Załącznik nr 11 do SWZ

Opis Przedmiotu Zamówienia

Cyberbezpieczna infrastruktura z wykorzystaniem wysokodostępnego klastra dla usług: zarządzania poprawności kopii zapasowych, dostępności infrastruktury, bezpieczeństwa danych (archiwizacja)

Wymagania ogólne

1. Wszystkie oferowane produkty elektryczne w przedmiotowym postępowaniu muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE.
2. Wszystkie oferowane Urządzenia muszą posiadać numer seryjny producenta umieszczony na obudowie.
3. Oferowane produkty muszą być sprawne, fabrycznie nowe i nieużywane oraz muszą być wyprodukowane nie wcześniej niż 6 (sześć) miesięcy przed datą dostawy, tj. w okresie 6 miesięcy przed dostawą, nie dopuszcza się użycia sprzętu odnawianego, demonstracyjnego lub powystawowego.
4. Oferowany sprzęt musi pochodzić z autoryzowanego kanału dystrybucji producenta i posiadać pakiet usług gwarancyjnych producenta obejmujący użytkowników z obszaru Rzeczypospolitej Polskiej.
5. Wykonawca dostarczy na wezwanie Zamawiającego oświadczenie producenta sprzętu, potwierdzające, że sprzęt jest fabrycznie nowy oraz pochodzi z oficjalnego kanału sprzedaży producenta.
6. Zamawiający wymaga, aby na etapie odbioru sprzętu, ale przed podpisaniem protokołu odbioru miał możliwość sprawdzenia z wykorzystaniem unikalnego numeru identyfikacyjnego dostarczonego sprzętu jego oryginalnej konfiguracji na stronie producenta sprzętu.
7. Ze względu na pożądaną pełną kompatybilność, zapewnienia jednego centralnego punktu monitorowania i zarządzania oraz scentralizowanego punktu powiadamiania producenta o awariach, dostarczane w ramach Zamówienia rozwiązania z poz. 1, 2, 3 powinny pochodzić od tego samego producenta, chyba że wymagania szczegółowe stanowią inaczej.
   W przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia Producentów o pełnej wzajemnej kompatybilności oraz oświadczenia o współpracy ich autoryzowanych placówek serwisowych w zakresie usuwania problemów powstających na styku rozwiązań.
8. Oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
9. Oprogramowanie dostarczone w ramach postępowania musi pochodzić od certyfikowanego dystrybutora oprogramowania.

10. Oprogramowanie dostarczone w ramach postępowania nie może być wcześniej używane, musi być fabrycznie nowe oraz nieaktywowane nigdy wcześniej na innym urządzeniu.

Wymagania szczególne

Poz. 1 Serwer – 1 szt. (Serwer kopii zapasowej, zarządzania dostępem)

Komponent	Wymagane parametry i właściwości
Obudowa	Obudowa maksymalnie 1U z możliwością montażu w szafie rack (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez jego wyłączania). Obudowa musi posiadać minimum 8 zatok dyskowych HotPlug.
Procesory	Dwa procesory maksymalnie 16 rdzeniowe, x86 - 64 bity, wynik wydajności procesorów zainstalowanych w oferowanym serwerze nie powinien być niższy niż 265 punktów w teście SPECrate®2017_int_base, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej oferowanego serwera (wydruk testu załączony do oferty).
Płyta główna	Dedykowana do pracy w serwerach, zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym umożliwiająca instalację dwóch procesorów, posiadająca minimum 32 sloty na pamięć operacyjną.
Pamięć operacyjna	Zainstalowane minimum 256 GB pamięci RAM typu DDR5 Registered, min. 5600MT/s w modułach o pojemności min. 32 GB. Obsługa zabezpieczeń: korekcja błędów pamięci lub równoważne.
Sloty rozszerzeń	Serwer musi posiadać minimum 3 gniazda PCI-Express generacji 5 x16 Serwer musi posiadać minimum 2 gniazda OCP
Dyski twarde	Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS i SSD, NVMe. Zainstalowane 2 dyski min. 480GB SSD MU HotPlug, 2,5”.
Kontroler	Serwer musi być wyposażony w kontroler RAID wspierający poziomy RAID: 0/1/5/6/10/50/60, zawierający 4GB pamięci cache wraz z modułem bateryjnym. Kontroler musi obsługiwać dyski min. 6G SATA, 12G SAS, 16G NVMe. Zaoferowany kontroler RAID nie może zajmować dostępnych slotów PCI-Express.
Interfejsy sieciowe	Karta LAN, nie zajmująca żadnego z dostępnych slotów PCIe posiadająca minimum 2 porty Ethernet 10Gb SFP+ wraz z wkładkami Karta Fibre Channel posiadająca minimum 2 porty FC 32Gb/s, do karty należy dostarczyć wkładki SFP+ 16Gb/s.
Karta graficzna	Zintegrowana karta graficzna 1920 x 1200 @ 60 Hz (32 bpp) z 16 MB Video Memory

