**Załącznik nr 2.1 do SWZ**

|  |
| --- |
| **MINIMALNE WYMAGANIA** |
| **Asortyment** | **Parametry wymagane** | **Parametry oferowane przez Wykonawcę (Wypełnia Wykonawca)** |
| **Laptop (3 sztuki)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |  |
| Przekątna Ekranu | 15,6” FHD (1920 x 1080), powłoką przeciwodblaskową, jasność 250 nits, kontrast min. 700:1, gama koloru min. NTSC 45% (typowo) |  |
| Procesor  | Wynik procesor osiąga w teście PassMark Performance Test co najmniej 10035 punktów w Passmark CPU Mark. Dostępny na stronie : <http://www.passmark.com/products/pt.htm> |  |
| Pamięć RAM | 16GB DDR4 3200MHz możliwość rozbudowy do min 32GB, 2 sloty na pamięci,  |  |
| Pamięć masowa | 512GB NVMe SSD M.2  |  |
| Karta graficzna | Zintegrowana karta graficzna  |  |
| Klawiatura | Klawiatura z $ i wbudowanym w klawiaturze podświetleniem, (układ US), min 98 klawiszy. Wszystkie klawisze funkcyjne typu: regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. Nie dopuszcza się innego układu a w szczególności między klawiszami ALT i CTRL (oprócz klawisza FN i Windows z lewej strony) |  |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W.Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy opatrzona wbudowaną mechaniczną przysłonę.czytnik kart microSD, 1 port audio typu combo (słuchawki i mikrofon) |  |
| Łączność bezprzewodowa | Intel® Wi-Fi 6 AX201 2x2 + Bluetooth 5.2  |  |
| Bateria i zasilanie | Bateria Polymer min. 4-ogniowa[min. 54Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.Zasilacz o mocy min. 65W |  |
| Waga i wymiary | Waga max 2kg z baterią 4-ogniowąSuma wymiarów notebooka nie większa niż 622mm (mierzone po krawędziach) |  |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Komputer spełniający normy MIL-STD-810H w zakresie min. 7 method [załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta]  |  |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag. Możliwość ustawienia hasła dla administratora, możliwość ustawienia hasła systemowego/użytkownika które jednocześnie będzie blokować uruchamianie systemu z jakichkolwiek urządzeń oraz umożliwia zalogowanie się do BIOS w celu zmiany swojego hasła, możliwość ustawienia hasła dla dysku NVMe, możliwość konfiguracji zależności między tymi hasłami, hasła muszą umożliwiać zawarcia w sobie znaków specjalnych, liczb i liter, Możliwość odczytania informacji o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS , po nadaniu numeru pole nie może być edytowalne. |  |
| Certyfikaty | Certyfikat ISO 9001 dla producenta sprzętu (należy załączyć do oferty)Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty)Deklaracja zgodności CE (załączyć do oferty)Certyfikat ISO 50001(należy załączyć do oferty)Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostkiPotwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony)EnergyStar – załączyć do oferty certyfikat lub wydruk z strony. |  |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 19dB (załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta)  |  |
| Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia: dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp. |  |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.Czytnik linii papilarnych  |  |
| System operacyjny | Oferowane modele komputerów muszą poprawnie współpracowaćz zamawianymi systemami operacyjnymi, tj.: (posiadający pełną funkcjonalność) z oryginalnym nośnikiem instalacyjnym lub kluczem licencyjnym umożliwiającym pobranie programu instalacyjnego ze strony producenta, zapewniający reinstalację, wsparcie dla Active Directory. Powyższe wymogi podyktowane są wykorzystaniem przy współpracy z oprogramowaniem zainstalowanym w sieci LAN zamawiającego:• Licencja powinna być nieograniczona w czasie,• Wykonawca zobowiązuje się dostarczyć niepowtarzalny (unikatowy) klucz do aktywacji dostarczonych licencji,• Oprogramowanie musi być fabrycznie nowe, objęte gwarancją oraz pochodzić z autoryzowanego kanału sprzedaży na rynek Unii Europejskiej,• Oprogramowanie nie może być wcześniej używane, regenerowane, serwisowane, rejestrowane ani aktywowane – Zamawiający zastrzega sobie prawo do weryfikacji czy dostarczone oprogramowanie (licencje) i powiązane z nimi elementy, takie jak certyfikaty/etykiety dołączone do oprogramowania są oryginalne, nowe i licencjonowane zgodnie z prawem oraz zasadami producenta oprogramowania,• Wykonawca zapewni kompatybilność (bezpieczeństwo, stabilnośći wydajność) nowych komputerów z wykorzystywanymi przez zamawiającego rozwiązaniami (zwłaszcza w kontekście udziałów sieciowych i uprawnień do nich) w oparciu o system domenw środowisku LAN.Jeżeli ze względu na zaoferowane oprogramowanie zaistnieje konieczność poniesienia przez zamawiającego dodatkowych nakładów (w szczególności na zmianę konfiguracji usług sieciowych, szkolenie pracowników, zwiększenie dotychczasowej czasochłonności przygotowania stanowisk komputerowych) niezbędnych do sprawnego funkcjonowania stacji roboczych w infrastrukturze teleinformatycznej zamawiającego, wszelkie koszty z tym związane poniesie wykonawca. |  |
