WM.PT.0810.27A.2022

MAZURY AIRPORT Sp. z o.o.
z siedzibą w Szymanach
Szymany 150, 12-100 Szczytno
NIP 7451842294, Reg. 281345971
KRS 0000399439

.....
(Pieczęć Zamawiającego)

Szymany, dnia 21.11.2022 r.

ZAPYTANIE OFERTOWE

(niniejsze zapytanie nie stanowi zapytania ofertowego w rozumieniu ustawy pzp i stanowi rozeznanie rynku)

Zwracamy się z prośbą o przesłanie oferty na poniżej opisany przedmiot zamówienia:

Sprzęt IT:

Część I: Urządzenia serwerowe

1. Serwer Dell DELL PowerEdge R650 (Zgodnie z załącznikiem nr 1)
2. Macierz Dell PowerVault ME4024 24x2.5"/2xSAS 12Gb/2x900GB HDD SAS/2x580W/3Yr Basic (Zgodnie z załącznikiem nr 2)
3. Serwer plików QNAP TS-431XeU-2GB w zestawie 4 dyski po 10TB (Zgodnie z załącznikiem nr 3)
4. Moxa switch przemysłowy z dwoma zasilaczami DC w zestawie 8port (Zgodnie z załącznikiem nr 4)
5. SZAFA RACK 42U Z patchpanelami 8 sz. (4 x RJ45, 4x światłowodowe), Organizerami 4 szt., Listwami zasilającymi 4 szt. , Patchcordy cat 6 1m 20szt, Patchcordy cat 6 0,5m 20szt (Zgodnie z załącznikiem nr 5)

Część II: Urządzenia sieciowe

6. Firewall Fortigane 100f + 3 letnia subskrypcja (Zgodnie z załącznikiem nr 6)
7. Switch Extreme x460- G2- 24p- 10GE4 – 2 szt. (Zgodnie z załącznikiem nr 7)

Termin realizacji zamówienia: do 30.12.2022 r.

Kryterium oceny ofert: cena 100%

Uwagi: Wycena ma na celu przeprowadzenie analizy rynku oraz wyłonienia dostawcy na zakup.

Ofertę prosimy przesłać pocztą elektroniczną na adres:
n.rykaczewska@mazuryairport.pl

W terminie do dnia: 25.11.2022 r. do godz.12.00

Zatwierdzam:

Dyrektor Techniczny
Tomasz Kamiński
.....
(Podpis Kierownika Komórki Organizacyjnej)

Załącznik nr 1 - Serwer

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów: BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory min. 24-rdzeniowe, min. 2.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 310 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 136GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Gniazda PCI	- minimum trzy sloty PCIe x16
Interfejsy sieciowe/FC/SAS	Wbudowane min. 6 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, dwa interfejsy 10GbE BASE-T, port SAS do podłączenia macierzy.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD. Zainstalowane 4 dyski 1,2TB SAS ISE 12Gb/s 10 tys. obr./min 512n 2,5" dysk twardy wymieniany bez wyłączania systemu Zainstalowane dwa dyski M.2 SATA o pojemności min 480GB Hot-Plug skonfigurowane w RAID 1. Zainstalowany modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 2.0 na przednim panelu obudowy i 1x USB 3.0 wewnętrzny, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 1100W każdy.
Bezpieczeństwo	Zainstalowany moduł TPM 2.0. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla dynamic DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera - możliwość zarządzania temperaturą - wirtualny schowek (możliwość wycinania i wklejania w zdalnej konsoli HTML5) - automatyczna rejestracja certyfikatu karty zarządzania dla certyfikatów SSL - inwentaryzację i monitorowanie GPU - inwentaryzację i monitorowanie optycznych wejść/wyjść SFP+ - wykrywanie bezczynności serwera - przechwytywanie bufora danych szeregowych systemu 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, , Linux SSH • Możliwość oskryptowywania procesu wykrywania urządzeń • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS • Grupowanie urządzeń w oparciu o kryteria użytkownika • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń • 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 • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is" do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ▪ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych - Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej)
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016, Microsoft Windows 2019.
Oprogramowanie	Windows Server 2022 Standard na odpowiednią ilość rdzeni
Warunki gwarancji	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

	Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Załącznik nr 2- Macierz

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do instalacji w standardowej szafie RACK 19", macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5".
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 12Gb SAS
Cache	16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.
Dyski	Zainstalowane: 2 dyski Hot-Plug o pojemności 1.2TB SAS 10K 2,5", Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Oprogramowanie/Funkcjonalności	Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.
Wsparcie dla systemów operacyjnych	Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi, Citrix XenServer
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Warunki gwarancji dla macierzy	3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. • Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015.

