*Załącznik nr 2 do SIWZ*

**FORMULARZ OFERTOWY**

Nazwa i adres Wykonawcy:

...............................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................

Tel………………………..……Fax. …………..…………..E-mail ……….....………………E-puap …………………………………..…

NIP:……………………………………… REGON:………………………………………… KRS /CEiDG……………………………………

W odpowiedzi na ogłoszenie o prowadzonym przez Urząd Państwowej Komisji do spraw wyjaśniania przypadków czynności skierowanych przeciwko wolności seksualnej i obyczajności wobec małoletniego poniżej lat 15 postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego nazakup i dostawę sprzętu komputerowego wraz z oprogramowaniem komputerowym składamy niniejszą ofertę ofertując wykonanie przedmiotu zamówienia zgodnie z warunkami SIWZ :

Za cenę:

brutto………………………………………………...…………………………………………

słownie ……………………………………………………………………………………………………..…..……w tym podatek VAT .

Zaoferowana cena wynika z następującej kalkulacji:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp | Nazwa pozycji | Ilość szt. | Cena brutto za 1 szt. | Cena brutto razem | Nazwa producenta, marka, model sprzętu/ nazwa producenta oprogramowania i jego nazwa (pełna nazwa produktu) |
| 1. | Serwer | 3 |  |  |  |
| 2. | Macierz | 1 |  |  |  |
| 3. | Szafa RACK 48 U | 1 |  |  |  |
| 4.  | Listwy zasilające do Szafy RACK | 4 |  |  |  |
| 5. | Konsola KVM | 1 |  |  |  |
| 6. | UPS | 1 |  |  |  |
| 7. | Switch szkieletowy 24 10G | 2 |  |  |  |
| 8. | Switch biurowy 48 1G POE | 2 |  |  |  |
| 9. | Access Point | 6 |  |  |  |
| 10. | Kontroler do Access Point | 1 |  |  |  |
| 11. | Router– firewall | 2 |  |  |  |
| 12. | Kabel do 10G po 1 m 10G SFP+ LC LR 10km SMF XCVR | 60 |  |  |  |
| 13. | Kabel do 1G po 1m | 100 |  |  |  |
| 14. | Wkładka na 10G | 60 |  |  |  |
| 15. | Wkładka na 1G | 100 |  |  |  |
| 16 | Windows Server Standard lub oprogramowanie równoważne | 15 |  |  |  |
| RAZEM |  |  |

Oferuję dostawę przedmiotu zamówienia w terminie …. dni\* od dnia podpisania umowy

*\*Maksymalny termin dostawy wynosi 14 dni od dnia zawarcia umowy*

Dodatkowa gwarancja na serwery i macierz~~:~~

|  |  |  |
| --- | --- | --- |
| TAK  | NIE | udzielam dodatkowej 12 miesięcznej gwarancji na oferowane serwery i macierz względem okresów minimalnych gwarancji wymaganych w OPZ dla tych sprzętów  |

