**Część nr 2**

**Załącznik nr 2 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest realizacja zadania pn.: „Podniesienie poziomu cyberbezpieczeństwa oraz modernizacja infrastruktury teleinformatycznej” w ramach, którego Wykonawca zobowiązany jest do:

1. Dostawy 4 zarządzalnych przełączników sieciowych oraz 8 modułów SFP+ 10G Duplex LC
2. Przedłużenie okresu gwarancyjnego o 24 miesiące dla użytkowanej przez Zamawiającego macierzy dyskowej
3. Dostawy dwóch urządzeń UTM wraz z instalacją, konfiguracją i wdrożeniem do klastra wysokiej dostępności w środowisku bezpieczeństwa sieciowego Zamawiającego.
4. Odnowienia licencji na oprogramowanie do wykonywania kopii zapasowych posiadane przez Zamawiającego na okres 24 miesięcy
5. Dostawy urządzenia pamięci masowej typu NAS.
6. Dostawy serwera wraz z systemem operacyjnym oraz szafą serwerową typu rack
7. Dostawy oprogramowania na rozwiązanie MFA dla 15 użytkowników, na okres 3 lat, przeznaczone do zabezpieczenia środowiska domenowego.
8. Rozszerzenia liczby licencji oprogramowania antywirusowego wykorzystywanego przez Zamawiającego o 45 sztuk
9. Dostawy punktów dostępowych, przełączników PoE oraz osprzętu instalacyjnego do budowy sieci Wi-Fi

|  |  |
| --- | --- |
| **1. DOSTAWA 4 ZARZĄDZALNYCH PRZEŁĄCZNIKÓW SIECIOWYCH ORAZ 8 MODUŁÓW SFP+ 10G DUPLEX LC** | |
| 1. Zakres zamówienia  Przedmiotem zamówienia jest:  - dostawa i wniesienie 4 szt. przełączników sieciowych typu rack 1U, przeznaczonych do pracy jako przełączniki dystrybucyjne L2+/L3 Lite w sieci LAN Zamawiającego,  - dostawa 8 szt. modułów SFP+ 10G Duplex LC, kompatybilnych z zaoferowanymi przełącznikami,  - dostawa okablowania zasilającego oraz elementów montażowych, w szczególności:  - kompletne uchwyty / szyny / kątowniki RACK 19" do montażu wszystkich przełączników,  - przewody zasilające przystosowane do gniazd stosowanych w Polsce,  - udzielenie gwarancji i wsparcia serwisowego na okres wskazany w niniejszym OPZ i w załączniku „Parametry techniczne”,  - dostawa dokumentacji (instrukcja obsługi, karta katalogowa / dane techniczne) w języku polskim lub angielskim.  2. Wymagania ogólne  Sprzęt musi być:  - fabrycznie nowy, nieużywany, niepochodzący z ekspozycji,  - w momencie dostawy znajdować się w aktualnej ofercie producenta,  - na dzień składania ofert oferowany model urządzenia nie może mieć ogłoszonego przez producenta zakończenia sprzedaży (End of Sale / Last Date of Order lub równoważne) ani zakończenia wsparcia (End of Support / End of Life / Last Date of Support lub równoważne).  Zamawiający dopuszcza rozwiązania równoważne, spełniające co najmniej poniższe wymagania minimalne. | |
| Przełącznik sieciowy – 4 sztuki | |
| **Parametr** | **Minimalne wymagania** |
| Przedmiot | Zarządzalny przełącznik sieciowy warstwy 2+/L3 Lite, przeznaczony do pracy jako przełącznik dystrybucyjny w sieci LAN Zamawiającego |
| Forma wykonania | Obudowa do montażu w szafie RACK 19", wysokość maks. 1U; w zestawie komplet elementów montażowych RACK |
| Porty dostępowe | Minimum 48 × 10/100/1000Base-T (RJ-45), auto-negocjacja prędkości i dupleksu, auto MDI/MDI-X |
| Porty uplink | Minimum 4 × slot SFP+ 1/10 Gb/s, do instalacji modułów SFP+ 10G |
| Wydajność | Przepustowość przełączająca co najmniej 170 Gbit/s, wydajność min. 120 Mpps, praca non-blocking |
| Tabela MAC / pamięć | Obsługa min. 16 000 adresów MAC, min. 1 GB RAM, min. 512 MB pamięci flash, bufor pakietów min. 1,5 MB |
| Funkcje L2 | Obsługa VLAN IEEE 802.1Q (min. 4093 VLAN), STP 802.1D, RSTP 802.1w, MSTP 802.1s, mechanizmy ochrony przed pętlami (loop protection, BPDU/Root Guard lub równoważne) |
| Agregacja łączy | Obsługa LACP (IEEE 802.3ad); możliwość utworzenia min. 8 grup LAG, każda z co najmniej 8 portami |
| Ramki jumbo | Obsługa ramek jumbo o wielkości co najmniej 9000 bajtów |
| Funkcje L3 | Routing IPv4/IPv6 typu L3 Lite, w tym routing między VLAN (SVI); możliwość konfiguracji min. 500 tras statycznych oraz min. 64 interfejsów L3 (SVI, fizyczne, LAG, loopback) |
| Routing dynamiczny | Obsługa co najmniej jednego protokołu dynamicznego routingu wewnętrznego (np. RIP v2 lub rozwiązanie równoważne) |
| Bezpieczeństwo portów | Obsługa 802.1X (port-based, z możliwością przypisania VLAN), Port Security (limit MAC na porcie), mechanizmy ochrony protokołów warstwy 2 |
| DHCP i ARP | Obsługa DHCP Snooping z portami zaufanymi/niezaufanymi, IP Source Guard oraz Dynamic ARP Inspection lub rozwiązań równoważnych |
| ACL | sprzętowa obsługa list ACL L2/L3/L4 (MAC, IPv4, IPv6, TCP/UDP); możliwość zdefiniowania co najmniej 512 reguł ACL i przypisania ich do portów, LAG i interfejsów SVI |
| Multicast | IGMP v1/v2/v3 oraz IGMP Snooping v1/v2/v3, możliwość pracy jako IGMP querier/proxy |
| QoS | Obsługa mechanizmów QoS, klasyfikacja ruchu (m.in. po DSCP/CoS/ACL), co najmniej 4 kolejki sprzętowe na port wyjściowy oraz mechanizmy kolejkowania (np. SP/WRR lub równoważne) |
| Stackowanie | Możliwość łączenia w stos (lub rozwiązanie równoważne typu virtual chassis) min. 4 przełączników, zarządzanych jako jedno urządzenie (jeden adres IP). Możliwość tworzenia agregacji LAG/LACP obejmującej porty z różnych jednostek stosu (distributed LAG/MLAG lub równoważne). |
| Zarządzanie | Zarządzanie przez CLI (port konsoli RJ-45 lub USB-C, SSHv2), interfejs WWW (HTTP/HTTPS), obsługa SNMP v1/v2c/v3, syslog, NTP/SNTP, RMON lub równoważne |
| Konfiguracja | Możliwość zapisu/odtworzenia konfiguracji z pliku tekstowego (np. TFTP/HTTP(S)/SCP), minimum oddzielne konfiguracje running/startup |
| Zasilanie | Wbudowany zasilacz 100–240 V AC, 50/60 Hz |
| Środowisko pracy | Temperatura pracy co najmniej 0–50°C, wilgotność 10–90% bez kondensacji |
| Wymiary | Obudowa 1U, szerokość 19", głębokość nie większa niż 300 mm |
| Gwarancja i wsparcie | Wymagana gwarancja producenta typu „limited lifetime” lub na okres co najmniej 5 lat. Serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta przez minimum 36 miesięcy. Minimalny sposób realizacji gwarancji: naprawa lub wymiana realizowana w serwisie, po odesłaniu urządzenia do serwisu i odesłaniu urządzenia naprawionego lub wymienionego do Zamawiającego. Wykonawca zapewni przyjmowanie zgłoszeń w dni robocze oraz wsparcie zdalne w diagnostyce i obsłudze zgłoszeń serwisowych. |
