ZAPYTANIE OFERTOWE

W nawiązaniu do zapytania ofertowego w zakresie szacunkowej wartości zamówienia w zakresie **Dostawy zintegrowanej platformy telemedycznej jako narzędzia innowacyjnego interdyscyplinarnego systemu dystrybucji i świadczenia usług e-medycznych z modelem domowej opieki holistycznej wraz z niezbędnym sprzętem teleinformatycznym** poniżej przedstawiamy uszczegółowienie w zakresie funkcjonalności platformy oraz wymagań technicznych wraz z koncepcją techniczną prosząc ponownie oferty.

TERMIN I MIEJSCE SKŁADANIA OFERT:

1. Ofertę należy złożyć w nieprzekraczalnym terminie do dnia 17.09.2020 r.
2. Oferta może być przesłana:
a. za pośrednictwem: poczty, kuriera lub też dostarczona osobiście na adres Zamawiającego tj. Polgrys Sp. z o.o Sp. k. ul. Dominikańska 25; 35-041 Rzeszów lub
b. Za pośrednictwem poczty elektronicznej, na adres: biuro@polgrys.pl
3. Osobą do kontaktu w sprawach związanych z zapytaniem ofertowym jest Pani Małgorzata Chodak – Rzym (tel. 533-070-502; e-mail: m.chodak-rzym@integratorfirm.pl)

WYKAZ FUNKCJONALNOSCI PLATFORMY TELEMEDYCZNEJ

MODUŁ OPIEKI HOLISTYCZNEJ

Aplikacja na urządzenia mobilne urządzenia (np.: tablety, smartfony), umożliwiająca zdalne zgłoszenie przez pacjenta potrzeb i pozwalająca personelowi medycznemu i opiekującemu na komunikacje z pacjentem celem zapewnienia i dokumentowania procesu holistycznej opieki.
Wymagania/funkcjonalności:

- możliwość doboru profilu dla pacjenta i dostępnych dla niego elementów interfejsu komunikacyjnego,
- możliwość ustawienia i dodania profilu opiekuna innego niż opieka profesjonalna [rodzina, sąsiedzi itp] wraz z możliwością konfiguracji obszarów zakresów działań które może lub potrafi wykonać taka osoba (podanie posiłku, karmienie, asystowanie przy czynnościach toalety).
- Optymalizowanie wykorzystania dostępnego i adekwatnego personelu medycznego i osób wspomagających proces opieki w ujęciu hierarchicznym zgłaszanej przez chorych
- dokumentowanie czasu po którym personel/opiekun wyłącza przywołanie - zaznacza, że odebrał wezwanie,
- obsługa różnego typu przywołania (alarm, lekarz, pielęgniarka, opiekun), możliwość przekierowania wezwania,
- kolejkowanie wezwania od różnych pacjentów i automatyzowanie doboru odpowiedniego personelu do typu wezwania - przyspieszenie obsługi pacjenta,
- bieżący dostęp personelu do danych pacjenta oraz informacji przez niego lub opiekunów wprowadzanych (przykładowo o lekach lub posiłkach, czy też danych z ciśnieniomierza lub glukometru) przy łóżku chorego
- dynamicznie modyfikowanie bieżących zadań przypisanych do personelu medycznego lub opiekunów dla uzyskania jak najszybszego rozwiązania zgłaszanego problemu
- wsparcie administracyjne personelu w realizacji zadań,
- weryfikowanie dostępności i lokalizacji (GPS) medyków lub opiekunów, (także pacjenta)
- wspomaganie tworzenia wstępnej wersji raportu dziennej opieki
- tworzenie elektronicznej dokumentacji medycznej procesu pielęgnowania oraz Integracja z systemem HIS dla możliwości dołączenia do historii choroby informacji o prowadzonych czynnościach pielęgnacyjnych,
- możliwość zlecania diet dla pacjentów (na wybrane okresy od-do), z możliwością ich wydruku/ umieszczenia w panelu pacjenta.

- obsługa planu żywienia z adnotacją o podaniu posiłku.
- generowanie zbiorczego zestawienia wystawionych zleceń na żywienie (z użyciem filtrów: pacjent, zlecający, status, data zlecenia od-do) z możliwością ich eksportu do plików CSV i XML.

MODUŁ KONSYLIUM

Aplikacja na urządzenia mobilne urządzenia (np.: tablety, smartfony), umożliwiająca prowadzenie zdalnego konsylium lekarskiego z opcjonalnym udziałem w nim pacjenta
Wymagania/funkcjonalności:

- możliwość udziału w konsylium poprzez Internet,
- zapewnienie dostępu do tych samych danych omawianych w ramach konsylium (zgromadzonych w HIS) w tym samym czasie,
- automatyczna synchronizacja pulpitów wszystkich uczestników konsylium dla eliminacji sytuacji w trakcie rozmowy uczestnicy widzieli adekwatne dane,
- dostęp do danych ograniczony funkcjonalnie (pacjent) lub merytorycznie (specjalista) w zależności od uprawnień,
- możliwość personalizowania profilu wyświetlanych danych przykładowo do specjalizacji Dzięki temu każdy z uczestników będzie mógł patrzeć na te same dane, w tym samym momencie, ale z różnej perspektywy,
- prezentację danych (mogą pochodzić z dowolnie zintegrowanego źródła np.: systemu HIS, PACS lub innych systemów opieki medycznej) na urządzeniach mobilnych przy wykorzystaniu dynamicznych komponentów do prezentacji danych pozwalających na dowolne integrowanie w jednym widoku danych tekstowych, obrazowych oraz wykresów trendowych.
- dokumentowanie decyzji zdalnych w postaci ankiet kończących proces omawianie danego pacjenta, w których uczestnicy spotkania online decydują o dalszej terapii pacjenta (lub jego kwalifikacji) w sposób jawny lub tajny (w zależności od wymagań).
- separację danych medycznych (zgromadzonych w HIS) nie wykorzystywanych w procesie decyzyjnym.
- możliwość udostępniania przygotowanego konsylium przed rzeczywistym terminem dla umożliwienia wcześniejszego przygotowania się zapoznania się lekarza/terapeuty z udostępnionym materiałem źródłowym wraz z możliwością wprowadzania przez niego uwag i notatek opisujących z analizy/ decyzji.
- możliwość prowadzenia i dołączania prywatnych notatek, tylko na potrzeby własnych wystąpień, które następnie mogą być dodawane jako stanowisko do ankiety decyzyjnej np.: jako odrębne zdanie specjalisty.
- możliwość współdzielenia plików i obrazów z dysków lokalnych prezentujących własne analizy porównawcze lub zawierające dodatkową dokumentację udostępnianą przez rodzinę pacjenta (lub pacjenta) w przypadku, gdy jest dopuszczona(y) do udziału w konsylium,
- możliwość wprowadzania i udostępniania offline (w formie wymiany komunikatów tekstowych) informacji oraz załączników plikowych w dowolnym momencie (przed spotkaniem lub po spotkaniu). W tym przypadku nie jest wymagana jednoczesna obecność konsultujących się uczestników, ale korespondencja zostanie im przekazania i archiwizowania
- możliwość nagrywania przebiegu spotkania w celu dokumentowania wyników konsultacji oraz ewidencjowania informacji przekazywanych przez pacjenta lub jego rodzinę
- możliwość powiązania profilu z językiem prezentacji, co pozwala na budowanie międzynarodowych zespołów do pracy z pacjentem przy wykorzystaniu tej samej technologii.
- dostęp do szczegółowych danych na żądanie polegający na tym, że możliwe będzie pozyskanie danych bardziej szczegółowych po odpowiedniej autoryzacji dostępu. Dane takie mogą być udostępniane przez systemu HIS na wyraźne żądanie specjalisty, kontrolowane przez koordynatora konsylium.
- możliwość zmiany profilu w locie pozwalająca na przedstawienie danych danego pacjenta z innej perspektywy w dowolnym momencie. Każdy uprawniony użytkownik będzie mógł przełączyć się na inny profil, by na te same dane spojrzeć z innej perspektywy bez konieczności poszukiwania odpowiednich komponentów oraz bez znajomości lokalizacji tych danych w systemie.

- prowadzenie konsultacji z wykorzystaniem transmisji dźwięku oraz obrazu w sposób szyfrowany, co zapewniać będzie poufność informacji poruszanych w ramach konsylium
- prowadzenie konsultacji jeden do jeden lub jeden – do wielu z możliwością identyfikacji oraz prezentacji osoby referującej w danej chwili
- możliwość prezentacji dokumentów skanowanych np.: dostarczanych przez pacjentów lub ich rodziny przez konsylium, które mogą być również prezentowane w ramach komponentów wizualnych,
- możliwość prezentacji dokumentacji elektronicznej przechowywanej w lokalnych lub centralnych repozytoriach dokumentacji medycznej, dzięki wykorzystaniu technologii REST/SOAP pozwalających na integrację się z usługami centralnymi do ewidencjonowania i udostępniania zgód.
- możliwość integracji z innymi systemami dziedzinowymi np.: modułem opieki pielęgniarskiej gromadzącym dane o przebiegu opieki nad pacjentem lub modułem zleceń lekarskich/badań pozwalających na weryfikację przygotowania pacjenta do terapii/zabiegu/konsylium
- prezentacja wyników badań laboratoryjnych w trybach: tabelarycznym, wykresu, tryb mini wykresu, na którym jest widoczna aktualna wartość wyniku oraz trend ostatnich badań

MODUŁ ANALIZ MEDYCZNYCH

Środowiska prowadzenia prac analitycznych dostępne dla użytkowników przez przeglądarkę internetową, umożliwiające agregowanie i wizualizację wiedzy o procesie leczenia i postępów terapii.
Funkcjonalności:

- Interfejs graficzny typu point-and-click oraz interfejs programistyczny.
- Gotowość do pracy w chmurze, elastyczność i skalowalność zarówno w chmurach publicznych, jak i prywatnych.
- Otwarte środowisko programistyczne i otwarta platforma rozwojowa zawiera interfejsy, które można wykorzystać do włączenia wsparcia analityki do innych istniejących aplikacji (także finansowo księgowej).
- Bezpieczne, skalowalne środowisko z równoczesnym dostępem dla wielu użytkowników.
- Zintegrowane środowisko, łatwe do zarządzania, utrzymania i nadzoru.
- Skalowalna, architektura, która może rosnąć (lub kurczyć się) zgodnie z rzeczywistymi potrzebami, wykorzystująca różnorodne infrastruktury sprzętowe i systemowe.
- Wsparcie eksploracji dużych wolumenów danych, umożliwiające szybkie rozpoznanie wzorców, trendów i dające możliwość do pogłębionej analizy.
- Możliwość tworzenia dedykowanych interaktywnych raportów.
- Możliwość prowadzenia wizualnej analizy danych - eksploracje i modelowanie.
- Dostęp do raportów przez przeglądarkę internetową i urządzenia mobilne.
- Możliwość łatwego podłączania danych z wielu, różnorodnych źródeł (bazy danych, pliki Excel, , …).
- Zarządzanie danymi przez użytkowników biznesowych. Interfejsy eksploracji danych i tworzenia raportów przygotowane dla użytkowników biznesowych bez znajomości języków programowania.
- Przetwarzanie danych w technologii in-memory zapewnia wysoką wydajność i umożliwia eksplorację i raportowanie dużych zbiorów danych w trybie on-line.
- Unifikacja wizualnej eksploracji danych oraz budowy raportów.
- Mechanizm automatycznego podpowiadania najlepszego wykresu prezentującego wybrane dane.
- Mechanizm proponujący przykładowe raporty, wykorzystujący sztuczną inteligencję do wstępnej analizy załadowanych danych.
- Definiowanie miar wyliczanych operujących zarówno na danych detalicznych jak też na danych zagregowanych.
- Użycie w miarach wyliczanych funkcji specyficznych dla czasu: agregacja na poziomie lat, miesięcy, itp. Porównanie z poprzednimi okresami/latami, z równoległymi okresami (np. dany miesiąc do odpowiadającego miesiąca rok wcześniej).

- Definiowanie sposobów agregacji danych: minimum, maksimum, suma, średnia, liczność, liczba unikalnych wystąpień i inne.
- Filtrowanie i ograniczanie danych na poziomie obiektów lub raportów.
- Rankingi na podstawie danych (np. 10 największych/najmniejszych).
- Reguły wyświetlania danych np. kolorujące dane według wybranego kryterium.
- Wyświetlane strony raportu mogą zawierać elementy sterujące służące do dynamicznego filtrowania danych w trakcie oglądania raportu.
- Na raportach mogą być używane obiekty wizualne używane najczęściej do prezentacji wskaźników typu KPI.
- Raporty mogą składać się z wielu sekcji/stron.
- Raporty mogą pokazywać w zbiorczej, wizualnej formie dane prezentowane za pomocą tabel lub różnego rodzaju wykresów i wizualizacji.
- Prezentowane na raportach mapy geograficzne umożliwiają wykorzystanie warstw informacji geograficznej dostępnej w standardzie OpenStreet lub jako serwisy ESRI.
- Możliwość wykorzystania funkcjonalności drill-down, przechodzenia od ogółu do szczegółów, według zdefiniowanych hierarchii drążenia danych. Funkcjonalność taka dostępna jest zarówno dla danych prezentowanych na tabelach, jak również na wykresach.
- W raportach mogą być wykorzystane wyróżnienia warunkowe pozwalające na graficzne uwidocznienie przekroczenia zadanych progów wartości.
- Możliwa jest zmiana typu wykresu w trakcie pracy nad budową raportu.
- Integracja zaawansowanych metod analitycznych prezentujących związki w danych
    - rozkłady danych i regresje linowe, kwadratowe, sześcienne,
    - macierze korelacji między zmiennymi,
    - metody drzew decyzyjnych,
- Integracja metod prognozowania szeregów czasowych
    - wybór najlepszej metody prognozowania w zależności od danych,
    - prezentacja wartości prognozowanych oraz przedziałów ufności,
    - użycie zmiennych niezależnych do poprawy jakości prognozy,
    - możliwość wykonywania analiz what-if obrazujących modyfikacje wartości zmiennych niezależnych.
- Prezentacja związków w danych w postaci diagramów sieciowych.
- Prognozowanie przychodów i kosztów na bazie szeregów czasowych - lepsza jakość wyników prognoz oznacza podejmowanie lepszych decyzji i zwiększenie efektywności.

MODUŁ HIS

System informatyczny do archiwizacji, przetwarzania i udostępniania danych związanych z realizacją procesu diagnostyczno-terapeutycznego. Moduł służący do zarządzania medycznymi, administracyjnymi, finansowymi i prawnymi aspektami funkcjonowania szpitala

Moduł powinien posiadać minimum funkcjonalności:

- Funkcjonalność automatycznego zapisywania generowanych dokumentów w wersji elektronicznej oraz zapamiętywania wszelkich zmian dokonywanych na tych dokumentach wraz kolejnym wydrukiem (wersjonowanie).
- Zapis wszystkich wydruków w formacie PDF w odpowiedniej wersji wraz z informacją o metadanych (tj. data i godzina powstania wersji, dane pacjenta, kiedy nastąpił wydruk, kto go wykonał oraz z jakiego powodu dokonano kolejnego wydruku).
- Możliwość przechowywania skanów lub filmów.
- Możliwość podglądu każdej z wersji wydruku i sprawdzenia poprzednich i kolejnych wersji dokumentu pod kątem zawartości.

Dla każdego dokumentu papierowego lub elektronicznego możliwość określenia:
- Powiązania z pacjentem,
- Miejsca wytworzenia,
- Typu dokumentu,
- Okresu i miejsca przechowywania,
- Rodzaju medium,
- Oryginał/kopia.

- Funkcjonalność pozwala na podpisywanie każdego dokumentu PDF podpisem elektronicznym.
- Na ekranie startowym aplikacji wyświetlana jest informacja o liczbie dokumentów wymagających podpisu. Po wywołaniu funkcji prezentującej użytkownikowi listę dokumentów do podpisania (które są powiązane z rolą do podpisu zalogowanego użytkownika) system prezentuje informację o tym, ile osób dokonało podpisu każdego dokumentu. Użytkownik ma możliwość wyszukiwania dokumentów po oddziale/poradni, pacjencie lub po opisie oraz możliwość podglądu wybranego dokumentu, jego podpisania lub odmowy podpisania (z podaniem przyczyny).
- Możliwe jest podpisanie/odmowa podpisania zbiorczo grupy dokumentów.
- Walidacja powiązania loginu zalogowanego do systemu użytkownika ze słownikiem personelu - użytkownikowi nie powiązanemu z personelem nie będzie udostępniana lista dokumentów wymagających podpisu.
- Funkcjonalność poglądu dokumentów niepodpisanych (dostępna dla użytkowników z prawami administratora) - na liście są wyświetlone dokumenty, które wymagają podpisu lub mają wprowadzoną odmowe podpisu. Użytkownik ma możliwość sortowania zawartości okna wg filtrów: wszystkie, niepodpisane, odmowa podpisu wraz z opcją tylko najnowsza wersja.
- Dla wskazanego dokumentu możliwość wyświetlenia informacji o pacjencie, dla którego został wygenerowany dokument, miejscu wytworzenia dokumentu, rodzaju dokumentu, informacji o tym, czy dokument został dodany w formie elektronicznej, dacie wytworzenia dokumentu, statusie podpisania.
- Dla wskazanego dokumentu możliwość wyświetlenia informacji o operacjach wykonanych dotychczas na tym dokumencie.
- Możliwość przeglądania wszystkich wersji wskazanego dokumentu.
- Możliwość przypisania ról w module EDM dla pracownika. Poprzez role można definiować listę osób, których podpis elektroniczny jest wymagany na danym dokumencie, oraz kolejność składania tych podpisów. Role mogą mieć zastosowanie ogólne lub oddziałowe z możliwością wskazania zastępstwa (dla roli ogólnej można wybrać dowolnego pracownika istniejącego w systemie, dla roli typu oddział wybór z listy podjednostek dostępnych we wskazanej jednostce).
- Możliwość przypisania ról EDM do wydruków: dla włączonej opcji generacji dokumentacji w formie elektronicznej użytkownik nie będzie posiadał możliwości wyboru opcji fizycznego wydruku dokumentacji, natomiast przy wyłączonej opcji generowania dokumentacji medycznej użytkownik ma możliwość wskazania domyślnej drukarki, opcji wyboru drukarki, wskazania ilości wydruku kopii oraz generowania okna podglądu wydruku.
- Możliwość zdefiniowania słowników dokumentów medycznych.
- Automatyczny druk dokumentu PDF podczas wydruków: karty informacyjnej, wypisu (z przypisaniem wydruku do historii choroby).
- Możliwość wymuszenia na użytkowniku każdorazowo podawania przyczyny zmiany lub ponownego wydruku wersji dokumentu.
- Adnotacja o osobie wypożyczającej wydającej dokumentacje medyczne.
- Możliwość ewidencjonowania pozycji archiwum papierowego.
- Możliwość ewidencjonowania zdarzeń na pozycjach archiwum.
- Możliwość wydrukowania potwierdzenia wykonanej operacji na pozycji archiwum (potwierdzenie wypożyczenia, potwierdzenie przeniesienia itd.).
- Możliwość drukowania potwierdzeń zbiorczych.

Możliwość nadania statusu dokumentacji medycznej:
- Wypożyczenie,

• Zwrot,
• Zniszczenie,
• Zagubienie,
• Odnalezienie,
• Utworzenie kopii,
• Planowe zniszczenie,
• Odmowa udostępnienia,
• Przeniesienie do Archiwum.

