

Załącznik nr 7 do SWZ - OPZ – Infrastruktura IT UG Opinogóra Górna

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa infrastruktury serwerowej, macierzowej, sieciowej oraz urządzeń NAS wraz z wdrożeniem

1. INFORMACJE OGÓLNE

Przedmiotem zamówienia jest dostawa fabrycznie nowego sprzętu informatycznego wraz z oprogramowaniem i licencjami, obejmująca infrastrukturę serwerową, macierz dyskową, urządzenia sieciowe (UTM, przełączniki) oraz serwer NAS, wraz z kompleksowym wdrożeniem obejmującym instalację, konfigurację, integrację z istniejącą infrastrukturą, migrację danych i usług, testy, szkolenie administratorów oraz dokumentację powykonawczą.

Wszystkie urządzenia muszą być wyprodukowane nie wcześniej niż w 2024 roku, pochodzić z oficjalnych kanałów dystrybucji producenta na terenie Unii Europejskiej oraz posiadać pełne wsparcie techniczne producenta realizowane na terenie Polski.

Zamawiający dopuszcza składanie ofert równoważnych. Za rozwiązanie równoważne uznaje się takie, które spełnia wszystkie wymagania minimalne określone w niniejszym opisie przedmiotu zamówienia. Wykonawca oferujący rozwiązanie równoważne zobowiązany jest wykazać, że oferowane przez niego produkty spełniają wymagania określone przez Zamawiającego.

2. ZADANIE 1 – Serwer kopii zapasowych

2.1. Wymagania ogólne

Serwer typu rack o wysokości maksymalnie 2U, przystosowany do montażu w standardowej szafie rack 19", przeznaczony do wykonywania i przechowywania kopii zapasowych. Obudowa musi obsługiwać minimum 8 dysków twardych 3,5" z interfejsem SAS/SATA, z możliwością instalacji dysków podczas pracy serwera (hot-plug).

UWAGA: Zamawiający posiada licencje oprogramowania Veeam Backup & Replication w wersji Enterprise Plus. W ramach zadania wymagana jest pełna konfiguracja i optymalizacja środowiska backupowego z wykorzystaniem posiadanych licencji.

2.2. Specyfikacja techniczna

Parametr	Wymagania minimalne
Obudowa	Typu rack max 2U; min. 8 dysków 3,5" hot-plug; szyny montażowe; organizator okablowania umożliwiający wysunięcie serwera (np. ramię organizujące lub inne rozwiązanie techniczne); panel diagnostyczny (LCD, LED lub moduł bezprzewodowy).
Płyta główna	Dedykowana płyta producenta serwera; TPM 2.0; zintegrowana karta sieciowa 2x 1GbE RJ45.
Procesory	Dwa procesory minimum 8 rdzeni/16 wątków; taktowanie minimum 2,6 GHz; cache minimum 22,5 MB; SPECrate2017_int_base minimum 169 pkt.
Pamięć RAM	Minimum 128 GB DDR5 RDIMM ECC 5600 MT/s; minimum 5 wolnych slotów; możliwość rozbudowy do 2 TB.
Kontroler RAID	Sprzętowy RAID SAS/SATA: RAID 0,1,5,6,10,50,60; cache minimum 4 GB z podtrzymaniem.
Kontroler HBA	HBA SAS 12Gb/s do macierzy zewnętrznej; PCIe Gen4; minimum 2 porty HD Mini-SAS.
Dyski SSD	2x SSD SATA minimum 480 GB; Read Intensive; RAID 1; przeznaczone na system operacyjny.
Dyski HDD	6x HDD SAS minimum 8 TB; 7200 RPM; 3,5" hot-plug; przeznaczone na dane backupu.
Karta sieciowa	Dwuportowa 10/25GbE SFP28 z iSCSI offload; wraz z 2 wkładkami SFP28 SR 25GbE.
Zarządzanie zdalne	Kontroler Enterprise; licencja bezterminowa; HTML5; IPMI 2.0, SNMP, SSH, Redfish.
Zasilanie	2x zasilacz hot-plug minimum 700W; 80 PLUS Titanium.
Chłodzenie	Redundantne wentylatory hot-plug.
System operacyjny	Windows Server 2025 Standard; licencja na minimum 16 rdzeni; prawo do 2 VM; 30 CAL User.
Gwarancja	36 miesięcy; serwis NBD w miejscu instalacji; usługa zachowania dysków twardych przez Zamawiającego w przypadku ich awarii (wymiana dysku bez konieczności zwrotu uszkodzonego – np. usługa typu Keep Your Drive / Defective Media Retention)."

