



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cyberbezpieczny
Samorząd

Powiat Tarnobrzeski
ul. 1 Maja 4
39-400 Tarnobrzeg

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup wraz z dostawą sprzętu komputerowego i oprogramowania, prace projektowe, wdrożeniowe, dokumentacyjne, konfiguracyjne, przy realizacji projektu „Cyberbezpieczny Powiat Tarnobrzeski”

Spis treści

1.	Przedmiot zamówienia.....	3
2.	Harmonogram realizacji.	3
3.	Podstawowe założenia	3
4.	Wymagania ogólne dotyczące przedmiotu zamówienia.	4
5.	Wymagania ogólne dotyczące wdrożenia.....	5
6.	Wymagania dodatkowe	6
7.	Równoważność rozwiązań	8
8.	Składniki zamówienia	8
8.1.	Świadczenie usług doradczych/ekspertkich.....	8
8.2.	Urządzenia UTM	9
8.2.1.	UTM wariant 1 – sztuk 7.....	9
8.2.2.	UTM wariant 2 – sztuk 4.....	18
8.3.	Tokeny do uwierzytelniania dwuskładnikowego 30 sztuk	26

8.4.	Rozwiązanie do monitorowania, raportowania i analizy ruchu sieciowego online ..	26
8.5.	Macierz dyskowa	29
8.6.	Serwery	34
8.6.1.	Wariant 1 – 2 sztuki	34
8.6.2.	Wariant 2 – 1 sztuka	42
8.6.3.	Kryteria stosowane w celu oceny równoważności Microsoft Windows Server Standard 2025	48
8.7.	Dostawa i uruchomienie zasilacza bezprzerwowego (UPS) – 1 sztuka	49
8.8.	Przełączniki sieciowe	51
8.8.1.	Przełącznik sieciowy wariant 1 - 2 sztuki.	51
8.8.2.	Przełącznik sieciowy wariant 2 - 1 sztuka	57
8.8.3.	Przełącznik sieciowy wariant 3 - 5 sztuk	62
8.8.4.	Przełącznik sieciowy wariant 4 - 1 sztuka	68
8.8.5.	Wkładki SFP+ do przełączników sieciowych	75
8.9.	Sieciowy punkt dostępowy - AccessPoint 16 sztuk	75
8.10.	Serwery NAS	77
8.10.1.	Serwer NAS wariant 1 - 1 sztuka	77
8.10.2.	Serwer NAS wariant 2 -11 sztuk	80
8.10.3.	Zasilacze bezprzerwowe (UPS) do serwerów NAS 12 sztuk	84
8.11.	Zewnętrzne dyski USB	85
8.12.	System kopii zapasowych	86
8.13.	Klucze sprzętowe do uwierzytelniania – 120 sztuk	89
8.14.	Zakup i wymiana akumulatorów w zasilaczu bezprzerwowym (UPS)	91
8.15.	System do zarządzania infrastrukturą IT w Starostwie	91
8.16.	System centralizujący zarządzanie infrastrukturą siecią LAN	98

1. Przedmiot zamówienia

Przedmiotem zamówienia w ramach niniejszego postępowania są prace analityczne, projektowe, wdrożeniowe, dokumentacyjne, instruktaże przy realizacji projektu „Cyberbezpieczny Powiat Tarnobrzelski” realizowanego w ramach projektu grantowego „Cyberbezpieczny Samorząd” w ramach programu operacyjnego Fundusze Europejskie na Rozwój Cyfrowy (FERC)

Zamówienie obejmuje następujące jednostki organizacyjne Powiatu Tarnobrzelskiego:

Nazwa	Adres
Starostwo Powiatowe w Tarnobrzegu	Tarnobrzeg ul. 1 Maja 4
Zespół Szkół Nr 1 w Nowej Dębie	Nowa Dęba ul. Mikołaja Reja 7
Zespół Szkół Nr 2 w Nowej Dębie	Nowa Dęba ul. Kościuszki 101
ZS Gorzyce	Gorzyce ul. Żwirki i Wigury 2
Specjalny Ośrodek Szkolno Wychowawczy w Grębowie	Grębów ul. Dolańskich 142
Zarząd Dróg Powiatu Tarnobrzelskiego	Nowa Dęba ul. Ogrodowa 20
Centrum Wsparcia i Rehabilitacji Społecznej w Gorzycach	Gorzyce ul. 11 Listopada 12
Środowiskowy Dom Pomocy Społecznej w Nowej Dębie	Nowa Dęba ul. Tadeusza Kościuszki 110
Poradnia Psychologiczno Pedagogiczna	Nowa Dęba ul. Mikołaja Reja 7
Dom Dziecka Skopanie	Skopanie ul. Leśna 2
Dom Pomocy Społecznej w Nowej Dębie	Nowa Dęba ul. Jana Pawła II 7
Powiatowe Centrum Pomocy Rodzinie w Tarnobrzegu	Tarnobrzeg ul. 1 Maja 4

2. Harmonogram realizacji.

Etap	Zakres	Maksymalny czas od podpisania umowy
1	Opracowanie Planu Realizacji Projektu, w tym procedur współpracy, procedur odbiorów, planu wdrożenia.	15 dni roboczych
2	Dostawa i konfiguracja sprzętu. Dostawa oprogramowania instalacja i konfiguracja oprogramowania.	3 miesiące
3	Opracowanie rekomendacji w zakresie zmian w polityce bezpieczeństwa dla Partnerów Projektu.	3 miesiące
4	Uruchomienie produkcyjne po zakończeniu testów - czas trwania testów wynosi do 6 dni roboczych od momentu ich rozpoczęcia.	4 miesiące

3. Podstawowe założenia

Z uwagi na to, że mamy do czynienia z jednostkami organizacyjnymi, należy przyjąć, że każda z nich ma własną politykę bezpieczeństwa, a co za tym idzie, musi mieć możliwość samodzielnego zarządzania urządzeniami sieciowymi realizującymi tę politykę.

Każda jednostka będzie administrować dostarczonym rozwiązaniem we własnym zakresie z wyjątkiem centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

4. Wymagania ogólne dotyczące przedmiotu zamówienia.

Wymaganie	Minimalne wymagania
1	Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na terenie kraju, zapewniających w szczególności realizację uprawnień gwarancyjnych, nie mogą pochodzić z rynku wtórnego. – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy.
2	Urządzenia nowe (tzn. wyprodukowane nie dawniej, niż na 12 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu realizacji procedur opisanych w zakresie Zamówienia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem).
3	Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne Wykonawcy w okresie wymaganym w SWZ. Jeżeli zgodnie z licencją producenta aktualizacja oprogramowania wymaga wykupienia odpowiedniego wsparcia u producenta to Wykonawca powinien takie wsparcie wykupić. Jeżeli do poprawnego działania wymaganych funkcjonalności konieczne jest wykupienie subskrypcji to Wykonawca powinien ją zapewnić na cały okres świadczenia usług gwarancyjnych.
4	Z uwagi na pożądaną pełną kompatybilność, łatwiejsze zarządzanie, wsparcie oraz zabezpieczenie uprawnień gwarancyjnych Zamawiającego, dostarczane w ramach Zamówienia rozwiązania (urządzenia oraz karty i moduły do nich itp.) powinny pochodzić od jednego producenta w ramach poszczególnych kategorii sprzętu chyba że wymagania szczegółowe stanowią inaczej. Muszą być w pełni kompatybilne z urządzeniami już używanymi przez Zamawiającego.
5	W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do: <ul style="list-style-type: none"> a) zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), b) zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych. c) jeżeli inspekcja, o której mowa powyżej wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów

	narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 20% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Strony w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych.
7	Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w stabilnej aktualnej wersji na dzień wdrożenia. Wymóg ten dotyczy również wersji firmware'u poszczególnych urządzeń.
8	Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
9	Cały dostarczony sprzęt musi być fabrycznie nowy, tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów jego poprawnej pracy.
10	Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych.
11	Dostarczenie obejmuje: <ul style="list-style-type: none"> a) wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack. b) urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać dostarczone w miejsce wskazane przez Zamawiającego, zamontowane, skonfigurowane i uruchomione. c) opakowania po urządzeniach muszą być usunięte wraz z innymi zbędnymi pozostałościami po procesie instalacji urządzeń.

5. Wymagania ogólne dotyczące wdrożenia

Wymaganie	Wymagania minimalne
1	Przeprowadzenie analizy przedwdrożeniowej w ramach której: <ul style="list-style-type: none"> a) powołania wspólnie z Zamawiającym Zespołu Roboczego, b) analizy infrastruktury Zamawiającego, c) analizy wymagań Zamawiającego, d) delegowania do pracy w Zespole Roboczym co najmniej jednego analityka do momentu zakończenia tych prac, e) opracowanie procedur współpracy, f) plan wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego i jednostek organizacyjnych oraz przewidującego rozwiązanie dla sytuacji kryzysowych wdrożenia,

	<ul style="list-style-type: none"> g) plan testów systemu uwzględniających sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności, h) sposób i propozycja terminów odbioru w podziale na każdego z partnerów, i) listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu, j) opis przypadków, w których projekt dopuszcza niedziałanie systemu.
2	Wdrożenie obejmuje dostawę, instalację, konfigurację i uruchomienie całości sprzętu i oprogramowania we wskazanych przez Zamawiającego lokalizacjach.
3	Przekazanie do Zamawiającego najpóźniej na 14 dni przed rozpoczęciem dostaw szczegółowego harmonogramu dostaw, instalacji i konfiguracji sprzętu i oprogramowania w podziale na partnerów projektu
4	Fizyczny montaż sprzętu w lokalizacjach wskazanych przez zamawiającego obejmujący podłączenie sprzętu do najbliższego punktu styku z Internetem oraz siecią energetyczną i wszystkimi wymaganymi instalacjami teletechnicznymi.
5	Przeprowadzenie instruktaży stanowiskowych.

6. Wymagania dodatkowe

Wymaganie	Minimalne wymagania
1.	W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową. Zamawiający wymaga następujących usług wdrożeniowych, realizowanych w porozumieniu z Zamawiającym
2.	<p>Sporządzenia Planu Realizacji Zamówienia w formie dokumentacji zawierającej wszystkie aspekty wdrożenia w szczególności:</p> <ul style="list-style-type: none"> a) procedury współpracy (m.in. sposób uzgadniania zawartości i układu formularzy elektronicznych oraz opisów usług, zakres i sposób przekazania przez Partnerów informacji niezbędnych do wdrożenia), b) plan wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązanie dla sytuacji kryzysowych wdrożenia, c) plan testów systemu uwzględniających sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności, d) sposób i termin odbioru w podziale na każdego z partnerów, e) listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu, f) opis przypadków, w których projekt dopuszcza niedziałanie systemu. g) potwierdzeniem prawidłowej realizacji przedmiotu Umowy, w zakresie Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu zawierający w szczególności:

	odbiór Dokumentacji Projektowej tj. Projektu Wdrożenia Systemu, Dokumentacji Testów Akceptacyjnych.
3.	Realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą.
4.	Dokumentacja Powykonawcza powinna w szczególności zawierać: <ul style="list-style-type: none"> a) szczegółową konfiguracją oraz opis infrastruktury technicznej wdrażanego rozwiązania, b) opis struktury i konfiguracji rozwiązania, c) zalecenia i procedury eksploatacyjne oraz zalecenia w zakresie konserwacji rozwiązania, d) numery seryjne dostarczonych urządzeń powiązane z ich fizyczną lokalizacją, e) listę adresów sprzętowych MAC interfejsów sieciowych f) procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji, g) procedury dotyczące wykonywania kopii bezpieczeństwa h) instrukcje dla administratorów i użytkowników, i) inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia, uzgodnione z Zamawiającym j) dokumentacja ta musi być sporządzona w języku polskim i dostarczona w formie elektronicznej, k) Procedury i instrukcje Producenta mogą być sporządzone w języku angielskim lub polskim.
5.	W ramach wymaganych usług wdrożeniowych Zamawiający wymaga dostarczenia wszystkich niezbędnych elementów przyłączeniowych takich jak: kable Ethernet, kable InfiniBand, kable zasilające, organizery, trwałe etykiety itp. wymagane do uzyskania opisanych w specyfikacji funkcjonalności.
6.	Zamawiający wymaga przeprowadzenia instruktażu stanowiskowego w zakresie obsługi dostarczonego sprzętu dla pracowników, w miejscu jego instalacji, w wymiarze 16 godzin dla Starostwa Powiatowego oraz 2 godzin dla pozostałych jednostek organizacyjnych. Tematyka instruktażu stanowiskowego powinna obejmować wszelkie czynności niezbędne do poprawnej eksploatacji dostarczonego sprzętu i oprogramowania, w tym modyfikacje topologii połączeń, wymiany komponentów sprzętowych oraz obsługę interfejsów zarządzających (zarówno poprzez konsolę graficzną jak i tekstową). Plan instruktażu stanowiskowego oraz termin jego przeprowadzenia muszą zostać uzgodnione z Zamawiającym i zaakceptowane przez Zamawiającego
7.	Warunkiem podpisania protokołu odbioru przez Zamawiającego jest zgodność stanu faktycznego wdrożenia z Dokumentacją Powykonawczą oraz pomyślne przeprowadzenie na dostarczonym sprzęcie testów według poniższej procedury:
7.1.	Czas trwania testów wynosi do 6 dni od momentu ich rozpoczęcia.
7.2.	Jeżeli w ciągu okresu trwania testów wystąpi jakakolwiek nieprawidłowość w funkcjonowaniu, np. samoczynny restart lub wyłączenie któregoś z dostarczonych elementów lub zanik łączności pomiędzy dostarczonymi

	elementami, musi być ona usunięta przez Wykonawcę i wówczas – jeżeli tak postanowi Zamawiający – cały test zostanie powtórzony.
7.3.	Wyłącznie pomyślne zakończenie ww. testów zobowiązuje podmiot odbierający do podpisania protokołu zdawczo-odbiorczego dostarczonego sprzętu.

