|  |  |  |
| --- | --- | --- |
| **MINIMALNE WYMAGANIA** | | |
| **Asortyment** | **Parametry wymagane** | **Parametry oferowane przez Wykonawcę (Wypełnia Wykonawca)** |
| **Komputery stacjonarne typu AIO,**  **typ 1**  **(63 sztuki)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Typ | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera. |  |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |  |
| Procesor | Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 14400 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net |  |
| Pamięć RAM | 8GB DDR4 3200MHz, jeden slot wolny. Możliwość rozbudowy do min 64GB. |  |
| Pamięć masowa | 256GB SSD M.2 NVMe  Możliwość instalacji dodatkowego dysku twardego |  |
| Wydajność grafiki | Karta graficzna zintegrowana |  |
| Rozmiar matrycy/ plamki | min.23,8” / max. 0,275mm |  |
| Rozdzielczość | FHD (1920x1080) |  |
| Jasność typowa | min. 250 cd/m² |  |
| Kontrast typowy | 1000:1 |  |
| Barwa koloru (typowa) | 99% sRGB |  |
| Kąty typowe | 178(+/- 89) / 178 (+/-89) |  |
| Rodzaj matrycy | Matowa IPS |  |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał.  Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP. Mechanicznie chowana w obudowie ( nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy)  Wbudowane w obudowę dwa mikrofony |  |
| Obudowa | Typu All-in-One zintegrowana z monitorem min. 23”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100,  Suma wymiarów obudowy bez zainstalowanego standu nie może przekraczać: 94cm  Zasilacz wewnętrzny o mocy min. 155W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%,  Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus  Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji.  Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS.  Podstawa jednostki typu All – in – One musi umożliwiać:  Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. |  |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). |  |
| Zdalne zarządzanie | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.:  - Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;  - Zdalną konfigurację ustawień BIOS,  - Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;  - Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.  - Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/). |  |
| Bezpieczeństwo | Płyta główna zawierająca 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  Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.  Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS |  |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera 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 systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu hasła systemowego/użytkownika w BIOS jest wstanie zidentyfikować ustawienia oraz dokonać zmiany hasła systemowego/użytkownika. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Dedykowane pole inwentarzowe umożliwiająca wpisanie oznaczenia sprzętu. Pole po nadaniu numeru nie może być edytowalne.  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. |  |
| Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)  Deklaracja zgodności CE (załączyć do oferty)  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001  Certyfikat TCO Edge, wymagana certyfikacja na stronie: <http://tcocertified.com/product-finder/>– załączyć do oferty wydruk z strony  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. |  |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB (załączyć opatrzone numerem postępowania oświadczenie wykonawcy poparte oświadczeniem producenta) |  |
| System Operacyjny | Zainstalowany system operacyjny klucz licencyjny zapisany trwale w BIOS, umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  - zainstalowany system operacyjny,  - klucz licencyjny zapisany trwale w BIOS,  - musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego  - polska wersja językowa,  - dostępność aktualizacji i poprawek do systemu u producenta systemu bezpłatnie i bez dodatkowych opłat licencyjnych z możliwością wyboru instalowanych poprawek,  - graficzne środowisko instalacji i konfiguracji,  - możliwość udostępniania plików i drukarek,  - zapewnienie wsparcia dla większości powszechnie używanych urządzeń (drukarek, urządzeń  sieciowych, standardów USB, urządzeń Plug & Play, WiFi,  - wyposażenie systemu w graficzny interfejs użytkownika w języku polskim,  - zapewnienie pełnej kompatybilności z oferowanym sprzętem,  - zintegrowanie z systemem modułu pomocy dla użytkownika w języku polskim,  - możliwość wykonywania kopii bezpieczeństwa wraz z możliwością automatycznego odzyskania  wersji wcześniejszej,  - zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie,  - licencja na system operacyjny musi być nieograniczona w czasie, pozwalać na wielokrotne  instalowanie systemu na oferowanym sprzęcie bez konieczności kontaktowania się przez  Zamawiającego z producentem systemu lub sprzętu,  - oprogramowanie powinno posiadać certyfikat autentyczności lub unikalny kod aktywacyjny,  - zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi  emulujących działanie systemów.  - 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  - Wykonawca zapewni kompatybilność (bezpieczeństwo, stabilność i wydajność) nowych komputerów z wykorzystywanymi przez Zamawiającego rozwiązaniami (zwłaszcza w kontekście udziałów sieciowych i uprawnień do nich) w oparciu o system domen w środowisku LAN  - 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,  System musi umożliwiać pracę w domenie – wsparcie dla Active Directory |  |
| Wymagania dodatkowe | Wbudowane porty:  1x DP++ 1.4/HDCP 2.3  1x HDMI In 1.4a  1 x HDMI 2.0  1x USB 3.2 Gen 2 Type-C port  2x USB 3.2 Gen 2 Type-A port  3x USB 3.2 Gen 1 Type-A port  Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp.  1x Universal audio jack  1x Line-out audio  1x RJ-45 port 10/100/1000 Mbps  Czytnik kart SD 4.0  Karta WiFi ax+ bluetooth 5.1  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi, przynajmniej jedno złącze z obsługą protokołu SATA III umożliwiające bezpośrednie podłączenie oraz zasilanie dodatkowego dysku 2.5” (bez stosowania kabli zasilających).  Klawiatura USB w układzie polski programisty  Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) |  |
