

Załącznik nr 1 do SWZ
Opis przedmiotu zamówienia

(Znak postępowania: ADM.26.28.2026)

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

CZ. I. SERWER DO KLASTRA HA I SERWER DLA USŁUG BEZPIECZEŃSTWA

Postanowienia ogólne dotyczące równoważności

Wszędzie tam, gdzie w OPZ wskazano nazwę produktu, producenta, normę, certyfikat lub program licencjonowania, Zamawiający dopuszcza rozwiązania równoważne, tzn. spełniające co najmniej te same parametry techniczne, funkcjonalne i jakościowe oraz zapewniające pełną kompatybilność z posiadaną przez Zamawiającego infrastrukturą sprzętową i programową. Wykonawca powołujący się na rozwiązanie równoważne jest obowiązany wykazać równoważność, składając na zasadach określonych w par. 4 ust. 5 umowy, dokumenty potwierdzające spełnienie kryteriów określonych w OPZ (karty katalogowe, certyfikaty, oświadczenia producenta, dokumentację techniczną). Ciężar udowodnienia równoważności spoczywa na Wykonawcy. Wskazanie przykładowego producenta serwera w pkt 4 części A zostało uzasadnione potrzebą zapewnienia bezawaryjnej pracy, jednolitego wsparcia i stabilności produkcyjnego klastra HA, zgodnie z art. 99 ust. 4 i 5 ustawy Pzp.

A. Przedmiotem zamówienia jest dostawa, montaż, konfiguracja oraz wdrożenie fabrycznie nowego serwera (1 szt.) do klastra HA wraz z licencjami systemu operacyjnego, 36-miesięcznym wsparciem technicznym producenta oraz usługami wdrożeniowymi.

1. Wymagania techniczne urządzenia

Zaoferowane urządzenie musi spełniać poniższe minimalne parametry techniczne i wydajnościowe:

Parametr / Cecha	Minimalne wymagania techniczne
Producent	Serwer HPE ProLiant DL360 w generacji nowszej niż Gen10 Plus lub inny serwer o wysokości 1U spełniający poniższe wymagania oraz charakteryzujący się pełną równoważnością technologiczną i funkcjonalną (uzasadnienie w pkt 4).
Obudowa	- Do zabudowy w szafie serwerowej 19", wraz ze wszystkimi elementami niezbędnymi do mocowania oraz wysuwania do celów serwisowych bez odpinania kabli. - Wszystkie wyspecyfikowane elementy serwera zamontowane w jednej obudowie o maksymalnej wysokości 1U. - Na frontowym panelu obudowy sygnalizacja statusu pracy serwera (co najmniej umożliwiająca łatwą lokalizację serwera poprzez zapalenie diody LED lub wyświetlacza LCD).
Typ procesora	- Procesor minimum 16 rdzeniowy - Taktowany zegarem minimum 2,3 GHz

	3. Zgodny z architekturą x86/64 bity, 4. Osiągający w teście PassMark CPU Mark wynik minimum 45.000 punktów według wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Kryterium równoważności (PassMark): wynik weryfikowany jest według wartości opublikowanej na stronie cpubenchmark.net Obowiązująca tabela z wynikami testu PassMark w Załączniku nr 1 do OPZ. Dla procesora nieobecnego na liście Wykonawca przedstawia raport z testu PassMark przeprowadzonego na zaoferowanej konfiguracji, wykazujący wynik nie niższy niż 45.000 punktów. Procesor producenta Intel, tego samego co w istniejących węzłach klastra, zapewniający Live Migration maszyn wirtualnych między wszystkimi trzema węzłami (uzasadnienie w pkt 4). Dopuszcza się tryb zgodności procesora (Processor Compatibility Mode).
Ilość procesorów	1 szt.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach.
Pamięć	1. Min. 128 GB pamięci DIMM DDR5 z Advanced ECC lub chipkill, 6400 MT/s, zainstalowane w min. 4 modułach. 2. Po zamontowaniu min. 12 wolnych slotów DIMM. 3. Możliwość rozbudowy pamięci do min. 4 TB.
Płyta główna	dedykowana do pracy w serwerach.
Złącza wewnętrzne	min. 1 wolne złącze PCIe 5.0 x16
Dyski	- Możliwość instalacji min. 8 dysków NVMe z opcją wyjmowania i instalowania na gorąco (bez wyłączania serwera) - Min. 2x 480GB NVMe Hot-Plug zainstalowane na dedykowanym kontrolerze sprzętowym (nie mogą zajmować wnęk przeznaczonych dla dysków NVMe z pierwszego punktu), pracujące w RAID 1 na system operacyjny hosta
Karty sieciowe	Min. 4 porty 10GbE RJ-45 (dopuszcza się kartę w złączu OCP), w tym min. 2 porty wyłącznie dla ruchu iSCSI, przy zachowaniu wolnego złącza PCIe 5.0 x16. Interfejsy obsługują iSCSI i MPIO. W komplecie patchcordy Cat. 6A w liczbie odpowiadającej liczbie portów.
Złącza zewnętrzne	min. 4x USB 3.2 Gen1 (w tym min. 1x z przodu obudowy, 1x wewnętrzny), min. 1xVGA
Zdalny interfejs zarządzający	Serwer musi być wyposażony w sprzętowe rozwiązanie zdalnego zarządzania, pochodzące od producenta serwera, niezależne od systemów operacyjnych, posiadające dedykowane złącze RJ-45, umożliwiające zdalny dostęp do graficznego interfejsu Web karty zarządzającej, zapewniające przynajmniej następujące funkcjonalności:

	• zdalne włączenie serwera, • zdalne wyłączenie serwera, • restart serwera, • podgląd logów sprzętowych serwera i karty, • przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu i restartu OS), • rozwiązanie musi być dostarczone wraz z niezbędnymi licencjami umożliwiającymi pracę zdalną na serwerze (wirtualny KVM) z użyciem przeglądarki internetowej, w tym pełną możliwość zdalnego podłączenia napędów wirtualnych typu CD/DVD oraz wirtualnych folderów.
Karta graficzna	Zintegrowana, pozwalająca na prace z rozdzielczością min. 1920x1200
Zasilacz	230V 50Hz, min. 2 szt. Hot-plug, Titanium, nadmiarowe (redundantne), każdy o mocy min. 800 W wystarczającej do pracy serwera w oferowanej konfiguracji z zapasem min. 30% oraz do rozbudowy pamięci do wartości maksymalnej
Chłodzenie	Nadmiarowe wentylatory typu hot-plug
Warunki pracy	Pomieszczenia biurowe, 10-30 °C.
Wyposażenie dodatkowe	kable zasilające i szyny montażowe w komplecie
Gwarancja	Przynajmniej 36 miesięcy gwarancji (na części, robociznę i pomoc techniczną) z czasem reakcji na zgłoszenie usterki maksymalnie w następnym dniu roboczym, przyjmowanie zgłoszeń 9 godzin na dobę, 5 dni w tygodniu. Zamawiający wymaga, aby zarządzanie gwarancją i zgłoszeniami gwarancyjnymi odbywało się przez system/stronę producenta (możliwość sprawdzenia stanu gwarancji, wykonywania zgłoszeń oraz sprawdzania stanu zgłoszeń bieżących i historycznych).
System operacyjny	Dostawa fabrycznie nowych, wieczystych licencji Microsoft Windows Server 2025 (edycja Standard lub Datacenter do wyboru Wykonawcy) w aktualnym programie licencjonowania zbiorowego (Microsoft CSP – Software lub równoważny), na pełną liczbę fizycznych rdzeni serwera (nie mniej niż 16), w liczbie umożliwiającej jednoczesne uruchomienie na nowym węźle min. 6 maszyn wirtualnych z systemem Windows Server, oraz 25 licencji dostępowych Windows Server CAL 2025 typu User CAL. Wymagania: • licencje w postaci elektronicznej, przypisane do profilu Zamawiającego w portalu administracyjnym producenta (Microsoft Admin Center), • licencje wieczyste, pochodzące z oficjalnego i autoryzowanego kanału dystrybucji producenta na rynek europejski, • licencja uprawnia do uruchomienia min. 6 maszyn wirtualnych na zlicencjonowanym serwerze, • licencje obejmują prawo do niższej wersji (downgrade), w tym do instalacji Windows Server 2022 oraz 2019, • licencje CAL uprawniają do dostępu do serwerów Windows Server w wersji 2025 i wcześniejszych (w tym do węzłów

	klastra pracujących w wersji 2019), pochodzą z tego samego programu licencjonowania co licencje serwerowe i są dostarczone bez dodatkowych kosztów po stronie Zamawiającego. Uzasadnienie: Zamawiający wymaga systemu Microsoft Windows Server, ponieważ klastr Hyper-V/WSFC składa się z węzłów Windows Server, a inne systemy nie umożliwiają budowy wspólnego klastra. W klastrze z migracją na żywo maszyny wirtualne mogą działać na dowolnym węźle, dlatego licencje muszą pokrywać min. 6 maszyn wirtualnych (obecna liczba maszyn w klastrze). Kryterium równoważności (licencje Windows Server i CAL): za równoważne uznaje się licencje serwerowe i dostępne producenta systemu serwerowego, który umożliwia budowę wspólnego klastra z istniejącymi węzłami Windows Server, w ramach programu licencjonowania zbiorowego, w którym licencje: (a) są wieczyste, (b) mają postać elektroniczną i są przypisane do profilu Zamawiającego w portalu producenta, (c) pochodzą z autoryzowanego kanału dystrybucji na rynek europejski, (d) obejmują prawo do niższej wersji, (e) w liczbie 25 uprawniają użytkowników do dostępu do serwerów w wersji nie niższej niż najwyższa wersja uruchomiona w klastrze. Dowód: oświadczenie Wykonawcy lub autoryzowanego partnera producenta z opisem licencji (nazwa, wersja, edycja, typ, liczba) składane na zasadach określonych w par. 4 ust. 5 umowy,.
--	--

2. Wsparcie techniczne producenta (36 miesięcy)

Wykonawca zapewni usługi wsparcia świadczone bezpośrednio przez producenta sprzętu na okres 36 miesięcy:

- wsparcie techniczne producenta (czas reakcji na zgłoszenie usterki maksymalnie w następnym dniu roboczym, przyjmowanie zgłoszeń 9 godzin na dobę, 5 dni w tygodniu);
- dostęp do serwisu i zgłoszeń 9x5,
- prawo do bezpłatnej aktualizacji oprogramowania układowego (firmware) i poprawek bezpieczeństwa,
- gwarancja naprawy/wymiany sprzętu w przypadku awarii z czasem wysyłki części zastępczej w następnym dniu roboczym (NBD).

3. Wymagania dotyczące usług wdrożeniowych i konfiguracji

Zakres prac: podłączenie nowego serwera (węzła) do klastra Windows Server Failover Clustering (WSFC) z macierzą NetApp

3.1. Przygotowanie serwera

- Weryfikacja wersji Windows Server: zgodność z pozostałymi węzłami klastra (ta sama wersja/build/patch level).
- Instalacja roli Failover Clustering (Add Roles and Features).
- Instalacja funkcji Multipath I/O (MPIO).
- Instalacja roli Hyper-V

- Instalacja NetApp Windows Host Utilities / DSM (Device Specific Module) zgodnie z IMT (lub natywnego MSDSM, jeśli IMT go dopuszcza).
- Aktualizacja sterowników i firmware karty sieciowej (iSCSI) do wersji zalecanej przez NetApp.
- Konfiguracja sieci: min. 2 porty dla klastra (Cluster/Heartbeat + Management), min. 2 porty w osobnej sieci/VLAN dla iSCSI (bez routingu na sieci produkcyjne), porty dla sieci maszyn wirtualnych i Live Migration zgodnie z architekturą klastra Zamawiającego.

Kryterium równoważności (zgodność wersji Windows Server): wymóg uznaje się za spełniony, gdy nowy węzeł pracuje w tej samej wersji co pozostałe węzły (w ramach prawa do niższej wersji). Jeżeli producent serwera nie wspiera tej wersji, dopuszcza się inną wersję, pod warunkiem wykazania wsparcia producenta serwera i Microsoft dla takiej konfiguracji, pozytywnego Test-Cluster i zachowania ciągłości działania. Dowód: oświadczenie Wykonawcy z opisem sposobu realizacji, składane na zasadach określonych w par. 4 ust. 5 umowy.

Kryterium równoważności (NetApp Host Utilities / DSM / MPIO): dopuszcza się rozwiązanie równoważne (inny moduł DSM/MPIO), pod warunkiem że: (a) jest wspierane przez NetApp dla wersji ONTAP i systemu operacyjnego Zamawiającego (potwierdzenie w IMT), (b) zapewnia min. 2 aktywne ścieżki do każdego LUN, (c) obsługuje ALUA i politykę równoważenia obciążenia zalecaną przez NetApp. Dowód: wydruk z IMT lub oświadczenie producenta składane na zasadach określonych w par. 4 ust. 5 umowy.