7. Równoważność rozwiązań

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym.

W związku z tym, Wykonawca może proponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację dostarczoną przez Wykonawcę potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

8. Składniki zamówienia

Gwarancja na cały zakupiony sprzęt i licencje musi wynosić przynajmniej 12 miesięcy. Taki sam okres obowiązuje na usługi wsparcia. Zamawiający nie dopuszcza składania ofert częściowych i ofert wariantowych.

8.1. Świadczenie usług doradczych/eksperckich

Usługi z zakresu cyberbezpieczeństwa na czas trwania projektu w kluczowych aspektach:

- a) analizy bezpieczeństwa sieci – pomoc przy analizie zdarzeń we wszystkich dziennikach i wykrywaniu anomalii w oferowanym w oferowanej platformie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
- b) konsultacje i doradztwo w zakresie zapobieganiu wykrytym anomaliiom,
- c) pomoc w automatyzacji zabezpieczeń,
- d) rekonfiguracji urządzeń UTM,

- e) świadczenie usług powdrożeniowych z zakresu wsparcia użytkowników,
- f) pomoc w zapobieganiu, wykrywaniu i korygowaniu wykrytych problemów bezpieczeństwa,
- g) opracowanie planów mających za zadanie przeprowadzenie niezbędnych działań zwiększających poziom cyberbezpieczeństwa nie zrealizowanych w projekcie Cyberbezpieczny Samorząd – starostwo + jednostki organizacyjne.
- h) czas świadczenia usług 12 miesięcy.

8.2. Urządzenia UTM

Przedmiotem zamówienia jest dostawa fabrycznie nowych urządzeń na potrzeby jednostek organizacyjnych Powiatu.

Obecnie infrastruktura sieciowa w starostwie chroniona jest w oparciu o urządzenie UTM firmy Fortinet, które nie podlega wymianie.

Usługa obejmuje zakup, dostawę i wdrożenie do wskazanych jednostek organizacyjnych Powiatu (dostawa z wyłączeniem starostwa – tylko usługa rekonfiguracji).

Celem uniknięcia modyfikacji istniejących struktur logicznych w jednostkach organizacyjnych rozwiązanie może być wdrożone w trybie transparentnym pomiędzy siecią LAN, a routerem.

Dobór urządzeń na podstawie poniższych danych:

8.2.1. UTM wariant 1 – sztuk 7

Lp.	Parametr lub warunek	Wymagania
1.	Wymagania ogólne	<ol style="list-style-type: none"> System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: <ol style="list-style-type: none"> 4.1. Firewall. 4.2. Ochrony w warstwie aplikacji. 4.3. Protokołów routingu dynamicznego.

2.	Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ol style="list-style-type: none"> 1.1. 4 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
4.	Parametry wydajnościowe	<ol style="list-style-type: none"> 1. W zakresie Firewall'a obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 3 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 750 Mbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 450 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

5.	Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> 1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6.	Polityki, Firewall	<ol style="list-style-type: none"> 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ol style="list-style-type: none"> 2.1. Translację jeden do jeden oraz jeden do wielu. 2.2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

		<p>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <p>7.1. Amazon Web Services (AWS).</p> <p>7.2. Microsoft Azure.</p> <p>7.3. Cisco ACI.</p> <p>7.4. Google Cloud Platform (GCP).</p> <p>7.5. OpenStack.</p> <p>7.6. VMware NSX.</p> <p>7.7. Kubernetes.</p>
7.	Połączenia VPN	<p>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <p>1.1. Wsparcie dla IKE v1 oraz v2.</p> <p>1.2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</p> <p>1.3. Obsługa protokołu Diffie-Hellman grup 19, 20.</p> <p>1.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</p> <p>1.5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</p> <p>1.6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>1.7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</p> <p>1.8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</p> <p>1.9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</p> <p>1.10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</p> <p>1.11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</p> <p>1.12. Mechanizm „Split tunneling” dla połączeń Client-to-Site.</p> <p>2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</p>

8.	Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9.	Funkcje SD-WAN	<ol style="list-style-type: none"> 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
10.	Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane,

		<p>uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <ol style="list-style-type: none"> 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
12.	Ochrona przed atakami	<ol style="list-style-type: none"> 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12.	Kontrola aplikacji	<ol style="list-style-type: none"> 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

		<ol style="list-style-type: none"> 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13.	Kontrola www	<ol style="list-style-type: none"> 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

14.	Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <ol style="list-style-type: none"> 1.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 1.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 1.3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
15.	Zarządzanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

		9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16.	Logowanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17.	Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).
18.	Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:</p> <p>Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.</p>
19.	Gwarancja	System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

8.2.2. UTM wariant 2 – sztuk 4

Lp.	Parametr lub warunek	Wymagania
1.	Wymagania ogólne	<ol style="list-style-type: none"> System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: <ol style="list-style-type: none"> 4.1. Firewall. 4.2. Ochrony w warstwie aplikacji. 4.3. Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ol style="list-style-type: none"> 1.1. 4 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.

4.	Parametry wydajnościowe	<ol style="list-style-type: none"> 1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 50 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
5.	Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> 1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

		<p>11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.</p> <p>12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</p>
6.	Polityki, Firewall	<p>1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <p>2.1. Translację jeden do jeden oraz jeden do wielu.</p> <p>2.2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</p> <p>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.</p> <p>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <p>7.1. Amazon Web Services (AWS).</p> <p>7.2. Microsoft Azure.</p> <p>7.3. Cisco ACI.</p> <p>7.4. Google Cloud Platform (GCP).</p> <p>7.5. OpenStack.</p> <p>7.6. VMware NSX.</p> <p>7.7. Kubernetes.</p>
7.	Połączenia VPN	<p>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <p>1.1. Wsparcie dla IKE v1 oraz v2.</p> <p>1.2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</p>

		<ul style="list-style-type: none"> 1.3. Obsługa protokołu Diffie-Hellman grup 19, 20. 1.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 1.5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 1.6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 1.7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 1.8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. 1.9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. 1.10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 1.11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 1.12. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8.	Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ul style="list-style-type: none"> 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9.	Funkcje SD-WAN	<ul style="list-style-type: none"> 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

10.	Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
12.	Ochrona przed atakami	<ol style="list-style-type: none"> 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.

		<ol style="list-style-type: none"> 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12.	Kontrola aplikacji	<ol style="list-style-type: none"> 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13.	Kontrola www	<ol style="list-style-type: none"> 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

		<ol style="list-style-type: none"> 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
14.	Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <ol style="list-style-type: none"> 1.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 1.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 1.3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
15.	Zarządzanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

		<ol style="list-style-type: none"> 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16.	Logowanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17.	Testy wydajnościowe	<p>Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie</p>

	oraz funkcjonalne	wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.
18.	Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
19.	Gwarancja	System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

8.3. Tokeny do uwierzytelniania dwuskładnikowego 30 sztuk

Lp	Parametr lub warunek	Wymagania
1.	Wymagania ogólne	<ol style="list-style-type: none"> 1. Do realizacji połączeń zdalnych VPN i VPN IPSEC. 2. Token tego samego producenta co oferowane urządzenia UTM. 3. Urządzenie do działania może wymagać baterii. 4. Urządzenie nie może być typem pamięci/dysków pendrive, czyli posiadać miejsce do przechowywania danych: pliki, katalogi. 5. Urządzenie nie może wymagać instalacji oprogramowania klienckiego. 6. Urządzenie nie może wymagać podłączenia do komputera. 7. Klasa szczelności IP67.
2.	Szyfrowanie / bezpieczeństwo	<ol style="list-style-type: none"> 1. SHA-1, SHA-256, 128-bit AES, 192-bit AES, 256-bit AES 2. Zgodność z OATH, TOTP. 3. Generowanie jednorazowych haseł.
3.	Gwarancja	12 miesięcy

8.4. Rozwiązanie do monitorowania, raportowania i analizy ruchu sieciowego online

Lp	Parametr lub warunek	Wymagania
----	----------------------	-----------

1.	Wymagania ogólne	<ol style="list-style-type: none"> 1. Dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. 2. System ma obejmować starostwo i jednostki organizacyjne biorące udział w projekcie.
2.	Parametry wydajnościowe	<ol style="list-style-type: none"> 1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 12 systemów (urządzeń – starostwo + jednostki organizacyjne). 3. Przestrzeń dyskowa umożliwiająca przechowywanie logów przez okres minimum jednego miesiąca z funkcjonalnością ich archiwizowania.
3.	Funkcjonalność logowanie	<p>W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej funkcje:</p> <ol style="list-style-type: none"> 1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: <ol style="list-style-type: none"> 3.1. Listę najczęściej wykrywanych ataków. 3.2. Listę najbardziej aktywnych użytkowników. 3.3. Listę najczęściej wykorzystywanych aplikacji. 3.4. Listę najczęściej odwiedzanych stron www. 3.5. Listę krajów do których nawiązywane są połączenia. 3.6. Listę najczęściej wykorzystywanych polityk Firewall. 3.7. Informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

4.	Funkcjonalność raportowanie	<p>W zakresie raportowania system musi zapewniać:</p> <ol style="list-style-type: none"> 1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
5.	Funkcjonalność korelacja logów	<p>W zakresie korelacji zdarzeń system musi zapewniać:</p> <ol style="list-style-type: none"> 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: <ol style="list-style-type: none"> 3.1. Malware. 3.2. Aplikacje sieciowe. 3.3. Email. 3.4. IPS. 3.5. Traffic. 3.6. Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. 4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
6.	Funkcjonalność zarządzanie	<ol style="list-style-type: none"> 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. <ol style="list-style-type: none"> 1.1. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
7.	Serwis i licencja	<ol style="list-style-type: none"> 1. Licencja 12 miesięcy licząc od daty wdrożenia

		<p>2. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.</p> <p>3. W ramach wsparcie będą świadczone dodatkowe usługi zgodnie z zapisami w punkcie 11.1 Świadczenie usług doradczych/eksperckich</p>
--	--	---

8.5. Macierz dyskowa

Lp		Parametr lub warunek	Wymagania
1.		Wymagania ogólne	<p>1. System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19" z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii.</p> <p>2. Macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach.</p> <p>3. Macierz musi obsługiwać min. 90 dysków wykonanych w technologii hot-plug.</p> <p>4. Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych.</p>
2.		Pojemność macierzy	13 szt. dysków 1,9TB SSD-SAS
3.		Kontrolery	<p>1. Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami.</p> <p>2. Każdy z kontrolerów macierzy musi posiadać po minimum 8GB pamięci podręcznej Cache.</p> <p>3. W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.</p> <p>4. Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 4TB poprzez instalację dodatkowych modułów pamięci w</p>

			<p>kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD.</p> <ol style="list-style-type: none"> 5. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. 6. Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online wolumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. 7. Każdy z kontrolerów RAID powinien posiadać dedykowany interfejs RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. 8. Kontrolery macierzy muszą obsługiwać do 84 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów. 9. Oferowana macierz musi mieć wyprowadzone 4 porty FC 16Gbps/iSCSI 10Gbps (wszystkie porty obsadzone modułami 10G/16G LC MMF) do dołączenia serwerów bezpośrednio lub do sieci SAN na każdy kontroler RAID. 10. Macierz musi umożliwiać wymianę zainstalowanych portów do transmisji danych na porty: <ol style="list-style-type: none"> 10.1. SAS 12 Gbps 10.2. FC 32 Gbps 10.3. iSCSI 25Gbps 10.4. iSCSI 10Gbps Base-T
4.		Poziomy RAID	<ol style="list-style-type: none"> 1. Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: <ol style="list-style-type: none"> 1.1. Raid-1 1.2. Raid-10 1.3. Raid-3 1.4. Raid-5 1.5. Raid-6 2. Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy. 3. Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być

			<p>przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.</p> <p>4. Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi.</p>
5.		Dyski	<p>1. Oferowana macierz musi wspierać dyski hot-plug:</p> <p>1.1. dyski elektroniczne SSD</p> <p>1.2. mechaniczne HDD z interfejsem SAS12Gb/s</p> <p>1.3. dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,</p> <p>2. Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5" i 3,5" zainstalowanych w dowolnym module rozwiązania.</p> <p>3. Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug.</p> <p>4. Macierz musi obsługiwać 90 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami.</p> <p>5. Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD.</p> <p>6. Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy).</p> <p>7. W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego, wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess).</p> <p>8. Macierz musi pozwalać na zaszyfrowanie danych na dedykowanych do tego dyskach kluczem AES256-bit zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST).</p>

			<p>9. Macierz musi posiadać możliwość skasowania wszystkich danych z dysku FDE celem bezpiecznego ponownego użycia w innym środowisku (Secure Erase).</p>
6.		Opcje programowe	<p>1. Macierz musi być wyposażona w system kopii migawkowych umożliwiające wykonanie 128 kopii migawkowych z opcją rozbudowy do 512.</p> <p>2. Macierz musi umożliwiać zdefiniowanie min. 500 woluminów (LUN).</p> <p>3. Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 128 ścieżek logicznych.</p> <p>4. Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączenia macierzy oraz bez konieczności wyłączenia ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów.</p> <p>5. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.</p> <p>6. Macierz musi posiadać wsparcie dla systemów operacyjnych:</p> <p>6.1. Microsoft Windows Server 2019, 2022, 2025</p> <p>6.2. SuSE Linux Enterprise Server 15, 12</p> <p>6.3. Red Hat Linux Enterprise Server 9, 8, 7</p> <p>6.4. Vmware vSphere 7.0, 8.0;</p> <p>7. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.</p> <p>8. Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie asynchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji</p>

			<p>danych. nie jest wymagane dostarczenie tej funkcjonalności - możliwość rozbudowy.</p> <p>9. Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych).</p> <p>10. Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin.</p>
7.		Zarządzanie	<p>1. Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej.</p> <p>2. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.</p> <p>3. Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (minimum Microsoft Edge, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.</p> <p>4. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.</p> <p>5. Wraz z systemem musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:</p> <p>5.1. wydajności i opóźnień na wolumenach.</p> <p>5.2. wydajności I/Ops, MB/s.</p> <p>5.3. trafności w cache.</p> <p>6. Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.</p> <p>7. Macierz musi posiadać oprogramowanie pozwalające na integrację Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter</p>

			8. Macierz musi posiadać wsparcie dla VMware vSphere Storage APIs Array Integration (VAAI)
8.		Gwarancja i serwis	<ol style="list-style-type: none"> 1. Całe rozwiązanie musi być objęte 12 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem reakcji końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. 2. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. 3. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. 4. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych. 5. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia. 6. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje.

