Kraków, dn. 03.04.2023 r.

SZP-271/8-2/2023

**Do wszystkich zainteresowanych**

**Dot. sprawy: SZP/7/2023 - wyjaśnienie i zmiany treści SWZ/Opisu potrzeb i Wymagań**

Dotyczy postępowania o udzielenie zamówienia publicznego na: „**Dostawa serwerów i macierzy, elementów sieciowych oraz UPS”.**

1. **WYJAŚNIENIA TREŚCI SWZ/ Opisu Potrzeb i Wymagań**

Działając na podstawieart. 135 ust. 2ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (zwana dalej: PZP), Zamawiający przekazuje poniżej treść zapytań, które wpłynęły do Zamawiającego wraz z wyjaśnieniami:

**Pytanie 1**

Pytania do SWZ dot. Pakietu 4 – Dostawa urządzeń UPS:

1) Ad. Wymaganie 5.

Czy Zamawiający dopuszcza możliwość zmiany ilości gniazd wyjściowych na 6 x IEC C13 + 3 x IEC C19?

**ODPOWIEDŹ: Tak, pod warunkiem, że Wykonawca dostarczy rozdzielacz z IEC C19 na IEC C13 z minimum 2 portami IEC C13 montowanymi w szafie 19’zapewniającyą obciążalność IEC C13 min 8A każdy (razem 16 A)**

**Pytanie 2**

Pytania do SWZ dot. Pakietu 4 – Dostawa urządzeń UPS:

2) Ad. Wymaganie 6.

Czy Zamawiający dopuszcza możliwość zastosowania listwy zaciskowej?

**ODPOWIEDŹ: TAK Zamawiający dopuszcza.**

**Pytanie 3**

Dotyczy pakietu nr 4 – Dostawa urządzeń UPS
Czy Zamawiający w parametrze liczba gniazd dopuści zaoferowanie urządzenia o następujących gniazdach: C13 x 6, C19 x 3?

**ODPOWIEDŹ: Odpowiedź jak w pytaniu nr 1**

**Pytanie 4**

Czy Zamawiający w parametrze typ gniazda sieciowego dopuści zaoferowanie urządzenia z listwą zaciskową?

**ODPOWIEDŹ: TAK, Zamawiający dopuszcza.**

**Pytanie 5**

Czy Zamawiający poprzez czas podtrzymania dla obciążenia 50% UPS, rozumie czas podtrzymania dla 2kW tj. 50% minimalnej mocy czynnej urządzenia?
Jeżeli zaproponujemy UPS o PF =1 (5kVA/5kW), to 50% mocy wyniesie 2,5kW, i obliczając czas podtrzymania dla takiej mocy lepsze rozwiązanie (wyższy współczynnik mocy), otrzyma mniejszą ilość punktów.

**ODPOWIEDŹ: Czas podtrzymania liczony dla 50% minimalnej wymaganej mocy, czyli odpowiednio 2 kW**

**Zapis wymagań w punkcie 11 pakietu nr 4 ulega zmianie**

**Było „**Czas podtrzymania dla obciążenia 50% UPS**”**

**Jest „**Czas podtrzymania dla 50% minimalnego wymaganego obciążenia UPS tj. 2 kW**”**

1. **ZMIANA TREŚCI SWZ/ Opisu Potrzeb i Wymagań**

Działając w oparciu o art. 137 ust. 2PZP, Zamawiający informuje, że zmianie uległy zapisy SWZ/Opisu Potrzeb i Wymagań.

Zamawiający informuje, że dokonuje następujących zmian:

* SWZ, Rozdz. XXIX OPIS KRYTERIÓW OCENY OFERT, ust. 1 pkt 4) Pakiet 4 - Dostawa urządzeń UP, w następujący sposób (zmiany zaznaczono kolorem czerwonym):
* cena oferty - waga 60 %
* parametry techniczne - waga 40 %

Punkty oferty zsumowane wg wzoru:

**Sof = Cof + Ptof**

gdzie:

 **Sof**  - suma punktów badanej oferty,

**Cof**  - ilość punktów uzyskanych za kryterium „cena”,

**Ptof** - ilość punktów uzyskanych za kryterium „parametry techniczne”.

1. W kryterium „cena” zostanie zastosowany następujący wzór:

**Cof = (Cmin : C) x 60 pkt**

gdzie:

**Cof**- liczba punktów w zakresie tego kryterium,

**C min** - najniższa zaoferowana cena brutto spośród badanych i nieodrzuconych ofert,

**C**- cena badanej oferty brutto,

* ceny w powyższym wzorze rozumiane są jako ceny brutto za realizację całości przedmiotu zamówienia (pakietu);
* maksymalna liczba punktów do uzyskania w kryterium „cena” – 60 pkt;
* ocenie w ramach kryterium „Cena” podlegać będzie cena łączna brutto podana w formularzu ofertowym - ZAŁĄCZNIK NR 1 DO SWZ.
* Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) usługi, których świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
1. W kryterium „parametry techniczne” zostanie zastosowany wzór:

**Ptof = (Pt: Ptmax) x 40 pkt**

gdzie:

|  |  |  |
| --- | --- | --- |
| **Pof** | - | liczba punktów w zakresie tego kryterium, |
| **Pt** | - | suma punktów badanej oferty, |
| **Ptmax** | - | maksymalna ilość punktów, uzyskana w zakresie tego kryterium wśród badanych i nieodrzuconych ofert |

* Ocena zostanie dokonana w oparciu o informacje podane w złożonym FORMULARZU CENOWYM WRAZ ZE SZCZEGÓŁOWYM OPISEM PRZEDMIOTU ZAMÓWIENIA ZAŁĄCZNIK NR 2 do SWZ.

|  |  |
| --- | --- |
| **Czas podtrzymania dla ~~obciążenia 50% UPS~~****50%minimalnego wymaganego obciążenia UPS tj. 2 kW** | * 10 min - 0 pkt
* powyżej 10 min – 30 min – za każde pełne dodatkowe 30 s + 1 pkt
* 30 min i powyżej - 40 pkt
 |

* maksymalna liczba punktów do uzyskania w kryterium „parametry techniczne” – 40 pkt;
* jeżeli wykonawca poda w ofercie czas podtrzymywania ~~dla obciążenia 50% UPS~~ 50% minimalnego wymaganego obciążenia UPS tj. 2 kW większy niż oceniany przez zamawiającego (większy niż 30 min), to zamawiający obliczy punkty dla maksymalnie punktowanego czasu podtrzymywania dla ~~obciążenia 50% UPS~~ 50% minimalnego wymaganego obciążenia UPS tj. 2 kW, czyli 30 min.
* Załącznik nr 2 do SWZ, Formularz cenowy wraz ze szczegółowym opisem przedmiotu zamówienia, w sposób wskazany w załączniku nr 1 do niniejszych odpowiedzi (zmiany zaznaczono kolorem czerwonym).