3.2. Konfiguracja MPIO

- Włączenie obsługi urządzeń MPIO dla macierzy NetApp (mpclaim lub GUI: MPIO Control Panel → Discover Multi-Paths → dodanie "NETAPP LUN").
- Ustawienie polityki Load Balance Policy zgodnie z rekomendacją NetApp (zwykle Round Robin lub ALUA).
- Weryfikacja obsługi ALUA (Asymmetric Logical Unit Access), zalecane dla ONTAP.
- Restart serwera po instalacji MPIO/DSM.

3.3. Podłączenie do storage (iSCSI)

- Konfiguracja iSCSI Initiator (iscsicpl): odczyt IQN serwera, podłączenie do portali docelowych NetApp (min. 2 sesje dla redundancji, MPIO per sesja), dodanie IQN do igroup (typ: Windows), trwałe (persistent) połączenie targetów po restarcie.

3.4. Konfiguracja LUN po stronie NetApp

- Udostępnienie nowemu węzłowi istniejących LUN-ów klastra.
- Mapowanie LUN do igroup zawierającej WSZYSTKIE węzły klastra (istniejące + nowy).
- Ustawienie ostype = windows oraz odpowiedniego LUN ID spójnego dla wszystkich węzłów.
- Weryfikacja, czy dysk quorum (Quorum Disk) jest widoczny z nowego węzła.

3.5. Konfiguracja dysków w Windows

- Skanowanie nowych urządzeń (Update-HostStorageCache, Diskmgmt.msc).
- Weryfikacja ścieżek MPIO (mpclaim -s -d): każdy LUN powinien mieć min. 2 aktywne ścieżki.

- Dyski klastrowe muszą pozostać Offline na nowym węźle do momentu dodania go do klastra. Windows zarządza stanem Online/Offline w zależności od tego, który węzeł posiada dany zasób.
- Brak inicjalizacji/formatowania: dyski są już sformatowane (NTFS/ReFS) i muszą zachować tę samą sygnaturę na wszystkich węzłach.

3.6. Dodanie węzła do klastra

- Add-ClusterNode -Name <NowyServer>.
- Test-Cluster: walidacja z uwzględnieniem nowego węzła (obowiązkowa).
- Weryfikacja, że wszystkie dyski klastrowe (Cluster Disks) są widoczne z nowego węzła jako potencjalne zasoby (Failover Cluster Manager → Disks).
- Sprawdzenie Possible Owners dla każdego zasobu dyskowego/roli i dodanie nowego węzła jako możliwego właściciela (Set-ClusterOwnerNode lub GUI).
- Jeśli istnieje dysk kworum (Disk Witness): weryfikacja widoczności z nowego węzła.

3.7. Konfiguracja sieci klastra

- Weryfikacja, że sieci klastra (heartbeat, sieć klienta) obejmują nowy węzeł, a sieć iSCSI jest wykluczona z komunikacji klastra. Nie przewiduje się zmiany adresacji ani topologii sieci istniejących węzłów.

3.8. Testy funkcjonalne (w oknie serwisowym uzgodnionym z Zamawiającym)

- Move-ClusterGroup: przeniesienie wybranej roli/grupy zasobów na nowy węzeł.
- Weryfikacja poprawnego przełączenia dysku Offline → Online na nowym węźle (bez błędów w Event Log – Disk/Cluster).
- Test failover maszyn wirtualnych na nowy węzeł przez kontrolowane wyłączenie węzła.
- Test Live Migration oraz kontrolowanego failover istniejącej maszyny wirtualnej z Microsoft SQL Server 2019 na nowy węzeł: weryfikacja, że maszyna uruchamia się poprawnie, usługa SQL Server startuje, a aplikacje klienckie systemu ERP ponownie nawiązują połączenie.
- Pomiar i udokumentowanie czasu przełączenia.

3.9. Dodatkowo – role klastra

- Weryfikacja działania istniejącej maszyny wirtualnej z Microsoft SQL Server 2019 na nowym węźle (uruchomienie usługi SQL Server, dostępność baz danych, zadania SQL Server Agent).

3.10. Dokumentacja

1. Aktualizacja listy Possible/Preferred Owners per rola
2. Cluster Validation Report (eksport)
3. Dokumentacja powykonawcza: konfiguracja sieci, MPIO i storage oraz wersje firmware i sterowników

3.11. Obowiązki Zamawiającego: zapewnienie portów i VLAN na przełącznikach (10GBASE-T), adresacji IP, dostępu administracyjnego do klastra, macierzy NetApp, maszyny z SQL Server i systemu ERP oraz okna serwisowego na czas testów.

4. Warunki dostawy i gwarancji

Pochodzenie sprzętu: z oficjalnego kanału dystrybucyjnego producenta na rynek UE, fabrycznie nowy (wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą), nieprzeznaczony przez producenta do wycofania z produkcji (EoL) na dzień składania ofert, objęty pełną opieką serwisową.

Wsparcie klastra: wsparcie dla rozbudowanego klastra (trzy serwery) świadczy jeden producent (HPE) lub Wykonawca zapewnia pełną spójność obsługi zgłoszeń serwisowych dla nowo dostarczanego węzła.

Certyfikat NetApp: Wykonawca (lub osoba skierowana do realizacji) musi wykazać w terminie określonym, w par. 4 umowy posiadanie uprawnień do rekonfiguracji macierzy NetApp. Dopuszcza się certyfikat, status partnerski lub inne potwierdzenie NetApp albo autoryzowanego dystrybutora o kompetencjach w zakresie ONTAP nie mniejszych niż wymagane. Dla certyfikatu osobowego dodatkowo wskazanie osoby i podstawy dysponowania nią.

Kryteria odbioru: (a) pozytywny Test-Cluster z istniejącymi węzłami, (b) min. 2 aktywne ścieżki do każdego LUN, (c) udane Live Migration i failover maszyn wirtualnych, w tym maszyny z SQL Server (start maszyny, usługi SQL, połączenie z bazą), (d) dokumentacja powykonawcza. W razie niepowodzenia Test-Cluster Wykonawca wymienia serwer lub usuwa przyczynę na własny koszt zgodnie z postanowieniami §5a ust. 5 pkt. 2) projektu umowy.

Wskazanie producenta referencyjnego (HPE):

Zamawiający wskazuje przykładowy serwer marki HPE, jako reprezentujący architekturę tożsamą z producentem istniejących węzłów klastra.

Uzasadnienie (art. 99 ust. 4 i 5 ustawy Pzp):

Zamawiający określił przedmiot zamówienia za pomocą wskazania marki referencyjnej, dopuszczając rozwiązania równoważne, z uwagi na fakt, że serwer jest trzecim węzłem produkcyjnego klastra, w którym pracują serwery HPE, w związku z czym:

- wsparcie i gwarancję całego klastra ma świadczyć jeden producent lub Wykonawca w ramach serwisu musi zapewnić jednoznaczny punkt kontaktowy w eliminacji sporów kompetencyjnych przy awariach obejmujących więcej niż jeden węzeł,
- węzły są zarządzane przez wspólny mechanizm zdalnego zarządzania i aktualizacji firmware producenta, a inna platforma bez natywnej integracji wymagałaby odrębnych procedur, narzędzi i szkoleń oraz zwiększałaby ryzyko niezgodności firmware i sterowników,
- węzeł innego producenta musi przeznaczyć i przejść bezbłędnie pełne testy zgodności klastra (Test-Cluster), a w razie niepowodzenia Wykonawca zobowiązany jest do usunięcia niezgodności na własny koszt.

Odrębnie, wymóg procesora Intel wynika z ograniczeń Hyper-V: migracja na żywo maszyn wirtualnych nie jest możliwa między węzłami z procesorami różnych producentów (Intel/AMD), a tryb zgodności procesora działa tylko w obrębie jednego producenta.

Dowody: Wykonawca składa na zasadach określonych w par. 4 ust. 5 umowy: kartę katalogową (QuickSpecs lub Data Sheet) serwera z numerami usług wsparcia oraz oświadczenie Wykonawcy o spełnieniu wymagań, w tym o objęciu klastra wsparciem spełniającym warunki OPZ. Najpóźniej przy dostawie oświadczenie producenta lub dystrybutora o pochodzeniu z kanału UE, dacie produkcji i braku zapowiedzi EoL.

- B. Przedmiotem zamówienia jest dostawa, montaż, konfiguracja oraz wdrożenie fabrycznie nowego serwera systemów bezpieczeństwa wraz z systemem operacyjnym, 36-miesięcznym pakietem subskrypcji usług bezpieczeństwa, wsparciem technicznym producenta oraz usługami wdrożeniowymi.**

Serwer bezpieczeństwa – opis funkcjonalny i architektura

- **Rola w infrastrukturze:**

Serwer fizyczny stanowi platformę pod środowisko wirtualizacyjne dedykowane dla usług bezpieczeństwa IT, monitorowania infrastruktury oraz zarządzania logami (systemy klasy SIEM, np. Wazuh oraz NMS, np. Zabbix). Wdrożenie obejmuje konfigurację dostępu do zasobów dyskowych posiadanej macierzy NetApp (poprzez LUN/datastore) w celu zapewnienia wysokiej wydajności i ciągłości przetwarzania danych operacyjnych.

- **Wymagania dotyczące przestrzeni dyskowej:**

Zainstalowane dyski fizyczne o pojemności 12 TB stanowią lokalne repozytorium danych na potrzeby długoterminowej retencji logów zdarzeń, danych historycznych z systemów monitoringu oraz buforowania danych analitycznych.

- **Skalowalność i obsługa zadań backupowych:**

Konstrukcja oraz wyposażenie sprzętowe serwera muszą umożliwiać bezobsługowe pełnienie funkcji lokalnego repozytorium backupowego w ramach rozbudowy środowiska. Serwer musi zapewniać pełne wsparcie dla integracji z oprogramowaniem do tworzenia kopii zapasowych (np. Veeam) oraz sprzętowymi napędami/bibliotekami taśmowymi (LTO).

Kryterium równoważności (Wazuh, Zabbix, Veeam, LTO): nazwy mają charakter przykładowy. Za równoważne uznaje się oprogramowanie o tożsamej funkcji (SIEM, monitoring, backup), wspierane na zaoferowanej platformie. Serwer musi: (a) umożliwiać pełnienie roli repozytorium backupowego, (b) obsługiwać napędy/biblioteki LTO przez kontroler SAS 12 Gb/s, (c) być zgodny z wymaganiami sprzętowymi producentów wskazanych klas oprogramowania. Dowód: oświadczenie Wykonawcy i dokumentacja kompatybilności producenta serwera składane na zasadach określonych w par. 4 ust. 5 umowy.

1. Wymagania techniczne urządzenia

Zaoferowane urządzenie musi spełniać poniższe minimalne parametry techniczne i wydajnościowe:

Parametr / Cecha	Minimalne wymagania techniczne
Obudowa	• Do zabudowy w szafie serwerowej 19", plus wszystkie elementy niezbędne do mocowania, oraz wysuwania do celów serwisowych bez odpinania kabli. • Wszystkie wyspecyfikowane elementy serwera muszą być zamontowane w jednej obudowie, o maksymalnej

	wysokości 2U. Na frontowym panelu obudowy sygnalizacja statusu pracy serwera (umożliwiająca co najmniej łatwą lokalizację serwera poprzez zapalenie diody LED lub wyświetlacza LCD).
Typ procesora	- Procesor minimum 16 rdzeniowy - Taktowany zegarem minimum 2,3 GHz - Zgodny z architekturą x86/64 bity, - Osiągający w teście PassMark CPU Mark wynik minimum 45.000 punktów według wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Kryterium równoważności (PassMark): wynik weryfikowany według wartości ze strony cpubenchmark.net Obowiązująca tabela z wynikami testu PassMark w Załączniku nr 1 do, dla procesora nieobecnego na liście raport z testu PassMark na zaoferowanej konfiguracji, wykazujący wynik nie niższy niż 45.000 punktów. Ponieważ serwer może w przyszłości stać się węzłem klastra wymagany jest procesor tego samego producenta (Intel) i architektury co procesory w istniejących węzłach klastra (HPE DL360 Gen10 Plus), zapewniający możliwość migracji na żywo (Live Migration) maszyn wirtualnych pomiędzy wszystkimi trzema węzłami klastra Hyper-V. Dopuszcza się stosowanie trybu zgodności procesora (Processor Compatibility Mode) dla maszyn wirtualnych, jeżeli Wykonawca wskaże to w dokumentach składanych na zasadach określonych w par. 4 ust. 5 umowy.
Ilość procesorów	1 szt.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach.
Pamięć	- Min. 64 GB w pełni buforowanej pamięci DIMM (DDR5) z technologią Advanced ECC lub chipkill, o transferze 6400 MT/s - Po zamontowaniu min. 15 wolnych slotów. - Możliwość rozbudowy pamięci do min. 4 TB.
Płyta główna	Dedykowana do pracy w serwerach.
Kontrolery dyskowe	- Kontroler macierzowy SAS 12Gb/s do obsługi dysków wewnętrznych, min. 8GB pamięci cache z podtrzymaniem baterijnym lub flash, obsługa RAID min. wersja 0/1/10/5/50/6/60 - Kontroler macierzowy SAS 12Gb/s do obsługi urządzeń zewnętrznych, umożliwiający podłączenie napędu LTO z biblioteki taśmowej
Dyski	Możliwość instalacji min. 12 dysków SAS/SATA z opcją wyjmowania i instalowania na gorąco (bez wyłączania

