**Parametry techniczne infrastruktury IT**

**Elementy Infrastruktury:**

a) Węzły klastra – 3 szt.
b) Przełącznik 24 portowy zarządzalny – 1 szt.
c) Klaster urządzeń UTM – 2 szt.
d) Serwerowa szafa Rack 42U – 1 szt.
e) UPS - 1 szt.
f) Zewnętrzny agregat prądotwórczy - 1 szt.

Parametry minimalne

***Węzły klastra – 3 szt.***

| | |
|---|---|
| **Typ sprzętu** | Serwer w obudowie typu RACK |
| **Procesor** | Dwa procesory serwerowe o łącznej minimalnej ilości 28 rdzeni, a maksymalnej 32 rdzeni. Bazowe takotowanie min. 3.0GHz.<br>Pojedyńczy procesor musi posiadać min. 128 linii PCIe 5.0 oraz wsparcie dla 12 kanałów pamięci DDR5 4800MT/s. Maksymalne typowe TDP: 200W |
| **Płyta główna - złącza wewnętrzne** | Ilości minimalne:<br>· Minimalnie 9 złączy PCIe Gen5 w tym 4x wolne/nieużywane aktywne, pełne złącza PCIe Gen5 x16<br>· 24 złącza DDR5 obsługujące min. 6144GB pamięci, z czego przynajmniej 50% złącz wolne/nieużywane.<br>· obsługa dwóch procesorów, min. 128 rdzeniowych, o TDP do 400W |

| | |
|---|---|
| **Złącza zewnętrzne** | Wbudowane (ilości minimalne):<br>· 4x USB 3.2<br>· 1x interfejs sieciowy RJ45 1GbE,<br>· interfejs RJ45 “out-of-band management / lights-out management” umożliwiający zarządzanie elementami sprzętowymi serwera oraz zdalny dostęp do konsoli (w tym w trybie graficznym)<br>Wymagana minimalna ilość i rozmieszczenie portów na zewnątrz obudowy nie może być osiągnięte w wyniku stosowania zewnętrznych konwerterów, przejściówek itp. |
| **Pamięć RAM** | Minimum 768GB RAM w 12 kościach pamięci DDR5. Kości powinny być tego samego modelu,<br>sygnowane logo producenta serwera. Min. Przepustowość 4800MHz, posiadające korekcje błędów. |
| **Dyski twarde** | Zainstalowane dyski:<br>· Minimum 7x 3,84TB SSD U.2 PCIe 4.0 - prędkość odczytu min. 6900MB/s, prędkość zapisu min. 4100MB/s, DWPD 1.0<br>· Minimum 2x 960GB SSD SATA 2,5" DWPD 1.0 przeznaczone na zainstalowany system operacyjny Dyski muszą być przystosowane do pracy ciągłej 24/7.<br>Dwa wolne złącza M.2 SATA/PCIe znajdujące się bezpośrednio na płycie głównej (nie dopuszcza się stosowania adapterów, przejściówek itp.)<br>Możliwość rozbudowy o minimum 15 dodatkowych dysków w tym min. 9 dysków NVMe |
| **Wyjścia ekranowe** | Minimum 1x VGA na tylnym panelu. Nie dopuszcza się wyjść ekranowych na przednim panelu serwera |
| **Kontroler RAID** | Sprzętowy kontroler RAID producenta serwera, umożliwiający m.in. konfigurację RAID 0, RAID 1, RAID 10, RAID 5, RAID 50, RAID 6 i RAID 60, posiadający wbudowane min. 2GB pamięci cache. |
| **Karta sieciowa** | Minimum:<br>· Dwuportowy kontroler sieciowy SFP 25 Gigabit z dwoma złączami SFP28 wraz z 4m kablem<br>· Dwuportowy kontroler sieciowy SFP 10Gbit SFP+ wraz z wkładami 10Gb 300m LC |
| **Zasilanie** | Redundantne zasilacze, każdy o mocy min. 1600W, działające w sieci 230V 50/60Hz prądu zmiennego z certyfikatem 80Plus Titanium lub równoważny tzn. zasilacze muszą wykazać się minimum 90% sprawnością przy 20% obciążenia, 94% sprawnością przy 50% obciążenia oraz 91% sprawnością przy pełnym obciążeniu, z funkcją Hot-plug (awaria jednego zasilacza pozwoli na ciągłe i w pełni funkcjonalne działanie serwera). |
| **Obudowa** | · Typu RACK (wraz z szynami mocującymi do szafy RACK 19”),<br>· Wysokość maksymalnie 2U,<br>· Kable muszą być przymocowane do elementów obudowy w sposób umożliwiający łatwą i szybką ich wymianę (bez użycia narzędzi). Długość okablowania musi być dopasowana do kształtu i wielkości obudowy,<br>· Maksymalna długość obudowy 843 mm<br>· Szyny montażowe w zestawie<br>· Możliwość montażu czterech dwu-slotowych kart graficznych |