| Oprogramowanie dodatkowe | Dołączone do oferowanego komputera oprogramowanie 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 :                a. o poprawkach i usprawnieniach dotyczących aktualizacji                b. dacie wydania ostatniej aktualizacji                c. priorytecie aktualizacji                d. zgodność z systemami operacyjnymi                e. jakiego komponentu sprzętu dotyczy aktualizacja                f.  wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.- 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.  |  |
| Porty i złącza | Wbudowane porty i złącza: 1x HDMI 1.4, 1x RJ-45, 2x USB 3.2 (w tym jeden zasilaniem), 1x USB 3.2 TYP-C z obsługą DP 1.2 i zasilaniem, 1x USB 2.0, port zasilania (nie zajmujący portów USB typ C), złącze linki zabezpieczającej. |  |
| Warunki gwarancyjne, wsparcie techniczne | 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)3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunkuFirma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta |  |
| **Serwer (1 sztuka)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Obudowa | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| Płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| Procesor | Zainstalowany jeden procesor min. 8-rdzeniowy, min. 2.8GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 129 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| RAM | Min. 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| Funkcjonalność pamięci RAM | Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing |  |
| Gniazda PCI | - minimum jeden slot PCIe x16 generacji 4  |  |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 porty 10GbE SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  |
| Dyski twarde | Możliwość instalacji dysków SAS, SATA, SSDZainstalowane 3 dyski SSD SATA MU o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug,Zainstalowane 3 dyski SAS o pojemności min. 2.4TB, 12Gb, 2,5“ Hot-Plug.Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |  |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. |  |
| Wbudowane porty | 4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim. |  |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| Zasilacze | Redundantne, Hot-Plug min. 800W każdy. |  |
| Bezpieczeństwo  | * Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
 |  |
| Diagnostyka | Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla IPv6;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
 |  |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022. |  |
| Warunki gwarancji | 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.Możliwość rozszerzenia gwarancji przez producenta do 7 lat.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |  |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Oprogramowanie (1 sztuka)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Wymagania | Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym. 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: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. W języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. login i hasło, b. karty z certyfikatami (smartcard), c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 19. 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. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. 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: I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. IV. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiająca: I. Dystrybucję certyfikatów poprzez http, II. Konsolidację CA dla wielu lasów domeny, III. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen, IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wsparcie dla algorytmów Suite B (RFC 4869), l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. 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: I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. III. Obsługi 4-KB sektorów dysków IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. 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. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  |  |
