

Załącznik nr 1 do SWZ – Opis przedmiotu zamówienia

RR.271.13.2025

Opis przedmiotu zamówienia dla części 1 i części 2 zamówienia

Przewidywany czas realizacji: do 60 dni od dnia podpisania umowy

Miejsce dostawy: Urząd Gminy Sułów, Sułów 63, 22-448 Sułów.

Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent lub pochodzenie, źródło lub szczególny proces, które wskazują lub mogłyby wskazywać na konkretnego producenta/dostawcę – nie stanowi to preferowania konkretnego wyrobu lub producenta/dostawcy, lecz ma na celu jedynie wskazanie cech – parametrów technicznych, użytkowych i jakościowych nie gorszych od podanych w opisie. Należy to więc traktować jedynie jako pomoc w opisie przedmiotu zamówienia.

Jeżeli Wykonawca stwierdzi, że użyte w opisie parametry lub normy krajowe lub przenoszące na normy europejskie lub normy międzynarodowe mogą wskazywać na producentów produktów lub źródła ich pochodzenia to oznacza, że mają takie znaczenie, że parametry techniczne tak wskazanych produktów określają wymagane przez Zamawiającego minimalne oczekiwania co do jakości produktów, które mają być użyte do wykonania przedmiotu umowy. Wykonawca jest uprawniony do stosowania produktów równoważnych, przez które rozumie się takie, które posiadają parametry techniczne nie gorsze od tych wskazanych w opisie, również dopuszcza się wykazanie normami równoważnymi w stosunku do tych wskazanych w zapytaniu ofertowym. Na Wykonawcy spoczywa ciężar wykazania "równoważności".

Wykonawca musi zaoferować spełniające min. takie wymagania i parametry techniczne, jak w opisie przedmiotu zamówienia. Wykonawca może zaoferować produkty o lepszych parametrach. Dostarczone przedmioty zamówienia powinny być fabrycznie nowe, wykonane zgodnie z wymaganiami i normami mającymi zastosowanie do danego wyrobu, wolne od wad, odpowiadać normom jakościowym, określonym we właściwych aktach prawnych, posiadać aktualne aprobaty techniczne, gwarancje producenta oraz winny spełniać wszelkie wymogi przewidziane obowiązującymi przepisami dla tego typu wyrobów.

CZĘŚĆ 1 ZAMÓWIENIA OBEJMUJE:**1. Serwer – 2 sztuki**

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą 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/ WIFI.
Płyta główna	- Płyta główna z możliwością zainstalowania do dwóch procesorów. - Obsługa procesorów 32 rdzeniowych. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. - Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, 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.
RAM	128GB DDR5 RDIMM 5600MT/s,
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający - Min. 8GB nieulotnej pamięci cache, - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. - Wsparcie dla dysków samoszyfrujących
Dyski twarde	- Zainstalowane 8x dysk SSD SAS o pojemności min. 1.2TB Hot-Plug. - Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.
Gniazda PCI	Trzy sloty PCIe LP
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Wbudowane porty	4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy - Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 700W klasy Titanium
Elementy montażowe	- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych - Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków

	twardych. • Wbudowany 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. • 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. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: ○ 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 autentykację i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); 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 automatycznej rejestracji DNS ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

	oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego 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 oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu 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 alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu 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 zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: ● Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemu pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników

	FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ● Aktualizacja firmware ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
--	--

- możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
 - Możliwość generowania raportów dla serwerów zawierających informację o:
 - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
 - Średnim obciążeniu: procesorów, pamięci RAM, IO,
 - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
 - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
 - Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo
 - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
 - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
 - Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
 - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
 - Urządzenie Producenta dostarczane w ramach postępowania
 - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent
 - Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;
- Możliwość rozszerzenia funkcjonalności
 - Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
- Inne

	○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
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.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć 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 serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym

	przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
--	---

2. Urządzenie UTM – 1 sztuka

Wymagania ogólne

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

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

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

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundacja, monitoring i wykrywanie awarii

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

Interfejsy, dysk, zasilanie

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

Parametry wydajnościowe

1. W zakresie Firewall'a obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 3 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 750 Mbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 450 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje systemu bezpieczeństwa

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

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

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

Polityki, Firewall

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

Połączenie VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości

lub umożliwiał konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.

