**Załącznik nr 8 do SIWZ**

# SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu IT/ICT dla projektu pn. "Partnerstwo na rzecz e-integracji w makroregionie śląsko-opolskim" dofinansowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa nr 3 „Cyfrowe kompetencje społeczeństwa" Działanie nr 3.1 „Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych".

## Serwer – 1 szt.

| LP | Parametr lub warunek | Minimalne wymagania |
|---|---|---|
| 1 | Obudowa | • Typu Rack, wysokość maksimum 2U;<br>• Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack; |
| 2 | Płyta główna | • Dwuprocesorowa, możliwość instalacji procesorów 28-rdzeniowych;<br>• Minimum 6 złącz PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16 i 3 złącza o prędkości x8;<br>• Wszystkie złącza PCI Express muszą być aktywne;<br>• Możliwość zainstalowania dwóch kart microSD o pojemności min. 64 GB każda przeznaczone dla wirtualizatora;<br>• Możliwość zintegrowania układu TPM z płyta główną; |
| 3 | Procesory | • Zainstalowane dwa procesory osiągające wynik w testach wydajności CPU2017 Integer Rates min. 73,7 pkt dla dowolnej platformy dwuprocesorowej producenta serwera, który jest oferowany w przedmiotowym postępowaniu. Wymagamy, aby był załączony PDF ze strony spec.org. |
| 4 | Pamięć RAM | • Zainstalowane 64 GB pamięci RAM w kościach o pojemności 32 GB;<br>• Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC;<br>• Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing";<br>• Minimum 24 gniazda pamięci RAM na płycie głównej, obsługa minimum 1536GB pamięci RAM; |
| 5 | Kontrolery dyskowe, I/O | • Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,10,50, min. 1GB pamięci cache |
| 6 | Dyski twarde | • Zainstalowane 6 dysków twardych 600GB;<br>• Minimum 8 wnęk dla dysków twardych Hotplug 2,5 (możliwość rozbudowy do minimum 16 wnęk); |
| 7 | Inne napędy zintegrowane | • Możliwość instalacji wewnętrznego napędu LTO-6 SAS lub LTO-7 SAS.<br><br>Alternatywnie dopuszcza się zaoferowanie dodatkowej obudowy rack max 1U dla napędu LTO6/7 wyposażonej w nadmiarowe zasilacze hotplug i okablowanie oraz dostarczenie oferowanego serwera wraz z zainstalowanym kontrolerem SAS HBA umożliwiającym podłączenie i poprawną pracę oferowanej obudowy wyposażonej w napęd LTO-6 lub LTO-7 z oferowanym serwerem; |
| 8 | Kontrolery LAN | • Wbudowana w płytę główną karta 2x1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;<br>• Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x1Gbit/s; |

| | | |
|---|---|---|
| | | • Karta LAN musi umożliwiać wymianę interfejsów na interfejsy: 2x 10Gbit/s SFP+ / 2x 10GBit/s RJ-45 / 4x10Gbit/s SFP+ bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express; |
| 10 | Porty | • karta graficzna ze złączem VGA;<br>• 2x USB 3.0 dostępne na froncie obudowy<br>• 2x USB 3.0 dostępne z tyłu serwera<br>• 1x USB 3.0 wewnątrz serwera<br>• Możliwość wyposażenia w port RS-232-C (możliwość wykorzystania przez kartę zarządzającą serwera);<br><br>Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; |
| 11 | Zasilanie, chłodzenie | • Redundantne zasilacze hotplug o mocy maksimum 800W, o sprawności 94%<br>• Redundantne wentylatory hotplug; |
| 12 | System operacyjny | • licencje dla 25 użytkowników;<br>• dodatkowo 3 szt. licencji RD. |
| 13 | Zarządzanie | • Wbudowane diody informacyjne informujące o stanie serwera;<br>• Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:<br>o Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;<br>o Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;<br>o Dostęp poprzez przeglądarkę Web (także SSL, SSH)<br>o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii<br>o Zarządzanie alarmami (zdarzenia poprzez SNMP)<br>o Możliwość przejęcia konsoli tekstowej<br>o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)<br>o Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych)<br>o Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 8Gbit/s)<br>o Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).<br>o Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB<br>o Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB);<br>o Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; |