Zamawiający informuje, że w wyniku dokonanych zmian dokonał zmiany treści ogłoszenia o zamówieniu. Sprostowanie ogłoszenia nie zostało opublikowane przed upływem 48 godzin od potwierdzenia przez UPUE otrzymania ogłoszenia.

Zamawiający informuje, że pozostałe zapisy SWZ nie ulegają zmianie.

Specjalista

ds. Zamówień Publicznych

mgr Anna Winiarska

**ZAŁĄCZNIK NR 1 DO ODPOWIEDZI NA PYTANIA**

**ZAŁĄCZNIK NR 2 DO SWZ**

**Formularz cenowy wraz ze szczegółowym opisem przedmiotu zamówienia**

**UWAGA**

1. Zamawiający wymaga sprzętu nowego nie starszego niż wyprodukowanego w 2022 r.
2. Obowiązek wykazania równoważności zaoferowanego sprzętu/urządzeń/oprogramowania leży po stronie Wykonawcy. W tym celu Wykonawca winien przedstawić oświadczenie i dokumenty potwierdzające równoważność.
3. Cenę oferty należy wyliczyć w sposób podany w poniższej tabeli

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość/ jednostka miary** | **Cena jednostkowa netto** | **Cena jednostkowa brutto** | **Stawka podatku VAT** | **Wartość netto** | **Wartość brutto** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| 1 | ….. | …. |   | suma ceny jednostkowej netto i iloczynu stawki podatku VAT i ceny jednostkowej netto |  | iloczyn ilości i ceny jednostkowej netto | suma wartości netto i iloczynu stawki podatku VAT i wartości netto |
| 2 | …. |   |   |  |  |  |  |

**Pakiet 1 - Dostawa macierzy dyskowych – 2 szt.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT**  | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | Macierze dyskowe | 2 szt. |  |  |  |  |  |
| **Razem:** |  |  |

|  |  |
| --- | --- |
| **Producent** |  |
| **Nazwa** |  |
| **Model** |  |
| **Okres gwarancji** *(min. okres gwarancji 36 miesięcy, max. punktowany okres gwarancji – 60 miesięcy)* | ………… miesiące/cy*\*) podać okres gwarancji w okresach sześciomiesięcznych* |
| **Przestrzeń netto dla dysku SSD (RAID 5)***(min. 5,5 TB)* | ………… TB |

|  |
| --- |
| **SERWIS GWARANCYJNY****(WYPEŁNIA OFERENT):** |
| Nazwa: |  |
| Adres: |  |
| Telefon: |  |
| e-mail: |  |
| Godz. urzędowania serwisu: |  |

1. Zamówienie dotyczy dostarczenia systemu pamięci masowej składającego się z pojedynczej macierzy. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN lub tak zwanym wirtualizatorem w sieci SAN.
2. Oferowane urządzenie musi być rozwiązaniem kompletnym, pochodzącym od jednego producenta, dostępne w ofercie Wykonawcy przed ukazaniem się niniejszego postępowania.
3. Macierze i ich elementy składowe zostaną zainstalowane w posiadanych przez Zamawiającego szafach zgodnych ze standardem typu Rack 19”.
4. Kompletna pojedyncza macierz (kontroler wraz z półkami dyskowymi, modułem zarządzającym, jeśli taki występuje) nie może przekroczyć wysokości 4U.
5. Macierz dyskowa musi być wyposażona w co najmniej jedną parę redundantnych kontrolerów pracujących w trybie active-active.
6. Ze względu na wydajność i wielowątkowość pracy wymagane jest, aby każdy kontroler macierzy wyposażony był w co najmniej 6 rdzeniowy procesor.
7. Wymagane jest, aby każdy kontroler oferowanej macierzy dyskowej wyposażony był w co najmniej 64 GB pamięci cache.
8. Macierz dyskowa musi posiadać funkcjonalność partycjonowania pamięci cache. Jeżeli funkcjonalność taka wymaga licencji to należy taką licencję dostarczyć.
9. Macierz musi być wyposażona w dwa redundantne zasilacze.
10. W przypadku awarii zasilania dane nie zapisane na dyskach, przechowywane w pamięci cache muszą być zabezpieczone metodą trwałego zapisu na dedykowany do tego celu dysk lub nieulotną pamięci podręczną.
11. Oferowana macierz dyskowa musi mieć możliwość obsługi połączeń do systemów klienckich o prędkościach i protokołach co najmniej:
12. 16Gbps FC,
13. 32Gbps FC,
14. 10Gbps iSCSI (zarówno przez interfejs optyczny jak i przez interfejs RJ45 BASE-T)
15. Oferowana macierz musi być macierzą blokową i wykonywać operacje I/O na poziomie bloków danych. Nie dopuszcza się rozwiązania, w którym blokowe wolumeny macierzy emulowane są w oparciu o wewnętrzny system plików proponowanego rozwiązania.
16. Oferowana macierz dyskowa musi być wyposażona w co najmniej 12 portów FC o prędkości 16Gbps FC
17. Ze względu na możliwości wydajnościowe i wielowątkowość operacji kontrolery obsługujące dyski muszą być wyposażone w minimum 16 połączeń, co najmniej 12 Gbps SAS każde. Wszystkie połączenia powinny być aktywne.
18. Macierz musi umożliwiać konfigurację replikacji synchronicznej i asynchronicznej. Jeżeli taka funkcjonalność jest dodatkowo licencjonowana, wymaga się dostarczenia takiej licencji bez ograniczeń w zakresie obsługiwanej przestrzeni dyskowej.
19. Macierz musi umożliwiać w przyszłości połączenie dwóch macierzy w klaster, w którym obydwie macierze służą do jednoczesnego odczytu i zapisu danych dla każdego z wolumenów (klaster typu active-active), bez konieczności zakupu dodatkowych urządzeń. Wolumen logiczny dla takiego klastra musi mieć swoją prezentację na obydwu macierzach. Jeżeli taka funkcjonalność jest dodatkowo licencjonowana, nie wymaga się dostarczenia takiej licencji w niniejszym postępowaniu,
20. Wymagane jest, aby macierz dyskowa wspierała różne poziomy zabezpieczeń RAID w tym, co najmniej RADI 1, RAID-5, RAID-6.
21. Macierz musi obsługiwać dyski typu: SSD, SAS 10k, NL-SAS 7,2k
22. Macierz musi umożliwiać rozbudowę do co najmniej 192 dysków.
23. Macierz musi być skalowalna do co najmniej 2,8PB przestrzeni na wewnętrznych dyskach. Poprzez rozbudowę rozumie się dołączenie do macierzy dyskowej kolejnych półek dyskowych producenta macierzy. Wymaga się dostarczenia licencji na pełną wartość obsługiwanej przestrzeni dyskowej.
24. Oferowana macierz musi posiadać możliwość zdefiniowania i udostępnienia serwerom co najmniej 16 tysięcy wolumenów logicznych bez konieczności dokupienia i instalacji dodatkowych licencji.
25. Macierz dyskowa musi umożliwiać utworzenie wolumenu logicznego o rozmiarze co najmniej 60TB.
26. Macierz musi posiadać możliwość definiowana wirtualnych wolumenów logicznych, których pojemność może być większa od rzeczywistej przestrzeni dyskowej skonfigurowanej w obrębie puli dysków twardych („thin provisioning”). Funkcjonalność „thin provisioning” musi być dostarczona wraz z oferowaną macierzą z licencją na nieograniczoną pojemność dyskową. Umożliwiać wystawienie cienkich wolumenów o łącznej pojemności 4.4 PB
27. Przestrzeń proponowanej macierzy dyskowej musi być zbudowana z min. 4 dysków o pojemności min. 1,9 TB SSD oraz 4 dysków 2,4TB NL-SAS. Dodatkowo wymaga się dostarczenia w ramach oferowanej konfiguracji dysków typu „hot-spare” dla każdego typu wymienionych dysków.

