Przedmiot zamówienia:

Dostawa sprzętu komputerowego – z podziałem na części

Opis Przedmiotu Zamówienia

(OPZ)

Opis Przedmiotu Zamówienia (OPZ) stanowi:

- Opis przedmiotu zamówienia (OPZ) – dla Części nr 1 i Części nr 2 (poniżej)

Zamówienie pn. ***Dostawa sprzętu komputerowego – z podziałem na części:***

Część nr 1 – urządzenie systemu bezpieczeństwa sieciowego

1. Wymagania ogólne

Zamawiający modernizuje swoją infrastrukturę bezpieczeństwa poprzez zwiększenie odporności na awarię w obrębie punktu styku sieci tworząc klaster wysokiej dostępności który finalnie ma być utworzony na dwóch urządzeniach typu NGFW.

Obecnie Zamawiający w swojej infrastrukturze posiada:

1. Pięć oddziałów (zdalnych lokalizacji) w innym miastach województwa połączonych za pomocą sieci oraz urządzeń FortiGate-61F
2. W Centrali Zamawiającego znajduje się obecnie UTM FortiGate-400F
3. W Centrali Zamawiający posiada w sieci LAN następujące urządzenia sieciowe:
    - FortiSwitch 1024D
    - FortiSwitch 524D
    - FortiSwitch 148F
    - FortiSwitch 124F-FPOE
4. Zamawiający posiada sieć bezprzewodową opartą o urządzenia FortiAP U433F.

Zamawiający wymaga, aby:

1. była zachowana logika i reguły działającego systemu, jakie obowiązywały do tej pory w używanym rozwiązaniu,
2. nastąpiło stworzenie klastra wysokiej dostępności poprzez dodanie w pełni kompatybilnego urządzenia z posiadanym przez Zamawiającego urządzeniem Fortigate 400F
3. oferowane komponenty (UTM) były kompatybilne z posiadanymi obecnie urządzeniami (podanymi powyżej) oraz oprogramowaniem, które posiada Zamawiający,
4. w ramach modernizacji istniejącego systemu zostaną uruchomione nowe urządzenie dostarczone w ramach powyższego postępowania.

Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów.

Zmodernizowany system bezpieczeństwa sieciowego będzie oparty o jedno urządzenie opisane w dalszej części SIWZ. Musi ono spełniać poniższe wymagania ogólne:

1. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
4. System wspiera protokoły IPv4 oraz IPv6 w zakresie:
    - Firewall
    - Ochrony w warstwie aplikacji
    - Protokołów routingu dynamicznego

2. Urządzenie systemu bezpieczeństwa sieciowego – 1 sztuka

Kategoria	Wymagane parametry techniczne
1. Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. 5. System ma pracować w postaci redundantnego klastra połączonego z urządzeniem FortiGate 400F. 6. System musi posiadać funkcję kontrolera LAN/WLAN z poziomu którego możliwe jest zarządzanie oraz monitorowanie przełączników i punktów dostępowych sieci bezprzewodowej posiadanych przez Zamawiającego w skład której wchodzą następujące modele: • FortiSwitch 1024D • FortiSwitch 524D • FortiSwitch 148F • FortiSwitch 124F-FPOE • FortiAP U433F
2. Interfejsy, dysk, zasilanie, moduły	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 18 portami Gigabit Ethernet RJ-45 • 6 gniazdami SFP 1 Gbps • 6 gniazdami SFP+ 10 Gbps 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC. 5. Wymagane jest, aby do systemu dołączone było 4 modułów SFP+ SR 10Gbs 850nm LC z czego: • 2 moduły muszą być kompatybilne z urządzeniami FortiSwitch-524D • 2 moduły muszą być kompatybilne z dostarczoną platformą

