1. Przedmiot zamówienia

Przedmiotem zamówienia jest rozbudowa istniejącej infrastruktury poprzez dostawę urządzeń i oprogramowania.

2. Wymagania architektoniczne i uzasadnienie kompatybilności sprzętowej

2.1. Opis istniejącego środowiska podlegającego rozbudowie

Istniejące środowisko w lokalizacji DRC podlegające rozbudowie opiera się na pojedynczym serwerze wyposażonym w procesory architektury Intel. Działa on pod kontrolą oprogramowania wirtualizacyjnego VMware vSphere 8, zarządzanego przez serwer vCenter. Maszyny wirtualne – funkcjonujące wyłącznie w oparciu o system Red Hat Enterprise Linux (RHEL) – lokowane są w przestrzeni dyskowej udostępnianej z macierzy przez protokół iSCSI (system plików VMFS6). System ochrony danych oparty jest na rozwiązaniu Veeam, wykonującym bezagentowe kopie zapasowe poprzez integrację z vCenter, a kopie są zapisywane na urządzeniach DataDomain i replikowane pomiędzy ośrodkami. Warstwę komunikacyjną i zabezpieczającą środowiska stanowią obecnie pojedyncze urządzenia: przełącznik sieciowy DCN CS6580-48S6CQ-HI oraz firewall Fortinet FortiGate 200F.

Środowisko to stanowi element architektury wieloośrodkowej. Procedury awaryjnego przełączania (Failover) oraz planowana migracja maszyn wirtualnych pomiędzy lokalizacją podstawową (DC) a lokalizacją zapasową (DRC) są w pełni zautomatyzowane i koordynowane za pomocą oprogramowania VMware Site Recovery Manager (SRM).

Przedmiotem niniejszego postępowania jest rozbudowa środowiska informatycznego Zamawiającego w celu przekształcenia go z architektury posiadającej wiele fizycznych SPOF (single point of failure) w architekturę o wysokiej dostępności (High Availability – HA) pozbawionej SPOF. Osiągnięcie założonego celu, gwarantującego ciągłość pracy systemów oraz wzrost poziomu bezpieczeństwa, wymaga dostarczenia rozwiązań sprzętowych i programowych w pełni kompatybilnych z funkcjonującą już infrastrukturą.

Z uwagi na specyfikę technologiczną środowiska informatycznego oraz cel projektu (utworzenie środowiska HA), Zamawiający określa następujące wymogi dla poszczególnych komponentów rozbudowy:

2.2 Specyfikacja minimalnych wymagań dla serwera rack – 1 szt.

Z uwagi na fakt, iż przedmiotowy serwer zostanie włączony do istniejącego środowiska wirtualizacyjnego VMware vSphere (docelowo klaster HA), Zamawiający wymaga zastosowania procesorów z rodziny **Intel**. Wymóg ten jest podyktowany ograniczeniami technologicznymi środowiska wirtualizacyjnego, które do bezprzerwowej migracji maszyn wirtualnych (vMotion) wymaga zgodności zestawu instrukcji procesora (architektury) we wszystkich węzłach klastra. Mechanizm ujednolicania generacji procesorów – VMware EVC (Enhanced vMotion Compatibility) – nie oferuje kompatybilności krzyżowej pomiędzy różnymi producentami (Intel i AMD). Zastosowanie procesorów innej marki uniemożliwiłoby poprawne funkcjonowanie kluczowych mechanizmów związanych z Live Migration - źródło: VMware KB 316536.

Lp.	Element	Parametry minimalne / wymagane
1.	**Procesor**	1 x procesor Intel Xeon Gold 6548Y+ (32 rdzenie, taktowanie bazowe 2.5 GHz, 60 MB pamięci cache L3, obsługa pamięci DDR5-5200) lub równoważny procesor Intel, zapewniający pełną kompatybilność z istniejącym środowiskiem Zamawiającego opartym na architekturze Intel oraz poprawne funkcjonowanie mechanizmów wirtualizacyjnych, w tym VMware vMotion i EVC - wydajność procesora nie może być niższa niż 70000 punktów w teście CPU Mark (Multithread Rating) publikowane w serwisu cpubenchmark.net, na dzień publikacji postępowania. Adres strony:

		https://www.cpubenchmark.net/
2.	**Pamięć RAM**	512 GB (8 x 64 GB) RDIMM, ECC, Dual Rank, DDR5, o prędkości 5200 MT/s.
3.	**Pamięć masowa (Boot)**	8 zatok dyskowych 2.5” z interfejsem SAS/SATA Hot-Plug 2x 1.2 TB HDD 10k RPM, SAS 12Gb/s, Hot-Plug.
4.	**Zarządzanie RAID**	Sprzętowy, 8 GB cache, 12 Gb/s, SAS/SATA, 0/1/5/6/10/50/60
5.	**Gniazda rozszerzeń**	Riser umożliwiający instalację min. 2 kart Low Profile (Gen5) x16
6.	**Karta sieciowa**	Łącznie 8 portów SFP28 wraz z niezbędnym kompletnym okablowaniem typu DAC umożliwiającym połączenie z przełącznikami (przełącznik SFP28). Wykonawca jest zobowiązany do dostarczenia na własny koszt kompletu (8 szt.) nowych, kompatybilnych kabli/wkładek (minimum 2 metry długości) lub okablowania DAC (minimum 2 metry). Dostarczone okablowanie/wkładki muszą być kompatybilne z posiadanymi przez Zamawiającego oraz oferowanymi przełącznikami. Karta sieciowa musi obsługiwać ramki Jumbo Frames (9000 MTU).

7.	**Zasilanie**	Zasilacze nadmiarowe – 2 szt. (1+1) z niezbędnym okablowaniem (C13/C14, 4m), Hot-Plug, moc min. 1100W (100-240Vac), certyfikat sprawności min. Platinum.
8.	**Obudowa i akcesoria**	Obudowa typu Rack z przednią maskownicą, szyny montażowe wysuwane z ramieniem do układania kabli (CMA).
9.	**Kontroler zarządzania**	Wirtualna Konsola (KVM over IP): Pełny zdalny dostęp do interfejsu graficznego i tekstowego serwera niezależnie od stanu systemu operacyjnego (poprzez HTML5, bez konieczności Java). Virtual Media: Możliwość zdalnego montowania obrazów ISO (np. instalacyjnych systemów operacyjnych) z komputera administratora. Zarządzanie energią: Monitoring zużycia prądu w czasie rzeczywistym oraz możliwość zdalnego włączania/wyłączania/restartowania serwera. Logi systemowe i alerty: Przesyłanie powiadomień o awariach sprzętowych (SNMP, e-mail) oraz pełna historia zdarzeń (System Event Log). Bezpieczeństwo: Obsługa protokołów szyfrowanych (HTTPS, SSH), integracja z Active Directory/LDAP oraz Wsparcie dla uwierzytelniania dwuskładnikowego (2FA). Aktualizacja firmware: Możliwość zdalnej aktualizacji biosu, oprogramowania kontrolerów i dysków bez

		fizycznej obecności przy serwerze. Dedykowany port RJ-45, pełna wirtualna konsola (HTML5), obsługa Virtual Media, zdalne monitorowanie energii.
10.	**Obudowa**	Obudowa Rack o wysokości max 2U
11.	**PCIe i inne**	Min. 3 gniazda PCIe Gen5 (min. x8) Moduł TPM 2.0 FIPS Porty: Tył: 2x USB Type-A. Przód: 1x USB 2.0, 1x VGA Chłodzenie: Łącznie min. 6 wentylatorów hotplug zapewniających pełną redundancję.
12.	**Gwarancja i wsparcie techniczne dla serwerów**	Okres gwarancji: 36 miesięcy / 48 miesięcy / 60 miesięcy. Typ wsparcia: producenta ProSupport for Infrastructure lub równoważne, świadczone w standardzie naprawy w następnym dniu roboczym (NBD) na miejscu instalacji. W przypadku awarii nośnika danych, uszkodzony element pozostaje u Zamawiającego po wymianie na nowy.