*\*zaznaczyć właściwy kwadrat*

**Oferowany sprzęt spełnia następujące parametry:**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Element konfiguracji | Wymagania minimalne | Parametry oferowanych **SERWERÓW** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Obudowa | Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli. Serwer z możliwością fabrycznego zamontowania czujnika otwarcia obudowy współpracującego z modułem zarządzania serwera. | SPEŁNIA/NIE SPEŁNIA |
| 2 | Procesor | Dwa (2) procesory szesnastordzeniowe, x86 - 64 bity, klasy Intel Xeon-Gold 6246R (3.4GHz/16-core/205W) lub równoważny procesor szesnastordzeniowy, osiągające w testach cpubenchmark.net minimum 30.000 punktów. Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz. | WSKAZAĆ NAZWĘ PROCESORA: |
| 3 | Liczba procesorów | Min. 2 procesory | SPEŁNIA/NIE SPEŁNIA |
| 4 | Pamięć operacyjna | Minimum 384 GB RDIMM DDR4 2933 MT/s w modułach o pojemności minimum 32GB każdy.Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację minimum 3TB pamięci RAM. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej).Obsługa zabezpieczeń: Advanced ECC, Memory Mirror, Online Spare (Rank Sparing). | SPEŁNIA/NIE SPEŁNIA |
| 5 | Sloty rozszerzeń | Serwer musi być wyposażony w:- 2 aktywne gniazda PCI-Express generacji 3, każde gniazdo x16 i pozwalać na rozbudowę do 3 aktywnych gniazd PCI-Express generacji 3, każde gniazdo x16 (szybkość slotu – bus width) Serwer musi mieć dodatkowo dedykowane dwa sloty PCI-Express:- na kontroler dyskowy;- na kartę sieciową 10Gb Ethernet dwuportową. | SPEŁNIA/NIE SPEŁNIA |
| 6 | Zasoby dyskowe | Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy oraz możliwość zainstalowania 1 dysku SFF SAS/SATA/SSD, 2,5” z tyłu serwera.Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Serwer wyposażony w:Dyski SSD – 4 szt. o pojemności nie mniejszej jak 900GB z interfejsem SATA 6Gb/s Dyski SAS – 5 szt. o pojemności nie mniejszej jak 2.4TB z interfejsem SAS 12Gb/s, o prędkości obrotowej nie mniejszej niż 10k obr/min  | SPEŁNIA/NIE SPEŁNIA |
| 7 | Kontroler | Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym.Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie | SPEŁNIA/NIE SPEŁNIA |
| 8 | Interfejsy sieciowe | Serwer musi być wyposażony w:- 1 dwuportowa karty 10Gb Ethernet SFP+, do kart należy dołączyć 2 sztuki wkładek 10Gb SFP+ z możliwością rozbudowy o kolejną taką kartę.- 1 czteroportowa karta 1Gb Ethernet. | SPEŁNIA/NIE SPEŁNIA |
| 9 | Karta graficzna | Zintegrowana karta graficzna | SPEŁNIA/NIE SPEŁNIA |
| 10 | Porty | 5x USB 3.0 (w tym 2 porty wewnętrzne)1x VGA Wewnętrzny slot na kartę micro SD.Możliwość rozbudowy o:- dodatkowy port DisplayPort dostępny z przodu serwera bez stosowania jakichkolwiek przejściówek;- port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI. | SPEŁNIA/NIE SPEŁNIA |
| 11 | Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W. | SPEŁNIA/NIE SPEŁNIA |
| 12 | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug | SPEŁNIA/NIE SPEŁNIA |
| 13 | Karta/moduł zarządzający i system zarządzania | Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej wymaganej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe
* dostęp do karty zarządzającej poprzez
	+ dedykowany port RJ45 z tyłu serwera lub
	+ przez współdzielony port zintegrowanej karty sieciowej serwera;
* dostęp do karty możliwy
	+ z poziomu przeglądarki webowej (GUI);
	+ z poziomu linii komend;
* wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB;
* monitorowanie zasilania oraz zużycia energii przez serwer z możliwością graficznej prezentacji;
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping);
* zdalna aktualizacja oprogramowania (firmware);
* wsparcie dla Microsoft Active Directory
 | SPEŁNIA/NIE SPEŁNIA |
| 14 | System monitorowania i analizowania konfiguracji serwerów  | Dostęp do systemu wymagany jest dla każdego oferowanego serwera. Jeżeli wymaga to dodatkowych licencji, to należy takie licencje dostarczyć. System musi być dostępny jako usługa webowa (z przeglądarki internetowej), System musi zapewniać: - scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.); - prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera; - prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach. - zalecenia dotyczące eliminacji źródeł/przyczyn problemów wydajnościowych serwerów | SPEŁNIA/NIE SPEŁNIA |
| 15 | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2019 lub nowszyRed Hat Enterprise Linux (RHEL) 7.x lub nowszySUSE Linux Enterprise Server (SLES) 12 lub nowszyVMware ESXi 6.7 lub nowszy | SPEŁNIA/NIE SPEŁNIA |
| 16 | Wsparcie techniczne | Min. 5-letnia gwarancja producenta w miejscu instalacji (ocena wg kryterium oceny ofert). Czas reakcji to kolejny dzień roboczy. W razie awarii dyski twarde nie podlegają zwrotowi i pozostają u Zamawiającego. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| L.p. | Cecha | Wymagania minimalne | Parametry oferowanej **MACIERZY** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Typ obudowy – urządzenie | Przez macierz dyskową Zamawiający rozumie zestaw nośników do składowania danych kontrolowanych przez dedykowane kontrolery macierzowe (bez dodatkowych urządzeń pośrednich, serwerów wirtualizujących, oprogramowania wirtualizującego itp.). | SPEŁNIA/NIE SPEŁNIA |
| 2 | Przestrzeń dyskowa | Macierz musi zapewnić minimalną przestrzeń użytkową (bez używania dodatkowych technologii redukcji objętości danych: deduplikacja, kompresja): 14.8 TiB zbudowaną na dyskach SSD i obrotowych. Jednostka pojemności 1TiB=1024GiB, 1GiB=1024MiB, itd. | SPEŁNIA/NIE SPEŁNIA |
| 3 | Dyski | Dyski SAS: minimum 21 dysków po 2TBDyski SSD: minimum 6 dysków po 960GB | SPEŁNIA/NIE SPEŁNIA |
| 4 | Możliwość rozbudowy | Cała oferowana przestrzeń użytkowa musi być zabezpieczona w sposób zapewniający ciągłą dostępność do danych w przypadku jednoczesnej awarii trzech dysków. Ilość dysków spare/przestrzeni zapasowej musi być dobrana według zaleceń producenta macierzy – nie wlicza się ona w wymaganą w punkcie poprzednim przestrzeń użytkową. | SPEŁNIA/NIE SPEŁNIA |
| 5 | Awaryjność | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych: redundancja kontrolerów, zasilaczy i wentylatorów.Awaria pojedynczego komponentu macierzy (w tym również kontrolera) nie może powodować utraty wydajności całej macierzy. | SPEŁNIA/NIE SPEŁNIA |
| 6 | Wydajność | Macierz musi posiadać wydajność 22000 IOPS dla bloku 4KB, ruch losowy, współczynnik ilości odczytów/zapisów 50%/50%. | SPEŁNIA/NIE SPEŁNIA |
| 7 | Architektura back-end macierzy | SAS 12 Gb/s.Macierz musi być wyposażona minimum w dwa kontrolery z łączną ilością portów: * 4 x 10GbE-T - dostawca dostarczy niezbędne wkładki dla wszystkich portów wraz z macierzą
* 4 x 10GbE SFP+ - dostawca dostarczy niezbędne wkładki dla wszystkich portów wraz z macierzą
* Możliwość rozbudowy o interfejsy FC 16 Gb/s.
 | SPEŁNIA/NIE SPEŁNIA |
| 8 | Rozbudowa | Macierz musi posiadać możliwość rozbudowy bez utraty danych i konieczności ich odtwarzania z backupu do co najmniej 130 TiB pojemności użytkowej (bez używania dodatkowych technologii redukcji objętości danych typu deduplikacja i kompresja) | SPEŁNIA/NIE SPEŁNIA |
| 9 | Pamięć cache | Zabezpieczenie pamięci Cache za pomocą mirrorowania pamięci Cache kontrolerów macierzowych. W przypadku awarii zasilania w celu ochrony danych zawartość pamięci Cache musi zostać trwale zapisana. Macierz musi być dostarczona z pamięcią Cache zbudowaną w oparciu o dyski SSD o pojemności łącznej minimum 5,76 TB. do operacji odczytu i zapisu. | SPEŁNIA/NIE SPEŁNIA |
| 10 | Firmware | Macierz musi umożliwiać uaktualnianie oprogramowania (firmware'u) macierzy (zarówno kontrolerów, jak i dysków) bez przerywania pracy macierzy i bez negatywnego wpływu na jej wydajność. | SPEŁNIA/NIE SPEŁNIA |
| 11 | Wymiana elementów | Wymiana elementów macierzy w trybie "Hot-Swap" bez konieczności wyłączania macierzy (kontrolery, zasilacze, wentylatory). | SPEŁNIA/NIE SPEŁNIA |
| 12 | Upgrade | Macierz musi mieć możliwość upgrade’u kontrolerów do wyższego i nowszego modelu bez konieczności wyłączania macierzy i utraty danych. | SPEŁNIA/NIE SPEŁNIA |
| 13 | Provisioning | Macierz musi mieć możliwość udostępniania zasobów dyskowych do serwerów w trybie typu Thin Provisioning. Wymagane jest dostarczenie licencji dla tej funkcjonalności. | SPEŁNIA/NIE SPEŁNIA |
| 13 | Kompresja | Macierz musi umożliwiać kompresję danych zmiennym blokiem wykonywaną na bieżąco (w locie) na poziomie pojedynczych wolumenów. Macierz powinna mieć możliwość współistnienia zarówno wolumenów skompresowanych, jak i nie-skompresowanych. Wymagane jest dostarczenie licencji dla tej funkcjonalności.  | SPEŁNIA/NIE SPEŁNIA |
| 14 | Deduplikacja | Macierz musi umożliwiać deduplikację danych zmiennym blokiem wykonywaną na bieżąco (w locie) na poziomie pojedynczych wolumenów. Macierz powinna mieć możliwość współistnienia zarówno wolumenów deduplikowanych, jak i nie-deduplikowanych. Wymagane jest dostarczenie licencji dla tej funkcjonalności. | SPEŁNIA/NIE SPEŁNIA |
| 15 | Szyfrowanie | Macierz musi posiadać możliwość szyfrowania danych algorytmem AES-256 potwierdzoną certyfikatem FIPS 140-2 na poziomie pojedynczych wolumenów. Wymagane jest dostarczenie licencji dla tej funkcjonalności. | SPEŁNIA/NIE SPEŁNIA |
| 16 | Zarządzanie wolumenami | Zarządzanie grupami dyskowymi oraz wolumenami logicznymi:* Macierz musi mieć możliwość zdefiniowania co najmniej 1024 wolumenów logicznych.
* Macierz musi mieć możliwość tworzenia wolumenów logicznych o wielkości nie mniejszej niż 120TB.
* Możliwość definiowania rozmiaru bloku danych dla wolumenu logicznego.
* Możliwość dynamicznego zwiększania pojemności wolumenów logicznych z poziomu kontrolera macierzowego bez przerywania dostępu do danych.
* Możliwość tworzenia wolumenu dyskowego zlokalizowanego na więcej niż jednej macierzy dyskowej tej samej rodziny (tzw. skalowanie poziome).
* Dla każdego wolumenu logicznego możliwość określenia parametrów wydajnościowych: maks. IO/s oraz maks. MB/s. Wymagane jest dostarczenie licencji dla tej funkcjonalności.
* Możliwość zdefiniowania grup spójności.
 | SPEŁNIA/NIE SPEŁNIA |
| 17 | Kanały I/O | Macierz musi mieć możliwość obsługa wielu kanałów I/O (ang. multipathing). Automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych. Wymagane jest dostarczenie licencji dla tej funkcjonalności. | SPEŁNIA/NIE SPEŁNIA |
| 18 | Systemy | Możliwość jednoczesnego podłączenia co najmniej 8 niezależnych systemów: VMware ESX 5/6, MS Windows 2012/2016/2019, RedHat Linux 6/7, SUSE/SLES 11/12. Macierz musi wspierać mechanizm VMware VVOL. Wsparcie powinno być dostępne w ramach oferowanych licencji oprogramowania. | SPEŁNIA/NIE SPEŁNIA |
| 19 | Kopie danych | Wewnętrzne kopie danych:* Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy.
* Macierz musi umożliwiać, dokonywania na żądanie, pełnej fizycznej kopii danych w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wymagane jest dostarczenie licencji dla tej funkcjonalności na całą pojemność macierzy.
* Macierz musi wspierać minimum 2048 wszystkich kopii migawkowych.
 | SPEŁNIA/NIE SPEŁNIA |
| 20 | Replikacja danych | Macierz musi wspierać sprzętową replikację synchroniczną i periodyczną/ asynchroniczną:* danych z granularnością na poziomie pojedynczych LUN lub grup LUN przez sieć WAN pomiędzy ośrodkami przetwarzania
* migawek z wykorzystaniem polityk i harmonogramów