	Zamawiający dopuszcza zastosowanie zamienników 6. Wymagane jest dostarczenie odpowiedniej liczby kabli połączeniowych (krosujących) umożliwiających połączenie platformy z przełącznikami FortiSwitch-524D
3. Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż7.2mln. jednoczesnych połączeń oraz 480 tys. nowych połączeń na sekundę 2. Przepustowość Stateful Firewall'a: nie mniej niż 76 Gbps dla pakietów 512 B 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26Gbps 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 50 Gbps 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 11 Gbps 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 9 Gbps 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7.2 Gbps
4. Funkcje systemu bezpieczeństwa	1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection 2. Kontrola Aplikacji 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN 4. Ochrona przed malware 5. Ochrona przed atakami - Intrusion Prevention System 6. Kontrola stron WWW 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3 8. Zarządzanie pasmem (QoS, Traffic shaping) 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

	13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa)
5. Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu • Dedykowany ALG (Application Level Gateway) dla protokołu SIP 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu: • Amazon Web Services (AWS) • Microsoft Azure • Cisco ACI • Google Cloud Platform (GCP) • OpenStack • VMware NSX • Kubernetes
6. Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2 • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM) • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności

	• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth • Mechanizm „Split tunneling" dla połączeń Client-to-Site 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0 • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji
7. Routing i obsługa łączy WAN	1. Routingu statycznego 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP) 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu 6. BFD (Bidirectional Forwarding Detection) 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu
8. Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec)

9. Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu 2. System daje możliwość określania pasma dla poszczególnych aplikacji 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL
10. Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android) 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu
11. Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach

	3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu HTTP 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie
12. Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021) 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80)
13. Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard

	4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex) 6. Filtr WWW daje możliwość wykonania akcji typu „*Warning*" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji
14. Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP
15. Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow

	5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM) 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP 10. Wymagane jest, aby dostarczona platforma pozwalała na skonsolidowany widok wszystkich urządzeń pracujących w centrali jak i oddziałach zarządzanych przez Zamawiającego. Platforma pod tym względem musi być kompatybilna z urządzeniami FortiGate 61F
16. Logowanie	1. Wymagane jest, aby dostarczony systemu bezpieczeństwa sieciowego musiał realizować logowanie do komercyjnej platformy sprzętowej umożliwiającej generowanie raportów z zdarzeń w obrębie organizacji. Zamawiający posiada platformę FortiAnalyzer 300F 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa 4. Możliwość włączenia logowania per reguła w polityce firewall 5. System zapewnia możliwość logowania do serwera SYSLOG 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS
17. Testy wydajnościowe oraz funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy

18. Serwisy i licencje	1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy z możliwością rozszerzenia do maksymalnie 60 miesięcy
19. Warunki gwarancji	1. Urządzenie musi zostać objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy z możliwością rozszerzenia do maksymalnie 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (*Advanced Hardware Replacement*). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 2. Wymagane jest wyrównanie czasu licencji oraz support w obrębie urządzeń pracujących w klastrze do daty najnowszego urządzenia w klastrze
20. Wymagania formalne	1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania 2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym

3. Usługi

W ramach wykonania zadania w przedmiotowym postępowaniu, Zamawiający wymaga wykonania następujących usług związanych z dostarczanym urządzeniem:

1. Analiza wymogów dotyczących bezpieczeństwa w zakresie transmisji danych oraz logicznego umiejscowienia serwerów/systemów będących w posiadaniu przez Zamawiającego
2. Analiza potrzeb biznesowych na funkcje UTM (weryfikacja działania obecnych systemów bezpieczeństwa IT oraz brakujących usług)
3. Aktualizacja firmware'u do najnowszej stabilnej wersji. Zamawiającym wymaga aby wykonana została aktualizacja następujących komponentów:
    i. Utworzonego klastra NGFW
    ii. Środowiska SecuritiFabric do kompatybilnej wersji z root Fabric.
4. Dostosowanie centralnego systemu zbierania logów do nowej platformy oraz jej integracja
5. Utworzenie klastra HA
6. Rekonfiguracja interfejsów agregujących do przełączników rdzeniowych znajdujących się w infrastrukturze Zamawiającego umożliwiające połączenie na 10G
7. Połączenie klastra NGFW z rdzeniem przełączników realizując najlepsze praktyki w obrębie dostępności i odporności na awarię posiadanego jak i implementowanego rozwiązania
8. Przeprowadzenie testów działania klastra
9. Przeprowadzenie testów działania uruchomionego Systemu Firewall w celu weryfikacji poprawności instalacji i konfiguracji Systemu zgodnie z przedstawionymi wymaganiami
10. Wykonanie dokumentacji powykonawczej użytkowej uruchomionego Systemu

Zamówienie pn. ***Dostawa sprzętu komputerowego – z podziałem na części:***

<u>Część nr 2 – urządzenia systemu cyfrowy bunkier</u>

Zamawiający rozbudowuje swój system kopii zapasowych o drugie urządzenia deduplikacyjne opisane w dalszej części SWZ komponenty.

