**Załącznik nr 1 do zapytania ofertowego nr 1/2022/Infostrateg**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakup i dostawa sprzętu komputerowego: 5 laptopów z systemem operacyjnym, licencji UTM oraz serwera zgodnie z określonymi parametrami w projekcie *AntyFakeNews, system do ochrony użytkowników przed fałszywymi informacjami dystrybuowanymi w sieci Internet***

Działanie realizowane i finansowane w ramach projektu ***AntyFakeNews, system do ochrony użytkowników przed fałszywymi informacjami dystrybuowanymi w sieci Internet***, zgodnie z umową o dofinansowanie Infostrateg/0043/2021-00, współfinansowanego ze środków krajowych Narodowego Centrum Badań i Rozwoju w ramach konkursu INFOSTRATEG I Program Strategiczny Program Badań Naukowych i Prac Rozwojowych „Zaawansowane technologie informacyjne, telekomunikacyjne, mechatroniczne”

|  |  |
| --- | --- |
| **Nazwa zadania** | **Wymagane parametry** |
| Zadanie 1: Zakup i dostawa 5 laptopów z systemem operacyjnym zgodnie z parametrami określonymi w załączniku nr 1 do zapytanie ofertowego. | **Procesor:**  Ilość rdzeni co najmniej 6  Pamięć cache co najmniej 11MB  Wynik testu wydajności Passmark v10 co najmniej 13000 punktów z wydajnością jednego wątku procesora co najmniej 2400 punktów  **Pamięć RAM:**  Ilość co najmniej 16GB  Prędkość co najmniej 3200MHz  **Dysk:**  Rozmiar dysku co najmniej 512GB  Dysk komunikujący się co najmniej protokołem NVME Możliwość zamontowania dodatkowych dysków tego samego typu  **Ekran:**  Przekątna ekranu co najmniej 15,6"  Rozdzielczość o najmniej 1920x1080  Jasność co najmniej 250cd/m2  Matowy typ ekranu  Typ matrycy WVA lub o równej charakterystyce  **Komunikacja:**  Wbudowane co najmniej 2 mikrofony  Wbudowana kamera o rozdzielczości co najmniej 1.0 Mpix  **Łączność:**  Wsparcie standardu WiFi 802.11AC  Możliwość łączności Bluetooth  Sprzęt musi posiadać następujące złącza:  USB 3.2 Gen. 1 - co najmniej 2 szt.  USB Typu C z wsparciem DisplayPort i Power Delivery HDMI 1.4 Czytnik kart pamięci SD Wyjście słuchawkowe/wejściowe mikrofonowe Wejście zasilania DC  **Bateria:**  Bateria typu litowo-jonowego o pojemności co najmniej 3420mAh  **Bezpieczeństwo:**  Wymagane jest wsparcie funkcjonalności szyfrowania TPM oraz czytnik linii papilarnych  **Wykonanie/konstrukcja:**  Laptop musi posiadać wydzieloną klawiaturę numeryczną Nie dopuszcza się konstrukcji wnętrza laptopa i pokrywy matrycy innych niż metalowe Maksymalna dopuszczalna waga laptopa to 1.65kg  Oprogramowanie:  Sprzęt musi zostać dostarczony z systemem operacyjnym Windows w wersji co najmniej 11  **Gwarancja:**  Sprzęt musi być objęty gwarancją sprzedawcy na okres co najmniej 24 miesięcy |
| Zadanie 2: Zakup i dostawa licencji UTM zgodnie z parametrami określonymi w załączniku nr 1 do zapytanie ofertowego. | 1. **ARCHITEKTURA SYSTEMU OCHRONY**   **Typ systemu ochrony**: System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.  Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).  **Wymagania systemowe**: System ochrony powinien spełniać wymagania w niżej wymienionym zakresie.  Obsługa nielimitowanej ilości hostów w sieci chronionej.  Typ procesora: AMD wielordzeniowy oraz dedykowany procesor sieciowy typu NPU  Pamięć RAM: nie mniej niż 32GB dla procesora głównego oraz nie mniej niż 8GB dla procesora NPU  Urządzenie przystosowane do pracy w szafie serwerowej Rack z adekwatnym osprzętem montażowym – rozmiar maksymalnie 1U  Minimalna liczba i typ interfejsów fizycznych: 4x GE (IEEE 1000Base-T), 4x SFP+, 4x 2.5GbE, 2x USB (Type-A), 1x Console (RJ-45 lub DB9)  Minimalna liczba portów rozszerzeń o dedykowane moduły z dodatkowymi interfejsami: 2  Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q)  Minimalna liczba nowych połączeń na sekundę: 368 000  Minimalna liczba jednoczesnych połączeń: 16 600 000  Minimalna przepustowość Firewall: 75 000 Mbps  Minimalna przepustowość IPS: 25 000 Mbps  Minimalna przepustowość Threat Protection: 4800 Mbps  Minimalna przepustowość IPSec: 9800 Mbps  Minimalna liczba równoczesnych tuneli IPSec VPN: 1000  Minimalna liczba równoczesnych tuneli SSL VPN: 270  Minimalna przepustowość rozszyfrowania ruchu SSL/TLS: 8000 Mbps  Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 240 GB.   1. **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY**   **Zarządzanie i utrzymanie**: Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI).  Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup.  Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.  Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy RSA, DSA lub ECDSA o długości min. 4096 bitów.  Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.  System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.  System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.  Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).  System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.  Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.  System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.  Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.  System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.  Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpwiednik).  System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych).  System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym on-premise lub on-cloud.  Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email.  Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.  Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.  Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.  Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud a synchronizacja subskrypcji on-line powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.  Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).  System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.  W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie).  **Zapora sieciowa, konfiguracja sieciowa oraz routing**: Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.  Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.  System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.  Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług.  Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.  System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN.  Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.  Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.  System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).  System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking).  System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).  Rozwiązanie powinno zapewniać obsługę routingu statycznego.  Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).  Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).  System powinien oferować wsparcie dla IGMP snooping.  Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy).  Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.  Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).  System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.  System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.  Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.  Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.  Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules.  Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta.  Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).  System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP.  System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania.  Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).  **Podstawowe kształtowanie pasma oraz limity ilości danych**: System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.  Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.  System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.  **Bezpieczna sieć bezprzewodowa**: System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania.  Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater.  Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu.  Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej.  Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej.  Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej.  Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.  Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication).  Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition).  System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów.  Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.  System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden.  System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe.  Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).  **Autoryzacja użytkowników**: Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.  Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.  System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+.  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.  Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password).  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.  System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.  Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.  **Samoobsługowy portal dla użytkowników**: Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci.  Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).  Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.  Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.  Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika.  Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.  **Podstawowe opcje VPN**: System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:  Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)  Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).  **Klient IPSec VPN (dostępny osobno)**: Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.  Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.  Wsparcie dla split-tunneling.  Wsparcie dla NAT-traversal.  Monitorowanie stanu połączenia   1. **OCHRONA SIECI**   **IPS**: Dodatkowy moduł ochrony klasy IPS z bazą minimum 7000 sygnatur.  Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.  Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.  Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.  System powinien generować alerty w przypadku wykrycia ataku.  **ATP**: System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.  **Clientless VPN**: Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.   1. **OCHRONA I KONTORLA WEB ORAZ APLIKACJI**   **Ochrona i kontrola Web**: Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.  Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).  System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.  Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups).  Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch).  Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.  System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.  System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.  Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies.  System powinien zapewniać możliwość emulacji skryptów JavaScript.  Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.  Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.  Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać blokadę stron HTTPS.  Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.  