| **Zasilacz awaryjny (1 sztuka)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Wymagania ogólne | Urządzenie musi posiadać moc pozorną min. 2200 VA Urządzenie musi posiadać moc czynną min. 1800W Urządzenie musi być wykonany w topologii line interactive VI z automatyczną regulacją napięcia AVR i czystym sinusoidalnym przebiegiem napięcia. Zasilacz UPS musi posiadać uniwersalną obudowę Tower/Rack i być dostarczony wraz z kompletem kabli oraz zestawem szyn do montażu w szafie Rack.Urządzenie musi posiadać czas przełączania na pracę bateryjną 2-6 ms |  |
| Urządzenie musi posiadać parametry na wejściu co najmniej takie jak:  | • Napięcie znamionowe: 230 V (1-fazowe)• Tolerancja napięcia 161– 276V +/- 4% • Częstotliwość : 50 / 60 Hz (ustawiana automatycznie)• Gniazdo IEC320 C20 (16A) |  |
| Urządzenie musi posiadać parametry na wyjściu co najmniej takie jak: | • Napięcie znamionowe: 230 V (1-f) +/- 5% • Częstotliwość :50 /60 Hz + /- 0,1 % • Współczynnik mocy 0,9 przy 2000 VA• Gniazda wyjściowe: 8 szt. IEC320 C13 (10A) (2 segmenty)• Gniazdo dla dodatkowych kart komunikacyjnych • Gniazdo do podłączenia dodatkowej baterii |  |
| Wymagania dodatkowe | Zasilacz UPS musi posiadać hermetyczne, bezobsługowe akumulatory 6 szt. x 12V/7 Ah o żywotności 3-5 lat wg klasyfikacji EUROBAT umieszczone wewnątrz UPS-a i zapewniające całkowity czas podtrzymania min. 4’30 minut dla obciążenia 1800W.Urządzenie musi mieć możliwość dodania co najmniej 2 szt. dodatkowych modułów baterii każdy wyposażony w 12 szt. akumulatorów 12V/7 Ah. Jeden dodatkowy moduł baterii musi wydłużyć czas podtrzymania do min. 23 minut dla obciążenia 1800W. Wraz z zasilaczem UPS musi zostać dostarczony jeden dodatkowy moduł baterii.Dwa dodatkowe (opcjoalne) moduły baterii muszą wydłużyć czas podtrzymania do min. 43’30 minut dla obciążenia 1800W.Urządzenie musi mieć czas ładowania baterii < 4 godz. do pojemności użytkowej 80 % wydajności po całkowitym rozładowaniu.Zasilacz UPS musi mieć możliwość wymiany akumulatory przez użytkownika. |  |
| Urządzenie musi posiadać wyświetlacz LCD z ikonami graficznymi wskazującymi: | • obciążenie obecne, • poziom obciążenia, • alarm ogólny, • awaria baterii/ wymiana baterii, • przeciążenie, • pojemność baterii, • tryb normalny/ praca z użyciem baterii, • automatyczna regulacja napięcia włączona, • wyjścia programowalne, • wartość na wejściu |  |
| Zasilacz UPS musi posiadać alarmy dźwiękowe sygnalizujące: | • tryb bateryjny, • przeciążenie, • konieczność wymiany bateriiUrządzenie musi posiadać port USB i RS232 oraz slot na kartę sieciową.Zasilacz UPS należy wyposażyć w kartę komunikacyjną posiadającą poniższe funkcje oraz parametry:o połączenie z siecią Ethernet 10/100 Mb (złącze RJ 45),o monitorowanie zasilacza UPS za pomocą przeglądarki internetowej,o zdalne wyłączanie serwerów autonomicznych (kompatybilność z JNC) lub działających środowisku wirtualnym (kompatybilność z VIRTUAL-JNC),o informacja o awariach wysyłana e-mailem na min. 8 adresów,o zarządzanie zasilaczem UPS za pomocą protokołu SNMP,o możliwość monitorowania warunków pracy (czujnik temperatury i wilgotności EMD).o Modbus TCPoraz musi wspierać poniższe protokoły sieciowe: IPv4 / v6, HTTP / HTTPs z certyfikatem, DHCP / BOOTP, SNMP v1 / v2c / v3 (MD5-SHA / DES-AES), SMTP over TLS, SSH, UPnP, NTP / ICMP, WOL, RADIUS, TFTP, SYSLOGWraz z zasilaczem UPS musi zostać dostarczone oprogramowanie do monitorowania i wyłączania stacji roboczych działające w systemach operacyjnych Windows®, Linux® i Mac OS X® oraz karta SNMP.Urządzenie musi posiadać możliwość ochrony linii danych: tłumik udarowy NTP: RJ45Urządzenie musi posiadać wyłącznik awaryjny EPO |  |
| Zasilacz UPS musi być zgodny z Normami | • Bezpieczeństwo: IEC/EN 62040-1• Kompatybilność elektromagnetyczna IEC/EN 62040-2• Certyfikaty: RoHS, CE |  |
| Zasilacz UPS musi spełniać parametry środowiskowe co najmniej takie jak: | • Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie tempera-tur od 15 °C do 25 °C)• Wilgotność: 95 % bez kondensacji• Poziom hałasu w odległości 1 m < 50 dBWymiary zasilacza UPS (stand. czas podtrzymania) nie mogą być większe niż: szer. x głęb. x wys. (mm) 440 x 608 x 87; 2U.Masa zasilacza UPS (stand. czas podtrzymania) – nie większa niż 28,2 kg.Wymiary dodatkowego modułu baterii EBM nie mogą być większe niż: szer. x głęb. x wys. (mm) 440 x 608 x 87; 2U.Masa dodatkowego modułu baterii nie może być większa niż 40 kg.Urządzenie musi mieć możliwość dodania ręcznego bezprzerwowego bypassu serwisowego typu HOT SWAP tego samego producenta co zasilacz UPS. |  |
