Miasto Gorlice

Gorlice, dnia 19.07.2023

OR-III.271.2.13.2023

do wszystkich Wykonawców

dotyczy: Zmiana treści Specyfikacji Warunków Zamówienia (SWZ) , wydłużenie terminu składania ofert w postępowaniu o zamówienie publiczne prowadzonym w trybie podstawowym na rozbudowę sieci LAN urzędu - elementy aktywne - serwery, oprogramowanie do wirtualizacji, UTM'y, macierz dyskowa z dyskami oraz pozostałe elementy - w ramach projektu "Cyfrowa Gmina"

1. <u>Zmiana treści SWZ:</u>

W związku z omyłką Zamawiającego polegającą na błędnym określeniu parametrów procesora serwera – w dokumentach zamówienia minimalny wynik osiągnięty przez procesor w teście „SPECrate2017_fp_base" określony jest na poziomie 149, gdy tymczasem prawidłowy to : **147.**
Mając na uwadze powyższe Zamawiający działając na podstawie art. 286 ust. 3 i 9 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (tj.: Dz.U. z 2022, poz. 1710 ze zm.) modyfikuje w całości treść Załączników nr 1 i 10 do SWZ na treść Załączników nr 1 i 10 dołączonych do niniejszego pisma (uwzględniających prawidłowy parametr).

2. <u>Przedłużenie terminu składania i otwarcia ofert</u>

Na podstawie przepisu art. 286 ust. 3 i 9 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (tj.: Dz.U. z 2022, poz. 1710 ze zm.) Zamawiający wydłuża termin składania ofert.

<u>Nowe, obowiązujące terminy:</u>

Termin składania ofert upływa dnia: 27.07.2023 r. godz. 13:00

Otwarcie ofert nastąpi dnia: 27.07.2023 r. godz. 13:30

Postanowienia ust. 13 SWZ - Wymagania dotyczące wadium należy zastosować odpowiednio, z uwzględnieniem przedłużonego terminu do składania ofert.

Dokonuje się odpowiednio zmiany terminu związania ofertą, w związku z czym postanowienie ust. 5 pkt 1) SWZ otrzymuje nową treść:

„5. TERMIN ZWIĄZANIA OFERTĄ

1) Termin związania ofertą wynosi 30 dni od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert. **Wykonawca jest związany ofertą do upływu terminu 25.08.2023 r."**

Zamawiający informuje jednocześnie o odpowiedniej zmianie ogłoszenia o zamówieniu nr 2023/BZP 00310487/01 z dnia 2023-07-17

3. <u>Załączniki :</u>

1. Nowy , obowiązujący załącznik nr 1 do SWZ – Opis przedmiotu zamówienia
2. Nowy,, obowiązujący załącznik nr 10 do SWZ - Oświadczenie wykonawcy o spełnieniu przez przedmiot zamówienia wymaganych cech, parametrów, właściwości i funkcjonalności.

Ko:

1) Strona internetowa prowadzonego postępowania
2) a/a

Z up. BURMISTRZA

Daniel Janeczek
Sekretarz Miasta

.....

(podpis kierownika Zamawiającego)

Sporządził : Mirosław Łopata - inspektor, Wydział Organizacyjny, Dział Zamówień Publicznych, tel. 183551252

Wymagania minimalne dla:

1. **Klaster urządzeń UTM - 1 komplet**

Lp.	Wymagania minimalne
1	**Firewall**
1.1	**Funkcjonalność Firewall**
1.1.1	Firewall umożliwia zdefiniowanie co najmniej 3 stref bezpieczeństwa
1.1.2	Firewall obsługuje protokoły dynamicznego routingu: RIP, OSPF i BGP
1.1.3	Firewall obsługuje statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie
1.1.4	Firewall obsługuje DHPC v6 na zewnętrznym interfejsie
1.1.5	Firewall umożliwia pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP, jako bridge (transpartent mode) lub z tym samym adresem IP na wszystkich portach.
1.1.6	Firewall ma możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu i dynamiczną selekcją drogi routowania.
1.1.7	Firewall ma możliwość obsługi łącza zapasowego typu LTE
1.1.8	Firewall obsługuje Dynamic DNS
1.1.9	Firewall obsługuje translację adresów: statyczną, dynamiczną i 1-1
1.1.10	Firewall obsługuje translację portów: PAT
1.1.11	Firewall obsługuje IPSec NAT traversal
1.1.12	Firewall obsługuje mechanizm policy-based NAT
1.1.13	Firewall obsługuje VLAN 802.1Q
1.1.14	Firewall zapewnia ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów
1.1.15	Firewall obsługuje pracę jako serwer DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
1.1.16	Firewall umożliwia pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP
1.1.17	Firewall umożliwia uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
1.1.18	Firewall umożliwia uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników.
1.1.19	Firewall umożliwia transparentne uwierzytelnianie użytkowników przez Active Directory.

1.1.20	Urządzenie umożliwia uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp.
1.1.21	Urządzenie nie ogranicza ilości urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
1.1.22	Firewall zapewnia możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
1.1.23	Firewall zapewnia możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
1.1.24	Firewall obsługuje mechanizmy Protocol Anomaly Detection (PAD) dla najpopularniejszych protokołów.
1.1.25	Firewall zapewnia wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
1.1.26	Firewall zapewnia ochronę z wykorzystaniem mechanizmów IPS.
1.1.27	Firewall zapewnia ochronę antywirusową dla obsługiwanych protokołów.
1.1.28	Firewall zapewnia możliwość filtrowania URL.
1.1.29	Firewall zapewnia inspekcję ruchu szyfrowanego HTTPS.
1.1.30	Firewall zapewnia ochronę przed niechcianą pocztą (AntySPAM).
1.1.31	Firewall zapewnia rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.
1.1.32	Urządzenie ma możliwość filtrowania treści według typu MIME.
1.1.33	Urządzenie umożliwia sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji.
1.1.34	Firewall udostępnia mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych.
1.1.35	Firewall może pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site
1.1.36	Firewall posiada mechanizm blokujący szkodliwe żądania DNS, zapewniając ochronę użytkowników końcowych przed atakami typu phishing.
1.2	**Wydajność firewall**
1.2.1	Firewall zapewnia obsługę na poziomie minimalnym: **5,7Gbps** dla pracy w trybie firewall (UDP 1518), **1,15Gbps** dla pracy w trybie UTM (pełny skan)
1.2.2	Firewall obsługuje minimum **3 400 000** jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z

	wydajnością minimalną **34 000** nowych połączeń na sekundę.
1.2.3	Ilość obsługiwanych sieci VLAN: minimum **100.**
1.2.4	Minimalna ilość fizycznych portów: - 8 portów 1Gbps RJ45 - 2 porty 10 Gbps SFP+
2	**VPN**
2.1	**Funkcje VPN**
2.1.1	Urządzenie obsługuje połączenia VPN site-to-site z wykorzystaniem IPSec oraz TLS.
2.1.2	Urządzenie w zakresie IPSec site-to-site VPN współpracuje z rozwiązaniami innych producentów.
2.1.3	Rozwiązanie wspiera mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
2.1.4	Rozwiązanie wspiera mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert.
2.1.5	Wsparcie dla Dead Peer Detection (DPD).
2.1.6	Urządzenie obsługuje IKEv1 i IKEv2
2.1.7	Urządzenie obsługuje Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web.
2.1.8	Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP.
2.1.9	Urządzenie zapewnia możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
2.1.10	Urządzenie obsługuje statyczne i dynamiczne (routowane) połączenia VPN do dostawców chmury obliczeniowej (AWS i MS Azure).
2.1.11	Urządzenie obsługuje połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP.
2.1.12	Połączenia client-to-site są możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
2.1.13	Dla połączeń IPSec client-to-site jest możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu.
2.1.14	Urządzenie zapewnia funkcję portalu dostępowego chronionego przez szyfrowanie https (TLS).
2.2	**Wydajność VPN**
2.2.1	Przepustowość IPSec VPN (UDP 1518) nie mniejsza niż **2,3Gbps**
2.2.2	Obsługa nie mniej niż: **70** tuneli IPSec site-to-site
2.2.3	Obsługa nie mniej niż: **70** tuneli client-to-site
3	**Filtrowanie zawartości URL**
3.1	Urządzenie umożliwia filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.

3.2	Funkcjonalność filtrowania zawartości daje możliwość filtrowania stron według minimalnie 120 kategorii.
3.3	Rozwiązanie pozwala na tworzenie białych list wyjątków dla filtrowania zawartości.
3.4	Baza zawartości URL jest dostępna on-line lub do ściągnięcia i zainstalowania miejscowo.
3.5	Funkcja filtruje treści w wielu językach, w tym w języku polskim.
3.6	Filtrowanie obsługuje również protokół https.
3.7	Urządzenie umożliwia wyłączenie inspekcji https dla wybranych kategorii stron www.
3.8	System kategoryzacji stron posiada kategorie: Command&control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware.
4	**Kontrola aplikacyjna**
4.1	System kontroli aplikacyjnej rozpoznaje aplikacje oraz kategorie aplikacji.
4.2	Aplikacje są rozpoznawane w oparciu o analizę ruchu a nie przez porty i protokoły.
4.3	Ilość rozpoznawanych aplikacji nie mniejsza niż 1800.
4.4	W ramach konkretnej aplikacji system umożliwia kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe).
4.5	Kontrola aplikacyjna rozpoznaje co najmniej aplikacje: Tor, CryptoAdmin, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
5	**Antywirus**
5.1	System ma możliwość uruchomienia co najmniej 2 skanerów antywirusowych.
5.2	Aktualizacja plików sygnatur antywirusowych może odbywać się automatycznie.
5.3	Aktualizacja plików sygnatur antywirusowych odbywa się nie rzadziej niż co 12 godzin.
5.4	Antywirus ma możliwość przeprowadzania kwarantanny e-mail.
5.5	Jeden ze skanerów antywirusowych bazuje na mechanizmach bezsygnaturowych.
5.6	Rozwiązanie ma możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen.
5.7	Wykrywanie i blokowanie spyware'u.
5.8	Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
5.9	Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.
5.10	Przepustowość AV w urządzeniu nie mniejsza niż **1,4Gbps**

5.11	W celu realizacji ochrony z wykorzystaniem 2 skanerów antywirusowych Zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia.
6	**Antyspam**
6.1	Antyspam zapewnia możliwość kwarantanny e-mail.
6.2	Antyspam posiada zintegrowaną antywirusową analizę spamu.
6.3	Rozwiązanie umożliwia blokowanie spamu w wielu językach w tym w języku polskim.
6.4	Możliwość blokowania spamu opartego na obrazach graficznych.
7	**IPS**
7.1	Automatyczna aktualizacja sygnatur IPS.
7.2	IPS ma możliwość dokonywania analizy warstwy aplikacji, a także ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
7.3	Automatyczne blokowanie znanych źródeł ataków.
7.4	System pozwala na blokowanie ataków typu DoS i DDoS.
7.5	Przepustowość IPS (pełny skan) w urządzeniu nie mniejsza niż **1,3Gbps**.
8	**Ochrona przed phishingiem**
8.1	System zapewnia dedykowaną (poza ochroną przed SPAMem) ochronę przed phishingiem.
8.2	System blokuje możliwość dostępu do spreparowanych stron.
8.3	System blokuje dostęp niezależnie od użytego protokołu czy portu komunikacyjnego.
8.4	Zablokowanie dostępu jest odpowiednio notyfikowane użytkownikowi, którego dotyczy, niezależnie od logów i raportów.
8.5	System chroni przed nadużyciem protokołu DNS.
9	**Zarządzanie**
9.1	Administracja urządzenia jest możliwa poprzez graficzny interfejs zarządzania w czasie rzeczywistym.
9.2	Urządzenie umożliwia zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH.
9.3	Urządzenie umożliwia zarządzanie za pomocą wbudowanego interfejsu www.
9.4	Interfejs WWW do zarządzania urządzeniem ma właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
9.5	Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów.
9.6	Rozwiązanie umożliwia wysyłanie alarmów przez SNMP lub e-mail.
9.7	Rozwiązanie umożliwia edytowanie polityk bezpieczeństwa w trybie online.

