



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

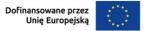
OPIS PRZEDMIOTU ZAMÓWIENIA

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

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE	
Тур	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	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.	





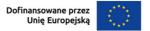




Intrusion Prevention	1.	System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma
System (IPS)		wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy
		heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
	2.	Moduł IPS ma być opracowany 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
	٥.	JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po
		usunięciu zagrożenia.
	6	
	6.	Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
	١_	
	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	1.	Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną
(Traffic Shapping)		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
	٥.	jedynie na śledzenie konkretnego typu ruchu (monitoring).
	_	
	4.	Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antyspam	1.	Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą
		niechcianą (SPAM).
	2.	Ochrona antyspam ma działać w oparciu o:
		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	1.	Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja)
prywatne (VPN)		lub site-to-site (lokalizacja-lokalizacja).
prymatric (*****)	2.	Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
	۷.	
		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.
	٥.	orządzenie nia umożniwiae tworzenie tulien irbet rolley based Oldz Route based.





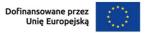




Filtr dostępu do stron	Urządzenie ma posiadać wbudowany filtr URL.	
WWW	Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co naji	mniei 50 kategorii
	tematycznych stron internetowych.	illiej 50 kategorii
	Administrator ma mieć możliwość dodawania własnych kategorii Uf	21
	Administrator ma mieć możliwość zdefiniowania akcji w przypadku	zakiasyfikowania danej strony
	do konkretnej kategorii. Do wyboru ma być przynajmniej:	
	a. blokowanie dostępu do adresu URL,	
	b. zezwolenie na dostęp do adresu URL,	
	 blokowanie dostępu do adresu URL oraz wyświetlenie stro administratora. 	ny HTML zdefiniowanej przez
	Administrator ma mieć możliwość skonfigurowania co najmniej 4 ró zablokowaniu strony.	żnych stron z komunikatem o
	Strona blokady ma umożliwiać wykorzystanie zmiennych środowisk	owych.
	Filtr URL musi uwzględniać komunikację po protokole HTTPS.	
	Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych MIME.	danych z wykorzystaniem typu
	Urządzenie ma umożliwiać stworzenie listy stron dostępnych po prodeszyfrowane.	itokole HTTPS, które nie będą
	. Urządzenie musi oferować możliwość filtrowania wyników wyszukiy	vania z użyciem SafeSearch
Uwierzytelnianie	Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmi	•
owierzy termanie	a. lokalną bazę użytkowników (wewnętrzny LDAP),	noj n oparola ol
	b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),	
	c. usługę katalogową Microsoft Active Directory.	
	Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różny	
	Urządzenie ma umożliwiać uruchomienie specjalnego portalu (capti na autoryzację użytkowników co najmniej w oparciu o protokoły:	ve portal), który ma zezwalać
	a. SSL,	
	b. Radius,	
	c. Kerberos.	
	Urządzenie ma umożliwiać transparentną autoryzację użytkowników Microsoft Active Directory w oparciu o co najmniej dwa mechanizm	
	Co najmniej jedna z metod transparentnej autoryzacji nie może wyr agenta.	
	Autoryzacja użytkowników z Microsoft Active Directory nie może w domeny.	ymagać modyfikacji schematu
	Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania	a użytkowników w ramach
	infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykow wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Ren	vanego agenta. Metoda ta musi
	Urządzenie musi posiadać wbudowany moduł zapewniający podwój	
	poprzez zastosowanie czasowych haseł jednorazowych (TOTP).	awierzyteinianie ZIA
	Wbudowany moduł 2FA musi dawać możliwość wykorzystania hase	ł TOTP w ramach tunoli
	SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, w administracyjnego i SSH.	
Administracja łączami	Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważe	nia obciażenia łaczy do sieci
do Internetu (ISP)	Internet (tzw. Load Balancing).	Obciqzeriia iączy ao sieci
20 memeta (131)	Mechanizm równoważenia obciążenia łącza internetowego ma dzia	łać w oparciu o pastepuiaco
	dwa mechanizmy:	ac w oparciu o następujące
	a. równoważenie względem adresu źródłowego,	
	 równoważenie względem połączenia. 	
	Mechanizm równoważenia obciążenia ma uwzględniać wagi przypis łączy do Internetu.	ywane osobno dla każdego z
	Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypa podstawowego (tzw. Failover).	adku awarii łącza
	Urządzenie ma wspierać mechanizm SD-WAN zapewniając automat najkorzystniejszego łącza.	yczną optymalizację i wybór
	W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu opóźnienia, jitter, wskaźnika utraty pakietów).	ı SLA (monitorowanie
	Monitorowanie dostępności łącza musi być możliwe w oparciu o ICN	MP oraz TCP
	Monitorowanie dostębności jącza masi być możnike w obatcia o ici	AIT UTAL TUT.