Porty	Min. 2 porty USB 2.0 w tym min. jeden wewnątrz obudowy; min. 4 porty USB 3.2 w tym min. jeden wewnątrz obudowy; min. 1 port DP z przodu obudowy oraz min. 1 port VGA - z tyłu obudowy. Liczba dostępnych złącz USB, DP i VGA nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera. Wymaganie minimalnej ilości portów USB dotyczy portów, które można wykorzystać w systemie operacyjnym zainstalowanym na serwerze do podłączania urządzeń zewnętrznych (np. klucz sprzętowy, napędy itp.) i wyklucza porty USB dedykowane do zarządzania serwerem (IPMI).
Zasilanie	Min. 2 redundantne zasilacze (1+1) typu HotPlug o mocy większej niż 750W i mniejszej od 900W klasy Titanium każdy wraz z kablami zasilającymi o długości min. 2m.
Bezpieczeństwo	Panel informacyjny umieszczony na obudowie serwera lub ramce zabezpieczającej, informujący minimum: • o stanie procesorów, modułów pamięci, zasilaczy, temperaturze. Zintegrowany z płytą główną moduł TPM 2.0. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące o numerze seryjnym • Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
Karta/moduł zarządzający	Karta niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów i stanu serwera: temperatura, stan zasilaczy, prędkość obrotowa wentylatorów, procesory, pamięć RAM, kontrolery RAID i dyski (fizyczne i logiczne), karty rozszerzeń; • wsparcie dla agentów zarządzających oraz/lub możliwość pracy w trybie bez agentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP; • dostęp do karty zarządzającej poprzez: dedykowany port RJ45 z tyłu serwera z poziomu przeglądarki webowej (GUI), wsparcie dla HTML 5 i z poziomu linii komend i poprzez interfejs IPMI 2.0 (Inteligent Platform Management Interface); • możliwość obsługi karty zarządzającej przez co najmniej dwóch administratorów jednocześnie; • możliwość konfiguracji wysłania powiadomień poprzez wiadomość e-mail do administratora o awariach lub istotnych zdarzeniach systemowych;

	• wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów; • możliwość monitorowania zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji osobno dla systemu i dla procesora graficznego; • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping); • zdalna aktualizacja oprogramowania (firmware); • wsparcie dla Microsoft Active Directory; • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API; • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP). Licencja na zarządzanie musi obejmować cały okres życia urządzenia.
Wsparcie dla systemów operacyjnych	Serwer zapewnia wsparcie co najmniej poniższych systemów: • Vmware vSphere 7 i wyższe • Microsoft Windows Server 2019 i wyższe • Red Hat Enterprise Linux (RHEL) 8 i wyższe
Oprogramowanie	Licencja Windows Server 2022 Standard obejmująca zaproponowaną liczbę rdzeni procesorów lub równoważna. Wymagania: Pełna wersja produktu, licencja na oprogramowanie nie może posiadać ograniczeń czasowych oraz funkcjonalnych (bezterminowa / dożywotnia licencja na użytkowanie), niedopuszczalne jest dostarczenie w wersji typu alpha, beta, Community Preview (CP), refurbished, trial, testowej, z ograniczeniem czasowym, edukacyjnej, oświatowej, lub innej, która zabrania używania oprogramowania przez placówkę samorządową. Dostarczone ze sprzętem licencje muszą być nowe i pochodzić z legalnego kanału dystrybucji na terenie kraju. Zamawiający ma prawo do weryfikacji źródła pochodzenia licencji u przedstawiciela producenta oprogramowania na terenie kraju lub bezpośrednio u producenta oprogramowania. W przypadku negatywnej weryfikacji źródła pochodzenia licencji Zamawiający ma prawo do odstąpienia od umowy i naliczenia kar umownych zgodnie z zapisami umowy. Opis kryteriów równoważności: • Współpraca z procesorami o architekturze x64. • Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. • Możliwość budowania klastrów składających się z 64 węzłów. • Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni. • Praca w roli klienta domeny Microsoft Active Directory.

	• Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2012. • Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. • Możliwość uruchomienia roli klienta i serwera czasu (NTP). • Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. • Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory • Możliwość uruchomienia roli serwera stron WWW. • W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. • W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych. • W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego. • Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: ▪ pozwalają na zmianę rozmiaru w czasie pracy systemu, ▪ umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, ▪ umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, ▪ umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET

	• Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Możliwość wykorzystania standardu http/2. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Dostępne dwa rodzaje graficznego interfejsu użytkownika: ▪ klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, ▪ dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. • Mechanizmy logowania w oparciu o: ▪ login i hasło, ▪ karty z certyfikatami (smartcard), ▪ wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). • 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. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. • Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). • Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: ▪ Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.

	▪ 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: ▪ Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ▪ Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, ▪ Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. ▪ Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników. • Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ▪ Dystrybucję certyfikatów poprzez http, ▪ Konsolidację CA dla wielu lasów domeny, ▪ Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ▪ Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509 • Szyfrowanie plików i folderów. • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec) • Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi • Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. • Serwis udostępniania stron WWW • Wsparcie dla protokołu IP w wersji 6 (IPv6). • Wsparcie dla algorytmów Suite B (RFC 4869). • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. • Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć

	Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. • Mechanizmy wirtualizacji mające wsparcie dla: ▪ Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ▪ Obsługi ramek typu jumbo frames dla maszyn wirtualnych. ▪ Obsługi 4-KB sektorów dysków, ▪ Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, ▪ Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. ▪ Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) ▪ Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego. • Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów. • Wsparcie dla rozwiązania Kubernetes. • 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. • Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). • Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF • Mechanizm konfiguracji połączenia VPN do platformy Azure. • Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. • Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów. • Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

	• Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Enterprise). W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. W przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.
Gwarancja	24 miesiące gwarancji Warunki szczegółowe: W trybie następnego dnia roboczego od dnia zgłoszenia Uszkodzone dyski pozostają u Zamawiającego. Naprawa musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis. W okresie obowiązywania gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. Wymagana jest możliwość sprawdzenia gwarancji na stronie producenta poprzez wpisanie numeru seryjnego urządzenia. Zgłoszenia awarii muszą odbywać się poprzez dedykowany portal producenta.

Poz. 2 Macierz dyskowa SAN – 1 szt. (Repozytorium danych klastra, logów i bezpiecznej przestrzeni użytkowników)

Komponent	Wymagane parametry i właściwości
Obudowa	Obudowa maksymalnie 2U z możliwością montażu w szafie rack wraz z zestawem do montażu w szafie rack
Przestrzeń dyskowa	Macierz musi być wyposażona w minimum 10 dysków SSD o pojemności 1,92TB każdy, z możliwością rozbudowy do 24 dysków bez dodatkowych półek dyskowych.

Obsługa dysków i sposób zabezpieczania danych	Macierz musi obsługiwać dyski SSD, SAS i NL SAS. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. Komunikacja z dyskami 12Gb SAS. Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków. Konfiguracja takiej grupy RAID musi umożliwiać zmianę rozmiaru takiej grupy poprzez dodawanie i odejmowanie pojedynczych dysków w trybie online bez konieczności przerywania dostępu do danych.
Kontrolery	Każdy kontroler macierzowy musi być wyposażony w minimum 12GB pamięci Cache, 24 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w technologii FiberChannel. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.
Interfejsy	4 x 16FC z wkładkami dla każdego kontrolera 1 x 12Gb SAS Expansion dla każdego kontrolera 1x 1Gb Ethernet dla każdego kontrolera
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z (DLP). poziomu przeglądarki internetowej. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: • administrator – pełen dostęp, • monitor – możliwość odczytu konfiguracji.
Rozbudowa	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 240 dysków twardych.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w

	trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
Serwis i utrzymanie	Możliwość uaktualniania oprogramowania i wsparcie w rozwiązywaniu problemów przez producenta w okresie 3 lat.
Wyposażenie dodatkowe	Zamawiający wymaga dostarczenia okablowania niezbędnego do prawidłowej pracy urządzenia (kable zasilające, do sieci LAN – min. 5m i SAN – min. 3m, inne).
Kompatybilność	Microsoft Windows® Server®; VMware Vsphere; SUSE® Linux® Enterprise Server (SLES); Red Hat® Enterprise Linux (RHEL); Ubuntu Server Edition LTS; Oracle Linux; Citrix® Hypevisor; HP-UX
Gwarancja	24 miesiące gwarancji Warunki szczegółowe: W trybie następnego dnia roboczego od dnia zgłoszenia Uszkodzone dyski pozostają u Zamawiającego. Naprawa musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis. W okresie obowiązywania gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. Wymagana jest możliwość sprawdzenia gwarancji poprzez ten sam portal producenta, który jest wykorzystywany do sprawdzania gwarancji zaoferowanego serwera poprzez wpisanie numeru seryjnego urządzenia. Zgłoszenia awarii muszą odbywać się poprzez ten sam portal producenta, który jest wykorzystywany do zgłaszania awarii zaoferowanego serwera.

Poz. 3 Urządzenie do archiwizacji kopii zapasowych - 1 szt.

Komponent	Wymagane parametry i właściwości
Obudowa	Obudowa maksymalnie 1U z możliwością montażu w szafie rack wraz z zestawem do montażu w szafie rack
Monitorowanie stanu pracy	Wyświetlacz LCD na froncie i diody informacyjne do wyświetlania komunikatów o stanie urządzenia, błędach itp.
Interfejsy komunikacyjne	USB, RJ45
Napędy	1x LTO-8 FC 8Gb
Sloty na taśmy	Minimum 8 Musi umożliwiać wymianę taśm bez wyłączania urządzenia, minimalnie 1.

Maksymalny pobór energii	80W
Niezawodność MTBF (godz)/MSFB(cykle)	min. 100 000 / 2 000 000
Współpraca z oprogramowaniem	Biblioteka wspierać oprogramowanie kopii zapasowych min.: • Arcserve Backup • Archiware P5 • BridgeHead HDM Suite • Commvault • Dell EMC NetWorker • HPE DMF • Veeam Backup • Veritas Backup Exec / NetBackup • YoYotta Automation • IBM Spectrum Protect (TSM) • Micro Focus Data Protector
Zarządzanie	Urządzenie musi udostępniać możliwość zarządzania za pomocą interfejsu WEB i obejmować min.: • uzyskanie informacji o stanie napędu jak i całego urządzenia • raportowanie błędów i stanu • obsługę dziennika błędów systemowych • możliwość przesyłania oprogramowania firmware urządzenia praz napędu LTO • wykonywanie testów diagnostycznych oraz generowanie informacji z nich • wsparcie dla taśmy czyszczącej • konfigurację bezpieczeństwa z kontrolą dostępu • obsługę protokołu SNMP • zarządzanie taśmami w celach organizacyjnych oraz konserwacyjnych
Wymagania dodatkowe	Czytnik kodów kreskowych, z możliwością automatycznej inwentaryzacji taśm. Wraz z biblioteką należy dostarczyć min. 8 szt. taśm LTO-8 RW i min. 1 szt. taśmy czyszczącej.
Dodatkowe oprogramowanie analityczne	Oferowane urządzenie musi być wyposażone w oprogramowanie producenta zaoferowanego sprzętu umożliwiające automatyczne i predykcyjne monitorowanie stanu taśm i napędów LTO oraz oprogramowanie umożliwiające analizę wydajności, utylizację stanu napędów taśmowych i nośników. Dodatkowo oprogramowanie musi umożliwiać monitorowanie oraz zarządzanie wieloma bibliotekami z poziomu jednej konsoli. Jeśli funkcjonalność taka wymaga dodatkowej licencji to nie jest ona wymagana w momencie składania oferty.
Gwarancja	24 miesiące gwarancji

	Warunki szczegółowe: W trybie następnego dnia roboczego od dnia zgłoszenia Naprawa musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis. W okresie obowiązywania gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. Wymagana jest możliwość sprawdzenia gwarancji poprzez ten sam portal producenta, który jest wykorzystywany do sprawdzania gwarancji zaoferowanego serwera poprzez wpisanie numeru seryjnego urządzenia. Zgłoszenia awarii muszą odbywać się poprzez ten sam portal producenta, który jest wykorzystywany do zgłaszania awarii zaoferowanego serwera.