Możliwość wyszukiwania dokumentacji z użyciem filtrów:
• Nazwisko pacjenta,
• PESEL pacjenta,
• Data i miejsce wytworzenia dokumentu,
• Okres i miejsce przechowywania,
• Data przyjęcia do archiwum,
• Status dokumentacji,
• Typ i rodzaj dokumentu,
• Termin zwrotu (przekroczony/nieprzekroczony),
• Identyfikator pacjenta, jednostki organizacyjnej, twórcy dokumentu,
• Nazwisko i/lub nr prawa wykonywania zawodu osoby dokonującej wpisu,
• Kod i/lub nazwa usługi,
• Kod chorobowy ICD10.

- System ma możliwość zarządzania obiegiem elektronicznej dokumentacji medycznej w zakresie:

• definiowania ról do użytkowników (np. lekarz, ordynator, pielęgniarka, anestezjolog) z podziałem na komórki organizacyjne lub w ramach całego podmiotu,
• definiowania wymagalności podpisywania elektronicznych dokumentów przez określone role użytkowników (wymagane role oraz kolejność podpisywania/akceptowania dokumentu),
• system prezentuje użytkownikowi listę dokumentów które muszą być przez niego elektronicznie podpisane/zatwierdzone,
• system daje możliwość wprowadzenia odmowy podpisania dokumentu przez użytkownika z adnotacją o przyczynach odmowy,
• system kontroluje, czy wszystkie wymagane role/użytkownicy podpisali się na danym dokumencie,
• system ma możliwość kontroli wersjonowania dokumentu.

- Informacja o lekarzu prowadzącym oraz operatorze na oknach z listami dokumentów do podpisu.
- Jeżeli dokument został opatrzony podpisem elektronicznym, system może wyświetlić komunikat z informacją o użytkowniku podpisującym oraz czasie wykonania podpisu.
- W przypadku dokumentów wielostronicowych system wyświetla informację o tym, na której stronie z ilu stron dokumentu ogółem znajduje się użytkownik.
- Dla każdego szablonu dokumentu system umożliwia ustawienie parametru wyłączenia z EDM – dokument nie zostanie odłożony do archiwum dokumentacji, zostanie od razu przesłany do wydruku na drukarkę.
- Na oknie zamówienia w księdze archiwum EDM możliwość wygenerowania spisu treści dla dodanych dokumentów. Spis treści zostanie wygenerowany po wskazaniu dokumentów.
- Możliwość zbiorczego wydruku dokumentów wprowadzonych w zamówieniu na wypożyczenie. System wygeneruje kolejno wszystkie wydruki wskazane w zamówieniu. Jeżeli brak dokumentu w lokalizacji, która została wskazana jako miejsce składowania dokumentacji EDM, system wyświetli komunikat o braku pliku.
- Możliwość czasowej dezaktywacji roli użytkownika oraz wskazania zastępstwa (dla roli ogólnej można wybrać dowolnego pracownika w systemie, dla roli oddziałowej - do wyboru z podjednostek dostępnych we wskazanej jednostce).
- Przy każdej pozycji wersji dokumentu jest wyświetlona informacja o tym, czy dokument został podpisany, czy też nastąpiła odmowa podpisu. Wyświetlany jest również login użytkownika

generującego dokument, a w przypadku odmowy podpisu - informacja o loginie użytkownika, który wprowadził odmowę podpisu.

- Możliwość pobrania dokumentacji elektronicznej w celu jej udostępnienia pacjentowi.
- Na oknie z listą dokumentów do podpisu wyświetlanie zawartości okna od najnowszych dokumentów oraz filtrowanie po dacie wytworzenia: wszystkie, dzisiaj, wczoraj, przedwczoraj, wcześniejsze.
- Możliwość dołączenia pliku XML z szablonu P1 podczas ręcznego dodawania plików do EDM.
- Możliwość dodawania przez pacjenta dokumentów nie związanych z historią choroby.
- Funkcjonalność umożliwiającą udostępnianie wskazanych dokumentów danego partnera. System pozwala na przypisanie partnera do pacjenta i udostępnianie partnerowi dostępu do danego dokumentu pacjenta:

• automatycznie – po wygenerowaniu dokumentu, zostanie od umieszczony w repozytorium dokumentacji medycznej i automatycznie zostanie powiązany z partnerem lub partnerami wskazanymi w danych pacjenta;
• jako funkcja wywołana na żądanie użytkownika. Po wygenerowaniu dostępu bądź zapisaniu informacji o dokumencie, dany dokument będzie widoczny na koncie www dla danego partnera.

- W przypadku, gdy dokument został załączony bezpośrednio przez jednego z pracowników partnera z poziomu platformy www, zostanie on automatycznie powiązany z danym partnerem, a jako uwaga do powiązania zostanie wprowadzona informacja wskazująca, że dokument został załączony przez pracownika jednostki partnerskiej.
- Filtr dający możliwość wyświetlenia wszystkich dokumentów lub takich, które zostały lub nie zostały podpisane, dokumentów widocznych z poziomu www, dokumentów powiązanych/niepowiązanych z partnerem oraz dokumentów, które zostały udostępnione wprowadzonemu partnerowi.
- Wykorzystanie słowników zarówno standardowych (ICD-10, ICD-9 CM, Słownik Kodów Terytorialnych GUS, słownik trybów przyjęcia, słownik powodów przyjęcia dla pacjentów kolejkowych, słownik płatników i instytucji zewnętrznych itp.), jak i wewnątrzzakładowych (np. ostrzeżeń o wykorzystaniu danego produktu w jednostce w określonym czasie itp.).
- Definiowanie i obsługa ksiąg wykorzystywanych w zakładzie (księga główna, księga odmów, księgi oddziałowe, księga oczekujących itp.).
- Obsługa systemu e-WUŚ - konfiguracja umożliwiająca co najmniej dwukrotną weryfikację uprawnień pacjentów hurtowo o ustalonych, zapisanych w harmonogramie godzinach.
- System umożliwia automatyczne przypisanie procedur ICD9 po otrzymaniu wyniku badania laboratoryjnego za pomocą protokołu HL7.
- System umożliwia automatyczne dodawanie procedur po ręcznym wpisaniu wyniku badania.
- Menadżer wydruków, umożliwiający tworzenie nowych wydruków i dostosowywanie istniejących wydruków do potrzeb placówki (użytkownik może wzorcowy dokument dostosować do swoich potrzeb, zmieniając np. jego format, orientację, rodzaj czcionki, dodając własne logo, dodając dodatkowe dane z bazy danych bądź usuwając informacje zbędne).
- Obsługa wydruków w formacie ODT.
- System e-usług działa na tej samej bazie danych co system obsługi pacjenta i obiegu dokumentacji medycznej EDM. System e-usług jest zintegrowany z repozytorium Elektronicznej Dokumentacji Medycznej (EDM).
- System jest zgodny z normami dotyczącymi służby zdrowia:

• ISO/IEC 27002 - norma określająca wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji,
• PN-ISO/IEC 20000-1 Technika informatyczna - Zarządzanie usługami - Część 1: Wymagania dla systemu zarządzania usługami,
• PN ISO/IEC 27001 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania,
• PN-ISO/IEC 27005 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji.

- System posiada moduł HL7 pozwalający na łatwe dołączanie do niego zewnętrznych systemów teleinformatycznych niezależnie od ich producenta.
- System spełnia zasady interoperacyjnego współdziałania na trzech poziomach: semantycznym, organizacyjnym oraz technologicznym zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 poz. 526, z późn. zm.).
- System jest przystosowany do uruchomienia na platformie wirtualizacyjnej w chmurze prywatnej.
- System ma możliwość pracy użytkowej przez 24 godziny na dobę, 7 dni w tygodniu, wszystkie dni w roku.

Wdrażany system posiada dwa środowiska:
• środowisko produkcyjne,
• środowisko testowo-szkoleniowe.

- Środowisko produkcyjne przeznaczone jest do eksploatacji produkcyjnej Systemu, a środowisko testowo-szkoleniowe dla prowadzenia testów poprawek programowych oprogramowania przed jego instalacją w środowisku produkcyjnym, a także do prowadzenia szkoleń Użytkowników systemu.
- System umożliwia tworzenie, archiwizowanie oraz udostępnianie elektronicznej dokumentacji medycznej wg zasad określonych w ustawie o z dnia 28 kwietnia 2011r. o systemie informacji w ochronie zdrowia (Dz. U. 2011 nr 113 poz. 657, z późn. zm.).
- System umożliwia integrację z platformami P1 i P2.
- System może być zintegrowany z systemami specjalistycznymi RIS/PACS i LIS, eksploatowanymi u Zamawiającego z wykorzystaniem protokołu HL7.
- System umożliwia tworzenie elektronicznych dokumentów medycznych oraz prowadzenie rejestru świadczeń opieki zdrowotnej, o którym mowa w Rozporządzeniu Ministra Zdrowia z dnia 20 czerwca 2008r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych według standardów i zgodnie z formatami określonymi w Rozporządzeniu Ministra Zdrowia w sprawie rodzajów Elektronicznej Dokumentacji Medycznej z dnia 8 maja 2018 r. (Dz.U. z 2018 r. poz. 941) oraz dokumentach opublikowanych przez Centrum Systemów Informacyjnych Ochrony Zdrowia.
- System może generować dokumenty medyczne w standardzie PDF.
- System umożliwia przesłanie do P1 informacji o trzech obszarach:

• informacja o zdarzeniu medycznym, tzw. ExtPLHealthcareEvent,
• indeksy dokumentów medycznych wytworzonych w ramach tego zdarzenia, tzw. XDSDocumentEntry,
• informacja o bieżącym komunikacie, tzw. XDSSubmissionSet.

- System w zakresie gromadzenia i udostępniania, za pośrednictwem P1, informacji o zdarzeniach medycznych oraz wytworzonej podczas zdarzenia medycznego elektronicznej dokumentacji medycznej, powinien posiadać następujące grupy funkcjonalne:

• dodawania i edycji danych medycznych,
• importu/migracji danych zewnętrznych,
• tworzenia dokumentacji medycznej,
• autoryzacji,
• wersjonowania,
• archiwizacji,
• uprawnień,
• dostępu.

- System działa w architekturze klient - serwer, w której baza danych znajduje się na serwerze centralnym obsługującym zarządzanie i przetwarzanie danych. Poszczególne aplikacje pracując na stacjach roboczych otrzymują z serwera wyniki obliczeń jednak również same mogą wykonywać indywidualne zadania lub obliczenia w ramach Systemu nie angażując serwera.

- System posiada narzędzia umożliwiające tworzenie raportów o odbytych wizytach i zrealizowanych usługach medycznych dla pacjentów.
- System posiada możliwość zdalnego połączenia się przez uprawnionych użytkowników z każdym komputerem pracującym w ramach Systemu.
- System posiada mechanizmy umożliwiające przeprowadzenie centralnej aktualizacji oprogramowania, zarówno w środowisku produkcyjnym jak i testowo-szkoleniowym, bez konieczności ręcznej aktualizacji na każdej stacji roboczej i tablecie z osobna.
- System działa i udostępnia wszystkie wymagane funkcjonalności na infrastrukturze sprzętowej przeznaczonej na potrzebę budowy systemu.
- System posiada mechanizmy umożliwiające użycie bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73) lub podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Powyższe dotyczy:

• elektronicznej dokumentacji medycznej,
• elektronicznej dokumentacji medycznej lub danych z tych dokumentów, w zakresie niezbędnym do wykonywania badań diagnostycznych, zapewnienia ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze, środki spożywcze specjalnego przeznaczenia żywieniowego i wyroby medyczne,

- System spełnia wymagania bezpieczeństwa na poziomie wysokim opisanym w Załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
- System informatyczny posiada zaimplementowane mechanizmy kontroli dostępu do danych.
- W Systemie jest rejestrowany odrębny identyfikator dla każdego użytkownika, przy czym nie jest dopuszczalna sytuacja, w której którykolwiek z podsystemów wymaga od użytkownika logowania się innym identyfikatorem, niż ten, który dla tego użytkownika jest zdefiniowany w systemie HIS Zamawiającego.
- System posiada spójny i zaawansowany mechanizm kontroli dostępu. Dostęp do danych w Systemie jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
- System wymusza zmianę hasła nie rzadziej, niż co 30 dni, a hasło musi składać się co najmniej z 8 znaków i zawierać: małe i wielkie litery oraz cyfry lub znaki specjalne.
- System posiada funkcjonalność automatycznego wylogowania się z aplikacji po określonym czasie nieaktywności użytkownika.
- System posiada ochronę przed zagrożeniami pochodzącymi z sieci publicznej opartą na fizycznych lub logicznych zabezpieczeniach chroniących przed nieuprawnionym dostępem.
- System jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
- System posiada mechanizmy backupu oraz archiwizacji danych.
- System umożliwia ograniczenie dostępu do danych, funkcji systemu, procesów systemowych stosownie do danego stanowiska pracy, tj. według zasady w systemie widzę tylko to co muszę, aby wypełniać swoje obowiązki.
- System tworzy i utrzymuje log systemowy współdzielony przez wszystkie moduły i podsystemy, w którym składowane są informacje (data i godzina z dokładnością do sekundy, adres IP stacji, unikalny identyfikator użytkownika, a jeżeli dane w systemie uległy zmianie, to również informacje o tym, z jakiej wartości i na jaką wartość została dokonana zmiana), rejestrujący w szczególności:

• zapisy o zalogowaniu do systemu i wylogowaniu z systemu każdego z użytkowników,
• zmianę parametrów konta każdego użytkownika, w szczególności zmianę uprawnień użytkownika,

• każdą inną zmianę danych zgromadzonych w systemie i dopisanie nowych danych do systemu (wartość początkowa danych powinna być wówczas pusta).

- System posiada mechanizm umożliwiający przeglądanie danych o logowaniu użytkowników do Systemu pozwalający na uzyskanie informacji o czasie i miejscach ich pracy, tj. kto, od kiedy do kiedy, w której jednostce organizacyjnej (adres IP, nazwa jednostki organizacyjnej) był zalogowany.
- W systemie może zostać odwzorowana struktura organizacyjna każdej z placówek Zamawiającego.
- System blokuje fizyczne usunięcie wpisu dokonanego w dokumentacji medycznej. Usunięcie wpisu oznacza jedynie jego dezaktywację, tj. przełączanie w tryb nieaktywny od daty i godziny pobranej automatycznie w momencie dezaktywacji. Usunięcia (tj. dezaktywacji) lub modyfikacji wpisu może dokonać osoba dokonująca wpisu lub osoba posiadająca specjalne wyodrębnione uprawnienie do tych operacji. Fakt ten jest odnotowany w Systemie (nie tylko w logu transakcji bazy danych) wraz z zachowaniem historii zmiany to jest: oznaczenia osoby dokonującej zmiany, czasu dokonania zmiany oraz zachowania wersji sprzed dokonania zamiany.
- Wszystkie udostępniane w systemie funkcjonalności użytkownika są w języku polskim.
- W oprogramowaniu systemu pola wymagane (obligatoryjne) są jednoznacznie rozróżnialne (np. inny kolor, kształt).
- W miejscach Interfejsu użytkownika oprogramowania, w których prezentowane są dane w formie tabelarycznej, istnieje możliwość sortowania poszczególnych kolumn po nagłówkach.
- Oprogramowanie systemu umożliwia wyszukiwanie elementów po fragmencie frazy bez uwzględniania wielkości znaków.
- System jest przygotowany do współpracy z czytnikami kodów kreskowych i drukarkami fiskalnymi (obsługiwane są np. niektóre modele Posnet, Novitus, Innova, Elzab).
- System posiada zaimplementowany słownik pocztowych kodów adresowych w powiązaniu z kodami terytorialnymi gminy danego adresu (TERYT).
- System wspiera proces obsługi badań medycyny pracy poprzez możliwość planowania całych zestawów badań/konsultacji, kontrolę wymaganych dokumentów dla poszczególnych typów stanowisk pracy lub zawodów, generowanie wszystkich wymaganych dokumentów z uwzględnieniem specyfiki stanowisk pracy.
- System ma możliwość utrzymania następujących przedmiotowych zbiorów słownikowych przez Administratora:

• płatników, takich jak oddziały NFZ, i umów z nimi zawartych,
• jednostek i lekarzy kierujących,
• katalogów badań,
• kosztów usług medycznych.

- Wszystkie dane słownikowe i rejestry wykorzystywane w podsystemach muszą być spójne z danymi słownikowymi i rejestrami systemu HIS i definiowane w jednym miejscu, którym jest baza danych systemu HIS.
- Proces zarządzania użytkownikami w tym sposób logowania i polityka haseł w modułach są jednolite.
- System posiada funkcjonalność automatycznego dostosowania szerokości kolumn do zawartości danych w kolumnie. Funkcjonalność dostępna jest na wszystkich oknach zawierających wyświetlanie list w kolumnach.
- Możliwość wprowadzania certyfikatów, brak konieczności wprowadzania PIN-u podczas powiązania użytkownika z podpisem dla centralnej aktualizacji.
- System dostosowany jest do obsługi podpisów kwalifikowanych oraz podpisów niekwalifikowanych ePUE dostarczanych przez ZUS (w celu poprawnego działania funkcjonalności Zamawiający winien złożyć wniosek o wygenerowanie klucza w ePUE lub zakup klucza kwalifikowanego).
- Na oknie danych pracownika na zakładce z logiem wyświetlanie informacji o zmianie miejsca pracy logującego się użytkownika.
- Prowadzenie dokumentacji medycznej (jak: karta informacyjna leczenia szpitalnego, karta odmowy przyjęcia do szpitala, informacja pisemna lekarza specjalisty do lekarza kierującego) w formie

elektronicznej zgodnej ze standardem HL7CDA. Dokumenty są generowane w 3 wersjach: PDF, HL7CDA P1 i HL7CDA XML.

- Na wszystkich ekranach zawierających listę badań pacjenta wyświetlanie informacji o tym, czy do danego badania został dołączony plik PDF.