| | |
|---|---|
| **Certyfikaty i standardy** | Wykonawca potwierdza, że oferowane produkty odpowiadają wymaganiom określonym przez Zamawiającego:<br>· Certyfikat ISO9001:2015 oraz ISO 14001 dla producenta sprzętu, lub równoważny<br>· Deklaracja zgodności CE, lub równoważny |
| **Wsparcie techniczne producenta** | · Dostęp do informacji o gwarancji, pierwotnej specyfikacji urządzenia i najnowszych sterowników i uaktualnień realizowany poprzez podanie numeru seryjnego lub modelu urządzenia, na dedykowanej stronie internetowej producenta sprzętu. |
| **Gwarancja** | - 36 miesięcy gwarancji od dnia dostarczenia sprzętu do Zamawiającego, obejmującej naprawę wszystkich części/podzespołów z których składa się serwer w następnym dniu roboczym w miejscu użytkowania sprzętu<br>· 36 miesięcy od dnia dostarczenia sprzętu do Zamawiającego, ochrony danych podczas uszkodzenia dysku - dysk pozostaje u Zamawiającego. |

| | |
|---|---|
| **Obsługiwane systemy operacyjne** | Wsparcie dla:<br>· Linux (Ubuntu/CentOS),<br>· Windows Server 2022<br>· Wirtualizator |
| **Dodatkowe wymagania** | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) i oprogramowanie mające m. in. funkcje:<br>· zdalnego włączenia, wyłączenia i ponownego uruchomienia serwera,<br>· wirtualnej konsoli umożliwiającej m. in. podgląd wyświetlanego przez serwer obrazu i zdalną instalację obsługiwanych przez serwer systemów operacyjnych w trybie graficznym,<br>· automatycznego wysyłania powiadomień/alertów zawierających informacje o części która uległa awarii za pośrednictwem wiadomości email (minimum przy użyciu protokołu SMTP),<br>· możliwość sprawdzenia adresów MAC dla interfejsów sieciowych z poziomu panelu zarządzającego<br>· możliwość podglądu numeru seryjnego oraz mocy zamontowanego zasilacza; aktualnej temperatury, napięcia wejściowego oraz wyjściowego oraz aktualnej pobieranej mocy<br>· możliwość ręcznego ustawienia prędkości obrotowych dla każdego z wentylatorów obudowy przy zdefiniowanej przez użytkownika temperaturze<br>· podgląd live napięć VBAT, +12V, +3.3VSB, +VCORE1, +VCORE2, VSOC1, VSOC2; podgląd live<br>temperatur procesora, pamięci RAM, prędkości obrotowych wentylatorów; ilość pobieranej energii przez procesor, pamięci oraz zasilacze.<br>· możliwość zamontowana obrazu ISO i instalacji systemu operacyjnego<br>· monitoringu procesorów, pamięci RAM, dysków, kontrolera RAID, zasilania, wentylatorów i karty sieciowej.<br>Oprogramowanie do zdalnego zarządzania musi dożywotnio posiadać wyżej wymienione funkcje bez ponoszenia dodatkowych kosztów |
| **Inne wymagania** | · Dostarczone urządzenie jak i podzespoły mają być fabrycznie nowe Serwer nie może być wyprodukowany wcześniej niż 3 miesiące od daty podpisania umowy.<br>· Dostarczone urządzenia/podzespoły nie mogą być oznaczone przez producenta jako „wycofane z produkcji" i mają być dostępne w aktualnej ofercie ich producenta.<br>· Do serwera mają być dołączone przewody zasilające, klawiatura i mysz producenta serwera.<br>· Wszystkie podzespoły w urządzeniu i do urządzenia muszą być zamontowane zgodnie z zaleceniami producenta. |
| **Licencje** | **Środowisko informatyczne w Spółce:**<br><br>Zamawiający posiada klaster niezawodnościowo-wydajnościowy oparty na dwóch nodach fizycznych działających w trybie wzajemnej replikacji w statusie Active/Pasive. Infrastruktura fizyczna oparta jest o witalizatory Hyper-V działające pod systemem Microsoft Windows Server. Uruchomione aplikacje oraz skrypty bazodanowe wykorzystują do swojego działania i obliczeń bazę danych MS SQL. Na środowisku serwerowym uruchomiona jest usługa domeny Active Directory wraz z serwerem terminalowym i wymaganymi licencjami Microsoft CAL RDS i Standard |