Replikacji mają podlegać wyłącznie unikalne bloki danych pomiędzy dowolną kombinację macierzy typu All Flash oraz Hybrid w co najmniej 3 ośrodkach przetwarzania. Macierz musi dodatkowo wsparcie dla VMware Storage Metro Cluster pomiędzy 2 macierzami/ośrodkami. | SPEŁNIA/NIE SPEŁNIA |
| 21 | Monitoring stanu | * + Zarządzanie macierzą z poziomu interfejsu graficznego i interfejsu znakowego. Wymagane jest stałe monitorowanie stanu macierzy oraz możliwość jej konfigurowania.
	+ Monitorowanie w czasie rzeczywistym wydajności macierzy (np. wolumenów logicznych).
	+ Wymagana możliwość historycznej kolekcji danych wydajnościowych – co najmniej 90 dni.
	+ Macierz musi umożliwiać automatyczne informowanie centrum serwisowego o awarii.
	+ Wymagane jest dostarczenie odpowiedniej licencji dla opisanych funkcjonalności.”
 | SPEŁNIA/NIE SPEŁNIA |
| 22 | Wsparcie wirtualizacji | Macierz musi przestawiać dane wydajnościowe obejmujące również środowiska witalizacyjne (co najmniej Vmware, Hyper-V) w poniższym zakresie:* Korelacja maszyn wirtualnych z wolumenami logicznymi macierzy.
* Wydajność i czas odpowiedzi maszyn wirtualnych.
* Czas odpowiedzi maszyn wirtualnych w podziale na opóźnienia wnoszone przez hosta, sieć, macierz.
* Możliwość historycznej kolekcji danych wydajnościowych – co najmniej 90 dni.
* Wymagane jest dostarczenie licencji dla tych funkcjonalności na całą pojemność macierzy.
 | SPEŁNIA/NIE SPEŁNIA |
| 23 | Wymiary fizyczne | W przypadku, jeśli oferowane rozwiązanie zajmuje więcej niż 4U oferent zobowiązany jest w ramach prowadzonego postępowania dostarczyć i macierz w szafie rack 19” o wysokości 42U i głębokości 1050 mm, wyposażonej w redundantne zasilanie 1 fazowe 230V 32A. | SPEŁNIA/NIE SPEŁNIA |
| 24 | Pobór energii elektrycznej | W przypadku, jeśli rozwiązanie w oferowane konfiguracji charakteryzuje się poborem mocy większym niż 750W, Oferent zobowiązany jest do dostarczenia UPS, zintegrowanego z oferowanym urządzeniem oraz Windows, VMware, Linux, HP-UX, AIX, Solaris, gwarantującego podtrzymanie zasilania macierzy przez 45 minut. | SPEŁNIA/NIE SPEŁNIA |
| 25 | Gwarancja i serwis | Min. 3-letnia gwarancja producenta w miejscu instalacji (ocena wg kryterium oceny ofert). Czas naprawy – maksymalnie następny dzień roboczy na wysłanie uszkodzonej części liczone od chwili stwierdzenia uszkodzenia. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. Nośniki SSD objęte są usługami wsparciem nieograniczonym intensywnością wykorzystania (bez względu na intensywność zapisów) | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanej **SZAFY RACK** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Wymiary szafy RACK 19” | Szafa wolnostojąca 19” Minimum 48U wewnętrznego miejsca do instalacji urządzeń. Szerokość szafy min. 60 cm. Głębokość szafy min. 111 cm  | SPEŁNIA/NIE SPEŁNIAWymiary oferowanej szafy są dostosowane do oferowanej macierzy |
| 2 | Rama | Rama powinna być skonstruowana jako rama stalowa spawana/skręcana wykończona malowaniem proszkowym. Musi umożliwiać instalację sprzętu o wadze min. 1360kg  (obciążenie statyczne). Dopuszczalne obciążenie podczas przemieszczania/przesuwania szafy 1022kg ( obciążenie dynamiczne) bez użycia dodatkowych środków technicznych (wózek, platforma itp.) | SPEŁNIA/NIE SPEŁNIA |
| 3 | Wyposażenie szafy RACK 19” | Szafa wyposażona w:* Drzwi przednie perforowane (perforacja min. 77%), wyposażone w zamek
* Drzwi powinny umożliwiać demontaż bez użycia narzędzi i założenie po przeciwnej stronie,
* Obie ściany boczne powinny być dzielone i zamykane
* Standardowy panel górny powinien być wykonany z blachy stalowej, dostosowany do demontażu bez użycia narzędzi.
* Minimum 2 przepusty kablowe - jeden w suficie, drugi w podłodze
* Szafa powinna być wyposażona w minimum 4 kółka samonastawne oraz dostępne od góry stopki poziomujące.
* Minimum 6 wentylatorów z wbudowanym termostatem pracującym w zakresie od 0 do +60 stopni Celsjusza.
* Minimum 2 półki
 | SPEŁNIA/NIE SPEŁNIA |
| 4 | Standardy przemysłowe dla szafy RACK19” | Szafa RACK 19” zaprojektowana zgodnie z następującymi normami lub certyfikatami:* EIA-310E
* RoHS
* UL2416
* REACH
 | SPEŁNIA/NIE SPEŁNIA |
| 5 | Inne  | Wszystkie elementy szafy (drzwi, panele boczne, panele górne, szyny 19’’, wsporniki listew PDU) powinny być bezpośrednio uziemione do ramy. Szafa musi posiadać gwarancję na wady materiałowe oraz wykonania na trzy (3) lata. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanych **LISTEW ZASILAJĄCYCH** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Wymiary listwy | Listwa przeznaczona do szafy wolnostojącej 19” Wysokość 1U  | SPEŁNIA/NIE SPEŁNIA |
| 2 | Liczba gniazd | Minimum 6 | SPEŁNIA/NIE SPEŁNIA |
| 3 | Typ gniazd wyjściowych | W standardzie IEC C14 + 2 wyjścia IEC - C19; gniazda dopasowane do oferowanego sprzętu (serwery, macierz, firewall, switche) | SPEŁNIA/NIE SPEŁNIA |
| 4 | Gwarancja | 12 miesięcy | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanej **KONSOLI** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Wymagania ogólne | * Urządzenie musi być fabrycznie przystosowane do instalacji w szafach rack 19” w orientacji poziomej.
* Wysokość instalacyjna urządzenia nie może przekraczać wysokości 1RU (Rack Unit).
 | SPEŁNIA/NIE SPEŁNIA |
| 2 | Właściwości użytkowe | * Urządzenie musi posiadać zintegrowany ekran LED LCD o przekątnej minimum 19”.
* Przekątna 16:9, rozdzielczość minimum 1600x1200
* Urządzenie musi posiadać wbudowaną klawiaturę z układem US (qwerty) oraz touchpad.
* Urządzenie musi posiadać wbudowane podświetlanie klawiatury i panelu dotykowego umożliwiające widoczność przy słabym oświetleniu
* Urządzenie musi posiadać wbudowany przełącznik KVM umożliwiający podpięcie minimum 8 komputerów poprzez moduły KVM do portów RJ-45
* Obsługa serwerów blade oraz Obsługa wieloplatformowych środowisk serwerowych: Urządzenia szeregowe Windows, Mac, Sun, Linux i VT100
* Dwie niezależne magistrale jedna dla dostępu lokalnego i jedna dla dostępu zdalnego poprzez IP
 | SPEŁNIA/NIE SPEŁNIA |
| 3 | Moduły | * Wraz z przełącznikiem należy dostarczyć niezbędną ilość modułów KVM do podłączenia serwerów z Interfejs VGA i USB i obsługą Virtual Media
 | SPEŁNIA/NIE SPEŁNIA |
| 4 | Inne | Konsola musi posiadać gwarancję na wady materiałowe oraz wykonania na trzy (3) lata. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanego **UPS** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Moc pozorna  | 5000 VA | SPEŁNIA/NIE SPEŁNIA |
| 2 | Moc rzeczywista  | 5000 W | SPEŁNIA/NIE SPEŁNIA |
| 3 | Topologia (klasyfikacja IEC 62040-3) | Podwójna konwersja on-line  | SPEŁNIA/NIE SPEŁNIA |
| 4 | Typ obudowy  | Uniwersalna tower/rack  | SPEŁNIA/NIE SPEŁNIA |
| 5 | Sprawność UPS'a | 95% w trybie podwójnego przetwarzania on-line przy 100% obciążeniu, 98% w trybie podwyższonej sprawności | SPEŁNIA/NIE SPEŁNIA |
| 6 | Liczba, typ gniazd wyjściowych  | W standardzie zaciski + 4 wyjścia IEC - C19 poprzez bypass serwisowy | SPEŁNIA/NIE SPEŁNIA |
