Opis przedmiotu Zamówienia

Opis techniczny środowiska sprzętowo programowego na potrzeby budowy laboratorium CyberSecLab.

Spis treści

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest **dostawa, instalacja i uruchomienie środowiska Laboratorium Analiz Ataków Cybernetycznych CyberSecLab**, zwanego dalej „Środowiskiem CyberSecLab" albo „CyberSecLab", wraz z techniczną infrastrukturą towarzyszącą, niezbędną do jego prawidłowego funkcjonowania obejmującą infrastrukturę zabezpieczeń, analizy, sieciową, serwerową oraz składowania danych.

Niniejsza specyfikacja nie podlega interpretacji. **Parametry zamawianych urządzeń oraz oprogramowania środowiska CyberSecLab zostały tak dobrane, aby można było w nim realizować specyficzne i niszowe zadania wynikające z przeznaczenia Laboratorium**. Jeśli zapisy specyfikacji są zdaniem Wykonawcy niejasne, niepełne, nieprecyzyjne lub niewłaściwe, to Wykonawca ma obowiązek zadać pytanie przed złożeniem oferty.

Wykonawca ma także możliwość przeprowadzenia wizji lokalnej w miejscu instalacji środowiska CyberSecLab: Wojskowy Instytut Łączności, ul. Warszawska 22A, 05-130 Zegrze Południowe po wcześniejszym ustaleniu terminu wizji.

2. CHARAKTERYSTYKA MIEJSCA INSTALACJI

2.1. Miejsce instalacji

Środowisko CyberSecLab wraz z niezbędną techniczną infrastrukturą towarzyszącą musi być dostarczone, zainstalowane i uruchomione w budynku Zamawiającego, zlokalizowanym w Zegrzu południowym przy ulicy Warszawskiej 22A.

Miejscem instalacji środowiska CyberSecLab oraz części infrastruktury towarzyszącej będzie serwerownia CyberSecLab:

- Na potrzeby instalacji serwerów obliczeniowych środowiska CyberSecLab zostaną przygotowane 4 szafy teleinformatyczne zabudowane w technologii zimnego korytarza oraz 1 szafę telekomunikacyjną.
- Na potrzeby instalacji serwerów usługowych środowiska CyberSecLab Zamawiający przygotuje szafę teleinformatyczną w serwerowni CyberSecLab.

2.2. Zasilanie

W budynku przeznaczonym do instalacji środowiska CyberSecLab dostępna będzie infrastruktura zasilania gwarantowanego, zabezpieczona urządzeniami UPS oraz dedykowanym agregatem prądotwórczym.

Instalacja elektryczna dystrybuująca zasilanie do poszczególnych szaf w serwerowni CyberSecLab jest wykonana w oparciu o 36 gniazd C13 oraz 12 gniazd C20 dla toru zasilania A, oraz 36 gniazd C13 oraz 12 gniazd C10 dla toru zasilania B.

2.3. Podłoga techniczna

Serwerownia CyberSecLab wyposażona jest w techniczną podłogę podniesioną o następujących parametrach technicznych:

- Wysokość podniesienia : około 54 cm do poziomu podłogi korytarza doprowadzającego do serwerowni CyberSecLab.
- Dopuszczalne obciążenie punktowe: maksimum 3,0 kN
- Dopuszczalne obciążenie powierzchniowe: maksimum 15 kN/m2

3. OPIS ŚRODOWISKA CYBERSECLAB

3.1. Parametry ogólne

Jeżeli zrealizowanie funkcjonalności opisanych przez Zamawiającego wymaga zakupu dodatkowych licencji oprogramowania, należy licencje te dostarczyć, chyba że Zamawiający wprost specyfikuje brak takiej konieczności.

Cały dostarczony sprzęt musi być fabrycznie nowy, tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów jego poprawnej pracy.

Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych.

Jeśli Zamawiający określa w niniejszej specyfikacji, że dany element ma posiadać określone cechy, to ten element ma efektywnie pracować z tymi cechami w instalowanej konfiguracji. Przykładowo, jeśli wymaga się dostarczenia modułów pamięci pracujących z prędkością 2133 MHz, to te moduły muszą efektywnie pracować z taką prędkością, a nie mieć tylko taką teoretyczną możliwość w konfiguracji innej niż dostarczana.

Zamawiający określa w tej specyfikacji cechy minimalne. Wykonawca może dostarczyć komponenty o cechach lepszych, pod warunkiem zachowania pełnej kompatybilności.

Wszystkie dostarczane elementy środowiska CyberSecLab będą pracować w trybie ciągłym: przez 24 godziny na dobę, 365 dni w roku i muszą zapewniać wydajną, stabilną i nieprzerwaną pracę pod maksymalnym obciążeniem wszystkich podzespołów (procesory, pamięć, interfejsy sieciowe itd.).

Opis wymagań dla poszczególnych komponentów sprzętowych podano w Zadaniach:

- Zadanie 1 - dla obszaru zabezpieczeń oraz sieci LAN,
- Zadanie 2 - dla obszaru obliczeń oraz składowania danych,
- Zadanie 3 - dla obszaru usługowego.

Wszystkie dostarczane elementy muszą posiadać najnowszą, stabilną wersję oprogramowania układowego (tzw. firmware).

Nazwy oraz hasła wszystkich kont użytkowników wykorzystywanych do zarządzania wszystkimi urządzeniami, na każdym poziomie, muszą zostać ustawione zgodnie z wytycznymi Zamawiającego przekazanymi na etapie wdrożenia.

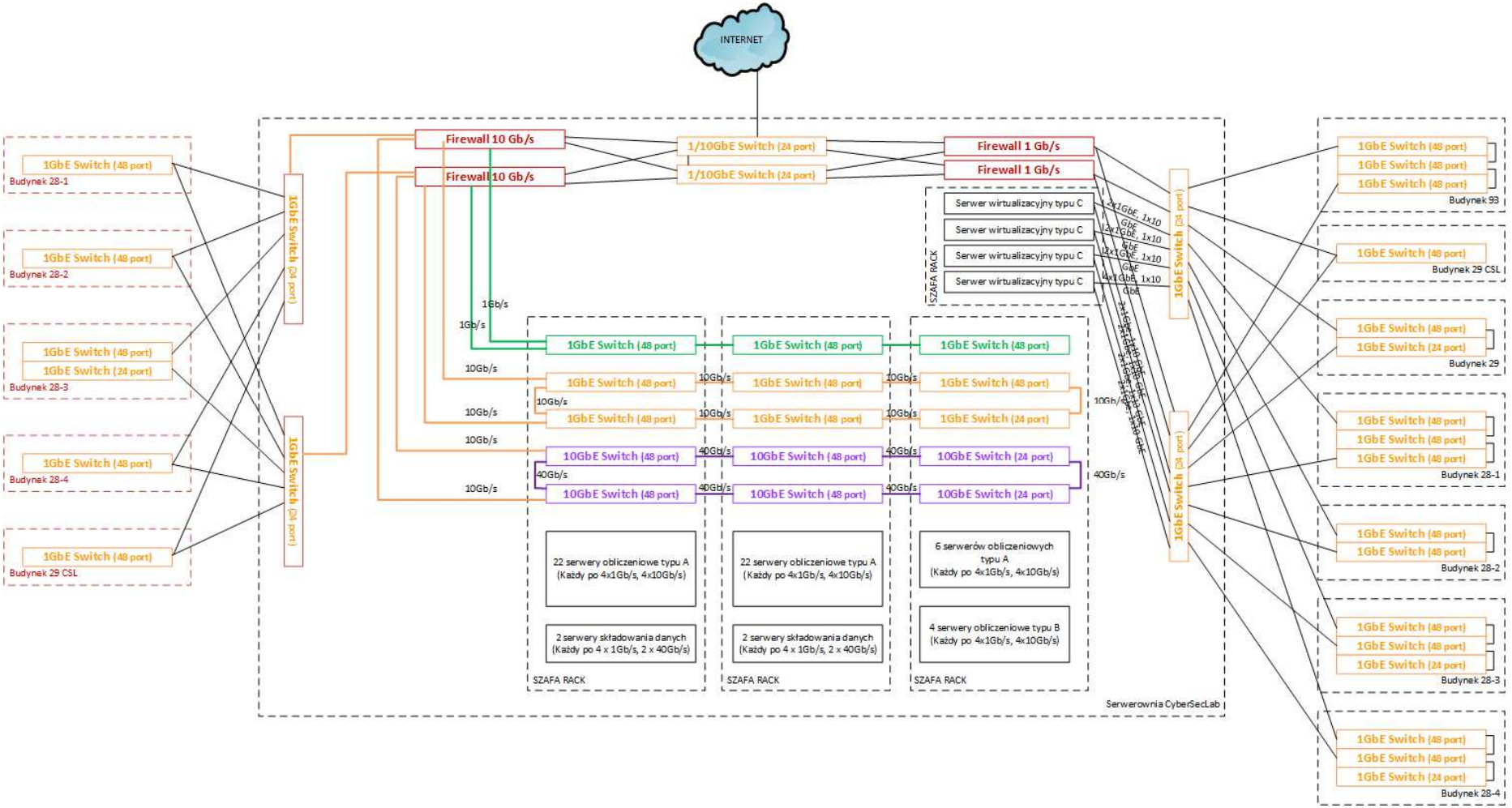
Wszystkie elementy środowiska mają być zainstalowane w serwerowni CyberSecLab i jeśli będzie to konieczne także w innych budynkach WIŁ przez autoryzowanych pracowników Wykonawcy.

Wszystkie kable sieciowe w obrębie przestrzeni przeznaczonej na instalację serwerów obliczeniowych powinny zostać poprowadzone zgodnie z najlepszymi praktykami, wewnątrz szaf rack lub w kanałach kablowych. Ewentualne nadmiary kabli powinny także zostać zebrane i spięte w ww. kanałach kablowych.

Każdy kabel powinien zostać czytelnie opisany na obu końcach za pomocą etykiety odpornej na podmuchy powietrza i podwyższoną temperaturę, zgodnie z wytycznymi Zamawiającego przekazanymi na etapie wdrożenia.

Topologia połączeń, numery VLAN oraz adresy IP wszystkich urządzeń we wszystkich sieciach muszą zostać przydzielone wg ustaleń z Zamawiającym na etapie wdrożenia środowiska CyberSecLab.

Planowane jest połączenie przełączników Ethernet określone w zadaniu 1 w logiczną strukturę zgodną z przedstawioną na poniższym rysunku (Rys. 1), umieszczoną w szafach rack wraz z odpowiadającymi im serwerami obliczeniowymi typu A i B oraz serwerami typu storage.



Rys.1 – Logiczna struktura sieciowa projektu

3.2. Zadanie nr 1

W skład zadania 1 wchodzą następujące komponenty sprzętowe

Urządzenia Firewall (klaster)

Komponent	Minimalne wymagania
Architektura systemu ochrony	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Wysoka dostępność	W przypadku systemu pełniącego funkcje: Firewall, IPSec, kontrola aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive. W ramach postępowania system powinien zostać dostarczony w postaci klastra wysoko dostępnego.
Zasilanie	Redundantne zasilacze. Zasilanie z sieci 230V/50Hz.
Monitoring	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN.
Tryb pracy	System realizujący funkcję Firewall powinien umożliwiać pracę w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
Interfejsy fizyczne	System realizujący funkcję Firewall powinien dysponować minimum 12 gniazdami SFP 1GbE (wyposażone we wkładki 1000BaseSX), 8 gniazdami SFP+ 10GbE z wkładkami 10GbE SFP+ short range, 8 portami GbE RJ45
Interfejsy wirtualne	System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
Wydajność firewall	W zakresie Firewall'a jest obsługa nie mniej niż 12 milionów jednoczesnych połączeń oraz 250 tys. nowych połączeń na sekundę, z przepustowością Firewall'a: nie mniej niż 50 Gbps dla pakietów 512 bajtów.
Wydajność VPN	Wydajność szyfrowania VPN IPSec: nie mniej niż 45 Gbps
Logowanie lub raportowanie	System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze lub producenci poszczególnych elementów systemu muszą oferować systemy logowania i raportowania w postaci odpowiednio zabezpieczonych platform sprzętowych lub programowych
Funkcjonalność systemu	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: •kontrola dostępu - zapora ogniowa klasy Stateful Inspection •poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL

	VPN •ochrona przed atakami - Intrusion Prevention System •kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma •kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P •system powinien rozpoznawać ruch botnet (komunikacja z C&C - może być rozpoznawana z wykorzystaniem różnych modułów) •możliwość analizy ruchu szyfrowanego protokołem SSL •mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) – wykrywanie zdefiniowanego ciągu znaków w przesyłanym strumieniu danych.
Klient VPN	W ramach funkcji IPSec VPN, SSL VPN – dostawca powinien dostarczać klienta VPN dla systemów operacyjnych rodziny Linux i Windows współpracującego z oferowanym rozwiązaniem.
Routing	Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, routing dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP
Wirtualne instancje	Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall, IPSec VPN, IPS.
NAT	Translacja adresów NAT adresu źródłowego i docelowego.
Reguły firewall	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
Strefy bezpieczeństwa	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
Silnik antywirusowy	System musi umożliwiać w przyszłości uruchomienia funkcjonalności o silnik antywirusowy. Powinien umożliwiać też skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
System IPS	Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 4500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.
Kontrola aplikacji	Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
Aktualizacje	Automatyczne aktualizacje sygnatur ataków, aplikacji i w przyszłości szczepionek antywirusowych.
Uwierzytelnienie	System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: •haseł statycznych i definicji użytkowników przechowywanych w lokalnej

	bazie systemu, •haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, •haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory.
Certyfikacje	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: •ICSA lub EAL4 dla funkcji Firewall
Zarządzanie	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 5 lat.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Przełączniki brzegowe (2 szt.)

