Załącznik nr 6 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**1. Serwer – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera.

**Wymagania:**

1. Obudowa Tower z możliwością instalacji min. 4 dysków 3.5".
2. Płyta główna z możliwością zainstalowania jednego procesora.
3. Chipset dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
4. Zainstalowany jeden procesor min. 4-rdzeniowy o taktowaniu min. 2.8GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 8 000 pkt. Wynik należy dołączyć do oferty.
5. Pamięć RAM min. 16GB pamięci RAM DDR4 ECC o częstotliwości pracy 3200MT/s. Możliwość rozbudowy do 128GB.
6. Wbudowane porty:
	1. min. 4 porty USB w tym min. 2 porty USB 3.2
	2. min. 1 port VGA
	3. min. 1 port RS232
	4. min. 1 port RJ-45 do zarządzania
7. Min. 3 aktywne sloty PCI-E 4.0 z czego min. 2 sloty x8
8. Zintegrowana karta sieciowa z min. 2 portami Ethernet 10/100/1000 Mb/s BaseT
9. Zintegrowana karta graficzna.
10. Zintegrowany kontroler RAID 0, 1, 5, 10
11. Pamięć masowa:
	1. Zainstalowane min. 2 dyski SSD o pojemności min. 480GB.
	2. Zainstalowane min. 2 dyski twarde o pojemności min. 2TB każdy.
12. Wbudowany wentylator zapewniający efektywne chłodzenia
13. Min. 1 zasilacz 80PLUS Gold o mocy min. 400W. W komplecie należy dostarczyć kabel zasilający o długości min. 1,8m.
14. Zainstalowany moduł TPM 2.0.
15. Zarządzanie IPMI 2.0.
16. Serwer musi posiadać deklarację CE.
17. Zgodność z normą ISO 9001, ISO 14001 oraz ISO 27001 lub równoważnymi.
18. Obsługiwane systemy:
	1. Red Hat Enterprise Linux Server 7.x/8x
	2. SUSE Linux Enterprise Server 15 (64-bit)
	3. Microsoft Windows Server 2019
	4. Microsoft Windows Server 2022
	5. Vmware ESXi 7.x/8.x
19. Razem z serwerem należy dostarczyć Windows Server 2022 Standard. Opis równoważności licencji oprogramowania:
	1. Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie w urzędzie oraz pełną współpracę z ActiveDirectory, które jest aktualnie wykorzystywane. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerze zakupionym w ramach niniejszego postępowania.
	2. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.
	3. Licencja bez ograniczeń czasowych.
	4. Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
	5. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
	6. Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;
	7. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;
	8. Praca w roli klienta domeny Microsoft Active Directory;
	9. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022;
	10. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);
	11. Zawarta możliwość uruchomienia roli serwera DNS;
	12. Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
	13. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
	14. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
	15. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
	16. Zawarta możliwość uruchomienia roli serwera stron WWW;
	17. Zawarta funkcjonalność szyfrowania dysków;
	18. Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
	19. W ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;
	20. W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
	21. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
	22. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
	23. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
	24. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
	25. Obsługa zdalnego pulpitu;
	26. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
	27. Obsługa PowerShell 4.0;
20. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
21. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta lub autoryzowanego dystrybutora oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
22. Gwarancja:
	1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
	2. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.
	3. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
	4. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.
	5. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
		* możliwość pobierania najnowszego firmware,
		* dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
		* dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
		* otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
23. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja serwera wraz z oprogramowaniem.
		* Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania serwera oraz oprogramowania.

**2. Przełącznik dostępowy zarządzalny (PoE 48-portowy) – dostawa i konfiguracja – 2 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 4 szt. przełączników dostępowych PoE 48-portowych klasy Enterprise.

**Wymagania:**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
	1. możliwość montażu w stelażu/szafie 19”
	2. wysokość maksymalna 1U
	3. głębokość bez zainstalowanego zasilacza nie większa niż 35 cm
	4. minimum jeden zasilacz 230V AC
	5. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C
	6. zakres wilgotności pracy co najmniej 5% - 90%
	7. waga bez zainstalowanego zasilacza nie większa niż 6 kg
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
	1. 48 portów 100/1000BASE-T zgodne ze standardem 802.3at (minimalny budżet mocy PoE: 370W)
	2. 6 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Przełącznik musi posiadać następujące porty służące do zarządzania:
	1. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
	1. Zarządzanie stosem poprzez jeden adres IP
	2. Do min. 9 jednostek w stosie
	3. Porty do stackowania mogą być współdzielone z portami typu uplink.
	4. Magistrala stackująca o wydajności minimum 80Gb/s
	5. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
	6. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
	7. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
	8. W stosie musi być możliwość budowania stosu pomiędzy wszystkimi przełącznikami w ramach tego postępowania
7. Układ przełączający o wydajności min. 216 Gbps, wydajność przełączania przynajmniej 160 Mpps
8. Obsługa min. 32 500 adresów MAC
9. Wbudowana pamięć RAM min. 1GB.
10. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz
11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB
12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
13. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie
14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
15. Obsługa minimum 120 grup LAG
16. Obsługa ramek jumbo o wielkości min. 9216 bajtów
17. Obsługa sFlow
18. Wsparcie dla G.8032 ERPS
19. Obsługa protokołu VRRP
20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
21. Wsparcie dla mechanizmu PVST+.
22. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
23. Obsługa min. 6 100 tras dla routingu IPv4
24. Obsługa min. 2 000 tras dla routingu IPv6
25. Obsługa min. 2 000 IPv6 neighbor discovery (ND)
26. Obsługa protokołów związanych z obsługą ruchu typu multicast:
	1. IGMP v1, v2 i v3
	2. IGMP Snooping v2 i v3
	3. PIM-SM, PIM-SSM i PIM-DM
	4. MSDP i MLD Snooping
	5. minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6
27. Minimalny rozmiar tablicy ARP 4000 wpisów
28. Obsługa protokołów LLDP i LLDP-MED.
29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
30. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
	1. min. 3 poziomy dostępu administracyjnego poprzez konsolę
	2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
	3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
	4. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL
	5. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
	6. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
	7. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard
	8. możliwość synchronizacji czasu zgodnie z NTP lub SNTP
31. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
	1. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
	2. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
32. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
33. Wymagane opcje zarządzania:
	1. możliwość lokalnej obserwacji ruchu na określonym porcie
	2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
	3. wsparcie dla skyptów python uruchamianych na urządzeniu
	4. wsparcie dla RMON
34. Wraz z urządzeniami muszą zostać dostarczone:
	1. pełna dokumentacja w języku polskim lub angielskim
	2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
35. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
36. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
37. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
38. Usługa serwisu musi być świadczona w języku polskim.
39. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
40. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
41. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
42. System centralnego zarządzania może być dostarczony w formie:
	1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
	2. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
43. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
44. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
45. System centralnego zarządzania musi umożliwiać:
	1. tworzenie VLANów
	2. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
	3. tworzenie połączeń zagregowanych
	4. monitorowanie statusu pracy przełącznika i portów
	5. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
	6. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
	7. interfejs do zarządzania w języku polskim lub angielskim
46. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja przełączników oraz podłączenie do sieci.
		* Konfiguracja przełączników zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania przełączników.

**3. Przełącznik dostępowy zarządzalny (PoE 24-portowy) – dostawa i konfiguracja – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. przełącznika dostępowego PoE 24-portowego klasy Enterprise.

**Wymagania:**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
	1. możliwość montażu w stelażu/szafie 19”
	2. wysokość maksymalna 1U
	3. głębokość bez zainstalowanego zasilacza nie większa niż 35 cm
	4. minimum jeden zasilacz 230V AC
	5. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C
	6. zakres wilgotności pracy co najmniej 5% - 90%
	7. waga bez zainstalowanego zasilacza nie większa niż 5,5 kg
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
	1. 24 porty 100/1000BASE-T zgodne ze standardem 802.3at (minimalny budżet mocy PoE: 370W)
	2. 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Przełącznik musi posiadać następujące porty służące do zarządzania:
	1. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
	1. Zarządzanie stosem poprzez jeden adres IP
	2. Do min. 9 jednostek w stosie
	3. Porty do stackowania mogą być współdzielone z portami typu uplink.
	4. Magistrala stackująca o wydajności minimum 80Gb/s
	5. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
	6. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
	7. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
	8. W stosie musi być możliwość budowania stosu pomiędzy wszystkimi przełącznikami w ramach tego postępowania
7. Układ przełączający o wydajności min. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps
8. Obsługa min. 32 500 adresów MAC
9. Wbudowana pamięć RAM min. 1GB.
10. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz
11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB
12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
13. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie
14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
15. Obsługa minimum 120 grup LAG
16. Obsługa ramek jumbo o wielkości min. 9216 bajtów
17. Obsługa sFlow
18. Wsparcie dla G.8032 ERPS
19. Obsługa protokołu VRRP
20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
21. Wsparcie dla mechanizmu PVST+.
22. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
23. Obsługa min. 6 100 tras dla routingu IPv4
24. Obsługa min. 2 000 tras dla routingu IPv6
25. Obsługa min. 2 020 IPv6 neighbor discovery (ND)
26. Obsługa protokołów związanych z obsługą ruchu typu multicast:
	1. IGMP v1, v2 i v3
	2. IGMP Snooping v2 i v3
	3. PIM-SM, PIM-SSM i PIM-DM
	4. MSDP i MLD Snooping
	5. minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6
27. Minimalny rozmiar tablicy ARP 4000 wpisów
28. Obsługa protokołów LLDP i LLDP-MED.
29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
30. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
	1. min. 3 poziomy dostępu administracyjnego poprzez konsolę
	2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
	3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
	4. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL
	5. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
	6. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
	7. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard
	8. możliwość synchronizacji czasu zgodnie z NTP lub SNTP
31. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
	1. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
	2. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
32. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
33. Wymagane opcje zarządzania:
	1. możliwość lokalnej obserwacji ruchu na określonym porcie
	2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
	3. wsparcie dla skyptów python uruchamianych na urządzeniu
	4. wsparcie dla RMON
34. Wraz z urządzeniami muszą zostać dostarczone:
	1. pełna dokumentacja w języku polskim lub angielskim
	2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
35. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
36. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
37. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
38. Usługa serwisu musi być świadczona w języku polskim.
39. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
40. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
41. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
42. System centralnego zarządzania może być dostarczony w formie:
	1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
	2. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
43. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
44. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
45. System centralnego zarządzania musi umożliwiać:
	1. tworzenie VLANów
	2. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
	3. tworzenie połączeń zagregowanych
	4. monitorowanie statusu pracy przełącznika i portów
	5. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
	6. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
46. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja przełączników oraz podłączenie do sieci.
		* Konfiguracja przełączników zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania przełączników.