| 7 | Urządzenie winno posiadać | Dwutorowe zasilanie wejścia: oddzielne wejście zasilania prostownika i bypassu wewnętrznego  | SPEŁNIA/NIE SPEŁNIA |
| 8 | Typ gniazda wejściowego  | Zaciski | SPEŁNIA/NIE SPEŁNIA |
| 9 | Wymagany czas podtrzymania dla obciążenia mocą 6 kW z zastosowaniem baterii zewn. | 5 minut | SPEŁNIA/NIE SPEŁNIA |
| 10 | Dodatkowe baterie  | Możliwość wydłużenia czasu podtrzymania do > 1h przy obc. mocą 10kW poprzez dołożenie dodatkowych modułów baterii zewnętrznych.  | SPEŁNIA/NIE SPEŁNIA |
| 11 | Napięcie znamionowe | 230V  | SPEŁNIA/NIE SPEŁNIA |
| 12 | Tolerancja napięcia prostownika | 100-276V przy 40% obciążeniu | SPEŁNIA/NIE SPEŁNIA |
| 13 | Częstotliwość znamionowa | 50/60 Hz autodetekcja | SPEŁNIA/NIE SPEŁNIA |
| 14 | Tolerancja częstotliwości | 40 – 70 Hz | SPEŁNIA/NIE SPEŁNIA |
| 15 | Kształt napięcia  | Sinusoidalny | SPEŁNIA/NIE SPEŁNIA |
| 16 | Napięcie znamionowe wyjściowe | 230 V (domyślnie) / 200/208/220/240/250V | SPEŁNIA/NIE SPEŁNIA |
| 17 | Zakres zmian napięcia wyjściowego |  +/-1% napięcia nominalnego | SPEŁNIA/NIE SPEŁNIA |
| 18 | Częstotliwość wyjściowa | 50/60 Hz +/-0,5%  | SPEŁNIA/NIE SPEŁNIA |
| 19 | Całkowite odkształcenia napięcia THDu | < 2% dla obciążenia liniowego | SPEŁNIA/NIE SPEŁNIA |
| 20 | Baterie wymieniane przez użytkownika "na gorąco" | Tak | SPEŁNIA/NIE SPEŁNIA |
| 21 | Ochrona przed przeładowaniem | Tak | SPEŁNIA/NIE SPEŁNIA |
| 22 | Ochrona przed głębokim rozładowaniem | Tak | SPEŁNIA/NIE SPEŁNIA |
| 23 | Okresowy automatyczny test baterii | Tak (standardowo co tydzień) | SPEŁNIA/NIE SPEŁNIA |
| 24 | Zimny start | Tak | SPEŁNIA/NIE SPEŁNIA |
| 25 | System zarządzania pracą baterii | System nieciągłego ładowania baterii. W ofercie opisać algorytm ładowania nieciągłego baterii- okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. | Opisać algorytm ładowania nieciągłego baterii:…………………Okres spoczynkowy w jednym cyklu ……. dni |
| 26 | Interfejs komunikacyjny  |  • USB • RS232 DB-9 żeński (HID) • miniport wyłącznik awaryjny RPO • miniport wyłącznik ON/OFF • DB-9 port przekaźnikowy • DB15 interfejs do komunikacji równoległej | SPEŁNIA/NIE SPEŁNIA |
| 27 | Panel sterowania z wyświetlaczem LCD |  • Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS’a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh) • Poziomy rząd przycisków sterowania • Poziomy rząd wskaźników stanu: trybu online (zielony), trybu bateryjnego (pomarańczowy), trybu bypass (pomarańczowy), usterki (czerwony) | SPEŁNIA/NIE SPEŁNIA |
| 28 | Przyciski sterujące i wskaźniki diodowe LED |  • sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie) • przycisk Escape (anulowanie) • przyciski funkcyjne (przewijanie w górę i w dół) • przycisk Enter (potwierdzający) | SPEŁNIA/NIE SPEŁNIA |
| 29 | Wyposażenie standardowe  |  • przycisk ON/OFF załączenia i wyłączenia  •  kabel RS232 • zewnętrzny bypass serwisowy •  kabel USB •  karta SNMP •  uchwyty kablowe •  podstawki do montażu pionowego (wieża) •  zestaw szyn montażowych do szafy 19" •  instrukcja obsługi  | SPEŁNIA/NIE SPEŁNIA |
| 30 | Karta SNMP  |  • kompatybilność z SNMP v1/v3 i IP v4/v6 • Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex /HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/ • cyberbezpieczeństwo - pakiet szyfrów TLS 1.2 z minimum SHA256 • certyfikat UL 2900-2-2 • protokoły MQTT/RNDIS/LDAP/NVD/SSH/PKI | SPEŁNIA/NIE SPEŁNIA |
| 31 | Czujnik środowiska | Pomiar temperatury i wilgotności. Dane z czujnika muszą być dostępne w oprogramowaniu monitorującym UPS. Przekroczenie zadeklarowanych wartości powinno inicjować procedurę uporządkowanego zamykania systemów operacyjnych. Czujnik winien być wyposażony w magnes umożliwiający montaż w dowolnym miejscu szafy. | SPEŁNIA/NIE SPEŁNIA |
| 32 | Oprogramowanie  |  • zdalne zarządzanie parametrami zamykania maszyn fizycznych oraz wirtualnych • wykonywanie zaplanowanych wyłączeń maszyn wirtualnych oraz hostów m.in.: VMware, HyperV, RedHat KVM i Xen, oraz macierzy • pełna integracja z systemem VMware vRealize Operations Manager • plugin do oprogramowania VMware vCenter lub Citrix XenCenter | SPEŁNIA/NIE SPEŁNIA |
| 33 | Maksymalna wysokość  | 130+130 mm (moduł baterii oraz moduł zasilania tworzą dwie bliźniacze obudowy) + 2 dodatkowe baterie po 130 mm - razem 12U | SPEŁNIA/NIE SPEŁNIA |
| 34 | Poziom hałasu w odl. 1m  | ≤ 50 dBA | SPEŁNIA/NIE SPEŁNIA |
| 35 | Gwarancja producenta  | 24 miesiące  | SPEŁNIA/NIE SPEŁNIA |
| 36 | Battery Pack | Jeśli moc samego UPSa jest niewystarczająca dopuszczalne jest dostarczenie urządzenia mniejszego wraz z battery pack, tak aby całość zestawu spełniała powyższe wymagania. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanych **SWITCH`Y SZKIELETOWYCH** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Typ przełącznika | Zarządzany, stackowalny. Przełącznik musi posiadać co najmniej 4 dedykowane porty umożliwiające łączenie w stos. Wydajność portów stackujących co najmniej 40 Gbps na port. Dopuszcza się rozwiązanie posiadające 2 dedykowane porty stackujące o wydajności co najmniej 80GBps na port. Oprogramowanie przełącznika musi umożliwiać połączenie co najmniej 10 urządzeń w stos. Przełączniki połączone w stos z punktu widzenia reszty infrastruktury muszą być widoczne jako jedno urządzenie, czyli muszą tworzyć jedno logiczne urządzenie zarządzane z jednej linii komend. Porty służące do połączenia w stos muszą być niezależne od minimalnej liczby wymaganych portów liniowych, nie mogą także ograniczać możliwości ich rozbudowy. Dopuszcza się porty stackujące w formie moduły, w takim przypadku moduł nie musi być dostarczony. | SPEŁNIA/NIE SPEŁNIA |
| 2 | Przełącznik wielowarstwowy | L2/L3. Obsługa protokołów rutingu: ruting statyczny, RIP v1, RIP v2, OSPF, OSPFv3, VRRP, PIM-SM, PIM-DM, BGP. Jeżeli do działania któregokolwiek z wymienionych protokołów wymagana jest dodatkowa licencja to należy ją dostarczyć. | SPEŁNIA/NIE SPEŁNIA |
| 3 | Porty  | 16x 10GE SFP+. Możliwość rozbudowy o dodatkowe 8 portów SFP+, 8 portów MGig (1000/2.5/5/10Gb/s) z interfejsem RJ-45 lub 2 porty QSFP+. Nie dopuszcza się uzyskania portów SFP+ poprzez zastosowanie kabli rozszywających. Dopuszcza się rozbudowę poprzez wymianę 8 portów SFP+. | SPEŁNIA/NIE SPEŁNIA |
| 4 | Moduły SFP | 4x10G | SPEŁNIA/NIE SPEŁNIA |
| 5 | Wielkość tablicy routingu: | minimum 10000 wpisów dla IPv4 i minimum 5000 wpisów dla IPv6 | SPEŁNIA/NIE SPEŁNIA |
| 6 | Standardy komunikacyjne  | IEEE 802.3,IEEE 802.3ab,IEEE 802.3af,IEEE 802.3at,IEEE 802.3u. | SPEŁNIA/NIE SPEŁNIA |
| 7 | Agregator połączenia  | Tak, zgodnie z LACP | SPEŁNIA/NIE SPEŁNIA |
| 8 | Obsługa sieci VLAN  | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 9 | Liczba VLAN  | 4094 tagi i 4094 jednocześnie obsługiwane sieci VLAN. | SPEŁNIA/NIE SPEŁNIA |
| 10 | Przepustowość rutowania/przełączania  | 480Gbps. | SPEŁNIA/NIE SPEŁNIA |
| 11 | Prędkość przekazywania  | 285Mpps. | SPEŁNIA/NIE SPEŁNIA |
| 12 | Wielkość tabeli adresów  | 64000. | SPEŁNIA/NIE SPEŁNIA |
| 13 | Pamięci bufora pakietów  | 13MB. | SPEŁNIA/NIE SPEŁNIA |