2.3 Urządzenia sieciowe

2.3.1 - Klaster HA dla przełączników sieciowych

Celem niniejszego zamówienia jest rozbudowa środowiska do klastra wysokiej dostępności (High Availability), w którym węzły współdzielą płaszczyznę sterowania (Control Plane) i pozwalają na obsługę urządzeń końcowych (np. serwerów VMware) za pomocą agregacji łączy w trybie Active-Active (LACP / IEEE 802.3ad) z wykorzystaniem portów obu przełączników jednocześnie. Całym klastrem należy zarządzać z wykorzystaniem pojedynczego adresu IP.

Zamawiający użytkuje obecnie w swojej infrastrukturze produkcyjnej przełącznik sieciowy DCN CS6580-48S6CQ-HI. Urządzenie to jest w pełni sprawne i może stanowić bazę wyjściową (jako pierwszy węzeł) do budowy docelowego klastra wysokiej dostępności (HA).

Ze względu na uwarunkowania technologiczne i brak rynkowych standardów pozwalających na tworzenie klastrów o współdzielonej płaszczyźnie sterowania pomiędzy urządzeniami różnych producentów, Zamawiający dopuszcza dwa równorzędne warianty realizacji zamówienia:

Wariant 1:

Rozbudowa przy użyciu urządzenia kompatybilnego. Dostawa 1 (jednej) sztuki przełącznika, który jest w pełni kompatybilny z posiadanym przez Zamawiającego urządzeniem DCN CS6580-48S6CQ-HI i umożliwia natywne, bezpośrednie zestawienie sprzętowego klastra (wirtualizacji przełączników, np. VSF) z wykorzystaniem obecnej infrastruktury.

Wariant ten składa się z:

1. dostawy 1 szt. przełącznika DCN CS6580-48S6CQ-HI wraz z gwarancją na sprzęt na okres 24 miesięcy / 36 miesięcy / 48 miesięcy / 60 miesięcy, liczony od daty dostawy.
2. Montaż urządzenia w szafie rack.

Wariant 2:

Dostawa kompletnego rozwiązania równoważnego. W przypadku zaoferowania rozwiązania równoważnego (urządzenia innej marki, innego producenta lub modelu, który nie potrafi utworzyć klastra HA ze współdzielonym Control Plane z posiadanym przez Zamawiającego przełącznikiem), niedopuszczalne jest zaoferowanie tylko jednego przełącznika. Wykonawca zobowiązany jest w takim przypadku do dostarczenia, w ramach oferty, kompletu 2 sztuk

(pary) fabrycznie nowych przełączników równoważnych, które wspólnie utworzą nowy, jednolity klaster HA zastępujący dotychczasowe rozwiązanie Zamawiającego. Ponadto, w Wariancie 2 Wykonawca jest zobowiązany do przeprowadzenia migracji dotychczasowej konfiguracji ze środowiska Zamawiającego na nowe rozwiązanie wraz z przeszkoleniem administratorów z obsługi zaoferowanego rozwiązania.

Wariant ten składa się z:

1. dostawy 2 szt. przełączników wraz z gwarancją na sprzęt na okres 24 miesięcy/ 36 miesięcy / 48 miesięcy / 60 miesięcy,, liczony od daty dostawy.
2. Montaż i konfiguracja oferowanych urządzeń
3. Migracja dotychczasowej konfiguracji na oferowane urządzenia
4. Szkolenie 2 administratorów z obsługi zaoferowanego rozwiązania, prowadzone przez osobę posiadającą udokumentowaną wiedzę potwierdzoną odpowiednim certyfikatem.

Minimalne wymagania równoważności dla przełącznika sieciowego:

Elementy	**Parametry minimalne / wymagane**
Obudowa	Urządzenie musi być wykonane w standardzie montażu w szafie rackowej 19" (1U).
Zasilanie	Urządzenie musi być wyposażone w modułowy, redundantny system zasilania (minimum 2 moduły) typu Hot-Swap (wymiennych w trakcie pracy).
Wentylatory	Urządzenie musi posiadać wymienne w trakcie pracy (Hot-Swap) wentylatory zapewniające odpowiedni przepływ powietrza (front-to-back).
Typ i przeznaczenie urządzenia	Przełącznik musi być przeznaczony do pracy w środowisku centrum danych, jako urządzenie warstwy 3 (L3) z obsługą routingu IPv4/IPv6.
Porty fizyczne	48 portów 10/25G SFP28, 6 portów 40/100G QSFP28 (uplink) Dopuszcza się większą liczbę portów Porty QSFP28 muszą umożliwiać podział kanału (breakout) na 4 niezależne porty 25Gb/s (wymagane dla elastyczności podłączeń). Co najmniej 1 port konsolowy (RJ-45) do konfiguracji lokalnej. Co najmniej 1 port zarządzania Ethernet (RJ-45) 10/100/1000Mb/s

	(OOB).
Wydajność przełączania	przepustowość przełączania: nie mniej niż 3 Tbps, wydajność packet forwarding: nie niższa niż 2500 Mp/s
STP	Wsparcie dla STP (IEEE 802.1D), RSTP (IEEE 802.1w) oraz MSTP (IEEE 802.1s).
Agregacja łączy	Wsparcie dla protokołu LACP (IEEE 802.3ad)
Ochrona topologii sieci (L2 Ring Protection)	Urządzenie musi wspierać zaawansowany protokół ochrony pierścieni sieciowych (w tym wielu pierścieni zagnieżdżonych), zapewniający czas zbieżności poniżej 50ms w przypadku awarii łącza.
Redundancja łączy uplink	Urządzenie musi wspierać mechanizm redundancji łączy uplink, umożliwiający grupowanie portów w pary aktywne/rezerwowe oraz automatyczne przełączanie ruchu w przypadku awarii głównego łącza.
Wykrywanie pętli	Urządzenie musi wspierać mechanizm wykrywania pętli na poziomie warstwy drugiej (Loopback Detection) w celu zapobiegania błędom konfiguracyjnym.
Izolacja portów	Urządzenie musi wspierać funkcję izolacji portów (Port Isolation), umożliwiającą blokowanie komunikacji bezpośredniej między portami należącymi do tej samej sieci VLAN (tzw. Private VLAN Edge).
Mirroring portów	Wsparcie dla funkcji Port Mirroring (SPAN), umożliwiającej kopiowanie ruchu z jednego lub wielu portów (source) do dedykowanego portu przeznaczenia (destination) w celach analitycznych i diagnostycznych.
Rozszerzony mirroring portów	Urządzenie musi wspierać funkcję zdalnego kopiowania ruchu z portów monitorowanych (mirror source) do portu docelowego znajdującego się w innej sieci VLAN lub na innym urządzeniu w sieci IP, poprzez enkapsulację kopiowanych ramek w protokole GRE (Generic Routing Encapsulation).
Zabezpieczenie portu	Urządzenie musi wspierać funkcję Port Security, pozwalającą na ograniczenie maksymalnej liczby adresów MAC aktywnych na pojedynczym porcie oraz definiowanie statycznych lub dynamicznych powiązań adresów MAC z portem w celu zapobiegania nieautoryzowanemu dostępowi.

