Załącznik nr 1a – *szczegółowy opis przedmiotu zamówienia*

Szczegółowy opis przedmiotu zamówienia

Część I

Dostawa:

Przełącznik dostępowy – 2 sztuki		
1.	Wymagania ogólne	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
2.	Wymagane parametry fizyczne	Wymagane parametry fizyczne a) możliwość montażu w szafie 19” b) jeden wewnętrzny zasilacze 230V AC typu hot-swap. Z możliwością dołożenia dodatkowe zasilacza o tych samych parametrach. (nie dopuszcza się rozwiązań zewnętrznych zasilaczy) c) port USB umożliwiający podłączenie zewnętrznej pamięci flash
3.	Wymagana konfiguracja portów	Przełącznik musi posiadać minimum: • Minimum 8 portów 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 8 jednostek w stosie c) Magistrala statkująca o wydajności 80Gb/s d) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie e) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.

5.	Matryca przełączająca	Matryca przełączająca o wydajności min. 240 Gbps, wydajność przełączania przynajmniej 208 Mpps.
		Obsługa min 16 000 adresów MAC
		Wbudowana pamięć RAM min. 1 GB
		Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB
		Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
		Obsługa ramek jumbo o wielkości min. 9 216 bajtów
		Obsługa protokołu GVRP lub równoważny
		Wsparcie dla protokołów: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu. • Ethernet Ring Protection version 2
		Obsługa min. 256 tras dla routingu IPv4
		Obsługa min. 128 tras dla routingu IPv6
		Obsługa protokołów routingu minimum: • IPv4: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów). • IPv6: minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów).
		Obsługa protokołów LLDP i LLDP-MED
		Przełącznik musi posiadać funkcjonalność DHCP Server
		Obsługa ruchu multicast: • IGMP Snooping v1, v2 i v3
		Obsługa mechanizmu DHCP snooping
6.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci	a) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL

		b) Możliwość uwierzytelnia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal. c) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP d) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny),
7.	Wymagania fukcjonalne	Implementacja co najmniej 4 kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: ● klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
8.	Protokoły	Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3.
9.	Wymagane opcje zarządzania	a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), c) urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, d) dedykowany port konsoli zgodny ze standardem RS-232, e) Obsługa skryptów BASH oraz Python f) Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
10.	Dokumentacja	Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim, b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
11.	Ogólne	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z

		wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
		Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.
12.	Gwarancja	Przełącznik być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła przełącznik spełniający minimalne parametry techniczne wskazane w niniejszym dokumencie

Przełącznik agregacyjny – 2szt.		
1.	Wymagania ogólne	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
2.	Wymagane parametry fizyczne	Wymagane parametry fizyczne d) możliwość montażu w szafie 19” e) jeden wewnętrzny zasilacze 230V AC f) port USB umożliwiający podłączenie zewnętrznej pamięci flash g) Urządzenie musi cechować się bezwiatrakową obudową (chłodzenie pasywne)
3.	Wymagana konfiguracja portów	Przełącznik musi posiadać minimum: • 48 portów gigabitowych w standardzie 100/1000BaseT • Minimum 2 porty typu COMBO 1Gb SFP/RJ45 • Minimum 2 porty typu 10Gb SFP+ Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: g) Zarządzanie stosem poprzez jeden adres IP h) Do min. 4 jednostek w stosie

		i) Magistrala statkująca o wydajności 40 Gb/s j) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie k) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree l) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów statkujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą (dwóch dodatkowych niezależnych od portów podstawowych) portów SFP+ w takim wypadku wymagane jest aby z przełącznikiem musi być dostarczony kabel do stackowania 10GE SFP+ od długości minimum 1m. UWAGA: Przełącznik powinien wspierać tzw. in-service software upgrade (ISSU) czyli aktualizację przełączników w stosie bez przerwania pracy całego stosu przełączników
5.	**Matryca przełączająca**	
	Matryca przełączająca o wydajności min. 140 Gbps	
	Obsługa min 16 000 adresów MAC	
	Wbudowana pamięć RAM min. 1 GB	
	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB	
	Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)	
	Obsługa ramek jumbo o wielkości min. 9 216 bajtów	
	Obsługa protokołu GVRP lub równoważny	
	Wsparcie dla protokołów: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu.	
	Obsługa min. 64 tras dla routingu IPv4	
	Obsługa min. 32 tras dla routingu IPv6	