8.6. Serwery

8.6.1. Wariant 1 – 2 sztuki

Dostawa serwerów wraz z systemem operacyjnym Microsoft Windows Server Standard 2025 lub równoważnego, spełniającego kryteria oceny równoważności wskazane w pkt. 11.6.3. **Cztery licencje**, instalacja i konfiguracja serwerów w ilości ośmiu maszyn wirtualnych. Migracja Active Directory na dostarczony serwer i konfiguracja zapasowego kontrolera domeny.

Dostawa licencji Microsoft Windows Server Standard 2025 lub równoważne – licencje na każdy serwer bez ograniczeń czasowych. Zakup licencji oprogramowania jest uzupełnieniem stanu licencyjnego oprogramowania eksploatowanego w środowisku serwerowym: Windows Server 2022.

Lp	Parametr lub warunek	Wymagania
1.	Obudowa	<ol style="list-style-type: none"> 1. Typu RACK, wysokość nie więcej niż 1U. 2. Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable. 3. Możliwość zainstalowania 10 dysków twardych hot plug 2,5" SATA/SAS 4. Możliwość rozbudowy o panel diagnostyczny z wyświetlaczem LCD umożliwiającym detekcję usterek umożliwiającą wyświetlenie następujących informacji: <ol style="list-style-type: none"> 4.1. aktywne ostrzeżenia, 4.2. status serwera, 4.3. typ oraz model serwera, numer seryjny, 4.4. wersje oprogramowania UEFI oraz modułu zarządzania, 4.5. informacje nt modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS, 4.6. dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii, 4.7. aktywne sesje połączeniowe do interfejsu zarządzania. 5. Zainstalowane 2 szt. dysków SSD SATA M.2 480GB, dyski skonfigurowane w RAID-1 podłączone do sprzętowego kontrolera RAID.
2.	Płyta główna	<ol style="list-style-type: none"> 1. Dwuprocesorowa. 2. Wyprodukowana i zaprojektowana przez producenta serwera. 3. Możliwość instalacji procesorów 60-rdzeniowych. 4. Moduł TPM 2.0. 5. 2 złącza PCI Express x16 generacji 4. 6. Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH. 7. 32 gniazda pamięci RAM. 8. Obsługa 8 TB pamięci operacyjnej RAM. 9. Wsparcie dla technologii: <ol style="list-style-type: none"> 9.1. Bounded Fault, 9.2. SDDC, 9.3. ECC, 9.4. Memory Mirroring, 9.5. ADDDC. 10. Wewnętrzny slot na kartę Micro SD.

3.	Procesory	<ol style="list-style-type: none"> 1. Jeden procesor 16-rdzeniowy, architektura x86_64. 2. Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 480 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera.
4.	Pamięć RAM	<ol style="list-style-type: none"> 1. 128GB pamięci RAM. 2. Registered 4800MT/s. 3. Pamięci obsadzone w sposób gwarantujący najwyższą możliwą wydajność.
5.	Kontroler LAN	<ol style="list-style-type: none"> 1. Interfejsy LAN, nie zajmujące slotów PCI Express (OCP). 2. 2x 10Gbit Base-T. 3. Możliwość uzyskania 2 interfejsów 100Gbit QSFP56 bez konieczności instalacji kart w slotach PCIe. 4. 1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB.
6.	Kontrolery I/O	<ol style="list-style-type: none"> 1. Kontroler FC 2x 16Gb MMF LC
7.	Porty	<ol style="list-style-type: none"> 1. Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu. 2. 3 porty USB dostępne z tyłu serwera w tym dwa w wersji USB 3.2. 3. 2 porty USB na panelu przednim w tym jeden w wersji USB 3.2; 4. Jeden z frontowych portów USB musi posiadać możliwość zarządzania serwerem. 5. Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera. 6. Opcjonalny port serial. 7. Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakiegokolwiek slot PCI Express i/lub USB serwera.
8.	Zasilanie, chłodzenie	<ol style="list-style-type: none"> 1. Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1100W. 2. Redundantne wentylatory hotplug dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni Celsjusza.

9.	Bezpieczeństwo	<ol style="list-style-type: none"> 1. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji. 2. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. 3. Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem. 4. Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych. 5. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. 6. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 7. Możliwość ustawienia hasła włączania serwera. 8. Możliwość ustawienia hasła administratora 9. Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.
10.	Zarządzanie	<ol style="list-style-type: none"> 1. Wymaga się aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu. 2. Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych. 3. Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera. 4. Funkcjonalność kontrolera zdalnego zarządzania: <ol style="list-style-type: none"> 4.1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna, 4.2. Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja,

		<p>4.3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów,</p> <p>4.4. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń,</p> <p>4.5. Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3,</p> <p>4.6. Update systemowego firmware,</p> <p>4.7. Monitoring i możliwość ograniczenia poboru prądu,</p> <p>4.8. Zdalne włączanie/wyłączanie/restart,</p> <p>4.9. Zapis video zdalnych sesji,</p> <p>4.10. Podmontowanie lokalnych mediów,</p> <p>4.11. Przekierowanie konsoli szeregowej przez IPMI,</p> <p>4.12. Zrzut ekranu w momencie zawieszenia systemu,</p> <p>4.13. Możliwość przejęcia zdalnego ekranu ,</p> <p>4.14. Możliwość zdalnej instalacji systemu operacyjnego,</p> <p>4.15. Alerty Syslog,</p> <p>4.16. Przekierowanie konsoli szeregowej, przez SSH,</p> <p>4.17. Wsparcie dla dynamic DNS</p> <p>4.18. Wyświetlanie danych aktualnych i historycznych dla zużycia energii oraz temperatury serwera,</p> <p>4.19. Wirtualna konsola z dostępem do myszy, klawiatury,</p> <p>4.20. Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy ActiveX (musi działać w oparciu o HTML5),</p> <p>4.21. Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS,</p> <p>4.22. Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę,</p> <p>4.23. wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API.</p> <p>5. Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.</p> <p>6. Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję</p>
--	--	--

		<p>RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.</p> <p>7. Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.</p> <p>8. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.</p> <p>9. Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 10.</p> <p>10. Możliwość opcjonalnej rozbudowy funkcjonalności zarządzania infrastrukturą DC poprzez zakup oprogramowania do zarządzania, spełniającego poniższe wymagania:</p> <p>10.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych,</p> <p>10.2. Integracja z Active Directory,</p> <p>10.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym,</p> <p>10.4. Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP,</p> <p>10.5. Szczegółowy opis wykrytych systemów oraz ich komponentów,</p> <p>10.6. Możliwość eksportu danych min do formatu CSV,</p> <p>10.7. Grupowanie urządzeń w oparciu o kryteria użytkownika,</p> <p>10.8. Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK,</p> <p>10.9. Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS,</p> <p>10.10. Szybki podgląd stanu środowiska,</p> <p>10.11. Podsumowanie stanu dla każdego urządzenia,</p> <p>10.12. Szczegółowy status urządzenia/elementu/komponentu</p> <p>10.13. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń,</p> <p>10.14. Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych,</p> <p>10.15. Możliwość przejęcia zdalnego pulpitu,</p> <p>10.16. Możliwość zamontowania wirtualnego napędu,</p>
--	--	--

		<p>10.17. Kreator umożliwiający dostosowanie akcji dla wybranych alertów,</p> <p>10.18. Przesyłanie alertów „as-is” do innych konsol firm trzecich,</p> <p>10.19. Możliwość definiowania ról administratorów,</p> <p>10.20. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów,</p> <p>10.21. Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta,</p> <p>10.22. Możliwość definiowania polityk aktualizacji (konkretne wersje firmware),</p> <p>10.23. Automatyczna polityka aktualizacji „Najnowsze dostępne”,</p> <p>10.24. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym,</p> <p>10.25. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów,</p> <p>10.26. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta,</p> <p>10.27. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji,</p> <p>10.28. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile,</p> <p>10.29. Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI,</p> <p>10.30. Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach,</p> <p>10.31. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</p>
11.	Certyfikowane systemy operacyjne	<p>1. Microsoft Windows Server 2025, 2022.</p> <p>2. VMWare ESXi 8.0, 7.0.</p> <p>3. Suse Linux Enterprise Server 15.</p> <p>4. Red Hat Enterprise Linux 9.x, 8.x.</p> <p>5. Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS.</p>

12.	Gwarancja	<ol style="list-style-type: none"> 1. 12 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowanym czasem naprawy w 24h. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde/pamięć masowa nie podlegają zwrotowi organizacji serwisowej. 2. Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu. 3. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. 4. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z wyżej opisanym SLA (podać koszt na dzień składania oferty).
13.	Dokumentacja i inne	<ol style="list-style-type: none"> 1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta. 2. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta. 3. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki. 4. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.
Panel diagnostyczny - 1 sztuka dla dwóch oferowanych serwerów		
Lp.	Wymagana funkcjonalność.	
1.	<ol style="list-style-type: none"> 1. Panel diagnostyczny z wyświetlaczem LCD umożliwiającym detekcję usterek, wyświetlającym następujące informacje: <ol style="list-style-type: none"> 1.1. aktywne ostrzeżenia. 1.2. status serwera. 1.3. typ oraz model serwera, numer seryjny. 1.4. wersje oprogramowania UEFI oraz modułu zarządzania. 1.5. informacje nt. modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS. 1.6. dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii. 	

	1.7. aktywne sesje połączeniowe do interfejsu zarządzania.
2.	Czas gwarancji tożsamy z czasem gwarancji serwer.

8.6.2. Wariant 2 – 1 sztuka

Dostawa serwera wraz z systemem operacyjnym Microsoft Windows Server Standard 2025 lub równoważnego, spełniającego kryteria oceny równoważności wskazane w pkt. 11.5.3.

Jedna licencja, instalacja i konfiguracja serwera – dwie maszyny wirtualne. Konfiguracja Active Directory na dostarczonym serwerze.

Dostawa licencji Microsoft Windows Server Standard 2025 lub równoważne – licencje na serwer bez ograniczeń czasowych.

Zamawiający wymaga dostarczenia Oprogramowania: Microsoft Windows Server Standard 2025, lub równoważnego, spełniającego kryteria oceny równoważności wskazane w pkt.

4.1.3

Lp	Parametr lub warunek	Wymagania
1.	Obudowa	<ol style="list-style-type: none"> 1. Typu Tower, opcjonalnie możliwość zamontowania w szafie rack za pomocą dedykowanego przez producenta zestawu montażowego. 2. Możliwość zainstalowania 8 dysków twardych hot plug 2,5”. 3. Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych. 4. Możliwość zainstalowania czujnika otwarcia obudowy zintegrowanego z modułem zarządzającym serwerem. 5. Zainstalowane 3 szt. dysków SAS 10000 obr./min.2,4TB Hot-Plug.
2.	Płyta główna	<ol style="list-style-type: none"> 1. Wyprodukowana i zaprojektowana przez producenta serwera. 2. Możliwość instalacji procesorów 8-rdzeniowych. 3. Zainstalowany moduł TPM 2.0. 4. Złącza PCI Express. 5. 1 interfejs PCIe 5.0 o prędkości x16. 6. 3 interfejsy PCIe 4.0 o prędkości x4. 7. 4 gniazda pamięci RAM. 8. Obsługa minimum 128 GB pamięci RAM DDR5 ECC. 9. Możliwość instalacji 2 dysków M.2 skonfigurowanych w RAID-1 na płycie głównej lub dedykowanej karcie PCI Express, dyski nie mogą zajmować klatek dla dysków hot-plug.
3.	Procesor	<ol style="list-style-type: none"> 1. Jeden procesor 8-rdzeniowy, architektura x86_64.

		2. Osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 96 pkt. Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera.
4.	Pamięć RAM	1. 32 GB pamięci RAM. 2. Pamięci obsadzone w trybie dwukanałowym.
5.	Kontroler LAN	1. Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express. 2. 2x 1Gbit Base-T z obsługą. 2.1. Teaming, 2.2. VLAN (IEEE 802.1Q), 2.3. IEEE 802.3ad, 2.4. PXE, 2.5. WoL, 2.6. Jumbo Frames, 2.7. IOV dla Vmware i Microsoft. 3. 1x 1Gbit Base-T port dedykowany do zarządzania OOB;
6.	Kontrolery I/O	1. Kontroler SAS RAID dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10,5 oraz możliwość pracy w trybie JBOD.
7.	Porty	1. Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera. 2. 4 porty USB dostępne z tyłu serwera w tym trzy w wersji USB 3.2. 3. 1 port USB 3.0 wewnętrzny. 4. 2 porty USB na panelu przednim w tym jeden w wersji USB 3.2. 5. Jeden z frontowych portów USB musi posiadać możliwość zarządzania serwerem. 6. 1 port serial. 7. Ilość dostępnych złącz USB/serial nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakiegokolwiek slot PCI Express i/lub USB serwera.
8.	Zasilanie, chłodzenie	Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 800W.
9.	Zarządzanie	1. Wymaga się aby serwer posiadał diody sygnalizującą awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.