Diagnostyka kabla	Urządzenie musi posiadać funkcję diagnostyki parametrów fizycznych łącza miedzianego (Time Domain Reflectometry), umożliwiającą zdalne wykrycie i lokalizację uszkodzeń kabla (np. przerwanie, zwarcie) oraz określenie przybliżonej długości kabla. Wsparcie funkcji DDM (Digital Diagnostic Monitoring) dla modułów SFP/SFP+, umożliwiające monitorowanie parametrów pracy transceiverów (moc optyczna, temperatura, napięcie).
Redundancja oprogramowania	Obsługa podwójnego obrazu systemu operacyjnego (Dual Image) pozwalająca na przechowywanie dwóch wersji oprogramowania i awaryjne uruchomienie alternatywnej wersji.
Redundancja konfiguracji,	Obsługa podwójnego pliku konfiguracyjnego (Dual Configuration).
Sieci VLAN	Zgodność ze standardem IEEE 802.1Q., Wsparcie dla co najmniej 4K aktywnych sieci VLAN.
QinQ (VLAN Stacking)	Zgodność ze standardem IEEE 802.1QinQ.,
Rejestracja dynamiczna VLAN,	Zgodność ze standardem IEEE 802.1Q GVRP (GARP VLAN Registration Protocol).
Priorytetyzacja ruchu	Zgodność ze standardem IEEE 802.1p Class of Service (CoS).
Kontrola przepływu	Zgodność ze standardem IEEE 802.3x Full duplex & Flow control
Ochrona przed Broadcaststorm	Możliwość ograniczenia ruchu rozgłoszeniowego (broadcast), grupowego (multicast) oraz ruchu o nieznanych adresach docelowych (unknown unicast) na poziomie portów.
IGMP Snooping	Wsparcie dla protokołu IGMP Snooping w wersjach v1, v2 oraz v3 w celu optymalizacji ruchu multicast.
Filtrowanie MAC	Możliwość filtrowania ramek na podstawie adresów MAC (Layer 2 MAC filtering).
DHCP Snooping	Wsparcie dla funkcji DHCP Snooping weryfikującej wiadomości DHCP i budującej bazę powiązań adresów MAC z adresami IP (DHCP

	Snooping Binding Database).
Dynamiczna inspekcja ARP	Wsparcie dla mechanizmu Dynamic ARP Inspection, weryfikującego pakiety ARP w oparciu o bazę DHCP Snooping.
Ochrona źródła IP	Wsparcie dla mechanizmu blokującego ruch z adresów IP nieznajdujących się w tabeli powiązań DHCP Snooping.
Autoryzacja portow	Zgodność ze standardem IEEE 802.1X.,
Uwierzytelnianie i autoryzacja	Wsparcie dla protokołów RADIUS oraz TACACS+.,
Bezpieczny dostęp zdalny	Wsparcie dla protokołu SSH v2 oraz HTTPS (SSL) do zarządzania urządzeniem.
Listy kontroli dostępu	Obsługa list kontroli dostępu (ACL) do filtrowania ruchu.
Kolejki priorytetowe QoS	Urządzenie musi obsługiwać co najmniej 8 kolejek priorytetowych na port (zgodnie z IEEE 802.1p).
Algorytmy kolejkowania QoS	Wsparcie dla algorytmów planowania ruchu: Strict Priority (SP), Weighted Round Robin (WRR) oraz trybu hybrydowego (SP + WRR).
Ograniczanie przepustowości QoS	Możliwość limitowania szybkości transmisji (Rate Limiting) dla ruchu przychodzącego (Ingress) oraz wychodzącego (Egress).
Zmiana priorytetów QoS	Możliwość zmiany znaczników priorytetu (Re-marking) w nagłówkach ramek/pakietów w oparciu o zdefiniowane zasady.
Multicast VLAN	Urządzenie musi wspierać funkcję dedykowanej sieci VLAN dla ruchu multicast, pozwalającą na przesyłanie pojedynczego strumienia multicast w sieci szkieletowej i jego dystrybucję do odbiorców znajdujących się w różnych sieciach VLAN użytkowników (funkcja eliminuje konieczność duplikowania strumieni dla każdejgo VLAN-u).
Routing statyczny,	Obsługa statycznych tras routingu (Static Routes)
Protokół RIP	Wsparcie dla protokołu routingu RIP (Routing Information Protocol) w wersjach v1 oraz v2.

Protokół OSPF	Wsparcie dla protokołu routingu OSPF v2 (Open Shortest Path First).
Protokół BGP	Wsparcie dla protokołu routingu BGP v4 (Border Gateway Protocol).
Routing IPv6	Wsparcie dla routingu w warstwie 3 dla protokołu IPv6 (Layer 3 IPv6).
Podwójny stos protokołów	Wsparcie dla mechanizmu Dual Stack (IPv4/IPv6), umożliwiającego współistnienie i jednoczesną obsługę obu wersji protokołów IP.
Routing statyczny IPv6	Obsługa statycznych tras routingu dla protokołu IPv6.
OSPF v3	Wsparcie dla protokołu OSPF v3 (Open Shortest Path First dla IPv6).
RIPng	Wsparcie dla protokołu RIPng (RIP next generation dla IPv6).
Interfejs zarządzania Web	Wsparcie dla zarządzania urządzeniem poprzez interfejs graficzny HTTP/HTTPS (Web GUI).
Dostęp zdalny (CLI)	Wsparcie dla dostępu zdalnego poprzez protokół SSH.
Protokół SNMP	Wsparcie dla protokołu SNMP (Simple Network Management Protocol) w wersjach v1, v2c oraz v3.
Monitorowanie RMON	Wsparcie dla standardu RMON (Remote Network Monitoring).
Zarządzanie konfiguracją	Możliwość wykonania kopii zapasowej konfiguracji oraz jej odtworzenia (Backup/Restore Configuration).
Rejestr zdarzeń	Obsługa logów systemowych (System Log) oraz możliwość wysyłania powiadomień do zewnętrznego serwera (np. Syslog).
Synchronizacja czasu	Wsparcie dla protokołów synchronizacji czasu NTP (Network Time Protocol) oraz SNTP (Simple Network Time Protocol).
Klient TFTP	Wsparcie dla protokołu TFTP (Trivial File Transfer Protocol) do przesyłania plików systemowych.
Serwer DHCP	Urządzenie musi posiadać funkcjonalność serwera DHCP (Dynamic Host Configuration Protocol), umożliwiającą dynamiczne przydzielanie adresów IP dla hostów w podłączonych podsieciach (definicja pul, wykluczeń, opcji DHCP).
DHCP Relay	Wsparcie dla funkcji DHCP Relay (Agent przekaźnikowy), umożliwiającej przekazywanie zapytań DHCP od klientów do zewnętrznego serwera DHCP znajdującego się w innej podsieci IP (zgodnie z RFC 3046 - Option 82).