Komponent	Minimalne wymagania
Ilość portów	• Urządzenie musi posiadać minimum 24 porty 10/100/1000Mbps RJ-45 Base-T. • Urządzenie musi posiadać co najmniej aktywne 8 portów 10GbE SFP+
Parametry wydajnościowe	Wydajność przełączania minimum 200 gigapakietów na sekundę. Wydajność przekazywania pakietów minimum 150 milionów pakietów na sekundę.
Funkcjonalność łączenia w stos	• Możliwość stackowania minimum 8 urządzeń. W przypadku dostarczenia urządzenia modularnego nie ma wymagania co do stackowania minimum 8 urządzeń. Wymagane jest natomiast zapewnienie rozbudowy do minimum 8 x 24 portów 10/100/1000Mbps i 8x 8 portów 10GbE SFP+. W przypadku przełączników modularnych do zapewnienia parametrów rozbudowy możliwe jest wykorzystanie więcej niż jednego

	przełącznika modularnego. • W przypadku urządzenia stackowalnego powinna być możliwość wykorzystania do stackowania modułów 10GbE lub równoważnych zapewniających sumaryczną przepustowość połączenia minimum 40Gbps w trybie full duplex lub połączeń równoważnych zapewniających wymaganą przepustowość między przełącznikami/modułami . • Obsługa trybu automatycznego przełączenia z aktywnego przełącznika master na jeden z pozostałych przełączników w grupie stack bez uruchamianie przełączników ponownie oraz bez utraty pakietów. • Możliwość dodania i usunięcia urządzenia ze stosu bez przerwy w jego działaniu.
Funkcjonalności warstwy L2	• Urządzenie musi obsługiwać min. 16000 adresów MAC oraz min. 4000 sieci VLAN. • Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad (LACP), min. 8 portów na jedno logiczne połączenie, min. 124 logicznych grup połączeń jednocześnie (w stosie). • Wsparcie dla RSTP, 802.1s – Multiple Spanning Tree oraz PVST/PVST+/PVRST • Obsługa do 254 instancji STP • Wsparcie dla 802.1x • Wsparcie dla pakietów tzw. „Jumbo frames” (co najmniej 9000 bajtów) • Obsługa BPDU Guard, Root Guard • Obsługa mechanizmu GVRP • Obsługa IGMP snooping v1, v2 • Obsługa mechanizmu MAC Address Locking, Port Security • Obsługa MLD Snooping (v1/v2) • Obsługa Mirroring - Port-based, ACL-based, MAC Filter-based, and VLAN-based. • Obsługa Port Loop Detection • Obsługa Private VLAN • Obsługa Protocol VLAN (802.1v), Subnet VLAN • Obsługa Uni-Directional Link Detection (UDLD) • Obsługa VLAN Stacking (Q-in-Q)
Funkcjonalności warstwy L3	• Statyczny routing IPv4 i IPv6 • Sprzętowa obsługa min 1000 (IPv4) i 1000 (IPv6) wpisów routingu • Wsparcie mechanizmu ECMP

	• Obsługa protokołu RIPv2 • Obsługa protokołu OSPFv2, OSPFv3 • Obsługa protokołu VRRP, VRRPv3 • Obsługa tuneli IPv6 over IPv4 • Obsługa VRF (IPv4 i IPv6) Jeśli funkcjonalności warstwy L3 wymagają licencji należy ją dostarczyć w ramach zamówienia.
Funkcje QoS	• Obsługa min. 6 kolejek QoS na jednym porcie fizycznym • Zarządzanie polityką jakości ruchu – "QoS" w oparciu o algorytmy Weighted Round Robin (WRR) lub odpowiedni, Strict Priotity (SP) i ich kombinację. • Mapowanie za pomocą ACL do kolejki priorytetowej • Mapowanie do kolejki priorytetowej na podstawie adresu MAC • Limitowanie pasma na wejściu w oparciu o port, ACL • Limitowanie pasma na wyjściu w oparciu o port, kolejkę • Limitowanie pasma dla pakietów BUM (Broadcast, multicast i unknown unicast) • Obsługa DHCP Relay • Obsługa Diffserv oraz 802.1p
Funkcje bezpieczeństwa	• Obsługa zarówno IPv4 ACL jak i IPv6 ACL • Możliwość konfiguracji mirroringu w oparciu o dany port, listy ACL i MAC oraz VLAN • Obsługa Private VLAN • Obsługa DHCP snooping • Obsługa Dynamic ARP inspection • Obsługa Authentication, Authorization, and Accounting • Wsparcie dla Advanced Encryption Standard (AES) i SSHv2 • Obsługa RADIUS/TACACS/TACACS+ • Obsługa Secure Copy (SCP) i Secure Shell (SSHv2) • Obsługa Change of Authorization (CoA) RFC 5176
Zgodność ze standardami	• RFC 783 TFTP • RFC 854 TELNET Client and Server • RFC 951 Bootp • RFC 1157 SNMPv1/v2c • RFC 1213 MIB-II • RFC 1493 Bridge MIB • RFC 1516 Repeater MIB

	• RFC 1573 SNMP MIB II • RFC 1643 Ethernet Interface MIB • RFC 1724 RIP v1/v2 MIB • RFC 1757 RMON MIB • RFC 2068 Embedded HTTP • RFC 2131 DHCP Server and DHCP Relay • RFC 2570 SNMPv3 Intro to Framework • RFC 2571 Architecture for Describing SNMP Framework • RFC 2572 SNMP Message Processing and Dispatching • RFC 2573 SNMPv3 Applications • RFC 2574 SNMPv3 User-based Security Model • RFC 2575 SNMP View-based Access Control Model SNMP • RFC 2818 Embedded HTTPS • RFC 3176 sFlow • 802.1D-2004 MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • 802.1x Port-based Network Access Control • 802.3 10Base-T • 802.3ab 1000Base-T • 802.3ad Link Aggregation (Dynamic and Static) • 802.3ae 10 Gigabit Ethernet • 802.3u 100Base-TX • 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.3az-2010 - EEE • 802.1Q VLAN Tagging
Zarządzanie, zabezpieczenia	• Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (Ethernet RJ-45) • Obsługa SNMP2/SNMP3 oraz uwierzytelnianie poprzez TACACS/Radius • Obsługa przez wbudowany serwer WWW • Obsługa DHCP Server • Obsługa NTP Network Time Protocol

	• Wsparcie dla protokołów OpenFlow v1.0 i v1.3 (SDN) • Obsługa 802.3az-2010 – IEEE
Wymiar	• Obudowa musi być przeznaczona do montażu w szafie rackowej 19”
Zasilanie	• Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej, wymienialne w trakcie pracy urządzenia - hot-swap, redundancja zasilaczy 1+1, możliwość zastosowania dodatkowego zewnętrznego zasilacza. • Chłodzenie musi być realizowane tył/przód, redundantne moduły wentylatorów, wymienialne w trakcie pracy urządzenia.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Ochrona portalu WWW (klaster)

Komponent	Minimalne wymagania
Architektura systemu	System ochrony aplikacji webowych oraz Firewall XML, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System powinien umożliwiać lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. Powinna istnieć możliwość implementacji systemu inline w trybach Reverse Proxy lub Transparentnym, jak również implementacji w trybie nasłuchu. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta. System ochrony musi zostać dostarczony w formie redundantnej w postaci klastra urządzeń.
System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.
Parametry fizyczne systemu	Nie mniej niż 4 porty Ethernet 10/100/1000 Base-T Powierzchnia dyskowa - minimum 1 TB W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive Obudowa urządzenia o wysokości do 1U z możliwością montażu w

	standardowej szafie teletechnicznej 19 cali
Funkcjonalności podstawowe i uzupełniające	System powinien realizować co najmniej poniższe funkcjonalności: • Tryb auto-uczenia – przyspieszający i ułatwiający implementację • Podział obciążenia na kilkanaście serwerów (loadbalancing) • Akceleracje SSL dla wybranych serwisów w centrum danych • Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje) • Firewall XML realizujący z możliwością routingu w oparciu o zawartość, walidację schematów XML • Firewall aplikacji webowych chroniący przed minimum takimi zagrożeniami jak: o SQL and OS Command Injection o Cross Site Scripting (XSS) o Cross Site Request Forgery o Outbound Data Leakage o HTTP Request Smuggling o Buffer Overflow o Encoding Attacks o Cookie Tampering / Poisoning o Session Hijacking o Broken Access Control o Forceful Browsing /Directory Traversal
Parametry wydajnościowe	Urządzenie musi obsługiwać przepustowość dla ruchu http - min. 100 Mbps, min. 10 000 transakcji na sekundę
Sygnatury, subscrypcje	Aktualizacja baz sygnatur powinna być systematycznie aktualizowana zgodnie ze zdefiniowanych harmonogramem
Zarządzanie	System udostępnia: lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS
Gwarancje , subskrypcje	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta. **Wymaga się, aby dostawa zawierała subskrypcję funkcji bezpieczeństwa na okres 60 miesięcy.**
Zasilanie	Zasilanie z sieci 230V/50Hz.

Analiza sieci – TAP

Komponent	Minimalne wymagania
Opis wymagań	1.System musi umożliwiać kopiowanie ruchu full duplex z linków wielomodowych o przepustowości 10Gbps z uwzględnieniem błędów wszystkich warstw. 2.Urządzenie powinno być wyposażone w kolektory LC do kopiowania ruchu ze światłowodu wielomodowy o długości fali 850 nm. 3.Wymagane jest, aby urządzenie było pasywne, czyli na wypadek własnej awarii nie powodowało przerw w pracy sieci. 4.Wymagane jest, aby urządzenie nie wymagało adresu IP. 5.Wymagane jest, aby ilość światła przekierowana na system analizy była nie mniejsza niż 50% (podział 50/50). 6.Urządzenie powinno być dostarczone z wszelkimi uchwytami umożliwiającymi montaż w szafie rackowej.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Analiza Sieci – Agregacja i filtracja

Komponent	Minimalne wymagania
Architektura systemu ochrony	Dostarczony system agregacji ruchu sieciowego musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym i skonfigurowanym systemem operacyjnym.
Interfejsy	System musi dysponować co najmniej: a. 20 gniazdami w standardzie SFP+ pracującymi z prędkością 10Gbps z dostarczonymi 6 szt. wkładek SFP+ jednomodowymi 10GbE SR b. 4 portami w standardzie RJ45, pracującymi z prędkością 1Gbps c. 1 portem w standardzie RJ45, dedykowanym do zarządzania
Zarządzanie ruchem	System musi umożliwiać pełne zarządzanie ruchem oraz definiowane portów wejściowych i wyjściowych (Ingress/Egress port)
Filtrowanie	System musi wspierać funkcję filtrowania przesyłanych pakietów po następujących parametrach: a) Źródłowy i docelowy adres MAC

	b) Źródłowy i docelowy adres IP ver. 4 c) Źródłowy i docelowy adres IP ver. 6 d) Port UDP e) Port TCP f) Tag VLAN g) Zawartość pola TOS w pakiecie IP
Wydajność	Wydajność ruchu obsługiwanego przez system w trybie pełnego filtrowania pakietów musi wynosić min 244Gbps Zmiana parametrów filtrowania podczas pracy systemu nie może mieć wpływu na jego wydajność.
Rozbudowa	System powinien być wyposażony co najmniej w dwa porty 10GbE SFP+ z wkładkami 10GbE SR umożliwiające filtrowania i modyfikacji przesyłanych pakietów, w oparciu o które będzie można realizować co najmniej następujące funkcje: a) Nadawanie znaczników czasowych przesyłanym pakietom, przy wykorzystaniu czasu lokalnego lub pobranego z przy pomocy protokołu NTP z zewnętrznego serwera b) Usuwanie z przesyłanych pakietów nagłówków następujących protokołów: min. GTP, MPLS, VLAN, VNTAG c) Obsługę aktualizacji czasu za pomocą protokołu NTP d) Deduplikację przesyłanych pakietów
Aktualizacja czasu	System musi wspierać aktualizację czasu za pomocą protokołu NTP
Obsługa protokołów	System musi wspierać obsługę następujących protokołów sieciowych a) SMTP v1, v2, v3 b) TACACS+
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Przełączniki sieci transportowej 10Gbps (6 szt.)

Komponent	Minimalne wymagania
Ilość portów	• Urządzenie musi umożliwiać obsadzenie minimum 48 portów 1GbE/10GbE definiowanych za pomocą wkładek SFP+ lub równoważnych. • Urządzenie musi posiadać co najmniej aktywne 4 porty 40GbE QSFP+ • Urządzenie musi obsługiwać wkładki typu 10GbE-SR oraz 10GbE-LR

	lub równoważne. • Urządzenie na wszystkich portach z pośród ww. musi umożliwiać pracę w trybie GigabitEthernet (1GbE) z możliwością instalacji wkładki interfejsowej SFP lub równoważnej. • Urządzenie musi obsługiwać kable typu 10GbE Twinax lub równoważne.
Parametry wydajnościowe	•Wymagane jest opóźnienie przełączania pakietów nie większe niż 4µs przy 10 Gbps. •Wymagana jest prędkość przełączania „wirespeed" dla każdego portu 10GbE przełącznika. •Wymagana jest przepustowość minimum 960 Mpps L2 i L3. •Wymagany jest obsługiwany rozmiar tabeli adresów MAC min. 120000.
Funkcjonalności portów 1/10 GbE	• Urządzenie musi wspierać sprzętowo na portach obsługę protokołów FCoE. Jeśli do uruchomienia powyższej funkcjonalności urządzenie wymaga licencji, dostarczenie licencji w tym przypadku nie jest przedmiotem tego postępowania. • Urządzenie musi obsługiwać sprzętowo protokół FC 2/4/8G. Jeśli do uruchomienia powyższej funkcjonalności urządzenie wymaga licencji, dostarczenie licencji w tym przypadku nie jest przedmiotem tego postępowania.
Obsługiwane standardy FC	• Standardowe typy portów Fibre Channel: E, F, • Wirtualizacja N-port identifier (NPIV), • Serwisy FC: Name server, login services, name-server zoning,
Implementacja zaleceń IEEE – Data Center Bridging	• IEEE związane z Data Center Bridging, • IEEE 802.1Qbb PFC (per-priority pause frame support), • Wsparcie dla DCBX Protocol, • IEEE 802.1Qaz Enhanced Transmission Selection,
Funkcjonalności warstwy L2	• Trunking IEEE 802.1Q VLAN, • Wsparcie dla minimum 4000 sieci VLAN, • IEEE 802.1w lub kompatybilny, • Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): min. 30 instancji, • Spanning Tree PortFast lub odpowiadający, • Spanning Tree Root Guard lub odpowiadający, • Internet Group Management Protocol (IGMP) Version 2, • Link Aggregation Control Protocol (LACP): IEEE 802.3ad, • Ramki Jumbo dla wszystkich portów (minimum 9000 bajtów), • Ramki Pause (IEEE 802.3x), • Sprzętowe wsparcie dla mechanizmu Trill lub Fabricpath lub

	odpowiadającej. Mechanizm ten ma umożliwić przełączanie pakietów pomiędzy przełącznikami pracującymi w architekturze ethernet fabric jednocześnie na wszystkich ścieżkach bez użycia spaning tree. • Musi istnieć możliwość podłączenia hosta zewnętrznego do dwóch różnych przełączników w chmurze przy użyciu standardowego protokołu LACP. • Wsparcie dla RSPAN.
Funkcjonalności warstwy L3	• Sprzętowe przełączanie pakietów w warstwie L3, • Routing w oparciu o trasy statyczne, • Obsługa minimum 8000 prefixów, • Wybór do 8-miu jednoczesnych ścieżek o równej metryce (ECMP), • Minimum 500 wejściowych lub wyjściowych wpisów dla ACL, • Obsługa protokołów routingu: Routing Statyczny, Open Shortest Path First Version 2 (OSPFv2), OSPFv3 Border Gateway Protocol v4 (BGPv4) • Obsługa Hot-Standby Router Protocol (HSRP) lub Virtual Router Redundancy Protocol (VRRP) lub mechanizmów odpowiadających. • Wsparcie dla protokołu Bidirectional Forwarding Detection (BFD).
Funkcje QoS	• Layer 2 IEEE 802.1p (CoS), • Dedykowana konfiguracja QoS dla każdego portu, • Przypisanie CoS na każdym porcie, • Kolejkowanie na wyjściu w oparciu o CoS, • Bezwzględne (strict-priority) kolejkowanie na wyjściu, • Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający.
Funkcje bezpieczeństwa	• Wejściowe ACL (standardowe oraz rozszerzone), • Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o adresy MAC adresy, • Wsparcie dla In-Service Software Upgrade (ISSU).
Zarządzanie, zabezpieczenia	• Port konsoli CLI, • Zarządzanie In-band, • Dedykowany port Ethernet do zarządzania urządzeniem, • Port USB, • SSHv2, • Authentication, authorization, and accounting (AAA), • RADIUS,

	• Syslog, • SNMP v2, v3, • Remote monitoring (RMON). • Możliwość wykorzystania protokołu NETCONF do zarządzania urządzeniem. • Możliwość zarządzania urządzeniem z wykorzystaniem infrastruktury OpenStack. • Wsparcie dla protokołów OpenFlow v1.3 (SDN).
Wymiar	• Obudowa musi być przeznaczona do montażu w szafie rackowej 19”.
Zasilanie	• Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej. • Chłodzenie musi być realizowane tył/przód.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Przełączniki sieci komunikacyjnej 1Gbps (6 szt.)

