa ramek Jumbo | O wielkości co najmniej 9216 bajtów |
| Funkcjonalność urządzenia | ◦ obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad),  ◦ wsparcie da LLDP oraz LLDP-MED  ◦ obsługa protokołu SNTP,  ◦ Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s)  ◦ Minimum 256 obsługiwanych sieci VLAN  ◦ Minimum 50 możliwych do utworzenia list ACL,  ◦ CoS zgodna z 802.1p  ◦ Voice VLAN  ◦ Minimum 509 wpisów ARP  ◦ Możliwość przechowywania dwóch obrazów oprogramowania: aktywny I zapasowy  ◦ Port Security  ◦ DHCP Snooping  ◦ Klient Radius  ◦ Port mirroring,  ◦ DHCP Relay,  ◦ DoS Protection,  ◦ ARP Attack Protection,  ◦ Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu |
| Zasilanie | Zasilacz 230V AC wbudowany |
| Temperatura pracy | 0°C do 40°C |
| Maksymalny pobór mocy | 36.9 W |
| Wentylacja | bezwentylatorowy |
| Zarządzanie | WWW (GUI), SNMP Manager, cloud-based web portal |
| Akcesoria | Razem z przełącznikiem należy dostarczyć:  1. Kabel  2. Wkładkę |
| Gwarancja | Produkty są objęte 90-dniowym całodobowym telefonicznym wsparciem technicznym. Przez pozostały okres  gwarancji, dostępne będzie tylko wsparcie techniczne za pomocą czatu. Ograniczona gwarancja dożywotnia, obowiązuje tak długo, jak produkt jest używany przez pierwszego właściciela, dodatkowo jest ograniczona do  pięciu (5) lat od daty wycofania produktu ze sprzedaży.  Dostęp do wersji oprogramowania przez cały okres posiadania dotyczy wszystkich ogólnodostępnych wersji oprogramowania / systemów operacyjnych dla wymienionych produktów,  gdy i jeśli są dostępne, przez cały okres posiadania produktu przez klienta. |
| Dokumenty | Wykonawca winien przedłożyć dokumenty:      1) Deklaracja zgodności CE oferowanego urządzenia – certyfikat potwierdzony za zgodność z oryginałem,      2) Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia. |

# 19.Wdrożenie( dostawa , instalacja i rozmieszczenie) oprogramowania typu SIEM do analizy logów w czasie rzeczywistym i powiadamiania o wykrytych nieprawidłowościach.( 1 szt.)

1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:
   1. System operacyjny powinien być na licencji Open Source.
   2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna w środowisku Proxmox
   3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source
   4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 2TB.
   5. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
   6. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
   7. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.
   8. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.
   9. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
   10. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:
   1. Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualnej.
   2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.
   3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
   4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
   5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:

* (1x) Urządzenie klasy UTM (dostarczane w ramach tego postępowania)
* (1x) Firewall Sieciowy (dostarczane w ramach tego postępowania)
* (3x) Urządzenia Access point (dostarczane w ramach tego postępowania)
* (1x) Macierz dyskowa (dostarczana w ramach tego postępowania)
* (5x) NAS oraz  dostarczane w ramach tego postępowania
* (3x) Przełączniki zarządzalne firmy **HP**
* (2x) Przełączniki zarządzalne firmy **Ubiquiti**
* (5x) Przełączniki zarządzalne dostarczane w ramach tego postępowania
* (4x) Serwery Windows oraz dostarczane w ramach tego postępowania
* (1x) Serwery Linux
* (4x) Serwer wirtualizacji Proxmox oraz dostarczane w ramach tego postępowania
* (60x) stacji roboczych Windows 10 i 11
* (1x) Rejestrator wideo
* (20x) Drukarki
  1. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
  2. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
  3. Wykonanie całkowitej rekonfiguracji aplikacji do monitorowania infrastruktury informatycznej w celu umożliwienia interakcji między rozwiązaniami, która umożliwi przesyłanie i analizę logów z wyżej wymienionego rozwiązania. Rekonfiguracja ma umożliwić pobieranie logów takich jak:
* Aktywność Administratorów w konsoli centralnego zarządzania, z klasyfikacją wykonanych czynności;
* Listę zdarzeń co do których aplikacja ogłasza alarm, z klasyfikacją na typ zdarzenia, istotność oraz źródło problemu;
  1. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
  2. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
  3. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
  4. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.

1. Gwarancja i asysta techniczna:
   1. Zamawiający wymaga aby Wykonawca od momentu wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu do dnia 30.06.2026 r.
   2. Zamawiający wymaga aby Wykonawca od momentu wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów do dnia 30.06.2026 r.
   3. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
   4. Zamawiający akceptuje fakt, ze każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.