Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Załącznik nr 1b do SWZ

Szczegółowy opis przedmiotu zamówienia na dostawę i wdrożenie sprzętu informatycznego w ramach konkursu grantowego „Cyberbezpieczny Samorząd”

Spis treści

Wstęp

W ramach zadania wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „Wdrożenie".
Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

a) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
b) Zamawiający wymaga, by dostarczone urządzenia były nowe oraz by nie były używane
c) Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;

d) Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
e) Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;

Serwer (1 sztuka)

LP	Parametr lub warunek minimalny	Minimalne wymagania
1.	**Obudowa**	● Typu RACK, wysokość nie więcej niż 1U; ● Szyny umożliwiające wysunięcie serwera z szafy stelażowej ● Możliwość zainstalowania 8 dysków twardych hot plug 2,5”; ● Możliwość zainstalowania zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; ● Zainstalowane 2 szt. dysków SSD M.2 960GB skonfigurowane w raid 1, ● Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
2.	**Płyta główna**	● Dwuprocesorowa; ● Wyprodukowana i zaprojektowana przez producenta serwera; ● Możliwość instalacji procesorów 60-rdzeniowych; ● zainstalowany moduł TPM 2.0; ● 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5; ● Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH; ● 32 gniazda pamięci RAM; ● Obsługa 8 TB pamięci operacyjnej RAM DDR4; ● Wsparcie dla technologii: ● Memory Scrubbing; ● SDDC; ● ECC;

		● Memory Mirroring; ● ADDDC; ● Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug. ● BIOS UEFI w specyfikacji 2.7.
3.	**Procesory**	● Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64; ● osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta.
4.	**Pamięć RAM**	● 128 GB pamięci RAM; ● DDR4 Registered 4800MT/s; ● Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;
5.	**Kontrolery I/O**	● karta 2x16GB FC
6.	**Kontrolery LAN**	● Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: ● 4x 1Gbit Base-T, ● Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; ● Interfejsy LAN zainstalowane w slotach PCI-e: 2x10Gbit SFP obsadzone wkładkami światłowodowymi MultiMode 10G
7.	**Kontroler**	● Kontroler pracujący w trybie Host Bus Adapter z zewnętrznym porteme SAS
8.	**Porty**	● Zintegrowana karta graficzna ze złączem VGA z tyłu serwera ● 2 porty USB 3.0 dostępne z tyłu serwera; ● 2 porty USB 3.0 na panelu przednim; ● Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;

		● Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
9.	**Zasilanie, chłodzenie**	● Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; ● Redundantne wentylatory hotplug.
10.	**Zarządzanie**	● Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; ● informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: ● karty rozszerzeń zainstalowane w dowolnym slocie PCI Express; ● procesory CPU; ● pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM; ● status karty zarządzającej serwera; ● wentylatory; ● bateria podtrzymująca ustawienia BIOS płyty głównej; ● zasilacze; ● system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym); ● Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: ● Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; ● Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ● Dostęp poprzez przeglądarkę Web, SSH; ● Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;

		● Zarządzanie alarmami (zdarzenia poprzez SNMP); ● Możliwość przejęcia konsoli tekstowej; ● Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); ● Obsługa serwerów proxy (autentykacja); ● Obsługa VLAN; ● Możliwość konfiguracji parametru Max. Transmission Unit (MTU); ● Wsparcie dla protokołu SSDP; ● Obsługa protokołów TLS 1.2, SSL v3; ● Obsługa protokołu LDAP; ● Integracja z HP SIM; ● Synchronizacja czasu poprzez protokół NTP; ● Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; ● Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); ● Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; ● Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
11.	**Wspierane OS**	● Microsoft Windows Server 2022, 2019; ● VMWare vSphere 8.0;; ● Suse Linux Enterprise Server 15;

		● Red Hat Enterprise Linux 9, 8; ● Microsoft Hyper-V Server 2019
12.	**Gwarancja**	● 5 lat gwarancji producenta serwera w trybie on-site z czasem skutecznej naprawy w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej; ● Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu; ● Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; ● Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; ● Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).
13.	**Dokumentacja, inne**	● Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; ● Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; ● Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; ● W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; ● Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach

		bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; ● Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwera. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV. ● Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; ● Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04; ● Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.

Serwerowy system operacyjny (4 sztuki)

LP	**Parametr lub warunek minimalny**	**Minimalne wymagania**
1.	**Minimalne parametry**	Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

		4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard),

		c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http

		ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

		28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Przełącznik sieciowy (1 sztuka)

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Zamawiający jest w posiadaniu rozwiązania Fortigate, model Fortiswitch 148poe. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem Fortigate, o następujących parametrach:

LP	Parametr lub warunek minimalny	Minimalne wymagania
1.	**Parametry fizyczne platformy**	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V. • Maksymalny pobór mocy: 60 W. • Minimalny zakres temperatury pracy: 0-40°C.
2.	**Interfejsy sieciowe - wymagania minimalne**	1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 48 porty GE RJ-45. e) 4 porty 10 GE SFP+.
3.	**Zarządzanie**	• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.

		• Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
4.	**Parametry wydajnościowe**	• Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. • Tablica adresów MAC o pojemności co najmniej 32k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
5.	**Wymagane funkcje**	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
6.	**Dodatkowe funkcje urządzenia**	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler)

	przy integracji z systemem centralnego zarządzania / NAC	(tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
7.	**Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

8.	**Gwarancja oraz wsparcie**	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
9.	**Opisy do wymagań ogólnych**	1.Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Access Point (4 sztuki)

LP	Parametr lub warunek minimalny	Minimalne wymagania
1.	**Wymagania minimalne**	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. 1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: a. Temperatura 0–50°C,

		b. Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington. 3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: a. 2.4 GHz 802.11b/g/n, b. 5 GHz 802.11a/n/ac/ax, c. 5/6 GHz 802.11a/n/ac/ax 4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. 5. Urządzenie musi być wyposażone w moduł BLE. 6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX, 7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: a. Tunnel, b. Bridge, c. Mesh. 9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST). 11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje: a. MIMO – 2x2,

		b. Maksymalna przepustowość dla poszczególnych modułów radiowych: i. 574 Mbps; ii. 1201 Mbps; iii. 2401 Mbps; c. Wymagana moc nadawania: i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; ii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; iii. min. 21 dBm dla pasma 6GHz z możliwością zmiany co 1dBm; d. Wsparcie dla 802.11n 20/40Mhz HT, e. Wsparcie dla kanałów 80 i 160MHz, f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz. g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, 12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512; 13. Funkcje dodatkowe: a. OFDMA UL i DL b. Spatial Reuse (BSS Coloring) c. UL-MU-MIMO d. DL-MU-MIMO e. Enhanced Target Wake Time (TWT) f. Wbudowany analizator widma g. Wbudowane mechanizmy WIPS/WIDS
2.	**Gwarancja oraz wsprarcie**	Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Macierz (1 sztuka)