**4. Przełącznik dostępowy zarządzalny (48-portowy) – dostawa i konfiguracja – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. przełącznika dostępowego 48-portowego klasy Enterprise.

**Wymagania:**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
	1. możliwość montażu w stelażu/szafie 19”
	2. wysokość maksymalna 1U
	3. głębokość bez zainstalowanego zasilacza nie większa niż 35 cm
	4. minimum jeden zasilacz 230V AC
	5. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C
	6. zakres wilgotności pracy co najmniej 5% - 90%
	7. waga bez zainstalowanego zasilacza nie większa niż 5 kg
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
	1. 48 portów 100/1000BASE-T
	2. 6 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Przełącznik musi posiadać następujące porty służące do zarządzania:
	1. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
	1. Zarządzanie stosem poprzez jeden adres IP
	2. Do min. 9 jednostek w stosie
	3. Porty do stackowania mogą być współdzielone z portami typu uplink.
	4. Magistrala stackująca o wydajności minimum 80Gb/s
	5. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
	6. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
	7. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
	8. W stosie musi być możliwość budowania stosu pomiędzy wszystkimi przełącznikami w ramach tego postępowania
7. Układ przełączający o wydajności min. 216 Gbps, wydajność przełączania przynajmniej 160 Mpps
8. Obsługa min. 32 500 adresów MAC
9. Wbudowana pamięć RAM min. 1GB.
10. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz
11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB
12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
13. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie
14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
15. Obsługa minimum 120 grup LAG
16. Obsługa ramek jumbo o wielkości min. 9216 bajtów
17. Obsługa sFlow
18. Wsparcie dla G.8032 ERPS
19. Obsługa protokołu VRRP
20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
21. Wsparcie dla mechanizmu PVST+.
22. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
23. Obsługa min. 6 100 tras dla routingu IPv4
24. Obsługa min. 2 000 tras dla routingu IPv6
25. Obsługa min. 2 000 IPv6 neighbor discovery (ND)
26. Obsługa protokołów związanych z obsługą ruchu typu multicast:
	1. IGMP v1, v2 i v3
	2. IGMP Snooping v2 i v3
	3. PIM-SM, PIM-SSM i PIM-DM
	4. MSDP i MLD Snooping
	5. minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6
27. Minimalny rozmiar tablicy ARP 4000 wpisów
28. Obsługa protokołów LLDP i LLDP-MED.
29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
30. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
	1. min. 3 poziomy dostępu administracyjnego poprzez konsolę
	2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
	3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
	4. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL
	5. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
	6. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
	7. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard
	8. możliwość synchronizacji czasu zgodnie z NTP lub SNTP
31. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
	1. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
	2. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
32. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
33. Wymagane opcje zarządzania:
	1. możliwość lokalnej obserwacji ruchu na określonym porcie
	2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
	3. wsparcie dla skyptów python uruchamianych na urządzeniu
	4. wsparcie dla RMON
34. Wraz z urządzeniami muszą zostać dostarczone:
	1. pełna dokumentacja w języku polskim lub angielskim
	2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
35. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
36. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
37. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
38. Usługa serwisu musi być świadczona w języku polskim.
39. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
40. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
41. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
42. System centralnego zarządzania może być dostarczony w formie:
	1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
	2. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
43. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
44. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
45. System centralnego zarządzania musi umożliwiać:
	1. tworzenie VLANów
	2. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
	3. tworzenie połączeń zagregowanych
	4. monitorowanie statusu pracy przełącznika i portów
	5. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
	6. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
	7. interfejs do zarządzania w języku polskim lub angielskim
46. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja przełączników oraz podłączenie do sieci.
		* Konfiguracja przełączników zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania przełączników.

**5. Przełącznik dostępowy zarządzalny (24-portowy) – dostawa i konfiguracja – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. przełącznika dostępowego 24-portowego klasy Enterprise.

**Wymagania:**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
	1. możliwość montażu w stelażu/szafie 19”
	2. wysokość maksymalna 1U
	3. głębokość bez zainstalowanego zasilacza nie większa niż 35 cm
	4. minimum jeden zasilacz 230V AC
	5. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C
	6. zakres wilgotności pracy co najmniej 5% - 90%
	7. waga bez zainstalowanego zasilacza nie większa niż 4,5 kg
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
	1. 24 porty 100/1000BASE-T
	2. 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Przełącznik musi posiadać następujące porty służące do zarządzania:
	1. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
	1. Zarządzanie stosem poprzez jeden adres IP
	2. Do min. 9 jednostek w stosie
	3. Porty do stackowania mogą być współdzielone z portami typu uplink.
	4. Magistrala stackująca o wydajności minimum 80Gb/s
	5. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
	6. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
	7. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
	8. W stosie musi być możliwość budowania stosu pomiędzy wszystkimi przełącznikami w ramach tego postępowania
7. Układ przełączający o wydajności min. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps
8. Obsługa min. 32 500 adresów MAC
9. Wbudowana pamięć RAM min. 1GB.
10. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz
11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB
12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
13. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie
14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
15. Obsługa minimum 120 grup LAG
16. Obsługa ramek jumbo o wielkości min. 9216 bajtów
17. Obsługa sFlow
18. Wsparcie dla G.8032 ERPS
19. Obsługa protokołu VRRP
20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
21. Wsparcie dla mechanizmu PVST+.
22. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
23. Obsługa min. 6 100 tras dla routingu IPv4
24. Obsługa min. 2 000 tras dla routingu IPv6
25. Obsługa min. 2 020 IPv6 neighbor discovery (ND)
26. Obsługa protokołów związanych z obsługą ruchu typu multicast:
	1. IGMP v1, v2 i v3
	2. IGMP Snooping v2 i v3
	3. PIM-SM, PIM-SSM i PIM-DM
	4. MSDP i MLD Snooping
	5. minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6
27. Minimalny rozmiar tablicy ARP 4000 wpisów
28. Obsługa protokołów LLDP i LLDP-MED.
29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
30. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
	1. min. 3 poziomy dostępu administracyjnego poprzez konsolę
	2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
	3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
	4. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL
	5. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
	6. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
	7. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard
	8. możliwość synchronizacji czasu zgodnie z NTP lub SNTP
31. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
	1. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
	2. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
32. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
33. Wymagane opcje zarządzania:
	1. możliwość lokalnej obserwacji ruchu na określonym porcie
	2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
	3. wsparcie dla skyptów python uruchamianych na urządzeniu
	4. wsparcie dla RMON
34. Wraz z urządzeniami muszą zostać dostarczone:
	1. pełna dokumentacja w języku polskim lub angielskim
	2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
35. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
36. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
37. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
38. Usługa serwisu musi być świadczona w języku polskim.
39. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
40. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
41. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
42. System centralnego zarządzania może być dostarczony w formie:
	1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
	2. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
43. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
44. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
45. System centralnego zarządzania musi umożliwiać:
	1. tworzenie VLANów
	2. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
	3. tworzenie połączeń zagregowanych
	4. monitorowanie statusu pracy przełącznika i portów
	5. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
	6. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
46. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja przełączników oraz podłączenie do sieci.
		* Konfiguracja przełączników zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania przełączników.

**6. Przełącznik dostępowy zarządzalny (48-portowy z routerem PPPoE) – dostawa i konfiguracja – 1 kpl.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja kompletu składającego się z przełącznika dostępowego 48-portowego klasy Enterprise oraz routera PPPoE.