	Obsługa protokołów routingu minimum: • IPv4: minimum: statyczny • IPv6: minimum: statyczny	
	Obsługa protokołów LLDP i LLDP-MED	
	Przełącznik musi posiadać funkcjonalność DHCP Server	
	Obsługa ruchu multicast: IGMP Snooping v1, v2 i v3 Obsługa 1000 grup multicast	
	Obsługa mechanizmu DHCP snooping Obsługa mechanizmu ARP spoof protection	
6.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: • min. 4 poziomy dostępu administracyjnego poprzez konsolę • autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL • możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www • zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 • możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP • obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny), • Możliwość uwierzytelnia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal.
7.	Wymagane opcje zarządzania	• możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, • plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), • urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, • dedykowany port konsoli zgodny ze standardem RS-232, • Obsługa skryptów BASH oraz Python

		• Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
8.	Wraz z urządzeniami muszą zostać dostarczone: • pełna dokumentacja w języku polskim lub angielskim, • dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.	
9.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.	
10.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.	
11.	Zamawiający wymaga, aby przełącznik posiadał gwarancje typu limited lifetime tj. serwis gwarancyjny na sprzęt – wymiana po odesłaniu uszkodzonego sprzętu do producenta w okresie 5 lat po zakończeniu sprzedaży modelu.	

Kabel do tworzenia stosu – 2 sztuki		
1.	Wymagania ogólne	1 metr 20 Gibabit QSFP+
Wkładka jednomodowa SFP+ – 20 sztuki		
1.	Wymagania ogólne	SFP +; SM LC; 6,2dB, zasięg 10 KM

Oprogramowanie do zarządzania siecią przewodową w/w urządzeń

Architektura i zarządzanie

1. Dedykowane oprogramowanie służące do zarządzania i monitorowania pracy wszystkimi przełącznikami opisanymi w tym zamówieniu. Należy zapewnić licencję na obsługę min. 20 aktywnych urządzeń sieciowych (przełączniki)
2. System Zarządzania i Monitoringu musi być tego samego producenta co urządzania LAN
3. Oprogramowanie musi mieć możliwość instalacji w środowisku wirtualnym Vmware, Hyper-V i KVM
4. Obsługa musi być możliwa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW
5. Oprogramowanie musi pracować w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego miejsca w sieci (po uzyskaniu odpowiednich uprawnień),
6. Funkcja definiowania poziomu dostępu dla administratorów (wymagana jest możliwość profilowania kont administratorskich a użytkownikami Active Directory) z przypisanymi:

a.Rolami
b.Segmentami sieci, do których uzyskuje się dostęp

7. Oprogramowanie musi umożliwiać zbieranie statystyk w wykorzystaniem SNMP;
8. Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania.
9. Możliwość podglądu obecnej aktywnej konfiguracji z konfiguracją aktywną w zadanym historycznym momencie z podglądem elementów: dodanych, usuniętych, zmienionych względem danych konfiguracji.
10. Możliwość wysyłania alarmów mailem i SMS'em w przypadku wystąpienia zdarzeń określonych jako krytyczne
11. Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta
12. Lokalizowanie użytkowników po adresie nazwie sieciowej użytkownika, IP oraz MAC
13. Oprogramowanie musi posiadać narzędzia do automatycznego wykrywania urządzeń sieciowych instalowanych w sieci,
14. Oprogramowanie musi umożliwiać aktualizację oprogramowania w urządzeniach sieciowych,
15. Oprogramowanie musi posiadać narzędzia pozwalające na:
    a.graficzną prezentację topologii sieci, w tym również graficzną, prezentację/budowę serwerowni lub dowolnego węzła sieciowego
    b.konfigurację i monitoring sieci VLAN,
    c.lokalizację oraz uzyskanie informacji o aktywności urządzeń w sieci,
16. Obrazowanie sieci w postaci mapki w tym lokalizacją urządzeń za pomocą Google Maps wraz z wyróżnianiem kolorami występujących alarmów na danych urządzeniach
17. Oprogramowanie musi umożliwiać zbieranie informacji o nieprawidłowych parametrach pracy zainstalowanego sprzętu wraz z możliwością generowania alertów o błędach czy przekroczeniu założonych parametrów (środowiskowych, wydajnościowych, dotyczących bezpieczeństwa),
18. Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA w szczególności funkcja monitorowania jakości oraz ilości połączeń Unified Communication and Collaboration.
19. Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach
20. Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępnie nie tylko monitorowanie ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń, które powinno odbywać się za pomocą:
    a. Autoprovisioningu urządzeń – czyli urządzenie podpięte do sieci bez konfiguracji powinno zgłosić się do oprogramowania do zarzadzania siecią o dedykowaną dla urządzenia konfiguracje
    b. Konfiguracja za pomocą Web GUI min. VLAN, IP Interfejsy, QoS, ACL
    c. CLI Scripting – czyli możliwość przygotowania zbiorowej konfiguracji dla przełączników wraz ze zmiennymi w zależności modelu urządzenia

Moduł zabezpieczenie dostępu do sieci LAN

1. Oprogramowanie musi umożliwiać Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x w tym musi posiadać wewnętrzny serwer uwierzytelniający, pozwalający na integracje z usługami Active Directory
2. Licencje oprogramowania muszą umożliwiać integracja z Active Directory/LDAP w tym profilowanie użytkowników poprzez atrybuty AD/LDAP minimalnie:
    a.Profilowanie użytkownika łączącego się do sieci bezprzewodowej z zależności od przypisania użytkownika do grupy AD/LDAP
    b.Profilowanie użytkownika łączącego się do sieci bezprzewodowej z zależności od posiadanego systemu operacyjnego.
    c.Poprzez profilowanie rozumiane jest:
        -przypisanie urządzeń użytkownika do zdefiniowanego VLAN
        -nadanie urządzeniom polityk QoS

-nadanie urządzeniom dostępu lub uniemożliwienie dostępu do konkretnych segmentów sieci (ACL L2/L3/L4 oraz L7 – warstwa aplikacyjna)

Moduł dostęp gościnny

1.Samodzielna rejestracja klientów gościnnych w oparciu o:
   a. Adres e-mail
   b. Numer telefonu (wiadomość SMS)
2.Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
3.Logowanie w oparciu o portale społecznościowe min. Google, Facebook
4.Funkcja personalizacji strony gościnnej w tym obsługa portalu WiFi4EU

Gwarancja: Na oprogramowanie powinno być dostarczone wsparcie na okres 5 lat, umożliwiające min. kontakt z działem technicznym, rozwiązywanie problemów, możliwość aktualizacji oprogramowania do najnowszej wersji.

Część II

Dostawa:

1.Szafa stojąca jednosekcyjna przeznaczona do budowy sieci, 19" – 1szt..

2. Zasilacz awaryjny – 1szt.

3. Laptop 15 cali wraz z oprogramowaniem– 2szt.

4. Monitor 27 cali – 2 szt.

Szafa stojąca jednosekcyjna przeznaczona do budowy sieci – 1szt.
Rodzaj szafy: Stojąca
Rozmiar: 19"
Wysokość teleinformatyczna: 42 U
Montaż: Do samodzielnego montażu
Klasa szczelności: IP20
Ilość sekcji: Jednosekcyjna
Głębokość montażowa: 860 mm
Maksymalne statyczne obciążenie: 800 kg
Rodzaj drzwi przednich: Szkło
Rodzaj drzwi tylnych: Metal