9.8	System zapewnia możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
9.9	Rozwiązanie wspiera instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
9.10	System posiada metodę porównywania różnych wersji konfiguracji.
9.11	Obsługa różnych ról administratorów.
9.12	Możliwość monitorowania logów ruchu w czasie rzeczywistym.
9.13	System posiada możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty).
9.14	Urządzenie umożliwia zarządzanie bezprzewodowymi punktami dostępowymi.
9.15	System zarządzania zapewnia korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów.
9.16	System zarządzania posiada graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop.
10	**Dzienniki i raporty**
10.1	Rozwiązanie umożliwia zbieranie i przechowywanie dzienników i raportów.
10.2	Rozwiązanie umożliwia przesyłanie logów do co najmniej 2 serwerów dziennika.
10.3	Dzienniki transmisji mogą być szyfrowane.
10.4	Rozwiązanie zapewnia narzędzie graficznej analizy logów.
10.5	Rozwiązanie udostępnia narzędzie analizy całości ruchu.
10.6	Rozwiązanie udostępnia narzędzie analizy incydentów bezpieczeństwa.
10.7	Rozwiązanie nie narzuca ograniczeń co do czasu przechowywania logów czy rozmiaru bazy danych.
10.8	Rozwiązanie posiada minimum 90 predefiniowanych typów raportów.
10.9	Predefiniowane raporty mają możliwość dopasowania do instytucji użytkującej rozwiązanie.
10.10	System ma możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
10.11	System jest w stanie zautomatyzować generowanie raportów i ma możliwość wysyłania tych sprawozdań pocztą e-mail.
10.12	Jest zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
10.13	System raportowania jest wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników.

10.14	System wspiera automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną.
10.15	Rozwiązanie umożliwia kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
10.16	System umożliwia pseudoanonimizację użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów.
10.17	System zapewnia wizualizację, opisującą w trybie graficznym stan przepustowości systemu.
11.	**Zero Day / Zaawansowana Detekcja Malware**
11.1	Funkcja zaawansowanego wykrywania szkodliwego oprogramowania w tym samym urządzeniu.
11.2	Zaawansowany Malware jest wykrywany przez uruchomienie plików w chmurze przy użyciu emulacji pełnego systemu.
11.3	Zaawansowana Detekcja Malware obsługuje wszystkie pliki wykonywalne systemu Windows, pliki zip, pdf, Microsoft Office, oraz pliki Android APK.
11.4	Szczegółowe raporty oraz informacje wskazujące na powody, dla których plik jest uważany za zaawansowany Malware.
11.5	W celu realizacji ochrony „Zero Day" zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia.
12.	**Architektura**
12.1	Rozwiązanie musi być dostarczone w formie klastra dwóch fizycznych urządzeń z licencjami umożliwiającymi ich pracę co najmniej w trybie klastra Aktywny/Pasywny (ang. Active/Passive).
12.1	Urządzenia wchodzące w skład klastra są urządzeniami tego samego producenta i modelu, oraz każde z tych urządzeń spełnia minimalne techniczne parametry wydajnościowe określone przez niniejszą specyfikację.
13.	**Gwarancja**
13.1	Okres wsparcia technicznego - minimum **3 lata**.
13.2	Urządzenie dostarczone ze wszystkimi licencjami/subskrypcjami umożliwiającymi uzyskanie funkcjonalności wymienionymi w niniejszej specyfikacji. Długość trwania licencji/subskrypcji nie może być krótsza niż okres wsparcia technicznego.
13.3	Możliwość zgłaszania incydentów za pomocą e-mail, portalu - 24 godziny na dobę 7 dni w tygodniu.
13.4	Wymiana urządzenia w przypadku zdiagnozowania awarii uniemożliwiającej funkcjonowanie, następowała na następny dzień roboczy od zdiagnozowania awarii (advanced hardware replacement NBD).

2. **Przełączniki LAN Typ 1 - 2 szt.**

Lp.	Wymagania minimalne
1	Typ Obudowy: Obudowa do montażu w szafie RACK 19" - 1U wraz z zestawem montażowym.
2	Porty: - 24 x 10 Gigabit Ethernet SFP+, - 2 x 40 Gigabit Ethernet QSFP+, Porty QSFP+ powinny mieć możliwość rozszycia w celu konfiguracji 4x10GbE - 1 x RJ45 console/management port (RS232), - 1 x RJ45 management port, - 1 x USB 2.0 type A, Umożliwia zestawienie stosu portami/magistralami minimum, Full Duplex 40GbE (do min. 2 urządzeń).
3	Wydajność: - Przepustowość przełącznika minimum 620Gb/s. - Wydajność przełączania minimum 460Mpps. - Obsługa minimum 32,000 adresów MAC. - Bufor pakietów minimum 1,5MB - Taktowanie procesora: 1GHz - Pamięć RAM 512MB
4	Zasilanie: Zasilanie 230V AC
5	Funkcje i protokoły: - Obsługuje następujące protokoły drzewa rozpinającego: • 802.1D - STP • 802.1w - RSTP • 802.1s - MSTP - Obsługuje jeden z protokołów do tworzenia wirtualnych nadmiarowych bram sieciowych np. (VRRP lub HSRP), - Obsługa multicastów z wykorzystaniem protokołów: • IGMP, • IGMP Snooping, - Możliwość monitorowania ruchu na porcie (Port Mirroring), - Możliwość agregacji połączeń z wykorzystaniem protokołu LACP - IEEE 802.3ad, - Obsługuje następujące protokoły odnajdywania urządzeń w sieci: • LLDP, • LLDP-MED, - Obsługuje następujące protokoły autoryzacji: • TACACS+, • RADIUS, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
6	Zarządzanie: - Posiada tekstowy interfejs zarządzania z podpowiedziami kontekstowymi,

	- Posiada tekstowy plik konfiguracyjny możliwy do wyeksportowania, edytowania poza urządzeniem i ponownego zaimportowania do urządzenia, - Możliwość zarządzania urządzeniem z wykorzystaniem protokołów SSHv2 oraz TELNET, - Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI), - Umożliwia bezpośredni dostęp do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji, - Obsługa wysyłania powiadomień o zdarzeniach z użyciem protokołów SNMPv1, SNMPv2c oraz SNMPv3, - Umożliwia przesyłanie dzienników zdarzeń z wykorzystaniem protokołu SYSLOG, - Obsługuje synchronizację czasu systemowego z użyciem protokołów SNTP lub NTP, - Możliwość konfiguracji pracy w trybie klienta DNS.
7	Wyposażenie: Niezbędne akcesoria w celu zbudowania nadmiarowej konstrukcji wykorzystując porty o przepustowości 40GbE
8	Gwarancja: Oferowane urządzenie jest objęte co najmniej 3-letnim wsparciem (gwarancją) producenta lub partnera na terenie Polski. Kontakt ze wsparciem w dni robocze, czas reakcji w miejscu instalacji sprzętu następny dzień roboczy.

3. **Przełączniki LAN Typ 2 - 3 szt.**

Lp.	Wymagania minimalne
1	Typ Obudowy: Obudowa do montażu w szafie RACK 19" - 1U wraz z zestawem montażowym.
2	Porty: - 48 x 1 Gigabit Ethernet 1000BASE-T (RJ45), - 2 x 1 Gigabit Ethernet SFP, - 2 x 10 Gigabit Ethernet SFP+, - 1 x RJ45 console/management port (RS232),
3	Wydajność: - Przepustowość przełącznika minimum 135Gbps. - Wydajność przełączania minimum 100Mpps.
4	Zasilanie: Zasilanie 230V AC
5	Funkcje i protokoły: - Obsługuje następujące protokoły drzewa rozpinającego: • 802.1D - STP • 802.1w - RSTP -- Możliwość agregacji połączeń z wykorzystaniem protokołu LACP - IEEE 802.3ad, - Obsługa protokołu, odnajdywania urządzeń w sieci: • LLDP, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
6	Zarządzanie: - Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI), - Możliwość bezpośredniego dostępu do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji, - Obsługa synchronizacji czasu systemowego z użyciem protokołów SNTP lub NTP,
7	Gwarancja: Oferowane urządzenie jest objęte co najmniej rocznym wsparciem producenta lub partnera na terenie Polski. Kontakt ze wsparciem w dni robocze.

4. **Przełączniki LAN Typ 3 - 2 szt.**

Lp.	Wymagania minimalne
1	Typ Obudowy: Obudowa do montażu w szafie RACK 19" - 1U wraz z zestawem montażowym.
2	Porty: - 16 x 1 Gigabit Ethernet 1000BASE-T (RJ45) PoE+, - 2 x 1 Gigabit Ethernet SFP, - 1 x RJ45 console/management port (RS232),
3	Wydajność: - Przepustowość przełącznika minimum 35Gbps. - Wydajność przełączania minimum 25Mpps. - Obsługa minimum 16000 adresów MAC.
4	Zasilanie: Zasilanie 230V AC
5	Funkcje i protokoły: - Obsługuje następujące protokoły drzewa rozpinającego: • 802.1D - STP • 802.1w - RSTP -- Możliwość agregacji połączeń z wykorzystaniem protokołu LACP - IEEE 802.3ad, - Obsługa protokołu, odnajdywania urządzeń w sieci: • LLDP, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
6	Zarządzanie: - Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI), - Możliwość bezpośredniego dostępu do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji, - Obsługa synchronizacji czasu systemowego z użyciem protokołów SNTP lub NTP,
7	Gwarancja: Oferowane urządzenie jest objęte co najmniej rocznym wsparciem producenta lub partnera na terenie Polski. Kontakt ze wsparciem w dni robocze.