1. Bezterminowe licencje systemu serwerowego Microsoft Windows Server 2022 Datacenter lub równoważne zgodnie z poniżej określonymi warunkami równoważności umożliwiające instalację na trzech serwerach fizycznych, z których każdy jest w konfiguracji dwuprocesorowej

2. Bezterminowe licencje dostępowe Microsoft Windows Server 2022 CAL User w ilości minimum 120 szt. lub równoważnymi

3. Bezterminowe licencje zdalnego dostępu Microsoft Windows Server 2022 Remote Desktop Services CAL User lub równoważnymi pozwalającymi na min. 50 jednoczesnych połączeń

4. Bezterminowe Licencje Microsoft Windows SQL lub równoważne w ilości pozwalającej na instalację 9 osobnych serwerów wirtualnych

5. Bezterminowe licencje Microsoft Windows SQL CAL User pozwalające na jednoczesne połączenia 120 użytkowników do silników bazodanowych SQL

Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Data Center 2022 wraz z 120 licencjami dostępowymi Microsoft Windows Server 2022 CAL User 50 licencjami zdalnego dostępu Microsoft Windows Server 2022 Remote Desktop Services CAL User.

- Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nieograniczonej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu dla minimum 120 użytkowników oraz 50 użytkowników w sposób zdalny

- 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.

- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy HyperThreading;
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich
- zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów

| | |
|---|---|
| | posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.<br>• Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.<br>• Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.<br>• Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.<br>• Wraz z licencjami Wykonawca dostarczy klucze aktywacyjne (jeśli są wymagane), nośniki instalacyjne lub dostęp do źródła z którego można pobrać pakiet instalacyjny, dokumenty lub informacje potwierdzające legalność dostarczonego oprogramowania.<br>• Wraz z licencjami Wykonawca dostarczy klucze aktywacyjne (jeśli są wymagane), nośniki instalacyjne lub dostęp do źródła z którego można pobrać pakiet instalacyjny, dokumenty lub informacje potwierdzające legalność dostarczonego oprogramowania.<br>• Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności.<br>• Dostarczone licencje muszą uprawniać Zamawiającego do wykorzystywania historycznie wydanych przez producenta oprogramowania, niższych wersji oprogramowania (prawo do wykonywania downgrade).<br>• Oprogramowanie dostarczone przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nimi oprogramowania<br>• Dostarczone oprogramowanie musi być kompatybilne i współdziałać w sposób niezakłócony ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego oraz nie może powodować zakłóceń pracy środowiska systemowo-programowego Zamawiającego, utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.<br>• Licencje dostarczonego oprogramowania muszą być licencjami wieczystymi.<br>• Oferowane licencje muszą być nowe, zakupione w autoryzowanym kanale dystrybucyjnym producenta oprogramowania oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia<br>• W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego, Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania oprogramowania równoważnego w środowisku sprzętowo-programowym Zamawiającego, dotyczy każdego odrębnie oprogramowania z wymienionych w tabeli nr<br>• Oprogramowanie równoważne oferowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta<br><br>Warunki równoważności dla dostawy oprogramowania Microsoft Windows SQL w ilości pozwalającej na instalację 9 osobnych serwerów wirtualnych. Licencje Microsoft Windows SQL CAL User pozwalające na jednoczesne połączenia 120 użytkowników do silników bazodanowych SQL<br><br>• Dostarczone licencje muszą pozwalać na instalację wcześniejszych wersji oprogramowania<br>• Muszą działać w architekturze klient-serwer, |