| Warunki gwarancji  Wsparcie techniczne | 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.  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.  Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego przedłużenia tego okresu do 4 lub 5 lat od daty dostawy.  Sposób realizacji usług wsparcia technicznego:  • Telefoniczne zgłaszanie usterek w trybie 24h / dobę, 7 dni w tygodniu (w języku polskim w dni robocze w godz. 8-17).  • Dostęp do bezpłatnego portalu technicznego producenta, który umożliwi zamawianie części zamiennych i/lub wizyt technika serwisowego, mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki.  • Opcjonalna pomoc techniczna za pośrednictwem czat online.  Wsparcie techniczne świadczone przez pracowników producenta urządzeń dla sprzętu i wybranego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzien roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Mozliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym.  Przydzielenie zasobu w postaci kierownika technicznego w przypadku eskalacji problemów serwisowych.  Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki, zdalnego zgłaszania awarii do serwisu i automatycznego zakładania zgłoszeń serwisowych. |  |
| Dodatkowe oprogramowanie | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją 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,  - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi  - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji  - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)  - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml  Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.  W ofercie należy podać nazwę oprogramowania |  |
| **Komputery stacjonarne typu AIO, typ 2**  **(7 sztuk)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Typ | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera. |  |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |  |
| Procesor | Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 20380 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net |  |
| Pamięć RAM | 16GB DDR4 3200MHz, jeden slot wolny. Możliwość rozbudowy do min 64GB. |  |
| Pamięć masowa | 512GB SSD M.2 NVMe  Możliwość instalacji dodatkowego dysku twardego |  |
| Wydajność grafiki | Karta graficzna zintegrowana |  |
| Rozmiar matrycy / plamki | min.23,8” / max. 0,275mm |  |
| Rozdzielczość | FHD (1920x1080) |  |
| Jasność typowa | min. 250 cd/m² |  |
| Kontrast typowy | 1000:1 |  |
| Barwa koloru (typowa) | 99% sRGB |  |
| Kąty typowe | 178(+/- 89) / 178 (+/-89) |  |
| Rodzaj matrycy | Matowa IPS |  |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał.  Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP. Mechanicznie chowana w obudowie ( nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy)  Wbudowane w obudowę dwa mikrofony |  |
| Obudowa | Typu All-in-One zintegrowana z monitorem min. 23”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100,  Suma wymiarów obudowy bez zainstalowanego standu nie może przekraczać: 94cm  Zasilacz wewnętrzny o mocy min. 155W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%,  Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus  Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji.  Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS.  Podstawa jednostki typu All – in – One musi umożliwiać:  Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. |  |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). |  |
| Zdalne zarządzanie | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.:  - Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;  - Zdalną konfigurację ustawień BIOS,  - Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;  - Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.  - Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/). |  |
| Bezpieczeństwo | Płyta główna zawierająca 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  Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.  Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS |  |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera 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 systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu hasła systemowego/użytkownika w BIOS jest wstanie zidentyfikować ustawienia oraz dokonać zmiany hasła systemowego/użytkownika. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Dedykowane pole inwentarzowe umożliwiająca wpisanie oznaczenia sprzętu. Pole po nadaniu numeru nie może być edytowalne.  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. |  |
| Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)  Deklaracja zgodności CE (załączyć do oferty)  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001  Certyfikat TCO Edge, wymagana certyfikacja na stronie: <http://tcocertified.com/product-finder/>– załączyć do oferty wydruk z strony  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. |  |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB (załączyć opatrzone numerem postępowania oświadczenie wykonawcy poparte oświadczeniem producenta) |  |
| System Operacyjny | Zainstalowany system operacyjny klucz licencyjny zapisany trwale w BIOS, umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  - zainstalowany system operacyjny,  - klucz licencyjny zapisany trwale w BIOS,  - musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego  - polska wersja językowa,  - dostępność aktualizacji i poprawek do systemu u producenta systemu bezpłatnie i bez  dodatkowych opłat licencyjnych z możliwością wyboru instalowanych poprawek,  - graficzne środowisko instalacji i konfiguracji,  - możliwość udostępniania plików i drukarek,  - zapewnienie wsparcia dla większości powszechnie używanych urządzeń (drukarek, urządzeń  sieciowych, standardów USB, urządzeń Plug & Play, WiFi,  - wyposażenie systemu w graficzny interfejs użytkownika w języku polskim,  - zapewnienie pełnej kompatybilności z oferowanym sprzętem,  - zintegrowanie z systemem modułu pomocy dla użytkownika w języku polskim,  - możliwość wykonywania kopii bezpieczeństwa wraz z możliwością automatycznego odzyskania  wersji wcześniejszej,  - zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie,  - licencja na system operacyjny musi być nieograniczona w czasie, pozwalać na wielokrotne  instalowanie systemu na oferowanym sprzęcie bez konieczności kontaktowania się przez  Zamawiającego z producentem systemu lub sprzętu,  - oprogramowanie powinno posiadać certyfikat autentyczności lub unikalny kod aktywacyjny,  - zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi  emulujących działanie systemów.  - 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  - Wykonawca zapewni kompatybilność (bezpieczeństwo, stabilność i wydajność) nowych komputerów z wykorzystywanymi przez Zamawiającego rozwiązaniami (zwłaszcza w kontekście udziałów sieciowych i uprawnień do nich) w oparciu o system domen w środowisku LAN  - 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,  System musi umożliwiać pracę w domenie – wsparcie dla Active Directory |  |