2.3. Zakres wdrożenia środowiska kopii zapasowych

Wykonawca zobowiązany jest do przeprowadzenia pełnej konfiguracji środowiska backupowego obejmującej:

a) instalację i konfigurację Veeam Backup Server na dostarczonym serwerze z wykorzystaniem licencji Enterprise Plus posiadanych przez Zamawiającego;

- b) konfigurację repozytoriów backupowych z wykorzystaniem deduplikacji i kompresji, w tym repozytorium typu Hardened Repository (immutable) dla ochrony przed ransomware;
- c) wdrożenie polityki kopii zapasowych zgodnej z zasadą 3-2-1 oraz schematów rotacji GFS (dzienne, tygodniowe, miesięczne);
- d) konfigurację Backup Copy Jobs z replikacją do serwera NAS QNAP w lokalizacji kolokacyjnej przez szyfrowany tunel VPN;
- e) wdrożenie mechanizmów weryfikacji integralności kopii (SureBackup) z automatycznym harmonogramem;
- f) konfigurację harmonogramów wykonywania kopii z uwzględnieniem okien serwisowych;
- g) integrację z Active Directory i systemami bazodanowymi (application-aware processing dla MS SQL);
- h) konfigurację powiadomień e-mail i raportowania;
- i) instalację i konfigurację agenta systemu zbierania logów bezpieczeństwa zapewniającego monitoring integralności infrastruktury backupowej, wykrywanie anomalii oraz alertowanie zgodnie z wymaganiami KRI.

3. ZADANIE 2 – Macierz dyskowa

3.1. Wymagania ogólne

Macierz dyskowa typu SAN w obudowie rack o wysokości maksymalnie 2U, przystosowana do montażu w szafie 19", obsługująca minimum 24 dyski 2,5". Macierz przeznaczona jest do pracy jako współdzielona pamięć masowa dla klastra serwerów (Zadanie 3), zapewniająca wysoką dostępność danych poprzez redundancję kontrolerów i dysków.

3.2. Specyfikacja techniczna

Parametr	Wymagania minimalne
Obudowa	Typu rack maksymalnie 2U; minimum 24 dysków 2,5" hot-plug; szyny montażowe.
Kontrolery	Dwa kontrolery Active-Active; każdy: minimum 8 portów SAS 12Gb/s, minimum 32 GB cache z podtrzymaniem, możliwość rozbudowy do 64 GB.
Dyski HDD	11x HDD SAS minimum 2,4 TB; 10 000 RPM; 2,5" hot-plug.
Dyski SSD	2x SSD SAS minimum 1,92 TB; 12Gb/s; Read Intensive; tier wydajnościowy.
Funkcjonalności	RAID 0,1,5,6,10 i rozproszony; automatyczny tiering SSD/HDD; thin provisioning; snapshot; replikacja; FC/iSCSI/SAS.
Zarządzanie	GUI WWW; API REST; monitoring wydajności; predykcja awarii; alerty e-mail/SNMP.
Zasilanie	2x zasilacz hot-plug minimum 580W.
Kable	2x kabel HD Mini-SAS do HD Mini-SAS minimum 2m.
Gwarancja	36 miesięcy; serwis NBD; Keep Your Hard Drive.