4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. 10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. 11. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

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

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

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

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

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

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

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

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 na okres 12 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Wdrożenie zintegrowanych rozwiązań w ramach dostawy

Wykonawca przeprowadzi wdrożenie dostarczonego urządzenia wraz z pełną konfiguracją polityk bezpieczeństwa i integracją z obecną infrastrukturą informatyczną Zamawiającego.

Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera – Koordynatora technicznego, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania UTM w zakresie:

- Certyfikat w zakresie Bezpieczeństwa Sieci (NS)
- Certyfikat w zakresie Bezpieczeństwa Chmury Publicznej (PCS)
- Certyfikat w zakresie Operacji Bezpieczeństwa (SO)
- Certyfikat w zakresie bezpiecznego dostępu na krawędzi sieci (SASE)

Certyfikaty osobowe załączyć do oferty.

3. Dysk sieciowy NAS – 1 sztuka

Procesor	Czterordzeniowy procesor min. AMD Ryzen V1500B 2,2 GHz lub o wyższych parametrach
Obudowa	Desktop o wymiarach nie większych niż 189 (Wysokość) x 330 (Szerokość) x 282 (Głębokość) mm
Pamięć RAM	8GB RAM DDR4 SO-DIMM – możliwość rozszerzenia do 64GB (2 sloty SO-DIMM)
Ilość obsługiwanych dysków	8 dysków 3,5-calowe SATA 6 Gb/s, 3 Gb/s o pojemności maksymalnej dysku 18TB, 2 x M.2 2280 PCIe Gen3 x1 slots
Interfejsy sieciowe	2 x 2,5 Gigabit sieci Ethernet (RJ45), możliwość dołożenia karty rozszerzeń na porty 10 Gigabit/ 5 Gigabit Ethernet Port, obsługa VLAN i Jumbo Frame.
Pamięć flash	5GB
Porty	3 x Type-A USB 3.2 Gen 2 10Gbps 1 x Type-C USB 3.2 Gen 1 5Gbps
Złącza PCIe	2x Gniazdo 1: PCIe Gen 3 x4
Wskaźniki LED	Stan/zasilanie, USB, LAN, dyski 1–8, M.2 SSD 1–2
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10, 50, 60
Funkcja Hot	RAID Hot Spare and Global Hot Spare

Spare	
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
Kompatybilny system operacyjny	Apple Mac OS 10.10 or later Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux IBM AIX 7, Solaris 10 or later UNIX Microsoft Windows 7, 8, and 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Serwer pocztowy Xeams, Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog,
Zarządzanie dyskami	Skanowanie w poszukiwaniu złych sektorów, odczyt S.M.A.R.T
Stacja monitoringu	Obsługa 24 kamer IP (8 licencji domyślnie).
Język GUI	Polski
Gwarancja	Gwarancja producenta 60 miesięcy
Waga	Maksymalnie 9 kg (brutto)
Pobór mocy	Praca poniżej 55W / Tryb uśpienia poniżej 26 W
System plików	Dyski wewnętrzne EXT4/ZFS. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+, exFAT (licencja opcjonalna)
iSCSI	Obsługa MPIO & MC/S, SPC-3 persistent reservation
Liczba iSCSI LUN	Do 256
Liczba kont użytkowników	Do 4096
Liczba grup	Do 512
Liczba jednoczesnych połączeń	Maksymalnie 2000
Liczba udziałów	512
Zasilanie	Wewnętrzny zasilacz 250W
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.
Dyski	8 dysków HDD 3,5" o parametrach: - pojemność 4TB - 5400 RPM - 256MB Cache - MTBF 1 mil. Godzin - Pobór mocy w trybie pracy max. 4.8W - Pobór mocy w trybie bezczynności max. 3.96W - Usługa odzyskiwania danych z dysków wykonywana przez producenta