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

Lp.	Wymagania minimalne
1	Urządzenie posiada minimum dwa kontrolery obsługujące dostęp do dysków, pracujące w trybie Active/Active. Moduł kontrolerów umożliwia instalację minimum 24 dysków 2,5". Urządzenie umożliwia instalację w szafach RACK 19" i będzie dostarczone z niezbędnym wyposażeniem do wykonania takiej instalacji.
2	Urządzenie posiada możliwość instalacji dodatkowych modułów dyskowych pozwalających na instalację w danym module minimum: - 24 szt. dysków 2,5" w obudowie max 2U, - 15 szt. dysków 3,5" w obudowie max 4U.
3	Urządzenie jest wyposażone w system redundantnego zasilania i chłodzenia, który gwarantuje możliwość pracy i utrzymanie bez przerw funkcjonalności urządzenia w tym działanie pamięci cache.
4	Urządzenie zapewnia w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez czas nieograniczony.
5	Urządzenie umożliwia utworzenie wolumenu LUN o rozmiarze minimum 64TB i systemu plików minimum 64TB.
6	Urządzenie będzie dostarczone w konfiguracji pozwalającej na obsługę minimum 128 GB pamięci podręcznej, obsługującej jednocześnie odczyty i zapisy. Pamięć będzie dostępna jednocześnie dla wszystkich wolumenów i kontrolerów macierzy. Włączenie lub wyłączenie pamięci podręcznej nie wymaga operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych.
7	Urządzenie jest wyposażone w następującą minimalną liczbę portów do podłączania hostów (porty Front-end): - cztery porty, 10 Gbps iSCSI SFP+.
8	Urządzenie wspiera architekturę bezpośredniego podłączania serwerów do macierzy (bez pośrednictwa przełączników SAN) przy pomocy protokołów FC i 10GbE iSCSI (jest to potwierdzone w oficjalnych dokumentach producenta urządzenia).

9	Urządzenie umożliwia zastosowanie dysków SSD, HDD 10k i HDD 7,2k RPM. Wszystkie dyski 2,5" i 3,5" są wyposażone w interfejsy SAS 12Gbps lub wydajniejsze.
10	Urządzenie jest wyposażona w dyski posiadające podwójne interfejsy.
11	Urządzenie posiada funkcjonalność globalnych dysków zapasowych lub globalnej przestrzeni Hot-Spare. W wypadku zastosowania technologii globalnej przestrzeni Hot-Spare, wymagane jest dostarczenie o 10% większej surowej przestrzeni dyskowej niż wymagana w punkcie 13, dla każdego rodzaju zaoferowanych dysków (dotyczy również dostarczanych ewentualnych dodatkowych modułów dyskowych).
12	Urządzenie umożliwia rozbudowę do co najmniej 480 napędów dyskowych w obrębie pojedynczego urządzenia, bez potrzeby wymiany kontrolerów macierzy dostarczonych w ramach niniejszego postępowania.
13	Pojemność surowa (ang. RAW) macierzy: - minimum 2,3 TB, na minimum 6 dyskach SSD 12Gbps, 2,5". - minimum 13 TB, na minimum 11 dyskach SAS 12Gbps, 2,5", 10K RPM.
14	Połączenia między dyskami, a kontrolerami są wykonane w technologii SAS 12Gbps lub wydajniejszej.
15	Urządzenie umożliwia równoczesną obsługę wielu poziomów RAID, minimum RAID 10, 5, 6.
16	Urządzenie posiada funkcjonalność tworzenia lokalnych kopii migawkowych wewnętrznymi mechanizmami macierzy w technologii "redirect on write". Dopuszcza się, aby macierz wykonywała lokalne kopie migawkowe z wykorzystaniem innych technologii, w takim wypadku wymaga się dostarczenia dodatkowych: - minimum 4 dysków SSD każdy o pojemności minimum 1,6TB 12Gbps, 2,5", DWPD minimum 3. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.
17	Urządzenie obsługuje minimum 64 kopii migawkowych per dysk logiczny LUN oraz 64 kopii per system plików.

	Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.
18	Przepełnienie przestrzeni dla kopii migawkowych nie powoduje błędów zapisu na przestrzeń produkcyjną.
19	W przypadku odtworzenia danych z dowolnej kopii migawkowej, urządzenie pozwala na poprawne zachowanie także wcześniejszych jak i późniejszych snapshotów, z zachowaniem możliwości kolejnego odtworzenia danych ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu.
20	Urządzenie obsługuje lun masking, lun mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy.
21	Urządzenie jest wyposażone w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż" (limit) dla następujących parametrów dostępu do dysku logicznego: a. Ilość operacji na sekundę (IOPS), b. Przepustowość (MB/s). Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.
22	Urządzenie umożliwia replikację synchroniczną i asynchroniczną danych blokowych oraz replikację asynchroniczną dla danych plikowych pomiędzy dwiema macierzami. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.
23	Urządzenie posiada funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych, w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje są wykonywane automatycznie bez udziału administratora. Pojedynczy migrowany obszar nie może być większy niż 256MB. Migracja danych odbywa się bez przerywania dostępu do danych od strony hostów i aplikacji. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.

24	Funkcjonalność tieringu jest możliwa pomiędzy wszystkimi typami stosowanych dysków (SSD, SAS, NLSAS).
25	Urządzenie umożliwia automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
26	Urządzenie zapewnia jednoczesne zastosowanie różnych trybów protekcji RAID dla różnych typów dysków fizycznych obsługujących pojedynczy dysk logiczny objęty mechanizmem tieringu.
27	Urządzenie zapewniać mechanizm Thin Provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała przydzielonej pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.
28	Urządzenie umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation).
29	Urządzenie oferuje funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.
30	Urządzenie wspiera wirtualizację serwerową w zakresie: VMware: VAAI, VASA, VVols 2.0, integracja macierzy z VMware vRealize Operations oraz Hyper-V: Offloaded Data Transfer (ODX) and Offload Copy for File.
31	Urządzenie obsługuje co najmniej protokoły blokowe: FC i iSCSI, oraz protokoły plikowe: NFS v4.1(MS Windows 2016 i 2019), NFSv3, SMB 2, SMB 3 i VMware VVols (Virtual Volumes) 2.0.
32	Urządzenie jest zgodne z normami UE i przeznaczone do sprzedaży na rynek UE. Urządzenie posiada certyfikat CE.
33	Dostarczone urządzenie jest fabrycznie nowe, nieregenerowane i wyprodukowane nie wcześniej niż w pierwszym półroczu 2023 r., pochodzi z oficjalnego kanału sprzedaży producenta na teren UE.
34	Urządzenie oraz jego oprogramowanie wewnętrzne jest objęte co najmniej 3-letnim wsparciem producenta (gwarancją). Kontakt ze wsparciem w dni robocze, czas reakcji w miejscu instalacji sprzętu: następny dzień roboczy.

	W okresie opieki wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Serwis zawiera usługę pozostawiania bez opłat u Zamawiającego uszkodzonych dysków w okresie obowiązywania gwarancji. Możliwość zgłaszania awarii poprzez linię telefoniczną producenta obsługiwaną w języku polskim.
35	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta oraz, że uszkodzone dyski w przypadku wymiany z powodu awarii w okresie obowiązywania gwarancji, pozostaną własnością Zamawiającego. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.

6. **Serwery - 2 szt.**

Lp.	Wymagania minimalne
1	Obudowa typu Rack o wysokości maksymalnie 1U. Komplet wysuwanych szyn i organizer okablowania, umożliwiający montaż w szafie rack i wysuwanie do celów serwisowych.
2	Płyta główna - pozwalająca na zainstalowanie minimum dwóch procesorów zaprojektowana przez producenta węzła i oznaczona jego znakiem firmowym.
3	Chipset - dedykowany przez producenta procesora do pracy w systemach dwuprocesorowych.
4	Procesory - zainstalowane dwa procesory maksimum 8-rdzeniowe klasy x86 uzyskujące w teście „SPECrate2017_fp_base" dostępnym na stronie www.spec.org dla konfiguracji z dwoma procesorami wynik min. 147 punktów, dla oferowanych procesorów. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanych procesorów. Maksymalna liczba rdzeni procesora ograniczona przez licencjonowanie zastosowanego w projekcie oprogramowania.
5	Pamięć RAM - minimum 192GB. Płyta główna obsługuje do minimum 1TB pamięci RAM dla konfiguracji dwu-procesorowej. Pojemność zastosowanych kości pamięci RAM min. 16 GB.
6	Zabezpieczenia pamięci RAM - Memory Mirror.
7	Gniazda PCI - minimum trzy sloty PCIe w tym minimum jeden x16.
8	Interfejsy sieciowe: - minimum 4 porty typu Ethernet 10/25Gbps SFP28, - minimum 2 porty typu Ethernet 1Gbps RJ45.
9	Przestrzeń dyskowa: Dedykowany fizyczny moduł pozwalający na konfigurację nadmiarowej przestrzeni dyskowej (min. RAID 1) zrealizowanej z wykorzystaniem min. dwóch nośników FLASH i/lub SSD o pojemności 240GB każdy, pozwalający na instalację i uruchamianie systemu operacyjnego serwera.
10	Wbudowane porty:

	- minimum 2 porty USB 2.0, - minimum 1 port USB 3.0, - 1 port RJ45 dedykowany do zarządzania, - 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym).
11	Video - zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
12	Wentylatory - redundantne
13	Zasilacze - redundantne, Hot-Plug minimum 750W.
14	Karta Zarządzania - niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność: - komunikacja poprzez interfejs RJ45, - podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging, - wbudowana diagnostyka, - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń, - monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym, - lokalna oraz zdalna konfiguracja serwera, - wsparcie dla IPv4 i IPv6, - możliwość zdalnego dostępu do konsoli graficznej, zainstalowanego systemu operacyjnego serwera.
15	Urządzenie wyprodukowane zgodnie z normą ISO-9001:2008 oraz ISO-14001. Urządzenie zgodne z normami UE i przeznaczone na rynek UE, posiada certyfikat CE.
16	Dostarczone urządzenia fabrycznie nowe, nieregenerowane i wyprodukowane nie wcześniej niż w pierwszym półroczu 2023 r., pochodzą z oficjalnego kanału sprzedaży producenta na teren Polski.
17	Oferowane urządzenie objęte co najmniej 3-letnim wsparciem producenta sprzętu. Kontakt ze wsparciem w dni robocze, czas reakcji w miejscu instalacji sprzętu: następny dzień roboczy. Możliwość sprawdzenia na stronie WWW producenta serwera, prowadzonej w języku polskim, po podaniu numeru seryjnego urządzenia, minimum:

	- okresu oraz poziomu gwarancji, - zainstalowanych komponentów (w tym m.in. procesorów, pamięci RAM, dysków, zasilaczy i kart komunikacyjnych). Adres strony WWW producenta na której można sprawdzić powyższe dane musi być podany w złożonej ofercie.
18	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.