ZAŁOŻENIA TECHNICZNE PROJEKTU INFRASTRUKTURY IT

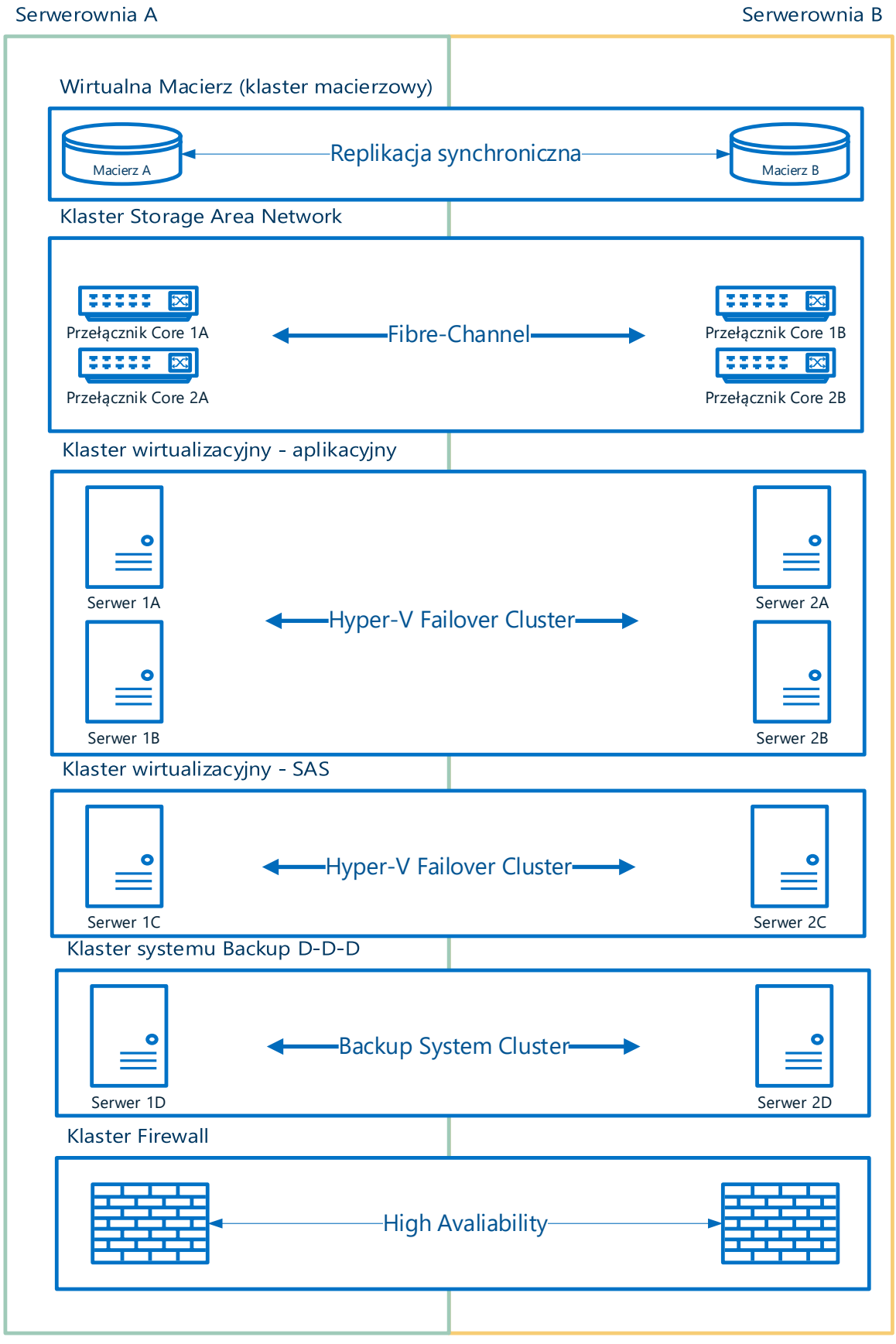
Projekt zakłada utrzymanie pełnej, niezawodnej i funkcjonalnej infrastruktury umożliwiającej świadczenie usług teleinformatycznych i telemedycznych dla odbiorców zewnętrznych. Projekt musi charakteryzować się architekturą wysokiej dostępności w tym w czasie awarii serwera (niezbędna redundancja) i wysokiej wydajności.

ARCHITEKTURA OGÓLNA

ZAŁOŻENIA

Projekt zakłada umieszczenie urządzeń krytycznych tj. macierzy, serwerów, przełączników rdzeniowych i routerów brzegowych w dwóch oddzielnych pomieszczeniach – serwerowniach. Projekt zakłada wielomodowe bezpośrednie połączenie światłowodowe pomiędzy serwerowniami umożliwiając rozszerzenie jednej sieci SAN na dwa pomieszczenia.
Projekt zakłada utworzenie 6 klastrów sprzętowo systemowych o odpowiednim przeznaczeniu opisanym poniżej.

Projekt


Serwerownia A
Serwerownia B
Wirtualna Macierz (klaster macierzowy)
Macierz A
Replikacja synchroniczna
Macierz B
Klaster Storage Area Network
Przełącznik Core 1A
Fibre-Channel
Przełącznik Core 1B
Przełącznik Core 2A
Przełącznik Core 2B
Klaster wirtualizacyjny - aplikacyjny
Serwer 1A
Hyper-V Failover Cluster
Serwer 2A
Serwer 1B
Serwer 2B
Klaster wirtualizacyjny - SAS
Serwer 1C
Hyper-V Failover Cluster
Serwer 2C
Klaster systemu Backup D-D-D
Serwer 1D
Backup System Cluster
Serwer 2D
Klaster Firewall
High Avaliability

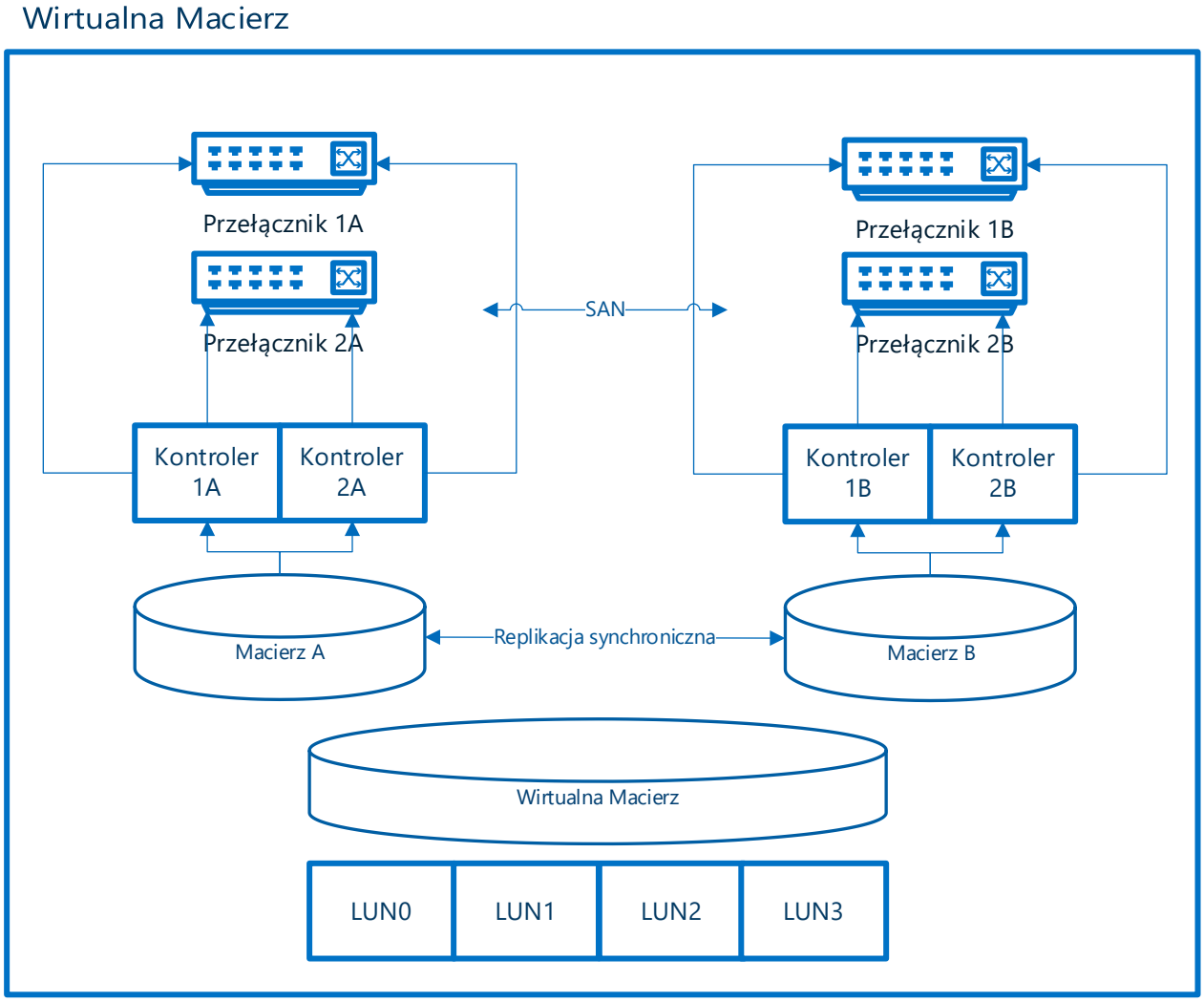
Infrastruktura stacjonarna w ramach projektu charakteryzuje się pełną wysokodostępnością analogicznie jak rozwiązania chmurowe, jednakże w tym przypadku wszystkie dane w tym dane wrażliwe - medyczne są przetwarzane w ramach infrastruktury właściciela z pełną kontrolą dostępu i zabezpieczeń architektury.
Projekt zakłada użycie wysokiej klasy oprogramowania analitycznego, którego używanie w ramach środowiska Cloud lub VPS nie jest rozwiązaniem ekonomicznym ze względu na wysokie wymagania uruchomieniowe RAM oraz CPU a w przełożeniu na comiesięczne koszta - jest to nieopłacalne.
Przy użyciu lokalnej infrastruktury według założeń następuje długofalowa amortyzacja finansowa środków, gdzie nawet po czasie trwania projektu (2-3) lata infrastktura będzie funkcjonować bez dodatkowych kosztów utrzymania (prócz zasobów energetycznych).
Użyte technologie w rozwiązaniu, w tym głównie technologie sprzętowe pozwalają na wykorzystanie pełnego potencjału sprzętu i zwiększenie wydajności rozwiązań aplikacyjnych.
Dostosowane rozwiązanie sprzętowe w lokalizacji klienta pozwala na pełen dostęp do usług z wewnątrz lokalizacji/budynku nawet w przypadku awarii dostawcy Internetu. Realizacja w obrębie jednej lokalizacij pozwala także na wysokowydajny dostęp stacji lokalnych do systemu za pomocą technologii aplikacji klienckich bez chmurowej wirtualizacji i transferu np. ruchu wideo, który obecnie jest bardzo problematycznym rozwiązaniem w przypadku wirtualizacji desktopów w chmurze.

WIRTUALNA MACIERZ

ZAŁOŻENIA

Projekt zakłada utworzenie wirtualnej macierzy na podstawie dwóch fizycznych macierz, dobór technologiczny umożliwi utworzenie pojedynczych elementów LUN równolegle synchronizowanych w czasie rzeczywistym. W przypadku awarii jednej macierzy / jednego punktu dystrybucyjnego (serwerowni) praca nie zostanie zatrzymana. Kolejno podczas uruchomienia punktu / macierzy która została wyłączona – urządzenie samo uaktualni zasoby.
Macierz odpowiednio posiada dwa niezależne kontrolery, a każdy kontroler podłączony jest do oddzielnego przełącznika rdzeniowego.

Projekt

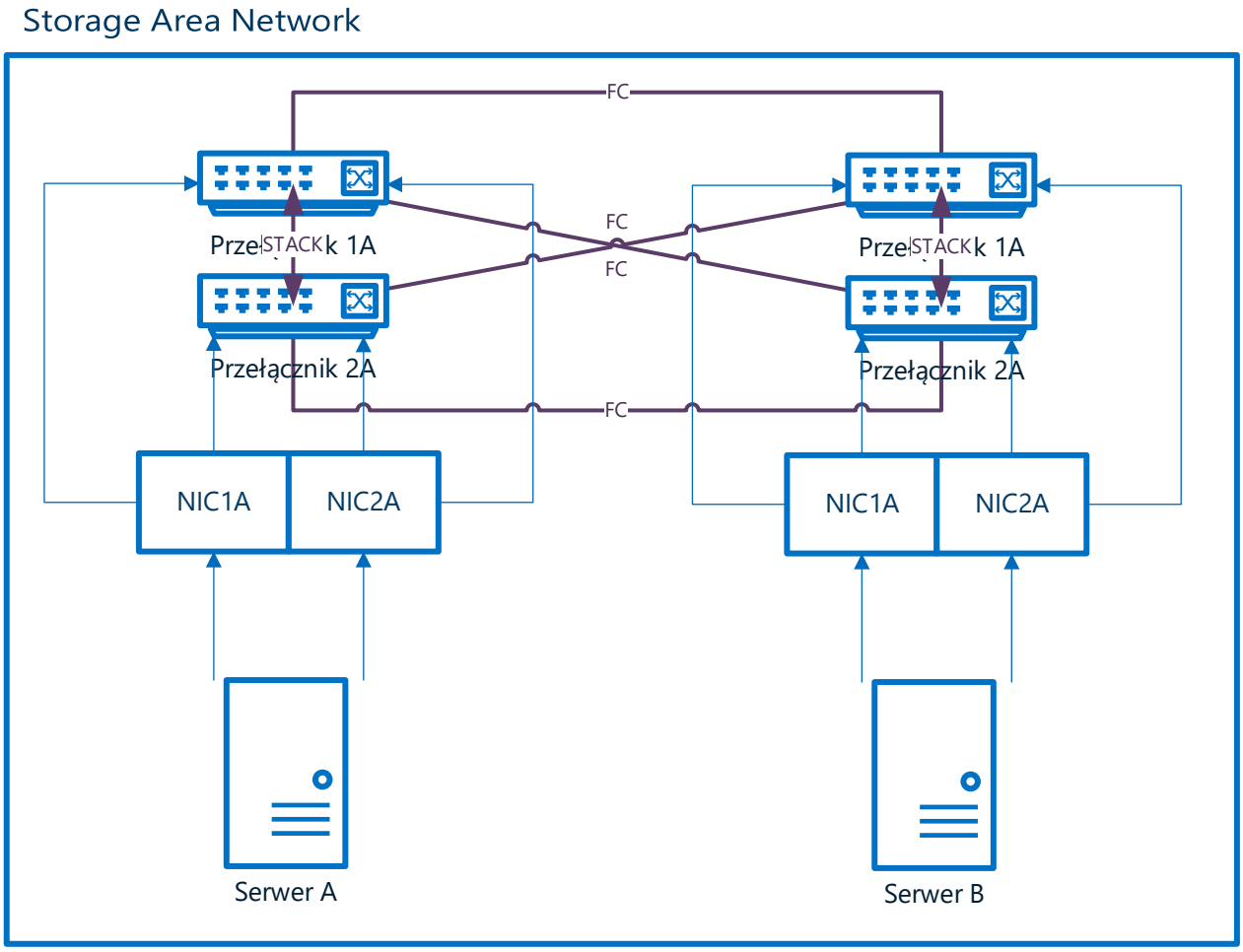


KLASTER STORAGE AREA NETWORK

ZAŁOŻENIA

Sieć rdzeniowa typu SAN powinna zapewniać wysoką dostępność i bezawaryjność, w przypadku awarii albo pojedynczego urządzenia, lub połączenia pomiędzy pomieszczeniami praca powinna pozostać w trybie ciągłym. Realizacja połączeń do macierzy, serwerów oparta powinna być na połączenia sparowane typu LAG (Linka Aggregation), tym samym zwiększając przepustowość i umożliwiając pracę w wysokiej dostępności.

Projekt

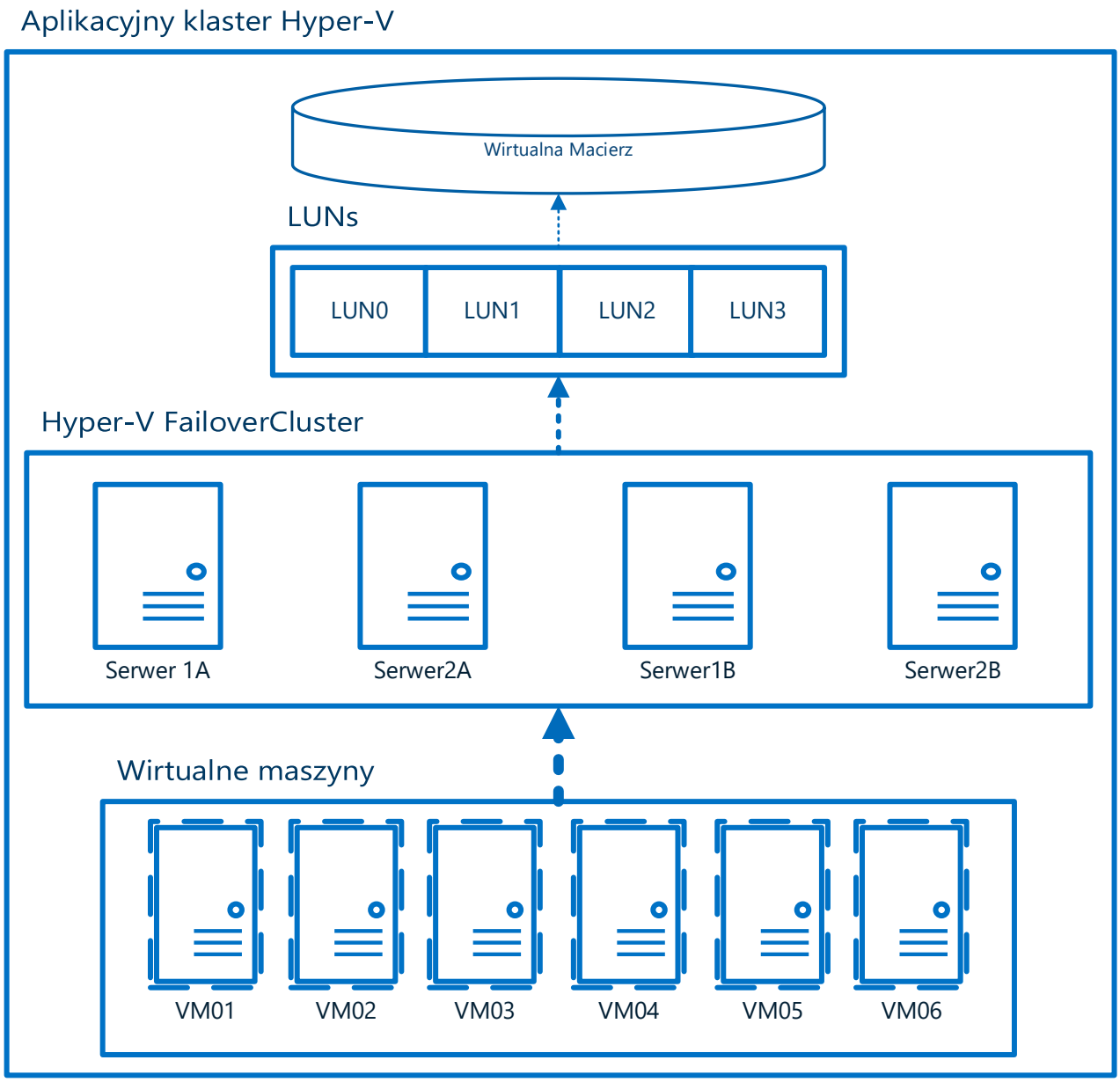


KLASTER WIRTUALIZACYJNY - APLIKACYJNY

ZAŁOŻENIA

Klaster wirtualizacyjny dedykowany dla wirtualnych serwerów związanych z infrastrukturą oraz usługami zostanie zrealizowany w obrębie czterech serwów – po dwa na każdy punkt przetwarzania (serwerownie). Wirtualna maszyna ma prawo do migracji i pracy na każdym z dostępnych serwerów. W przypadku awarii węzła, bądź maszyny fizycznej – wirtualna maszyna przechodzi na inną dostępną.