Projekt „Partnerstwo na rzecz e-integracji w makroregionie śląsko-opolskim jest realizowany w ramach Programy Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa nr 3 „Cyfrowe kompetencje społeczeństwa" Działanie nr 3.1 „Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych"

| | | |
|---|---|---|
| | | ○ Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;<br>○ Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji;<br>○ Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);<br>○ Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;<br>○ Karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania serwisu o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego w systemie). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji; |
| 14 | Wspierane OS | Windows 2016 Hyper-V, Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL |
| 15 | Gwarancja | • Minimum 2 lata gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki<br>• W przypadku wymiany dysków twardy pozostają u Zamawiającego;<br>• Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;<br>• Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji takowa licencja musi być uwzględniona w konfiguracji; |
| 16 | Dokumentacja, inne | • Elementy, z których zbudowane są serwery muszą być objęte gwarancją o wymaganym w specyfikacji poziomie SLA.<br>• Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce;<br>• Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;<br>• Ogólnopolska, telefoniczna infolinia/linia techniczna (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;<br>• Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www; |

Projekt „Partnerstwo na rzecz e-integracji w makroregionie śląsko-opolskim jest realizowany w ramach Programy Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa nr 3 „Cyfrowe kompetencje społeczeństwa" Działanie nr 3.1 „Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych"

## Zasilanie awaryjne – UPS – 1 szt.

| **PARAMETRY\TYP** | **Wymagania minimalne** |
|---|---|
| Moc wyjściowa (pozorna / czynna) | minimum 3000 VA |
| | minimum 3000 W |
| **DANE OGÓLNE I ŚRODOWISKOWE** | |
| Topologia | VI (line interactive) |
| Typ obudowy | Rack/Tower |
| Chłodzenie | Wymuszone, wewnętrzne wentylatory |
| WEJŚCIE | |
| Napięcie znamionowe (wartość skuteczna) | 230 V AC |
| Zakres napięcia wejściowego (wartości skuteczne) i tolerancja | 178 ÷ 281 V AC ± 2 % |
| Częstotliwość znamionowa napięcia wejściowego | 50 Hz |
| Zakres częstotliwości i tolerancja | 45 ÷ 55 Hz ± 1 Hz |
| Progi przełączania: sieć – UPS | 178 ÷ 281 V AC ± 2 % |
| WYJŚCIE | |
| Napięcie znamionowe (wartość skuteczna) | 230 V AC |
| Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa | 195 ÷ 253 V AC ± 2 % |
| Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa | 230 V AC ± 5 % |
| Automatyczna regulacja napięcia (AVR) | ± 10 % |
| Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej) | Sinusoidalny / Tak jak na wejściu |
| Częstotliwość znamionowa napięcia wyjściowego | 50 Hz |
| Filtracja napięcia wyjściowego | Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy |
| Progi przełączania: UPS – sieć | 183 ÷ 276 V AC ± 2 % |
| Czas przełączenia na pracę rezerwową | < 3 ms |
| Czas powrotu na pracę sieciową | 0 ms |
| Przeciążalność | > 105% - 15 s (wyłączenie UPS) |
| **AKUMULATORY I CZASY PODTRZYMANIA** | |
| Akumulatory wewnętrzne | minimum 8x 12 V / 7 Ah VRLA |
| możliwość podpięcia modułów bateryjnych | wymagane minimum 1szt |
| Czas podtrzymania z baterii wewnętrznych (80 % / 50 % Pmax) | minimum 4 / 7 min |
| Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza). | do 4 h |
| **PARAMETRY MECHANICZNE** | |
| Wymiary – Rack (wys. X szer. X gł.) | nie większe niż 132 x 440 x 630 mm |
| Masa zasilacza | nie większa niż 43 kg |
| **ZABEZPIECZENIA** | |
| Zabezpieczenie wejściowe | Przeciwzwarciowe – Bezpiecznik automatyczny |
| | 16 A / 250 V AC |
| | Przeciwprzepięciowe |
| Zabezpieczenie wyjściowe | Elektroniczne – przeciwzwarciowe i przeciążeniowe |
| Zabezpieczenia wejścia DC (akumulatory wewnętrzne) | Zabezpieczenie nadprądowe |
| Zabezpieczenia DC (zewnętrzny moduł bateryjny) | Zabezpieczenie nadprądowe |

