

Znak postępowania: AIR.271.8.2025

Zał. nr 1A do SWZ

Część 1 – Wzmocnienie cyberbezpieczeństwa w Gminie Pszów poprzez dostawę sprzętu sieciowego i komputerowego oraz licencji systemowych

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa, wdrożenie i utrzymanie systemu UTM spełniającego wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Typ	Dwa urządzenia sieciowe typu UTM pracujące w trybie klastra HA wraz z niezbędnymi licencjami pozwalającymi na ich używanie co poprawi wyniki związane z zarządzaniem ciągłością działania.
Licencja	2 lata.
Zawartość licencji	Licencja powinna pozwalać na korzystanie z funkcji Firewall z IPS, bezpiecznych połączeń VPN, filtrowania stron na podstawie 15 kategorii tematycznych, antywirusa oraz antyspam.
Obsługa sieci	Urządzenie ma 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.
Firewall	<ol style="list-style-type: none"> 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion Prevention System (IPS)	<ol style="list-style-type: none"> 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator ma 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. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (Traffic Shapping)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antyspam	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: <ol style="list-style-type: none"> a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: <ol style="list-style-type: none"> a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 3. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

Filtr dostępu do stron WWW	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator ma mieć możliwość dodawania własnych kategorii URL. 4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: <ol style="list-style-type: none"> 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. 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
Uwierzytelnianie	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: <ol style="list-style-type: none"> a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: <ol style="list-style-type: none"> a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Administracja łączami do Internetu (ISP)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy: <ol style="list-style-type: none"> a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.

Routing (trasowanie)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
Administracja urządzeniem	<ol style="list-style-type: none"> 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: <ol style="list-style-type: none"> a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

Raportowanie	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 5. Urządzenie ma posiadać usługę DNS Proxy. 6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 7. Urządzenie musi mieć zaimplementowane Open API 8. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. 9. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
Gwarancja i serwis	<ol style="list-style-type: none"> 1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

Parametry sprzętowe	<ol style="list-style-type: none"> 1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. 3. Liczba portów Ethernet 2,5Gbps – min. 8. 4. Liczba portów światłowodowych 1Gbps – min. 1. 5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 6. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps. 7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. 8. Przepustowość filtrowania Antywirusowego – minimum 1Gbps. 9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps. 10. Maksymalna liczba tuneli VPN IPSec – minimum 100. 11. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100. 12. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 100. 13. Obsługa interfejsów 802.11q (VLAN) – minimum 128 14. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę. 15. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 16. Urządzenie nie ma limitu na liczbę użytkowników. 17. Liczba reguł filtrowania – minimum 8 192. 18. Liczba tras statycznego routingu – minimum 512. 19. Liczba tras dynamicznego routingu – minimum 10 000. 20. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. 21. Urządzenie musi być wyposażone w moduł TPM.
Prace wdrożeniowe	<p>Wykonania pełnego audytu obecnej konfiguracji oraz przeprojektowanie i wdrożenie wszystkich istniejących obecnie reguł zapory sieciowej i NAT w nowych urządzeniach. Wydzielenie VLAN w szczególności dla systemów backupu, dla dostępu pracowników do aplikacji wewnętrznych oraz dla sieci bezprzewodowej. Przeprowadzenie testów funkcjonalnych i wydajnościowych dla każdej podsieci, w tym symulacja scenariuszy awaryjnych w celu weryfikacji działania klastra HA.</p> <p>Optymalizacja konfiguracji na podstawie wyników testów, zapewniająca maksymalną wydajność i bezpieczeństwo.</p> <p>Przeprowadzenie szkolenia administratorów, które zapewnią kompleksową możliwość konfiguracji i obsługi dostarczonego rozwiązania.</p> <p>Zapewnienie wsparcia technicznego przez okres co najmniej 3 miesięcy po wdrożeniu, obejmującego pomoc w rozwiązywaniu problemów i optymalizacji konfiguracji. Możliwość zdalnego lub lokalnego wsparcia w przypadku incydentów związanych z działaniem urządzeń UTM.</p>