**Wymagania dotyczące przełącznika:**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
	1. możliwość montażu w stelażu/szafie 19”
	2. wysokość maksymalna 1U
	3. głębokość bez zainstalowanego zasilacza nie większa niż 35 cm
	4. minimum jeden zasilacz 230V AC
	5. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C
	6. zakres wilgotności pracy co najmniej 5% - 90%
	7. waga bez zainstalowanego zasilacza nie większa niż 5 kg
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
	1. 48 portów 100/1000BASE-T
	2. 6 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Przełącznik musi posiadać następujące porty służące do zarządzania:
	1. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
	1. Zarządzanie stosem poprzez jeden adres IP
	2. Do min. 9 jednostek w stosie
	3. Porty do stackowania mogą być współdzielone z portami typu uplink.
	4. Magistrala stackująca o wydajności minimum 80Gb/s
	5. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
	6. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
	7. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
	8. W stosie musi być możliwość budowania stosu pomiędzy wszystkimi przełącznikami w ramach tego postępowania
7. Układ przełączający o wydajności min. 216 Gbps, wydajność przełączania przynajmniej 160 Mpps
8. Obsługa min. 32 500 adresów MAC
9. Wbudowana pamięć RAM min. 1GB.
10. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz
11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB
12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
13. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie
14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
15. Obsługa minimum 120 grup LAG
16. Obsługa ramek jumbo o wielkości min. 9216 bajtów
17. Obsługa sFlow
18. Wsparcie dla G.8032 ERPS
19. Obsługa protokołu VRRP
20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
21. Wsparcie dla mechanizmu PVST+.
22. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
23. Obsługa min. 6 100 tras dla routingu IPv4
24. Obsługa min. 2 000 tras dla routingu IPv6
25. Obsługa min. 2 000 IPv6 neighbor discovery (ND)
26. Obsługa protokołów związanych z obsługą ruchu typu multicast:
	1. IGMP v1, v2 i v3
	2. IGMP Snooping v2 i v3
	3. PIM-SM, PIM-SSM i PIM-DM
	4. MSDP i MLD Snooping
	5. minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6
27. Minimalny rozmiar tablicy ARP 4000 wpisów
28. Obsługa protokołów LLDP i LLDP-MED.
29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
30. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
	1. min. 3 poziomy dostępu administracyjnego poprzez konsolę
	2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
	3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
	4. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL
	5. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
	6. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
	7. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard
	8. możliwość synchronizacji czasu zgodnie z NTP lub SNTP
31. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
	1. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
	2. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
32. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
33. Wymagane opcje zarządzania:
	1. możliwość lokalnej obserwacji ruchu na określonym porcie
	2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
	3. wsparcie dla skyptów python uruchamianych na urządzeniu
	4. wsparcie dla RMON

**Wymagania dotyczące routera:**

1. Router musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
	1. możliwość montażu w stelażu/szafie 19”
	2. wysokość maksymalna 1U
	3. głębokość bez zainstalowanego zasilacza nie większa niż 25 cm
	4. minimum jeden zasilacz 230V AC
	5. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C
	6. zakres wilgotności pracy co najmniej 5% - 90%
	7. waga nie większa niż 2,5 kg
3. Router musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
	1. 2 porty WAN o prędkości 1000BASE-T
	2. 4 porty LAN o prędkości 1000BASE-T
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Router musi posiadać następujące porty służące do zarządzania:
	1. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
6. Wbudowana pamięć RAM min. 1GB.
7. Procesor wielordzeniowy. Minimalne taktowanie procesora 800MHz
8. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 256MB
9. Obsługa VLAN (port-based VLAN, guest VLAN) oraz obsługa 802.1Q tunneling (QinQ)
10. Obsługa sFlow oraz NetStream
11. Obsługa PPP, PPPoE client oraz PPPoE server
12. Obsługa protokołów VRRP oraz VRRPv3
13. Load balancing i backup łącza WAN na podstawie pasma
14. Load balancing i backup łącza WAN na podstawie adresu IP
15. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
16. Obsługa protokołów routingu dynamicznego OSPFv2, OSPFv3, RIPv1/v2, RIPng, IS-IS, IS-ISv6, BGP, BGP4+. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
17. Obsługa protokołów związanych z obsługą ruchu typu multicast:
	1. IGMP v1, v2 i v3
	2. PIM-SM i PIM-DM
	3. MSDP i MGBP
	4. MLD v1 i v2
18. Router musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client

**Pozostałe wymagania dotyczące przełącznika i routera:**

1. Wraz z urządzeniami muszą zostać dostarczone:
	1. pełna dokumentacja w języku polskim lub angielskim
	2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
2. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
3. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
4. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
5. Usługa serwisu musi być świadczona w języku polskim.
6. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
7. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
8. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
9. System centralnego zarządzania może być dostarczony w formie:
	1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
	2. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
10. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
11. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
12. System centralnego zarządzania musi umożliwiać:
	1. tworzenie VLANów
	2. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
	3. tworzenie połączeń zagregowanych
	4. monitorowanie statusu pracy przełącznika i portów
	5. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
	6. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
	7. interfejs do zarządzania w języku polskim lub angielskim
13. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja przełącznika i routera oraz podłączenie do sieci.
		* Konfiguracja przełącznika i routera zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania przełącznika i routera.

**7. AP WIFI zarządzalny – dostawa i konfiguracja (bezprzewodowe punkty dostępowe) – 4 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 4 szt. bezprzewodowych punktów dostępowych klasy Enterprise.

**Wymagania:**

1. Punkt dostępowy musi być dedykowanym urządzeniem sieciowym przystosowanym do zamontowania na suficie i na ścianie. Wymagane dostarczenie z zestawu montażowego. System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. Oprogramowanie do pracy w trybie tzw „lekkiego AP”, możliwość pracy jako tzw “grubego AP (FAT AP)”oraz możliwość pracy jako tzw. Leader AP, czyli jeden z punktów dostępowych musi mieć możliwość pracy jako kontroler WLAN.
2. Urządzenie w trybie FAT musi umożliwiać zarządzać pracą dodatkowych access-pointów tego samego producenta. Funkcjonalność zarządzania pracą pozostałymi access-pointami musi umożliwiać transfer ruchu w trybie „local forwarding” (ruch z każdego access-pointa przesyłany jest w bezpośrednio w sieci lokalnej) oraz „Gateway” (access-point w trybie FAT działa jako brama sieci dla pozostałych access-pointów, realizując m.in. funkcjonalność NAT). Funkcjonalność zarządzania pracą pozostałymi urządzeniami musi być realizowana z poziomu przeglądarki urządzenia FAT, jak również z poziomu CLI (z wykorzystaniem m.in. protokołu SSH) urządzenia FAT
3. Wymagane parametry fizyczne:
	1. możliwość montażu na suficie oraz ścianie (wraz z urządzeniem należy dostarczyć elementy to montowania)
	2. wysokość maksymalna 5 cm
	3. możliwość zasilania przez zasilacz DC
	4. zakres temperatur pracy ciągłej co najmniej 0°C – +45°C
	5. zakres wilgotności pracy co najmniej 5% - 95%
	6. waga nie większa niż 0,8kg
4. Punkt dostępowy musi posiadać:
	1. dedykowany port konsolowy
	2. minimum 1 port 100/1000Mbit Base-T PoE
5. Obsługiwane standardy radiowe: 802.11a/b/g/n/ac/ac Wave 2/11ax, jednoczesna obsługa minimum 16 SSID dla każdego radia.
6. Wbudowane anteny minimum 4dBi dla 2,4GHz oraz 6dBi dla 5GHz z pracą w standardzie minimum MIMO: 2.4G: 2x2, 5G: 2x2
7. Wsparcie dla standardów/funkcjonalności bezpieczeństwa: WPA, WPA2, WPA3, 802.1x, IP Source Guard (IPSG) oraz tworzenie ACL
8. Wsparcie dla roamingu zgodnego z 802.11k, 802.11v, 802.11r
9. Obsługa minimum 1000 równocześnie podłączonych użytkowników do punktu dostępowego
10. Wydajność minimum 1,7Gbps w tym minimum 500Mbps dla 2.4GHz oraz 1,2Gbps dla 5GHz
11. Obsługa BLE w wersji 5.0
12. Zużycie mocy nie większe niż 15W
13. Możliwość zarządzania poprzez:
	1. WWW over HTTPS
	2. kontroler tego samego producenta
	3. SNMP v1, v2c, v3
	4. Dedykowany port konsoli
	5. SSHv2
14. Kompatybilność dla protokołów oraz standardów sieciowych takich jak: IPv6, LLDP, mDNS, NAT, IPsec
15. Urządzenie musi posiadać standard bezpieczeństwa EN62368-1
16. Tunel CAPWAP dla komunikacji z kontrolerem muszą być zaszyfrowane celem ochrony przed możliwością podsłuchania transmisji w sieci kablowej
17. Wsparcie dla protokołów i standardów:
	1. 802.11e
	2. 802.11i
	3. 802.11d
	4. 802.11h
	5. 802.11u
	6. 802.11w
	7. 802.15.1
	8. LLPD
	9. MLD Snooping i IGMP Snooping
	10. DTLS encryption
18. Obsługa NTP lub SNTP
19. Wraz z urządzeniami muszą zostać dostarczone:
	1. pełna dokumentacja w języku polskim lub angielskim
	2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
20. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
21. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
22. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
23. Usługa serwisu musi być świadczona w języku polskim.
24. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
25. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
26. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
27. System centralnego zarządzania może być dostarczony w formie:
	1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej

Lub

* 1. Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
1. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
2. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
3. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja punktów dostępowych oraz podłączenie do sieci.
		* Konfiguracja punktów dostępowych zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania punktów dostępowych.