Parametr oceniany przestrzeń netto dla dysków SSD (RAID 5)

5,5 TB -> 0 pkt

Powyżej 5,5 TB do 15,5 TB Za każdy pełny 1 TB -> 2 pkt

15,5 TB i powyżej - 20 pkt

1. Macierz musi obsługiwać rozkładanie danych w oparciu o architekturę trzy poziomowego tieringu. Tiering danych musi mieć możliwość zbudowania puli dyskowej w oparciu o warstwy dysków: flash/SSD, SAS, NL-SAS. Jeżeli ta funkcjonalność wymaga licencji to należy ją dostarczyć na pełną przestrzeń wewnętrzną obsługiwaną przez macierz.
2. Tiering danych musi być zaimplementowany w kontrolerach macierzy dyskowej i musi posiadać możliwość dynamicznego i automatycznego relokowania fragmentów wolumenów logicznych pomiędzy co najmniej dwoma różnymi klasami pamięci masowej („auto tiering”). Administrator musi mieć możliwość wyboru polityki definiującej warstwę, na którą zapisywane są dane w pierwszej kolejności. Dane z warstwy niższej muszą być promowane do warstwy zbudowanej w oparciu o dyski flash/SSD w sposób natychmiastowy, bez konieczności oczekiwania na zakończenie cyklu monitorowania. Funkcjonalność ta ma być dostarczona wraz z oferowaną macierzą z licencją na nieograniczoną pojemność dyskową. Jeżeli ta funkcjonalność wymaga licencji to należy ją dostarczyć na pełną przestrzeń wewnętrzną obsługiwaną przez macierz.
3. Macierz posiada możliwość wykonywania pełnych kopii typu klon i pozwalać na:
4. wykonywanie co najmniej 3 kopii pełnych dla pojedynczego wolumenu źródłowego.
5. re-synchronizację danych pomiędzy wolumenami źródłowym i kopią. Podczas wykonywania re-synchronizacji pomiędzy wolumenami kopiowane powinny być tylko dane różnicowe.
6. funkcjonalność ta ma być dostarczona z licencją na nieograniczoną pojemność dyskową oraz nieograniczoną ilość wolumenów.
7. Macierz musi posiadać możliwość migracji całych wolumenów pomiędzy różnymi dyskami wewnątrz macierzy. Migracja ma odbywać się w sposób przeźroczysty dla aplikacji (online). Funkcjonalność ta musi być dostarczona wraz z oferowaną macierzą z licencją na nieograniczoną pojemność dyskową.
8. Macierz posiada wsparcie producenta na okres deklarowany w złożonej ofercie jednak nie krótszy niż 36 miesięcy. Bezwzględnie wymagana jest opcja pozostawiania uszkodzonych dysków u Zamawiającego

Parametr oceniany

36 miesięcy - 0 pkt

42 miesiące – 5 pkt

48 miesięcy – 10 pkt

54 miesiące – 15 pkt

60 miesięcy lub więcej - 20 pkt

1. Macierze musi posiadać oprogramowanie do zarządzania, pozwalające na co najmniej:
2. Tworzenie i nazywanie wolumenów logicznych LUN
3. Mapowanie wolumenów logicznych do serwerów
4. Monitorowanie wykorzystywanej przestrzeni, efektywnej i surowej (RAW) macierzy
5. Tworzenie raportów z konfiguracji macierzy dyskowej
6. Zarządzanie macierzą za pomocą CLI i możliwości tworzenia skryptów z wykorzystaniem komend
7. Zarządzanie wieloma macierzami jednego producenta z jednej konsoli graficznej
8. Należy dostarczyć oprogramowanie pozwalające na całodobowe monitorowanie stanu macierzy i automatyczne informowanie administratorów Zamawiającego o wystąpieniu ewentualnej awarii macierzy. Jeżeli ta funkcjonalność wymaga licencji to należy ją dostarczyć wraz z urządzeniem.
9. Macierz musi być fabrycznie nowa i pochodzić z oficjalnego kanału dystrybucyjnego.