| 14 | Montowanie w stelażu  | Tak wraz z wyposażeniem do instalacji w szafie Rack. | SPEŁNIA/NIE SPEŁNIA |
| 15 | Układ | 1U | SPEŁNIA/NIE SPEŁNIA |
| 16 | Pamięć wewnętrzna DRAM  | Minimum 4Gb | SPEŁNIA/NIE SPEŁNIA |
| 17 | Pamięć Flash  | Minimum 1GB | SPEŁNIA/NIE SPEŁNIA |
| 18 | IPv6 | Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping) | SPEŁNIA/NIE SPEŁNIA |
| 19 | OpenFlow | Obsługa protokołu OpenFlow w wersji co najmniej 1.0 i 1.3 lub równoważne. | SPEŁNIA/NIE SPEŁNIA |
| 20 | Dedykowany port do zarządzania  | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 21 | RJ-45 Serial Console Port | Tak. Pełne zarządzanie z poziomu konsoli | SPEŁNIA/NIE SPEŁNIA |
| 22 | Redundantny zasilacz  | Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. Modularne, redundantne wentylatory. Moduł wentylatorów musi mieć możliwość wymiany „na gorąco” (na działającym urządzeniu) | SPEŁNIA/NIE SPEŁNIA |
| 23 | Licencje | Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.  | SPEŁNIA/NIE SPEŁNIA |
| 24 | Gwarancja | 10 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie technicznego (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 10 lat. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanych **SWITCH`Y BIUROWYCH** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Typ przełącznika | Zarządzany. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane. | SPEŁNIA/NIE SPEŁNIA |
| 2 | Przełącznik wielowarstwowy | L2/L3. Routing minimum: statyczny, RIPv2, RIPng, OSPF i OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów) | SPEŁNIA/NIE SPEŁNIA |
| 3 | Porty RJ-45 | 48x GE. | SPEŁNIA/NIE SPEŁNIA |
| 4 | Moduły SFP | 4x GE SFP. | SPEŁNIA/NIE SPEŁNIA |
| 5 | Standardy komunikacyjne | IEEE 802.1D,IEEE 802.1p,IEEE 802.1s,IEEE 802.1w,IEEE 802.1x,IEEE 802.3,IEEE 802.3ab,IEEE 802.3ad,IEEE 802.3ae,IEEE 802.3af,IEEE 802.3at,IEEE 802.3u,IEEE 802.3x,IEEE 802.3z | SPEŁNIA/NIE SPEŁNIA |
| 6 | Dublowanie portów | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 7 | Pełny dupleks | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 8 | Agregator połączenia | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 9 | Kontrola wzrostu natężenia ruchu | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 10 | Automatyczne MDI/MDI-X | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 11 | Auto-Negocjacja | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 12 | Obsługa sieci VLAN | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 13 | Liczba VLAN | Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLA | SPEŁNIA/NIE SPEŁNIA |
| 14 | Przepustowość rutowania/przełączania | 104Gbps. | SPEŁNIA/NIE SPEŁNIA |
| 15 | Prędkość przekazywania | 77Mpps. | SPEŁNIA/NIE SPEŁNIA |
| 16 | Wielkość tabeli adresów | 32000. | SPEŁNIA/NIE SPEŁNIA |
| 17 | Zgodność z Jumbo Frames | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 18 | OpenFlow | Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3 | SPEŁNIA/NIE SPEŁNIA |
| 19 | Funkcje DHCP | DHCP client, DHCP relay, DHCP snooping. | SPEŁNIA/NIE SPEŁNIA |
| 20 | IGMP snooping | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 21 | Uwierzytelnianie | Guest VLAN, Uwierzytelnianie oparte na MAC, Uwierzytelnianie na podstawie portów. | SPEŁNIA/NIE SPEŁNIA |
| 22 | Obsługa Multicast | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 23 | Pamięci bufora pakietów | 12 MB. | SPEŁNIA/NIE SPEŁNIA |
| 24 | Montowanie w stelażu | Tak wraz z wyposażeniem do instalacji w szafie Rack. | SPEŁNIA/NIE SPEŁNIA |
| 25 | Układ | 1U. | SPEŁNIA/NIE SPEŁNIA |
| 26 | Pamięć wewnętrzna DRAM | 1GB. | SPEŁNIA/NIE SPEŁNIA |
| 27 | Pamięć Flash | 4GB. | SPEŁNIA/NIE SPEŁNIA |
| 28 | Obsługa PoE | 24x 802.3af/802.3at. | SPEŁNIA/NIE SPEŁNIA |
| 29 | Zasilanie PoE | 370W | SPEŁNIA/NIE SPEŁNIA |
| 30 | Dedykowany port do zarządzania | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 31 | RJ-45 Serial Console Port | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 32 | Licencje i oprogramowanie | Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.  | SPEŁNIA/NIE SPEŁNIA |
| 33 | Gwarancja | 10 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie technicznego (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 10 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanych **ACCESS POINT** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Typ punktu dostępowego | Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax, oraz 2.4GHz b/g/n/ax. | SPEŁNIA/NIE SPEŁNIA |
| 2 | Zarządzanie | Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej | SPEŁNIA/NIE SPEŁNIA |
| 3 | Praca autonomiczna | Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: * Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https
* Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki
* Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.
 | SPEŁNIA/NIE SPEŁNIA |
| 4 | Provisoining | Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: * System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego
* W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny
* Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe
* Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję
* Tworzenie klastra do 130 urządzeń
 | SPEŁNIA/NIE SPEŁNIA |
| 5 | Ilość SSID | Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID na każdym module radiowym | SPEŁNIA/NIE SPEŁNIA |
| 6 | Interfejs sieciowy  | 1 interfejs 100/1000BaseT z funkcją auto-sensing link oraz MDI/MDX z funkcją PoE/PoE+ ze wsparciem dla standardu 802.3az Energy Efficient Ethernet (EEE) | SPEŁNIA/NIE SPEŁNIA |
| 7 | Zasilanie | Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE oraz przy pomocy lokalnego zasilacza DC (zasilacz nie musi być dołączony) | SPEŁNIA/NIE SPEŁNIA |
| 8 | Anteny | Punkt dostępowy musi posiadać co najmniej 2 wbudowane anteny pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 4.3 dBi dla 2,4GHz, 5.5 dBi dla 5 GHz | SPEŁNIA/NIE SPEŁNIA |
| 9 | Zabezpieczenie przed kradzieżą  | Tak. | SPEŁNIA/NIE SPEŁNIA |
| 10 | Opcje montażu  | Sufit, ściana | SPEŁNIA/NIE SPEŁNIA |
| 11 | Prędkości transmisji | Prędkości transmisji: do 400 Mbps dla 802.11n, do 1000 Mbps dla 802.11ac, do 574 Mbps dla 802.11ax (2,4GHz), do 1200 Mbps dla 802.11ax (5GHz) | SPEŁNIA/NIE SPEŁNIA |
| 12 | Licencje i oprogramowanie | Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.  | SPEŁNIA/NIE SPEŁNIA |
| 13 | Gwarancja | Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| LP. | Parametry | Charakterystyka minimalna | Parametry oferowanego **KONTROLERA** **ACCESS POINT** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Wymagania do współpracy z punktami dostępowymi | Kontroler musi w pełni obsługiwać punkty dostępowe opisane w tym postępowaniu | SPEŁNIA/NIE SPEŁNIA |
| 2 | Minimalna ilość punktów dostępowych | Kontroler musi zarządzać siecią bezprzewodową złożoną z 12 punktów dostępowych z możliwością rozbudowy do co najmniej 32 punktów dostępowych | SPEŁNIA/NIE SPEŁNIA |