	serwera) • Min. 6 dysków 12 TB SAS 12Gb/s, min. 7200 obr/min, skonfigurowanych w RAID 6, zapewniających pojemność użyteczną co najmniej 40 TB • Min. 2x 480GB NVMe Hot-Plug zainstalowane bezpośrednio na kontrolerze (nie mogą zajmować wnęk przeznaczonych dla dysków 12 TB) pracujące w RAID 1, na system operacyjny hosta
Karty sieciowa	Min. dwie dwuportowe 10GbE RJ-45. Interfejsy 10GbE z obsługą iSCSI i MPIO; zapewnić osobne porty dla ruchu iSCSI.
Złącza zewnętrzne	• min. 4x USB 3.2 Gen1 (w tym min. 1x z przodu obudowy, 1x wewnętrzny), • min. 1xVGA
Zdalny interfejs zarządzający	Serwer musi być wyposażony w sprzętowe rozwiązanie zdalnego zarządzania, pochodzące od producenta serwera, niezależne od systemów operacyjnych, posiadające dedykowane złącze RJ-45, umożliwiające zdalny dostęp do graficznego interfejsu Web karty zarządzającej, zapewniające przynajmniej następujące funkcjonalności: • Zdalne włączenie serwera, • Zdalne wyłączenie serwera, • Restart serwera, • Podgląd logów sprzętowych serwera i karty, • Przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS), • Rozwiązanie musi być dostarczone wraz z niezbędnymi licencjami umożliwiającymi pracę zdalną na serwerze (wirtualny KVM) z użyciem przeglądarki internetowej. Licencja musi zawierać pełną możliwość zdalnego podłączenia napędów wirtualnych typu: CD/DVD, wirtualnych folderów. Kryterium równoważności (zdalne zarządzanie): równoważne sprzętowe rozwiązanie zintegrowane z platformą serwerową, niezależne od OS, z dedykowanym portem RJ-45 i wszystkimi funkcjami wskazanymi powyżej, wraz z licencjami. Dowód: karta katalogowa lub dokumentacja producenta składana na zasadach określonych w par. 4 ust. 5 umowy.
Karta graficzna	Zintegrowana, pozwalająca na prace z rozdzielczością min. 1920x1200
Zasilacz	230V 50Hz, min. 2 szt. Hot-plug, Titanium, nadmiarowe (redundantne), każdy o mocy wystarczającej do pracy serwera oraz przyszłej rozbudowy o pamięć Kryterium równoważności (zasilacze): sprawność nie niższa niż klasa 80 PLUS Titanium. Dowód: karta katalogowa

	serwera lub certyfikat 80 PLUS składana na zasadach określonych w par. 4 ust. 5 umowy.
Chłodzenie	Nadmiarowe wentylatory typu hot-plug
Warunki pracy	Pomieszczenia biurowe, 10-30 °C.
Gwarancja	Przynajmniej 36 miesięcy gwarancji (na części, robociznę i pomoc techniczną) z czasem reakcji na zgłoszenie usterki maksymalnie w następnym dniu roboczym, świadczone całodobowo, 7 dni w tygodniu, 365 dni w roku (24/7/365). Zamawiający wymaga aby zarządzanie gwarancją i zgłoszeniami gwarancyjnymi odbywało się przez system/stronę producenta (rozumiane jest to jako możliwość sprawdzenia stanu gwarancji, wykonywania zgłoszeń oraz sprawdzania stanu zgłoszeń bieżących i historycznych). Kryterium równoważności (gwarancja i serwis producenta): oświadczenie producenta (lub numery usług/kody SKU) wskazane na zasadach określonych w par. 4 ust. 5 umowy) potwierdzające świadczenie usług bezpośrednio przez producenta oraz dostęp Zamawiającego do portalu gwarancyjnego producenta.
System operacyjny i wirtualizacja	Dostawa fabrycznie nowych, wieczystych licencji Microsoft Windows Server 2025 Datacenter w aktualnym programie licencjonowania zbiorowego, w liczbie pokrywającej wszystkie fizyczne rdzenie serwera (zgodnie z minimami producenta), w wersji elektronicznej przypisanej do profilu Zamawiającego. Licencja musi umożliwiać uruchomienie na serwerze roli Hyper-V i nieograniczonej liczby maszyn wirtualnych, w tym minimum: maszyny wirtualnej z systemem SIEM (np. Wazuh), maszyny wirtualnej z systemem monitoringu NMS (np. Zabbix), repozytorium backupowego (np. Veeam). Systemy SIEM/NMS działają na maszynach wirtualnych z systemem Linux. Zamawiający nie ponosi kosztów licencji systemów Linux, a jeśli Wykonawca wybierze dystrybucję płatną, jej koszt wchodzi w cenę oferty. Kryterium równoważności: system wirtualizacji spełniający łącznie: (a) obsługa maszyn wirtualnych Linux i Windows, (b) obsługa dysków iSCSI/MPIO z NetApp, (c) aktywne wsparcie producenta i poprawki bezpieczeństwa przez min. 36 miesięcy od dostawy, (d) wsparcie oprogramowania do backupu (np. Veeam lub równoważnego) w ramach listy wspieranych platform. Dowód: oświadczenie Wykonawcy i dokumentacja kompatybilności składane na zasadach określonych w par. 4 ust. 5 umowy.

1. Wymagania dotyczące licencji i subskrypcji (36 miesięcy)

Wykonawca dostarczy komplet licencji i usług subskrypcyjnych świadczonych bezpośrednio przez producenta sprzętu na okres **36 miesięcy**:

- **Wsparcie techniczne producenta (24x7):**

- Dostęp do serwisu i zgłoszeń 24/7/365.
- Prawo do bezpłatnej aktualizacji oprogramowania układowego (firmware) i poprawek bezpieczeństwa.
- Gwarancja naprawy/wymiany sprzętu w przypadku awarii z czasem wysyłki części zastępczej w następnym dniu roboczym (NBD).

3. Wymagania dotyczące usług wdrożeniowych i konfiguracji: przygotowanie serwera pod środowisko SIEM/NMS i repozytorium backupow

Zakres obejmuje wyłącznie infrastrukturę: przygotowanie hosta (system operacyjny, rola Hyper-V, konfiguracja RAID i sieci), podłączenie LUN z NetApp, utworzenie maszyn wirtualnych z systemem operacyjnym (z przydziałem zasobów wg zaleceń producentów oprogramowania SIEM/NMS), przygotowanie wolumenu pod repozytorium backupowe. Zakres nie obejmuje instalacji ani konfiguracji aplikacji Wazuh, Zabbix i Veeam, które Zamawiający wykona we własnym zakresie.

4. Warunki dostawy i gwarancji

- Gwarancja: min. 36 miesięcy gwarancji producenta realizowanej z wymianą sprzętową NBD oraz wsparciem 24/7/365.
- Pochodzenie sprzętu: całość dostarczanego sprzętu musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek Unii Europejskiej, być fabrycznie nowe (tzn. wyprodukowane nie później, niż na 6 miesięcy przed ich dostarczeniem), oferowane urządzenia na dzień składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji (EoL) i objęte pełną opieką serwisową.

Dowód: Wykonawca składa na zasadach określonych w par. 4 ust. 5 umowy oświadczenie producenta lub dystrybutora potwierdzające dostawę z oficjalnego kanału na rynek UE, datę produkcji oraz brak zapowiedzi wycofania z produkcji (EoL) na dzień składania ofert.

- Ponieważ zasoby macierzowe NetApp będą wykorzystywane przez serwer, od Wykonawcy wymaga się certyfikatu NetApp potwierdzającego uprawnienia Wykonawcy lub osoby skierowanej do realizacji zamówienia do rekonfiguracji macierzy NetApp, które Wykonawca składa na zasadach określonych w par. 4 ust. 5 umowy.

Kryterium równoważności (certyfikat NetApp): dopuszcza się certyfikat, status partnerski lub inne potwierdzenie wydane przez NetApp albo autoryzowanego dystrybutora, z którego wynika, że Wykonawca lub osoba skierowana do realizacji zamówienia posiada uprawnienia i kompetencje do konfiguracji i rekonfiguracji macierzy NetApp (ONTAP) nie mniejsze niż wymagane w postępowaniu. Dowód: kopia dokumentu; dla certyfikatu osobowego dodatkowo wskazanie osoby i podstawy dysponowania nią składane na zasadach określonych w par. 4 ust. 5 umowy.

CZ. II. URZĄDZENIA KLASY NEXT-GENERATION FIREWALL (NGFW)

SZT. 2 – KLASTER HA

Postanowienia ogólne dotyczące równoważności

Wszędzie tam, gdzie w OPZ wskazano nazwę produktu, producenta, normę, certyfikat lub program licencjonowania, Zamawiający dopuszcza rozwiązania równoważne, tzn. spełniające co najmniej te same parametry techniczne, funkcjonalne i jakościowe oraz zapewniające pełną kompatybilność z posiadaną przez Zamawiającego infrastrukturą sprzętową i programową. Wykonawca powołujący się na rozwiązanie równoważne jest obowiązany wykazać tę równoważność, składając na zasadach określonych w par. 4 ust. 5 umowy dokumenty potwierdzające spełnienie kryteriów określonych w OPZ (karty katalogowe, certyfikaty, oświadczenia producenta, dokumentację techniczną). Ciężar udowodnienia równoważności spoczywa na Wykonawcy. Wszelkie wskazania nazw własnych, standardów czy technologii mają charakter wyłącznie przykładowy i służą określeniu minimalnego poziomu oczekiwanej funkcjonalności.

A. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż, konfiguracja oraz wdrożenie dwóch fabrycznie nowych urządzeń klasy Next-Generation Firewall (NGFW), pracujących w wysokiej dostępności HA (High Availability), wraz z wymaganymi przez producenta licencjami/subskrypcjami bezpieczeństwa na okres min. 12 miesięcy, wsparciem technicznym producenta oraz usługami wdrożeniowymi.

Urządzenia muszą zapewniać co najmniej:

- zaporę sieciową stateful inspection;
- kontrolę aplikacji;
- IPS/IDS;
- ochronę antywirusową/antymalware;
- filtrowanie WWW/DNS;
- ochronę przed zagrożeniami typu zero-day;
- VPN IPsec;
- zdalny dostęp VPN, jeżeli jest wymagany w architekturze Zamawiającego;
- segmentację sieci;
- centralne logowanie i monitorowanie;
- wysoką dostępność HA.

Dopuszcza się rozwiązania wykorzystujące CPU, ASIC, NPU, FPGA lub inne mechanizmy sprzętowej bądź programowej akceleracji, pod warunkiem spełnienia wymaganych parametrów funkcjonalnych i wydajnościowych.

1. Wymagania techniczne urządzeń NGFW

- Obudowa

Urządzenie musi być przeznaczone do montażu w szafie RACK. Dopuszcza się obudowy o wysokości maksymalnie 2U. Wykonawca musi zapewnić możliwość prawidłowego montażu obu urządzeń w standardowej szafie RACK Zamawiającego.

- Architektura i wydajność

Urządzenie musi zapewniać przetwarzanie ruchu z wykorzystaniem mechanizmów optymalizujących wydajność przetwarzania pakietów i funkcji bezpieczeństwa. Dopuszcza się zarówno rozwiązania posiadające dedykowane układy akcelerujące, jak i rozwiązania oparte na procesorach ogólnego przeznaczenia lub innych architekturach, jeżeli zapewniają wymagane parametry.

- Zasilanie

Każde urządzenie musi posiadać redundantne źródło zasilania, zapewniające ciągłość pracy urządzenia w przypadku awarii pojedynczego źródła zasilania. Dopuszcza się dwa wbudowane zasilacze, zasilacze wymienne typu hot-swap lub inne rozwiązanie producenta zapewniające równoważny poziom redundancji.

2. Interfejsy sieciowe

Urządzenie musi posiadać wystarczającą liczbę interfejsów umożliwiających realizację architektury Zamawiającego, w tym połączenie sieci LAN, WAN oraz pozostałych wymaganych segmentów.