7. **Zasilacz awaryjny UPS Typ 1 - 1 szt.**

Lp.	Wymagania minimalne
1	Typ obudowy i wymiary maksymalne: - wolnostojący, - wymiary maksymalne (w mm): 400x800x1400
2	Typ urządzenia: 3-fazowy, zintegrowana bateria,
3	Moc urządzenia: Minimum 15 kVA, 13,5 kW,
4	Gniazdo zasilania (wejścia): 400V 3-fazy+N
5	Gniazda wyjściowe: - 400V 3-fazy + N - 230V 1-faza + N
6	Czas podtrzymania bateryjnego dla mocy nominalnej 12kW: minimum 15 minut.
7	Zewnętrzny BYPASS serwisowy
8	Wskaźnik graficzny wyświetlający stan urządzenia, informujący minimum o: - Trybie pracy (normalny/z użyciem baterii) - Parametrach zasilania na wejściu - Stanie naładowania baterii - Poziomie obciążenia - Wystąpieniu alarmu/awarii
9	Urządzenie musi być wyposażone w port komunikacyjny RJ-45 umożliwiający: - działanie z prędkością min. 10/100 Mbps - Obsługę adresacji IPv4 oraz IPv6 - obsługę protokołów: • HTTP/HTTPS • DHCP • SNMP (v1,v2c,v3) • SMTP (z obsługą min. STARTTLS) • SSH • SYSLOG • FTP • SCP • NTP
10	Zamawiający przygotuje, zgodnie z zaleceniami dostarczanego UPS: - okablowanie, - rozdzielnie elektryczną, - zabezpieczenia pomiędzy rozdzielnią UPS - zasilaczem UPS, rozdzielnicą odbiorów.
11	Oferowane urządzenie musi być objęte co najmniej 2-letnią gwarancją producenta.

8. **Zasilacz awaryjny UPS Typ 2 - 1 szt.**

Lp.	Wymagania minimalne
1	Typ obudowy i wymiary maksymalne: - wolnostojący, - wymiary maksymalne (w mm): 450x850x1450
2	Typ urządzenia: 3-fazowy, zintegrowana bateria,
3	Moc urządzenia: Minimum 20 kVA, 18 kW,
4	Gniazdo zasilania (wejścia): 400V 3-fazy+N
5	Gniazda wyjściowe: - 400V 3-fazy + N - 230V 1-faza + N
6	Czas podtrzymania bateryjnego dla mocy nominalnej 18kW: minimum 15 minut.
7	Zewnętrzny BYPASS serwisowy
8	Wskaźnik graficzny wyświetlający stan urządzenia, informujący minimum o: - Trybie pracy (normalny/z użyciem baterii) - Parametrach zasilania na wejściu - Stanie naładowania baterii - Poziomie obciążenia - Wystąpieniu alarmu/awarii
9	Urządzenie musi być wyposażone w port komunikacyjny RJ-45 umożliwiający: - działanie z prędkością min. 10/100 Mbps - Obsługę adresacji IPv4 oraz IPv6 - obsługę protokołów: • HTTP/HTTPS • DHCP • SNMP (v1,v2c,v3) • SMTP (z obsługą min. STARTTLS) • SSH • SYSLOG • FTP • SCP • NTP
10	Zamawiający przygotuje, zgodnie z zaleceniami dostarczanego UPS: - okablowanie, - rozdzielnie elektryczną, - zabezpieczenia pomiędzy rozdzielnią UPS - zasilaczem UPS, rozdzielnicą odbiorów.
11	Oferowane urządzenie musi być objęte co najmniej 2-letnią gwarancją producenta.

9. **Wyposażenie dodatkowe**

Lp.	Wymagania minimalne
1	Moduły SFP+: - 20 sztuk SFP+ LR 10Gbs 1310nm LC SMF 10km, kompatybilne z dostarczanymi przełącznikami sieciowymi. - 6 sztuk SFP LR 1Gbps 1310nm LC SMF 20km, kompatybilne z dostarczanymi przełącznikami sieciowymi,
2	Kable DAC: - 14 szt. DAC SFP+ to SFP+ 10GbE, 3m.

10. Oprogramowanie do wirtualizacji serwerów

Lp.	Wymagania minimalne
1	Oprogramowanie do wirtualizacji serwerów: VMware vSphere 8 Essentials Plus Kit - 1 szt. lub równoważne. Licencje dostarczone wraz z minimum rocznym wsparciem technicznym. Wsparcie techniczne umożliwia zgłaszanie problemów w trybie co najmniej 5 dni/8 godz. Możliwość pobierania nowych wersji i poprawek w całym okresie trwania oferowanego wsparcia.

Opis równoważności dla Oprogramowania Systemu Wirtualizacji Serwerów:

Cechy równoważnego oprogramowania typu VMware vSphere Essentials Plus Kit:

I. Pakiet oprogramowania systemu wirtualizacyjnego będzie przeznaczony do wirtualizacji serwerów. Oprogramowanie do wirtualizacji serwerów będzie przeznaczone na klaster wirtualizacyjny składający się docelowo z maksymalnie trzech serwerów dwuprocesorowych.

II. Oprogramowanie Wirtualizacji Serwerów musi posiadać następujące cechy i funkcjonalności:

1) Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
2) Oprogramowanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług;
3) Oprogramowanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
4) Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2022, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 8.1, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Debian GNU/Linux, CentOS w tym dostarczone systemy operacyjne.
5) Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
6) Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej.
7) Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
8) Oprogramowanie musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów

operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.

9) Oprogramowanie musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
10) Oprogramowanie oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
11) Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
12) Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
13) Oprogramowanie musi zapewniać odpowiednią nadmiarowość i posiadać mechanizm klastra wysokiej dostępności HA, aby w przypadku awarii lub niedostępności serwera fizycznego hypervisora wirtualizacji uruchomione na nim wirtualne maszyny mogły zostać automatycznie uruchomione na innych serwerach fizycznych będących w tym klastrze.
14) Oprogramowanie musi posiadać funkcjonalność przenoszenia wirtualnych maszyn pomiędzy serwerami hypervisorami klastra bez utraty dostępu do usług uruchomionych na tych serwerach w trakcie wykonywania tej operacji.
15) Wraz z oprogramowaniem należy dostarczyć oprogramowanie do replikacji wirtualnych maszyn na nim uruchomionych.
16) Oprogramowanie musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów;
17) Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
18) Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).

11. **Licencje oprogramowania systemów operacyjnych serwerów**

Lp.	Wymagania minimalne
1	Oprogramowanie Systemu Operacyjnego: Microsoft Windows Server 2022 Standard - 2 szt. lub równoważne Licencja bezterminowa, umożliwia obsługę wszystkie fizycznych rdzeni procesora dla każdego z serwerów dostarczonych w niniejszym postępowaniu. Licencje połączeniowe Microsoft Windows Server 2022 Device CAL - 30 szt.

Opis równoważności dla Oprogramowania Systemu Operacyjnego:

Cechy równoważnego oprogramowania typu Microsoft Windows Server 2022 Standard Edition:

I. Zamawiający dopuszcza zastosowanie oprogramowania równoważnego, poprzez które należy rozumieć oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co oprogramowanie określone w opisie przedmiotu zamówienia.

II. Oprogramowanie Systemu Operacyjnego musi posiadać następujące cechy, funkcje i minimalne parametry:

1) Współpraca z procesorami o architekturze x86-64.
2) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3) Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) - natywnie lub z wykorzystaniem sterowników producenta sprzętu.
4) Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2016.
5) Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
6) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
9) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.

10) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
11) Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
12) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
13) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
14) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,
    - Pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.
    - Zdalna dystrybucja oprogramowania na stacje robocze.
    - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
    - PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - Dystrybucję certyfikatów poprzez http,
        - Konsolidację CA dla wielu lasów domeny,
        - Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen.
    - Szyfrowanie plików i folderów.
    - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    - Serwis udostępniania stron WWW.
    - Wsparcie dla protokołu IP w wersji 6 (IPv6).
    - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
17) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
18) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
19) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; W przypadku zaoferowania przez Wykonawcę rozwiązania

równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania.

20) Możliwość przystosowania sysytemu dla osób niepełnosprawnych (np. słabo widzących).

12. Oprogramowanie do zarządzania infrastrukturą

lp.	Wymagania minimalne
1.	**Wymagania ogólne:** Oprogramowanie oraz dokumentacja dostępna w języku polskim. Oprogramowanie posiadające konstrukcje modułową, zarządzane z jednej konsoli administracyjnej. Oprogramowanie posiada agentów, instalowanych na systemach operacyjnych klienckich, agenci muszą być kompatybilni z systemami operacyjnymi: Windows 8.1, Windows 10, Windows 11 Wbudowana funkcjonalność ochrony agenta przed usunięciem przez użytkownika. Oprogramowanie pozwala na równoległa prace wielu administratorów w tym samym czasie.
2.	**Zarządzanie siecią:** Funkcjonalności modułu zarządzania siecią: a) Budowanie interaktywnej mapy sieci oraz połączeń sieciowych b) Wykrywanie urządzeń sieciowych oraz serwisów poprzez skanowanie c) Wykrywanie ruchu na portach sieciowych routerów oraz przełączników sieciowych d) Obsługa pułapek SNMP v1/v2c/3 e) Możliwość dodawania nowych plików MIB f) Obsługa serwera syslog g) Monitorowanie serwisów sieciowych w tym: http/HTTPS/FTP/LDAP/IMAP h) Generowanie alarmów na podstawie dostępności urządzenia lub serwisu i) Monitorowanie systemów operacyjnych Windows poprzez WMI
3.	**Inwentaryzacja:** Funkcjonalności modułu inwentaryzacji: a) Automatyczne gromadzenie informacji o konfiguracji sprzętowej oraz oprogramowaniu stacji roboczych z zainstalowanym systemem operacyjnym Windows b) Możliwość zdalnego dostępu do plików użytkownika i ich modyfikacji/usuwania c) Audyt sprzętu oraz oprogramowania d) Inwentaryzacja oraz zarządzenie środkami trwałymi e) Możliwość generowania alarmów, podczas zmian sprzętowych

	f) Możliwość instalacji oprogramowania wykorzystując pakiety MSI
4.	**Obsługa użytkowników:** Funkcjonalności modułu do obsługi użytkowników: a) Integracja z domeną MS Active Directory b) Możliwość zablokowania uruchomionych aplikacji c) Blokowanie stron www d) Audyt czasu pracy e) Audyt używanych i nie używanych aplikacji f) Audyt informacji o odwiedzanych stronach www (w tym: czas wizyty, adres strony) g) Podgląd pulpitu zdalnego użytkownika h) Możliwość zrealizowania zrzutu ekranu użytkownika i) Audyt wydruków realizowanych przez użytkownika
5.	**Wsparcie dla użytkowników - HelpDesk** Funkcjonalności modułu dla wsparcia użytkowników a) Tworzenie zgłoszeń serwisowych oraz ich zarządzanie b) Możliwość przypisania zgłoszeń serwisowych do różnych administratorów c) Wbudowana baza zgłoszeń wraz z wyszukiwarką d) System raportowania e) Wewnętrzny komunikator w formie czatu f) Czat powinien umożliwiać przesyłanie plików g) Możliwość zdalnego połączenia do komputera h) Możliwość zdalnej instalacji oprogramowania i) Możliwość zdalnego zarządzania kontami lokalnych użytkowników Windows. **j)** Możliwość zdalnej edycji rejestru na komputerach z zainstalowanym agentem oprogramowania
6.	**Kontrola dostępu do danych** Funkcjonalności modułu dla kontroli dostępu do danych: a) Integracja z Windows Defender b) Możliwość zdalnego szyfrowania dysków c) Zestawienie informacji o urządzeniach podłączonych do danego komputera d) Zarządzanie uprawnieniami (odczyt, uruchamianie, zapis) dla urządzeń, komputerów i użytkowników e) Wykrywanie oprogramowania antywirusowego f) Audyt podłączeń i operacji na przenośnych urządzeniach oraz na udziałach sieciowych
7.	**Licencja:** Obsługa minimum 130 użytkowników.
8.	**Gwarancja:** 12 miesięcy gwarancji oraz wsparcia technicznego producenta.