Załącznik nr 3- Serwer plików

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Min. 4-core AnnapurnaLabs Alpine AL-314 1.7 GHz
Obudowa	Rack 1U o wymiarach, 44(H) x 439(W) x 291(D) mm
Pamięć RAM	2GB DDR3 RAM, z możliwością rozbudowy do 8GB
Pamięć Flash	512 MB
Ilość obsługiwanych dysków	4 dyski 2.5"/3.5" SATA3 z możliwością konfiguracji Hot Swap
Ilość zamontowanych dysków	4x dyski twarde o pojemności 10TB, z listy kompatybilności NAS, minimum 2,5mln roboczogodzin MTBF
Interfejsy sieciowe	2 x Gigabit (10/100/1000), 1 x 10 Gigabit SFP+ możliwość podłączenia dongle wireless przez port USB, obsługa VLAN i Jumbo Frame.
Porty	4x USB 3.2 Gen1
Wskaźniki LED	HDD 1-4, Status, LAN, Power, USB
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,6,10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów. Mechanizm szyfrowania z akceleracją sprzętową.
System Operacyjny	Windows 7, Windows 8, Windows 10, Windows Server 2003/2008 R2/2012/2012R2, Apple Mac OS 10.7+, Linux & UNIX
Stacja monitoringu	Obsługa do 30 kamer IP (2 licencje domyślnie).
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker)
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Język GUI	Polski, Angielski
Gwarancja	Gwarancja 36 miesięcy
Waga	Maksymalnie 6 kg
Pobór mocy	Uśpienie: 13 W Praca max: 32 W
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	100W
Wentylatory	Minimum 3, każdy po 4 cm.
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS

Załącznik nr4 - Switch przemysłowy oraz dwa kompatybilne zasilacze prądu stałego w zestawie

Parametr	Charakterystyka (wymagania minimalne)
Interfejsy Ethernet	
Standardy	IEEE 802.3 10BaseT, IEEE 802.3u, 100BaseT(X) oraz 100BaseFX IEEE 802.3x flow control
Porty 10/100BaseT(X) (złącze RJ45)	Full/Half duplex mode Auto MDI/MDI-X connection Auto negotiation speed
Porty 100BaseFX (wielomodowe, złącza SC)	EDS-208-M-SC: jest
Porty 100BaseFX (wielomodowe, złącza ST)	EDS-208-M-ST: jest
Właściwości switcha	
Rodzaj przetwarzania	Store and Forward
Wielkość tablicy MAC	2K
Wielkość bufora pakietów	768 kbit
Zasilanie	
Napięcie wejściowe	24VDC
Prąd (@ 24VDC)	EDS-208: 0.07 A @ 24 VDC Seria EDS-208-M: 0.1 A @ 24 VDC
Dopuszczalny zakres napięcia wejściowego	12 do 48 VDC
Złącze	Zdejmowalny, 3-pinowy bloczek zasilania
Ochrona przed odwrotną polaryzacją	Tak
Ochrona przed przeciążeniem	2,5A @ 24VDC
Charakterystyka fizyczna	
Obudowa	Tworzywo sztuczne
Stopień ochrony	IP30
Wymiary (W x H x D)	40 x 100 x 86.5 mm
Masa	170 g
Instalacja	Na szynie DIN (zintegrowany uchwyt)
Warunki zewnętrzne	
Temperatura pracy	-10 do +60°C
Temperatura przechowywania	-40 do +85°C
Wilgotność względna	5 do 95% (bez kondensacji)

Certyfikaty i gwarancja	
Safety	UL 508
EMC	EN 55032/24
EMI	CISPR 32, FCC Part 15B Class A
EMS	IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV IEC 61000-4-3 RS: 80 MHz do 1 GHz: 3 V/m IEC 61000-4-4 EFT: Power: 1 kV; Signal: 0.5 kV IEC 61000-4-5 Surge: Power: 1 kV; Signal: 1 kV IEC 61000-4-6 CS: 3 V IEC 61000-4-8 PFMF
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-31
Vibration	IEC 60068-2-6
MTBF	EDS-208: 401624 hrs Seria EDS-208-M: 368353 hrs, Telcordia (Bellcore), GB

Załącznik nr 5 - szafa RACK 19" 42U 800x800

Parametr	Charakterystyka (wymagania minimalne)
Rodzaj szafy	Wolnostojąca (serwerowa)
Wysokość robocza	42U
Szerokość montażowa	19"
Wymiary [mm] (szerokość x głębokość x wysokość):	800x800x2055,
Kolor	czarny
Drzwi przednie	pojedyncze szklane - szkło hartowane
Drzwi tylne	pojedyncze metalowe - pełna stal
Maksymalne obciążenie	Do 1000 kg
Gwarancja	Min. 12 miesięcy
Jakość certyfikowana deklaracją zgodności	zgodności z ogólnymi wymogami bezpieczeństwa zawartymi w dyrektywie Unii Europejskiej nr 2014/35/EU z dnia 26 lutego 2014 roku, poprzez spełnienie odpowiednich wymagań normy PN-EN 62368-1:2015-03.
Wyposażenie standardowe	miejsce na panel wentylacyjny (4 wentylatory)
	3 x patchpanel (2x RJ45 CAT 6 ekranowany 24 keystony w zestawie oraz 1x światłowodowy S.C. UPC z adapterami)
	4 x Organizery poziome 1 U
	3 x Listwy zasilający 1U
Wyposażenie dodatkowe	Patchcordy cat 6 1m 20szt,
	Patchcordy cat 6 0,5m 20szt
	1x zamek drzwi przednich z klamką,
	1x zamek drzwi tylnych,
	4x kółka transportowe (2 z hamulcem),
	4 nóżki poziomujące,
	śruby montażowe z koszykiem
	4 kółka + 4 nóżki