**Pakiet 2 - Dostawa serwerów i oprogramowania**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT**  | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | Serwery | 2 szt. |  |  |  |  |  |
|  | Oprogramowanie do wirtualizacji | 1 szt. |  |  |  |  |  |
|  | System operacyjny MS SQL Standard | 2 szt. |  |  |  |  |  |
|  | System do wykonywania kopii zapasowych – oprogramowanie do backupu | 1 szt. |  |  |  |  |  |
| **Razem:** |  |  |

**Urządzenia oferowane**

|  |  |
| --- | --- |
| **Producent** |  |
| **Nazwa** |  |
| **Model** |  |

|  |  |
| --- | --- |
| **Dodatkowy okres gwarancji** *(dodatkowe 12 miesięcy gwarancji)*Tak – 5 pktNie – 0 pkt |  |
| **Dodatkowy okres gwarancji** *(dodatkowe wsparcie z gwarantowanym czasem naprawy w ciągu 6 godzin)*Tak – 5 pktNie – 0 pkt |  |
| **Pamięć operacyjna** *(min. 256 GB*) | ………… GB |
| **Dyski** *(min. 480 GB)* | ………… GB |

|  |
| --- |
| **SERWIS GWARANCYJNY****(WYPEŁNIA OFERENT):** |
| Nazwa |  |
| Adres: |  |
| Telefon: |  |
| e-mail: |  |
| Adres strony internetowej serwisu |  |
| Numer infolinii telefonicznej |  |
| Godz. urzędowania serwisu: |  |

|  |  |  |
| --- | --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis wymagań Serwerów** | **Wymagania oferowane****(wypełnia oferent)** |
| **Obudowa** | Do instalacji w szafie Rack 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Obudowa ma umożliwiać instalację do 12 dysków 2,5”  |  |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – maksymalnie 140W. Wymagana ilość rdzeni dla procesora – 8. Minimalna częstotliwość pracy procesora 3.2GHz. Procesor obsługuje pamięć z prędkością 3200MHz. Minimalna ilość kanałów procesora – 8. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie może być niższy niż 138 punktów base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. (dołączyć wydruk PDF) |  |
| **Liczba zainstalowanych procesorów**  | 2 |  |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta bądź wyprodukowana na zlecenie producenta serwera z możliwością zainstalowania do dwóch procesorów w architekturze x86 wykonujących 64-bitowe instrukcje  |  |
| **Pamięć operacyjna** | Zainstalowane minimum 256GB pamięci RAM o częstotliwości 3200MHz. Kości pamięci min. 32GB. Zainstalowana pamięć ma być sygnowana i zoptymalizowana do użycia przez producenta serwera. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM przy użyciu pamięci RDIMM.Łączna ilość możliwej do zainstalowana pamięci RDIMM oraz pamięci persistent memory ma wynosić minimum 12TBParametr oceniany: 256 GB- > 0 pktPowyżej 256GB do 512 GB **-** 2,5 pkt za każde dodatkowe 32GB512 GB i więcej 20 pkt |  |
| **Zabezpieczenie pamięci** | Memory mirroring, ECC, SDDC |  |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. |  |
| **Dyski** | Trzy identyczne dyski SSD 2,5” o pojemności minimum 480GB każdy. Dyski muszą mieć wytrzymałość na poziomie minimum 1.5 DWPD.Parametr oceniany:480 GB -> 0 PKTpowyżej 480 GB-> do 1,9 TG za każde dodatkowe 240 GB 1 pkt 1,9 TB lub więcej -> 10 PKT |  |
| **Rozbudowa dysków** | Serwer musi posiadać w momencie dostawy możliwość zainstalowania minimum 8 dysków SAS/SATA 2,5”. Możliwość instalacji modułu na 7mm dyski SSD lub NVMe. Moduł musi mieć możliwość instalacji 2 dysków spiętych w RAID 1. Możliwość instalacji modułu na dyski M.2. SSD lub NVMe Moduł musi mieć możliwość instalacji 2 dysków spiętych w RAID 1. |  |
| **Kontroler dyskowy** | Serwer musi mieć zainstalowany kontroler dyskowy obsługujący poziomy RAID 0/1/10/5/50. Możliwość wymiany kontrolera na kontroler posiadający min 8GB pamięci cache.  |  |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinum. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji. |  |
| **Interfejsy sieciowe** | Zainstalowana jedna dwuportowa karta 10/25Gb SFP28. Karta nie może zajmować żadnego ze slotów PICe. Karta musi być wyposażona we wkładki optyczne 10Gb Multimode. Wymagana funkcjonalność zainstalowanych kart: sprzętowa obsługa protokołów VXLAN, NVGRE, GENEVE, obsługa ruchu sieciowego z podziałem na poszczególne maszyny wirtualne, obsługa do 256 kolejek dla maszyn wirtualnych, obsługa ramek Jumbo do 9.6Kb, obsługa 802.1p, 802.3ad.Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. Jedna dwuportowa karta FC HBA 16Gb |  |
| **Sloty I/O PCIe** | Serwer ma posiadać 2 sloty PCIe x16 generacji 4. Możliwość rozbudowy o kolejny slot PCIe x16 generacji 4. |  |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.1, 1x USB 2.0 (współdzielony z systemem zarządzania). Możliwość zainstalowania portu VGA z przodu obudowy
* z tyłu obudowy: 3x USB 3.1, 1x VGA Możliwość instalacji portu DB9
* wewnątrz: 1x USB 3.1
 |  |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |  |
| **Zarządzanie** | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający:* Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
* Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O
* Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
* Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.
* Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3
* Update systemowego firmware
* Monitoring i możliwość ograniczenia poboru prądu
* Zdalne włączanie/wyłączanie/restart
* Zapis video zdalnych sesji
* Podmontowanie lokalnych mediów z wykorzystaniem Java client
* Przekierowanie konsoli szeregowej przez IPMI
* Zrzut ekranu w momencie zawieszenia systemu
* Możliwość przejęcia zdalnego ekranu
* Możliwość zdalnej instalacji systemu operacyjnego
* Alerty Syslog
* Przekierowanie konsoli szeregowej przez SSH
* Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera
* Możliwość mapowania obrazów ISO z lokalnego dysku operatora
* Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
* Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
* wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API
* Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.