Dostawa 10 szt. zarządzalnych przełączników sieciowych (switch) spełniających wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Typ	Zarządzalny przełącznik sieciowy (switch).
Porty	<ul style="list-style-type: none"> • 8 portów RJ45 10/100/1000 Mb/s • 2 gigabitowe sloty SFP • 1 port konsolowy RJ45 1 port konsolowy microUSB
Zasilanie	100-240 V AC~50/60 Hz
Montaż	Możliwość montażu w szafie rack/na blacie
Maks. zużycie energii	7 W
Wydajność przełącznika	20 Gb/s
Szybkość przekierowań pakietów	14,89 Mp/s
Tablica adresów MAC	8K
Bufor pakietów	4,1 Mb
Ramki jumbo	9 KB
Funkcja Quality of Service	<ul style="list-style-type: none"> • 8 kolejek priorytetowania • Obsługa priorytetowania 802.1p CoS/DSCP • Tryb harmonogramu priorytetowania: <ul style="list-style-type: none"> - SP (Strict Priority) - WRR (Weighted Round Robin) - SP+WRR • Kontrola przepustowości - Ograniczanie prędkości transferu w oparciu o port/przepływ danych • Płynniejsze działanie • Działania dla przepływów <ul style="list-style-type: none"> - Mirror (do obsługiwanego interfejsu) - Redirect (do obsługiwanego interfejsu) - Limit prędkości - QoS Remark
Cechy przełącznika L3	<ul style="list-style-type: none"> • 16 interfejsów IPv4/IPv6 • Routing statyczny <ul style="list-style-type: none"> - 48 tras statycznych • Statyczne wpisy ARP • 316 wpisów ARP • Proxy ARP • Gratuitous ARP • Serwer DHCP • DHCP Relay • DHCP L2 Relay
Funkcje L2 i L2+	<ul style="list-style-type: none"> • Agregacja łączy <ul style="list-style-type: none"> - Statyczna agregacja łączy - LACP 802.3ad - Do 8 grup agregacji i do 8 portów na grupę • Protokół drzewa rozpinającego (STP) <ul style="list-style-type: none"> - STP 802.1D - RSTP 802.1w - MSTP 802.1s - Zabezpieczenia STP: ochrona TC, filtrowanie poprzez pakiety BPDU, ochrona BPDU, ochrona Root • Wykrywanie pętli zwrotnych <ul style="list-style-type: none"> - Oparte na portach - Oparte na VLAN • Kontrola przepływu <ul style="list-style-type: none"> - Kontrola przepływu 802.3x - Zapobieganie blokowaniu HOL • Mirroring <ul style="list-style-type: none"> - Port Mirroring - Mirroring procesora - Przesył One-to-One - Przesył Many-to-One - Port wejścia/wyjścia / obydwie porty

L2 Multicast	<ul style="list-style-type: none"> • Obsługa 511 grup IGMP (IPv4, IPv6) • IGMP Snooping <ul style="list-style-type: none"> - IGMP v1/v2/v3 Snooping - Fast Leave - IGMP Snooping Querier - Uwierzytelnianie IGMP • Uwierzytelnianie IGMP • MVR • MLD Snooping <ul style="list-style-type: none"> - MLD v1/v2 Snooping - Fast Leave - MLD Snooping Querier - Konfiguracja grupy statycznej - Ograniczone przekazywanie IP Multicast • Filtrowanie transmisji Multicast: 256 profili i 16 wpisów na profil
Funkcje zaawansowane	<ul style="list-style-type: none"> • Automatyczne wykrywanie urządzeń • Konfiguracje grupowe • Grupowe aktualizacje oprogramowania • Inteligentne monitorowanie stanu sieci • Ostrzeżenia o nietypowych zdarzeniach • Ujednolicony proces konfiguracji • Harmonogram restartu
Sieci VLAN	<ul style="list-style-type: none"> • Grupy VLAN <ul style="list-style-type: none"> - Maks. 4K grup VLAN • Tagowanie 802.1Q VLAN • Adres MAC VLAN: 12 wpisów • Protokół VLAN • GVRP • VLAN VPN (QinQ) <ul style="list-style-type: none"> - QinQ oparty na portach - Selective QinQ • Głosowa sieć VLAN
Listy kontroli dostępu	<ul style="list-style-type: none"> • Lista kontroli dostępu (ACL) oparta o czas • Adres MAC ACL <ul style="list-style-type: none"> - Źródłowy adres MAC - Docelowy adres MAC - ID sieci VLAN - User Priority - Ethertype • Adres IP ACL <ul style="list-style-type: none"> - Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu • Łączona ACL • Polityka kontroli dostępu <ul style="list-style-type: none"> - Mirroring - Limit prędkości - Redirect - QoS Remark • ACL do portu/VLAN
Bezpieczeństwo transmisji	<ul style="list-style-type: none"> • Wiązanie adresów IP, MAC i portów <ul style="list-style-type: none"> - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4 • Wiązanie adresów IPv6, MAC i portów <ul style="list-style-type: none"> - DHCPv6 Snooping - Wykrywanie ND