Projekt

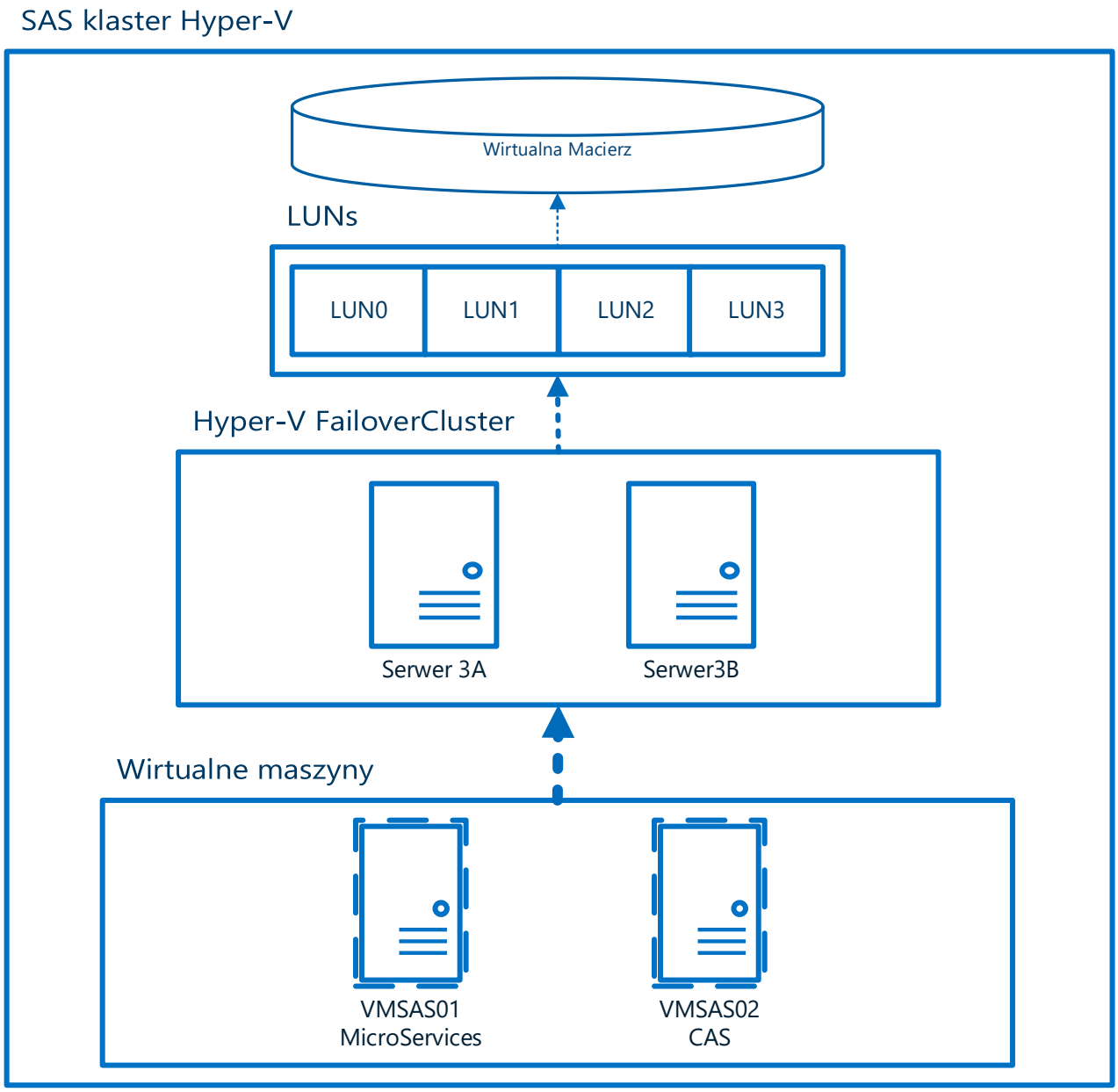


KLASTER WIRTUALIZACYJNY – ŚRODOWISKO ANALITYCZNE

ZAŁOŻENIA

Środowisko analityczne wykonuje skomplikowane wyliczenia i korzysta z dużej ilości RAM, zaleca się aby maszyny pracujące w obrębie klastra środkowiska funkcjonowały oddzielnie niż inne serwery aplikacji. Analogicznie jak poprzedni klaster – w przypadku uszkodzenia węzła, bądź maszyny fizycznej maszyna wirtualna pozostanie pracująca

Projekt

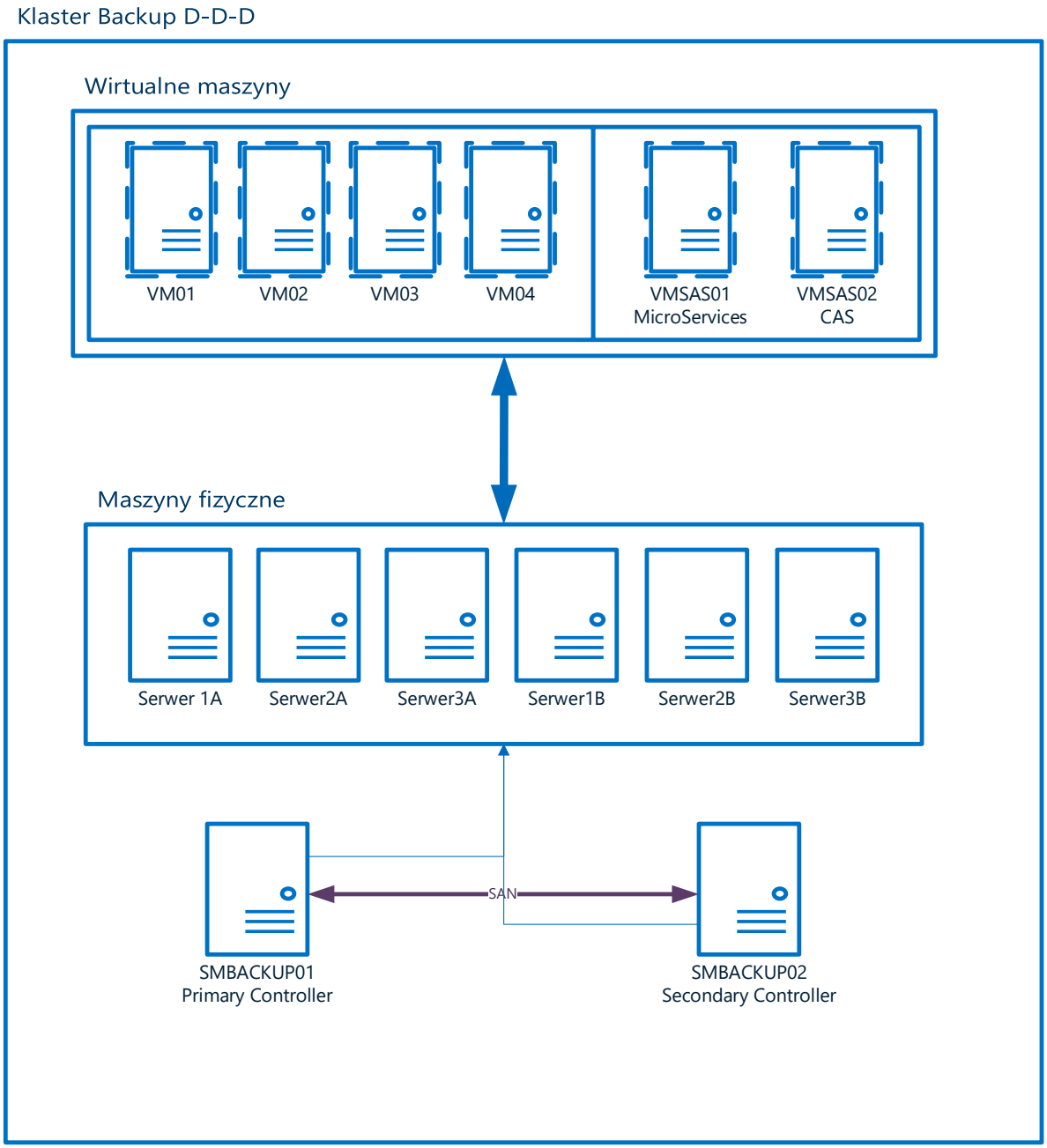


KLASTER SYSTEMU BACKUP D-D-D

ZAŁOŻENIA

Rozwiązanie zakłada system tworzenia kopii zapasowych postaci Disk to Disk to Disk, tak, że zapis danych odbywa się w dwóch lokalizacjach, a odtworzenie danych będzie dostępne nawet w przypadku awarii całego punktu dystrybucyjnego.

Projekt

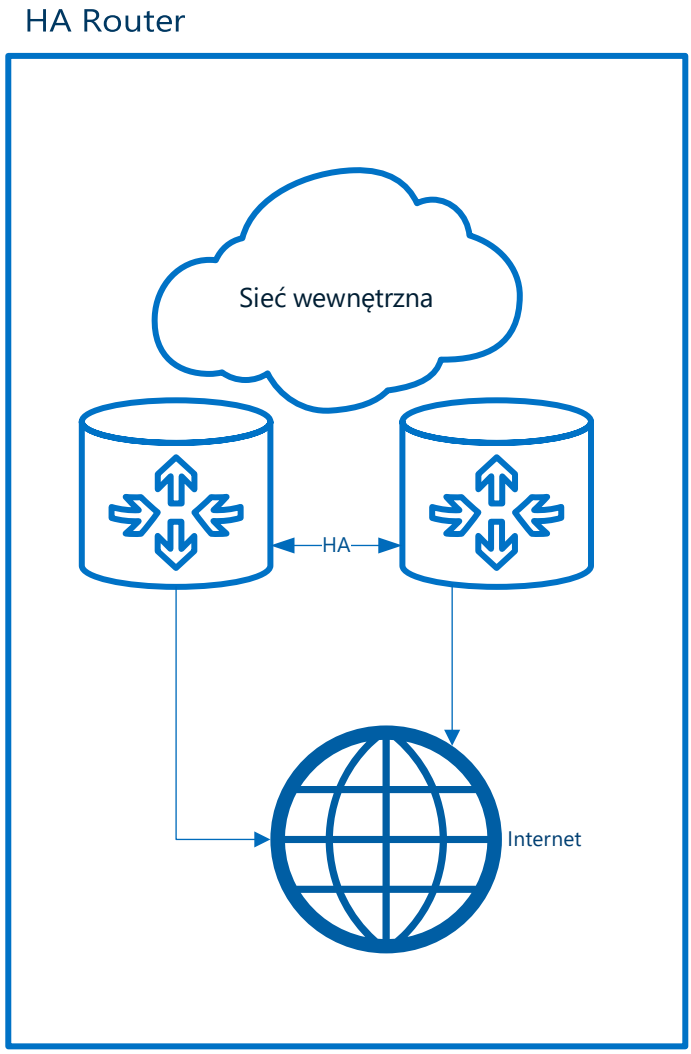


KLASTER FIREWALL

ZAŁOŻENIA

Projekt zakłada redundancje na poziomie routingu sprzętowego, zapory sieciowej oraz usług ochrony. W założeniu ISP (usługodawca internetowy) doprowadza połączenie WAN w LAG do każdej serwerowni celem podtrzymania stabilności usługi dla podmiotów zewnętrznych

Projekt



WYMAGANE PARAMETRY INFRASTRUKTURY IT (W TYM SERWEROWNIA) DLA PLATFORMY TELEMEDYCZNEJ NA PODSTAWIE POWYŻSZEGO PROJEKTU TECHNICZNEGO

- **All In One**

Technologia	All-In-One
Ilośc fizycznych procesorów	1
Minimalne taktowanie procesora	1,6 GHz
Możliwe taktowanie procesora	powyżej 2 GHz
Ilość rdzeni procesora	minimum 4
Ilość wątków procesora	minimum 6
Pojemność dysku	minumum 250 GB
Dopuszczalne technologie dysków	SSD Sata, SSD M.2. , NVMe
Karta sieciowa przewodowa	pracująca w trybie 100/1000 Mbit/s
Karta sieciowa bezprzewodowa	pracująca w standardzie 802.11 ac
Przekątna ekranu	minimum 23"
Rozdzielczość ekranu	minimum 1920 x 1080 px
Pamięć RAM	minimum 8 GB
Typ pamięcie RAM	DDR4
Karta graficzna	zintegrowana
Karta dźwiękowa	zintegrowana
System operacyjny	Windows 10 Professional x64
Wyposażenie dodatkowe w obrębie tej samej obudowy/urządzenia	Kamera internetowa, wbudowany mikrofon, głośniki
Kamera internetowa	o minminalnej rozdzielczości 1280 x 720 px
Bluetooth	tak
Ilość złączy USB 3.*	minimum 2
Dopuszcza się aby dostawca dostarczył licencje systemu operacyjnego do urządzeń oddzielnie	
Nie dopuszcza się aby peryferia postaci bluetooth, karta sieciowa itp. były realizowane za pomocą urządzeń zewnętrznych za pomocą interfejsów USB	

- **Laptop dla rehabilitantów**

Ilośc fizycznych procesorów	1
Minimalne taktowanie procesora	0,9 GHz
Możliwe taktowanie procesora	powyżej 3,5 GHz
Ilość rdzeni procesora	minimum 4
Ilość wątków procesora	minimum 6
Pojemność dysku	minumum 500 GB
Dopuszczalne technologie dysków	SSD Sata, SSD M.2. , NVMe, PCIe
Karta sieciowa	zintegrowana pracująca w trybie 100/1000 Mbit/s
Karta sieciowa bezprzewodowa	pracująca w standardzie 802.11 ax
Przekątna wyświetlacza	14"-14,9"
Rozdzielczość ekranu	minimum 1920 x 1080 px

Pamięć RAM	minimum 8 GB
Matryca	Matowa
Typ pamięcie RAM	DDR4
Karta graficzna	zintegrowana
Karta dźwiękowa	zintegrowana
System operacyjny	Windows 10 Professional x64
Wyposażenie dodatkowe w obrębie tej samej obudowy	Kamera internetowa, wbudowany mikrofon, ekran dotykowy, głośniki
Kamera internetowa	Wbudowana w obudowie
Bluetooth	Tak
Ilość złączy USB 3.* (nie typ C)	minimum 1
Ilość złączy USB-C	minimum 1
HDMI	minimum 1
Waga	Do 2 kg
Obudowa	Aluminiowa
Dopuszcza się aby dostawca dostarczył licencje systemu operacyjnego do urządzeń oddzielnie	
Nie dopuszcza się aby peryferia postaci bluetooth, karta sieciowa itp. były realizowane za pomocą urządzeń zewnętrznych za pomocą interfejsów USB	

- **Laptop dla lekarzy**

Ilośc fizycznych procesorów	1
Minimalne taktowanie procesora	0,9 GHz
Możliwe taktowanie procesora	powyżej 3,5 GHz
Ilość rdzeni procesora	minimum 4
Ilość wątków procesora	minimum 6
Pojemność dysku	minumum 500 GB
Dopuszczalne technologie dysków	SSD Sata, SSD M.2. , NVMe, PCIe
Karta sieciowa	zintegrowana 10/100/1000 Mbit/s
Karta sieciowa bezprzewodowa	pracująca w standardzie 802.11 ax
Przekątna wyświetlacza	15"-15,9"
Rozdzielczość ekranu	minimum 1920 x 1080 px
Pamięć RAM	minimum 8 GB
Typ pamięcie RAM	DDR4
Karta graficzna	zintegrowana
Karta dźwiękowa	zintegrowana
System operacyjny	Windows 10 Professional x64
Wyposażenie dodatkowe w obrębie tej samej obudowy	Kamera internetowa, wbudowany mikrofon, ekran dotykowy, głośniki
Kamera internetowa	Wbudowa w obudowe
Bluetooth	Tak
Ilość złączy USB 3.* (nie typ C)	minimum 1
Ilość złączy USB-C	minimum 1
HDMI	minimum 1
Napęd DVD	Za pomocą peryferium USB
Obudowa	aluminiowa

Matryca	Matowa
Dopuszcza się aby dostawca dostarczył licencje systemu operacyjnego do urządzeń oddzielnie	
Nie dopuszcza się aby peryferia postaci bluetooth, karta sieciowa itp. prócz napędu CD/DVD były realizowane za pomocą urządzeń zewnętrznych za pomocą interfejsów USB	

- **Serwer infrastruktury Microsoft**

Procesor:	
Ilosć procesorów	2
Minimalne taktowanie procesora	3.1 GHz
Ilość rdzeni procesora	8
Ilość wątków procesora	16
Minimalny Cache procesora	10 MB
Następujące wsparcie technologi procesora:	
Intel® Deep Learning Boost (Intel® DL Boost)	Tak
Technologia Intel® Resource Director (Intel® RDT)	Tak
Technologia Intel® Speed Shift	Tak
Technologia Intel® Turbo Boost	W wersji 2.0
Intel® vPro™ — kryteria kwalifikowalności platformy	Tak
Technologia Intel® Hyper-Threading	Tak
Technologia Intel® Virtualization (VT-x)	Tak
Technologia Intel® Virtualization for Directed I/O (VT-d)	Tak
Technologia Intel® VT-x with Extended Page Tables (EPT)	Tak
Intel® TSX-NI	Tak
Intel® 64	Tak
Udoskonalona technologia Intel SpeedStep®	Tak
Intel® Volume Management Device (VMD)	Tak
Pamięć:	
Rodzaj pamięci RAM	DDR4
Wielkośc pamięci RAM	256 GB
Ilość dysków twardych	2
Rodzaj dysków twardych	SSD
Wielkość jednego dysku twardego	240 GB
Kontrolery	
RAID	obsługujący RAID 0,1,10, no-cache
Komunikacja	
Ilość portów 10 GE SFP+	4
Ilośc portów 1 GE	2
Zasilanie	
Ilość zasilaczy	2
Chasis	
Rozmiar serwera	1U
Wymiar Chasis	8 * 2,5"
Wymagana certyfikacja	CE, UL, FCC, CCC, RHoS

- **Serwer infrastruktury do zarządzania**

Procesor:	
Ilosć procesorów	2
Minimalne taktowanie procesora	3.1 GHz
Ilość rdzeni procesora	8
Ilość wątków procesora	16
Minimalny Cache procesora	10 MB
Następujące wsparcie technologi procesora:	
Intel® Deep Learning Boost (Intel® DL Boost)	Tak
Technologia Intel® Resource Director (Intel® RDT)	Tak
Technologia Intel® Speed Shift	Tak
Technologia Intel® Turbo Boost	W wersji 2.0
Intel® vPro™ — kryteria kwalifikowalności platformy	Tak
Technologia Intel® Hyper-Threading	Tak
Technologia Intel® Virtualization (VT-x)	Tak
Technologia Intel® Virtualization for Directed I/O (VT-d)	Tak
Technologia Intel® VT-x with Extended Page Tables (EPT)	Tak
Intel® TSX-NI	Tak
Intel® 64	Tak
Udoskonalona technologia Intel SpeedStep®	Tak
Intel® Volume Management Device (VMD)	Tak
Pamięć:	
Rodzaj pamięci RAM	DDR4
Wielkosc pamięci RAM	256 GB
Ilość dysków twardych	2
Rodzaj dysków twardych	SSD
Wielkość jednego dysku twardego	240 GB
Kontrolery	
RAID	obsługujący RAID 0,1,10, no-cache
Komunikacja	
Ilość portów 10 GE SFP+	4
Ilosc portów 1 GE	2
Zasilanie	
Ilość zasilaczy	2
Chasis	
Rozmiar serwera	1U
Wymiar Chasis	8 * 2,5"
Wymagana certyfikacja	CE, UL, FCC, CCC, RHoS