| Cykl życia produktu | Na dzień składania ofert brak ogłoszonego zakończenia sprzedaży (End of Sale) i wsparcia (End of Support) |
| Stan i pochodzenie | Urządzenia fabrycznie nowe, nieużywane, z autoryzowanego kanału dystrybucji na teren UE, oznakowanie CE |
| Moduł SFP+ 10G Duplex LC – 8 sztuk | |
| **Parametr** | **Minimalne wymagania** |
| Rodzaj | Moduł optyczny SFP+ 10G Ethernet |
| Interfejs | Złącze optyczne duplex LC |
| Typ transmisji | Praca na światłowodzie jednomodowym (SM / OS2) w standardzie 10GBASE-LR (1310 nm) lub równoważnym |
| Zasięg | Min. 10 km na światłowodzie SM (OS2) (lub równoważny – nie mniejszy) |
| Zgodność | Zgodność ze standardem MSA, obsługa DDM (Digital Diagnostic Monitoring) |
| Kompatybilność | Pełna kompatybilność z oferowanymi przełącznikami (praca w trybie 10G, bez blokowania portu i bez ograniczania funkcjonalności); dopuszcza się moduły OEM/kompatybilne, o ile spełniają wymagania |
| Montaż | Możliwość instalacji w trybie hot-plug w slotach SFP+ przełącznika |
| Środowisko pracy | Temperatura pracy co najmniej 0–70°C |
| Gwarancja | Gwarancja min. 36 miesięcy, moduły fabrycznie nowe, oznakowanie CE |

|  |
| --- |
| **2. PRZEDŁUŻENIE OKRESU GWARANCYJNEGO O 24 MIESIĄCE DLA UŻYTKOWANEJ PRZEZ ZAMAWIAJĄCEGO MACIERZY DYSKOWEJ** |
| Przedmiotem zamówienia jest przedłużenie o okres 24 miesięcy gwarancji oraz wsparcia producenta dla użytkowanej przez Zamawiającego macierzy dyskowej typu RACK, wykorzystywanej w środowisku produkcyjnym.  Model: NetApp E2824  S/N: 952103001490  Aktualny zakres:  ● Non Returnable Disk Fee Plus do 30.04.2026  ● NBD Parts Delivery WTY do 30.04.2026  ● HARDWARE do 30.04.2026  ● Disk Drives do 30.04.2026  ● SSP All SW do 30.04.2026  Przedłużone wsparcie musi obejmować co najmniej zakres funkcjonalny aktualnie posiadany przez Zamawiającego, w tym:   1. Wsparcie sprzętowe (hardware support)    * pełna gwarancja producenta na komponenty macierzy,    * dostawa części zamiennych w trybie NBD – Next Business Day,    * możliwość realizacji napraw na miejscu u Zamawiającego (on-site),    * obsługa awarii podzespołów krytycznych, w tym kontrolerów, zasilaczy, modułów pamięci cache, modułów interfejsów oraz elementów sieciowych. 2. Wsparcie dla dysków twardych i SSD    * gwarancja na dyski z utrzymaniem pełnej funkcjonalności i wymianą w trybie NBD,    * wsparcie obejmujące wszystkie aktualnie zainstalowane dyski macierzy,    * utrzymanie poziomu usług odpowiadającego dotychczas posiadanej ochronie (np. programy rozszerzonego serwisu dla nośników). 3. Wsparcie oprogramowania macierzy    * aktualizacje oprogramowania układowego (firmware) macierzy i jej komponentów,    * aktualizacje oraz wsparcie dla oprogramowania zarządzającego, monitorującego i funkcjonalnego,    * dostęp do dokumentacji, poprawek, biuletynów bezpieczeństwa oraz materiałów technicznych producenta,    * dostęp do serwisu producenta w zakresie diagnostyki i rozwiązywania zgłoszeń. 4. Elementy rozszerzonego wsparcia    * wsparcie w trybach identycznych lub równoważnych do posiadanych obecnie świadczeń,    * kontynuacja usługi niewymagający zwrotu uszkodzonych dysków,    * obsługa zgłoszeń w ramach portalu serwisowego producenta przez cały okres trwania przedłużenia.   Zamawiający wymaga oświadczenia producenta lub dystrybutora, że serwis został wykupiony w autoryzowanym kanale sprzedaży NetApp. |

|  |  |
| --- | --- |
| **3. DOSTAWA DWÓCH URZĄDZEŃ UTM WRAZ Z INSTALACJĄ, KONFIGURACJĄ I WDROŻENIEM DO KLASTRA WYSOKIEJ DOSTĘPNOŚCI W ŚRODOWISKU BEZPIECZEŃSTWA SIECIOWEGO ZAMAWIAJĄCEGO.** | |
| Zamawiający wymaga dostarczenia dwóch nowych, identycznych urządzeń klasy UTM wraz z gwarancją oraz dostępem do aktualizacji oprogramowania zabezpieczającego przez okres 36 miesięcy. Wykonawca musi opracować: projekt wymiany obecnych urządzeń brzegowych (tj. urządzeń pracujących na styku sieci LAN oraz WAN), projekt podziału sieci LAN na wirtualne podsieci, harmonogram wdrożenia oraz zakres wdrożenia, który przedstawi Zamawiającemu do akceptacji. Wykonawca musi: wdrożyć dostarczane urządzenia, w tym min. skonfigurować je do pracy w klastrze wysokiej dostępności; opracować politykę deszyfracji danych szyfrowanych SSL (Secure Sockets Layer), opracować reguły działania w zależności od rodzaju ruchu, opracować polityki ponownego szyfrowania danych, skonfigurować urządzenia UTM do analizy ruchu SSL, opracować koncepcję segmentacji sieci, a w szczególności: skonfigurować wirtualne sieci LAN, strefy, skonfigurować urządzenia UTM oraz wszystkie przełączniki sieciowe. Ponadto Wykonawca wykona instruktaż z zakresu administracji dostarczonych urządzeń UTM; opracuje dokumentację powykonawczą. Wymagany klaster dwóch urządzeń UTM musi spełniać wszystkie wymienione poniżej funkcje sieciowe oraz bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Wymaga się dostarczenia dokumentu potwierdzającego gotowość świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia. System UTM realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Musi być możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. | |
| **Parametr** | **Minimalne wymagania** |
| Obudowa | Obudowa przystosowana do montażu w szafie RACK 19", wysokość 1U. |
| Interfejsy sieciowe | Co najmniej: • 1 port GE RJ45 przeznaczony do funkcji HA • 1 port GE RJ45 przeznaczony do funkcji zarządzania (MGMT) • 1 port GE RJ45 konsolowy • 1 port USB • 8 portów GE RJ45 przeznaczonych do ruchu użytkowego, • 8 portów 5/2.5/GE RJ45 przeznaczonych do ruchu użytkowego, • 4 porty GE SFP, • 8 portów 10GE SFP+ (SFP+/SFP) umożliwiających połączenia światłowodowe. Możliwość logicznego grupowania interfejsów, tworzenia VLAN oraz stref bezpieczeństwa. |
| Routowanie i SD-WAN | Obsługa routingu IPv4 i IPv6 (statycznego i dynamicznego) oraz mechanizmów SD-WAN lub równoważnych do zarządzania wieloma łączami WAN. |
| Praca w klastrze | Możliwość pracy w klastrze wysokiej dostępności (HA) w trybie aktywny/pasywny lub aktywny/aktywny, z pełną synchronizacją konfiguracji oraz sesji. |
| Zasilanie | Redundantne zasilanie AC w konfiguracji 1+1 (dwa zasilacze), zapewniające ciągłość pracy urządzenia. |
| Wydajność – firewall | Przepustowość zapory (firewall throughput) nie mniejsza niż 39 Gbit/s (wartość referencyjna producenta). |