Komponent	Minimalne wymagania
Ilość portów	• Urządzenie musi umożliwiać obsadzenie minimum 48 portów 1GbE/10GbE Base-T. **Jeśli do uruchomienia prędkości portów 10Gbps urządzenie wymaga licencji, dostarczenie licencji w tym przypadku nie jest przedmiotem tego postępowania.** • Urządzenie musi posiadać co najmniej aktywne 4 porty 40GbE.
Parametry wydajnościowe	•Wymagane jest opóźnienie przełączania pakietów nie większe niż 4µs przy 10 Gbps – wg specyfikacji producenta w przypadku rozszerzenia możliwości sprzętu. •Wymagana jest prędkość przełączania „wirespeed” dla każdego portu 1GE/10GE przełącznika. •Wymagana jest przepustowość minimum 960 Mpps L2 i L3. •Wymagany jest obsługiwany rozmiar tabeli adresów MAC min. 120000.
Implementacja zaleceń IEEE – Data Center Bridging	• IEEE związane z Data Center Bridging, • IEEE 802.1Qbb PFC (per-priority pause frame support), • Wsparcie dla DCBX Protocol,

	• IEEE 802.1Qaz Enhanced Transmission Selection,
Funkcjonalności warstwy L2	• Trunking IEEE 802.1Q VLAN, • Wsparcie dla minimum 4000 sieci VLAN, • IEEE 802.1w lub kompatybilny, • Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): min. 30 instancji, • Spanning Tree PortFast lub odpowiadający, • Spanning Tree Root Guard lub odpowiadający, • Internet Group Management Protocol (IGMP) Version 2, • Link Aggregation Control Protocol (LACP): IEEE 802.3ad, • obsługa ramek Jumbo dla wszystkich portów (minimum 9000 bajtów), • obsługa ramek Pause (IEEE 802.3x), • Sprzętowe wsparcie dla mechanizmu Trill lub Fabricpath lub odpowiadającej. Mechanizm ten ma umożliwić przełączanie pakietów pomiędzy przełącznikami pracującymi w architekturze ethernet fabric jednocześnie na wszystkich ścieżkach bez użycia spaning tree. • Musi istnieć możliwość podłączenia hosta zewnętrznego do dwóch różnych przełączników w chmurze przy użyciu standardowego protokołu LACP. • Wsparcie dla RSPAN.
Funkcjonalności warstwy L3	• Sprzętowe przełączanie pakietów w warstwie L3, • Routing w oparciu o trasy statyczne, • Obsługa minimum 8000 prefixów, • Wybór do 8-miu jednoczesnych ścieżek o równej metryce (ECMP), • Minimum 500 wejściowych lub wyjściowych wpisów dla ACL, • Obsługa protokołów routingu: Routing Statyczny, Open Shortest Path First Version 2 (OSPFv2), OSPFv3 Border Gateway Protocol v4 (BGPv4) • Obsługa Hot-Standby Router Protocol (HSRP) lub Virtual Router Redundancy Protocol (VRRP) lub mechanizmów odpowiadających. • Wsparcie dla protokołu Bidirectional Forwarding Detection (BFD).
Funkcje QoS	• Layer 2 IEEE 802.1p (CoS), • Dedykowana konfiguracja QoS dla każdego portu, • Przypisanie CoS na każdym porcie, • Kolejkowanie na wyjściu w oparciu o CoS,

	• Bezwzględne (strict-priority) kolejkowanie na wyjściu, • Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający.
Funkcje bezpieczeństwa	• Wejściowe ACL (standardowe oraz rozszerzone), • Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o adresy MAC adresy, • Wsparcie dla In-Service Software Upgrade (ISSU).
Zarządzanie, zabezpieczenia	• Port konsoli CLI, • Zarządzanie In-band, • Dedykowany port Ethernet do zarządzania urządzeniem, • Port USB, • SSHv2, • Authentication, authorization, and accounting, • RADIUS, • Syslog, • SNMP v2, v3, • Remote monitoring (RMON). • Możliwość wykorzystania protokołu NETCONF do zarządzania urządzeniem. • Możliwość zarządzania urządzeniem z wykorzystaniem infrastruktury OpenStack. • Wsparcie dla protokołów OpenFlow v1.3 (SDN).
Wymiar	• Obudowa musi być przeznaczona do montażu w szafie rackowej 19”, wysokość urządzenia nie może przekraczać 1U.
Zasilanie	• Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej. • Chłodzenie musi być realizowane tył/przód.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Przełączniki sieci zarządzającej 1Gbps (3 szt.)

Komponent	Minimalne wymagania
Ilość portów	• Urządzenie musi posiadać minimum 48 portów 10/100/1000Mbps RJ-45 Base-T.

	• Urządzenie musi posiadać co najmniej aktywne 8 porty 10GbE
Parametry wydajnościowe	Wydajność przełączania min. 200 gigapakietów na sekundę. Wydajność przekazywania pakietów min. 150 milionów pakietów na sekundę.
Funkcjonalność łączenia w stos	• Możliwość stackowania minimum 8 urządzeń. W przypadku dostarczenia urządzenia modularnego nie ma wymagania co do stackowania minimum 8 urządzeń wymagane jest natomiast zapewnienie rozbudowy do minimum 8 x 24 portów 10/100/1000Mbps i 8x 8 portów 10GbE . W przypadku przełączników modularnych do zapewnienia parametrów rozbudowy możliwe jest wykorzystanie więcej niż jednego przełącznika modularnego. • W przypadku urządzenia stackowalnego powinno mieć możliwość wykorzystania do stackowania modułów 10GbE lub równoważnych zapewniających przepustowość połączenia minimum 40Gbps w trybie full duplex, lub połączeń równoważnych zapewniających wymaganą przepustowość. • Obsługa trybu automatycznego przełączenia z aktywnego przełącznika master na jeden z pozostałych przełączników w grupie stack bez uruchamianie przełączników ponownie oraz bez utraty pakietów. • Możliwość dodania i usunięcia urządzenia ze stosu bez przerwy w jego działaniu.
Funkcjonalności warstwy L2	• Urządzenie musi obsługiwać min. 16000 adresów MAC oraz min. 4000 sieci VLAN. • Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad (LACP), min. 8 portów na jedno logiczne połączenie, min. 124 logicznych grup połączeń jednocześnie (w stosie). • Wsparcie dla RSTP oraz, 802.1s – Multiple Spanning Tree oraz PVST/PVST+/PVRST • Obsługa do 254 instancji STP • Wsparcie dla 802.1x • Wsparcie dla pakietów tzw. „Jumbo frames” (co najmniej 9000 bajtów) • Obsługa BPDU Guard, Root Guard • Obsługa mechanizmu GVRP • Obsługa IGMP snooping v1, v2 • Obsługa mechanizmu MAC Address Locking, Port Security. • Obsługa MLD Snooping (v1/v2). • Obsługa Multi-device Authentication.

	• Obsługa Mirroring - Port-based, ACL-based, MAC Filter-based, and VLAN-based. • Obsługa Port Loop Detection • Obsługa Private VLAN • Obsługa Protocol VLAN (802.1v), Subnet VLAN • Obsługa Single-instance Spanning Tree. • Obsługa Uni-Directional Link Detection (UDLD). • Obsługa VLAN Stacking (Q-in-Q)
Funkcjonalności warstwy L3	• Statyczny routing IPv4 i IPv6. • Sprzętowa obsługa do 12000 (IPv4) i 1000 (IPv6) wpisów routingu. • Wsparcie mechanizmu ECMP • Obsługa protokołu RIPv2 • Obsługa protokołu OSPFv2, OSPFv3 • Obsługa protokołu VRRP, VRRPv3 • Obsługa tuneli IPv6 over IPv4 • Obsługa VRF (IPv4 i IPv6) Jeśli funkcjonalności warstwy L3 wymagają licencji należy ją dostarczyć w ramach zamówienia.
Funkcje QoS	• Obsługa 6 kolejek QoS na jednym porcie fizycznym. • Zarządzanie polityką jakości ruchu – “QoS” w oparciu o algorytmy Weighted Round Robin (WRR) lub odpowiedni, Strict Priotity (SP) i ich kombinację. • Mapowanie za pomocą ACL do kolejki priorytetowej. • Mapowanie do kolejki priorytetowej na podstawie adresu MAC. • Limitowanie pasma na wejściu w oparciu o port, ACL. • Limitowanie pasma na wyjściu w oparciu o port, kolejkę. • Limitowanie pasma dla pakietów BUM (Broadcast, multicast i unknown unicast). • Obsługa DHCP Relay. • Obsługa Diffserv oraz DSCP/802.1p
Funkcje bezpieczeństwa	• Obsługa zarówno IPv4 ACL jak i IPv6 ACL. • Możliwość konfiguracji mirroringu w oparciu o dany port, listy ACL i MAC, oraz VLAN. • Obsługa Private Vlan. • Obsługa DHCP snooping • Obsługa Dynamic ARP inspection • Obsługa Authentication, Authorization, and Accounting

	• Wsparcie dla Advanced Encryption Standard (AES) i SSHv2 • Obsługa RADIUS/TACACS/TACACS+ • Obsługa Secure Copy (SCP) i Secure Shell (SSHv2) • Obsługa Change of Authorization (CoA) RFC 5176
Zgodność ze standardami	• RFC 783 TFTP • RFC 854 TELNET Client and Server • RFC 951 Bootp • RFC 1157 SNMPv1/v2c • RFC 1213 MIB-II • RFC 1493 Bridge MIB • RFC 1516 Repeater MIB • RFC 1573 SNMP MIB II • RFC 1643 Ethernet Interface MIB • RFC 1724 RIP v1/v2 MIB • RFC 1757 RMON MIB • RFC 2068 Embedded HTTP • RFC 2131 DHCP Server and DHCP Relay • RFC 2570 SNMPv3 Intro to Framework • RFC 2571 Architecture for Describing SNMP Framework • RFC 2572 SNMP Message Processing and Dispatching • RFC 2573 SNMPv3 Applications • RFC 2574 SNMPv3 User-based Security Model • RFC 2575 SNMP View-based Access Control Model SNMP • RFC 2818 Embedded HTTPS • RFC 3176 sFlow • 802.1D-2004 MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • 802.1x Port-based Network Access Control • 802.3 10Base-T • 802.3ab 1000Base-T • 802.3ad Link Aggregation (Dynamic and Static) • 802.3ae 10 Gigabit Ethernet • 802.3u 100Base-TX

	• 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.3az-2010 - IEEE • 802.1Q VLAN Tagging
Zarządzanie, zabezpieczenia	• Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (Ethernet RJ-45) • Obsługa SNMP2/SNMP3 oraz uwierzytelnianie poprzez TACACS/Radius. • Obsługa przez wbudowany serwer WWW • Obsługa DHCP Server • Obsługa NTP Network Time Protocol • Wsparcie dla protokołów OpenFlow v1.0 i v1.3 (SDN) • Obsługa 802.3az-2010 – IEEE
Wymiar	• Obudowa musi być przeznaczona do montażu w szafie rackowej 19”
Zasilanie	• Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej, wymienialne w trakcie pracy urządzenia - hot-swap, redundancja zasilaczy 1+1, możliwość zastosowania dodatkowego zewnętrznego zasilacza. • Chłodzenie musi być realizowane tył/przód, redundantne moduły wentylatorów, wymienialne w trakcie pracy urządzenia.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Moduły i kable połączeniowe

W ramach zamówienia należy dostarczyć następujące moduły i kable połączeniowe.

Komponent	Długość	Ilość
Kabel Twinax 10 Gb/s	3 m.	288
Kabel Twinax 10 Gb/s	1 m.	20
Kabel Twinax 40 Gb/s	3 m.	8
Kabel Twinax 40 Gb/s	1 m.	4
Kabel Split 40 Gb/s na 4 x 10 Gb/s	N/A	24

Moduł optyczny 10Gb/s SFP+ do 300m	N/A	152
Moduł optyczny 40 Gb/s QSFP+ do 300m	N/A	10
Moduł optyczny 10Gb/s SFP+ do 80km (ZR)	N/A	1

Oprogramowanie do zarządzania siecią LAN

W ramach zamówienia należy dostarczyć oprogramowanie do zarządzania przełącznikami sieciowymi dostarczanymi w ramach tego zamówienia z licencją umożliwiającą zarządzanie co najmniej 50 urządzeniami.

Kontroler SDN (1 szt.)

W ramach zamówienia należy dostarczyć kontroler sieci SDN obsługujący oferowane przełączniki sieci komunikacyjnej i transportowej (1Gb/s i 10Gb/s). Kontroler powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

3.3. Zadanie nr 2

Wszystkie dostarczane serwery muszą poprawnie pracować pod kontrolą systemu operacyjnego CentOS 7 lub nowszego, po uzgodnieniu z Zamawiającym.

Serwery Obliczeniowe typu A (50 szt.)

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Rack o wysokości maksymalnej 1U, wraz kompletem szyn umożliwiających montaż w standardowej szafie Rack, wysuwanie serwera do celów serwisowych, wraz z organizatorem kabli.
Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 12 slotów na pamięci z możliwością zainstalowania do minimum 384GB pamięci RAM, możliwe zabezpieczenia pamięci ECC.
Procesor	Dwa procesory, każdy o wydajności nie mniejszej niż 840 punktów SPEC-CFP2006-Base (https://www.spec.org/cpu2006/results/rfp2006.html). **Wynik dla zainstalowanego procesora w oferowanym serwerze powinien znajdować się na liście (kolumna „Base”).**
Pamięć RAM	Minimum 192 GB pamięci RAM o częstotliwości taktowania minimum 2133MHz
Sloty PCI Express	Sloty PCI Express generacji 3.0: - minimum dwa sloty x16 generacji 3, min. połowy wysokości, min. połowy długości
Wbudowane porty	Minimum 5 portów USB z czego min. 2 w technologii 3.0, pozostałe

	nie gorsze niż w technologii 2.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 2x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum cztery interfejsy sieciowe 1GbE ze złączami BaseT nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB. Dwie dodatkowe dwuportowe karty sieciowe 10GbE w standardzie SFP+.
Kontroler pamięci masowej	Możliwość instalacji kontrolera dyskowego obsługującego wewnętrzną pamięć dyskową.
Wewnętrzna pamięć masowa	Możliwość instalacji min. 16TB w wewnętrznej pamięci masowej typu Hot Plug 7.2k RPM, możliwość instalacji dysków twardych typu: SATA, NearLine SAS, SAS, SSD dostępnych w ofercie producenta serwera. Zainstalowane min. dwa dyski twarde typu SAS o pojemności min. 1,2TB. Zainstalowana dodatkowa redundantna, wewnętrzna pamięć masowa typu flash, dedykowana dla hypervisora wirtualizacyjnego o łącznej pojemności min. 32GB, umożliwiająca konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia wymaganej minimalnej ilości wewnętrzej pamięci masowej w serwerze oraz dostępnych portów USB.
Napęd optyczny	Możliwość instalacji wewnętrznego napędu optycznego
Diagnostyka i bezpieczeństwo	- zintegrowany z płytą główną moduł TPM - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą lub oprogramowanie umożliwiające monitorowanie przez Administratora zmian konfiguracji serwera, m.in. kart PCI Express, dysków twardych, procesorów, pamięci RAM.
Chłodzenie i zasilanie	Minimum 4 redundantne wentylatory pracujące w trybie Fault Tolerant. Dwa redundantne zasilacze Hot Plug o mocy minimum 550 Wat każdy wraz z kablami zasilającymi.
Zarządzanie	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność : - podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0, SNMP, VLAN tagging - wbudowana diagnostyka

	- wbudowane narzędzia do instalacji systemów operacyjnych - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - lokalna oraz zdalna konfiguracja serwera - zdalna instalacja systemów operacyjnych - wsparcie dla IPv4 i IPv6 - integracja z Active Directory - wirtualna konsola z dostępem do myszy i klawiatury - udostępnianie wirtualnej konsoli - autentykacja poprzez publiczny klucz (dla SSH) - możliwość obsługi poprzez dwóch administratorów równocześnie - wysyłanie do administratora powiadomienia o awarii lub zmianie konfiguracji sprzętowej Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia - Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia - Filtry raportów umożliwiające podgląd zdarzeń - Możliwość przejęcia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi

	producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat. W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2. Zgodność z wirtualizatorami Citrix, VMware vSphere, Microsoft Hyper-V. Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere.