4. Zasilacz UPS i akumulatory – 1 sztuka

CECHY OGÓLNE

Typ	Jednofazowy online (VFI)
Fazy (wejście-wyjście)	1-1
Współczynnik kształtu	Stojak, wieża
Jednostki rackowe [U]	2U
Pojemność mocy	3000VA / 3000W
Współczynnik mocy wyjściowej	1
WEJŚCIE	
Zakres napięcia wejściowego	160-300 V przy obciążeniu 100%, 110-160 V przy liniowym obniżeniu do 50% obciążenia
Maksymalne THDi	≤5%
Zakres częstotliwości	40Hz – 70Hz
Częstotliwość (zakres synchronizowany)	45Hz – 55Hz lub 54Hz – 66Hz przy obciążeniu >60%
WEJŚCIE PRĄDU STAŁEGO (PV)	
Współczynnik mocy wejściowej	> 0,99 przy pełnym obciążeniu
WYJŚCIE	
Kształt fali	Czysta fala sinusoidalna
VA	3000
Współczynnik szczytu obciążenia	3:1
Nominalne napięcie wyjściowe	200/208/220/230/240 VAC (obniżenie o 10% przy 208 V, obniżenie o 20% przy 200 V)
THDv	≤1% przy 100% obciążeniu liniowym, ≤5% przy 100% obciążeniu nieliniowym
Częstotliwość (tryb bateryjny)	±0,2 Hz
Współczynnik mocy wyjściowej	1
ZŁĄCZA WEJŚCIOWE I WYJŚCIOWE	
Złącze wejściowe	C20

IEC C13 8

IEC C19 1

SZCZEGÓŁY TECHNICZNE

Sprawność trybu
liniowego [%] (pełne
obciążenie) 93,0

Sprawność w trybie ECO
[%] (pełne obciążenie) 97,0

Czas przełączania (z
trybu AC/sieciowego lub
trybu akumulatorowego
na tryb ECO) [ms] 10 ms

Czas przełączania (z
trybu AC/sieciowego na
tryb baterijny) [ms] 0 ms

Czas przełączania (z
trybu ECO na tryb
AC/sieciowy lub
akumulatorowy) [ms] 10 ms

Czas przełączania (z
trybu sieciowego lub
baterijnego na tryb
obejściowy) [ms] 4 ms

Współczynnik szczytu
obciążenia 3:1

Dodatkowe funkcje Dostępny tryb CVCF, śruba wyrównująca potencjały,
akumulatory z możliwością wymiany podczas pracy,
OBM – zoptymalizowane zarządzanie akumulatorem,
wyświetlacz LCD, współczynnik mocy Unity 1.0,
dostępny akumulator, IoT – łączność z chmurą,
zgodność z generatorem, EPO – wyłącznik awaryjny,
dostępny programowalny segment, HID – urządzenie
interfejsu użytkownika, EBM – zewnętrzny moduł
akumulatorowy – automatyczne wykrywanie

Klasyfikacja IEC 62040-3 VFI-SS-311

BATERIE I AUTONOMIA

Baterie 6x 12,0 V/9,0 Ah

Napięcie stałe 6x 12,0 V

Czas ładowania 3h do 90%

Czas podtrzymania
pełnego obciążenia [min] 3.7

Czas podtrzymania
połowy obciążenia [min] 10.1

Rumak 1,5 A

Zewnętrzny akumulator Anderson PP45 x2

Czas ładowania 3h do 90%

KOMUNIKACJA

Komunikacja Styk suchy, RS-232, port WLAN – do połączenia internetowego, gniazdo karty zarządzającej, RJ-45 – do połączenia internetowego

ZARZĄDZANIE I ŚRODOWISKO

Komunikacja Styk suchy, RS-232, port WLAN – do połączenia internetowego, gniazdo karty zarządzającej, RJ-45 – do połączenia internetowego

Poziom hałasu < 50dB

Logika wentylatora Zawsze włączony , automatyczna kontrola prędkości

Temperatura 0°C – 40°C

Wilgotność 0% – 95% wilgotności względnej (bez kondensacji)

IP IP 20

CZĘŚĆ 2 ZAMÓWIENIA OBEJMUJE:

1. Agregat prądotwórczy – 1 sztuka

Parametr	Wymagania techniczne minimum
Przygotowany do pracy	Dostarczony agregat powinien być w pełni skonfigurowany pod potrzeby Zamawiającego tj. Agregat zalany olejem silnikowym oraz płynem chłodniczym.
Rodzaj	Stacjonarny
Rok produkcji	2025
Stan agregatu	Fabrycznie nowy
Gwarancja	36 miesięcy
Moc agregatu	20 kW 25 kW
Stopień sprężania	19:01
System zasysania	Naturalny
Typ agregatu	Trójfazowy