| Wydajność – IPS | Przepustowość systemu IPS nie mniejsza niż 9 Gbit/s. |
| Wydajność – NGFW | Przepustowość NGFW (inspekcja aplikacyjna) nie mniejsza niż 7 Gbit/s. |
| Wydajność – ochrona przed zagrożeniami | Przepustowość ochrony przed zagrożeniami (Threat Protection) nie mniejsza niż 6 Gbit/s. |
| Wydajność – inspekcja SSL/TLS | Przepustowość inspekcji ruchu szyfrowanego SSL/TLS nie mniejsza niż 7 Gbit/s. |
| Wydajność – VPN IPsec | Przepustowość VPN IPsec nie mniejsza niż 36 Gbit/s. |
| Sesje i połączenia | Obsługa nie mniej niż 11 000 000 jednoczesnych sesji oraz nie mniej niż 400 000 nowych sesji na sekundę. |
| Funkcje bezpieczeństwa | Pełna funkcjonalność zapory nowej generacji (NGFW), w tym: • system zapobiegania włamaniom (IPS) z aktualizowanymi sygnaturami, • zaawansowana ochrona przed złośliwym oprogramowaniem, w tym analiza podejrzanych plików (sandboxing) lub równoważna, • filtrowanie ruchu WWW z wykorzystaniem kategorii oraz reputacji stron, • filtrowanie poczty elektronicznej (antyspam, antyphishing), • kontrola aplikacji (Application Control), • możliwość inspekcji ruchu szyfrowanego SSL/TLS, • segmentacja sieci (strefy bezpieczeństwa, VLAN), • obsługa VPN IPsec oraz SSL VPN. |
| Integracja i logowanie | Możliwość integracji z systemami logowania i analityki (lokalnymi lub chmurowymi), w tym eksport logów do zewnętrznych systemów SIEM oraz współpraca z rozwiązaniami do centralnego zarządzania i raportowania wykorzystywanymi przez Zamawiającego. |
| Polityki oparte o użytkownika | Możliwość tworzenia polityk bezpieczeństwa opartych o użytkownika, grupy oraz urządzenia, z integracją z usługą katalogową. |
| Licencje bezpieczeństwa | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagany jest pakiet licencji zawierający funkcjonalności minimalne: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Ochrona przez zagrożeniami typu Malware oparta na sztucznej inteligencji, Funkcjonalność zapobiegająca wyciekowi danych wrażliwych na okres 36 miesięcy. |
| Wsparcie techniczne | System UTM będzie objęty rozszerzonym wsparciem technicznym gwarantującym min.:  • Wsparcie telefoniczne zespołu certyfikowanych inżynierów.  • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.  • Doradztwo w zakresie konfiguracji.  • Doradztwo w zakresie podnoszenia poziomu bezpieczeństwa.  • Zdalne wsparcie techniczne.  • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.  • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).  • Przygotowanie systemu UTM do zdalnej konfiguracji.  • Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.  • Rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.  • Usługa zdalnego przeglądu konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.  • Zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.  • Min. 24 godziny wsparcia inżyniera w każdym roku kalendarzowym (łącznie 72 roboczogodziny przez 3 lata dla klastra UTM)  Dla zapewnienia wysokiego poziomu usług serwisowych, podmiot świadczący wsparcie musi posiadać certyfikat ISO 27001 lub równoważny. Zgłoszenia serwisowe będą przyjmowane w języku polskim przez dedykowany serwisowy moduł internetowy oraz infolinię w godzinach od 8:00 do 20:00. Wymagany jest czas reakcji na zgłoszenie nie dłuższy niż 4 godziny dla połączeń telefonicznych.  Na żądanie Zamawiającego Wykonawca przedstawi informacje o sposobie realizacji wsparcia zawierające: adres strony internetowej, numer infolinii telefonicznej oraz certyfikat ISO 27001 lub równoważny. |
| Gwarancja | Urządzenie musi być objęte standardowym serwisem gwarancyjnym producenta przez okres 36 miesięcy.  Dodatkowo wymagana jest rozszerzona gwarancja na urządzenia, polegająca na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement) w czasie nie dłuższym niż 24 godziny w dni robocze, dla zgłoszeń utworzonych do godz. 14:00 w dni robocze.  Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie Zamawiającego, realizowana przez producenta lub autoryzowanego partnera w języku polskim. |
| Usługa wdrożenia | Wykonawca dostarczy system UTM, zainstaluje, skonfiguruje oraz dokona przeniesienia całej obecnej konfiguracji z obecnie używanego systemu firewall. Wdrożenie będzie obejmować co najmniej:  • konfigurację ogólną systemu - adresy IP, DNS, DHCP, routing, NTP,  • konfiguracja interfejsów sieciowych - WAN, LAN, DMZ. Konfiguracja dodatkowego łącza zapasowego, łącznie z ustawieniem routingu oraz przygotowanie odpowiednich polityk  • integracja nowego systemu UTM z Active Directory,  • przeniesienie całej konfiguracji z istniejącego urządzenia Firewall na nowy system UTM z najnowszą stabilną wersją oprogramowania  • audyt reguł i ustawień, weryfikacja i poprawienie reguł oraz ustawień, optymalizacja używanych dotychczas reguł, zgodnie z dobrymi praktykami,  • konfiguracja loadbalancingu dla min. dwóch łączy WAN,  • konfiguracja QoS oraz kształtowania pasma dla co najmniej 8 profili,  • przeniesienie istniejących obiektów sieciowych – około 68 obiektów,  • przeniesienie istniejących reguł firewall oraz NAT – około 100 reguł,  • przeniesienie konfiguracji IPSec VPN,  • przeniesienie filtrów URL oraz SSL, konfiguracja inspekcji SSL – około 41 obiektów URL oraz około 37 obiektów SSL,  • opracowanie polityki deszyfracji danych szyfrowanych SSL (Secure Sockets Layer), opracowanie reguł działania w zależności od rodzaju ruchu, opracowanie polityki ponownego szyfrowania danych, konfiguracja urządzeń UTM  • konfiguracja przesyłania logów do posiadanych przez Zamawiającego instancji zbierających i przechowujących logi,  • wykonanie projektu podziału sieci LAN Zamawiającego  • utworzenie wirtualnych sieci LAN, konfiguracja przełączników, urządzeń UTM, konfiguracja polityk  Zamawiający może wymagać skonfigurowania dodatkowych parametrów systemu UTM, jeśli podczas wdrożenia zajdzie taka potrzeba.  Zamawiający wymaga, aby wdrożenie przeprowadził inżynier posiadający certyfikat techniczny producenta oferowanego rozwiązania, potwierdzający kompetencje z zakresu wdrażania systemów UTM. |
| Dokumentacja powykonawcza | Wykonawca dostarczy co najmniej w formie elektronicznej dokumentację powykonawczą. Dokumentacja powinna zawierać wszystkie dane dostępowe do konfigurowanych urządzeń, systemów, schematy podłączenia urządzeń do sieci LAN, opis konfiguracji dostarczonego i wdrożonego systemu UTM, opis wdrożonych polityk. |

