Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Projekt „Cyfrowa Gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego
w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020.

Wstęp

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego realizacji projektu pn.: „Cyfrowa Gmina" realizowanego przez Gminę Bojadła.

Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowa Gmina" dla Gminy Bojadła o numerze:

1. Serwer z oprogramowaniem

Parametr	Wymagania minimalne
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug 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 - z możliwością 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 minimum dwóch procesorów.
Chipset	Chipset dedykowany do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory 20-rdzeniowe, min. 2.3 GHz (Turbo Speed min. 3.4 GHz), klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 37260 w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/. na dzień 24.05.2022 r.
RAM	RAM min. 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	minimum cztery sloty PCIe z czego przynajmniej trzy generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane: • Min. 2 dyski SSD SATA MU o pojemności min. 480GB, 6Gb, Hot-Plug, • Min. 4 dyski NLSAS o pojemności min. 2TB, 12Gbps, 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.
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/dodatkowe oprogramowanie	Zamawiający wymaga, aby dostarczyć serwer wraz z oprogramowaniem systemowym na płycie DVD, w najnowszej aktualnej wersji, nieograniczonym czasowo wraz z licencją dostępową dla 25 użytkowników. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Wykonawca odpowiada za sprawne i wydajne działanie systemu operacyjnego na dostarczonym sprzęcie serwerowym. Poniższy opis należy traktować jako zbiór wymagań minimalnych, ponieważ Wykonawca musi zapewnić odpowiednie parametry i spełnić wszystkie wymagania licencyjne oferowanego systemu operacyjnego, niezbędne do poprawnego uruchomienia rozwiązania. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 2 fizycznych procesorów (brak ograniczeń liczby obsługiwanych rdzeni) oraz co najmniej 64 GB pamięci RAM w środowisku fizycznym, b) Możliwość uruchamiania min. 2 maszyn wirtualnych,

	c) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, d) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), e) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,

	u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, VI. szyfrowanie plików i folderów, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 2 aktywnych środowisk wirtualnych systemów operacyjnych. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej

	karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlanie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 800W każdy
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 • 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.
Diagnostyka	Serwer wyposażony w 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
Certyfikaty/normy	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub inna równoważną. Serwer musi posiadać deklaracja CE lub inny równoważny. 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.

Warunki gwarancji	Minimum 3 lat (36 miesięcy) gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta. Zamawiający wymaga dołączenia dokumentów potwierdzających, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 lub inny równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń Wymagane dołączenie do oferty dokumentów potwierdzających, 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.
Ilość	1 szt.

2.Przełączniki zarządzalne

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Porty	Minimum 48 porty 10/100/1000Mbps RJ45, minimum 2 porty SFP/SFP+ 1/10GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE

	Obsługa modułów SFP+: 10GbE, SR, LR, ER
Wydajność przełącznika	Minimum 8000 adresów MAC Switch fabric capacity min. 100Gbps Forwarding rate min. 100Mpps Pamięć flash min. 16MB
Funkcjonalność warstwy II	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
Inne Funkcjonalności	Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIv2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB

	2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIv2 2246 TLS v1 2271 SNMP Framework MIB 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Inne	Przystosowanie do pracy w temperaturze 0-40 stopni Celsjusza
Ilość	2 szt.

3.Urządzenie do backupu

Specyfikacja sprzętowa	
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 32GB
Pamięć RAM liczba slotów	Minimum 2 sloty

Pamięć RAM - możliwość rozbudowy np. poprzez wymianę kości na większe	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 9 zatok, w tym minimum 5 zatok 3,5"
Obsługiwane dyski w zatokach 3,5"	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SSD SATA
Obsługiwane dyski w zatokach 2,5"	2.5" HDD SATA oraz 2.5" SSD SATA oraz 2,5" U2 SSD NVME (minimum 2 zatoki z interfejsem U2)
Pojemność dysków twardych o pojemności	do 20TB
Dyski twarde	zamontowane min.4 dyski 3,5-cala HDD, min. 8TB SATA, 7200RPM, 256MB cache, przeznaczony do pracy 24/7, gwarancja producenta 36 miesięcy z transferem do 255MB/s
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2x RJ-45
Porty LAN 10 GbE	Minimum 1x RJ-45
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen2	Minimum 3
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40˚C

Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	max. 130W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek

Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer. Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN

Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL

	Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	Minimum 3 lata
Ilość	1 kpl

4.Oprogramowanie do backupu

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do backupu i archiwizacji komputerów w sieciach LAN
Wymagania funkcjonalne	• Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich • Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, Linux, BSD, Mac OS X, QNAP, Synology • Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, Linux, BSD, Mac OS X, QNAP, Synology • Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) • Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS) • Automatyczny backup przy wyłączaniu komputera

	• Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ? • Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows) • Backup baz danych i plików poczty w trybie online i offline • Kopie rotacyjne (wersjonowanie) • Zapis archiwów w otwartym formacie (ZIP 64-bit) • Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) • Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej • Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych • Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO • Kompresja po stronie stacji roboczej • Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, • Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows) • Centralne sterowanie całym Systemem z jednego miejsca • Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników • Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN • Wysyłanie Alertów administracyjnych na e-mail • Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych • Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki • Automatyczna aktualizacja oprogramowania na komputerach zdalnych
Licencja	Licencja dla: Min. 30 stanowisk klienckich Bezterminowa licencja - licencja nie może być ograniczona czasowo z dodatkowym wsparciem technicznym producenta na okres minimum 12 miesięcy
Wymagania dodatkowe	Interfejs, instrukcja i pomoc techniczna w języku polskim
Ilość	1 kpl.

5.Oprogramowanie do monitorowania sieci

Nazwa	Minimalne wymagania dla oprogramowania

Typ	Oprogramowanie do monitorowania sieci i pracowników posiadające następujące minimalne funkcjonalności
Monitorowanie infrastruktury	Oprogramowanie musi umożliwiać minimum: Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci. Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów. Serwerów pocztowych: - program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę, - program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS), w razie, gdyby przestały one odpowiadać lub funkcjonowały wadliwie, - program powinien mieć możliwość wykonywania operacji testowych, - program powinien mieć możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa. Monitorowanie serwerów WWW i adresów URL. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP). Obsługa komunikatów syslog i pułapek SNMP. Monitoring routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych, - ruchu generowanego przez podłączone stacje robocze. Wydajności systemów z rodziny Windows posiadanych przez Zamawiającego: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
Gromadzenie informacji o sprzęcie i oprogramowaniu	Oprogramowanie musi umożliwiać minimum: Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.

	Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. Możliwość odczytania numeru seryjnego (klucze licencyjne). Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań.
Zdalna pomoc dla użytkowników	Oprogramowanie musi umożliwiać minimum: W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. Pobieranie listy użytkowników z usługi katalogowej, Przypisywanie pracowników helpdesk do kategorii zgłoszeń. Procesowanie zgłoszeń użytkowników z wiadomości e-mail. Dołączanie załączników do zgłoszeń. Zrzuty ekranowe (podgląd pulpitu). Dystrybucję oprogramowania przez Agentów. Dystrybucję oraz uruchamianie plików za pomocą Agentów. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń. Planowanie nieobecności pracowników helpdesk. Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA). Generowanie raportów obsługi helpdesk. Zdalne wykonywanie poleceń poprzez Agentów (utworzenie / edycja konta lokalnego użytkownika systemu). Możliwość użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Oprogramowanie powinno posiadać komunikator. Oprogramowanie powinno posiadać bazę zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.

Licencja	Licencja powinna pozwalać na bezpłatne użytkowanie oprogramowania przez minimum 30 użytkowników wraz z suportem producenta dostępnego przez minimum 12 miesięcy.
Ilość	1 szt.

6.Urządzenie klasy UTM

Nazwa	Minimalne wymagania dla urządzenia
Typ	Urządzenie klasy UTM wraz z niezbędnymi serwisami i aktualizacjami oraz wdrożeniem i szkoleniem

Wymagania techniczne	Dostarczone urządzenie klasy UTM musi posiadać następujące minimalne funkcje: 1. Obsługa sieci w zakresie minimum: Urządzenie musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. 2. Zapora korporacyjna musi posiadać minimum: ● Urządzenie musi być wyposażone w Firewall klasy Stateful Inspection. ● Urządzenie musi obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. ● Urządzenie musi dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). ● Interface (GUI) do konfiguracji firewall musi umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca musi mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. ● Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokalizacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. ● Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. ● Administrator musi mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall. ● Edytor reguł na firewallu musi posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). ● Firewall musi umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). 3. INTRUSION PREVENTION SYSTEM (IPS) w zakresie minimum: ● System detekcji i prewencji włamań (IPS) musi być zaimplementowany w jądrze systemu i ma wykrywać

	włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. ● Urządzenie musi posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. ● Moduł skanujący musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. ● Moduł musi nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu. ● Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. ● Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. ● Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. ● Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. ● Urządzenie musi mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. ● Administrator urządzenia musi mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. ● Urządzenie musi mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 4. Kształtowanie pasma (Traffic Shapping) w zakresie minimum: ● Urządzenie musi mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. ● Ograniczenie pasma lub priorytetyzacja musi być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. ● Rozwiązanie musi umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). ● Urządzenie musi umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