Załącznik nr 10 do SWZ - Oświadczenie wykonawcy o spełnieniu przez przedmiot zamówienia wymaganych cech, parametrów, właściwości i funkcjonalności

Wymagania minimalne dla:

13. Klaster urządzeń UTM - 1 komplet

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	**Firewall**	
1.1	**Funkcjonalność Firewall**	
1.1.1	Firewall umożliwia zdefiniowanie co najmniej 3 stref bezpieczeństwa	
1.1.2	Firewall obsługuje protokoły dynamicznego routingu: RIP, OSPF i BGP	
1.1.3	Firewall obsługuje statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie	
1.1.4	Firewall obsługuje DHPC v6 na zewnętrznym interfejsie	
1.1.5	Firewall umożliwia pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP, jako bridge (transpartent mode) lub z tym samym adresem IP na wszystkich portach.	
1.1.6	Firewall ma możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu i dynamiczną selekcją drogi routowania.	
1.1.7	Firewall ma możliwość obsługi łącza zapasowego typu LTE	
1.1.8	Firewall obsługuje Dynamic DNS	
1.1.9	Firewall obsługuje translację adresów: statyczną, dynamiczną i 1-1	
1.1.10	Firewall obsługuje translację portów: PAT	
1.1.11	Firewall obsługuje IPSec NAT traversal	
1.1.12	Firewall obsługuje mechanizm policy-based NAT	
1.1.13	Firewall obsługuje VLAN 802.1Q	
1.1.14	Firewall zapewnia ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów	
1.1.15	Firewall obsługuje pracę jako serwer DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.	
1.1.16	Firewall umożliwia pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP	
1.1.17	Firewall umożliwia uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.	
1.1.18	Firewall umożliwia uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników.	

1.1.19	Firewall umożliwia transparentne uwierzytelnianie użytkowników przez Active Directory.	
1.1.20	Urządzenie umożliwia uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp.	
1.1.21	Urządzenie nie ogranicza ilości urządzeń, adresów IP czy użytkowników sieci wewnętrznej.	
1.1.22	Firewall zapewnia możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.	
1.1.23	Firewall zapewnia możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.	
1.1.24	Firewall obsługuje mechanizmy Protocol Anomaly Detection (PAD) dla najpopularniejszych protokołów.	
1.1.25	Firewall zapewnia wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.	
1.1.26	Firewall zapewnia ochronę z wykorzystaniem mechanizmów IPS.	
1.1.27	Firewall zapewnia ochronę antywirusową dla obsługiwanych protokołów.	
1.1.28	Firewall zapewnia możliwość filtrowania URL.	
1.1.29	Firewall zapewnia inspekcję ruchu szyfrowanego HTTPS.	
1.1.30	Firewall zapewnia ochronę przed niechcianą pocztą (AntySPAM).	
1.1.31	Firewall zapewnia rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.	
1.1.32	Urządzenie ma możliwość filtrowania treści według typu MIME.	
1.1.33	Urządzenie umożliwia sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji.	
1.1.34	Firewall udostępnia mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych.	
1.1.35	Firewall może pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site	
1.1.36	Firewall posiada mechanizm blokujący szkodliwe żądania DNS, zapewniając ochronę użytkowników końcowych przed atakami typu phishing.	
1.2	**Wydajność firewall**	
1.2.1	Firewall zapewnia obsługę na poziomie minimalnym: **5,7Gbps** dla pracy w trybie firewall (UDP 1518), **1,15Gbps** dla pracy w trybie UTM (pełny skan)	

1.2.2	Firewall obsługuje minimum **3 400 000** jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną **34 000** nowych połączeń na sekundę.	
1.2.3	Ilość obsługiwanych sieci VLAN: minimum **100.**	
1.2.4	Minimalna ilość fizycznych portów: - 8 portów 1Gbps RJ45 - 2 porty 10 Gbps SFP+	
2	**VPN**	
2.1	**Funkcje VPN**	
2.1.1	Urządzenie obsługuje połączenia VPN site-to-site z wykorzystaniem IPSec oraz TLS.	
2.1.2	Urządzenie w zakresie IPSec site-to-site VPN współpracuje z rozwiązaniami innych producentów.	
2.1.3	Rozwiązanie wspiera mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.	
2.1.4	Rozwiązanie wspiera mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert.	
2.1.5	Wsparcie dla Dead Peer Detection (DPD).	
2.1.6	Urządzenie obsługuje IKEv1 i IKEv2	
2.1.7	Urządzenie obsługuje Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web.	
2.1.8	Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP.	
2.1.9	Urządzenie zapewnia możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.	
2.1.10	Urządzenie obsługuje statyczne i dynamiczne (routowane) połączenia VPN do dostawców chmury obliczeniowej (AWS i MS Azure).	
2.1.11	Urządzenie obsługuje połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP.	
2.1.12	Połączenia client-to-site są możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.	
2.1.13	Dla połączeń IPSec client-to-site jest możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu.	
2.1.14	Urządzenie zapewnia funkcję portalu dostępowego chronionego przez szyfrowanie https (TLS).	
2.2	**Wydajność VPN**	
2.2.1	Przepustowość IPSec VPN (UDP 1518) nie mniejsza niż **2,3Gbps**	
2.2.2	Obsługa nie mniej niż: **70** tuneli IPSec site-to-site	
2.2.3	Obsługa nie mniej niż: **70** tuneli client-to-site	
3	**Filtrowanie zawartości URL**	

3.1	Urządzenie umożliwia filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.	
3.2	Funkcjonalność filtrowania zawartości daje możliwość filtrowania stron według minimalnie 120 kategorii.	
3.3	Rozwiązanie pozwala na tworzenie białych list wyjątków dla filtrowania zawartości.	
3.4	Baza zawartości URL jest dostępna on-line lub do ściągnięcia i zainstalowania miejscowo.	
3.5	Funkcja filtruje treści w wielu językach, w tym w języku polskim.	
3.6	Filtrowanie obsługuje również protokół https.	
3.7	Urządzenie umożliwia wyłączenie inspekcji https dla wybranych kategorii stron www.	
3.8	System kategoryzacji stron posiada kategorie: Command&control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware.	
4	**Kontrola aplikacyjna**	
4.1	System kontroli aplikacyjnej rozpoznaje aplikacje oraz kategorie aplikacji.	
4.2	Aplikacje są rozpoznawane w oparciu o analizę ruchu a nie przez porty i protokoły.	
4.3	Ilość rozpoznawanych aplikacji nie mniejsza niż 1800.	
4.4	W ramach konkretnej aplikacji system umożliwia kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe).	
4.5	Kontrola aplikacyjna rozpoznaje co najmniej aplikacje: Tor, CryptoAdmin, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.	
5	**Antywirus**	
5.1	System ma możliwość uruchomienia co najmniej 2 skanerów antywirusowych.	
5.2	Aktualizacja plików sygnatur antywirusowych może odbywać się automatycznie.	
5.3	Aktualizacja plików sygnatur antywirusowych odbywa się nie rzadziej niż co 12 godzin.	
5.4	Antywirus ma możliwość przeprowadzania kwarantanny e-mail.	
5.5	Jeden ze skanerów antywirusowych bazuje na mechanizmach bezsygnaturowych.	
5.6	Rozwiązanie ma możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen.	
5.7	Wykrywanie i blokowanie spyware'u.	
5.8	Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.	
5.9	Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.	

5.10	Przepustowość AV w urządzeniu nie mniejsza niż **1,4Gbps**	
5.11	W celu realizacji ochrony z wykorzystaniem 2 skanerów antywirusowych Zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia.	
6	**Antyspam**	
6.1	Antyspam zapewnia możliwość kwarantanny e-mail.	
6.2	Antyspam posiada zintegrowaną antywirusową analizę spamu.	
6.3	Rozwiązanie umożliwia blokowanie spamu w wielu językach w tym w języku polskim.	
6.4	Możliwość blokowania spamu opartego na obrazach graficznych.	
7	**IPS**	
7.1	Automatyczna aktualizacja sygnatur IPS.	
7.2	IPS ma możliwość dokonywania analizy warstwy aplikacji, a także ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.	
7.3	Automatyczne blokowanie znanych źródeł ataków.	
7.4	System pozwala na blokowanie ataków typu DoS i DDoS.	
7.5	Przepustowość IPS (pełny skan) w urządzeniu nie mniejsza niż **1,3Gbps**.	
8	**Ochrona przed phishingiem**	
8.1	System zapewnia dedykowaną (poza ochroną przed SPAMem) ochronę przed phishingiem.	
8.2	System blokuje możliwość dostępu do spreparowanych stron.	
8.3	System blokuje dostęp niezależnie od użytego protokołu czy portu komunikacyjnego.	
8.4	Zablokowanie dostępu jest odpowiednio notyfikowane użytkownikowi, którego dotyczy, niezależnie od logów i raportów.	
8.5	System chroni przed nadużyciem protokołu DNS.	
9	**Zarządzanie**	
9.1	Administracja urządzenia jest możliwa poprzez graficzny interfejs zarządzania w czasie rzeczywistym.	
9.2	Urządzenie umożliwia zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH.	
9.3	Urządzenie umożliwia zarządzanie za pomocą wbudowanego interfejsu www.	
9.4	Interfejs WWW do zarządzania urządzeniem ma właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.	
9.5	Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów.	
9.6	Rozwiązanie umożliwia wysyłanie alarmów przez SNMP lub e-mail.	