|  |
| --- |
| **4. ODNOWIENIE LICENCJI NA OPROGRAMOWANIE DO WYKONYWANIA KOPII ZAPASOWYCH POSIADANE PRZEZ ZAMAWIAJĄCEGO NA OKRES 24 MIESIĘCY** |
| Przedmiotem zamówienia jest odnowienie licencji na oprogramowanie Veeam Backup and Replication (15 instancji) od momentu zakończenia obecnej licencji, która wygasa 11.07.2026, na okres 24 miesięcy oraz rozszerzenie obecnej licencji o dodatkowe 5 instancji. Co łącznie będzie stanowiło 20 instancji, które umożliwią utworzenie kopii zapasowych dla 20 maszyn.  Oprogramowanie objęte odnowieniem:   1. musi być w pełni kompatybilne z wersją i środowiskiem backupowym aktualnie eksploatowanym przez Zamawiającego, 2. musi umożliwiać nieprzerwane działanie istniejącej instalacji i zachowanie ciągłości wykonywania kopii zapasowych, 3. musi obejmować pełny pakiet funkcjonalności dostępnych w posiadanej przez Zamawiającego edycji, 4. musi zapewniać dostęp do aktualizacji, poprawek oraz wsparcia technicznego producenta przez cały okres odnowienia.   W ramach odnowienia licencji wykonawca zapewni:   * ciągłość wsparcia producenta przez okres 24 miesięcy, * możliwość pobierania aktualnych wersji oprogramowania, * wsparcie techniczne zgodne z obecnie wykorzystywanym poziomem serwisowym.   Zamawiający dopuszcza możliwość zaoferowania rozwiązania równoważnego. W przypadku zaoferowania produktu równoważnego, Wykonawca musi na własny koszt, do dnia 15.05.2026 roku, wykonać następujące czynności:  • zmigrować konfigurację dotychczasowej konsoli zarządzającej,  • przeprowadzić szkolenie stacjonarnie dla 3 pracowników IT w zakresie konfiguracji i obsługi zaproponowanego rozwiązania równoważnego minimum 12h,  • dostarczyć dokumentację powdrożeniową,  • cały zakres prac ma się odbyć stacjonarnie.  Wykonawca ponosi pełną odpowiedzialność za prawidłowe wdrożenie rozwiązania równoważnego, ciągłość ochrony środowiska Zamawiającego oraz zachowanie funkcjonalności nie mniejszej niż posiadany system.  Zaproponowane rozwiązanie równoważne musi spełniać poniższe wymagania: |
| **Wymagania ogólne** |
| Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, |
| Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej |
| Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy. |
| Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
| **Całkowite koszty posiadania** |
| Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
| Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
| 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 |
| Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |
| Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla conajmniej trzech pamięci masowych to takiej puli. |
| Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta. |
| Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. |
| Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. |
| Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
| Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) |
| Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |
| Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |
| Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
| 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 |
| Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
| Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
| Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |
| Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) |
| Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS) |
| Oprogramowanie musi posiadać integracje z systemami typu SIEM |
| Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. |
| **Wymagania RPO** |
| Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
| Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |
| Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V |
| Oprogramowanie 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 powinna działać w środowisku VMware. |
| Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
| Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). |
| Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
| Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. |
| Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. |
| Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
| Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |
| Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |
| Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
| Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
| Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| **Wymagania RTO** |
| Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. |
| Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
| 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 |
| Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre |
| Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. |
| Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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 |
| Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell |
| Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM |
| Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |
| Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. |
| Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications oraz logi audytowe i sign-in. |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. |
| 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. |
| Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. |
| Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. |
| Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2 |
| Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| **Ograniczenie ryzyka** |
| Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
| Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych |
| 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 |
| Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. |
| Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych |
| Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware |
| Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania |
| Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków |
| Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise |
| Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR |
| **Środowiska fizyczne** |
| Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego |
| Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych |
| Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux |
| Rozwiązanie musi wspierać system operacyjny macOS |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix |
| Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) |
| Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster |
| Rozwiązanie 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 |
| Rozwiązanie musi wspierać backup podłączonych dysków USB |
| Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym |
| Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) |
| Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone |
| Rozwiązanie musi wspierać kontrolę pasma sieciowego |
| Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych |
| Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN |
| Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft |
| Rozwiązanie musi wspierać technologię BitLocker |
| Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania |
| Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych |
| Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych |
| Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. |
| Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform |
| Rozwiązanie musi wspierać szyfrowanie |
| Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne |
| Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego |
| Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej |
| Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| **Monitoring** |
| System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich |
| System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
| System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
| System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter |
| System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |
| System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |
| System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk |
| System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |
| System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |
| System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) |
| System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |
| System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |
| System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |
| System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |
| System 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. |
| System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
| **Raportowanie** |
| System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
| System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
| System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. |
| System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V |
| System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF |
| System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc |
| System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach |
| System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów |
| System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych |
| System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych |
| System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury |
| System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta |
| System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. |
| System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. |
| System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
| System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) |
| System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

|  |  |
| --- | --- |
| **5. DOSTAWA URZĄDZENIA PAMIĘCI MASOWEJ TYPU NAS.** | |
| **Parametr** | **Minimalne wymagania** |
| Typ urządzenia | Sieciowy serwer plików w obudowie RACK, przystosowany do montażu w szafie 19” |
| Procesor | Procesor 64 bit wielordzeniowy, minimum 4 rdzenie fizyczne, przeznaczony do pracy ciągłej w urządzeniach magazynujących, o taktowaniu nie niższym niż 1,7 GHz lub równoważnym, zapewniającym stabilną pracę usług plikowych i obsługę konfiguracji RAID |
| Pamięć RAM | Minimum 4 GB pamięci operacyjnej |
| Obsługiwane dyski | Minimum 12 kieszeni na dyski 3.5” lub 2.5” SATA lub równoważne, Hot-Plug / Hot-Swap |
| Pojemność pamięci masowej | Łączna pojemność dostępnej przestrzeni po konfiguracji w RAID 6 musi wynosić minimum 86 TB |
| Konfiguracja RAID | Obsługa RAID 0/1/5/6/10 lub równoważnych; docelowa konfiguracja RAID 6 zapewniająca odporność na awarię dwóch dysków |
| Interfejsy sieciowe | Minimum 2 x 2,5G Minimum 2 x 10GbE SFP+ wraz ze dwoma wkładkami SFP+ 10GBASE-SR (MMF) po stronie serwera NAS oraz dwoma wkładkami SFP+ 10GBASE-SR (MMF) po stronie switcha Zamawiającego. Oraz 4 przewody do połączenia tych wkładek (patchcord) każdy o długości 1 m. |
| Diody LED | Minimum Status, LAN, HDD |
| Porty USB 3.2 | Minimum 4 |
| Przyciski | Reset, Zasilanie |
| Temperatura robocza | 0–40°C |
| Funkcje sieciowe | Obsługa serwerów plików dla środowisk Windows, Linux, macOS; możliwość integracji z usługami katalogowymi; obsługa protokołów NFS, SMB, iSCSI |
| Zasilanie | Redundantne zasilacze typu Hot‑Plug o wysokiej sprawności wraz z przewodami zasilającymi |
| Zarządzanie | Interfejs administracyjny dostępny przez przeglądarkę; możliwość monitorowania stanu dysków, temperatury, obciążenia oraz generowania alertów |
| Aktualizacje | Możliwość regularnej aktualizacji oprogramowania układowego |
| Oprogramowanie | Wbudowana w oprogramowanie funkcja do synchronizacji danych między urządzeniem zamawianym a urządzeniem posiadanym przez Zamawiającego.  Oprogramowanie w języku polskim. |
| Uwagi | Dostarczony sprzęt musi być fabrycznie nowy, wolny od wad fizycznych i prawnych, nieużywany. Wykonawca zapewni minimum 36 miesięcy gwarancji producenta na cały sprzęt, realizowanej w trybie on-site u Zamawiającego. Gwarancja musi obejmować pełne wsparcie techniczne, w tym naprawę lub wymianę uszkodzonych komponentów na miejscu u Zamawiającego, bez dodatkowych kosztów.  W przypadku wymiany uszkodzonych dysków, dyski zostają u Zamawiającego. W okresie gwarancyjnym Wykonawca zapewni dostęp do aktualizacji firmware oraz oprogramowania układowego zgodnie z zasadami producenta. Wszelkie naprawy muszą być wykonywane wyłącznie z użyciem nowych, oryginalnych lub równoważnych części zamiennych.  Oferowany sprzęt oraz oprogramowanie muszą znajdować się w aktywnym cyklu życia producenta oraz nie mogą być objęte planowanym zakończeniem wsparcia technicznego (End of Life / End of Support) wcześniej niż po upływie minimalnego okresu gwarancji wymaganej w zamówieniu. |