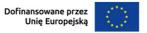




Routing (trasowanie)	Urządzenie ma umożliwiać stat	yczne trasowanie pakietów.
, , , , , , , , , , , , , , , , , , ,		owanie połączeń IPv6 co najmniej w zakresie trasowania
		przełączenia na łącze zapasowe w przypadku awarii łącza
		owanie pakietów z poziomu wybranej reguły firewall (tzw. Policy
	Urządzenie ma umożliwiać dyna RIPv2, OSPF oraz BGP.	amiczne trasowanie pakietów w oparciu co najmniej o protokoły:
Administracja	Konfiguracja urządzenia ma być	możliwa z wykorzystaniem polskiego interfejsu graficznego.
urządzeniem		dostępny poprzez przeglądarkę internetową, a komunikacja ma niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
	Administrator ma mieć możliwo	ość wskazania do komunikacji innego portu niż 443 TCP.
	Urządzenie ma umożliwiać zarz nakładającymi się) uprawnienia	ądzanie przez dowolną liczbę administratorów z różnymi (także mi.
	-	liwość wykorzystania wbudowanych profili administracyjnych ególnych modułów systemu na prawach: brak dostępu, dostęp yt i zapis.
	Urządzenie ma umożliwiać zarz	ądzenia z poziomu konsoli (SSH)
	Urządzenie ma umożliwiać zarz	ądzanie poprzez dedykowaną platformę centralnego zarządzania.
		my centralnego zarządzania ma być dostępny poprzez przeglądarkę
		być zabezpieczona za pomocą protokołu HTTPS.
	Wbudowany webowy, graficzny diagnostyczne, co najmniej ping	v interfejs administracyjny urządzenia musi oferować narzędzia g, traceroute, nslookup.
		v interfejs administracyjny musi oferować narzędzia do świetlania otwartych połączeń sieciowych.
		v interfejs administracyjny musi oferować możliwość zdefiniowania ałym systemie w zakresie minimalnej ilości znaków czy złożoności
		r interfejs administracyjny musi oferować możliwość generowania anych przez administratora (script recording).
	System musi oferować możliwo certyfikatów, usług internetowy	ść zdefiniowania własnych obiektów sieciowych, obiektów URL, ych (web services).
	Urządzenie musi oferować port	al uwierzytelniania (captive portal) dla użytkowników.
	Urządzenie ma umożliwiać eksp transmisji nieszyfrowanej jak i s	ortowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem zyfrowanej (TLS).
	Urządzenie ma umożliwiać eksp	ortowanie logów za pomocą protokołu IPFIX.
	Urządzenie ma umożliwiać eksp zakresie:	ortowanie backupu konfiguracji (kopia zapasowa) co najmniej w
		i do pliku w dowolnym momencie czasu,
		ortu do serwerów producenta lub na dedykowany serwer ninistratora, z możliwością wyboru częstotliwości co najmniej: raz niu, raz w miesiącu
	Urządzenie ma umożliwiać odty	vorzenie backupu konfiguracji pochodzących bezpośrednio z lykowanego serwera zarządzanego przez administratora.
	Urządzenie ma umożliwiać ano nazwy użytkownika.	nimizację logów co najmniej w zakresie adresu źródłowego oraz
	Rozwiązanie musi dawać możliwaktualizacji w trybie offline z po	vość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku ziomu interfejsu graficznego.