| | |
|---|---|
| **WYPOSAŻENIE I FUNKCJE DODATKOWE** | |
| Przyłącze zasilania UPS | 1 x IEC 320 C20 (16 A) |
| Przyłącza wyjściowe (liczba i typ gniazd) | minimum 6 x IEC320 C13 (10 A) |
| | minimum 1 x IEC320 C19 (16 A) |
| | minimum 2 x PL (z bolcem uziemiającym) |
| Sygnalizacja | Akustyczno – optyczna; graficzny wyświetlacz LCD, dioda LED |
| Interfejsy komunikacyjne | USB HID, SNMP/HTTP |
| Gniazdo na dodatkowe karty rozszerzeń | wymagane minimum 1 wolne gniazdo |
| Filtr teleinformatyczny (linii danych) – RJ45 | LAN 1 Gbit/s |
| Wsporniki do montażu w szafie RACK | wymagane |
| Oprogramowanie monitorująco-zarządzające | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS. |
| | możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP) |
| | możliwość edycji nazw urządzeń na liście monitorowanych UPSów |
| | wymagane wsparcie (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. |
| | wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer |
| Możliwość aktualizacji oprogramowania firmware przez użytkownika | wymagane |
| **ZASTOSOWANE STANDARDY** | |
| Deklaracje | CE |
| Normy | PN-EN 62040-1:2009, PN-EN 62040-2:2008 lub równoważne |
| **GWARANCJA/SERWIS** | |
| Gwarancja | min 24 miesiące na elektronikę i na akumulatory; serwis realizowany w systemie door to door |
| **DODATKOWE OŚWIADCZENIA/DOKUMENTY** | |
| | ISO 9001:2015 lub równoważny dla obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań |
| | karta katalogowa oferowanego sprzętu |

## Laptopy – 30 szt.

| | |
|---|---|
| Ekran | • 10-punktowa matryca o przekątnej minimum 10" z podświetleniem LED, rozdzielczość minimum 1800 x 1200, (217PPI), kontrast minimum 1500:1; jasność min. 415 cd/m2. Zintegrowana z obudową ekranu kamera przednia minimum 5.0MP, oraz tylna o rozdzielczości minimum 8.0MP z autofokusem i obsługą 1080p Full HD. |
| Obudowa | • Obudowa z możliwością dołączania/odłączania klawiatury. Wbudowana podstawka pozwalająca na ustawienie urządzenia na podłożu pod wybranym kątem.<br>• Wymiary maksymalne: 250mm x 180 mm x 9mm |

| | |
|---|---|
| Procesor | Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny na stronie internetowej: https://www.cpubenchmark.net/cpu_list.php) co najmniej wynik 2150 punktów Passmark CPU Mark |
| BIOS | Musi posiadać:<br>• BIOS zgodny ze specyfikacją UEFI.<br>• Możliwość odczytania z BIOS informacji o:<br>  ○ wersji BIOS,<br>  ○ nr seryjnego komputera,<br>  ○ Funkcja blokowania/odblokowania BOOT-owania urządzenia z zewnętrznych urządzeń,<br>  ○ Funkcja blokowania/odblokowania BOOT-owania urządzenia z USB<br>• Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora |
| Pamięć RAM | Co najmniej 4GB. |
| Dysk twardy | min. 64GB |
| Dźwięk | • Mikrofon<br>• 2W głośniki |
| Porty/złącza | Minimum:<br>• 1x USB-C<br>• 1x złącze stacji dokującej<br>• 1x microSDXC card reader<br>• 1x 3,5mm Headphone jack<br>• 1x złącze klawiatury |
| Wbudowane karty sieciowe | • Wi-Fi:<br>• IEEE 802.11 a/b/g/n/ac kompatybilne z technologią Bluetooth Wireless 4.1<br>• GPS |
| Wbudowane urządzenia | • kamera przednia umożliwiająca autentykacje użytkownika<br>• czujnik światła<br>• kamera przednia o rozdzielczości minimum 5 MP<br>• kamera tylna o rozdzielczości minimum 8 MP z automatycznie ustawianą ostrości<br>• mikrofon z redukcją szumów<br>• 2 głośniki stereo<br>• Akcelerometr<br>• Żyroskop<br>• NFC. |
| Klawiatura | Klawiatura w układzie QWERTY z podświetleniem od spodu klawiszy umożliwiającym pracę przy całkowicie zaciemnionym pomieszczeniu, z możliwością wielkokrotnego podłączania i odłączenia od urządzenia. |
| Bateria\Zasilanie | • Czas pracy na baterii wg producenta 9 godzin.<br>• Zasilacz zewnętrzny 110-240 V, |

