Załącznik nr 4

Szczegółowy opis

Warstwy sieciowej eCareMed

Uproszczony przebieg procesów platformy rozproszonej eCareMed

ZISIS wytwarza dokumentację medyczną w tym EDM. BOSK (Bramka do Oprogramowania Serwera Komunikacyjnego) komunikuje się z ZISIS (Zintegrowany Informatyczny System Informacyjny Szpitala) i poprzez HL7 CDA przekazuje dane do i z OSK (Oprogramowanie Serwera Komunikacyjnego). OSK działa w jednolitej sieci wymiany informacji umożliwiającej stworzenie rozproszonej platformy sieciowej opartej o internet oraz zaawansowane rozwiązania typu „każdy z każdym". Komunikacja prowadzona będzie zgodnie z HL7 CDA, dane obrazowe przekazywane będą w standardzie DICOM. OSK komunikuje się z: ZISIS poprzez BOSK, systemem P1 zgodnie z unikalnym OID (rejestr węzłów prowadzony przez CSIOZ), innymi jednostkami zdrowia oraz z pacjentem. OSK zapewnią świadczenie e-usług na poziomie regionalnym.

Wymagania co do platformy sieciowej i security

Wymaga się aby Warstwa Transportowa oraz Bezpieczeństwa nie były zrealizowane za pomocą tych samych urządzeń/oprogramowania.

Wymaga się aby „Warstwa dostępowa dla podmiotów trzecich" nie była zrealizowana za pomocą tych samych rozwiązań co Warstwa Transportowa czy Bezpieczeństwa.

1. Warstwa Transportowa

Zamawiający wymaga dostarczenia rozwiązania technologicznego zapewniającego bezpieczną komunikację pomiędzy oddziałami uczestniczącymi w projekcie wymiany informacji o stanie zdrowia pacjentów.

Wymagane jest aby wszystkie komponenty w zakresie sprzętu (hardware) jak i oprogramowania (software) przedmiotowego rozwiązania pochodziły od jednego producenta i były objęte wsparciem technicznym producenta na okres min 60 m-cy od daty odbioru, zapewniającym:

- przyjmowanie zgłoszeń serwisowych w trybie 24x7,
- wymianę uszkodzonych podzespołów/urządzeń na nowe w czasie nie dłuższym niż na następny dzień roboczy licząc od chwili zgłoszenia serwisowego, dostawa musi być wykonana do miejsca instalacji sprzętu (w różnych lokalizacjach na terenie województwa śląskiego), bez ponoszenia jakichkolwiek dotykowych opłat przez Zamawiającego,
- zapewnienie prawa do aktualizacji oprogramowania w okresie trwania wsparcia,
- zapewnienie wsparcia technicznego ze strony producenta w zakresie rozwiązywanie problemów technicznych,

Przedmiotowe rozwiązanie musi składać się z następujących elementów:

- urządzenia brzegowe (routery) zapewniające możliwość podłączenia środowiska serwerowego w lokalizacji do sieci rozległej,

- centralny system do zarządzania całością rozwiązania,

Przedmiotowe rozwiązanie musi zapewniać możliwość wykorzystania dowolnego typu łączy sieciowych tj.

- Internet,
- MPLS,
- Linie dzierżawione,
- LTE,

w celu realizacji połączeń pomiędzy lokalizacjami w trybie „każdy z każdym" (full mesh). Przedmiotowe połączenia muszą być szyfrowane z wykorzystaniem protokołów co najmniej TLS, DTLS czy IPsec. Nie dopuszcza się rozwiązań opartych wyłącznie o protokoły SSL.

Rozwiązanie musi zapewniać monitoring, telemetrię jak i możliwość konfiguracji parametrów jakościowych transmisji danych definiowanych programowo (tzw. software defined) dla urządzeń brzegowych jak i aktywnych połączeń z poziomu centralnego systemu zarządzania.

Rozwiązanie musi zapewniać skalowalność w zakresie ilości węzłów jak i przepustowości, która może być wyłącznie uzależniona od typu poszczególnych urządzeń brzegowych i ewentualnie powiązanych z nimi licencji. Wymaga się aby dostępne były urządzenia brzegowe dedykowane obsłudze ruchu sieciowego w zakresie od 10 Mbps do 1 Gbps co pozwoli na instalację odpowiednich urządzeń, dostosowanych do potrzeb poszczególnych lokalizacji (uczestniczących w projekcie) bez konieczności ponoszenia nieuzasadnionych kosztów.