- **Serwer do analityki**

Procesor:	
Ilosć procesorów	2
Minimalne taktowanie procesora	3.1 GHz

Ilość rdzeni procesora	8
Ilość wątków procesora	16
Minimalny Cache procesora	10 MB
Następujące wsparcie technologi procesora:	
Intel® Deep Learning Boost (Intel® DL Boost)	Tak
Technologia Intel® Resource Director (Intel® RDT)	Tak
Technologia Intel® Speed Shift	Tak
Technologia Intel® Turbo Boost	W wersji 2.0
Intel® vPro™ — kryteria kwalifikowalności platformy	Tak
Technologia Intel® Hyper-Threading	Tak
Technologia Intel® Virtualization (VT-x)	Tak
Technologia Intel® Virtualization for Directed I/O (VT-d)	Tak
Technologia Intel® VT-x with Extended Page Tables (EPT)	Tak
Intel® TSX-NI	Tak
Intel® 64	Tak
Udoskonalona technologia Intel SpeedStep®	Tak
Intel® Volume Management Device (VMD)	Tak
Pamięć:	
Rodzaj pamięci RAM	DDR4
Wielkośc pamięci RAM	512 GB
Ilość dysków SAS/SATA SSD 960 GB typu ReadIntensive	2
Ilość dysków NVMe 2TB PCIe typu ReadIntensive	2
Kontrolery	
RAID	obsługujący RAID 0,1,10, no-cache
Komunikacja	
Ilość portów 10 GE SFP+	4
Ilośc portów 1 GE	2
Zasilanie	
Ilość zasilaczy	2
Chasis	
Rozmiar serwera	1U
Wymiar Chasis	10 * SAS/SATA, 4 * NVMe
Wymagana certyfikacja	CE, UL, FCC, CCC, RHoS

- **Serwer infrastruktury Backup**

Procesor:	
Ilośc procesorów	1
Minimalne taktowanie procesora	3.1 GHz
Ilość rdzeni procesora	8
Ilość wątków procesora	16
Minimalny Cache procesora	10 MB
Następujące wsparcie technologi procesora:	
Intel® Deep Learning Boost (Intel® DL Boost)	Tak

Technologia Intel® Resource Director (Intel® RDT)	Tak
Technologia Intel® Speed Shift	Tak
Technologia Intel® Turbo Boost	W wersji 2.0
Intel® vPro™ — kryteria kwalifikowalności platformy	Tak
Technologia Intel® Hyper-Threading	Tak
Technologia Intel® Virtualization (VT-x)	Tak
Technologia Intel® Virtualization for Directed I/O (VT-d)	Tak
Technologia Intel® VT-x with Extended Page Tables (EPT)	Tak
Intel® TSX-NI	Tak
Intel® 64	Tak
Udoskonalona technologia Intel SpeedStep®	Tak
Intel® Volume Management Device (VMD)	Tak
Pamięć:	
Rodzaj pamięci RAM	DDR4
Wielkośc pamięci RAM	64 GB
Ilość dysków SAS/SATA HDD 16 TB	4
Kontrolery	
RAID	obsługujący RAID 0,1,10,5,6
Komunikacja	
Ilość portów 10 GE SFP+	2
Ilośc portów 1 GE	2
Zasilanie	
Ilość zasilaczy	2
Chasis	
Rozmiar serwera	1U
Wymiar Chasis	4 * 3,5" SAS/SATA
Wymagana certyfikacja	CE, UL, FCC, CCC, RHoS

- **Macierz dyskowa**

Technologia:	
Pamięć Cache	32 GB
Wspierane protkoły	FC, iSCI, NFS, CIFS, HTTP, FTP
Maksymalna liczba modułów Hot-Swapppable per kontroller	2
Maksymalna liczba dysków przy dwóch kontrolerach	500
Obsługiwane typy dysków	SSD, SAS, NL-SAS
Maksymalna ilość snapshotów (LUN)	2048
Maksymalna ilość LUN	4096
Maksymalna wielkość jednego pliku	256 TB
Maksymalna ilość obsługiwanych kontrolerów	8
Przedział zasilania AC	100V - 240V
Przedział zasilania DC	192V - 288V lub -48 V do -60 V
Dopuszczalna wilgotność powietrza podczas pracy	5% RH do 90% RH
Możliwe rodzaje przednich portów (Front-End)	1/10/25 Gbit/s Ethernet oraz 8/16 /32Gbit/s Fibre Channel

Możliwe rodzaje tylnich portów (Back-End)	SAS 3.0 (każdy port wspierający 4 x 12 Gbit/s)
Zasoby dyskowe per macierz:	
2.4TB 10K RPM SAS	6
1.92TB SSD SAS	5
10TB 7.2K RPM NL-SAS	6
Kontroler per macierz:	
Ilość kontrolerów	2
Ilość zasilaczy per kontroler	2
Ilość portów SFP+ per kontroler (10 Gb Eth/FCoE)	8
Ilość portów zarządzających 1 GbE per kontroler	2
Oprogramowanie:	
Licencja umożliwiająca replikację synchroniczną dwóch macierzy w czasie rzeczywistym	
Licencja umożliwiająca tworzenie cyklicznych snapshotów macierzy	
Informacje dodatkowe	
Macierz umożliwiająca utworzenie sieci SAN	
Dopuszcza się aby macierz posiadała dodatkowe półki dyskowe	
Wsparcie dla hiperwisorów Vmware, XenServer oraz Hyper-V	
Wsparcie dla MultiPathingu	

- **Przełącznik rdzeniowy sieci SAN**

Parametry urządzenia:	
Wydajność przesyłania	490M
Wydajność przełączania2	960 Gb/s / 2,4 Tb/s
Porty stałe	24 x 10 Gig SFP+, 6 x 40 Gig QSFP+
VXLAN	Bramy VXLAN warstwy 2 i 3
	Scentralizowane i rozproszone bramy
	BGP-EVPN
	Skonfigurowany za pomocą protokołu NETCONF
Technologia SVF (Super Virtual Fabric)	FRealizuje działania jako nadrzędny węzeł wirtualizujący pionowo dalsze przełączniki i punkty dostępu do postaci jednego, łatwo zarządzanego urządzena
	Obsługuje dwuwarstwową architekturę klienta
	Obsługuje urządzenia innych firm między rodzicem SVF a klientami
iPCA	Zbiór statystyk w czasie rzeczywistym dotyczących liczby utraconych pakietów i współczynnika utraty pakietów na poziomie sieci i urządzenia
Bezpieczeństwo	Analiza zaszyfrowanej komunikacji (ECA)
	Technologia pułapek na zagrożenia
	Współpraca w zakresie bezpieczeństwa w całej sieci
Współdziałanie	VBST (kompatybilne z PVST, PVST+ oraz RPVST)
	LNP (zbliżony do DTP)
	VCMP (zbliżony do VTP)
Rozmiar	1U
Ilość zasilaczy	2
Ilość wiatraków	4

Właściwości urządzenia, wspierane protokoły	
MAC	Up to 64K MAC address entries
	IEEE 802.1d standards compliance
	MAC address learning and aging
	Static, dynamic, and blackhole MAC address entries
	Packet filtering based on source MAC addresses
VLAN	4K VLANs
	Guest VLANs and voice VLANs
	GVRP
	MUX VLAN
	VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports
	VLAN mapping
ARP	Static ARP
	Dynamic ARP
IP routing	Static routes, RIP v1/2, RIPng, OSPF, OSPFv3, IS-IS, IS-ISv6, BGP, BGP4+, ECMP, routing policy
	Up to 64K FIBv4 entries
	Up to 32K FIBv6 entries
Interoperability	VLAN-Based Spanning Tree (VBST), working with PVST, PVST+, and RPVST
	Link-type Negotiation Protocol (LNP), similar to DTP
	VLAN Central Management Protocol (VCMP), similar to VTP
Ethernet loop protection	RRPP ring topology and RRPP multi-instance
	Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protection switchover
	SEP
	ERPS (G.8032)
	BFD for OSPF, BFD for IS-IS, BFD for VRRP, and BFD for PIM
	STP (IEEE 802.1d), RSTP (IEEE 802.1w), and MSTP (IEEE 802.1s)
	BPDU protection, root protection, and loop protection
IPv6 features	Neighbor Discover (ND)
	PMTU
	IPv6 Ping, IPv6 Tracert, IPv6 Telnet
	ACLs based on source IPv6 addresses, destination IPv6 addresses, Layer 4 ports, or protocol types
Multicast	Listener Discovery snooping (MLDv1/v2)
	IPv6 addresses configured for sub-interfaces, VRRP6, DHCPv6, and L3VPN
	Multicast IGMP v1/v2/v3 snooping and IGMP fast leave
	Multicast forwarding in a VLAN and multicast replication between VLANs
	Multicast load balancing among member ports of a trunk
	Controllable multicast
	Port-based multicast traffic statistics
	IGMP v1/v2/v3, PIM-SM, PIM-DM, and PIM-SSM
	MSDP

	Multicast VPN
QoS/ACL	Rate limiting in the inbound and outbound directions of a port
	Packet redirection
	Port-based traffic policing and two-rate three-color CAR
	Eight queues on each port
	DRR, SP, and DRR+SP queue scheduling algorithms
	WRED
	Re-marking of the 802.1p and DSCP fields of packets
	Packet filtering at Layer 2 to Layer 4, filtering out invalid frames based on the source MAC address, destination MAC address, source IP address, destination IP address, TCP/UDP
	address, destination MAC address, source IP address, destination IP address, TCP/UDP source/destination port number, protocol type, and VLAN ID
	Queue-based rate limiting and shaping on ports
Security	Hierarchical user management and password protection
	DoS attack defense, ARP attack defense, and ICMP attack defense
	Binding of the IP address, MAC address, port number, and VLAN ID
	Port isolation, port security, and sticky MAC
	MAC Forced Forwarding (MFF)
	Blackhole MAC address entries
	Limit on the number of learned MAC addresses
	IEEE 802.1X authentication and limit on the number of users on a port
	AAA authentication, RADIUS authentication, and HWTACACS authentication
	NAC
	SSH V2.0
	HTTPS
	CPU protection
	Blacklist and whitelist
	Attack source tracing and punishment for IPv6 packets such as ND, DHCPv6, and MLD packets
	IPSec for management packet encryption
	ECA
	Deception
Reliability	LACP
	E-Trunk
	Ethernet OAM (IEEE 802.3ah and IEEE 802.1ag)
	ITU-Y.1731
	DLDP
	LLDP
	BFD for BGP, BFD for IS-IS, BFD for OSPF, BFD for static routes
Management and maintenance	Cloud-based management
	Virtual cable test
	SNMP v1/v2/v3

	RMON
	Web-based NMS
	System logs and alarms of different severities
	GVRP
	MUX VLAN
	NetStream
	Telemetry

- **Przełącznik rdzeniowy sieci NET**

Parametry urządzenia:	
Wydajność przesyłania	490M
Wydajność przełączania2	960 Gb/s / 2,4 Tb/s
Porty stałe	24 x 10 Gig SFP+, 6 x 40 Gig QSFP+
VXLAN	Bramy VXLAN warstwy 2 i 3
	Scentralizowane i rozproszone bramy
	BGP-EVPN
	Skonfigurowany za pomocą protokołu NETCONF
Technologia SVF (Super Virtual Fabric)	FRealizuje działania jako nadrzędny węzeł wirtualizujący pionowo dalsze przełączniki i punkty dostępu do postaci jednego, łatwo zarządzanego urządzena
	Obsługuje dwuwarstwową architekturę klienta
	Obsługuje urządzenia innych firm między rodzicem SVF a klientami
iPCA	Zbiór statystyk w czasie rzeczywistym dotyczących liczby utraconych pakietów i współczynnika utraty pakietów na poziomie sieci i urządzenia
Bezpieczeństwo	Analiza zaszyfrowanej komunikacji (ECA)
	Technologia pułapek na zagrożenia
	Współpraca w zakresie bezpieczeństwa w całej sieci
Współdziałanie	VBST (kompatybilne z PVST, PVST+ oraz RPVST)
	LNP (zbliżony do DTP)
	VCMP (zbliżony do VTP)
Rozmiar	1U
Ilość zasilaczy	2
Ilość wiatraków	4
Właściwości urządzenia, wspierane protokoły	
MAC	Up to 64K MAC address entries
	IEEE 802.1d standards compliance
	MAC address learning and aging
	Static, dynamic, and blackhole MAC address entries
	Packet filtering based on source MAC addresses
VLAN	4K VLANs
	Guest VLANs and voice VLANs
	GVRP
	MUX VLAN

	VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports
	VLAN mapping
ARP	Static ARP
	Dynamic ARP
IP routing	Static routes, RIP v1/2, RIPng, OSPF, OSPFv3, IS-IS, IS-ISv6, BGP, BGP4+, ECMP, routing policy
	Up to 64K FIBv4 entries
	Up to 32K FIBv6 entries
Interoperability	VLAN-Based Spanning Tree (VBST), working with PVST, PVST+, and RPVST
	Link-type Negotiation Protocol (LNP), similar to DTP
	VLAN Central Management Protocol (VCMP), similar to VTP
Ethernet loop protection	RRPP ring topology and RRPP multi-instance
	Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protection switchover
	SEP
	ERPS (G.8032)
	BFD for OSPF, BFD for IS-IS, BFD for VRRP, and BFD for PIM
	STP (IEEE 802.1d), RSTP (IEEE 802.1w), and MSTP (IEEE 802.1s)
	BPDU protection, root protection, and loop protection
IPv6 features	Neighbor Discover (ND)
	PMTU
	IPv6 Ping, IPv6 Tracert, IPv6 Telnet
	ACLs based on source IPv6 addresses, destination IPv6 addresses, Layer 4 ports, or protocol types
Multicast	Listener Discovery snooping (MLDv1/v2)
	IPv6 addresses configured for sub-interfaces, VRRP6, DHCPv6, and L3VPN
	Multicast IGMP v1/v2/v3 snooping and IGMP fast leave
	Multicast forwarding in a VLAN and multicast replication between VLANs
	Multicast load balancing among member ports of a trunk
	Controllable multicast
	Port-based multicast traffic statistics
	IGMP v1/v2/v3, PIM-SM, PIM-DM, and PIM-SSM
	MSDP
	Multicast VPN
QoS/ACL	Rate limiting in the inbound and outbound directions of a port
	Packet redirection
	Port-based traffic policing and two-rate three-color CAR
	Eight queues on each port
	DRR, SP, and DRR+SP queue scheduling algorithms
	WRED
	Re-marking of the 802.1p and DSCP fields of packets

	Packet filtering at Layer 2 to Layer 4, filtering out invalid frames based on the source MAC address, destination MAC address, source IP address, destination IP address, TCP/UDP
	address, destination MAC address, source IP address, destination IP address, TCP/UDP source/destination port number, protocol type, and VLAN ID
	Queue-based rate limiting and shaping on ports
Security	Hierarchical user management and password protection
	DoS attack defense, ARP attack defense, and ICMP attack defense
	Binding of the IP address, MAC address, port number, and VLAN ID
	Port isolation, port security, and sticky MAC
	MAC Forced Forwarding (MFF)
	Blackhole MAC address entries
	Limit on the number of learned MAC addresses
	IEEE 802.1X authentication and limit on the number of users on a port
	AAA authentication, RADIUS authentication, and HWTACACS authentication
	NAC
	SSH V2.0
	HTTPS
	CPU protection
	Blacklist and whitelist
	Attack source tracing and punishment for IPv6 packets such as ND, DHCPv6, and MLD packets
	IPSec for management packet encryption
	ECA
	Deception
Reliability	LACP
	E-Trunk
	Ethernet OAM (IEEE 802.3ah and IEEE 802.1ag)
	ITU-Y.1731
	DLDP
	LLDP
	BFD for BGP, BFD for IS-IS, BFD for OSPF, BFD for static routes
Management and maintenance	Cloud-based management
	Virtual cable test
	SNMP v1/v2/v3
	RMON
	Web-based NMS
	System logs and alarms of different severities
	GVRP
	MUX VLAN
	NetStream
	Telemetry

- **Switche dostępowe**

Parametry urządzenia:		
Wydajność przesyłania	132M	
Wydajność przełączania2	176 Gbit/s/432 Gbit/s	
Porty stałe	48 x 10/100/1000BASET ports, 4 x 10 GE SFP+ ports	
PoE	Brak	
MAC	MAC address auto-learning and aging	
	Static, dynamic, and blackhole MAC address entries	
	Packet filtering based on source MAC addresses	
	Interface-based MAC address learning limiting	
VLAN	4094 VLANs	
	Guest VLAN, Voice VLAN	
	GVRP	
	MUX VLAN	
	VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports	
	1:1 and N:1 VLAN mapping	
IP Routing	Static route, RIP, RIPng, OSPF, OSPFv3	
Super Virtual Fabric	Plug-and-play SVF clients	
	Automatic software package and patch loading to SVF clients	
	One-click and automatic delivery of service configurations	
	Independent SVF client operations	
Interoperability	VBST (compatible with PVST/PVST+/RPVST)	
	LNP (similar to DTP)	
	VCMP (similar to VTP)	
Wsparcie dla technologii		
Ethernet basics	Full-duplex, half-duplex, and auto-negotiation	Tak
	Rate auto-negotiation on an interface	Tak
	Auto MDI and MDI-X	Tak
	Flow control on an interface	Tak
	Jumbo frames	Tak
	Link aggregation	Tak
	Load balancing among links of a trunk	Tak
	Transparent transmission of Layer 2 protocol packets	Tak
	Device Link Detection Protocol (DLDP)	Tak
	Link Layer Discovery Protocol (LLDP)	Tak
	Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)	Tak
	Interface isolation	Tak
	Broadcast traffic suppression on an interface	Tak
	Multicast traffic suppression on an interface	Tak
	Unknown unicast traffic suppression on an interface	Tak
	VLAN broadcast traffic suppression	Tak
	VLAN multicast traffic suppression	Tak
	VLAN unknown unicast traffic suppression	Tak

	VLAN specification	4094
	VLANIF interface specification	1024
	Access mode	Tak
	Trunk mode	Tak
	Hybrid mode	Tak
	QinQ mode	Tak
	Default VLAN	Tak
	VLAN assignment based on interfaces	Tak
	VLAN assignment based on protocols	Tak
	VLAN assignment based on IP subnets	Tak
	VLAN assignment based on MAC addresses	Tak
	VLAN assignment based on MAC address + IP address	Tak
	VLAN assignment based on MAC address + IP address + interface number	Tak
	Adding double VLAN tags to packets based on interfaces	Tak
	VLAN mapping	Tak
	Selective QinQ	Tak
	MUX VLAN	Tak
	Voice VLAN	Tak
VLAN	Guest VLAN	Tak
	GARP	Tak
GVRP	GVRP	Tak
VCMP	VCMP	Tak
	MAC address	16512
	Automatic learning of MAC addresses	Tak
	Automatic aging of MAC addresses	Tak
	Static, dynamic, and blackhole MAC address entries	Tak
	Interface-based MAC address learning limiting	Tak
	Sticky MAC	Tak
	MAC address flapping detection	Tak
	MAC address spoofing defense	Tak
MAC	Port bridge	Tak
	Static ARP	Tak
	Dynamic ARP	Tak
	ARP entry	4096
	ARP aging detection	Tak
	Intra-VLAN proxy ARP	Tak
ARP	Routed proxy ARP	Tak
	STP	Tak
	RSTP	Tak
	MSTP	Tak
	VBST	Tak
MSTP	BPDU protection	Tak

