Fundusze Europejskie Polska Cyfrowa

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia

sierpień 2022

Spis treści

1 Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- Sprzęt i oprogramowanie musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- Sprzęt musi być nowy nie używany wcześniej (wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą);

2 Wymagania gwarancyjne.

Sprzęt

- Na dostarczony sprzęt wymagana jest min. roczna gwarancja (chyba, że zapisy szczegółowe stanowią inaczej)
- Na dostarczony sprzęt wymagana jest gwarancji producenta
- Serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego (chyba, że zapisy szczegółowe stanowią inaczej);
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań;

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

3 Zestawienie zakresu dostaw.

Lp.	Nazwa	Długość gwarancji, wsparcie producenta , długość licencji (minimum) [m-ce]	Ilość	Uwagi
1.	Serwery do uruchomienia maszyn wirtualnych wraz z systemem operacyjnym	- Gwarancja 36(**kryterium oceny**) - Licencja na system operacyjny dożywotnia	2szt	Serwer do wirtualizacji (kontroler domeny, serwer plików, serwer DNS, serwer DHCP, itp.) system operacyjny.
2.	Licencja na dodatkowy system operacyjny	- Licencja na system operacyjny dożywotni	1szt	Licencja na dodatkowy system operacyjny umożliwiająca uruchomienie dodatkowych maszyn wirtualnych
3.	Licencje dostępowe CAL	- dożywotnia	55szt	Licencje klienckie w opcji na użytkownika umożliwiające korzystanie z usług udostępnionych przez serwery
4.	Switch zarządzany 24 port	- Licencja na wsparcie techniczne producenta 12	1szt	Switch zarządzany, 24 portowy
5.	Switch zarządzany 48 port	- Licencja na wsparcie techniczne producenta 12	3szt	Switch zarządzany, 48 portowy
6.	Oprogramowanie do backupu wraz z licencją	- Licencja na oprogramowanie dożywotnia	1szt	Licencja wraz z oprogramowaniem do tworzenia kopii zapasowych (backupów)
7.	Stacje robocze	- Gwarancja 24 (**kryterium oceny**)	10szt	Komputery stacjonarne do pracy biurowej, z zainstalowanym systemem operacyjnym, oraz oprogramowaniem biurowym.

		- Licencja na system operacyjny dożywotnia		
8.	Laptopy	- Gwarancja 24 (**kryterium oceny**) - Licencja na system operacyjny dożywotnia	11szt	Komputery przenośne do pracy biurowej, z zainstalowanym system operacyjny, oraz oprogramowaniem biurowym
9.	Laptop	- Gwarancja 24 (**kryterium oceny**) - Licencja na system operacyjny dożywotnia	1szt	Komputer przenośny o podwyższonych parametrach do uruchomienia wirtualnego środowiska do przeprowadzania testów (wydajnościowych, bezpieczeństwa), testów penetracyjnych środowiska produkcyjnego, oraz pracy biurowej, z zainstalowanym system operacyjnym, i oprogramowaniem biurowym
10.	Licencje dostępowe RDS	- dożywotnia	5szt	Licencje umożliwiające dostęp do serwera terminali, wykorzystywane do uzyskania dostępu do pulpitu zdalnego (usługa Remote Desktop Services)
11.	Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS)	- Licencja na wsparcie techniczne producenta 12	1szt	Zakup urządzenia UTM.
12.	Zakup specjalistycznego oprogramowania typu EDR	- Licencja na oprogramowanie 12	1szt	Zakup oprogramowania klasy EDR