Poz. 4 Zakup licencji dostępowych

Komponent	Wymagane parametry i właściwości
55 CAL User Windows Serwer 2022 lub równoważne	• licencja dostępowa przypisana na użytkownika, • dostęp do serwera przez użytkownika w celu korzystania z usług, takich jak przechowywanie plików lub drukowanie, niezależnie od liczby urządzeń, z których korzysta użytkownik w celu uzyskania dostępu

Poz. 5 Router z funkcjonalnością NGFW/UTM

Komponent	Wymagane parametry i właściwości
Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania

	co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. - System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Porty komunikacyjne	System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45, w tym: • 2x RJ45 1GbE port WAN • 1x RJ45 1GbE port DMZ • 2x RJ45 1GbE port typu FortiLink • 5x RJ45 1GbE porty typu Internal Port System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż: 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.

	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. • Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. • Analiza ruchu szyfrowanego protokołem TLS 1.3, TLS 1.2 - Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hash'e złośliwych plików. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS) • Microsoft Azure • Google Cloud Platform (GCP) • OpenStack • VMware NSX
Połączenia VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

	• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączą WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu
Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, rar. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

	System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

	Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. Urządzenie musi mieć możliwość integracji z FortiAuthenticator VM oraz być w pełni z nim zgodne.
Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

	Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
Dodatkowe elementy	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and Sandbox Cloud Service), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
Gwarancja	24 miesięcy gwarancji Warunki szczegółowe: Gwarancja musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis. Gwarancja producenta na dostarczone urządzenie polega na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W okresie obowiązywania gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania.

Poz. 6 Przełącznik LAN – 1szt.

Komponent	Wymagane parametry i właściwości
Obudowa	Obudowa maksymalnie 1U do montażu w szafie rack z zestawem do montażu w szafie rack
Porty	minimum: 16 portów SFP+ 10GbE wraz z wkładkami, 1 porty konsolowy Micro-USB, 1 port GE management
Przepustowość	238 Mpps
Zdolność przełączania	320 Gbps
Wielkość tablicy MAC adresów	32000
Bufor Pakietów	24 Mb
Ramki jumbo	9 KB
Funkcje zawansowane	Automatyczne wykrywanie urządzeń Konfiguracje grupowe Grupowe aktualizacje oprogramowania Inteligentne monitorowanie stanu sieci Ostrzeżenia o nietypowych zdarzeniach Ujednolicony proces konfiguracji Harmonogram restartu Wiązanie adresów IP, MAC i portów - 512 wpisów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4: 100 wpisów Wiązanie adresów IPv6, MAC i portów - 512 wpisów - DHCPv6 Snooping - Wykrywanie ND - Ochrona źródłowego adresu IPv6: 100 wpisów Ochrona przed atakami DoS Ochrona portów poprzez ich statyczną/dynamiczną konfigurację - Do 64 adresów MAC na port Storm Control Broadcast/Multicast/Unicast - tryb kontroli (kb/s/wskaźnik) Uwierzytelnianie 802.1X - Uwierzytelnianie w oparciu o port - Uwierzytelnianie w oparciu o adres MAC

	- Przydzielanie VLAN - MAB - Sieć VLAN dla gości - Uwierzytelnianie i autoryzowanie poprzez Radius AAA (w tym TACACS+) Izolacja portów Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2 Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2 Kontrola dostępu w oparciu o IP/port/MAC
Standardy i protokoły	IEEE 802.3 ad IEEE 802.1 d IEEE 802.1 p IEEE 802.1 s IEEE 802.1 w IEEE 802.1 x
Zasilacz	Wbudowane zasilanie.
Gwarancja	24 miesięcy gwarancji Warunki szczegółowe: Gwarancja musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis. Gwarancja producenta na dostarczone urządzenie polega na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W okresie obowiązywania gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania.

Poz. 7 Doposażenie istniejącego serwera Dell R450 o kartę FC 16GB - 1szt

Komponent	Wymagane parametry i właściwości
Interfejsy	Dwa porty SFP+ 16 Gbps
Funkcjonalność	• Forward error correction • Link cable beaconing • D-Port Diagnostics • Fabric Device Management Interface • Read Diagnostic Parameters
Obsługiwane prędkości	16 Gbps / 8 Gbps / 4 Gbps
Złączne	PCI Express 3.0 x8

Kompatybilność	Karty muszą być kompatybilne z obecnie posiadanym serwerem
Dodatkowe wymagania	Razem z kartą należy dostarczyć dwie wkładki SFP+ 16 Gbps.
Gwarancja	24 miesiące gwarancji Warunki szczegółowe: Gwarancja musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis.