LP	**Parametr lub warunek minimalny**	**Minimalne wymagania**
1.	**Sprzęt**	Dostarczenie macierzy dyskowej umożliwiających pracę w trybie (synchronicznym/ asynchronicznym) Active/Active. Macierz musi być gotowa na pracę z drugą macierzą pomiędzy zdalnymi lokalizacjami (min.20 km) oraz szyfrowanie danych. Wyposażona w dwa kontrolery pracujące w trybie active/active w zakresie danych wejściowych, zamawiający dopuszcza tryb ALUA w przypadku zaoferowania rozwiązania z pamięcią cache min 512GB na kontroler. Tryb Active/Active nie może powodować obniżenia któregokolwiek z parametrów macierzy. Połączenia pomiędzy komponentami macierzy dyskowej muszą być realizowane w oparciu o technologię technologii PCIe lub NVMe. Macierz musi obsługiwać wyłącznie dyski typu NVMe niezależnie od skali systemu. Macierz musi być wyposażona w procesory wyposażone we wsparcie dla protokołu NVME. Zamawiający dopuszcza architekturę X86 dwóch producentów procesorów Intel (z generacją co najmniej Skylake) oraz AMD (z generacją Epyc). Oferowana macierz dyskowa musi posiadać minimum 192 GB pamięci cache na kontroler. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD lub kart pamięci FLASH jako pamięci cache. Macierz musi posiadać dwa niezależne kontrolery z możliwością rozbudowy poprzez bezprzerwową wymianę kontrolerów do modelu wyższego. Proces wymiany nie może wymagać od zamawiającego okien serwisowych, producent musi zapewnić konsystencje danych w trakcie w.w procesu. Wydajność i pojemność takiej macierzy musi wówczas rosnąć liniowo. Zabrania się wykonywania ww. rozbudowy poprzez wymianę macierzy na model z innej rodziny produktowej. Macierz musi mieć możliwość zainstalowania w standardowej szafie serwerowej 19” lub musi być dostarczona z dedykowaną szafą umożliwiającą podłączenie do infrastruktury zamawiającego. Macierz dyskowa musi się cechować zużyciem energii poniżej 1 kWh na 3U rozmiaru fizycznego w szafie RACK.

2.	**Pojemność**	Macierz musi gwarantować 22 TB przestrzeni z uwzględnieniem ochrony danych na poziomie RAID6 oraz mechanizmów deduplikacji oraz kompresji danych bez wykorzystania Thin Provisioningu. Macierz musi umożliwiać rozbudowę do konfiguracji gwarantującej przestrzeń RAW nie mniejszą niż 94 TB.
3.	**Wydajność**	Oczekiwana wydajność to minimum 200 000 IOPS. Dla wydajności macierzy proszę przyjąć warunki: zapis/odczyt na poziomie 30/70, 100% losowo przy bloku 8kB, zerowych trafieniach w pamięć CACHE oraz przy dopuszczalnym średnim opóźnieniu max 0.4 ms. Wydajność jest liczona w obrębie dwóch kontrolerów, przy czym awaria kontrolera macierzy nie może powodować spadku wydajności systemu. Deduplikacja, kompresja, implementacja podwójnej parzystości, szyfrowanie wszystkich danych oraz uruchomione snapshoty nie mogą wpływać na wydajność macierzy.
4.	**Wysoka dostępność**	Kontrolery muszą pracować w trybie wysokiej dostępności, tzn. w przypadku awarii jednego kontrolera, inny kontroler automatycznie przejmuje jego funkcje, czyli udostępnia klientom (tzw. hostom) wszystkie zdefiniowane w macierzy zasoby bez utraty połączenia do tych zasobów. Awaria kontrolera nie może powodować spadku wydajności macierzy w punktu widzenia hostów. Macierz będzie zasilana jednocześnie z dwóch niezależnych źródeł zasilania. Zanik jednego z nich nie może powodować przerwy w pracy urządzenia. Wszystkie krytyczne komponenty macierzy: kontrolery, zasilacze, wentylatory muszą pracować w trybie nadmiarowym, tak aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Możliwość uaktualniania oprogramowania (firmware'u) macierzy bez przerywania pracy systemu i bez przerwy w dostępie do danych od strony hostów oraz bez spadku wydajności w trakcie trwania w.w operacji. Macierz musi zapewniać poziom protekcji danych odpowiadający cechom RAID 6. W przypadku awarii dwóch dysków w grupie dyskowej odbudowa nie może mieć wpływu na wydajność systemu. Macierz musi wspierać obsługę wielu kanałów I/O (multipathing). W przypadku awarii ścieżki dostępu do macierzy musi nastąpić automatyczne przełączenie kanału komunikacji. Przełączanie kanałów

		I/O musi być wspierane przez natywne mechanizmy systemów operacyjnych wspieranych przez macierz.
5.	**Bezpieczeństwo danych**	Macierz muszą realizować szyfrowanie danych algorytmem AES 256 lub lepszym – globalnie i domyślnie dla wszystkich danych zapisywanych na systemie. Dodatkowo macierz musi realizować szyfrowanie wszystkich zainstalowanych dysków. Oba niezależne klucze szyfrujące muszą być wymieniane domyślnie co 24h oraz po każdym zdarzeniu wyjęcia nośnika danych. Macierz mogą zostać zabezpieczone kluczem sprzętowym w celu zablokowania dostępu do danych na wypadek próby uruchomienia macierzy w sposób nieautoryzowany. Usunięcie klucza sprzętowego z macierzy uniemożliwia odczyt danych użytkownika. Macierz musi wspierać szyfrowanie dysków natywnie lub za pomocą dostarczonych narzędzi zewnętrznych bez wpływu na wydajność macierzy. a. Szyfrowanie powinno umożliwiać zabezpieczenie danych zgodnie z minimum FIPS 140-2. b. Produkt lub oprogramowanie do szyfrowania musi znajdować się na liście weryfikacji programu FIPS 140-3 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list c. Wszystkie zasoby macierzy, w tym klony i kopie migawkowe (snapshoty), mogą być objęte konfigurowalną retencją danych o długości do 30 dni d. Usunięcie dowolnego zasobu, w tym klona czy migawki, nie oznacza jego skasowania przynajmniej na okres 24 godzin. e. Usunięte zasoby macierzy, w tym klony i migawki, mogą zostać przywrócone przez określony (konfigurowalny) czas. f. Ostateczne skasowanie dowolnego zasobu macierzy, w tym klona czy migawki, nie może odbyć się z pominięciem skonfigurowanego czasu retencji (np. od razu po jego usunięciu). g. Czas retencji może zostać skonfigurowany globalnie dla wszystkich zasobów i/lub za pomocą reguł dla wybranej grupy zasobów. h. Czas retencji może zostać zablokowany w taki sposób, aby administrator macierzy nie miał możliwości jego skrócenia niezależnie od poziomu jego uprawnień. i. Czas retencji może być zablokowany w taki sposób, aby administrator nie miał możliwości ostatecznego skasowania zasobów macierzy, w tym migawek czy klonów, przed upływem skonfigurowanego dla tych zasobów czasu retencji i niezależnie od poziomu uprawnień administracyjnych. j. Zapełnienie macierzy w 100% dostępnej pojemności nie może powodować utraty dostępu do danych.

