**Załącznik nr 4 do SWZ**

**ZNAK SPRAWY: GK.271.14.2022**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dostawa sprzętu komputerowego w ramach zadania pn.:** **Realizacja projektu grantowego „Cyfrowa Gmina”**

* + - 1. **LOKALIZACJA.**

Działania będą realizowane na terenie budynku Urzędu Miejskiego w Lidzbarku Warmińskim ul. Świętochowskiego 14 .

* + - 1. **OGÓLNE WARUNKI DOSTAWY SPRZĘTÓW INFORMATYCZNYCH.**

1. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego
2. Wykonawca zapewni transport sprzętów na miejsce ich instalacji.
3. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nie noszący oznak użytkowania.
4. Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
5. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta.
6. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
7. Urządzenie na etapie dostawy producent a zamawiający nie mogą podlegać modyfikacjom.
8. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
9. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
10. Prace instalacyjne należy realizować w dni robocze w godzinach pracy Zamawiającego, w ustaleniu z Zamawiającym.
11. Ewentualne odstępstwa mogą być realizowane wyłącznie za zgodą Zamawiającego.
12. Wykonawca jest zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i systemów, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i systemów.
13. Gwarancja i serwis na urządzenia musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku gdy Oferent nie posiada takiej autoryzacji.
14. Możliwość sprawdzenia statusu gwarancji dla pełnej konfiguracji oferowanych urządzeń na stronie producenta po podaniu nr seryjnego serwera (jeśli producent oferuje taką możliwość).
15. Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
16. Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

**CZĘŚĆ 1 – MACIERZ DYSKOWA ORAZ PRZEŁĄCZNIKI SZKIELETOWE**

1. **Macierz dyskowa - 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne pojedynczej macierzy** |
| 1. | Obudowa | Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu. |
| 2. | Kontrolery dyskowe | 1. Minimum dwa kontrolery pracujące w trybie Symmetrical Active-Active (SAN-only), to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery muszą pozwalać na udostępnianie zasobów protokołem FC, iSCSI w zależności od zastosowanych kart komunikacyjnych. 2. Komunikacja pomiędzy parą kontrolerów (synchronizacja cache) macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband. 3. Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze wielu kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego. |
| 3. | Możliwość rozbudowy | 1. Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 2 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązanie oparte o wirtualizator. 2. Macierz musi umożliwiać rozbudowę do co najmniej 6 par kontrolerów dyskowych tworzących jedna logiczną macierz, bez konieczności wymiany zaoferowanej pary kontrolerów. 3. Macierz musi być skonstruowana wyłącznie do obsługi modułów pamięci SSD i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych. |
| 4. | Wymagana przestrzeń | 1. Całkowita pojemność brutto (fizyczna) urządzenia musi wynosić minimum 30 TB i musi być zbudowana wyłącznie w oparciu o moduły pamięci SSD. Rozmiar pojedynczego modułu nie może być większy niż 4 TB. 2. Macierz musi umożliwiać rozbudowę do co najmniej 70 sztuk oferowanego typu modułów pamięci, bez wymiany kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek i modułów SSD) |
| 5. | Procesory/Pamięć Cache | 1. Kontrolery łącznie muszą być wyposażone w procesory o sumarycznej ilości min. 48 rdzeni (ang.: core). Procesory w macierzy muszą obsługiwać protokół PCI Express Generacji 4. 2. Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. |
| 6. | Zabezpieczenie danych | 1. Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. 2. Urządzenie musi obsługiwać poziomy RAID5 i RAID6 (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare) lub równoważne poziomy RAID zabezpieczające przed awarią dwóch dysków jednocześnie. 3. Macierz musi umożliwiać skonfigurowanie poziomu RAID zapewniającego odporność na jednoczesną awarię 3 dysków w grupie RAID. |