Wraz z serwerem musi zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:- zarządzenie infrastruktura serwerów, przełączników i storage bez udziału dedykowanego agenta- przedstawianie graficznej reprezentacji zarządzanych urządzeń- możliwość skalowania do minimum 1000 urządzeń- obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2- wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych- udostępnianie szybkiego podgląd stanu środowiska- udostępnianie podsumowania stanu dla każdego urządzenia- tworzenie alertów przy zmianie stanu urządzenia- monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,- konsola zarzadzania oparta o HTML 5- dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,- automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja- możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania- definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń- definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell- obsługa SNMP, SYSLOG, Email Forwarding- autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML- obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami- przedstawianie historycznych aktywności użytkowników-blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv- Obsługa NTP- przesyłanie alertów do konsoli firm trzecich- tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie- możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesypem plików diagnostycznych,Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami:VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. |  |
| **Funkcje zabezpieczeń** | Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł TPM. Możliwość zainstalowania przedniego panelu zamykanego na klucz.  |  |
| **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. |  |
| **Obsługa** | Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser’ów PCIe, backplane’ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych. |  |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAIDMożliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera. |  |
| **Wspierane Systemy operacyjne** | Microsoft Windows Server 2016, 2019, 2022, Red Hat Enterprise Linux 7, 8, 9 SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6, 7, Ubuntu 18, 20, 22 |  |
| **Gwarancja** | 36 miesięcy gwarancji producenta z oknem serwisowym 9x5, z czasem reakcji NBD. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalne jak i wydajnościowo wymagane powyżej urządzenia. Wszystkie komponenty nadmiarowego serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.Parametr oceniany- dodatkowe wsparcie z gwarantowanym czasem naprawy w ciągu 6 godzin – 5 pkt- dodatkowe 12 miesięcy gwarancji - 5 pkt |  |

1. **Oprogramowanie do wirtualizacji**

**Oferowane oprogramowanie**

|  |  |
| --- | --- |
| **Producent** |  |
| **Nazwa** |  |

VMware vSphere 7 Essentials Plus Kit lub równoważne.

Zamawiający wymaga, aby licencje dostarczone były wraz ze wsparciem technicznym (w okresie gwarancji serwerów). Wsparcie musi być świadczone przez producenta serwerów lub podmiot wskazany przez producenta serwerów. Możliwość pobierania nowych wersji i poprawek w całym okresie trwania oferowanego wsparcia.

**Opis równoważności dla systemu wirtualizacji:**

Cechy równoważnego oprogramowania typu VMware vSphere 7 Essentials Plus Kit:

1. Pakiet oprogramowania systemu wirtualizacyjnego będzie przeznaczony do wirtualizacji serwerów. Oprogramowanie do wirtualizacji serwerów będzie przeznaczone na klaster wirtualizacyjny składający się docelowo z maksymalnie trzech serwerów dwuprocesorowych.
2. Oferowany system wirtualizacji musi posiadać następujące cechy i funkcjonalności:
	1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
	2. Musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług;
	3. Powinien w możliwie największym stopniu być niezależny od producenta platformy sprzętowej.
	4. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012/R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10/11, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Solaris, Debian GNU/Linux, CentOS, w tym oferowany System Operacyjny.
	5. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
	6. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej.
	7. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
	8. Powinien zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
	9. Musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
	10. System wirtualizacyjny oraz oprogramowanie zarządzające tymże systemem musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
	11. Rozwiązanie musi mieć możliwość przenoszenia uruchomionych maszyn wirtualnych pomiędzy serwerami fizycznymi (tzw. „migracja na gorąco”). Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
	12. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
	13. Musi umożliwiać zapewnienie odpowiedniej redundancji i takiego mechanizmu (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego działające na nim wirtualne maszyny zostały automatycznie uruchomione na innych fizycznych serwerach klastra z zainstalowanym oferowanym oprogramowaniem wirtualizacyjnym.
	14. Musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów;
	15. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
	16. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
3. **System Operacyjny**

Windows Server 2022 Standard - 16 Core License Pack - 2 szt lub równoważny

MS SQL Standard 2 szt lub równoważny

Równoważność:

Zamawiający dopuszcza możliwość dostawy licencji oprogramowania równoważnego, o parametrach nie gorszych niż wskazane, o ile będzie to oprogramowanie w pełni zgodne i kompatybilne z aplikacjami ERP enova oraz spełniające poniższe wymagania minimalne:

a) Oprogramowanie silnika baz danych przeznaczone do instalacji w ramach lokalnej infrastruktury sprzętowej i programowej posiadanej przez Zamawiającego. Silnik zostanie zainstalowany na serwerze Microsoft Windows Server Standard 2022 lub alternatywnie instancja zgodnego systemu operacyjnego dostarczonego przez Wykonawcę wraz z silnikiem baz danych może być zainstalowana na maszynie wirtualnej działającej pod kontrolą dostarczonego przez wykonawcę wirtualizatora (pkt 2 pakietu)

b) Ilość oferowanych licencji oprogramowania silnika baz danych musi zapewnić wykorzystanie mocy obliczeniowej min. 16 rdzeni procesora oraz min. 256 GB pamięci RAM

c) Ilość oferowanych licencji oprogramowania silnika baz danych musi umożliwiać pełne wykorzystanie silnika dla min. 3 użytkowników z nieograniczonej puli stanowisk dostępowych

d) Zarządzanie silnikiem baz danych dostępne będzie z poziomu narzędzia graficznego (aplikacja typu desktop lub aplikacja obsługiwana w przeglądarce WWW). Wszystkie funkcje zarządzania muszą być dostępne lokalnie bez wymaganego dostępu do sieci Internet. Narzędzie graficzne do zarządzania silnikiem musi zapewniać możliwość zarządzania i konfiguracji wszystkich usług implementowanych przez silnik baz danych.

e) Dostępna funkcja profilowania silnika baz danych, rejestrująca określone wg filtra zapytania spływające do silnika baz danych w czasie rzeczywistym w formie dziennika zdarzeń, której zadaniem będzie identyfikacja ewentualnych problemów lub błędów w działaniu aplikacji

f) Zarządzanie silnikiem baz danych dostępne będzie z poziomu narzędzia linii poleceń umożliwiające automatyzację czynności administracyjnych, min.:

a. Wykonywanie zadań kopii zapasowych

b. Zarządzanie kontami użytkowników

c. Zarządzanie uprawnieniami użytkowników

d. Zarządzanie pracą silnika baz danych (min. akcje uruchomienia i zatrzymania pracy silnika)

e. Wykonywanie zapisanych skryptów poleceń SQL z obsługą przekierowywania wyjścia na standardowe wyjście konsoli lub do pliku

g) Obsługa aktualizacji automatycznych dla silnika musi umożliwiać automatyczne ściąganie i instalację poprawek bezpieczeństwa producenta oprogramowania dla minimalizacji zagrożeń powodowanych przez wykryte luki w zabezpieczeniach oprogramowania silnika

h) Silnik baz danych musi posiadać mechanizm pozwalający na duplikację określonych baz danych między dwiema instancjami, zapewniający replikację danych w czasie rzeczywistym

i) Silnik baz danych musi obsługiwać mechanizm kompresji kopii zapasowych w trakcie ich tworzenia

j) Obsługa automatycznego szyfrowania kopii zapasowych baz danych (w trakcie wykonywania) przy użyciu min. funkcji kryptograficznej AES-256 z użyciem klucza asymetrycznego. Możliwość szyfrowania kopii zapasowych baz danych niezaszyfrowanych.