		k. Analiza i ochrona wolumenów pod kątem ataków ransomware. l. Migawki i klony są zawsze oparte o wskaźniki (metadane) m. Wykonanie migawki dowolnego zasobu jest natychmiastowe i nie zajmuje dodatkowego miejsca na dane n. Wykonanie migawki nie inicjuje żadnego procesu kopiowania danych o. Dla zasobów replikowanych synchronicznie, polityka retencji danych również podlega replikacji i jest spójna dla obu macierzy biorących udział w relacji replikacji synchronicznej. p. Dla zasobów replikowanych asynchronicznie, polityka retencji danych może być skonfigurowana niezależnie dla źródła i celu w relacji replikacji. q. Dla zasobów klonowanych polityka retencji danych może być inna niż dla zasobów źródłowych. Uszkodzone dyski pozostają własnością Zamawiającego. Rozwiązanie równoważne – macierz szyfruje wszystkie dane i nośniki algorytmem minimum AES256 z wymianą kluczy szyfrujących domyślnie co 24h oraz po każdym zdarzeniu wyjęcia nośnika danych.
6.	**Protokoły / Porty dostępowe**	Macierz musi prezentować dane z użyciem FC 32/64Gb, iSCSI, NVMe-o-Fabric (TCP, FCP, RDMA) oraz natywnie realizować usługi plikowe dla protokołów NFS v3/v4 i SMB v2/v3 Natywna obsługa protokołów NFS oraz SMB musi być realizowana w obrębie kontrolerów macierzy bez konieczności dodawania zewnętrznych głowic NAS lub wewnętrznego oprogramowania producentów innych niż producent macierzy np. w postaci kontenera, wirtualnej maszyny itp. Oprogramowanie macierzy musi realizować: a. Wsparcie dla wolumenów blokowych LUN min. 64TiB b. Wsparcie dla wolumenów Plikowych NAS CIFS/NFS min. 1PiB c. Obsługę minimum 5 miliardów plików per system Macierz musi posiadać możliwość podłączenia do sieci SAN co najmniej 4 portami SFP+ 64Gbps FC (wkładki 32Gbit/s FC będą dołączone do macierzy). Macierz musi posiadać możliwość podłączenia do sieci Ethernet co najmniej 4 portami SFP+ 10/25Gbps (wkładki światłowodowe obsługujące transfer 10Gbps będą dołączone do macierzy).
7.	**Efektywność danych**	a. Deduplikacja, kompresja oraz thin provisioning nie wymagają żadnej konfiguracji i są zawsze włączone oraz zachodzą dla wszystkich danych zapisywanych na macierzy w trybie in-line oraz post-process. b. Deduplikacja odbywa się zmiennym blokiem od 512B do 32KB – zamawiający dopuści rozwiązanie deduplikujące stałym blokiem w przypadku zaoferowania 2x większej pojemności netto tj. 44TB netto)

		c. Kompresja implementowana jest minimum 5 zmiennymi algorytmami. d. Deduplikacja, kompresja i thin provisioning nie wpływają na wydajność macierzy. e. Macierz raportują globalny współczynnik redukcji danych i jego zmiany w czasie. f. Raportowany współczynnik redukcji danych uwzględnia tylko dane użytkowe i nie obejmuje kopii migawkowych.
8.	**Kopie zapasowe**	Macierz musi umożliwiać tworzenie snapshotów istniejących wolumenów (minimalna liczba snapshotów 100 tys). Migawki (snapshoty) mogą być tworzone w oparciu o harmonogramy, niezależnie, dla różnych grup zasobów wraz z konfigurowalną, automatyczną retencją. a. Migawki i klony są zawsze oparte o wskaźniki. b. Wykonanie migawki dowolnego zasobu jest natychmiastowe. c. Wykonanie migawki wielu zasobów jest natychmiastowe. d. Wykonanie migawki nie inicjuje żadnego procesu kopiowania danych. e. Wykonanie klona nie inicjuje żadnego procesu kopiowania danych. f. Odtworzenie danych z migawki nie inicjuje żadnego procesu kopiowania danych. g. Odtworzenie danych z klona nie inicjuje żadnego procesu kopiowania danych. h. Klonowanie zasobów jest natychmiastowe, niezależnie od rozmiaru oraz ilości klonowanych zasobów. i. Klonowaniu podlega również rozmiar wolumenu źródłowego. j. Wykonanie migawki na zasobach replikowanych synchronicznie odbywa się na obu macierzach jednocześnie i nie inicjuje żadnego procesu kopiowania danych. k. Odtworzenie z migawki zasobów replikowanych synchronicznie nie zaburza procesu replikacji synchronicznej i odbywa się w sposób natychmiastowy i niewymagający resynchronizacji danych. l. Po sklonowaniu zasobu (klon dostępny R/W), zasób źródłowy może być od razu usunięty. Usunięcie nie inicjuje żadnego procesu kopiowania danych. m. Migawki i klony w momencie utworzenia nie zajmują przestrzeni dyskowej (cienkie klony oraz cienkie migawki oparte o wskaźniki - pointers). n. Migawki mogą być tworzone w oparciu o harmonogramy, niezależnie, dla różnych grup zasobów wraz z konfigurowalną, automatyczną retencją. o. Przywrócenie wolumenu z migawki lub klona przywraca również rozmiar zapisany w klonie lub migawce. p. Tworzenie migawek lub klonów nie blokuje żadnych operacji administracyjnych na wolumenie (np. można zmienić rozmiar wolumenu pomimo istniejących migawek czy klonów tego wolumenu).

		q. Utworzenie klona nie tworzy żadnej relacji pomiędzy klonem a wolumenem źródłowym. r. Wydajność klona jest taka sama jak wolumenu źródłowego od razu po zainicjowaniu operacji klonowania. s. Klon jest dostępny dla hostów w trybie R/W od razu po zainicjowaniu operacji klonowania.
9.	**Replikacja synchroniczna**	Macierz musi posiadać możliwość replikacji danych w trybie synchronicznym. Funkcjonalność replikacji musi spełniać następujące założenia: a. Parametry danego zasobu (rozmiar, nazwa) również podlegają replikacji. b. Migawki danego zasobu również podlegają replikacji synchronicznej. c. Zasoby replikowane synchronicznie mogą być replikowane również asynchronicznie (kaskadowo lub niezależnie) d. Klony dowolnych zasobów są automatycznie replikowane synchronicznie. e. Komunikacja z mediatorem (świadkiem, quorum) klastra odbywa się z użyciem protokołu TCP/IP (HTTPS), f. Zmiana mediatora (świadka) w relacji synchronicznej nie wymaga przerwania procesów replikacji danych. g. Replikacja może odbywać się z użyciem zarówno sieci IP lub FC. h. W przypadku awarii jednej z macierzy lub połączenia między macierzami mechanizm replikacji synchronicznej gwarantuje dostępność danych na co najmniej jednej macierzy. Przywrócenie połączenia automatycznie resynchronizuje dane i automatycznie przywraca dostęp do danych z obu macierzy jednocześnie – nie jest dozwolone wymaganie interwencji manualnej celem przywrócenia działania replikacji. i. Replikacja synchroniczna zasobów może być zamieniona na replikację asynchroniczną bez przerwania dostępu do danych. j. Replikacja asynchroniczna zasobów może być zamieniona na replikację synchroniczną bez przerwania dostępu do danych. k. Mediator w replikacji synchronicznej musi umożliwiać konfigurację usługi na minimum 2000 wolumenów. l. System musi wspierać RTT na poziomie min 10ms. umożliwiając replikację w mniej wydajnych sieciach
10.	**Replikacja asynchroniczna**	a. Migawki mogą podlegać replikacji asynchronicznej niezależnie od innych mechanizmów replikacji danych. b. Replikacja asynchroniczna migawek zasobów replikowanych synchronicznie. c. Replikacja wg harmonogramu replikacji z konfigurowalną retencją, niezależnie, na macierzy źródłowej i docelowej. d. Replikacja dowolnego zasobu na inną macierz na życzenie.
11.	**Replikacja semi-synchroniczna**	a. Wbudowana w macierz jako natywna usługa replikacji