3.1 Serwery do uruchomienia maszyn wirtualnych - 2szt – wymagania minimalne

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Serwery służące jako hosty do wirtualizacji. Maszyny wirtualne będą świadczyły usługi między innymi: Kontrolera domeny (Active directory), serwera baz danych (MS SQL, Firebird, sybase, postegreSQL), serwera certyfikatów dla domeny, serwera DHCP, serwera plików, serwera terminali, serwera systemu obiegu dokumentów, serwera backupu, serwera aplikacji (z serwerem IIS) , serwera logów, serwera wydruków W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta jak również dostarczenie karty katalogowej umożliwiającej sprawdzenie parametrów technicznych dostarczanego urządzenia
2.	Obudowa	Obudowa Rack o wysokości 1U z możliwością instalacji min 8 dysków 2.5" HotPlug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack. Możliwość zamontowania przedniego panelu z wyświetlaczem zamykanym na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
3.	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
4.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
5.	Procesor	Dwa procesory do zastosowań w serwerach posiadające minimum 8 fizycznych rdzeni z technologią HT o taktowaniu podstawowym wynoszącym min. 2.8GHz i 12MB pamięci podręcznej. Osiągający wynik min w teście 19010 pkt w teście CPU Benchmark dostępnym na stornie https://www.cpubenchmark.net/high_end_cpus.html
6.	Pamięć RAM	96 GB pamięci RAM typu RDIMM o częstotliwości pracy 3200MHz, możliwość rozbudowy do minimum 1024GB pamięci RAM, na płycie powinno się znajdować minimum 16 wolnych slotów przeznaczonych na pamięć Zabezpieczenia pamięci: Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
7.	Sloty PCI Express	Min. jeden slot PCIe gen4 umożliwiający instalację karty niskoprofilowej.
8.	Karta graficzna	Zintegrowana karta graficzna umożliwiająca pracę w rozdzielczości min. 1920x1200.
9.	Wbudowane porty	min. trzy porty USB z czego min 2 porty 3.0 , 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), 1 port OCP 3.0
10.	Kontroler dysków	Sprzętowy kontroler dyskowy z mini. 4GB cache, umożliwiający obsługę dysków z prędkościami transferu 6, 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID o poziomach min. 0, 1, 10 Dodatkowa karta HBA SAS 12G z portami zewnętrznymi
11.	Pamięć masowa	Możliwość instalacji wewnętrznej pamięci masowej typu SATA, NearLine SAS, SAS, SSD oraz SED dostępnych w ofercie producenta serwera. Zainstalowane min. 2 dyski HDD o pojemności 2400GB SAS 12Gb/s 10k Możliwość instalacji dodatkowej wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości minimalnej ilości wewnętrznej pamięci masowej w serwerze.
12.	Zasilanie	Dwa redundantne zasilacze hot plug o mocy min. 800W każdy
13.	Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM 2.0 v3. Wbudowany czujnik otwarcia obudowy

		współpracujący z BIOS i kartą zarządzającą
14.	Karta zarządzająca	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność: • 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, uwierzytelnianie dwuskładnikowe; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do ekranu, 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 minimum 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
15.	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
16.	Gwarancja	Minimum 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta 24h/7 Diagnostyka wykonywana przez autoryzowanego serwisanta, w miejscu instalacji sprzętu. Możliwość przedłużenia gwarancji do minimum 7lat. 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 sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji.
17.	System operacyjny	Licencja na system operacyjny Microsoft Windows Server 2022 Standard lub system operacyjny Microsoft Windows Server wydanie umożliwiające darmowy upgrade do najnowszego wydania systemu operacyjnego Microsoft Windows Server dostępnego na rynku lub równoważny system operacyjny. Opis równoważności systemu znajduje się w pkt.4.3 (SOPZ).

3.2 Licencja na dodatkowy system operacyjny

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Licencja na dodatkowy system operacyjny będzie służyć do uruchomienia dodatkowych maszyn wirtualnych na dostarczonych serwerach. System operacyjny dostarczony w ramach licencji musi być zgodny z dostarczonym systemem wraz z serwerami
2.	System operacyjny	Licencja na system operacyjny Microsoft Windows Server 2022 Standard lub system operacyjny Microsoft Windows Server wydanie umożliwiające darmowy upgrade do najnowszego wydania systemu operacyjnego Microsoft Windows Server dostępnego na rynku lub równoważny system operacyjny. Opis równoważności systemu znajduje się w pkt.4.3 (SOPZ).

3.3 Licencje dostępowe CAL – 55szt

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Licencje umożliwiające korzystanie przez użytkowników z usług oprogramowania zainstalowane na dostarczonych serwerach
2.	Wymagania niezbędne	1. Wersja licencji musi być odpowiednia dla zainstalowanego systemu na dostarczonych serwerach. 2. Wymagane jest aby licencjonowanie odbywało się w opcji na użytkownika

3.4 Switch zarządzany 24 port – 1szt – wymagania minimalne

Lp.		
1.	Wymagania ogólne	W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest aby dostarczony switch współpracował z dostarczonymi urządzeniem w ramach rozbudowy zabezpieczeń logicznych (firewall, systemy IDS, IPS) w minimalnym zakresie podanym w pkt. 7 Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania W ofercie wymagane jest podanie modelu, symbolu oraz producenta jak również dostarczenie karty katalogowej umożliwiającej sprawdzenie parametrów technicznych dostarczanego urządzenia
2.	Parametry fizyczne platformy	1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Maksymalny pobór mocy: 30W.
3.	Interfejsy, Dysk, Zasilanie Interfejsy sieciowe - wymagania minimalne	1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: • 24 porty GE RJ-45. • 4 porty 10 GE, SFP+.
4.	Zarządzanie	1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. 2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 3. Wsparcie dla SNMP w wersjach 1-3 4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 9. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 10. Automatycznie wykonywane rewizje konfiguracji.
5.	Parametry wydajnościowe	1. Przepustowość urządzenia - min. 15 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 32 k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6.	Wymagane funkcje	1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames. 3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Agregacja portów zgodna ze standardem 802.3ad. 5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. 6. Obsługa routingu statycznego.