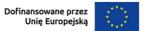




Raportowanie	1.	Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
	2.	System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
	3.	System raportowania ma posiadać 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	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	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

- 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.
- 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.

obsługi dostarczonego rozwiązania.

Prace wdrożeniowe

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.

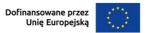
Optymalizacja konfiguracji na podstawie wyników testów, zapewniająca maksymalną wydajność i

bezpieczeństwo. Przeprowadzenie szkolenia administratorów, które zapewnią kompleksową możliwość konfiguracji i

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.







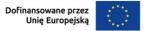


Dostawa 10 szt. zarządzalnych przełączników sieciowych (switch) spełniających wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Тур	Zarządzalny przełącznik sieciowy (switch).
Porty	• 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	20 Gb/s
przełącznika	
Szybkość przekierowań	14,89 Mp/s
pakietów	
Tablica adresów MAC	8K
Bufor pakietów	4,1 Mb
Ramki jumbo	9 KB
Funkcja Quality of	8 kolejek priorytetowania
Service	Obsługa priorytetowania 802.1p CoS/DSCP
	Tryb harmonogramu priorytetowania:
	- 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
	- Mirror (do obsługiwanego interfejsu)
	- Redirect (do obsługiwanego interfejsu)
	- Limit prędkości - QoS Remark
Cechy przełącznika L3	16 interfejsów IPv4/IPv6
Cecity przeiącznika LS	Routing statyczny
	- 48 tras statycznych
	Statyczne wpisy ARP
	• 316 wpisów ARP
	Proxy ARP
	Gratuitous ARP
	Serwer DHCP
	DHCP Relay
	DHCP L2 Relay
Funkcje L2 i L2+	Agregacja łączy
	- Statyczna agregacja łączy
	- LACP 802.3ad
	- Do 8 grup agregacji i do 8 portów na grupę
	Protokół drzewa rozpinającego (STP)
	- STP 802.1D
	- RSTP 802.1w
	- MSTP 802.1s
	- Zabezpieczenia STP: ochrona TC, filtrowanie poprzez pakiety BPDU, ochrona BPDU, ochrona Root
	Wykrywanie pętli zwrotnych Operto na postach
	- Oparte na VI AN
	Oparte na VLAN Kontrola przepływu
	- Kontrola przepływu 802.3x
	- Zapobieganie blokowaniu HOL
	Mirroring
	- Port Mirroring
	- Mirroring procesora
	- Przesył One-to-One
	- Przesył Many-to-One
	1 1 1