Serwery Obliczeniowe typu B (4 szt.)

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Rack, wraz kompletem szyn umożliwiających montaż w standardowej szafie Rack, wysuwanie serwera do celów serwisowych, wraz z organizatorem kabli.
Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 24 sloty na pamięci z możliwością zainstalowania do minimum 768GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Dwa procesory, każdy o wydajności nie mniejszej niż 660 punktów SPEC-CFP2006-Base (https://www.spec.org/cpu2006/results/rfp2006.html). **Wynik dla zainstalowanego procesora w oferowanym serwerze powinien znajdować się na liście (kolumna „Base").**
Pamięć RAM	Minimum 192 GB pamięci RAM o częstotliwości taktowania minimum 2133MHz
Sloty PCI Express	Minimum 6 slotów PCI Express generacji 3.0 w tym: - minimum 2 sloty umożliwiające instalację dostarczanych

	akceleratorów graficznych GPU - minimum 3 sloty o prędkości x8
Wbudowane porty	Minimum 5 portów USB z czego min. 2 w technologii 3.0, pozostałe nie gorsze niż w technologii 2.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 2x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum cztery interfejsy sieciowe 10Gb Ethernet SFP+, interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express oraz portów USB. Wsparcie dla protokołów iSCSI Boot oraz IPv6. Możliwość instalacji wymiennie modułów udostępniających: • dwa interfejsy sieciowe 1GbE w standardzie BaseT oraz dwa interfejsy sieciowe 10GbE ze złączami w standardzie SFP+ • cztery interfejsy sieciowe 1GbE w standardzie BaseT Dodatkowa czteroportowa karta 1GbE w standardzie BaseT.
Kontroler pamięci masowej	Sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6, 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60, wyposażony w wbudowaną, nieulotną pamięć cache o pojemności min. 1GB.
Wewnętrzna pamięć masowa	Możliwość instalacji min. 4.5TB w wewnętrznej pamięci masowej typu Hot Plug 15k RPM, możliwość instalacji dysków twardych typu: SATA, NearLine SAS, SAS, SSD, PCI Express Flash dostępnych w ofercie producenta serwera. Zainstalowane min. dwa dyski twarde typu SAS o pojemności min. 1,2TB. Możliwość instalacji dodatkowej wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości minimalnej ilości wewnętrzej pamięci masowej w serwerze oraz dostępnych portów USB.
Napęd optyczny	Możliwość instalacji wewnętrznego napędu optycznego
Akcelerator graficzny GPU	Zainstalowane fabrycznie minimum 2 karty GPU, dedykowane przez producenta serwera i posiadające jego wsparcie o parametrach: - Wydajność obliczeń zmiennoprzecinkowych podwójnej precyzji [GPU Boost] dla wszystkich akceleratorów (suma) - minimum 5.7 Tflops - Wydajność obliczeń zmiennoprzecinkowych pojedynczej precyzji [GPU Boost] dla wszystkich akceleratorów (suma) -minimum 17 Tflops - Przepustowość pamięci dla pojedynczego procesora w ramach

	akceleratora - minimum 240GB/s - Minimum 12GB pamięci GDDR5 dla pojedynczego procesora w ramach akceleratora - Środowisko tworzenia aplikacji: OpenCL lub CUDA
Diagnostyka i bezpieczeństwo	- zintegrowany z płytą główną moduł TPM - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą lub oprogramowanie umożliwiające monitorowanie przez Administratora zmian konfiguracji serwera, m.in. kart PCI Express, dysków twardych, procesorów, pamięci RAM.
Chłodzenie i zasilanie	Minimum 6 redundantnych wentylatorów z możliwością wyjęcia podczas pracy (Hot Plug) Dwa redundantne zasilacze Hot Plug o mocy minimum 1100 Wat każdy wraz z kablami zasilającymi.
Zarządzanie	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność : - podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0, SNMP, VLAN tagging - wbudowana diagnostyka - wbudowane narzędzia do instalacji systemów operacyjnych - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - lokalna oraz zdalna konfiguracja serwera - zdalna instalacja systemów operacyjnych - wsparcie dla IPv4 i IPv6 - integracja z Active Directory - wirtualna konsola z dostępem do myszy i klawiatury - udostępnianie wirtualnej konsoli - uwierzytelnienie poprzez publiczny klucz (dla SSH) - możliwość obsługi poprzez dwóch administratorów równocześnie - wysyłanie do administratora powiadomienia o awarii lub zmianie konfiguracji sprzętowej Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:

	- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia - Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia - Filtry raportów umożliwiające podgląd zdarzeń - Możliwość przejęcia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat. W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2. Zgodność z wirtualizatorami Citrix, VMware vSphere, Microsoft

	Hyper-V. Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere.

System składowania danych realizowany będzie za pomocą dwóch rozwiązań dedykowanej macierzy dyskowej oraz grupie 4 serwerów typu „storage", na których Wykonawca zaimplementuje klaster rozwiązania CEPH, w najnowszej stabilnej wersji na dzień składania oferty lub innej, uzgodnionej z Zamawiającym.

Serwery składowania danych (4 szt.)

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Rack o wysokości maksymalnej 2U, wraz kompletem szyn umożliwiających montaż w standardowej szafie Rack, wysuwanie serwera do celów serwisowych, wraz z organizatorem kabli.
Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 24 sloty na pamięci z możliwością zainstalowania do minimum 768GB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	Dwa procesory, każdy o wydajności nie mniejszej niż 660 punktów SPEC-CFP2006-Base (https://www.spec.org/cpu2006/results/rfp2006.html). **Wynik dla zainstalowanego procesora w oferowanym serwerze powinien znajdować się na liście (kolumna „Base").**
Pamięć RAM	Minimum 192 GB pamięci RAM o częstotliwości taktowania minimum 2133MHz
Sloty PCI Express	Funkcjonujące sloty PCI Express: - minimum cztery sloty x8 generacji 3, o niskim profilu - minimum dwa sloty x16 generacji 3
Wbudowane porty	Minimum 4 porty USB, z czego min. 2 w technologii 3.0, pozostałe nie gorsze niż w technologii 2.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 2x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express oraz portów USB. Wsparcie dla protokołów iSCSI Boot oraz IPv6. Możliwość instalacji wymiennie modułów udostępniających: - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+

	- dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT Dodatkowa dwuportowa karta sieciowa 1Gb/s Ethernet w standardzie BaseT. Dodatkowa dwuportowa, karta sieciowa 40Gb/s w standardzie QSFP+/Direct Attach wraz z dedykowanymi wkładkami optycznymi.
Kontroler pamięci masowej	Sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6, 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60, wyposażony w wbudowaną, nieulotną pamięć cache o pojemności min. 1GB.
Wewnętrzna pamięć masowa	Możliwość instalacji min. 15.5TB w wewnętrznej pamięci masowej typu Hot Plug 15k RPM, możliwość instalacji dysków twardych typu: SATA, NearLine SAS, SAS, SSD, PCI Express Flash oraz SED dostępnych w ofercie producenta serwera. Zainstalowane dyski : Min. 20 dysków twardych typu SAS o pojemności min. 1.2TB Min. 2 dyski twarde typu SAS o pojemności min. 300GB Min. 4 dyski twarde typu Flash MLC o pojemności min. 400GB każdy Możliwość instalacji dodatkowej wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości minimalnej ilości wewnętrzej pamięci masowej w serwerze.
Bezpieczeństwo i diagnostyka	- zintegrowany z płytą główną moduł TPM - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą lub oprogramowanie umożliwiające monitorowanie przez Administratora zmian konfiguracji serwera, m.in. kart PCI Express, dysków twardych, procesorów, pamięci RAM.
Chłodzenie i zasilanie	Minimum 6 redundantnych wentylatorów z możliwością wyjęcia podczas pracy (Hot Plug) Dwa redundantne zasilacze Hot Plug o mocy minimum 750 Wat każdy wraz z kablami zasilającymi.
Zarządzanie	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność : - podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0,

	SNMP, VLAN tagging - wbudowana diagnostyka - wbudowane narzędzia do instalacji systemów operacyjnych - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - lokalna oraz zdalna konfiguracja serwera - zdalna instalacja systemów operacyjnych - wsparcie dla IPv4 i IPv6 - integracja z Active Directory - wirtualna konsola z dostępem do myszy i klawiatury - udostępnianie wirtualnej konsoli - autentykacja poprzez publiczny klucz (dla SSH) - możliwość obsługi poprzez dwóch administratorów równocześnie - wysyłanie do administratora powiadomienia o awarii lub zmianie konfiguracji sprzętowej Dodatkowe opogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach- Szybki podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia - Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń - Możliwość przejęcia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do

	następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat. W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2. Zgodność z wirtualizatorami Citrix, VMware vSphere, Microsoft Hyper-V. Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere.

Macierz dyskowa typ. A (1 szt.)

LP	Minimalne wymagania
1	Macierz musi być wyposażona w co najmniej 4 kontrolery odpowiedzialne za obsługę dostępu do danych i komunikację z systemami operacyjnymi i aplikacyjnymi.
2	Macierz powinna być wyposażona w przynajmniej dwa moduły do transmisji z możliwością obsługi danych z protokołami blokowymi: FC, iSCSI, FCoE,
3	Macierz powinna być wyposażona w przynajmniej dwa moduły do transmisji z możliwością obsługi danych z protokołami plikowymi: CIFS (wersje 2.0, 3.0), NFS (wersje V2, V3, V4), FTP.
4	Macierz powinna być wyposażona w, redundantne moduły odpowiedzialne za obsługę zarządzanej przestrzeni dyskowej, jej konfigurację, liczenie RAID.
5	Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
6	Macierz musi być wyposażona w co najmniej 256GB (pojemność efektywna dostępna dla operacji zapisu po uwzględnieniu mechanizmu cache mirror zabezpieczającej przed

	awarią pamięci cache) przestrzeni cache służącej do buforowania operacji odczytu oraz zapisu dostępne dla każdego wolumenu macierzy. Cache (do odczytu i zapisu) musi mieć możliwość rozbudowy do 512GB przy pomocy modułów DDR/kolejnych kontrolerów/dysków SSD. Dla dysków SSD nie może być to funkcjonalność tieringu.
7	Cała macierz musi być zabezpieczona przez nieograniczony czas przed utratą danych w przypadku awarii zasilania. Macierz musi być wyposażona w wewnętrzny system podtrzymywania bateryjnego, pozwalający w przypadku utraty zasilania wykonanie zapisu danych z pamięci cache na dyski twarde (opróżnienie buforu zapisania) i bezpieczne wyłącznie macierzy. Jeśli oferowana macierz nie posiada takiej opcji Zamawiający dopuszcza dostarczenie oddzielnego modułu UPS wraz z oprogramowaniem/skryptami automatyzującymi zrzut danych w przypadku braku dostępu do zasilania. Producent UPS i/lub skryptów musi zagwarantować kompatybilność rozwiązania
8	Urządzenie powinno być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwalność pracy i utrzymanie funkcjonalności macierzy w szczególności działania pamięci cache w przypadku awarii jednego ze źródeł zasilania.
9	Macierz powinna współpracować równocześnie z dyskami Flash, SAS, jak i pojemnymi dyskami Near Line SAS. Dostarczona macierz powinna być wyposażona, w co najmniej: a. 45 dysków typu SAS 2,5” o pojemności min. 900 GB b. 30 dysków typu SATA albo NL-SAS 3,5” o pojemności min. 4TB
10	Macierz musi umożliwiać pracę dysków SSD, SAS i Near Line SAS w obrębie jednej półki.
11	Wymagana jest obsługa min. 24 dysków 2.5” w półce o wysokości max. 2U i jednoczesna możliwość obsługi min. 12 dysków 3.5” w obrębie jednej półki o wysokości max. 3U.
12	Macierz powinna pozwalać na rozbudowę do co najmniej 250 dysków twardych. Dodawanie kolejnych dysków, jak i kolejnych półek dyskowych powinno odbywać się w trybie on-line.
13	Macierz musi wspierać tworzenie wolumenów logicznych w rozmiarach do 256 TB.
14	Na podstawie informacji o wykorzystaniu obszarów LUN'a macierz musi posiadać funkcjonalność automatycznego migrowania gorących obszarów (o największej liczbie IOPS) na najszybszą warstwę, a obszary zimne (o najmniejszej liczbie IOPS) na wolniejszą warstwę. Dopuszcza się technologie umożliwiające migrację blokiem nie większym niż 1GB. Migracja musi być możliwa pomiędzy wszystkimi warstwami tj.: SSD, SAS i Near Line SAS i musi być przezroczysta dla hostów i aplikacji. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
15	Macierz musi wspierać obsługę funkcjonalności dostarczających szczegółowych informacji dotyczących wydajności macierzy, umożliwiających badanie wzorców i trendów wydajności. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
16	Wymagana jest obsługa kompresji na poziomie bloków danych. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
17	Macierz powinna umożliwiać równoczesną obsługę wielu poziomów RAID. Ze względu na zakładane przeznaczenie niniejszego urządzenia zamawiający wymaga, by obsługiwało ono, co najmniej RAID 0, 1, 5 lub 4, 6 lub DP i 10.

18	Macierz powinna zapewniać mechanizm thin provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu. W przypadku zbliżenia się do fizycznych granic systemu plików, musi istnieć możliwość automatycznego jego rozszerzenia bez konieczności interwencji administratora. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
19	Macierz musi obsługiwać lun masking, lun mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy.
20	Macierz musi być wyposażona w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż" dla następujących parametrów dostępu do dysku logicznego: a. Ilość operacji na sekundę (IOPS), b. Przepustowość (MB/s).
21	Macierz powinna zapewniać obsługę klonów oraz kopii migawkowych. Rozwiązanie ma pozwalać na automatyczne zwiększanie przestrzeni dla kopii migawkowych. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
22	Macierz musi umożliwiać wykonywanie kopii migawkowej w trybie Copy On First Write (COFW).
23	Macierz musi wspierać mechanizm zdalnej replikacji z poziomu macierzy na drugą zapasową macierz, w trybie synchronicznym oraz asynchronicznym). **Licencja umożliwiająca wykorzystanie powyższych funkcjonalności nie jest przedmiotem oferty. Powinna pozwalać jedynie o możliwość rozbudowy w przyszłości o tą funkcjonalność.**
24	Macierz musi być wyposażona, w co najmniej: a.8 portów FC min. 8 Gbps do komunikacji z hostami b. 8 portów min. 10GbE ze sprzętową obsługą iSCSI do komunikacji z hostami c. 8 portów min. 1GbE do obsługi ruchu za pomocą protokołów CIFS i NFS
25	Macierz powinna mieć możliwość rozbudowy do 16 portów FC min. 8Gbps bez dokładania dodatkowych kontrolerów (modułów odpowiedzialnych za obsługę zarządzanej przestrzeni dyskowej, jej konfigurację, liczenie RAID oraz wyposażonych w pamięć cache do obsługi buforowania operacji odczytu i zapisu).
26	Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
27	Macierz musi zapewniać jednoczesne zastosowanie różnych trybów protekcji RAID dla różnych typów dysków fizycznych obsługujących pojedynczy dysk logiczny objęty mechanizmem tieringu.
28	Macierz musi pozwalać na agregację portów Ethernetowych przeznaczonych do obsługi danych plikowych w łącza logiczne za pomocą np. protokołu IEEE 802.3ad lub Cisco EtherChannel oraz zapewniać mechanizm zapewniający ciągłą dostępność do danych nawet w przypadku awarii przełącznika Ethernetowego.
29	Macierz po rozbudowie powinna posiadać możliwość wykonywania kopii zapasowej

	bezpośrednio na nośniki taśmowe bez uczestnictwa oddzielnego oprogramowania do wykonywania kopii zapasowej.
30	Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation).
31	Macierz powinna być zarządzana zarówno z poziomu linii komend (CLI), jak również poprzez jeden interfejs graficzny (GUI).
32	Wraz z macierzą musi być dostarczone oprogramowanie monitorujące umożliwiacie tworzenie i generowanie własnych raportów (tzw. custom reports) - w zakresie raportowania wydajności i pojemności macierzy. Oprogramowanie musi posiadać również funkcjonalność rozliczania wykorzystywanych zasobów storage, tzw. chargeback.
33	Macierz powinna oferować funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.
34	Macierz oraz ich oprogramowanie wewnętrzne musi być objęte opieką serwisową producenta przez okres 5 lat. W okresie opieki wymagany jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania
35	Macierz powinna zawierać szyny umożliwiające montaż w szafie rack, okablowanie zasilające oraz patchcordy (min. 2× UTP Cat. 6, 3m). Gwarancja powinna być świadczona w trybie 5x8, z czasem reakcji następnego dnia roboczego.
36	Oferowane urządzenia muszą być fabrycznie nowe i pochodzić z autoryzowanego kanału dystrybucji producenta w Polsce.