Obecnie Zamawiający posiada następującą infrastrukturę:

1. Zamawiający posiada:
   - sieć LAN
   - system wirtualizacji serwerowej
   - bibliotekę taśmową
   - oprogramowanie firmy Veeam służące do wykonywania kopii zapasowych
2. Jako zbiornik danych dla aplikacji Zamawiającego wykorzystywana jest macierz Dell EMC ME4024.
3. Zamawiający posiada w lokalizacji podstawowej deduplikator firmy Huawei model OceanProtect X3000 Backup Storage
4. Zamawiający posiada bazy danych (np. MS SQL) oraz aplikacje administracyjne pracujące pod kontrolą systemu operacyjnego Windows. Zamawiający nie przewiduje wymiany eksploatowanych obecnie aplikacji.

Zamawiający wymaga, aby:

1. Oferowane drugie urządzenie deduplikacyjne musi być kompatybilne z posiadanymi obecnie urządzeniami (podanymi powyżej) oraz oprogramowaniem, które posiada Zamawiający.
2. Oferowane urządzenie deduplikacyjne musi być kompatybilne z posiadanym obecnie urządzeniem deduplikującym, w szczególności musi być możliwość replikacji danych z wykorzystaniem wbudowanych mechanizmów deduplikatora, bez udziału oprogramowania firm trzecich
3. W ramach dalszej rozbudowy systemu kopii zapasowych będzie stworzenie cyfrowego bunkra poprzez dodanie drugiego takiego samego urządzenia deduplikacyjnego oraz serwera sterującego pracą obu urządzeń deduplikacyjnych.

1. **<u>Urządzenie deduplikacyjne – 1 sztuka</u>**

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	**Obudowa**	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów.
2.	**Kontrolery**	Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.
3.	**Wymagana przestrzeń**	Przestrzeń użytkowa po zbudowaniu RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot spare równą pojemności min. 1 dysku musi wynosić min 17TB. Rozmiar RAW pojedynczego dysku nie może być większy niż 4 TB. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o pojemności RAW min 960 GB jako cache pod zapis backupu. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń spare i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji.
4.	**Zabezpieczenia RAID**	Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej, tolerującej jednoczesną awarię 2 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-M poprzez mechanizm nadpisywania danych.
5.	**Pamięć Cache**	Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.
6.	**Dostępne interfejsy**	Urządzenie musi posiadać minimum: • 4 porty Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne.
7.	**Obsługiwane protokoły**	Wymagane wsparcie dla FC, iSCSI, NFS, CIFS.
8.	**Zarządzanie**	Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak: - cały deduplikator - kontrolery

		- CPU - porty front-end - porty logiczne - dyski - file systemy Pod kątem parametrów takich jak: - operacje wejścia/wyjścia IOPS - przepustowość (KB/s lub MB/s) - czas odpowiedzi (*latency*) - średnie użycie (w % dla CPU) Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Wymagany dostęp do informacji o wykorzystanej przestrzeni. Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje to ich dostarczenie jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej.
9.	**Redukcja danych**	Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia oraz należy je uwzględnić w cenie ofertowej.
10.	**Kontrola zasobów plikowych**	Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni, z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń.

		Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej.
11.	**Ochrona zasobów plikowych**	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. *snapshot*) file systemów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora oraz należy je uwzględnić w cenie ofertowej. Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej.
12.	**Replikacja danych**	Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję. Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60 min) lub konkretnych okien czasowych (np. w każdą sobotę o godz. 20:00). Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej. Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączanie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania.
13.	**Wspierane systemy backup**	Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication.