		b. Umożliwiająca replikowanie dużych zasobów danych bez wpływu na wydajność zasobów źródłowych c. Obsługa wolumenów Blokowych oraz Plikowych d. Mechanizm kontroli konsystencji oparty o Journal Log e. Możliwość pre-mapowania hostów z wolumenami zdalnymi f. Tolerancja dla dowolnej latencji i długości łącza
12.	**Kompatybilność**	Macierz musi wspierać następujące najnowsze systemy operacyjne (tj. wersje datowane na ostatnie 6 miesięcy) bez konieczności zakupu dodatkowego płatnego oprogramowania dla następujących platform operacyjnych: a. Windows Server b. Linux – CentOS, Ubuntu, RedHat c. Vmware System operacyjny macierzy musi umożliwiać integrację z Vmware vSphere poprzez instalację wtyczki (pluginu) do Vmware vCenter, Vmware vRealize (Orchestrator oraz Operations Manager) oraz VM Log Insight. Wymienione aplikacje muszą rozpoznawać natywnie oferowaną macierz oraz intepretować jej statystyki. System operacyjny macierzy musi się integrować z funkcjonalnością Commvault Intellisnap i być przez nią obsługiwany. Potwierdzenie integracji musi być potwierdzone przez dokumentację producenta CommVaulte na stronie: https://documentation.commvault.com/snap/#/storage_search Należy dostarczyć wszystkie wymagane licencje jeżeli są wymagane do poprawianego działania systemu kopii zapasowych CommVault Intellisnap z oferowanym systemem. System operacyjny macierzy musi się integrować z funkcjonalnością Veeam Backup and Recovery minimum v12 i być przez nią natywnie obsługiwany.
13.	**Zarządzanie**	Macierz musi posiadać graficzny interfejs web umożliwiający zdalne zarządzanie macierzą. Macierzami można zarządzać z poziomu wbudowanego GUI(HTML5), CLI (SSH) oraz REST API bez konieczności użycia oprogramowania instalowanego poza macierzą. Dostęp do GUI i/lub CLI może zostać skonfigurowany z użyciem Active Directory. Dla CLI, dodatkowo, dostęp może odbywać się z użyciem kluczy SSH. Macierz posiada REST API i CLI umożliwiające automatyzację jakichkolwiek funkcjonalności dostępnych w ramach macierzy, zgodnie ogólnie przyjętymi, najlepszymi praktykami w zakresie bezpieczeństwa tego typu operacji.

14.	**Monitorowanie**	Macierz powinna być dostarczona z oprogramowaniem pozwalającym na ciągłe monitorowanie i raportowanie zasobów i wydajności. Obsługa Usługi Phonehome/Call home, za pomocą bezpiecznego kanału komunikacji (HTTPS oparty o SSL minimum 128 bit) między produktami macierzą a platformą analityczną, pozwalajaca na przesyłanie danych telemetrycznych i logów do chmury, gdzie są one przetwarzane na potrzeby analizy wsparcia oraz wykorzystywane przez różne interfejsy użytkownika. a. Macierz mają możliwość wysyłania telemetrii bezpośrednio do producenta z możliwością podglądu przez administratora, również danych historycznych. b. Macierz mają możliwość nawiązania zdalnej sesji VPN do centrum serwisowego w celu umożliwienia dostępu przez personel producenta. Funkcjonalność jest włączana lub wyłączana w dowolnej chwili przez administratora macierzy.
15.	**Platforma monitoringu**	Platforma Analityczna zarządzania oraz monitoringu pamięcią masową, która musi oferować szereg funkcji ułatwiających zarządzanie infrastrukturą pamięci masowej, takich jak: a. monitorowanie wydajności i stanu pamięci masowej w czasie rzeczywistym. Użytkownicy mogą śledzić wykorzystanie zasobów, wydajność i inne kluczowe wskaźniki. b. wykorzystanie narzędzi do planowania pojemności i wydajności, pozwalające na lepsze zarządzanie zasobami macierzowym oraz unikanie problemów związanych z przeciążeniem. c. Musi umożliwiać zarządzanie pamięcią masową na podstawie zdefiniowanych polityk, pozwalając na automatyzację i optymalizację operacji. d. Musi umożliwiać automatyczne rebalansowanie obciążeń i zarządzanie wieloma systemami pamięci masowej jako jedną spójną całość. e. Platforma musi umożliwiać monitoring bezpieczeństwa oprogramowania wraz z wykonywać zdalną bezprzerwową aktualizację oprogramowania oraz zabezpieczeń macierzy na żądanie użytkownika bez ingerencji wsparcia technicznego. f. Ocena odporności danych, wybudowane narzędzie do śledzenia polityk adaptacji technologii ochrony danych, wraz ze wskaźnikiem oceny poziomu ochrony danych na skali od 0 do 5. g. Wykrywanie anomalii redukcji danych – musi zawierać funkcje analizy zmiany poziomu redukcji danych wraz z potencjalną identyfikacją ataku ransomware, wspomagając szybsze odzyskiwanie danych. h. Oznaczanie (tagowanie) zasobów, Musi umożliwiać użytkownikom kategoryzowanie zasobów, takich jak Macierz, wolumeny czy inne urządzenia, za pomocą tagów. Tagi mogą być używane do

		raportowania, zarządzania cyklem życia, alertów, powiadomień, polityk bezpieczeństwa i ochrony. i. Platforma Analityczna umożliwia zarządzanie dostępem do funkcji za pomocą flag funkcji, co pozwala na kontrolowanie, które funkcje są dostępne dla określonych organizacji lub użytkowników. Wraz z macierzą musi zostać dostarczone oprogramowanie do analityki end-to-end środowiska Vmware vSphere Zamawiającego korzystającego z zasobów oferowanej macierzy. Oprogramowanie musi: a. być dostępne dla administratora poprzez przeglądarkę WWW b. Umożliwiać jednoczesną analizę co najmniej: pojedynczej maszyny wirtualnej, pojedynczego pliku VMDK, pojedynczego hosta ESXi, pojedynczego wolumenu macierzy c. raportować następujące metryki w formie numerycznej i graficznej a. IOPS b. Przepustowość na sekundę (MB/GB per second) c. Opóźnienie (latencję) w ms d. Obciążenie CPU i pamięci dla maszyn wirtualnych d. Wskazywać w formie graficznej korelację analizowanego komponentu z pozostałymi monitorowanymi komponentami środowiska Vmware. Komponentem jest VM, plik VMDK, host ESXi, wolumen macierzy, kontroler macierzy. e. Raportować powyższe metryki historycznie na co najmniej 7 dni wstecz Jeżeli do działania w/w oprogramowania wymagana jest licencja musi ona zostać dostarczona na pełną oferowaną pojemność macierzy ze wsparciem producenta na okres zgodny z gwarancją macierzy.
16.	**Gwarancja**	Urządzenie musi być objęte gwarancją min. 3 lat 24/7 z NBD czasem wymiany uszkodzonych komponentów, niezależnie od ilości danych zapisanych na nośnikach półprzewodnikowych. Tryb gwarancji musi umożliwiać ciągłe rozszerzenie/przedłużenie gwarancji dla macierzy przez producenta. System musi umożliwiać bezprzewodową aktualizację oprogramowania oraz sprzętu do wyższych generacji w ramach usługi gwarancyjnej producenta. W ramach aktualizacji oprogramowania oraz wymiany sprzętu, nie może wystąpić konieczność ustawiania okien serwisowych, oznacza to że system powinien podczas prac aktualizacyjnych być w pełni dostępny, a prace te nie powinny wpływać na wydajność systemu.

