# Załącznik nr 1 do SWZ – formularz ofertowy

|  |  |
| --- | --- |
| Pełna nazwa: | |
|  | |
| Adres: | |
| NIP:  REGON: | KRS: |
| Nr telefonu: | |
| E-mail: | |

W odpowiedzi na ogłoszenie o udzielenie zamówienia publicznego pn. ***Dostawa sprzętu IT w ramach projektu „Cyfrowa Gmina”****,*znaksprawy RGT.ZP.50.2022, składam(-y) następującą ofertę:

1. Łączna cena brutto ……………….. zł (słownie .............................………….........................), w tym należny podatek VAT, zgodnie z poniższą tabelą:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa asortymentu** | **J.m.** | **Ilość** | **Cena jednostkowa** | **Wartość brutto**  **(4x5)** |
| 1 | Serwer NAS | szt. | 1 |  |  |
| 2 | Serwer NAS | szt. | 1 |  |  |
| 3 | Urządzenie UTM | szt. | 2 |  |  |
| 4 | Serwer wraz z systemem operacyjnym | szt. | 1 |  |  |
| 5 | Stacje robocze | szt. | 3 |  |  |
| **Razem wartość brutto** | | | | |  |

1. Proponowany okres gwarancji ….. lat -a (podać zgodnie z §16 SWZ)
2. Oświadczam(y), że:
   1. zapoznaliśmy się z ogłoszeniem o zamówieniu, SWZ oraz wyjaśnieniami i zmianami SWZ przekazanymi przez Zamawiającego i uznajemy się za związanych określonymi w nich postanowieniami i zasadami postępowania oraz zdobyłem(liśmy) konieczne informacje potrzebne do właściwego wykonania zamówienia,
   2. zawarty w SWZ wzór umowy został przeze mnie (nas) zaakceptowany bez zastrzeżeń i zobowiązuję(emy) się, w przypadku wybrania mojej (naszej) oferty do zawarcia umowy na warunkach określonych w SWZ oraz w miejscu i terminie wyznaczonym przez Zamawiającego,
   3. nie wykonywałem (liśmy) żadnych czynności związanych z przygotowaniem niniejszego postępowania o udzielenie zamówienia publicznego, a w celu sporządzenia oferty nie posługiwałem(liśmy) się osobami uczestniczącymi w dokonaniu tych czynności,
   4. akceptuję(emy) warunki płatności określone przez Zamawiającego w projekcie Umowy.
3. Nazwisko i imię osoby odpowiedzialnej do kontaktu ze strony Wykonawcy ...................................... tel. …............………........ e-mail…..................................
4. Następujące prace zamierzamy zlecić podwykonawcom:

|  |  |  |
| --- | --- | --- |
| **Nazwa i adres podwykonawcy (o ile znany)** | **Część zamówienia, której wykonanie zostanie powierzone podwykonawcom** | **Procentowa wartość części zamówienia, której wykonanie zostanie powierzone podwykonawcom (fakultatywnie - Wykonawca nie musi jej wypełniać** |
|  |  |  |
|  |  |  |

1. Oświadczamy, że Wykonawca, którego reprezentujemy jest:

🞏 mikro przedsiębiorcą(podmiot nie będący żadnym z poniższych)

🞏 małym przedsiębiorcą (małe przedsiębiorstwo definiuje się jako przedsiębiorstwo, które zatrudnia mniej niż 50 pracowników i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR)

🞏 średnim przedsiębiorcą (średnie przedsiębiorstwo definiuje się jako przedsiębiorstwo, które zatrudnia mniej niż 250 pracowników i którego roczny obrót nie przekracza 50 milionów lub roczna suma bilansowa nie przekracza 43 milionów EUR)

🞏 dużym przedsiębiorstwem

1. Oświadczam(y), że oferta nie zawiera/ zawiera (niepotrzebne skreślić) informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach: .................................................................................
2. Oświadczam, że wybór naszej oferty

🞏 nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tekst jednolity Dz.U. z 2020 r., poz. 106 ze zm.),

🞏 będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tekst jednolity Dz.U. z 2020 r., poz. 106 ze zm.), w związku z powyższym wskazujemy:

* 1. nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego: ………………………………..………………,
  2. wartość towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku: …………………………………………………………………………
  3. stawkę podatku od towarów i usług, która będzie miała zastosowanie: ………………………………………………

1. Oświadczam, że wypełniłem/liśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[[1]](#footnote-2)wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu[[2]](#footnote-3).
2. Informuję, że zamawiający może uzyskać odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru za pomocą bezpłatnych i ogólnodostępnych baz danych:

🞏 <https://ems.ms.gov.pl/krs/wyszukiwaniepodmiotu?t:lb=t>,

🞏 <https://prod.ceidg.gov.pl>

|  |  |
| --- | --- |
|  | - kwalifikowany podpis elektroniczny / podpis zaufany / podpis osobisty  Wykonawcy lub osoby upoważnionej |

# Załącznik nr 2 do SWZ – opis przedmiotu zamówienia

*……………………………………………………………………………………………………………………………………………………*

*……………………………………………………………………………………………………………………………………………………*

*……………………………………………………………………………………………………………………………………………………*

*(pełna nazwa/firma, adres)*

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Nazwa elementu, parametru lub cechy** | **Minimalne parametry techniczne (poniższe parametry techniczne są minimalnymi wymogami zamawiającego jednocześnie stanowią wskazanie minimalne wymogi dla urządzeń równoważnych)** | **Wypełnia Wykonawca podaje producenta, model oraz dane techniczne oferowanego urządzenia (dane techniczne należy podać tylko wówczas, gdy w danym wierszu brak jest słowa „spełnia”).** |
| **Przedmiot zamówienia – serwer NAS nr 1** | | | **Oświadczenia Wykonawcy** |
| Nazwa producenta: …………………………………….  Model urządzenia: …………………………………….  Dane techniczne oferowanego urządzenia: | | | |
| **1.** | **Stan** | Nowy | Spełnia |
| **2.** | **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych. | Wysokość obudowy: ………..  Pozostałe wymogi - spełnia |
| **3.** | **Procesor** | Jeden procesor 4-rdzeniowy 64-bitowy x86, min. 2.0GHz częstotliwości nominalnej, osiągający w testach PassMark CPU Mark wynik 4000 pkt  Wynik testu musi być opublikowany na stronie www.cpubenchmark.net w dniu złożenia oferty.  **Do oferty należy załączyć wyniki testów.** | Częstotliwość:……………………  Pozostałe wymogi - spełnia |
| **4.** | **Pamięć systemowa** | Min. 4 GB DDR4 z możliwością rozbudowy do min. 16GB. | Wielkość:……………………..  Pozostałe wymogi - spełnia |
| **5.** | **Dyski twarde** | 8 szt. identycznych dysków o pojemności każdego dysku min. 6TB i prędkości obrotowej talerzy min. 7200 rpm.  Interfejs dysków SATA 6Gb/s.  Dyski twarde dedykowane do zastosowań profesjonalnych (enterprise). | Pojemność dysków:…………….  Prędkość obrotowa:…………….  Pozostałe wymogi - spełnia |
| **6.** | **Kontroler pamięci masowej** | Obsługiwane tryby RAID: min. 0,1,5,6,10. | Obsługiwane tryby RAID:……………………. |
| **7.** | **Zasilacze** | Min. 2 szt., każdy o mocy min. 250W. | Moc: ………………….. |
| **8.** | **Płyta główna** | Min. 1 wolne złącze PCI-E celem możliwości instalacji opcjonalnych kart rozszerzeń. | Ilość wolnych złączy:…………….. |
| **9.** | **Karty sieciowe** | Min. 2 porty RJ45 o przepustowości 1Gb/s.  Min. 2 porty SFP+ o przepustowości 10Gb/s.  Wymagana ilość portów kart sieciowych może być osiągnięta w wyniku zastosowania karty rozszerzeń. | Ilość portów RJ45:……………..  Ilość portów SFP+:……………  Pozostałe wymogi - spełnia |
| **10.** | **Wbudowane porty** | Min. 2x USB 3.0 (lub nowsze).  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, rozgałęziaczy, przejściówek, itp. | Porty USB: ……………..  Pozostałe wymogi - spełnia |
| **11.** | **Certyfikaty i standardy** | Serwer musi posiadać deklarację CE. | Spełnia |
| **12.** | **System operacyjny - funkcje** | Obsługa autoryzacji Windows AD i LDAP.  Wbudowany serwer FTP i CIFS/SMB.  Obsługa protokołu iSCSI (MultiLUN Target, LUN Backup).  Kompatybilność ze środowiskami wirtualizacyjnymi Vmware vSphere, Microsoft Hyper-V.  Obsługa protokołów NFS v3/NFS v4, TFTP, HTTP, HTTPS, SSH, SNMP, SMTP. | Spełnia |
| **13.** | **Warunki gwarancji** | 36 miesięcy gwarancji.  W przypadku awarii dyski twarde pozostają własnością Zamawiającego. | Spełnia |
| **14.** | **Dodatkowe akcesoria** | 2 szt. kabli SFP+ 10GbE Direct Attach o długości 3m. | Spełnia |