Klient DNS	Urządzenie musi wspierać funkcję klienta DNS, umożliwiającą rozwiązywanie nazw domenowych na adresy IP (zarówno IPv4 jak i IPv6).
CFM	Zgodność ze standardem IEEE 802.1ag (Connectivity Fault Management - CFM).
LLDP	Zgodność ze standardem IEEE 802.1ab (LLDP - Link Layer Discovery Protocol).
LLDP-MED	Rozszerzenie protokołu LLDP (Link Layer Discovery Protocol for Media Endpoint Devices), wspierające automatyczną konfigurację parametrów QoS oraz lokalizacji dla urządzeń końcowych (np. telefonów VoIP).
MIB	Urządzenie musi wspierać następujące standardy MIB (Management Information Base): - RFC1066 (TCP/IP MIB), - RFC1213 (MIB II), - RFC1493 (Bridge MIB), - RFC1643 (Ethernet MIB), - RFC1724 (RIP-2 MIB), - RFC1850 (OSPF v2 MIB), - RFC2618 (RADIUS Authentication Client MIB), - RFC2737 (Entity MIB), - RFC2863 (Interfaces Group MIB), - RFC4293 (MIB for IPv6).
Obsługa technologii wirtualizacji przełączników / klastra HA	Urządzenie musi umożliwiać budowę sprzętowego klastra HA w parze, w szczególności: • obsługę technologii wirtualizacji przełączników w trybie Active-Active • musi pozwalać na współdzielenie tablic adresów MAC, routing i konfigurację między urządzeniami w grupie oraz zapewniać transparentność dla protokołów routingu. • możliwość synchronizacji płaszczyzny sterowania (control plane) i stanów protokołów między urządzeniami klastra, • **obsługę agregacji łączy LACP (IEEE 802.3ad) dla urządzeń**

	<u>końcowych w topologii Active-Active.</u> • W przypadku pracy w trybie klastra wirtualizacji przełączników (np. VSF), oferowane urządzenie musi umożliwiać zarządzanie całym klastrem (obydwoma przełącznikami) za pomocą jednego, wspólnego adresu IP (Single Management IP) oraz jednego spójnego pliku konfiguracyjnego
Mechanizm redundancji między przełącznikami	Rozwiązanie klastra HA między przełącznikami nie może opierać się na protokole Spanning Tree (STP, RSTP, MSTP) jako mechanizmie redundancji łączy międzyprzełącznikowych (ISL). W szczególności: • Konwergencja po awarii węzła lub łącza ISL musi być niezauważalna dla protokołu iSCSI i wynosić poniżej 100 milisekund (przełączanie sprzętowe w warstwie L2 bez interwencji procesora głównego CPU do przeliczania topologii • nie jest dopuszczalne rozwiązanie, w którym po awarii łącza ISL ruch jest wstrzymywany na czas konwergencji STP (typowo 10–50 sekund), co zgodnie z wiedzą techniczną VMware powoduje utratę łączności sieciowej hostów ESXi i maszyn wirtualnych (źródło: VMware KB 344314 https://knowledge.broadcom.com/external/article?legacyId=1003804). • Nie dopuszcza się zastosowanie funkcji szybkiego przełączania (np. PortFast / Boundary Port / EdgePort) w celu ominięcia SpanningTree, ponieważ z uwagi na ryzyko krytycznej pętli sieciowej funkcja ta nie może być stosowana na łączach międzyprzełącznikowych (ISL).
Obsługa protokołów iSCSI i VMware	Urządzenie musi zapewniać obsługę Jumbo Frames o wielkości co najmniej 9000 bajtów.
Kompatybilność optyki (Wkładki SFP28/QSFP28 i kable DAC)	Oferowane urządzenie musi być w pełni kompatybilne na poziomie warstwy fizycznej (rozpoznawanie modułów i brak blokad programowych tzw. vendor-lock) z wkładkami optycznymi oraz kablami typu Direct Attach Cable (DAC), które są obecnie wykorzystywane przez Zamawiającego w przełączniku wzorcowym. W przypadku braku

	takiej kompatybilności, Wykonawca jest zobowiązany do dostarczenia na własny koszt kompletu nowych, kompatybilnych kabli/wkładek dla wszystkich podłączonych obecnie urządzeń i interfejsów sieciowych.
Gwarancja i wsparcie	Okres gwarancji: 24 miesiące od daty dostawy. Typ wsparcia: o standardzie naprawy w następnym dniu roboczym – NBD na miejscu) Producent musi zapewnić dostęp do aktualizacji oprogramowania układowego (firmware) na okres min. 24 miesięcy od daty dostawy.
	Urządzenie musi zostać dostarczone wraz z kompletem modułów zasilających i wentylatorów zapewniających pełną redundantność. Wymagane dołączenie kabli konsolowych oraz zestawu montażowego do szafy RACK.

2.3.2 - Klaster HA dla zapory sieciowej

Celem niniejszego zamówienia jest rozbudowa środowiska do klastra wysokiej dostępności, przez co rozumie się pracę w trybie Active-Passive (lub Active-Active), sprzętową synchronizację stanu sesji (Stateful Failover zapobiegający zerwaniu połączeń po awarii węzła) oraz zarządzanie oboma węzłami z poziomu jednej, spójnej polityki bezpieczeństwa.

Zamawiający użytkuje obecnie jedno urządzenie Fortinet FortiGate 200F. Urządzenie to jest w pełni sprawne i może stanowić bazę wyjściową (jako pierwszy węzeł) do budowy docelowego klastra wysokiej dostępności (HA).

Ze względu na uwarunkowania technologiczne i brak rynkowych standardów pozwalających na tworzenie klastrów HA (ze współdzieleniem płaszczyzny sterowania i stanu sesji) pomiędzy urządzeniami różnych producentów, Zamawiający dopuszcza dwa równorzędne warianty realizacji zamówienia:

Wariant 1: Rozbudowa przy użyciu urządzenia kompatybilnego tj. Dostawa 1 sztuki (jednego) urządzenia, które jest w pełni kompatybilne z posiadanym przez Zamawiającego urządzeniem FortiGate 200F i umożliwia natywne, bezpośrednie zestawienie klastra sprzętowego HA z wykorzystaniem obecnej infrastruktury.