- co najmniej 16 fizycznych interfejsów Ethernet 1 Gb/s lub szybszych, dostępnych dla ruchu sieciowego;
- co najmniej 8 interfejsów Ethernet obsługujących połączenia światłowodowe 1/10 Gb/s lub szybsze, z wykorzystaniem modułów SFP/SFP+ lub rozwiązania funkcjonalnie równoważnego;
- interfejs zarządzający lub możliwość logicznego wydzielenia interfejsu zarządzającego;
- interfejs lub funkcja umożliwiająca realizację komunikacji HA pomiędzy urządzeniami klastra;
- port konsolowy lub równoważny mechanizm dostępu administracyjnego.

Dopuszcza się, aby wymagane funkcje były realizowane przez porty fizyczne, porty współdzielone, porty wielofunkcyjne lub interfejsy o większej przepustowości, jeżeli zapewniają wymaganą funkcjonalność. Nie wymaga się określonego rozmieszczenia ani nazewnictwa portów.

3. Wydajność

Parametr	Wymaganie minimalne
Firewall throughput	≥ 10 Gb/s
IPS throughput	≥ 5 Gb/s
NGFW throughput	≥ 3 Gb/s
Threat Protection / pełna inspekcja bezpieczeństwa	≥ 2,5 Gb/s
IPsec VPN	≥ 20 Gb/s
Równoczesne sesje	≥ 3 000 000
Nowe sesje / sekundę	≥ 50 000

Wartości przepustowości należy podawać zgodnie z metodologią testową producenta, z jednoznacznym wskazaniem konfiguracji testowej oraz zakresu aktywnych funkcji. Dla parametrów obejmujących jednocześnie działanie kilku mechanizmów bezpieczeństwa Wykonawca musi wskazać, jakie funkcje były aktywne podczas deklarowanego testu.

4. Wirtualizacja i segmentacja

Urządzenie musi umożliwiać logiczne wydzielenie co najmniej 10 niezależnych instancji funkcji firewall, domen bezpieczeństwa, wirtualnych firewalli lub funkcjonalności równoważnej. Każda instancja musi umożliwiać niezależną konfigurację co najmniej interfejsów, routingu, polityk bezpieczeństwa, NAT i logowania.

Dopuszcza się realizację tej funkcji poprzez VDOM, virtual firewall, security context, virtual system lub inne rozwiązanie producenta o równoważnej funkcjonalności.

5. Wysoka dostępność HA

- automatyczne wykrywanie awarii urządzenia;
- automatyczne przejęcie obsługi ruchu przez urządzenie zapasowe;
- synchronizację konfiguracji;
- synchronizację stanu połączeń lub funkcjonalność równoważną, jeżeli jest wspierana przez daną architekturę;
- możliwość ręcznego przełączenia urządzenia aktywnego;
- monitorowanie stanu członków klastra;
- możliwość przeprowadzenia testu przełączenia bez utraty lub z minimalną utratą obsługiwanych połączeń, odpowiednio do zastosowanej technologii.

Dopuszcza się tryby Active/Passive, Active/Active lub rozwiązanie równoważne.

6. Funkcje bezpieczeństwa i licencje

Wykonawca dostarczy wszystkie wymagane przez producenta licencje/subskrypcje niezbędne do realizacji funkcji określonych w OPZ na okres 12 miesięcy.

- IPS/IDS;
- ochrona antywirusowa/antymalware;
- analiza behawioralna/heurystyczna, jeżeli jest dostępna w oferowanym rozwiązaniu;
- kontrola aplikacji;
- filtrowanie WWW;
- filtrowanie DNS lub funkcja równoważna;
- ochrona przed phishingiem;
- ochrona przed spamem – jeżeli funkcja jest oferowana w ramach platformy;
- analiza nieznanego plików i zagrożeń typu zero-day, realizowana lokalnie lub w chmurze;
- aktualizacje sygnatur i baz bezpieczeństwa;
- aktualizacje oprogramowania oraz poprawki bezpieczeństwa.

Dopuszcza się realizację poszczególnych funkcji przez różne komponenty jednego rozwiązania, pod warunkiem ich integracji.

7. VPN

- IPsec VPN;
- IKEv2;
- VPN site-to-site;
- zdalny dostęp użytkowników;
- MFA;
- certyfikaty cyfrowe;
- możliwość integracji z katalogiem użytkowników.

Jeżeli producent stosuje inne rozwiązanie zdalnego dostępu niż SSL-VPN, ale zapewnia funkcjonalność równoważną lub wyższą, rozwiązanie takie należy uznać za dopuszczalne.

8. Integracja

NGFW musi umożliwiać integrację co najmniej z Active Directory / LDAP, systemem DNS, systemami Syslog, systemami SIEM, systemami monitoringu oraz infrastrukturą PKI i rozwiązaniem MFA.

Komunikacja może odbywać się za pomocą Syslog, API, SNMP, REST API, standardowych protokołów uwierzytelniania lub innych udokumentowanych mechanizmów producenta.

9. Gwarancja i wsparcie producenta

- gwarancja na urządzenia i usługi min. 12 miesięcy
- wsparcie techniczne producenta 24x7x365;
- dostęp do aktualizacji firmware/software min. 12 miesięcy;
- dostęp do poprawek bezpieczeństwa min. 12 miesięcy;
- dostęp do aktualizacji baz bezpieczeństwa min. 12 miesięcy;
- obsługa zgłoszeń serwisowych min. 12 miesięcy;
- wymiana uszkodzonego sprzętu w trybie NBD lub równoważnym min. 12 miesięcy.

10. Warunki dostawy i gwarancji

- Gwarancja: min. 12 miesięcy gwarancji producenta realizowanej z wymianą sprzętową NBD.
- Pochodzenie sprzętu: całość dostarczanego sprzętu musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek Unii Europejskiej, być fabrycznie nowe (tzn. wyprodukowane nie później, niż na 6 miesięcy przed ich dostarczeniem), oferowane urządzenia na dzień składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji (12EoL) i objęte pełną opieką serwisową.

B. OPROGRAMOWANIE VPN/ZTNA – 50 UŻYTKOWNIKÓW/URZĄDZEŃ

Przedmiotem zamówienia jest dostawa, wdrożenie i zapewnienie 12-miesięcznego wsparcia dla komercyjnego rozwiązania VPN/ZTNA dla minimum 50 użytkowników lub urządzeń, współpracującego z dostarczonym rozwiązaniem NGFW. Rozwiązanie musi posiadać centralne zarządzanie.

Dopuszcza się architekturę, w której klient VPN/ZTNA, konsola zarządzająca oraz brama bezpieczeństwa pochodzą od tego samego lub różnych producentów, pod warunkiem zapewnienia wymaganej funkcjonalności oraz udokumentowanej integracji.

2. Uwierzytelnianie

- SSO z wykorzystaniem SAML 2.0 lub równoważnego standardu;
- integracja z Active Directory / LDAP;
- integracja z Microsoft Entra ID;
- integracja z innym dostawcą tożsamości obsługującym standardy SAML/OIDC;
- MFA;
- TOTP;
- mechanizm push lub równoważny mechanizm zatwierdzania logowania;
- wykorzystanie certyfikatu urządzenia jako dodatkowego czynnika uwierzytelniającego;
- wymuszenie ponownego uwierzytelnienia po określonym czasie.

3. Posture Check

Agent endpointowy musi umożliwiać ocenę stanu bezpieczeństwa urządzenia co najmniej w zakresie:

- obecności i działania mechanizmu antywirusowego/EDR;
- aktualności mechanizmu ochronnego;
- aktualności systemu operacyjnego;
- stanu zapory hostowej;
- obecności wymaganego certyfikatu;
- przynależności urządzenia do domeny;
- szyfrowania dysku;
- wersji systemu operacyjnego;
- obecności określonych procesów;
- obecności określonych plików;
- wartości określonych parametrów konfiguracyjnych.

Dopuszcza się realizację powyższych kontroli za pomocą innych mechanizmów, jeżeli zapewniają równoważny poziom kontroli stanu bezpieczeństwa urządzenia.

4. Polityki zgodności i ZTNA

- automatyczną klasyfikację urządzeń według stanu bezpieczeństwa;
- definiowanie własnych kategorii/tagów;
- tworzenie reguł z wykorzystaniem operatorów logicznych AND/OR;
- wykorzystanie informacji o stanie urządzenia w decyzji o udzieleniu dostępu;
- przekazanie informacji o stanie endpointu do systemu egzekwującego politykę dostępu;
- automatyczne odebranie dostępu po utracie wymaganego poziomu zgodności.

5. Ciągła weryfikacja

- monitorowanie stanu bezpieczeństwa okresowo i podczas aktywnej sesji;
- automatyczne ograniczenie lub odebranie dostępu do chronionej aplikacji w czasie nie dłuższym niż 1 minuta od wykrycia utraty wymaganej zgodności;
- automatyczne przywrócenie dostępu po przywróceniu zgodności, zgodnie z polityką;
- rejestrowanie zmian stanu urządzenia, zmian klasyfikacji/tagów i decyzji dotyczących dostępu.

6. Dostęp ZTNA

Rozwiązanie musi umożliwiać kontrolowany dostęp do aplikacji co najmniej dla protokołów HTTP/HTTPS, RDP, SSH, SMB i TCP. Dopuszcza się inne protokoły obsługiwane przez oferowaną platformę.

Rozwiązanie musi również umożliwiać zdalny dostęp sieciowy poprzez IPsec/IKEv2 lub równoważny bezpieczny protokół tunelowania.

7. Centralne zarządzanie

- zarządzanie agentami;
- dystrybucję konfiguracji;
- tworzenie profili;
- konfigurację Posture Check;

- definiowanie polityk ZTNA;
- zarządzanie tagami/kategoriami urządzeń;
- monitorowanie zgodności;
- generowanie raportów;
- zdalną aktualizację agenta;
- zdalne wdrażanie agenta;
- ograniczenie możliwości modyfikowania konfiguracji przez użytkownika;
- kontrolę odinstalowania agenta;
- eksport logów do Syslog lub SIEM.

Dopuszcza się zarządzanie w lokalnej infrastrukturze Zamawiającego, w chmurze producenta lub w modelu hybrydowym, o ile spełnione są wymagania dotyczące bezpieczeństwa, zarządzania i logowania.

8. Systemy operacyjne

Agent musi obsługiwać Windows 10, Windows 11 oraz macOS w zakresie funkcji wymaganych w OPZ. Dopuszcza się dodatkowe platformy.

9. Licencjonowanie

Wykonawca dostarczy minimum 50 licencji użytkownika/urządzenia, licencje VPN/ZTNA oraz licencje centralnego zarządzania i wymagane licencje dodatkowych komponentów na okres min. 12 miesięcy. Licencje muszą być zarejestrowane na Zamawiającego. Dopuszcza się licencjonowanie per użytkownik, per urządzenie lub per endpoint, pod warunkiem zapewnienia co najmniej zakresu 50 użytkowników/urządzeń.

10. MFA

Zamawiający wymaga możliwości zastosowania co najmniej 50 mechanizmów MFA. Dopuszcza się tokeny sprzętowe, tokeny programowe, aplikacje mobilne, TOTP, push MFA lub integrację z istniejącym systemem MFA Zamawiającego.

11. Integracja z NGFW

Oferowane rozwiązanie VPN/ZTNA musi współpracować z dostarczonym NGFW poprzez co najmniej jeden z następujących mechanizmów: natywną integrację producenta, API, standardowe protokoły uwierzytelniania, wymianę informacji o stanie endpointów, integrację z systemem tożsamości lub integrację z systemem zarządzania politykami.

W przypadku rozwiązania pochodzącego od innego producenta niż NGFW Wykonawca musi zapewnić wszystkie wymagane komponenty integracyjne w ramach ceny oferty.

Nie dopuszcza się konieczności zakupu dodatkowego urządzenia sprzętowego wyłącznie w celu zapewnienia podstawowej funkcjonalności wymaganej w OPZ.

12. Wdrożenie

Wykonawca przeprowadzi:

- analizę przedwdrożeńową;
- instalację urządzeń NGFW;
- konfigurację HA;
- konfigurację VLAN, routingu i NAT;

- konfigurację polityk bezpieczeństwa;
- konfigurację IPS/AV/Web/DNS/Application Control;
- konfigurację VPN;
- konfigurację MFA;
- integrację z AD/LDAP/Entra ID lub istniejącym systemem IAM;
- instalację i konfigurację systemu centralnego zarządzania ZTNA;
- przygotowanie polityk Posture Check;
- konfigurację polityk ZTNA;
- pilotaż dla grupy testowej;
- wdrożenie produkcyjne;
- konfigurację logowania do Syslog/SIEM;
- testy funkcjonalne i bezpieczeństwa.

13. Testy odbiorowe

NGFW – odbiór musi obejmować co najmniej: test pracy klastra HA, test przełączenia urządzeń, test routingu, NAT, IPS, kontroli aplikacji, filtrowania WWW/DNS, ochrony antywirusowej, VPN, logowania oraz aktualizacji baz bezpieczeństwa.