		<ol style="list-style-type: none"> 2. Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych. 3. Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera. 4. Funkcjonalność kontrolera zdalnego zarządzania: <ol style="list-style-type: none"> 4.1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna, 4.2. Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja, 4.3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów, 4.4. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń, 4.5. Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 4.6. Update systemowego firmware, 4.7. Monitoring i możliwość ograniczenia poboru prądu, 4.8. Zdalne włączanie/wyłączanie/restart, 4.9. Zapis video zdalnych sesji, 4.10. Podmontowanie lokalnych mediów z wykorzystaniem Java client, 4.11. Przekierowanie konsoli szeregowej przez IPMI, 4.12. Zrzut ekranu w momencie zawieszenia systemu, 4.13. Możliwość przejęcia zdalnego ekranu, 4.14. Możliwość zdalnej instalacji systemu operacyjnego, 4.15. Alerty Syslog, 4.16. Przekierowanie konsoli szeregowej przez SSH, 4.17. Wsparcie dla dynamic DNS, 4.18. Wyświetlanie danych aktualnych i historycznych dla zużycia energii oraz temperatury serwera, 4.19. Wirtualna konsola z dostępem do myszy, klawiatury,
--	--	---

		<p>4.20. Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy ActiveX (musi działać w oparciu o HTML5),</p> <p>4.21. Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS,</p> <p>4.22. Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę,</p> <p>4.23. wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API,</p> <p>4.24. Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego,</p> <p>4.25. Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.</p> <p>4.26. Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.</p> <p>4.27. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.</p> <p>4.28. Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.</p> <p>4.29. Możliwość opcjonalnej rozbudowy funkcjonalności zarządzania infrastrukturą DC poprzez zakup oprogramowania do zarządzania, spełniającego poniższe wymagania:</p> <p>4.29.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</p> <p>4.29.2. Integracja z Active Directory</p> <p>4.29.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym</p> <p>4.29.4. Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP</p>
--	--	---

		<p>4.29.5. Szczegółowy opis wykrytych systemów oraz ich komponentów</p> <p>4.29.6. Możliwość eksportu danych min do formatu CSV</p> <p>4.29.7. Grupowanie urządzeń w oparciu o kryteria użytkownika</p> <p>4.29.8. Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK</p> <p>4.29.9. Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS</p> <p>4.29.10. Szybki podgląd stanu środowiska</p> <p>4.29.11. Podsumowanie stanu dla każdego urządzenia</p> <p>4.29.12. Szczegółowy status urządzenia/elementu/komponentu</p> <p>4.29.13. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</p> <p>4.29.14. Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych</p> <p>4.29.15. Możliwość przejęcia zdalnego pulpitu</p> <p>4.29.16. Możliwość zamontowania wirtualnego napędu</p> <p>4.29.17. Kreator umożliwiający dostosowanie akcji dla wybranych alertów</p> <p>4.29.18. Przesyłanie alertów „as-is” do innych konsol firm trzecich</p> <p>4.29.19. Możliwość definiowania ról administratorów</p> <p>4.29.20. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</p> <p>4.29.21. Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta</p> <p>4.29.22. Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)</p> <p>4.29.23. Automatyczna polityka aktualizacji „Najnowsze dostępne”</p> <p>4.29.24. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym</p>
--	--	---

		<p>4.29.25. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</p> <p>4.29.26. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta</p> <p>4.29.27. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.</p> <p>4.29.28. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile</p> <p>4.29.29. Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI</p> <p>4.29.30. Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach</p> <p>4.29.31. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</p>
10.	Certyfikowane systemy operacyjne	<ol style="list-style-type: none"> 1. Microsoft Windows Server 2025, 2022. 2. VMWare vSphere 8.0. 3. Suse Linux Enterprise Server 15. 4. Red Hat Enterprise Linux 9, 8. 5. Ubuntu 24.04.
11.	Gwarancja	<ol style="list-style-type: none"> 1. 12 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowanym czasem naprawy w 24h. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej. 2. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu. 3. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. 4. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w 24h od zgłoszenia usterki (podać koszt na dzień składania oferty).

12.	Dokumentacja i inne	<ol style="list-style-type: none"> 1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta. 2. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta. 3. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki. 4. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. 5. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera 6. Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 80 %. 7. Zgodność z normami: NIST SP 800-147B, RoHS oraz CE.
-----	---------------------	--

8.6.3. Kryteria stosowane w celu oceny równoważności Microsoft Windows Server Standard 2025

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2025 Standard, Zamawiający wymaga dostarczenia licencji dla serwerów, oraz instalacji i migracji obecnego środowiska AD i systemów dziedzicznych. Zamawiający wymaga aby produkt równoważny spełniał niżej wymienione wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Obsługa minimum 1 TB pamięci RAM.
2. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 1 procesor oraz 16 rdzeni.
3. Możliwość obsługi minimum 70 użytkowników.
4. Współpraca z procesorami o architekturze x86-64.
5. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
6. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory.
7. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.

8. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
9. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Zawarta możliwość uruchomienia roli serwera DNS.
11. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).
12. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
13. Zawarta możliwość uruchomienia roli serwera Windows Server Update Services.
14. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
15. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
16. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
17. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
18. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
19. Interfejs i pomoc w języku polskim lub angielskim.
20. Licencja umożliwiająca na korzystanie z dwóch środowisk OSE lub maszyn wirtualnych. Funkcjonalność pełnienia rolę zapasowego kontrolera domeny.
21. Pełna kompatybilność z dostarczonymi rozwiązaniami systemowymi w ramach projektu Cyberbezpieczny Samorząd.

8.7. Dostawa i uruchomienie zasilacza bezprzerwowego (UPS) – 1 sztuka

Lp	Parametr lub warunek	Wymagania
1.	Technologia	VFI (true on-line, podwójne przetwarzanie energii).
2.	Moc znamionowa	6kVA / 6kW
3.	Wyjściowy współczynnik mocy (PF)	1
4.	Wejściowy współczynnik mocy	$\cos\phi \geq 0,99$
5.	Napięcie wejściowe	208/220/230/240 VAC + N
6.	Minimalna sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	$\geq 94\%$

7.	Minimalna sprawność w trybie ECO	≥98,0% dla 100% obciążenia.
8.	Możliwość rozbudowy mocy w okresie eksploatacji (praca równoległa)	do 4 jednostek.
9.	Napięcie wyjściowe	208/220/230/240 VAC
10.	Częstotliwość wyjściowa	50/60Hz (programowalna)
11.	Panel lcd	Wymagane
12.	Stabilizacja napięcia wyjściowego	±1%
13.	Zniekształcenia napięcia wyjściowego	1. ≤ 1% z obciążeniem liniowym 2. ≤ 4% z obciążeniem nieliniowym
14.	Współczynnik szczytu przy obciążeniu znamionowym	3:1
15.	Przeciążenie inwertera	1. 102%-110% przez 10 minut 2. 110% -125% przez 1 minutę 3. 125% -150% przez 30 sekund
16.	Złącze interfejsów	USB
17.	Interfejs EPO (do wyłącznika ppoż.)	Wymagane
18.	Wbudowana karta sieciowa SNMP	Wymagane, jedna karta pozwalająca na komunikację poprzez protokoły: SNMP, Modbus TCP/IP, Modbus RTU
19.	Możliwość pracy jako konwerter częstotliwości	Wymagane
20.	Baterie	Szczelne, bezobsługowe, w technologii AGM o żywotności projektowanej minimum 5 lat w temperaturze 25 stopni Celsjusza.
21.	Możliwość zainstalowania akumulatorów wewnątrz modułu zasilacza UPS (bez konieczności użycia modułu baterijnego)	Wymagane.

22.	Możliwość regulacji stosu bateryjnego	Tak, 16-20 sztuk
23.	Inteligentne zarządzanie baterią akumulatorów, zwiększające żywotnością baterii	Wymagane.
24.	Test baterijny	Wymagane.
25.	Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane.
26.	Rejestr zdarzeń	Wymagane.
27.	Spełnienie wszystkich obowiązujących norm bezpieczeństwa potwierdzone deklaracją zgodności CE	Wymagane.
28.	Obudowa	1. Maksimum 4U 2. Zestaw szyn montażowych do szafy RACK
29.	Gwarancja	12 miesięcy

8.8. Przełączniki sieciowe

Oferowane urządzenia muszą zapewniać pełną zgodność i kompatybilność z posiadanymi przełącznikami sieciowymi firmy D-Link modele: DSG-1510-28X i DSG-1510-52X.

8.8.1. Przełącznik sieciowy wariant 1 - 2 sztuki.

Lp.	Parametr lub warunek	Wymagania
1.	Charakterystyka sprzętowa	1. 48 x 1000Base-T IEEE 802.3ab. 2. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). 3. Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. 4. 4 x SFP+ IEEE 802.3ae/802.3ak. Porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z. 5. Konsola szeregową RS-232.

		6. Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. 7. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie. 8. Zasilanie AC 230V. 9. Pojemność przełączania nie mniej, niż 176 Gb/s. Wydajność przełączania nie mniej niż 130 Mp/s. 10. Architektura nieblokującą (wire-speed). 11. Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych. 12. Ilość RAM nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. 13. Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B. 14. Bufor pakietów nie mniej, niż 3 MB. 15. MTBF > 410000 godzin. 16. Obudowa RACK 1U lub 2 U - urządzenia musi być dostarczone z wszystkimi komponentami do instalacji w szafie rackn19".
2.	Funkcjonalności warstwy 2	1. IGMP Snooping v3 - obsługa nie mniej, niż 510 grup multicast w tym co najmniej 256 grup statycznych. 2. MLD Snooping v2 - obsługa nie mniej, niż 31 grup multicast w tym co najmniej 31 grup statycznych. 3. IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN. 4. Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP. 5. Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP. 6. LLDP (802.1AB) oraz LLDP-MED. 7. ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni. 8. DHCP Relay w tym opcji 60 i 61 oraz opcji 82, DHCP Local Relay + opcja 82. DHCP Relay dla IPv6. 9. Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu.
3.	Obsługa sieci VLAN	1. 802.1Q VLAN, co najmniej 4094, 802.1v GVRP. 2. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. 3. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN.

		4. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
4.	Funkcjonalności warstwy 3	<ol style="list-style-type: none"> 1. Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. 2. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. 3. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. 4. Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. 5. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. 6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. 7. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. 8. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). 9. Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. 10. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
5.	Quality of Service	<ol style="list-style-type: none"> 1. Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. 2. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. 3. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.

		4. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
6.	Filtrowanie ruchu	<ol style="list-style-type: none"> 1. Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. 2. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
7.	Funkcje bezpieczeństwa	<ol style="list-style-type: none"> 1. Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 120 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. 2. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. 3. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. 4. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. 5. Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta. 6. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. 7. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. 8. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.

		<p>9. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.</p> <p>10. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.).</p> <p>11. Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.</p> <p>12. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany.</p> <p>13. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci.</p> <p>14. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU.</p> <p>15. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service.</p> <p>16. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.</p> <p>17. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.</p>
8.	Zarządzanie	<p>1. Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+.</p> <p>2. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP.</p> <p>3. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia.</p>

		<ol style="list-style-type: none"> 4. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednocześnie) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. 5. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. 6. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. 7. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. 8. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. 9. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. 10. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. 11. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. 12. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. 13. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. 14. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. 15. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego. 16. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC.
--	--	--

		<p>17. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.</p> <p>18. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.</p> <p>19. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC.</p> <p>20. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.</p> <p>21. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware.</p> <p>22. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.</p> <p>23. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).</p> <p>24. Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.</p>
9.	Pozostałe	<p>1. Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.</p> <p>2. Gwarancja 12 miesięcy.</p>

8.8.2. Przełącznik sieciowy wariant 2 - 1 sztuka

Lp.	Parametr lub warunek	Wymagania
1.	Charakterystyka sprzętowa	<p>1. 8 x 10GBase-T IEEE 802.3ae</p> <p>2. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X).</p> <p>3. Musi istnieć możliwość zmiany prędkości i duplexu każdego portu i wyłączenia trybu FlowControl dla każdego portu.</p> <p>4. Porty 10GBase-T muszą wspierać standard NBase-T (2.5Gb/s, 5Gb/s).</p>

		<ul style="list-style-type: none"> 5. 2 x SFP+ IEEE 802.3ae/802.3ak. Porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z; 6. Konsola szeregową RS-232. 7. Zasilanie AC 230V. 8. Pojemność przełączania nie mniej, niż 200 Gb/s. Wydajność przełączania nie mniej niż 148 Mp/s. 9. Architektura nieblokującą (wire-speed). 10. Pojemność tablicy MAC nie mniej, niż 32K. Możliwość wprowadzenia co najmniej 120 wpisów statycznych. 11. Ilość RAM nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 128 MB. 12. Obsługa ramek Jumbo o rozmiarze co najmniej 10240 B. 13. Bufor pakietów nie mniej, niż 2 MB. 14. Temperatura pracy w zakresie co najmniej od -5C do 50 stopni Celsjusza. 15. MTBF > 570000 godzin. 16. Obudowa RACK 1U lub 2 U - urządzenia musi być dostarczone z wszystkimi komponentami do instalacji w szafie rackn19”.
2.	Funkcjonalności warstwy 2	<ul style="list-style-type: none"> 1. IGMP Snooping v2, 3 (awareness) - obsługa nie mniej, niż 380 grup multicast w tym co najmniej 384 grup statycznych. 2. MLD Snooping v1, 2 (awareness) - obsługa nie mniej, niż 380 grup multicast w tym co najmniej 128 grup statycznych. 3. IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN. 4. Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP. 5. Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 8 grup na urządzenie z obsługą LACP. 6. LLDP (802.1AB) oraz LLDP-MED. 7. ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni. 8. Port monitoring/mirroring/span oraz monitorowania ruchu na port w innym przełączniku (RSPAN).
3.	Obsługa sieci VLAN	<ul style="list-style-type: none"> 1. 802.1Q VLAN, co najmniej 4094 GVRP. 2. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. 3. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
4.	Funkcjonalności warstwy 3	<ul style="list-style-type: none"> 1. Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 8 takich interfejsów.