| 3 | Firewall | Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall) | SPEŁNIA/NIE SPEŁNIA |
| 4 | VPN | Musi posiadać funkcje VPN Gateway | SPEŁNIA/NIE SPEŁNIA |
| 5 | Inne | Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym. | SPEŁNIA/NIE SPEŁNIA |
| 6 | Niezawodność | Kontroler musi mieć funkcję pracy w klastrze HA | SPEŁNIA/NIE SPEŁNIA |
| 7 | Komunikacja | Komunikacja pomiędzy kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych. | SPEŁNIA/NIE SPEŁNIA |
| 8 | Zarządzanie punktami dostępowymi | Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania | SPEŁNIA/NIE SPEŁNIA |
| 9 | Licencje dla punktów dostępowych | Kontroler musi zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuję więcej niż jedne kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom. | SPEŁNIA/NIE SPEŁNIA |
| 10 | Minimalne parametry sieciowe | Kontroler musi posiadać następujące parametry sieciowe:* możliwość wdrożenia w warstwie 2 i 3 ISO/OSI,
* wsparcie dla sieci VLAN w tym również trunk 802.1q
* wbudowany serwer DHCP
* obsługa SNMPv2, SNMPv3
* routing dynamiczny OSPF
 | SPEŁNIA/NIE SPEŁNIA |
| 11 | Obsługiwane funkcjonalności | Kontroler sieci WLAN musi obsługiwać co najmniej:1.Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST, DES, 3DES, AES-CBC 2.Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze 3.Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit 4.Autoryzację dostępu użytkowników: * 1. Typy uwierzytelnienia: IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal”, 802.1X i MAC
	2. Możliwość wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia
	3. Wsparcie dla autoryzacji: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC
	4. Możliwość utworzenia nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal”
	5. Możliwość wykorzystania mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)
	6. Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym
	7. Uwierzytelnienie oraz autoryzacja muszą być możliwe przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius.
1. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających.
	1. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu
2. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia
 | SPEŁNIA/NIE SPEŁNIA |
| 12 | Obsługiwana transmisja i kolejkowanie | Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci:* Integracja jednoczesnej transmisji danych i głosu
* Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p
* Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming)
* Ograniczanie pasma dla użytkownika oraz dla roli użytkownika
* Ograniczenie pasma dla poszczególnych aplikacji
* Ograniczenie pasma dla poszczególnych kategorii stron internetowych bądź też poziomu zaufania
* Ograniczenie pasma dla poszczególnych SSID
 | SPEŁNIA/NIE SPEŁNIA |
| 13 | Integracja | Kontroler musi umożliwiać integrację ze środowiskiem Microsoft Lync/Teams/O365 poprzez SDN API. | SPEŁNIA/NIE SPEŁNIA |
| 14 | Captive Portal | Kontroler musi umożliwiać stworzenie strony dla gości tzw. Captive Portal | SPEŁNIA/NIE SPEŁNIA |
| 15 | Konta i sieć guest | Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni)  | SPEŁNIA/NIE SPEŁNIA |
| 16 | Zarządzanie pasmem | Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym:* Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe
* Stałe monitorowanie pasma oraz usług
* Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi
* Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma
* Wykrywanie urządzeń obsługujących MU-MIMO i podłączenie ich do punktów dostępowych obsługujących tą technologię (pracujących w standardzie 802.11ac 2Wave)
* Przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie
* Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b)
* Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
* Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w
* Integracja z systemami RFID - wymagane jest wbudowane stosowne API
 | SPEŁNIA/NIE SPEŁNIA |
| 17 | Funkcjonalność zapory sieciowej | Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności:* + Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia
	+ Mirroring sesji
	+ Szczegółowe logi (per packet) do późniejszej analizy
	+ ALG (Application Layer gateway) co najmniej dla protokołów FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP
	+ Translacja źródłowa, docelowa adresów IP
	+ Identyfikacja i blokowanie ataków DoS
	+ Obsługa protokołu GRE
	+ Deep packet inspection (DPI)
	+ Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi
 | SPEŁNIA/NIE SPEŁNIA |
| 18 | Funkcjonalność VPN | Kontroler musi mieć wbudowany serwer VPN, charakteryzujący się następującymi parametrami, nie mniej niż:* + Site-to-site oraz client-site VPN
	+ Terminacja ruchu L2TP/IPSEC VPN, XAUTH/IPSEC, PPTP
	+ Obsługa tokenów
	+ Wsparcie dla serwerów Radius i LDAP w celu uwierzytelnienia sesji VPN przy użyciu: PAP CHAP, MS-CHAP, MS-CHAP2
	+ Wsparcie u jest wymagana na tym etapie). Moduł WIPS musi posiadać co najmniej następujące funkcje:
	+ Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.
	+ Identyfikacja i możliwość blokowania sieci Adhoc
	+ Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging
	+ Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler
	+ Identyfikacja błędów konfiguracji klientów WLAN
	+ Identyfikacja podszywania się pod autoryzowane punkty dostępowe
 | SPEŁNIA/NIE SPEŁNIA |
| 19 | Analiza pasma i widma | Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie). | SPEŁNIA/NIE SPEŁNIA |
| 20 | Zarządzanie kontrolerem | Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli. | SPEŁNIA/NIE SPEŁNIA |
| 21 | Protokoły wspierające | Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA | SPEŁNIA/NIE SPEŁNIA |
| 22 | Parametry wydajnościowe | Kontroler musi być zgodny z następującymi parametrami ilościowymi/wydajnościowymi:* + Liczba obsługiwanych punktów dostępowych nie mniej niż 32
	+ Ilość jednocześnie obsługiwanych adresów MAC nie mniej niż 2000
	+ Liczba aktywnych sesji zapory sieciowej nie mniej niż 64000, przepustowość zapory sieciowej nie mniej niż 4Gbps
	+ Liczba jednoczesnych tuneli IPSec nie mniej niż 2000
	+ Przepustowość ruchu szyfrowanego nie mniejsza niż 4 Gbps dla algorytmu 3DES oraz AES-GCM-256
	+ Minimum 4 porty 10/100/1000Base-T
	+ 1 interfejs konsoli (mini USB/RJ-45)
	+ 1 port USB 2.0
	+ Zużycie energii nie większe niż 30W
 | SPEŁNIA/NIE SPEŁNIA |
| 23 | Zgodność z normami | Dla kontrolera wymagana zgodność z normami:* + FCC Part 15 Class B
	+ EN 55022 Class B
	+ EN 55024
	+ IEC/EN 60950
	+ CE Marking
	+ cTUVus Marked
	+ CB Scheme Certified
 | SPEŁNIA/NIE SPEŁNIA |
| 24 | Chłodzenie | Kontroler powinien posiadać pasywne chłodzenie – ale wentylatory są dopuszczalne | SPEŁNIA/NIE SPEŁNIA |
| 25 | Montaż rack | Kontroler musi posiadać zestaw akcesoriów pozwalający na montaż w szafie rack. | SPEŁNIA/NIE SPEŁNIA |
| 26 | Gwarancja i serwis | Minimum 3 letnia gwarancja producenta obejmująca wszystkie elementy urządzenia (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 8x5 na wszystkie elementy i licencje. | SPEŁNIA/NIE SPEŁNIA |