	<ul style="list-style-type: none"> - Ochrona źródłowego adresu IPv6 • Ochrona przed atakami DoS • Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację - Do 64 adresów MAC na port • Storm Control Broadcast/Multicast/Unicast - tryb kontroli (kb/s/wskaźnik) • Kontrola dostępu w oparciu o IP/port/MAC • Uwierzytelnianie 802.1X - Uwierzytelnianie w oparciu o port - Uwierzytelnianie w oparciu o adres MAC - Przydzielanie VLAN - MAB - Sieć VLAN dla gości - Uwierzytelnianie i autoryzowanie poprzez Radius • AAA (w tym TACACS+) • Izolacja portów • Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2 • Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2
IPv6	<ul style="list-style-type: none"> • IPv6 Dual IPv4/IPv6 • Multicast Listener Discovery (MLD) Snooping • ACL IPv6 • Interfejs IPv6 • Statyczny routing IPv6 • Funkcja neighbor discovery (ND) wykorzystywana przez węzły IPv6 • Path maximum transmission unit (MTU) discovery • ICMP v6 • TCP v6/UDP v6 • Zastosowania protokołu IPv6: <ul style="list-style-type: none"> - Klient DHCPv6 - Ping6 - Tracert6 - Telnet (v6) - SNMP IPv6 - SSH IPv6 - SSL IPv6 - Http/Https - TFTP IPv6
MIB	<ul style="list-style-type: none"> • MIB II (RFC1213) • Bridge MIB (RFC1493) • P/Q-Bridge MIB (RFC2674) • Radius Accounting Client MIB (RFC2620) • Radius Authentication Client MIB (RFC2618) • Zdalny Ping, Traceroute MIB (RFC2925) • Wsparcie dla prywatnego TP-Link MIB • RMON MIB(RFC1757, rmon 1,2,3,9)
Funkcje panelu zarządzania	<ul style="list-style-type: none"> • Interfejs graficzny GUI • Interfejs linii poleceń CLI • SNMP v1/v2c/v3 <ul style="list-style-type: none"> - Trap/Inform - RMON (grupy 1, 2, 3, 9) • Szablon SDM • Klient DHCP/BOOTP • 802.1ab LLDP/LLDP-MED • Autoinstalacja DHCP • Dual Image, Dual Configuration • Monitorowanie zużycia procesora • Diagnostyka kabli • EEE • Odzyskiwanie hasła • SNTP • Logi systemowe
Certyfikaty	CE, FCC, RoHS
Zawartość opakowania	<ul style="list-style-type: none"> • Przełącznik • Przewód zasilający



	<ul style="list-style-type: none">• Instrukcja instalacji• Zestaw montażowy• Gumowe nóżki
Warunki gwarancji	Gwarancja producenta - 2 lata.