Ilość miejsc na wentylatory: 4
Kolor: Czarny
Grubość drzwi przednich: 5 mm
Grubość górnego & dolnego panelu: 1.2 mm
Grubość bocznego panelu: 1 mm
Grubość szyn montażowych: 2 mm
Grubość pozostałych elementów: 1.2 mm
Głębokość: 1000 mm
Szerokość: 800 mm
Wysokość: 2047.5 mm
Waga: 138.6 kg
Akcesoria w zestawie: - Kółka z hamulcem – Nóżki - Panel Wentylacyjny (4 wentylatory) - Pionowy organizer kabli x2 - Śruby M6 - Zamek przedni - Zamek tylny - Zamki boczne
Gwarancja : 12 miesiące

Zamawiający dopuszcza wymiary zbliżone do w/w maksymalnie do 10% wartości

Zasilacz awaryjny 8000 Watts /8000 VA RACK, - 1szt.
Moc wyjściowa: 8.0kW / 8.0kVA
Wysokość w szafie: 6U
Napięcie wyjściowe: 230V
Nominalne napięcie wejściowe : 230V, 400V 3PH
Typ gniazda wejściowego: Hard wire 3-wire (1P + N + E), Hard wire 5-wire (3P + N + E)
Złącza wyjściowe: (4) IEC 60320 C19 (Zasilanie zapasowe), (1) Hard Wire 3-wire (H N + G) (Zasilanie zapasowe), (1) Hard wire 3-wire (H N + E) (Zasilanie zapasowe),(4) IEC 320 C19 (Zasilanie zapasowe), (6) IEC 60320 C13 (Zasilanie zapasowe), (6) IEC 320 C13 (Zasilanie zapasowe), (3) IEC Jumpers (Zasilanie zapasowe)
Typ akumulatora: Akumulator kwasowo-ołowiowy
Typowy czas ładowania: 1.5godziny
Komunikacja i zarządzanie
Interfejs Port (s) :RJ-45 10/100 Base-T, RJ-45 Serial, Smart-Slot, USB

Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna lcd
Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia
Awaryjny wyłącznik zasilania : Tak
Certyfikaty i zgodność z normami polskimi
Okres gwarancji : Gwarancja podstawowa na urządzenia i baterie
Oprogramowanie do obsługi w komplecie

- **Zamawiający dopuszcza wymiary zbliżone do w/w maksymalnie do 10% wartości**

Dostawa laptopa 15 cali wraz z oprogramowaniem – 2szt.

Dane techniczne:
Procesor Liczba rdzeni: 6
Procesor Intel Core i7-10750Hlub równoważny Taktowanie procesora [GHz]: 2.6 - 5
Dyski, pamięci, napędy Pojemność dysku SSD [GB]: 512
Typ pamięci RAM DDR4 Wielkość pamięci RAM [GB: 8
Częstotliwość pamięci RAM [MHz]: 2933
Interfejs modyfikowanego dysku: M.2 NVMe
Liczba gniazd pamięci RAM: 2
Maksymalna obsługiwana ilość pamięci RAM [GB] :16
Możliwość rozbudowy pamięci dyskowej: Tak
Wbudowany napęd optyczny: Nie
Ekran Przekątna ekranu [cal]: 15.6
Rozdzielczość ekranu: 1920 x 1080
Częstotliwość odświeżania obrazu [Hz]:min 120
Ekran dotykowy: Nie
Rodzaj matrycy Matowa
Typ matrycy: IPS lub równoważna
Obraz i dźwięk