		<ol style="list-style-type: none"> Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 8 takich interfejsów. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,7K wpisów oraz umożliwiać wprowadzenie co najmniej 768 wpisów statycznych. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 760 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 384 takich tras dla IPv6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 64 takich tras dla IPv6. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 60 tras). Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
5.	Quality of Service	<ol style="list-style-type: none"> Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, WRR. Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s oraz umożliwiać gwarantowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
6.	Filtrowanie ruchu	<ol style="list-style-type: none"> Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, pole EtherType, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.

7.	Funkcje bezpieczeństwa	<ol style="list-style-type: none"> 1. Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 6650 takich adresów MAC na pojedynczym porcie fizycznym. 2. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. 3. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. 4. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN. 5. Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników. 6. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. 7. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). 8. Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. 9. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. 10. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 1pps), Multicast (z krokiem minimalnym co najwyżej 1pps), Broadcast (z krokiem minimalnym co najwyżej 1pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.
----	------------------------	--

		11. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
8.	Zarządzanie	<ol style="list-style-type: none"> 1. Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. 2. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. 3. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. 4. Urządzenie powinno być również zarządzane na bazie profili z poziomu centralnej aplikacji zarządzającej. 5. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. 6. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. 7. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON. 8. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. 9. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. 10. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. 11. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. 12. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.

		<p>13. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego oraz wspierać traceroute dla IPv6.</p> <p>14. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6.</p> <p>15. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.</p> <p>16. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.</p> <p>17. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji.</p> <p>18. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).</p> <p>19. Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.</p>
9.	Pozostałe	<p>1. Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.</p> <p>2. Gwarancja 12 miesięcy.</p>

8.8.3. Przełącznik sieciowy wariant 3 - 5 sztuk

Lp.	Parametr lub warunek	Wymagania
1.	Charakterystyka sprzętowa	<p>1. 24 x 1000Base-T IEEE 802.3ab/802.3at</p> <p>2. 2 x SFP IEEE 802.3z z możliwością instalacji modułów 1000Base-SX/LX/LH/ZX</p> <p>3. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X).</p> <p>4. Musi istnieć możliwość zmiany prędkości i duplexu każdego portu i wyłączenia trybu FlowControl dla każdego portu.</p> <p>5. 2 x SFP+ IEEE 802.3ae/802.3ak. Porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z;</p> <p>6. Uruchamianie zasilania PoE na portach sterowane kalendarzem.</p>

		<p>7. Aktywne monitorowanie przyłączonych urządzeń PoE z możliwością ponownego uruchomienia podłączonych urządzeń przez wyłączenie i włączenie zasilania.</p> <p>8. Konsola szeregową RS-232.</p> <p>9. Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie.</p> <p>10. Zasilanie AC 230V.</p> <p>11. Budżet mocy dla urządzeń PoE co najmniej 193 watów.</p> <p>12. Pojemność przełączania nie mniej, niż 92 Gb/s. Wydajność przełączania nie mniej niż 68 Mp/s.</p> <p>13. Architektura nieblokującą (wire-speed).</p> <p>14. Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych.</p> <p>15. Ilość RAM nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB.</p> <p>16. Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B.</p> <p>17. Bufor pakietów nie mniej, niż 1,5 MB.</p> <p>18. Temperatura pracy w zakresie co najmniej od -5C do 50 stopni Celsjusza.</p> <p>19. MTBF > 270000 godzin.</p> <p>20. Obudowa RACK 1U lub 2 U - urządzenia musi być dostarczone z wszystkimi komponentami do instalacji w szafie rackn19".</p>
2.	Funkcjonalności warstwy 2	<p>1. IGMP Snooping v3 - obsługa nie mniej, niż 510 grup multicast w tym co najmniej 256 grup statycznych.</p> <p>2. MLD Snooping v2 - obsługa nie mniej, niż 31 grup multicast w tym co najmniej 31 grup statycznych.</p> <p>3. IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN.</p> <p>4. Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP.</p> <p>5. Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP.</p> <p>6. LLDP (802.1AB) oraz LLDP-MED.</p> <p>7. ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni.</p> <p>8. DHCP Relay w tym opcji 60 i 61 oraz opcji 82, DHCP Local Relay + opcja 82. DHCP Relay dla IPv6.</p> <p>9. Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu.</p>

3.	Obsługa sieci VLAN	<ol style="list-style-type: none"> 1. 802.1Q VLAN, co najmniej 4094, 802.1v GVRP. 2. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. 3. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. 4. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
4.	Funkcjonalności warstwy 3	<ol style="list-style-type: none"> 1. Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. 2. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. 3. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. 4. Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. 5. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. 6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. 7. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. 8. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). 9. Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. 10. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
5.	Quality of Service	<ol style="list-style-type: none"> 1. Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6.

		<ol style="list-style-type: none"> Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
6.	Filtrowanie ruchu	<ol style="list-style-type: none"> Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
7.	Funkcje bezpieczeństwa	<ol style="list-style-type: none"> Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 120 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6.

		<p>7. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN.</p> <p>8. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.</p> <p>9. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.</p> <p>10. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.).</p> <p>11. Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.</p> <p>12. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany.</p> <p>13. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci.</p> <p>14. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU.</p> <p>15. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service.</p> <p>16. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.</p> <p>17. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.</p>
8.	Zarządzanie	<p>1. Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+.</p> <p>2. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP.</p>

		<ol style="list-style-type: none"> 3. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. 4. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. 5. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. 6. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. 7. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. 8. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. 9. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. 10. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. 11. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. 12. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. 13. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. 14. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. 15. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.
--	--	--

		<p>16. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego.</p> <p>17. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC.</p> <p>18. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.</p> <p>19. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.</p> <p>20. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC.</p> <p>21. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.</p> <p>22. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware.</p> <p>23. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.</p> <p>24. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).</p> <p>25. Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.</p>
9.	Pozostałe	<p>1. Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.</p> <p>2. Gwarancja 12 miesięcy.</p>

8.8.4. Przełącznik sieciowy wariant 4 - 1 sztuka

Lp.	Parametr lub warunek	Wymagania
1.	Charakterystyka sprzętowa	1. 24 x 1000Base-T IEEE 802.3ab

		<ol style="list-style-type: none"> 2. Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). 3. Musi istnieć możliwość zmiany prędkości i duplexu każdego portu i wyłączenia trybu FlowControl dla każdego portu. 4. 4 x SFP+ IEEE 802.3ae/802.3ak. Porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z; 5. Konsola szeregową RS-232. 6. Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie. 7. Zasilanie AC 230V. 8. Pojemność przełączania nie mniej, niż 128 Gb/s. Wydajność przełączania nie mniej niż 95 Mp/s. 9. Architektura nieblokująca (wire-speed). 10. Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych. 11. Ilość RAM nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. 12. Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B. 13. Bufor pakietów nie mniej, niż 1,5 MB. 14. Temperatura pracy w zakresie co najmniej od -5C do 50 stopni Celsjusza. 15. MTBF > 510000 godzin. 16. Obudowa RACK 1U lub 2 U - urządzenia musi być dostarczone z wszystkimi komponentami do instalacji w szafie rackn19".
2.	Funkcjonalności warstwy 2	<ol style="list-style-type: none"> 1. IGMP Snooping v3 - obsługa nie mniej, niż 510 grup multicast w tym co najmniej 256 grup statycznych. 2. MLD Snooping v2 - obsługa nie mniej, niż 31 grup multicast w tym co najmniej 31 grup statycznych. 3. IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN. 4. Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP. 5. Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP. 6. LLDP (802.1AB) oraz LLDP-MED. 7. ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni.

		<p>8. DHCP Relay w tym opcji 60 i 61 oraz opcji 82, DHCP Local Relay + opcja 82. DHCP Relay dla IPv6.</p> <p>9. Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu.</p>
3.	Obsługa sieci VLAN	<p>1. 802.1Q VLAN, co najmniej 4094, 802.1v GVRP.</p> <p>2. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN.</p> <p>3. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN.</p> <p>4. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.</p>
4.	Funkcjonalności warstwy 3	<p>1. Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów.</p> <p>2. Przełącznik musi posiadać funkcjonalność Gratuitous ARP.</p> <p>3. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci.</p> <p>4. Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP.</p> <p>5. Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych.</p> <p>6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6.</p> <p>7. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6.</p> <p>8. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras).</p> <p>9. Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4.</p> <p>10. Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.</p>
5.	Quality of Service	<p>1. Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać</p>

		<p>się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6.</p> <ol style="list-style-type: none"> 2. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. 3. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. 4. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
6.	Filtrowanie ruchu	<ol style="list-style-type: none"> 1. Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. 2. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
7.	Funkcje bezpieczeństwa	<ol style="list-style-type: none"> 1. Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 120 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. 2. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. 3. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. 4. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. 5. Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta.

		<ol style="list-style-type: none"> 6. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. 7. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. 8. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. 9. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. 10. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). 11. Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. 12. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany. 13. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. 14. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. 15. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. 16. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. 17. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
--	--	--

8.	Zarządzanie	<ol style="list-style-type: none"> 1. Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. 2. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. 3. Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. 4. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. 5. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet. 6. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. 7. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. 8. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. 9. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. 10. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. 11. Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. 12. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. 13. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6.
----	-------------	--

		<p>14. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.</p> <p>15. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.</p> <p>16. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego.</p> <p>17. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC.</p> <p>18. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.</p> <p>19. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.</p> <p>20. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC.</p> <p>21. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.</p> <p>22. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware.</p> <p>23. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.</p> <p>24. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).</p> <p>25. Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.</p>
9.	Pozostałe	<p>1. Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.</p> <p>2. Gwarancja 12 miesięcy.</p>

8.8.5. Wkładki SFP+ do przełączników sieciowych

Wkładki SFP+	20 sztuk
Wkładki tego samego producenta co przełączniki sieciowe i muszą być objęte wsparciem na okresie tożsamy z okresem wsparcia oferowanym dla przełączników i czasem gwarancji.	

8.9. Sieciowy punkt dostępowy - AccessPoint 16 sztuk

Lp	Parametr lub warunek	Wymagania
1	Rodzaj	<ol style="list-style-type: none"> 1. Urządzenie wewnętrzne. 2. Musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. 3. Funkcjonalność pozwalająca na zarządzanie urządzeniem z jednej konsoli wraz z urządzeniem UTM.
2	Obudowa	<ol style="list-style-type: none"> 1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: <ol style="list-style-type: none"> 1.1. Temperatura 0–50°C, 1.2. Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3	Funkcjonalność	<ol style="list-style-type: none"> 1. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: <ol style="list-style-type: none"> 1.1. 2.4 GHz 802.11b/g/n, 1.2. 5 GHz 802.11a/n/ac/ax, 1.3. 5/6 GHz 802.11a/n/ac/ax 2. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. 3. Urządzenie musi być wyposażone w moduł BLE. 4. Urządzenie musi być wyposażone w przynajmniej dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX. 5. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at. 6. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: <ol style="list-style-type: none"> 6.1. Tunnel, 6.2. Bridge, 6.3. Mesh. 7. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.

		<p>8. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).</p> <p>9. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:</p> <p>9.1. MIMO - 2x2,</p> <p>9.2. Maksymalna przepustowość dla poszczególnych modułów radiowych:</p> <p>9.2.1. 574 Mbps;</p> <p>9.2.2. 1201 Mbps;</p> <p>9.2.3. 2401 Mbps;</p> <p>9.3. Wymagana moc nadawania:</p> <p>9.3.1. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;</p> <p>9.3.2. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;</p> <p>9.3.3. min. 21 dBm dla pasma 6GHz z możliwością zmiany co 1dBm;</p> <p>9.4. Wsparcie dla 802.11n 20/40Mhz HT,</p> <p>9.5. Wsparcie dla kanałów 80 i 160MHz,</p> <p>9.6. Anteny - wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz.</p> <p>9.7. Możliwość wyłączenia nieużywanego modułu radiowego programowo w celu obniżenia poboru mocy,</p> <p>10. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512;</p> <p>10.1. Funkcje dodatkowe:</p> <p>10.2. OFDMA UL i DL</p> <p>10.3. Spatial Reuse (BSS Coloring)</p> <p>10.4. UL-MU-MIMO</p> <p>10.5. DL-MU-MIMO</p> <p>10.6. Enhanced Target Wake Time (TWT)</p> <p>10.7. Wbudowany analizator widma</p> <p>10.8. Wbudowane mechanizmy WIPS/WIDS</p>
4.	Gwarancja	<p>1. 12 miesięcy.</p> <p>2. Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania w czasie trwania gwarancji.</p> <p>3. Wsparcie techniczne w trybie 24x7.</p>

8.10. Serwery NAS

8.10.1. Serwer NAS wariant 1 - 1 sztuka

Urządzenie musi zapewniać synchronizację danych (plików) z aktualnie używanymi w Starostwie urządzeniami firmy QNAP: TS-432XU-RP i TS-873AeU-RP

Lp	Parametr lub warunek	Wymagania
1	Obudowa	<ol style="list-style-type: none">1. Typu RACK 1U lub 2U;2. Przyciski na obudowie zasilanie i reset;3. Zestaw dedykowanych szyn do montażu w szafie;4. 8 wnęk dla dysków twardych;5. Kompatybilność dysków:<ol style="list-style-type: none">5.1. 3,5-calowe dyski twarde SATA,5.2. 2,5-calowe dyski twarde SATA,5.3. 2,5-calowe dyski SSD SATA.6. Możliwość podłączenia minimum dwóch modułów rozszerzających.
2	Wskaźniki i przyciski na obudowie	<ol style="list-style-type: none">1. Zasilanie, LAN, dysków 1-8, USB;2. Zasilanie i reset.
3	Procesor	<ol style="list-style-type: none">1. Typu x86, wykonujący instrukcje 64 bitowe;2. Osiągający wynik co najmniej 4700pkt w teście SysMark2007 w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php3. Wykaz przykładowych procesorów w punkcie 9 specyfikacji;4. W przypadku braku zaoferowanego przez Wykonawcę procesora na w/w liście lub stronie internetowej http://www.cpubenchmark.net/cpu_list.php, Wykonawca obowiązany jest przeprowadzić test Passmarka i jego wynik załączyć do oferty z informacją, że test został wykonany przez Wykonawcę;
4	Pamięć RAM	<ol style="list-style-type: none">1. Minimum dwa sloty;2. 8 GB pamięci z możliwością rozbudowy do 64GB;3. Wymagane wolne jedno gniazdo pamięci.
5	Interfejsy sieciowe	<ol style="list-style-type: none">1. 2 x port 2,5 Gigabit Ethernet z funkcją Wake on LAN (WOL)2. 1 x port 10 Gigabit Ethernet RJ-45
6	Dyski twarde	<ol style="list-style-type: none">1. Osiem dysków twardych 3,5" o pojemności 20TB każdy.2. Oferowane dyski muszą się znajdować na liście zgodności/kompatybilności na stronie internetowej producenta urządzenia.