14.	**Warunki gwarancji**	Deduplikator musi posiadać możliwość upgrade'u firmware-u kontrolerów bez przerywania dostępu do danych. Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania. Urządzenie musi umożliwiać zdalne zarządzanie. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP. Deduplikator musi zostać objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy z możliwością rozszerzenia do maksymalnie 60 miesięcy, z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
15.	**Dodatkowe oprogramowanie (licencja jest wymagana)**	Wymagane jest dostarczenie oprogramowania, które potrafi sterować replikacją dysków logicznych lub systemów plików pomiędzy macierzami tego samego producenta znajdującymi się w dwóch różnych lokalizacjach. Po wykonaniu replikacji w centrum zapasowym powinien automatycznie wykonywać się bezpieczny snapshot zabezpieczający zreplikowane dane przed zmianą. Jako bezpieczny rozumiany jest snapshot, który posiada zabezpieczenie przez przypadkowym lub celowym usunięciem przez administratora przez zdefiniowany okres czasu. Oprogramowanie umożliwia skonfigurowanie częstotliwości wykonywania replikacji oraz czas retencji snapshota w lokalizacji zdalnej. Oprogramowanie umożliwia konfigurację, w której porty służące do replikacji są dostępne tylko na czas jej wykonywania. Poza czasem trwania replikacji są one odłączone i nie ma możliwości uzyskania przez nie dostępu do zasobów macierzy. Serwer zarządzający oprogramowania wspiera instalację na systemie operacyjnym SUSE Linux Enterprise Server 12. Wymagane jest wsparcie instalacji na serwerze fizycznym oraz wirtualnej maszynie VMware lub Hyper-V. Oprogramowanie musi być kompatybilne z urządzeniem Huawei OceanProtect X3000 posiadanym przez Zamawiającego.

2. <u>Serwer do sterowania urządzeniami deduplikacyjnymi – 1 sztuka</u>

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	**Obudowa**	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
2.	**Płyta główna**	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
4.	**Procesor**	Zainstalowany jeden procesor 12-rdzeniowy, min. 2.4GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 239w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
5.	**RAM**	Minimum 64GB DDR4 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
6.	**Funkcjonalność pamięci RAM**	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
7.	**Gniazda PCI**	- minimum jeden slot PCIe x16 generacji 4
8.	**Interfejsy sieciowe/FC/SAS**	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
9.	**Dyski twarde**	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 3 dyski SSD SAS o pojemności min. 1.92TB SSD SAS, 12Gb, 2,5“ Hot-Plug. Dodatkowo zainstalowane dwa dyski M.2 SATA/NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1.

10.	**Kontroler RAID**	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
11.	**Wbudowane porty**	4 x USB z czego nie mniej niż 1x USB 3.0, 1xVGA
12.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
13.	**Zasilacze**	Redundantne, Hot-Plug min. 1100W każdy.
14.	**Bezpieczeństwo**	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
15.	**Diagnostyka**	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
16.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

		• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
17.	**Oprogramowanie do zarządzania**	• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich

		• Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
18.	**Certyfikaty**	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019, Microsoft Windows 2022 oraz Microsoft Windows 2025
19.	**Warunki gwarancji**	Serwer musi zostać objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy z możliwością rozszerzenia do maksymalnie 60 miesięcy, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.

		Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
20.	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

3. <u>Serwer backupu – 1 sztuka</u>

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	**Obudowa**	Obudowa Rack o wysokości max 1U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
2.	**Płyta główna**	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
4.	**Procesor**	Zainstalowany jeden procesor 12-rdzeniowy, min. 2.4GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 239 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej..
5.	**RAM**	Minimum 64GB DDR4 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
6.	**Funkcjonalność pamięci RAM**	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
7.	**Gniazda PCI**	- minimum dwa sloty PCIe x16 generacji 4
8.	**Interfejsy sieciowe/FC/SAS**	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dodatkowo zainstalowana w slocie PCIe karta SAS 12Gb
9.	**Dyski twarde**	Zainstalowane dwa dyski M.2 SATA/NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1.
10.	**Kontroler RAID**	Nie wymagany.
11.	**Wbudowane porty**	4 x USB z czego nie mniej niż 1x USB 3.0, 1xVGA.