| | |
|---|---|
| System operacyjny | System operacyjny w wersji polskiej nie wymagający aktywacji za pomocą telefonu lub Internetu. Zainstalowane oprogramowanie z bezterminową licencją do wykonywania aktualizacji systemu i jego zasobów umożliwiające:<br>• określenie preferencji aktualizacji<br>• ustawienie priorytetu aktualizacji<br>• użycia opcji planowania aktualizacji bieżących wersji sterowników,<br>Zainstalowane oprogramowanie z bezterminową licencją dedykowane do ochrony danych i systemu zapewniające:<br>• wykrywanie zagrożeń bezpieczeństwa danych<br>• ochronę danych poprzez egzekwowanie polityki kontroli dostępu, uwierzytelnienie i szyfrowanie poufnych danych<br>• automatyczną aktualizację urządzeń i śledzenie zmian dla urządzeń chronionych.<br>Zainstalowane oprogramowanie z bezterminową licencją tworzenia kopii zapasowych i przywracania danych, umożliwiające:<br>• tworzenie kopii zapasowych na podstawie harmonogramu<br>• tworzenie OS media<br>• tworzenie kopii zapasowych na wskazanych przez użytkownika lokalizacjach [ min. lokalnie, sieć, chmura]<br>Ważna uwaga: Zamawiający nie dopuszcza stosowania emulatorów ani środowisk wirtualnych do uruchomienia wymienionego wcześniej oprogramowania.<br>Zamawiający jednocześnie wymaga umożliwienia:<br>• Łączenia z sieciami firmowymi przy użyciu funkcji przyłączania do domeny |
| Bezpieczeństwo | Zaimplementowany i uruchamiany z BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. |
| inne | Możliwość dołączenia aktywnego rysiku/piórka do ekranu dotykowego, zasilanego baterią AAAA, z minimum 4096 poziomami nacisku, wymiennymi końcówkami, działający w technologii BT 4.0 LE z przyciskami funkcyjnymi konfigurowanymi z poziomu systemu operacyjnego, magnetycznie mocowany do obudowy urządzenia |
| Wsparcie techniczne producenta | Ogólnopolska, telefoniczna infolinia/linia techniczna dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:<br>• weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć),<br>• czasu obowiązywania i typ udzielonej gwarancji.<br>Posiada możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania lub bezpośrednio z sieci Internet za pośrednictwem strony www po podaniu numeru seryjnego komputera lub modelu komputera.<br>Posiada możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www. |
| Gwarancja | Czas trwania gwarancji: minimum 2 lata. |

## Szafa typu RACK – 1 szt.

| | |
|---|---|
| **Wysokość wewnętrzna** | 27U |
| **Typ szafy rack** | Stojąca |
| **Rodzaj drzwi** | Szklane |
| **Możliwość zdejmowania paneli bocznych** | Tak |
| **Obciążalność** | Nie mniej niż 500 kg |
| **Wysokość** | Nie mniej niż 1190 mm |
| **Głębokość szafy** | Nie mniej niż 1000 mm |
| **Szerokość szafy** | Nie mniej niż 600 mm |
| **Inne** | Drzwi boczne demontowane są na zatrzaskach z możliwością montażu zamka, kółka, stopki do regulacji wysokości, dodatkowa półka rack |
| **Grubość materiału** | Rama, góra, dół, przednie drzwi, tylne drzwi, boczne drzwi: 1,2 mm |
| **Szyny poziome** | 1,5 mm |
| **Szyny pionowe** | 2,0 mm |
| **Gwarancja** | Minimum 2 lata |
| **Drzwi przednie** | Przeszklone z zamkiem, wentylowane, wykonane z blachy stalowej z wklejoną szybą hartowaną |
| **Drzwi tylnie** | Stalowe z zamkiem, wentylowane |
| **Wentylatory** | Panel 4 wentylatorów do instalacji w płucie górnej szafy |