Dostawa 3 szt. zarządzalnych przełączników sieciowych (switch) spełniających wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Typ	Zarządzalny przełącznik sieciowy (switch).
Porty	<ul style="list-style-type: none"> • 24 porty RJ45 10/100/1000 Mb/s • 4 sloty SFP+ 10 G • 1 port konsolowy RJ45 • 1 port konsolowy microUSB
Zasilanie	100-240 V AC~50/60 Hz
Montaż	Możliwość montażu w szafie rack/na blacie
Maks. zużycie energii	24 W
Wydajność przełącznika	128 Gb/s
Szybkość przekierowań pakietów	95,23 Mp/s
Tablica adresów MAC	16K
Bufor pakietów	12 Mb
Ramki jumbo	9 KB
Funkcja Quality of Service	<ul style="list-style-type: none"> • 8 kolejek priorytetowania • Obsługa priorytetowania 802.1p CoS/DSCP • Tryb harmonogramu priorytetowania: <ul style="list-style-type: none"> - SP (Strict Priority) - WRR (Weighted Round Robin) - SP+WRR • Kontrola przepustowości - Ograniczanie prędkości transferu w oparciu o port/przepływ danych • Płynniejsze działanie • Działania dla przepływów <ul style="list-style-type: none"> - Mirror (do obsługiwanego interfejsu) - Redirect (do obsługiwanego interfejsu) - Limit prędkości - QoS Remark
Cechy przełącznika L3	<ul style="list-style-type: none"> • 128 interfejsów IPv4/IPv6 • Routing statyczny <ul style="list-style-type: none"> - 48 tras statycznych • Wpisy statyczne ARP <ul style="list-style-type: none"> - 128 wpisów statycznych • Proxy ARP • Gratuitous ARP • Serwer DHCP • DHCP Relay <ul style="list-style-type: none"> - DHCP Interface Relay - DHCP VLAN Relay • DHCP L2 Relay
Funkcje L2 i L2+	<ul style="list-style-type: none"> • Agregacja łączy <ul style="list-style-type: none"> - Statyczna agregacja łączy - LACP 802.3ad - Do 8 grup agregacji i do 8 portów na grupę • Protokół drzewa rozpinającego (STP) <ul style="list-style-type: none"> - STP 802.1D - RSTP 802.1w - MSTP 802.1s - Zabezpieczenia STP: ochrona TC, filtrowanie poprzez pakiety BPDU, ochrona Root • Wykrywanie pętli zwrotnych <ul style="list-style-type: none"> - Oparte na portach - Oparte na VLAN • Kontrola przepływu <ul style="list-style-type: none"> - Kontrola przepływu 802.3x - Zapobieganie blokowaniu HOL • Mirroring <ul style="list-style-type: none"> - Port Mirroring - Mirroring procesora - Przesył One-to-One - Przesył Many-to-One



	- Port wejścia/wyjścia / obydwie porty
L2 Multicast	<ul style="list-style-type: none"> • IGMP Snooping - IGMP v1/v2/v3 Snooping - Fast Leave - IGMP Snooping Querier - Uwierzytelnianie IGMP • Uwierzytelnianie IGMP • MVR • MLD Snooping - MLD v1/v2 Snooping - Fast Leave - MLD Snooping Querier - Konfiguracja grupy statycznej - Ograniczone przekazywanie IP Multicast • Filtrowanie transmisji Multicast: 256 profili i 16 wpisów na profil
Funkcje zaawansowane	<ul style="list-style-type: none"> • Automatyczne wykrywanie urządzeń • Konfiguracje grupowe • Grupowe aktualizacje oprogramowania • Inteligentne monitorowanie stanu sieci • Ostrzeżenia o nietypowych zdarzeniach • Ujednolicony proces konfiguracji • Harmonogram restartu
Sieci VLAN	<ul style="list-style-type: none"> • Grupy VLAN - Maks. 4K grup VLAN • Tagowanie 802.1Q VLAN • Adres MAC VLAN: 7 wpisów • Protokół VLAN • Prywatna sieć VLAN • GVRP • VLAN VPN (QinQ) - QinQ oparty na portach - Selective QinQ • Głosowa sieć VLAN
Listy kontroli dostępu	<ul style="list-style-type: none"> • Lista kontroli dostępu (ACL) oparta o czas • Adres MAC ACL - Źródłowy adres MAC - Docelowy adres MAC - ID sieci VLAN - User Priority - Ethertype • Adres IP ACL - Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu • Łączona ACL • Polityka kontroli dostępu - Mirroring - Limit prędkości - Redirect - QoS Remark • ACL do portu/VLAN
Bezpieczeństwo transmisji	<ul style="list-style-type: none"> • Wiązanie adresów IP, MAC i portów - 512 wpisów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4: 100 wpisów • Wiązanie adresów IPv6, MAC i portów