|  |  |  |  |
| --- | --- | --- | --- |
| **Przedmiot zamówienia – serwer NAS nr 2** | | | **Oświadczenia Wykonawcy** |
| Nazwa producenta: …………………………………….  Model urządzenia: …………………………………….  Dane techniczne oferowanego urządzenia: | | | |
| **1.** | **Stan** | Nowy | Spełnia |
| **2.** | **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych. | Wysokość obudowy: ………..  Pozostałe wymogi - spełnia |
| **3.** | **Procesor** | Jeden procesor 4-rdzeniowy 64-bitowy x86, min. 2.0GHz częstotliwości nominalnej, osiągający w testach PassMark CPU Mark wynik 4000 pkt  Wynik testu musi być opublikowany na stronie www.cpubenchmark.net w dniu złożenia oferty.  **Do oferty należy załączyć wyniki testów**. | Częstotliwość:……………………  Pozostałe wymogi - spełnia |
| **4.** | **Pamięć systemowa** | Min. 4 GB DDR4 z możliwością rozbudowy do min. 16GB. | Wielkość:……………………..  Pozostałe wymogi - spełnia |
| **5.** | **Dyski twarde** | 4 szt. identycznych dysków o pojemności każdego dysku min. 4TB i prędkości obrotowej talerzy min. 7200 rpm.  Interfejs dysków SATA 6Gb/s.  Dyski twarde dedykowane do zastosowań profesjonalnych (enterprise). | Pojemność dysków:…………….  Prędkość obrotowa:…………….  Pozostałe wymogi - spełnia |
| **6.** | **Kontroler pamięci masowej** | Obsługiwane tryby RAID: min. 0,1,5,6,10.  Obsługiwane typy dysków: SATA. | Obsługiwane tryby RAID:…………………….  Pozostałe wymogi - spełnia |
| **7.** | **Zasilacze** | Min. 1 szt., o mocy min. 250W. | Moc: ………………….. |
| **8.** | **Płyta główna** | Min. 1 wolne złącze PCI-E celem możliwości instalacji opcjonalnych kart rozszerzeń. | Ilość wolnych złączy:…………….. |
| **9.** | **Karty sieciowe** | Min. 2 porty RJ45 o przepustowości 1Gb/s.  Wymagana ilość portów kart sieciowych może być osiągnięta w wyniku zastosowania karty rozszerzeń. | Ilość portów: ……………………..  Pozostałe wymogi - spełnia |
| **10.** | **Wbudowane porty** | Min. 2x USB3.0 (lub nowsze);  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, rozgałęziaczy, przejściówek, itp. | Porty USB: ……………..  Pozostałe wymogi - spełnia |
| **11.** | **Certyfikaty i standardy** | Serwer musi posiadać deklaracja CE. | Spełnia |
| **12.** | **System operacyjny - funkcje** | Obsługa autoryzacji Windows AD i LDAP.  Wbudowany serwer FTP i CIFS/SMB.  Obsługa protokołów NFS v3/NFS v4, TFTP, HTTP, HTTPS, SSH, SNMP. | Spełnia |
| **13.** | **Warunki gwarancji** | 36 miesięcy gwarancji  W przypadku awarii dyski twarde pozostają własnością Zamawiającego. | Spełnia |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Przedmiot zamówienia – UTM – 2 sztuki** | | | **Oświadczenia Wykonawcy** | |
| Nazwa producenta: …………………………………….  Model urządzenia: …………………………………….  Dane techniczne oferowanego urządzenia: | | | | |
| **1.** | **Stan** | Nowy | | Spełnia |
| **2.** | **Ogólne** - Zapora Sieciowa Nowej Generacji (NGFW) musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall’a, systemu ochrony IPS oraz usług sieciowych takich jak np. DHCP Server; VPN Gateway; Application Control.  Oferowany w ramach postępowania sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta w Polsce. | | | Spełnia |
| **3.** | **Zapora sieciowa (Firewall)**   1. Urządzenie musi umożliwiać inspekcję stanową (full-state Inspection) opartą na granularnej analizie komunikacji sieciowej oraz rozpoznawaniu i analizie warstwy aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu. 2. Urządzenie ma obsługiwać translacje adresów NAT typu: n:1, NAT1:1; PAT; Network MAP/NAT. 3. Urządzenie musi posiadać możliwość ustawienia trybu pracy jako router/brama warstwy trzeciej, jako bridge warstwy drugiej (Transparent mode) oraz w trybie analizatora ruch TAP monitor port. 4. Graficzny interfejs użytkownika (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Administrator ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, serwisy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola Quality Of Service, godziny oraz dnia obwiązywania (aktywności) reguły. 6. Administrator ma możliwość zdefiniowania minimum sześciu (niezależnie konfigurowalnych) typów reguł/polityk na firewall’u. 7. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, pozwalający na sprawdzanie jaka reguła będzie stosowana dla danego typu ruchu i eliminujący sprzeczności w konfiguracji reguł. 8. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, zewnętrzny serwer LDAP; Microsoft Active Directory z możliwością wdrożenia strategii autoryzacji wieloskładnikowej (Multi-Factor-Authentication MFA) | | | Spełnia |