| Wymagania dodatkowe | Wbudowane porty:  1x DP++ 1.4/HDCP 2.3  1x HDMI In 1.4a  1 x HDMI 2.0  1x USB 3.2 Gen 2 Type-C port  2x USB 3.2 Gen 2 Type-A port  3x USB 3.2 Gen 1 Type-A port  Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp.  1x Universal audio jack  1x Line-out audio  1x RJ-45 port 10/100/1000 Mbps  Czytnik kart SD 4.0  Karta WiFi ax+ bluetooth 5.1  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi, przynajmniej jedno złącze z obsługą protokołu SATA III umożliwiające bezpośrednie podłączenie oraz zasilanie dodatkowego dysku 2.5” (bez stosowania kabli zasilających).  Klawiatura USB w układzie polski programisty  Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) |  |
| Warunki gwarancji  Wsparcie techniczne | 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.  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.  Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego przedłużenia tego okresu do 4 lub 5 lat od daty dostawy.  Sposób realizacji usług wsparcia technicznego:  • Telefoniczne zgłaszanie usterek w trybie 24h / dobę, 7 dni w tygodniu (w języku polskim w dni robocze w godz. 8-17).  • Dostęp do bezpłatnego portalu technicznego producenta, który umożliwi zamawianie części zamiennych i/lub wizyt technika serwisowego, mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki.  • Opcjonalna pomoc techniczna za pośrednictwem czat online.  Wsparcie techniczne świadczone przez pracowników producenta urządzeń dla sprzętu i wybranego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym.  Przydzielenie zasobu w postaci kierownika technicznego w przypadku eskalacji problemów serwisowych.  Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki, zdalnego zgłaszania awarii do serwisu i automatycznego zakładania zgłoszeń serwisowych. |  |
| Dodatkowe oprogramowanie | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją 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,  - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi  - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji  - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)  - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml  Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.  W ofercie należy podać nazwę oprogramowania |  |
| **Monitor**  **(7 sztuk)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Rodzaj wyświetlacza | Monitor LCD z podświetleniem LED / matryca aktywna TFT |  |
| Przekątna | Min. 23” |  |
| Współczynnik kształtu | 16:9 |  |
| Rozdzielczość | Full HD (1080p) 1920 x 1080 przy 60 Hz |  |
| Rozstaw pikseli | Max. 0,28 mm |  |
| Jasność | Min. 250 cd/m² |  |
| Współczynnik kontrastu | 1000:1 |  |
| Obsługa kolorów | 16,7 miliony kolorów |  |
| Czas reakcji | 8 ms (szary do szarego) |  |
| Kąt widzenia poziom/pion | 178 |  |
| Powłoka ekranu | Antyrefleksyjna |  |
| Blue Light | Tak |  |
| Złącza | Min. 1xHDMI, 1xVGA |  |
| Regulacja pozycji ekranu | Odchylenie |  |
| Kąt pochylenia | -5/+21 |  |
| VESA | 100 x 100 mm |  |
| Pobór Mocy | Max. 30 wat |  |
| Waga | Max. 4,5 kg |  |
| Gwarancja | Min. 3 lata |  |
| **Oprogramowanie, typ 1**  **(55 sztuk)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Pakiet biurowy Microsoft Office zawierający minimum oprogramowanie | MS Excel, MS Word, MS PowerPoint, MS Outlook, MS OneNote, MS Access, MS Publisher lub oprogramowanie równoważne |  |
| Opis równoważności | 1) pakiet posiada wszystkie funkcjonalności i parametry identyczne z funkcjonalnościami i parametrami wymienionego oprogramowania,  2) producent oprogramowania zapewnia infolinię techniczną w języku polskim czynną w godzinach pracy Urzędu - istnieje możliwość sprawdzenia legalności oprogramowania przez tę infolinię po podaniu klucza produktu.  Zamawiający nie dopuszcza możliwości dostawy wersji niższej niż MS Office 2021 PL (lub wersja najnowsza dla produktu równoważnego do MS Office) wraz z aktualizacjami do wersji najnowszej, zarówno w przypadku pakietu MS Office, jak i produktu równoważnego.  Zamawiający wymaga, aby w przypadku zaoferowania pakietu biurowego innego niż wzorcowy, Wykonawca wykazał i udokumentował spełnienie wszystkich wymaganych cech.  Zamawiający zastrzega sobie prawo zażądania testów poszczególnych funkcjonalności przed wyborem oferty. Dodatkowo, w przypadku dostarczenia oprogramowania równoważnego, wymagana jest jego instalacja i konfiguracja na sprzęcie wg wskazówek Zamawiającego.  • Zainstalowany pakiet biurowy musi spełniać wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.  • Wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi;  • Wymagana dostępna, pełna, polska wersja językowa interfejsu użytkownika, systemu komunikatów i podręcznej kontekstowej pomocy technicznej,  • Wymagane wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013, MS Office 2019, MS Office 2021, bez utraty danych oraz bez konieczności przerabiania dokumentów;  • Oprogramowanie winno posiadać pełną kompatybilność z systemem operacyjnym: Microsoft Windows 11 lub równoważnym, oraz posiadać licencję bezterminową zawierającą indywidualny klucz licencji,  • Oprogramowanie musi być nowe, nieużywane, nieprzypisane |  |
| **Oprogramowanie, typ 2**  **(100 sztuk)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Administracja zdalna | 1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. 8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). 10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. 15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami |  |
| Ochrona stacji roboczych | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. |  |
| Ochrona serwera | 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |  |
| Ochrona urządzeń mobilnych opartych o system Android | 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła |  |
| Ochrona danych - szyfrowanie | 1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server  2008 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. |  |
| **Przełącznik sieciowy, typ 1 (3 sztuki)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Całkowita przepustowość bez blokowania | Min. 70 Gbps |  |
| Zdolność przełączania | Min. 140 Gbps |  |
| Szybkość przekazywania | 104.16 Mpps |  |
| Zużycie prądu przemiennego | Max. 56W |  |
| Metoda zasilania | AC 100-240VAC/50-60Hz, wejście uniwersalne  DC 56 W, 25 do 16 V, ze złączem DC Power Inline 2,5 mm |  |
| Diody LED (Prędkość/Łącze/Aktywność) | Porty danych RJ45  Porty danych SFP+/SFP |  |
| Interfejsy sieciowe | 48 - Porty Ethernet RJ45 10/100/1000 Mb/s  2 - porty Ethernet SFP+ 1/10 Gb/s  2 - porty Ethernet SFP 1 Gb/s |  |
| Interfejs zarządzania | 1 - Port szeregowy RJ45, pasmo wejścia/wyjścia Ethernet |  |
| Montaż w szafie | Tak |  |
| Wymiary | Max. 445 x 45 x 290 mm |  |
| Waga | Max. 4 kg |  |