12.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
13.	**Zasilacze**	Redundantne, Hot-Plug min. 1100W każdy.
14.	**Bezpieczeństwo**	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
15.	**Diagnostyka**	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
16.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory;

		• możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
17.	**Oprogramowanie do zarządzania**	• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich

		• Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
18.	**Certyfikaty**	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019, Microsoft Windows 2022 oraz Microsoft Windows 2025
19.	**Warunki gwarancji**	Serwer musi zostać objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy z możliwością rozszerzenia do maksymalnie 60 miesięcy, z czasem reakcji do następnego dnia

		roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
20.	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

4. <u>Serwerowy system operacyjny – 2 sztuki</u>

L.p.	Parametr	Minimalne wymagania
1.	**W zakresie licencji**	Microsoft Windows Server Standard 2025 z możliwością obniżenia wersji systemu do Microsoft Windows Server 2022 **Standard** 64-bit **lub równoważny**. Zamawiający wymaga aby licencje umożliwiały uruchomienie 2 maszyn wirtualnych na każdym z zamawianych w tym postępowaniu hostów wyposażonych w jeden 16 rdzeniowy procesory każdy. Jako równoważne rozumie się: Obsługa następujących ról: • Serwer usług katalogowych zgodny z Active Directory, • Serwer DNS, • Serwer Plików, • Serwer Internetowych usług informacyjnych zgodny z Microsoft IIS 8, • Serwer DHCP, • Serwer wydruku, • Serwer zasad sieciowych z obsługą serwera RADIUS; • Obsługa .NET Framework 4.5., • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, graficzny interfejs użytkownika, • 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 na stacje robocze, serwery z systemem Windows wykorzystywane przez Zamawiającego, • Zdalna dystrybucja oprogramowania na stacje robocze, serwery Windows bez konieczności instalowania na w/w stacjach jakichkolwiek agentów, Możliwość instalacji na dostarczonym SSO oprogramowania wszystkich składników Platformy.
2.	**Równoważność w zakresie licencji**	Licencja uprawniająca do bezterminowego, nieograniczonego czasowo korzystania z oprogramowania. Licencja umożliwiająca instalację jednej kopii oprogramowania na serwerze fizycznym i **minimum** dwóch ilości kopii oprogramowania w środowisku wirtualnym. Najnowsza, dostępna w momencie składania oferty wersja oprogramowania, z możliwością legalnej instalacji co najmniej dwóch wersji wcześniejszych. Zamawiający dopuszcza licencje typu OEM lub ROK.

		Zamawiający wymaga dostarczenia legalnej licencji na SSO uprawniającej Zamawiającego do nieograniczonego czasowo używania oprogramowania**.** Zamawiający nie dopuszcza odsprzedaży używanych licencji. Niedopuszczalne jest dostarczenie licencji, dla których niemożliwe jest spełnienie warunków ich używania. Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonego systemu operacyjnego u Producenta oprogramowania jako element procedury odbioru.
		W ramach dostawy należy dostarczyć taką ilość licencji aby spełnić wymagania licencyjne producenta oprogramowania.
3.	**Równoważność w zakresie funkcjonalności**	Pełna obsługa wszystkich podzespołów serwerów będących składnikiem niniejszego zamówienia.

5. <u>Usługi</u>

Zamawiający wymaga wykonania następujących usług związanych z dostarczanym urządzeniem deduplikacyjnym oraz dostarczonymi serwerami