| Gwarancja | Urządzenie musi być objęte gwarancja producenta na okres co najmniej 36 miesięcy na moduł elektroniki oraz akumulatory. |  |
| **Przełącznik sieciowy (2 sztuki)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Przełącznik powinien posiadać interfejsy w minimalnej ilości: | • 48 portów PoE 10/100/1000 Mbps PoE+• 4 x SFP |  |
| Wymagane standardy, protokoły oraz funkcje | • IEEE® 802.3 10BASE-T• IEEE 802.3u 100BASE-TX• IEEE 802.3ab 1000BASE-T• IEEE 802.3z 1000BASE-X• IEEE 802.3x full-duplex flow control• IEEE 802.3az (EEE)• IEEE 802.3af (DTE Power via MDI)• IEEE 802.3at (DTE Power via MDI Enhancements)• IEEE 8021.Q VLAN (256 groups, Static)• IEEE 802.1p Class of Service (CoS)• 8 kolejek sprzętowych • Port-based QoS• IEEE 802.3ad Static or Dynamic Link Aggregation (LACP)• IEEE 802.1D Spanning Tree Protocol• IEEE 802.1w Rapid Spanning Tree Protocol• IEEE 802.1s Multiple Spanning Tree Protocol• SNMP v1, v2c, v3• RFC 1213 MIB II• RFC 1643 Ethernet Interface MIB• RFC 1493 Bridge MIB• RFC 2131 DHCP client• IEEE 802.1x (RADIUS)• RADIUS accounting• IEEE 802.1x Dynamic VLAN Assignment• HTTPS/SSL: Secure HTTP GUI• Layer 3 (DSCP) Quality of Service (QoS)• TACACS+• Port-based security by locked MAC addresses• TCP/UDP-based priority mapping• IGMP snooping v1, v2, v3• MLD snooping• ACLs (MAC, IPv4, IPv6 and TCP/UDP based)• Ograniczenie przepustowości na wejściu oraz wyjściu• SNTP• DNS• Ochrona przed DoS oraz Auto DoS• IPv6 management, multicast and QoS• Static Routing• DHCP snooping• Protocol and MAC-based VLAN• RMON group 1, 2, 3, 9• Private Enterprise MIB• Port mirroring – many-to-one• IEEE 802.3ab LLDP• LLDP-MED• Protected ports• Możliwość wykonania prostego testu okablowania |  |
| Funkcje oszczędności energii | • Zgodność z EEE (Energy Efficient Ethernet)• Obniżenie poboru energii w trybie bezczynności, lub krótkiego kabla |  |
| Wymagana wydajność | • Magistrala 104 Gbps • Budżet PoE: min. 380W• Bufor pakietów: 1,5 MB• Pamięćć RAM min. 128 MB• Ilość MAC: 16 K • Ilość VLANs: min 256; • Ilość kals 802.1p: 7• Ilość LAGs: 8• Ilość statycznych tras: 32• Ilość wpisów ARP: 1024• Kolejek DiffServ: 7• Ilość ACLs (IPv4/IPv6): min 100• Ilość grup multicast: 512 |  |
| Czas bezawaryjnej pracy | min. 1,7mln godzin |  |
| Gwarancja | 36 miesięcy |  |
| **Oprogramowanie (6 sztuk)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Ochrona danych - szyfrowanie | 1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit oraz Microsoft Windows 7/8/10 32-bit i 64-bit.2. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2005, 2008, 2012.3. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.4. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.5. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.6. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.7. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.8. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.9. Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:a) ilość znaków,b) czy hasło ma zawierać wielkie litery,c) czy hasło ma zawierać małe litery,d) czy hasło ma zawierać cyfry,e) czy hasło ma zawierać znaki specjalne,f ) okres ważności,g) ilość nieudanych logowań.10. Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:a) ilość znaków,b) czy hasło ma zawierać wielkie litery,c) czy hasło ma zawierać małe litery,d) czy hasło ma zawierać cyfry,e) czy hasło ma zawierać znaki specjalne,f ) okres ważności,g) ilość nieudanych logowań,h) możliwość zmiany hasła.12. Konsola centralnego zarządzania musi gromadzić informacje o:a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,c) dacie aktywacji klienta systemu szyfrowania danych,d) statusu szyfrowania,e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,f) stanie polityki,g) wersji klienta systemu szyfrowania danych,h) wersji systemu operacyjnego stacji roboczej,i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.13. Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.14. Konsola musi być dostępna z poziomu interfejsu WWW.15. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.16. Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.17. Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.18. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:a) instalacji klienta na stacji,b) zaszyfrowania/odszyfrowania stacji,c) wygenerowania klucza aktywacyjnego dla użytkownika,d) administrowania kluczami szyfrującymi,e) administrowania użytkownikami, którzy mają dostęp do stacji,f) administrowania profilem ustawień dla użytkowników,g) administrowania profilem ustawień dla stacji roboczych,h) wymuszenia zmiany hasła,i) zarządzania wieloma organizacjami z poziomu jednej konsoli. |  |