| | |
|---|---|
| | • muszą zapewniać integralność i bezpieczeństwo danych<br>• Muszą zapewniać możliwość wykorzystania jako silnika relacyjnej, analitycznej lub wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji.<br>• Muszą umożliwiać dostęp do danych poprzez strukturalny język zapytań SQL, 6. Muszą pozwalać na wielodostępność danych, 7. Muszą posiadać narzędzia do definiowania raportów i wykonywania analiz biznesowych, tworzenia procesów ETL 8. Muszą umożliwiać automatyczne aktualizacje i instalację wszelkich poprawek producenta oprogramowania, 9. Muszą zapewniać skalowanie,<br>• Muszą zapewniać możliwość przypisania użytkownikowi określonej roli, która przydziela użytkownikowi określony zestaw uprawnień do obiektów oraz do wykonywania określonych operacji, 12. Muszą zapewniać możliwość uwierzytelnienia użytkowników i grup zarządzanych przez usługę Active Directory systemu Windows, 13. Muszą pozwalać na odtworzenie zawartości bazy danych po awarii, 14. Muszą posiadać mechanizm optymalizujący wykorzystanie pamięci operacyjnej, 15. Muszą posiadać mechanizm optymalizujący czas dostępu do danych, 16. Muszą posiadać mechanizm zarządzający optymalnym rozłożeniem danych na dyskach, w celu uzyskania lepszej wydajności rozwiązania, 17. Muszą zapewniać możliwość wykorzystania co najmniej 24 rdzeni procesora i co najmniej 128 GB pamięci RAM,<br>• Oprogramowanie musi zapewniać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu, tj. baza relacyjna, usługi analityczne, Strona 4 z 7 usługi raportowe, usługi transformacji danych. Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.<br>• Oprogramowanie musi udostępniać mechanizm zarządzania systemem bazodanowym za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem. 20. Oprogramowanie musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. 21. Oprogramowanie musi umożliwiać wykonywanie typowych zadań administracyjnych, w tym indeksowanie, backup, odtwarzanie danych bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy.<br>• Oprogramowanie musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania, redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania. 23. Oprogramowanie musi umożliwiać tworzenie klastrów niezawodnościowych. 24. Oprogramowanie musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema, podstawową i zapasową przy zachowaniu następujących cech: a) bez dodatkowego sprzętu, poprzez rozwiązanie programowe, b) niezawodne powielanie danych w czasie rzeczywistym, potwierdzone transakcje bazodanowe, c) użytkownicy bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach, 25. Oprogramowanie musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha oprogramowania niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych. |

| | |
|---|---|
| | • Oprogramowanie musi umożliwiać definiowanie reguł wymuszanych przez system i zarządzania nimi, np. uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność. 27. Oprogramowanie musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:<br>○ odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych w celu wychwytywania zapytań znacząco obciążających system,<br>○ wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas, wychwytywanie długo trwających zapytań lub procedur,<br>○ para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy w celu wychwytywania długotrwałych blokad obiektów bazy<br>• Oprogramowanie musi umożliwiać tworzenie procedur składowanych, które mogą być udostępnione i wywoływane jako WebServices, bez wykorzystania dodatkowego oprogramowania. 29. Oprogramowanie musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci. 30. Oprogramowanie musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do “potomków” obiektu, “rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.<br>• Oprogramowanie musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:<br>• udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,<br>• udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,<br>• udostępniać język zapytań do struktur XML,<br>• udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),<br>• udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.<br>• Oprogramowanie musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego systemu bazodanowego. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debuggowania.<br>• Oprogramowanie musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania |

| | |
|---|---|
| | specjalnych procedur i wywoływania ich w sposób rekurencyjny.<br>• Oprogramowanie musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.<br>• Oprogramowanie musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych. W wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób. Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji systemu bazodanowego, wprowadzeniu zmian sprzętowych serwera.<br>• Oprogramowanie musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych, kostki OLAP. Powinno być możliwe tworzenie: wymiarów, miar<br>• Oprogramowanie musi posiadać wbudowany system analityczny pozwalający na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).<br>• Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.<br>• Wbudowany system analityczny powinien obsługiwać wielojęzyczność, tworzenie obiektów wielowymiarowych w wielu językach, w zależności od ustawień na komputerze użytkownika.<br>• Oprogramowanie musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.<br>• Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).<br>• Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT<br>• Oprogramowanie musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie.<br>• licencje równoważne nie mogą zakłócić pracy środowiska systemowo - programowego Zamawiającego,<br>• W przypadku zaoferowania licencji równoważnych muszą one być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Microsoft SQL Server funkcjonującym u Zamawiającego |