9.7	Rozwiązanie umożliwia edytowanie polityk bezpieczeństwa w trybie online.	
9.8	System zapewnia możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.	
9.9	Rozwiązanie wspiera instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.	
9.10	System posiada metodę porównywania różnych wersji konfiguracji.	
9.11	Obsługa różnych ról administratorów.	
9.12	Możliwość monitorowania logów ruchu w czasie rzeczywistym.	
9.13	System posiada możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty).	
9.14	Urządzenie umożliwia zarządzanie bezprzewodowymi punktami dostępowymi.	
9.15	System zarządzania zapewnia korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów.	
9.16	System zarządzania posiada graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop.	
10	**Dzienniki i raporty**	
10.1	Rozwiązanie umożliwia zbieranie i przechowywanie dzienników i raportów.	
10.2	Rozwiązanie umożliwia przesyłanie logów do co najmniej 2 serwerów dziennika.	
10.3	Dzienniki transmisji mogą być szyfrowane.	
10.4	Rozwiązanie zapewnia narzędzie graficznej analizy logów.	
10.5	Rozwiązanie udostępnia narzędzie analizy całości ruchu.	
10.6	Rozwiązanie udostępnia narzędzie analizy incydentów bezpieczeństwa.	
10.7	Rozwiązanie nie narzuca ograniczeń co do czasu przechowywania logów czy rozmiaru bazy danych.	
10.8	Rozwiązanie posiada minimum 90 predefiniowanych typów raportów.	
10.9	Predefiniowane raporty mają możliwość dopasowania do instytucji użytkującej rozwiązanie.	
10.10	System ma możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.	
10.11	System jest w stanie zautomatyzować generowanie raportów i ma możliwość wysyłania tych sprawozdań pocztą e-mail.	
10.12	Jest zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.	

10.13	System raportowania jest wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników.	
10.14	System wspiera automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną.	
10.15	Rozwiązanie umożliwia kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.	
10.16	System umożliwia pseudoanonimizację użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów.	
10.17	System zapewnia wizualizację, opisującą w trybie graficznym stan przepustowości systemu.	
11.	**Zero Day / Zaawansowana Detekcja Malware**	
11.1	Funkcja zaawansowanego wykrywania szkodliwego oprogramowania w tym samym urządzeniu.	
11.2	Zaawansowany Malware jest wykrywany przez uruchomienie plików w chmurze przy użyciu emulacji pełnego systemu.	
11.3	Zaawansowana Detekcja Malware obsługuje wszystkie pliki wykonywalne systemu Windows, pliki zip, pdf, Microsoft Office, oraz pliki Android APK.	
11.4	Szczegółowe raporty oraz informacje wskazujące na powody, dla których plik jest uważany za zaawansowany Malware.	
11.5	W celu realizacji ochrony „Zero Day" zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia.	
12.	**Architektura**	
12.1	Rozwiązanie musi być dostarczone w formie klastra dwóch fizycznych urządzeń z licencjami umożliwiającymi ich pracę co najmniej w trybie klastra Aktywny/Pasywny (ang. Active/Passive).	
12.1	Urządzenia wchodzące w skład klastra są urządzeniami tego samego producenta i modelu, oraz każde z tych urządzeń spełnia minimalne techniczne parametry wydajnościowe określone przez niniejszą specyfikację.	
13.	**Gwarancja**	
13.1	Okres wsparcia technicznego - minimum **3 lata**.	
13.2	Urządzenie dostarczone ze wszystkimi licencjami/subskrypcjami umożliwiającymi uzyskanie funkcjonalności wymienionymi w niniejszej specyfikacji. Długość trwania licencji/subskrypcji nie może być krótsza niż okres wsparcia technicznego.	
13.3	Możliwość zgłaszania incydentów za pomocą e-mail, portalu - 24 godziny na dobę 7 dni w tygodniu.	
13.4	Wymiana urządzenia w przypadku zdiagnozowania awarii uniemożliwiającej funkcjonowanie, następowała na następny	

	dzień roboczy od zdiagnozowania awarii (advanced hardware replacement NBD).	

14. Przełączniki LAN Typ 1 - 2 szt.

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Typ Obudowy: Obudowa do montażu w szafie RACK 19" - 1U wraz z zestawem montażowym.	
2	Porty: - 24 x 10 Gigabit Ethernet SFP+, - 2 x 40 Gigabit Ethernet QSFP+, Porty QSFP+ powinny mieć możliwość rozszycia w celu konfiguracji 4x10GbE - 1 x RJ45 console/management port (RS232), - 1 x RJ45 management port, - 1 x USB 2.0 type A, Umożliwia zestawienie stosu portami/magistralami minimum, Full Duplex 40GbE (do min. 2 urządzeń).	
3	Wydajność: - Przepustowość przełącznika minimum 620Gb/s. - Wydajność przełączania minimum 460Mpps. - Obsługa minimum 32,000 adresów MAC. - Bufor pakietów minimum 1,5MB - Taktowanie procesora: 1GHz - Pamięć RAM 512MB	
4	Zasilanie: Zasilanie 230V AC	
5	Funkcje i protokoły: - Obsługuje następujące protokoły drzewa rozpinającego: • 802.1D - STP • 802.1w - RSTP • 802.1s - MSTP - Obsługuje jeden z protokołów do tworzenia wirtualnych nadmiarowych bram sieciowych np. (VRRP lub HSRP), - Obsługa multicastów z wykorzystaniem protokołów: • IGMP, • IGMP Snooping, - Możliwość monitorowania ruchu na porcie (Port Mirroring), - Możliwość agregacji połączeń z wykorzystaniem protokołu LACP - IEEE 802.3ad, - Obsługuje następujące protokoły odnajdywania urządzeń w sieci: • LLDP, • LLDP-MED, - Obsługuje następujące protokoły autoryzacji: • TACACS+, • RADIUS, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,	
6	Zarządzanie:	

	- Posiada tekstowy interfejs zarządzania z podpowiedziami kontekstowymi, - Posiada tekstowy plik konfiguracyjny możliwy do wyeksportowania, edytowania poza urządzeniem i ponownego zaimportowania do urządzenia, - Możliwość zarządzania urządzeniem z wykorzystaniem protokołów SSHv2 oraz TELNET, - Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI), - Umożliwia bezpośredni dostęp do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji, - Obsługa wysyłania powiadomień o zdarzeniach z użyciem protokołów SNMPv1, SNMPv2c oraz SNMPv3, - Umożliwia przesyłanie dzienników zdarzeń z wykorzystaniem protokołu SYSLOG, - Obsługuje synchronizację czasu systemowego z użyciem protokołów SNTP lub NTP, - Możliwość konfiguracji pracy w trybie klienta DNS.	
7	Wyposażenie: Niezbędne akcesoria w celu zbudowania nadmiarowej konstrukcji wykorzystując porty o przepustowości 40GbE	
8	Gwarancja: Oferowane urządzenie jest objęte co najmniej 3-letnim wsparciem (gwarancją) producenta lub partnera na terenie Polski. Kontakt ze wsparciem w dni robocze, czas reakcji w miejscu instalacji sprzętu następny dzień roboczy.	

15. Przełączniki LAN Typ 2 - 3 szt.

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Typ Obudowy: Obudowa do montażu w szafie RACK 19" - 1U wraz z zestawem montażowym.	
2	Porty: - 48 x 1 Gigabit Ethernet 1000BASE-T (RJ45), - 2 x 1 Gigabit Ethernet SFP, - 2 x 10 Gigabit Ethernet SFP+, - 1 x RJ45 console/management port (RS232),	
3	Wydajność: - Przepustowość przełącznika minimum 135Gbps. - Wydajność przełączania minimum 100Mpps.	
4	Zasilanie: Zasilanie 230V AC	
5	Funkcje i protokoły: - Obsługuje następujące protokoły drzewa rozpinającego: • 802.1D - STP • 802.1w - RSTP -- Możliwość agregacji połączeń z wykorzystaniem protokołu LACP - IEEE 802.3ad, - Obsługa protokołu, odnajdywania urządzeń w sieci: • LLDP, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,	
6	Zarządzanie: - Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI), - Możliwość bezpośredniego dostępu do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji, - Obsługa synchronizacji czasu systemowego z użyciem protokołów SNTP lub NTP,	
7	Gwarancja: Oferowane urządzenie jest objęte co najmniej rocznym wsparciem producenta lub partnera na terenie Polski. Kontakt ze wsparciem w dni robocze.	

16. Przełączniki LAN Typ 3 - 2 szt.

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Typ Obudowy: Obudowa do montażu w szafie RACK 19" - 1U wraz z zestawem montażowym.	
2	Porty: - 16 x 1 Gigabit Ethernet 1000BASE-T (RJ45) PoE+, - 2 x 1 Gigabit Ethernet SFP, - 1 x RJ45 console/management port (RS232),	
3	Wydajność: - Przepustowość przełącznika minimum 35Gbps. - Wydajność przełączania minimum 25Mpps. - Obsługa minimum 16000 adresów MAC.	
4	Zasilanie: Zasilanie 230V AC	
5	Funkcje i protokoły: - Obsługuje następujące protokoły drzewa rozpinającego: • 802.1D - STP • 802.1w - RSTP -- Możliwość agregacji połączeń z wykorzystaniem protokołu LACP - IEEE 802.3ad, - Obsługa protokołu, odnajdywania urządzeń w sieci: • LLDP, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,	
6	Zarządzanie: - Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI), - Możliwość bezpośredniego dostępu do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji, - Obsługa synchronizacji czasu systemowego z użyciem protokołów SNTP lub NTP,	
7	Gwarancja: Oferowane urządzenie jest objęte co najmniej rocznym wsparciem producenta lub partnera na terenie Polski. Kontakt ze wsparciem w dni robocze.	

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

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Urządzenie posiada minimum dwa kontrolery obsługujące dostęp do dysków, pracujące w trybie Active/Active. Moduł kontrolerów umożliwia instalację minimum 24 dysków 2,5". Urządzenie umożliwia instalację w szafach RACK 19" i będzie dostarczone z niezbędnym wyposażeniem do wykonania takiej instalacji.	
2	Urządzenie posiada możliwość instalacji dodatkowych modułów dyskowych pozwalających na instalację w danym module minimum: - 24 szt. dysków 2,5" w obudowie max 2U, - 15 szt. dysków 3,5" w obudowie max 4U.	
3	Urządzenie jest wyposażone w system redundantnego zasilania i chłodzenia, który gwarantuje możliwość pracy i utrzymanie bez przerw funkcjonalności urządzenia w tym działanie pamięci cache.	
4	Urządzenie zapewnia w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez czas nieograniczony.	
5	Urządzenie umożliwia utworzenie wolumenu LUN o rozmiarze minimum 64TB i systemu plików minimum 64TB.	
6	Urządzenie będzie dostarczone w konfiguracji pozwalającej na obsługę minimum 128 GB pamięci podręcznej, obsługującej jednocześnie odczyty i zapisy. Pamięć będzie dostępna jednocześnie dla wszystkich wolumenów i kontrolerów macierzy. Włączenie lub wyłączenie pamięci podręcznej nie wymaga operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych.	
7	Urządzenie jest wyposażone w następującą minimalną liczbę portów do podłączania hostów (porty Front-end): - cztery porty, 10 Gbps iSCSI SFP+.	
8	Urządzenie wspiera architekturę bezpośredniego podłączania serwerów do macierzy (bez pośrednictwa przełączników SAN) przy pomocy protokołów FC i 10GbE iSCSI (jest to potwierdzone w oficjalnych dokumentach producenta urządzenia).	