	<ul style="list-style-type: none"> - 512 wpisów - DHCPv6 Snooping - Wykrywanie ND - Ochrona źródłowego adresu IPv6: 100 wpisów • Ochrona przed atakami DoS • Ochrona portów poprzez ich statyczną/dynamiczną/statą konfigurację - Do 64 adresów MAC na port • Storm Control Broadcast/Multicast/Unicast - tryb kontroli (kb/s/wskaźnik) • Uwierzytelnianie 802.1X - Uwierzytelnianie w oparciu o port - Uwierzytelnianie w oparciu o adres MAC - Przydzielanie VLAN - MAB - Sieć VLAN dla gości - Uwierzytelnianie i autoryzowanie poprzez Radius • AAA (w tym TACACS+) • Izolacja portów • Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2 • Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2 • Kontrola dostępu w oparciu o IP/port/MAC
IPv6	<ul style="list-style-type: none"> • IPv6 Dual IPv4/IPv6 • Multicast Listener Discovery (MLD) Snooping • ACL IPv6 • Interfejs IPv6 • Statyczny routing IPv6 • Funkcja neighbor discovery (ND) wykorzystywana przez węzły IPv6 • Path maximum transmission unit (MTU) discovery • ICMP v6 • TCP v6/UDP v6 • Zastosowania protokołu IPv6: - Klient DHCPv6 - Ping6 - Tracert6 - Telnet (v6) - SNMP IPv6 - SSH IPv6 - SSL IPv6 - Http/Https - TFTP IPv6
MIB	<ul style="list-style-type: none"> • Bazy danych MIB II (RFC1213) • Porty MIB (RFC2233) • Port Ethernet MIB (RFC1643) • Bridge MIB (RFC1493) • P/Q-Bridge MIB (RFC2674) • RMON MIB (RFC2819) • RMON2 MIB (RFC2021) • Radius Accounting Client MIB (RFC2620) • Radius Authentication Client MIB (RFC2618) • Pakiety Ping i Traceroute do interfejsu MIB (RFC2925) • Obsługa prywatnych baz danych MIB TP-Link
Funkcje panelu zarządzania	<ul style="list-style-type: none"> • Interfejs graficzny GUI • Interfejs linii poleceń CLI • SNMP v1/v2c/v3 - Trap/Inform - RMON (grupy 1, 2, 3, 9) • Szablon SDM • Klient DHCP/BOOTP • 802.1ab LLDP/LLDP-MED • Autoinstalacja DHCP • Dual Image, Dual Configuration • Monitorowanie zużycia procesora • Diagnostyka kabli • EEE



	<ul style="list-style-type: none">• Odzyskiwanie hasła• SNTP• Logi systemowe
Certyfikaty	CE, FCC, RoHS
Zawartość opakowania	<ul style="list-style-type: none">• Przełącznik• Przewód zasilający• Instrukcja instalacji• Zestaw montażowy• Gumowe nóżki
Warunki gwarancji	Gwarancja producenta - 2 lata.



Dostawa 10 szt. zasilaczy awaryjnych UPS spełniającego wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Typ	Zasilacz awaryjny UPS.
Akumulator	1 x 12V/9Ah
Moc	480W
Napięcie wejściowe	220/230/240 V
Częstotliwość wejściowa	50/60 Hz
Napięcie wyjściowe	230V AC
Częstotliwość wyjściowa	50Hz lub 60Hz (automatyczne wykrywanie)
Czas reakcji	2-6 ms
Kształt napięcia wyjściowego	Modyfikowana sinusoida
Czas ładowania	6-8 h
Gniazda	6x Schuko
Moc pozorna	600VA-999VA
topologia	Line-Interactive AVR
Zabezpieczenia	termiczne, przeciwprzepięciowe, przeciwzwarcowe
Zabezpieczenie przed przepięciami	RJ45
Warunki gwarancji	Gwarancja - 2 lata. Gwarancja na akumulator - 12 miesięcy.