3.3. Zakres wdrożenia macierzy dyskowej

Wykonawca zobowiązany jest do przeprowadzenia następujących prac:

- montaż macierzy w szafie rack, podłączenie do infrastruktury elektrycznej i aktualizacja firmware;
- utworzenie grup dysków i konfiguracja poziomów RAID (RAID 6 dla HDD, RAID 1 dla SSD);
- konfiguracja automatycznego tieringu między warstwą SSD i HDD oraz thin provisioning;
- utworzenie wolumenów logicznych (LUN) dla środowiska wirtualizacji i quorum klastra;
- podłączenie macierzy do serwerów klastra kablem SAS i konfiguracja MPIO;
- konfiguracja migawek (snapshot), monitoringu i eksportu logów do centralnego systemu zbierania logów (Syslog).

4. ZADANIE 3 – Serwery klastra wysokiej dostępności

4.1. Wymagania ogólne

Dwa identyczne serwery typu rack o wysokości maksymalnie 2U każdy, przeznaczone do pracy w klastrze wysokiej dostępności (Failover Cluster). Serwery będą korzystać ze współdzielonej macierzy dyskowej (Zadanie 2) jako pamięci masowej dla maszyn wirtualnych. Każdy serwer musi być wyposażony w serwerowy system operacyjny z licencją umożliwiającą wirtualizację (Hyper-V) i pracę w klastrze (Failover Clustering).

Poniższa specyfikacja dotyczy pojedynczego serwera – wymagana dostawa 2 sztuk o identycznej konfiguracji.

UWAGA: Licencje systemu operacyjnego muszą być dostarczone dla każdego serwera z osobna (łącznie 2 licencje na minimum 80 rdzeni każda).

4.2. Specyfikacja techniczna (na każdy serwer)

Parametr	Wymagania minimalne
Obudowa	Identyczna jak w Zadaniu 1.
Płyta główna	Identyczna jak w Zadaniu 1.
Procesory	Identyczne jak w Zadaniu 1.
Pamięć RAM	Minimum 256 GB DDR5 RDIMM ECC 5600 MT/s na serwer (512 GB łącznie); możliwość rozbudowy do 4 TB.
Kontroler RAID	Sprzętowy RAID SAS/SATA: RAID 0,1,10; cache minimum 4 GB.
Kontroler HBA	HBA SAS 12Gb/s; minimum 2 porty HD Mini-SAS.
Dysk wewnętrzny	1x HDD SAS minimum 600 GB; 10 000 RPM.
Dyski M.2	Kontroler M.2 z RAID 1; 2x M.2 NVMe minimum 480 GB w RAID 1.
Karta sieciowa 25GbE	Dwuportowa 10/25GbE SFP28; wraz z 2 wkładkami SFP28 SR 25GbE.
Karta sieciowa 1GbE	Czteroportowa 1GbE RJ45 PCIe; dedykowane 2 porty dla heartbeat klastra.
Zarządzanie zdalne	Identyczne jak w Zadaniu 1.
Zasilanie/Chłodzenie	Identyczne jak w Zadaniu 1.
System operacyjny	Windows Server 2025 Datacenter (lub równoważny, najnowszy dostępny); licencja musi obejmować wszystkie fizyczne rdzenie serwera (min. 16 core) i zapewniać prawo do uruchamiania nielimitowanej liczby środowisk wirtualnych (OSE) na każdym węźle klastra (niezbędne dla migracji Live Migration). Wymagane licencje dostępowe (CAL) w liczbie 30 szt. (jeśli nie ujęto w Zadaniu 1).
Gwarancja	Identyczna jak w Zadaniu 1.

4.3. Wymagania dla klastra wysokiej dostępności

Serwery muszą zapewniać: automatyczne przełączanie usług między węzłami (failover) z czasem przełączenia do 60 sekund; wspólny dostęp do zasobów na macierzy z MPIO; mechanizmy quorum z zewnętrznym świadkiem; migrację maszyn wirtualnych bez przestoju (Live Migration); dedykowane porty dla komunikacji klastrowej (heartbeat).