**8. Firewall z UTM – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. zapory sieciowej z pakietem bezpieczeństwa UTM które zapewnia zaawansowaną ochronę w infrastrukturze informatycznej zamawiającego. Zamówienie obejmuje zarówno dostawę urządzeń fizycznych firewall jak i licencje na oprogramowanie UTM na minimum 24 miesiące oraz usługi wdrożeniowe, dlatego wymagane jest uwzględnienie wszystkich elementów w ofercie.

**UWAGA: Zamawiający wymaga zadeklarowania gwarancji licencji ważnej do 30.06.2026 r.**

**Wymagania:**

1. 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.
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. 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.
6. 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.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
13. 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.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. 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.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. 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.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. 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).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
30. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
31. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
32. Ochrona antyspam ma działać w oparciu o:
	1. białe/czarne listy,
	2. DNS RBL,
	3. Skaner heurystyczny.
33. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
35. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
36. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
	1. PPTP VPN,
	2. IPSec VPN,
	3. SSL VPN.
37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
38. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
39. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
43. Urządzenie ma posiadać wbudowany filtr URL.
44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
45. Administrator ma mieć możliwość dodawania własnych kategorii URL.
46. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
47. blokowanie dostępu do adresu URL,
48. zezwolenie na dostęp do adresu URL,
49. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
50. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
51. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
52. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
53. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
54. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
55. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
56. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
	1. lokalną bazę użytkowników (wewnętrzny LDAP),
	2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
	3. usługę katalogową Microsoft Active Directory.
57. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
58. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
	1. SSL,
	2. Radius,
	3. Kerberos.
59. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
60. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
61. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
62. 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).
63. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
64. 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.
65. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
66. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
	1. równoważenie względem adresu źródłowego,
	2. równoważenie względem połączenia.
67. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
68. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
69. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
70. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
71. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
72. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
73. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
74. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
75. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
76. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
77. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
78. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
79. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
80. 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.
81. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
82. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
83. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
84. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
85. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
86. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
88. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
89. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
90. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
91. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
92. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
	1. manualnego eksportu do pliku w dowolnym momencie czasu,
	2. 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
93. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
94. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
95. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
96. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
97. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
98. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
99. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
100. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
101. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
102. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
103. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
104. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
105. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
106. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
107. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
108. 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).
109. Urządzenie ma posiadać usługę DNS Proxy.
110. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
111. Urządzenie musi mieć zaimplementowane Open API
112. 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.
113. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
114. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
115. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
116. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
117. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
118. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
119. Liczba portów Ethernet 2,5Gbps – min. 8.
120. Liczba portów światłowodowych 1Gbps – min. 1.
121. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
122. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
123. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
124. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
125. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
126. Maksymalna liczba tuneli VPN IPSec – minimum 100.
127. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
128. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
129. Obsługa interfejsów 802.11q (VLAN) – minimum 128
130. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
131. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
132. Urządzenie nie ma limitu na liczbę użytkowników.
133. Liczba reguł filtrowania – minimum 8 192.
134. Liczba tras statycznego routingu – minimum 512.
135. Liczba tras dynamicznego routingu – minimum 10 000.
136. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
137. Urządzenie musi być wyposażone w moduł TPM.
138. Gwarancja
	1. Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także muszą być objęte serwisem producenta na terenie RP.
	2. Urządzenia objęte minimum 24 miesięcznym okresem gwarancji.
	3. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
	4. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego rozwiązania, potwierdzające pochodzenie urządzeń z licencjami z oficjalnego kanału dystrybucyjnego producenta.
	5. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
	6. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
		* możliwość pobierania najnowszego firmware,
		* dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
		* dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
		* otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
139. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja urządzeń firewall wraz z oprogramowaniem UTM.
		* Konfiguracja urządzeń i oprogramowania UTM zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego wraz z przeniesieniem konfiguracji z obecnie używanych urządzeń.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania urządzeń firewall oraz oprogramowania UTM.

**9. Serwer NAS – dostawa, instalacja i konfiguracja (do backupu) – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera do przechowywania danych.

**Wymagania:**

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 zatokami na dyski SATA HDD i SSD o wielkości 3,5 cala oraz 2,5 cala.
2. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack. Maksymalna głębokość urządzenia nie powinna przekraczać 300 mm z uwagi na możliwość instalacji w kompaktowych szafach serwerowych z ograniczoną przestrzenią.
3. Zainstalowany 1 procesor klasy x86 min. 8-rdzeniowy o taktowaniu min. 2.7GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 8 600 pkt. Wynik należy dołączyć do oferty.
4. Pamięć RAM min. 8 GB DDR4 z możliwością rozbudowy do co najmniej 64 GB.
5. Wbudowane min. 4 porty USB 3.2
6. Powyższe porty USB nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
7. Możliwość instalacji portu HDMI przez PCI-E
8. Min. 2 aktywne sloty PCI-E 3.0 umożliwiające instalację dodatkowych kart rozszerzeń, takich jak karty sieciowe, karty SSD NVMe lub inne, które mogą zwiększyć funkcjonalność i wydajność systemu.
9. Zainstalowane i w pełni funkcjonalne minimum 2 porty sieciowe Ethernet 2.5GbE RJ45 z obsługą Link Aggregation w celu zwiększenia wydajności transferu i odporności na awarie. Porty nie mogą zajmować slotów PCI-E
10. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 5, 6, 10, 50, 60.
11. Pamięć masowa:
	1. Zainstalowane 2 dyski SSD M2 PCIe NVMe o pojemności min. 1 TB każdy, które umożliwiają korzystanie z technologii buforowania SSD w celu zapewnienia optymalnej wydajności serwera.
	2. Zainstalowane min. 6 dysków HDD SATA o pojemności min. 4 TB każdy.
12. Minimum 3 wentylatory.
13. Min. 2 identyczne zasilacze o mocy min. 300W zainstalowane wewnątrz serwera, pracujące redundantni w celu zapewnienia ciągłości pracy w przypadku awarii jednego z nich.
14. Urządzenie powinno oferować zaawansowane funkcje zabezpieczeń, takie jak szyfrowanie danych AES-256, dwustopniowe uwierzytelnianie, zapora sieciowa, oraz ochrona przed atakami typu brute-force.
15. Diody LED umieszczone z przodu obudowy serwera informujące o statusie: dysków, portów LAN, portów USB i zasilaniu.
16. Wraz ze serwerem dostarczone powinno być oprogramowanie do tworzenia i zarządzania kopiami zapasowymi komputerów, serwerów i maszyn wirtualnych w środowiskach wirtualizacyjnych. Oprogramowanie powinno zapewniać pełne bezpieczeństwo danych, niezawodność, oraz wsparcie dla popularnych platform wirtualizacji. Wymagania:
	1. Kompatybilność z platformami wirtualizacyjnymi: Oprogramowanie musi być kompatybilne z wiodącymi platformami wirtualizacji, w tym VMware vSphere (wersje 6.5 i wyższe) oraz Microsoft Hyper-V (wersje z Windows Server 2016 i wyższe).
	2. Funkcjonalność tworzenia kopii zapasowych:
		* Oprogramowanie powinno umożliwiać tworzenie pełnych, różnicowych oraz przyrostowych kopii zapasowych maszyn wirtualnych, z możliwością planowania zadań backupu według harmonogramu ustalonego przez administratora.
		* Musi wspierać technologię deduplikacji, co pozwala na oszczędność przestrzeni dyskowej przez eliminację zduplikowanych danych w kopiach zapasowych.
		* Musi wspierać technologię kompresji, co znacznie skraca czas tworzenia kopii zapasowych, magazynowania i przywracania danych.
		* Musi wspierać jednoczesne tworzenie kopii zapasowych wielu maszyn wirtualnych.
		* Musi oferować funkcję tworzenia kopii zapasowych z komputerów oraz serwerów z systemem Windows.
		* Powinno oferować funkcję backupu bezagentowego, umożliwiającą tworzenie kopii zapasowych bez potrzeby instalacji dodatkowego oprogramowania na maszynach wirtualnych.
	3. Zarządzanie kopiami zapasowymi:
		* Oprogramowanie powinno posiadać centralny interfejs zarządzania, umożliwiający monitorowanie, konfigurowanie i zarządzanie wszystkimi zadaniami backupu z jednego miejsca.
		* Musi oferować zaawansowane raportowanie oraz generowanie logów, które ułatwią śledzenie statusu zadań oraz identyfikację potencjalnych problemów.
		* Powinno umożliwiać automatyczne usuwanie starych kopii zapasowych na podstawie określonych polityk, co pomoże w efektywnym zarządzaniu przestrzenią dyskową.
	4. Funkcje przywracania danych:
		* Oprogramowanie musi umożliwiać szybkie i elastyczne przywracanie danych, w tym pełnych maszyn wirtualnych, poszczególnych plików lub katalogów, oraz punktów w czasie (instant recovery).
		* Powinno wspierać funkcję przywracania na poziomie plików (file-level recovery), umożliwiającą selektywne odzyskiwanie plików bez potrzeby przywracania całej maszyny wirtualnej.
	5. Zabezpieczenia i ochrona danych:
		* Oprogramowanie musi oferować zaawansowane opcje szyfrowania danych zarówno podczas tworzenia kopii zapasowych, jak i w trakcie ich przesyłania (np. szyfrowanie AES-256).
		* Powinno wspierać funkcję tworzenia zaszyfrowanych kopii zapasowych, które mogą być przechowywane w bezpiecznych lokalizacjach (np. na serwerach zdalnych lub w chmurze).
	6. Wsparcie dla środowisk chmurowych:
		* Oprogramowanie powinno być kompatybilne z popularnymi usługami chmurowymi, umożliwiając przechowywanie kopii zapasowych w takich środowiskach jak Amazon S3, Microsoft Azure, Google Cloud, itp.
		* Powinno oferować funkcję zautomatyzowanego tworzenia kopii zapasowych do chmury, z możliwością szybkiego odzyskiwania danych w przypadku awarii lokalnej infrastruktury.
	7. Zamawiający oczekuje licencji na minimum 10 maszyn wirtualnych, z możliwością rozszerzenia w przyszłości. Licencje powinny być wieczyste (perpetual) bez konieczności ponoszenia jakichkolwiek w przyszłości.
	8. Wykonawca powinien zapewnić wsparcie techniczne oraz dostęp do aktualizacji oprogramowania przez okres minimum 3 lat od daty dostawy. Wsparcie powinno obejmować pomoc w instalacji, konfiguracji, oraz rozwiązywaniu problemów związanych z działaniem oprogramowania.
17. Zgodność z normą ISO 9001 oraz ISO 14001 lub równoważnymi.
18. Serwer musi posiadać deklaracja CE.
19. Zainstalowany specjalistyczny system operacyjny przeznaczony dla serwerów do przechowywania danych, oferujący zaawansowane funkcje takie jak: zarządzanie plikami, wirtualizacja, obsługa kontenerów, backup, synchronizacja z chmurą, oraz wsparcie dla wielu użytkowników z zaawansowanymi ustawieniami uprawnień.
20. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
21. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
22. Serwer musi być kompatybilny z popularnymi systemami backupu oraz oprogramowaniem do wirtualizacji, takimi jak Vmware i Hyper-V.
23. Gwarancja:
	1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
	2. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji.
	3. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
	4. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.
	5. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
		* możliwość pobierania najnowszego firmware,
		* dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
		* dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
24. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja serwera oraz oprogramowania oprogramowanie do tworzenia i zarządzania kopiami zapasowymi na serwerze.
		* Konfiguracja dysków SSD w RAID 1 oraz dysków HDD w RAID 5.
		* Konfiguracja zabezpieczeń.
		* Konfiguracja serwera oraz oprogramowania zgodnie z wymaganiami zamawiającego. Serwer będzie zainstalowany w innej lokalizacji niż dane, więc należy skonfigurować łącze VPN pomiędzy dwoma lokalizacjami.
		* Integracja z istniejącymi systemami IT zamawiającego uwzględniając umiejscowienie serwera w innej lokalizacji niż dane przeznaczone do backupu.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania serwera wraz z oprogramowaniem.

