**Załącznik nr 7 do SWZ**

**IR.ZP.EM.271.7.23**

**Opis Przedmiotu Zamówienia**

w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji o wartości zamówienia nie przekraczającej progów unijnych, o jakich stanowi art. 3 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 z późn. zm.) – dalej Pzp na dostawę pn. **Zakup i dostawa sprzętu komputerowego IT wraz z oprogramowaniem i licencjami   
w ramach projektu grantowego „Cyfrowa Gmina”**

w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina”

1. Przedmiotem zamówienia jest:

zakup i dostawa sprzętu komputerowego IT wraz z oprogramowaniem, licencjami i jego wdrożeniem, w ramach projektu grantowego „Cyfrowa Gmina”, z podziałem na 3 części:

**Część nr 1. Zakup i dostawa serwera RACK, macierzy dyskowej i zasilaczy UPS wraz z uruchomieniem i wdrożeniem systemu.**

**Część nr 2. Zakup i dostawa zapory UTM.**

**Część nr 3. Zakup i dostawa stacji roboczych wraz z monitorami oraz laptopów.**

1. Zakres zamówienia:
2. **Część nr 1 obejmuje zakup i dostawę:**

* **s**erwera RACK - 2 szt.,
* macierzy dyskowej – 1szt.
* zasilacz UPS - 2 szt, według poniższych tabel,
* uruchomienie i wdrożenia klastra dwuwęzłowego oraz migracji maszyn wirtualnych wskazanych przez Zamawiającego (maks. 3 VM) z systemami dziedzinowymi firmy RADIX, będącymi w posiadaniu Zamawiającego i migracji baz danych tych systemów. Wymagana jest autoryzacja firmy RADIX.