Serwery muszą posiadać zasoby obliczeniowe pozwalające na uruchomienie, oprócz planowanych usług produkcyjnych, również centralnego systemu zbierania i korelacji logów bezpieczeństwa z całej infrastruktury IT, zgodnego z wymaganiami Krajowych Ram Interoperacyjności (KRI) oraz RODO. System będzie działał w architekturze wysokiej dostępności wykorzystując mechanizmy klastrowe.

4.4. Zakres wdrożenia klastra i środowiska wirtualizacji

Wykonawca zobowiązany jest do przeprowadzenia następujących prac:

- a) instalacja systemów operacyjnych Windows Server na obu serwerach z aktualizacjami i dołączeniem do domeny AD;
- b) utworzenie klastra Failover Cluster z konfiguracją quorum, sieci klastrowych i Cluster Shared Volumes;
- c) instalacja roli Hyper-V, konfiguracja przełączników wirtualnych i ustawień Live Migration;
- d) wdrożenie centralnego systemu zbierania i korelacji logów (SIEM). Wymagania wdrożeniowe:
 - Podłączenie źródeł: AD, Serwery Plików, UTM, Macierz.
 - Konfiguracja retencji danych: min. 30 dni on-line.
 - Implementacja minimum 15 scenariuszy korelacyjnych (Use Cases), np.: wielokrotne błędne logowanie, dodanie użytkownika do grupy Admin, wykrycie skanowania portów, komunikacja z podejrzanyimi IP (Threat Intel).
 - Utworzenie dashboardu wizualizującego stan bezpieczeństwa.
- e) instalację agentów monitoringu na wszystkich serwerach Windows zapewniających zbieranie logów, monitoring integralności plików (FIM), wykrywanie zagrożeń i raportowanie zgodności.

5. ZADANIE 4 – Urządzenie UTM Firewall oraz przełączniki sieciowe

5.1. Urządzenie UTM Firewall (1 sztuka)

5.1.1. Wymagania ogólne

Urządzenie klasy UTM (Unified Threat Management) typu Next-Generation Firewall zapewniające kompleksową ochronę sieci. Urządzenie musi umożliwiać centralne zarządzanie przełącznikami dostarczonymi w ramach niniejszego zadania (funkcja Switch Controller).

5.1.2. Specyfikacja techniczna

Parametr	Wymagania minimalne
Interfejsy sieciowe	Minimum 10 portów GbE RJ45 (7 LAN/DMZ, 2 WAN, 1 HA/zarządzanie).
Przepustowość firewall	Minimum 8 Gbps (UDP 1518B).
Przepustowość IPS	Minimum 1,4 Gbps.
Przepustowość VPN IPSec	Minimum 5 Gbps (AES-256).
Przepustowość Threat Protection	Minimum 800 Mbps (IPS+AppControl+Antimalware).
Sesje jednoczesne	Minimum 1 500 000.
System IPS	IPS/IDS z aktualizowaną bazą sygnatur.
Ochrona antymalware	AMP z funkcją sandboxing.
Kontrola aplikacji	Identyfikacja minimum 3000 aplikacji.
Filtrowanie URL/DNS	Kategoryzacja stron (minimum 70 kategorii); DNS Security.
VPN	IPSec site-to-site; SSL VPN z klientem dla Windows/macOS/Linux/iOS/Android.
Switch Controller	Centralne zarządzanie przełącznikami tego samego producenta.
Logowanie	Lokalne logi; eksport Syslog/API do zewnętrznego SIEM.
Subskrypcja	Licencja na IPS, AMP, AppControl, URL/DNS Filtering na 12 miesięcy.
Gwarancja	12 miesięcy gwarancji sprzętowej.

