**Załącznik nr 10 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem niniejszego zamówienia jest realizacja usług oraz dostawa sprzętów teleinformatycznych zgodnie z założeniami projektowymi Zamawiającego zawartymi w projekcie grantowym Cyberbezpieczny Samorząd, w tym:

**Część 1:**

* dostawa serwera dla Urzędu Gminy w Purdzie;
* dostawa systemu do przechowywania kopii zapasowych dla Urzędu Gminy w Purdzie;
* dostawa systemu kontroli dostępu do sieci lokalnej wraz z dostawą urządzeń dostępowych.

**Część 2:**

* dostawa agregatu prądotwórczego dla Urzędu Gminy w Purdzie.

**CZĘŚĆ I:**

**ROZDZIAŁ 1 - DOSTAWA SERWERA DLA URZĘDU GMINY W PURDZIE**

Zamawiający wymaga dostawy serwera spełniającego poniższe wymagania:

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| Obudowa  | Obudowa Rack o wysokości max. 2U umożliwiającą instalację min. 12 dysków 3,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  |
| Płyta główna  | Płyta główna z możliwością zainstalowania 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 maksymalnie 8-rdzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 196 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. Dla oferowanego serwera |
| RAM  | Min. 256GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.  |
| Zabezpieczenia pamięci RAM  | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) |
| Gniazda PCIe  | minimum dwa sloty PCIe x8 oraz cztery sloty PCIe x16 generacji 4 w tym dwa pełnej wysokości. |
| Interfejsy sieciowe/FC/SAS  | Cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  nie zajmujące slotów PCIe. Możliwość instalacji wymiennie modułów udostępniających: - dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT- dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+- dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28- cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ - cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.Dodatkowo zainstalowane:- jedna karta dwuportowa 25Gb Ethernet ze złączami SFP28 |
| Dyski twarde  | Zainstalowane 7 x 1.92TB SSD SATA skonfigurowane fabrycznie w RAID 5.Zainstalowane dwa dyski hot-swap M.2 NVMe o pojemności min. 480GB skonfigurowane w RAID 1.  |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| Wbudowane porty  | min. port USB 2.0 oraz port USB 3.0, port VGA. |
| Video  | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900  |
| Wentylatory  | Redundantne Hot-Plug  |
| Zasilacze  | Min. dwa zasilacze Hot-Plug min. 1100W Titanium  |
|  Bezpieczeństwo  | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serweraMożliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.Możliwość integracji z RSA SecurIDWbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. |
| Karta Zarządzania  | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: * zdalny dostęp do graficznego interfejsu Web karty zarządzającej
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika
* możliwość podmontowania zdalnych wirtualnych napędów
* wirtualną konsolę z dostępem do myszy, klawiatury
* wsparcie dla IPv6
* wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
* integracja z Active Directory
* możliwość obsługi przez ośmiu administratorów jednocześnie
* Wsparcie dla automatycznej rejestracji DNS
* wsparcie dla LLDP
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
* możliwość podłączenia lokalnego poprzez złącze RS-232.
* możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.
* Monitorowanie zużycia dysków SSD
* możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
* Automatyczne zgłaszanie alertów do centrum serwisowego producenta
* Automatyczne update firmware dla wszystkich komponentów serwera
* Możliwość przywrócenia poprzednich wersji firmware
* Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
* Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
* Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.
* Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera
* Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.

Możliwość rozszerzenia funkcjonalności karty o:* możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych
* kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania
* Automatyczne odświeżanie certyfikatów SSL
* możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej
* możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień
* możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera
* możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer
* możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe
* monitorowanie przepływu powietrza na bieżąco
 |
| Oprogramowanie do zarządzania |  Możliwość zainstalowania oprogrmowania producenta serwera do zarządznia, spełniające poniższe wymagania: * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
* integracja z Active Directory
* Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
* Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
* Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
* Szczegółowy opis wykrytych systemów oraz ich komponentów
* Możliwość eksportu raportu do CSV, HTML, XLS, PDF
* Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu.
* Grupowanie urządzeń w oparciu o kryteria użytkownika
* Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
* Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
* Szybki podgląd stanu środowiska
* Podsumowanie stanu dla każdego urządzenia
* Szczegółowy status urządzenia/elementu/komponentu
* Generowanie alertów przy zmianie stanu urządzenia.
* Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
* Integracja z service desk producenta dostarczonej platformy sprzętowej
* Możliwość przejęcia zdalnego pulpitu
* Możliwość podmontowania wirtualnego napędu
* Kreator umożliwiający dostosowanie akcji dla wybranych alertów
* Możliwość importu plików MIB
* Przesyłanie alertów „as-is” do innych konsol firm trzecich
* Możliwość definiowania ról administratorów
* Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
* Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
* Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
* Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
* Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
* Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności.
* Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu o profile
* Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
* Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
* Zdalne uruchamianie diagnostyki serwera.
* Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarzadzającym.
* Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
 |
| System Operacyjny | Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego klasy Microsoft Windows Serwer Standard w najnowszej wersji oferowanej przez producenta na dzień składania ofert wraz z 60 licencjami dostępowymi umożliwiającymi korzystanie przez 60 użytkowników zapewniającego możliwość pobierania aktualizacji w okresie 5 lat po okresie wsparcia podstawowego oraz możliwości uruchomienia 4 maszyn wirtualnych lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.Warunki równoważności dla dostawy oprogramowania klasy Microsoft Windows Serwer Standard:1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i czterech wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.2) Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.3) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny.4) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 5) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.7) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.8) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.9) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.10) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;11) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.12) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.13) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.14) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.15) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.18) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).19) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.20) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).21) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.22) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.23) O ile to konieczne ze względu na licencjonowanie producenta oferowanego serwerowego systemu operacyjnego Zamawiający wymaga dostarczenia licencji dostępowych dla 60 użytkowników. |
| Certyfikaty  | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.  |
| Normy Środowiskowe  | Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Rozporządzenia nr 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera.  |
| Warunki gwarancji  | Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365  następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej  (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowychZamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.  |
| 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.  |