9	Urządzenie umożliwia zastosowanie dysków SSD, HDD 10k i HDD 7,2k RPM. Wszystkie dyski 2,5" i 3,5" są wyposażone w interfejsy SAS 12Gbps lub wydajniejsze.	
10	Urządzenie jest wyposażona w dyski posiadające podwójne interfejsy.	
11	Urządzenie posiada funkcjonalność globalnych dysków zapasowych lub globalnej przestrzeni Hot-Spare. W wypadku zastosowania technologii globalnej przestrzeni Hot-Spare, wymagane jest dostarczenie o 10% większej surowej przestrzeni dyskowej niż wymagana w punkcie 13, dla każdego rodzaju zaoferowanych dysków (dotyczy również dostarczanych ewentualnych dodatkowych modułów dyskowych).	
12	Urządzenie umożliwia rozbudowę do co najmniej 480 napędów dyskowych w obrębie pojedynczego urządzenia, bez potrzeby wymiany kontrolerów macierzy dostarczonych w ramach niniejszego postępowania.	
13	Pojemność surowa (ang. RAW) macierzy: - minimum 2,3 TB, na minimum 6 dyskach SSD 12Gbps, 2,5". - minimum 13 TB, na minimum 11 dyskach SAS 12Gbps, 2,5", 10K RPM.	
14	Połączenia między dyskami, a kontrolerami są wykonane w technologii SAS 12Gbps lub wydajniejszej.	
15	Urządzenie umożliwia równoczesną obsługę wielu poziomów RAID, minimum RAID 10, 5, 6.	
16	Urządzenie posiada funkcjonalność tworzenia lokalnych kopii migawkowych wewnętrznymi mechanizmami macierzy w technologii "redirect on write". Dopuszcza się, aby macierz wykonywała lokalne kopie migawkowe z wykorzystaniem innych technologii, w takim wypadku wymaga się dostarczenia dodatkowych: - minimum 4 dysków SSD każdy o pojemności minimum 1,6TB 12Gbps, 2,5", DWPD minimum 3. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.	
17	Urządzenie obsługuje minimum 64 kopii migawkowych per dysk logiczny LUN oraz 64 kopii per system plików.	

	Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.	
18	Przepełnienie przestrzeni dla kopii migawkowych nie powoduje błędów zapisu na przestrzeń produkcyjną.	
19	W przypadku odtworzenia danych z dowolnej kopii migawkowej, urządzenie pozwala na poprawne zachowanie także wcześniejszych jak i późniejszych snapshotów, z zachowaniem możliwości kolejnego odtworzenia danych ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu.	
20	Urządzenie obsługuje lun masking, lun mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy.	
21	Urządzenie jest wyposażone w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż" (limit) dla następujących parametrów dostępu do dysku logicznego: a. Ilość operacji na sekundę (IOPS), b. Przepustowość (MB/s). Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.	
22	Urządzenie umożliwia replikację synchroniczną i asynchroniczną danych blokowych oraz replikację asynchroniczną dla danych plikowych pomiędzy dwiema macierzami. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.	
23	Urządzenie posiada funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych, w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje są wykonywane automatycznie bez udziału administratora. Pojedynczy migrowany obszar nie może być większy niż 256MB. Migracja danych odbywa się bez przerywania dostępu do danych od strony hostów i aplikacji. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.	

24	Funkcjonalność tieringu jest możliwa pomiędzy wszystkimi typami stosowanych dysków (SSD, SAS, NLSAS).	
25	Urządzenie umożliwia automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.	
26	Urządzenie zapewnia jednoczesne zastosowanie różnych trybów protekcji RAID dla różnych typów dysków fizycznych obsługujących pojedynczy dysk logiczny objęty mechanizmem tieringu.	
27	Urządzenie zapewniać mechanizm Thin Provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała przydzielonej pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.	
28	Urządzenie umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation).	
29	Urządzenie oferuje funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.	
30	Urządzenie wspiera wirtualizację serwerową w zakresie: VMware: VAAI, VASA, VVols 2.0, integracja macierzy z VMware vRealize Operations oraz Hyper-V: Offloaded Data Transfer (ODX) and Offload Copy for File.	
31	Urządzenie obsługuje co najmniej protokoły blokowe: FC i iSCSI, oraz protokoły plikowe: NFS v4.1(MS Windows 2016 i 2019), NFSv3, SMB 2, SMB 3 i VMware VVols (Virtual Volumes) 2.0.	
32	Urządzenie jest zgodne z normami UE i przeznaczone do sprzedaży na rynek UE. Urządzenie posiada certyfikat CE.	
33	Dostarczone urządzenie jest fabrycznie nowe, nieregenerowane i wyprodukowane nie wcześniej niż w pierwszym półroczu 2023 r., pochodzi z oficjalnego kanału sprzedaży producenta na teren UE.	
34	Urządzenie oraz jego oprogramowanie wewnętrzne jest objęte co najmniej 3-letnim wsparciem producenta (gwarancją). Kontakt ze wsparciem w dni robocze, czas reakcji w miejscu instalacji sprzętu: następny dzień roboczy.	

	W okresie opieki wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Serwis zawiera usługę pozostawiania bez opłat u Zamawiającego uszkodzonych dysków w okresie obowiązywania gwarancji. Możliwość zgłaszania awarii poprzez linię telefoniczną producenta obsługiwaną w języku polskim.	
35	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta oraz, że uszkodzone dyski w przypadku wymiany z powodu awarii w okresie obowiązywania gwarancji, pozostaną własnością Zamawiającego. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.	

18. Serwery - 2 szt.

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Obudowa typu Rack o wysokości maksymalnie 1U. Komplet wysuwanych szyn i organizer okablowania, umożliwiający montaż w szafie rack i wysuwanie do celów serwisowych.	
2	Płyta główna - pozwalająca na zainstalowanie minimum dwóch procesorów zaprojektowana przez producenta węzła i oznaczona jego znakiem firmowym.	
3	Chipset - dedykowany przez producenta procesora do pracy w systemach dwuprocesorowych.	
4	Procesory - zainstalowane dwa procesory maksimum 8-rdzeniowe klasy x86 uzyskujące w teście „SPECrate2017_fp_base" dostępnym na stronie www.spec.org dla konfiguracji z dwoma procesorami wynik min. 147 punktów, dla oferowanych procesorów. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanych procesorów. Maksymalna liczba rdzeni procesora ograniczona przez licencjonowanie zastosowanego w projekcie oprogramowania.	
5	Pamięć RAM - minimum 192GB. Płyta główna obsługuje do minimum 1TB pamięci RAM dla konfiguracji dwu-procesorowej. Pojemność zastosowanych kości pamięci RAM min. 16 GB.	
6	Zabezpieczenia pamięci RAM - Memory Mirror.	
7	Gniazda PCI - minimum trzy sloty PCIe w tym minimum jeden x16.	
8	Interfejsy sieciowe: - minimum 4 porty typu Ethernet 10/25Gbps SFP28, - minimum 2 porty typu Ethernet 1Gbps RJ45.	
9	Przestrzeń dyskowa: Dedykowany fizyczny moduł pozwalający na konfigurację nadmiarowej przestrzeni dyskowej (min. RAID 1) zrealizowanej z wykorzystaniem min.	

	dwóch nośników FLASH i/lub SSD o pojemności 240GB każdy, pozwalający na instalację i uruchamianie systemu operacyjnego serwera.	
10	Wbudowane porty: - minimum 2 porty USB 2.0, - minimum 1 port USB 3.0, - 1 port RJ45 dedykowany do zarządzania, - 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym).	
11	Video - zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024	
12	Wentylatory - redundantne	
13	Zasilacze - redundantne, Hot-Plug minimum 750W.	
14	Karta Zarządzania - niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność: - komunikacja poprzez interfejs RJ45, - podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging, - wbudowana diagnostyka, - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń, - monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym, - lokalna oraz zdalna konfiguracja serwera, - wsparcie dla IPv4 i IPv6, - możliwość zdalnego dostępu do konsoli graficznej, zainstalowanego systemu operacyjnego serwera.	
15	Urządzenie wyprodukowane zgodnie z normą ISO-9001:2008 oraz ISO-14001. Urządzenie zgodne z normami UE i przeznaczone na rynek UE, posiada certyfikat CE.	
16	Dostarczone urządzenia fabrycznie nowe, nieregenerowane i wyprodukowane nie wcześniej niż w drugim półroczu 2022 r., pochodzą z oficjalnego kanału sprzedaży producenta na teren Polski.	
17	Oferowane urządzenie objęte co najmniej 3-letnim wsparciem producenta sprzętu. Kontakt ze wsparciem w dni robocze, czas reakcji w miejscu instalacji sprzętu: następny dzień roboczy.	

	Możliwość sprawdzenia na stronie WWW producenta serwera, prowadzonej w języku polskim, po podaniu numeru seryjnego urządzenia, minimum: - okresu oraz poziomu gwarancji, - zainstalowanych komponentów (w tym m.in. procesorów, pamięci RAM, dysków, zasilaczy i kart komunikacyjnych). Adres strony WWW producenta na której można sprawdzić powyższe dane musi być podany w złożonej ofercie.	
18	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.	

19. Zasilacz awaryjny UPS Typ 1 - 1 szt.

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Typ obudowy i wymiary maksymalne: - wolnostojący, - wymiary maksymalne (w mm): 400x800x1400	
2	Typ urządzenia: 3-fazowy, zintegrowana bateria,	
3	Moc urządzenia: Minimum 15 kVA, 13,5 kW,	
4	Gniazdo zasilania (wejścia): 400V 3-fazy+N	
5	Gniazda wyjściowe: - 400V 3-fazy + N - 230V 1-faza + N	
6	Czas podtrzymania bateryjnego dla mocy nominalnej 12kW: minimum 15 minut.	
7	Zewnętrzny BYPASS serwisowy	
8	Wskaźnik graficzny wyświetlający stan urządzenia, informujący minimum o: - Trybie pracy (normalny/z użyciem baterii) - Parametrach zasilania na wejściu - Stanie naładowania baterii - Poziomie obciążenia - Wystąpieniu alarmu/awarii	
9	Urządzenie musi być wyposażone w port komunikacyjny RJ-45 umożliwiający: - działanie z prędkością min. 10/100 Mbps - Obsługę adresacji IPv4 oraz IPv6 - obsługę protokołów: • HTTP/HTTPS • DHCP • SNMP (v1,v2c,v3) • SMTP (z obsługą min. STARTTLS) • SSH • SYSLOG • FTP • SCP • NTP	
10	Zamawiający przygotuje, zgodnie z zaleceniami dostarczanego UPS: - okablowanie, - rozdzielnie elektryczną, - zabezpieczenia pomiędzy rozdzielnią UPS - zasilaczem UPS, rozdzielnicą odbiorów.	
11	Oferowane urządzenie musi być objęte co najmniej 2-letnią gwarancją producenta.	