| Główne funkcje przełączania | • ANSI/TIA-1057: LLDP-Media Endpoint Discovery (MED)  • IEEE 802.1AB: Link Layer Discovery Protocol (LLDP)  • IEEE 802.1D: Spanning Tree Compatibility  • IEEE 802.1S: Multiple Spanning Tree Compatibility  • IEEE 802.1W: Rapid Spanning Tree Compatibility  • IEEE 802.1Q: Virtual LANs with Port-Based VLANs  • IEEE 802.1p: Ethernet Priority with User Provisioning and Mapping  • IEEE 802.1X: Port-Based Authentication with Guest VLAN Support  • IEEE 802.3: 10BASE-T  • IEEE 802.3u: 100BASE-T  • IEEE 802.3ab: 1000BASE-T  • IEEE 802.1ak: Virtual Bridged Local Area Networks - Amendment 07: Multiple Registration Protocol  • IEEE 802.3ac: VLAN Tagging  • IEEE 802.3ad: Link Aggregation  • IEEE 802.3x: Flow Control  • IEEE 802.1D-2004: Generic Attribute Registration Protocol: Clause 12 (GARP)  • IEEE 802.1D-2004: Dynamic L2 multicast registration: Clause 10 (GMRP)  • IEEE 802.1Q-2003: Dynamic VLAN registration: Clause 11.2 (GVRP)  • RFC 4541: Considerations for Internet Group Management Protocol (IGMP) Snooping Switches |  |
| Zaawansowane funkcje warstwy Layer 2 | Odzyskiwanie burzy rozgłoszeniowej  Broadcast / Multicast / Unknown Unicast Storm Recovery  Śledzenie DHCP  Zapytanie IGMP Snooping  Niezależne uczenie się sieci VLAN (IVL)  Obsługa ramek Jumbo Ethernet  Blokowanie portu MAC  Dublowanie portów  Chronione porty  Statyczne filtrowanie adresów MAC  TACACS+  Głosowa sieć VLAN  Nieuwierzytelniona sieć VLAN  Wewnętrzny serwer uwierzytelniania 802.1X |  |
| Pozostałe funkcje | DHCP serwer  • Maksymalna liczba pul: 128  • Maksymalna liczba leasingów (łącznie): 2048  • Wytyczanie  • Liczba tras: 16  • Liczba interfejsów routingu: 15  • Sieci VLAN: 4093  • Adresy MAC: 16 384  • Instancje MSTP: 4  • LGD: 6  • Listy ACL: 100 z 10 regułami na port  • Klasy ruchu (kolejki): 8 |  |
| Właściwości systemowe | • Funkcja rejestrowania zdarzeń i błędów  • Możliwość pobierania czasu pracy i konfiguracji  • Narzędzie PING  • Transfery FTP/TFTP przez IPv4/IPv6  • Wykrywanie złośliwego kodu  • BootP i DHCP  • RFC 2021: Baza informacji zarządzania zdalnym monitorowaniem sieci w wersji 2  • RFC 2030: Prosty protokół czasu sieciowego (SNTP)  • RFC 2819: Zdalna baza informacji zarządzania monitorowaniem sieci  • RFC 2865: klient RADIUS  • RFC 2866: Rachunkowość RADIUS  • RFC 2868: Atrybuty RADIUS dla obsługi protokołu tunelowego  • RFC 2869: rozszerzenia RADIUS  • RFC 3579: obsługa protokołu RADIUS dla protokołu EAP  • RFC 3580: wytyczne dotyczące użytkowania IEEE 802.1X RADIUS  • RFC 3164: protokół Syslog BSD |  |
| Zarządzanie | Interfejs sieciowy  • CLI zgodne ze standardami branżowymi  • Zarządzanie IPv6  • Zarządzanie hasłami  • Obsługa automatycznej instalacji obrazów oprogramowania sprzętowego i plików konfiguracyjnych  • SNMP v1, v2 i v3  • SSH 1,5 i 2,0  • SSL 3.0 i TLS 1.0  • Bezpieczna kopia (SCP)  • Telnet (obsługa wielu sesji) |  |
| Routing w warstwie 3 | • Routing statyczny |  |
| QoS | • Listy kontroli dostępu (ACL), akcje zezwolenia/odmowy dla przychodzącego adresu IP i klasyfikacja ruchu w warstwie 2 na podstawie:  • Lista ACL oparta na czasie  • Źródłowy/docelowy adres IP  • Port źródłowy/docelowy TCP/UDP  • Typ protokołu IP  • Pole typu usługi (ToS) lub usług zróżnicowanych (DSCP)  • Źródłowy/docelowy adres MAC  • Typ eteru  • Priorytet użytkownika IEEE 802.1p  • Identyfikator VLAN  • RFC 1858: względy bezpieczeństwa przy filtrowaniu fragmentów IP  • Opcjonalne atrybuty reguł ACL  • Przypisz przepływ do kolejki określonej klasy usług (CoS)  • Przekieruj pasujące przepływy ruchu  • Zróżnicowane usługi (DiffServ)  • Klasyfikuj ruch na podstawie tych samych kryteriów, co listy ACL  • Zaznacz IP DSCP lub pola nagłówka pierwszeństwa, opcjonalnie  • Kontroluj przepływ w określonym tempie dzięki obsłudze dwóch kolorów  • RFC 2474: definicja pola usług zróżnicowanych (pole DS) w nagłówkach IPv4 i IPv6  • RFC 2475: Architektura dla zróżnicowanych usług  • RFC 2597: Grupa gwarantowanego przekazywania na przeskok (PHB)  • RFC 3246: przyspieszone przekazywanie PHB  • RFC 3260: Nowa terminologia i wyjaśnienia dotyczące DiffServ  • Konfiguracja mapowania kolejki klasy usługi (CoS)  • AutoVoIP: automatyczne ustawienia CoS dla VoIP  • Mapowanie IP DSCP na kolejkę  • Konfigurowalny tryb zaufania interfejsu (IEEE 802.1p, DSCP lub niezaufany)  • Szybkość kształtowania wyjścia interfejsu  • Ścisły priorytet w porównaniu z planowaniem ważonym na kolejkę |  |
| **Przełącznik sieciowy, typ 2 (1 sztuka)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Całkowita przepustowość bez blokowania | Min. 25 Gbps |  |
| Zdolność przełączania | Min. 52 Gbps |  |
| Szybkość przekazywania | Min. 38 Mpps |  |
| Pobór energii | Max. 25W |  |
| Metoda zasilania | AC: 100-240VAC, 50/60 Hz |  |
| Zasilacz | AC/DC, wewnętrzny, 36W |  |
| Interfejsy sieciowe | Min. 24 Porty Ethernet RJ45 10/100/1000 Mb/s  Min. 2 porty SFP 1 Gb/s |  |
| Interfejs zarządzania | Ethernet w paśmie |  |
| Tryby | Przełącznik Gigabit Ethernet warstwy 2 |  |
| Ochrona ESD/EMP | Powietrze: ± 16 kV, Kontakt: ± 12 kV |  |
| Temperatura pracy | -5 do 40°C |  |
| Wilgotność pracy | 10 - 90% bez kondensacji |  |
| Diody LED | System, Ethernet, SFP |  |
| Wymiary | Suma wymiarów nie może przekroczyć 69 cm |  |
| Waga | Max. 2,80 kg |  |
| **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 szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  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 | Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 129 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| RAM | Minimum 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 dwa sloty PCIe x16 generacji 4 |  |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT |  |
| Dyski twarde | Możliwość instalacji dysków SAS, SATA, SSD  Zainstalowane:  3 dyski SSD SATA o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug.  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. |  |
| System operacyjny/dodatkowe oprogramowanie | 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. |  |
| 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 panela 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, typ 3**  **(1 sztuka)** | **Nazwa oferowanego asortymentu spełniającego poniższe wymagania Zamawiającego - należy podać markę oraz model.** |  |