| 7. | Dostępne interfejsy | 1. Macierz musi posiadać minimum 4 porty 10Gb/s obsługujące protokół iSCSI na każdy kontroler. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), wymaga się ich dostarczenia wraz z urządzeniem. 2. Możliwość rozbudowy macierzy o minimum 8 portów 16Gb/s obsługujących protokół NVMe over FibreChannel w ramach zaoferowanej ilości kontrolerów oraz możliwość podłączania serwerów bezpośrednio do tych portów macierzy bez użycia przełączników. Możliwość rozbudowy o wskazane porty nie może ograniczać rozbudowy do wymaganej ilości modułów pamięci. |
| 8. | Brak pojedynczego punktu awarii | Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy. |
| 9. | Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning) | Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation).  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| 10. | Snapshoty | Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 5000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write).  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.  Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii). |
| 11. | Funkcje kopiujące | Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| 12. | Redukcja danych | Macierz musi mieć możliwość włączenia funkcjonalności deduplikacji i kompresji danych w trybie in-line, a ponadto musi ona umożliwiać:   * włączenie deduplikacji dla poszczególnych wolumenów, * wyłączenie deduplikacji dla poszczególnych wolumenów na których wcześniej deduplikacja była włączona, * włączenie kompresji dla poszczególnych wolumenów, * wyłączenie kompresji dla poszczególnych wolumenów na których wcześniej kompresja była włączona, * uruchomienia jednocześnie deduplikacji i kompresji dla dowolnego wolumenu,   Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| 13. | Replikacja danych | Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| 14. | Klaster wysokiej dostępności | Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. 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 macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać klastrownie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| 15. | Priorytety zadań | Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| 16. | Kompatybilność | Model oferowanej macierzy musi znajdować się na oficjalnej liście zgodności VMware (dostępnej na stronie <https://www.vmware.com/resources/compatibility/search.php>) dla kryterium wyszukiwania “Site Recovery Manager (SRM) for SRA” i produktu “SRM 8.3” lub jego nowszej dostępnej aktualizacji. |
| 17. | Wielościeżkowość | Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows Server 2016/2019, Vmware 6.7 i 7.0, CentOS. |
| 18. | Zasilanie | Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap. |
| 19. | Zarządzanie macierzą | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów NVME. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI co najmniej 1 rok wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożlwiającym zbieranie i przeglądanie danych historycznych.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| 20. | Serwisowalność | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.  Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.  Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną. |
| 21. | Gwarancja, wsparcie serwisowe | 1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP. 2. Macierz dyskowa musi zostać objęta **minimum 60 miesięcznym okresem gwarancji** w trybie onsite z gwarantowanym czasem reakcji najpóźniej w 24 godziny od momentu zgłoszenia usterki. 3. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. 4. Usługi gwarancyjne świadczone przez wykonawcę/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001:2008 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001:2008 lub równoważny. 5. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:  * bezpłatna możliwość aktualizacje firmware; * dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń; * dostęp do centrum pomocy technicznej producenta; * otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware; * otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy |

1. **Przełącznik szkieletowy - 2 szt.**

|  |  |
| --- | --- |
| Lp. | **Wymagane minimalne parametry techniczne pojedynczego przełącznika szkieletowego** |
| 1. | Urządzenie musi być wyposażone w minimum 48 portów Gigabit Ethernet oraz 4 porty 10Gigabit Ethernet SFP+ mogących pracować jako Gigabit Ethernet SFP . |
| 2. | Urządzenie musi być dostarczone przewód DAC SFP+ do połączenia przełączników szkieletowych ze sobą w stos. kable DAC muszą pochodzić od producenta przełącznika celem uniknięcia problemów z serwisowaniem urządzenia. |
| 3. | Urządzenie musi mieć możliwość zainstalowania modułu rozszerzającego przełącznik o dodatkowe 8 portów SFP+ lub 2 QSFP. Przełącznik należy dostarczyć z modułem rozszerzającym o 8 SFP+ |
| 4. | Urządzenie musi umożliwiać stworzenie wirtualnego systemu - złożonego z min. 5 przełączników zarządzanych jako jedno urządzenie logiczne. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10Gigabit Ethernet oraz modułów optycznych lub kabli DAC. Musi istnieć możliwość terminowania połączeń link aggregation na dwóch przełącznikach tworzących taki system wirtualny (tzw. multi-chassis link aggregation) |
| 5. | Urządzenie musi być wyposażone w wewnętrzne redundantne zasilacze 230V AC wspierające mechanizm HotSwap. |
| 6. | Urządzenie musi być wyposażone w wewnętrzne redundantne wentylatory |
| 7. | Przepływ powietrza musi odbywać się od strony portów (zasysanie) w kierunku zasilaczy i modułów wentylacyjnych (wydmuch) |
| 8. Minimalne wymagane parametry wydajnościowe | |
|  | 1. Switching capacity: minimum 336 Gbps 2. min. 280 000 wpisów w tablicy adresów MAC 3. min. 120 000 wpisów w tablicy ARP 4. min. 500 000 wpisów w tablicy routingowej IPv4 5. min. 60 000 wpisów w tablicy routingowej IPv6 6. min. 1 000 interfejsów VLAN 7. min. 4 094 aktywnych/jednoczesnych sieci VLAN |
| 9. | Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4, ISIS-IPv4 |
| 10. | Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), BGP4+, ISIS-IPv6 |
| 11. | Obsługuje protokoły multicastowe w tym PIM Sparse i Dense Mode, IGMP/MLD |
| 12. | Musi umożliwiać rozbudowę o funkcjonalność VxLAN w przyszłości poprzez np.: zakup licencji |
| 13. Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: | |
|  | 1. mechanizm BFD (Bidirectional Forwarding Detection) 2. Wspracie dla: IEEE 802.1w Rapid Spanning Tree orazIEEE 802.1s Multiple Spanning Tree 3. IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów. |
| 14. Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS): | |
|  | 1. Obsługa min. 8 kolejek per port, w tym co najmniej jedna kolejka ze statusem strict priority 2. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji:, źródłowy/docelowy adres IP, żródłowy/docelowy port TCP |
| 15. Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem: | |
|  | 1. Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 3 poziomów uprawnień 2. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu 3. Obsługa co najmniej następujących mechanizmów DHCP Snooping, Dynamic ARP Inspection, 4. Weryfikacja źródła pakietu względem tablicy routingu (uRPF) –IPv4 5. Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP 6. Listy kontroli dostępu także dla IPv6 7. Mechanizmy ochrony warstwy kontrolnej |
| 16. | Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame) |
| 17. | Przystosowane do montażu w szafie 19”, wysokość nie większa niż 1RU, elementy niezbędne do montażu muszą być dostarczone z urządzeniem |
| 18. Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem: | |
|  | 1. Ma możliwość zarządzania przez WEB Gui (HTTPS), SNMPv3 oraz SSH v2 2. Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet out-of-band management 3. Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+ 4. Posiada port USB 5. Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie (SPAN,RSPAN), polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu 6. Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow, sFlow lub odpowiednik). 7. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania co najmniej 3 plików konfiguracyjnych. |
| 19. | Urządzenie musi mieć możliwość wyposażenia w zintegrowany kontroler sieci WLAN zdolny do pracy w klastrze HA przy utworzeniu stosu przełączników. Wymagane Parametry kontrolera sieci WLAN: |
|  | 1. Kontroler sieci bezprzewodowej umożliwia centralne zarządzanie minimum 16 bezprzewodowymi punktami dostępowymi z możliwością rozbudowy poprzez dokupienie licencji do minimum 1000 bezprzewodowych punktów dostępowych. 2. Kontroler WLAN musi umożliwiać zarządzanie punktami dostępowymi znajdowującymi się w tej samej domenie rozgłoszeniowej oraz znajdującymi się w innej podsieci IP |
| 20. | Możliwość łączenia kontrolerów w grupy urządzeń w celu zapewnienia redundancji (wymagane tryby 1+1 oraz N+1) |
| 21. | Wymagany jest **serwis gwarancyjny i serwis oprogramowania świadczony** **przez minimum 60 miesięcy.** |
| 22. | Dostępność serwisu 8x5xNBD w języku polskim. Rozwiązywanie problemów ze sprzętem i oprogramowaniem. |
| 23. | Gwarantowany czas naprawy sprzętu – 2 dni robocze od momentu potwierdzenia awarii. |
| 24. | Dostęp do poprawek i nowych wersji oprogramowania w okresie trwania serwisu. |

* + - 1. **Dostawa dodatkowych dwuportowych karty 10 Gbit/s BaseT - SFP+ z wkładkami:**