VPN/ZTNA – odbiór musi obejmować co najmniej: test SSO, MFA, Posture Check, nadawania kategorii/tagów, dostępu do aplikacji, odebrania dostępu po utracie zgodności, automatycznego przywrócenia dostępu, integracji z NGFW, logowania zdarzeń do Syslog/SIEM oraz wycofania dostępu użytkownika.

14. Warunki dostawy i gwarancji oraz wsparcia

- minimalny okres gwarancji: 12 miesięcy;
- wsparcie producenta 24x7x365;
- aktualizacje oprogramowania;
- poprawki bezpieczeństwa;
- wymiana uszkodzonego urządzenia w następnym dniu roboczym lub świadczenie równoważne;
- wsparcie Wykonawcy w języku polskim;
- czas reakcji maksymalnie 4 godziny dla zgłoszeń krytycznych;
- czas reakcji maksymalnie 1 dzień roboczy dla pozostałych zgłoszeń.

15. Dokumentacja i szkolenie

Wykonawca dostarczy Zamawiającemu

- dokumentację powdrożeniową;
- schemat połączeń;
- konfigurację HA;
- mapowanie interfejsów;
- wykaz podstawowych polityk;
- dokumentację konfiguracji VPN/ZTNA;
- instrukcję użytkownika;
- instrukcję administratora;
- materiały dla helpdesku;
- Wykonawca przeprowadzi szkolenie administratorów w wymiarze minimum 4 godzin.

16. Wymagania dotyczące równoważności

Za rozwiązanie równoważne uznaje się rozwiązanie, które spełnia wszystkie wymagania minimalne określone w OPZ, zapewnia wymaganą funkcjonalność, parametry wydajnościowe, architekturę HA, poziom bezpieczeństwa, integrację z systemami Zamawiającego, wsparcie producenta, aktualizacje bezpieczeństwa przez okres min. 12 miesięcy oraz centralne zarządzanie i możliwość eksportu logów do Syslog/SIEM.

Nie wymaga się zastosowania technologii, architektury sprzętowej, nazwy funkcji, nazwy licencji, nazwy systemu zarządzania ani nazwy protokołu charakterystycznej dla konkretnego producenta, jeżeli oferowane rozwiązanie zapewnia funkcjonalność określoną w OPZ.

CZ. III. MODERNIZACJA I REKONFIGURACJA SIECI LAN NA TERENIE ZESPOŁU PAŁACOWO-PARKOWEGO

Przedmiotem zamówienia jest kompleksowa modernizacja i rekonfiguracja lokalnej sieci komputerowej (LAN) na terenie zespołu, obejmująca audyt stanu istniejącego, przebudowę architektury sieci, wdrożenie mechanizmów bezpieczeństwa, redundancji i monitorowania oraz opracowanie wymaganej dokumentacji, zgodnie z wymogami dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2) oraz dobrymi praktykami normy ISO/IEC 27001 i ISO/IEC 27002.

1. Cel zamówienia

- Podniesienie poziomu bezpieczeństwa i odporności operacyjnej sieci LAN.
- Zapewnienie zgodności z wymogami zarządzania ryzykiem i zgłaszania incydentów wynikającymi z NIS2.
- Wdrożenie segmentacji sieci i kontroli dostępu ograniczających skutki potencjalnego incydentu.
- Zapewnienie ciągłości działania kluczowych systemów sieciowych.
- Uporządkowanie dokumentacji technicznej i proceduralnej sieci.

2. Zakres prac obejmuje następujące obszary:

- Inwentaryzacja i analiza ryzyka:
 - inwentaryzacja aktywnej infrastruktury sieciowej (switche, routery, AP, firewalle, UPS) wraz z raportem
 - opracowanie mapy fizycznej i logicznej sieci LAN (topologia, okablowanie, punkty dystrybucyjne)
 - analiza ryzyka i opracowanie Deklaracji Stosowania (SoA) w zakresie sieci LAN wg ISO/IEC 27001
- Infrastruktura aktywna i okablowanie strukturalne:
 - dostawa i konfiguracja switchy rdzeniowe L3 z obsługą VLAN, ACL, redundancją zasilania 48 portów — 2 szt.;
 - dostawa i konfiguracja switcha dostępowego L2/L2+ zarządzalnego z obsługą 802.1X i PoE — 1 szt.;
 - punkty dostępowe (AP) Wi-Fi zarządzalne centralnie z obsługą sieci gościnnej — sprawdzenie poprawności konfiguracji;
 - klastrer HA firewalli/UTM nowej generacji na styku sieci (NGFW) — sprawdzenie poprawności konfiguracji w klastrze dostarczonym i skonfigurowanym (cz. II niniejszego OPZ);
 - zasilacze awaryjne UPS do szaf dystrybucyjnych — sprawdzenie poprawności konfiguracji;
 - Uporządkowanie i oznakowanie okablowania w szafach dystrybucyjnych
- Segmentacja sieci i kontrola dostępu (VLAN, 802.1X/NAC):
 - projekt i wdrożenie segmentacji VLAN (biuro, administracja, bezpieczeństwo fizyczne [CCTV, KD, SSWiN, PPOŻ], goście, IoT/OT, multimedia)
 - konfiguracja list kontroli dostępu (ACL) i reguł firewall między segmentami
 - wdrożenie uwierzytelniania portów 802.1X / systemu NAC
 - rekonfiguracja wydzielonej sieci gościnnej z portalem captive
- Redundancja i ciągłość działania (BCP/DRP):
 - konfiguracja mechanizmów odpornościowych (RSTP, VRRP/HSRP, LACP)
 - Wdrożenie redundancji łączy rdzeniowych (stack/HA)
 - Opracowanie planu ciągłości działania i odtwarzania po awarii (BCP/DRP) dla warstwy sieciowej
- Monitorowanie, logowanie i wykrywanie incydentów (SIEM, NMS, IDS/IPS):
 - analiza centralnego systemu logowania / SIEM wraz z integracją urządzeń sieciowych

- analiza systemu monitorowania sieci (NMS) z alertowaniem
- analiza IDS/IPS na styku sieci i w kluczowych segmentach
- analiza serwera NTP dla synchronizacji czasu urządzeń
- Hardening i bezpieczeństwo urządzeń
 - hardening konfiguracji urządzeń sieciowych wg dobrych praktyk (CIS Benchmarks)
 - wdrożenie bezpiecznych protokołów zarządzania (SSH, HTTPS, SNMPv3) i wyłączenie protokołów niezabezpieczonych
 - aktualizacja firmware/oprogramowania urządzeń sieciowych
- Dokumentacja i zgodność formalna (polityki, procedury, SoA):
 - aktualizacja polityki bezpieczeństwa sieci LAN
 - opracowanie procedury zarządzania zmianą (change management) w infrastrukturze sieciowej
 - opracowanie procedury reagowania na incydenty (Incident Response Plan) zgodnej z wytycznymi dyrektywy NIS2
 - dokumentacja powykonawcza sieci (as-built) wraz z planem ciągłości działania (Szacowanie Ryzyka i plan ochrony Infrastruktury)
- Testy, odbiór końcowy i szkolenia personelu:
 - Testy penetracyjne powdrożeniowe
 - Testy redundancji i mechanizmów failover
 - Testy weryfikujące skuteczność segmentacji (izolacja VLAN)
 - Szkolenie administratorów z obsługi wdrożonej infrastruktury i procedur
 - Szkolenie kadry zarządzającej z obowiązków wynikających z dyrektywy NIS2

3. Wymagania techniczne

- Segmentacja i kontrola dostępu
 - Wydzielenie co najmniej segmentów: administracja, sieć produkcyjna/dydaktyczna, sieć gości, urządzenia IoT/OT, sieć zarządzania (out-of-band).
 - Zasada najmniejszych uprawnień (least privilege) w ruchu między segmentami.
 - Uwierzytelnianie urządzeń na poziomie portu (802.1X) lub równoważny mechanizm NAC.
- Redundancja
 - Brak pojedynczego punktu awarii (SPOF) w warstwie rdzenia sieci.
 - Redundancja zasilania kluczowych elementów aktywnych (UPS).
- Monitorowanie i reagowanie na incydenty
 - Centralne zbieranie logów z urządzeń sieciowych z retencją zgodną z polityką bezpieczeństwa zamawiającego.
 - Zdolność do wykrycia i wstępnej klasyfikacji incydentu w czasie umożliwiającym zgłoszenie do CSIRT w terminie 24h (zgłoszenie wstępne) i 72h (raport szczegółowy) zgodnie z NIS2.
- Bezpieczeństwo konfiguracji
 - Zarządzanie urządzeniami wyłącznie przez szyfrowane protokoły (SSH, HTTPS, SNMPv3).
 - Konfiguracja zgodna z dobrymi praktykami branżowymi (np. CIS Benchmarks) dla użytych platform.

4. Wymagania kompetencyjne:

- Audytor bezpieczeństwa systemu musi spełniać wymagania określone w art. 15 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.) i przepisami wykonawczymi do niej, w tym posiadać

wymienione w ww. przepisach certyfikaty,

5. Wymagania formalne i dokumentacyjne

- Wykonawca dostarczy pełną dokumentację powykonawczą w wersji elektronicznej i papierowej.
- Wykonawca opracuje lub zaktualizuje politykę bezpieczeństwa sieci LAN oraz procedurę zarządzania zmianą.
- Wykonawca opracuje procedurę reagowania na incydenty spójną z obowiązkami zgłoszeniowymi do CSIRT NASK na platformie S46.
- Wszystkie prace należy udokumentować w sposób umożliwiający wykazanie zgodności podczas audytu/kontroli.

6. Termin, warunki realizacji, gwarancja i serwis

- Prace należy zrealizować w sposób minimalizujący przerwy w działaniu sieci (poza uzgodnionymi oknami serwisowymi).
- Wymagany okres gwarancji na dostarczony sprzęt i wykonane prace: min. 36 miesięcy.
- Wykonawca zapewni wsparcie powdrożeniowe w okresie gwarancyjnym.
- Wykonawca przeprowadzi szkolenie personelu IT oraz kadry zarządzającej
- Zakres

- Okres: cały okres gwarancji (min. 36 mies. od odbioru końcowego).
- Obiekt SLA: dostarczony sprzęt, konfiguracja i mechanizmy bezpieczeństwa sieci LAN oraz weryfikowane AP i klaster NGFW (cz. II).

2. Obsługa

- Zgłoszenia: e-mail, ticket, telefon (P1 – telefon). Obsługa pn–pt 8:00–16:00; dyżur 24/7 tylko dla P1.
- Czas liczony od zgłoszenia do potwierdzenia przywrócenia działania.
- Priorytety i czasy

Priorytet	Reakcja	Usunięcie	Przykład
P1 – krytyczny	1 h (24/7)	8 h (24 h przy wymianie sprzętu)	Awaria rdzenia/NGFW bez redundancji, incydent bezpieczeństwa
P2 – wysoki	4 h rob.	2 dni rob.	Awaria VLAN/segmentu, utrata redundancji, CCTV/KD/SSWiN
P3 – średni	8 h rob.	5 dni rob.	Awaria pojedynczego AP/portu, błąd konfiguracji
P4 – niski	1 dzień rob.	10 dni rob.	Zapytania, drobne zmiany

- Dostępność i sprzęt
 - Dostępność rdzenia sieci: min. 99,9% miesięcznie (bez uzgodnionych okien serwisowych).

- Wymiana sprzętu: NBD lub urządzenie zastępcze dla P1; Wykonawca odtwarza konfigurację z kopii.
- NIS2 i bezpieczeństwo
 - Dane techniczne do zgłoszenia wstępnego (24 h) – w ciągu 4 h od zgłoszenia; do raportu szczegółowego (72 h) – w ciągu 48 h.
 - Poprawki podatności krytycznych (CVSS $\geq 9,0$) – 7 dni, wysokich (7,0–8,9) – 30 dni.
 - Przegląd okresowy 1× w roku (kopie konfiguracji, CIS, failover, dokumentacja).
- 6. Raportowanie
 - Miesięczny raport SLA; raport RCA dla P1 w ciągu 5 dni roboczych.
- Wyłączenia
 - Siła wyższa, działania Zamawiającego niezgodne z dokumentacją, awarie zasilania poza UPS i łączy operatora, zmiany bez uzgodnienia z Wykonawcą.

IV. DOSTAWA, INSTALACJA I KONFIGURACJA SYSTEMU KLASY SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) I SYSTEMU KLASY MONITORING INFRASTRUKTURY IT ORAZ ICH INTEGRACJĘ

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja systemu klasy SIEM i systemu klasy monitoring infrastruktury IT i ich integrację (dalej łącznie: „System” lub „Przedmiot zamówienia”).