Administracja urządzeniami sieciowymi oraz zarządzanie połączeniami musi odbywać się z poziomu centralnego systemu w oparciu o graficzną konsolę administracyjną umożliwiającą:

- Konfigurowanie urządzeń brzegowych z wykorzystaniem wzorców konfiguracyjnych (tzw. template) pozwalających na szybką, łatwą implementację zmian konfiguracyjnych dla grupy urządzeń. Takie podejście zapewni Zamawiającemu integralność konfiguracji systemu a przez to stabilność działania,
- Konfigurowanie połączeń (jak i ich parametrów jakościowych) służących transmisji danych z wykorzystaniem wzorców konfiguracyjnych (tzw. template) pozwalających na szybką, łatwą implementację zmian konfiguracyjnych dla grupy urządzeń,
- Łatwe wycofywanie wprowadzonych zmian poprzez wersjonowanie konfiguracji,
- Monitoring oraz telemetrię urządzeń jak i aktywnych połączeń,
- Narzędzia do diagnostyki i rozwiązywania problemów, umożliwiające śledzenie ruchu (tzw. packet tracking) czy wizualizację routingu,

Centralny System Zarządzania musi być zrealizowany jako dedykowane urządzenia do instalacji we wskazanym przez Zamawiającego DC lub jako maszyny wirtualne do uruchomienia na infrastrukturze Zamawiającego. Wymaga się zapewnienia wysokiej dostępności w przypadku rozwiązania bazującego na urządzeniach fizycznych. Zamawiający nie dopuszcza wersji chmurowej (tzw. Cloud) dla Centralnego Systemu Zarządzania.

Urządzenia brzegowe (routery) muszą spełniać następujące kryteria:

- wydajność dla transmisji ruchu szyfrowanego min. 1 Gbps,
- jeśli kwestia wydajności wiąże się z stosowną licencją Zamawiający wymaga zapewnienia minimum 100 Mbps dla ruchu szyfrowanego na początkowym etapie projektu,

- min. 4 interfejsy gigabitethernet,
- min. 1 interfejs 4G LTE, ze wbudowanym modemem LTE pracującym z sieciach komórkowych dostępnych na terenie Polski. Zamawiający nie dopuszcza rozwiązań typu modem USB.
- min. 2 redundantne zasilacze AC 230 V,
- możliwość zainstalowania dodatkowych interfejsów sieciowych w postaci karty „Network Module",
- dostęp do urządzenia poprzez Centralny System Zarządzania, ssh oraz „serial console",
- możliwość uruchomienia bez udziału specjalisty IT w miejscu instalacji oraz dalszej zdalnej konfiguracji urządzenia tzw. plug-and-play,
- możliwość wylistowania aktywnej konfiguracji urządzenia z poziomu ssh i wyeksportowanie jej w postaci pliku tekstowego,
- wsparcie dla protokołów routingu statycznego jak i dynamicznego (co najmniej OSPF, BGP)
- obsługa wirtualnych tablic routingu, osobnej dla prefixów warstwy połączeń fizycznych jak i osobnej dla połączeń logicznych dedykowanych transmisji danych produkcyjnych,
- identyfikacja urządzenia poprzez Centralny System Zarządzania na podstawie certyfikatu elektronicznego,
- wsparcie dla technologii kryptograficznej w oparciu o TLS, DTLS, IPSec,
- wsparcie dla mechanizmów QoS umożliwiających priorytetyzację ruchu dla poszczególnych klas,
- możliwość rozpoznawania ruchu na poziomie aplikacji i definiowania na ich podstawie polityk QoS .

Wszystkie komponenty przedmiotowego rozwiązania muszą pochodzić z oficjalnego kanału dystrybucyjnego na terytorium Polski. Urządzenia muszą być nowe, nie używane w innych projektach, nie dopuszcza się urządzeń po renowacji (refubrished).

