TWORZENIE DODATKOWYCH WĘZŁÓW ECARMED W RAMACH PROJEKTU ŚUM

1. Warstwa komunikacyjna

Warunkiem dołączenia placówki do wspólnej chmury komunikacyjnej eCareMed jest sprzęt sieciowy o następujących, minimalnych parametrach funkcjonalnych:

a) Obsługa połączeń w technologii IPSec w trybie route-based (wirtualny tunel zabezpieczony za pomocą technik kryptografii),

b) Wsparcie dla szyfrowania na następującym poziomie (lub lepszym/wyższym)

Faza I :

- Authentication method - Pre-shared key
- Encryption algorithm - AES-256
- Authentication algorithm - SHA2-256
- PFS - DH Group14
- Lifetime – 28800 sec

Faza II :

- Security protocol – ESP
- Encryption algorithm - AES-256
- Authentication algorithm - SHA2-256
- PFS – none
- Lifetime – 3600 sec

c) Wydajność urządzenia (urządzeń) na poziomie min. 1 Gbps z załączonymi mechanizmami inspekcji ruchu (threat prevention) oraz w IPsec. W razie wykorzystania istniejących urządzeń należy wymaganą wydajność potraktować jako zapas obecnie niewykorzystywanej wydajności.

d) Zdolność do inspekcji ruchu w warstwach 3,4 oraz 7 (NGFW) z rozpoznawaniem aplikacji,

e) Urządzenia muszą być objęte aktywnym wsparciem producenta zapewniającym bieżące aktualizacje sygnatur antimalware oraz intrusion protection,

f) Urządzenia muszą pracować w układzie wysokiej dostępności (HA) active-passive lub active-active,

g) Wymagane jest wsparcie do obsługi routingu dynamicznego BGP,

h) Rozwiązanie musi oferować kolekcję logów z ruchu sieciowego (traffic log) z retencją na okres min. 12 m-cy,

i) Podmiot dołączany musi dysponować łączem internetowym o zarezerwowanej przepustowości min. 100 Mbps dla zestawienia kanałów IPsec.

Obecna topologia sieci (chmury) eCareMed opiera się na połączeniach każdy z każdym (full-mesh).

2. Warstwa dostępowa dla podmiotów trzecich

Środowisko eCareMed w przedmiotowym zakresie bazuje na rozwiązaniach Web Application Firewall o następujących parametrach funkcjonalnych:

- Wsparcie dla min. 5 serwerów obsługiwanych przez WAF (tzw. backend)
- Wydajność min. 50 Mbps,
- Wydajność transakcji HTTPS/SSL – min. 1000/sek,
- Ochrona aplikacji internetowych w zakresie OWASP Top 10
- Geo-IP i reputacja IP (w tym publiczne serwery proxy i węzły Tor)
- Ochrona przed kradzieżą danych wychodzących (Karty kredytowe, PESEL, SSN itp.)
- Kontrola wgrywanych plików
- Zabezpieczenia wgrywanych plików (antywirus i Zaawansowana ochrona przed zagrożeniami)
- Maskowanie strony internetowej
- Kontrola protokołu dla ruchu HTTP i HTTPS
- Szczegółowe zasady dotyczące poszczególnych adresów URL/parametrów
- Kontrola ilości zapytań
- Monitoring „życia" backend serwera poprzez cykliczne wysyłanie żądań do aplikacji, pakiety icmp,
- Ochrona API w zakresie OWASP Top 10
- Bezpieczeństwo interfejsu API (JSON)
- Bezpieczeństwo API (XML)
- Wykrywanie API (JSON)
- Wykrywanie API (XML)
- Ochrona przed skanowaniem stron internetowych, w tym Baza danych znanych botów
- Ochrona przed spamem botów
- Ochrona przed spamem formularzy
- Ochrona przed wstrzykiwaniem poświadczeń
- Ochrona przed atakami Brute Force
- Obsługa CAPTCHA (wewnętrzna, reCAPTCHA v2 i v3)
- Ochrona aplikacji przed atakami DDoS
- TLS/SSL Offloading
- Równoważenie obciążenia i routing zawartości
- Dynamiczne szyfrowanie adresu URL
- Obsługa protokołów HTTP/1.0, HTTP/1.1, HTTP/2.0, WebSocket, FTP/S i IPv6
- Kontrola żądań i odpowiedzi (tłumaczenie adresów URL)
- Buforowanie i kompresja
- Lokalni użytkownicy/grupy (wewnętrzny LDAP), Certyfikaty klienta
- Wsparcie dla LDAP/Active Directory, RADIUS, Kerberos v5, kody dostępu SMS,
- Jedno- i wielodomenowe logowanie jednokrotne
- Usługa Przeciwdziałania zagrożeniom dostarczana przez producenta rozwiązania
- Obsługa implementowania zabezpieczeń dla przynajmniej 8 znanych skanerów podatności
- Wbudowane logowanie (min, dzienniki dostępu, dzienniki audytu, dzienniki zapory sieciowej i dzienniki systemowe)
- Raportowanie na żądanie i zaplanowane z możliwością customizacji raportów

