Załącznik nr 1 do SWZ

Znak sprawy: IRP.272.4.40.2023

OPIS PRZEDMIOTU ZAMÓWIENIA

Zadanie 1

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3,5” • Możliwość wyposażenia w panel LCD • 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 powinna obsługiwać do 1TB pamięci RAM. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Możliwość obsługi procesorów 32 rdzeniowych
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	• Zainstalowane dwa procesory min. 12-rdzeniowe, min. 2.1GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 168 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• Minimum 192GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
Funkcjonalność pamięci RAM	• Advanced ECC, • Memory Page Retire, • Fault Resilient Memory, • Memory Self-Healing lub PPR, • Partial Cache Line Sparing

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących.

Dyski twarde	• Zainstalowane:
	  ○ 5 dysków SAS o pojemności min. 8TB, 7.2K, Hot-Plug.
	  ○ 2 dyski SSD vSAS MU o pojemności min. 1.92TB, Hot-Plug.
	• Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
	• Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

Zasilacze	• Redundantne, Hot-Plug min. 1400W każdy.
Gniazda PCI	• Min. 5 slotów PCIe generacji 4
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Dodatkowa, dwuportowa karta 16Gb FC
Wkładki/kable	• Nie wymagane
Porty	• 4x USB w tym przynajmniej 1x USB 3.0 • 2x VGA w tym jedno z przodu serwera

System operacyjny/System wirtualizacji	• Microsoft Windows Server 2022 Datacenter wraz z:
	  ○ Nośnik CD/DVD z systemem operacyjnym
	  ○ Nośnik CD/DVD do downgrade-u do wersji Windows Server 2019 Datacenter
	  ○ Licencja musi pokrywać wszystkie fizyczne rdzenie procesora

Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
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 V3 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, 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 oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach

	○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ 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 oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji 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 i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Wspierane systemy operacyjne	• Canonical® Ubuntu® Server LTS • Citrix® Hypervisor® • Microsoft® Windows Server® with Hyper-V • Red Hat® Enterprise Linux • SUSE® Linux Enterprise server

	• VMware® ESXi®
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • 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 - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
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.
Warunki gwarancji	• Gwarancji producenta: 7 lat • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.

	• Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • 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 oraz ISO-27001 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 rozszerzenia gwarancji o: • Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało: o Monitorowanie zdarzeń w obrębie infrastruktury o Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji • Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche) • Zdalne lub na miejscu wdrażanie poprawek - 2x w roku • Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie)

Wdrożenie (Opis)	
Przedmiotem Zamówienia jest instalacja w szafach rack zamówionych urządzeń i migracja obecnie działającego środowiska Zamawiającego. Zestawy dostarczanych urządzeń będą umieszczone w obiekcie Zamawiającego tj. w Starostwie Powiatowym w Łęcznej ul. Aleja Jana Pawła II 95A, 21-010 Łęczna Etap I: migracja z VMware 5.1 do Hyper-V 2022 1. Przygotowanie maszyn wirtualnych VMware do migracji na środowisko Hyper-V poprzez usunięcie narzędzi, sterowników i usług VMware. 2. Konwersja dysków VMware na format Hyper-V 3. Odtworzenie konfiguracji przełączników	Wymagane: Termin realizacji 27 października 2023r.

VMware w Hyper-V 4. Konfiguracja maszyn wirtualnych Hyper-V dla dysków VMware po konwersji. 5. Uruchomienie maszyn wirtualnych Hyper-V i weryfikacja poprawności ich działania w nowym środowisku. 6. Włączenie nowego środowiska do systemu kopii zapasowej i weryfikacja poprawności wykonywania kopii zapasowej oraz jej przywracania. Etap II: migracja w Windows 2012 do Windows 2022 1. Dwustopniowa aktualizacja systemu Windows 2012 do wersji 2022 na w przypadku, gdy taka operacja jest wspierana dla oprogramowania i usług zainstalowanych na maszynach wirtualnych. 2. Migracja domeny Active Directory z Windows 2012 do Windows 2022. 3. W przypadku maszyn wirtualnych na których jest zainstalowane oprogramowanie lub usługi, które uniemożliwiają aktualizacje systemu Windows należy przygotować nowe maszyny wirtualne z Windows 2022 oraz przenieść wymagane oprogramowanie oraz dane we współpracy z dostawcami oprogramowania. 4. Weryfikacja poprawności działania zaktualizowanych oraz nowych maszyn wirtualnych. 5. Włączenie zaktualizowanych oraz nowych maszyn wirtualnych do systemu kopii	

zapasowej i weryfikacja poprawności wykonywania kopii zapasowej oraz jej przywracania.	
Maszyny wirtualne (obecnie)	