***Przełącznik 24 portowy zarządzalny – 1 szt.***

| | |
|---|---|
| **Typ i liczba portów** | • 24 portów 10/100/1000BaseT RJ-45<br>• 4 porty 1/10G SFP+<br>• bufor pakietów – 6MB |
| **Zasilanie i chłodzenie** | • Zasilacz AC 230V. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)<br>• Redundantne wentylatory |

| | |
|---|---|
| **Parametry wydajnościowe** | • Przepustowość przełącznika zapewniająca pracę z pełną wydajnością wszystkich portów, w tym również dla pakietów 64-bajtowych (przełącznik line-rate)<br>• Pamięć DRAM – 2GB<br>• Pamięć flash – 4GB |
| **Obsługa** | • 500 sieci VLAN/interfejsów SVI |
| | • 16.000 adresów MAC<br>• 3.000 tras IPv4<br>• 1.500 tras IPv6<br>• Ilość wpisów w listach kontroli dostępu Security ACL – 1.500<br>• ilość wpisów w listach kontroli dostępu QoS ACL – 1.000 |
| **Mechanizmy związane z bezpieczeństwem sieci** | • Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)<br>• Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością:<br>- dynamicznego przypisania użytkownika do określonej sieci VLAN<br>- dynamicznego przypisania listy ACL<br>• Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X<br>• Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC<br>• Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X<br>• Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem<br>• Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176<br>• Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)<br>• Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard<br>• Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)<br>• Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+<br>• Obsługa list kontroli dostępu (ACL)<br>• Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika kluczami o długości 128-bitów (gcm-aes-128)<br>• Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)<br>• Funkcja Private VLAN |

| | |
|---|---|
| **Mechanizmy związane z zapewnieniem jakości usług w sieci** | • Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi<br>• Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)<br>• Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP<br>• Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi<br>• Kontrola sztormów dla ruchu broadcast/multicast/unicast<br>• Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie<br>IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP |
| **Obsługa protokołów i mechanizmów routingu** | • Routing statyczny dla IPv4 i IPv6<br>• Routing dynamiczny – RIP, OSPF, PIM Stub<br>• Policy-based routing (PBR)<br>• Obsługa protokołu redundancji bramy (VRRP) |
| **Zarządzanie** | • Port konsoli<br>• Dedykowany port Ethernet do zarządzania out-of-band<br>• Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją<br>• Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog<br>• Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów<br>• Obsługa protokołu gRPC Dial-Out i RESTCONF<br>• Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych<br>• Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą |

| | |
|---|---|
| | • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB<br>• Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie |
| **Montaż** | • Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU |
| **Wymagania dodatkowe** | • Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow)<br>• Możliwość rozszerzenia funkcjonalności przełącznika o możliwość stackowania z zapewnieniem następujących funkcjonalności:<br>- Przepustowość w ramach stosu - 80Gb/s<br>- 8 urządzeń w stosie<br>- Zarządzanie poprzez jeden adres IP<br>- Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad<br>• Obsługa protokołu NTP<br>• Obsługa IGMPv1/2/3 i MLDv1/2 Snooping<br>• Obsługa protokołu LLDP i LLDP-MED.<br>• Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC<br>• Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego<br>• Możliwość uruchomienia funkcji serwera DHCP<br>• Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:<br>- podpisywanie cyfrowe i weryfikację podpisu wszystkich komponentów programowych przełącznika (BIOS, firmware itp.)<br>- wyposażenie przełączników w bezpieczne, odporne na manipulacje układy kryptograficzne, gwarantujące uwierzytelnienie oryginalności sprzętu i jego jednoznaczną identyfikację<br>- bezpieczne uruchamianie (secure boot), zapewniające sprzętową weryfikację sekwencji startowej i uniemożliwiające uruchomienie nielegalnie zmodyfikowanego oprogramowania systemowego<br>• Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN<br>• Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)<br>• Możliwość rozszerzenia funkcjonalności przełącznika poprzez zakup i aktywację odpowiedniej licencji (bez konieczności modyfikacji sprzętowych) o:<br>- Wsparcie dla protokołu LISP zgodnie z RFC 6830<br>- Obsługę routingu IS-IS dla IPv4 i IPv6<br>- Routing multicastów - PIM-SM, PIM-SSM<br>- Multicast Source Discovery Protocol (MSDP)<br>- Możliwość enkapsulacji ruchu w pakiety VXLAN |

| | |
|---|---|
| **Gwarancje** | Urządzenie musi być objęty min. 36-miesięcznym (3 lata) serwisem opartym na serwisie producenta<br>urządzenia |