Realizacja przedmiotu zamówienia ma na celu wypełnienie przez Zamawiającego obowiązków wynikających z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawy o krajowym systemie cyberbezpieczeństwa implementującej dyrektywę NIS2 oraz rozporządzeń wykonawczych do tych aktów, w zakresie rejestrowania zdarzeń, monitorowania bezpieczeństwa sieci i systemów informacyjnych oraz zdolności do wykrywania i obsługi incydentów.

Zamówienie obejmuje w szczególności następujące elementy składowe:

- dostawę oprogramowania / licencji / subskrypcji dla systemu klasy SIEM (Security Information and Event Management) służącego do centralnego gromadzenia i analizy logów bezpieczeństwa, obejmującego co najmniej następujące moduły funkcjonalne: moduł menedżera logów (centralne zbieranie, normalizacja i korelacja zdarzeń z wielu źródeł), moduł analizy integralności plików (File Integrity Monitoring – wykrywanie nieautoryzowanych zmian w plikach i konfiguracjach krytycznych), moduł wykrywania podatności (automatyczna identyfikacja podatności w oparciu o bazy CVE i ich powiązanie z zasobami), moduł oceny zgodności regulacyjnej (mapowanie zdarzeń i konfiguracji na wymagania norm/standardów bezpieczeństwa), moduł reagowania aktywnego (automatyczne działania zaradcze wyzwalane w odpowiedzi na wykryte zagrożenia, np. blokowanie adresów IP, izolacja hosta) oraz moduł rozszerzonej detekcji i reagowania (XDR – korelacja danych z wielu warstw środowiska IT: punktów końcowych, sieci, chmury – w celu wykrywania złożonych ataków);
- dostawę oprogramowania / licencji dla systemu klasy monitoring infrastruktury IT, umożliwiającego: monitorowanie dostępności i wydajności serwerów (fizycznych i wirtualnych), monitorowanie urządzeń sieciowych (w tym z wykorzystaniem protokołu SNMP), monitorowanie stanu i wydajności usług aplikacyjnych, a także monitorowanie logów systemowych za pomocą mechanizmu agentowego instalowanego na monitorowanych hostach, z możliwością definiowania wzorców (np. wyrażeń regularnych) wyzwalających alerty przy wystąpieniu określonych wpisów w dziennikach zdarzeń.;
- konfigurację niezbędnej infrastruktury serwerowej (wirtualnej) wraz z systemami operacyjnymi oraz oprogramowaniem bazodanowym wymaganych do prawidłowego działania Systemu;
- instalację, konfigurację i wdrożenie produkcyjne obu platform w architekturze wysokiej dostępności (High Availability), zgodnie z wymaganiami rozdziału 6 i 7;
- integrację obu systemów oraz podłączenie źródeł logów (serwery, stacje robocze, urządzenia sieciowe, systemy bezpieczeństwa, aplikacje) zgodnie z inwentaryzacją przekazaną przez Zamawiającego;
- konfigurację mechanizmów zgodnych z wymogami dyrektywy NIS2 w zakresie rejestrowania zdarzeń, retencji logów, alarmowania i raportowania incydentów;
- przeprowadzenie testów akceptacyjnych i odbiorowych;
- przeprowadzenie szkoleń administratorów i operatorów Zamawiającego;

- opracowanie i przekazanie dokumentacji powykonawczej, w tym polityk retencji i procedur eksploatacyjnych;
- świadczenie usług gwarancyjnych, wsparcia technicznego (asysty).

1. Wymagania dotyczące realizacji zamówienia

• **Zgodność z OPZ**

- Zamawiający zastrzega, że wszystkie wymagania minimalne określone w niniejszym OPZ oznaczone jako obligatoryjne (musi / zapewni / nie mniej niż) stanowią warunki brzegowe, których niespełnienie skutkować będzie brakiem odbioru przedmiotu zamówienia.

• **Architektura docelowa**

- System musi zostać zaprojektowany i wdrożony w architekturze zapewniającej wysoką dostępność kluczowych komponentów.

• **Środowisko docelowe**

- Wykonawca zrealizuje wdrożenie w środowisku zwirtualizowanym Hyper-V. Wykonawca skonfiguruje maszyny wirtualne zgodnie z wymaganiami sprzętowymi określonymi przez producenta oprogramowania w zasobach udostępnionych przez Zamawiającego.

2. Wymagania funkcjonalne — system klasy SIEM / log management

• **Gromadzenie i przetwarzanie logów**

- scentralizowane, agentowe i bezagentowe (syslog, API) zbieranie logów z systemów operacyjnych (Windows, Linux, Unix), urządzeń sieciowych, systemów bezpieczeństwa (firewall, IDS/IPS, WAF), baz danych, kontenerów oraz aplikacji webowych;
- obsługa min. 300 jednoczesnych agentów z możliwością skalowania do min. 1000 bez zmiany architektury systemu;
- normalizacja i dekodowanie logów z wykorzystaniem reguł predefiniowanych oraz możliwość tworzenia reguł i dekodowników własnych (custom rules/decoders);
- mechanizm korelacji zdarzeń w czasie rzeczywistym (near real-time) z możliwością budowy reguł wieloetapowych (multi-event correlation);
- wsparcie standardu integralności logów uniemożliwiającego niezauważalną modyfikację zapisanych zdarzeń (np. sumy kontrolne, podpis kryptograficzny łańcucha zdarzeń).

• **Detekcja zagrożeń i reagowanie**

- wbudowany moduł monitorowania integralności plików (FIM – File Integrity Monitoring) z alertowaniem o nieautoryzowanych zmianach w plikach krytycznych;
- moduł wykrywania podatności (Vulnerability Detection) oparty o bazy CVE, z automatycznym powiązaniem wykrytych podatności z zainwentaryzowanymi zasobami;
- moduł oceny zgodności konfiguracji (Security Configuration Assessment) z uznanymi standardami (np. CIS Benchmarks);
- możliwość automatycznej reakcji aktywnej (active response), np. blokady adresu IP, izolacji hosta, w oparciu o zdefiniowane reguły i progi;

- integracja z bazami reputacji / feedami Threat Intelligence (np. MISP, listy IOC) w celu wzbogacania alertów o kontekst zagrożeń;
- mapowanie wykrywanych technik ataków do macierzy MITRE ATT&CK w interfejsie analitycznym.
- **Panel analityczny, alarmowanie i raportowanie**
 - graficzny interfejs webowy (dashboard) z możliwością budowy niestandardowych widoków, wykresów i list zdarzeń;
 - mechanizm powiadomień (e-mail, webhook, integracja z systemami klasy ITSM/ticketing oraz komunikatorami zespołowymi) o zdarzeniach spełniających zdefiniowane kryteria istotności;
 - wielopoziomowa klasyfikacja istotności zdarzeń (severity/level) z możliwością konfiguracji progów alarmowych przez administratora;
 - generowanie raportów okresowych (dobowych, tygodniowych, miesięcznych) oraz raportów doraźnych na potrzeby zgłoszeń do CSIRT, zgodnie z rozdziałem 8;
 - mechanizm kontroli dostępu oparty o role (RBAC) z rozdzieleniem uprawnień administratora, analityka SOC i audytora (dostęp tylko do odczytu).
- **Zgodność regulacyjna**

System musi zawierać wbudowane lub konfigurowalne moduły/mapowania zgodności regulacyjnej odnoszące się co najmniej do: PCI DSS, ISO/IEC 27001, NIST 800-53, RODO – oraz umożliwiać rozszerzenie o mapowanie kontroli na potrzeby wymogów krajowego systemu cyberbezpieczeństwa (NIS2).

3. Wymagania funkcjonalne — system monitorowania infrastruktury

- **Monitorowanie dostępności i wydajności**
 - monitorowanie dostępności i parametrów wydajnościowych (CPU, RAM, dyski, sieć) serwerów fizycznych i wirtualnych, urządzeń sieciowych (SNMP) oraz usług aplikacyjnych;
 - obsługa min. 500 monitorowanych urządzeń/hostów z możliwością skalowania bez wymiany architektury;
 - automatyczne wykrywanie urządzeń w sieci oraz szablony monitorowania dla popularnych systemów operacyjnych, baz danych i urządzeń sieciowych;
 - monitorowanie logów systemowych z zdefiniowanymi wzorcami wyzwalającymi alerty przy wystąpieniu określonych wpisów;
 - mapy sieciowe wizualizujące zależności i status monitorowanych elementów infrastruktury.
- **Alarmowanie i eskalacja**
 - elastyczny mechanizm reguł wyzwalających z obsługą progów, korelacji wielu warunków oraz eskalacją powiadomień w czasie;
 - powiadomienia wielokanałowe: e-mail, SMS (poprzez bramkę), webhook / integracja z systemami ticketowymi i komunikatorami;
 - kalendarze dyżurów i okna serwisowe wykluczające fałszywe alarmy podczas planowanych prac.
- **Raportowanie i SLA**

- moduł raportowania dostępności usług (SLA reports) z możliwością definiowania i śledzenia poziomów SLA dla wybranych usług krytycznych;
- eksport danych i raportów do formatów PDF/CSV/XLSX oraz udostępnianie raportów cyklicznych drogą mailową.

4. Wymagania integracyjne oraz zgodności z dyrektywą NIS2

- **Integracja systemu klasy SIEM z system monitorowania infrastruktury**
 - Wykonawca skonfiguruje jednokierunkową lub dwukierunkową integrację obu platform w sposób umożliwiający: przekazywanie alertów bezpieczeństwa z systemu klasy SIEM do systemu monitorowania infrastruktury (lub odwrotnie) w celu uzyskania jednego, spójnego punktu widoku operacyjnego (single pane of glass) dla zespołu utrzymania; korelację zdarzeń dostępnościowych (systemu monitorowania infrastruktury) ze zdarzeniami bezpieczeństwa (systemu klasy SIEM) dotyczącymi tych samych zasobów.
- **Inwentaryzacja i podłączenie źródeł logów**
 - Wykonawca przeprowadzi, we współpracy z Zamawiającym, inwentaryzację systemów, urządzeń i aplikacji stanowiących źródła logów, a następnie podłączy do Systemu wszystkie wskazane przez Zamawiającego zasoby.
- **Rejestrowanie zdarzeń wymaganych przepisami**
 - System musi zapewniać rejestrowanie co najmniej następujących kategorii zdarzeń, niezbędnych do wykazania zgodności z obowiązkami zarządzania ryzykiem cyberbezpieczeństwa i wykrywania incydentów:
 - logowania i próby logowania (udane i nieudane) do systemów, w tym uwierzytelnianie uprzywilejowane;
 - zmiany uprawnień, ról i kont użytkowników (nadanie/odebranie uprawnień administracyjnych);
 - zdarzenia dotyczące integralności plików konfiguracyjnych i systemowych krytycznych zasobów;
 - zdarzenia sieciowe generowane przez systemy bezpieczeństwa brzegowego (firewall, IDS/IPS);
 - zdarzenia dotyczące instalacji/deinstalacji oprogramowania oraz zmian konfiguracyjnych systemów krytycznych;
 - błędy i zdarzenia świadczące o niedostępności usług kluczowych oraz naruszeniu ciągłości działania.
- **Retencja i integralność logów**
 - Wykonawca skonfiguruje politykę retencji logów zapewniającą przechowywanie danych „gorących” (przeszukiwalnych operacyjnie) przez okres nie krótszy niż 90 dni oraz archiwizację logów w warstwie „zimnej” (cold storage) przez okres nie krótszy niż 24 miesiące, zgodnie z wewnętrzną polityką bezpieczeństwa Zamawiającego oraz obowiązującymi przepisami. Zarchiwizowane logi muszą być chronione przed nieautoryzowaną modyfikacją i usunięciem (np. poprzez zapis w trybie WORM, sumy kontrolne lub równoważny mechanizm).
- **Wsparcie procesu zgłaszania incydentów do CSIRT**
 - System musi umożliwiać wygenerowanie w sposób zautomatyzowany lub półautomatyczny zestawu danych niezbędnych do sporządzenia zgłoszenia incydentu do właściwego CSIRT w terminach określonych przepisami wdrażającymi NIS2, tj. zgłoszenia wczesnego ostrzeżenia w ciągu 24 godzin od

powzięcia wiadomości o incydencie, zgłoszenia incydentu w ciągu 72 godzin oraz raportu końcowego w terminie miesiąca od zgłoszenia incydentu.

- **Wymagania bezpieczeństwa Systemu**

- szyfrowanie transmisji danych pomiędzy agentami/źródłami a serwerami centralnymi (TLS min. 1.2, zalecane 1.3);
- szyfrowanie danych składowanych dla warstwy archiwalnej logów;
- uwierzytelnianie administratorów Systemu z wykorzystaniem uwierzytelniania wieloskładnikowego (MFA) oraz, integracja z centralnym systemem tożsamości (Active Directory);
- pełne, niemodyfikowalne logowanie działań administracyjnych w samym Systemie;
- segmentacja sieciowa komponentów Systemu zgodnie z zasadami Zero Trust i minimalizacji powierzchni ataku, zaprojektowana i wdrożona przez Wykonawcę w uzgodnieniu z Zamawiającym;
- dostarczenie przez Wykonawcę dokumentu analizy ryzyka wdrożenia oraz potwierdzenia przeprowadzenia testów bezpieczeństwa konfiguracji (hardening) przed odbiorem produkcyjnym.