	Root protection	Tak
	Loop protection	Tak
	Defense against TC BPDU attacks	Tak
Loopback detection	Loop detection on an interface	Tak
SEP	SEP	Tak
	Smart Link	Tak
	Smart Link multi-instance	Tak
Smart Link	Monitor Link	Tak
	RRPP	Tak
	Single RRPP ring	Tak
	Tangent RRPP ring	Tak
	Intersecting RRPP ring	Tak
RRPP	Hybrid networking of RRPP rings and other ring networks	Tak
	G.8032 v1	Tak
	G.8032 v2	Tak
	ERPS semi-ring topology	Tak
ERPS	ERPS closed-ring topology	Tak
	IPv4 static routing	Tak
	VRF	Tak
	DHCP client	Tak
	DHCP server	Tak
	DHCP relay	Tak
	Routing policies	Tak
	IPv4 routes	4096
	RIPv1	Tak
	RIPv2	Tak
	OSPF	Tak
IPv4 and unicast routing	Policy-based routing (PBR)	Tak
	IGMPv1/v2/v3	Tak
	PIM-DM	Tak
	PIM-SM	Tak
	MSDP	Tak
	IPv4 multicast routes	1500
	IPv6 multicast routes	1500
	Multicast routing policies	Tak
Multicast routing features	RPF	Tak
	IPv6 protocol stack	Tak
	ND	Tak
	ND entry	1024
	ND snooping	Tak
	DHCPv6 snooping	Tak
	RIPng	Tak
IPv6 features	DHCPv6 server	Tak

	DHCPv6 relay	Tak
	OSPFv3	Tak
	IPv6 routes	1024
	VRRP6	Tak
	MLDv1/v2	Tak
	PIM-DM for IPv6	Tak
	PIM-SM for IPv6	Tak
	IGMPv1/v2/v3 snooping	Tak
	IGMP snooping proxy	Tak
	MLD snooping	Tak
	Multicast traffic suppression	Tak
	Inter-VLAN multicast replication	Tak
	Service interface-based stacking	Tak
	Maximum number of stacked devices	9
Stacking	Stack bandwidth (Unidirectional)	40Gbps(MAX)
VRRP	VRRP standard protocol	Tak
	Automatic discovery of links	Tak
	Link fault detection	Tak
	Link troubleshooting	Tak
EFM (802.3ah)	Remote loopback	Tak
	Software-level CCM	Tak
	802.1ag MAC ping	Tak
CFM (802.1ag)	802.1ag MAC trace	Tak
OAM association	Association between 802.1ag and 802.3ah	Tak
	Unidirectional delay and jitter measurement	Tak
Y.1731	Bidirectional delay and jitter measurement	Tak
	Traffic classification based on ACLs	Tak
	Configuring traffic classification priorities	Tak
Traffic classification	Matching the simple domains of packets	Tak
	Traffic filtering	Tak
	Traffic policing (CAR)	Tak
	Modifying the packet priorities	Tak
	Modifying the simple domains of packets	Tak
Traffic behavior	Modifying the packet VLANs	Tak
	Traffic shaping on an egress interface	Tak
Traffic shaping	Traffic shaping on queues on an interface	Tak
Congestion avoidance	Tail drop	Tak
	Priority Queuing (PQ)	Tak
	Weighted Deficit Round Robin (WDRR)	Tak
	PQ+WDRR	Tak
	Weighted Round Robin (WRR)	Tak
Congestion management	PQ+WRR	Tak
Packet filtering at Layer 2 to Layer 4	Number of rules per IPv4 ACL	2K

	Number of rules per IPv6 ACL	2K
	Basic IPv4 ACL	Tak
	Advanced IPv4 ACL	Tak
	Basic IPv6 ACL	Tak
	Advanced IPv6 ACL	Tak
	Layer 2 ACL	Tak
	User-defined ACL	Tak
	Command line interface (CLI)-based configuration	Tak
	Console terminal service	Tak
	Telnet terminal service	Tak
	SSH v1.5	Tak
	SSH v2.0	Tak
	SNMP-based NMS for unified configuration	Tak
	Web page-based configuration and management	Tak
	EasyDeploy (client)	Tak
	SVF	Tak
	Cloud management	Tak
Login and configuration management	OPS	Tak
	Directory and file management	Tak
File system	File upload and download	Tak
	eMDI	Tak
	Hardware monitoring	Tak
	Log information output	Tak
	Alarm information output	Tak
	Debugging information output	Tak
	Port mirroring	Tak
	Flow mirroring	Tak
	Remote mirroring	Tak
Monitoring and maintenance	Energy saving	Tak
	Version upgrade	Tak
Version upgrade	Version rollback	Tak
	ARP packet rate limiting	Tak
	ARP anti-spoofing	Tak
	Association between ARP and STP	Tak
	Dynamic ARP Inspection (DAI)	Tak
	Static ARP Inspection (SAI)	Tak
ARP security	Egress ARP Inspection (EAI)	Tak
	ICMP attack defense	Tak
	IPSG for IPv4	Tak
	IPSG user capacity	1K
	IPSG for IPv6	Tak
IP security	IPSGv6 user capacity	512
Local attack defense	CPU attack defense	Tak

MFF	MFF	Tak
DHCP snooping	DHCP snooping	Tak
	Option 82 function	Tak
	Dynamic rate limiting for DHCP packets	Tak
Attack defense	Defense against malformed packet attacks	Tak
	Defense against UDP flood attacks	Tak
	Defense against TCP SYN flood attacks	Tak
	Defense against ICMP flood attacks	Tak
	Defense against packet fragment attacks	Tak
	Local URPF	Tak
AAA	Local authentication	Tak
	Local authorization	Tak
	RADIUS authentication	Tak
	RADIUS authorization	Tak
	RADIUS accounting	Tak
	HWTACACS authentication	Tak
	HWTACACS authorization	Tak
	HWTACACS accounting	Tak
NAC	802.1X authentication	Tak
	MAC address authentication	Tak
	Portal authentication	Tak
	Hybrid authentication	Tak
Policy association	Functioning as the access device	Tak
	Ping	Tak
	Tracert	Tak
	NQA	Tak
	NTP	Tak
	sFlow	Tak
	SNMP v1	Tak
	SNMP v2c	Tak
	SNMP v3	Tak
	HTTP	Tak
	HTTPS	Tak
	RMON	Tak
	NETCONF/YANG	Tak
	VLAN-based Spanning Tree (VBST)	Tak
	Link-type Negotiation Protocol (LNP)	Tak
	VLAN Central Management Protocol (VCMP)	Tak

- **Switche PoE**

Parametry urządzenia:	
Wydajność przesyłania	132M
Wydajność przełączania2	176 Gbit/s/432 Gbit/s

Porty stałe	48 x 10/100/1000BASET PoE+ ports, 4 x 10 GE SFP+ ports	
PoE	PoE+	
MAC	MAC address auto-learning and aging	
	Static, dynamic, and blackhole MAC address entries	
	Packet filtering based on source MAC addresses	
	Interface-based MAC address learning limiting	
VLAN	4094 VLANs	
	Guest VLAN, Voice VLAN	
	GVRP	
	MUX VLAN	
	VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports	
	1:1 and N:1 VLAN mapping	
IP Routing	Static route, RIP, RIPng, OSPF, OSPFv3	
Super Virtual Fabric	Plug-and-play SVF clients	
	Automatic software package and patch loading to SVF clients	
	One-click and automatic delivery of service configurations	
	Independent SVF client operations	
Interoperability	VBST (compatible with PVST/PVST+/RPVST)	
	LNP (similar to DTP)	
	VCMP (similar to VTP)	
Wsparcie dla technologii		
Ethernet basics	Full-duplex, half-duplex, and auto-negotiation	Tak
	Rate auto-negotiation on an interface	Tak
	Auto MDI and MDI-X	Tak
	Flow control on an interface	Tak
	Jumbo frames	Tak
	Link aggregation	Tak
	Load balancing among links of a trunk	Tak
	Transparent transmission of Layer 2 protocol packets	Tak
	Device Link Detection Protocol (DLDP)	Tak
	Link Layer Discovery Protocol (LLDP)	Tak
	Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)	Tak
	Interface isolation	Tak
	Broadcast traffic suppression on an interface	Tak
	Multicast traffic suppression on an interface	Tak
	Unknown unicast traffic suppression on an interface	Tak
	VLAN broadcast traffic suppression	Tak
	VLAN multicast traffic suppression	Tak
	VLAN unknown unicast traffic suppression	Tak
VLAN	VLAN specification	4094
	VLANIF interface specification	1024
	Access mode	Tak

	Trunk mode	Tak
	Hybrid mode	Tak
	QinQ mode	Tak
	Default VLAN	Tak
	VLAN assignment based on interfaces	Tak
	VLAN assignment based on protocols	Tak
	VLAN assignment based on IP subnets	Tak
	VLAN assignment based on MAC addresses	Tak
	VLAN assignment based on MAC address + IP address	Tak
	VLAN assignment based on MAC address + IP address + interface number	Tak
	Adding double VLAN tags to packets based on interfaces	Tak
	VLAN mapping	Tak
	Selective QinQ	Tak
	MUX VLAN	Tak
	Voice VLAN	Tak
	Guest VLAN	Tak
	GARP	Tak
GVRP	GVRP	Tak
VCMP	VCMP	Tak
	MAC address	16512
	Automatic learning of MAC addresses	Tak
	Automatic aging of MAC addresses	Tak
	Static, dynamic, and blackhole MAC address entries	Tak
	Interface-based MAC address learning limiting	Tak
	Sticky MAC	Tak
	MAC address flapping detection	Tak
	MAC address spoofing defense	Tak
MAC	Port bridge	Tak
	Static ARP	Tak
	Dynamic ARP	Tak
	ARP entry	4096
	ARP aging detection	Tak
	Intra-VLAN proxy ARP	Tak
ARP	Routed proxy ARP	Tak
	STP	Tak
	RSTP	Tak
	MSTP	Tak
	VBST	Tak
	BPDU protection	Tak
	Root protection	Tak
	Loop protection	Tak
MSTP	Defense against TC BPDU attacks	Tak
Loopback detection	Loop detection on an interface	Tak

SEP	SEP	Tak
Smart Link	Smart Link	Tak
	Smart Link multi-instance	Tak
	Monitor Link	Tak
RRPP	RRPP	Tak
	Single RRPP ring	Tak
	Tangent RRPP ring	Tak
	Intersecting RRPP ring	Tak
	Hybrid networking of RRPP rings and other ring networks	Tak
ERPS	G.8032 v1	Tak
	G.8032 v2	Tak
	ERPS semi-ring topology	Tak
	ERPS closed-ring topology	Tak
IPv4 and unicast routing	IPv4 static routing	Tak
	VRF	Tak
	DHCP client	Tak
	DHCP server	Tak
	DHCP relay	Tak
	Routing policies	Tak
	IPv4 routes	4096
	RIPv1	Tak
	RIPv2	Tak
	OSPF	Tak
	Policy-based routing (PBR)	Tak
Multicast routing features	IGMPv1/v2/v3	Tak
	PIM-DM	Tak
	PIM-SM	Tak
	MSDP	Tak
	IPv4 multicast routes	1500
	IPv6 multicast routes	1500
	Multicast routing policies	Tak
	RPF	Tak
IPv6 features	IPv6 protocol stack	Tak
	ND	Tak
	ND entry	1024
	ND snooping	Tak
	DHCPv6 snooping	Tak
	RIPng	Tak
	DHCPv6 server	Tak
	DHCPv6 relay	Tak
	OSPFv3	Tak
	IPv6 routes	1024
	VRRP6	Tak

	MLDv1/v2	Tak
	PIM-DM for IPv6	Tak
	PIM-SM for IPv6	Tak
	IGMPv1/v2/v3 snooping	Tak
	IGMP snooping proxy	Tak
	MLD snooping	Tak
	Multicast traffic suppression	Tak
	Inter-VLAN multicast replication	Tak
	Service interface-based stacking	Tak
	Maximum number of stacked devices	9
Stacking	Stack bandwidth (Unidirectional)	40Gbps(MAX)
VRRP	VRRP standard protocol	Tak
	Automatic discovery of links	Tak
	Link fault detection	Tak
	Link troubleshooting	Tak
EFM (802.3ah)	Remote loopback	Tak
	Software-level CCM	Tak
	802.1ag MAC ping	Tak
CFM (802.1ag)	802.1ag MAC trace	Tak
OAM association	Association between 802.1ag and 802.3ah	Tak
	Unidirectional delay and jitter measurement	Tak
Y.1731	Bidirectional delay and jitter measurement	Tak
	Traffic classification based on ACLs	Tak
	Configuring traffic classification priorities	Tak
Traffic classification	Matching the simple domains of packets	Tak
	Traffic filtering	Tak
	Traffic policing (CAR)	Tak
	Modifying the packet priorities	Tak
	Modifying the simple domains of packets	Tak
Traffic behavior	Modifying the packet VLANs	Tak
	Traffic shaping on an egress interface	Tak
Traffic shaping	Traffic shaping on queues on an interface	Tak
Congestion avoidance	Tail drop	Tak
	Priority Queuing (PQ)	Tak
	Weighted Deficit Round Robin (WDRR)	Tak
	PQ+WDRR	Tak
	Weighted Round Robin (WRR)	Tak
Congestion management	PQ+WRR	Tak
	Number of rules per IPv4 ACL	2K
	Number of rules per IPv6 ACL	2K
	Basic IPv4 ACL	Tak
	Advanced IPv4 ACL	Tak
Packet filtering at Layer 2 to Layer 4	Basic IPv6 ACL	Tak

	Advanced IPv6 ACL	Tak
	Layer 2 ACL	Tak
	User-defined ACL	Tak
Login and configuration management	Command line interface (CLI)-based configuration	Tak
	Console terminal service	Tak
	Telnet terminal service	Tak
	SSH v1.5	Tak
	SSH v2.0	Tak
	SNMP-based NMS for unified configuration	Tak
	Web page-based configuration and management	Tak
	EasyDeploy (client)	Tak
	SVF	Tak
	Cloud management	Tak
	OPS	Tak
File system	Directory and file management	Tak
	File upload and download	Tak
Monitoring and maintenance	eMDI	Tak
	Hardware monitoring	Tak
	Log information output	Tak
	Alarm information output	Tak
	Debugging information output	Tak
	Port mirroring	Tak
	Flow mirroring	Tak
	Remote mirroring	Tak
	Energy saving	Tak
Version upgrade	Version upgrade	Tak
	Version rollback	Tak
ARP security	ARP packet rate limiting	Tak
	ARP anti-spoofing	Tak
	Association between ARP and STP	Tak
	Dynamic ARP Inspection (DAI)	Tak
	Static ARP Inspection (SAI)	Tak
	Egress ARP Inspection (EAI)	Tak
IP security	ICMP attack defense	Tak
	IPSG for IPv4	Tak
	IPSG user capacity	1K
	IPSG for IPv6	Tak
	IPSGv6 user capacity	512
Local attack defense	CPU attack defense	Tak
MFF	MFF	Tak
DHCP snooping	DHCP snooping	Tak
	Option 82 function	Tak
	Dynamic rate limiting for DHCP packets	Tak

	Defense against malformed packet attacks	Tak
	Defense against UDP flood attacks	Tak
	Defense against TCP SYN flood attacks	Tak
	Defense against ICMP flood attacks	Tak
	Defense against packet fragment attacks	Tak
Attack defense	Local URPF	Tak
	Local authentication	Tak
	Local authorization	Tak
	RADIUS authentication	Tak
	RADIUS authorization	Tak
	RADIUS accounting	Tak
	HWTACACS authentication	Tak
	HWTACACS authorization	Tak
AAA	HWTACACS accounting	Tak
	802.1X authentication	Tak
	MAC address authentication	Tak
	Portal authentication	Tak
NAC	Hybrid authentication	Tak
	Functioning as the access device	Tak
	Ping	Tak
	Tracert	Tak
	NQA	Tak
	NTP	Tak
	sFlow	Tak
	SNMP v1	Tak
	SNMP v2c	Tak
	SNMP v3	Tak
	HTTP	Tak
	HTTPS	Tak
	RMON	Tak
	NETCONF/YANG	Tak
	VLAN-based Spanning Tree (VBST)	Tak
	Link-type Negotiation Protocol (LNP)	Tak
Policy association	VLAN Central Management Protocol (VCMP)	Tak

- **Access Point**

Parametry urządzenia:	
Zasialnie DC	12 V +/- 10%
Zasilanie PoE	Według standardu 802.3at
Antena	Wbudowana
Ilość SSID per radio	do 16
Obsługiwana ilość użytkowników	do 512
Moc transmisji 2.4 G	25 dBm

Moc transmiji 5 G	25 dBm
MIMO : Spatial Streams	2.4G: 2 x 2:2 5G: 2 x 2:2
Obsługiwane protokoły	802.11a/b/g/n/ac/ac Wave 2/11ax
Maksymalny przesył	1.774 Gbit/s
Wzmocnienie antenowe	2.4 G: 3.5 dBi, 5G: 5 dBi
Maksymalna Ilość kanałów dla odpowiednich standardów (non-overlaping)	2.4 GHz (2.412 GHz to 2.472 GHz) 802.11b/g − 20 MHz: 3 802.11n − 20 MHz: 3 − 40 MHz: 1 802.11ax − 20 MHz: 3 − 40 MHz: 1 5 GHz (5.18 GHz to 5.825 GHz) 802.11a − 20 MHz: 13 802.11n − 20 MHz: 13 − 40 MHz: 6 802.11ac − 20 MHz: 13 − 40 MHz: 6 − 80 MHz: 3 802.11ax − 20 MHz: 13 − 40 MHz: 6 − 80 MHz: 3
Standardy:	
Zabezpieczenia	802.11i, Wi-Fi Protected Access 2(WPA2), WPA, WPA2, WPA2-Enterprise, WPA2-PSK, WPA3*, WAPI* 802.1X Advanced Encryption Standards(AES), Temporal Key Integrity Protocol(TKIP), WEP, Open EAP Type(s)
Spełniane standardy	UL 62368–1 EN 62368–1 IEC 62368–1 GB 4943 EN 60950–1 UL 60950–1 CAN/CSA 22.2 No.60950-1 IEC 60950–1 ETSI EN 300 328 ETSI EN 301 893 RSS-210 AS/NZS 4268 EN 301 489–1 EN 301 489–17

	ETSI EN 60601-1-2 FCC Part 15 ICES-003 YD/T 1312.2-2004 ITU k.20 GB 9254 GB 17625.1 AS/NZS CISPR22 EN 55022 EN 55024 CISPR 22 CISPR 24 IEC61000-4-6 IEC61000-4-2 IEEE 802.11a/b/g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11h IEEE 802.11d IEEE 802.11e IEEE 802.11k IEEE 802.11u IEEE 802.11v IEEE 802.11w IEEE 802.11r CENELEC EN 62311 CENELEC EN 50385 OET65 RSS-102 FCC Part1&2 FCC KDB Series Directive 2002/95/EC & 2011/65/EU Regulation 1907/2006/EC Directive 2002/96/EC & 2012/19/EU

- **Router brzegowy**

Porty stałe	
Ilość portów GE WAN	2
Ilość portów GE Combo Ports	8
Ilość portów 10GE SFP+	2
Parametry technologiczne i bezpieczeństwa	
Firewall Throughput1 (1518/512/64-byte, UDP)	6/6/3.6 Gbit/s
IPv6 Firewall Throughput1 (1518/512/84-byte, UDP)	6/6/1.6 Gbit/s
Firewall Throughput (Packets Per Second)	6 Mpps
Firewall Latency (64-byte, UDP)	18 µs
FW + SA* Throughput2	3 Gbit/s
FW + SA + IPS Throughput2	2.2 Gbit/s
FW + SA + IPS + Antivirus Throughput2	2.2 Gbit/s
Full protection Throughput3	1.7 Gbit/s
Full protection Throughput (Realworld)4	0.9 Gbit/s
Concurrent Sessions (HTTP1.1)1	4,000,000
New Sessions/Second (HTTP1.1)1	80