***Klaster urządzeń UTM – 2 szt.***

| | |
|---|---|
| **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.<br>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.<br>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji<br>systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. |
| | Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.<br>System wspiera protokoły IPv4 oraz IPv6 w zakresie:<br>• Firewall.<br>• Ochrony w warstwie aplikacji.<br>• Protokołów routingu dynamicznego. |
| **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.<br>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.<br>3. Monitoring stanu realizowanych połączeń VPN.<br>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:<br>• 16 portami Gigabit Ethernet RJ-45.<br>• 8 gniazdami SFP 1 Gbps.<br>• 2 gniazdami SFP+ 10 Gbps.<br>2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.<br>3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.<br>4. System jest wyposażony w zasilanie AC. |

| | |
|---|---|
| **Parametry wydajnościowe** | 1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.<br>2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.<br>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.<br>4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.<br>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.<br>6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.<br>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. |
| **Funkcje Systemu Bezpieczeństwa** | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:<br>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>2. Kontrola Aplikacji.<br>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>4. Ochrona przed malware.<br>5. Ochrona przed atakami - Intrusion Prevention System.<br>6. Kontrola stron WWW.<br>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.<br>8. Zarządzanie pasmem (QoS, Traffic shaping).<br>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).<br>10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.<br>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.<br>12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.<br>13. 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:<br>• Translację jeden do jeden oraz jeden do wielu.<br>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.<br>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.<br>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.<br>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.<br>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.<br>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.<br>• Amazon Web Services (AWS).<br>• Microsoft Azure.<br>• Cisco ACI.<br>• Google Cloud Platform (GCP).<br>• OpenStack.<br>• VMware NSX.<br>• Kubernetes. |
| **Połączenia VPN** | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:<br>• Wsparcie dla IKE v1 oraz v2.<br>• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).<br>• Obsługa protokołu Diffie-Hellman grup 19, 20.<br>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.<br>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.<br>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.<br>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.<br>• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.<br>• Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.<br>• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.<br>• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.<br>• Mechanizm „Split tunneling” dla połączeń Client-to-Site.<br>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:<br>• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. |

| | |
|---|---|
| | • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.<br>• 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:<br>1. Routingu statycznego.<br>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).<br>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.<br>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.<br>5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.<br>6. BFD (Bidirectional Forwarding Detection).<br>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.<br>2. System daje możliwość określania pasma dla poszczególnych aplikacji.<br>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.<br>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).<br>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.<br>3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.<br>4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.<br>5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>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 chmurze.<br>8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.<br>9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.<br>10. 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.<br>2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.<br>3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).<br>7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.<br>8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.<br>9. 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.<br>2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.<br>4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.<br>6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).<br>7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |

| | |
|---|---|
| **Kontrola WWW** | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.<br>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.<br>3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.<br>4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.<br>5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).<br>6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.<br>7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.<br>8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.<br>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:<br>• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.<br>• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.<br>• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.<br>2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.<br>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.<br>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.<br>2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.<br>3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.<br>4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.<br>5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.<br>6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.<br>7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.<br>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).<br>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.<br>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.<br>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.<br>4. Możliwość włączenia logowania per reguła w polityce firewall. |

| | |
|---|---|
| | 5. System zapewnia możliwość logowania do serwera SYSLOG.<br>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 oraz wykonane testy. |
| **Gwarancja oraz wsparcie** | System objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

***Serwerowa szafa Rack 42U – 1 szt.***

| | |
|---|---|
| **Wielkość** | Minimum 42U |
| **Perforacja** | Wymagana przednia i tylna perforacja |