Wariant ten składa się z:

1. dostawa 1 szt. zapory sieciowej Fortinet Fortigate 200F wraz z pakietem funkcjonalności Advanced Malware Protection, FortiGuard IPS Service, FortiGuard URL, DNS & Video

Filtering Service oraz AntiSpam, ważnym do dnia 12.12.2028 roku , a także z gwarancją na sprzęt ważną do dnia 12.12.2028 r. Zamawiający wymaga synchronizacji (ujednolicenia) terminów ważności licencji/subskrypcji usług bezpieczeństwa, wsparcia producenta oraz gwarancji nowo dostarczanego urządzenia z terminami ważności posiadanego przez Zamawiającego urządzenia FortiGate 200F w celu zapewnienia spójności klastra HA. Spełnienie tego wymogu musi zostać potwierdzone poprzez rejestrację urządzenia i subskrypcji na koncie Zamawiającego oraz możliwość weryfikacji dat w portalu producenta.

2. Montaż urządzenia w szafie rack

Wariant 2: Dostawa kompletnego rozwiązania równoważnego. W przypadku zaoferowania rozwiązania równoważnego (urządzenia innej marki, innego producenta lub modelu, który nie potrafi utworzyć klastra HA z obecnie posiadanym przez Zamawiającego sprzętem), niedopuszczalne jest zaoferowanie tylko jednego urządzenia. Wykonawca zobowiązany jest w takim przypadku do dostarczenia, w ramach oferty, kompletu 2 sztuk (pary) fabrycznie nowych urządzeń równoważnych, które wspólnie utworzą nowy, kompletny i niezależny klaster HA zastępujący dotychczasowe urządzenie Zamawiającego. Ponadto, w Wariancie 2 Wykonawca jest zobowiązany do przeprowadzenia migracji dotychczasowej konfiguracji, polityk bezpieczeństwa oraz tuneli VPN ze środowiska Zamawiającego na nowe rozwiązanie wraz z przeszkoleniem administratorów z obsługi zaoferowanego rozwiązania.

Wariant ten składa się z:

1. Dostawy 2 szt. zapór sieciowych wraz z pakietem funkcjonalności (subskrypcje usług bezpieczeństwa) oraz wsparciem producenta i gwarancją na sprzęt na okres 24 miesięcy liczonych od daty dostawy; subskrypcje oraz wsparcie muszą być aktywne dla obu urządzeń przez ten sam okres.
2. Montaż i konfiguracja oferowanych urządzeń
3. Migracja dotychczasowej konfiguracji na oferowane urządzenia
4. Transfer wiedzy - szkolenia administratorów z obsługi zaoferowanego rozwiązania przez osobę posiadającą udokumentowaną wiedzę potwierdzona odpowiednim certyfikatem. Szkolenie obejmujące tematy z zakresu tworzenia na oferowanych urządzeniach VLAN, routingu, klastrowania, tworzenia polityk bezpieczeństwa oraz monitorowania.

Wymagania równoważności dla zapory sieciowej – wariant 2:

Elementy	Parametry minimalne / wymagane
Obudowa	Urządzenie musi być wykonane w standardzie montażu w szafie rackowej 19" (1U).
Zasilanie	Urządzenie musi być wyposażone w redundantny system zasilania (1+1) zapewniający ciągłość pracy w przypadku awarii jednego z modułów
Porty	16 portów 1GbE BaseT. 4 porty 10 GbE SFP+ 8 portów 10GbE SFP 2 dedykowane porty HA (High Availability) typu SFP. 1 porty zarządzania (Management) RJ45. 1 port USB.
Funkcje modułu Firewall, router i switching	1. Zamawiający wymaga, aby na dostarczane rozwiązanie składały się następujące moduły/funkcjonalności: a. Zapora sieciowa wraz z inspekcją SSL b. NAT c. VPN IPSec d. Routing oraz switching e. Ochronę antywirusową. f. Możliwość filtrowania URL. g. Ochronę z wykorzystaniem mechanizmów IPS. h. Rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego i. SSL VPN
Zapora sieciowa	1. Zapora sieciowa powinna posiadać mechanizm inspekcji SSL (ssl inspection). 2. Zapora sieciowa powinna funkcjonować w oparciu o interfejsy, adresy (IP i FQDN), grupy adresów (IP i FQDN), oraz użytkowników. 3. Musi obsługiwać statyczny routing. 4. Musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF. 5. Musi obsługiwać policy-based routing. 6. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie.

	7. Musi umożliwiać pracę jako router i bridge (transparent mode). 8. Musi obsługiwać translację adresów: SNAT, DNAT. 9. Musi obsługiwać translację portów: PAT. 10. Musi obsługiwać VLAN 802.1Q. 11. Musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów. 12. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego. 13. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory. 14. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej. 15. Musi umożliwiać sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa użytkowników, protokół, interfejs sieciowy, adres (IP oraz FQDN) i grupa adresów (IP oraz FQDN). 16. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
Wymagane funkcje VPN systemu	1. Obsluga tuneli: Site-to-Site 2. Wsparcie dla algorytmów szyfrowania IKE: AES-GCM, AES256, AES128, 3DES, DES 3. Minimum wsparcie dla algorytmów autentykacji IKE: MD5, SHA-1, SHA-256, SHA-512 4. Rodzaje autentykacji: Preshared key oraz PKI X.509 5. IPsec: wsparcie dla przynajmniej jednego z poniższych: o Authentication Header (AH) o Encapsulating Security Payload (ESP) 6. Wsparcie dla IKEv1 i IKEv2. 7. Urządzenie musi obsługiwać Perfect Forward Secrecy oraz Anti Reply (Reply Detection) 8. Obsługa Dead Peer Detection (DPD). 9. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem IPSec 10. Możliwość jednoczesnego podłączenia przynajmniej 10 klientów poprzez IPSec.
W ramach filtrowania zawartości URL system musi	1. Filtrowanie URL z wykorzystaniem baz reputacji i kategorii stron dostępnych w formie subskrypcji. 2. Baza filtrów url powinna zawierać kategorie istotne z punktu

zapewniać	widzenia bezpieczeństwa: przykładowo Spam, Malicious Websites. 3. Możliwość tworzenia wyjątków dla filtrowania zawartości http.
W ramach kontroli aplikacyjnej system musi zapewniać	1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły. 2. Możliwość kształtowania ruchu (np., ograniczanie przepustowości) dla aplikacji lub kategorii. 3. Tworzenie reguł zapory sieciowej w oparciu o aplikacje. 4. Rozpoznawanie aplikacji co najmniej p2p, dostęp zdalny, proxy, usługi dysków sieciowych (np. dropbox).
W ramach kontroli Antywirusowej system musi zapewniać	1. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 24 godzin. 2. Skanowanie plików skompresowanych: zip, tar, gzip. 3. Wsparcie dla głównych protokołów: http, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.
W ramach ochrony przed atakami system musi zapewniać	1. Automatyczną aktualizację bazy sygnatur IPS. 2. Automatyczne blokowanie znanych źródeł ataków. 3. Mechanizmy ochrony przed atakami typu DoS i DdoS.
W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać	1. Analizę behawioralną w oparciu o platformę typu sandbox. 2. W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów zewnętrznej chmury (w granicach Unii Europejskiej). 3. Analizę plików pobieranych przez http/https.
Zarządzanie	1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH). 2. Urządzenie musi posiadać interfejs Ethernet obsługujący połączenia z prędkością minimum 100 mbit/s - dla zdalnego zarządzania.
Kompatybilność klastra HA	Urządzenia muszą posiadać techniczną możliwość zestawienia sprzętowego klastra wysokiej dostępności (High Availability) w trybie Active-Passive oraz Active-Active. Wymagane jest, aby klaster działał jako jedna jednostka zarządzająca z pełną synchronizacją konfiguracji.
Synchronizacja sesji	Węzły klastra muszą prowadzić ciągłą replikację tablicy połączeń