**10. Serwer NAS – dostawa, instalacja i konfiguracja (do backupu) – 1 kpl.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja zestawu składającego się z 2 szt. serwerów do przechowywania danych.

**Wymagania:**

1. Obudowa Tower z min. 2 zatokami na dyski SATA HDD i SSD o wielkości 3,5 cala oraz 2,5 cala.
2. Zainstalowany 1 procesor klasy x86 min. 4-rdzeniowy o taktowaniu min. 2.0GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 2 900 pkt. Wynik należy dołączyć do oferty.
3. Pamięć RAM min. 2 GB DDR4 z możliwością rozbudowy do co najmniej 6 GB.
4. Wbudowane min. 2 porty USB 3.2
5. Powyższe porty USB nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
6. Zainstalowane i w pełni funkcjonalne minimum 2 porty 1GbE RJ45. Porty nie mogą zajmować slotów PCI-E
7. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1.
8. Pamięć masowa:
	1. Zainstalowane min. 2 dyski HDD SATA o pojemności min. 4 TB każdy.
9. Min. 1 wentylator.
10. Min. 1 zasilacz o mocy min. 60W, zainstalowany wewnątrz serwera.
11. Diody LED umieszczone z przodu obudowy serwera informujące o statusie: dysków, LAN i zasilaniu.
12. Wraz ze serwerem dostarczone powinno być oprogramowanie do tworzenia kopii zapasowych i odzyskiwania danych komputerów, serwerów i maszyn wirtualnych w środowiskach wirtualizacyjnych. Oprogramowanie powinno zapewniać pełne bezpieczeństwo danych, niezawodność, oraz wsparcie dla popularnych platform wirtualizacji. Wymagania:
	1. Zaawansowane funkcje tworzenia kopii zapasowych
	2. Ochrona integralności danych oraz infrastruktury IT
	3. Natychmiastowe odzyskiwanie po awarii
	4. Deduplikacja
	5. Szyfrowanie i kompresja
	6. Statystyki użycia
	7. Wstrzymywanie i wznawianie tworzenia kopii zapasowych
13. Zgodność z normą ISO 9001.
14. Serwer musi posiadać deklaracja CE.
15. Zainstalowany specjalistyczny system operacyjny przeznaczony dla serwerów do przechowywania danych.
16. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
17. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
18. Serwer musi być kompatybilny z popularnymi systemami backupu oraz oprogramowaniem do wirtualizacji.
19. Gwarancja:
	1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
	2. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji.
	3. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
	4. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.
	5. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
		* możliwość pobierania najnowszego firmware,
		* dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
		* dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
20. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja serwera oraz oprogramowania oprogramowanie do tworzenia i zarządzania kopiami zapasowymi na serwerze.
		* Konfiguracja dysków HDD w RAID 5.
		* Konfiguracja zabezpieczeń.
		* Konfiguracja serwera oraz oprogramowania zgodnie z wymaganiami zamawiającego.
		* Integracja z istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania serwera wraz z oprogramowaniem.

**11. UPS centralny – dostawa i instalacja – 1 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. UPS centralnego.

**Wymagania:**

1. MOC min. 30000VA/27000W
2. Obudowa Tower
3. Maksymalna wysokość/głębokość rozwiązania: 1600mm/850mm (dotyczy zarówno jednostki zasilającej jak i szaf bateryjnych)
4. Waga modułu UPS: max. 90 kg.
5. Kolorowy wyświetlacz LCD z panelem dotykowym
6. Topologia podwójnej konwersji online
7. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne
8. Trójfazowa konstrukcja wejścia/wyjścia
9. Efektywność trybu ECO online do 98%
10. Wejściowy prąd znamionowy: 42 A
11. THDI <3% (Full Linear Load)
12. Współczynnik mocy wejściowej: 0.99
13. Tolerancja napięcia wyjściowego: 1.5%
14. Tolerancja napięcia w trybie ECO: ± 10%
15. Współczynnik szczytu: 3 : 1
16. Zniekształcenia harmoniczne (obciążenie liniowe): THD＜1%
17. Zniekształcenia harmoniczne (obciążenie nieliniowe): THD＜5.5%
18. Czas przełączania 0 ms
19. Konstrukcja z dwoma wejściami umożliwiając podłączenie jednego wejścia ze źródła zasilania prądem przemiennym i drugiego wejścia z innego źródła zasilania.
20. Serwisowy przełącznik obejściowy do płynnego przełączania zasilania na źródło sieciowe w trybie obejścia.
21. Kompatybilność z generatorem z wbudowaną funkcją automatycznej regulacji napięcia (AVR) do stabilizacji niestabilnych poziomów napięcia prądu z generatora.
22. Zgodne typy baterii: VRLA, AGM, Gel
23. Czas podtrzymania systemu min. 7 minut dla mocy 18 kW
24. Możliwość wydłużenia czasu podtrzymania przez dołożenie zestawów bateryjnych dostarczonych w zamkniętych szafach.
25. Możliwość ładowania szaf bateryjnych z mocą do 20% mocy UPS.
26. Możliwość pracy równoległej.
27. Możliwość łączenia równoległego do min. 4 jednostek UPS
28. Gniazdo wyjściowe: Kostka zaciskowa do łączenia przewodów
29. Złącze wejściowe: Kostka zaciskowa do łączenia przewodów
30. Porty komunikacyjne: RS232, RS485, SNMP, EPO, Dry contact
31. Zdalna komunikacja po protokole SNMP oraz http
32. Oprogramowanie w języku polskim do zarządzania UPSem z możliwością monitorowania zużycia energii oraz współpracy ze środowiskiem VMware ESXi 8.0 U2
33. Certyfikaty CE, IEC62040-1, IEC62040-2.
34. Gwarancja min. 24 miesiące.
35. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
36. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
37. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja UPS i zestawów bateryjnych oraz podłączenie do sieci.
		* Konfiguracja UPS zgodnie z wymaganiami zamawiającego.
		* Integracja UPS z agregatem będącym przedmiotem tego postępowania oraz istniejącymi systemami IT zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania UPS oraz zestawów bateryjnych

**12. UPS stanowiskowy – dostawa i instalacja – 8 szt.**

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 8 szt. UPS stanowiskowych.