5.2. Przełączniki sieciowe (2 sztuki)

5.2.1. Wymagania ogólne

Przełącznik sieciowy warstwy 2 (L2) kompatybilny z urządzeniem UTM dostarczonym w ramach niniejszego zadania. Przełącznik musi być zarządzany z poziomu urządzenia UTM (funkcja Switch Controller). Konstrukcja bezwentylatorowa (fanless). Wymagana dostawa 2 identycznych sztuk.

5.2.2. Specyfikacja techniczna (na każdy przełącznik)

Parametr	Wymagania minimalne
Porty dostępne	Minimum 48 portów GbE RJ45.
Porty uplink	Minimum 4 porty SFP+/SFP 10G/1G.
Przepustowość	Minimum 56 Gbps full-duplex.
Tablica MAC	Minimum 16 000 adresów.
Funkcjonalności L2	VLAN 802.1Q (min. 256); LACP 802.3ad; STP/RSTP/MSTP; Port Mirroring; IGMP Snooping.
QoS	802.1p, DSCP; minimum 8 kolejek na port.
Zarządzanie	Z poziomu Switch Controller na UTM; opcjonalnie autonomiczne GUI/CLI.
Konstrukcja	Przystosowana do montażu w szafie Rack 19". Chłodzenie: pasywne lub aktywne (wentylatorowe) – przystosowane do pracy ciągłej. W przypadku chłodzenia aktywnego wymagana regulacja obrotów lub niski poziom hałasu.

Parametr	Wymagania minimalne
Subskrypcja	Wsparcie producenta na 12 miesięcy.
Gwarancja	12 miesięcy.

5.3. Zakres wdrożenia infrastruktury sieciowej

Wykonawca zobowiązany jest do przeprowadzenia następujących prac:

- a) montaż urządzeń w szafie rack, aktualizacja firmware, aktywacja licencji i konfiguracja Switch Controller;
- b) konfiguracja interfejsów sieciowych UTM (WAN, LAN, DMZ), routingu i NAT/PAT;
- c) opracowanie i wdrożenie polityki firewall zgodnie z zasadą najmniejszych uprawnień;
- d) konfiguracja IPS, ochrony antymalware z sandboxing, kontroli aplikacji i filtrowania URL/DNS;
- e) konfiguracja VPN IPSec site-to-site do kolokacji oraz VPN SSL dla użytkowników zdalnych;
- f) konfiguracja przełączników: VLAN, agregacja łączy (LACP), Spanning Tree, Port Mirroring;
- g) konfiguracja eksportu logów z UTM do centralnego systemu zbierania logów (Syslog/API).

6. ZADANIE 5 – Serwer NAS

6.1. Wymagania ogólne

Serwer pamięci masowej typu NAS (Network Attached Storage) przeznaczony do przechowywania danych i udostępniania zasobów w sieci lokalnej. Urządzenie typu rack o wysokości maksymalnie 3U z możliwością instalacji dysków 3,5" oraz 2,5". System operacyjny wbudowany, oparty na systemie plików ZFS lub równoważnym zapewniającym integralność danych.

6.2. Specyfikacja techniczna

Parametr	Wymagania minimalne
Obudowa	Typu rack maksymalnie 3U; umożliwiającą instalację minimum 16 dysków logicznych (w konfiguracji np. 12x 3,5" LFF lub 24x 2,5" SFF, lub konfiguracji mieszanej), zapewniającą wymaganą przez Zamawiającego przestrzeń użyteczną danych.
Procesor	x86-64; minimum 4 rdzenie/8 wątków; minimum 2,6 GHz.
Pamięć RAM	Minimum 32 GB DDR4 ECC; możliwość rozbudowy do 128 GB.
Interfejsy sieciowe	Minimum 4x GbE RJ45 z agregacją; minimum 2x 10GbE SFP+ lub RJ45.
Porty rozszerzeń	Minimum 2 sloty PCIe; minimum 2 porty USB 3.0.
System plików	ZFS lub równoważny z checksum, self-healing, kompresją.
Poziomy RAID	RAID 0,1,5,6,10, RAIDZ/RAIDZ2/RAIDZ3.
Protokoły	SMB/CIFS 3.0, NFS v3/v4, iSCSI, FTP/SFTP.
Funkcjonalności	Snapshots z harmonogramem; Previous Versions; replikacja; szyfrowanie AES-256; integracja AD/LDAP.
Zasilanie	2x redundantny zasilacz hot-swap.
Zarządzanie	GUI WWW; alerty e-mail/SNMP; eksport logów Syslog.
Gwarancja	24 miesiące.