(Stateful Failover)	w czasie rzeczywistym. W przypadku awarii urządzenia lub łącza, system musi przejąć przetwarzanie bez zrywania sesji. Funkcja Session Pick-up musi działać dla sesji TCP, UDP oraz ICMP
Wersja oprogramowania	Urządzenie musi pozwalać na pracę w klastrze z drugim urządzeniem przy użyciu tej samej wersji systemu operacyjnego (firmware), instalowanej bez konieczności modyfikacji konfiguracji posiadanego urządzenia. Ponadto, zaoferowane urządzenia muszą zostać dostarczone z tożsamym poziomem subskrypcji (jeśli dotyczy zaoferowanego rozwiązania) usług bezpieczeństwa (ochrona UTM/NGFW), aby zagwarantować pełną symetrię weryfikacji ruchu sieciowego (w tym sygnatur IPS, Antivirus i Web Filtering) w przypadku przełączenia węzła.
Porty fizyczne i interfejsy zarządzające	Urządzenie musi również pozwalać na wydzielenie dedykowanych portów sprzętowych (Hardware Heartbeat) do bezstratnej komunikacji klastra lub posiadać takie dedykowane porty.
Zarządzanie	Urządzenie musi być zarządzane z tego samego poziomu administracyjnego co urządzenie wzorcowe (pojedynczy punkt zarządzania politykami bezpieczeństwa dla obu węzłów).
Wsparcie i gwarancja dla urządzenia	Okres gwarancji o standardzie naprawy w następnym dniu roboczym – NBD na miejscu) Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.) oraz system zgłoszeniowy producenta. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej infrastruktury oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Zakres wsparcia technicznego producenta a. Dostęp do pomocy technicznej; b. Dostęp do poprawek i nowych wersji oprogramowania i/lub

	systemu; c. Dostęp do dokumentacji technicznej; d. Dostęp do konta wsparcia urządzenia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.
Uplink	Po cztery przewody światłowodowe per urządzenie o długości minimum 2m wraz z kompletem modułów 10GbE SFP+ kompatybilnymi z urządzeniami oraz przełącznikami. Zamawiający jako równoważne dopuszcza kompatybilne z oferowanym przełącznikami i urządzeniami okablowanie DAC (2m). 2. Niezbędne kable zasilające. 3. Komplet szyn umożliwiających montaż w szafie rack

2.4 Oprogramowanie.

2.4.1 Wymagane oprogramowanie

1. System operacyjny (OS): Red Hat Enterprise Linux for Virtual Datacenters (VDC) lub równoważne ze wsparciem producenta na poziomie Standard (wsparcie w godzinach roboczych) do dnia 05.12.2028. Licencja musi umożliwiać uruchomienie nielimitowanej liczby wirtualnych instancji systemu Red Hat Enterprise Linux na oferowanym serwerze fizycznym objętym niniejszym zamówieniem.
2. Oprogramowanie do kopii zapasowych: Veeam Data Platform Foundation Enterprise Plus lub równoważne.
    1) Przedłużenie wsparcia dla posiadanej licencji wieczystej na 2 CPU (ważnego do 30.01.2027) do dnia 30.01.2028
    2) Dostarczenie nowej licencji wieczystej obejmujące zasoby oferowanego serwera (licencjonowanie per gniazdo CPU / socket) na okres do 30.01.2028.

2.4.2 Warunki równoważności i kompatybilności operacyjnej

Z uwagi na fakt, iż przedmiot zamówienia stanowi rozbudowę krytycznego, działającego środowiska Zamawiającego, każde oferowane rozwiązanie równoważne musi zapewniać pełną, natywną kompatybilność operacyjną oraz zgodność architektoniczną z obecnie użytkowanym stosem technologicznym zarówno w rozbudowywanej lokalizacji jak i innych lokalizacjach.

W przypadku zaoferowania rozwiązania innego niż obecnie użytkowane (np. inny system operacyjny), które wymagałoby migracji istniejących zasobów lub zmiany modelu licencjonowania dla infrastruktury pozostałej w innej lokalizacji, Wykonawca jest zobowiązany wykonać taką migrację oraz pokryć wszelkie koszty licencji niezbędne do zachowania jednolitości środowiska (tj. dostarczyć licencje na nowy software również dla "starych" serwerów) w ramach oferty.

Zamawiający wskazuje, iż w docelowej architekturze wysokiej dostępności (Multi-Site / Disaster Recovery) maszyny wirtualne są w sposób dynamiczny oraz awaryjny (Failover) przenoszone pomiędzy ośrodkiem podstawowym (DC) a ośrodkiem zapasowym (DRC), zachowując przy tym niezmieniony system operacyjny gościa (Guest OS).

W przypadku zaoferowania oprogramowania innego niż wskazane powyżej (punkt 2.4.1 niniejszego OPZ) jako wzorcowe, Wykonawca musi udowodnić spełnienie warunków równoważności.

2.4.2.1 Równoważność w warstwie Systemu Operacyjnego (RHEL VDC):

Zamawiający wykorzystuje obecnie systemy Red Hat Enterprise Linux (RHEL) jako standardowy i wspierany system operacyjny dla wszystkich maszyn wirtualnych (systemów gości). Zgodność licencyjna utrzymywana jest poprzez model licencjonowania warstwy sprzętowej (Virtual Datacenter), pozwalający na uruchamianie nielimitowanej liczby maszyn z systemem RHEL na objętych subskrypcją hostach fizycznych.

W celu zachowania ciągłości wsparcia producenta dla systemów gości w przypadku migracji maszyn między ośrodkami w przypadku awarii (Failover), aby zapobiec naruszeniu praw autorskich i niedolicencjonowania (underlicensing - PRODUCT APPENDIX 1 SOFTWARE AND SUPPORT SUBSCRIPTIONS punkt 1.2 dla RHEL) Zamawiający dopuszcza dwa równorzędne warianty:

Wariant 1: Rozbudowa licencji wzorcowych (RHEL)

Dostawa systemu operacyjnego Red Hat Enterprise Linux for Virtual Datacenters (VDC) ze wsparciem Standard dla nowo dostarczanego serwera fizycznego. Zastosowanie tego wariantu automatycznie zabezpiecza prawnie i technicznie proces migracji dowolnych maszyn Zamawiającego zarówno pomiędzy hostami wewnątrz klastra jak i tez pomiędzy lokalizacjami.