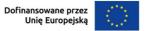




1.2 84	- Obshires E44 cross ICMD (ID-4 ID-C)
L2 Multicast	Obsługa 511 grup IGMP (IPv4, IPv6) ICOAD Granding
	• IGMP Snooping
	- IGMP v1/v2/v3 Snooping
	- Fast Leave
	- IGMP Snooping Querier
	- Uwierzytelnianie IGMP
	Uwierzytelnianie IGMP
	• MVR
	MLD Snooping
	- MLD v1/v2 Snooping
	- Fast Leave
	- MLD Snooping Querier
	- Konfiguracja grupy statycznej
	- Ograniczone przekazywanie IP Multicast
	Filtrowanie transmisji Multicast: 256 profili i 16 wpisów na profil
Funkcje zaawansowane	Automatyczne wykrywanie urządzeń
•	Konfiguracje grupowe
	Grupowe aktualizacje oprogramowania
	Inteligentne monitorowanie stanu sieci
	Ostrzeżenia o nietypowych zdarzeniach
	Ujednolicony proces konfiguracji
	Harmonogram restartu
Sieci VLAN	• Grupy VLAN
SIECI VLAIN	- Maks. 4K grup VLAN
	• Tagowanie 802.1Q VLAN
	Adres MAC VLAN: 12 wpisów
	Protokół VLAN COURD
	• GVRP
	• VLAN VPN (QinQ)
	- QinQ oparty na portach
	- Selective QinQ
	Głosowa sieć VLAN
Listy kontroli dostępu	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
	Add to the Add
	- Źródłowy adres IP
	- Źródłowy adres IP
	- Źródłowy adres IP - Docelowy adres IP
	- Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP
	- Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP
	- Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP
	- Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP - Port TCP/UDP
	- Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP - Port TCP/UDP - TOS DSCP/IP
	- Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6
	- Źródłowy adres IP - Docelowy adres IP - Fragment - Protokół IP - Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu
	- 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
	- 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
	- 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
	- 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
	- 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
	- 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
Rozniaczoństwo	- 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 transmisii	- 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 - Wiązanie adresów IP, MAC i portów
Bezpieczeństwo transmisji	- 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 • Wiązanie adresów IP, MAC i portów - DHCP Snooping
-	- 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 - Wiązanie adresów IP, MAC i portów - DHCP Snooping - Inspekcja ARP
-	- 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 • Wiązanie adresów IP, MAC i portów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4
-	- 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 - Wiązanie adresów IP, MAC i portów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4 - Wiązanie adresów IPv6, MAC i portów
-	- 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 • Wiązanie adresów IP, MAC i portów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4





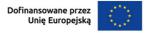




	- Ochrona źródłowego adresu IPv6
	Ochrona przed atakami DoS
	Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację
	- Do 64 adresów MAC na port
	Storm Control Broadcast/Multicast/Unicast
	- tryb kontroli (kb/s/wskaźnik)
	Kontrola dostępu w oparciu o IP/port/MAC
	Uwierzytelnianie 802.1X
	- 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 webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2
	Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2
IPv6	• 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	• 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	Interfejs graficzny GUI
zarządzania	Interfejs linii poleceń CLI
zarząuzama	• SNMP v1/v2c/v3
	- Trap/Inform
	- RMON (grupy 1, 2, 3, 9)
	• Szablon SDM
	Klient DHCP/BOOTP COS 4 L LUDD (LUDD ALED)
	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	Przełącznik
_arrai tose opanowania	Przewód zasilający
	r rection ensuringly





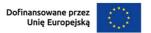




	Instrukcja instalacji
	Zestaw montażowy
	Gumowe nóżki
Warunki gwarancji	Gwarancja producenta - 2 lata.







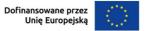


Dostawa 3 szt. zarządzalnych przełączników sieciowych (switch) spełniających wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Тур	Zarządzalny przełącznik sieciowy (switch).
Porty	• 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	128 Gb/s
przełącznika	
Szybkość przekierowań	95,23 Mp/s
pakietów	
Tablica adresów MAC	16K
Bufor pakietów	12 Mb
Ramki jumbo	9 KB
Funkcja Quality of	8 kolejek priorytetowania
Service	Obsługa priorytetowania 802.1p CoS/DSCP
	• Tryb harmonogramu priorytetowania:
	- SP (Strict Priority)
	- WRR (Weighted Round Robin)
	- SP+WRR
	Kontrola przepustowości Ograniczneje przekłości transforu w oparcju o port/przephru danych
	 Ograniczanie prędkości transferu w oparciu o port/przepływ danych Płynniejsze działanie
	Działania dla przepływów
	- Mirror (do obsługiwanego interfejsu)
	- Redirect (do obsługiwanego interrejsu)
	- Limit prędkości
	- QoS Remark
Cechy przełącznika L3	• 128 interfejsów IPv4/IPv6
Cony przerącznika 25	Routing statyczny
	- 48 tras statycznych
	Wpisy statyczne ARP
	- 128 wpisów statycznych
	• Proxy ARP
	Gratuitous ARP
	• Serwer DHCP
	DHCP Relay
	- DHCP Interface Relay
	- DHCP VLAN Relay
	DHCP L2 Relay
Funkcje L2 i L2+	Agregacja łączy
	- Statyczna agregacja łączy
	- LACP 802.3ad
	- Do 8 grup agregacji i do 8 portów na grupę
	Protokół drzewa rozpinającego (STP) CTD 003 4 D
	- STP 802.1D
	- RSTP 802.1w
	- MSTP 802.1s
	- Zabezpieczenia STP: ochrona TC, filtrowanie poprzez pakiety BPDU, ochrona Root
	Wykrywanie pętli zwrotnych Oparte na portach
	- Oparte na VLAN
	Kontrola przepływu
	- Kontrola przepływu - Kontrola przepływu 802.3x
	- Zapobieganie blokowaniu HOL
	Mirroring
	- Port Mirroring
	- Mirroring procesora
	- Przesył One-to-One
	- Przesył Many-to-One
	· · · · · · · · · · · · · · · · · · ·