| **4.** | **Intrusion prevention system (IPS)**   1. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 2. Moduł IPS musi posiadać bazę „na urządzeniu” co najmniej 10 000 sygnatur które są utrzymane i aktualizowane przez producenta. 3. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 4. Moduł IPS powinien wykrywać oraz blokować szkodliwą zawartość w kodzie HTML oraz Javascript. 5. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POPS oraz SMTPS. 6. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. 7. Moduł skanujący musi działać na urządzeniu (firewall’u). Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. 8. Urządzenie w ramach działania modułu IPS musi posiadać możliwość powiadamiania o wykrytych podatnościach w ruchu wraz z informacją o kodzie CVE. 9. Administrator musi mieć możliwość konfiguracji jednego z trybów pracy modułu proaktywnej ochrony i inspekcji pakietów IPS w zakresie: tryb aktywny IPS, tryb passywny IDS; musi być możliwość konfiguracji baza wyjątków modułu IPS dla wybranych adresów IP (źródłowych i docelowych), portów docelowych; sygnatur bazy CVE. | | | Spełnia |
| **5.** | **Kształtowanie pasma (Traffic Shapping)**   1. Urządzenie musi pozwalać na kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia z uwzględnieniem kierunku przesyłanych danych (upload / download). Kwalfikacja Traffic Shapping z uwzględnienim adresu IP (źródłowego i docelowego), portów docelowych; autoryzowanego użytkownika. 3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. 5. Traffic Shapping powinien działać w oparciu o profile QoS Band tzw. klasyfikatory ruchu które będą kolejkowane do fizycznych lub logicznych interfejsów firewall’a | | | Spełnia |
| **6.** | Ochrona antywirusowa   1. Rozwiązanie ma umożliwiać inspekcję przez skaner antywirusowy, co najmniej jeden silnik antywirusowy powinien być dostarczony przez firmę inną niż producent rozwiązania. 2. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 3. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji. Proponowany system powinien umożliwiać wysyłanie powiadomienia email o załączniku, który został zablokowany. 4. Ochrona antyspam ma działać w oparciu o DNS RBL. 5. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. | | | Spełnia |
| **7.** | **Wirtualne sieci prywatne (VPN)**   1. Urządzenie musi posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Odpowiednio kanały VPN można budować w oparciu o:    * PPTP VPN,    * L2TP VPN    * IPSec VPN,    * SSL VPN 3. SSL VPN musi działać w trybach Tunel i Portal. 4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma posiadać wsparcie dla technologii XAuth oraz Hub ‘n’ Spoke. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. 8. Urządzenie musi być dostarczone wraz z dedykowanym klientem IPSec VPN. 9. Rozwiązanie ma obsługiwać multitransport VPN – tworzenie do 24 transportów w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień. 10. Rozwiązanie ma zapewnić możliwość łączenia transportów VPN (agregacja łączy na poziomie pakietów, lub sesji) i wyznaczania transportów zapasowych. 11. Rozwiązanie ma zapewniać kompresję i deduplikację danych przesyłanych w tunelach VPN. 12. Rozwiązanie ma mieć możliwość buforowania danych przesyłanych w tunelach VPN dla protokołów zdefiniowanych przez administratora. | | | Spełnia |
| **8.** | **Filtr dostępu do stron www (URL filtering)**   1. Urządzenie musi posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą kategorie tematyczne stron internetowych; wymagana ilość rozpoznawanych kategorii 86. 3. Urządzenie powinno wspierać mechanizmy białych i czarnych list 4. Urządzenie nie może posiadać ograniczenia w postaci limitu ilości białych i czarnych list definiowanych przez administratora 5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:    * blokowanie dostępu do adresu URL,    * zezwolenie na dostęp do adresu URL,    * blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 7. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 8. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 9. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 10. Urządzenie musi dawać możliwość utworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. Baza wyjątków tworzona co najmniej przy użyciu dwóch metod:     1. wskazanie/wpisanie docelowej domeny (np. \*.skype.com; \*.microsoft.com);     2. wskazanie kategorii ruch (np. Bankowość i Finanse). 11. Urządzenie musi umożliwiać włączenia pamięci cache dla ruchu http. 12. Urządzenie musi posiadać wbudowany i rekonfigurowany WEB portal powiadomień zwrotnych służący do informowania użytkowników o nałożonych restrykcjach/ograniczeniach wynikających z wdrożonej polityki bezpieczeństwa (np. zablokowanie strony WWW danego portalu z powodu niedozwolonej kategorii) | | | Spełnia |