Licencje na oprogramowanie dostarczone w ramach niniejszego rozwiązania muszą być zarejestrowane na Zamawiającego.

Urządzenia muszą być dostosowane do zasilania napięciem przemiennym 230V, 50Hz. Kable zasilające muszą być przystosowane do powszechnie używanych w Polsce gniazd zasilających.

2. Warstwa Bezpieczeństwa

Zamawiający wymaga dostarczenia rozwiązania technologicznego zapewniającego mechanizmy bezpieczeństwa w ruchu sieciowym pomiędzy poszczególnymi segmentami środowiska serwerowego jak i od strony użytkownika końcowego. Opisywane rozwiązanie jest dedykowane dla pojedynczej lokalizacji biorącej udział w projekcie.

Wymagane jest aby wszystkie komponenty w zakresie sprzętu (hardware) jak

i oprogramowania (software) przedmiotowego rozwiązania pochodziły od jednego producenta i były objęte wsparciem technicznym producenta na okres min 60 m-cy od daty odbioru, zapewniającym:

- przyjmowanie zgłoszeń serwisowych w trybie 24x7,
- wymianę uszkodzonych podzespołów/urządzeń na nowe w czasie nie dłuższym niż na następny dzień roboczy licząc od chwili zgłoszenia serwisowego, dostawa musi być wykonana do miejsca instalacji sprzętu (w różnych lokalizacjach na terenie województwa śląskiego), bez ponoszenia jakichkolwiek dodatkowych opłat przez Zamawiającego,
- zapewnienie prawa do aktualizacji oprogramowania w okresie trwania wsparcia,
- zapewnienie prawa do aktualizacji sygnatur AntyMalware oraz IPS (intrusion protection),

- zapewnienie wsparcia technicznego ze strony producenta w zakresie rozwiązywania problemów technicznych,

Przedmiotowe rozwiązanie musi składać się z następujących elementów:

- Zestaw urządzeń klasy NGFW (Next Generation Firewall) złożony z co najmniej dwóch jednostek mogących pracować w układzie co najmniej Active-Standby,
- Systemu do kolekcji oraz archiwizacji logów z ruchu sieciowego przechodzącego przez ww. urządzenia,
- Stosownych licencji jak i subskrypcji zapewniających realizację niżej wymieniowych funkcjonalności.

oraz spełniać poniższe kryteria:

- co najmniej 12 interfejsów gigabitethernet z czego min 4 definiowane poprzez SFP,
- możliwość definiowania interfejsów logicznych w użyciem technologii vlan tagging oraz interfejsów zagregowanych w wykorzystaniem protokołu LACP,
- minimalna wydajność systemu to 1 Gbps dla ruchu z włączoną obsługą mechanizmów firewall, IPS, Application Control, Antimalware Protection oraz aktywnym logowaniem ruchu,
- minimum 100 000 sesji jednoczesnych,
- minimum 10 000 nowych sesji na sekundę,
- możliwość zdefiniowania wirtualnych systemów (min.4) będących logicznymi instancjami firewall'a,
- możliwość zdefiniowania min. 4 odrębnych tablic routingu,
- obsługa protokołów routingu dynamicznego co najmniej OSPF, BGP,
- możliwość zdefiniowania stref bezpieczeństwa będących logiczną reprezentacją interfejsów oraz obiektów,
- obsługa protokołów IPSec, TLS,
- wsparcie dla Network Address Translation,
- możliwość zdefiniowania co najmniej 2 000 polityk bezpieczeństwa,
- możliwość logowania ruchu przechodzącego przez firewall w postaci – otwarcie, zamknięcie sesji, ilość danych przesłana w jedną i drugą stronę, akcja - permit/deny/drop/reject, widok źrodła, destynacji, interfejsów (zone) źródłowych, docelowych, protokołów/portów, aplikacji
- możliwość definiowania polityk bezpieczeństwa z użyciem:
    1. kont użytkowników, strefa bezpieczeństwa, podsieć jako warunki źródłowe
    2. aplikacja, strefa bezpieczeństwa, podsieć, protokół/port jako warunki docelowe,
    3. mechanizmów bezpieczeństwa w postaci inspekcji antymalwarowej przesyłanych plików,
    4. mechanizmów bezpieczeństwa w postaci inspekcji oraz przeciwdziałaniu włamaniom (IPS),

Systemu do kolekcji oraz archiwizacji logów z ruchu sieciowego przechodzącego przez firewalle powinien być zrealizowany jako dedykowane urządzenie (tzw. appliance) dla każdej z lokalizacji uczestniczących w projekcie.