Karta graficzna NVIDIA GeForce GTX 1650 Ti lub równoważna
Pamięć karty graficznej: 4 GB
Karta dźwiękowa: Realtek ALC3287
Wbudowane głośniki: Tak
Wbudowany mikrofon: Tak
Wejście do mikrofonu: Tak
Wyjście audio: Tak
Techniczne:
Urządzenie wskazujące: Touchpad Multi-touch
Podświetlana klawiatura: Tak
Czytnik linii papilarnych: Nie
Wbudowana kamera: Tak
Komunikacja Wi-Fi – standard 802.11 a/b/g/n/ac/ax
Karta sieciowa – standard 10/100/1000
Modem – obecność: Nie
Bluetooth 5.0
Złącze USB 3.1 Typ C : 0
Liczba złączy USB 3.0: 4
Liczba złączy USB 2.0 0
Wyjście HDMI – obecność: Tak
DisplayPort – obecność: Nie
Wyjście VGA (D-Sub) – obecność Nie wymagane
Czytnik kart pamięci :Nie
Pozostałe złącza 1 x USB Typ-C 3.0, Gniazdo Kensington Lock
Fizyczne: Wysokość [cm] 2.6 Szerokość [cm] 36.3 Głębokość [cm] 26 Waga [kg] 2.3
Oprogramowanie: System operacyjny WINDOWS 10 Professional x64
Inne oprogramowanie: Microsoft Office 2019 dla Użytkowników Domowych i Małych Firm PL
Parametry Kolor obudowy: Czarny

Wyposażenie: Instrukcja obsługi w języku polskim, Karta gwarancyjna, Zasilacz
Gwarancja: 24 miesiące

Monitor 27 cali – 2 szt.

Monitor 27 cali
Dane techniczne:
Ekran
Przekątna ekranu [cal]: 27
Rozdzielczość: ekranu 1920 x 1080
Zakrzywiony ekran: Nie
Ekran dotykowy: Nie
Ekran obrotowy (pivot) :Nie
Proporcje ekranu: 16:9
Podświetlenie ekranu: W-LED
Technologia 3D :Nie
Przekątna ekranu [cm]: 68
Obraz:
Częstotliwość odświeżania obrazu [Hz] :144
Powłoka matrycy: Matowa
Rodzaj matrycy: IPS
Czas reakcji matrycy [ms]: 1
Jasność ekranu [cd/m2] :350
Kontrast statyczny: 1000:1
Liczba wyświetlanych kolorów: 16.7 mln
Wielkość plamki :0.311
Kąt widzenia w pionie / w poziomie 178 (pion), 178 (poziom)
Techniczne dane:

Głośniki: Nie
Mikrofon: Nie
Kamera internetowa: Nie
Pilot: Nie
Możliwość zawieszenia na ścianie: Tak
Standard VESA [mm]: 100 x 100
Złącza:
Wejście komponentowe :Nie
Złącze USB: 0
Wejście DVI :0
Złącze DisplayPort: 1
Wejście liniowe audio: Nie
Wejście HDMI :2
Cyfrowe złącze optyczne: Nie
Złącze EURO (Scart): Nie
Wyjście liniowe audio: Tak
Wejście D-Sub (VGA) 0
Fizyczne:
Waga [kg] 5.8 Wysokość [cm] 45.4 Głębokość [cm] 22.5 Szerokość [cm] 61.4
Załączona dokumentacja: Instrukcja obsługi w języku polskim, Karta gwarancyjna
Gwarancja : 24 miesiące
Kolor obudowy : Czarny
Wyposażenie: Kabel HDMI, Kabel zasilający

Część III

Dostawa:

Oprogramowanie do kopii zapasowych- 1szt

Oprogramowanie do kopii zapasowych
Wymagania: obsługa :8 stacji roboczych oraz min. 2 serwerów ,5 maszyn wirtualnych typ licencji: wieczysta oprogramowanie ma być objęte 3 letnim wsparciem producenta na aktualizacje/support
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
Oprogramowanie musi posiadać wsparcie dla NDMP
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwosc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
o Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
o BSD: UFS, UFS2
o Solaris: ZFS, UFS
o Mac: HFS, HFS+
o Windows: NTFS, FAT, FAT32, ReFS
o Novell OES: NSS
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Oprogramowanie wspierające (agents)
Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux:
o Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
Rozwiązanie musi wspierać systemy operacyjne macOS
Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików:
o NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2
Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
Rozwiązanie musi wspierać backup podłączonych dysków USB
Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:
o Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny
o Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire
o Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
o Zcentralizowanym repozytorium danych
o Bezpośrednio na zasobach Chmury
Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
Rozwiązanie musi wspierać kontrolę pasma sieciowego
Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
Rozwiązanie musi wspierać technologię BitLocker
Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:
o Microsoft Exchange 2010 i nowszych
o Microsoft Active Directory 2003 i nowszych
o Microsoft Sharepoint 2010 i nowszych
o Microsoft SQL 2005 i nowszych
o Oracle 11g i nowszych
Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
Rozwiązanie musi wspierać szyfrowanie
Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