| Wymagania ogólne | ● Oprogramowanie może być dostarczane w dwóch scenariuszach:  ○ Cloud(Software as Service),  ○ On-premise.  ● Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.  ● Interfejs systemu dostępny jest w języku:  ○ polskim,  ○ angielskim,  ● Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,  ● Oprogramowanie może być uruchomione w kontenerze docker,  ● Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:  ○ Debian: 9+  ○ Ubuntu: 16.04+  ○ Fedora: 29+  ○ centOS: 7+  ○ RHEL: 6+  ○ openSUSE: 15+  ○ SUSE Enterprise Linux (SLES): 12 SP2+  ○ Windows Client: 7, 8.1, 10 (1607+)  ○ Windows Server: 2008 R2+,  ● System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,  ● Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju), |  |
| Wsparcie techniczne: | ● Pomoc techniczna w językach:  ○ polskim,  ○ angielskim.  ● Materiały samopomocowe:  ○ Baza wiedzy:  ■ polski,  ■ angielski |  |
| Zarządzanie: | ● Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej,  ● Zarządzanie całym systemem poprzez dashboardy,  ● Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,  ● System posiada wbudowane predefiniowane zadania backupowe,  ● System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.  ● Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,  ● Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,  ● Monitorowanie postępu działania zadania,  ● Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:  ○ Zadanie zostało zakończone pomyślnie,  ○ Zadanie zostało zakończone z ostrzeżeniami,  ○ Zadanie zostało zakończone z błędem,  ○ Zadanie zostało anulowane,  ○ Zadanie nie zostało uruchomione.  ● System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.  ● Możliwość zdefiniowania okna backupowego dla każdego z zadań,  ● Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,  ● System pozwala na klonowanie planów kopii zapasowych,  ● System umożliwia reset hasła administratora w przypadku jego utraty,  ● Oprogramowanie umożliwia definiowanie retencji według schematów:  ○ GFS(Grandfather-Father-Son),  ○ FIFO(First-In, First-Out).  ● Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,  ● Konta użytkowników mogą być tworzone poprzez import pliku CSV,  ● Oprogramowanie umożliwia tworzenie grup urządzeń,  ● Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).  ● System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:  ○ System Administrator,  ○ Backup operator,  ○ Restore operator,  ○ Viewer. |  |
| Składowanie danych: | ● Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,  ● System umożliwia składowanie danych:  ○ Lokalnie:  ■ Zasób SMB,  ■ Zasób NFS,  ■ Zasób ISCSI,  ■ Zasób S3,  ■ Katalog zabezpieczonego urządzenia.  ○ W chmurze:  ■ Amazon Web Service,  ■ Magazyn zgodny z S3,  ■ Dostarczanej przez producenta.  ● System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,  ● System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.  ● System umożliwia replikacje danych między magazynami. |  |
| Odtwarzanie: | ● Odtwarzanie granularne:  ○ Pojedynczych plików z kopii obrazu dysku,  ○ Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,  ● Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:  ○ Windows: 7+,  ○ Windows Server: 2008 R2+,  ● Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.  ● Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive’a,  ● Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.  ● Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),  ● Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),  ● Odtwarzanie zasobów plikowych z prawami dostępu,  ● Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),  ● Odtwarzanie danych według harmonogramu,  ● Przywracanie danych z określonego urządzenia/użytkownika,  ● Przywracanie kopii z wybranego magazynu.  ● Przywracanie danych Microsoft 365:  ○ do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:  ■ pst,  ■ mbox.  ○ do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),  ● System posiada możliwość nieodwracalnego kasowania danych,  ● Przywracanie repozytoriów GIT:  ○ Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket),  ○ przywracanie między kontami. |  |
| Backup | ● Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:  ○ Systemów operacyjnych:  ■ Alpine 3.10+,  ■ Debian: 9+,  ■ Ubuntu: 16.04+,  ■ Fedora: 29+,  ■ centOS: 7+,  ■ RHEL: 6+,  ■ openSUSE: 15+,  ■ SUSE Enterprise Linux(SLES): 12 SP2+,  ■ macOS: 10.13+,  ■ Windows: 7, 8.1, 10(1607+),  ■ Windows Server: 2008 R2+,  ○ Środowisk wirtualnych:  ■ Hyper-V,  ■ VMware: 6.7+.  ○ Repozytoriów GIT:  ■ GitHub,  ■ Bitbucket.  ● Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:  ○ Baz danych:  ■ Microsoft SQL,  ■ MySQL,  ■ PostgreSQL,  ■ Firebird,  ■ Dowolnych innych przez podpięcie skryptów pre/post.  ● Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:  ○ 128 bit,  ○ 192 bit,  ○ 256 bit.  ● Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:  ○ ZStandard,  ○ LZ4.  ● Oprogramowanie umożliwia zarządzanie poziomem kompresji,  ● Wykonywanie kopii zapasowej otwartych plików(VSS),  ● System umożliwia uruchamianie skryptów przed i po backupie,  ● System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,  ● System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,  ● Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,  ● Backup plikowy,  ● Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,  ● Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,  ● Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,  ● Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.  ● Oprogramowanie pozwala na backup zaszyfrowanych partycji. |  |
| GIT | ● Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),  ● Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki). |  |
| Licencjonowanie | ● Sposób licencjonowania opiera się na:  ○ Ilości serwerów/endpointów- dla fizycznych urządzeń,  ○ Ilości fizycznych hostów - dla środowisk wirtualnych,  ○ Ilości repozytoriów - dla GIT.  ● Licencje powinny pozwalać na zabezpieczenie w wersji dożywotniej:  ○ 3 serwerów fizycznych bez wirtualizacji,  ○ 40 stacji roboczych,  ● Wsparcie techniczne:  o Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,  o Zapewnia dostęp do aktualizacji oprogramowania,  o Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,  o Obowiązuje przez okres minimum 12 miesięcy. |  |
| **Urządzenie typu firewall UTM, typ 1**  **(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. 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. |  |