**Wymagania:**

1. MOC min. 850VA/520W
2. Obudowa Tower
3. Topologia offline
4. Klasa energetyczna sprzętu przeciwprzepięciowego: 310 J
5. Zabezpieczenie przeciwprzepięciowe: bezpiecznik minimum 7A
6. Nominalne napięcie wejściowe 230V
7. Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie)
8. Standard wtyczki: Francuska/Belgijska
9. Zmienny zakres napięcia wejściowego w trybie podstawowym 180 - 266V
10. Napięcie wyjściowe 230V
11. Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz +/- 1 Hz
12. Współczynnik mocy: minimum 0.6
13. Typ przebiegu przy pracy bateryjnej: Schodkowa aproksymacja sinusoidy
14. Złącza/gniazda wyjściowe:
	1. 8 gniazd francuskich/belgijskich: 6 z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania, 2 z zabezpieczeniem przeciwprzepięciowym.
	2. 1 gniazdo USB-A 2.4A, 1 gniazdo USB-C 2.4A
15. Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu
16. Czas autonomii:
	1. min. 2 minuty 15 sekund dla pełnego obciążenia
	2. min. 9 minut 45 sekund dla połowy obciążenia
17. Czas ładowania: max. 16 h
18. Baterie wymieniane bez wyłączania urządzenia (hot-swap)
19. Diody statusu LED: praca na baterii, zasilanie z sieci, alert wymiany baterii
20. Alarm dźwiękowy: Praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, zastępcza bateria wykryta
21. Certyfikaty: CE, RoHS, REACH
22. Gwarancja: min. 24 miesiące naprawy lub wymiany
23. Żywotność akumulatora: min. 2 lata
24. Oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowe lub USB i oferujące:
	1. Monitorowania i zarządzania zasilaczy UPS
	2. Bezobsługowego, bezpiecznego wyłączania podczas problemów z zasilaniem
	3. Bezpieczny dostęp do internetowego interfejsu użytkownika (UI)
	4. Możliwość dokładnego określania czasu i sekwencji zdarzeń powodujących zdarzenie za pomocą dziennika zdarzeń
	5. Identyfikacja potencjalnie niebezpiecznych trendów zanim dojdzie do eskalacji problemu lub eksportowanie dziennika w celu analizy
25. Czas przełączania: max. 10ms
26. UPS musi posiadać możliwość łatwej wymiany baterii, bez użycia żadnych narzędzi.
27. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
28. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
29. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		* Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
		* Opracowanie planu wdrożenia.
	2. Wdrożenie i konfiguracja:
		* Instalacja UPS oraz podłączenie do wskazanych urządzeń.
		* Konfiguracja UPS zgodnie z wymaganiami zamawiającego.
	3. Testy akceptacyjne:
		* Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
		* Weryfikacja poprawności działania UPS.

**13. Oprogramowanie do monitoringu urządzeń sieciowych, stacji roboczych, inwentaryzacji sprzętu i oprogramowania – instalacja, konfiguracja oraz wdrożenie – 1 szt.**

Przedmiotem zamówienia jest dostawa i wdrożenie systemu monitorowania infrastruktury IT, który zapewni kompleksową kontrolę nad zasobami sieciowymi, serwerami, aplikacjami oraz usługami IT. System ma zapewnić pełne wsparcie dla operacji IT, wczesne wykrywanie problemów, automatyzację zadań oraz zapewnienie wysokiej dostępności i wydajności infrastruktury. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