3.4. Zadanie nr 3

W ramach zadania nr 3 Wykonawca skonfiguruje 2 środowiska:

1) Środowisko zarządzające infrastrukturą OpenStack
2) Środowisko usługowe WIŁ

Środowisko zarządzające infrastrukturą OpenStack powstanie na bazie Klastra wirtualizacyjnego 3 serwerów fizycznych typu A podłączonego do Macierzy dyskowej Typu A za pomocą interfejsów iSCSI lub NFS.

Środowisko usługowe WIŁ powstanie na bazie 4 serwerów fizycznych typu C z czego 3 z nich będą stanowiły klaster wirtualizacyjny natomiast 4 host będzie hostem dla kopii zapasowych.

Wszystkie te serwery będą podłączone za pomocą przełączników FC do macierzy dyskowej typu B.

Serwery Wirtualizacyjne typu C (4 szt.)

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Rack o wysokości maksymalnej 1U, wraz kompletem szyn umożliwiających montaż w standardowej szafie Rack, wysuwanie serwera do celów serwisowych, wraz z organizatorem kabli.
Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 12 slotów na pamięci z możliwością zainstalowania do minimum 384GB pamięci RAM, możliwe

	zabezpieczenia pamięci ECC.
Procesor	Dwa procesory, każdy o wydajności nie mniejszej niż 840 punktów SPEC-CFP2006-Base (https://www.spec.org/cpu2006/results/rfp2006.html). **Wynik dla zainstalowanego procesora w oferowanym serwerze powinien znajdować się na liście (kolumna „Base").**
Pamięć RAM	Minimum 192 GB pamięci RAM o częstotliwości taktowania minimum 2133MHz
Sloty PCI Express	Sloty PCI Express generacji 3.0: - minimum dwa sloty x16 generacji 3, min. połowy wysokości, min. połowy długości
Wbudowane porty	Minimum 5 portów USB z czego min. 2 w technologii 3.0, pozostałe nie gorsze niż w technologii 2.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 2x VGA D-Sub
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Interfejsy sieciowe	Minimum cztery interfejsy sieciowe 1GbE ze złączami BaseT nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB. Jedna dodatkowa dwuportowa karta sieciowe 10GbE w standardzie SFP+. Jedna dodatkowa dwuportowa karta FC min. 8Gb/s.
Kontroler pamięci masowej	Możliwość instalacji kontrolera dyskowego obsługującego wewnętrzną pamięć dyskową.
Wewnętrzna pamięć masowa	Możliwość instalacji min. 16TB w wewnętrznej pamięci masowej typu Hot Plug 7.2k RPM, możliwość instalacji dysków twardych typu: SATA, NearLine SAS, SAS, SSD dostępnych w ofercie producenta serwera. Zainstalowane min. dwa dyski twarde typu SAS o pojemności min. 1,2TB. Zainstalowana dodatkowa redundantna, wewnętrzna pamięć masowa typu flash, dedykowana dla hypervisora wirtualizacyjnego o łącznej pojemności min. 32GB, umożliwiająca konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia wymaganej minimalnej ilości wewnętrzej pamięci masowej w serwerze oraz dostępnych portów USB.
Napęd optyczny	Możliwość instalacji wewnętrznego napędu optycznego
Diagnostyka i bezpieczeństwo	- zintegrowany z płytą główną moduł TPM - wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą lub oprogramowanie umożliwiające monitorowanie przez Administratora zmian konfiguracji serwera, m.in. kart PCI Express, dysków twardych, procesorów, pamięci RAM.

Chłodzenie i zasilanie	Minimum 4 redundantne wentylatory pracujące w trybie Fault Tolerant. Dwa redundantne zasilacze Hot Plug o mocy minimum 550 Wat każdy wraz z kablami zasilającymi.
Zarządzanie	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność : - podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0, SNMP, VLAN tagging - wbudowana diagnostyka - wbudowane narzędzia do instalacji systemów operacyjnych - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - lokalna oraz zdalna konfiguracja serwera - zdalna instalacja systemów operacyjnych - wsparcie dla IPv4 i IPv6 - integracja z Active Directory - wirtualna konsola z dostępem do myszy i klawiatury - udostępnianie wirtualnej konsoli - autentykacja poprzez publiczny klucz (dla SSH) - możliwość obsługi poprzez dwóch administratorów równocześnie - wysyłanie do administratora powiadomienia o awarii lub zmianie konfiguracji sprzętowej Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia

	- Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia - Filtry raportów umożliwiające podgląd zdarzeń - Możliwość przejęcia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat. W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela. Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2. Zgodność z wirtualizatorami Citrix, VMware vSphere, Microsoft Hyper-V. Zgodność z systemami SUSE Linux Enterprise Server, RedHat Enterprise Linux, Citrix XenServer, VMware vSphere.

Przełączniki FC (2 szt.)

Lp.	Wymaganie minimalne
1.	Przełącznik FC musi być wykonany w technologii FC min. 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2, 1 Gb/s z funkcją auto negocjacji prędkości.

2.	Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 8 portów FC przełącznika.
3.	Przełącznik musi być dostarczony wraz z minimum 8 modułami SFP FC min. 8 Gb/s.
4.	Rodzaj obsługiwanych portów: E, F, N oraz FL.
5.	Przełącznik FC musi mieć wysokość maksymalnie 1 U (jednostka wysokości szaty montażowej) oraz zapewniać techniczną możliwość montażu w szafie 19”.
6.	Przełącznik FC musi posiadać nadmiarowe wentylatory N+1.
7.	Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiające blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
8.	Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk" oraz obsługiwać grupy połączeń „trunk” o różnych długościach.
9.	Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów.
10.	Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
11.	Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: 1. Listy Kontroli Dostępu definiując urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric 2. Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-Cl-IAP i FCAP 3. Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP 4. Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów 5. Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHV2. 6. Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. 7. Konta użytkowników definiowane w środowisku RADIUS lub LDAP. 8. Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS. 9. Obsługa SNMP V3.
12.	Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.

13.	Przełącznik FC musi mieć możliwość instalacji jedno modowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10 km.
14.	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC
15.	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)
16.	Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP
17.	Maksymalny dopuszczalny pobór mocy przełącznika FC to 60W
18.	Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.
19.	Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns.
20.	Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN
21.	Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID.
22.	Możliwość wymiany w trybie „na gorąco” minimum w odniesieniu do modułów portów Fibre Channel (SFP).
23.	Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
24.	Urządzenie powinno być objęte gwarancją na sprzęt przynajmniej na 5 lat. Gwarancja powinna być świadczona w trybie co najmniej 5x8, z czasem reakcji w następnym dniu roboczym.
25.	Zestaw powinien zawierać szyny umożliwiające montaż w szafie rack oraz okablowanie zasilające.
26.	Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.

Macierz dyskowa typu B (1 szt.)

Lp.	Wymaganie minimalne
1	Macierz musi być wyposażona w co najmniej 4 kontrolery odpowiedzialne za obsługę dostępu do danych i komunikację z systemami operacyjnymi i aplikacyjnymi.
2	Macierz powinna być wyposażona w przynajmniej dwa moduły do transmisji z możliwością obsługi danych z protokołami blokowymi: FC, iSCSI, FCoE,
3	Macierz powinna być wyposażona w przynajmniej dwa moduły do transmisji z możliwością obsługi danych z protokołami plikowymi: CIFS (wersje 2.0, 3.0), NFS (wersje

	V2, V3, V4), FTP.
4	Macierz powinna być wyposażona w, redundantne moduły odpowiedzialne za obsługę zarządzanej przestrzeni dyskowej, jej konfigurację, liczenie RAID.
5	Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
6	Macierz musi być wyposażona w co najmniej 96GB (pojemność efektywna dostępna dla operacji zapisu po uwzględnieniu mechanizmu cache mirror zabezpieczającej przed awarią pamięci cache) przestrzeni cache służącej do buforowania operacji odczytu oraz zapisu dostępne dla każdego wolumenu macierzy. Cache (do odczytu i zapisu) musi mieć możliwość rozbudowy do 256GB przy pomocy modułów DDR/kolejnych kontrolerów/dysków SSD. Dla dysków SSD nie może być to funkcjonalność tieringu.
7	Cała macierz musi być zabezpieczona przez nieograniczony czas przed utratą danych w przypadku awarii zasilania. Macierz musi być wyposażona w wewnętrzny system podtrzymywania bateryjnego, pozwalający, w przypadku utraty zasilania wykonanie zapisu danych z pamięci cache na dyski twarde (opróżnienie buforu zapisania) i bezpieczne wyłącznie macierzy. Jeśli oferowana macierz nie posiada takiej opcji Zamawiający dopuszcza dostarczenie oddzielnego modułu UPS wraz z oprogramowaniem/skryptami automatyzującymi zrzut danych w przypadku braku dostępu do zasilania. Producent UPS i/lub skryptów musi zagwarantować kompatybilność rozwiązania
8	Urządzenie powinno być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwalność pracy i utrzymanie funkcjonalności macierzy w szczególności działania pamięci cache w przypadku awarii jednego ze źródeł zasilania.
9	Macierz powinna współpracować równocześnie z dyskami Flash, SAS, jak i pojemnymi dyskami Near Line SAS. Dostarczona macierz powinna być wyposażona, w co najmniej 25 dysków typu SAS 2,5” o pojemności min. 1,2TB
10	Macierz musi umożliwiać pracę dysków SSD, SAS i Near Line SAS w obrębie jednej półki.
11	Wymagana jest obsługa min 24 dysków 2.5” w półce o wysokości max. 2U i jednoczesna możliwość obsługi min 12 dysków 3.5” w obrębie jednej półki o wysokości max. 3U.
12	Macierz powinna pozwalać na rozbudowę, do co najmniej 120 dysków twardych. Dodawanie kolejnych dysków, jak i kolejnych półek dyskowych powinno odbywać się w trybie on-line.
13	Macierz musi wspierać tworzenie wolumenów logicznych w rozmiarach do 256 TB.
14	Na podstawie informacji o wykorzystaniu obszarów LUN'a macierz musi posiadać funkcjonalność automatycznego migrowania gorących obszarów (o największej liczbie IOPS) na najszybszą warstwę, a obszary zimne (o najmniejszej liczbie IOPS) na wolniejszą warstwę. Dopuszcza się technologie umożliwiające migrację blokiem nie większym niż 1GB. Migracja musi być możliwa pomiędzy wszystkimi warstwami tj.: SSD, SAS i Near Line SAS i musi być przezroczysta dla hostów i aplikacji. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
15	Macierz musi wspierać obsługę funkcjonalności dostarczających szczegółowych informacji dotyczących wydajności macierzy, umożliwiających badanie wzorców i

	trendów wydajności. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
16	Wymagana jest obsługa kompresji na poziomie bloków danych. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
17	Macierz powinna umożliwiać równoczesną obsługę wielu poziomów RAID. Ze względu na zakładane przeznaczenie niniejszego urządzenia zamawiający wymaga, by obsługiwało ono, co najmniej RAID 0, 1, 5 lub 4, 6 lub DP i 10.
18	Macierz powinna zapewniać mechanizm thin provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu. W przypadku zbliżenia się do fizycznych granic systemu plików, musi istnieć możliwość automatycznego jego rozszerzenia bez konieczności interwencji administratora**. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.**
19	Macierz musi obsługiwać lun masking, lun mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy.
20	Macierz musi być wyposażona w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż" dla następujących parametrów dostępu do dysku logicznego: a. Ilość operacji na sekundę (IOPS), b. Przepustowość (MB/s).
21	Macierz powinna zapewniać obsługę klonów oraz kopii migawkowych. Rozwiązanie ma pozwalać na automatyczne zwiększanie przestrzeni dla kopii migawkowych. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. **Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia**.
22	Macierz musi umożliwiać wykonywanie kopii migawkowej w trybie Copy On First Write (COFW).
23	Macierz musi wspierać mechanizm zdalnej replikacji z poziomu macierzy na drugą zapasową macierz, w trybie synchronicznym oraz asynchronicznym). **Licencja umożliwiająca wykorzystanie powyższych funkcjonalności nie jest przedmiotem oferty. Powinna pozwalać jedynie na możliwość rozbudowy w przyszłości o tą funkcjonalność.**
24	Macierz musi być wyposażona, w co najmniej 8 portów FC min. 8 Gbps do komunikacji z hostami
25	Macierz powinna mieć możliwość rozbudowy do 16 portów FC 8Gbps bez dokładania dodatkowych kontrolerów (modułów odpowiedzialnych za obsługę zarządzanej przestrzeni dyskowej, jej konfigurację, liczenie RAID oraz wyposażonych w pamięć cache do obsługi buforowania operacji odczytu i zapisu).
26	Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
27	Macierz musi zapewniać jednoczesne zastosowanie różnych trybów protekcji RAID dla różnych typów dysków fizycznych obsługujących pojedynczy dysk logiczny objęty

	mechanizmem tieringu.
28	Macierz musi pozwalać na agregację portów Ethernetowych przeznaczonych do obsługi danych plikowych w łącza logiczne za pomocą np. protokołu IEEE 802.3ad lub Cisco EtherChannel oraz zapewniać mechanizm zapewniający ciągłą dostępność do danych nawet w przypadku awarii przełącznika Ethernetowego.
29	Macierz po rozbudowie powinna posiadać możliwość wykonywania kopii zapasowej bezpośrednio na nośniki taśmowe bez uczestnictwa oddzielnego oprogramowania do wykonywania kopii zapasowej.
30	Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation).
31	Macierz powinna być zarządzana zarówno z poziomu linii komend (CLI), jak również poprzez jeden interfejs graficzny (GUI).
32	Wraz z macierzą musi być dostarczone oprogramowanie monitorujące umożliwiacie tworzenie i generowanie własnych raportów (tzw. custom reports) - w zakresie raportowania wydajności i pojemności macierzy. Oprogramowanie musi posiadać również funkcjonalność rozliczania wykorzystywanych zasobów storage, tzw. chargeback.
33	Macierz powinna oferować funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.
34	Macierz oraz ich oprogramowanie wewnętrzne musi być objęte opieką serwisową producenta przez okres 5 lat. W okresie opieki wymagany jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania
35	Macierz powinna zawierać szyny umożliwiające montaż w szafie rack, okablowanie zasilające oraz patchcordy (min. 2× UTP Cat 6 3m). Maksymalny dopuszczalna wysokość macierzy to 7U w szafie rack. Gwarancja powinna być świadczona w trybie 5x8, z czasem reakcji następnego dnia roboczego
36	Oferowane urządzenia musza być fabrycznie nowe i pochodzić z autoryzowanego kanału dystrybucji producenta w Polsce.

Przełączniki rdzeniowe 1/10Gbps (4 szt.)