Dostawa i wdrożenie rozwiązania do tworzenia i odtwarzania kopii zapasowych spełniającego wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Typ	Dedykowany serwer i oprogramowanie do realizacji oraz odtwarzania kopii zapasowych.
Konstrukcja	<p>Typu RACK, wysokość 2U;</p> <p>Szyny umożliwiające wysunięcie serwera z szafy stelażowej, umożliwiające instalację ramienia porządkującego kable;</p> <p>Możliwość zainstalowania 10 dysków twardych hot plug 3,5”;</p> <p>Możliwość rozbudowy o fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;</p> <p>Zainstalowane 2 szt. dysków SSD SATA 960GB Hot-Plug DWPD min 5 oraz 3 szt. 8TB SATA Hot Plug;</p> <p>Możliwość instalacji wewnętrznego napędu optyczny umożliwiający zapisanie 25GB danych na jednym nośniku.</p>
Płyta główna	<p>Dwuprocesorowa;</p> <p>Wyprodukowana i zaprojektowana przez producenta serwera;</p> <p>Możliwość instalacji procesorów 38-rdzeniowych;</p> <p>Zainstalowany moduł TPM 2.0;</p> <p>6 złącz PCI Express generacji 4 w tym:</p> <p>4 fizyczne złącza o prędkości x16;</p> <p>2 fizyczne złącza o prędkości x8;</p> <p>Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;</p> <p>Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;</p> <p>32 gniazda pamięci RAM;</p> <p>Obsługa minimum 6 TB pamięci RAM DDR4;</p> <p>Wsparcie dla technologii:</p> <p>Memory Scrubbing;</p> <p>SDDC;</p> <p>ECC;</p> <p>Memory Mirroring;</p> <p>ADDDC;</p> <p>Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.</p>
Procesory	<p>Procesor 8-rdzeniowy, taktowanie bazowe 2,8GHz, architektura x86_64.</p> <p>W teście SPEC CPU2017 Integer Rate wynik SPECrate2017_int_base 130 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta.</p>
Pamięć RAM	<p>64 GB pamięci RAM.</p> <p>DDR4 Registered 3200MT/s.</p>
Dyski twarde	Zainstalowane 2 szt. dysków SSD SATA 960GB Hot-Plug DWPD min 5 oraz 3 szt. 8TB SATA Hot Plug
Kontrolery LAN	<p>4x 1Gbit Base-T</p> <p>2x 10Gbit SFP+</p>
Kontrolery I/O	Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache zabezpieczonej przed utratą danych w przypadku zaniku zasilania, obsługujący poziomy RAID: 0,1,10,5,50,6,60
Porty	<p>Zintegrowana karta graficzna ze złączem VGA z tyłu serwera,</p> <p>2 porty USB 3.0 dostępne z tyłu serwera,</p> <p>2 porty USB 3.0 na panelu przednim,</p> <p>2 porty USB 3.0 wewnątrz serwera,</p> <p>Możliwość rozbudowy o 1 port serial, możliwość wykorzystania portu serial do zarządzania serwerem,</p> <p>Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych</p>



	przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
Zasilanie, chłodzenie	Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W, Redundantne wentylatory hotplug.
Zarządzanie	<p>Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;</p> <ul style="list-style-type: none"> informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: <ul style="list-style-type: none"> karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express; procesory CPU; pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM; nośnik pamięci M.2 SSD; status karty zarządzającej serwera; wentylatory; bateria podtrzymująca ustawienia BIOS płyty głównej; zasilacze; system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym); <p>Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p> <ul style="list-style-type: none"> Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; Dostęp poprzez przeglądarkę Web, SSH; Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; Zarządzanie alarmami (zdarzenia poprzez SNMP); Możliwość przejęcia konsoli tekstowej; Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); Obsługa serwerów proxy (autentykacja); Obsługa VLAN; Możliwość konfiguracji parametru Max. Transmission Unit (MTU); Wsparcie dla protokołu SSDP; Obsługa protokołów TLS 1.2, SSL v3; Obsługa protokołu LDAP; Integracja z HP SIM; Synchronizacja czasu poprzez protokół NTP; Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; <p>Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski,</p>



	<p>zasilacze, płyta główna, procesory, pamięć operacyjna);</p> <p>Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;</p> <p>Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.</p>
Wspierane OS	<p>Microsoft Windows Server 2022, 2019;</p> <p>VMWare vSphere 8.0;</p> <p>Suse Linux Enterprise Server 15;</p> <p>Red Hat Enterprise Linux 9, 8;</p> <p>Microsoft Hyper-V Server 2019.</p>
Gwarancja	<p>5 lat gwarancji producenta serwera w trybie on-site z czasem reakcji do końca następnego dnia od zgłoszenia z opcją pozostawienia zepsutych dysków u klienta. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.</p> <p>Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w systemie helpdesk/servicedesk producenta sprzętu;</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;</p> <p>Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;</p> <p>Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).</p>
Certyfikaty	Zgodność z normami: CB, RoHS, WEEE oraz CE.
Dokumentacja, inne	<p>Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta.</p> <p>Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta.</p> <p>Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila, na który można zgłaszać usterki.</p> <p>W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardej, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji.</p> <p>Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.</p>
Oprogramowanie	<p>Wdrożenie rozwiązania zapewniającego odporność na ataki złośliwego oprogramowania ransomware. Rozwiązanie ze statutem zgodności z kluczowymi regulacjami dotyczącymi niezmienności przechowywania danych, m.in.:</p> <ul style="list-style-type: none"> • w Stanach Zjednoczonych: <ul style="list-style-type: none"> SEC 17a-4(f), FINRA 4511(c), CFTC 1.31(c)-(d), • w Niemczech: <ul style="list-style-type: none"> IDW PS 880.
Bezpieczeństwo kopii zapasowych	<p>Proponowane rozwiązanie powinno zabezpieczać kopie zapasowe składowane na nośnikach dyskowych i pod względem odporności na ransomware musi być równoważne do wdrożenia biblioteki taśmowej (taśmy streamera posiadają natywną odporność na ransomware).</p> <p>Proponowane rozwiązanie powinno być oparte na obiektowej pamięci masowej z niezmiennością (immutability). Repozytorium (nośnik kopii zapasowych) powinno stanowić fizyczny serwer.</p>