**Serwer RACK – 2 szt:**

|  |  |  |
| --- | --- | --- |
| L.p. | Parametr lub warunek | Minimalne wymagania |
| 1 | Obudowa | * Typu RACK, wysokość nie więcej niż 1U * Szyny umożliwiające wysunięcie serwera z szafy stelażowej * Możliwość zainstalowania 4 dysków twardych hot plug 3,5” * Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych * Zainstalowane 2 szt. dysków SSD SATA 240GB Hot-PLug, dyski skonfigurowane w RAID-1 podłączone do sprzętowego kontrolera RAID * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray |
| 2 | Procesor | * Jeden procesor 8-rdzeniowy, taktowanie bazowe 2,8 GHz, architektura x86\_64 * osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 154 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org/cpu2017/results/cpu2017.html> dla dowolnego serwera z oferty producenta. |
| 3 | Pamięć RAM | * 128 GB pamięci RAM * DDR4 Registered 3200Mhz |
| 4 | Płyta główna | * Dwuprocesorowa * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji procesorów 40-rdzeniowych * Zainstalowany moduł TPM 2.0 * 4 złącza PCI Express generacji 4 w tym:   + 3 fizyczne złącza o prędkości x16   + 1 fizyczne złącza o prędkości x8   + Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH * 32 gniazda pamięci RAM * Obsługa 4TB pamięci operacyjnej RAM DDR4 * Obsługa 10TB pamięci operacyjnej w konfiguracji RAM DDR4 + pamięć nieulotna * Wsparcie dla technologii:   + Memory Scrubbing   + SDDC   + ECC   + Memory Mirroring   + ADDDC * Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) * 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug * BIOS UEFI w specyfikacji 2.7 |
| 5 | Kontrolery dyskowe, I/O | * Kontroler SAS RAID dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10,5,50 * Kontroler FC 2x 16Gb MMF LC (wraz z przewodami 2 x FC OM4 LC/LC 5 metrów każdy) |
| 6 | Kontrolery LAN (Ethernet) | * Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:   + 4x 1GbitBase-T   + Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe |
| 7 | Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera * 1 port USB 3.0 wewnętrzne * 2 porty USB 3.0 dostępne z tyłu serwera * 2 porty USB 3.0 na panelu przednim * Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera. |
| 8 | Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W * Redundantne wentylatory hotplug |
| 9 | Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii   + informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:     - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express     - procesory CPU     - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM     - wbudowany na płycie głównej nośnik pamięci M.2 SSD     - status karty zarządzającej serwera     - wentylatory     - bateria podtrzymująca ustawienia BIOS płyty głównej     - zasilacze     - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym) * Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   + Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera   + Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym   + Dostęp poprzez przeglądarkę Web, SSH   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii   + Zarządzanie alarmami (zdarzenia poprzez SNMP)   + Możliwość przejęcia konsoli tekstowej   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)   + Obsługa serwerów proxy (autentykacja)   + Obsługa VLAN   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU)   + Wsparcie dla protokołu SSDP   + Obsługa protokołów TLS 1.2, SSL v3   + Obsługa protokołu LDAP   + Integracja z HP SIM   + Synchronizacja czasu poprzez protokół NTP   + Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna) * Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN * Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej |
| 10 | Wspierane systemy operacyjne | * Microsoft Windows Server 2022, 2019, 2016 * VMWare vSphere 6.7, 7.0 * Suse Linux Enterprise Server 15 * Red Hat Enterprise Linux 7.9, 8.3 * Hyper-V Server 2016, 2019 |
| 11 | Gwarancja | * 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). |
| 12 | Dokumentacja, inne | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 % * Zgodność z normami: CB, RoHS, WEEE, GS oraz CE. |
| 13 | System operacyjny | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego.  Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: 10. pozwalają na zmianę rozmiaru w czasie pracy systemu, 11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 12. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 13. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 14. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 15. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 16. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 17. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 18. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 19. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 20. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 21. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 22. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 24. Mechanizmy logowania w oparciu o: 25. Login i hasło, 26. Karty z certyfikatami (smartcard), 27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 28. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 29. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 32. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 35. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 36. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 37. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 38. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 39. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. 40. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. 41. Zdalna dystrybucja oprogramowania na stacje robocze. 42. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej 43. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 44. Dystrybucję certyfikatów poprzez http 45. Konsolidację CA dla wielu lasów domeny, 46. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, 47. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 48. Szyfrowanie plików i folderów. 49. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 50. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. 51. Serwis udostępniania stron WWW. 52. Wsparcie dla protokołu IP w wersji 6 (IPv6), 53. Wsparcie dla algorytmów Suite B (RFC 4869), 54. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 55. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 56. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 57. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. 58. Obsługi 4-KB sektorów dysków 59. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra 60. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. 61. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 62. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 63. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 64. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 65. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 66. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 67. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim |

**Macierz dyskowa - 1 szt.**

|  |  |  |
| --- | --- | --- |
| **LP** | **Parametr lub warunek** | **Minimalne wymagania** |
| 1 | **Ogólne** | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzewodową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek, aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać min. 142 dyski wykonane w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug NL-SAS i SSD. Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5” + 3,5”). |
| 2 | **Pojemność macierzy** | 5 dysków SSD-SAS umożliwiających udostępnienie 3,4 TB pojemności dostępnej dla hostów, w konfiguracji RAID-5 |
| 3 | **Kontrolery** | * Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi 2 kontrolerami; * Każdy z kontrolerów macierzy musi posiadać po 16GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu; * Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD, * W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk. * Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia; * Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. * Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. * Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej. * Kontrolery macierzy muszą obsługiwać do 70 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów * Oferowana macierz musi mieć wyprowadzone 2 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do sieci san na każdy kontroler RAID. * Macierz musi umożliwiać dołożenie do każdego z kontrolerów portów do transmisji danych (bez konieczności usuwania istniejących): * 2x FC 16 Gb/s * 2x iSCSI 10Gb/s SFP+ * 2x SAS 12Gb/s * 2x FC 32Gb/s   Dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych   * Macierz posiada obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy |
| 4 | **Poziomy RAID** | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:   * Raid-1 * Raid-10 * Raid-5 * Raid-50 * Raid-6 |
| 5 | **Dyski** | Oferowana macierz musi wspierać dyski hot-plug:   * dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s * dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,   Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;  Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex  Macierz musi obsługiwać min. 140 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;  Możliwość rozbudowy oferowanego modelu macierzy do 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;  Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) lub wirtualna przestrzeń zapasowa:   * Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID * Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID   W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess) lub nie wymaga zwolnienia zapasowej przestrzeni wirtualnej.  Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit dla danych blokowych – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą.  Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit. |
| 6 | **Opcje programowe** | * Macierz musi być wyposażona w system umożliwiający wykonanie kopii migawkowych * Macierz musi umożliwiać zdefiniowanie 4000 woluminów (LUN) * Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez 1000 ścieżek logicznych FC * Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów * Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową * Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere; * Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI. * Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy; * Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy; * Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’. * Macierz musi obsługiwać adresację IP v.4 i IP v.6 * Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji * Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. * Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NL-SAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy * Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy * Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników * Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN * Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy |
| 7 | **Zarządzanie** | * Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej * Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. * Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora * Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. |
| 8 | **Gwarancjai i serwis** | * Całe rozwiązanie musi być objęte 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowaną skuteczną naprawą do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. * Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego. * Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat. * System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta. * Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych * Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); * Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje. |

**Zasilacz UPS – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **LP** | **Parametr lub warunek** | **Minimalne wymagania** |
| 1 | **Moc** | 1500VA / 1500W |
| 2 | **Obudowa** | Typu RACK, max wysokość 2U, z elementami umożliwiającymi instalację w szafie RACK (szyny itp.) |
| 3 | **Napiecie wyjściowe** | 230 V |
| 4 | **Napięcie wejściowe** | 230 V |
| 5 | **Topologia UPS** | Line-Interactive |
| 6 | **Gniazda wyjściowe** | 10x IEC C13 w tym 5x obciążenia krytyczne i 5x obciążenia niekrytyczne |
| 7 | **Gniazdo wejściowe** | IEC C14 – wraz z kablem i wtyczką |
| 8 | **Czas podtrzymania przy pełnym obciążeniu** | Minimum 6 min |
| 9 | **Zarządzanie** | Karta zarządzająca wpinana do sieci LAN z interfejsem web umożliwiająca pełną kontrolę UPS, monitorowanie jego pracy, konfigurację alarmów, sprawdzenie stanu podzespołów, |
| 10 | **Oprogramowanie** | Wymagane oprogramowanie do zarządzania UPS, obsługiwane platformy: Windows, Linux |
| 11 | **Inne** | Wymagane:   * możliwość wymiany baterii przez użytkownika * wyświetlacz LCD z podstawową konfiguracją * funkcja Hot-Swap * port wyłącznika awaryjnego (EPO) * alarmy dźwiękowe (Tryb baterii, Niski poziom baterii, Przeciążenie, Przeładowanie, Przegrzanie) * certyfikat Energy Star, |
| 12 | **Gwarancja** | * 1. miesiące |

1. **Część nr 2 obejmuje zakup i dostawę:**

* **zapory UTM** - 1 szt., według poniższej tabeli:

**Zapora UTM – 1 szt.**

|  |  |  |
| --- | --- | --- |
| **LP** | **Parametr lub warunek** | **Minimalne wymagania** |
| 1. | **Wymagania Ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| 2 | **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| 3 | **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum:  * 16 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 2 gniazdami SFP+ 10 Gbps.  1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System musi być wyposażony w dwa zasilania AC. |
| 4 | **Parametry wydajnościowe** | 1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 56 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B. 4. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 1518 B. 5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.2 Gbps. 6. Wydajność szyfrowania IPSec VPN nie mniej niż 11 Gbps. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.6 Gbps. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. |
| 5 | **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH. |
| 6 | **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure * Cisco ACI. * Google Cloud Platform (GCP). * Nuage Networks VSP. * OpenStack. * VMware vCenter (ESXi). * VMware NSX. |
| **7** | **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |
| 8 | **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |
| 9 | **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| 10 | **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
| 11 | **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| 12 | **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| 13 | **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |
| 14 | **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| 15 | **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| 16 | **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. |
| 17 | **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. |
| 18 | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. |
| 19 | **Gwarancja oraz wsparcie** | 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.   Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty. |