| Funkcje modułu Firewall | 1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).  2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.  3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).  4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.  5. Musi obsługiwać Multicast routing.  6. Musi obsługiwać Policy Based routing.  7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.  8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.  9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.  10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).  11. Musi obsługiwać Dynamic DNS.  12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.  13. Musi obsługiwać translację portów: PAT.  14. Musi obsługiwać IPSec NAT traversal.  15. Musi obsługiwać mechanizm Policy Based NAT.  16. Musi obsługiwać VLAN 802.1Q.  17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.  18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.  19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.  20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.  21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.  22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.  23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.  24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.  25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.  26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.  27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.  28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego  agenta na stacjach roboczych użytkowników.  29. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.  30. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.  31. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.  32. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.  33. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.  34. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.  35. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.  36. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.  37. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.  38. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.  39. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.  40. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site. |  |
| Dostarczony system bezpieczeństwa musi zapewniać | 1. Ochronę z wykorzystaniem mechanizmów IPS.  2. Ochronę antywirusową.  3. Ochronę przed nieznanymi zagrożeniami.  4. Ochronę przed phishingiem.  5. Ochronę przed niechcianą pocztą.  6. Kontrolę wykorzystywanych aplikacji.  7. Możliwość filtrowania URL. |  |
| Parametry fizyczne systemu Firewall / Element systemu pełniący funkcję Firewall musi dysponować | • 8 portami 1Gb RJ45.  • System powinien umożliwiać rozbudowę o dodatkowe porty: 4 x 1Gb SFP lub  2 x 10Gb SFP+ lub 4 x 1Gb RJ45.  • Minimum 4 GB pamięci RAM.  • Minimum 2 porty USB 3.0.  • Minimum jeden port typu Console.  • Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza. |  |
| Parametry wydajnościowe systemu | • Przepustowość Firewall minimum: 5.8 Gbps.  • Przepustowość IPSec VPN nie mniejsza niż: 2.4 Gbps.  • Przepustowość skanowania antywirusowego nie mniejsza niż: 1.4 Gbps.  • Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 1.3 Gbps.  • Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 1.1 Gbps.  • Obsługa nie mniej niż: 75 tuneli IPSec site-to-site.  • Obsługa nie mniej niż: 75 tuneli client-to-site.  • Obsługa nie mniej niż: 3.500.000 jednoczesnych połączeń.  • Obsługa nie mniej niż: 34.000 nowych połączeń na sekundę.  • W ramach Firewall system musi obsługiwać minimum: 100 sieci VLAN |  |
| W ramach ochrony przed atakami system musi zapewniać | 1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 4500 definicji sygnatur.  2. Automatyczne blokowanie znanych źródeł ataków.  3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.  4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).  5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.  6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku. |  |
| W ramach kontroli antywirusowej system musi zapewniać | 1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.  2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.  3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.  4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.  5. Możliwość zdefiniowania rozmiaru skanowanego pliku.  6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.  7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.  8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.  9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS. |  |
| W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać | 1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:  • W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).  • Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.  • Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.  • Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.  • Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.  • Możliwość analizy plików o rozmiarze co najmniej 10MB.  • Brak ograniczeń co do ilości analizowanych plików. |  |
| W ramach ochrony przed phishingiem system musi zapewniać | 1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:  • Możliwość blokowania dostępu do spreparowanych stron.  • Ochronę przed phishingiem nie zależnie od typu połączenia, protokołu, portu.  • Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.  • Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.  • Kontrolę zapytań DNS. |  |
| W ramach kontroli antyspamowej system musi zapewniać | 1. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.  2. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.  3. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.  4. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.  5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail. |  |
| W ramach filtrowania zawartości URL system musi zapewniać | 1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.  2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.  3. Odpytywanie bazy on-line w czasie rzeczywistym.  4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.  5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.  6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.  7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.  8. Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.  9. Możliwość filtrowania treści w oparciu o typy MIME.  10. Możliwość blokowania plików cookies dla określonych domen.  11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.  12. Analizę treści dla protokołu https.  13. Wyłączenie inspekcji https dla wybranych kategorii stron www. |  |
| W ramach kontroli aplikacyjnej system musi zapewniać | 1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.  2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.  3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).  4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.  5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji. |  |