System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji.  **Ochrona i kontrola aplikacji:** Rozwiązanie powinno oferować bazę danych opisująca co najmniej 2500 aplikacji.  Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.  Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.  Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.  Rozwiązanie powinno umożliwiać blokowanie:  - aplikacji, które pozwalają na transfer plików (np. P2P).  - komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.  - proxy uruchamianych poprzez przeglądarki internetowe.  - streaming media (radio internetowe, Youtube, Vimeo).  Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo.  **Kształtowanie pasma dla Web i Aplikacji**: Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie.  Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.  Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared).   1. **LOGOWANIE I RAPORTOWANIE**   **Logowanie i raportowanie:** System powinien umożliwiać składowanie oraz archiwizację logów.  System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.  System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali.  System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.  System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).  Rozwiązanie powinno umożliwiać wysyłanie raportów via email.  Rozwiązanie powinno generować raporty w PDF, HTML i XLS.  Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.  System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza  System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację  Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.  System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora.  System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.   1. **POZOSTAŁE**   **Certyfikaty:** CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, RCM, NOM, Anatel  **Subskrypcje:** Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 12miesięcy z możliwością wydłużenia  **Gwarancja i wsparcie:** Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż 12miesięcy z możliwością wydłużenia  Gwarancja na sprzęt na okres nie krótszy niż 12miesięcy z możliwością wydłużenia  Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.  Czas reakcji 1h na awarię, naprawa na miejscu, dostawca zobowiązany jest do przekazania nowego sprzętu tej samej klasy lub lepszego na czas naprawy. |
| Zadanie 3: Zakup i dostawa serwera zgodnie z parametrami określonymi w załączniku nr 1 do zapytanie ofertowego. | **Obudowa:**  Obudowa Rack o wysokości max 2U z możliwością instalacji min. 16 dysków 2.5” NVMe wraz z kompletem szyn wraz z organizerem do kabli umożliwiających montaż w szafie rack.  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 (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI..  **Płyta główna:**  Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  **Chipset:**  Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.  **Procesor:**  Zainstalowane dwa procesory klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 317 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów.  **Pamięć RAM:**  Min. 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczonych do instalacji pamięci.  **Gniazda PCIe:**  5 x PCIe o prędkości x16 pełnej długości  **Zabezpieczenia pamięci RAM:**  Patrol scrubbing, Failed DIMM isolation, parity protection  **Interfejsy sieciowe/FC:**  Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T.  **Dyski twarde:**  Zainstalowane 8 x 1.6TB SSD NVMe MixUse  Możliwość zainstalowania wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności minimum 64GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.  Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB, możliwość skonfigurowania RAID 1.  **Kontroler RAID:**  Dwa sprzętowe kontrolery dyskowe z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,10,5,6,50,60.  **Wbudowane porty:**  min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty RJ45, 1 port VGA na tylnym panelu.  **Video:**  Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900.  **GPU:**  Karta spełniająca minimalne wymagania,wydajność:  - min. 7680 rdzeni  - min. 11,5 TFLOPs dla rozwiązać HPC  - 32GB HMB2 ECC Memory  - 1,2TB/s przepustowość pamięci  - PCIe Gen4  **Wentylatory**  Redundantne  **Zasilacze**  Redundantne, Hot-Plug maksymalnie 2400W.  **Bezpieczeństwo:**  Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM 2.0  **Karta Zarządzania:**  Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet 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 (SSLv3) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH * 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 podłączenia lokalnego poprzez złącze RS-232. * Producent systemu musi posiadać dedykowane rozwiązanie które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe. * możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. * możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów. * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi. * możliwość zablokowania konfiguracji oraz odnowienia oprogramowania  karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty.   **Certyfikaty:**  Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 bądź inną równoważną normą jakości. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Windows Server 2019, Windows Server 2022.  **Normy Środowiskowe:**  Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku      Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr  **Warunki gwarancji:**  60 miesięcy 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.  Firma serwisująca musi posiadać ISO 9001:2015 lub inny równoważny certyfikat na świadczenie usług serwisowych. |