		7. Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP. 8. Port-mirroring. 9. Uwierzytelnianie 802.1x na poziomie portu. 10. Uwierzytelnianie 802.1x w oparciu o adres MAC. 11. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). 12. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 13. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. 14. Obsługa protokołu sFlow.
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing
9.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. 2. Wykonawca musi zapewnić przez okres trwania licencji pełne wsparcie techniczne realizowane przez etatowego pracownika posiadającego autoryzowany certyfikat producenta, potwierdzający doświadczenie i umiejętność obsługi dostarczonego

		rozwiązania (certyfikat delegowanego pracownika należy załączyć do oferty), wsparcie techniczne ma być świadczone poprzez telefon, email i dedykowany system HelpDesk (należy podać adres strony WWW 3. Wykonawca będzie zobligowany do przeprowadzenia audytu konfiguracji urządzenia UTM wg. zakresu: • aktualizacja oprogramowania do najnowszej wersji • weryfikacja i ew. poprawa polityk bezpieczeństwa • podniesienie poziomu bezpieczeństwa (dodatkowa konfiguracja polityk w oparciu o profile UTM) • testy poprawności działania urządzenia

3.5 Switch zarządzany 48 port – 3szt – wymagania minimalne

Lp.		
1.	Wymagania ogólne	W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest aby dostarczony switch współpracował z dostarczonymi urządzeniem w ramach rozbudowy zabezpieczeń logicznych (firewall, systemy IDS, IPS) w minimalnym zakresie podanym w pkt. 7 Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania W ofercie wymagane jest podanie modelu, symbolu oraz producenta jak również dostarczenie karty katalogowej umożliwiającej sprawdzenie parametrów technicznych dostarczanego urządzenia
2.	Parametry fizyczne platformy	1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Maksymalny pobór mocy: 20W.
3.	Interfejsy, Dysk, Zasilanie Interfejsy sieciowe - wymagania minimalne	1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: • 48 porty GE RJ-45. • 4 porty GE, SFP+.
4.	Zarządzanie	1. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 2. Wsparcie dla SNMP w wersjach 1-3 3. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 4. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 5. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 6. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 7. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 8. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 9. Automatycznie wykonywane rewizje konfiguracji.
5.	Parametry wydajnościowe	1. Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 32k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6.	Wymagane funkcje	1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames. 3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Agregacja portów zgodna ze standardem 802.3ad. 5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. 6. Port-mirroring. 7. Uwierzytelnianie 802.1x na poziomie portu.

		8. Uwierzytelnianie 802.1x w oparciu o adres MAC. 9. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). 10. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 11. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. 12. Obsługa protokołu sFlow.
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
9.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. 2. Wykonawca musi zapewnić przez okres trwania licencji pełne wsparcie techniczne realizowane przez etatowego pracownika posiadającego autoryzowany certyfikat producenta, potwierdzający doświadczenie i umiejętność obsługi dostarczonego rozwiązania (certyfikat delegowanego pracownika należy załączyć do oferty), wsparcie techniczne ma być świadczone poprzez telefon, email i dedykowany system HelpDesk

		(należy podać adres strony WWW). 3. Wykonawca będzie zobligowany do przeprowadzenia audytu konfiguracji urządzenia UTM wg. zakresu: • aktualizacja oprogramowania do najnowszej wersji • weryfikacja i ew. poprawa polityk bezpieczeństwa • podniesienie poziomu bezpieczeństwa (dodatkowa konfiguracja polityk w oparciu o profile UTM) • testy poprawności działania urządzenia

3.6 Oprogramowanie do backupu wraz z licencją -1szt – minimalne wymagania

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Oprogramowanie do tworzenia kopi bezpieczeństwa, wirtualnych maszyn, dysków i plików. W ofercie wymagane jest podanie nazwy oprogramowania oraz producenta jak również Dostarczona licencja powinna umożliwiać wykonywanie kopi bezpieczeństwa minimum dwóch maszyn fizycznych oraz 13 maszyn wirtualnych W ofercie wymagane jest podanie nazwy oprogramowania oraz producenta jak również dostarczenie karty katalogowej dostarczanego oprogramowania umożliwiającej sprawdzenie funkcjonalności oprogramowania
2.	Wymagania minimalne	1. Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji • Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012 • Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012, 2008R2 • Microsoft 365 (Exchange online, One Drive for Business, Sharepoint) 2. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk MS Hyper-V 3. Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia: • na serwerze Windows lub Linux • jako maszyna wirtualna 4. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS 5. Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania 6. Oprogramowanie musi wspierać natywną obsługę taśm dla zautomatyzowanych bibliotek taśmowych, w tym wirtualnych bibliotek taśmowych (VTL), a także autonomicznych napędów taśmowych. 7. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
3.	Licencjonowanie	1. Wszystkie funkcje i komponenty oprogramowania dla środowisk wirtualizacji powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności 2. Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska 3. W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania 4. W ramach dostawy wymagane jest dostarczenie licencji na ochronę minimum 4 gniazd procesorów w hostach Hyper-V 5. Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
4.	Ochrona danych	1. Oprogramowanie musi posiadać funkcje backupu i replikacji: • Backup maszyn wirtualnych Vmware • Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu • Backup maszyn wirtualnych Hyper-V

		• Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu • Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych • Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie • Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu • Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym • Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych • Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem • Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania • Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji • Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami.
5.	Optymalizacja wykorzystania miejsca na dane	1. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych: • Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane • Kompresja backupu, w tym konfigurowalny stopień kompresji • Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
6.	Spójność danych	1. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych: • Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux • Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu • Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: - Microsoft SQL 2008, 2008R2, 2012, 2014, 2016, 2017, 2019 • Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska witrualnego poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki • Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych minimum Hyper-V • Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania • Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
7.	Przywracanie danych	1. Oprogramowanie musi posiadać poniższe funkcje: • Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub

		innego serwera wirtualizacji • Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku wirtualnym (bez wcześniejszego przywracania maszyny wirtualnej) • Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej) • Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): - Active Directory - MS SQL
8.	Wydajność	1. Oprogramowanie do backupu musi pozwalać na: • Tworzenie backupu I replik przyrostowo przy wykorzystaniu minimum Hyper-V RCT • Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych • Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN • Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
9.	Zarządzanie	1. Oprogramowanie musi pozwalać na następujące formy zarządzania: • Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych • Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej • Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania • Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport. • Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji • Oprogramowanie musi umożliwiać integrację z Active Directory • Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania

Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

3.7 Stacje robocze – szt.10– wymagania minimalne

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Komputer przeznaczone do pracy biurowej, tworzenia i przeglądania dokumentów, pracy z arkuszami kalkulacyjnymi, tworzenia prezentacji multimedialnych, korzystania z internetu, korzystania z poczty elektronicznej, oraz aplikacji wykorzystywanych w codziennej pracy. W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta jak również dostarczenie karty katalogowej umożliwiającej sprawdzenie parametrów technicznych dostarczanego urządzenia
2.	Obudowa	Typu SFF z obsługą kart PCI Express o niskim profilu: - 1 x PCI Express x16, - 1 x PCI Express x1, Wyposażona w min: - 1 szt. 5,25” (dopuszcza się zastosowanie jednej kieszeni 5,25” w wersji SLIM dla napędu optycznego) - 1 szt. 3,5” + 1 szt. 2,5’’ lub 2 szt. 2,5” Obudowa musi być wyposażona w czujnik otwarcia. Wbudowany głośnik o mocy 1W
3.	Chipset	Dostosowany do zaoferowanego procesora
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 2 złącza M.2 z czego 1 dedykowane dla dysku SSD PCIe.
5.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi AMD Ryzen 5 Pro 4650G na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu
6.	Pamięć operacyjna	Min. 8GB GB, 3200MHz DDR4, 4 sloty na pamięć, z czego min. 3 wolne. Możliwość pracy pamięci w trybie dual channel. Możliwość rozbudowy pamięci do minimum 128GB RAM.
7.	Dysk twardy	Min 256GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
8.	Napęd optyczny	Nagrywarka DVD +/-RW
9.	Karta graficzna	Zintegrowana karta graficzna z procesorem
10.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition
11.	Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000 wspierająca WoL
12.	Porty/złącza	Wbudowane porty: - 1 x HDMI, - 2 x DP, - 8 x USB-A w tym min.: 4x USB 3.2 z przodu obudowy - 1 x USB-C z przodu obudowy - port sieciowy RJ-45, - port szeregowy RS-232 - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy - czytnik kart pamięci

		Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp
13.	Klawiatura/mysz	Klawiatura w układzie US + mysz optyczna z rolką
14.	Zasilacz	Energooszczędny zasilacz
15.	System operacyjny	Licencja na system operacyjny Microsoft Windows 11 Professional X64 PL lub system operacyjny Microsoft Windows w wersji Professional x64 PL wydanie umożliwiające darmowy upgrade do najnowszego wydania systemu operacyjnego Microsoft Windows Professional x64 PL dostępnego na rynku lub równoważny system operacyjny. Opis równoważności znajduje się w pkt.4.1 (SOPZ).
16.	Zintegrowany system diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor: Nazwa, taktowanie • Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
17.	Certyfikaty i standardy	- Energy Star min. 8.0 - Certyfikat TCO - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
18.	Waga/rozmiary urządzenia	Dwa wymiary nie większe niż 10 cm i 30 cm
19.	Bezpieczeństwo	- Złącze typu Kensington Lock - Oczko na kłódkę - Moduł TPM 2.0 z certyfikacją TCG
20.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
21.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą

		sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
22.	Gwarancja	3 lata świadczona w miejscu użytkowania sprzętu (on-site) Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
23.	Wsparcie techniczne producenta	- - możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
24.	Oprogramowanie biurowe	Licencja wieczysta na oprogramowanie biurowe Microsoft Office 2021 Home&Business PL 32/64 lub oprogramowanie Microsoft Office, wersja minimum z aplikacjami Word, Excel, PowerPoint, Outlook, wydanie umożliwiające bezpłatny upgrade do najnowszego wydania Microsoft Office dostępnego na rynku w wersji do zastosowania w biznesie lub równoważne. Opis równoważności znajduje się w pkt.4.2 (SOPZ).
25.	Monitor	1. Przekątna ekranu 23,3” 2. Matryca typu IPS/PLS/MVA/WVA o wykończeniu matowym (nie dopuszcza się naklejek matowiących matrycę) 3. Rozdzielczość nie mniejsza niż: FHD (1920x1080), Piksel nie większy niż – 0.28 mm 4. Kąty widzenia min. 170 stopni w pionie i min. 170 stopni w poziomie 5. Nie mniejszy niż 72% (CIE 1931 lub równoważny) 6. Kontrast nie mniejszy niż: 1000:1, Jasność nie mniejsza niż 250 cd/m2 7. Minimalna ilość dostępnych złącz monitora: • 1x DP • 1x HDMI • 1x VGA 8. Do monitora producent dołącza minimum kable: • HDMI • Kabel zasilający 9. Stopa podstawa monitora musi umożliwiać • obrót w poziomie min. 90 stopni (-360 / 360) • przechylenie w pionie min. 27 stopni (-5 / 22) • regulacja wysokości o wartości min. 155 mm • Obrót (Pivot) 90 stopni 10. Obudowa musi: • Umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) • Umożliwiać zainstalowanie monitora na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100) • Posiadać wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora • Wbudowane w obudowie głośniki stereo min 2 x 1,5W

		• Wbudowany zasilacz w obudowie 11. Certyfikaty i standardy • Certyfikat EPEAT na poziomie co najmniej Silver. • TCO 8.0 lub wyższy • TCO Edge 2.0 lub wyższy • Energy Star • TÜV Eye Comfort 12. Gwarancja minimum 3 lata 13. Wsparcie techniczne producenta • Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. • możliwość weryfikacji na stronie producenta modelu monitora • możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji • możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego

3.8 Laptopy – 11szt – wymagania minimalne

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Laptop przeznaczone do pracy biurowej, tworzenia i przeglądania dokumentów, pracy z arkuszami kalkulacyjnymi, tworzenia prezentacji multimedialnych, korzystania z internetu, korzystania z poczty elektronicznej, oraz aplikacji wykorzystywanych do codziennej. W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta jak również dostarczenie karty katalogowej umożliwiającej sprawdzenie parametrów technicznych dostarczanego urządzenia
2.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core i5-1235U na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/.
3.	Pamięć RAM	Min. 8 GB 3200 MHz non-ECC. Jeden slot wolny na dalszą rozbudowę. Możliwość rozbudowy pamięci do min. 40GB
4.	Pamięć masowa	Min 256GB M.2 PCIe NVMe, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii
5.	Zintegrowana karta graficzna	Zintegrowana z procesorem
6.	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
7.	Obudowa	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H.
8.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.
9.	Bezpieczeństwo	TPM 2.0 Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington
10.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
11.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości - informacja o licencji systemu operacyjnego, która została zaimplementowana w

		BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość ustawienia hasła Administratora - Możliwość ustawienia hasła Użytkownika - Możliwość ustawienia hasła dysku twardego - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth
12.	Ekran	Matowy, matryca TFT 15” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 300nits, kontrast 800:1 w technologii IPS/PLS/WVA Kąt otwarcia pokrywy ekranu min.180 stopni.
13.	Interfejsy komunikacyjne	4xUSB 3.2 z czego minimum 2 złącza Typu-C umożliwiające podłączenie stacji dokującej lub zasilania notebooka i dodatkowego ekranu (niezależnie od wybranego portu USB-C). Złącze słuchawek i złącze mikrofonu typu COMBO, HDMI 2.0, RJ-45. Komputer musi obsługiwać komunikację Thunderbolt 4 za pomocą min. 1 złącza USB-C. Czytnik kart pamięci.
14.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2 Bluetooth 5.1
15.	Klawiatura	Klawiatura odporna na zalanie cieczą, z wydzieloną klawiaturą numeryczną, układ US, klawiatura wyposażona w podświetlenie przycisków.
16.	Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych
17.	Akumulator	Pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – załączyć test Mobile Mark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w nie dłuższym czasie niż 30 minut od 0% do 50%.
18.	Zasilacz	Zasilacz zewnętrzny
19.	Certyfikaty oświadczenia i standardy	Komputer spełniający: - ENERGY STAR 8.0 - EPEAT na poziomie Gold - Mil-STD-810H - Ochronę oczu TÜV Low Blue Light - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
20.	Wymiary i waga	Waga urządzenia z akumulatorem nie większa niż 1,7 kg Grubość notebooka nie większa niż: 19 mm
21.	System operacyjny	Licencja na system operacyjny Microsoft Windows 11 Professional X64 PL lub system operacyjny Microsoft Windows w wersji Professional x64 PL wydanie umożliwiające darmowy upgrade do najnowszego wydania systemu operacyjnego Microsoft Windows Professional x64 PL dostępnego na rynku lub równoważny system operacyjny. Opis równoważności systemu znajduje się w pkt.4.1 (SOPZ).