k) Wsparcie dla zastosowanych w MIK reguł bezpieczeństwa, min. zastosowanie mechanizmu weryfikacji dostatecznego poziomu długości i komplikacji haseł użytkowników, możliwość zintegrowania uwierzytelniania użytkowników z Acive Directory

l) Automatyczne rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym o następujących cechach:

a. Zredukowany do minimum negatywny wpływ logowania na wydajność silnika baz danych

b. Możliwość selektywnego wybierania rejestrowanych zdarzeń takich jak: monitorowanie stanu obciążenia silnika, operacje odczytu i zapisu danych na dysku, przekroczenie czasu wykonywania operacji, aktywność użytkownika

m) Możliwość definiowania nowych typów danych przechowywania z obsługą danych hierarchicznych. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Wykonawcę języku programowania SQL.

n) Obsługa danych w formacie XML w zakresie umożliwiającym składowanie i obróbkę danych w postaci struktur XML. Silnik musi zapewniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli oraz zapewnić mechanizm do walidacji struktur XML wykorzystując szablony XSD. Ponadto silnik musi udostępniać język zapytań zgodny ze standardem XQuery do obsługi struktur XML

o) Obsługa tworzenia funkcji i procedur w innych językach programowania z możliwością ich uruchomienia z poziomu zapytań SQL lub wyzwalaczy SQL Trigger

W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji oraz konwersji istniejących baz danych do formatu zgodnego z oferowanym silnikiem baz danych, zapewniając identyczne funkcjonowanie całego środowiska w stosunku do środowiska testowego z oprogramowaniem ERP enowa. Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do dostarczenia innego rozwiązania spełniającego wymagania OPZ. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

1. **System do wykonywania kopii zapasowych - oprogramowanie do backupu –1 szt.**

|  |  |
| --- | --- |
| **Producent** |  |
| **Nazwa** |  |

Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia oprogramowania do zabezpieczania środowiska Data Center Zamawiającego (baz danych, maszyn wirtualnych, serwerów plików, serwerów wolnostojących) zwanego dalej oprogramowaniem. Zabezpieczone backupem muszą być objęte wszystkie dostarczone w ramach niniejszego postępowania serwery oraz będący w posiadaniu Zamawiającego serwer kompresji (jako serwer fizyczny)

Wymagane jest dostarczenie wszystkich modułów oprogramowania tak, aby zapewnić backup całości wyspecyfikowanego środowiska oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności.

**Wymagania dotyczące backupu serwerów zwirtualizowanych**

1. Oprogramowanie do musi współpracować z oprogramowaniem wyspecyfikowanym w pkt 2 i 3 pakietu nr 2
2. Oprogramowanie musi współpracować z hostami zarządzanymi przez oprogramowanie wyspecyfikowane w pkt 2 pakietu nr 2 oraz pojedynczymi hostami.
3. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez oprogramowanie wyspecyfikowany w pkt 2 pakietu nr 2.
4. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
5. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
6. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
7. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe.
8. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
9. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu.
10. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
11. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
12. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów baz danych MS SQL oraz Oracle.
13. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu webowym.
14. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
15. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
16. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
18. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
19. Oprogramowanie musi integrować się bezpośrednio z HPE StoreServe, Nimble Storage Dell EMC VNX, VNXe, Unity, IBM Spectrum Virtualize (IBM Storwize, IBM SVC, Lenovo Storage V-series), Huawei OceanStor, Pure Storage FlashArray, i musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność musi działać w oprogramowaniu wyspecyfikowanym w pkt 2 pakietu nr 2.
20. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
21. Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server.
22. Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
23. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
24. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
25. Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
26. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
27. Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z oprogramowanie wyspecyfikowane w pkt 2 pakietu nr 2, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
28. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
29. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
30. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
31. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego oprogramowania wyspecyfikowanego w pkt 2 pakietu nr 2.
32. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).
33. Oprogramowanie musi umożliwiać uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny.
34. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
35. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
36. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
37. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla oprogramowania wyspecyfikowanego w pkt 2 pakietu nr 2.
38. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	1. Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs,
	2. Windows: NTFS, FAT, FAT32, ReFS.
39. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, rekordy DNS zintegrowane z AD, Microsoft System Objects, elementy AD Sites.
40. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.
41. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
42. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
43. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
44. Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
45. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
46. Oprogramowanie musi pozwalać na odtworzenie maszyn wirtualnych z macierzowych snapshotów ze wspieranych macierzy.
47. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
48. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
49. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
50. Oprogramowanie musi mieć podobne mechanizmy dla replik.
51. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

**Wymagania dotyczące backupu serwerów zwirtualizowanych**

1. Oprogramowanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
2. Oprogramowanie musi wspierać Windows 8 lub nowsze oraz Windows Server 2008 R2 SP1 lub nowsze.
3. Oprogramowanie musi wspierać Linux kernel 2.6.32 lub nowsze (zarówno 32 jak i 64bit) oraz wspierać następujące dystrybucje:
	1. Debian 6 – 9.7,
	2. Ubuntu 10.04 – 18.10,
	3. CentOS / Oracle Linux / RHEL 6 – 7.6,
	4. Oracle Linux (UEK) R4 U6, R4 U7,
	5. Fedora 23 – 29,
	6. openSUSE 11.3 - 13.2,
	7. openSUSE Leap 42.2 – 42.3,
	8. SLES 11 SP4 – 15,
	9. SLES for SAP 11 SP4 – 15,
4. Oprogramowanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików:
	1. NTFS,
	2. ReFS,
	3. FAT32,
	4. ext2, ext3, ext4,
	5. ReiserFS,
	6. JFS,
	7. XFS,
	8. F2FS,
	9. HFS,
	10. HFS+,
	11. NILFS2,
	12. Btrfs (dla kernela 3.16 i nowszych).
5. Oprogramowanie musi mieć możliwość instalacji oraz zarządzania poprzez centralną konsolę zarządzającą.
6. Oprogramowanie musi wspierać systemy oparte o Microsoft Failover Cluster.
7. Oprogramowanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.
8. Oprogramowanie musi wspierać backup podłączonych dysków USB.
9. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.
10. Oprogramowanie musi pozwalać na przechowywanie kopii zapasowych na:
	1. Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny.
	2. Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire.
	3. Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
	4. Zcentralizowanym repozytorium danych.
	5. Bezpośrednio na zasobach Chmury.
	6. Microsoft OneDrive/OneDrive for Business.
11. Oprogramowanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.
12. Oprogramowanie musi wspierać kontrolę pasma sieciowego.
13. Oprogramowanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.
14. Oprogramowanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.
15. Oprogramowanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Technologia śledzenia bloków dla systemów Windows Server musi być certyfikowana przez Microsoft.
16. Oprogramowanie musi wspierać technologię BitLocker.
17. Oprogramowanie musi wspierać uruchamianie z nośnika odtwarzania. Nośnik odtwarzania musi być automatycznie tworzony przez oprogramowanie.
18. Oprogramowanie musi wspierać wgrywanie dodatkowych sterowników podczas odtwarzania z wykorzystaniem nośnika odtwarzania.
19. Oprogramowanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
20. Oprogramowanie musi wspierać szyfrowanie.
21. Oprogramowanie musi wspierać tworzenie kopii zapasowych wykorzystując konsolę tekstową lub CLI na maszynie zabezpieczanej.
22. Oprogramowanie musi wspierać tworzenie wielu zadań backupowych.