1. Instalacja urządzenia deduplikacyjnego we wskazanej przez Zamawiającego lokalizacji:
    a. Montaż urządzenia deduplikacyjnego w szafie Rack
    b. Podłączenie urządzenia deduplikacyjnego do infrastruktury LAN
    c. Uruchomienie urządzenia
    d. Inicjalizacja urządzenia
    e. Aktualizacja oprogramowania układowego (firmware) urządzenia deduplikacyjnego do najnowszej, zalecanej przez producenta wersji
    f. Aktywacja wszystkich wymaganych funkcjonalności poprzez instalację właściwych oraz permanentnych kluczy licencyjnych
    g. Konfiguracja przestrzeni dyskowej (grupy RAID, dyski zapasowe typu HotSpare), zgodnie z najlepszymi praktykami, zalecanymi przez producenta urządzenia
    h. Konfiguracja interfejsów sieciowych (agregacja portów sieciowych)
    i. Konfiguracja adresacji IP interfejsów sieciowych właściwych dla odpowiednich sieci wirtualnych VLAN
    j. Konfiguracja wirtualnych sieci VLAN na portach przełączników sieciowych, do których zostanie podłączone urządzenie deduplikacyjne
    k. Konfiguracja protokołów dostępu do urządzenia deduplikacyjnego: CIFS, protokół deduplikacji na źródle, NFS

l. Prezentacja przestrzeni dyskowej dla systemów informatycznych z wykorzystaniem protokołów: CIFS, NFS, protokół deduplikacji
m. Konfiguracja mechanizmu notyfikacji SMTP
n. Konfiguracja mechanizmu monitorowania SNMP
o. Konfiguracja mechanizmu automatycznego systemu powiadomień o zdarzeniach krytycznych, wysyłanych do producenta urządzenia

2. Instalacja systemu sterowania cyfrowym bunkrem danych we wskazanej przez Zamawiającego lokalizacji:
    a. Instalacja serwera fizycznego w szafie Rack
    b. Podłączenie dostarczonego serwera do zasilania oraz infrastruktury sieci LAN
    c. Instalacja systemu wirtualizacji serwerowej (kompatybilnej z dostarczonym oprogramowaniem sterującym bunkrem danych) na dostarczonym serwerze
    d. Instalacja systemu operacyjnego w maszynie wirtualnej wraz z aplikacją sterującą funkcjonalnościami bunkra danych (wersja systemu operacyjnego zgodna z zaleceniami instalowanego systemu sterującego)
    e. Przygotowanie sieci wirtualnych VLAN w miejscu instalacji bunkra danych
    f. Przygotowanie reguł dostępu na urządzeniach UTM, dla komunikacji/replikacji pomiędzy obecnie wykorzystywanym deduplikatorem a nowo dostarczonym zainstalowanym we wskazanej przez Zamawiającego lokalizacji.
    g. Integracja systemu sterowania cyfrowym bunkrem wraz z dostarczonym deduplikatorem danych, a w szczególności:
        i. Definicje okien replikacji z parametryzacją odłączenia bunkra danych od sieci LAN (*AirGap*)
        ii. Zabezpieczenie replikowanych danych poprzez mechanizmy kopii migawkowych z blokadą przed modyfikacją/usunięciem danych
        iii. Definicje czasu zabezpieczenia danych przed usunięciem (retencja danych)

3. Instalacja serwera backupu:
    a. Instalacja serwera fizycznego w szafie Rack
    b. Podłączenie dostarczonego serwera do zasilania oraz infrastruktury sieci LAN
    c. Instalacja systemu operacyjnego, zgodnego z obecnie wykorzystywanym przez Zamawiającego systemem backupowania i odtwarzania danych
    d. Migracja pełnej konfiguracji systemu kopiowania danych z maszyny obecnie wykorzystywanej przez Zamawiającego na nowo dostarczony serwer do backupu
    e. Podłączenie do serwera backupu biblioteki taśmowej.

f. Po wykonaniu migracji konfiguracji oraz stanu systemu backupowego na nowo dostarczoną maszynę serwera Zamawiający wymaga przeprowadzenia testów akceptacyjnych:
    a. Wykonanie kopii zapasowych na urządzenia deduplikacyjne oraz taśmowe
    b. Wykonanie testowego odtworzenia danych, wskazanych przez Zamawiającego z urządzenia deduplikacyjnego oraz taśmowego

4. Testy kopiowania danych (*backup*/replika) na dostarczone urządzenie deduplikacyjne.
5. Testy odtwarzania danych (*restore*) z dostarczonego urządzenia deduplikacyjnego.
6. Usługi powdrożeniowe w formie 3-miesięcznej opieki serwisowej (telefoniczna, zdalna, mailowa, w miejscu instalacji) od danych zakończenia projektu.