1. zgodne z HP ProLiant DL385p Gen8 - 2 szt.
2. zgodne z HP ProLiant DL385p Gen10 - 1 szt.
   * + 1. **Usługi wymagane podczas wdrożenia:**
3. Instalacja macierzy i przełączników szkieletowych w szafie Zamawiającego.
4. Podłączenie przełączników szkieletowych do istniejącej sieci komputerowej (konfiguracja VLAN zgodnie z wymaganiami Zamawiającego) – do przełącznika ARUBA za pomocą połączeń SFP+ (dostarczenie niezbędnych przewodów oraz wkładek SFP+ należy do Wykonawcy ).
5. Podłączenie przełączników szkieletowych do serwerów serwerów Vmware vSphere zamawiającego (3 szt.) oraz 1 urządzenia QNAP za pomocą połączeń SFP+ (dostarczenie niezbędnych przewodów oraz wkładek SFP+ należy do Wykonawcy) zapewniając redundancję wszystkich połączeń.
6. Inicjalizacja i konfiguracja macierzy.
7. Dopięcie macierzy do serwerów Vmware vSphere.
8. Utworzenie nowych dysków i wystawienie ich do Vmware vSphere.
9. Konfiguracja Vmware vSphere tak aby w pełni wykorzystać możliwości macierzy z dyskami NVME oraz przełączników zapewniając niezbędną bezawaryjność rozwiązania.
10. Instalacja dodatkowych kart SFP+ w serwerach Zamawiającego 2 x HP ProLiant DL385p Gen8, 1 x HP ProLiant DL385p Gen10.
11. Migracja danych na nowe zasoby ze starej macierzy zamawiającego HP p2000 G3.
12. Opracowanie dokumentacji powdrożeniowej opisującej sposób podłączenia, zastosowane technologie, sposób działania w przypadku awarii macierzy lub przełączników szkieletowych.
    * + 1. **Wymagania dodatkowe odnośnie wdrożenia:**

Inżynier instalujący i konfigurujący dostarczony sprzęt musi posiadać certyfikaty minimum:

* Vmware Certified Professional – Data Center Virtualization,
* Certyfikat techniczny wydany przez producenta dostarczonej macierzy.

**CZĘŚĆ 2 – ZESTAWY KOMPUTEROWE ORAZ LAPTOP**

1. **Komputer stacjonarny 39 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne komputerów** |
| **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| **Wydajność obliczeniowa** | Procesor min. 6-rdzeniowy dedykowany do pracy w komputerach stacjonarnych, osiągający w teście PassMark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 12200 punktów według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> |
| **Pamięć RAM** | 16GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB. Min. |
| **Pamięć masowa** | Dysk SSD M.2 PCIe NVMe min. 240GB  Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5” |
| **Wydajność grafiki** | Zintegrowana z procesorem |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port Combo, na tylnym panelu port audio Line-out z możliwością konfiguracji jako Line-in. |
| **Obudowa** | Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm.  Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, wymagany certyfikat 80 Plus Bronze. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| **Bezpieczeństwo** | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do Internetu i sieci lokalnej.  Procedura POST traktowana jest jako oddzielna funkcjonalność. |
| **BIOS** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Możliwość dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym.  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **Zgodność z systemami operacyjnymi i standardami** | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi |
| **System operacyjny** | Zainstalowany system operacyjny Windows 10 Pro, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| **Certyfikaty i standardy** | Urządzenia muszą być wyprodukowane zgodnie z normą ISO 50001:2018 oraz ISO 9001:2015.  Deklaracja zgodności CE (załączyć do oferty)  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki, w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. |
| Wymagania dodatkowe | Wbudowane porty: 2x Display Port 1.4, port audio typu combo (słuchawka/mikrofon) na przednim panelu, port audio Line-out na tylnym panelu obudowy (z możliwościa konfiguracji jako Line-in), 1xRJ-45, 8 portów USB wyprowadzonych na zewnątrz obudowy, w tym min. 2 porty USB na przednim panelu obudowy i min. 4 porty USB 3.2.  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługęWoL (funkcja włączana przez użytkownika),  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen. 3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 x SATA 3.0.  Jedno złącze M.2 dla dysków SSD oraz jedno złącze M.2 dla bezprzewodowej karty sieciowej.  Klawiatura USB w układzie polski programisty  Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w trybie pracy jałowej (IDLE) wynosząca maksymalnie 22 dB (załączyć oświadczenie producenta). |
| **Wsparcie techniczne producenta** | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku Recovery systemu operacyjnego). |
| **Warunki gwarancji** | Gwarancja producenta **minimum 24 miesiące**, świadczona na miejscu u klienta.  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |
| **Dodatkowe oprogramowanie** | 1. Oprogramowanie zarządzające producenta komputera, instalowane na etapie produkcji komputera, umożliwiające min.:  - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów  - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu  - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów  - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.  2. Bezpłatne oprogramowanie dostępne do pobrania na stronie internetowej producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:  -upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  -możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, jakiego komponentu sprzętu dotyczy aktualizacja, wszystkich poprzednich aktualizacjach z informacjami jak powyżej.  - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )  - sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr) i wersją (rewizja wydania)  - dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |

1. **Monitor – 39 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| Rodzaj | LCD |
| Przekątna | W przedziale od 23,8 do 24 cali |
| Proporcje obrazu | 16:9 (panoramiczny) |
| Typ matrycy | IPS, matowa (warstwa przeciwodblaskowa), podświetlanie LED |
| Rozdzielczość nominalna | 1920x1080 piksele |
| Kontrast | 1000:1 |
| Jasność | 250 cd/m² |
| Czas reakcji matrycy | Maksymalnie 6 ms (od szarego do szarego) |
| Kąt widzenia pion | 178 ° |
| Kąt widzenia poziom | 178 ° |
| Wbudowane głośniki | głośniki stereo |
| Złącza | 1x displayPort (wersja 1.2) 1x HDMI (wersja 1.4)  1x VGA |
| Obudowa | * Czarna lub grafitowa, matowa (nie błyszcząca) * Funkcja PIVOT * Mocowanie VESA |
| Okablowanie | kabel zasilający, DisplayPort, |
| Inne | wbudowany zasilacz |
| Gwarancja | **Minimum 24 miesiące**, z całkowitym brakiem „jasnych pikseli” przez cały okres obowiązywania gwarancji. |

1. **Komputer przenośny – laptop konwertowalny 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| Wielkość matrycy (przekątna) | 14 cali |
| Wydajność procesora | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej niż 10500 pkt. na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. |
| Ilość pamięci RAM | min. 16 GB |
| Rodzaj dysku twardego | Półprzewodnikowy (SSD – solid-state drive) |
| Pojemność dysku twardego | minimum 500 GB |
| Rodzaj matrycy | dotykowa |
| Rozdzielczość matrycy | co najmniej 1920 x 1080 pikseli |
| Rodzaj karty graficznej | zintegrowana |
| Łączność bezprzewodowa | Wi-FI 6 (802.11 a/b/g/n/ac/ax), moduł Bluetooth |
| Wejścia/wyjścia | min. USB 3.0; USB-C; HDMI; czytnik kart microSD; wyjście/wejście typu mini jack |
| Materiał wykonania obudowy | dowolny |
| Waga | maksymalnie 1500 gram |
| Możliwość pracy w trybie tabletu | przekształcenie w tabletu poprzez obrót ekranu na zawiasach, w taki sposób, że tylna obudowa matrycy opiera się na dolnej obudowie korpusu laptopa. |
| Czytnik linii papilarnych | do logowania w OS |
| System operacyjny | Zainstalowany Microsoft Windows 10 Professional PL - 64 bit lub równoważny, o parametrach równoważności podanych poniżej. Zainstalowany system operacyjny nie wymagający już aktywacji za pomocą telefonu lub Internetu w firmie producenta oprogramowania. Dołączony nośnik z oprogramowaniem. Parametry równoważności: Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012; Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI; Zainstalowany system operacyjny nie wymaga aktywacji za pomocą telefonu lub Internetu; Pełna integracja Płatnik; Pełna obsługa ActiveX Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji. |
| Dodatkowe akcesoria | Oryginalny rysik wielodotykowy do ekranu, Zasilacz, HUB USB-C – minimum 4 x USB , instrukcja obsługi |
| Torba transportowa | wyposażona w 3 komory zapinane zamkiem błyskawicznym z dwoma suwakami każdy. Wykonana z poliuretanów lub poliamidów. Dwie komory główne, z czego jedna dedykowana komora do transportu laptopa. Trzecia komora z kieszonkami na akcesoria takie jak telefon, długopisy, mysz bezprzewodowa. Torba wyposażona w uchwyt do noszenia w ręce oraz w regulowany, odpinany pasek do noszenia na ramieniu. Waga torby nie większa niż 1200 gram |
| Gwarancja | **Minimum 24 miesiące** |

**CZĘŚĆ 3 –URZĄDZENIA UTM**

**Urządzenia UTM – 2 szt.**

**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 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. 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.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

* 5 portami Gigabit Ethernet RJ-45.

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 100 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
5. 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 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
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 także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

**Polityki, Firewall**

1. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 3. 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. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. 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
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.

**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.

**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.

**Funkcje SD-WAN**

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

**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.

**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.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

**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.

**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.

**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. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

**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.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**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.

**Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

**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 24 miesiące.

**Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez **okres minimum 24 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.

**Opisy do wymagań ogólnych**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.