|  |  |
| --- | --- |
| **6. DOSTAWA SERWERA WRAZ Z SYSTEMEM OPERACYJNYM ORAZ SZAFĄ SERWEROWĄ TYPU RACK** | |
| **Parametr** | **Minimalne wymagania** |
| Obudowa | RACK 2U o wymiarach pasujących do szafy rack 19” o głębokości 1000 mm  W obudowie powinien być zainstalowany zestaw redundantnych wentylatorów. |
| System operacyjny | System operacyjny Windows Server 2025 Datacenter lub równoważny nie starszy niż 2 lata od daty premiery, zgodny z posiadanym przez Zamawiającego środowiskiem serwerowym oraz umożliwiający uruchamianie i zarządzanie maszynami wirtualnymi w technologii wykorzystywanej przez Zamawiającego, z możliwością wykorzystania posiadanych przez Zamawiającego licencji dostępowych.  Oprogramowanie systemowe musi posiadać wbudowane usługi katalogowe umożliwiające centralne zarządzanie użytkownikami i komputerami, wbudowane mechanizmy wirtualizacji umożliwiające migrację maszyn wirtualnych bez przerywania ich pracy oraz wbudowane centrum certyfikatów umożliwiające automatyczną dystrybucję certyfikatów. Funkcjonalności te muszą być dostępne bez konieczności instalowania dodatkowego oprogramowania innych producentów. |
| Licencje | Licencje dostępowej typu Device CAL lub równoważne dla minimum 20 urządzeń. |
| Pamięć RAM | Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci taktowaną przynajmniej z częstotliwością 3200MT/s.  384GB pamięci RAM z częstotliwością co najmniej 3200MT/s.  Po zainstalowaniu pamięci 384GB powinno pozostać minimum 4 sloty wolne. |
| Procesor | Liczba rdzeni: min. 16, liczba wątków: min. 32, częstotliwość bazowa min. 2,3 GHz, częstotliwość maksymalna (Turbo) min. 3,4 GHz, pamięć cache min. 24 MB, architektura 64-bitowa , wydajność pozwalająca na uruchomienie min. 20 maszyn wirtualnych |
| Płyta główna | • Płyta główna z możliwością zainstalowania jednego lub dwóch procesorów.  • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  • musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust),  • Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera.  • Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0 V3 |
| Zatoki dyskowe | Możliwość instalacji min. 12 dysków 3,5” lub 2.5'' Hot‑Plug. Po zainstalowaniu dysków wolnych zatok musi pozostać min. 4. |
| Pamięć masowa | Serwer musi być wyposażony w dyski SSD min. 2 x 960GB SATA Read Intensive 6Gbps Hot-plug i HDD o wielkości netto min. 24TB przy zastosowaniu RAID 6. Dyski przeznaczone do pracy ciągłej w środowisku serwerowym, zainstalowane w zatokach typu Hot-Plug. |
| Video | Zintegrowana karta graficzna. |
| Kontroler RAID | Kontroler sprzętowy z cache min. 8 GB, obsługa min. RAID 0/1/5/6/10 |
| Zasilanie | Redundantne zasilacze typu Hot‑Plug o wysokiej sprawności ( min. 80 PLUS Titanium) wraz z przewodami zasilającymi |
| Interfejsy sieciowe | Minimum 2 x 10 Gb/s po medium optycznym lub miedzianym. W zależności od użytego medium jeżeli są wymagane wkładki to również muszą być dołączone po stronie serwer jak i switcha Zamawiającego razem z przewodami (patchcord) każdy o długości 1 m.  Minimum 2 zintegrowane interfejsy sieciowe 1 Gb/s |
| Interfejsy dodatkowe | Porty USB, port zarządzania, wyjście wideo |
| Zarządzanie | Zdalne zarządzanie przez dedykowany port. Dostęp poprzez przeglądarkę internetową. |
| Złącza – przód | USB (złącze serwisowe z przewodem do podłączenia laptopa) USB-A 2.0  Złącze video |
| Złącza - tył | Złącze video  2 x RJ-45  2 x interfejsy sieciowe 10 Gb/s  RJ-45 (złącze serwisowe)  2 x USB-A |
| Elementy montażowe | Komplet wysuwanych szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych,  Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych. |
| Bezpieczeństwo | • Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.  • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  • Moduł TPM 2.0  • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera  • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem  • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| Certyfikaty | • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001  • Serwer musi posiadać deklaracja CE.  • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 lub nowszy. |
| Szafa RACK | • typ szafy: Stojąca  • wysokość: min. 37U max. 42U  • standard: RACK 19"  • wymiar całkowity: 600x1000 (szer./gł)  • nośność statyczna: do 800kg  • drzwi przednie szyba hartowana zamykane na klucz z możliwością montażu prawo lub lewo stronnego  • drzwi tylnie stalowe zamykane na klucz  • drzwi boczne zatrzaskowe  • otwory na przewody:  ◦ od góry  ◦ od dołu  • otwory wentylacyjne:  ◦ w górnej części z min 4 wentylatorami  • Panel podłogowy: 4 kółka z hamulcem + regulowane nóżki  • Materiał wykonania: Wysokiej jakości stal walcowana, malowana proszkowo  • szafa do samodzielnego montażu  • Szafa RACK musi spełniać aktualnie obowiązujące normy i standardy stosowane na rynku dla szaf teleinformatycznych. |
| Gwarancja | Dostarczony sprzęt musi być fabrycznie nowy, wolny od wad fizycznych i prawnych, nieużywany. Wykonawca zapewni minimum **60** miesięcy gwarancji producenta na cały sprzęt, realizowanej w trybie on-site u Zamawiającego.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Gwarancja musi obejmować pełne wsparcie techniczne, w tym naprawę lub wymianę uszkodzonych komponentów na miejscu u Zamawiającego, bez dodatkowych kosztów. W okresie gwarancyjnym Wykonawca zapewni dostęp do aktualizacji firmware oraz oprogramowania układowego zgodnie z zasadami producenta. Wszelkie naprawy muszą być wykonywane wyłącznie z użyciem nowych, oryginalnych lub równoważnych części zamiennych.  Oferowany sprzęt oraz oprogramowanie muszą znajdować się w aktywnym cyklu życia producenta oraz nie mogą być objęte planowanym zakończeniem wsparcia technicznego (End of Life / End of Support) wcześniej niż po upływie minimalnego okresu gwarancji wymaganej w zamówieniu. |