| **9.** | **Uwierzytelnianie**   1. Urządzenie musi zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:    * lokalną bazę użytkowników,    * zewnętrzną bazę użytkowników (zewnętrzny LDAP),    * usługę katalogową Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 2 różnych baz LDAP. 3. Rozwiązanie musi zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:    * SSL,    * Radius,    * Kerberos. 4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 5. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. | | | Spełnia |
| **10.** | **Administracja łączami do Internetu (ISP)**   1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:    * równoważenie względem adresu źródłowego,    * równoważenie względem połączenia. 3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 9. Rozwiązanie powinno wspierać technologię Link Aggregation. | | | Spełnia |
| **11.** | **Pozostałe usługi i funkcje rozwiązania**   1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci z możliwością określenia różnych bram, a także serwerów DNS. 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy. | | | Spełnia |
| **12.** | **Administracja urządzeniem**   1. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 2. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w zakresie konfiguracji podstawowej i zaawansowanej. 3. Urządzenie posiada możliwość eksportu informacji przez syslog. Wysyłanie logów powinno być możliwe do wielu serwerów, równocześnie. 4. Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogiczny np. protokołu IPFIX 5. Komunikacja z interfejsem zarządzania może odbywać się na porcie innym niż https (443 TCP). 6. Urządzenie powinno umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 7. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 8. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową lub poprzez dedykowaną aplikację do zarządzania a komunikacja musi być zabezpieczona (autoryzacja i szyfrowanie ruchu). 9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji w sposób:     * bezpośrednio z centralnej konsoli zarządzania;     * przywrócenie konfiguracji z lokalnego graficznego interfejsu zarządzania GUI;     * przywrócenie konfiguracji z lokalnego tekstowego interfejsu zarządzania (console port);     * przywrócenie konfiguracji ze zdalnego trybu tekstowego zarządzania (SSH);     * przywrócenie systemu operacyjnego i konfiguracji z użyciem klucza USB-Stick. 11. Zapory sieciowe muszą być wyposażone w aplikację lub system umożliwiający zdalne zarządzanie firewallem, serwerem VPN oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej przynajmniej pod kontrolą systemu Windows lub Linux. | | | Spełnia |
| **13.** | **Raportowanie**   1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów. 3. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 4. Firewall musi posiadać ujednolicony pulpit (Dashboard) monitorujący i raportujący o bezpieczeństwie chronionego środowiska IT z uwzględnieniem raportowania w przedziałach czasu (aktualna sytuacja do 60min; ostatnia godzina; ostatnie 24h; ostatni dzień; ostatnie 7dni; ostatni tydzień; obecny miesiąc; ostatni miesiąc) 5. System raportujący powinien posiadać wbudowane wzorce gotowych raportów dotyczących min. aplikacji, aktywność użytkownika, użycia VPN, bezpieczeństwa sieci i oceny ryzyka. | | | Spełnia |
| **14.** | **Parametry**   1. Urządzenie musi posiadać dysk o pojemności nie mniejszej niż 100 GB. 2. Urządzenie w formie (hardware appliance) urządzenia sprzętowego posiadającego:    * przynajmniej 5 portów 1000Base-T RJ45,    * przynajmniej 1 port Console (RS232 lub RJ45),    * przynajmniej 2 porty USB. 3. Wysokość urządzenia nie może przekroczyć 1U. 4. Przepustowość firewalla: min. 2.0 Gb/s. 5. Wydajność firewalla (włączona kontrola IPS): min. 600 Mb/s. 6. Wydajność z włączonymi modułami ochrony IPS, Application Control, URL Filtering i Anti-Virus: min. 1.2Gbps w warunkach produkcyjnych (pakiety i sesje charakterystyczne dla ruchu do Internetu). 7. Przepustowość tunelu VPN przy szyfrowaniu AES-128: min. 720 Mb/s. 8. Obsługa sieci logicznych min. 256 VLAN. 9. Liczba równoczesnych sesji - min. 80 000 i nie mniej niż 12 000 nowych sesji/sekundę. 10. Rozwiązanie musi mieć możliwość rozbudowy do działania w układzie klastra niezwodnościowego HA w trybie Active/Pasive. 11. Urządzenie powinno wspierać tworzenie tuneli VPN za pomocą graficznego interfejsu w modelu Drag&Drop bez potrzeby użycia narzędzi konsolowych (command line). 12. Urządzenie musi posiadać dedykowany port konsoli ze złączem RS232 lub RJ45. 13. Wyposażenie w elementy umożliwiające montaż urządzenia w 19” szafie stelażowej. 14. Uruchomienie zestawu w tym szczególnie instalacja i pełna konfiguracja firewalli według ustaleń projektowych zaakceptowanych przez Zamawiającego. Wymagany jest podstawowy i zaawansowany zakres konfiguracji. 15. Poszczególne użyte do budowy zestawu komponenty sprzętowe nie mogą w żaden sposób ograniczać maksymalnej przepustowości i prędkości pracy zestawu. 16. Zaoferowane urządzenia nie mogą być przewidziane przez producenta do zastąpienia nowszym modelem przez co najmniej trzy lata począwszy od dnia podpisania umowy. | | | Pojemność dysku:……….  Przepustowość firewalla:…………  Wydajność firewalla:…………..  Przepustowość tunelu VPN: ………….......  Obsł. Sieci logicznych: ……………….  Pozostałe wymogi - spełnia |