1. **Część nr 3 obejmuje zakup i dostawę:**

- stacji roboczych wraz z monitorami – 7 kompletów, wraz z systemem operacyjnym   
i oprogramowaniem biurowym,

- laptopów – 2 szt. wraz systemem operacyjnym, według poniższych tabel:

**Stacje robocze z monitorami – 7 szt.**

|  |  |  |
| --- | --- | --- |
| **LP** | **Parametr lub warunek** | **Minimalne wymagania** |
| 1 | **Komputer stacjonarny - 7 szt.** | * **Obudowa:** Mini Tower/SFF * **Procesor:** zaprojektowany do pracy w komputerach stacjonarnych, co najmniej sześciordzeniowy o wydajności uzyskiwanej w teście Passmark co najmniej ---19537 pkt., wydruk w załączeniu. * **Pamięć RAM:** min. 16GB DIMM DDR4, 3200 MHz, * **Dysk twardy:** min. 512 GB SSD (Solid State Disk) M.2 lub SATA, * **Karta graficzna:** zintegrowana, * **Karta dźwiękowa:** karta dźwiękowa zintegrowana z płytą główną, * **Interfejsy** **i porty:** 1 x Displayport, 1 x HDMI – na płycie głównej, min. 8 x USB (panel przedni i tylny) w tym min. 2 x USB 3.2 na panelu przednim, 1x wyjście na mikrofon, 1 x wyjście liniowe, 1 x wyjście słuchawkowe (lub combo) 1 x RJ-45 LAN 10/100/1000 Mbps, * **Napęd optyczny:** wewnętrzny, odtwarzanie nośników CD, DVD-RW, * **Zasilanie:** Zasilacz wewnętrzny, kabel z wtyczką standard europejski, 230V, * **Dołączone wyposażenie:** klawiatura i mysz, * **Gwarancja:** 36 miesięcy na miejscu u klienta, * **Certyfikaty i wymagania:**  1. Certyfikat EPEAT na poziomie **SILVER**. Certyfikat ważny w dniu składania oferty i potwierdzony wydrukiem ze strony [www.epeat.net](http://www.epeat.net/), 2. Komputer musi być zaprojektowany i wyprodukowany w całości przez jednego producenta oraz wszystkie elementy komputera muszą pochodzić od tego samego producenta lub być przez niego sygnowane (opatrzone jego numerem katalogowym),  * **System Operacyjny:** Windows 11 Pro PL lub równoważny preinstalowany z licencją. Nie dopuszcza się w tym zakresie licencji pochodzącej z rynku wtórnego. Zamawiający zastrzega możliwość weryfikacji autentyczności legalności systemu operacyjnego. Równoważność:System operacyjny musi posiadać pełną zgodność z obecnym rozwiązaniem zarządzania komputerami w sieci Urzędu Miasta i Gminy Dobrzyń nad Wisłą (Microsoft Active Directory). * **Oprogramowanie biurowe:** Microsoft Office 2021 H&B - licencja nieograniczona czasowo lub inne równoważne, charakteryzujące się następującymi parametrami: * oprogramowanie musi zawierać: edytor tekstów, arkusz kalkulacyjny, program komunikacyjny zapewniający ujednolicone miejsce do zarządzania pocztą e-mail, kalendarzami, kontaktami, program do tworzenia prezentacji multimedialnych, * dokumenty utworzone w programach pakietu MS Office (edytor tekstów, arkusz kalkulacyjny oraz program do tworzenia prezentacji) otwarte na zaoferowanym przez wykonawcę programie musi poprawnie się uruchamiać, wydruk musi wyglądać identycznie bez jakiejkolwiek konieczności dodatkowej jego edycji oraz wszystkie funkcje muszą działać poprawnie a ich wynik musi być identyczny jak w przypadku programu z pakietu MS Office, bez konieczności reedycji otwartego dokumentu, * prawa licencyjne nie mogą ograniczać możliwości wykorzystania oprogramowania przez użytkowników zamawiającego, * warunki licencji nie mogą ograniczać możliwości przeniesienia jej na inny komputer, * produkt musi być w 100% nowy, wcześniej nie rejestrowany, produkt musi pochodzić z legalnego źródła. |
|  | **Monitory – 7 szt.** | * **Format ekranu:** panoramiczny * **Rodzaj matrycy:** matowa * **Technologia podświetlenia:** LED,IPS * **Przekątna ekranu:** 23,8” * **Rozdzielczość obrazu:** 1920x1080 (FullHD) * **Częstotliwość odświeżania:** 75Hz * **Montaż:** na dołączonej stopie * **Wbudowane głośniki:** Tak * R**egulacja kąta pochylenia:** Tak * **Pivot:** Tak * **Zasilanie:** przewód lub zasilacz z wtyczką standard europejski – 230V * **Interfejsy:** DisplayPort, HDMI * **Wyposażenie:** dołączony przewód DisplayPort 1.8 m |