Wariant 2: Dostawa systemu operacyjnego równoważnego. W przypadku zaoferowania rozwiązania równoważnego, tj. subskrypcji/licencji na inny system operacyjny klasy

Enterprise Linux (np. Oracle Linux, SUSE Linux Enterprise Server), Wykonawca jest zobowiązany zapewnić Zamawiającemu 100% legalność środowiska i ciągłość wsparcia technicznego podczas procesów migracji i DR pomiędzy lokalizacjami. W tym celu Wykonawca zobowiązany jest (w ramach ceny oferty) do:

1. Dostarczenia odpowiednich licencji na okres 24 miesięcy klasy "Datacenter" oferowanego systemu równoważnego dla wszystkich hostów (nowych oraz dotychczasowych) we wszystkich lokalizacjach, pozwalających na nielimitowaną wirtualizację tego systemu operacyjnego.
2. Dostarczenia niezbędnych narzędzi oraz przeprowadzenia pełnej migracji/konwersji systemów operacyjnych gości wewnątrz posiadanych przez Zamawiającego maszyn wirtualnych z systemu RHEL do zaoferowanego systemu równoważnego.
3. Wykonawca bierze na siebie pełną odpowiedzialność (tzw. bug-for-bug compatibility) za to, że wszystkie aplikacje i bazy danych użytkowane obecnie przez Zamawiającego na systemach RHEL będą funkcjonować prawidłowo i bez spadku wydajności na zaoferowanym systemie równoważnym. W przypadku wystąpienia niekompatybilności, Wykonawca na własny koszt dokona niezbędnych modyfikacji środowiska aplikacyjnego Zamawiającego.
4. Zaoferowany równoważny system operacyjny nie może wymagać od Zamawiającego ponoszenia opłat za dostęp do aktualizacji bezpieczeństwa (erraty, patche) przez okres równy okresowi wsparcia wymaganemu w Wariancie 1.
5. Przeprowadzenia certyfikowanego lub autoryzowanego szkolenia dla administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiających pełne poznanie produktu równoważnego. Wykonawca najpóźniej w dniu podpisania Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram warsztatów.

Wymagania równoważności dla systemu operacyjnego:

Lp.	Parametry minimalne / wymagane
1.	Serwerowy system operacyjny musi być oparty na jądrze typu Linux w pełni zgodnym ze standardem jądra RedHat Kernel.
2.	Serwerowy system operacyjny powinien obsługiwać minimum systemy plików: Ext3, Ext4, GFS, GFS2, XFS.
3.	Dostarczona subskrypcja na oprogramowanie musi umożliwiać uruchomienie

	nielimitowanej liczby serwerów wirtualnych na serwerze fizycznym.
4.	System operacyjny musi posiadać lokalne repozytorium pakietów aplikacyjnych, uaktualnień i poprawek oprogramowania zarządzanych systemów
5.	System powinien umożliwiać pełną obsługę oprogramowania dostarczaną w postaci pakietów RPM (plik z rozszerzeniem .rpm).
6.	Umożliwia definiowanie własnych repozytoriów oprogramowania bez konieczności podłączenia zarządzanych systemów do zewnętrznych źródeł w sieci Internet, umożliwia dystrybucję oprogramowania w sieci lokalnej
7.	Umożliwia automatyczne skanowanie systemów w poszukiwaniu potencjalnych problemów konfiguracyjnych, czy zgodności z dobrymi praktykami.
8.	Posiada filtrowanie dostępnych pakietów poprzez definiowanie wirtualnych widoków, które precyzyjnie ograniczają zawartość do wybranych produktów, pakietów oraz ich wersji.
9.	Posiada możliwość analizy stanu zarządzanych systemów i rekomendacji optymalizacji w następujących kategoriach: bezpieczeństwo, stabilność, dostępność oraz wydajność. W wyniku dokonanej analizy generuje automatyczne skrypty, mogące posłużyć do zautomatyzowania procesu naprawy lub eliminacji zagrożenia.
10.	Oprogramowanie w systemie umożliwia automatyczną analizę stanu środowiska w poszukiwaniu znanych przypadków oraz rekomendacji wynikających z dobrych praktyk.
11.	W ramach dostarczonego oprogramowania Zamawiający powinien mieć dostęp do: a) Aktualnych łatek, b) Aktualnych poprawek błędów, c) Uaktualnień, d) Nowych wersji oprogramowania, e) Specjalistycznej wiedzy poprzez: a. Portal producenta oprogramowania, b. Dostęp do bazy wiedzy.
12.	Zaoferowany system operacyjny Linux powinien posiadać bezpośrednie komercyjne wsparcie producenta w pierwszej linii wsparcia
13.	Produkt powinien posiadać gwarantowany czas życia przez producenta na co najmniej 10 lat od momentu pojawienia się na rynku. Gwarantowane są: • przez okres przynajmniej 5 lat - nowe funkcjonalności • przez okres przynajmniej 10 lat - nielimitowana liczba zgłoszeń, poprawki bezpieczeństwa, poprawki błędów
14.	Wsparcie producenta zaoferowanego systemu operacyjnego Linux powinno być świadczone w standardzie nie gorszym niż w trybie Standard dla oprogramowania Red Hat Enterprise Linux for Virtual Datacenters, w tym powinno zapewniać: a)

	Możliwość zgłaszania awarii za pośrednictwem strony internetowej producenta lub telefonicznie w trybie minimum 8 godzin roboczych na dobę, 5 dni roboczych w tygodniu (w godzinach pracy producenta). b) Brak ograniczeń dotyczących liczby zgłoszeń w miesiącu. c) Czas reakcji na zgłaszane problemy, w zależności od istotności problemu powinien wynosić nie więcej niż: a. 1 godzina dnia roboczego dla problemów, o Pilnym poziomie istotności. Problem, o Pilnym poziomie istotności to taki który poważnie wpływa na korzystanie z oprogramowania w środowisku produkcyjnym (np. utrata danych produkcyjnych lub niedziałanie systemów produkcyjnych). Sytuacja wstrzymuje operacje biznesowe i nie istnieje żadne obejście proceduralne. b. 4 godziny robocze dla problemów, o Wysokim poziomie istotności. Problem, o Wysokim poziomie istotności, to taki, w którym oprogramowanie działa, ale korzystanie z niego w środowisku produkcyjnym jest znacznie ograniczone. Sytuacja ma duży wpływ na część operacji biznesowych i nie istnieje żadne obejście proceduralne. c. 1 dzień roboczy dla problemów, o Średnim poziomie istotności. Problem, o Średnim poziomie istotności, to taki, który obejmuje częściową, niekrytyczną utratę możliwości korzystania z oprogramowania w środowisku produkcyjnym lub środowisku programistycznym. W przypadku środowisk produkcyjnych wpływ na firmę jest średni do niskiego, ale firma nadal działa, w tym dzięki zastosowaniu obejścia proceduralnego. W przypadku środowisk programistycznych sytuacja powoduje, że projekt nie jest już kontynuowany ani migrowany do środowiska produkcyjnego. d. 2 dni robocze dla problemów, o Niskim poziomie istotności. Problem, o Niskim poziomie istotności obejmuje ogólne pytanie dotyczące użytkowania, zgłoszenie błędu w dokumentacji lub zalecenie przyszłego ulepszenia lub modyfikacji produktu. W środowiskach produkcyjnych nie ma to wpływu na firmę, wydajność lub funkcjonalność systemu. W przypadku środowisk programistycznych istnieje średni lub niski wpływ na firmę, ale firma nadal działa, w tym dzięki zastosowaniu obejścia proceduralnego.
15.	Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
16.	Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania

	równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 1 roku licząc od momentu złożenia oferty