**ROZDZIAŁ 2 - DOSTAWA SYSTEMU DO PRZECHOWYWANIA KOPII ZAPASOWYCH DLA URZĘDU GMINY
W PURDZIE**

Zamawiający wymaga dostawy systemu do przechowywania kopii zapasowych dla Urzędu Gminy
w Purdzie.

|  |  |
| --- | --- |
| Typ urządzenia | Serwer NAS |
| Obudowa | Rack |
| Procesor  | Czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz) |
| Sprzętowy mechanizm szyfrowania  | Tak (AES-NI) |
| Pamięć RAM | min. 16 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 32 GB |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband |
| Dyski  | Urządzenie główne musi być wyposażone w 12 dysków twardych SATA 3.5”- znajdujące się na liście kompatybilności producenta o pojemności min. 6TB każdy. Dyski muszą być wykonane w technologii CMR, cache min. 256MB, transfer min. 202 MB/s. Średni czas do awarii (MTTF) musi wynosić min. 1 mln godzin.Możliwość przeprowadzania aktualizacji oprogramowania sprzętowego dysku bezpośrednio na urządzeniu NAS, co umożliwia dyskom korzystanie z najnowszych poprawek bez konieczności ich wyjmowania. |
| Porty zewnętrzne  | Minimum:* 2 porty USB 3.2.1
* 1 gniazdo rozszerzenia
 |
| Porty sieciowe | Minimum:* 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
* 1 port 10GbE RJ45
* Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8
 |
| Funkcja Wake on LAN/WAN | Tak |
| Gniazdo rozszerzeń PCIe 3.0 | Min. 1x 4-liniowe gniazdo x8 Gen. 3 |
| Wentylator obudowy | Min. 3 wentylatory 60 mm x 60 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:
	+ 200 TB (wymagana pamięć 32 GB)
	+ 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 SMB/NFS/AFP/FTP: 2 000
 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| Wirtualizacja | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack® |
| Usługa katalogowa | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń. |
| Bezpieczeństwo | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczneblokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| Obsługiwane przeglądarki | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 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 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.
 |
| Konserwacja | * Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
 |
| Gwarancja | Wykonawca udzieli gwarancji:* min. 3 lata na urządzenie główne
* 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack
 |

**ROZDZIAŁ 3 - DOSTAWA SYSTEMU KONTROLI DOSTĘPU DO SIECI LOKALNEJ WRAZ Z DOSTAWĄ URZĄDZEŃ DOSTĘPOWYCH**

**Podstawowa funkcjonalność systemu NAC:**

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
	* VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
	* Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
	* serwera RADIUS dla infrastruktury sieciowej,
	* serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
	* serwera SYSLOG,
	* serwera TACACS+,
	* serwera Monitoringu,
	* serwera DHCP,
	* serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
	* serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
	* Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
	* Czy włączony jest firewall
	* Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
	* Czy jest włączone szyfrowanie dysku systemowego
	* Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
	* Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
	* Czy w systemie są uruchomione procesy wskazane przez administratora
	* Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
	* Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
		+ Wartości klucza rejestru
		+ Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
	* Microsoft Windows
	* Mac OS
	* iOS
	* Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

**Mechanizmy uwierzytelniania**

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
	* MAC,
	* PAP/ASCII,
	* CHAP,
	* SNMP,
	* 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
	* Tożsamość/Urządzenie końcowe,
	* Grupa tożsamości/urządzeń końcowych,
	* Parametry urządzeń końcowych, min: system operacyjny, wersja,
	* Atrybuty Active Directory,
	* Jednostka organizacyjna tożsamości/urządzeń końcowych,
	* Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
	* Grupy urządzeń sieciowych,
	* Porty urządzeń sieciowych,
	* Grupy portów urządzeń sieciowych,
	* Jednostka organizacyjna portów,
	* Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
	* Data, czas ważności polityki,
	* Wewnętrzny Captive Portal,
	* Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

**Obsługa serwerów certyfikatów CA**

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

**Obsługa serwerów DHCP**

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
	* Uruchamianie usługi dla wybranych podsieci,
	* Przypisanie ustalonego adresu IP dla adresu MAC.
	* Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
	* Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
	* Możliwość określania braku dostępu dla wybranych adresów MAC,
	* Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
	* Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
	* Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
	* Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
	* Dokonywanie zmian bez konieczności wyłączania usług.