System kontroli i zarządzania dostępem do sieci (NAC)

Przedmiotem postępowania jest dostarczenie centralnego systemu kontroli i zarządzania dostępem do sieci LAN oraz WLAN współpracującego z posiadaną przez Zamawiającego infrastrukturą dostępową.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu NAC były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy wirtualne wraz z odpowiednio zabezpieczonym systemem operacyjnym. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: Vmware vSphere oraz Microsoft Hyper-V.

W ramach postępowania muszą zostać dostarczone wszystkie elementy fizyczne lub wirtualne niezbędne do monitorowania i zarządzania kontrolą dostępu.

LP	Parametr lub warunek minimalny	Minimalne wymagania
1.	**Architektura**	1. System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu (skalowanie). 2. Elementy Systemu muszą umożliwiać klastrowanie active-passive. 3. Wszystkie elementy Sytemu powinny być zarządzane centralnie. 4. System i jego wszystkie funkcje muszą w pełni współpracować z urządzeniami Zamawiającego (tj. można na nich wydawać polecenia konfiguracyjne z poziomu systemu kontroli i zarządzania dostępem do sieci): • Firewall: Fortigate 60F • Przełączniki Fortiswitch148F-POE • Domena Active Directory
2.	**Funkcje Systemu**	1. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem: • standardu 802.1X • adresu MAC urządzenia • formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników w Systemie.

		2. System musi obsługiwać uwierzytelnianie w oparciu o: wbudowany serwer RADIUS, zewnętrzny serwer Radius, protokół LDAP, jak również w oparciu o wewnętrzną bazę użytkowników i urządzeń. 3. System musi obsługiwać autoryzację w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS. 4. System musi zapewniać automatyczne wykrywanie urządzeń końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych. W ramach postępowania muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci. 5. System powinien logować i przetrzymywać we własnej bazie danych co najmniej następujące informacje: • adresy MAC przełączników, urządzeń końcowych i dostępowych, • adresy IP ww. urządzeń • identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe • stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena. w oparciu skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów • informacje o użytkownikach • nazwa użytkownika do którego przypisany jest urządzenie końcowe • nazwa zalogowanego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja • profil/rola jak została przydzielona urządzeniowi końcowemu przez System • data zarejestrowania urządzenia końcowego w Systemie • data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia 6. System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) opartych o złożone i wielowarunkowe polityki bezpieczeństwa. Powinny one obejmować co najmniej: lokalizacja

		urządzenia w sieci, przynależność do grupy administracyjnej, parametr opisujący urządzenie lub użytkownika. 7. System musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione mechanizmy automatycznej kwarantanny oraz blokowania. 8. System musi zapewniać możliwość powiadamiania poprzez SYSLOG oraz pocztę elektroniczną o sytuacjach krytycznych np. związanych z próbą nieautoryzowanego dostępu do sieci lub awarii wewnętrznych usług Systemu NAC. 9. System musi posiadać wewnętrzną bazę urządzeń. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Systemu lub z wykorzystaniem API. 10. System musi wykorzystywać informacje zawarte w bazie urządzeń końcowych dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji. 11. System musi posiadać bazę minimum 30 kategorii urządzeń końcowych. 12. System musi mieć możliwość klasyfikacji jednorazowej przy wstępnym uwierzytelnianiu/rejestracji bądź klasyfikacji wielokrotnej. Klasyfikacja urządzeń i użytkowników musi bazować na harmonogramie z częstotliwością w przedziale od kilku minut do kilku tygodni. 13. System musi umożliwiać wykonywanie na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa. 14. System musi obsługiwać telefony IP wraz z możliwością podłączenia do nich stacji końcowych (przez wbudowany przełącznik w telefonie) przypisując każdemu z urządzeń dedykowane polityki bezpieczeństwa. 15. System musi podejmować decyzję o przyłączeniu urządzeń końcowych do sieci poprzez ocenę ich zgodności ze zdefiniowanymi wymaganiami. Ocena zgodności musi być realizowana zarówno bez dedykowanego agenta instalowanego na stacji końcowej (za pomocą metod takich jak: WinRM, WMI) jak i z użyciem agenta. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect" przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci.

		16. Klasyfikacja urządzeń końcowych z użyciem agenta dedykowanego dla komputerów z systemem Windows i MAC OS X musi umożliwiać przeprowadzenie następujących testów: a. Sprawdzenie wersji agenta b. Sprawdzenie wersji systemu operacyjnego, c. Sprawdzenie obecności i stanu oprogramowania antywirusowego (niezainstalowany/zainstalowany, uruchomiona ochrona, zaktualizowany), d. test zapory (włączona/wyłączona), e. test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie), f. test usługi Windows Update z opcją automatycznego naprawienia niezgodności g. test obecności/niewystępowania pliku o określonej nazwie h. test obecności procesu (uruchomiony/nieuruchomiony) i. test rejestru dla systemów Windows (obecność klucza o zdefiniowanej nazwie, typie wartości i wartości, równy bądź różny zadanemu) j. test stanu usługi (uruchomiona/nieuruchomiona) k. test obecności aplikacji (sprawdzenie czy aplikacja zdefiniowanej nazwie jest zainstalowana) 17. System musi mieć możliwość przeprowadzania różnych metod testowania w zależności od lokalizacji urządzenia w sieci, przynależności do grupy administracyjnej, parametru opisującego urządzenie lub użytkownika. 18. Podczas oceniania urządzenia końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów w przypadku braku zgodności. 19. System musi mieć możliwość przeniesienia urządzenia do kwarantanny w przypadku braku komunikacji z agentem. 20. Na urządzeniu podlegającym kwarantannie musi zostać wyświetlona informacja o fakcie przeniesienia urządzenia do kwarantanny oraz informacja z wytycznymi o działaniach jakie użytkownik urządzenia musi podjąć w celu usunięcia niezgodności.

		21. Administrator musi mieć możliwość określenia poziomu niezgodności z politykami, po którym będzie następowało przeniesienia stacji do kwarantanny. 22. System musi zapewniać integrację z rozwiązaniami bezpieczeństwa (platformy Firewall, systemy SIEM, systemy Antymalware, systemy MDM) na potrzeby oceny stanu urządzeń końcowych oraz określenia ich zgodności z polityką bezpieczeństwa NAC. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect" przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci.
3.	**Profilowanie urządzeń**	1. System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, 2. System musi posiadać funkcję automatycznego profilowania urządzeń nie posiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci. 3. System musi umożliwiać dodawania rozpoznanych urządzeń do grup systemowych. 4. System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu. 5. System musi rozpoznawać co najmniej następujące rodzaje urządzeń: • urządzenia z systemem Android, • urządzenia Apple (iPad, iPhone, iPod) • drukarki sieciowe, • telefony IP, • stacje robocza z systemem Microsoft Windows, • stacje robocza z systemem MAC OS, • stacje robocza z systemem Linux.
4.	**Logowanie, Raportowanie i Alarmowanie**	1. System musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).