Poz. 8 Doposażenie istniejącego serwera Dell R250 o kartę FC 16GB - 1szt

Komponent	Wymagane parametry i właściwości
Interfejsy	Jeden port SFP+ 16 Gbps
Funkcjonalność	• Forward error correction • Link cable beaconing • D-Port Diagnostics • Fabric Device Management Interface • Read Diagnostic Parameters
Obsługiwane prędkości	16 Gbps / 8 Gbps / 4 Gbps
Złączne	PCI Express 3.0 x8
Kompatybilność	Karty muszą być kompatybilne z obecnie posiadanym serwerem
Dodatkowe wymagania	Razem z kartą należy dostarczyć dwie wkładki SFP+ 16 Gbps.
Gwarancja	24 miesiące gwarancji Warunki szczegółowe: Gwarancja musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis.

Poz. 9. Usługi konieczne do wykonania, związane z dostarczonym sprzętem – wdrożenie

Usługi związane z dostarczeniem sprzętu polegają na stworzeniu cyberbezpiecznego środowiska minimalizującego ryzyko utraty lub przestojów dostępności do danych w przypadku cyberataku lub awarii, utworzenie mechanizmów uwierzytelniania i kontroli dostępu, dzięki klastrowi wysokiej dostępności oraz opracowaniu strategii odzyskiwania danych i przywrócenia działania systemów.
Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego dokumentację, która składa się z niżej wymienionych zakresów:
   - Analizy Przedwdrożeniowej

- Planu Wdrożenia
- Dokumentacji Powykonawczej

2. Powyższa dokumentacja będzie zawierać bazowe zapisy opisujące budowane rozwiązanie, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone poszczególne etapy realizowane w ramach Przedmiotu zamówienia. Dokumenty te wraz ze Specyfikacją Warunków Zamówienia wraz z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja planu wdrożenia warunkuje rozpoczęcie prac Wykonawcy.
4. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.

Analiza Przedwdrożeniowa

1. Analiza przedwdrożeniowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeniowej Wykonawca przedstawi Zamawiającemu plan wdrożenia, na podstawie, którego będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. Analiza Przedwdrożeniowa będzie podlegała uzgodnieniu z Zamawiającym.

Plan wdrożenia

Zawartość planu wdrożenia:

- Sposób dostawy sprzętu i oprogramowania do miejsca wskazanego przez Zamawiającego
- Opis instalacji i wdrożenia dostarczanego sprzętu wraz z reorganizacją infrastruktury sieciowej
- Wykaz niezbędnych prac konfiguracyjnych

Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta powinna zawierać:

– Opis architektury technicznej:
  - wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych i systemowych występujących i wymaganych do poprawnej pracy
  - konfiguracja musi obejmować wszystkie urządzenia wdrożone, zainstalowane w ramach budowy infrastruktury
– Zestaw danych konfiguracyjnych

Zestaw wymaganych danych konfiguracyjnych musi obejmować:

- serwer – parametry sprzętowe (procesor, pamięć, dyski, karty sieciowe, zasilanie, itp.)
- sieć (adresacja IP, itp.)
- podsystem dyskowy (punkty montowania/litery dysków, wolumeny logiczne, grupy wolumenowe, zasoby dyskowe, RAID, itp.)
- system operacyjny (parametry systemu)
- listę zainstalowanego oprogramowania

  - macierz – parametry sprzętowe (cache, półki dyskowe, dyski, karty/porty fibre channel), grupy dyskowe, zasoby dyskowe, replikacja
  - infrastrukturę sieciową– parametry sprzętowe (porty fibre channel, aktywne licencje)
- Mapa i opis Interface'ów
  - interfejsy muszą zawierać szczegółowy opis techniczny, w szczególności zawierać informację o: typie interfejsu, przeznaczenie portu
- Dokumentacja administracyjna związana z poprawną eksploatacją
  - opis wszystkich rutynowych czynności administracyjnych dla infrastruktury (dziennych, tygodniowych, miesięcznych) oraz działań pozwalających na utrzymanie wymaganej dostępności, wydajności i bezpieczeństwa

Zakres prac związanych z realizacją zadania (wdrożenie) musi obejmować:

1. Wykonawca dostarczy na swój koszt i ryzyko Przedmiot Zamówienia bezpośrednio do lokalizacji wskazanej przez Zamawiającego.
2. Dostarczenie Przedmiotu Zamówienia obejmuje: transport bezpośrednio do Zamawiającego, koszty załadunku oraz rozładunku i wniesienia do pomieszczeń Zamawiającego w miejscu przez niego wskazanym.
3. Reorganizację szaf rack w serwerowni Zamawiającego.
   - Uporządkowanie urządzeń w szafie rack wskazanych przez Zamawiającego.
   - Przeniesienie urządzeń w szafie rack między Rack Unit w celu optymalizacji miejsca oraz połączeń.
   - Uporządkowanie kabli sieciowych, kabli zasilających zapewniając odpowiednie ich zabezpieczenie.
   - Proces reorganizacji nie może mieć wpływu na działanie infrastruktury Zamawiającego w godzinach pracy.
4. Instalację dostarczonych urządzeń w szafie rack w miejscu wskazanym przez Zamawiającego:
   - Montaż serwera kopii zapasowej i zarządzania dostępem
   - Montaż macierzy dyskowej
   - Montaż przełącznika sieciowego LAN
   - Montaż routera z funkcjonalnością NGFW/UTM
   - Montaż urządzenia archiwizującego
   - Rozbudowa posiadanych przez Zamawiającego serwerów o karty FC HBA
   - Rozbudowa posiadanego przez Zamawiającego serwera o pamięci RAM
5. Wykonanie połączeń elektrycznych do zainstalowanych urządzeń w sposób umożliwiający redundancję połączeń.
6. Wykonanie testów zasilania zainstalowanych urządzeń z uwzględnieniem zasilacza awaryjnego UPS posiadanego przez Zamawiającego. Sprawdzenie redundancji zasilania poszczególnych urządzeń wdrażanej infrastruktury poprzez zdjęcie zasilania z jednego z redundantnych zasilaczy.
7. Wykonanie połączeń logicznych do zainstalowanych urządzeń.
8. Opracowanie wspólnie z Zamawiającym schematów adresacji dla poszczególnych podsieci, zaprojektowanie i ustalenie zakresów podsieci poprzez ustawienie odpowiednich parametrów na potrzeby zwiększenia bezpieczeństwa poprzez separację odpowiednich segmentów sieci.
9. Rekonfigurację posiadanych przez Zamawiającego urządzeń sieciowych do których podłączone będą serwer oraz urządzenie do archiwizacji, w sposób umożliwiający

skonfigurowanie zabezpieczonego środowiska wysokiej dostępności w najbardziej wydajny transfer danych i zapewniający bezpieczną pracę środowiska.

10. Rekonfiguracja urządzeń sieciowych LAN Zamawiającego zgodnie z jego zaleceniami i założeniami:
    - Ustawienie kont oraz uprawnień zgodnie z założeniami Zamawiającego
    - Utworzenie separacji sieci
    - Odseparowanie ruchu sieciowego przeznaczonego dla użytkowników mający na celu zwiększenie bezpieczeństwa transferu danych między serwerami
    - Wydzielenie w ustaleniu z Zamawiającym osobnej podsieci dla interfejsów zarządzających dostarczonych urządzeń
11. Konfiguracja interfejsów zarządzających zainstalowanych urządzeń zgodnie z ustaleniami Zamawiającego.
12. Wykonanie aktualizacji oprogramowania układowego dla dostarczanych urządzeń do najnowszej stabilnej wersji w celu uniknięcia luk i podatności CVE.
13. Konfiguracja dostarczonego serwera:
    - Konfiguracja kont administracyjnych i monitoringu
    - Konfiguracja zdalnego zarządzania
    - Konfiguracja interfejsów serwerów w sposób umożliwiający najbardziej wydajny transfer danych
14. Konfiguracja macierzy dyskowej
    - Konfiguracja kont administracyjnych i monitoringu
    - Konfiguracja zdalnego zarządzania
    - Konfiguracja interfejsów macierzy w sposób umożliwiający najbardziej wydajny transfer danych
    - Konfiguracja parametrów macierzy dla kart Fibre Channel
    - Utworzenie wolumenów logicznych zgodnie z wymaganiami budowanego tworzonego bezpiecznego redundantnego środowiska Zamawiającego
    - Konfiguracja dodatkowej ochrony wolumenów opartej na przestrzeni “spare”
    - Konfiguracja LUN oraz ustawienie udostępnień wolumenów dla serwerów
    - Konfiguracja wielościeżkowych połączeń do macierzy gwarantująca bezpieczną i redundantną komunikację wolumenów logicznych przez wszystkie kontrolery
15. Konfiguracja urządzenia archiwizującego
    - Ustawienie kont administracyjnych oraz uprawnień zgodnie z założeniami Zamawiającego
    - Wykonanie inwentaryzacji
    - Utworzenie użytkowej puli kaset
    - Zadeklarowanie slotu i ustawienie automatycznego użycia kasety czyszczącej
16. Instalacja systemu operacyjnego na serwerze.
17. Konfiguracja systemu operacyjnego zgodnie z założeniami Zamawiającego tworząc bezpieczne środowisko systemowe odporne na zewnętrzną ingerencję z uwzględnieniem kontroli dostępu użytkowników, konfiguracji sieciowej i sprzętowej wykorzystując połączenia wielościeżkowe (multipathing) do macierzy, zapewniające ciągłość dostępu do danych w przypadku awarii.
18. Utworzenie, instalacja i konfiguracja w ramach dostarczonego sprzętu oraz sprzętu będącego w posiadaniu Zamawiającego cyberbezpiecznego środowiska minimalizującego ryzyko utraty lub przestoju dostępu do danych (cyberbezpiecznego klastra wysokiej dostępności). Dla