**Laptopy – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **LP** | **Parametr lub warunek** | **Minimalne wymagania** |
| 1 | **Laptop – 2 szt** | * **Ekran:** matowy, antyodblaskowy,przekątna 15,6 cala, podświetlenie LED, rozdzielczość ekranu 1920 x 1080(FullHD), * **Procesor:** zaprojektowany do pracy w komputerach przenośnych, co najmniej 4-rdzeniowy o wydajności uzyskiwanej w teście Passmark co najmniej 9952 pkt., według danych na dzień ogłoszenia przetargu (wydruk w załączeniu), * **Pamięć RAM:** 16GB * **Dysk HDD:** 512GB SSD * **Karta graficzna:** zintegrowana * **Multimedia:** karta dźwiękowa zintegrowana z płytą główną, wbudowane głośniki, wbudowany mikrofon, wbudowana kamera internetowa * **Interfejsy** **i porty:** 1 x HDMI, min. 3 USB, w tym min. 2 x USB 3.2, złącze słuchawkowe i mikrofonowe lub COMBO, karta przewodowej transmisji LAN (1Gb), karta bezprzewodowej transmisji WiFi 5, klawiatura QWERTY z wydzieloną klawiaturą numeryczną, moduł bluetooth, czytnik kart SD * **Urządzenie wskazujące:** touch pad, dodatkowa mysz bezprzewodowa * **Zabezpieczenia:** szyfrowanie TPM, możliwość zabezpieczenia linką * **Zasilanie:** kabel zasilający wtyczka standard europejski 230V oraz zasilanie z wewnętrznej baterii * **Bateria:** 3-komorowa * **System operacyjny:** * Windows 11 Pro PL lub równoważny preinstalowany z licencją. Nie dopuszcza się w tym zakresie licencji pochodzącej z rynku wtórnego. Zamawiający zastrzega możliwość weryfikacji autentyczności legalności systemu operacyjnego. * Równoważność: * System operacyjny musi posiadać pełną zgodność z obecnym rozwiązaniem zarządzania komputerami w sieci Urzędu Miasta i Gminy Dobrzyń nad Wisłą (Microsoft Active Directory). * **Oprogramowanie biurowe:** Microsoft Office 2021 H&B - licencja nieograniczona czasowo lub inne równoważne, charakteryzujące się następującymi parametrami: * oprogramowanie musi zawierać: edytor tekstów, arkusz kalkulacyjny, program komunikacyjny zapewniający ujednolicone miejsce do zarządzania pocztą e-mail, kalendarzami, kontaktami, program do tworzenia prezentacji multimedialnych, * dokumenty utworzone w programach pakietu MS Office (edytor tekstów, arkusz kalkulacyjny oraz program do tworzenia prezentacji) otwarte na zaoferowanym przez wykonawcę programie musi poprawnie się uruchamiać, wydruk musi wyglądać identycznie bez jakiejkolwiek konieczności dodatkowej jego edycji oraz wszystkie funkcje muszą działać poprawnie a ich wynik musi być identyczny jak w przypadku programu z pakietu MS Office, bez konieczności reedycji otwartego dokumentu, * prawa licencyjne nie mogą ograniczać możliwości wykorzystania oprogramowania przez użytkowników zamawiającego , * warunki licencji nie mogą ograniczać możliwości przeniesienia jej na inny komputer, * produkt musi być w 100% nowy, wcześniej nie rejestrowany, produkt musi pochodzić z legalnego źródła. |