L.p	*Środowisko*
1	*Microsoft Windows Server 2012 (64 bit)*
2	*Microsoft Windows Server 2012 (64 bit)*
3	*Microsoft Windows Server 2012 (64 bit)*
4	*Microsoft Windows Server 2012 (64 bit)*
5	*Microsoft Windows Server 2012 (64 bit)*
6	*Microsoft Windows Server 2012 (64 bit)*
7	*Microsoft Windows Server 2008 R2 (64 bit)*
8	*Microsoft Windows Server 2008 R2 (64 bit)*
9	*Microsoft Windows Server 2012 (64 bit)*

Serwer plików

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Min. 4 rdzeniowy o taktowaniu 2,2GHz Przekraczający w teście PassMark 4500pkt
RAID	0,1,5,6,10
Pamięć RAM	Min. 4GB DDR4
Obsługiwana pojemność	128TB
Dyski	6x dysk 4TB interfejs SATA III o prędkości obrotowej 7200obr./min
Rodzaje wyjść/wejść	USB 3.2 Gen. 1 - 2 szt. RJ45 (LAN) 1 Gbps - 4 szt. eSATA - 1 szt. AC-in RS232 - 1 szt.
Protokoły sieciowe	AFP

	HTTP HTTPS iSCSI CIFS Serwer DLNA Serwer FTP NFS SNMP WebDAV LDAP CalDAV
System plików	EXT4 Btrfs
System plik dla dysków zewnętrznych	NTFS HFS+ EXT3 EXT4 Btrfs
Dodatkowe funkcje	• Wake on LAN • Możliwość montażu w szafie rack
Obudowa	Rack 2U
Dołączone akcesoria	• Kable zasilające • Karta sieciowa interfejs PCI Express, prędkość transferu 10Gb/s, Full Duplex • Szyny do montażu w szafie rack kompatybilne z zaoferowanym produktem
Gwarancja	36miesięcy

System ochrony sieci	
W ofercie należy wpisać Producent, model, nr produktu producenta: [tutaj wpisać]	
Minimalne wymagane parametry	**Szczegółowy opis oferowanego przedmiotu, umożliwiający identyfikację**
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję ochrony sieci musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi wspierać IPv4 oraz IPv6 w zakresie: Ochrony w	

warstwie aplikacji, Protokołów routingu dynamicznego. W przypadku systemu pełniącego funkcje: IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji ochrony siecil. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System realizujący funkcję ochrony sieci musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. System ochrony sieci musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu ochrony sieci powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. W zakresie frewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. Przepustowość stateful dla ochrony sieci: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość ochrony sieci z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: Kontrola dostępu - zapora ogniowa klasy Stateful Inspection; Kontrola Aplikacji; Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN; Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS; Ochrona przed atakami - Intrusion Prevention System; Kontrola stron WWW; Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3; Zarządzanie pasmem (QoS, Traffic shaping); Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP); 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; Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2; Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. Polityka ochrony sieci musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu; Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików. Element systemu realizujący funkcję ochrony sieci 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; System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: Wsparcie dla IKE v1 oraz v2; Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM); Obsługa protokołu Diffie-Hellman grup 19 i 20; Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE; Tworzenie połączeń typu Site-to-Site	

oraz Client-to-Site; Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego; Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth; Mechanizm „Split tunneling" dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0; Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta; Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego; Policy Based Routingu; Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. System ochrony sieci musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak:	

Google, oraz Yahoo. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. System ochrony sieci musi umożliwiać weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję ochrony sieci musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji ochrony sieci. Element systemu realizujący funkcję ochrony sieci musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. W ramach logowania system pełniący funkcję ochrony siecil musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG. Z urządzeniem należy dostarczyć licencje upoważniające do korzystania w okresie gwarancji na urządzenie z aktualnych baz funkcji ochronnych producenta i serwisów w zakresie: 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. Roczna gwarancja producenta. Dostawa nowego urządzenia do 8 godzin od awarii. Wsparcie w reżimie 24x7 w językach angielskim i polskim. W ramach dostawy wykonawca dokona pełnego wdrożenia oferowanego przedmiotu zamówienia wg wytycznych Zamawiającego.	