| **15.** | **Licencje**  Wszystkie dostarczone licencje w ramach rozwiązania muszą obejmować wymagany okres 36-miesięcy i nie mogą posiadać limitu użytkowników.  Wraz z urządzeniem wykonawca dostarczy wymagane do prawidłowej pracy licencje:   * 36-miesięczna subskrypcją na aktualizację: systemu operacyjnego; aktualizację sygnatur dla silnika IPS, aktualizację sygnatur dla silnika dynamicznego rozpoznawania aplikacji. * 36-miesięczna subskrypcją na ochronę antywirusową; aktualizacje sygnatur spamu oraz dostęp do serwerów RBL DNS. * 36-miesięczna subskrypcją na poszerzoną ochronę ATP (Sanboxing) w zakresie zawansowanej analizy załączników i ochrona przed zagrożeniami dnia zerowego; ochrona przed atakami typu ransomware. Wymagane aby analiza/ocena (wykonywana przez NGFW/ATP Services) bezpieczeństwa dla załącznika mailowego lub pobieranego pliku, była wykonywana w trybie bezpiecznym tzn. kwalifikacja zakresie poprawności/zdrowia załącznika lub pliku przed dostarczeniem do użytkownika. * System powinien mieć możliwość aktywacji funkcjonalności dostępu zdalnego w technologii dostęp zdalny w technologii SSL-VPN; urządzenie musi obsługiwać portal Usługowy w trybie HTTPS oraz umożliwiać zdalny dostęp (SSL-VPN) przy użyciu zunifikowanej aplikacji mobilnej; wymagana obsługa dwu-etapowej MFA / wieloskładnikowej metody autoryzacji. * 36-miesięczna subskrypcja dostępu do platformy zarządzania umożliwiająca m.in.:   + zapisywanie całej historii zmian konfiguracji urządzenia (administrator musi mieć możliwość powrotu do konfiguracji danego modułu z danego dnia oraz informację, jaki użytkownik wprowadził zmianę). Ponadto funkcja musi pozwalać na tworzenie audytów, które pokazują wszystkie zmiany dokonane w konfiguracji wraz z informacją jaki użytkownik je wprowadził.   + administrację urządzeniem opartą na rolach i współdzieleniu pracy kilku administratorów jednocześnie – system umożliwia jednoczesną pracę kilku administratorom i zapobiega konfliktom między administratorami oraz loguje wszystkie zmiany.   + konfigurację urządzenia z wykorzystaniem aplikacji mobilnej do monitoringu; aplikacja musi być dostępna na co najmniej jednym z systemów mobilnych (Android/iOS). Aplikacja musi umożliwiać co najmniej: prezentację ogólnych danych urządzenia (m.in. czas pracy, status licencji, wersja firmware, model i numer seryjny), wyświetlanie statusu urządzenia (obciążenie procesora i sieci, zużycia pamięci RAM oraz wykorzystania powierzchni dyskowej a także dane z czujników sprzętowych), dynamiczne prezentowanie wykresów dla: przepustowości, ilości sesji dozwolonych i zablokowanych, wykonanie restartu urządzenia, restartu usług, używanie pełnego dostępu terminalowego (SSH), włączanie i wyłączanie dynamicznych reguł zapory (na przykład w celu zapewnienia zespołowi tymczasowego dostępu do zablokowanych aplikacji internetowych). | | | Spełnia |
| **16.** | **Gwarancja i wsparcie techniczne**  Minimum 36-miesięczna gwarancja sprzętowa producenta obejmująca wszystkie elementy urządzenia zapewniająca w przypadku awarii wysłanie sprawnego sprzętu na wymianę urządzenia wg procedur RMA Producenta.  Gwarancja musi zapewniać również dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00 (e-mail; telefon; web-portal).  Wymagane jest zapewnienie możliwości zgłaszania awarii mailem/telefon w języku polskim w trybie 8/5 przez oficjalnego dystrybutora rozwiązania na terenie kraju z czasem reakcji na zgłoszenie serwisowe SLA - 4h. W ramach utrzymania wymagana jest realizacja zleceń konsultacyjnych o łącznym czasie do 2h miesięcznie lub do max. 4 zleceń miesięcznie. Obsługa konsultacyjna w języku polskim w trybie zaplanowanego działania SLA-NBD+; przyjęcie /rejestracja zgłoszeń konsultacyjnych SLA - do 8h (zgłoszenia konsultacyjne mail/telefon).  Po upływie co najwyżej 4 lat Zamawiający musi posiadać możliwość nieodpłatnej wymiany sprzętu na fabrycznie nowe urządzenie w nowszej wersji sprzętowej w ramach tej samej serii/linii produktowej. | | | Spełnia |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Przedmiot zamówienia – serwer wraz z systemem operacyjnym** | | | **Oświadczenia Wykonawcy** | |