***UPS – 1 szt***

| | |
|---|---|
| **Moc pozorna** | minimum 5000 VA |
| **Moc rzeczywista** | minimum 4500 W |
| **Architektura UPSa** | on-line |
| **Typ obudowy** | Rack 3U, Z urządzeniem dostarczone elementy wymagane do instalacji w szafie RACK 19” |
| **Liczba, typ gniazd wyj. Z podtrzymaniem zasilania i ochroną przepięciową** | minimum 6 x IEC320 C13 (10A)<br><br>minimum 4 x IEC320 C19 (16A) |
| **Typ gniazda wejściowego** | Zaciski 3 przewodowe |
| **Segmentacja gniazd odbiorów** | Gniazda odbiorcze podzielone muszą być na co najmniej dwa segmenty, których sterowanie odbywać się powinno za pomocą dołączonego oprogramowania. Każdy segment winien umożliwiać pomiar energii. |

| | |
|---|---|
| **Topologia** | Double Conversion Online |
| **Kształt napięcia wyjściowego przy pracy bateryjnej** | Sinusoidalny |
| **Częstotliwość wejściowa** | 40 – 70 Hz |
| **Czas podtrzymania dla 100% obciążenia** | minimum 3 min 50sek |

| | |
|---|---|
| **Czas podtrzymania dla 50% obciążenia** | minimum 11min 30sek |
| **Poziom hałasu** | < 56 dBA |
| **Zakres napięcia wejściowego** | 120 – 275 V |
| **Baterie wymieniane przez użytkownika „na gorąco" od frontu UPS** | Tak |
| **Wyświetlacz informacyjny** | LCD instalowany na froncie<br>Z możliwością zmiany konta instalacji o 90 stopni (w przypadku instalacji w pionie) |
| **Interfejs komunikacyjny** | • port USB i RS232 |
| | • port zdalnego włączania i wyłączania awaryjnego EPO |
| | • port przekaźnikowy |
| | • gniazdo karty SNMP/Web (RJ-45) |
| **Wyposażenie standardowe** | • kable sygnałowe USB i RS232 |
| | • kabel odbiorów 1.8m IEC320 C13/C14 – min. 2 szt. |
| | • zestaw montażowy do szafy 19" |
| **Karta SNMP** | • cyberbezpieczeństwo (szyfry TLS, MQTT) |
| | • certyfikaty CA i PKI |
| | • prędkość gigabit'owa (half-duplex, full-duplex) |
| | • różne poziomy nadawania dostępu do konta administratora lub użytkownika |
| **Dodatkowe funkcje karty do zarządzania** | Dostęp przez przeglądarkę, zdalne restartowanie sprzętu, monitorowanie temperatury, zdalne zarządzanie urządzeniem, rejestracja zdarzeń |
| **Oprogramowanie** | Monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie systemów komputerowych, pozwalające na integrację z platformą wirtualizacyjną Hyper-V, Windows. |
| **Czujniki** | Dołączony czujnik temperatury |

| | |
|---|---|
| **Zimny start** | tak |
| **Maksymalny ciężar** | 55 kg |
| **Cechy** | Możliwość wydłużenia czasu podtrzymania do minimum 190 min. Przy 100% obciążeniu poprzez dołączenie baterii zewnętrznych |
| **Gwarancja, co najmniej** | 36 miesięcy na urządzenie oraz min. 24 miesiące na baterię |
| **Certyfikaty** | Urządzenie musi posiadać deklaracje CE. |

**Moduł bateryjny zgodny z UPS**

| | |
|---|---|
| **Typ obudowy** | Rack 3U, Z urządzeniem dostarczone elementy wymagane do instalacji w szafie RACK 19” |
| **Napięcie akumulatora** | 192V |
| **Czas podtrzymania zestawu (UPS + moduł) dla 100% obciążenia** | Minimum 20min 20sek |
| **Czas podtrzymania zestawu (UPS + moduł) dla 50% obciążenia** | minimum 46min |
| **Maksymalny ciężar** | 91kg |
| **Gwarancja, co najmniej** | min. 24 miesiące |

***Zewnętrzny agregat prądotwórczy – 1 szt.***

| | |
|---|---|
| **Wymagania ogólne** | - agregat fabrycznie nowy<br>- moc podstawowa zespołu prądotwórczego PRP: 30 kVA / 24 kW<br>- moc rezerwowa Stand-by ESP: 33 kVA / 26 kW<br>- napięcie: 400V / 230V<br>- ilość faz: 3<br>- częstotliwość: 50 Hz<br>- wersja obudowana szczelnie wyciszona o poziomie hałasu LP (dBA) nie większym niż: 65 dBA z 7m,<br>- akumulatory rozruchowe<br>- prostownik buforowy akumulatorów rozruchowych, zapewniający odpowiedni do rozruchu<br>poziom naładowania akumulatorów w czasie postoju zespołu prądotwórczego<br>- FLS,<br>- komunikacja MODBUS, możliwość współpracy z BMS<br>- elektroniczny panel sterowania typ TJ509MK3 – menu w j. polskim<br>- fabryczny zbiornik paliwa 90 l w podstawie agregatu,<br>- zużycie paliwa nie większe niż 7,6 l/h przy 100% obciążenia PRP agregatu<br>- max wymiary agregatu (długość x szerokość x wysokość): 2200 x 950 x 1450 mm; przy czym rama na której jest posadowiony agregat na podłożu |