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Parametry | Charakterystyka | Parametry oferowanych **ROUTERÓW** (należy skreślić nieprawidłowe lub wypełnić wpisując wymagane dane- w zależności od polecenia w rubryce) |
| 1 | Rodzaj urządzenia | Firewall. | SPEŁNIA/NIE SPEŁNIA |
| 2 | Porty | 4 x 10/100/1000, 8 x 1G SFP, port zarządzania 10/100/1000, port konsoli, port USB | SPEŁNIA/NIE SPEŁNIA |
|  |
| 3 | Dysk SSD | 200 GB. | SPEŁNIA/NIE SPEŁNIA |  |
| Przepustowość IPS | 800 Mb/s. | SPEŁNIA/NIE SPEŁNIA |  |
| 4 | Przepustowość NGFW | 800 Mb/s. | SPEŁNIA/NIE SPEŁNIA |  |
| 5 | Przepustowość Threat Protection | 800 Mb/s. | SPEŁNIA/NIE SPEŁNIA |  |
| 6 | Sesje równoległe (TCP) | 120 000. | SPEŁNIA/NIE SPEŁNIA |  |
| 7 | Nowe sesje na sekundę (TCP) | 8 000. | SPEŁNIA/NIE SPEŁNIA |  |
| 8 | Polityki Firewall | 1500. | SPEŁNIA/NIE SPEŁNIA |  |
| 9 | Przepustowość IPsec VPN | 1 Gb/s. | SPEŁNIA/NIE SPEŁNIA |  |
| 10 | Tunele IPsec typu Brama-Brama | 1000 | SPEŁNIA/NIE SPEŁNIA |  |
| 11 | Tunele IPsec typu Klient-Brama  | 1000 | SPEŁNIA/NIE SPEŁNIA |  |
| 12 | Przepustowość kontroli aplikacji (HTTP 64K) | 1,5 Gb/s. | SPEŁNIA/NIE SPEŁNIA |  |
| 13 | Konfiguracje wysokiej dostępności | Active/Active, Active/Passive, | SPEŁNIA/NIE SPEŁNIA |  |
| 14 | Zarządzanie trybem pracy  | Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.).  | SPEŁNIA/NIE SPEŁNIA |  |
| 15 | Liczba VLAN (definiowanych w oparciu o standard IEEE 802.1q)  | Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.  | SPEŁNIA/NIE SPEŁNIA |  |
| 16 | Translacja adresów IP  | Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.  | SPEŁNIA/NIE SPEŁNIA |  |
| 17 | Uwierzytelnianie  | Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.  | SPEŁNIA/NIE SPEŁNIA |  |
| a. Polityki definiujące powinny umożliwiać wykorzystanie  |  |  |
| * adresów źródłowych,
 |  |  |
| * adresów docelowych,
 |  |  |
| * użytkowników,
 |  |  |
| * numerów portów usług
 |  |  |
| * kategorie URL.
 |  |  |
| b. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia  |  |  |
| * RADIUS lub TACACS+,
 |  |  |
| * LDAP,
 |  |  |
| * SAML 2.0.
 |  |  |
| 18 | Zarządzanie pasmem sieci (QoS)  | Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej  | SPEŁNIA/NIE SPEŁNIA |  |
| * oznaczania pakietów znacznikami DiffServ,
 |  |  |
| * utworzenia co najmniej 8 klas ruchu sieciowego,
 |  |  |
| * kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.
 |  |  |
| 19 | Ochrona przed atakami typu DoS  | Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.  | SPEŁNIA/NIE SPEŁNIA |  |
| 20 | Routing  | Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.  | SPEŁNIA/NIE SPEŁNIA |  |
| 21 | Liczba wirtualnych routerów  | Urządzenie musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu  | SPEŁNIA/NIE SPEŁNIA |  |
| 22 | Mechanizm PBR  | Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.  | SPEŁNIA/NIE SPEŁNIA |  |
| 23 | Polityka bezpieczeństwa systemu  | Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1500 reguł polityki bezpieczeństwa oraz obsługę minimum 25 stref bezpieczeństwa.  | SPEŁNIA/NIE SPEŁNIA |  |
| 24 | Funkcjonalność rozpoznawania aplikacji  | Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.  | SPEŁNIA/NIE SPEŁNIA |  |
| Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.  |  |  |
| 25 | Funkcjonalność kontroli aplikacji  | Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość” w polityce.  | SPEŁNIA/NIE SPEŁNIA |  |
| 26 | Definiowanie profili ochrony  | Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.  | SPEŁNIA/NIE SPEŁNIA |  |
| 27 | Funkcjonalność blokowania transmisji plików  | Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia  | SPEŁNIA/NIE SPEŁNIA |  |
| 28 | Analiza i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach  | Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji  | SPEŁNIA/NIE SPEŁNIA |  |
| 29 | Ochrona przed atakami typu „Drive-by-download”  | Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download”  | SPEŁNIA/NIE SPEŁNIA |  |
| 30 | Definiowanie ruchu SSL  | Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.  | SPEŁNIA/NIE SPEŁNIA |  |
| 31 | Inspekcja szyfrowanej komunikacji SSH  | Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH  | SPEŁNIA/NIE SPEŁNIA |  |
| 32 | Uwierzytelnienie użytkowników  | Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:  | SPEŁNIA/NIE SPEŁNIA |  |
| a. Microsoft Active Directory,  |  |  |
| b. usługi katalogowe LDAP,  |  |  |
| c. serwery Terminal Services.  |  |  |
| d. informacje z logów SYSLOG  |  |  |
| 33 | Polityka dostępu do urządzenia  | Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.  | SPEŁNIA/NIE SPEŁNIA |  |
| 34 | Funkcjonalność IPS  | Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji.  |  |  |
| System IPS musi działać w warstwie 7 modelu OSI.  |  |  |
| Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia.  |  |  |
| Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  | SPEŁNIA/NIE SPEŁNIA |  |
| Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.  |  |  |
| Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania.  |  |  |
| **Zamawiający wymaga dostarczenia licencji na IPS wraz z urządzeniem** |  |  |
| 35 | Funkcjonalność AV  | Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji.Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  | SPEŁNIA/NIE SPEŁNIA |  |
| **Zamawiający wymaga dostarczenia licencji na ochronę antywirusową wraz z urządzeniem** |  |  |
| 36 | Ochrona przed atakami typu Spyware  | Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.  |  |  |
| Reguły/silnik anty-spyware musi być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  | SPEŁNIA/NIE SPEŁNIA |  |
| Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu, bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.  |  |  |
| Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. **Zamawiający wymaga dostarczenia licencji na silnik Antyspyware wraz z urządzeniem** |  |  |
| 37 | Wykrywanie i blokada domen uznanych za złośliwe  | Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).  | SPEŁNIA/NIE SPEŁNIA |  |
| **Zamawiający wymaga dostarczenia licencji na ochronę DNS wraz z urządzeniem** |  |  |
| 38 | Wykrywanie aktywności sieci typu Botnet  | Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie wbudowanej analityki (wykraczającej poza statyczną listę wskazującą centra botnetów).  | SPEŁNIA/NIE SPEŁNIA |  |
| 39 | Funkcjonalność URL Flitering  | Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering.  |  |  |
| Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL.  |  |  |
| Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  | SPEŁNIA/NIE SPEŁNIA |  |
| Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.  |  |  |
| Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania.  |  |  |
| **Zamawiający wymaga dostarczenia licencji na URL Filtering wraz z urządzeniem** |  |  |
| 40 | Funkcjonalność ochrony przed atakami „zero day” i współpracy z sandboxem  | Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem.  |  |  |
| Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day.  | SPEŁNIA/NIE SPEŁNIA |  |
| Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. **Zamawiający wymaga dostarczenia licencji na wysyłanie plików wykonywalnych do sandboxa lokalnego i sandboxa chmurowego wraz z urządzeniem.** |  |  |
| 41 | Zarządzanie urządzeniem  | Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).  | SPEŁNIA/NIE SPEŁNIA |  |
| 42 | Definiowanie administratorów systemu oraz metoda ich uwierzytelniania  | System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu:  |  |  |
| a. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu  |  |  |
| b. Operator, który ma możliwość tylko odczytu konfiguracji.  |  |  |
| Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą  |  |  |
| a. bazy lokalnej,  |  |  |
| b. serwera LDAP,  | SPEŁNIA/NIE SPEŁNIA |  |
| c. RADIUS lub TACACS+  |  |  |
| d. SAML 2.0  |  |  |
| Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).  |  |  |
| 43 | Tryb pracy na urządzeniu  | Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej.  | SPEŁNIA/NIE SPEŁNIA |  |
| Realizacja tego wymagania musi opierać się o samo urządzenie – dopuszcza się realizacji koncepcji kandydackiej z wykorzystaniem centralnej konsoli zarządzania. Wówczas należy dostarczyć centralny system/konsolę zarządzania. Konsola ta musi zarządzać min. 5 firewallami fizycznymi producenta i przechowywanie co najmniej 3TB logów przy założeniu obsługi co najmniej 4000 zdarzeń na sekundę (peak EPS). |  |  |
| Funkcja ta musi być realizowana co najmniej przez graficzny interfejs zarządzania firewallem (GUI).  |  |  |
| 44 | Interfejs API  | Urządzenie musi zapewniać interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).  | SPEŁNIA/NIE SPEŁNIA |  |
| Urządzenie musi wspierać co najmniej jeden z poniższych standardów API  |  |  |
| a. JSON,  |  |  |
| b. REST,  |  |  |
| c. XML  |  |  |
| 45 | Pamięć konfiguracji  | Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia.  | SPEŁNIA/NIE SPEŁNIA |  |
| Urządzenie musi mieć możliwość przywrócenia konfiguracji z określonego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.  |  |  |
| 46 | Eksport logów  | Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.  | SPEŁNIA/NIE SPEŁNIA |  |
| 47 | Zasilanie  | Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie  | SPEŁNIA/NIE SPEŁNIA |  |
| 48 | GwarancjaUsługa wsparcia technicznego  | Gwarantująca poprawne działanie urządzenia bądź jego wymianę w przypadku awarii oraz telefoniczne wsparcie serwisowe w trybie 24x7 zapewniająca wymianę uszkodzonego urządzenia na następny dzień Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.  | SPEŁNIA/NIE SPEŁNIA |  |
|  |