## Firewall – 1 szt.

1. Zapora sieciowa typu Next Generation Firewall (NGFW)
2. Mechanizm pozwalający na dwustronną analizę ruchu.
3. Minimalna ilość interfejsów:
    a. 10 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.
    b. 2 interfejsy USB dla przyszłych potrzeb i do podłączenia modemu 3G
    c. 1 interfejs konsoli do zarządzania zaporą
    d. 1 slot rozszerzający
4. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
5. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji
6. Możliwość utworzenia przynajmniej 50 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
7. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
8. Minimalna ilość jednocześnie obsługiwanych połączeń: 150 000
9. Możliwość obsłużenia przynajmniej 12 000 nowych połączeń w ciągu 1 sekundy.
10. Przepustowość urządzenia pracującego w trybie stateful firewall: 1.5 Gbps – dla ramki 1518B zgodnie z RFC 2544
11. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1.1 Gbps
12. Przepustowość urządzenia pracującego jako koncentrator VPN: 1.1 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544

13. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń, jeśli chodzi o wielkość skanowanych plików) – 500 Mbps
14. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 50
15. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 25.
16. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.
17. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 200 Mbps.
18. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP
19. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)
20. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa)
21. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
22. Wsparcie dla Dynamicznego DNS tzw. DDNS
23. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
24. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate lub równoważne (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).
25. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
    a. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron)
    b. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony
    c. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
26. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps
27. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
28. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec

VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.

29. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
30. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)
31. Kontrola dostępności zestawionych tuneli VPN
32. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
33. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
34. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
35. Funkcja NAT oparta o reguły bezpieczeństwa.
36. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
37. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
38. Zintegrowany system skanowania antyspyware
39. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
40. System IPS musi używać algorytmu szeregowego przetwarzania.
41. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
42. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji
    a. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
    b. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur
    c. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
43. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
44. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa

45. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi
46. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p
47. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń
48. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 3 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Licencja na tą funkcjonalność nie jest przedmiotem przetargu, ale urządzenie powinno zapewniać taką funkcjonalność w celu późniejszej rozbudowy systemu.
49. Dodatkowe: Zamawiający wymaga dostarczenia wraz z Firewall funkcjonalności Web application firewall (WAF) o parametrach nie gorszych niż:
    a. System WAF powinien funkcjonować na zasadzie reverse-proxy oraz powinien umożliwiać automatyczne zrywanie wygasłych sesji z użytkownikiem.
    b. System musi mieć możliwość realizacji równoważenia (load balancingu) połączeń do serwerów aplikacyjnych z możliwością badania stanu aplikacji webowej.
    c. Ochrona aplikacji webowych przed głównymi dziesięcioma atakami zdefiniowanymi przez OWASP Foundation (Open Web Application Security Protection) takimi jak SQL Injection, XSS/CSRF itp.
    d. Ochrona przed wyciekiem informacji poufnych prezentowanych przez aplikacje webowe takich jak np. numery kart kredytowych.
    e. Wsparcie mechanizmu HSTS – HTTP Strict Transport Security
    f. Integracja z serwisem Let's Encrypt umożliwiająca zarządzanie certyfikatami aplikacji. Funkcjonalność powinna umożliwiać monitorowanie, wydawanie i odnawianie certyfikatów z poziomu konsoli systemu WAF.
    g. Możliwość dołożenia uwierzytelniania dwuskładnikowego do aplikacji, która natywnie nie wspiera dodatkowych mechanizmów uwierzytelniania.
    h. Pełne zarządzanie systemem z poziomu graficznego interfejsu użytkownika (GUI)
    i. Możliwość wysyłania logów do zewnętrznych serwerów syslog
    j. System powinien zostać dostarczony jako wirtualna maszyna ze wsparciem hypervisora ESX oraz HyperV
    k. System nie powinien posiadać ograniczeń licencyjnych, jeśli chodzi o ilość zasobów sprzętowych jakie możemy przypisać do maszyny wirtualnej i wykorzystać przez WAF.
    l. System powinien zapewnić licencje zapewniające ochronę jednej aplikacji, do której miesięczny sumaryczny transfer (z i do aplikacji) może wynosić 10GB.
    m. Powinny zostać dostarczone wsparcie techniczne oraz gwarancja i niezbędne licencje na wymienione cechy funkcjonalne na okres 3 lat.

**Wymagane licencje:**

1. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji oraz zapewnienie wsparcia technicznego 24x7 na okres minimum 3 lat.