| | |
|---|---|
| | o wymiarach nie większych niż (długość x szerokość): 1650 x 950 mm<br>- gwarancja producenta 24 miesiące |
| **Silnik** | - diesel ,<br>- liczna cylindrów/konfiguracja: 4 / rzędowy<br>- pojemność 2,3L<br>- wysokoprężny z turbodoładowaniem |

| | |
|---|---|
| | - stopień sprężania 17,5:1<br>- chłodzony cieczą, z grzałką cieczy chłodzącej podgrzewającą płyn podczas postoju zespołu prądotwórczego,<br>- elektroniczna regulacja obrotów |
| **Prądnica** | - napięcie 400/230 V, 3-fazowa 50Hz<br>- bezszczotkowa, samowzbudna, samoregulująca, synchroniczna, z wewnętrznymi obwodami tłumiącymi<br>- klasa izolacji: H<br>- sprzęgnięta bezpośrednio z silnikiem<br>- współczynnik cos fi >= 0,8<br>- system wzbudzania AVR<br>- regulacja napięcia (stan ustalony) ± 1%<br>- sprawność do 87 %<br>- stopień ochrony IP23<br>- całkowite THD < 2,5 % |
| **Układ chłodzenia** | - podstawowy napęd wentylatora chłodnicy – mechaniczny przenoszony z wału silnika<br>- kratka zabezpieczająca wentylator i wirujące części<br>- posiada zabezpieczające osłony termiczne na elementach o wysokiej temperaturze |
| **Automatyka /Sterowanie agregatem/Zabezpieczenia** | Panel sterowania z kontrolerem oparty na mikroprocesorze umożliwia monitorowanie i kontrole stanów pracy agregatu. Panel LCD z wyświetlanymi komunikatami w języku polskim. Panel posiadający funkcję współpracy z SZR-em oraz funkcję badania stanu sieci zasilającej. Panel z możliwością współpracy z BMS w tym poprzez protokół RS 232 oraz MODBUS (RS485) |
| **Podstawowe właściwości** | - sterowanie ręczne<br>- sterowanie automatyczne<br>- wyłącznik awaryjny<br>- zasilanie akumulatorowe<br>- zapisywanie zdarzeń urządzenia minimum 200 ostatnich<br>- elektroniczna kontrola i monitoring silnika przez J1939 CAN<br>- wskaźniki alarmowe oraz ostrzegawcze<br>- wskaźnik o wykonaniu przeglądu |
| **Pomiary wyświetlane na panelu** | - pomiar napięcia fazowego, międzyfazowego i częstotliwości agregatu<br>- pomiar natężenia prądu agregatu na każdej fazie<br>- pomiar napięcia fazowego, międzyfazowego i częstotliwości podstawowego źródła zasilania<br>- pomiar napięcia baterii<br>- pomiar całkowitej mocy czynnej i pobieranej dla każdej z faz agregatu<br>- pomiar współczynnika mocy<br>- pomiar ciśnienia oleju<br>- pomiar temperatury płynu chłodzącego<br>- pomiar prędkości obrotowej<br>- % odczyt poziomu paliwa |

| | |
|---|---|
| **Ostrzeżenia i alarmy wyświetlane przez panel:** | - niskie / wysokie obroty,<br>- niska / wysoka temperatura płynu chłodzącego,<br>- niski poziom płynu chłodzącego<br>- niskie ciśnienie oleju,<br>- wysoka temperatura oleju,<br>- niskie / wysokie napięcie wyjściowe agregatu,<br>- nieprawidłowa kolejność wirowania faz,<br>- awaria alternatora silnika napędowego / zerwany pasek klinowy,<br>- niskie / wysokie napięcie DC baterii akumulatorów rozruchowych,<br>- błąd zatrzymania,<br>- przeciążenie<br>- awaryjny przycisk zatrzymujący<br>- konieczny serwis |

4