**Obsługa serwerów TACACS+**

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

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

**Raportowanie i monitoring**

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
	* Logowania, wylogowania z system w tym błędne logowania
	* Logowania do sieci 802.1X

**Alarmy**

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

**Wymagania dotyczące wdrożenia i harmonogram ramowy:**

* Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
* Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
* Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).
* Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
* Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) i urządzeń sieciowych (switchy) posiadanych przez zamawiającego z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
* Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych zamawiającego (komputerach, telefonach voip, drukarkach sieciowych itp.)
* Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
* Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla 1 osoby po 6h dziennie.
* Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

**Szkolenia/warsztaty:**

* Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC
* Warsztaty zostaną przeprowadzone dla 1 osoby i będą uwzględniać informacje z zakresu wdrożonego systemu NAC
* Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC
* Warsztaty odbędą się w formie zdalnej.
* Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
* Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym

**Licencja wsparcia technicznego producenta oprogramowania:**

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 12 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:

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

**Wymagania dla urządzeń dostępowych**

Zamawiający wymaga dostawy urządzeń dostępowych – przełączników sieciowych w ilości 2 szt.:

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa parametru | Wymagane parametry |
| 1 | Obudowa | Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19”Maksymalne wymiary:Szerokość – 44,5 cm Głębokość – 33 cmWysokość – 4,5 cm. Waga do 5 kg |
| 2 | Interfejsy 1Gb | Minimum 48 gigabitowe interfejsy PoE RJ-45 100/1000 Mbps, 2 interfejsy PoE 100M/1G/2.5G/5G/10G Ethernet (RJ-45)4 interfejsy 1G SFP/10G SFP+Port konsoli USB-C |
| 3 | Wydajność | * Potencjał przełączania nie mniejszy niż 216 Gbps
* Prędkość przełączania nie mniejsza niż 161 Mbps
* Bufor pakietu nie mniejszy niż 2 Mbyte
* Tabela adresów MAC nie mniejsza niż 32K
* Jumbo frame (byte) – 9K
* Flash nie mniej 64 MB
* RAM nie mniej niż 1GB
* L3 forwarding table - Max. 1 K IPv4 entries; Max. 512 IPv6 entries
* Routing table – 64
* Budżet PoE – 600W
* Obsługa EEE 802.3bt (PoE++, 60 W)
 |
| 4 | Tryby pracy | * Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia
 |
| 5 | Zgodność ze standardami | • IEEE 802.3z 1000BASE-X• IEEE 802.3ab 1000BASE-T Ethernet• IEEE 802.3an 10G BASE-T Ethernet• IEEE 802.3ae 10 Gbit/s Ethernet over fiber• IEEE 802.3az EEE • IEEE 802.3x flow control • IEEE 802.1AB LLDP/LLDP-MED• IEEE 802.1Q VLAN tagging • IEEE 802.1p Class of Service (CoS) prioritization• IEEE 802.1X port authentication• IEEE 802.3af PoE• IEEE 802.3at PoE plus• IEEE 802.3bt (60 W) PoE over 4 pair |
| 6 | Odporność i dostępność | • IEEE 802.1D Spanning Tree Protocol (STP)• IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)• IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) • Static port trunking • IEEE 802.3ad LACP • Loop guard (with broadcast packet detection mechanism) • Root guard • BPDU guard • ErrDisable recovery • Dual configuration files • Dual images • ZULD • Flex link • Physical stacking |
| 7 | Kontrola ruchu | • 802.1Q static VLANs/dynamic VLANs: 4 K/4 K • Port-based VLAN • VLAN isolation • Vendor ID based VLAN • Protocol-based VLAN • IP subnet-based VLAN • MAC-based VLAN • Private VLAN • Voice VLAN• Independent VLAN Learning (IVL) • VLAN Translation • VLAN trunking • VLAN mapping • IEEE 802.1AD VLAN stacking (QinQ) • VLAN ingress filtering • LACP algorithm of source/ destination IP or MAC • GVRP • L2PT |
| 8 | Bezpieczeństwo | • Port security • Layer 2 MAC filtering • Layer 3 IP filtering • Layer 4 TCP/UDP socket filtering • Static MAC forwarding • Multiple RADIUS servers• Multiple TACACS+ servers • 802.1x VLAN and 802.1p assignment by RADIUS • Login authentication by RADIUS • Login authentication by TACACS+ • TACACS+ accounting • RADIUS accounting • Authorization on RADIUS • Compound authentication • Authorization on TACACS+ • SSH v2 • SSL • MAC freeze • IP source guard (IPv4/IPv6) • DHCP snooping • DHCP Server Guard • ARP inspection • ARP freeze • Anti-ARP scan • Static IP-MAC-Port binding • Policy-based security filtering • Port isolation • MAC search • Guest VLAN • ACL packet filtering (IPv4/IPv6) • CPU protection • Interface related trap enable/disable (by port) • MAC-based authentication per VLAN • BPDU transparency • WoL/WoL Relay• PPPoE relay agent/option82 |