		Klucz instalacyjny systemu operacyjnego powinien być fabrycznie zapisany w BIOS komputera i wykorzystywany do instalacji tego systemu oraz jego aktywowania. System operacyjny ma być fabrycznie zainstalowany przez producenta.
22.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
23.	Gwarancja	3 lata świadczona w miejscu użytkowania sprzętu (on-site) Firma serwisująca musi posiadać ISO 9001 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.
24.	Wsparcie techniczne producenta	- Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera - Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. - Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera - Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie w godzinach minimum od 9:00- do 18:00 Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.
25.	Oprogramowanie biurowe	Licencja wieczysta na oprogramowanie biurowe Microsoft Office 2021 Home&Business PL 32/64 lub oprogramowanie Microsoft Office, wersja minimum z aplikacjami Word, Excel, PowerPoint, Outlook, wydanie umożliwiające bezpłatny upgrade do najnowszego wydania Microsoft Office dostępnego na rynku w wersji do zastosowania w biznesie lub równoważne. Opis równoważności znajduje się w pkt.4.2 (SOPZ).

3.9 Laptop – 1szt – wymagania minimalne

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Laptop przeznaczony do stworzenia testowego środowiska wirtualnego przeznaczonego do testów zabezpieczeń, testów penetracyjnych z wykorzystaniem maszyn wirtualnych, oraz do pracy biurowej, tworzenia i przeglądania dokumentów, pracy z arkuszami kalkulacyjnymi, tworzenia prezentacji multimedialnych, korzystania z internetu, korzystania z poczty elektronicznej, a także jako stacja programistyczna oraz do uruchamiania aplikacji wykorzystywanych w codziennej pracy. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. W ofercie wymagane jest podanie modelu, symbolu oraz producenta jak również dostarczenie karty katalogowej umożliwiającej sprawdzenie parametrów technicznych dostarczanego urządzenia
2.	Ekran	Matryca 14" z podświetleniem w technologii LED, obsługująca minimum 10-cio punktowy dotyk z gestami - matryca o parametrach: WUXGA 1920x1200, 500nits, IPS z powłoką antyrefleksyjną, z dodatkowo wbudowanym filtrem prywatności (nie dopuszcza się zewnętrznych nakładek). Kąt otwarcia matrycy 360 stopni.
3.	Obudowa	Obudowa komputera wykonana z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzująca się wzmocnioną konstrukcją, tzw „businessrugged",według normy Mil-Std-810H. Obudowa wyposażona jest w: - zasilany slot dokujący dla rysika, który bez wykorzystania zewnętrznych portów USB umożliwia ładowanie rysika.
4.	Chipset	Dostosowany do zaoferowanego procesora
5.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera
6.	Procesor	Procesor klasy x86, zaprojektowany w komputerach przenośnych o wysokiej wydajności, Intel i7-1260P lub równoważny na poziomie wydajności liczonej w punktach na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
7.	Pamięć operacyjna	Min 16GB, rodzaj pamięci LPDDR5-5200 działająca w trybie 8-channel
8.	Dysk twardy	Min 512GB, M.2 SSD PCIe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Wspierający sprzętowe szyfrowanie dysku.
9.	Karta graficzna	Zintegrowana karta graficzna
10.	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x2W, wbudowane cztery mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera IR FHD 1080p
11.	Komunikacja	Komputer wyposażony w technologię NFC (Near Field Communication)
12.	Porty/Złącza	2xUSB 3.2 oraz 2xThunderbolt 4, złącze słuchawek i złącze mikrofonu typu COMBO, HDMI 2.0. Jeden z portów USB 3.2 musi działać w trybie Always-ON. Złącze umożliwiające podpięcie linki antykradzieżowej.
13.	Rysik	Rysik rozpoznający min. 4000 poziomów nacisku

14.	Klawiatura	Klawiatura odporna na zalanie cieczą (funkcjonalność potwierdzona w ulotce katalogowej produktu), układ US, z wbudowanym joystikiem do obsługi wskaźnika myszy, klawiatura wyposażona w podświetlanie przycisków
15.	Karta WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2
16.	Karta sieciowa WWAN	Modem LTE, zintegrowany w obudowie komputera i niewystający po za jej obrys. Dedykowany slot w notebooku umożliwiający instalację karty np. nanoSIM operatora.
17.	Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych
18.	Bluetooth	Wbudowany moduł Bluetooth 5.2
19.	Napęd optyczny	Możliwość podłączenia napędu optycznego przez port USB
20.	Bateria	Notebook wyposażony w jedną baterię min. 57Wh
21.	Zasilacz	Zasilacz zewnętrzny wspierający szybkie ładowanie notebooka – do minimum 80% w ciągu 1 godziny.
22.	System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test matrycy LCD • test magistrali PCI-e • test portów USB • test CPU Wizualna sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • Notebook: Producent, PN, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie, obsługiwane instrukcje, ilości pamięci L1, L2, L3 • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, prędkość obrotowa, temperatura pracy • LCD: producent, model, rozmiar, rozdzielczość, System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
23.	BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS wraz z datą, - nr seryjnym komputera - ilości pamięciami RAM - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej - unikalnych nr inwentażowych tzw. Asset Tag'ów