20. Zasilacz awaryjny UPS Typ 2 - 1 szt.

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Typ obudowy i wymiary maksymalne: - wolnostojący, - wymiary maksymalne (w mm): 450x850x1450	
2	Typ urządzenia: 3-fazowy, zintegrowana bateria,	
3	Moc urządzenia: Minimum 20 kVA, 18 kW,	
4	Gniazdo zasilania (wejścia): 400V 3-fazy+N	
5	Gniazda wyjściowe: - 400V 3-fazy + N - 230V 1-faza + N	
6	Czas podtrzymania bateryjnego dla mocy nominalnej 18kW: minimum 15 minut.	
7	Zewnętrzny BYPASS serwisowy	
8	Wskaźnik graficzny wyświetlający stan urządzenia, informujący minimum o: - Trybie pracy (normalny/z użyciem baterii) - Parametrach zasilania na wejściu - Stanie naładowania baterii - Poziomie obciążenia - Wystąpieniu alarmu/awarii	
9	Urządzenie musi być wyposażone w port komunikacyjny RJ-45 umożliwiający: - działanie z prędkością min. 10/100 Mbps - Obsługę adresacji IPv4 oraz IPv6 - obsługę protokołów: • HTTP/HTTPS • DHCP • SNMP (v1,v2c,v3) • SMTP (z obsługą min. STARTTLS) • SSH • SYSLOG • FTP • SCP • NTP	
10	Zamawiający przygotuje, zgodnie z zaleceniami dostarczanego UPS: - okablowanie, - rozdzielnie elektryczną, - zabezpieczenia pomiędzy rozdzielnią UPS - zasilaczem UPS, rozdzielnicą odbiorów.	
11	Oferowane urządzenie musi być objęte co najmniej 2-letnią gwarancją producenta.	

21. Wyposażenie dodatkowe

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Moduły SFP+: - 20 sztuk SFP+ LR 10Gbs 1310nm LC SMF 10km, kompatybilne z dostarczanymi przełącznikami sieciowymi. - 6 sztuk SFP LR 1Gbps 1310nm LC SMF 20km, kompatybilne z dostarczanymi przełącznikami sieciowymi,	
2	Kable DAC: - 14 szt. DAC SFP+ to SFP+ 10GbE, 3m.	

22. **Oprogramowanie do wirtualizacji serwerów**

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Oprogramowanie do wirtualizacji serwerów: VMware vSphere 8 Essentials Plus Kit - 1 szt. lub równoważne. Licencje dostarczone wraz z minimum rocznym wsparciem technicznym. Wsparcie techniczne umożliwia zgłaszanie problemów w trybie co najmniej 5 dni/8 godz. Możliwość pobierania nowych wersji i poprawek w całym okresie trwania oferowanego wsparcia.	

Opis równoważności dla Oprogramowania Systemu Wirtualizacji Serwerów:

Cechy równoważnego oprogramowania typu VMware vSphere Essentials Plus Kit:

III. Pakiet oprogramowania systemu wirtualizacyjnego będzie przeznaczony do wirtualizacji serwerów. Oprogramowanie do wirtualizacji serwerów będzie przeznaczone na klaster wirtualizacyjny składający się docelowo z maksymalnie trzech serwerów dwuprocesorowych.

IV. Oprogramowanie Wirtualizacji Serwerów musi posiadać następujące cechy i funkcjonalności:

1) Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
2) Oprogramowanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług;
3) Oprogramowanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
4) Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2022, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 8.1, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Debian GNU/Linux, CentOS w tym dostarczone systemy operacyjne.
5) Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
6) Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej.
7) Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na

dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.

8) Oprogramowanie musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
9) Oprogramowanie musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
10) Oprogramowanie oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
11) Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
12) Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
13) Oprogramowanie musi zapewniać odpowiednią nadmiarowość i posiadać mechanizm klastra wysokiej dostępności HA, aby w przypadku awarii lub niedostępności serwera fizycznego hypervisora wirtualizacji uruchomione na nim wirtualne maszyny mogły zostać automatycznie uruchomione na innych serwerach fizycznych będących w tym klastrze.
14) Oprogramowanie musi posiadać funkcjonalność przenoszenia wirtualnych maszyn pomiędzy serwerami hypervisorami klastra bez utraty dostępu do usług uruchomionych na tych serwerach w trakcie wykonywania tej operacji.
15) Wraz z oprogramowaniem należy dostarczyć oprogramowanie do replikacji wirtualnych maszyn na nim uruchomionych.
16) Oprogramowanie musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów;
17) Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
18) Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).

23. **Licencje oprogramowania systemów operacyjnych serwerów**

Lp.	Wymagania minimalne	Spełnia Tak/Nie
1	Oprogramowanie Systemu Operacyjnego: Microsoft Windows Server 2022 Standard - 2 szt. lub równoważne Licencja bezterminowa, umożliwia obsługę wszystkie fizycznych rdzeni procesora dla każdego z serwerów dostarczonych w niniejszym postępowaniu. Licencje połączeniowe Microsoft Windows Server 2022 Device CAL - 30 szt.	

Opis równoważności dla Oprogramowania Systemu Operacyjnego:

Cechy równoważnego oprogramowania typu Microsoft Windows Server 2022 Standard Edition:

III. Zamawiający dopuszcza zastosowanie oprogramowania równoważnego, poprzez które należy rozumieć oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co oprogramowanie określone w opisie przedmiotu zamówienia.

IV. Oprogramowanie Systemu Operacyjnego musi posiadać następujące cechy, funkcje i minimalne parametry:

1) Współpraca z procesorami o architekturze x86-64.
2) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3) Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) - natywnie lub z wykorzystaniem sterowników producenta sprzętu.
4) Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2016.
5) Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
6) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

9) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
10) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
11) Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
12) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
13) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
14) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,
    - Pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.
    - Zdalna dystrybucja oprogramowania na stacje robocze.
    - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
    - PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - Dystrybucję certyfikatów poprzez http,
        - Konsolidację CA dla wielu lasów domeny,
        - Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen.
    - Szyfrowanie plików i folderów.
    - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    - Serwis udostępniania stron WWW.
    - Wsparcie dla protokołu IP w wersji 6 (IPv6).
    - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
17) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
18) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

19) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania.
20) Możliwość przystosowania systemu dla osób niepełnosprawnych (np. słabo widzących).

24. Oprogramowanie do zarządzania infrastrukturą

lp.	Wymagania minimalne	Spełnia Tak/Nie
1.	**Wymagania ogólne:** Oprogramowanie oraz dokumentacja dostępna w języku polskim. Oprogramowanie posiadające konstrukcje modułową, zarządzane z jednej konsoli administracyjnej. Oprogramowanie posiada agentów, instalowanych na systemach operacyjnych klienckich, agenci muszą być kompatybilni z systemami operacyjnymi: Windows 8.1, Windows 10, Windows 11 Wbudowana funkcjonalność ochrony agenta przed usunięciem przez użytkownika. Oprogramowanie pozwala na równoległa prace wielu administratorów w tym samym czasie.	
2.	**Zarządzanie siecią:** Funkcjonalności modułu zarządzania siecią: j) Budowanie interaktywnej mapy sieci oraz połączeń sieciowych k) Wykrywanie urządzeń sieciowych oraz serwisów poprzez skanowanie l) Wykrywanie ruchu na portach sieciowych routerów oraz przełączników sieciowych m) Obsługa pułapek SNMP v1/v2c/3 n) Możliwość dodawania nowych plików MIB o) Obsługa serwera syslog p) Monitorowanie serwisów sieciowych w tym: http/HTTPS/FTP/LDAP/IMAP q) Generowanie alarmów na podstawie dostępności urządzenia lub serwisu r) Monitorowanie systemów operacyjnych Windows poprzez WMI	
3.	**Inwentaryzacja:** Funkcjonalności modułu inwentaryzacji: g) Automatyczne gromadzenie informacji o konfiguracji sprzętowej oraz oprogramowaniu stacji roboczych z zainstalowanym systemem operacyjnym Windows h) Możliwość zdalnego dostępu do plików użytkownika i ich modyfikacji/usuwania i) Audyt sprzętu oraz oprogramowania j) Inwentaryzacja oraz zarządzenie środkami trwałymi k) Możliwość generowania alarmów, podczas zmian sprzętowych	

	l) Możliwość instalacji oprogramowania wykorzystując pakiety MSI	
4.	**Obsługa użytkowników:** Funkcjonalności modułu do obsługi użytkowników: j) Integracja z domeną MS Active Directory k) Możliwość zablokowania uruchomionych aplikacji l) Blokowanie stron www m) Audyt czasu pracy n) Audyt używanych i nie używanych aplikacji o) Audyt informacji o odwiedzanych stronach www (w tym: czas wizyty, adres strony) p) Podgląd pulpitu zdalnego użytkownika q) Możliwość zrealizowania zrzutu ekranu użytkownika r) Audyt wydruków realizowanych przez użytkownika	
5.	**Wsparcie dla użytkowników - HelpDesk** Funkcjonalności modułu dla wsparcia użytkowników k) Tworzenie zgłoszeń serwisowych oraz ich zarządzanie l) Możliwość przypisania zgłoszeń serwisowych do różnych administratorów m) Wbudowana baza zgłoszeń wraz z wyszukiwarką n) System raportowania o) Wewnętrzny komunikator w formie czatu p) Czat powinien umożliwiać przesyłanie plików q) Możliwość zdalnego połączenia do komputera r) Możliwość zdalnej instalacji oprogramowania s) Możliwość zdalnego zarządzania kontami lokalnych użytkowników Windows. **t)** Możliwość zdalnej edycji rejestru na komputerach z zainstalowanym agentem oprogramowania	
6.	**Kontrola dostępu do danych** Funkcjonalności modułu dla kontroli dostępu do danych: g) Integracja z Windows Defender h) Możliwość zdalnego szyfrowania dysków i) Zestawienie informacji o urządzeniach podłączonych do danego komputera j) Zarządzanie uprawnieniami (odczyt, uruchamianie, zapis) dla urządzeń, komputerów i użytkowników k) Wykrywanie oprogramowania antywirusowego l) Audyt podłączeń i operacji na przenośnych urządzeniach oraz na udziałach sieciowych	
7.	**Licencja:** Obsługa minimum 130 użytkowników.	
8.	**Gwarancja:** 12 miesięcy gwarancji oraz wsparcia technicznego producenta.	