1. Na dostarczony przedmiot zamówienia, w odniesieniu do każdej części z osobna, Wykonawca udzieli gwarancji na okres wynikający z powyższego opisu przedmiotu zamówienia.
2. Nazwy i kody Wspólnego Słownika Zamówień (CPV):

* CPV 48820000-2 Serwer RACK
* CPV 30233141-1 Macierz dyskowa
* CPV 31682530-4 Zasilacz UPS
* CPV 32420000-3 Zapora UTM
* CPV 30213000-5 Komputery osobiste
* CPV 30213100-6 Komputery przenośne

1. Wszystkie parametry podane w powyższym opisie technicznym zamówienia należy traktować jako minimalne, chyba że z opisu przedmiotu zamówienia wynika inny opis. Zamawiający dopuszcza dostawę sprzętu i oprogramowania o o parametrach równoważnych lub wyższych.

Jeżeli powyższy opis wskazywałyby w odniesieniu do niektórych materiałów lub urządzeń znaki towarowe, patenty, technologię lub pochodzenie - Zamawiający, zgodnie z art. 101 ust. 4 ustawy Pzp, dopuszcza oferowanie rozwiązań równoważnych opisywanym powyżej. Wykonawca robót może zastąpić je materiałami, urządzeniami i produktami nie gorszymi, przy zachowaniu równorzędnych parametrów jakościowych i technicznych. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy.

Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt   
o wskazanych lub lepszych parametrach.

1. Dostarczone produkty muszą być fabrycznie nowe, nieuszkodzone i nienoszące śladów użytkowania.
2. Do obowiązków Wykonawcy należy dostawa, ubezpieczenie na czas transportu, transport, wniesienie przedmiotu zamówienia do siedziby Zamawiającego, tj. Urzędu Miasta i Gminy w Dobrzyniu nad Wisłą, ul. Szkolna 1, 87-610 Dobrzyń nad Wisłą.
3. O terminie dostawy Wykonawca zawiadomi Zamawiającego, co najmniej dwa dni robocze przed planowaną dostawą.
4. Termin wykonania przedmiotu zamówienia: Wykonawca zobowiązany jest zrealizować przedmiot zamówienia **w terminie zaoferowanym w złożonej ofercie jednak nie dłuższym niż 55 dni od** dnia zawarcia umowy, dla każdej części zamówienia z osobna.
5. Płatność wynagrodzenia zostanie dokonana na podstawie jednej faktury końcowej, wystawionej po dokonaniu przez Zamawiającego odbioru przedmiotu zamówienia   
   z osobna dla każdej części, w terminie 30 dni od momentu otrzymania prawidłowo wystawionej faktury.
6. Szczegółowe zagadnienia dotyczące realizacji przedmiotowego zamówienia określone są we Wzorze umowy, stanowiącym Załącznik nr 6 do SWZ.