IPsec VPN Throughput1 (AES-256 + SHA256, 1420-byte)	6 Gbit/s
Maximum IPsec VPN Tunnels (GW to GW)	4000
Maximum IPsec VPN Tunnels (Client to GW)	4000
SSL Inspection Throughput5	500 Mbit/s
SSL VPN Throughput6	480 Mbit/s
Concurrent SSL VPN Users *(Default/Maximum)	100/1000
Security Policies (Maximum)	15
Virtual Firewalls	100
Fixed Interfaces	2×10GE (SFP+) + 8×GE Combo + 2×GE WAN
External Storage	Optional, SSD (M.2) card supported, 240 GB
Oprogramowanie NGFW	
Pakiet bezpieczeństwa Threat Protection (IPS, AV, URL)	z dwuletnimi aktualizacjami

- **Router brzegowy HA**

Porty stałe	
Ilość portów GE WAN	2
Ilość portów GE Combo Ports	8
Ilość portów 10GE SFP+	2
Parametry technologiczne i bezpieczeństwa	
Firewall Throughput1 (1518/512/64-byte, UDP)	6/6/3.6 Gbit/s
IPv6 Firewall Throughput1 (1518/512/84-byte, UDP)	6/6/1.6 Gbit/s
Firewall Throughput (Packets Per Second)	6 Mpps
Firewall Latency (64-byte, UDP)	18 µs
FW + SA* Throughput2	3 Gbit/s
FW + SA + IPS Throughput2	2.2 Gbit/s
FW + SA + IPS + Antivirus Throughput2	2.2 Gbit/s
Full protection Throughput3	1.7 Gbit/s
Full protection Throughput (Realworld)4	0.9 Gbit/s
Concurrent Sessions (HTTP1.1)1	4,000,000
New Sessions/Second (HTTP1.1)1	80
IPsec VPN Throughput1 (AES-256 + SHA256, 1420-byte)	6 Gbit/s
Maximum IPsec VPN Tunnels (GW to GW)	4000
Maximum IPsec VPN Tunnels (Client to GW)	4000
SSL Inspection Throughput5	500 Mbit/s
SSL VPN Throughput6	480 Mbit/s
Concurrent SSL VPN Users *(Default/Maximum)	100/1000
Security Policies (Maximum)	15
Virtual Firewalls	100
Fixed Interfaces	2×10GE (SFP+) + 8×GE Combo + 2×GE WAN
External Storage	Optional, SSD (M.2) card supported, 240 GB
Oprogramowanie NGFW	

Pakiet bezpieczeństwa Threat Protection (IPS, AV, URL) dla urządzenia pracującego w HA	z dwuletnimi aktualizacjami
Licencja utrzymaniowa urządzenia zapasowego HA	

- **Sterownik dostępu WLAN**

Parametry urządzenia:	
Porty	10 x GE + 2 x 10 GE SFP+
Zasilanie	AC/DC adapter
Wydajność przesyłania	6 Gb/s
Maksymalna liczba zarządzanych AP	256
Maksymalna ilość użytkowników	4 tys.
Sieć AP-AC	Sieć Warstwy 2 lub Warstwy 3
Tryby przekazywania	Bezpośrednie przekazywanie lub przekazywanie tunelowe
Tryb aktywny/gotowości AC	1+1 HSB lub N+1 backup
Protokoły radiowe	802.11 a/b/g/n/ac/ac Wave 2/ax
Technologia przełączania, forwardowania, i inne wymagania technologiczne	
Ethernet	Operating modes of full duplex, half duplex, and auto-negotiation
	Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto- negotiation
	Flow control on interfaces
	Jumbo frames
	Link aggregation
	Load balancing among links of a trunk
	Interface isolation and forwarding restriction
	Broadcast storm suppression
VLAN	Access modes of access, trunk, and hybrid Default VLAN
	VLAN pool
MAC	Automatic learning and aging of MAC addresses Static, dynamic, and blackhole MAC address entries Packet filtering based on source MAC addresses
	Interface-based MAC learning limiting
ARP	Static and dynamic ARP entries ARP in a VLAN
	Aging of ARP entries
LLDP	LLDP
MSTP	STP RSTP MSTP
	BPDU protection, root protection, and loop protection
	Partitioned STP
IPv4 features	ARP and RARP ARP proxy Auto-detection NAT
	Bonjour protocol
Unicast routing features	Static route
	RIP-1 and RIP-2 OSPF
	BGP IS-IS
	Routing policies and policy-based routing URPF check
	DHCP server and relay
	DHCP snooping

	IGMPv1, IGMPv2, and IGMPv3 PIM-SM
	Multicast routing policies
Multicast routing features	RPF
IPv6 features	ND protocol
	Static route RIPng OSPFv3 BGP4+
	IS-IS IPv6 DHCPv6
	DHCPv6 snooping
Unicast routing features	Description
	MLD
Multicast routing features	MLD snooping
BFD	BFD
	IGMP snooping Prompt leave Multicast traffic control
Layer 2 multicast	Inter-VLAN multicast replication
	Neighbor discovery Link monitoring Fault notification
EFM OAM	Remote loopback
Traffic classification	Traffic classification based on the combination of the L2 protocol header, IP 5- tuple, and 802.1p priority
	Access control after traffic classification Traffic policing based on traffic classification
	Re-marking packets based on traffic classifiers Class-based packet queuing
Action	Associating traffic classifiers with traffic behaviors
	PQ scheduling DRR scheduling
	PQ+DRR scheduling WRR scheduling
Queue scheduling	PQ+WRR scheduling
Congestion avoidance	SRED WRED
Application control	Smart Application Control (SAC)
	Configurations using command lines
	Error message and help information in English Login through console and Telnet terminals
Terminal service	Send function and data communications between terminal users
	File systems
	Directory and file management
File system	File uploading and downloading using FTP and TFTP
	Unified management over logs, alarms, and debugging information Electronic labels
	User operation logs
	Detailed debugging information for network fault diagnosis Network test tools such as traceroute and ping commands Intelligent diagnosis
Debugging and maintenance	Interface mirroring and flow mirroring
	Device software loading and online software loading
	Description
	BIOS online upgrade
Version upgrade	In-service patching

	ICMP-based ping and traceroute SNMPv1, SNMPv2c, and SNMPv3
	Standard MIB RMON
Network management	NetStream
	Different user levels for commands, preventing unauthorized users from accessing device
	SSHv2.0
	RADIUS and HWTACACS authentication for login users ACL filtering
	DHCP packet filtering (with the Option 82 field)
	Local attack defense function that can protect the CPU and ensure that the CPU can process services
	Defense against control packet attacks
	Defenses against attacks such as source address spoofing, Land, SYN flood (TCP SYN), Smurf, ping flood (ICMP echo), Teardrop, broadcast flood, and Ping of Death attacks
	IPSec
	URL filtering Antivirus
System security	Intrusion prevention
	APs and WLAN ACs can be connected through a Layer 2 or Layer 3 network. APs can be directly connected to a WLAN AC.
	APs are deployed on a private network, while WLAN ACs are deployed on the public network to implement NAT traversal.
	WLAN ACs can be used for Layer 2 bridge forwarding or Layer 3 routing.
Networking between APs and WLAN ACs	WAN authentication escape is supported between APs and WLAN ACs. In local forwarding mode, this feature retains the online state of existing STAs and allows access of new STAs when APs are disconnected from WLAN ACs, ensuring service continuity.
	Direct forwarding (distributed forwarding or local forwarding) Tunnel forwarding (centralized forwarding)
	Centralized authentication and distributed forwarding
	In direct forwarding mode, user authentication packets support tunnel forwarding.
	Soft GRE forwarding.
Forwarding mode	Tunnel forwarding + EoGRE tunnel
	An AP can obtain the device's IP address in any of the following ways:
	Static configuration
	DHCP
	DNS
	The WLAN AC uses DHCP or DHCPv6 to allocate IP addresses to APs. DHCP or DHCPv6 relay is supported.
WLAN AC discovery	On a Layer 2 network, APs can discover the WLAN AC by sending broadcast CAPWAP packets.
	WDS bridging:
	Point-to-point (P2P) wireless bridging
Wireless networking mode	Point-to-multipoint (P2MP) wireless bridging

	Automatic topology detection and loop prevention (STP) Wireless mesh network
	Access authentication for mesh devices
	Mesh routing algorithm
	Go-online without configuration
	Mesh network with multiple MPPs
	Vehicle-ground fast link handover
	Mesh client mode
CAPWAP tunnel	Centralized CAPWAP
	CAPWAP control tunnel and data tunnel (optional)
	CAPWAP tunnel forwarding and direct forwarding in an extended service set (ESS)
	Datagram Transport Layer Security (DTLS) encryption, which is enabled by default for the CAPWAP control tunnel
	Heartbeat detection and tunnel reconnection
Active and standby WLAN ACs	Enables and disables the switchback function. Supports load balancing.
	Supports 1+1 hot backup.
	NOTE
	In 1+1 VRRP HSB mode, WLAN ACs share one virtual IP address, simplifying the network topology.
	Supports N+1 backup.
	Supports wireless configuration synchronization between WLAN ACs.
AP access control	Displays MAC addresses or SNs of APs in the whitelist.
	Adds a single AP or multiple APs (by specifying a range of MAC addresses or SNs) to the whitelist.
	Automatically discovering and manually confirming APs.
	Automatically discovering APs without manually confirming them.
AP profile management	Specifies the default AP profile that is applied to automatically discovered APs.
AP group management	The AP group function is used to configure multiple APs in batches. When multiple APs managed by a WLAN AC require the same configurations, you can add these APs to one
	AP group and configure the AP group to complete AP configuration.
AP region management	Supports three AP region deployment modes:
	Distributed deployment: APs are deployed independently. An AP is equivalent to a region and does not interfere with other APs. APs work at the maximum power anddo not perform radio calibration.
	Common deployment: APs are loosely deployed. The transmit power of each radiois less than 50% of the maximum transmit power.
	Centralized deployment: APs are densely deployed. The transmit power of each radio is less than 25% of the maximum transmit power.
	Specifies the default region to which automatically discovered APs are added.
AP type management	Manages AP attributes including the number of interfaces, AP types, number of radios, radio types, maximum number

	of virtual access points (VAPs), maximum number of associated users, and radio gain (for APs deployed indoors).
	Provides default AP types.
Network topology management	Supports LLDP topology detection.
AP working mode management	Supports AP working mode switchover. The AP working mode can be switched to the Fat or cloud mode on the AC.
Radio profile management	The following parameters can be configured in a radio profile:
	Radio working mode and rate
	Automatic or manual channel and power adjustment mode
	Radio calibration interval
	The radio type can be set to 802.11b, 802.11b/g, 802.11b/g/n, 802.11g, 802.11n, 802.11g/n, 802.11a, 802.11a/n, 802.11ac, or 802.11ax.
	You can bind a radio to a specified radio profile.
	Supports MU-MIMO.
Unified static configuration of parameters	Radio parameters such as the channel and power of each radio are configured on the WLAN AC and then delivered to APs.
Dynamic management	APs can automatically select working channels and power when they go online.
	In an AP region, APs automatically adjust working channels and power in the event of signal interference:
	Partial calibration: The optimal working channel and power of a specified AP canbe adjusted.
	Global calibration: The optimal working channels and power of all the APs in aspecified region can be adjusted.
	When an AP is removed or goes offline, the WLAN AC increases the power of neighboring APs to compensate for the coverage hole.
	Automatic selection and calibration of radio parameters in AP regions are supported.
Enhanced service capabilities	Band steering: Enables terminals to preferentially access the 5G frequency band, achieving load balancing between the 2.4G and 5G frequency bands.
	Smart roaming: Enables sticky terminals to roam to APs with better signals.
	802.11k and 802.11v smart roaming
	802.11r fast roaming (≤ 50 ms)
ESS management	Allows you to enable SSID broadcast, set the maximum number of access users, and set the association aging time in an ESS.
	Isolates APs at Layer 2 in an ESS. Maps an ESS to a service VLAN.
	Associates an ESS with a security profile or a QoS profile. Enables IGMP for APs in an ESS.
	Supports Chinese SSIDs.
VAP-based service management	Adds multiple VAPs at a time by binding radios to ESSs.
	Displays information about a single VAP, VAPs with a specified ESS, or all VAPs. Supports configuration of offline APs.
	Creates VAPs according to batch delivered service provisioning rules in automatic AP discovery mode.

Service provisioning management	Supports service provisioning rules configured for a specified radio of a specified AP type.
	Adds automatically discovered APs to the default AP region. The default AP region is configurable.
	Applies a service provisioning rule to a region to enable APs in the region to go online.
Multicast service management	Supports IGMP snooping. Supports IGMP proxy.
Load balancing	Performs load balancing among radios in a load balancing group.
	Supports two load balancing modes:
	− Based on the number of STAs connected to each radio
	− Based on the traffic volume on each radio
Bring Your Own Device (BYOD)	Identifies device types according to the OUI in the MAC address.
	Identifies device types according to the user agent (UA) field in an HTTP packet.
	Identifies device types according to DHCP Option information.
	Carries device type information in RADIUS authentication and accounting packets.
Location services	Locates AeroScout and Ekahau tags. Locates Wi-Fi terminals.
	Locates Bluetooth terminals.
	Locates Bluetooth tags.
Spectrum analysis	Identifies the following interference sources: Bluetooth, microwave ovens, cordless phones, ZigBee, game controller, 2.4 GHz/5 GHz wireless audio and video devices, and baby monitors.
	Works with the eSight to display spectrums of interference sources.
Hotspot2.0	Supports a Hotspot2.0 network.
Internet of Things (IoT)	Supports IoT cards on the AP to converge the WLAN and IoT.
Navi WLAN AC	Supports remote STA access on the Navi WLAN AC.
Feature	Description
Centralized license control	Supports a license server as the centralized AP license control point. Allows a license server to manage license clients.
	Supports license synchronization between a license server and clients.
Feature	Description
Address allocation of wireless users	Functions as a DHCP server to assign IP addresses to wireless users.
WLAN user management	Supports user blacklist and whitelist. Controls the number of access users:
	Based on APs
	Based on SSIDs
	Logs out users in any of the following ways:
	Using RADIUS DM messages
	Using commands
	Supports various methods to view information:
	Allows you to view the user status by specifying the user MAC address, AP ID, radio ID, or WLAN ID.

	Displays the number of online users in an ESS, AP, or radio.
	Collects packet statistics on air interface based on user.
WLAN user roaming	Supports intra-AC Layer 2 roaming.
	NOTE
	Users can roam between APs connected to different physical ports on a WLAN AC.
	Supports inter-VLAN Layer 3 roaming on a WLAN AC. Supports roaming between WLAN ACs.
	Supports fast key negotiation in 802.1X authentication.
	Authenticates users who request to reassociate with the WLAN AC and rejects the requests of unauthorized users.
	Delays clearing user information after a user goes offline so that the user can rapidly go online again.
User group management	Supports ACLs. Supports user isolation:
	Inter-group isolation
	Intra-group isolation
Feature	Description
WLAN security profile management	Manages authentication and encryption modes using WLAN security profiles.
Authentication modes	Open system authentication with no encryption WEP authentication/encryption
	WPA/WPA2/WPA3 authentication and encryption:
	WPA/WPA2-PSK+TKIP
	WPA/WPA2-PSK+CCMP
	WPA/WPA2-802.1X+TKIP
	WPA/WPA2-802.1X+CCMP
	WPA3-802.1X+GCMP256
	WPA/WPA2-PSK+TKIP-CCMP
	WPA/WPA2-802.1X+TKIP-CCMP WPA/WPA2-PPSK authentication and encryption WPA3-SAE+CCMP authentication and encryption WAPI authentication and encryption:
	Supports centralized WAPI authentication.
	Supports three-certificate WAPI authentication, which is compatible withtraditional two-certificate authentication.
	Issues a certificate file together with a private key.
	Allows users to use MAC addresses as accounts for authentication by the RADIUS server.
	Portal authentication:
	Authentication through an external Portal server
	Built-in Portal authentication and authentication page customization 802.1X authentication:
	Authentication through an external 802.1X server.
	Built-in 802.1X authentication.
Combined authentication	Combined MAC authentication:
	PSK+MAC authentication MAC+portal authentication:
	MAC authentication is used first. When MAC authentication fails, portalauthentication is used.
AAA	Local authentication/local accounts (MAC addresses and accounts) RADIUS authentication

	Multiple authentication servers:
	Supports backup authentication servers.
	Specifies authentication servers based on the account.
	Configures authentication servers based on the account.
	Binds user accounts to SSIDs.
Security isolation	Port-based isolation
	User group-based isolation
Security standards	802.11i, Wi-Fi Protected Access 2 (WPA2), WPA,802.1X
	Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP), and Extensible Authentication
	Protocol (EAP) types:
	EAP-Transport Layer Security (TLS)
	EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)
	Protected EAP (PEAP) v0 or EAP-MSCHAPv2
	EAP-Flexible Authentication via Secure Tunneling (FAST)
	PEAP v1 or EAP-Generic Token Card (GTC) EAP-Subscriber Identity Module (SIM)
WIDS	Rogue device scan, identification, defense, and countermeasures, whichincludes dynamic blacklist configuration and detection of rogue APs, STAs, and network attacks.
Authority control	ACL limit based on the following:
	Port
	User group
	User
Other security features	SSID hiding
	IP source guard:
	Configures IP and MAC binding entries statically.
	Generates IP and MAC binding entries dynamically.
Number of managed APs	Central APs：32
	Common APs and RUs：256
	NOTE
	The RUs managed by the WLAN AC do not occupy the AC's license resources. However, the total number of managed common APs and RUs cannot exceed the upper limit allowed by the AC.
Number of access users	4K
	NOTE
	The maximum number of access users varies depending on the authentication mode.
Number of MAC address entries	8K
Forwarding capability	6Gbit/s
	NOTE
	Packet length: 1024 bytes
Number of VLANs	4K
Number of routing entries	IPv4: 8K

	IPv6: 2K
Number of ARP entries	6K
Number of multicast forwarding entries	2K
Number of DHCP IP address pools	64 IP address pools, each of which contains a maximum of 8K IP addresses
Number of local accounts	4K
Number of ACLs	4K
Item	Description
Safety standards	IEC60950-1
	Description
	UL60950-1
	CSA C22.2#60950-1 EN60950-1
	AS/NZS 60950.1
Item	GB 4943
	FCC Part15B ETSI EN 300 386 IEC61000-4-11 IEC 61000-4-4 IEC61000-4-2 IEC61000-4-3 IEC61000-4-5 IEC61000-4-6 IEC 61000-3-2
	IEC 61000-3-3
	AS/NZS CISPR 32 EN55032/EN55024 ICES-003
EMC standards	GB9254
RoHS	Directive 2002/95/EC & 2011/65/EU
Reach	Regulation 1907/2006/EC
WEEE	Directive 2002/96/EC & 2012/19/EU
Oprogramowanie i licencje	
Oprogramowanie do obsługi następującej ilość AP w ramach projektu	100