Część IV

Dostawa : Urządzenie UTM – 2szt.

Wymagania Ogólne –Firewalla

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 2 gniazdami SFP 1 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

Funkcje Systemu Bezpieczeństwa:
W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [60] miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. Posiadanie : Certyfikat ISO 9001 podmiotu serwisującego.

Część V

Dostawa: Serwera - 2szt. , Macierz – 1 szt.

Serwery -2szt.	
Parametr lub warunek	**Minimalne wymagania serwerów**
Obudowa	- Typu Rack, wysokość maksimum 3U; - Dostarczona wraz z szynami umożliwiającymi montaż serwera w szafie rack; - Możliwość instalacji minimum 8 dysków 2.5" typu Hot-Plug.
Płyta główna	- Wieloprocesorowa (2 lub 4 procesorowa), wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 28-rdzeniowych; - Wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3TB pamięci RAM DDR4 2933 MHz. Możliwość rozbudowy do minimum 384GB pamięci RAM bez konieczności zmiany komponentów dostarczonych w oferowanej konfiguracji; - Obsługa w oferowanym modelu serwera pamięci nieulotnej instalowanej w gniazdach pamięci (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania bez konieczności bateryjnego podtrzymania stanu pamięci);

	- Możliwość rozbudowy/rekonfiguracji serwera do minimum 4 złączy PCI Express generacji 3, w tym minimum 3 złączy o prędkości x16. W zaoferowanej konfiguracji wymaga się minimum 3 złączy PCI Express aktywnych w tym 1 złącza x16; - Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express); - Wew. pamięci flash przeznaczona dla wirtualizatora o poj. 64GB nie zajmująca klatek dyskowych serwera. lub 2 dyski ssd /m2 128 gb
Procesory	Zainstalowany 1 procesor 16-rdzeniowy w architekturze x86 z możliwością rozbudowy do konfiguracji dwuprocesorowej. Procesor osiągający w oferowanym serwerze w testach wydajności SPECrate2017_int_base wynik minimum 190 pkt. dla konfiguracji 2-procesorowej (po rozbudowie); Wynik dla oferowanego serwera wraz z oferowanymi procesorami dostępny na stronie spec.org.
Pamięć RAM	- Zainstalowane minimum 128 GB pamięci RAM typu DDR4 Registered, 2933 MHz; - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC lub równoważne; - Wsparcie modelu serwera dla konfiguracji kopii lustrzanej pamięci RAM.
Kontrolery dyskowe, I/O	- Zainstalowany dedykowany sprzętowy kontroler SAS 3.0 ze wsparciem dla poziomów RAID: 0, 1, 5, 6, 50, 60; - Kontroler wyposażony w minimum 2GB pamięci podręcznej Cache;
Dyski twarde	- Zainstalowane 2 dyski SSD minimum 480GB SATA, dyski hotplug; - Zainstalowane 6 dyski HDD minimum 600GB SAS 10k, dyski hotplug;
Interfejsy sieciowe	- Zintegrowane 2 porty 1GbE RJ-45; - Dodatkowa karat sieciowa posiadająca 4 porty 10GbE w standardzie SFP lub równoważne - Dwie dodatkowe karty sieciowe 2-portowe w standardzie 1GbE RJ-45 lub równoważne
Porty	- Zintegrowana karta graficzna ze złączem VGA; - 2x USB 2.0 lub 3.0 dostępne na froncie obudowy; - 2x USB 3.0 dostępne z tyłu serwera; - 1x USB 3.0 wewnątrz serwera; - Możliwość rozbudowy o dodatkowe złącze VGA dostępne z przodu serwera; - Możliwość rozbudowy o dodatkowe złącze szeregowe w standardzie RS-232-C; - Wszystkie opisywane złącza VGA i USB osiągnięte bez stosowania zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
Zasilanie, chłodzenie	- Redundantne zasilacze Hot-Plug o sprawności 94%; - Redundantne wentylatory Hot-Plug;
Zarządzanie	- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania/rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera; - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego

	zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH); • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; • Zarządzanie alarmami (zdarzenia poprzez SNMP); • Możliwość przejęcia konsoli tekstowej; • Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych); • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska; W/w rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); o Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; o Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; o Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; o Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;
Wspierane OS	- Windows 2019; - Windows 2016; - VMWare; - SuSE; - RHEL.
Oprogramowanie	- Dostarczony system operacyjny Microsoft Windows Server/Datacenter 2019 lub równoważny. Licencja wieczysta dla oferowanego serwera i uprawniająca do uruchomienia 8 instancji systemu operacyjnego jako maszyny wirtualne;
Gwarancja i inne	- 3 lat gwarancji producenta serwera; - Oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt został zaaferowany przez Producenta serwera na potrzeby oferty; - Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;

	- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera; - Serwer fabrycznie nowy, pochodzący z oficjalnego kanału dystrybucyjnego w Polsce; - Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;

MACIERZ – 1 szt.	
Parametr lub warunek	**Minimalne wymagania :**
Ogólne	
Rodzaj urządzenia	Macierz dyskowa
Rodzaj obudowy	Do montowania w stojaku - 2U
Obudowy	
Ilość Zatok dyskowych	24
Obsługiwane rodzaj napędów	SAS-3
Pamięć masowa	
Interfejs zewnętrznej tablicy HDD	iSCSI (10 GbE)
Kontroler pamięci masowej – 1 szt.	
Typ	RAID
Typ interfejsu	SAS 12Gb/s
Szybkość transmisji danych	1.2 GBps
Poziom RAID	RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Pamięć	32GB
Dysk twardy	
Typ/ilość	min. 1,8 TB 10K 2,5" HDD – 6 szt. min 800 GB 2,5" SSD- 2 szt. Zamawiający wymaga aby dostarczone dyski spełniały parametr : min DWPD: 10
Rozszerzenie / połączenie	
Interfejsy	Ethernet 1000 (zarządzający) - RJ-45 – 1 szt. Ethernet 10Gb (iSCSI) - SFP+ - 2szt
Różne	
Dołączone przewody	przewód zasilający (C13-C14) - 1.5 m

Dołączone akcesoria	Zestaw do montażu szafy rack – 1szt.
Zasilanie	
Zasilacz	1 x wewnętrzne źródło mocy
Zasilanie nadmiarowe	Tak
Wymagane napięcie	AC 120/230 V - 50/60 Hz
Oprogramowanie/ obsługa	Zarządzanie urządzeniem gui, obsługa ssh, ssl ldap Dynamiczne pule dyskowe -możliwość dynamicznego rozszerzania przestrzeni Dyskowej poprzez dołączanie nowych dysków, pamięć podręczna odczytu SSD, możliwość: cienkie Szyfrowanie- możliwość szyfrowania danych przy użyciu kontrolerów macierzy lub dysków samoszyfrujących np. SED
Gwarancja	- 3 lat gwarancji producenta serwera w trybie onsite z czasem reakcji serwisu w następnym dniu roboczym; - Oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt został zaaferowany przez Producenta serwera na potrzeby oferty; - Dostępność części zamiennych przez 3 lat od momentu zakupu serwera;

Informacje uzupełniające	
Wymagane dokumenty wraz z dostawą	- instrukcja obsługi - karta/książka gwarancyjna, - inne wymagane prawnie dokumenty