Komponent	Minimalne wymagania
Ilość portów	• Urządzenie musi posiadać minimum 48 portów 10/100/1000Mbps RJ-45 Base-T. • Urządzenie musi posiadać co najmniej 12 aktywnych portów 10GbE
Parametry wydajnościowe	Wydajność przełączania minimum 200 gigapakietów na sekundę. Wydajność przekazywania pakietów minimum 150 milionów pakietów na sekundę.
Funkcjonalność łączenia w stos	• Możliwość stackowania minimum 8 urządzeń. W przypadku dostarczenia urządzenia modularnego nie ma wymagania co do stackowania minimum 8 urządzeń wymagane jest natomiast zapewnienie rozbudowy do minimum 8 x 48 portów 10/100/1000Mbps z uwzględnieniem wymaganych modułów z wymagania Ilość portów. W przypadku przełączników modularnych

	do zapewnienia parametrów rozbudowy możliwe jest zastosowanie więcej niż jednego przełącznika modularnego. • W przypadku urządzenia stackowalnego powinno mieć możliwość wykorzystania do stackowania modułów 40G lub modułów 10G lub równoważnych zapewniających przepustowość połączenia minimum 80Gbps w trybie full duplex, lub połączeń równoważnych zapewniających wymaganą przepustowość. • Obsługa trybu automatycznego przełączenia z aktywnego przełącznika master na jeden z pozostałych przełączników w grupie stack bez uruchamianie przełączników ponownie oraz bez utraty pakietów. • Możliwość dodania i usunięcia urządzenia ze stosu bez przerwy w jego działaniu.
Funkcjonalności warstwy L2	• Urządzenie musi obsługiwać min. 16000 adresów MAC oraz min. 4000 sieci VLAN. • Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad (LACP), min. 8 portów na jedno logiczne połączenie, min. 124 logicznych grup połączeń jednocześnie (w stosie). • Wsparcie dla RSTP, 802.1s – Multiple Spanning Tree oraz PVST/PVST+/PVRST • Obsługa do 254 instancji STP • Wsparcie dla 802.1x • Wsparcie dla pakietów tzw. „Jumbo frames” (co najmniej 9000 bajtów) • Obsługa BPDU Guard, Root Guard • Obsługa mechanizmu GVRP • Obsługa IGMP snooping v1, v2 • Obsługa mechanizmu MAC Address Locking, Port Security • Obsługa MLD Snooping (v1/v2) • Obsługa Mirroring - Port-based, ACL-based, MAC Filter-based, and VLAN-based. • Obsługa Port Loop Detection • Obsługa Private VLAN • Obsługa Protocol VLAN (802.1v), Subnet VLAN • Obsługa Uni-Directional Link Detection (UDLD) • Obsługa VLAN Stacking (Q-in-Q)
Funkcjonalności warstwy L3	• Statyczny routing IPv4 i IPv6 • Sprzętowa obsługa min 1000 (IPv4) i 1000 (IPv6) wpisów routingu • Wsparcie mechanizmu ECMP

	• Obsługa protokołu RIPv2 • Obsługa protokołu OSPFv2, OSPFv3 • Obsługa protokołu VRRP, VRRPv3 • Obsługa tuneli IPv6 over IPv4 • Obsługa VRF (IPv4 i IPv6) Jeśli funkcjonalności warstwy L3 wymagają licencji należy ją dostarczyć w ramach zamówienia.
Funkcje QoS	• Obsługa 8 kolejek QoS na jednym porcie fizycznym. • Zarządzanie polityką jakości ruchu – "QoS" w oparciu o algorytmy Weighted Round Robin (WRR) lub odpowiedni, Strict Priotity (SP) i ich kombinację. • Mapowanie za pomocą ACL do kolejki priorytetowej. • Mapowanie do kolejki priorytetowej na podstawie adresu MAC. • Limitowanie pasma na wejściu w oparciu o port, ACL. • Limitowanie pasma na wyjściu w oparciu o port, kolejkę. • Limitowanie pasma dla pakietów BUM (Broadcast, multicast i unknown unicast). • Obsługa DHCP Relay. • Obsługa Diffserv oraz 802.1p
Funkcje bezpieczeństwa	• Obsługa zarówno IPv4 ACL jak i IPv6 ACL. • Możliwość konfiguracji mirroringu w oparciu o dany port, listy ACL i MAC, oraz VLAN. • Obsługa Private Vlan. • Obsługa DHCP snooping • Obsługa Dynamic ARP inspection • Obsługa Authentication, Authorization, and Accounting • Wsparcie dla Advanced Encryption Standard (AES) i SSHv2 • Obsługa RADIUS/TACACS/TACACS+ • Obsługa Secure Copy (SCP) i Secure Shell (SSHv2) • Obsługa Change of Authorization (CoA) RFC 5176
Zgodność ze standardami	• RFC 783 TFTP • RFC 854 TELNET Client and Server • RFC 951 Bootp • RFC 1157 SNMPv1/v2c • RFC 1213 MIB-II • RFC 1493 Bridge MIB • RFC 1516 Repeater MIB

	• RFC 1573 SNMP MIB II • RFC 1643 Ethernet Interface MIB • RFC 1724 RIP v1/v2 MIB • RFC 1757 RMON MIB • RFC 2068 Embedded HTTP • RFC 2131 DHCP Server and DHCP Relay • RFC 2570 SNMPv3 Intro to Framework • RFC 2571 Architecture for Describing SNMP Framework • RFC 2572 SNMP Message Processing and Dispatching • RFC 2573 SNMPv3 Applications • RFC 2574 SNMPv3 User-based Security Model • RFC 2575 SNMP View-based Access Control Model SNMP • RFC 2818 Embedded HTTPS • RFC 3176 sFlow • 802.1D-2004 MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • 802.1x Port-based Network Access Control • 802.3 10Base-T • 802.3ab 1000Base-T • 802.3ad Link Aggregation (Dynamic and Static) • 802.3ae 10 Gigabit Ethernet • 802.3u 100Base-TX • 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.3az-2010 - EEE • 802.1Q VLAN Tagging
Zarządzanie, zabezpieczenia	• Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (Ethernet RJ-45). • Obsługa SNMP2/SNMP3 oraz uwierzytelnianie poprzez TACACS/Radius. • Obsługa przez wbudowany serwer WWW. • Obsługa DHCP Server. • Obsługa NTP Network Time Protocol.

	• Wsparcie dla protokołów OpenFlow v1.0 i v1.3 (SDN). • Obsługa 802.3az-2010 – IEEE.
Wymiar	Obudowa musi być przeznaczona do montażu w szafie rackowej 19”,
Zasilanie	• Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej, wymienialne w trakcie pracy urządzenia - hot-swap, redundancja zasilaczy 1+1. • Chłodzenie musi być realizowane przód/tył, redundantne moduły wentylatorów, wymienialne w trakcie pracy urządzenia.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta

Przełączniki dostępowe typu A - 1Gbps (17 szt.)

Komponent	Minimalne wymagania
Ilość portów	• Urządzenie musi posiadać minimum 24 porty 10/100/1000Mbps RJ-45 Base-T. • Urządzenie musi posiadać co najmniej 8 aktywnych portów 10GbE
Parametry wydajnościowe	Wydajność przełączania min. 200 gigapakietów na sekundę. Wydajność przekazywania pakietów min. 150 milionów pakietów na sekundę.
Funkcjonalność łączenia w stos	• Możliwość stackowania minimum 8 urządzeń. W przypadku dostarczenia urządzenia modularnego nie ma wymagania co do stackowania minimum 8 urządzeń wymagane jest natomiast zapewnienie rozbudowy do minimum 8 x 24 portów 10/100/1000Mbps i 8x 8 portów 10GbE . W przypadku przełączników modularnych do zapewnienia parametrów rozbudowy możliwe jest wykorzystanie więcej niż jednego przełącznika modularnego. • W przypadku urządzenia stackowalnego powinno mieć możliwość wykorzystania do stackowania modułów 10GbE lub równoważnych zapewniających przepustowość połączenia minimum 40Gbps w trybie full duplex, lub połączeń równoważnych zapewniających wymaganą przepustowość. • Obsługa trybu automatycznego przełączenia z aktywnego przełącznika master na jeden z pozostałych przełączników w grupie stack bez uruchamianie przełączników ponownie oraz bez utraty pakietów. • Możliwość dodania i usunięcia urządzenia ze stosu bez przerwy w

	jego działaniu.
Funkcjonalności warstwy L2	• Urządzenie musi obsługiwać min. 16000 adresów MAC oraz min. 4000 sieci VLAN. • Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad (LACP), min. 8 portów na jedno logiczne połączenie, min. 124 logicznych grup połączeń jednocześnie (w stosie). • Wsparcie dla RSTP oraz, 802.1s – Multiple Spanning Tree oraz PVST/PVST+/PVRST • Obsługa do 254 instancji STP • Wsparcie dla 802.1x • Wsparcie dla pakietów tzw. „Jumbo frames” (co najmniej 9000 bajtów) • Obsługa BPDU Guard, Root Guard • Obsługa mechanizmu GVRP • Obsługa IGMP snooping v1, v2 • Obsługa mechanizmu MAC Address Locking, Port Security. • Obsługa MLD Snooping (v1/v2). • Obsługa Multi-device Authentication. • Obsługa Mirroring - Port-based, ACL-based, MAC Filter-based, and VLAN-based. • Obsługa Port Loop Detection • Obsługa Private VLAN • Obsługa Protocol VLAN (802.1v), Subnet VLAN • Obsługa Single-instance Spanning Tree. • Obsługa Uni-Directional Link Detection (UDLD). • Obsługa VLAN Stacking (Q-in-Q)
Funkcjonalności warstwy L3	• Statyczny routing IPv4 i IPv6. • Sprzętowa obsługa do 12000 (IPv4) i 1000 (IPv6) wpisów routingu. • Wsparcie mechanizmu ECMP • Obsługa protokołu RIPv2 • Obsługa protokołu OSPFv2, OSPFv3 • Obsługa protokołu VRRP, VRRPv3 • Obsługa tuneli IPv6 over IPv4 • Obsługa VRF (IPv4 i IPv6) Jeśli funkcjonalności warstwy L3 wymagają licencji należy ją dostarczyć w ramach zamówienia.
Funkcje QoS	• Obsługa 6 kolejek QoS na jednym porcie fizycznym.

	• Zarządzanie polityką jakości ruchu – “QoS” w oparciu o algorytmy Weighted Round Robin (WRR) lub odpowiedni, Strict Priotity (SP) i ich kombinację. • Mapowanie za pomocą ACL do kolejki priorytetowej. • Mapowanie do kolejki priorytetowej na podstawie adresu MAC. • Limitowanie pasma na wejściu w oparciu o port, ACL. • Limitowanie pasma na wyjściu w oparciu o port, kolejkę. • Limitowanie pasma dla pakietów BUM (Broadcast, multicast i unknown unicast). • Obsługa DHCP Relay. • Obsługa Diffserv oraz DSCP/802.1p
Funkcje bezpieczeństwa	• Obsługa zarówno IPv4 ACL jak i IPv6 ACL. • Możliwość konfiguracji mirroringu w oparciu o dany port, listy ACL i MAC, oraz VLAN. • Obsługa Private Vlan. • Obsługa DHCP snooping • Obsługa Dynamic ARP inspection • Obsługa Authentication, Authorization, and Accounting • Wsparcie dla Advanced Encryption Standard (AES) i SSHv2 • Obsługa RADIUS/TACACS/TACACS+ • Obsługa Secure Copy (SCP) i Secure Shell (SSHv2) • Obsługa Change of Authorization (CoA) RFC 5176
Zgodność ze standardami	• RFC 783 TFTP • RFC 854 TELNET Client and Server • RFC 951 Bootp • RFC 1157 SNMPv1/v2c • RFC 1213 MIB-II • RFC 1493 Bridge MIB • RFC 1516 Repeater MIB • RFC 1573 SNMP MIB II • RFC 1643 Ethernet Interface MIB • RFC 1724 RIP v1/v2 MIB • RFC 1757 RMON MIB • RFC 2068 Embedded HTTP • RFC 2131 DHCP Server and DHCP Relay • RFC 2570 SNMPv3 Intro to Framework • RFC 2571 Architecture for Describing SNMP Framework

	• RFC 2572 SNMP Message Processing and Dispatching • RFC 2573 SNMPv3 Applications • RFC 2574 SNMPv3 User-based Security Model • RFC 2575 SNMP View-based Access Control Model SNMP • RFC 2818 Embedded HTTPS • RFC 3176 sFlow • 802.1D-2004 MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • 802.1x Port-based Network Access Control • 802.3 10Base-T • 802.3ab 1000Base-T • 802.3ad Link Aggregation (Dynamic and Static) • 802.3ae 10 Gigabit Ethernet • 802.3u 100Base-TX • 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.3az-2010 - IEEE • 802.1Q VLAN Tagging
Zarządzanie, zabezpieczenia	• Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (Ethernet RJ-45) • Obsługa SNMP2/SNMP3 oraz uwierzytelnianie poprzez TACACS/Radius. • Obsługa przez wbudowany serwer WWW • Obsługa DHCP Server • Obsługa NTP Network Time Protocol • Wsparcie dla protokołów OpenFlow v1.0 i v1.3 (SDN) • Obsługa 802.3az-2010 – IEEE
Wymiar	• Obudowa musi być przeznaczona do montażu w szafie rackowej 19”
Zasilanie	• Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej, wymienialne w trakcie pracy urządzenia - hot-swap, redundancja zasilaczy 1+1, możliwość zastosowania dodatkowego zewnętrznego zasilacza. • Chłodzenie musi być realizowane tył/przód, redundantne moduły

	wentylatorów, wymienialne w trakcie pracy urządzenia.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Przełączniki dostępowe typu B - 1Gbps (6 szt.)

Komponent	Minimalne wymagania
Ilość portów	• Urządzenie musi posiadać minimum 48 portów 10/100/1000Mbps RJ-45 Base-T. • Urządzenie musi posiadać co najmniej 8 aktywnych portów 10GbE
Parametry wydajnościowe	Wydajność przełączania min. 200 gigapakietów na sekundę. Wydajność przekazywania pakietów min. 150 milionów pakietów na sekundę.
Funkcjonalność łączenia w stos	• Możliwość stackowania minimum 8 urządzeń. W przypadku dostarczenia urządzenia modularnego nie ma wymagania co do stackowania minimum 8 urządzeń wymagane jest natomiast zapewnienie rozbudowy do minimum 8 x 24 portów 10/100/1000Mbps i 8x 8 portów 10GbE . W przypadku przełączników modularnych do zapewnienia parametrów rozbudowy możliwe jest wykorzystanie więcej niż jednego przełącznika modularnego. • W przypadku urządzenia stackowalnego powinno mieć możliwość wykorzystania do stackowania modułów 10GbE lub równoważnych zapewniających przepustowość połączenia minimum 40Gbps w trybie full duplex, lub połączeń równoważnych zapewniających wymaganą przepustowość. • Obsługa trybu automatycznego przełączenia z aktywnego przełącznika master na jeden z pozostałych przełączników w grupie stack bez uruchamianie przełączników ponownie oraz bez utraty pakietów. • Możliwość dodania i usunięcia urządzenia ze stosu bez przerwy w jego działaniu.
Funkcjonalności warstwy L2	• Urządzenie musi obsługiwać min. 16000 adresów MAC oraz min. 4000 sieci VLAN. • Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad (LACP), min. 8 portów na jedno logiczne połączenie, min. 124 logicznych grup połączeń jednocześnie (w stosie). • Wsparcie dla RSTP oraz, 802.1s – Multiple Spanning Tree oraz

	PVST/PVST+/PVRST • Obsługa do 254 instancji STP • Wsparcie dla 802.1x • Wsparcie dla pakietów tzw. „Jumbo frames” (co najmniej 9000 bajtów) • Obsługa BPDU Guard, Root Guard • Obsługa mechanizmu GVRP • Obsługa IGMP snooping v1, v2 • Obsługa mechanizmu MAC Address Locking, Port Security. • Obsługa MLD Snooping (v1/v2). • Obsługa Multi-device Authentication. • Obsługa Mirroring - Port-based, ACL-based, MAC Filter-based, and VLAN-based. • Obsługa Port Loop Detection • Obsługa Private VLAN • Obsługa Protocol VLAN (802.1v), Subnet VLAN • Obsługa Single-instance Spanning Tree. • Obsługa Uni-Directional Link Detection (UDLD). • Obsługa VLAN Stacking (Q-in-Q)
Funkcjonalności warstwy L3	• Statyczny routing IPv4 i IPv6. • Sprzętowa obsługa do 12000 (IPv4) i 1000 (IPv6) wpisów routingu. • Wsparcie mechanizmu ECMP • Obsługa protokołu RIPv2 • Obsługa protokołu OSPFv2, OSPFv3 • Obsługa protokołu VRRP, VRRPv3 • Obsługa tuneli IPv6 over IPv4 • Obsługa VRF (IPv4 i IPv6) Jeśli funkcjonalności warstwy L3 wymagają licencji należy ją dostarczyć w ramach zamówienia.
Funkcje QoS	• Obsługa 6 kolejek QoS na jednym porcie fizycznym. • Zarządzanie polityką jakości ruchu – “QoS” w oparciu o algorytmy Weighted Round Robin (WRR) lub odpowiedni, Strict Priotity (SP) i ich kombinację. • Mapowanie za pomocą ACL do kolejki priorytetowej. • Mapowanie do kolejki priorytetowej na podstawie adresu MAC. • Limitowanie pasma na wejściu w oparciu o port, ACL. • Limitowanie pasma na wyjściu w oparciu o port, kolejkę.