| Wymagania systemowe aplikacji klienckiej | 1. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server, 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit.2. System musi posiadać certyfikat FIPS 140-2 Level 1 |  |
| Wymagania dotyczące uwierzytelniania | 1. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.2. Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.3. Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).4. Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.5. Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot). |  |
| Wymagania dotyczące ustawień aplikacji klienckiej | 1. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.2. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania.3. Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:a) sektor po sektorze,b) kontener.4. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.5. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.6. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.7. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.8. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.9. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.10. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.11. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.12. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.13. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.14. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.15. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.16. Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:a) Guttman.b) US Department of Defence 5220.22-M (8-306. /E).c) US Department of Defence 5220.22-M (8-306. /E, CiE).d) Kryptograficzne losowe dane liczbowe.17. Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.18. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.19. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.20. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.21. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI. |  |
| Wymagania dotyczące szyfrowania | 1. Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.2. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.3. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.4. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza.5. Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:a) AES (Rijndael).b) Blowfish.c) Triple DES (3DES).6. Aplikacja musi umożliwiać współpracę z dyskami SSD.7. Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL.8. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.9. Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.10. Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku. |  |
| Wymagania dotyczące sytuacji krytycznych | 1. W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora.2. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania. |  |
| **Oprogramowanie (25 sztuk)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Wymagania | Licencja umożliwiająca pracę z urządzeniami podpiętymi do sieci wewnętrznej Zamawiającego. Licencja dostępowa dla urządzeń uzyskujących dostęp do serwera, bez względu na liczbę użytkowników, którzy korzystają z serwera za pośrednictwem danego urządzenia.Licencja musi mieć możliwość uruchomiania aplikacji będących w posiadaniu Zamawiającego.Licencja musi posiadać funkcjonalność taką jak co najmniej udostępnianie plików, udostępnianie drukarek. |  |
| **Urządzenie typu firewall UTM (1 sztuka)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| 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: 10 portami Gigabit Ethernet RJ-45.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.4. 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 10 Gbps dla pakietów 512 B.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 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 1.4 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 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. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.11. 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 | 12. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 13. 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. 14. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.15. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.16. 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.2. 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. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.4. 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. |  |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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. |  |