		- nr seryjnym płyty głównej komputera Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość autentykacji użytkownika w BIOS z wykorzystaniem czytnika linii papilarnych - Możliwość ustawienia hasła dla twardego dysku - Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password - Możliwość ustawienia minimalnych wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego. - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU - Możliwość ustawienia kolejności bootowania - Możliwość Wyłączania/Włączania: karty sieciowej, czytnika linii papilarnych mikrofonu, zintegrowanej kamery, portów USB, bluetooth, NFC, modemu LTE
24.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji
25.	Certyfikaty i standardy	- ENERGY STAR 8.0 - EPEAT Gold - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
26.	Waga/Wymiar	Waga urządzenia z baterią podstawową max 1.4kg, grubość notebooka poniżej 16mm
27.	Szyfrowanie	Zintegrowany z płytą główną 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 zapisanego w TPM2.0. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej
28.	System operacyjny	Licencja na system operacyjny Microsoft Windows 11 Professional X64 PL lub system operacyjny Microsoft Windows w wersji Professional x64 PL wydanie umożliwiające darmowy upgrade do najnowszego wydania systemu operacyjnego Microsoft Windows Professional x64 PL dostępnego na rynku lub równoważny system operacyjny. Opis równoważności systemu znajduje się w pkt.4.1 (SOPZ).
29.	Oprogramowanie biurowe	Licencja wieczysta na oprogramowanie biurowe Microsoft Office 2021 Home&Business PL 32/64 lub oprogramowanie Microsoft Office, wersja minimum z aplikacjami Word, Excel, PowerPoint, Outlook, wydanie umożliwiające bezpłatny upgrade do najnowszego wydania Microsoft Office dostępnego na rynku w wersji do zastosowania w biznesie lub równoważne. Opis równoważności znajduje się w pkt.4.2 (SOPZ).
30.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca
31.	Gwarancja	Minimalny czas trwania gwarancji producenta 3 lata. Firma serwisująca musi posiadać ISO 9001 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.
32.	Wsparcie techniczne producenta	- możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. - Możliwość zagwarantowania naprawy na następny dzień roboczy przy założeniu, że usterka zostanie zgłoszona w sposób skuteczny do godziny 11:00.

3.10 Licencje dostępowe RDS – 5szt

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Licencje umożliwiające dostęp dla użytkowników do zdalnego pulpitu systemu zainstalowanego na dostarczonych serwerach
2.	Wymagania niezbędne	1. Wersja licencji musi być odpowiednia dla zainstalowanego systemu operacyjnego na dostarczonym serwerze. 2. Wymagane jest aby licencjonowanie odbywało się w opcji na użytkownika

3.11 Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS) – 1szt – minimalne wymagania

Lp.		
1.	Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest aby dostarczony system zabezpieczeń współpracował z dostarczonymi przełącznikami w minimalnym zakresie: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. W ofercie wymagane jest podanie modelu, symbolu oraz producenta jak również dostarczenie karty katalogowej umożliwiającej sprawdzenie parametrów technicznych dostarczanego urządzenia
2.	Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: • 10 portami Gigabit Ethernet RJ-45.

		• 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
4.	Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
5.	Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
6.	Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa

		np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.
7.	Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
8.	Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
9.	Funkcje SD-WAN	4. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 5. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
10.	Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

		2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL
11.	Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
12.	Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet
13.	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
14.	Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

<table>
<tr><td></td><td></td><td>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</td></tr>
<tr><td>15.</td><td>Uwierzytelnianie użytkowników w ramach sesj</td><td>1. System musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</td></tr>
<tr><td>16.</td><td>Zarządzanie</td><td>1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</td></tr>
<tr><td>17.</td><td>Logowanie</td><td>1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie</td></tr>
</table>

		danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
18.	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
19.	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
20.	Gwarancja oraz wsparcie	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. 2. Wykonawca musi zapewnić przez okres trwania licencji pełne wsparcie techniczne realizowane przez etatowego pracownika posiadającego autoryzowany certyfikat producenta, potwierdzający doświadczenie i umiejętność obsługi dostarczonego rozwiązania (certyfikat delegowanego pracownika należy załączyć do oferty), wsparcie techniczne ma być świadczone poprzez telefon, email i dedykowany system HelpDesk (należy podać adres strony WWW). 3. Wykonawca będzie zobligowany do przeprowadzenia audytu konfiguracji urządzenia UTM wg. zakresu: • aktualizacja oprogramowania do najnowszej wersji • weryfikacja i ew. poprawa polityk bezpieczeństwa • podniesienie poziomu bezpieczeństwa (dodatkowa konfiguracja polityk w oparciu o profile UTM) • testy poprawności działania urządzenia