**Switch - 1 szt.**

**Przełącznik dostępowy 48 portowy z POE wraz 4 portami SFP+**

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 1G 10/100/1000BASE-T oraz dodatkowo minimum 4 porty 1/10 Gigabit Ethernet SFP+
2. Przełącznik musi być wyposażony w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3at oraz 802.3af
3. Przełącznik musi zapewniać, standard 802.3at jednocześnie na wszystkich 48 portach 1G 10/100/1000BASE-T
4. Przełącznik ma oferować zgodnie ze standardem 802.3af jednocześnie na wszystkich 48 portach 1G 10/100/1000BASE-T np. poprzez zastosowanie dodatkowego źródła zasilania
5. Przełącznik musi mieć możliwość doposażenia w system redundantnego zasilania zapewniający normalną pracę urządzenia oraz zasilanie dla wszystkich portów PoE
6. Przełącznik musi obsługiwać optykę 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-LRM
7. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T
8. Wysokość urządzenia 1U
9. Przełącznik musi posiadać wbudowany zasilacz 230V AC
10. Nieblokującą architekturę o wydajności przełączania minimum 175 Gb/s
11. Szybkość przełączania minimum 130 Milionów pakietów na sekundę
12. Łączenie do 8 przełączników w stos
13. Realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych
14. Tablica MAC adresów minimum 16k
15. Pamięć operacyjna: minimum 1GB pamięci DRAM
16. Pamięć flash: minimum 2GB pamięci Flash
17. Pojemność bufora pakietów minimum 2MB
18. Obsługa sieci wirtualnych IEEE 802.1Q – minimum 4000
19. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
20. Wsparcie dla ramek Jumbo Frames (minimum 9216 bajtów)
21. Obsługa Q-in-Q IEEE 802.1ad
22. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym

Projekt „Partnerstwo na rzecz e-integracji w makroregionie śląsko-opolskim jest realizowany w ramach Programy Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa nr 3 „Cyfrowe kompetencje społeczeństwa" Działanie nr 3.1 „Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych"

23. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
24. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
25. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
26. Wbudowany DHCP serwer i klient
27. Instalacja minimum dwóch wersji oprogramowania – firmware
28. Przechowywanie minimum kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
29. Monitorowanie zajętości CPU
30. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
31. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.

Obsługa Routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding
2. Pojemność tabeli routingu minimum 450 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
    a. RIPv1/v2
    b. OSPFv2–możliwość rozszerzenia przez licencję oprogramowania
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4

Obsługa Routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding
2. Pojemność tabeli routingu minimum 225 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
5. Obsługa MLDv1 (Multicast Listener Discovery version 1)
6. Obsługa MLDv2 (Multicast Listener Discovery version 2)
7. Policy Based Routing dla IPv6
8. Obsługa DHCP/BootP Relay dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

Obsługa Multicastów

1. Statyczne przyłączenie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa Multicast VLAN Registration – MVR
4. Obsługa IGMP v1 (RFC 1112)
5. Obsługa IGMP v2 (RFC 2236)
6. Obsługa IGMP v3 (RFC 3376)
7. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo

1. Obsługa Network Login
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
2. Obsługa wielu klientów (minimum 4) Network Login na jednym porcie (Multiple supplicants)
3. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
4. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
6. Obsługa Guest VLAN dla IEEE 802.1x
7. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
8. Wbudowana obrona procesora urządzenia przed atakami DoS
9. Obsługa TACACS+ (RFC 1492)
10. Obsługa RADIUS Authentication (RFC 2138) (RFC 2865)
11. Obsługa RADIUS Accounting (RFC 2139) (RFC 2866)
12. RADIUS and TACACS+ per-command Authentication
13. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
14. Funkcja wyłączenia MAC learning
15. Obsługa SNMPv1/v2/v3
16. Klient SSH2
17. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
18. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
19. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
20. Obsługa bezpiecznego transferu plików SCP/SFTP
21. Obsługa DHCP Option 82
22. Obsługa Gratuitous ARP Protection
23. Obsługa Trusted DHCP Server
24. Obsługa DHCP Snooping
25. Obsługa DHCP Secured ARP/ARP Validation
26. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x
27. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s

Bezpieczeństwo sieciowe

1. Konfiguracja portu głównego i zapasowego
2. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
6. Obsługa PVST+
7. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
8. Obsługa G.8032
9. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów

Zarządzanie

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
2. Obsługa synchronizacji czasu NTP
3. Zarządzanie przez SNMP v1/v2/v3
4. Zarządzanie przez przeglądarkę WWW – protokół http i https
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON minimum 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)

Inne

1. Obsługa skryptów CLI
2. Edycja skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
3. Uruchamianie skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym
4. Gwarancja: nie mniej niż 2 lata