|  |  |
| --- | --- |
| **7. DOSTAWA OPROGRAMOWANIA NA ROZWIĄZANIE MFA DLA 15 UŻYTKOWNIKÓW, NA OKRES 3 LAT, PRZEZNACZONE DO ZABEZPIECZENIA ŚRODOWISKA DOMENOWEGO.** | |
| **Parametr** | **Minimalne wymagania** |
| Rodzaj rozwiązania | Oprogramowanie/usługa do uwierzytelniania wieloskładnikowego (MFA / 2-FA), chroniące dostęp do kont domenowych Cisco Duo lub równoważne. |
| Integracja z infrastrukturą | Musi współpracować z istniejącym środowiskiem katalogowym opartym na Active Directory, umożliwiając uwierzytelnianie użytkowników domenowych |
| Funkcjonalność | Dwustopniowa weryfikacja tożsamości: standardowy login + hasło + dodatkowy czynnik (np. aplikacja mobilna, kod OTP, token, push, inne – wg możliwości rozwiązania) |
| Zabezpieczenia | MFA musi być odporne na ataki phishingowe, uwzględniając nowoczesne mechanizmy (np. push, tokeny, klucze, MFA adaptacyjne / kontekstowe) |
| Ilość licencji | 15 użytkowników |
| Okres obowiązywania licencji | 36 miesięcy |
| Zarządzanie i administracja | Panel administracyjny umożliwiający zarządzanie użytkownikami, przypisywanie MFA, regenerację/odejście drugiego czynnika, resetowanie dostępu, przywracanie dostępu (np. po utracie urządzenia) |
| Polityki bezpieczeństwa | Możliwość definiowania reguł dostępu: np. wymóg MFA w zależności od grupy użytkowników, roli, typu urządzenia, lokalizacji, aplikacji lub ryzyka |
| Wsparcie i aktualizacje | Producent lub dostawca usługi musi zapewniać wsparcie techniczne, aktualizacje oprogramowania / komponentów uwierzytelniających przez cały okres licencji |
| Bezpieczeństwo danych | Wszystkie dane uwierzytelniające muszą być przechowywane z odpowiednim poziomem bezpieczeństwa (szyfrowanie, zgodność z normami ochrony danych) |
| Raportowanie i logi | System musi zapewniać możliwość prowadzenia logów logowań, MFA oraz generowania raportów dostępu dla celów audytu i bezpieczeństwa |

|  |
| --- |
| **8. ROZSZERZENIE LICZBY LICENCJI SYSTEMU OCHRONY STACJI ROBOCZYCH I SERWERÓW KLASY EDR/XDR WYKORZYSTYWANEGO PRZEZ ZAMAWIAJĄCEGO O 45 SZTUK.** |
| Przedmiotem zamówienia jest dostawa dodatkowych 45 licencji systemu ochrony stacji roboczych i serwerów klasy EDR/XDR wykorzystywanego przez Zamawiającego, zgodnego i w pełni kompatybilnego z rozwiązaniem bezpieczeństwa aktualnie wykorzystywanym przez Zamawiającego.  Licencje muszą być udzielone na okres tożsamy z posiadanym przez Zamawiającego oprogramowaniem, tj. do dnia 14 lipca 2027 r.  Oferowane licencje muszą:   1. być rozszerzeniem istniejącej subskrypcji Zamawiającego, 2. działać w ramach obecnie wykorzystywanej konsoli zarządzającej, 3. umożliwiać centralne zarządzanie, raportowanie i konfigurację zgodnie z dotychczas używanym systemem, 4. obejmować wszystkie funkcjonalności dostępne w posiadanym przez Zamawiającego pakiecie bezpieczeństwa.   Wykonawca zobowiązany jest dostarczyć licencje w sposób umożliwiający ich natychmiastową aktywację w istniejącym środowisku bezpieczeństwa Zamawiającego.  Zamawiający dopuszcza możliwość zaoferowania rozwiązania równoważnego. Zaproponowane rozwiązanie równoważne musi współpracować i być w pełni kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem eksploatowanym u Zamawiającego.  W przypadku zaoferowania produktu równoważnego, Wykonawca musi na własny koszt, do dnia 15.05.2026 roku, wykonać następujące czynności:  • dostarczenia łącznie 200 licencji systemu ochrony punktów końcowych klasy EDR/XDR, obejmujących:  - 45 licencji objętych przedmiotem zamówienia, finansowanych przez Zamawiającego,  - 155 licencji zapewnionych przez Wykonawcę na własny koszt, w celu zastąpienia całego dotychczasowego systemu,  • migrować konfigurację dotychczasowej konsoli zarządzającej  • wdrożyć konsolę zarządzają dla 200 stacji roboczych w tym serwerów  • zainstalować 200 agentów dla stacji roboczych i serwerów  • przeprowadzić szkolenie stacjonarnie dla 3 pracowników IT w zakresie konfiguracji i obsługi zaproponowanego rozwiązania równoważnego minimum 12h  • cały zakres prac ma się odbyć stacjonarnie  • zapewnienia, że po zakończeniu wdrożenia w środowisku Zamawiającego funkcjonuje wyłącznie jeden system ochrony punktów końcowych klasy EDR/XDR.  Wykonawca ponosi pełną odpowiedzialność za prawidłowe wdrożenie rozwiązania równoważnego, ciągłość ochrony środowiska Zamawiającego oraz zachowanie funkcjonalności nie mniejszej niż posiadany system klasy EDR/XDR. |

|  |  |
| --- | --- |
| **9. DOSTAWA PUNKTÓW DOSTĘPOWYCH, PRZEŁĄCZNIKÓW POE ORAZ OSPRZĘTU INSTALACYJNEGO DO BUDOWY SIECI WI-FI** | |
| 1. Zakres zamówienia  Przedmiotem zamówienia jest:  • dostawa i wniesienie 21 szt. punktów dostępowych sieci bezprzewodowej (wewnętrznych, tri-band, Wi-Fi 7),  • dostawa i wniesienie 8 szt. zarządzalnych przełączników PoE+ (małogabarytowych) do montażu w przestrzeni międzysufitowej, przeznaczonych do zasilenia 2–3 punktów dostępowych każdy,  • dostawa 8 szt. łączników modularnych RJ45 typu „beczka” kat. 6A/7 STP, beznarzędziowych,  • dostawa 8 szt. wtyków RJ45 STP kat. 6A/7, beznarzędziowych,  • dostawa kabla instalacyjnego kat. 6A S/FTP – 300 m.,  • udzielenie gwarancji i wsparcia serwisowego na okres wskazany w niniejszym OPZ i w załączniku „Parametry techniczne”,  • dostawa dokumentacji (instrukcja obsługi, karta katalogowa / dane techniczne) w języku polskim lub angielskim.  2. Wymagania ogólne  Sprzęt musi być:  • fabrycznie nowy, nieużywany, niepochodzący z ekspozycji,  • z autoryzowanego kanału dystrybucji na teren UE, oznakowanie CE,  • w momencie dostawy znajdować się w aktualnej ofercie producenta,  • na dzień składania ofert oferowany model urządzenia nie może mieć ogłoszonego przez producenta zakończenia sprzedaży (End of Sale / Last Date of Order lub równoważne) ani zakończenia wsparcia (End of Support / End of Life / Last Date of Support lub równoważne).  Zamawiający dopuszcza rozwiązania równoważne, spełniające co najmniej poniższe wymagania minimalne. | |
| **Punkt dostępowy sieci bezprzewodowej (wewnętrzny) – 21 sztuk:** | |
| **Parametr** | **Minimalne wymagania** |
| Przedmiot | Punkt dostępowy WLAN, przeznaczony do pracy w sieci Zamawiającego, do montażu wewnątrz budynku. |
| Standard sieci bezprzewodowej | Zgodność co najmniej z IEEE 802.11be (Wi‑Fi 7). |