7	Zarządzanie dyskami	<ol style="list-style-type: none"> 1. RAID 1,5,6,10. 2. Obsługa Hot Spare per grupa RAID oraz global hot spare. 3. Rozszerzanie pojemności Online RAID. 4. Migracja poziomów Online RAID. 5. HDD S.M.A.R.T. 6. Skanowanie uszkodzonych bloków (pliku). 7. Przywracanie macierzy RAID. 8. Obsługa map bitowych. 9. Pula pamięci masowej. 10. Obsługa migawek. 11. Obsługa replikacji migawek.
8	Gniazda	<ol style="list-style-type: none"> 1. M.2 PCIe Gen3 x 1 – 2 sztuki; 2. PCIe Gen3 x8 – 1 sztuka.
9	Porty	<ol style="list-style-type: none"> 1. 4 x USB 3.2 Gen 2 w tym: 2 x typ A, 2 x typ C 2. Ilość dostępnych złączy USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakiegokolwiek slot PCI Express i/lub USB serwera
10	Pamięć flash	Z mechanizmem ochrony systemu operacyjnego przed podwójnym rozruchem – nie mniej niż 5GB
11	Zasilanie	Redundancja – 2 zasilacze
12	Język GUI	Polski, Angielski
13	Obsługiwane systemy plików	<ol style="list-style-type: none"> 1. Dyski wewnętrzne: EXT4. 2. Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+.
14	Oprogramowanie narzędziowe	<ol style="list-style-type: none"> 1. Zapewniające synchronizację plików pomiędzy różnymi urządzeniami w sposób tak aby dane na urządzeniach powiązanych z serwerem NAS zostały jednocześnie zaktualizowane po wprowadzeniu zmian. Możliwość synchronizacji wybranych danych, plików. 2. Zapewniające możliwość tworzenia kopii zapasowych wybranych plików, całych dysków przez zapisanie ich na serwerze NAS.
15	Pozostałe	<ol style="list-style-type: none"> 1. Agregacja łączy. 2. Szyfrowanie wolumenów min AES 256. 3. Szyfrowanie dysków zewnętrznych. 4. Wbudowana obsługa iSCSI. <ol style="list-style-type: none"> 4.1. Ograniczenie dostępnej pojemności dysku dla użytkownika. 4.2. Importowanie listy użytkowników. 4.3. Zarządzanie kontami użytkowników.

		<ul style="list-style-type: none"> 4.4. Zarządzanie grupą użytkowników. 4.5. Zarządzanie współdzieleniem w sieci. 4.6. Tworzenie użytkowników za pomocą makr. 4.7. Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL". 5. Obsługa VPN client / VPN server. Obsługa PPTP, OpenVPN. 6. Zabezpieczenia <ul style="list-style-type: none"> 6.1. "Połączenia HTTP/HTTPS. 6.2. Powiadamianie przez e-mail (uwierzytelnianie SMTP). 6.3. Powiadamianie przez SMS. 6.4. Ustawienia inteligentnego chłodzenia. 6.5. DDNS oraz zdalny dostęp w chmurze. 6.6. SNMP (v2 & v3). 6.7. Obsługa UPS z zarządzaniem SNMP (USB). 6.8. Obsługa sieciowej jednostki UPS. 6.9. Monitor zasobów. 6.10. Kosz sieciowy dla CIFS/SMB oraz AFP. 6.11. Monitor zasobów systemu w czasie rzeczywistym. 6.12. Rejestr zdarzeń. 6.13. Całkowity rejestr systemowy (poziom pliku). 6.14. Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line. 6.15. Aktualizacja oprogramowania. 6.16. Możliwość aktualizacji oprogramowania. 6.17. Ustawienia: Back up, przywracania, resetowania systemu". 7. Administracja systemu <ul style="list-style-type: none"> 7.1. "Połączenia HTTP/HTTPS. 7.2. Powiadamianie przez e-mail (uwierzytelnianie SMTP). 7.3. Powiadamianie przez SMS. 7.4. Ustawienia inteligentnego chłodzenia. 7.5. DDNS oraz zdalny dostęp w chmurze. 7.6. SNMP (v2 & v3). 7.7. Obsługa UPS z zarządzaniem SNMP (USB). 7.8. Obsługa sieciowej jednostki UPS. 7.9. Monitor zasobów. 7.10. Kosz sieciowy dla CIFS/SMB oraz AFP. 7.11. Monitor zasobów systemu w czasie rzeczywistym. 7.12. Rejestr zdarzeń. 7.13. Całkowity rejestr systemowy (poziom pliku). 7.14. Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line. 7.15. Aktualizacja oprogramowania. 7.16. Możliwość aktualizacji oprogramowania. 7.17. Ustawienia: Back up, przywracania, resetowania systemu".
--	--	---

		8. Zarządzanie prawami dostępu. 8.1. Ograniczenie dostępnej pojemności dysku dla użytkownika. 8.2. Importowanie listy użytkowników. 8.3. Zarządzanie kontami użytkowników. 8.4. Zarządzanie grupą użytkowników. 8.5. Zarządzanie współdzieleniem w sieci. 8.6. Tworzenie użytkowników za pomocą makr. 8.7. Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL. 9. Obsługa logowania Windows AD 9.1. Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web 9.2. Funkcja serwera LDAP 10. Minimum obsługiwane serwery. 10.1. Serwer plików. 10.2. Serwer FTP. 10.3. Serwer kopii zapasowych. 11. Wirtualizacja - wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. 12. Możliwość instalacji dodatkowego oprogramowania.
16	Gwarancja	12 miesięcy

8.10.2. Serwer NAS wariant 2 -11 sztuk

Lp	Parametr lub warunek	Wymagania
1	Obudowa	1. Typu RACK 1U2U; 2. Przyciski na obudowie zasilanie i reset; 3. Zestaw dedykowanych szyn do montażu w szafie; 4. 8 wnęk dla dysków twardych; 5. Kompatybilność dysków: 5.1. 3,5-calowe dyski twarde SATA, 5.2. 2,5-calowe dyski twarde SATA, 5.3. 2,5-calowe dyski SSD SATA. 6. Możliwość podłączenia minimum dwóch modułów rozszerzających.
2	Wskaźniki i przyciski na obudowie	1. Zasilanie, LAN, dysków 1-8, USB; 2. Zasilanie i reset.
3	Procesor	1. Typu x86, wykonujący instrukcje 64 bitowe;

		<ol style="list-style-type: none"> Osiągający wynik co najmniej 3900 pkt w teście SysMark2007 w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php Wykaz przykładowych procesorów w punkcie 9 specyfikacji; W przypadku braku zaoferowanego przez Wykonawcę procesora na w/w liście lub stronie internetowej http://www.cpubenchmark.net/cpu_list.php, Wykonawca obowiązany jest przeprowadzić test Passmarka i jego wynik załączyć do oferty z informacją, że test został wykonany przez Wykonawcę;
4	Pamięć RAM	<ol style="list-style-type: none"> Minimum dwa sloty; 8 GB pamięci z możliwością rozbudowy do 16GB; Wymagane wolne jedno gniazdo pamięci.
5	Interfejsy sieciowe	2 x port 2,5 Gigabit Ethernet
6	Dyski twarde	Ilość i wielkość dysków w tabeli poniżej. Oferowane dyski muszą się znajdować na liście zgodności/kompatybilności na stronie internetowej producenta urządzenia.
7	Zarządzanie dyskami	<ol style="list-style-type: none"> RAID 1,5,6,10. Obsługa Hot Spare per grupa RAID oraz global hot spare. Rozszerzanie pojemności Online RAID. Migracja poziomów Online RAID. HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku). Przywracanie macierzy RAID. Obsługa map bitowych. Pula pamięci masowej. Obsługa migawek. Obsługa replikacji migawek. Obsługa dysków do 22TB.
8	Gniazda	PCIe Gen3 x8 – 1 sztuka.
9	Porty	<ol style="list-style-type: none"> 4 x USB w tym: 2 x USB3.2 Gen2, 2 x USB 2.0 Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera
10	Pamięć flash	Z mechanizmem ochrony systemu operacyjnego przed podwójnym rozruchem
11	Zasilanie	Redundancja – 2 zasilacze

12	Język GUI	Polski, Angielski
13	System plików	Obsługa dysków zewnętrznych exFAT. W przypadku, gdy uzyskanie powyżej funkcjonalności wymaga zapewnienia odpłatnych licencji, to należy takie licencje zapewnić w ramach zaoferowanego urządzenia.
14	Oprogramowanie narzędziowe działające w środowisku Windows	<ol style="list-style-type: none"> 1. Zapewniające synchronizację plików pomiędzy różnymi urządzeniami w sposób tak aby dane na urządzeniach powiązanych z serwerem NAS zostały jednocześnie zaktualizowane po wprowadzeniu zmian. Możliwość synchronizacji wybranych danych, plików. 2. Zapewniające możliwość tworzenia kopii zapasowych wybranych plików, całych dysków przez zapisanie ich na serwerze NAS.
15	Pozostałe	<ol style="list-style-type: none"> 1. Agregacja łączy. 2. Szyfrowanie wolumenów min AES 256. 3. Szyfrowanie dysków zewnętrznych. 4. Wbudowana obsługa iSCSI. <ol style="list-style-type: none"> 4.1. "Multi-LUNs na Target 4.2. Obsługa LUN Mapping & Masking 4.3. Obsługa SPC-3 Persistent Reservation 4.4. Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN 5. Obsługa VPN client / VPN server. Obsługa PPTP, OpenVPN. 6. Zabezpieczenia <ol style="list-style-type: none"> 6.1. "Filtracja IP 6.2. Ochrona dostępu do sieci z automatycznym blokowaniem 6.3. Połączenie HTTPS 6.4. FTP z SSL/TLS (Explicit) 6.5. Obsługa SFTP 6.6. Szyfrowanie AES 256-bit 6.7. Szyfrowana zdalna replikacja (Rsync poprzez SSH) 6.8. Import certyfikatu SSL 6.9. Powiadomienia o zdarzeniach za pośrednictwem email i sms" 7. Administracja systemu. <ol style="list-style-type: none"> 7.1. Połączenia HTTP/HTTPS. 7.2. Powiadamianie przez e-mail (uwierzytelnianie SMTP). 7.3. Powiadamianie przez sms. 7.4. Ustawienia inteligentnego chłodzenia. 7.5. DDNS oraz zdalny dostęp w chmurze. 7.6. SNMP (v2 & v3). 7.7. Obsługa UPS z zarządzaniem SNMP (USB). 7.8. Obsługa sieciowej jednostki UPS.

		<p>7.9. Monitor zasobów.</p> <p>7.10. Kosz sieciowy dla CIFS/SMB oraz AFP.</p> <p>7.11. Monitor zasobów systemu w czasie rzeczywistym.</p> <p>7.12. Rejestr zdarzeń.</p> <p>7.13. System plików dziennika.</p> <p>7.14. Całkowity rejestr systemowy (poziom pliku).</p> <p>7.15. Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line.</p> <p>7.16. Aktualizacja oprogramowania.</p> <p>7.17. Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu.</p> <p>8. Zarządzanie prawami dostępu</p> <p>8.1. Ograniczenie dostępnej pojemności dysku dla użytkownika.</p> <p>8.2. Importowanie listy użytkowników.</p> <p>8.3. Zarządzanie kontami użytkowników.</p> <p>8.4. Zarządzanie grupą użytkowników.</p> <p>8.5. Zarządzanie współdzieleniem w sieci.</p> <p>8.6. Tworzenie użytkowników za pomocą makr.</p> <p>8.7. Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL.</p> <p>9. Obsługa Windows AD</p> <p>9.1. Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web.</p> <p>9.2. Funkcja serwera LDAP.</p> <p>10. Funkcje backup - oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde.</p> <p>11. Współpraca z zewnętrznymi dostawcami usług chmury: przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box</p> <p>12. Minimum obsługiwane serwery.</p> <p>12.1. Serwer plików.</p> <p>12.2. Serwer FTP.</p> <p>12.3. Serwer kopii zapasowych.</p> <p>13. Wirtualizacja - wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.</p> <p>14. Konteneryzacja - możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker</p> <p>15. Możliwość instalacji dodatkowego oprogramowania.</p>
16	Gwarancja	12 miesięcy
Dyski do serwerów NAS Wariant 2 – dla 11 urządzeń		

Pojemność dysku	Ilość dysków
4TB	28 sztuk
8TB	16 sztuk

8.10.3. Zasilacze bezprzerwowe (UPS) do serwerów NAS 12 sztuk

Lp	Parametr lub warunek	Wymagania
1.	Obudowa	Wolnostojąca TOWER.
2.	Moc (VA)	1000
3.	Moc (W)	550
4.	Topologia UPS	Line-interactive.
5.	Kształt fali przy pracy baterii	Symulowana fala sinusoidalna.
6.	Faza	Jednofazowe
7.	Nominalne napięcie wejściowe (Vac)	$230 \pm 10\%$
8.	Częstotliwość wejściowa (Hz)	50 ± 5 60 ± 5
9.	Rodzaj złącza wejściowego	IEC C14
10.	Automatyczna regulacja napięcia (AVR)	TAK
11.	Ochrona przed przeciążeniem	TAK
12.	Liczba gniazd	4
13.	Rodzaj gniazd wyjściowych	1. FR. 2. W przypadku gniazd EC 320 C13 IEC dostarczyć komplet kabli przyłączeniowych.
14.	Port komunikacyjny	USB - dostarczyć kabel.
15.	Czas pracy przy pełnym obciążeniu (min)	1

16.	Typowy czas transferu (ms)	4
17.	Typowy czas ponownego ładowania w godzinach	Maksimum 8
18.	Informacje na panelu przednim	1. Rodzaj działania. 2. Stan zasilania. 3. Stan baterii. 4. Stan obciążenia. 5. Usterka. 6. Ostrzeżenie.
19.	Alarmy dźwiękowe	TAK
20.	Typy alarmów dźwiękowych	1. Niski poziom baterii. 2. Przeciążenie 3. Usterka UPS.
21.	Wymiary	Wysokość do 240mm.
22.	Okres gwarancji na produkt i baterie	12 miesięcy.