	5. Ochrona antywirusowa w zakresie minimum: ● Rozwiązanie musi zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). ● Co najmniej jeden z dwóch skanerów antywirusowych musi być dostarczany w ramach podstawowej licencji. ● Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. ● Urządzenie musi być dostarczone wraz z komercyjnym skanerem Antywirusowym, nie dopuszcza się stosowania skanera rozwijanego w ramach projektów OpenSource. ● Administrator musi mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. 6. Ochrona antyspam w zakresie minimum: ● Producent musi udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). ● Ochrona antyspam musi działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. ● W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. ● Wpis w nagłówku wiadomości zaklasyfikowanej jako spam musi być w formacie zgodnym z formatem programu Spamassassin. 7. WIRTUALNE SIECI PRYWANTE (VPN) minimum: ● Urządzenie musi posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). ● Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN ● SSL VPN musi działać w trybach Tunel i Portal. ● W ramach funkcji SSL VPN producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.

	● Urządzenie musi posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). ● Urządzenie musi posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. ● Urządzenie musi umożliwiać tworzenie tuneli w oparciu o technologię Route Based. 8. Filtr dostępu do stron WWW w zakresie minimum: ● Urządzenie musi posiadać wbudowany filtr URL. ● Filtr URL musi działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. ● Administrator musi mieć możliwość dodawania własnych kategorii URL. ● Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. ● Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. ● Administrator musi posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. ● Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. ● Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. ● Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. ● Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. ● Urządzenie musi posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 9. Uwierzytelnianie w zakresie minimalnym: ● Urządzenie musi zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. ● Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. ● Rozwiązanie musi zezwalać na uruchomienie specjalnego portalu, który umożliwia

	● autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. ● Urządzenie musi posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. ● Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. ● Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. 10. Administracja łączami do internetu (isp) w zakresie minimalnym: ● Urządzenie musi posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). ● Mechanizm równoważenia obciążenia łącza internetowego musi działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. ● Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. ● Urządzenie musi posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. ● Urządzenie musi posiadać mechanizm statycznego trasowania pakietów. ● Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. ● Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. ● Rozwiązanie musi zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 11. Dodatkowe wymagania minimalne: ● Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. ● Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. ● Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. ● Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS

	● Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. ● Urządzenie musi posiadać usługę DNS Proxy. 12. Administracja urządzeniem – wymagania minimalne: ● Konfiguracja urządzenia musi być możliwa z wykorzystaniem polskiego interfejsu graficznego. ● Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. ● Komunikacja może odbywać się na porcie innym niż https (443 TCP). ● Urządzenie musi być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. ● Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. ● Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. ● Urządzenie musi mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). ● Rozwiązanie musi mieć możliwość eksportowania logów za pomocą protokołu IPFIX. ● Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. ● Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. ● Urządzenie musi posiadać funkcjonalność anonimizacji logów. ● Urządzenie musi mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów ● Wraz z urządzeniem musi zostać dostarczona kompatybilna z urządzeniem klasy UTM, karta pamięci typu SD o pojemności minimum 128GB, o klasie prędkości minimum 10. 13. Raportowanie – zakres minimalny: ● Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

	● System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. ● System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. ● System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. ● System raportujący musi dawać możliwość edycji konfiguracji z poziomu raportu. ● W ramach podstawowej licencji zamawiający musi otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. ● Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy 14. Parametry minimalne dla sprzętu: ● Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. ● Liczba portów Ethernet 10/100/1000Mbps – min.8. ● Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. ● Przepustowość Firewall – min. 2 Gbps. ● Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min. 1.6 Gbps. ● Przepustowość filtrowania Antywirusowego – min. 400 Mbps. ● Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps. ● Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 50. ● Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. ● Obsługa min. VLAN 64. ● Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15000 nowych sesji/sekundę. ● Urządzenie nie może być nielimitowane na użytkowników. ● Urządzenie musi mieć możliwość utworzenia 4096 reguł filtrowania. ● Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów.
Gwarancja	Wymaga się, aby dostawa obejmowała również minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.