utworzonego rozwiązania Wykonawca przeszkoli przyszłych administratorów w zakresie konfiguracji, obsługi i usuwania potencjalnych problemów.

19. Migracja istniejących systemów do maszyn wirtualnych klastra. Proces migracji nie może mieć wpływu na działanie infrastruktury Zamawiającego w godzinach pracy Zamawiającego.
20. Wykonanie testów funkcjonalnych działania klastra, zawierających schemat utrzymania bezpieczeństwa i integracji danych w przypadku awarii któregokolwiek z komponentów klastra. Symulacja awarii jednego “node” klastra, symulacja awarii jednego z połączeń sieciowych.
21. Rekonfiguracja systemu kopii zapasowych w oparciu o oprogramowanie posiadane przez Zamawiającego.

Rekonfiguracja musi obejmować m. in.:

- Utworzenie repozytorium kopii zapasowych
- Konfigurację zadań kopii zapasowych wg. harmonogramu uzgodnionego z Zamawiającym
- Konfigurację archiwizacji tworzonych kopii na dostarczone urządzenie do archiwizacji
- Backupem i archiwizacją należy objąć nowe środowisko wraz ze znajdującymi się na nim maszynami wirtualnymi
- Wykonanie kopii zapasowych oraz ich archiwizacji dla wybranych maszyn wirtualnych

22. Konfiguracja usługi Active Directory opierając się na dostarczonych do serwerów systemach operacyjnych musi obejmować min.:
    - Zaimplementowanie struktury katalogowej
    - Opracowanie i wdrożenie struktury Zasad Grup Zabezpieczeń
    - Automatyzacja aktualizacji Zasad Grupy dla poszczególnych stacji roboczych
    - Konfiguracja środowiska zdefiniowanych grup użytkowników za pomocą zasad grupy
    - Przypisanie kont użytkowników do odpowiednich grup zabezpieczeń
    - Konfiguracja praw dostępu do zasobów sieciowych
    - Wykonanie ograniczeń na katalogach oraz powiadomień o zajętości
    - Konfiguracja polityki bezpiecznych haseł wraz z powiadomieniami o ich wygasaniu
    - Przeniesienie profili użytkowników i ich danych
    - Przygotowanie procedury podłączenia stacji roboczych do domeny
    - Konfiguracja usługi DNS i innych niezbędnych usług sieciowych
    - Opracowanie i konfiguracja skryptów logowania użytkowników uwzględniających ustalone dostępy do zasobów i oprogramowania
    - Konfiguracja kopii zapasowych i odzyskiwania Active Directory Domain Services
    - Konfiguracja polityk aktualizacji systemu operacyjnego

23. Konfiguracja możliwości zdalnej pracy dla użytkowników pracujących poza siedzibą Zamawiającego zapewniającą bezpieczny, monitorowany dostęp do zasobów Zamawiającego. Konfiguracja oparta o bezpieczny Tunel VPN umożliwiający dostęp do zasobów, realizowana na urządzeniu brzegowym w oparciu o protokoły SSLVPN. Konfiguracja musi zapewniać możliwość monitorowania połączeń VPN oraz historię logowań użytkowników. Dostęp do zasobów musi być realizowany za pomocą połączeń szyfrowanych, pozwalający na dostęp tylko do zasobów przypisanych dla konkretnego użytkownika/grup użytkowników.