**Wymagania:**

1. Oprogramowanie musi być dostępne w wersji komercyjnej gotowej do instalacji i konfiguracji w środowisku Zamawiającego.
2. Oprogramowanie musi być dostępne w oficjalnej dystrybucji na terenie Polski.
3. Oprogramowanie musi być opatrzone licencją i ścieżką rozwoju producenta.
4. Licencjonowanie musi być oparte o ilość unikatowych monitorowanych adresów IP.
5. Licencjonowanie nie może ograniczać ilości monitorowanych metryk w ramach monitorowanego adresu IP.
6. System musi być dostarczony w najnowszej dostępnej wersji oprogramowania.
7. System musi być dostarczony z licencją bezterminową dla 30 hostów/adresów IP.
8. System musi być dostarczony wraz ze wsparciem produktowym producenta przez okres minimum 24 miesiące (upgrade do najnowszej wersji, pomoc techniczna). Oferowane oprogramowanie musi posiadać wsparcie, którego co najmniej pierwsza linia jest świadczona w języku polskim.
9. Dołączona dokumentacja, instrukcje/prezentacje konfiguracji i obsługi oprogramowania.
10. Monitorowanie serwerów i urządzeń sieciowych:
	1. Możliwość monitorowania różnorodnych systemów operacyjnych (Windows, Linux, Unix).
	2. Obsługa monitorowania urządzeń sieciowych (routery, switchy, firewalle).
	3. Monitorowanie zasobów fizycznych (CPU, pamięć, dyski twarde).
11. Monitorowanie aplikacji i usług:
	1. Monitorowanie dostępności i wydajności aplikacji webowych oraz baz danych.
	2. Wsparcie dla monitorowania aplikacji chmurowych (AWS, Azure, Google Cloud).
	3. Możliwość monitorowania usług takich jak HTTP, HTTPS, FTP, SMTP, DNS itp.
12. Monitorowanie użytkowników i aplikacji www:
	1. Realizacja automatycznych testów pracy użytkownika w aplikacji www
	2. Monitorowanie wydajności aplikacji z perspektywy użytkownika końcowego.
	3. Kontrola międzyczasów podstron/kroków scenariusza pracy użytkownika aplikacji www.
13. Alertowanie i powiadomienia:
	1. Definiowanie progów alarmowych i automatyczne powiadamianie (e-mail, SMS, powiadomienia PUSH).
	2. Możliwość konfiguracji alertów w zależności od krytyczności incydentu.
	3. Integracja z systemami zarządzania incydentami (ITSM).
	4. Eskalacja powiadomień
14. Raportowanie i analiza danych
	1. Generowanie raportów dotyczących dostępności, wydajności oraz wykorzystania zasobów.
	2. Wizualizacja danych w postaci wykresów i dashboardów.
	3. Możliwość eksportu raportów do formatów takich jak PDF, CSV.
	4. Tworzenie i modyfikacja raportów za pośrednictwem interfejsu WWW bez konieczności instalacji dodatkowego oprogramowania (poza przeglądarką i ew. technologiami Java, Flash itp.).
	5. Narzędzie raportujące musi umożliwiać automatyczną generację dowolnych raportów według zdefiniowanego harmonogramu, możliwość generowania raportów dostępności (wg hostów lub usług), raportów SLA (wg hostów lub usług), raportowanie incydentów, awarii itp., raportowanie wydajności sieci, zapis raportów do plików PDF, okresowe wysyłanie raportów e-mailem do wskazanych użytkowników, powiadomienia e-mail o incydencie, zapis zdefiniowanych parametrów raportów celem późniejszego wywołania.
15. Automatyzacja i orkiestracja
	1. Automatyczna konfiguracja nowych urządzeń
	2. Automatyczne wykonywanie skryptów w odpowiedzi na zdarzenia.
	3. Integracja z narzędziami do zarządzania konfiguracją (Ansible, Puppet, Chef).
	4. Możliwość definiowania i uruchamiania zadań uwzględniając harmonogram dni i godzin.
16. Bezpieczeństwo i audyt
	1. Zapewnienie szyfrowanej komunikacji między komponentami systemu.
	2. Monitorowanie i audytowanie zdarzeń związanych z bezpieczeństwem.
	3. Wbudowany mechanizm tworzenia kopii zapasowych ustawień systemu (monitorowane hosty i usługi).
	4. Wbudowany mechanizm zarządzania użytkownikami systemu.
	5. Możliwość tworzenia grup użytkowników.
	6. Historia danych statystycznych.
	7. Mechanizm przydzielania uprawnień użytkowników (dostęp do danych nt. hostów lub usług, możliwość konfiguracji obiektów, powiadomienia).
	8. Audyt pracy uzytkownika w systemie
17. Integracje i API
	1. Otwarte API umożliwiające integrację z innymi systemami.
	2. Wsparcie dla integracji z popularnymi narzędziami do zarządzania IT (np. ServiceNow, Jira).
	3. Natywna integracja z systemami do centralnego gromadzenia logów i analizy zdarzeń opartymi o architekturę Elasticsearch, Opensearch
	4. Natywna integracja z systemami klasy SOAR
	5. Możliwość korzystania z webhooków do przesyłania danych w czasie rzeczywistym.
	6. Możliwość konfiguracji oprogramowania poprzez stronę www oraz programistyczne, udokumentowane API.
18. Interfejs użytkownika
	1. Interfejs graficzny do wizualizacji struktury sieci.
	2. Interfejs graficzny do wizualizacji poszczególnych wybranych parametrów urządzeń.
	3. Przyjazny i intuicyjny interfejs webowy dostępny z poziomu przeglądarki.
	4. Możliwość personalizacji podstawowego ekranu aplikacji w powiązaniu z użytkownikiem systemu oraz dowolnej konfiguracji składników wyświetlanych na podstawowym ekranie aplikacji poprzez wybór odpowiednich widget’ów.
	5. Możliwość tworzenia wielu dashboardów
	6. Możliwość tworzenia dashboardów prywatnych jak i współdzielnych pomiędzy innymi użytkownikami aplikacji
	7. Możliwość tworzenia dashboardów typu iFrame - będącymi oknem aplikacji zewnętrznych
	8. Możliwość tworzenia własnych dodatków do dashboardów w formie obietków programistycznych typu Widget. Aplikacja musi wspierać dodawanie własnych rozszerzeń do dashboardów.
	9. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień push.
	10. Możliwość tworzenia i zapisywania filtrów dla monitorowanych urządzeń i ich parametrów
	11. Możliwość wykorzystania filtrów podczas tworzenia dashboardów
19. Monitorowanie specyficznych parametrów i elementów infrastruktury
	1. Monitorowanie podstawowych parametrów sprzętowych bez użycia dodatkowych agentów oraz pozostałych parametrów działania systemu operacyjnego i usług za pomocą dedykowanych agentów (w zależności od konfiguracji monitorowanego hosta).
	2. Możliwość monitorowania aplikacji i procesów o dynamicznym zachowaniu.
	3. Możliwość monitorowania min. krytycznych elementów infrastruktury, aplikacji, usług sieciowych, protokołów sieciowych, wskaźników systemowych, infrastruktury sieciowej, portów.
	4. Możliwość śledzenia parametrów takich jak:
		1. Telnet na wybrany port - nasłuch na porcie,
		2. Ping dostępność urządzenia,
		3. Odczyt, przetwarzanie i generowanie alertów z pułapek SNMP,
		4. Poprawne działanie serwera DHCP,
		5. Poprawne działanie serwera czasu NTP,
		6. Zajętość danych na poszczególnych partycjach,
		7. Zajętość RAM,
		8. Obciążenie systemu,
		9. Obciążenie dysków,
		10. Ilość zalogowanych użytkowników,
		11. Ilość procesów,
		12. Obecność procesów w systemie,
		13. Synchronizacja dysków programowego RAID,
		14. Synchronizacja dysków sprzętowego RAID,
		15. Kontrola parametrów polecenia VMSTAT,
		16. Obecność SSH.
	5. Możliwość śledzenia parametrów monitoringu systemu poczty:
		1. Poprawne działanie serwera SMTP,
		2. Poprawne działanie serwera POP3,
		3. Poprawne działanie serwera IMAP,
		4. Ilość listów w kolejkach serwera Postfix.
	6. Możliwość śledzenia parametrów monitoringu DNS:
		1. Poprawne działanie DNS,
		2. Rozwiązywanie zadanych domen na adresy IP,
		3. Parametry serwerów WWW,
		4. Poprawne działanie serwera WWW,
		5. Kontrola występowania oczekiwanych treści na stronie,
		6. Czas odpowiedzi serwera WWW.
	7. Możliwość śledzenia parametrów monitoringu bazy danych:
		1. Poprawna praca bazy,
		2. Kontrola stanu synchronizacji baz,
		3. Zajętość przestrzeni danych.
	8. Możliwość śledzenia parametrów DRBD i HEARTBEAT:
		1. Poprawne działanie klastra,
		2. Poprawne działanie replikacji danych.
	9. Możliwość śledzenia parametrów macierzy dyskowych:
		1. Analiza statusów ogólnych urządzenia,
		2. Analiza dysków urządzenia.
20. Dodatkowe Elementy Infrastruktury Informatycznej do Monitorowania
	1. Monitorowanie zasobów wirtualnych (maszyny wirtualne, hypervisory).
	2. Monitorowanie infrastruktury kontenerowej (Docker, Kubernetes).
	3. Monitorowanie systemów backupowych i urządzeń magazynujących.
	4. Monitorowanie systemów IoT i urządzeń edge computing.
	5. Monitorowanie systemów SCADA i przemysłowych systemów sterowania.
	6. Monitorowanie infrastruktury zasilania (UPS, generatory).
	7. Monitorowanie systemów HVAC (Heating, Ventilation, and Air Conditioning).
21. Architektura Systemu
	1. System musi działać w modelu klient-serwer.
	2. System pracuje pod kontrolą środowiska systemu operacyjnego Open Source
	3. Możliwość wdrożenia systemu zarówno on-premises, jak i w chmurze.
	4. Wsparcie dla skalowalności poziomej i pionowej.
	5. System musi wspierać architekturę wysokiej dostępności dla każdej warstwy systemu.
22. System musi umożliwić rozbudowę, pozwalającą na monitorowanie nieograniczonej wydajnością liczby urządzeń w sieci. Architektura musi umożliwiać rozkładanie obciążenia pomiędzy elementy systemu.
23. Wymagania dotyczące składowania danych
	1. Możliwość replikacji i backupu danych.
	2. Gromadzone dane muszą musza być składowane w nierelacyjnej bazy danych.
24. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień.
25. Dostęp do bazy wiedzy i dokumentacji technicznej.
26. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		1. Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania.
		2. Opracowanie szczegółowego planu wdrożenia.
	2. Instalacja i konfiguracja:
		1. Instalacja i konfiguracja oprogramowania na serwerze.
		2. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
		3. Testy funkcjonalne systemu.
	3. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

Dodatkowo należy dostarczyć, zainstalować, skonfigurować oraz wdrożyć system do analizy oraz reakcji na zagrożenia w celu kompleksowej ochrony infrastruktury IT. System musi bazować na nowoczesnych technologiach klasy SIEM (Security Information and Event Management), a także umożliwia holistyczne podejście do bezpieczeństwa oraz zarządzanie incydentami w sposób wysoce zautomatyzowany i skalowalny. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

**Wymagania:**

1. Zbieranie i analiza danych:

System musi gromadzić dane z różnorodnych źródeł, takich jak:

* Logi systemowe (systemów operacyjnych, serwerów, aplikacji, urządzeń sieciowych).
* Informacje o zdarzeniach (np. próby logowania, zmiany uprawnień, działania użytkowników).
* Dane dotyczące konfiguracji infrastruktury IT (np. plików konfiguracyjnych, polityk bezpieczeństwa).

System musi automatycznie analizować te dane w czasie rzeczywistym, identyfikując potencjalne zagrożenia oraz anomalie na podstawie wcześniej zdefiniowanych reguł, sygnatur oraz zaawansowanych algorytmów analitycznych.

2. Monitorowanie bezpieczeństwa

Kluczową funkcją systemu musi być ciągłe monitorowanie stanu bezpieczeństwa w czasie rzeczywistym. System musi umożliwiać:

* Wczesne wykrywanie zagrożeń: Wykorzystanie analizy behawioralnej oraz sztucznej inteligencji do identyfikacji nietypowych zachowań użytkowników, urządzeń i aplikacji.
* Pełna widoczność nad wszystkimi elementami infrastruktury IT, w tym także nad środowiskami wirtualnymi i chmurowymi.
* Analiza historyczna zdarzeń: System musi umożliwiać retrospektywne badanie logów i zdarzeń, co jest niezbędne do dochodzeń powłamaniowych i audytów bezpieczeństwa.

3. Wykrywanie i reagowanie na zagrożenia

System musi posiadać zaawansowane wykrywanie zagrożeń w różnych środowiskach, takich jak:

* Środowiska chmurowe (AWS, Azure, Google Cloud).
* Kontenery (Docker, Kubernetes).
* Urządzenia końcowe.

Oraz rozszerzać możliwości SIEM, pozwalając na:

* Skoordynowane wykrywanie zagrożeń w całym środowisku IT.
* Szybkie reagowanie na incydenty dzięki integracji z innymi narzędziami do zarządzania i automatyzacji (np. firewalle, narzędzia do zarządzania zasobami IT).
* Automatyzację działań naprawczych, co redukuje czas reakcji na zagrożenia oraz minimalizuje ryzyko.

4. Zarządzanie incydentami bezpieczeństwa

System musi wspierać zarządzanie incydentami bezpieczeństwa poprzez:

* Automatyczne powiadomienia o wykrytych zagrożeniach, pozwalające administratorom na szybkie podjęcie działań.
* Raportowanie incydentów z pełnym zestawem informacji potrzebnych do analizy i dalszych działań naprawczych.
* Korelowanie zdarzeń z różnych źródeł w celu lepszego zrozumienia zagrożeń i zidentyfikowania ich źródła.

5. Zarządzanie zgodnością z regulacjami

System musi pomagać organizacji w utrzymywaniu zgodności z regulacjami prawnymi i standardami bezpieczeństwa poprzez:

* Monitorowanie działań użytkowników i zapis zmian w systemach, co pozwala na śledzenie operacji oraz wykrywanie nieautoryzowanych działań.
* Automatyczne generowanie raportów audytowych i zgodności, które można przedstawić audytorom oraz organom nadzoru.
* Tworzenie alertów zgodności, które informują o potencjalnych naruszeniach polityk bezpieczeństwa.