| 9 | QoS | • No. of hardware queues per port (Standalone/stacking): 8/6 • Storm control and event log: Broadcast, multicast, unknown unicast (DLF) • Port-based rate limiting (ingress/ egress) • Rate limiting per IP/TCP/UDP per port • Policy-based rate limiting • 802.3x flow control • 802.1p Class of Service (SPQ, WFQ, WRR, hybrid-SPQ combination capable) • DiffServ (DSCP) • Storm Control: Broadcast/Unknown Multicast/Unknown Unicast (DLF) |
| 10 | Layer 2 Multicast | • L2 multicast • IGMP snooping (v1, v2, v3) • IGMP snooping fast leave • IGMP snooping immediate leave • Configurable IGMP snooping timer and priority • IGMP snooping statistics • IGMP throttling • IGMP filtering • IGMP proxy mode & snooping mode selection • Multicast load balance over trunking port • Static mulitcast • MVR support • MLD snooping (MLD v1/v2) |
| 11 | Routing | • Static route • IP port moving • DHCP relay |
| 12 | Zarządzanie  | • SNMP v1, v2c, v3 • SNMP trap group • RMON (1, 2, 3, 9) • ICMP echo/echo reply • Syslog • IEEE 802.1AB LLDP/LLDP-MED • Custom default • Syslog (IPv4/IPv6) • Display port utilization |
| 13 | Zarządzanie IPv6  | • IPv6 over Ethernet (RFC 2464) • IPv6 addressing architecture (RFC 4291) • Dual stack (RFC 4213) • ICMPv6 (RFC 4443) • Path MTU (RFC 1981) • Minimum path MTU size of 1280 (RFC 5095) • Encapsulation for maximum PMTU of 1500 • Neighbor discovery (RFC 4861) • DHCPv6 snooping • IPv6 binding- static/dynamic • Extend Radius server • DHCPv6 relay • Default DHCP client mode |
| 14 | Zarządzanie urządzeniem | • Standalone management by Web interface • Cloud management • Networked AV mode by Web Interface • Intuitive Cloud connection status • Management through Console, Telnet, SNMP • Remote firmware upgrade by FTP/ Web/TFTP • Configuration saving and retrieving • Multiple logins supported • Configure clone • Custom default Configuration • Multilevel CLI • CLI (Cisco-like) • DHCP server • DHCP relay per VLAN • DHCP client IPv4/IPv6 • DHCP client option 60 • DHCP option 82 • Daylight saving • DHCP relay MAC proxy • Auto PD Recovery • NTP supports IPv4/IPv6 • Port mirroring• Policy-based mirroring • Mirror CPU• VLAN-based mirroring • USB-C out-of-band console port • Auto PD Recovery • LLDP power via MDI • sFlow • Fiber Module Rescue• Scheduled PoE• PoE default consumption mode• Continuous PoE |
| 15 | MIB | • RFC 1066 TCP/IP-based MIB • RFC 1213, 1157 SNMPv2c/v3 MIB • RFC 1493, 4188 bridge MIB • RFC 1643 Ethernet MIB • RFC 1757 RMON group 1, 2, 3, 9 • RFC 2011, 2012, 2013 SNMPv2 MIB • RFC 2233 SMIv2 MIB • RFC 2358 Ethernet-like MIB • RFC 2674 bridge MIB extension • RFC 2819, 2925 remote management MIB • RFC 3621 power Ethernet MIB • RFC 4022 management information base for transmission control protocol • RFC 4113 management information base for user datagram protocol • RFC 4292 IP forwarding table MIB • RFC 4293 Management Information Base (MIB) for IP • Cable diagnostic MIB |
| 16 | Zakres temperaturowy pracy | -20°C do 50°C |
| 17 | Zasilanie | Maksymalna moc pobierana przez urządzenie nie może przekraczać 755. |
| 18 | Ochrona przed wyładowaniami elektrostatycznymi/przepięciami | Zabezpieczenie przeciwprzepięciowe portu Ethernet – 2KVOchrona zasilacza Linia-GND – 2KVOchrona zasilacza Linia-Linia – 1KVOchrona ESD portu Ethernet (powietrze/kontakt) - 8 KV/6 KV |
| 19 | Rozpraszanie ciepła (BTU/godz.) | 2571.52 |
| 20 | Hałas akustyczny przy 25°C (min./maks., dBA) | 25.21/50.23 |
| 21 | MTBF (hr) | Parametr te nie powinien być niższy niż 214,388 |
| 22 | Gwarancja | Urządzenie powinno posiadać ograniczoną dożywotnią gwarancję producenta |
| 23 | Serwis | W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat. |
| 24 | Wymagane Certyfikaty | Bezpieczeństwo• LVD • BSMI EMC • FCC Part 15 (Class A) • CE EMC (Class A) • BSMI EMC RoHS • Level A |
| 25 | Pozostałe | Sprzęt musi być fabrycznie nowy i pochodzić z polskiego kanału dystrybucji |

**CZĘŚĆ II:**

**ROZDZIAŁ 1 - DOSTAWA AGREGATU PRĄDOTWÓRCZEGO DLA URZĘDU GMINY W PURDZIE**

Zamawiający wymaga, aby oferowany agregat prądotwórczy został zaprojektowany, wykonany i dostarczony zgodnie z aktualnie obowiązującymi przepisami prawa oraz uznanymi normami technicznymi, mającymi zastosowanie do tego typu urządzeń. W szczególności urządzenie musi spełniać wymagania określone w następujących aktach prawnych oraz normach:

* Dyrektywa 2006/42/WE (Dyrektywa Maszynowa) – dotycząca bezpieczeństwa maszyn, nakładająca obowiązek projektowania i konstruowania urządzeń w sposób zapewniający ich bezpieczne użytkowanie przez operatorów i osoby trzecie;
* Dyrektywa 2014/30/UE – w zakresie kompatybilności elektromagnetycznej (EMC), zapewniająca odporność agregatu na zakłócenia elektromagnetyczne oraz ograniczająca emisję takich zakłóceń do poziomów niezakłócających działania innych urządzeń;
* Dyrektywa 2014/35/UE – dotycząca sprzętu elektrycznego przeznaczonego do stosowania w określonych granicach napięcia, mająca na celu zagwarantowanie bezpieczeństwa użytkowania urządzeń zasilanych napięciem od 50 do 1000 V AC i od 75 do 1500 V DC;
* PN-EN ISO 8528-13:2016-07 – określająca szczegółowe wymagania dotyczące systemów sterowania, systemów monitorowania i automatyki agregatów prądotwórczych;
* PN-EN ISO 3744:2011 – określająca metody pomiaru poziomu mocy akustycznej generowanej przez urządzenie, w celu spełnienia wymagań akustycznych w zakresie ochrony środowiska i zdrowia pracowników;
* ISO 8528-1:2005 – zawierająca ogólne wymagania dotyczące projektowania, wykonania i badania agregatów prądotwórczych napędzanych silnikami spalinowymi;
* Dyrektywa 2000/14/WE oraz Dyrektywa 2005/88/WE (tzw. Dyrektywy Hałasowe) – ustanawiające dopuszczalne poziomy emisji hałasu dla urządzeń stosowanych na zewnątrz budynków, w tym agregatów prądotwórczych, wraz z obowiązkiem oznakowania poziomu hałasu na urządzeniu.

**W celu zapewnienia wysokiej jakości wykonania oraz nadzoru nad procesami produkcyjnymi, Zamawiający wymaga, aby producent urządzenia posiadał:**

* **Certyfikowany system zarządzania jakością zgodny z normą ISO 9001:2015**, potwierdzający wdrożenie skutecznych mechanizmów zarządzania jakością w procesie projektowania, produkcji, testowania i obsługi urządzeń technicznych;

Dla pełnego wsparcia wymagane jest, aby:

* Wykonawca posiadał umowę o współpracy z producentem agregatu w zakresie dostawy, uruchomienia i serwisowania dostarczonych maszyn i urządzeń dodatkowych;
* producent agregatu posiadał co najmniej 10 lat własny oddział, serwis oraz magazyn części zamiennych i materiałów eksploatacyjnych.

**Zamawiający wymaga, aby dostarczony agregat prądotwórczy spełniał poniższe wymagania konstrukcyjne, eksploatacyjne i jakościowe:**