- **Sterownik dostpępu WLAN HA**

Parametry urządzenia:	
Porty	10 x GE + 2 x 10 GE SFP+
Zasilanie	AC/DC adapter
Wydajność przesyłania	6 Gb/s
Maksymalna liczba zarządzanych AP	256
Maksymalna ilość użytkowników	4 tys.
Sieć AP-AC	Sieć Warstwy 2 lub Warstwy 3
Tryby przekazywania	Bezpośrednie przekazywanie lub przekazywanie tunelowe
Tryb aktywny/gotowości AC	1+1 HSB lub N+1 backup
Protokoły radiowe	802.11 a/b/g/n/ac/ac Wave 2/ax
Technologia przełączania, forwardowania, i inne wymagania technologiczne	
	Operating modes of full duplex, half duplex, and auto-negotiation
	Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto- negotiation
	Flow control on interfaces
	Jumbo frames
Ethernet	Link aggregation

	Load balancing among links of a trunk
	Interface isolation and forwarding restriction
	Broadcast storm suppression
	Access modes of access, trunk, and hybrid Default VLAN
VLAN	VLAN pool
	Automatic learning and aging of MAC addresses Static, dynamic, and blackhole MAC address entries Packet filtering based on source MAC addresses
MAC	Interface-based MAC learning limiting
	Static and dynamic ARP entries ARP in a VLAN
ARP	Aging of ARP entries
LLDP	LLDP
	STP RSTP MSTP
	BPDU protection, root protection, and loop protection
MSTP	Partitioned STP
	ARP and RARP ARP proxy Auto-detection NAT
IPv4 features	Bonjour protocol
	Static route
	RIP-1 and RIP-2 OSPF
	BGP IS-IS
	Routing policies and policy-based routing URPF check
	DHCP server and relay
Unicast routing features	DHCP snooping
	IGMPv1, IGMPv2, and IGMPv3 PIM-SM
	Multicast routing policies
Multicast routing features	RPF
IPv6 features	ND protocol
	Static route RIPng OSPFv3 BGP4+
	IS-IS IPv6 DHCPv6
	DHCPv6 snooping
Unicast routing features	Description
	MLD
Multicast routing features	MLD snooping
BFD	BFD
	IGMP snooping Prompt leave Multicast traffic control
Layer 2 multicast	Inter-VLAN multicast replication
	Neighbor discovery Link monitoring Fault notification
EFM OAM	Remote loopback
Traffic classification	Traffic classification based on the combination of the L2 protocol header, IP 5- tuple, and 802.1p priority
	Access control after traffic classification Traffic policing based on traffic classification
	Re-marking packets based on traffic classifiers Class-based packet queuing
Action	Associating traffic classifiers with traffic behaviors

Queue scheduling	PQ scheduling DRR scheduling
	PQ+DRR scheduling WRR scheduling
	PQ+WRR scheduling
Congestion avoidance	SRED WRED
Application control	Smart Application Control (SAC)
Terminal service	Configurations using command lines
	Error message and help information in English Login through console and Telnet terminals
	Send function and data communications between terminal users
File system	File systems
	Directory and file management
	File uploading and downloading using FTP and TFTP
Debugging and maintenance	Unified management over logs, alarms, and debugging information Electronic labels
	User operation logs
	Detailed debugging information for network fault diagnosis Network test tools such as traceroute and ping commands Intelligent diagnosis
	Interface mirroring and flow mirroring
Version upgrade	Device software loading and online software loading
	Description
	BIOS online upgrade
	In-service patching
Network management	ICMP-based ping and traceroute SNMPv1, SNMPv2c, and SNMPv3
	Standard MIB RMON
	NetStream
System security	Different user levels for commands, preventing unauthorized users from accessing device
	SSHv2.0
	RADIUS and HWTACACS authentication for login users ACL filtering
	DHCP packet filtering (with the Option 82 field)
	Local attack defense function that can protect the CPU and ensure that the CPU can process services
	Defense against control packet attacks
	Defenses against attacks such as source address spoofing, Land, SYN flood (TCP SYN), Smurf, ping flood (ICMP echo), Teardrop, broadcast flood, and Ping of Death attacks
	IPSec
	URL filtering Antivirus
	Intrusion prevention
Networking between APs and WLAN ACs	APs and WLAN ACs can be connected through a Layer 2 or Layer 3 network. APs can be directly connected to a WLAN AC.
	APs are deployed on a private network, while WLAN ACs are deployed on the public network to implement NAT traversal.

	WLAN ACs can be used for Layer 2 bridge forwarding or Layer 3 routing.
	WAN authentication escape is supported between APs and WLAN ACs. In local forwarding mode, this feature retains the online state of existing STAs and allows access of new STAs when APs are disconnected from WLAN ACs, ensuring service continuity.
Forwarding mode	Direct forwarding (distributed forwarding or local forwarding) Tunnel forwarding (centralized forwarding)
	Centralized authentication and distributed forwarding
	In direct forwarding mode, user authentication packets support tunnel forwarding.
	Soft GRE forwarding.
	Tunnel forwarding + EoGRE tunnel
WLAN AC discovery	An AP can obtain the device's IP address in any of the following ways:
	Static configuration
	DHCP
	DNS
	The WLAN AC uses DHCP or DHCPv6 to allocate IP addresses to APs. DHCP or DHCPv6 relay is supported.
	On a Layer 2 network, APs can discover the WLAN AC by sending broadcast CAPWAP packets.
Wireless networking mode	WDS bridging:
	Point-to-point (P2P) wireless bridging
	Point-to-multipoint (P2MP) wireless bridging
	Automatic topology detection and loop prevention (STP) Wireless mesh network
	Access authentication for mesh devices
	Mesh routing algorithm
	Go-online without configuration
	Mesh network with multiple MPPs
	Vehicle-ground fast link handover
	Mesh client mode
CAPWAP tunnel	Centralized CAPWAP
	CAPWAP control tunnel and data tunnel (optional)
	CAPWAP tunnel forwarding and direct forwarding in an extended service set (ESS)
	Datagram Transport Layer Security (DTLS) encryption, which is enabled by default for the CAPWAP control tunnel
	Heartbeat detection and tunnel reconnection
Active and standby WLAN ACs	Enables and disables the switchback function. Supports load balancing.
	Supports 1+1 hot backup.
	NOTE
	In 1+1 VRRP HSB mode, WLAN ACs share one virtual IP address, simplifying the network topology.
	Supports N+1 backup.
	Supports wireless configuration synchronization between WLAN ACs.

AP access control	Displays MAC addresses or SNs of APs in the whitelist.
	Adds a single AP or multiple APs (by specifying a range of MAC addresses or SNs) to the whitelist.
	Automatically discovering and manually confirming APs.
	Automatically discovering APs without manually confirming them.
AP profile management	Specifies the default AP profile that is applied to automatically discovered APs.
AP group management	The AP group function is used to configure multiple APs in batches. When multiple APs managed by a WLAN AC require the same configurations, you can add these APs to one
	AP group and configure the AP group to complete AP configuration.
AP region management	Supports three AP region deployment modes:
	Distributed deployment: APs are deployed independently. An AP is equivalent to a region and does not interfere with other APs. APs work at the maximum power anddo not perform radio calibration.
	Common deployment: APs are loosely deployed. The transmit power of each radiois less than 50% of the maximum transmit power.
	Centralized deployment: APs are densely deployed. The transmit power of each radio is less than 25% of the maximum transmit power.
	Specifies the default region to which automatically discovered APs are added.
AP type management	Manages AP attributes including the number of interfaces, AP types, number of radios, radio types, maximum number of virtual access points (VAPs), maximum number of associated users, and radio gain (for APs deployed indoors).
	Provides default AP types.
Network topology management	Supports LLDP topology detection.
AP working mode management	Supports AP working mode switchover. The AP working mode can be switched to the Fat or cloud mode on the AC.
Radio profile management	The following parameters can be configured in a radio profile:
	Radio working mode and rate
	Automatic or manual channel and power adjustment mode
	Radio calibration interval
	The radio type can be set to 802.11b, 802.11b/g, 802.11b/g/n, 802.11g, 802.11n, 802.11g/n, 802.11a, 802.11a/n, 802.11ac, or 802.11ax.
	You can bind a radio to a specified radio profile.
	Supports MU-MIMO.
Unified static configuration of parameters	Radio parameters such as the channel and power of each radio are configured on the WLAN AC and then delivered to APs.
Dynamic management	APs can automatically select working channels and power when they go online.
	In an AP region, APs automatically adjust working channels and power in the event of signal interference:
	Partial calibration: The optimal working channel and power of a specified AP canbe adjusted.

	Global calibration: The optimal working channels and power of all the APs in aspecified region can be adjusted.
	When an AP is removed or goes offline, the WLAN AC increases the power of neighboring APs to compensate for the coverage hole.
	Automatic selection and calibration of radio parameters in AP regions are supported.
Enhanced service capabilities	Band steering: Enables terminals to preferentially access the 5G frequency band, achieving load balancing between the 2.4G and 5G frequency bands.
	Smart roaming: Enables sticky terminals to roam to APs with better signals.
	802.11k and 802.11v smart roaming
	802.11r fast roaming (≤ 50 ms)
ESS management	Allows you to enable SSID broadcast, set the maximum number of access users, and set the association aging time in an ESS.
	Isolates APs at Layer 2 in an ESS. Maps an ESS to a service VLAN.
	Associates an ESS with a security profile or a QoS profile. Enables IGMP for APs in an ESS.
	Supports Chinese SSIDs.
VAP-based service management	Adds multiple VAPs at a time by binding radios to ESSs.
	Displays information about a single VAP, VAPs with a specified ESS, or all VAPs. Supports configuration of offline APs.
	Creates VAPs according to batch delivered service provisioning rules in automatic AP discovery mode.
Service provisioning management	Supports service provisioning rules configured for a specified radio of a specified AP type.
	Adds automatically discovered APs to the default AP region. The default AP region is configurable.
	Applies a service provisioning rule to a region to enable APs in the region to go online.
Multicast service management	Supports IGMP snooping. Supports IGMP proxy.
Load balancing	Performs load balancing among radios in a load balancing group.
	Supports two load balancing modes:
	− Based on the number of STAs connected to each radio
	− Based on the traffic volume on each radio
Bring Your Own Device (BYOD)	Identifies device types according to the OUI in the MAC address.
	Identifies device types according to the user agent (UA) field in an HTTP packet.
	Identifies device types according to DHCP Option information.
	Carries device type information in RADIUS authentication and accounting packets.
Location services	Locates AeroScout and Ekahau tags. Locates Wi-Fi terminals.
	Locates Bluetooth terminals.
	Locates Bluetooth tags.
Spectrum analysis	Identifies the following interference sources: Bluetooth, microwave ovens, cordless phones, ZigBee, game

	controller, 2.4 GHz/5 GHz wireless audio and video devices, and baby monitors.
	Works with the eSight to display spectrums of interference sources.
Hotspot2.0	Supports a Hotspot2.0 network.
Internet of Things (IoT)	Supports IoT cards on the AP to converge the WLAN and IoT.
Navi WLAN AC	Supports remote STA access on the Navi WLAN AC.
Feature	Description
	Supports a license server as the centralized AP license control point. Allows a license server to manage license clients.
Centralized license control	Supports license synchronization between a license server and clients.
Feature	Description
Address allocation of wireless users	Functions as a DHCP server to assign IP addresses to wireless users.
	Supports user blacklist and whitelist. Controls the number of access users:
	Based on APs
	Based on SSIDs
	Logs out users in any of the following ways:
	Using RADIUS DM messages
	Using commands
	Supports various methods to view information:
	Allows you to view the user status by specifying the user MAC address, AP ID, radio ID, or WLAN ID.
	Displays the number of online users in an ESS, AP, or radio.
WLAN user management	Collects packet statistics on air interface based on user.
	Supports intra-AC Layer 2 roaming.
	NOTE
	Users can roam between APs connected to different physical ports on a WLAN AC.
	Supports inter-VLAN Layer 3 roaming on a WLAN AC. Supports roaming between WLAN ACs.
	Supports fast key negotiation in 802.1X authentication.
	Authenticates users who request to reassociate with the WLAN AC and rejects the requests of unauthorized users.
WLAN user roaming	Delays clearing user information after a user goes offline so that the user can rapidly go online again.
	Supports ACLs. Supports user isolation:
	Inter-group isolation
User group management	Intra-group isolation
Feature	Description
WLAN security profile management	Manages authentication and encryption modes using WLAN security profiles.
	Open system authentication with no encryption WEP authentication/encryption
	WPA/WPA2/WPA3 authentication and encryption:
Authentication modes	WPA/WPA2-PSK+TKIP

	WPA/WPA2-PSK+CCMP
	WPA/WPA2-802.1X+TKIP
	WPA/WPA2-802.1X+CCMP
	WPA3-802.1X+GCMP256
	WPA/WPA2-PSK+TKIP-CCMP
	WPA/WPA2-802.1X+TKIP-CCMP WPA/WPA2-PPSK authentication and encryption WPA3-SAE+CCMP authentication and encryption WAPI authentication and encryption:
	Supports centralized WAPI authentication.
	Supports three-certificate WAPI authentication, which is compatible withtraditional two-certificate authentication.
	Issues a certificate file together with a private key.
	Allows users to use MAC addresses as accounts for authentication by the RADIUS server.
	Portal authentication:
	Authentication through an external Portal server
	Built-in Portal authentication and authentication page customization 802.1X authentication:
	Authentication through an external 802.1X server.
	Built-in 802.1X authentication.
Combined authentication	Combined MAC authentication:
	PSK+MAC authentication MAC+portal authentication:
	MAC authentication is used first. When MAC authentication fails, portalauthentication is used.
AAA	Local authentication/local accounts (MAC addresses and accounts) RADIUS authentication
	Multiple authentication servers:
	Supports backup authentication servers.
	Specifies authentication servers based on the account.
	Configures authentication servers based on the account.
	Binds user accounts to SSIDs.
Security isolation	Port-based isolation
	User group-based isolation
Security standards	802.11i, Wi-Fi Protected Access 2 (WPA2), WPA,802.1X
	Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP), and Extensible Authentication
	Protocol (EAP) types:
	EAP-Transport Layer Security (TLS)
	EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)
	Protected EAP (PEAP) v0 or EAP-MSCHAPv2
	EAP-Flexible Authentication via Secure Tunneling (FAST)
	PEAP v1 or EAP-Generic Token Card (GTC) EAP-Subscriber Identity Module (SIM)
WIDS	Rogue device scan, identification, defense, and countermeasures, whichincludes dynamic blacklist configuration and detection of rogue APs, STAs, and network attacks.

Authority control	ACL limit based on the following: Port User group User
Other security features	SSID hiding IP source guard: Configures IP and MAC binding entries statically. Generates IP and MAC binding entries dynamically.
Number of managed APs	Central APs：32 Common APs and RUs：256 NOTE The RUs managed by the WLAN AC do not occupy the AC's license resources. However, the total number of managed common APs and RUs cannot exceed the upper limit allowed by the AC.
Number of access users	4K NOTE The maximum number of access users varies depending on the authentication mode.
Number of MAC address entries	8K
Forwarding capability	6Gbit/s NOTE Packet length: 1024 bytes
Number of VLANs	4K
Number of routing entries	IPv4: 8K IPv6: 2K
Number of ARP entries	6K
Number of multicast forwarding entries	2K
Number of DHCP IP address pools	64 IP address pools, each of which contains a maximum of 8K IP addresses
Number of local accounts	4K
Number of ACLs	4K
Item	Description
Safety standards	IEC60950-1
Item	Description UL60950-1 CSA C22.2#60950-1 EN60950-1 AS/NZS 60950.1 GB 4943
EMC standards	FCC Part15B ETSI EN 300 386 IEC61000-4-11 IEC 61000-4-4 IEC61000-4-2 IEC61000-4-3 IEC61000-4-5 IEC61000-4-6 IEC 61000-3-2 IEC 61000-3-3 AS/NZS CISPR 32 EN55032/EN55024 ICES-003 GB9254
RoHS	Directive 2002/95/EC & 2011/65/EU

Reach	Regulation 1907/2006/EC
WEEE	Directive 2002/96/EC & 2012/19/EU
Oprogramowanie i licencje	
Oprogramowanie do obsługi następującej ilość AP w ramach projektu w trybie HA	100

- **Oprogramowanie Backup**

Licencje	
Ilość hostów do obsłużenia	6
Kompatybilnośc z hiperwisorami	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Microsoft Hyper-V Server (Core) VMware vCenter 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 & 7.0 VMware vSphere 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 & 7.0 VMware ESXi 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 & 7.0
Wymagania obsługi	
Retencja backupów	Automatyczna
CMC	Tak
Opcja Backupu do MS Azure	Tak
Opcja Backupu do Amazon S3	Tak
Opcja Backupu do Wasabi	Tak
Replikacja z optymalizacją WAN	Tak
Ciągła ochrona danych (Continous Data Protection - CDP)	Tak
Wsparcei dla MS Azure Stack HCI	Tak
Liniowa deduplikacja	Tak
Wsparcie dla klastrów Hyper-V (CSV) i Vmware vCenter	Tak
Umożliwienie bootowania z backupu	Tak
Archiwizacja GFS (Grandfather-Fathker-Son)	Tak
Możliwość wielu lokalziacji backupów	Tak
Możliwość odtwarzania na poziomie plików	Tak
Odtwarzanie wirtualnych maszyn na inny host	Tak
Otdtwarzanie writualnych maszyn w trybie Sandbox	Tak
Kopie zapasowe bez przerywania pracy	Tak
Możliwosc odtwarzania wirtulanej maszyny na tym samym hoście lecz z inną nazwa i identyfikatorem	Tak
Szyfrowanie kopi zapasowych AES	Tak
Instalacja klasy On-Permise z wieczystą licencją	Tak

- **Oprogramowanie Wirtualizacyjne**

Wymagania Per Host	
Maksymalna ilość logicznych procesorów do obsłużenia	512

Maksymalna Ilość fizycznej pamięci do obsłużenia	24 TB
Maksymalna ilośc wirtualnych procesórw per Host	2048
Maksymalna ilość wirtulanych maszyn per Host	1024
Wymagania Per Wirtualna Maszyna	
Maksymalna ilość wirtulanych procesorów per wirtualna maszyna	240 dla Gen2 64 dla Gen1
Maksymalna wielkośc wirtualnego dysku	64 TB dla VHDX 2040 dla VHD
Maksymalna ilość dysków	256
Wymagania Per Klaster	
Maksymalna ilośc węzłów	64
Maksymalna ilość wirtulanych maszyn per Host	8000
Wymagania funkcjonalne	
Technologia Live-Migration	Tak
Technologia Storage Live-Migration	Tak
Storage/Network QoS	Tak
Możliwość dodawania w trybie "Hot-Add" wirtualnych dysków, kart sieciowych i RAM	Tak
Możliwość usuwania w trybie "Hot-Remove" wirtualnych dysków, kart sieciowych i RAM	Tak
Dopuszczalna instalacja w ramach bezpłatnych wersji lub jako zezwolenie licencyjne od dostawcy oprgoramowania na podstawie posiadanych już licencji	

- **Oprogramowanie systemów operacyjnych**
- **Licencje dostępowe CAL**
- **Licencje dostępowe RDS CAL**

PREZES ZARZĄDU Zbigniew Ferenc

PROKURENT Bogusław Wójtowicz

Polgrys
Kruszywa Sp. z o.o. Sp.k.
35-041 Rzeszów, ul. Dominikańska 25
e-mail: biuro@polgrys.pl
NIP 813-366-67-94 REGON 180770801