5. Wymagania licencyjne

Wykonawca dostarczy licencje/subskrypcje w liczbie i zakresie niezbędnym do objęcia monitoringiem oraz gromadzeniem logów wszystkich zasobów wskazanych przez Zamawiającego, wraz z prawem do aktualizacji, poprawek bezpieczeństwa oraz wsparcia producenta przez cały okres gwarancji (min. 24 miesiące). W przypadku komponentów opartych na licencji open-source, Wykonawca przedstawi jednoznaczną informację o modelu licencyjnym, ewentualnych ograniczeniach wersji społecznościowej (Community) wobec wersji komercyjnej oraz zapewni, że wybrany wariant spełnia wszystkie wymagania funkcjonalne OPZ.

6. Realizacja wdrożenia

- Analiza i przedwdrożeniowa obejmująca m.in.:
 - inwentaryzację źródeł logów,
 - analiza wolumenu (EPS),
 - opracowanie i uzgodnienie projektu technicznego
- Dostawa i instalacja obejmująca:
 - Dostawę licencji,
 - instalacja infrastruktury i oprogramowania
- Konfiguracja i integracja obejmująca:
 - Konfigurację reguł korelacji,
 - podłączenie źródeł logów,
 - integracja system klasy SIEM – system monitorowania infrastruktury,
 - konfiguracja polityk retencji
- Testy akceptacyjne (UAT):
 - funkcjonalne,
 - wydajnościowe,

- bezpieczeństwa
- testy scenariuszy incydentów
- Szkolenia administratorów i operatorów SOC
- Odbiór końcowy i dokumentacja: przekazanie dokumentacji powykonawczej, podpisanie protokołu odbioru

7. Szkolenia

- szkolenie administracyjne z zakresu instalacji, konfiguracji i utrzymania systemu klasy SIEM — dla min 2 osób, w wymiarze min. 16 godzin dydaktycznych dopuszczalne w formie on-line;
- szkolenie administracyjne z zakresu instalacji, konfiguracji i utrzymania systemu monitorowania infrastruktury — dla min. 2 osób, w wymiarze min. 16 godzin dydaktycznych dopuszczalne w formie on-line;
- szkolenie operacyjne (obsługa alertów, analiza incydentów, obsługa procedury zgłoszeń do CSIRT z wykorzystaniem Systemu) — dla min. 3 osób, w wymiarze min. 8 godzin dydaktycznych dopuszczalne w formie on-line;
- szkolenia zostaną przeprowadzone w siedzibie Zamawiającego lub w formie zdalnej – w uzgodnieniu z Zamawiającym – i zakończone przekazaniem materiałów szkoleniowych oraz imiennych zaświadczeń uczestnictwa.

8. Zasada odpowiedzialności

Każdy Wykonawca odpowiada za dostarczony przez siebie sprzęt, wykonaną konfigurację oraz udzieloną gwarancję w zakresie swojej części zamówienia. Wykonawca (cz. IV) nie odpowiada za wady, awarie ani konfigurację elementów dostarczonych w cz. II i III, z wyjątkiem obowiązków określonych w ust. 2–5.

- Obowiązek informacyjny.

Wykonawca (cz. IV) jest obowiązany pisemnie poinformować Zamawiającego o wszystkich zagrożeniach bezpieczeństwa lub ciągłości działania sieci LAN oraz infrastruktury wynikających z elementów dostarczonych lub skonfigurowanych w ramach innej części zamówienia oraz elementów istniejących, w szczególności o: błędnej lub niezgodnej z architekturą konfiguracji, nieaktualnym oprogramowaniu i znanych podatnościach, niezabezpieczonych protokołach zarządzania, brakach redundancji, nadmiernych uprawnieniach i obejściach segmentacji.

- Terminy zgłoszenia.
 - Zagrożenia wykryte w trakcie wdrożenia: wpis do raportu z audytu i raportu z testów, zgłoszenie bez zbędnej zwłoki, nie później niż w ciągu 3 dni roboczych od wykrycia.
 - Zagrożenia krytyczne (możliwość naruszenia bezpieczeństwa, utrata ciągłości): w ciągu 24 h od wykrycia.
 - W okresie gwarancji: zgłoszenie w ramach przeglądu rocznego oraz każdorazowo po wykryciu zagrożenia.
- Treść zgłoszenia.

Zgłoszenie zawiera: opis zagrożenia, element, którego dotyczy, ocenę ryzyka (np. CVSS lub skala wysokie/średnie/niskie), skutki dla sieci, rekomendowane działania oraz wskazanie odpowiedzialnego wykonawcy lub dostawcy. Wykonawca (cz. IV) przekazuje kopię zgłoszenia wskazanemu przez Zamawiającego wykonawcy innej części.

- Granice obowiązku.

„Wykonawca cz. III nie jest zobowiązany do usunięcia zagrożenia w elementach spoza swojego zakresu. Wykonawca ten odpowiada za rzetelność i terminowość zgłoszenia oraz za dostosowanie własnej konfiguracji (ACL, segmentacja, reguły), jeśli pozwala to ograniczyć zagrożenie, po uzgodnieniu z Zamawiającym.”

- Skutek zgłoszenia.

„Po prawidłowym i terminowym zgłoszeniu zagrożenia Wykonawca cz. III nie ponosi odpowiedzialności za skutki jego zaniechania przez Zamawiającego lub wykonawcę innej części. Niezgłoszenie zagrożenia znanego Wykonawcy lub możliwego do wykrycia przy dochowaniu należytej staranności stanowi niewykonanie zobowiązania.”

9. Realizacja, gwarancja, wsparcie techniczne, poziomy usług (SLA):

- Wykonawca udzieli gwarancji na dostarczone i wdrożone rozwiązanie na okres nie krótszy niż 24 miesiące od dnia podpisania protokołu odbioru końcowego bez zastrzeżeń, obejmującej usuwanie awarii, błędów konfiguracyjnych oraz zapewnienie aktualizacji bezpieczeństwa. W okresie gwarancji oraz w okresie asysty technicznej Wykonawca zapewni wsparcie zgodnie z poniższymi poziomami SLA:

Priorytet	Definicja	Czas reakcji	Czas przywrócenia działania
Krytyczny (P1)	Całkowita niedostępność Systemu lub utrata zdolności gromadzenia logów	do 1 godziny (24/7)	do 4 godzin
Wysoki (P2)	Istotne ograniczenie funkcjonalności (np. brak alertowania, awaria jednego węzła klastra)	do 4 godzin (dni robocze)	do 8 godzin roboczych
Średni (P3)	Błędy niekrytyczne, niewpływające na kluczowe funkcje bezpieczeństwa	do 1 dnia roboczego	do 3 dni roboczych
Niski (P4)	Pytania konfiguracyjne, drobne usprawnienia	do 2 dni roboczych	do 5 dni roboczych

10. Warunki odbioru

- Odbiór nastąpi po pozytywnym zakończeniu testów akceptacyjnych (UAT), przekazaniu pełnej dokumentacji powykonawczej oraz przeprowadzeniu szkoleń, na podstawie protokołu odbioru końcowego.
- Zamawiający zastrzega prawo zgłoszenia uwag i wad w terminie 14 dni od dnia zgłoszenia gotowości do odbioru; Wykonawca zobowiązany jest do ich usunięcia w terminie uzgodnionym z Zamawiającym, nie dłuższym niż 14 dni, przed ponownym zgłoszeniem do odbioru.
- Warunkiem podpisania protokołu odbioru końcowego bez zastrzeżeń jest spełnienie wszystkich wymagań obligatoryjnych określonych w niniejszym OPZ zgodnie z oświadczeniem zawartym w ofercie Wykonawcy.

11. Dokumentacja powykonawcza

Wykonawca prześle Zamawiającemu, w języku polskim, w formie elektronicznej edytowalnej i PDF, co najmniej następujące dokumenty:

- dokumentację architektury technicznej wdrożonego rozwiązania (diagramy sieciowe, wykaz komponentów, adresacja);
- dokumentację konfiguracji (reguły korelacji, polityki retencji, szablony monitorowania, integracje);
- procedury eksploatacyjne (uruchamianie, zatrzymywanie, kopie zapasowe, odtwarzanie po awarii — backup & recovery), w określenie RTO (Recovery Time Objective – docelowy czas odtwarzania, określający czas potrzebny na przywrócenie działania Systemu po awarii) / RPO (Recovery Point Objective – docelowy punkt odtwarzania, określający dopuszczalny wiek danych w kopii zapasowej w przypadku awarii);
- procedurę obsługi incydentu z wykorzystaniem Systemu, uwzględniającą terminy zgłoszeń do CSIRT;
- raport z testów akceptacyjnych i testów bezpieczeństwa (hardening);
- materiały szkoleniowe przekazane uczestnikom szkoleń.

CZ. V. ROZBUDOWA SIECI WIFI NA TERENIE ZESPOŁU PAŁACOWO-PARKOWEGO

Przedmiotem zamówienia jest rozbudowa istniejącej zewnętrznej sieci Wi-Fi na terenie zespołu pałacowo-parkowego w Kozłówce w oparciu o urządzenia zgodne z posiadanymi przez Zamawiającego obsługiwany przez centralny system posiadany przez Zamawiającego. Zamawiający posiada sieć Wi-Fi zbudowaną w oparciu o urządzenia Cambium Networks i zarządzaną w systemie cnMaestro. Rozbudowa ma być wykonana w tej samej technologii, a wszystkie dostarczone urządzenia mają stanowić integralną część istniejącej sieci.

1. Zakres prac obejmuje:

- dostawę urządzeń wraz z wymaganymi licencjami i osprzętem,
- montaż i podłączenie urządzeń,
- konfigurację urządzeń oraz ich integrację z systemem cnMaestro posiadanym przez Zamawiającego,
- zabezpieczenie sieci zgodnie z wymaganiami dyrektywy NIS2 (dyrektywa (UE) 2022/2555) i przepisami krajowymi ją wdrażającymi (m.in. segmentacja VLAN, silne uwierzytelnianie i szyfrowanie, rejestrowanie zdarzeń i połączeń),
- przeprowadzenie testów przy udziale Zamawiającego,
- opracowanie dokumentacji technicznej wdrożonego rozwiązania,
- świadczenie serwisu gwarancyjnego.

2. Uzasadnienie opisu przedmiotu zamówienia przez odniesienie do systemu Cambium / cnMaestro (art. 99 ust. 4 ustawy Pzp):

Zamawiający eksploatuje sieć Wi-Fi opartą o urządzenia Cambium Networks zarządzaną centralnie w systemie cnMaestro. Wymóg zarządzania wszystkimi nowymi urządzeniami w tym samym systemie wynika ze specyfiki przedmiotu zamówienia i potrzeby zapewnienia kompatybilności z istniejącą infrastrukturą, tj. z koniecznością: (1) utrzymania jednej, spójnej polityki konfiguracji, VLAN i bezpieczeństwa, (2) zapewnienia roamingu i mesh pomiędzy nowymi i istniejącymi punktami dostępowymi, (3) uniknięcia utrzymywania drugiego systemu zarządzania, co zwiększyłoby koszty eksploatacji i powierzchnię ataku, a tym samym utrudniało spełnienie wymagań NIS2, (4) zapewnienia jednego punktu monitorowania i zdalnych interwencji. Przedmiotu zamówienia nie można opisać w inny, dostatecznie dokładny i zrozumiały sposób bez odniesienia do systemu cnMaestro. Z tego względu Zamawiający dopuszcza rozwiązania równoważne na zasadach określonych w niniejszym OPZ.

3. OBSZAR OBJĘTY ZADANIEM I UWARUNKOWANIA

- Teren zespołu pałacowo-parkowego w Kozłówce objęty zadaniem:
 - - plac przed kaplicą,
 - - park (obszar ogrodu francuskiego),
 - - teren przed pałacem od strony południowej,
 - - parking,
 - - część dziedzińca głównego od strony zachodniej,
 - - teren rożarium,
 - - dziedziniec przed pawilonem północnym od strony północnej,
 - - dziedziniec gospodarczy przed oficyną południową od strony południowej.
- Uwarunkowania związane z wykonywaniem zamówienia:
 - - teren objęty ochroną konserwatora wojewódzkiego, powierzchnia 3,99 ha,
 - - budynki pokryte dachami z blachy miedzianej,
 - - ściany wewnętrzne budynków o grubości od 55 do 100 cm, ściany zewnętrzne ok. 100 cm,
 - - brak możliwości bruzdowania ścian, podłóg i sufitów; prace należy prowadzić

bez ingerencji w substancję zabytkową, a sposób wykonania podłączenia urządzeń i miejsca montażu urządzeń uzgodnić z Zamawiającym przed rozpoczęciem prac,

- o - w każdym budynku dostępna jest szafa krosownicza; budynki są połączone światłowodem.