Dodatkowe	Wymagane jest dostarczenie wraz z urządzeniem klasy UTM półki do szafy rackowej „19” W ramach dostawy Wykonawca zobowiązany jest do przeprowadzenia: Wdrożenie -Wstępna konfiguracja urządzenia (zaadresowanie interface'ów, konfiguracja routingu, DNS, NTP), -Konfiguracja profilów administracyjnych, Podpięcie weryfikacja statusu licencji, -Konfiguracja obiektów adresowych na potrzeby polityk Firewall (na podstawie przygotowanej wcześniej listy), -Konfiguracja polityk Firewall pomiędzy strefami bezpieczeństwa, -Weryfikacja komunikacji pomiędzy strefami bezpieczeństwa, -Konfiguracja lokalnej bazy użytkowników oraz zdefiniowanie grup, oraz podłączenie do usługi LDAP/AD Konfiguracja VPN wg potrzeby -Konfiguracja IPSec VPN site-to-site, --Konfiguracja IPSec VPN client-to-site, -Konfiguracja SSL VPN client-to-site, -Konfiguracja profilów kontroli Antywirusowej i podpięcie do polityk FW, -Konfiguracja profilów ochrony przed atakami IPS i podpięcie do polityk FW, -Konfiguracja profilów kontroli aplikacji i podpięcie do polityk FW, -Konfiguracja profilów kontroli WWW i podpięcie do polityk FW, -Konfiguracja profilów antyspamowych i podpięcie do polityk FW, -Test zastosowanych funkcji ochronnych, -Przygotowania ogólnej dokumentacji z zakresu zdefiniowanych funkcji. Instruktaż Wymagane jest, aby wdrożenie oraz instruktaż został wykonany przez inżynierów certyfikowanych przez producenta dostarczonego rozwiązania klasy UTM (certyfikaty inżynierów należy dołączyć do oferty w minimalnym zakresie: -Przeszkolenie z zakresu zarządzania wszystkimi elementami podlegającymi konfiguracji w punkcie “Wdrożenie” -Szkolenie musi trwać minimum 3h -Szkolenie z odtwarzania konfiguracji po awarii urządzenia backup lokalny/backup z chmury producenta. -Przeszkolenie z zakresu prostych narzędzi do rozwiązywania problemów.
Ilość	1 szt.

7.Audyt cyberbezpieczeństwa

Nazwa	Minimalne wymagania dla usługi
Typ	Wykonanie audytu diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej - Cyfrowa Gmina. Diagnoza cyberbezpieczeństwa powinna zostać przeprowadzona w terminie do 3 miesięcy od podpisania umowy. Wynikiem przeprowadzenia diagnozy musi być raport dotyczący audytowanego środowiska oraz wypełnienie formularza diagnozy i dostarczenia go za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: /NASK-Instytut/SkrytkaESP.
Plan audytu	Audyt musi składać się z minimum: 1. Audyt dokumentacji i procesów: - ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC) - ocena wybranych aspektów bezpieczeństwa systemów informatycznych - ocena dojrzałości wybranych procesów bezpieczeństwa - opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny 2. Testy penetracyjne infrastruktury sieciowej - Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci - skanowanie sieci, rekonesans sieci (skanowanie musi zostać powtórzone dla każdej wskazanej przez Zamawiającego sieci) - skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), który zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł - weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych - weryfikacja zabezpieczeń urządzeń sieciowych - testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej - wykonanie raportu zawierającego minimum: ● opis wszystkich elementów, które zostały poddane audytowi ● podział podatności ze względu na ryzyko: wysoki, średni, niski ● wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności ● wylistowanie wszystkich podatności ze względu na ryzyko: wysoki, średni, niski

	● określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności - Wsparcie poaudytowe - Udzielenie informacji na temat audytowanych elementów wynikających z raportu. Czas dla klienta na zapoznanie się z raportem i zadawanie pytań odnośnie raportu.
Wymagania dla audytora	Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu: 1. Certified Internal Auditor (CIA); 2. Certified Information System Auditor (CISA); 3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób; 4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób; 5. Certified Information Security Manager (CISM); 6. Certified in Risk and Information Systems Control (CRISC); 7. Certified in the Governance of Enterprise IT (CGEIT); 8. Certified Information Systems Security Professional (CISSP); 9. Systems Security Certified Practitioner (SSCP); 10. Certified Reliability Professional; 11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

Wymagania dodatkowe

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.