6.3. Zakres wdrożenia serwera NAS

Wykonawca zobowiązany jest do przeprowadzenia następujących prac:

- montaż serwera NAS w szafie rack, aktualizacja firmware, konfiguracja sieci i agregacji łączy;
- utworzenie puli dyskowej z konfiguracją RAID (RAIDZ2 lub RAID 6);
- utworzenie wolumenów/udziałów SMB/CIFS i NFS zgodnie z wymaganiami Zamawiającego;
- integracja z Active Directory i konfiguracja uprawnień dostępu;
- konfiguracja automatycznych migawek (snapshots) i funkcji Previous Versions;
- konfiguracja monitoringu, alertów i eksportu logów do centralnego systemu zbierania logów (Syslog);
- opcjonalnie: konfiguracja usługi iSCSI Target dla świadka quorum klastra.

7. ZAKRES PRAC WDROŻENIOWYCH WSPÓLNYCH

7.1. Instalacja fizyczna

Transport sprzętu do siedziby Zamawiającego, rozpakowanie i weryfikacja kompletności dostawy z protokołem numerów seryjnych. Montaż wszystkich urządzeń w szafach rack 19" z wykorzystaniem szyn montażowych i ramion kablowych. Podłączenie do infrastruktury elektrycznej z wykorzystaniem redundantnych zasilaczy. Wykonanie okablowania strukturalnego (SAS, 25GbE, 1GbE) z oznakowaniem wszystkich kabli i portów. Konfiguracja kontrolerów zdalnego zarządzania (iLO/iDRAC).

7.2. Integracja z istniejącą infrastrukturą

Integracja nowej infrastruktury sieciowej z istniejącą siecią Zamawiającego. Integracja serwerów z usługą katalogową Active Directory. Konfiguracja uwierzytelniania AD dla wszystkich komponentów (UTM, NAS, Veeam). Konfiguracja replikacji backupów do serwera QNAP w kolokacji przez VPN. Integracja systemu powiadomień z infrastrukturą e-mail Zamawiającego.

7.3. Migracja danych i usług

Szczegółowa inwentaryzacja maszyn wirtualnych i danych do migracji. Opracowanie planu migracji z określeniem kolejności, okien migracyjnych i procedur rollback. Wykonanie pełnych kopii zapasowych przed migracją. Migracja maszyn wirtualnych na nową infrastrukturę klastrową (V2V lub P2V). Migracja danych na nowy serwer NAS z zachowaniem struktury i uprawnień NTFS/ACL. Migracja konfiguracji firewall i VPN na nowe urządzenie UTM. Rekonfiguracja zadań backupowych na nowe środowisko.

7.4. Testy i walidacja

Testy funkcjonalne wszystkich komponentów. Testy wydajnościowe (benchmark macierzy, przepustowość sieci). Testy wysokiej dostępności klastra (failover/failback). Testy odtwarzania z kopii zapasowych (pełne VM, granular restore). Testy bezpieczeństwa (weryfikacja reguł firewall, VPN, skanowanie podatności). Testy systemu zbierania logów (weryfikacja źródeł, alertów, korelacji). Sporządzenie dokumentacji wyników testów.