| Nazwa producenta: …………………………………….  Model urządzenia: …………………………………….  Dane techniczne oferowanego urządzenia: | | | | |
| **1.** | **Stan** | Nowy | | Spełnia |
| **2.** | **Obudowa**  Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych.  Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze oraz chroniący dyski przed nieautoryzowanym usunięciem.  Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. Android/ Apple iOS przy użyciu jednego z protokołów NFC/ BLE/ WIFI. | | | Spełnia |
| **3.** | **Płyta główna** z możliwością zainstalowania minimum dwóch procesorów.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | | | Spełnia |
| **4.** | **Chipset** - dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. | | |  |
| **5.** | **Procesor** | Jeden procesor 8-rdzeniowy, min. 2.1GHz częstotliwości nominalnej, osiągający w testach PassMark CPU Mark wynik 11000pkt  Wynik testu musi być opublikowany na stronie www.cpubenchmark.net w dniu złożenia oferty.  **Do oferty należy załączyć wyniki testów.** | | Częstotliwość nominalna: …………..  Pozostałe wymogi - spełnia |
| **6.** | **Pamięć RAM** | 32GB DDR4 RDIMM 3200MHz w układzie 2x 16GB,  Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512GB pamięci RAM.  Zabezpieczenia pamięci RAM: Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling | | Spełnia |
| **7.** | **Gniazda PCI** | Min. jeden slot PCIe Gen 3 o prędkości min. x16 | | Ilość slotów:…………. |
| **8.** | **Interfejsy sieciowe** | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T 1 Gb/s. | | Ilość portów: ……………. |
| **9.** | **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.  Zainstalowane 4 dyski min. 960GB SSD SATA Hot-Plug typu ReadIntensive DWPD>=1  Możliwość zainstalowania wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash o pojemności minimum 64GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. | | Spełnia |
| **10.** | **Kontroler RAID** | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10  Wsparcie dla dysków samoszyfrujących. | | Spełnia |
| **11.** | **Napęd optyczny** | Wbudowany wewnętrzny napęd optyczny DVD-RW lub DVD-ROM | | Spełnia |
| **12.** | **Wbudowane porty** | min. 4port USB t tym min, 3x USB 3.0, 2 porty RJ45, 2 porty VGA (1 na przednim, drugi na tylnym panelu obudowy), min. 1 port RS232. | | Spełnia |
| **13.** | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 | | Spełnia |
| **14.** | **Zasilanie** | Redundante, Hot-Plug maksimum 550W.  C13 do C14, styl PDU, 10 amperów, przewód zasilający o długości 2m | | Spełnia |
| **15.** | **Bezpieczeństwo** | Zintegrowany z płytą główną moduł TPM.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. | | Spełnia |
| **16.** | **System operacyjny** - Microsoft Windows Server 2022 Essential lub równoważne spełniające następujące kryteria:   * Instalacja i użytkowanie aplikacji 32-bit. i 64- bit. na dostarczonym systemie operacyjnym * Współpraca z procesorami o architekturze x86-64 − Ilość obsługiwanych przez system rdzeni w ramach dostarczonej licencji - co najmniej 8 * Praca w roli kontrolera domeny Active Directory * Zawarta możliwość uruchomienia roli serwera DHCP * Zawarta możliwość uruchomienia roli serwera DNS * Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP) * Zawarta możliwość uruchomienia roli serwera usług informacyjnych WWW * Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Active Directory * Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Active Directory * Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Active Directory * W ramach dostarczonej licencji zawarte prawo do użytkowania i dostępu do oprogramowania oferowanego przez producenta systemu operacyjnego. | | | Spełnia |
| **17.** | **Zarządzanie** - niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   Karta powinna posiadać możliwość wyposażenia we wbudowaną wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych. | | | Spełnia |
| **18.** | **Certyfikaty** - Serwer musi być wyprodukowany zgodnie z normą  ISO-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklaracja CE. | | | Spełnia |
| **19.** | **Warunki gwarancji** - 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu przez organizację serwisową producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  W przypadku awarii dyski twarde pozostają własnością Zamawiającego.  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.  Do oferty należy załączyć Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. | | | Spełnia |