Załącznik nr 6 - Firewall

Parametr	Charakterystyka (wymagania minimalne)
Wymagania Ogólne	System bezpieczeństwa ma realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę 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 wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Opisy do wymagań ogólnych	W stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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.
	Wymagany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.
Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
	Monitoring stanu realizowanych połączeń VPN.
	System ma umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 2 gniazdami SFP+ 10 Gbps.
	System Firewall ma posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
	System Firewall ma pozwalać na skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
	System ma być wyposażony w zasilanie AC.
Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
	Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
	Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.
	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.

	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
Funkcje Systemu Bezpieczeństwa W ramach systemu ochrony są realizowane wszystkie wymienione funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:	Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
	Kontrola Aplikacji.
	Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
	Ochrona przed malware.
	Ochrona przed atakami - Intrusion Prevention System.
	Kontrola stron WWW.
	Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
	Zarządzanie pasmem (QoS, Traffic shaping).
	Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
	Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
	Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
	Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
	Rozwiązanie ma posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
	• System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
	W ramach systemu ma istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
	Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
	Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
	Element systemu realizujący funkcję Firewall integruje 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. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	System ma umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • 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.

	• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site.
	System ma umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN W zakresie routingu rozwiązanie zapewnia obsługę:	Routingu statycznego.
	Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
	Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
	Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
	ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
	BFD (Bidirectional Forwarding Detection).
	Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	System ma umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
	SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
	System ma dać możliwość określania pasma dla poszczególnych aplikacji.
	System ma pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
	System ma zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
	Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
	System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
	System ma umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
	System ma dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
	Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
	System ma współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
	System ma zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
	Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
	Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami	Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
	System ma chronić przed atakami na aplikacje pracujące na niestandardowych portach.
	Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
	Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
	System ma zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
	Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
	Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
	Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
	Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
	Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
	Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
	Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
	Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
	System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
	W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
	Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
	Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
	Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
	Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
	Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
	Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
	System ma pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	System Firewall ma 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.
	System ma dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
	System ma umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
	Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
	Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
	Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
	System ma współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
	System ma dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
	Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
	Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
	Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
	Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
	W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
	Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
	Możliwość włączenia logowania per reguła w polityce firewall.
	System zapewnia możliwość logowania do serwera SYSLOG.
	Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następującą certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy
Gwarancja	System musi być objęty serwisem gwarancyjnym producenta przez okres [36] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewni dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wsparcie **HEZO SERWIS SOS 24x7x8 HEZO**	System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie, dostarczenie oraz instalację sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia w miejscu instalacji wykonana przez certyfikowanego inżyniera w zakresie oferowanego rozwiązania, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [36] miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

	Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.

Załącznik nr 7 - Switch

Parametr	Charakterystyka (wymagania minimalne)
Porty	24 x 10/100/1000BASE-T PoE-Plus - 4 porty combo
	8 x 100/1000BASE-X (SFP) 4 porty combo w tym Porty 10GbE Ports– 6 szt.
	4 x 10GBASE-X SFP+
	1 x port consolowy port RJ-45
	1 x 10/100/1000BASE-T port zarządzający
	1 x USB port
Protokół wymagany	kompatybilność z zaimplementowanym w środowisku zamawianego protokołem tras nadmiarowych EAPS
Dodatkowe wyposażenie	dodatkowa wkładka z portami 40GbE Ports – 2 szt
Przepustowość	Przepustowość przełacznika - 296 Gbps
	Szybkość przesyłania ramek - 220.2 Mpps
Zasilanie	Dwa zasilacze 715W
Waga	Waga do max 6.62 kg
Dodatkowe wyposażenie	Wentylator kompatybilny z urządzeniem
Wymiary	Wysokość 1U 4.4 cm
	Szerokość 44.1 cm
	Głębokość 48.8 cm
Parametry sprzętowe	64-bitowy procesor MIPS , z zegarem 1 GHz
	1GB ECC DDR3 DRAM
	4GB eMMC pamięci Flash
Parametry urządzenia	poniżej 4 mikrosekund opóźnienia (64-byte)
	Warstwa 2/ Adresy MAC: 96 tys (98 304)
	Adresy hostów IPv4 62 tys
	4096 VLANów
	maksymalny rozmiar pakieru w bajtach 9216 (Jumbo Frame)
	Możliwość użytkowania polityk
	Autoryzowani użytkownicy polityk per switch do 12 288
	Autoryzowani użytkownicy polityk per port do 12 288
	Unikalne zasady Permit/Deny per switch: 1 464
	Reguły MAC do 512
	Reguły IPv4 do 1280
	Reguły IPv6 do 256
	Reguły L2 do 184