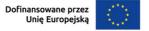




	- Port wejścia/wyjścia / obydwa porty
L2 Multicast	IGMP Snooping
	- IGMP v1/v2/v3 Snooping
	- Fast Leave
	- IGMP Snooping Querier
	- Uwierzytelnianie IGMP
	Uwierzytelnianie IGMP
	• MVR
	MLD Snooping
	- MLD v1/v2 Snooping
	- Fast Leave
	- MLD Snooping Querier
	- Konfiguracja grupy statycznej
	- Ograniczone przekazywanie IP Multicast
	Filtrowanie transmisji Multicast: 256 profili i 16 wpisów na profil
Funkcje zaawansowane	Automatyczne wykrywanie urządzeń
	Konfiguracje grupowe
	Grupowe aktualizacje oprogramowania
	Inteligentne monitorowanie stanu sieci
	Ostrzeżenia o nietypowych zdarzeniach
	Ujednolicony proces konfiguracji
	Harmonogram restartu
Sieci VLAN	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
Lietu kontuoli dostonu	Głosowa sieć VLAN Lista kontroli dostony (ACL) posta o gras
Listy kontroli dostępu	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
	- Flaga TCP - Port TCP/UDP
	- Flaga TCP
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu • Łączona ACL
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu • Łączona ACL • Polityka kontroli dostępu
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu • Łączona ACL • Polityka kontroli dostępu - Mirroring
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu • Łączona ACL • Polityka kontroli dostępu - Mirroring - Limit prędkości
	- Flaga TCP - Port TCP/UDP - TOS DSCP/IP - User Priority • ACL IPv6 • ACL zawartości pakietu • Łączona ACL • Polityka kontroli dostępu - Mirroring - Limit prędkości - Redirect
Bezpieczeństwo	- 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
Bezpieczeństwo transmisji	- 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
-	- 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
-	- 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 • Wiązanie adresów IP, MAC i portów - 512 wpisów - DHCP Snooping - Inspekcja ARP
-	- 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 • Wiązanie adresów IP, MAC i portów - 512 wpisów - DHCP Snooping