1. **Obudowa dźwiękochłonna:**
	* agregat musi być wyposażony w solidną, wyciszoną obudowę dźwiękochłonną, wykonaną z materiałów odpornych na warunki atmosferyczne i korozję;
	* wnętrze obudowy powinno być wyłożone **specjalną, niepalną pianką wygłuszającą**, zapewniającą skuteczne tłumienie hałasu emitowanego przez urządzenie;
	* obudowa powinna posiadać **drzwi dostępowe i serwisowe** umożliwiające łatwy dostęp do podzespołów agregatu w celu przeprowadzenia obsługi technicznej i przeglądów.
	* powierzchnia zewnętrzna obudowy musi być **malowana proszkowo** z zachowaniem estetyki wykonania i odporności na działanie czynników zewnętrznych.
2. **Pochodzenie i linia produkcyjna:**
	* agregat musi pochodzić z **seryjnej i bieżącej produkcji** – wyklucza się dostawy urządzeń magazynowanych, wycofanych z produkcji lub składanych na potrzeby jednorazowego zamówienia;
	* urządzenie powinno być **wyprodukowane w Polsce**, co należy potwierdzić odpowiednim oświadczeniem producenta lub dokumentacją techniczną;
	* urządzenie musi być spreparowane przez jednego producenta, zaś jakiekolwiek modyfikacje ingerujące w jego konstrukcję nie są dopuszczalne.
3. **Parametry techniczne:**
	* **moc znamionowa agregatu:** minimum **40 kVA** (32 kW);
	* **moc awaryjna (maksymalna):** nie mniej niż **44 kVA** (35 kW);
	* **napięcie wyjściowe:** 400/230 V (3-fazowe);
	* **częstotliwość wyjściowa:** 50 Hz.
4. **Zgodność i certyfikacja:**
	* agregat musi być oznakowany znakiem **CE**, potwierdzającym zgodność z obowiązującymi dyrektywami unijnymi, w tym dyrektywą maszynową, kompatybilności elektromagnetycznej, niskonapięciową oraz dyrektywą hałasową
5. Konstrukcja, rama, wymiary:
* agregat musi posiadać bardzo mocną konstrukcję z możliwością transportu wózkiem widłowym, dźwigiem, HDS – na pasach, widłach lub łańcuchach
* rama dodatkowo izolowana od podłoża za pomocą stóp (stożków) gumowych przykręcanych do ramy, z możliwością regulacji wysokości (poziomowania);
* klasa wykonania minimum G2;
* wymagany zewnętrzny przycisk zatrzymania awaryjnego.
* wymagane wysokowydajne amortyzatory drgań silnika i prądnicy;
* wymiary nieprzekraczające (dł/szer/wys) – 2300 mm/ 1100 mm/ 1600 mm;
* stalowy tłumik dźwięków -35db(A) – zabudowany wewnątrz agregatu
1. Zaciski na listwie sterowniczej:
* NC do podłączenia zewnętrznego stopu pożarowego;
* dla kabla potrzeb własnych agregatu;
* dla kabla sterowniczego, sterowania układem SZR.
1. Zbiornik i wlew paliwa:
* co najmniej o pojemności 100 dm3;
* pozwalający na ciągłą pracę agregatu przy 75% obciążenia co najmniej przez 11,9 h;
* pozwalający na ciągłą pracę agregatu przy 100% obciążenia co najmniej 10 h;
* wymagany czujnik poziomu paliwa ze wskazaniem na sterowniku;
* wymagany alarm poziomu paliwa przy poziomie 15% (rezerwa);
* wymagane automatyczne wyłączenie agregatu przy poziomie paliwa 5% (zabezpieczenie przed zapowietrzeniem);
* wymagany również korek spustowy zbiornika oraz co najmniej jeden niezależny, otwór w zbiorniku zaślepiony deklem na śrubach, umożliwiający montaż i podłączenie dodatkowej instalacji paliwowej, lub przeniesienie wlewu paliwa na drugą stronę zbiornika;
* wlew paliwa - korek zamykany kluczykiem, wewnątrz obudowy.
1. Silnik
* turbodiesel, np. Y4105D lub inny spełniający wymagania;
* silnik diesla o mocy znamionowej PRP nie mniejszej niż – 38kW;
* liczba i układ cylindrów – 4 L;
* wymagany typ wtrysku – bezpośredni;
* elektroniczna regulacja obrotów;
* podgrzewanie bloku – grzałka silnika kontrolowana przez sterownik agregatu;
* spalanie przy 75% obciążenia nie więcej niż – 8,5 l/h;
* spalanie przy 100% obciążenia nie więcej niż – 10,0 l/h;
* filtr powietrza suchy;
* silnik chłodzony glikolem;
* prędkość obrotowa – 1500 r.p.m.;
* układ elektryczny 12V;
* akumulator 12V;
* automatyczna ładowarka buforowa akumulatora/ów w czasie czuwania;
* osłona elementów gorących oraz ruchomych.