| Wymagane funkcje VPN systemu | 1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.  2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.  3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.  4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.  5. Obsługa Dead Peer Detection (DPD).  6. Wsparcie dla IKEv1 i IKEv2.  7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.  8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).  9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.  10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.  11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.  12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.  13. Dla połączeń Client-to-Site możliwość zastosowania dwuskładnikowego uwierzytelnienia w oparciu o tokeny sprzętowe lub programowe.  14. Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.  15. Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.  16. Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML. |  |
| Zarządzanie | 1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.  2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.  3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.  4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).  5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.  6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.  7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.  8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania. |  |
| Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania | 1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.  2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.  3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online  4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.  5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.  6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.  7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.  8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.  9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.  10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.  11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.  12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.  13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.  14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.  15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.  16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.  17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.  18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.  19. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.  20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.  21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.  22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.  23. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów. |  |
| Licencje i wsparcie techniczne | 1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:  • Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem – na 3 lata.  2. System musi być objęty serwisem gwarancyjnym producenta przez 3 lata, 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 (świadczone telefonicznie lub poprzez portal). |  |
| **Urządzenie typu firewall UTM, typ 2**  **(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. 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. |  |
| Funkcje modułu Firewall | 1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).  2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.  3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).  4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.  5. Musi obsługiwać Multicast routing.  6. Musi obsługiwać Policy Based routing.  7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.  8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.  9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.  10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).  11. Musi obsługiwać Dynamic DNS.  12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.  13. Musi obsługiwać translację portów: PAT.  14. Musi obsługiwać IPSec NAT traversal.  15. Musi obsługiwać mechanizm Policy Based NAT.  16. Musi obsługiwać VLAN 802.1Q.  17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.  18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.  19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.  20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.  21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.  22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.  23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.  24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.  25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.  26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.  27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.  28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego  agenta na stacjach roboczych użytkowników.  29. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.  30. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.  31. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.  32. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.  33. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.  34. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.  35. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.  36. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.  37. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.  38. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.  39. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.  40. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site. |  |
| Dostarczony system bezpieczeństwa musi zapewniać | 1. Ochronę z wykorzystaniem mechanizmów IPS.  2. Ochronę antywirusową.  3. Ochronę przed nieznanymi zagrożeniami.  4. Ochronę przed phishingiem.  5. Ochronę przed niechcianą pocztą.  6. Kontrolę wykorzystywanych aplikacji.  7. Możliwość filtrowania URL. |  |
| Parametry fizyczne systemu Firewall /  Element systemu pełniący funkcję Firewall musi dysponować | • 5 portami 1Gb RJ45.  • Minimum 4 GB pamięci RAM.  • Minimum 2 porty USB 3.0.  • Minimum jeden port typu Console.  • Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza. |  |
| Parametry wydajnościowe systemu | • Przepustowość Firewall minimum: 3.4 Gbps.  • Przepustowość IPSec VPN nie mniejsza niż: 880 Mbps.  • Przepustowość skanowania antywirusowego nie mniejsza niż: 623 Mbps.  • Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 510 Mbps.  • Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 300 Mbps.  • Obsługa nie mniej niż: 30 tuneli IPSec site-to-site.  • Obsługa nie mniej niż: 30 tuneli client-to-site.  • Obsługa nie mniej niż: 500.000 jednoczesnych połączeń.  • Obsługa nie mniej niż: 18.000 nowych połączeń na sekundę.  • W ramach Firewall system musi obsługiwać minimum: 50 sieci VLAN. |  |