8.11. Zewnętrzne dyski USB

Lp	Parametr lub warunek	Wymagania
1.	Ogólne	1. Przenośne dyski z wbudowaną klawiaturą. 2. 256-bitowe szyfrowanie sprzętowe AES. 3. Płynne szyfrowanie wszystkich danych na dysku w czasie rzeczywistym. 4. Interfejs USB 3.1 GEN 1 ze złączem USB-C. 5. Przewód USB-C do USB-A z przejściówką USB-A do USB-C. 6. Rozwiązanie nie zapisujące haseł na komputerze ani w pamięci ulotnej systemu. 7. Zgodność z komputerami PC i Mac. 8. Zasilanie z magistrali przez przewód USB. 9. Gwarancje 12 miesięcy.
Pojemności i ilość dysków.		
Pojemność dysku		Ilość dysków
1TB USB 3.2 Gen 1		22 sztuk
2TB USB 3.2 Gen 1		10 sztuk

8.12. System kopii zapasowych

Lp	Parametr lub warunek	Wymagania
1.	Ogólne	<ol style="list-style-type: none"> Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk wirtualizacyjnych. Licencja na dwa serwery fizyczne z nielimitowaną ilością maszyn wirtualnych. Interfejs w języku polskim.
2.	Wymagania systemowe	<ol style="list-style-type: none"> Oprogramowanie musi wspierać co najmniej systemy operacyjne: <ol style="list-style-type: none"> VMware ESX/ESX(i) 6.0, 6.5, 6.7, 7.0, 8.0. Hyper-V Red Hat Virtualization 4.0, 4.1. Linux KVM Dla maszyn wirtualnych: <ol style="list-style-type: none"> Windows Server 2016/2019/2022/2025, Linux OS macOS
3.	Zarządzanie systemem kopii zapasowych	<ol style="list-style-type: none"> Musi posiadać, co najmniej poniższe funkcjonalności: <ol style="list-style-type: none"> Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek i ich najnowszymi wersjami. Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu). Definiowanie uprawnień dla administratorów system kopii zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.). Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami. Wsparcie dla Single Sign On dla logowania do systemu. Zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.

		<p>1.9. Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).</p> <p>1.10. Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopii zapasowych.</p> <p>1.11. Możliwość zdalnej instalacji agentów kopii zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.</p> <p>1.12. Zdalne uaktualniania agentów kopii zapasowych.</p> <p>1.13. Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.</p> <p>1.14. Możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopii zapasowej).</p> <p>1.15. Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.</p> <p>1.16. Centralny katalog wszystkich danych zapisanych w kopiach zapasowych</p> <p>1.17. Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.</p>
4.	Funkcjonalność systemu kopii zapasowych	<p>1. Kopie zapasowe całych dysków i partycji.</p> <p>2. Kopie zapasowe wybranych plików i folderów.</p> <p>3. Kopia zapasowa udziałów sieciowych.</p> <p>4. Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi).</p> <p>5. Kopie zapasowe aplikacji (SQL, SharePoint, Active Directory)</p> <p>6. Kopie zapasowe hostów Hyper-V i VMWare ESXi.</p> <p>7. Możliwość zapisu kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopii zapasowych.</p> <p>8. Zapis kopii zapasowych na udziały sieciowe.</p> <p>9. Zapis kopii zapasowych na serwer SFTP.</p> <p>10. Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.</p> <p>11. Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloader).</p> <p>12. Możliwość wyszukiwania plików w kopiach zapasowych.</p> <p>13. Szyfrowanie plików kopii zapasowych.</p> <p>14. Wsparcie dla technologii VSS.</p>

		<p>15. Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.</p> <p>16. Kompresja plików kopi zapasowych</p> <p>17. Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).</p> <p>18. Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopii zapasowych.</p>
5.	Odtwarzanie kopii zapasowych	<p>1. Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore</p> <p>2. Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.</p> <p>3. Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej.</p> <p>4. Odtworzenie poszczególnych plików i folderów.</p> <p>5. Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonana kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).</p> <p>6. Granularne odtwarzanie baz danych Microsoft SQL.</p> <p>7. Granularne odtwarzanie witryn i plików Microsoft SharePoint.</p> <p>8. Odtwarzanie kontrolerów domeny Microsoft Active Directory.</p> <p>9. Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.</p> <p>10. Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.</p>
6.	Wymagania dla systemów Windows 8.1, 10 i 11	<p>1. Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów Windows 10 i nowszych:</p> <p>1.1. Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.</p> <p>1.2. Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.</p>
7.	Licencja	Licencja na okres 12 miesięcy.
8.	Licencjonowanie	<p>1. Możliwość zakupu (odnowienia) licencji subskrypcyjnych w okresie od 1 roku do 5 lat.</p> <p>2. Model licencjonowania oparty na maszynach fizycznych – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji).</p>

9.	Wdrożenie	<ol style="list-style-type: none"> 1. Wdrożenia, konfiguracja oraz profilowanie ustawień. 2. Instruktarz wdrożeniowy w wymiarze 7 godzin – elementy: <ol style="list-style-type: none"> 2.1. Instalacja i konfiguracja. 2.2. Konsola administracyjna. 2.3. Administrowanie kontami i uprawnieniami. 2.4. Tworzenie planów kopii zapasowej. 2.5. Odzyskiwanie kopii zapasowej – metody odtwarzania.
----	-----------	--

8.13. Klucze sprzętowe do uwierzytelniania – 120 sztuk

Lp	Parametr lub warunek	Wymagania
1.	Wymagania ogólne	<ol style="list-style-type: none"> 1. Zapewniający dostęp do kluczowych uprawnień w systemie tylko uprawnionym użytkownikom przez uwierzytelnienie dwuskładnikowe. 2. Integracja rozwiązania z Microsoft Active Directory. 3. Urządzenie musi posiadać wsparcie dla platform: Microsoft Windows, Mac OS, Linux, Chrome OS. 4. Urządzenie musi umożliwiać współpracę z mobilnymi systemami operacyjnymi iOS oraz Android. 5. Urządzenie musi być kompatybilne z przeglądarkami: Chrome, Edge, Opera, Safari, Firefox. 6. Urządzenie musi być kompatybilne z serwisami: Google, Microsoft, Twitter, Facebook, Instagram, Gmail, Google Drive i YouTube. 7. Urządzenie musi posiadać możliwość potwierdzenia logowania dotknięciem przycisku - obowiązkowa interakcja użytkownika podczas logowania. 8. Urządzenie musi być odporne na zgniecenie. 9. Urządzenie musi posiadać klasę szczelności IP68. 10. Urządzenie do działania nie może wymagać baterii. 11. Urządzenie do działania nie może wymagać połączenia internetowego. 12. Urządzenie nie może być typem pamięci/dysków pendrive, czyli posiadać miejsce do przechowywania danych: pliki, katalogi. 13. Urządzenie nie może działać po Bluetooth. 14. Urządzenie nie może obsługiwać logowania za pomocą biometrii. 15. Urządzenie musi być tak fizycznie skonstruowane, by uniemożliwić jego rozłożenie na części i ponowne złożenie. 16. Urządzenie musi posiadać możliwość wygrawerowania loga/kodu. 17. Urządzenie musi umożliwiać przechowywanie na nim kodów OTP, zamiast np: w aplikacji mobilnej.

		<p>18. Urządzenie musi posiadać specjalne wzmocnione oczko umożliwiające zawieszenie urządzenia.</p> <p>19. Klucz musi być produkowany wyłącznie na terenie EU lub USA.</p> <p>20. Klucz musi posiadać NFC, by można było zdalnie przekazać kod do urządzenia mobilnego.</p> <p>21. Urządzenie musi posiadać wymiary nie większe niż 4,5 cm x 2 cm x 1 cm (wysokość/szerokość/grubość) i o wadze nie większej niż 15 gram.</p> <p>22. Klucz jest tak zabezpieczony przez producenta, że nie ma możliwości wykonania jego kopii na inny klucz czy też dokonania manipulacji w obrębie jego oprogramowania.</p> <p>23. Oprogramowanie do zarządzania kluczem powinno być udostępnione bezpłatnie do pobrania ze strony producenta.</p> <p>24. Dostępność oprogramowania/bibliotek/API na stronie producenta na zasadzie open source, w celu integracji z niestandardowymi aplikacjami.</p> <p>25. Urządzenie musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na co należy przedłożyć zaświadczenie od dystrybutora lub producenta.</p>
2.	Bezpieczeństwo	<p>1. Urządzenie musi być rozwiązaniem sprzętowym skutecznie chroniącym m.in. przed phishingiem.</p> <p>2. Urządzenie musi posiadać wsparcie dla PKCS#11.</p> <p>3. Urządzenie musi obsługiwać algorytmy kryptograficzne: RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384.</p> <p>4. Klucz sprzętowy do dwupoziomowego uwierzytelnienia, który posiada certyfikację U2F i FIDO2.</p> <p>5. Klucz musi być zasilany tylko z portu USB lub wyzwać tag NFC po przyłożeniu do urządzenia mobilnego.</p> <p>6. Klucz wyzwala tag NFC (kod FIDO/FIDO2 w aplikacji mobilnej) po przyłożeniu do urządzenia mobilnego.</p> <p>7. Klucz sprzętowy musi posiadać oprócz U2F i FIDO2 również inne możliwości logowania czy obsługi szyfrowania, jak: smart card, Open PGP, OTP, kody zdarzeniowe i czasowe TOTP/HOTP, statyczne hasło oraz Challenge-Response.</p> <p>8. Klucz musi posiadać możliwość zaprogramowania dwóch dodatkowych portów o dodatkowe funkcje:</p> <p>8.1. OTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą darmowej aplikacji producenta)</p> <p>8.2. kody zdarzeniowe i czasowe TOTP/HOTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą darmowej aplikacji producenta)</p> <p>8.3. statyczne hasło</p> <p>8.4. Challenge-Response</p>

3.	Interfejs	Złącze fizyczne: USB A.
4.	Gwarancja	12 miesięcy

8.14. Zakup i wymiana akumulatorów w zasilaczu bezprzerwowym (UPS)

Lp	Parametr lub warunek	Wymagania
1.	Model urządzenia	UPS APC SMT22000I
2.	Opis ogólny	Oryginalna wymienna kaseta akumulatorowa wyposażona w fabrycznie zamontowane kable i wtyki zapewniająca 100% zgodności z zasilaczem UPS.
3.	Gwarancja	12 miesięcy

8.15. System do zarządzania infrastrukturą IT w Starostwie

Lp	Parametr lub warunek	Wymagania
1.	Architektura/budowa	<ol style="list-style-type: none"> Bezproblemowa obsługa co najmniej 100 klientów jednocześnie. <ol style="list-style-type: none"> Klient - komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przysyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej. Konfiguracja Architektury: <ol style="list-style-type: none"> Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.

		2.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.
2.	Wymagania systemowe	<ol style="list-style-type: none"> 1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5. 2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2019, 2022, 2025, Windows 10, 11, MacOS 10.7, 10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. <ol style="list-style-type: none"> 2.1. Klient wspiera aktualne wersje przeglądarek internetowych w zakresie monitorowania aktywności użytkownika w sieci takie jak: Chrome, Firefox i Microsoft Edge. 3. Serwer musi działać na systemach 64 bitowych: Windows Server 2022/2025. 4. Baza danych działająca na najnowszej stabilnej wersji silnika Microsoft SQL Server, MS SQL Server Express. 5. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V .
3.	Interfejsy	<ol style="list-style-type: none"> 1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. 2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL. 3. System zapewnia integrację z modelem LLM.
4.	Funkcjonalność systemu zarządzania infrastrukturą IT	<ol style="list-style-type: none"> 1. Funkcjonalność Klienta. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownika. 2. Funkcjonalność konsoli administracyjnej <ol style="list-style-type: none"> 2.1. Konsola administracyjna musi być w języku polskim i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.