		2. System musi mieć możliwość generowania szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu urządzenia końcowego. 3. System musi rejestrować dane o atrybutach urządzeń końcowych i raportować zmiany w atrybutach np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia w Systemie. 4. System musi zapewniać dane historyczne o zmianach stanu konfiguracji portów dostępowych. 5. System musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy. 6. System musi oferować możliwość tworzenia własnych szablonów raportów. 7. System musi umożliwiać logowanie do zewnętrznych serwerów logowania z wykorzystaniem Syslog. 8. System musi umożliwiać konfigurację generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora.
5.	**Zarządzanie systemem**	1. System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową w wersji oferowanej przez producenta przeglądarki lub dedykowaną aplikację. 2. System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników lub zewnętrzne repozytorium użytkowników (LDAP lub Radius). 3. System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania - RBA. 4. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do poszczególnych elementów systemu. 5. System musi umożliwiać personalizację wyglądu interfejsu zarządzania, w tym co najmniej zmianę koloru tła i czcionek, treści, grafiki. 6. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych.

6.	**Zarządzanie dostępem gościnnym**	1. System musi umożliwiać przyznawanie dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez wypełnienie formularza w portalu rejestracyjnym. 2. System musi umożliwiać realizację usług BYOD dla urządzeń prywatnych pracowników. 3. Funkcja portalu rejestracyjnego powinna działać bez udziału lub przy minimalnym udziale pracowników IT. System powinien posiadać możliwość delegowania uprawnień do akceptowania kont gości przez pracowników nieposiadających uprawnień administracyjnych w Systemie. 4. Wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego. 5. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych. 6. System musi umożliwiać przyznanie dostępu czasowego dla gości. 7. System musi umożliwiać dopasowanie wyglądu portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.
7.	**Licencje i serwisy**	1. W ramach postępowania koniecznym jest dostarczenie 200 licencji umożliwiających uruchomienie wszystkich wyżej wymienionych funkcji z zastosowaniem agenta na stacjach końcowych, z założeniem że są one równocześnie podłączone do sieci lokalnej LAN i sieci bezprzewodowej WLAN. 5. Licencje w ramach rozwiązania powinny być dostarczone w modelu permanentnym. Zamawiający nie dopuszcza licencji bazujących na subskrypcji. 6. Dostarczony System NAC musi zawierać wszystkie niezbędne komponenty programowe, na których możliwa będzie licencyjna rozbudowa do min. 200 urządzeń równocześnie podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN, z uwzględnieniem instalacji agentowej. 7. Wsparcie: System musi być objęty serwisem producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. 8. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla

		rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
8.	**Opisy wymagań ogólnych**	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Szkolenie NAC

Przedmiotem zamówienia jest przeprowadzenie szkolenia dla działu IT Zamawiającego z obsługi systemu Network Access Control (NAC), który zostanie dostarczony przez Wykonawcę w ramach niniejszego postępowania. Celem szkolenia jest przygotowanie działu iT do skutecznego zarządzania i monitorowania systemu NAC, aby umożliwić kontrolę dostępu do sieci oraz realizację polityki bezpieczeństwa sieciowej organizacji.

LP	**Parametr lub warunek minimalny**	**Minimalne wymagania**
1.	**Wymagania minimalne**	Zakres szkolenia: Podstawy działania systemu NAC – omówienie architektury i głównych funkcji systemu, w tym zasad dostępu do sieci, procesów autoryzacyjnych oraz polityk bezpieczeństwa. Konfiguracja systemu – wprowadzenie do konfiguracji polityk dostępowych, metod uwierzytelniania oraz integracji z innymi systemami bezpieczeństwa, zgodnie z funkcjonalnością dostarczonego przez Wykonawcę rozwiązania.

		Monitorowanie i analiza zdarzeń – nauka monitorowania aktywności sieciowej oraz reagowania na incydenty związane z naruszeniami polityk bezpieczeństwa. Raportowanie i audyt – szkolenie z obsługi narzędzi raportujących oraz przeprowadzania audytów, zgodnie z funkcjonalnością dostarczonego rozwiązania NAC. Praktyczne ćwiczenia – warsztaty z samodzielnego zarządzania i rozwiązywania problemów w ramach systemu NAC, dostosowane do interfejsu i specyfiki rozwiązania dostarczonego przez Wykonawcę. Wymagania dotyczące szkolenia: Szkolenie musi być przeprowadzone w formie stacjonarnej. Szkolenie powinno obejmować część teoretyczną oraz praktyczną, tak aby uczestnicy nabyli umiejętności konieczne do samodzielnej obsługi i zarządzania systemem NAC w środowisku Zamawiającego.

System do zbierania logów

LP	Parametr lub warunek minimalny	Minimalne wymagania
1.	**Wymagania ogólne**	W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
2.	**Interfejsy, Dysk:**	1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.
3.	**Parametry wydajnościowe**	1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

		W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:
4.	**Logowanie**	1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
5.	**Raportowanie**	W zakresie raportowania system musi zapewniać: 1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów.

		5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
6.	**Korelacja logów**	W zakresie korelacji zdarzeń system musi zapewniać: 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. 4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
7.	**Zarządzanie**	1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
8.	**Serwisy i licencje**	1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla

		rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. 2. Wsparcie: System musi być objęty serwisem producenta upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7 oraz mieć zalicencjonowaną funkcję analizy logów archiwalnych przez okres 24 miesięcy.
9.	**Opisy wymagań ogólnych**	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

System kopii bezpieczeństwa

Całe rozwiązanie musi być kompleksowe tj. składać się z biblioteki, dedykowanego serwera oraz odpowiedniego oprogramowania do backup'u. Minimalne parametry poszczególnych elementów poniżej:

LP	**Parametr lub warunek minimalny**	**Minimalne wymagania**
	Biblioteka	
1.	**Autoloader/biblioteka taśmowa w obudowie RACK**	● Typ napędu zainstalowanego napędu – LTO 8 z interfejsem SAS ● Liczba zainstalowanych napędów – 1 szt. ● Liczba obsługiwanych napędów - 1 szt. ● Liczba dostarczonych aktywnych slotów – 8 szt.

		● Liczba slotów Import/Export - 1 szt. ● Wbudowany skaner kodów paskowych na nośnikach LTO ● Lokalne zarządzanie za pomocą panelu/pulpitu operatora ● Obsługa szyfrowania danych na nośniku LTO ● Obsługa nośników LTO RW oraz LTO WORM ● Gwarantowana kompatybilność odczytu taśm LTO-7 ● Gwarantowana kompatybilność zapisu taśm LTO-7 ● Interfejs zdalnego zarządzania - Ethernet 10/100Mb/s złącze RJ-45 ● Zapis danych: 300 MB/s ● Odczyt danych: 750 MB/s ● Rozmiar bufora: 1000 MB ● 1 nośnik czyszczący LTO ● 8 nośników LTO-8 RW
2.	**Gwarancja jakości producenta**	● 60 miesięczny okres gwarancji ze skuteczną naprawą w następny dzień roboczy ● Realizowana w miejscu instalacji sprzętu, gwarantowana wizyta certyfikowanego serwisanta producenta w miejscu użytkowania sprzętu do końca następnego dnia roboczego od zgłoszenia. ● Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.
3.	**Spełniane normy i standardy**	● EN 60950-1, IEC 60950-1, UL 60950-1, CSA 60950-1 ● EN 55022 Class A, EN 61000-3-3, EN 61000-3-2, ICES 003 Class A, FCC Part-15 Class A, VCCI Class A, AS/NZS CISPR22 Class A, CNS 13438, EN 55024 ● RoHS, Weee, 2011/65/EC
Oprogramowanie do backupu		
1.	**Wymagania minimalne**	1 Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji

		a) Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012 b) Vmware vSphere min. w wersjach v5.5 - v8.0U3 c) Nutanix AHV v6.5.4 (LTS) d) Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012 e) Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams) 2. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V 3. Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia: a) na serwerze Windows lub Linux b) jako maszyna wirtualna Vmware c) jako maszyna wirtualna Amazon d) na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital 4. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS 5. Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania 6. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
2.	**Licencjonowanie**	1. Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności 2. Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta

		powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska 3. W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 2 lat wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania 4. W ramach dostawy wymagane jest dostarczenie licencji na ochronę 4 gniazd procesorów w hostach Vmware lub Hyper-V 5. Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
3.	**Ochrona danych**	1. Oprogramowanie musi posiadać funkcje backupu i replikacji: a) Backup maszyn wirtualnych Vmware b) Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu c) Backup maszyn wirtualnych Hyper-V d) Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu e) Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych f) Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie g) Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu h) Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym i) "Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem"

		j) Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania k) Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji l) Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
4.	**Optymalizacja wykorzystania miejsca na dane**	1. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych: a) Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane b) Kompresja backupu, w tym konfigurowalny stopień kompresji c) Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
5.	**Spójność danych**	1. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych: a) Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux b) Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu c) Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: Microsoft Exchange 2013, 2016, 2019 Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022 d) Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki e) Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V

		f) Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania g) Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
6.	**Przywracanie danych**	1. Oprogramowanie musi posiadać poniższe funkcje: a) Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji b) Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej) c) Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej) d) Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): Microsoft Exchange MS Active Directory MS SQL e) Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
7.	**Wydajność**	1. Oprogramowanie do backupu musi pozwalać na: a) Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT b) Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych c) Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN d) Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci e) Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
8.	**Zarządzanie**	1. Oprogramowanie musi pozwalać na następujące formy zarządzania:

		a) Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych b) Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej c) Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania d) Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport. e) Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji f) Oprogramowanie musi umożliwiać integrację z Active Directory g) Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach
Serwer		
1.	**Obudowa**	● Typu RACK, wysokość nie więcej niż 1U; ● Szyny umożliwiające wysunięcie serwera z szafy stelażowej ● Możliwość zainstalowania 8 dysków twardych hot plug 2,5”; ● Możliwość zainstalowania zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; ● Zainstalowane 2 szt. dysków SSD M.2 960GB skonfigurowane w raid 1, ● Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
2.	**Płyta główna**	● Dwuprocesorowa; ● Wyprodukowana i zaprojektowana przez producenta serwera; ● Możliwość instalacji procesorów 60-rdzeniowych; ● zainstalowany moduł TPM 2.0;

		● 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5; ● Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH; ● 32 gniazda pamięci RAM; ● Obsługa 8 TB pamięci operacyjnej RAM DDR4; ● Wsparcie dla technologii: ● Memory Scrubbing; ● SDDC; ● ECC; ● Memory Mirroring; ● ADDDC; ● Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug. ● BIOS UEFI w specyfikacji 2.7.
3.	**Procesory**	● Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64; ● osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta.
4.	**Pamięć RAM**	● 128 GB pamięci RAM; ● DDR4 Registered 4800MT/s; ● Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;
5.	**Kontrolery I/O**	● karta 2x16GB FC
6.	**Kontrolery LAN**	● Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: ● 4x 1Gbit Base-T, ● Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

		● Interfejsy LAN zainstalowane w slotach PCI-e: 2x10Gbit SFP obsadzone wkładkami światłowodowymi MultiMode 10G
7.	**Kontroler**	● Kontroler pracujący w trybie Host Bus Adapter z zewnętrznym porteme SAS
8.	**Porty**	● Zintegrowana karta graficzna ze złączem VGA z tyłu serwera ● 2 porty USB 3.0 dostępne z tyłu serwera; ● 2 porty USB 3.0 na panelu przednim; ● Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; ● Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
9.	**Zasilanie, chłodzenie**	● Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; ● Redundantne wentylatory hotplug.
10.	**Zarządzanie**	● Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; ● informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: ● karty rozszerzeń zainstalowane w dowolnym slocie PCI Express; ● procesory CPU; ● pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM; ● status karty zarządzającej serwera; ● wentylatory; ● bateria podtrzymująca ustawienia BIOS płyty głównej; ● zasilacze; ● system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);

		● Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: ● Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; ● Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ● Dostęp poprzez przeglądarkę Web, SSH; ● Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ● Zarządzanie alarmami (zdarzenia poprzez SNMP); ● Możliwość przejęcia konsoli tekstowej; ● Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); ● Obsługa serwerów proxy (autentykacja); ● Obsługa VLAN; ● Możliwość konfiguracji parametru Max. Transmission Unit (MTU); ● Wsparcie dla protokołu SSDP; ● Obsługa protokołów TLS 1.2, SSL v3; ● Obsługa protokołu LDAP; ● Integracja z HP SIM; ● Synchronizacja czasu poprzez protokół NTP; ● Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; ● Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); ● Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów

		zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; ● Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
11.	**Wspierane OS**	● Microsoft Windows Server 2022, 2019; ● VMWare vSphere 8.0;; ● Suse Linux Enterprise Server 15; ● Red Hat Enterprise Linux 9, 8; ● Microsoft Hyper-V Server 2019
12.	**Gwarancja**	● 5 lat gwarancji producenta serwera w trybie on-site z czasem skutecznej naprawy w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej; ● Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu; ● Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; ● Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; ● Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).
13.	**Dokumentacja, inne**	● Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; ● Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

		● Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; ● W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; ● Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; ● Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwera. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV. ● Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; ● Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04; ● Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.

UPS (25 sztuk)

LP	Parametr	Wymagania minimalne
1.	**Moc pozorna**	minimum 650VA
2.	**Moc rzeczywista**	minimum 360W
3.	**Technologia**	minimum line-interactive
4.	**Typ obudowy**	tower
	Wejście	
5.	**Napięcie wejściowe**	minimum 220/230/240 VAC

6.	**Zakres napięcia wejściowego**	minimum 140-300 VAC
7.	**Częstotliwość**	minimum 50/60 Hz (auto wykrywanie)
	Wyjście	
8.	**Regulacja napięcia**	minimum '+/- 10 %
9.	**Kształt napięcia wyjściowego**	minimum symulowana sinusoida
10.	**Typowy czas przełączania**	2-6 ms
	Baterie	
11.	**Baterie wewnętrzne w UPS**	minimum 12V 7Ah; szczelne, bezobsługowe
12.	**Czas podtrzymania (50 % Pmax)**	minimum 5 minut
	Pozostałe	
13.	**Wejście zasilania**	kabel zamontowany na stałe w obudowie UPS zakończony wtykiem PL/FR
14.	**Ilość i typ gniazd wyjściowych**	minimum 2 gniazda Schuko z podtrzymaniem
15.	**Stabilizacja napięcia AVR Boost & Buck**	wymagana
16.	**Filtr RJ45**	wymagany
17.	**Funkcja autorestartu po powrocie zasilania**	wymagana
18.	**Funkcja zimnego startu**	wymagana
19.	**Sygnalizacja**	Wyświetlacz LCD, dźwiękowa
20.	**Informacje wyświetlane na panelu LCD**	minimum napięcie wejściowe i wyjściowe, poziom obciążenia, poziom naładowania baterii, praca z sieci/baterii, przeciążenie, niski poziom baterii
21.	**Interfejs komunikacyjny**	USB
22.	**Zabezpieczenia**	minimum przed zwarciem, przeciążeniem, rozładowaniem
23.	**Alarmy dźwiękowe**	minimum informujące o trybie bateryjnym, rozładowaniu baterii, przeciążeniu, awarii
24.	**Waga UPS**	do 4,5 kg
25.	**Wymiary UPS**	nie większe niż: głębokość 290 mm, szerokość 105 mm, wysokość 145 mm
26.	**Gwarancja**	minimum 24 miesiące na elektronikę i 12 miesięcy na baterie
27.	**Serwis**	autoryzowany serwis producenta zlokalizowany w Polsce. naprawa w maksymalnie 14 dni roboczych serwis realizowany w systemie door to door