4. WYMAGANIA OGÓLNE DLA CAŁEGO ROZWIĄZANIA

- Zarządzanie. Wszystkie dostarczane urządzenia (punkty dostępowe i przełączniki) muszą być natywnie obsługiwane przez system cnMaestro posiadany przez Zamawiającego i zarządzane z poziomu tej samej instancji, w której zarządzana jest istniejąca sieć (w zakresie: dołączania i konfiguracji urządzeń, monitorowania, alarmów, aktualizacji oprogramowania, zdalnych interwencji). Dostarczone urządzenia nie mogą wymagać ani być obsługiwane przez inny, odrębny system, kontroler, bramę ani aplikację zarządzającą.
- Licencje. Wykonawca dostarczy wszystkie licencje i subskrypcje (w tym licencje systemu zarządzania w zakresie niezbędnym do spełnienia wymagań niniejszego OPZ) na cały okres serwisu gwarancyjnego, tj. 24 miesiące od odbioru końcowego. Zamawiający nie poniesie dodatkowych kosztów z tego tytułu.
- Współpraca z istniejącą siecią. Nowe punkty dostępowe muszą współpracować z istniejącymi punktami dostępowymi Zamawiającego w zakresie roamingu, mesh, wspólnych SSID i polityk bezpieczeństwa oraz VLAN, bez konieczności zmiany lub wymiany istniejących urządzeń.
- Wymagana przepływność sieci: min. 1 Gb/s.
- Bezpieczeństwo: zintegrowane usługi bezpieczeństwa w całej sieci bezprzewodowej i przewodowej w ramach jednej struktury z logicznym podziałem na VLAN.
- Rozwiązania równoważne. Zamawiający dopuszcza zaoferowanie urządzeń innych producentów niż Cambium Networks (lub równoważnych) pod warunkiem spełnienia łącznie następujących kryteriów równoważności:
 - o spełnienie wszystkich parametrów minimalnych określonych w pkt 5-9,
 - o natywna obsługa przez system cnMaestro Zamawiającego (urządzenia ujęte w oficjalnej dokumentacji lub liście wspieranych urządzeń producenta systemu cnMaestro), bez pośredniczących integracji, bram i dodatkowych systemów zarządzania,
 - o brak konieczności uruchamiania odrębnego systemu zarządzania i ponoszenia przez Zamawiającego dodatkowych opłat licencyjnych,
 - o pełna współpraca z istniejącą siecią.

Wykonawca, który powołuje się na rozwiązania równoważne, jest obowiązany wykazać, że oferowane dostawy spełniają wymagania Zamawiającego, w szczególności przedkładając na zasadach określonych w par. 4 ust. 5 umowy karty katalogowe oraz dokument producenta systemu cnMaestro lub inny wiarygodny dokument potwierdzający wsparcie oferowanych urządzeń przez cnMaestro. Ciężar wykazania równoważności spoczywa na Wykonawcy.

5. PUNKTY DOSTĘPOWE - 8 szt.

Zewnętrzny bezprzewodowy punkt dostępowy Wi-Fi 6 (np. Cambium Networks lub równoważny w rozumieniu pkt 4 (rozwiązania równoważne) o następujących parametrach minimalnych:

- standardy: IEEE 802.11 a/b/g/n/ac/ax; praca dwupasowa 2,4 GHz (802.11 b/g/n/ax, 2x2:2) i 5 GHz (802.11 a/n/ac/ax, 2x2:2),
- prędkość transmisji bezprzewodowej: 5 GHz min. 1200 Mb/s, 2,4 GHz min. 570 Mb/s, łącznie min. 1750 Mb/s,
- interfejs LAN: min. 1 x RJ-45 1000BASE-T (dopuszcza się 2,5 GbE),
- zasilanie: PoE 802.3af, pobór mocy max 11 W,

- anteny zintegrowane, MIMO 2x2,
- mesh: multi-hop, w każdym paśmie,
- bezpieczeństwo SSID i uwierzytelnianie: OPEN, OWE (Enhanced Open), WPA2-AES (CCMP, 802.11i) z PSK, ePSK i Enterprise (802.1X/EAP), WPA3-SAE, WPA3-Enterprise (w tym CNSA), OSEN, PMF (802.11w); uwierzytelnianie MAC z lokalną lub zewnętrzną bazą danych (RADIUS 802.1X z EAP-TTLS, EAP-TLS, MSCHAPv2, PEAP, EAP-SIM/AKA/AKA', FAST); Hotspot 2.0,
- zarządzanie dostępem WLAN za pomocą kalendarza,
- możliwość limitowania: ilości danych, liczby klientów, czasu i przepustowości klienta na SSID,
- możliwość rejestracji i przechowywania danych użytkowników sieci (wymóg cyberbezpieczeństwa),
- opcje sieciowe: dziennik połączeń TCP, zaporę z rejestrowaniem NAT, serwer DHCP, DHCP relay (opcja 82), obsługa VLAN, atrybuty RADIUS, VID VLAN na SSID i na użytkownika, ePSK z przypisaniem VLAN do PSK,
- natywna integracja i zarządzanie w systemie cnMaestro Zamawiającego,
- MTBF: min. 4 500 000 h w temperaturze 25°C,
- certyfikaty / zgodność: Wi-Fi Alliance (802.11 a/b/g/n/ac/ax), CE, FCC, IC, IEC/EN 62368-1, EN 62311, WEEE, RoHS,
- waga max 500 g,
- warunki pracy: temperatura 0°C - 50°C, wilgotność względna do 95% (bez kondensacji),
- - gwarancja: min. 24 miesiące z wymianą uszkodzonego sprzętu.

6. PRZEŁĄCZNIK ZARZĄDZALNY WIELOWARSTWOWY L2/L3 - 3 szt.

Przełącznik (np. Cambium Networks cnMatrix lub równoważny w rozumieniu pkt 4 (rozwiązania równoważne) o następujących parametrach minimalnych:

- - typ: zarządzalny, wielowarstwowy L2/L3 (z obsługą routingu między VLAN),
- - porty: 8 x RJ-45 Gigabit Ethernet 10/100/1000 z PoE+ (802.3at), min. 30 W na port; budżet PoE min. 120 W,
- - 1 x USB 2.0, port konsoli (RS-232),
- - tablica adresów MAC: min. 16 000 wpisów,
- - wydajność przełączania: min. 16 Gb/s; wydajność przekazywania: min. 11,9 Mpps,
- - montaż w szafie rack 19", wysokość max 1U (zestaw montażowy w komplecie),
- - przycisk reset, diody LED (działanie, link, PoE),
- - Jumbo Frames: min. 9000 B; obsługa multicast,
- - pamięć operacyjna min. 512 MB, pamięć flash min. 128 MB, wbudowany procesor,
- - ACL, QoS (klasyfikacja i kształtowanie ruchu), algorytmy kolejowania SP, WRR, WRR+SP,
- - zarządzanie: strona WWW (HTTPS), CLI (SSH), zarządzanie w chmurze, natywna integracja i zarządzanie w systemie cnMaestro Zamawiającego,
- - bezpieczeństwo: ochrona hasłem, HTTPS, SSH v2, SSL/TLS, 802.1X i RADIUS (uwierzytelnianie na podstawie portów), filtrowanie / ochrona BPDU,
- - DHCP: klient, relay, serwer, DHCP snooping,
- - standardy: IEEE 802.1D, 802.1Q, 802.1AB, 802.1p, 802.1s, 802.1w, 802.1X, 802.3, 802.3ab, 802.3ac, 802.3ad, 802.3u, 802.3x,
- - funkcje: dublowanie portów (port mirroring), pełny duplex z kontrolą przepływu 802.3x, agregacja łączy (LACP), kontrola wzrostu natężenia ruchu (storm control), limitowanie przepustowości, protokół drzewa rozpinającego (STP/RSTP/MSTP),
- - VLAN: port-based i tagged, min. 4000 VLAN,
- - zasilanie: AC 100-240 V, zasilacz / kabel zasilający w zestawie,

- - MTBF: min. 300 000 h,
- - warunki pracy: temperatura 0°C - 50°C, wilgotność względna do 95% (bez kondensacji),
- - waga max 2 kg,
- - gwarancja: min. 24 miesiące z wymianą uszkodzonego sprzętu.

7. PRZEŁĄCZNIK ZARZĄDZALNY Z SLOTEMI SFP – 1 szt. oraz MODUŁY SFP - 2 szt.

- Przełącznik (np. Cambium Networks cnMatrix lub równoważny w rozumieniu pkt 4 (Rozwiązania równoważne) o następujących parametrach minimalnych:
 - - typ: zarządzalny, z natywną obsługą w systemie cnMaestro onPremise Zamawiającego,
 - - porty: 8 x RJ-45 Gigabit Ethernet 10/100/1000 z obsługą PoE (IEEE 802.3af/802.3at) oraz 4 sloty SFP,
 - - pamięć operacyjna min. 128 MB, pamięć flash min. 16 MB,
 - - gniazdo zasilania DC; zasilacz w zestawie,
 - - warunki pracy: temperatura 0°C - 40°C, wilgotność względna do 95% (bez kondensacji),
 - - gwarancja: min. 24 miesiące z wymianą uszkodzonego sprzętu.

8. WYMAGANIA DOTYCZĄCE DOSTAWY, DOKUMENTACJI I LICENCJI

- Dostawa dotyczy urządzeń fabrycznie nowych, tj. nieużywanych przed dniem dostarczenia (z wyłączeniem użycia niezbędnego do przeprowadzenia testu poprawnej pracy), pochodzących z oficjalnych kanałów dystrybucyjnych producenta zapewniających realizację uprawnień gwarancyjnych.
- Wykonawca dostarczy wraz z urządzeniami: instrukcje obsługi, dokumentację techniczną i użytkową, dokumenty gwarancyjne wystawione przez producenta oraz wszelkie niezbędne do prawidłowego działania przewody, kable, złącza i osprzęt.
- Wykonawca dostarczy wszystkie niezbędne do prawidłowego działania urządzeń licencje i oprogramowanie (zgodnie z pkt 4 Licencje).
- Wykonawca przeprowadzi testy pracy urządzeń przy udziale Zamawiającego.
- Wykonawca opracuje dokumentację techniczną wdrożonego rozwiązania (m.in. rozmieszczenie urządzeń, schemat logiczny, adresacja, VLAN, SSID, konfiguracje urządzeń).
- Dodatkowe wymagania:
 - Zamawiający zastrzega sobie prawo weryfikacji parametrów zainstalowanych urządzeń. W razie niespełnienia któregośkolwiek z wymaganych parametrów Wykonawca na własny koszt zdemontuje urządzenie i dostarczy urządzenie spełniające wszystkie wymagania OPZ.
 - Oferowane urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed dostarczeniem.
 - Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji (EoL).
 - Całość sprzętu musi pochodzić z autoryzowanego kanału dystrybucji w Polsce.

9. SERWIS GWARANCYJNY

- Wykonawca zapewni serwis gwarancyjny przez 24 miesiące od odbioru końcowego urządzeń, obejmujący naprawę wszystkich usterek, wad i uszkodzeń ujawnionych w trakcie eksploatacji.
- Wykonawca zapewni wsparcie techniczne obejmujące dostęp on-line do wiedzy technicznej producenta, aktualizacje i poprawki oprogramowania oraz licencje niezbędne do pobierania aktualizacji firmware i software przez cały okres serwisu.
- Serwis jest realizowany przez producenta lub podmiot autoryzowany przez producenta.
- Wykonawca przyjmuje zgłoszenia we wszystkie dni tygodnia, 24 godziny na dobę. Zgłoszenia mogą być dokonywane telefonicznie lub e-mailem; brak potwierdzenia przyjęcia zgłoszenia przez Wykonawcę nie oznacza braku zgłoszenia.

- Reakcja Wykonawcy (łącznie z diagnozą) następuje najpóźniej w następnym dniu roboczym po zgłoszeniu. Jeżeli awaria nie może zostać usunięta tego samego dnia, Wykonawca dostarczy, zainstaluje i uruchomi sprzęt zastępczy o parametrach nie gorszych niż urządzenie zastępowane, na cały czas potrzebny do usunięcia awarii.
- Jeżeli w następnym dniu roboczym po zgłoszeniu nie zostanie dokonana naprawa i zapewniony zostanie sprzęt zastępczy, Strony ustalą termin naprawy lub usunięcia wad. Naprawa może być wykonana w siedzibie Wykonawcy.
- Wszelkie koszty naprawy, w tym transportu, instalacji, konfiguracji i uruchomienia urządzeń w siedzibie Zamawiającego, ponosi Wykonawca.