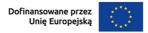




	- 512 wpisów
	- DHCPv6 Snooping
	- Wykrywanie ND
	- Ochrona źródłowego adresu IPv6: 100 wpisów
	Ochrona przed atakami DoS
	Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację
	- Do 64 adresów MAC na port
	Storm Control Broadcast/Multicast/Unicast
	- tryb kontroli (kb/s/wskaźnik)
	Uwierzytelnianie 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 CLLz szyfrowaniem SSLv4/SSLv4
	Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2 Kontrola dostopu w oparciu o IR/port/MAC
ID. C	Kontrola dostępu w oparciu o IP/port/MAC IDv6 Dva IDv6 /IDv6
IPv6	IPv6 Dual IPv4/IPv6 Naukingsk Listensky Discovery (NALD) Spagning
	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	Bazy danych MIB II (RFC1213)
IVIID	• Porty MIB (RFC2233)
	• Port Ethernet MIB (RFC1643)
	Bridge MIB (RFC1493)
	P/Q-Bridge MIB (RFC2674) PMON MIB (RFC2810)
	• RMON MIB (RFC2819)
	RMON2 MIB (RFC2021) Padius Associating Client MID (RFC2620)
	Radius Accounting Client MIB (RFC2620) Redus Accounting Client MIB (RFC26200) Redus Accounting Client MIB (RFC26000) Redus Accounting Client MIB (RFC260
	Radius Authentication Client MIB (RFC2618) Authority Common Co
	Pakiety Ping i Traceroute do interfejsu MIB (RFC2925)
	Obsługa prywatnych baz danych MIB TP-Link
Funkcje panelu	Interfejs graficzny GUI
zarządzania	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





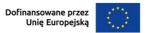




	Odzyskiwanie hasła
	• SNTP
	Logi systemowe
Certyfikaty	CE, FCC, RoHS
Zawartość opakowania	Przełącznik
	Przewód zasilający
	Instrukcja instalacji
	Zestaw montażowy
	Gumowe nóżki
Warunki gwarancji	Gwarancja producenta - 2 lata.







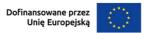


Dostawa 10 szt. zasilaczy awaryjnych UPS spełniającego wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Тур	Zasilacz awaryjny UPS.
Akumulator	1 x 12V/9Ah
Мос	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
opologia	Line-Interactive AVR
Zabezpieczenia	termiczne, przeciwprzepięciowe, przeciwzwarciowe
Zabezpieczenie przed przepięciami	RJ45
Warunki gwarancji	Gwarancja - 2 lata. Gwarancja na akumulator - 12 miesięcy.







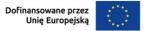


Dostawa i wdrożenie rozwiązania do tworzenia i odtwarzania kopii zapasowych spełniającego wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Тур	Dedykowany serwer i oprogramowanie do realizacji oraz odtwarzania kopii zapasowych.
Konstrukcja	Typu RACK, wysokość 2U;
	Szyny umożliwiające wysunięcie serwera z szafy stelażowej, umożliwiające instalację ramienia porządkującego kable;
	Możliwość zainstalowania 10 dysków twardych hot plug 3,5";
	Możliwość rozbudowy o fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
	Zainstalowane 2 szt. dysków SSD SATA 960GB Hot-Plug DWPD min 5 oraz 3 szt. 8TB SATA Hot Plug;
	Możliwość instalacji wewnętrznego napędu optyczny umożliwiający zapisanie 25GB danych na jednym nośniku.
Płyta główna	Dwuprocesorowa;
	Wyprodukowana i zaprojektowana przez producenta serwera;
	Możliwość instalacji procesorów 38-rdzeniowych;
	Zainstalowany moduł TPM 2.0;
	6 złącz PCI Express generacji 4 w tym:
	4 fizyczne złącza o prędkości x16;
	2 fizyczne złącza o prędkości x8;
	Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
	Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
	32 gniazda pamięci RAM;
	Obsługa minimum 6 TB pamięci RAM DDR4;
	Wsparcie dla technologii:
	Memory Scrubbing;
	SDDC;
	ECC;
	Memory Mirroring;
	ADDDC;
	Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.
Procesory	Procesor 8-rdzeniowy, taktowanie bazowe 2,8GHz, architektura x86_64.
	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.
Pamięć RAM	64 GB pamięci RAM.
	DDR4 Registered 3200MT/s.
Dyski twarde	Zainstalowane 2 szt. dysków SSD SATA 960GB Hot-Plug DWPD min 5 oraz 3 szt. 8TB SATA Hot Plug
Kontrolery LAN	4x 1Gbit Base-T
, –	2x 10Gbit SFP+
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	Zintegrowana karta graficzna ze złączem VGA z tyłu serwera,
	2 porty USB 3.0 dostępne z tyłu serwera,
	2 porty USB 3.0 na panelu przednim,
	2 porty USB 3.0 wewnątrz serwera,
	Możliwość rozbudowy o 1 port serial, możliwość wykorzystania portu serial do zarządzania serwerem,
	llość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych





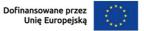




	przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
Zasilanie, chłodzenie	Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W,
	Redundantne wentylatory hotplug.
Zarządzanie	Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
	 informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
	 karty rozszerzeń zainstalowane w dowolnym slocie 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);
	Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
	 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;
	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,





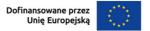




	zasilacze, płyta główna, procesory, pamięć operacyjna);
	Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
	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.
Wspierane OS	Microsoft Windows Server 2022, 2019;
	VMWare vSphere 8.0;
	Suse Linux Enterprise Server 15;
	Red Hat Enterprise Linux 9, 8;
	Microsoft Hyper-V Server 2019.
Gwarancja	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.
	Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w systemie helpdesk/servicedesk producenta sprzętu;
	Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
	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;
	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).
Certyfikaty	Zgodność z normami: CB, RoHS, WEEE oraz CE.
Dokumentacja, inne	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.
	Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta.
	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.
	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 twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji.
	Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.
Oprogramowanie	Wdrożenie rozwiązania zapewniającego odporność na ataki złośliwego oprogramowania ransomware. Rozwiązanie ze statutem zgodności z kluczowymi regulacjami dotyczącym niezmienności przechowywania danych, m.in.:
	• w Stanach Zjednoczonych:
	SEC 17a-4(f),
	FINRA 4511(c),
	CFTC 1.31(c)-(d),
	• w Niemczech:
	IDW PS 880.
Bezpieczeństwo kopii zapasowych	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).
	Proponowane rozwiązanie powinno być oparte na obiektowej pamięci masowej z niezmiennością (immutability). Repozytorium (nośnik kopii zapasowych) powinno stanowić fizyczny serwer.





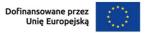




	Bezpieczeństwo składowania kopii zapasowych powinno być zapewnione poprzez odpowiednią instalację i konfigurację (hardening) systemu.
	Pliki kopii zapasowych muszą mieć ustawiany atrybut "immutability", który uniemożliwia usunięcie lub modyfikację kopii zapasowej przed wcześniej zdefiniowanym okresem czasu.
	Repozytorium musi być zainstalowane na serwerze sprzętowym, nie wirtualnym.
	Proponowane repozytorium może być podstawowym miejscem składowania kopii zapasowych, jak i dodatkowym.
Wdrożenie	Wdrożenie powinno obejmować następujące działania:
	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.
	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.
	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.
Rok produkcji	Serwer musi być fabrycznie nowy i nieużywany przed dniem dostarczenia do siedziby Zamawiającego, z wyłączeniem użycia niezbędnego dla przeprowadzenia testu poprawnej pracy. Dostarczone wraz z serwerem licencje oprogramowania mają upoważniać do użytkowania oprogramowania na czas nieokreślony.







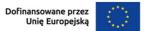


Dostawa 2 kompletów licencji systemu serwerowego spełniającego wymagania, jak niżej:

Nazwa	WYMAGANE MINIMALNE PARAMETRY
Licencja	Każdy komplet licencji serwerowych systemu operacyjnego musi uprawniać do uruchamiania co
	najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym.
	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.
	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.
	Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz
	pozwalała na legalne używanie na serwerze Zamawiającego.
	Serwerowy system operacyjny, który jest w pełni kompatybilny z licencjami dostępowymi (CAL) dla
	Windows Server 2019.
Cash., sam., sam.	Licencja nie może być ograniczona czasowo.
Cechy serwerowego	1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w
systemu operacyjnego	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 uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
	13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
	14. Wbudowana zapora internetowa (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 dotykiem 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),
- I. 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 interfeis 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.