	<p>Bezpieczeństwo składowania kopii zapasowych powinno być zapewnione poprzez odpowiednią instalację i konfigurację (hardening) systemu.</p> <p>Pliki kopii zapasowych muszą mieć ustawiany atrybut „immutability”, który uniemożliwia usunięcie lub modyfikację kopii zapasowej przed wcześniej zdefiniowanym okresem czasu.</p> <p>Repozytorium musi być zainstalowane na serwerze sprzętowym, nie wirtualnym.</p> <p>Proponowane repozytorium może być podstawowym miejscem składowania kopii zapasowych, jak i dodatkowym.</p>
Wdrożenie	<p>Wdrożenie powinno obejmować następujące działania:</p> <ul style="list-style-type: none">• Konfiguracja serwera sprzętowego.• Instalacja i konfiguracja (hardening) systemu operacyjnego.• Instalacja i konfiguracja repozytorium na serwerze.• Konfiguracja zadań backupu.• Szkolenie administratorów z podstawowej obsługi systemu.• Opracowanie dokumentacji powykonawczej. <p>Zamawiający wymaga także usługi wdrożenia serwera, w tym w szczególności instalacji i konfiguracji serwerów backup na dedykowanej infrastrukturze, a także integrację z istniejącymi serwerami i systemami IT.</p> <p>Zapewnienie wsparcia technicznego przez okres co najmniej 3 miesięcy po wdrożeniu, obejmującego pomoc w rozwiązywaniu problemów i optymalizacji konfiguracji. Możliwość zdalnego lub lokalnego wsparcia w przypadku incydentów związanych z działaniem serwera backupu.</p>
Rok produkcji	<p>Serwer musi być fabrycznie nowy i nieużywany przed dniem dostarczenia do siedziby Zamawiającego, z wyłączeniem użycia niezbędnego dla przeprowadzenia testu poprawnej pracy.</p> <p>Dostarczone wraz z serwerem licencje oprogramowania mają upoważniać do użytkowania oprogramowania na czas nieokreślony.</p>

Dostawa 2 kompletów licencji systemu serwerowego spełniającego wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY
Licencja	<p>Każdy komplet licencji serwerowych systemu operacyjnego musi uprawniać do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym.</p> <p>Licencje mają obejmować dwa procesory fizyczne zainstalowane w serwerze Zamawiającego, z których każdy posiada 16 rdzeni, co łącznie daje 32 rdzenie do pokrycia jednym kompletem.</p> <p>Wymagane jest, aby oba komplety licencji łącznie pokrywały wszystkie 32 rdzenie fizyczne serwera dwukrotnie, zgodnie z zasadami licencjonowania producenta, co umożliwi legalne uruchomienie czterech maszyn wirtualnych Windows Server Standard.</p> <p>Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na serwerze Zamawiającego.</p> <p>Serwerowy system operacyjny, który jest w pełni kompatybilny z licencjami dostępowymi (CAL) dla Windows Server 2019.</p> <p>Licencja nie może być ograniczona czasowo.</p>
Cechy serwerowego systemu operacyjnego	<ol style="list-style-type: none"> 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy HyperThreading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykkiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie



zdefiniowanego zestawu polityk bezpieczeństwa.

23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

- a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
- b. 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:
 - i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
- c. Zdalna dystrybucja oprogramowania na stacje robocze.
- d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
- e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http
 - ii. Konsolidację CA dla wielu lasów domeny,
 - iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- f. Szyfrowanie plików i folderów.
- g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.
- i. Serwis udostępniania stron WWW.
- j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
- k. Wsparcie dla algorytmów Suite B (RFC 4869),
- l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
 - i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - iii. Obsługi 4-KB sektorów dysków
 - iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.