3.12 Zakup specjalistycznego oprogramowania typu EDR – 1szt – minimalne wymagania

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Oprogramowanie klasy EDR (Endpoint Detection and Response) służące do identyfikacji anomalii systemowy, uzupełniający o dodatkową warstwę zabezpieczeń system antywirusowy. Oprogramowanie działające w technologii klient serwer W ofercie wymagane jest podanie nazwy oprogramowania oraz producenta jak również dostarczenie karty katalogowej dostarczanego oprogramowania umożliwiającej sprawdzenie funkcjonalności oprogramowania
2.	Serwer	1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych. 2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. 4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. 6. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 7. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 8. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 9. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 10. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 11. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 12. Serwer musi posiadać minimum 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 13. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne. 14. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 15. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali. 16. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 17. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 18. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 19. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość

		szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 20. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 21. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy. 22. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: 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) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 23. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). 24. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 25. Konsola administracyjna musi mieć możliwość tagowania obiektów. 26. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli. 27. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci. 28. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. 29. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.
3.	Agent (Klient)	1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10 oraz Windows Server 2008/2012/2016/2019. 2. Pełne wsparcie dla systemów macOS 10.12 i nowszych. 3. Wsparcie dla systemów Linux. 4. Wsparcie dla 32 i 64-bitowej wersji systemu Windows. 5. Agent musi współpracować z produktem antywirusowym tego samego producenta. 6. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta. 7. Połączenie agenta do serwera zarządzającego musi być szyfrowane. 8. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.
4.	Licencja	1. Licencja powinna umożliwić instalację, monitoring i ochronę minimum 79 stacji roboczych (komputery stacjonarne i laptopy), 14 serwerów

4 Równoważności

4.1 System operacyjny MS Windows Professional 64bit PL lub równoważne, spełniający poniższe warunki

- System operacyjny dla komputerów stacjonarnych i przenośnych, z graficznym interfejsem użytkownika,
- System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego w szczególności: MS Office 2013, 2021, Oprogramowanie dziedzinowe firmy Softres, Oprogramowanie firmy Clanet, Oprogramowanie SJOBESTIA, Oprogramowanie firmy CLANET
- Interfejsy użytkownika dostępne minimum w języku Polskim.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
- Wbudowany system pomocy w języku polskim,
- Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
- Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
- Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
- Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
- Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
- Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
- Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
- Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
- Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
- Mechanizmy logowania do domeny w oparciu o:
    - Login i hasło,
    - Karty z certyfikatami (smartcard),
    - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- Mechanizmy wieloelementowego uwierzytelniania.
- Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
- Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
- Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;

- Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
- Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
- Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową, Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
- Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
- Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
- Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
- Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
- Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
- Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
- Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
- Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
- Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

4.2 Oprogramowanie Microsoft Office lub równoważne, spełniające minimum poniższe warunki

- Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. Musi zawierać co najmniej następujące komponenty:
  - edytor tekstu,
  - arkusz kalkulacyjny,
  - program do przygotowywania i prowadzenia prezentacji,
  - program do zarządzania informacją przez użytkownika (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami);
- 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;
- Dostępna pełna polska wersja językowa interfejsu użytkownika, systemu komunikatów i podręcznej kontekstowej pomocy technicznej;
- Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, w tym obsługa formatowania bez utraty parametrów i cech użytkowych (zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów);
- 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 2016 oraz MS Office 2021 bez utraty danych oraz bez konieczności przerabiania dokumentów;
- Możliwość zapisywania wytworzonych dokumentów bezpośrednio w formacie PDF;
- Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory;
- Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich elementów;
- Możliwość jednoczesnej pracy wielu użytkowników na udostępnionym dokumencie arkusza kalkulacyjnego;
- Posiadać pełną kompatybilność z systemami operacyjnymi:
  - MS Windows 10 (32 i 64-bit),
  - MS Windows 11 (32 i 64-bit).

4.3 System operacyjny Microsoft Windows Server 2022 Standard lub równoważne spełniający poniższe warunki

- System operacyjny przeznaczony dla serwerów, z interfejsem graficznym.
- Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory
- Wbudowany mechanizm wirtualizacji typu hypervisor
- możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP)
- możliwość uruchomienia roli serwera DNS bez zakupu dodatkowych licencji
- możliwość uruchomienia roli klienta i serwera czasu (NTP) bez zakupu dodatkowych licencji
- możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory bez zakupu dodatkowych licencji
- możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory bez zakupu dodatkowych licencji
- możliwość uruchomienia roli serwera stron WWW z uwierzytelnianiem i autoryzacją dostępu w domenie Microsoft Active Directory bez zakupu dodatkowych licencji
- możliwość uruchomienia serwera terminali.
- w ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera
- w ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych
- Możliwość instalacji i uruchomienia serwera MS SQL serwer z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory, oraz ze wsparciem producenta MS SQL serwera.
- Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
- Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
- Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
- Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
- Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
- Możliwość zarządzania serwerem poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
- Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.

- Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
- Mechanizmy logowania do domeny w oparciu o:
    - Login i hasło,
    - Karty z certyfikatami (smartcard),
    - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- Mechanizmy wieloelementowego uwierzytelniania.
- Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
- Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
- Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
- Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
- Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
- Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
- Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
- Licencja musi umożliwiać uruchomienie na dostarczonych serwerach.