**Monitoring środowiska oprogramowania**

1. Oprogramowanie musi umożliwiać monitorowanie środowiska wirtualizacyjnego zaoferowanego w niniejszym postępowaniu i być certyfikowane przed producenta oprogramowania wirtualizacyjnego.
2. Oprogramowanie musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w systemie zarządzania środowiskiem wirtualnym.
3. Oprogramowanie musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
4. Oprogramowanie musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
5. Oprogramowanie musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
6. Oprogramowanie musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
7. Oprogramowanie musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
8. Oprogramowanie musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
9. Oprogramowanie musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
10. Oprogramowanie musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
11. Oprogramowanie musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
12. Oprogramowanie musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
13. Oprogramowanie musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy wirtualizacyjnej.

**Raportowanie**

1. Oprogramowanie raportowania musi umożliwić tworzenie raportów z dostarczonej infrastruktury wirtualnej.
2. Oprogramowanie musi być certyfikowany przez producenta dostarczonego systemu wirtualizacji.
3. Oprogramowanie musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach.
4. Oprogramowanie musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
5. Oprogramowanie musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
6. Oprogramowanie musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
7. Oprogramowanie w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
8. Oprogramowanie musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
9. Oprogramowanie musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
10. Oprogramowanie musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
11. Oprogramowanie musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
12. Oprogramowanie musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
13. Oprogramowanie musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
14. Oprogramowanie musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy wirtualizacyjnej.

**Pakiet 3 – Urządzenia sieciowe**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT**  | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | UTM | 2 szt. |  |  |  |  |  |
|  | Switch | 2 szt. |  |  |  |  |  |
| **Razem:** |  |  |

|  |  |
| --- | --- |
| **Okres gwarancji na cały przedmiot zamówienia określony w pakiecie 3***(min. okres gwarancji 24 miesiące, max. punktowany okres gwarancji – 60 miesięcy)* | ………… miesiące/cy*(podać okres licencji w dwunastomiesięcznych okresach)* |

**UTM**

**Urządzenia oferowane**

|  |  |
| --- | --- |
| **Producent** |  |
| **Nazwa** |  |
| **Model** |  |

|  |  |
| --- | --- |
| **Interfejsy, Dysk, Zasilanie***(ilość portów/gniazd*) | ………… RJ45…………SFP 1 GB |
| **Licencja na oprogramowanie** *(min. okres licencji 36 miesięcy, max punktowany okres gwarancji 60 miesięcy)* | …………miesiące/cy*(podać okres licencji w dwunastomiesięcznych okresach)* |

|  |
| --- |
| **SERWIS GWARANCYJNY****(WYPEŁNIA OFERENT):** |
| Nazwa: |  |
| Adres: |  |
| Telefon: |  |
| e-mail: |  |
| Adres strony internetowej serwisu |  |
| Numer infolinii telefonicznej |  |
| Godz. urzędowania serwisu: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymaganie** | **Opis wymagania** | **Wymagania oferowane****(wypełnia oferent)** |
|  | Wymagania Ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.System musi wspierać IPv4 oraz IPv6 w zakresie:* Firewall.
* Ochrony w warstwie aplikacji.

Protokołów routingu dynamicznego. |  |
|  | Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
 |  |
|  | Interfejsy, Dysk, Zasilanie: | 1. System realizujący funkcję Firewall musi dysponować minimum:
* 12 portami Gigabit Ethernet RJ-45.
* 2 gniazdami SFP 1 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall musi być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

Parametry oceniane:- 16 portów Gigabit Ethernet RJ-45 = 2 pkt- 18 portów Gigabit Ethernet RJ-45 = 4 pkt- 20 lub więcej portów Gigabit Ethernet RJ-45 = 6 pkt- 4 gniazdami SFP 1 Gbps = 4 pkt. |  |
|  | Parametry wydajnościowe: | 1. W zakresie Firewall’a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 8 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.2 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 820 Mbps.
 |  |
|  | Funkcje Systemu Bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania muszą zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.
 |  |
|  | Polityki, Firewall | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
 |  |
|  | Połączenia VPN | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM)
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 |  |
|  | Routing i obsługa łączy WAN | 1. W zakresie routingu rozwiązanie musi zapewniać obsługę:
* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
 |  |
|  | Zarządzanie pasmem | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
 |  |
|  | Kontrola Antywirusowa | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
 |  |
|  | Ochrona przed atakami | 1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System ma chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
 |  |
|  | Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji ma umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) mają być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |  |
|  | Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
 |  |
|  | Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. Rozwiązanie ma umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
 |  |
|  | Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
 |  |
|  | Logowanie | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.
 |  |
|  | Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa posiadają następujące certyfikacje:* ICSA lub EAL4 dla funkcji Firewall.
* ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
* ICSA dla funkcji IPSec VPN.
* ICSA dla funkcji SSL VPN.

lub równoważne dla poszczególnych funkcji. |  |
|  | Gwarancja  | 3-letnia gwarancja na części, robociznę i naprawę w miejscu instalacji typu On-Site z czasem reakcji next-buissness-day.Usługa wsparcia technicznego musi być świadczona przez serwis autoryzowany przez producenta urządzeń.  |  |
|  | Licencje | Licencja na oprogramowanie (aktualizacje dla wszystkich funkcjonalności) na okres min 36 miesięcyParametr oceniany: 36 miesięcy - 0 pkt48 miesięcy – 10 pkt60 miesięcy - 20 pkt |  |
|  | Obsługa serwisowa | Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8 godz./5 dni w tygodniu.  |  |
|  | Dodatkowe  | Moduł SFP+ 10GE long range 10km – 2 szt. (moduły pochodzące od producenta oferowanego urządzenia i w pełni z nim kompatybilne)  |  |