Dopuszcza się realizację kolektora logów w wersji centralnej (jednego dla wszystkich lokalizacji) jednakże w tym wypadku wymagana jest architektura wysokiej dostępności.

Wymaga się aby przedmiotowy system umożliwiał kolekcję logów z ruchu sieciowego (traffic log) na okres co najmniej 12 miesięcy. Rozwiązanie musi oferować graficzny interfejs użytkownika oferujący podgląd bieżących logów, wyszukiwanie przynajmniej na podstawie kryteriów takich jak:

- source/destination IP
- source/destination port
- action deny/permit
- security policy
- application
- przedział czasowy
- strefa bezpieczeństwa/ interfejs

oraz tworzenie raportów, statystyk.

Wszystkie powyższe komponenty muszą pochodzić od jednego producenta i być objęte jego wsparciem technicznym.

Z uwagi na konieczność zachowania powtarzalności oraz spójności konfiguracji (na etapie eksploatacji) przedmiotowych urządzeń wymaga się aby zapewniony został również Centralny System Zarządzania oferujący przynajmniej następujące funkcje:

- możliwość konfigurowania poszczególnych urządzeń z użyciem wspólnej bazy obiektów (adresy, sieci, usługi, aplikacje),
- wersjonowanie konfiguracji,
- przydzielanie administratorom uprawnień do poszczególnych urządzeń,
- rejestrowanie zmian w konfiguracji urządzeń,

Centralny System Zarządzania musi być zrealizowany jako dedykowane urządzenia do instalacji w miejscu wskazanym przez Zamawiającego lub jako maszyny wirtualne do uruchomienia na infrastrukturze Zamawiającego. Wymaga się zapewnienia wysokiej dostępności

w przypadku rozwiązania bazującego na urządzeniach fizycznych. Zamawiający nie dopuszcza wersji chmurowej (tzw. Cloud) dla Centralnego Systemu Zarządzania.

Wszystkie komponenty przedmiotowego rozwiązania muszą pochodzić z oficjalnego kanału dystrybucyjnego na terytorium Polski. Urządzenia muszą być nowe, nie używane w innych projektach, nie dopuszcza się urządzeń po renowacji (refubrished).

Licencje na oprogramowanie dostarczone w ramach niniejszego rozwiązania muszą być zarejestrowane na Zamawiającego.

Urządzenia muszą być dostosowane do zasilania napięciem przemiennym 230V, 50Hz. Kable zasilające muszą być przystosowane do powszechnie używanych w Polsce gniazd zasilających.

3. Warstwa dostępowa dla podmiotów trzecich.

Zamawiający wymaga dostarczenia i wdrożenia rozwiązania klasy WAF (Web Application Firewall) odpowiedzialnego za ochrony aplikacji webowej udostępniającej dane podmiotom trzecim (nieuczestniczącym bezpośrednio w projekcie) za pośrednictwem sieci Internet.

Niniejsze rozwiązanie ma być dostarczone jako dedykowany sprzęt (tzw. appliance) wraz

z stosownymi licencjami oraz subskrypcjami (jeśli wymagane) na okres min. 5 lat dla realizacji niżej wymienionych funkcjonalności:

- Wsparcie dla min. 5 serwerów obsługiwanych przez WAF (tzw. backend)
- Wydajność min. 50 Mbps,
- Wydajność transakcji HTTPS/SSL – min. 1000/sek,
- Autentykacja dla dostępu administracyjnego co najmniej poprzez LDAP,
- Możliwość definiowania różnych poziomów dostępu dla administratorów,
- SSL offloading,
- Możliwość pracy w układzie active/standby, active/active
- Detekcja i ochrona przed automatycznymi atakami (BOT),
- Możliwość definiowania granularnych białych list odzwierciedlających
- Analiza ruchu i ochrona przed atakami typu odmowa usługi (DOS)
- Maskowanie danych identyfikacyjnych backend serwerów poprzez blokowanie odpowiedzi typu „kod błędu", „http header", „return code" itd.,
- Mechanizmy ochrony przed atakami OWASP top 10,
- Monitoring „życia" backend serwera poprzez cykliczne wysyłanie żądań do aplikacji, pakiety icmp,
- Analiza i raportowanie w zakresie ataków z listy OWASP top 10,
- Możliwość integracji z zewnętrznymi systemami poprzez REST API oparte na standardach JSON,
- Inspekcja danych wychodzących pod kątem wycieku danych (tzw. DLP) z możliwością usuwania czy maskowania wrażliwych danych (w oparciu o zdefiniowane wzorce), logowanie oraz raportowanie zaistniałych zdarzeń tego obszaru.
- Obsługa uwierzytelnienia w oparciu o następujące metody:
    1. SAML v2 dla „web based single-sign-on (SSO),
    2. Weryfikacja certyfikatu klienta,
    3. Integracja z Active Directory, LDAP, Active Directory Federation Services,
    4. Współpraca z systemami podwójnego uwierzytelnienia (tzw. Two-Factor-Authentication" takimi jak RSASecure ID czy DUO Security,

- Możliwość eksportu logów (client request, admin access, firewall traffic log) poprzez protokół syslog oraz FTP,

Wymagane jest aby wszystkie komponenty w zakresie sprzętu (hardware) jak

i oprogramowania (software) przedmiotowego rozwiązania pochodziły od jednego producenta i były objęte wsparciem technicznym producenta na okres min 60 m-cy od daty odbioru, zapewniającym:

- przyjmowanie zgłoszeń serwisowych w trybie 24x7,

- wymianę uszkodzonych podzespołów/urządzeń na nowe w czasie nie dłuższym niż na następny dzień roboczy licząc od chwili otwarcia zgłoszenia serwisowego, dostawa musi być wykonana do miejsca instalacji sprzętu (w różnych lokalizacjach na terenie województwa śląskiego), bez ponoszenia jakichkolwiek dotykowych opłat przez Zamawiającego,
- zapewnienie prawa do aktualizacji oprogramowania w okresie trwania wsparcia,
- zapewnienie wsparcia technicznego ze strony producenta w zakresie rozwiązywanie problemów technicznych,

Wszystkie komponenty przedmiotowego rozwiązania muszą pochodzić z oficjalnego kanału dystrybucyjnego na terytorium Polski. Urządzenia muszą być nowe, nie używane w innych projektach, nie dopuszcza się urządzeń po renowacji (refubrished).

Licencje na oprogramowanie dostarczone w ramach niniejszego rozwiązania muszą być zarejestrowane na Zamawiającego.

Urządzenia muszą być dostosowane do zasilania napięciem przemiennym 230V, 50Hz. Kable zasilające muszą być przystosowane do powszechnie używanych w Polsce gniazd zasilających.

4. Wymagania dla Wykonawcy

Wykonawca jest zobowiązany:

- Dostarczyć wszystkie wymaganych komponentów zarówno sprzętowych jak i programowych do miejsca instalacji,
- Wykonać konfigurację rozwiązania tak aby zapewnić minimalny, wymagany poziom funkcjonalności zdefiniowany przez Koordynatora Projektu ze strony Zamawiającego,
- Opracować dokumentację rozwiązania zawierającą schematy sieci w ujęciu L2 oraz L3, opis kluczowych komponentów rozwiązania oraz zestaw procedur utrzymaniowych,
- Przeszkolić personel techniczny Zamawiającego z zakresu obsługi rozwiązania,
- Zapewnić wsparcie techniczne w trakcie pierwszego roku po przekazaniu rozwiązania Zamawiającemu w wymiarze co najmniej 40 roboczogodzin w ujęciu miesięcznym, szczególnie w zakresie implementacji zmian w konfiguracji oraz rozwiązywaniu problemów eksploatacyjnych,
- Zapewnić wsparcie techniczne w pozostałym okresie w wymiarze co najmniej 8 roboczogodzin w ujęciu miesięcznym, szczególnie w zakresie implementacji zmian w konfiguracji oraz rozwiązywaniu problemów eksploatacyjnych.