6. Skalowalność i integracja

System musi oferować wysoką skalowalność oraz zapewniać integrację z szeroką gamą innych rozwiązań i narzędzi używanych w ramach zabezpieczeń IT.

7. Zakres prac wdrożeniowych:

a) Analiza przedwdrożeniowa:

* Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania.
* Opracowanie szczegółowego planu wdrożenia.

b) Instalacja i konfiguracja:

* Instalacja i konfiguracja oprogramowania na serwerze.
* Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
* Testy funkcjonalne systemu.

c) Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

Dodatkowo należy również dostarczyć, zainstalować, skonfigurować oraz wdrożyć oprogramowanie na 25 stacji roboczych do zarządzania uprawnieniami użytkowników. Oprogramowanie to ma na celu zapewnienie bezpiecznej i efektywnej kontroli nad przydzielaniem i wykorzystywaniem uprawnień administracyjnych, umożliwiając użytkownikom wykonywanie zadań wymagających podwyższonych uprawnień, bez konieczności stałego posiadania pełnych praw administratora. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

**Wymagania:**

1. Kontrola dostępu administracyjnego:
	1. Możliwość przyznawania tymczasowych uprawnień administracyjnych na żądanie użytkownika, na określony czas lub tylko do konkretnej aplikacji.
	2. Funkcjonalność logowania i monitorowania wszystkich działań wykonywanych przy użyciu podwyższonych uprawnień.
	3. Możliwość blokowania dostępu do określonych funkcji systemu operacyjnego oraz aplikacji, nawet po przyznaniu uprawnień administracyjnych.
	4. Uwierzytelnianie wieloskładnikowe (MFA) w celu zapewnienia drugiego poziom kontroli bezpieczeństwa przed udzieleniem uprawnień administratora.
	5. MFA dla użytkowników w dostępie do aplikacji.
2. Zarządzanie uprawnieniami:
	1. Centralne zarządzanie politykami uprawnień, które mogą być dostosowane do różnych grup użytkowników.
	2. Automatyczne cofanie uprawnień administracyjnych po zakończeniu zadania wymagającego podwyższonych uprawnień.
3. Bezpieczeństwo i zgodność z przepisami:
	1. Zgodność z wymaganiami dotyczącymi audytu bezpieczeństwa oraz przepisami RODO, poprzez szczegółowe rejestrowanie i raportowanie aktywności użytkowników, logowań administratorów i instalacji oprogramowania. Zakres zgodności z RODO musi być opisany w dokumentacji oprogramowania.
	2. Zgodność z normą ISO 27001. Zakres zgodności z normą ISO 27001 musi być opisany w dokumentacji oprogramowania.
	3. Zgodność z dyrektywą NIS2. Zakres zgodności z dyrektywą NIS2 musi być opisany w dokumentacji oprogramowania.
	4. Integracja z istniejącymi systemami bezpieczeństwa IT, w tym z systemami SIEM, w celu monitorowania i analizowania logów.
4. Wsparcie dla różnych platform:
	1. Kompatybilność z Windows 10/11, macOS oraz Linux.
	2. Możliwość integracji z rozwiązaniami chmurowymi oraz lokalnymi infrastrukturami IT.
5. Interfejs użytkownika:
	1. Intuicyjny i łatwy w obsłudze interfejs dla użytkowników końcowych oraz administratorów IT w języku polskim.
	2. Możliwość dostosowania interfejsu do indywidualnych potrzeb organizacji.
6. Oprogramowanie powinno być dostarczone w formie agenta instalowanego tylko dla punktów końcowych, lekkie (plik instalacyjny max. 3MB) i łatwe do wdrożenia i nie obciążające zasobów stacji roboczych, centralne i zdalne zarządzanie z dowolnego miejsca z poziomu środowiska hostowanego SaaS klasy korporacyjnej (Microsoft Azure, AWS lub Google Cloud) bez konieczności instalacji aplikacji na lokalnych serwerach.
7. Możliwość zarządzania uprawnieniami ze smartfona za pomocą aplikacji mobilnej na Android i Apple.
8. Rozwiązanie musi działać zarówno online, jak i offline. W przypadku offline zatwierdzenie zmian lub uprawnień musi odbywać się kodem PIN.
9. Możliwość odinstalowania agenta lokalnie na stacji roboczej tylko przy wpisaniu kodu PIN.
10. Jednoczesna obsługa punktów końcowych bez AD, wielodomenowych Active Directory i Azure Active Directory.
11. Wsparcie techniczne oraz aktualizacje oprogramowania na okres co najmniej 24 miesiące.
12. Dostępność szczegółowej dokumentacji technicznej w języku polskim dla administratorów systemu.
13. Zakres prac wdrożeniowych:
	1. Analiza przedwdrożeniowa:
		1. Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania.
		2. Opracowanie szczegółowego planu wdrożenia.
	2. Instalacja i konfiguracja:
		1. Instalacja i konfiguracja oprogramowania na wskazanych stacjach roboczych.
		2. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
		3. Testy funkcjonalne systemu.
	3. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

**14. Oprogramowanie do wykonywania kopii zapasowych (backupu) – 1 kpl.**

Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania do backupu 10 instancji (stacji roboczych i serwerów) w postaci licencji wieczystej, z możliwością rozbudowy o rozwiązania chmurowe i funkcje ochrony przed zagrożeniami zewnętrznymi, w tym ransomware. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

**Wymagania:**

1. Oprogramowanie musi zapewniać efektywną ochronę danych dla środowisk wirtualnych i fizycznych działających lokalnie. Powinno obsługiwać backup maszyn wirtualnych (VM) oraz serwerów fizycznych i punktów końcowych, zarówno z systemami Windows, jak i Linux.
2. Oprogramowanie powinno umożliwiać szybkie i granularne przywracanie danych na poziomie plików oraz elementów aplikacyjnych. Wymagane jest wsparcie dla rozwiązań Microsoft, takich jak Microsoft Exchange, SharePoint, Active Directory oraz SQL Server, z możliwością szybkiego odtwarzania wybranych elementów aplikacji za pomocą Veeam Explorers.
3. Oprogramowanie musi oferować możliwość replikacji danych, co pozwoli na tworzenie bootowalnych kopii zapasowych obciążeń roboczych w lokalizacjach lokalnych lub zdalnych. Rozwiązanie powinno wspierać funkcje związane z migracją danych oraz odzyskiwaniem danych w przypadku awarii (disaster recovery).
4. Oprogramowanie powinno oferować możliwość przywracania i migracji maszyn wirtualnych Windows/Linux, serwerów fizycznych oraz punktów końcowych do środowisk chmurowych, takich jak AWS, Azure oraz Azure Stack. Integracja z chmurą musi być intuicyjna i zapewniać bezproblemową migrację oraz odtwarzanie danych.
5. Rozwiązanie musi umożliwiać weryfikację backupów pod kątem obecności złośliwego oprogramowania (malware), co pozwoli na bezpieczne przywracanie danych do środowiska produkcyjnego, eliminując ryzyko infekcji złośliwym oprogramowaniem.
6. Oprogramowanie powinno oferować prostą i skuteczną ochronę nieustrukturyzowanych danych poprzez intuicyjny kreator. Ochrona plików musi być prosta w obsłudze, zapewniając przy tym wysoką niezawodność.
7. Oprogramowanie musi być dostarczone w wersji licencji wieczystej z możliwością rozszerzenia funkcjonalności poprzez zakup dodatkowych licencji.
8. Intuicyjny interfejs użytkownika, umożliwiający łatwą konfigurację backupów i odtwarzania danych.
9. Rozwiązanie powinno być niezawodne i skalowalne, zapewniając wsparcie zarówno dla małych, jak i większych infrastruktur IT.
10. Skuteczna ochrona danych zarówno w środowisku fizycznym, jak i wirtualnym.
11. Szybkie odzyskiwanie danych na poziomie plików i aplikacji.
12. Elastyczność w zarządzaniu replikacją i migracją danych do środowisk chmurowych.
13. Wysoki poziom zabezpieczenia przed zagrożeniami związanymi z ransomware.
14. Łatwa w obsłudze ochrona plików i nieustrukturyzowanych danych.
15. W ramach zamówienia Wykonawca powinien zapewnić wsparcie techniczne oraz dostęp do aktualizacji oprogramowania przez okres minimum 24 miesięcy od daty dostawy. Wsparcie powinno obejmować pomoc w zakresie instalacji, konfiguracji oraz rozwiązywania problemów związanych z działaniem oprogramowania.
16. Wykonawca zobowiązany jest do dostarczenia pełnej dokumentacji technicznej w języku polskim lub angielskim, w tym instrukcji instalacji, konfiguracji oraz obsługi oprogramowania.
17. Zakres prac wdrożeniowych:
a. Analiza przedwdrożeniowa:
 - Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania do backupu na wskazanych serwerach i stacjach roboczych.
 - Opracowanie szczegółowego planu wdrożenia.
b. Instalacja i konfiguracja:
 - Instalacja i konfiguracja oprogramowania do backupu na wskazanych serwerach i stacjach roboczych.
 - Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
 - Testy funkcjonalne systemu.
c. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.