	• Limitowanie pasma dla pakietów BUM (Broadcast, multicast i unknown unicast). • Obsługa DHCP Relay. • Obsługa Diffserv oraz DSCP/802.1p
Funkcje bezpieczeństwa	• Obsługa zarówno IPv4 ACL jak i IPv6 ACL. • Możliwość konfiguracji mirroringu w oparciu o dany port, listy ACL i MAC, oraz VLAN. • Obsługa Private Vlan. • Obsługa DHCP snooping • Obsługa Dynamic ARP inspection • Obsługa Authentication, Authorization, and Accounting • Wsparcie dla Advanced Encryption Standard (AES) i SSHv2 • Obsługa RADIUS/TACACS/TACACS+ • Obsługa Secure Copy (SCP) i Secure Shell (SSHv2) • Obsługa Change of Authorization (CoA) RFC 5176
Zgodność ze standardami	• RFC 783 TFTP • RFC 854 TELNET Client and Server • RFC 951 Bootp • RFC 1157 SNMPv1/v2c • RFC 1213 MIB-II • RFC 1493 Bridge MIB • RFC 1516 Repeater MIB • RFC 1573 SNMP MIB II • RFC 1643 Ethernet Interface MIB • RFC 1724 RIP v1/v2 MIB • RFC 1757 RMON MIB • RFC 2068 Embedded HTTP • RFC 2131 DHCP Server and DHCP Relay • RFC 2570 SNMPv3 Intro to Framework • RFC 2571 Architecture for Describing SNMP Framework • RFC 2572 SNMP Message Processing and Dispatching • RFC 2573 SNMPv3 Applications • RFC 2574 SNMPv3 User-based Security Model • RFC 2575 SNMP View-based Access Control Model SNMP • RFC 2818 Embedded HTTPS • RFC 3176 sFlow

	• 802.1D-2004 MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • 802.1x Port-based Network Access Control • 802.3 10Base-T • 802.3ab 1000Base-T • 802.3ad Link Aggregation (Dynamic and Static) • 802.3ae 10 Gigabit Ethernet • 802.3u 100Base-TX • 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.3az-2010 - IEEE • 802.1Q VLAN Tagging
Zarządzanie, zabezpieczenia	• Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (Ethernet RJ-45) • Obsługa SNMP2/SNMP3 oraz uwierzytelnianie poprzez TACACS/Radius. • Obsługa przez wbudowany serwer WWW • Obsługa DHCP Server • Obsługa NTP Network Time Protocol • Wsparcie dla protokołów OpenFlow v1.0 i v1.3 (SDN) • Obsługa 802.3az-2010 – IEEE
Wymiar	• Obudowa musi być przeznaczona do montażu w szafie rackowej 19”
Zasilanie	• Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej, wymienialne w trakcie pracy urządzenia - hot-swap, redundancja zasilaczy 1+1, możliwość zastosowania dodatkowego zewnętrznego zasilacza. • Chłodzenie musi być realizowane tył/przód, redundantne moduły wentylatorów, wymienialne w trakcie pracy urządzenia.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

Klastry wirtualizacyjne – do rozbudowy istniejącego środowiska Zamawiającego

W celu uruchomienia infrastruktury OpenStack oraz środowiska usługowego WIŁ i umożliwieniu integracji oraz wspólnego zarządzania z posiadanym przez Wojskowy Instytut Łączności Oprogramowaniem VMWare vSphere 5.x wymagane jest dostarczenie:

- 12 licencji procesorowych oprogramowania wirtualizacyjnego VMWare vSphere Standard z 60 miesięcznym wsparciem producenta na poziomie basic.
- 2 licencji vCenter Server Standard z 60 miesięcznym wsparciem producenta na poziomie basic.

Oprogramowanie backup

Lp.	**Wymaganie minimalne**
1	Oprogramowanie powinno współpracować z infrastrukturą wirtualizacji opartą na VMware ESX oraz ESXi w wersjach 3.5, 4.0, 4.1, 5, 5.1 oraz 5.5, jak również Hyper-V 2008 R2, 2012, 2012 R2 (w tym obsługa formatu dysków wirtualnych *.vhdx).
2	Rozwiązanie powinno współpracować z hostami ESX i ESXi zarządzanymi przez VMware vCenter jak i hostami niezarządzanymi (standalone).
3	Rozwiązanie powinno współpracować z hostami Hyper-V zarządzanymi przez System Center Virtual Machine Manager, zgrupowanymi w klastry jak i niezarządzanymi (standalone).
4	Rozwiązanie nie może instalować żadnych swoich komponentów (agent) w archiwizowanych maszynach wirtualnych.
5	Rozwiązanie musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez VMware i Hyper-V.
6	Rozwiązanie powinno mieć możliwość instalacji na następujących systemach operacyjnych: Microsoft Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2
7	Rozwiązanie powinno dawać możliwość odzyskiwania całych obrazów maszyn wirtualnych z obrazów, pojedynczych plików z systemu plików znajdujących się wewnątrz wirtualnej maszyny. Rozwiązanie musi umożliwiać odzyskanie plików i/lub całych maszyn wirtualnych na zasadzie „one-click restore”. Rozwiązanie musi umożliwiać odzyskiwanie plików z następujących systemów plików: Linux ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS BSD UFS, UFS2 Solaris ZFS Mac

	HFS, HFS+ Windows NTFS, FAT, FAT32, ReFS
8	Rozwiązanie powinno umożliwiać natychmiastowe odzyskanie wirtualnej maszyny i jej uruchomienie bez kopiowania na zasoby dyskowe podłączone do hostów ESX (wbudowana funkcjonalność NFS Server) i Hyper-V.
9	Rozwiązanie powinno umożliwiać odzyskiwanie bezpośrednie odzyskiwanie obiektów z takich usług jak Active Directory (użytkownicy i grupy), Microsoft SharePoint (dokumenty) i Microsoft SQL (tabele i rekordy) z maszyn wirtualnych środowiska VMware i Hyper-V.
10	Rozwiązanie musi zapewniać szybkie odzyskiwanie danych z witryn Microsoft SharePoint 2010/2013 bez potrzeby uruchamiania maszyny wirtualnej (odzyskiwanie bezpośrednio z bazy danych *.MDF).
11	Rozwiązanie powinno umożliwiać indeksowanie plików zawartych w archiwach maszyn wirtualnych z systemem operacyjnym Windows w celu szybkiego ich przeszukiwania.
12	Rozwiązanie powinno umożliwiać równoczesne przetwarzanie wielu maszyn wirtualnych
13	Rozwiązanie powinno w pełni korzystać z mechanizmów zawartych w VMware vStorage API for Data Protection a w szczególności być zgodnym z mechanizmem Changed Block Tracking.
14	Rozwiązanie powinno umożliwiać wykorzystanie technologii CBT dla platformy VMware również dla maszyn wirtualnych, które posiadają już migawkę.
15	Rozwiązanie powinno mieć wbudowane mechanizmy podobne do technologii CBT również dla platformy Hyper-V w celu przyśpieszenia procesu backupu.
16	Rozwiązanie powinno korzystać z mechanizmów VSS (Volume Shadow Copy Service) wbudowanych w najnowsze systemy operacyjne z rodziny Windows.
17	Rozwiązanie powinno mieć wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej.
18	Rozwiązanie powinno mieć możliwość archiwizacji na napędach taśmowych
19	Rozwiązanie powinno mieć możliwość instalacji centralnej konsoli do zarządzania większą ilością serwerów archiwizujących oraz jednoczesnego zarządzania backupami środowiska VMware i Hyper-V.
20	Rozwiązanie powinno mieć wbudowany mechanizm informowania o pomyślnym lub niepomyślnym zakończeniu procesu archiwizacji poprzez email, zapis do Event Log'u Windows lub wysłanie komunikatu SNMP.
21	Rozwiązanie powinno mieć możliwość rozbudowy procesu archiwizacji o dowolne skrypty tworzone przez administratora i dołączane do zadań archiwizacyjnych.
22	Rozwiązanie powinno mieć wbudowaną możliwość replikacji wirtualnych maszyn pomiędzy hostami ESX i ESXi w tym możliwość replikacji ciągłej
23	Rozwiązanie powinno mieć wbudowaną możliwość replikacji maszyn wirtualnych pomiędzy hostami Hyper-V w tym możliwość replikacji ciągłej.
24	Rozwiązanie powinno mieć możliwość tworzenia środowiska wirtualnego laboratorium w środowisku VMware lub Hyper-V.
25	Rozwiązanie powinno mieć możliwość tworzenia środowiska wirtualnego laboratorium dla

	zreplikowanego środowiska VMware.
26	Rozwiązanie powinno zapewnić możliwość sprawdzenia poprawności wykonania archiwum poprzez odtworzenie wirtualnej maszyny w izolowanym środowisku i jej uruchomienie w środowisku VMware lub Hyper-V.
27	Rozwiązanie powinno zapewnić możliwość sprawdzenia poprawności wykonania replikacji poprzez odtworzenie wirtualnej maszyny w izolowanym środowisku i jej uruchomienie w środowisku VMware.
28	Rozwiązanie powinno być zgodne z konfiguracją rozproszonego przełącznika VMware (Distributed Virtual Switch).
29	Rozwiązanie powinno mieć możliwość integracji z środowiskiem VMware vCloud Director a w szczególności możliwość archiwizacji metadanych vCD i atrybutów vApps oraz odzyskiwanie tych elementów bezpośrednio do vCD.
30	Rozwiązanie powinno umożliwiać przedstawienie informacji o archiwizacji środowiska VMware bezpośrednio w webowym kliencie vSphere
31	Rozwiązanie powinno mieć możliwość automatycznej zmiany numeracji IP maszyn przywracanych w środowiskach centrum zapasowego w przypadku awarii centrum podstawowego.
32	Rozwiązanie musi umożliwiać zapisanie konfiguracji całej instalacji w celu przywrócenia jej po reinstalacji całego systemu.
33	Rozwiązanie powinno mieć możliwość dodatkowego skopiowania punktów przywracania do innej lokalizacji.
34	Rozwiązanie powinno mieć możliwość wykonywania archiwizacji zgodnie z rotacyjnym schematem GFS (grandfather-father-son).
35	Rozwiązanie powinno mieć możliwość kopiowania archiwum do zdalnej lokalizacji przy pomocy technologii opartej na akceleracji WAN.
36	Licencjonowanie: Musi zapewniać możliwość obsługi środowiska Zamawiającego zawierającego: • 6 fizycznych procesorów • Przestrzeń dyskowa całkowita: 25 dysków 900 GB, 1 napęd biblioteki taśmowej

Biblioteka taśmowa

Komponent	Minimalne wymagania
Obudowa	- Oferowana biblioteka taśmowa musi być przystosowana do

	montażu w standardowej szafie typu rack 19” - Urządzenie należy dostarczyć z niezbędnymi elementami do zamontowania w szafie typu rack 19”
Rodzaj napędu	LTO 6 typu „Hot-Plug” Min. przepustowość natywna/ z kompresją - 160/ 400 MB/s Min. pojemność taśmy natywna/ z kompresją – 2500/ 6250 GB
Liczba napędów	1
Interfejs napędu	Native Fibre Channel min. 8Gbs
Interace biblioteki	Fibre Channel min. 8Gbs
Liczba slotów (miejsc na tasiemki w magazynku	- Minimum 24 szt. - Możliwość zdefiniowania min. 2 slotów Import Export (Mail slot) - Czytnik kodów kreskowych
Możliwości rozbudowy	- Możliwość rozbudowy do 2 napędów LTO6 oraz 40 slotów na taśmy - Robot powinien mieć możliwość dostępu do wszystkich oferowanych slotów biblioteki - Możliwość instalacji napędów ze złączem FC
Zarządzanie	- Poprzez przeglądarkę WWW (przez wbudowany port Ethernet), - Obsługa za pomocą panelu umieszczonego z przodu biblioteki
Taśmy	• Min. 12 taśm do wielokrotnego zapisu o pojemności min.2500 GB bez kompresji danych • Min. 1 taśma czyszcząca
Okres gwarancji	Gwarancja producenta 60 miesięcy z czasem reakcji w następnym dniu roboczym (NBD). Zgłaszanie awarii w trybie 5x8.

Licencje Windows – do rozbudowy istniejącego środowiska Zamawiającego

Dostawa niewyłącznych, nieograniczonych czasowo licencji oprogramowania

a) Microsoft Windows Server Standard 2012 R2 GOV OLP NL 2proc (licencja rządowa) – 8 szt.
Microsoft Windows Server CAL 2012 GOV OLP NL User CAL (licencja rządowa)– 200 szt.

Licencje Exchange – do rozbudowy istniejącego środowiska Zamawiającego

Dostawa niewyłącznych, nieograniczonych czasowo licencji oprogramowania

a) Microsoft Exchange Server Standard 2013(lub nowszy) OLP NL GOV (licencja rządowa) – 2 szt.
b) Microsoft Exchange Standard CAL 2013 (lub nowszy) OLP NL GOV User CAL dla 200 jednoczesnych użytkowników (licencja rządowa) – 200 szt.