|  |  |  |  |
| --- | --- | --- | --- |
| **Przedmiot zamówienia – stacje robocze – 3 sztuki** | | | **Oświadczenia Wykonawcy** |
| Nazwa producenta: …………………………………….  Model urządzenia: …………………………………….  Dane techniczne oferowanego urządzenia: | | |  |
| **1.** | **Stan** | Nowy | Spełnia |
| **2.** | **Obudowa** | typu SFF (Small Form Factor) | Spełnia |
| **3.** | **Wydajność obliczeniowa:**   * procesor wielordzeniowy, co najmniej sześciordzeniowy, o podstawowym taktowaniu co najmniej 3,0 GHz do co najmniej 4,2 GHz w trybie turbo, o średniej wydajności ocenianej na co najmniej 12000 pkt. w teście PassMark CPU Mark według wyników opublikowanych na stronie www.cpubenchmark.net, * wykonawca załączy na wezwanie Zamawiającego wydruk ww. strony z datą nie wcześniejszą niż 2 dni przed składaniem ofert ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów. Wydruk strony musi być podpisany przez Wykonawcę, * chłodzenie procesora będzie wystarczające do zachowania optymalnej temperatury pracy pod obciążeniem,   wszystkie oferowane komponenty wchodzące w skład komputera będą ze sobą kompatybilne i nie będą obniżać jego wydajności. Zamawiający nie dopuszcza sprzętu, w którym zaoferowane komponenty komputera będą pracowały na niższych parametrach niż opisywane w SIWZ. | | Podstawowe taktowanie ………… GHz  Średnia wydajność w teście PassMark CPU Mark ………………………….. pkt  Pozostałe wymogi - spełnia |
| **4.** | **Pamięć operacyjna:** | * minimum 8 GB RAM DDR4, o taktowaniu co najmniej 3200 MHz,   możliwość rozbudowy do co najmniej 32 GB. | Wielkość ……………… GB  Taktowanie ………………….. MHz  Pozostałe wymogi - spełnia |
| **5.** | **Karta graficzna:** | Zintegrowana, z możliwością dynamicznego przydzielenia pamięci w obrębie pamięci systemowej. | Spełnia |
| **6.** | **Dysk Twardy:** | SSD PCIe M.2 o pojemności co najmniej 256 GB, | Pojemność ………… GB  Pozostałe wymogi – spełnia |
| **7.** | **Wyposażenie**:   * karta dźwiękowa zintegrowana z płytą główną, * interfejs RJ-45 obsługujący sieci 10/100/1000BASE-T, * co najmniej 4 porty USB w tym co najmniej jeden USB Type-C, * wyjście HDMI lub Display Port, * porty audio w obudowie: wejście na mikrofon, wyjście na słuchawki, * klawiatura oraz myszka. | | Spełnia |
| **8.** | **Zabezpieczenia:** Zintegrowany układ szyfrujący Trusted Platform Module w wersji 2.0. | | Spełnia |
| **9.** | **Zasilanie:** Zasilacz min. 200W 230V 50Hz, przewód zasilający w zestawie. | | Spełnia |
| **10.** | **System operacyjny:** Zainstalowany system Microsoft Windows 10 Pro lub nowszy ze wszystkimi sterownikami. Nie dopuszcza się w tym zakresie licencji pochodzących z rynku wtórnego. Umieszczony na obudowie Certyfikat Autentyczności w postaci specjalnej naklejki zabezpieczającej lub Załączone potwierdzenie wykonawcy / producenta komputera o legalności dostarczonego oprogramowania systemowego. | | Spełnia |
| **11.** | **Wsparcie techniczne:** Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń, realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej - Wykonawca w ofercie poda adres strony oraz sposób realizacji wymagania (opis uzyskania w/w informacji). | | Spełnia |
| **12.** | **Dokumenty:** Deklaracja zgodności CE dla oferowanego modelu komputera (załączyć na wezwanie Zamawiającego) lub równoważne. | | Spełnia |
| **13.** | **Warunki gwarancji:** Minimum 36 miesięcy gwarancji liczona od daty dostawy. | | Spełnia |

|  |  |
| --- | --- |
|  | - kwalifikowany podpis elektroniczny / podpis zaufany / podpis osobisty  Wykonawcy lub osoby upoważnionej |

1. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1) [↑](#footnote-ref-2)
2. W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (należy usunąć treści oświadczenia przez jego wykreślenie) [↑](#footnote-ref-3)