1. Prądnica:
* wyposażona w automatyczną regulację napięcia;
* obudowa (wg IEC-34-5) - IP23;
* złącze – elastyczny dysk;
* klasa izolacji – H;
* wymagane wykonanie, gdzie stojan prądnicy jest nawinięty z poskokiem 2/3, ponieważ zapewnia to eliminację krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Poskok 2/3 minimalizuje indukowanie się nadmiernych prądów w obwodzie neutralnym;
* wytrzymałość zwarciowa prądnicy >300% obciążenia znamionowego.
1. Sterownik
* np SMART 500 MKII lub inny spełniający wymagania, z pełną obsługą rozwiązań producenta;
* sterownik z komunikatami w języku polskim, pozwalający na kontrolę parametrów sieci i agregatu (napięć , prądów, mocy, częstotliwości, cosɸ, napięcia ładowania akumulatora, ilość paliwa w zbiorniku, czasu pracy agregatu, parametrów silnika);
* panel sterownika wyposażony w tabliczkę z diodami sygnalizacyjnymi dla łatwej obsługi i szybkiej identyfikacji stanów pracy urządzenia;
* wymagana jest identyfikacja alarmów dotyczących działania baterii, pracy alternatora, poziomu paliwa, ciśnienia oleju oraz dwa dodatkowe do zdefiniowania. Sterownik musi posiadać w tylnej ścianie wolne sloty do podłączenia dodatkowych modułów sygnalizacyjnych np. GSM, ETHERNET, styków/wyjść przekaźnikowych dla sygnałów bezpotencjałowych (do zdefiniowania przez użytkownika);
* szafa elektryczna/automatyki agregatu zbudowana na podzespołach renomowanych producentów elektryki i elektroniki, według norm i standardów;
* sterownik musi posiadać:
* datakom SMART 500-MK2 to ekonomiczny kontroler agregatu gotowy do integracji BMS i monitorowania poprzez internet posiadającego cechy:
* obsługa agregatów na olej napędowy i gaz;
* obsługa 400 Hz;
* dziennik - 400 zdarzeń;
* możliwość edycji wszystkich parametrów na panelu przednim;
* 3-poziomowe hasło konfiguracyjne;
* graficzny wyświetlacz LCD 128x64;
* języki do pobrania (domyślnie – polski);
* wyświetlanie przebiegów napięcia i prądów;
* analiza harmonicznych;
* wyjścia 16 A MCB i GCB;
* 8 konfigurowalnych wejść cyfrowych;
* wejścia rozszerzalne do 40;
* 6 konfigurowalnych wyjść cyfrowych;
* wyjścia z możliwością rozszerzenia do 38;
* 3 konfigurowalne wejścia analogowe;
* zarówno CANBUS-J1939, jak i MPU;
* 3 konfigurowalne alarmy serwisowe;
* tygodniowy harmonogram pracy;
* ręczna „precyzyjna regulacja prędkości” w wybranych ECU;
* automatyczne sterowanie pompą paliwa;
* ochrona przed nadmierną mocą;
* odwrotna ochrona zasilania;
* zabezpieczenie przed przeciążeniem IDMT;
* zrzut obciążenia, obciążenie zastępcze;
* zarządzanie wieloma obciążeniami;
* zabezpieczenie od asymetrii prądu;
* ochrona przed asymetrią napięcia;
* zegar czasu rzeczywistego z podtrzymaniem bateryjnym;
* kontrola prędkości biegu jałowego;
* ładowanie akumulatora włączone;
* siele parametrów nominalnych;
* napęd Tactor i MCB;
* 4 kwadrantowe liczniki mocy agregatu;
* liczniki zasilania sieciowego;
* wskazania poziomu paliwa;
* wyświetlacz diagnostyczny modemu;
* konfigurowalny przez USB, RS-485 i GPRS;
* darmowy program konfiguracyjny;
* gotowy do centralnego monitorowania;
* obsługa mobilnych agregatów prądotwórczych;
* łatwa aktualizacja oprogramowania sprzętowego USB;
* stopień ochrony IP65 ze standardową uszczelką.
1. Pomiary:
* napięcia sieci i agregatu PN / PP;
* częstotliwość sieci i agregatu;
* prądy fazowe sieci i agregatu;
* prądy neutralne sieci i agregatu;
* sieć i agregat, faza i suma, kW, kVA, kVAr, pf;
* prędkość silnika;
* napięcie baterii;
* temperatura silnika;
* ciśnienie oleju;
* zużycie paliwa (dla silników wyposażonych w ECU);
1. KOMUNIKACJA
* 4-pasmowy modem GPRS (opcjonalnie);
* port USB;
* RS-485 (2400-115200) (opcjonalnie);
* RS-232 (2400-115200);
* J1939-CANBUS;
* centralny monitoring internetowy;
* wysyłanie wiadomości SMS (opcjonalnie);
* wysyłanie e-mail (opcjonalnie);
* darmowe oprogramowanie na PC: Rainbow Plus;
* Modbus RTU.