Składając niniejszą ofertę , oświadczam/y, że:

* + - 1. Zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia, w tym projektem umowy, jak też z innymi dokumentami oraz warunkami wykonania zamówienia. Do dokumentów i warunków nie wnosimy zastrzeżeń i uznajemy się za związanych określonymi w nich postanowieniami, a w przypadku wyboru naszej oferty podpiszemy umowę zgodnie z treścią przedstawioną przez Zamawiającego i w terminie wskazanym przez Zamawiającego,
			2. Zaoferowana przez nas cena obejmuje pełny zakres przedmiotu zamówienia i wszystkie koszty, które są związane z wykonanie przedmiotu zamówienia.
			3. Akceptujemy wskazany w SIWZ termin związania ofertą.
			4. Odpis z właściwego rejestru dostępny jest pod adresem internetowym:

………………………………………………………………………………………………

* + - 1. Oświadczamy, że zamówienie zrealizujemy sami\* / z udziałem podwykonawców w następujących częściach zamówienia\*:

..................................................................................................................................................................

*(wskazać nazwę i adres podwykonawcy i części zamówienia podlegające realizacji przez podwykonawców)*

* + - 1. Pod groźbą odpowiedzialności karnej oświadczam/y, że załączone do oferty dokumenty opisują stan prawny i faktyczny aktualny na dzień upływu terminu składania ofert (art. 297 k.k.).
			2. Następujące dokumenty znajdują się w posiadaniu Zamawiającego:

 ...............................................................................................................................................................

* + - 1. Wartość lub procentowa część zamówienia, jaka zostanie powierzona podwykonawcy lub podwykonawcom (jeżeli dotyczy) ……....……………….
			2. Oświadczam, że wykonałem obowiązek informacyjny RODO.
			3. Jesteśmy związani ofertą przez okres 60 dni.
			4. Wadium należy zwrócić na rachunek nr ……………………………………………………………………………..

11.Załącznikami do niniejszej oferty są**:**

…………………………………

…………………………………

7. Informujemy, że jesteśmy:

* mikroprzedsiębiorstwem (przedsiębiorstwo które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 000 000 euro)
* małym przedsiębiorstwem (przedsiębiorstwo które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 000 000 euro
* średnim przedsiębiorstwem (przedsiębiorstwo które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudnia mniej niż 250 osób i którego roczny obrót nie przekracza 50 000 000 euro lub roczna suma bilansowa nie przekracza 43 000 000 euro)
* żadne z powyższych

Zaznaczyć właściwe. Informacje te wymagane są wyłącznie do celów statystycznych.

*\* niepotrzebne skreślić*

.............................., dnia ......... ……. roku .............................................................. *podpis osoby upoważnionej do reprezentowania Wykonawcy*