**Przełączniki sieciowe – 2 szt.**

**Urządzenia oferowane**

|  |  |
| --- | --- |
| **Producent** |  |
| **Nazwa** |  |
| **Model** |  |

|  |
| --- |
| **SERWIS GWARANCYJNY****(WYPEŁNIA OFERENT):** |
| Nazwa: |  |
| Adres: |  |
| Telefon: |  |
| e-mail: |  |
| Adres strony internetowej serwisu |  |
| Numer infolinii telefonicznej |  |
| Godz. urzędowania serwisu: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymaganie** | **Opis wymagania** | **Wymagania oferowane****(wypełnia oferent)** |
|  | Liczba Protów | Min 24 porty SFP+ oraz min 16 portów 10GbaseTMożliwość rozbudowy poprzez dołożenie kolejnych modułów o kolejne 20 portów 10GBaseT lub SFP+ lub 10 portów 40Gb QSFP+ |  |
|  | Parametry Fizyczne  | Wielkość maksymalnie 2U |  |
|  | Zasilanie | Dwa redudantne zasilania |  |
|  | Tablica MAC | min. 128K |  |
|  | Wydajność | min. 720 Mp/s |  |
|  | Przepustowość | min. 1,9 Tb/s |  |
|  | Porty: | Min. 1 x USBPort konsoli RJ45 |  |
|  | Obsługiwane protokoły i zarządzanie  | Min:• SSH• RSPAN• Radius• DiffServ• IPv4/IPv6 Multicast filtering• IGMPv3 MLDv2 Snooping• IGMPv1,v2 Querier• Policy-based routing (PBR)• LLDP-MED• RSTP• PV(R)STP• BPDU/STRG Root Guard• GVRP/GMRP• Q in Q,• Private VLAN• DOT1X • MAB• Dynamic ARP Inspection• IP Source Guard• sFlow• RIPv2• OSPFv3• UDLD• LLPF• DHCPv6 Snooping |  |
|  | Procesor  | min 1,4 Ghz |  |
|  | Pamięć RAM  | min. 2GB  |  |
|  | Buffor: | min. 256MB Flsh |  |
|  | Ilość sieci VLAN | min. 4000 |  |
|  | Gwarancja | Wymagany okres gwarancji liczony od daty protokołu odbioru min. 24 miesiące, max. punktowany okres gwarancji – 60 miesięcy. Parametry oceniane:* 24 miesiące – 0 pkt
* 36 miesięcy – 3 pkt
* 48 miesięcy – 6 pkt
* 60 miesięcy i więcej – 10 pkt
 |  |
|  | **Dodatkowe wyposażenie**  | Wraz z dostawą urządzenia Zamawiający wymaga dostawy modułów (zestaw – 2 sztuki) światłowodowych SFP+ 10Gb/s Single Mode LC o zasięgu: * 20 km – 2 szt.

oraz Multi Mode LC o zasięgu* 100m – 12 szt.

Moduły muszą pochodzić od producenta oferowanego urządzenia i być w pełni z nim kompatybilne  |  |

**Pakiet 4 – Dostawa urządzeń UPS**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT**  | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | UPS | 2 szt. |  |  |  |  |  |
| **Razem:** |  |  |

**UPS – 2 szt.**

**Urządzenia oferowane**

|  |  |
| --- | --- |
| **Producent** |  |
| **Nazwa** |  |
| **Model** |  |

|  |  |
| --- | --- |
| **Czas podtrzymania dla ~~obciążenia 50% UPS~~ 50% minimalnego wymaganego obciążenia UPS tj. 2 kW***(min. czas potrzymania dla obciążenia 10 min, max punktowany czas podtrzymania obciążenia 30 min)* | ………… min |

|  |
| --- |
| **SERWIS GWARANCYJNY****(WYPEŁNIA OFERENT):** |
| Nazwa: |  |
| Adres: |  |
| Telefon: |  |
| e-mail: |  |
| Adres strony internetowej serwisu  |  |
| Numer infolinii telefonicznej |  |
| Godz. urzędowania serwisu: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymaganie** | **Opis wymagania** | **Wymagania oferowane****(wypełnia oferent)** |
|  | Nazwa komponentu  | Minimalne wymagane parametry  |  |
|  | UPS – zasilacz awaryjny | Zasilacz awaryjny UPS – montaż w szafie RACK 19 cali |  |
|  | Moc pozorna | Min. 5000 VA |  |
|  | Moc czynna | Min. 4000 Wat |  |
|  | Liczba, typ gniazd wyj. z podtrzymaniem zasilania | Min. 8 x zasilanie IEC 60320 C132 x zasilanie IEC 60320 C19 |  |
|  | Typ gniazda wejściowego | 1 x zasilanie IEC 60320 C20 |  |
|  | Zakres napięcia wejściowego w trybie podstawowym | Min. 160 – 270 V |  |
|  | Topologia | On-line double conversion  |  |
|  | Tryb przebiegu | Sinusoida  |  |
|  | Czas podtrzymania dla obciążenia 100% UPS | Min. 3:55 min.  |  |
|  | Czas podtrzymania dla ~~obciążenia 50% UPS~~ 50% minimalnego wymaganego obciążenia UPS tj. 2 kW | Min. 10 min. Parametr oceniany10 min - 0 ppowyżej 10 min do 30 min -> za każde pełne dodatkowe 30 s +1pkt powyżej 30min – 40 pkt |  |
|  | Porty komunikacji | Min. 1 x RJ-45, 1 x USB 2.0 |  |
|  | Slot karty rozszerzeń | Min .1  |  |
|  | Wyświetlacz informacyjny | Tak |  |
|  | Karta rozszerzeń do zarządzania przez sieć LAN | Tak |  |
|  | Awaryjny wyłącznik zasilania  | Tak |  |
|  | Zestaw do montażu w szafie RACK | TAK |  |
|  | Wysokość zasilacza UPS | Maksymalnie: 4U |  |
|  | Poziom hałasu | Nie więcej jak 55 dBA |  |
|  | Gwarancja  | Min. 2 lata na całość |  |