		<p>2.2. Funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.</p> <p>2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.</p> <p>3. Funkcjonalność panelu pracownika. Musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.</p> <p>4. Zarządzanie licencjami. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.</p> <p>5. Wzorce aplikacji i pakietów. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.</p> <p>6. Inwentaryzacja sprzętu komputerowego i urządzeń.</p> <p>6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.</p> <p>6.2. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie</p>
--	--	--

		<p>skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.</p> <p>6.3. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.</p> <p>6.4. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.</p> <p>7. Zdalna administracja komputerami.</p> <p>7.1. System musi zapewnić kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.</p> <p>7.2. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.</p> <p>7.3. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.</p> <p>7.4. System musi umożliwiać zdalną instalację pakietów MSI i plików .exe, korzystając z Windows Management Instrumentation (WMI) oraz usługi Klient bez dodatkowych poświadczeń, wykorzystując lokalne i sieciowe repozytoria. Powinien obsługiwać tworzenie repozytorium instalatorów z możliwością dodawania aplikacji, zarządzania wersjami oraz kategoryzacji. System musi również umożliwiać tworzenie grup instalacyjnych, definiowanie schematów instalacyjnych i automatyzację procesu instalacji na nowych urządzeniach. Powinien zawierać kiosk aplikacji umożliwiający użytkownikom samodzielną instalację aplikacji oraz</p>
--	--	--

		<p>rejestrować i raportować wszystkie procesy instalacji, umożliwiając również ich przerwanie.</p> <p>8. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.</p> <p>9. Automatyzacja czynności. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.</p> <p>10. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.</p> <p>11. Repozytorium. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.</p> <p>12. Wspieranie obsługi kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.</p> <p>13. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z</p>
--	--	---

		<p>możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.</p> <p>14. Monitorowanie drukarek sieciowych i wydruków.</p> <p>14.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.</p> <p>15. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.</p> <p>16. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.</p> <p>17. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.</p> <p>18. System musi umożliwiać monitorowanie komunikatów Syslog.</p> <p>19. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.</p> <p>20. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.</p> <p>21. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.</p> <p>22. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.</p> <p>23. Worktime manager. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w</p>
--	--	--

		<p>aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.</p> <p>24. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.</p> <p>25. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.</p> <p>26. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.</p> <p>27. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.</p>
5.	Licencja	<p>1. Bezterminowa.</p> <p>2. Serwis oprogramowania 12 miesięcy od zakończenia Wdrożenia.</p>
6.	Pomoc techniczna i wsparcie	<p>1. Pomoc musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.</p> <p>2. Zapewnienie wsparcia w formie zapewnienia ciągłości działania oraz dostarczania aktualizacji 12 miesięcy od daty zakupu.</p>
7.	Wdrożenie	<p>1. Wdrożenia, konfiguracja oraz profilowanie ustawień.</p> <p>2. Instruktarz wdrożeniowy w wymiarze 3 godzin.</p>

8.16. System centralizujący zarządzanie infrastrukturą siecią LAN

Lp	Parametr lub warunek	Wymagania
1.	Ogólne	<ol style="list-style-type: none"> 1. Zakup systemu centralizującego zarządzanie infrastrukturą siecią, łączącego funkcjonalność IPAM (IP Address Management), NAC (Network Access Control) oraz monitoring RADIUS spełniającego łącznie wymagania określone w pkt 2. 2. Interfejs w języku polskim. 3. Usługa dostawy i wdrożenia systemu spełniające łącznie wymagania określone w pkt 3. 4. Serwis techniczny systemu, spełniający łącznie wymagania określone w pkt 4.
2.	Wymagania systemowe	<ol style="list-style-type: none"> 1. Architektura. <ol style="list-style-type: none"> 1.1. System powinien mieć postać zamkniętej platformy wirtualnej (virtual appliance) do implementacji w ramach środowiska Zamawiającego. Przez virtual appliance, Zamawiający rozumie specjalizowane rozwiązanie, mające postać maszyny wirtualnej w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu. 1.2. System musi współpracować z urządzeniem klasy UTM aktualnie użytkowanym przez Zamawiającego oraz zarządzalnymi przełącznikami sieciowymi wspierającymi standard RADIUS Port Based Access Control (znane też jako: RADIUS MAC Based Authentication, IEEE 802.1X RADIUS port access authentication, IEEE 802.1X RADIUS Network Access Control). 1.3. Interfejs użytkownika systemu musi być dostępny przez przeglądarkę internetową, bez konieczności instalacji na urządzeniach końcowych. 1.4. Konsola zarządzania musi umożliwiać dostęp szyfrowany z pomoc protokołu TLS. 1.5. Praca Systemu musi pozwalać na działanie bez dostępu do Internetu. 2. Uwierzytelniania, hasła, autoryzacja i separacja uprawnień. <ol style="list-style-type: none"> 2.1. System musi zapewnić możliwość integracji kont użytkowników systemu z mechanizmami uwierzytelniania takimi jak hasła i Active Directory. 2.2. System musi zapewniać możliwość dwuskładnikowego uwierzytelniania metodami: HOTP - IETF RFC 4226, TOTP - IETF RFC 6238, WebAuthn. 2.3. System musi zapewnić możliwość ograniczenia dostępu użytkowników do wybranych systemów docelowych.

		<p>2.4. System musi umożliwić utworzenie wielu administratorów, którzy będą mieli możliwość nadawania dostępów dla użytkowników oraz sprzętów komputerowych.</p> <p>2.5. System powinien mieć możliwość wyodrębnienia hierarchii uprawnień dla Administratorów, która określi możliwości Administratora w ramach procesów akceptacji wniosków, nadawania dostępów, dodawania nowych urządzeń do sieci oraz konfigurację dostępów.</p> <p>2.6. System musi zapewnić możliwość oddzielenia ról: użytkownika (operator lub administrator danego systemu docelowego), administratora (zarządzający adresacją sieci i dostęпами sieciowymi), gościa (uprawniony do terminowo wydzielonego przez administratora dostępu do danego fragmentu sieci wewnętrznej).</p> <p>3. Zarządzanie dostęпами sieciowymi i kontrola nad dostęпами sieciowymi (NAC).</p> <p>3.1. System w integracji z urządzeniami UTM oraz przełącznikami sieciowymi musi umożliwić centralne zarządzania dostęпами.</p> <p>3.2. System musi uniemożliwiać dostęp do sieci wewnętrznej dla użytkownika przed zalogowaniem się i aktywacją dostępów z poziomu interfejsu webowego systemu.</p> <p>3.3. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).</p> <p>3.4. System musi mieć możliwość tworzenia grup użytkowników, którym nadawane będą ujednolicone dostępy sieciowe.</p> <p>3.5. System musi umożliwić przypisywanie użytkownika do wielu grup oraz jednocześnie nadawanie mu dostępów indywidualnie.</p> <p>3.6. System musi w zautomatyzowany sposób tworzyć reguły dostępowe do połączeń zdalnych (SSL-VPN) dla wybranych użytkowników sieci.</p> <p>3.7. System musi mieć możliwość tworzenia dostępów harmonogramowych (w określonym czasie) oraz dostępów tymczasowych (automatycznie blokowanych po upływie określonego w momencie nadawania dostępu czasu) dla wybranych użytkowników. Minimum możliwość definiowania dwóch okresów czasowych na dobę.</p> <p>3.8. System musi umożliwić użytkownikom wnioskowanie o dostępy do określonego zasoby sieciowego z poziomu interfejsu webowego systemu.</p> <p>3.9. System musi umożliwić Administratorowi zarządzanie wnioskami o dostępy sieciowe z poziomu interfejsu webowego systemu poprzez akceptację lub odrzucenie</p>
--	--	---

		<p>wniosku oraz zmianę statusu wniosku widoczną przez Administratora oraz wnioskującego użytkownika sieci.</p> <p>3.10. System musi umożliwić nadawanie dostępu dla gości, z określeniem czasu wygaśnięcia dostępu.</p> <p>3.11. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych.</p> <p>3.12. System musi mieć możliwość szyfrowania danych uwierzytelniania SNMP i kluczy dostępowych API.</p> <p>3.13. System musi pozwalać na szyfrację i anonimizację wrażliwych danych gości zgodnie z rozporządzeniem RODO.</p> <p>4. Wykrywanie nieautoryzowanych urządzeń i ataków na sieć.</p> <p>4.1. System musi na bieżąco pobierać informacje z urządzeń infrastruktury sieciowej (przełączniki oraz urządzenia UTM) za pomocą udostępnionych API i SNMP w poszukiwaniu nieautoryzowanych urządzeń i ataków na sieć</p> <p>4.2. System musi wykrywać niewystępujące w bazie danych urządzenia podłączone do sieci.</p> <p>4.3. System korzystając z protokołu RADIUS musi blokować dostęp dla nieautoryzowanych urządzeń oraz urządzeń nieprzypisanych do danego portu przełącznika sieciowego.</p> <p>4.4. System musi wykrywać podwojone adresy MAC w sieci (ataki MAC spoofing).</p> <p>4.5. System musi wykrywać wielokrotne próby połączenia do sieci tym samym portem z różnym adresem MAC (ataki brute-force).</p> <p>4.6. System musi na bieżąco informować Administratora o próbach przeprowadzenia ataków typu MAC spoofing oraz brute-force na sieć.</p> <p>4.7. System musi mieć możliwość gromadzenia i analizy przepływów ruchu sieciowego NetFlow i sFlow.</p> <p>4.8. System musi odbierać komunikaty SNMP Trap od połączonych urządzeń infrastruktury sieciowej.</p> <p>5. Tworzenie raportów</p> <p>5.1. System musi na żądanie tworzyć zestawienia posiadanych przez Zamawiającego urządzeń końcowych i urządzeń sieciowych.</p> <p>5.2. System musi na żądanie tworzyć zestawienie zdarzeń dotyczących bezpieczeństwa sieci.</p> <p>5.3. System musi gromadzić informacje o zapytaniach wykonanych do API Systemu i umożliwiać ich późniejszą analizę.</p>
--	--	---

3.	Dostawa, instalacja i wdrożenie	<ol style="list-style-type: none"> 1. Konfiguracja systemu musi uwzględniać: <ol style="list-style-type: none"> 1.1. Utworzenie kont użytkowników i grup dostępowych zgodnie z wymaganiami Zamawiającego. 1.2. Integracja uwierzytelniania i autoryzacji użytkowników systemu z Active Directory Zamawiającego. 1.3. Utworzenie dostępów dla użytkowników sieci zgodnie z wymaganiami Zamawiającego. 1.4. Konfiguracja urządzeń końcowych i urządzeń sieciowych zgodnie z wymaganiami Zamawiającego. 2. Dokumentacja systemu. <ol style="list-style-type: none"> 2.1. Wykonana wg obowiązujących standardów dla tego typu dokumentów w języku polskim i dostarczona w formie elektronicznej. 2.2. Zawartość merytoryczna musi zawierać <ol style="list-style-type: none"> 2.2.1. Schemat infrastruktury systemu wraz z opisem. 2.2.2. Konfigurację sprzętową i logiczną elementów infrastruktury systemu. 2.2.3. Procedurę konfiguracji wszystkich elementów systemu „krok po kroku”. 2.2.4. Procedury uruchamiania, zatrzymywania systemu oraz elementów infrastruktury. 2.2.5. Procedury opisujące standardowe działania administracyjne. 2.2.6. Wytyczne (dobre praktyki) dla administratorów. 2.2.7. Procedury zgłaszania problemów do serwisu.
4.	Licencja i serwis oprogramowania	<ol style="list-style-type: none"> 1. Licencja bezterminowa. 2. Serwis oprogramowania 12 miesięcy od zakończenia Wdrożenia. <ol style="list-style-type: none"> 2.1. Dostęp do serwisu przez WWW, mail i wyznaczony telefon kontaktowy.. 2.2. Dostępność serwisu w godzinach od 8:00 do 16:00 w dni robocze. 3. Usługi wsparcia <ol style="list-style-type: none"> 3.1. Pomoc w analizie i rozwiązywaniu problemów z oprogramowaniem. 3.2. Doradztwo i pomoc w zakresie obsługi oprogramowania. 3.3. Rozwiązywanie błędów w działaniu oprogramowania zgłaszanych do serwisu . 3.4. Informowanie o znanych problemach z oprogramowaniem i sposobach ich rozwiązywania. 4. Usługi reaktywne <ol style="list-style-type: none"> 4.1. Czas reakcji dla: <ol style="list-style-type: none"> 4.1.1. Awarii (rozumianej jako niezgodne z opisany w Dokumentacji funkcjonowanie systemu, które powoduje zawieszenie się pracy systemu, wprowadza techniczną niespójność w bazie danych lub zaburzenia w integralności danych lub sytuacja, w której system w

		<p>ogóle nie funkcjonuje lub funkcjonuje z czasami działania uniemożliwiającymi działalność operacyjną, w tym poprawną realizację usług dla klientów, czyli w sytuacji gdzie średni czas wszystkich odpowiedzi systemu na żądania Użytkowników przekracza 10 sekund) ≤ 6 godzin.</p> <p>4.1.2. Błędu (funkcjonowanie systemu niezgodne z dokumentacją, w szczególności działanie ograniczające funkcjonalność lub wydajność lub pojemność systemu) ≤ 1 dzień roboczy.</p> <p>4.1.3. Usterka (wada inna niż awaria i błąd) ≤ 5 dni roboczych to okres od chwili przyjęcia i zarejestrowania zgłoszenia do czasu rozpoczęcia realizacji zgłoszenia</p> <p>4.2. W przypadku wystąpienia problemów, których nie można rozwiązać zdalnie, pomoc techniczna w miejscu instalacji. Po przybyciu serwisu na miejsce, prace serwisowe będą kontynuowane, aż do momentu uzyskania dostępności systemu lub do momentu osiągnięcia widocznej poprawy. Dopuszczalne jest zawieszenie czynności naprawczych, jeśli potrzebne są dodatkowe materiały lub informacje, ale praca zostaje wznowiona natychmiast po ich uzyskaniu.</p> <p>4.3. Gwarantowany czas naprawy lub dostarczenia obejścia dla:</p> <p>4.3.1. Awarii (definicja, patrz powyżej) ≤ 48 godzin</p> <p>4.3.2. Błędu (definicja, patrz powyżej) ≤ 5 dni roboczych</p> <p>4.3.3. Usterki (definicja, patrz powyżej) ≤ 60 dni roboczych to zobowiązanie do zdiagnozowania i naprawienia wady we wskazanym czasie od zgłoszenia.</p> <p>5. Dostęp do aktualizacji i baz wiedzy.</p> <p>5.1. Dostęp do nowych wersji, aktualizacji i poprawek do oprogramowania.</p> <p>5.2. Licencje na użytkowanie i kopiowanie nowych wersji, aktualizacji i poprawek do oprogramowania.</p> <p>5.3. Dostęp do elektronicznych kanałów informacji i usług wsparcia.</p>
--	--	--