28.	**Oprogramowanie**	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS wsparcie dla systemów: Windows, Linux wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe)
29.	**Certyfikaty producenta (załączyć do oferty)**	deklaracja zgodności CE
30.	**Oświadczenia / dokumenty (załączyć do oferty)**	oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji
		certyfikat lub oświadczenie producenta o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilaczy UPS jeżeli oferent nie jest producentem danego urządzenia

Wdrożenie

Serwery z macierzą

a) Przygotowanie planu wdrożenia i migracji środowiska
b) Instalacja dostarczonego sprzętu w szafie rack w siedzibie Zamawiającego
c) Aktualizacja firmware, bios, konfiguracja zarządzania, konfiguracja sprzętowa,
d) Podłączenie macierzy dyskowej i serwerów z posiadaną przez Zamawiającego infrastrukturą
e) Konfiguracja:
f) Konfiguracja dostarczonych serwerów, macierzy dyskowej i oprogramowania, w celu uruchomienia protokołu FC – wymagana jest pełna konfiguracja hypervisora oraz dostarczonych systemów operacyjnych i sprzętu. Zamawiający wymaga takiej konfiguracji, aby zapewnić wielościeżkowość dla serwera i macierzy dyskowej z wykorzystaniem protokołu FC. System musi działać w klastrze wysokiej dostępności.
g) Konfiguracja wirtualizacji
h) Środowisko oparte o 2 serwery fizyczne oraz współdzielony zasób macierzowy.
i) Konfiguracja klastra HA dla maszyn wirtualnych na 2 maszynach fizycznych
j) Automatyczne przenoszenie i uruchomienie maszyn wirtualnych podczas awarii jednego z serwerów fizycznych na host nieuszkodzony.
k) Konfiguracja wirtualnych przełączników dla obsługi Dynamic VMMQ oraz RDMA.
l) Migracja serwerów wirtualnych posiadanych przez Zamawiającego do nowej infrastruktury serwerowej.
m) Przeniesienie baz danych oraz kluczowych aplikacji Zamawiającego na nowy system operacyjny. Wykonawca przeprowadzi testy poprawności działania przeniesionego oprogramowania (baz danych) oraz wykonywania połączeń z zasobami sieciowymi, logowaniem i autoryzacją użytkowników, zasadami użytkowników, dostępem do sieci Internet.
n) Przeniesienie wszystkich niezbędnych aplikacji z punktu widzenia Zamawiającego wraz z testami poprawności działania po migracji na nowy system operacyjny.

o) Testowanie poprawności działania serwerów wirtualnych po migracji na nowo powstałe środowisko, oraz wykonywania połączeń z zasobami sieciowymi, logowaniem i autoryzacją użytkowników wraz z weryfikacją zasad dotyczących użytkowników i komputerów.

Przełączniki sieciowe

a) Nadanie adresu IP
b) Konfiguracja dostępu SSH
c) Zmiana haseł dostępu
d) Aktualizacja oprogramowania do najnowszej możliwej wersji
e) Konfiguracja segmentacji sieci VLAN
f) Uruchomienie protokół zapobiegania pętlą MSTP lub równoważny
g) Konfiguracja protokołu ELRP lub równoważny
h) Konfiguracja wysyłania logów do serwera logów
i) Konfiguracja funkcjonalności wykrywania telefonów IP, protokół LLDP lub równoważny
j) Uruchomienie protokołu DHCP Snooping lub równoważny
k) Konfiguracja VLANów na wszystkich urządzeniach
l) Konfiguracja protokołu STP
m) Konfiguracja protokołu loop protect

Konfiguracja systemu kontroli dostępu do sieci.

a) Analiza istniejącej infrastruktury sieciowej, w tym identyfikacja urządzeń i użytkowników, którzy będą objęci kontrolą NAC
b) Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji)
c) Przygotowanie mechanizmów redundancji oraz zaplanowanie architektury wysokiej dostępności (HA) systemu NAC.
d) Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
e) Utworzenie polityk dostępowych (np. kto i jakie urządzenia mogą mieć dostęp do określonych zasobów).
f) Integracja NAC z infrastrukturą sieciową (przełączniki, zapory ogniowe, routery, punkty dostępowe Wi-Fi) poprzez mechanizmy 802.1X, SNMP, RADIUS, MAC lub inne protokoły.
g) Uruchomienie uwierzytelniania w oparciu o 802.1X na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
h) Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, testy.
i) Połączenie NAC z istniejącymi systemami bezpieczeństwa (np. SIEM, logs) w celu zarządzania autoryzacją i monitorowaniem zdarzeń.
j) Przeprowadzenie testów autoryzacji w losowych miejscach w organizacji.

System korelacji logów

a) Wdrożenie platformy zarządzania logami
b) Integracja systemu z posiadamy przez zamawiającego urządzeniem firewall.
c) Konfiguracja retencji przechowywania logów.

System wykonywania kopii zapasowej

a) Przygotowanie zdalnych repozytoriów, gdzie będą przechowywane kopie zapasowe (np. dyski, SAN, NAS, lub chmura).
b) Instalacja oprogramowania do backupu.
c) Dodanie serwerów do ochrony: Zainstalowanie agentów na serwerach fizycznych lub dodanie hostów wirtualnych (np. VMware vSphere lub Microsoft Hyper-V), które mają być chronione.
d) Utworzenie zadań backupowych, konfiguracja zadań pełnych, różnicowych oraz przyrostowych kopii zapasowych, jak również harmonogramy automatycznych backupów.
e) Wykonanie testów backupów, testy przywracania.
f) Szkolenie z obsługi systemu.

Biblioteka taśmowa

g) Instalacja i konfiguracja biblioteki taśmowej dla obsługi długoterminowej kopii bezpieczeństwa
h) Konfiguracja dostępu, puli dyskowej, integracja z systemem kopii bezpieczeństwa
i) Instalacja serwera i konfiguracja systemu dla obsługi oprogramowania zarządzającego kopiami bezpieczeństwa
j) Konfiguracja repozytoriów danych
k) Konfiguracja zadań kopii bezpieczeństwa, retencji i zabezpieczeń.
l) Konfiguracja zapisu ja LTO

UPS

a) Instalacja i konfiguracja urządzeń zabezpieczenia prądowego typu UPS

Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:
a) przeprowadzić testy poprawności działania całej infrastruktury
b) przygotować dokumentację powykonawczą zawierająca listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów
c) Ze względu na krytyczne aplikacje które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

- urządzenia dedykowane (embeded), na przykład routery i przełączniki;
- punkty styku z sieciami obcymi
- zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz
- Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:
  - określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
  - wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;

- Badaniu będą podlegały następujące systemy:
  - ✓ rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);
  - ✓ Linux 2.4.x, 2.6.x, 3.x.x;
  - ✓ IBM AIX;
  - ✓ CISCO IOS;
  - ✓ Microsoft SQL;
  - ✓ MySQL;