# Układ SZR

# **u**kład SZR typu RTSE na przełączniku z napędem silnikowym SOCOMEC ATyS d M 63A lub innym spełniającym wymagania**;**

# **b**lokada elektryczna - odpowiednie połączenie modułu sterowania uniemożliwiające równoczesne wysterowanie tych samych pozycji**;**

# **b**lokada mechaniczna – przełącznik źródła zasilana z napędem silnikowym składający się z dwóch niezależnych rozłączników. Zamienne załączenie rozłączników odbywa się z przerwą czasową i przez pozycję 0**;**

# **b**lokada programowa – blokada ta uniemożliwia jednoczesne wysterowanie dwóchprzekaźników zabudowanych wewnątrz układu SZR**;**

# **z**amienne załączanie rozłączników odbywa się z przerwą czasową i zawsze przez pozycję „0”. Dzięki temu nie ma możliwości (nawet przy uszkodzeniu układu sterowania) jednoczesnego załączenia obu **łączników,** czyli spotkania się napięcia sieci i generatora**;**

# **t**ryby sterowania**:**

* sterowanie automatyczne - w momencie zaniku napięcia sieci sterownik agregatu rozpoczyna odliczanie zaprogramowanej zwłoki czasowej. Po upłynięciu nastawionego czasu i utrzymującego się braku napięcia sieci sterownik przełącza się w pozycję „0” i wystawia sygnał START agregat, który rozpoczyna procedurę startu silnika napędzającego generator według zaprogramowanych w sterowniku agregatu parametrów (czas startowania i przerwa, ilość możliwych prób startowania itp.). Po pojawieniu się napięcia generatora, sterownik agregatu sprawdza jego parametry (wartość, częstotliwość) i gdy mieszczą się w dopuszczalnych granicach - przełącza układ w pozycję „II” przechodząc przez pozycję „0” i załącza kierunek zasilania z generatora. Tym samym napięcie generatora podane jest na odbiory;
* powrót napięcia - W momencie ponownego pojawienia się napięcia sieci i jego utrzymywania się przez odpowiedni czas, sterownik agregatu przełącza układ w pozycję „I” przechodząc przez pozycję „0” i załącza kierunek zasilania z sieci. Następnie utrzymuje jeszcze pracę silnika przez określony czas ok. 2 min, w celu umożliwienia wychłodzenia silnika bez obciążenia. Po upłynięciu tego czasu, sterownik agregatu wyłącza silnik napędzający generator i wraca do stanu wyjściowego tzn. do czuwania i monitorowania sieci;
* sterowanie ręczne mechaniczne - Przełącznik SZR można przestawiać przy pomocy dołączonej rączki.
1. Zabezpieczenie przed przedostaniem się napięcia generatora na sieć energetyczną:
* w przypadku wyłączenia energii przez Zakład Energetyczny musi istnieć pewność, że napięcie z agregatu nie przedostanie się do sieci zasilającej. Podobnie rzecz ma się w drugim kierunku -napięcie z sieci nie może zostać podane na agregat. Musi to być zapewnione przez niżej wymienione środki:
* budowa mechaniczna przełącznika – przełącznik źródła zasilania z napędem silnikowym Socomec ATys d M 63A o trzech stabilnych pozycjach 1-0-2, składa się z dwóch niezależnych rozłączników 4-polowych izolacyjnych (tory główne) połączonych mechanicznie w sposób uniemożliwiający ich jednoczesne załączenie. Przełączenie źródeł odbywa się z przejściem przez pozycję 0;
* blokada elektryczna sterowania przełącznika – przełącznik posiada wewnętrzną blokadę uniemożliwiającą równoczesne wysterowanie dwóch pozycji przełącznika. Blokadę elektryczną zapewnia także układ mini SZR-a na zasilaniu i sterowaniu przełącznika zbudowany na ministycznikach z własną blokadą mechaniczną i elektryczną;
* blokada programowa – blokada ta uniemożliwia jednoczesne wysterowanie dwóch przekaźników zabudowanych wewnątrz sterownika agregatu podających sygnały do przełączania SZR-a.
1. Dane przełączeniowe przy zastosowaniu przełączników ATyS d M:
I - czas trwania przerwy beznapięciowej przy przejściu z pozycji I do II bez postoju w poz.0  - tbn = 0,06 s

II - czas trwania przerwy beznapięciowej z uwzględnieniem sterownika w trybie I-0-II i II-0-I (czas w poz.0 ustawiany w sterowniku) - tbn > 1,06 s

III - czas przełączania w trybie I-0-II i II-0-I - tp > 1,18 s

1. Próby fabryczne
* Przed dostarczeniem agregatu na obiekt należy umożliwić Zamawiającemu wykonanie próby FAT u producenta, w obecności komisji zamawiającego i do dokumentacji powykonawczej załączyć stosowny protokół.

**PODSUMOWANIE OPISU PRZEDMIOTU ZAMÓWIENIA**

Zamawiający wymaga, aby wszystkie oferowane przez Wykonawcę urządzenia, sprzęty
i oprogramowania były nowe, a także aby pochodziły z oficjalnego kanału dystrybucyjnego.

Zamawiający informuje, że dopuszcza rozwiązania równoważne. W przypadku stwierdzenia użycia
w postępowaniu nazw własnych, znaków towarowych lub określeń w sposób bezpośredni wskazujących typ, model, pochodzenie bądź konkretnego producenta - Zamawiający informuje, że stanowią one określenia materiałów, sprzętów czy innych powszechnie dostępnych, które stanowią określenie pożądanej jakości oraz efektu docelowego. Należy przyjąć charakterystyczne dla danego materiału parametry jako odniesienie do standardu określonego przez Zamawiającego. Zamawiający informuje, że Wykonawcy przysługuje prawo do użycia materiału, urządzenia, wyrobu czy rozwiązania równoważnego, spełniającego wymagania jakościowe i funkcjonalne opisane w postępowaniu i zapis ten odnosi się do całości postępowania.

W związku z powyższym Zamawiający nie narzuca użycia materiałów, wyrobów czy urządzeń żadnego konkretnego producenta czy dostawcy. Zaproponowane rozwiązania równoważne muszą spełniać co najmniej założenia przyjęte w postępowaniu. Zamawiający dopuszcza możliwość zaproponowania rozwiązań równoważnych w stosunku do opisanych, z zastosowaniem tych samych standardów technicznych i jakościowych niezbędnych do prawidłowego funkcjonowania przedmiotu zamówienia.

Poprzez pojęcie rozwiązań równoważnych należy rozumieć rozwiązania zapewniające uzyskanie parametrów technicznych, jakościowych i użytkowych nie gorszych niż założone w opisie przedmiotu zamówienia. Wykonawca, który powołuje się na rozwiązania równoważne do rozwiązań opisywanych przez Zamawiającego, zobowiązany jest wykazać, że oferowany przez niego przedmiot zamówienia spełnia wymagania określone przez Zamawiającego.

Tam, gdzie w opisie przedmiotu zamówienia został wskazany konkretny typ, znak towarowy, marka, producent, dostawca, patent, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczone przez konkretnego wykonawcę, Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych w stosunku do wskazanych w opisie przedmiotu zamówienia pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych od założonych w opisie oraz będą zgodne pod względem:

‒ charakteru użytkowego (tożsamość funkcji),

‒ parametrów technicznych (wytrzymałość, trwałość, dane techniczne),

‒ parametrów bezpieczeństwa użytkowania.