7.5. Szkolenia

Przeprowadzenie szkolenia dla minimum 2 administratorów Zamawiającego w wymiarze minimum 16 godzin zegarowych (2 dni robocze). Szkolenie w siedzibie Zamawiającego na wdrożonej infrastrukturze (hands-on). Zakres: administracja serwerami Windows Server, zarządzanie klastrem Failover i Hyper-V, administracja macierzą i NAS, zarządzanie środowiskiem backupowym Veeam, administracja UTM, obsługa systemu zbierania i analizy logów bezpieczeństwa. Przygotowanie materiałów szkoleniowych w języku polskim. Wydanie zaświadczeń o ukończeniu szkolenia.

7.6. Dokumentacja powykonawcza

Dokumentacja powykonawcza infrastruktury (schematy logiczne i fizyczne sieci, konfiguracje, wykaz numerów seryjnych i licencji). Dokumentacja dostępów administracyjnych w zabezpieczonej kopercie. Instrukcje administracyjne w języku polskim dla wszystkich systemów. Procedury backup i odtwarzania awaryjnego zgodne z ISO 22301. Procedury obsługi incydentów bezpieczeństwa z wykorzystaniem wdrożonego systemu monitoringu. Dokumentacja testów. Całość w formie elektronicznej i 2 egzemplarzach papierowych.

8. WARUNKI DOSTAWY I REALIZACJI

8.1. Termin realizacji

Maksymalny termin realizacji całości przedmiotu zamówienia: 35 dni kalendarzowych od dnia podpisania umowy.

8.2. Warunki dostawy

Dostawa na koszt i ryzyko Wykonawcy do siedziby Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta. Wykonawca zobowiązany jest dostarczyć dokumentację techniczną w języku polskim lub angielskim. Wraz z dostawą należy przekazać karty gwarancyjne, licencje oraz nośniki instalacyjne (jeśli dotyczy).

9. ZESTAWIENIE ILOŚCIOWE

Lp.	Nazwa	Ilość
1	Serwer kopii zapasowych z systemem operacyjnym i wdrożeniem	1 szt.
2	Macierz dyskowa z wdrożeniem	1 szt.
3	Serwer klastra z systemem operacyjnym i wdrożeniem	2 szt.
4a	Urządzenie UTM Firewall z licencją 12 mies. i wdrożeniem	1 szt.
4b	Przełącznik sieciowy L2 z licencją 12 mies. i wdrożeniem	2 szt.
5	Serwer NAS z wdrożeniem	1 szt.

10. INFORMACJE DODATKOWE

Wszystkie urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Unii Europejskiej.

Zamawiający wymaga możliwości weryfikacji legalności i źródła pochodzenia sprzętu u producenta na podstawie numeru seryjnego.

Serwisy gwarancyjne muszą być realizowane przez autoryzowany serwis producenta na terenie Polski.

Urządzenia sieciowe (UTM i przełączniki) muszą pochodzić od tego samego producenta i być ze sobą kompatybilne w zakresie centralnego zarządzania.

Wymóg kompatybilności urządzeń sieciowych (UTM i Przełączniki) wynika z konieczności zapewnienia zautomatyzowanej ochrony sieci wewnętrznej (tzw. Security Fabric / SD-Branch). System musi umożliwiać zarządzanie portami przełączników bezpośrednio z interfejsu UTM lub jednej centralnej konsoli, w tym automatyczną izolację zainfekowanego hosta na poziomie portu switcha po wykryciu zagrożenia przez system IPS.

W przypadku zaoferowania rozwiązań równoważnych, Wykonawca załączy do oferty szczegółową specyfikację techniczną potwierdzającą spełnienie wymagań.

Zamawiający posiada licencje oprogramowania Veeam Backup & Replication w wersji Enterprise Plus – w ramach wdrożenia wymagana jest pełna konfiguracja istniejącego środowiska.

Centralny system zbierania i korelacji logów bezpieczeństwa musi być oparty na oprogramowaniu open-source lub dostarczony z licencją bezterminową bez ograniczeń liczby monitorowanych urządzeń i użytkowników.

Wykonawca udzieli wsparcia technicznego w okresie 30 dni od daty podpisania protokołu odbioru końcowego.