| Pasma / radia | Tri‑band 2,4 GHz + 5 GHz + 6 GHz; co najmniej 3 radia Wi‑Fi, obsługa pracy jednoczesnej w trzech pasmach.\* |
| MIMO / strumienie | Co najmniej 2×2 MU‑MIMO w każdym z pasm roboczych. |
| Port przewodowy | Co najmniej 1× port RJ45 MultiGig (NBASE-T) obsługujący 100/1000/2.5G/5G. |
| Zasilanie | Zasilanie PoE zgodne co najmniej z IEEE 802.3at; dopuszcza się zasilanie z injektora PoE lub zasilacza (o ile jest wymagany – dostarczony w komplecie). |
| Bezpieczeństwo Wi‑Fi | Obsługa co najmniej WPA2/WPA3, 802.1X, możliwość pracy z izolacją klientów oraz portalem uwierzytelniającym (captive portal) lub rozwiązaniem równoważnym. |
| Zarządzanie i kompatybilność | Urządzenie musi być w pełni zarządzalne przez posiadany przez Zamawiającego system bezpieczeństwa sieci klasy UTM/NGFW lub zapewni kontroler/zarządzanie w cenie , pełniący funkcję kontrolera WLAN, w szczególności: adopcja/rejestracja punktu dostępowego, centralna konfiguracja, monitoring, aktualizacje oprogramowania. Nie dopuszcza się konieczności zakupu dodatkowego kontrolera sprzętowego ani usługi kontrolera w chmurze. |
| Funkcje radiowe | Możliwość prowadzenia skanowania/monitoringu widma w tle (background scanning) przy jednoczesnym świadczeniu usługi dostępowej w pasmach 2,4/5/6 GHz lub rozwiązanie równoważne zapewniające monitoring środowiska radiowego bez przerywania pracy sieci i bez istotnego ograniczenia jej funkcjonalności. |
| Montaż | Możliwość montażu co najmniej: sufit / szyna T‑Rail / ściana; w zestawie komplet elementów montażowych. |
| Wymiary i pobór mocy | Wymiary nie większe niż 180 × 180 × 56 mm; pobór mocy maks. 17 W (zasilanie PoE). |
| Gwarancja i wsparcie | Gwarancja producenta min. 36 miesięcy. Minimalny sposób realizacji gwarancji: naprawa lub wymiana realizowana w serwisie, po odesłaniu urządzenia do serwisu i odesłaniu urządzenia naprawionego lub wymienionego do Zamawiającego. Wykonawca zapewni przyjmowanie zgłoszeń w dni robocze oraz wsparcie zdalne w diagnostyce. |
| Cykl życia produktu | Na dzień składania ofert brak ogłoszonego zakończenia sprzedaży i wsparcia dla oferowanego modelu; wykonawca składa stosowne oświadczenie. |
| Stan i pochodzenie | Urządzenia fabrycznie nowe, nieużywane, z autoryzowanego kanału dystrybucji na teren UE, oznakowanie CE. |
| Uwagi | \* Użycie pasma 6 GHz podlega ograniczeniom/regulacjom krajowym; urządzenie musi wspierać pracę w dopuszczonych kanałach na terenie kraju instalacji. |
| **Przełącznik sieciowy PoE+ (zarządzalny, małogabarytowy) – 8 sztuk** | |
| Parametr | Minimalne wymagania |
| Przedmiot | Zarządzalny przełącznik sieciowy warstwy 2, przeznaczony do pracy jako przełącznik dostępowy w sieci LAN, do instalacji w przestrzeni międzysufitowej. |
| Porty | Minimum 8 × port 10/100/1000Base‑T (RJ‑45), auto‑negocjacja, auto MDI/MDI‑X; minimum 4 porty z funkcją PoE+. |
| PoE | Zgodność co najmniej z IEEE 802.3af oraz 802.3at; budżet PoE (łączny) min. 60 W; moc na port min. 30 W na portach PoE+. |
| Wydajność | Przepustowość przełączająca co najmniej 16 Gb/s; tabela adresów MAC min. 8 000; obsługa ramek jumbo min. 9 KB. |
| Funkcje L2 | Obsługa VLAN IEEE 802.1Q (min. 4 000 VLAN), STP/RSTP/MSTP (802.1D/802.1w/802.1s) lub równoważne, agregacja łączy LACP (IEEE 802.3ad) lub równoważna, port mirroring. |
| Multicast | Obsługa co najmniej IGMP snooping (v1/v2/v3) lub równoważna. |
| QoS | Obsługa priorytetyzacji ruchu CoS/DSCP (802.1p) lub równoważna; min. 4 kolejki na port. |
| Zarządzanie | Zarządzanie poprzez interfejs WWW (HTTP/HTTPS) oraz SNMP (v1/v2c/v3) lub równoważne; możliwość konfiguracji i kopii konfiguracji. |
| Konstrukcja | Obudowa metalowa lub równoważna, pasywne chłodzenie (fanless). Zasilacz 230 V AC w komplecie (wtyczka EU/PL). |
| Gwarancja i wsparcie | Gwarancja producenta min. 36 miesięcy. Minimalny sposób realizacji gwarancji: naprawa lub wymiana realizowana w serwisie, po odesłaniu urządzenia do serwisu i odesłaniu urządzenia naprawionego lub wymienionego do Zamawiającego. |
| Cykl życia produktu | Na dzień składania ofert brak ogłoszonego zakończenia sprzedaży i wsparcia dla oferowanego modelu; wykonawca składa stosowne oświadczenie. |
| Stan i pochodzenie | Urządzenia fabrycznie nowe, nieużywane, z autoryzowanego kanału dystrybucji na teren UE, oznakowanie CE. |
| **Łącznik modularny RJ45 typu „beczka” kat. 6A/7 STP, beznarzędziowy – 8 sztuk** | |
| Parametr | Minimalne wymagania |
| Przedmiot | Łącznik modularny RJ45 (RJ45‑RJ45) do łączenia dwóch przewodów zakończonych wtykiem RJ45. |
| Kategoria / ekranowanie | Kategoria co najmniej 6A (dopuszcza się kat. 7); ekranowanie STP/FTP; przystosowany do 10GBASE‑T. |
| Montaż | Beznarzędziowy (IDC lub równoważny), możliwość montażu bez użycia specjalistycznych narzędzi. |
| Zgodność przewodów | Obsługa przewodów skrętkowych z żyłą jednodrutową oraz wielodrutową (typowo instalacyjnych i patchcordowych). |
| Gwarancja | Gwarancja min. 24 miesiące; elementy fabrycznie nowe, oznakowanie CE (jeśli dotyczy). |
| **Wtyk RJ45 STP kat. 6A/7, beznarzędziowy – 8 sztuk** | |
| Parametr | Minimalne wymagania |
| Przedmiot | Wtyk RJ45 ekranowany do zakończenia kabla miedzianego skrętki. |
| Kategoria / ekranowanie | Kategoria co najmniej 6A (dopuszcza się kat. 7); ekranowanie STP; przystosowany do 10GBASE‑T. |
| Montaż | Beznarzędziowy (IDC lub równoważny), możliwość montażu bez zaciskarki. |
| Zgodność przewodów | Obsługa przewodów instalacyjnych i/lub patchcordowych; zakres obsługiwanych średnic żyły co najmniej AWG 26–23 (lub równoważny). |
| Gwarancja | Gwarancja min. 24 miesiące; elementy fabrycznie nowe. |
| **Kabel instalacyjny 300m** | |
| Parametr | Minimalne wymagania |
| Przedmiot | Kabel teleinformatyczny instalacyjny do okablowania strukturalnego (wewnątrz budynku) |
| Kategoria / zastosowanie | Min. kat. 6A, przeznaczony do transmisji 10GbE (10GBASE-T) |
| Ekranowanie | S/FTP (ekran na każdej parze + ekran całościowy) lub równoważne o nie gorszych parametrach EMC |
| Żyła | Drut (solid), min. AWG 23/1, żyły w całości z miedzi (nie dopuszcza się aluminium ani żył miedziowanych). |
| Powłoka | LSZH/LS0H lub równoważna o nie gorszych parametrach w zakresie emisji dymu i halogenów |
| Długość | 300 m |
| Gwarancja | Gwarancja min. 24 miesiące; wyrób fabrycznie nowy. |