| W ramach ochrony przed atakami system musi zapewniać | 1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 4500 definicji sygnatur.  2. Automatyczne blokowanie znanych źródeł ataków.  3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.  4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).  5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.  6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku. |  |
| W ramach kontroli antywirusowej system musi zapewniać | 1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.  2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.  3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.  4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.  5. Możliwość zdefiniowania rozmiaru skanowanego pliku.  6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.  7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.  8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.  9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS. |  |
| W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać | 1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:  • W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).  • Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.  • Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.  • Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.  • Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.  • Możliwość analizy plików o rozmiarze co najmniej 10MB.  • Brak ograniczeń co do ilości analizowanych plików. |  |
| W ramach ochrony przed phishingiem system musi zapewniać | 1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:  • Możliwość blokowania dostępu do spreparowanych stron.  • Ochronę przed phishingiem nie zależnie od typu połączenia, protokołu, portu.  • Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.  • Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.  • Kontrolę zapytań DNS. |  |
| W ramach kontroli antyspamowej system musi zapewniać | 1. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.  2. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.  3. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.  4. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.  5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail. |  |
| W ramach filtrowania zawartości URL system musi zapewniać | 1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.  2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.  3. Odpytywanie bazy on-line w czasie rzeczywistym.  4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.  5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.  6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.  7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.  8. Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.  9. Możliwość filtrowania treści w oparciu o typy MIME.  10. Możliwość blokowania plików cookies dla określonych domen.  11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.  12. Analizę treści dla protokołu https.  13. Wyłączenie inspekcji https dla wybranych kategorii stron www. |  |
| W ramach kontroli aplikacyjnej system musi zapewniać | 1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.  2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.  3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).  4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.  5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji. |  |
| Wymagane funkcje VPN systemu | 1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.  2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.  3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.  4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.  5. Obsługa Dead Peer Detection (DPD).  6. Wsparcie dla IKEv1 i IKEv2.  7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.  8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).  9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.  10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.  11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.  12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.  13. Dla połączeń Client-to-Site możliwość zastosowania dwuskładnikowego uwierzytelnienia w oparciu o tokeny sprzętowe lub programowe.  14. Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.  15. Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.  16. Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML. |  |
| Zarządzanie | 1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.  2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.  3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.  4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).  5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.  6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.  7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.  8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania. |  |
| Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania | 1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.  2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.  3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online  4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.  5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.  6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.  7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.  8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.  9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.  10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.  11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.  12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.  13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.  14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.  15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.  16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.  17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.  18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.  19. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.  20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.  21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.  22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.  23. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów. |  |
| Licencje i wsparcie techniczne | 1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:  • Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem – na 3 lata.  2. System musi być objęty serwisem gwarancyjnym producenta przez 3 lata, 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 (świadczone telefonicznie lub poprzez portal). |  |