2.4.2.2 Rozbudowa systemu wykonywania kopii zapasowych

Zamawiający użytkuje obecnie system kopii zapasowych oparty o oprogramowanie Veeam Backup & Replication, funkcjonujący w topologii obejmującej lokalizację podstawową oraz lokalizację zapasową (DRC), z wdrożoną replikacją pomiędzy ośrodkami.

Ze względu na potrzebę zachowania spójności zarządzania i niezawodności, Zamawiający dopuszcza dwa warianty realizacji zamówienia:

Wariant 1: Rozbudowa (Dostawa licencji natywnie kompatybilnych)

Przedłużenie i dostawa rozszerzenia posiadanych licencji, w pełni i natywnie integrujących się z obecną konsolą oprogramowania Zamawiającego i niewymagających rekonfiguracji zadań wykonywanych kopii zapasowych oraz przebudowy repozytoriów.

Wariant 2: Dostawa kompletnego rozwiązania równoważnego dla całego środowiska.

W przypadku zaoferowania oprogramowania innego producenta, które nie potrafi utworzyć spójnego środowiska z obecnym systemem Zamawiającego (np. Odtwarzania kopii zapasowych wykonanych przez Veeam i odtwarzaniu ich w innej lokalizacji), Wykonawca jest zobowiązany do:

- Dostarczenia pełnych licencji oprogramowania równoważnego (nowe oprogramowanie) pozwalających na zabezpieczenie całego środowiska Zamawiającego (zarówno w ośrodku podstawowym, jak i DRC) na okres 24 miesięcy liczony od daty dostawy.
- Instalacja i konfiguracja zaoferowanego oprogramowania
- Przeprowadzenia na koszt i ryzyko Wykonawcy pełnej migracji polityk, harmonogramów oraz zadań backupu z obecnego rozwiązania do nowego.
- Zapewnienia mechanizmów umożliwiających ciągłość dostępu (odzyskiwania danych) z archiwalnych kopii zapasowych Zamawiającego.
- Zapewnienia pełnego wsparcia dla posiadanych przez zamawiającego urządzeń Data Domain (protokół DD-BOOST).
- Przeprowadzenia certyfikowanego lub autoryzowanego szkolenia dla administratorów Zamawiającego (min. 8 godzin) z obsługi nowego systemu od podstaw.

Wymagania równoważności dla oprogramowania do tworzenia kopii zapasowych:

Lp.	Parametry minimalne / wymagane
1.	Oprogramowanie musi być kompatybilne z używanym przez Zamawiającego wirtualizatorem.
2.	Oprogramowanie musi być licencjonowanie w modelu “per fizyczne CPU”. Wszystkie wymienione poniżej funkcjonalności muszą być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone.
3.	Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
4.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
5.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
6.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
7.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
8.	Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
9.	Oprogramowanie musi mieć możliwość tworzenia kopii zapasowych ze snapshotów (migawek) realizowanych przez pamięć masową (macierz).
10.	Oprogramowanie musi mieć możliwość tworzenia spójnych - z aplikacjami zorientowanymi na przetwarzanie danych – kopii zapasowych maszyn wirtualnych (np. transakcje dla SQL)
11.	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
12.	Oprogramowanie musi mieć możliwość odtworzenia plików przy pomocy VMware VIX API
13.	Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i

	po zadaniu backupowym lub przed i po wykonaniu zadania snapshota
14.	Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie.
15.	Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
16.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
17.	Oprogramowanie musi automatycznie wykrywać i usuwać osierocone snapshoty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
18.	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn do zdalnej lokalizacji z wykorzystaniem wbudowanej akceleracji WAN.
19.	Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
20.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik (łańcuch replik)
21.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
22.	Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych
23.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
24.	Oprogramowanie musi umożliwić odtworzenie plików na dowolną maszynę, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą

	przywracanych plików
25.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej
26.	Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD
27.	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
28.	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowanego środowiska) w oparciu o wirtualizator, używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
29.	Oprogramowanie musi w pełni wspierać i obsługiwać posiadane deduplikatory (datadomain) oraz protokół deduplikacji (dd-boost) na źródle.

2.4.2.5 Zgodność licencyjna przenoszonych środowisk

1. Zamawiający nie dopuszcza sytuacji, w której zachowanie zgodności licencyjnej wymagałoby od niego ponoszenia jakichkolwiek ukrytych kosztów w przyszłości, ani scenariusza, w którym na czas awarii lub migracji wymusza się reinstalację systemu gościa do innej dystrybucji.

3. Dostawa urządzeń objętych zamówieniem:

- Sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
- Wszystkie elementy muszą być fabrycznie nowe i nieużywane.
- Urządzenia muszą zostać dostarczone do wskazanego przez Zamawiającego DataCenter oraz zamontowane w szafie rack tego samego dnia co dostawa danego urządzenia. Nie dopuszcza się dostawy jednego dnia i montażu innego dnia. Zamawiający dopuszcza wcześniejszą dostawę przełącznika sieciowego oraz zapory sieciowej pod warunkiem, że ich montaż w szafie rack nastąpi w dniu dostawy tych

urządzeń. Dopuszcza się również późniejszą dostawę serwera pod warunkiem, że jego montaż w szafie rack nastąpi w dniu jego dostawy.

- Do celów szacowania oraz porównania ofert Wykonawca wskaże w tabeli ofertowej przy każdym elemencie sprzętowym orientacyjny termin realizacji (dostawy) urządzeń.
- Dostawa oprogramowania (Veeam oraz system operacyjny) nie może nastąpić przed dostawą serwera.

4. Informacje dodatkowe:

1. Zamawiający wymaga przypisania licencji na system operacyjny do konta Red Hat nr 10050136.
2. Zamawiający wymaga przypisania licencji Veeam do konta sbt@ncbr.gov.pl .
3. Zamawiający wymaga przypisania urządzenia i licencji dla dostarczanych zapór sieciowych do konta:
    1) Dla wariantu 1: 1142703/Narodowe Centrum Badań i Rozwoju
    2) Dla wariantu 2: sbt@ncbr.gov.pl
4. Zamawiający wymaga przypisania urządzenia i licencji dla dostarczanych przełączników sieciowych do konta:
    1) Dla wariantu 2: sbt@ncbr.gov.pl
5. Zamawiający wymaga przypisania u producenta oferowanego serwera wsparcia i gwarancji do konta sbt@ncbr.gov.pl