Sprawność $\cos \Phi$	0.8
Rodzaj paliwa	Olej napędowy (Diesel)
Rodzaj silnika	Wysokoprężny (Diesel), 4-suwowy
Spalanie	7.0 litrów na godzinę (przy 100% mocy maksymalnej) 6.0 litrów na godzinę (przy 75% mocy maksymalnej) 3.7 litrów na godzinę (przy 50% mocy maksymalnej)
Ilość cylindrów	4
Wtrysk bezpośredni	Tak
Konfiguracja silnika	Rzędowy (R4)
Rodzaj chłodzenia	Cieczą (Agregat posiada chłodnicę)
Pojemność skokowa	3610 cc3
Ilość obrotów na minutę (RPM)	1500
Dopuszczalny maksymalny czas pracy (1 cykl)	24 godziny
Czas chłodzenia (po 1 cyklu)	60 minut
Czujnik ciśnienia oleju	Tak
Czujnik stanu oleju	Tak
Rodzaj rozrządu	Zaworowy napędzany kołem zębatym
Czujnik poziomu płynu chłodniczego	Tak
Regulator obrotów silnika	Mechaniczny
Sposób smarowania	Wymuszone, silnik z pompą olejową
Rozrusznik	1500W
Pojemność miski olejowej	8.0l
Rodzaj zaworu	Elektromagnetyczny, sterowany pojedynczym elektromagnesem
Prądnica Moc znamionowa 400V	20000 Watt (20kW / 25kVA)
Prądnica Moc maksymalna 400V (do 15 minut)	24000 Watt (24kW / 30 kVA)
Moc znamionowa 230V	6650 Watt
Moc maksymalna 230V (do 15 minut)	8000 Watt
Prąd znamionowy (400V)	43.0 A
Napięcie	230/400V
Zabezpieczenia prądowe	C16, C32, główne - 100A
Częstotliwość	50 Hz
Budowa prądnicy	Synchroniczna
Stopień ochrony (prądnicy)	IP 23
Typ zabudowy	Zabudowane - Wyciszone
Możliwość odprowadzenia spalin poza obiekt	Tak
Zabudowa odporna na opady atmosferyczne	Tak
Poziom ciśnienia akustycznego	85dB (pomiar - 5m, otwarta przestrzeń)
Ilość gniazd trójfazowych	1 sztuka (32A 5-bolcowe)
Ilość gniazd jednofazowych	2 sztuki (16A)
Pojemność zbiornika paliwa	80 litrów
Czas pracy na pełnym zbiorniku (Średni)	20 godzin
Zestaw transportowy	Tak - Otwory na widły

	Tak - Haki do transportu HDS
Długość	219 cm
Wysokość	128 cm
Waga netto	900 kg
Waga brutto	1015 kg
Automatyczny start (SZR)	Tak - wyposażony Tak - przystosowany
Stabilizator napięcia (AVR)	Tak - 2%, Stamford SX460
Rodzaj rozruchu	Elektryczny Automatyczny
Zabezpieczenie przeciążeniowe termiczne	Tak
Świece żarowe	Tak
Podgrzewanie miski olejowej	Tak
Podgrzewanie cieczy chłodzącej	Tak
Wskaźnik poziomu paliwa	Tak
Akumulator	2 sztuki 40Ah
Licznik motogodzin	Tak
Amperomierz	Tak
Woltomierz	
Logika PLC	Wbudowana logika PLC i edytor PLC
Rozszerzenia modułu CAN	Tak
Integracja z systemem SCADA	Tak
Dodatkowe wyjścia	Dwa gniazda na moduły wtykowe do połączeń 4G, Ethernet, RS232/485 oraz dodatkowe wejścia i wyjścia binarne
Dodatkowe	Podstawowe szkolenie z obsługi agregatu prądotwórczego Uruchomienie agregatu w trybie manualnym na miejscu dostawy Dołączyć kartę katalogowa do oferty