Urządzenia typu Firewall/UTM (klaster)

Komponent	Minimalne wymagania
Architektura systemu ochrony	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Wysoka dostępność	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive. **W ramach postępowania system powinien zostać dostarczony w postaci klastra wysoko dostępnego.**
Zasilanie	Redundantne zasilacze. Zasilanie z sieci 230V/50Hz.
Monitoring	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN.
Tryb pracy	System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
Interfejsy fizyczne	System realizujący funkcję Firewall powinien dysponować minimum 6 portami Ethernet 10/100/1000 Base-TX oraz 4 gniazdami SFP 1Gbps z wkładkami 1000 Base SX.
Interfejsy wirtualne	System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
Wydajność firewall	W zakresie Firewall'a obsługa nie mniej niż 5 milionów jednoczesnych połączeń oraz 200 tys. nowych połączeń na sekundę, i przepustowością Firewall'a: nie mniej niż 8 Gbps dla pakietów 512bajtów.
Wydajność VPN	Wydajność szyfrowania VPN IPSec: nie mniej niż 7 Gbps
Logowanie lub raportowanie	1) System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze lub producenci poszczególnych elementów systemu muszą oferować systemy logowania i raportowania w postaci odpowiednio zabezpieczonych platform sprzętowych lub programowych
Funkcjonalność systemu	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection • Ochrona przed wirusami – co najmniej dla protokołów SMTP,

	POP3, IMAP, HTTP, FTP, HTTPS • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN • Ochrona przed atakami - Intrusion Prevention System • Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. • Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP • Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P • system powinien rozpoznawać ruch botnet (komunikacja z C&C - może być rozpoznawana z wykorzystaniem różnych modułów) • Możliwość analizy ruchu szyfrowanego protokołem SSL • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
Klient VPN	W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
Routing	Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
Wirtualne instancje	Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a, IPS'a.
NAT	Translacja adresów NAT adresu źródłowego i docelowego.
Reguły firewall	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
Strefy bezpieczeństwa	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
Silnik antywirusowy	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
System IPS	Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 4500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.
Kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na

	wartościach portów TCP/UDP
Filtracja WWW	Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
Aktualizacje	Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych.
Autentykacja	System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: •Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu •haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP •haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych •Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
Certyfikacje	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: •ICSA lub EAL4 dla funkcji Firewall
Zarządzanie	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 5 lat.
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, realizowanym w miejscu instalacji sprzętu, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent powinien gwarantować czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz możliwość zgłaszania awarii w trybie 5x8 do polskojęzycznej obsługi producenta.

4. OPIS WDROŻENIA

Instalacja całości rozwiązania odbędzie się na podstawie projektu wykonawczego opracowanego w trybie roboczym przez Wykonawcę w uzgodnieniu z Zamawiającym w trakcie warsztatów inicjujących projekt, warsztaty te mają odbywać się w siedzibie zamawiającego i trwać od 5 do 7 dni roboczych. Projekt wykonawczy powinien zawierać w szczególności dokładny plan rozmieszczenia elementów środowiska w serwerowni CyberSecLab wraz z zaplanowaniem rozmieszczenia urządzeń w poszczególnych szafach.

Wykonawca zobowiązany jest w szczególności do:

1) opracowania niezbędnych projektów wdrożeniowych,
2) dostawy, instalacji i uruchomienia wszystkich elementów składowych środowiska,
3) wykonania niezbędnych instalacji technicznych,
4) dostarczenia dokumentacji powykonawczej,
5) przeszkolenia pracowników Zamawiającego w zakresie obsługi dostarczanej infrastruktury,
6) bieżącej obsługi serwisowej wszystkich dostarczanych elementów klastra obliczeniowego wraz z techniczną infrastrukturą towarzyszącą.

Każdy z projektów wdrożeniowych przedstawionych przez Wykonawcę do realizacji wymaga wcześniejszego uzgodnienia z Zamawiającym. Procedura uzgodnienia projektów nie pociąga za sobą żadnych skutków w postaci przeniesienia na Zamawiającego jakiejkolwiek odpowiedzialności za projekty.

Wszystkie projekty muszą uwzględniać wszelkie ograniczenia, jakie wynikają z lokalizacji i działania już istniejących w budynku instalacji technicznych.

Wykonawca najpóźniej w dniu podpisania protokołu odbioru przeniesie na Zamawiającego autorskie prawa majątkowe do projektów i dokumentacji powykonawczej, wraz z zezwoleniem na wykonywanie zależnych praw autorskich.

Wykonawca zobowiązany jest przeprowadzić wszelkie prace wdrożeniowe tak, aby zapewnić właściwe i ciągłe działanie nie tylko dostarczanego środowiska CyberSecLab wraz z techniczną infrastrukturą towarzyszącą, ale również aktualnie eksploatowanych systemów w miejscu instalacji przedmiotu zamówienia.

Obowiązkiem Wykonawcy jest dokonanie naprawy wszelkich uszkodzeń, które wynikły w trakcie realizacji przedmiotu zamówienia oraz przywrócenie właściwego stanu obiektu.

Obowiązkiem Wykonawcy jest usunięcie wszelkich elementów pozostałych po procesie instalacji, takich jak: opakowania, resztki materiału, etc.

Wykonawca zobowiązany jest dostarczyć Zamawiającemu propozycję harmonogramu wdrożenia w terminie do jednego tygodnia od daty podpisania umowy, a projektu wykonawczego w terminie do 2 tygodni od daty podpisania umowy. Ostateczny harmonogram prac oraz projekt wykonawczy zostaną uzgodnione z Zamawiającym w trybie roboczym.

4.1. Opis wdrożenia OpenStack i CEPH

W ramach wdrożenia OpenStack należy zaprojektować i wdrożyć pełną infrastrukturę OpenStack (wszystkie usługi) w architekturze wysoko dostępnej (o ile realizacja danej usługi to umożliwia) tj.:

- Horizon
- Nova

- Neutron
- Swift
- Cinder
- Glance
- Keystone
- Ceilometer.

Funkcje storage Openstack muszą być oparte na klastrze CEPH 4 serwerów storage opisanych w zadaniu nr 2.

W ramach realizacji funkcji sieciowych musi zostać zintegrowany oferowany kontroler SDN.

W zakresie wdrożenia znajduje się również przygotowanie przez Wykonawcę gotowych do wydawania w ramach architektury OpenStack szablonów dla systemów operacyjnych, minimum:

- Windows XP
- Windows XP 64-bit Edition
- Windows Server 2003
- Windows XP Professional x64 Edition
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows Server 2012
- Windows 8
- Windows 8.1
- Windows Server 2012 R2
- Windows 10
- Ubuntu 15.04 (Vivid Vervet)
- Ubuntu 14.10 (Utopic Unicorn)
- Ubuntu 14.04.2 LTS (Trusty Tahr)
- Ubuntu 12.04.5 LTS (Precise Pangolin)
- Ubuntu 10.04.4 LTS (Lucid Lynx)
- CentOS 7
- CentOS 6
- CentOS 5
- NetBSD 6.1.5
- FreeBSD 10.1
- FreeBSD 9.3
- FreeBSD 8.4
- Debian 8
- Debian 7
- Debian 6
- OpenSUSE 13.2
- OpenSUSE 12.3
- OpenSUSE 11.4
- Scientific Linux 5
- Scientific Linux 6
- Scientific Linux 7.

Szczegółowy zakres wdrożenia oraz architekturę systemu Wykonawca opracuje podczas warsztatów inicjujących projekt.

Wykonawca sporządzi dokumentację tworzenia i wydawania systemów operacyjnych w ramach architektury OpenStack.

4.2. Opis wdrożenia środowiska usługowego WIŁ

W ramach wdrożenia należy zaprojektować:

- Instalację, konfigurację i uruchomienie nowych przełączników sieci LAN dostarczanych w ramach postępowania we wskazanych przez Zamawiającego punktach dystrybucyjnych
- Instalację, konfigurację i uruchomienie przełączników rdzeniowych dla sieci LAN oraz zaplanowanie i zaimplementowanie planu adresacji IP oraz segmentacji sieci na VLAN-y
- Instalację i konfigurację klastra urządzeń UTM do środowiska WIŁ i wystawienie obecnie działających usług do Internetu za pomocą tych urządzeń.
- Wirtualizację i aktualizację kontrolerów do najnowszej dostarczanej w ramach postępowania licencji serwerowej.
- Wirtualizacja i aktualizacja serwerów:
    - Windows Server 2003, Symfonia Premium, baza pervasive v9
    - Windows Server 2008 – S.C., CA, SQL Server 2008, Symfonia Kadry i Płace
    - Windows Server 2003 - DHCP
    - Windows Server 2003 IIS
    - Fedora 8.
- Aktualizacja Exchange 2007 do najnowszej dostępnej wersji systemu pocztowego dostarczanego w ramach tego postepowania wraz z automatyczną migracją danych (bez reformatowania), automatyczna rekonfiguracja klientów pocztowych Outlook do pracy z nowym systemem.
- Konfiguracja posiadanego przez Zamawiającego systemu Barracuda Spam & Virus Firewall do współpracy ze zmodyfikowanym systemem pocztowym.
- Migracja wszystkich komputerów biznesowych WIŁ do jednej domeny zarządzania realizowanej przez oprogramowanie serwerowe.
- Uruchomienie w ramach struktury sieciowej usług DHCP oraz dynamicznego DNS.
- Uruchomienie Centrum certyfikacji i automatyczne wydanie certyfikatów dla wszystkich komputerów na potrzeby autoryzacji 802.1x.
- Uruchomienie na przełącznikach sieciowych implementacji 802.1x i włączenie polityk dostępowych.
- Konfiguracja automatycznego mechanizmu wymuszającego stosowanie zasad Polityki Bezpieczeństwa Informacji.

5. PROCEDURA ODBIORU

5.1. Odbiór środowiska CyberSecLab

Zamawiający ma prawo żądać od Wykonawcy uruchomienia dowolnej funkcji wchodzącej w skład wdrożenia oraz ma prawo żądać sprawdzenia dowolnego parametru/specyfikacji sprzętu podlegającego wdrożeniu.

5.2. Odbiór licencji oprogramowania

- Dostawa oprogramowania systemowego będzie potwierdzana przez Zamawiającego Protokołem Odbioru w dniu przekazania Zamawiającemu poszczególnych pakietów oprogramowania.
- Protokół Odbioru musi potwierdzać dostawę oprogramowania spełniającego wymagania niniejszego postępowania oraz zawierać jego dane identyfikacyjne, w tym numery seryjne lub kody licencyjne.
- W przypadku kiedy dostarczany jest pakiet oprogramowania zawierający zestaw różnych produktów, wymagane jest dostarczenie szczegółowej listy składowego oprogramowania dołączonej do protokołu odbioru.

5.3. Odbiór dokumentacji powykonawczej

Wymagane jest dostarczenie edytowalnego dokumentu w jednym z formatów CSV/XLS/XLSX/ODS, zawierającego zestawienie konfiguracji sprzętowej każdego z serwerów oraz przełączników sieciowych. Konkretny format zostanie uzgodniony z Zamawiającym na etapie wdrożenia.

Wymagane jest dostarczenie w postaci edytowalnego schematu wektorowego w formacie SVG:

- topologii połączeń każdej sieci Ethernet,
- szczegółowego schematu lokalizacji wszystkich urządzeń w szafach rack,
- schematu lokalizacji wszystkich dostarczanych urządzeń,
- ustawionych na podłodze technicznej w serwerowni.

Wymagane jest dostarczenie w formacie elektronicznym, umożliwiającym przeszukiwanie tekstu: dokumentacji technicznej, procedur eksploatacyjnych i serwisowych dla każdego z dostarczanych urządzeń.

5.4. Szkolenia

Wymagane jest przeprowadzenie niżej wymienionych szkoleń w siedzibie Zamawiającego:

w zakresie obsługi dostarczanego środowiska CyberSecLab dla maksymalnie 10 osób w wymiarze 40 godzin, w języku polskim.

Szczegółowy program oraz termin szkoleń zostanie ustalony z Zamawiającym.

Szkolenia muszą obejmować wszystkie aspekty zarządzania dostarczoną infrastrukturą niezbędne do utrzymania jej produkcyjnego działania, wraz z potencjalnymi możliwymi modyfikacjami związanymi z obsługą serwisową.

6. GWARANCJA I WARUNKI WSPARCIA TECHNICZNEGO

- Na dostarczony przedmiot zamówienia Wykonawca udzieli Zamawiającemu gwarancji na okres minimum 60 miesięcy.
- Gwarancja rozpoczyna swój bieg od daty podpisania bez zastrzeżeń Protokołu Odbioru Końcowego przedmiotu zamówienia przez strony Umowy.
- Wszelkie koszty naprawy, w tym koszt transportu, instalacji i uruchomienia przedmiotu zamówienia ponosi Wykonawca.
- Serwis gwarancyjny będzie realizowany przez autoryzowany przez producenta podmiot lub bezpośrednio przez producenta.
- W okresie trwania gwarancji Wykonawca zobowiązuje się do nieodpłatnego udzielania Zamawiającemu konsultacji i pomocy technicznej, w zakresie działania przedmiotu zamówienia. Odpowiedź na każde zapytanie musi zostać udzielona Zamawiającemu drogą elektroniczną lub telefonicznie w ciągu 7 dni roboczych.
- Wykonawca zobowiązany jest do świadczenia usług serwisu gwarancyjnego dla przedmiotu zamówienia na każde zgłoszenie serwisowe Zamawiającego.
- Formalne potwierdzenie Zgłoszenia Serwisowego stanowi zgłoszenie przesłane przez Zamawiającego do Wykonawcy na adres email lub fax, wskazany w umowie.
- W okresie gwarancji zgłoszenia o awariach, wadach, usterkach przedmiotu umowy przyjmowane będą przez Wykonawcę lub producenta minimum od godziny 9:00 do 17:00, przez 5 dni roboczych w tygodniu.
- Termin naprawy biegnie od momentu wysłania zgłoszenia.
- Wymagany czas usunięcia wady, awarii lub usterki sprzętu, wynosi maksymalnie 14 dni kalendarzowych. W szczególnych przypadkach Zamawiający może zdecydować o przedłużeniu czasu

naprawy danego elementu. W takim wypadku kary umowne zostaną naliczone dopiero od momentu przekroczenia wydłużonego terminu naprawy.

- W przypadku braku możliwości technicznych wykonania naprawy niesprawnego przedmiotu zamówienia Wykonawca zobowiązuje się w terminie 30 dni do dostarczenia Zamawiającemu kompatybilnego rozwiązania wolnego od wad, o parametrach wydajnościowych i funkcjonalnych takich samych lub wyższych od niesprawnego.
- Wykonawca jest zobowiązany do odbioru i utylizacji uszkodzonych elementów podlegających wymianie, chyba że Zamawiający zdecyduje inaczej informując o tym Wykonawcę.
- Wykonawca zobowiązuje się do prowadzenia rejestru interwencji serwisowych i dostarczania Zamawiającemu po każdych sześciu miesiącach rejestru zawierającego liczbę interwencji, czas naprawy, specyfikację naprawianego sprzętu, wymienione lub naprawione podzespoły. Rejestr będzie podlegał weryfikacji przez Zamawiającego. W przypadku stwierdzenia nieprawidłowości w zapisach Zamawiający zwraca rejestr Wykonawcy w celu uzupełnienia/poprawienia.
- Zamawiający rezerwuje sobie prawo do dodawania nowych komponentów (sprzętowych i programowych) dowolnych producentów oraz wymiany zainstalowanych komponentów samodzielnie lub z pomocą Wykonawcy, bez utraty gwarancji na zakupiony sprzęt, przy zachowaniu pełnej kompatybilności. Zamawiający będzie dokonywał dodawania i/lub wymiany podzespołów samodzielnie po wcześniejszej konsultacji z Wykonawcą.
- W okresie gwarancji Wykonawca zobowiązany jest, bez dodatkowego wynagrodzenia, udostępniać Zamawiającemu nowe wersje firmware'ów, sterowników, oprogramowania zarządzającego oraz uaktualnień innego oprogramowania będącego przedmiotem zamówienia. W przypadku, gdy dostęp do aktualizacji wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu te informacje. Zamawiający będzie dokonywał aktualizacji oprogramowania samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. Jeżeli Wykonawca nie udzieli zgody na samodzielną aktualizację przez Zamawiającego, wówczas jest obowiązany sam dokonać takiej aktualizacji w terminie 7 dni od przyjęcia zgłoszenia od Zamawiającego.
- Zamawiający nie jest zobowiązany do instalacji wszystkich dostępnych aktualizacji oprogramowania. Niewykonanie aktualizacji oprogramowania przez Zamawiającego nie zwalnia Wykonawcy z obowiązku świadczenia gwarancji.
- Wykonawca zobowiązuje się do świadczenia usług serwisu gwarancyjnego z należytą starannością z uwzględnieniem ogólnie przyjętych i stosowanych standardów i procedur przy tego rodzaju usługach a także zaleceń i/lub procedur określonych przez producentów przedmiotu zamówienia.