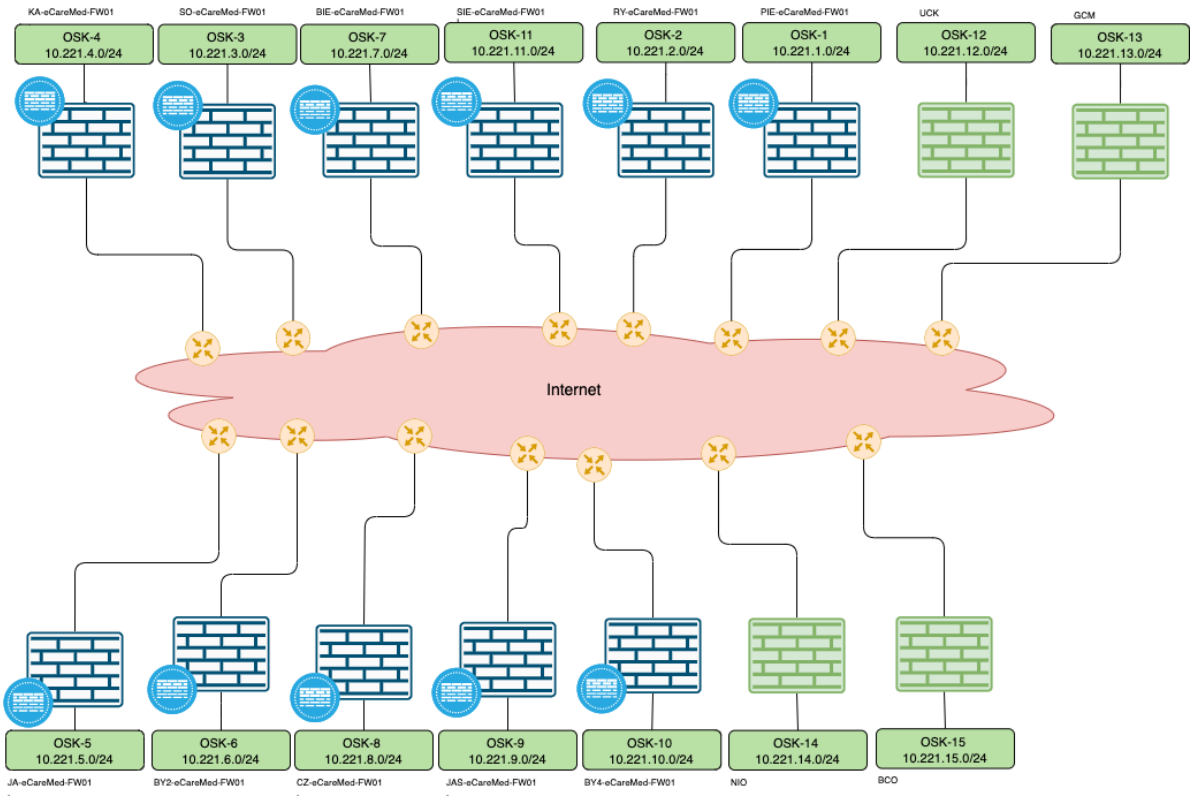
- Możliwość wykorzystania zewnętrznego SysLoga
- Sieciowe listy ACL
- Dodatkowa Zaawansowana ochrona przed botami w trybie subskrypcji
- Dodatkowa Zaawansowana ochrona przed zagrożeniami w trybie subskrypcji

Przedmiotowe wymagania w pełnym zakresie są realizowane przez rekomendowane urządzenia Barracuda Web Application Firewall w wersji nie niższej niż 660. Z uwagi na złożoną architekturę aplikacji zabezpieczanych przez WAF, związaną między innymi z wykorzystywaniem autentykacji poprzez certyfikaty zastosowane rozwiązanie musi zapewniać zaawansowane mechanizmy analizy i ochrony aplikacji web, mechanizmy monitoringu i inspekcji oraz tworzenia profilów aplikacji na podstawie analizy zapytań kierowanych do kontentu backend. Ze względu na wielość lokalizacji, w których serwowana jest aplikacja rozwiązanie musi zapewniać możliwość tworzenia szablonów polityk bezpieczeństwa i łatwej ich dystrybucji pomiędzy urządzeniami w pozostałych lokalizacjach.
Z powyższych przyczyn rekomenduje się zastosowanie urządzeń wymienionych powyżej. Podyktowane jest to zachowaniem spójności środowiska i zapewnieniem maksymalnej ochrony udostępnianych w projekcie rozwiązań. Zastosowanie innych rozwiązań może wywołać komplikacje na poziomie funkcjonowania zabezpieczanych aplikacji, które dana jednostka będzie musiała rozwiązać we własnym zakresie. Jednak WAF nie może mieć gorszych parametrów niż wyżej przedstawione.

3. Topologia połączeń sieciowych

Sieć połączeniowa eCareMed funkcjonuje w modelu full-mesh, gdzie urządzenia brzegowe (firewalle) mają wykreowane połączenia IPsec z trybie każdy z każdym. Oznacza to konieczność zestawiania połączenia IPsec w każdym węźle fullmesh dla 4 jednostek ŚUM. Każda jednostka ŚUM musi zestawić połączenie dla 14 pozostałych jednostek.
Minimalne parametry łącza jak i urządzenie brzegowego są tożsame z pozostałymi jednostki i znajdują się w punkcie 1 wraz z parametrami samego IPsec.

Topologie połączeń przedstawia poniższy diagram.

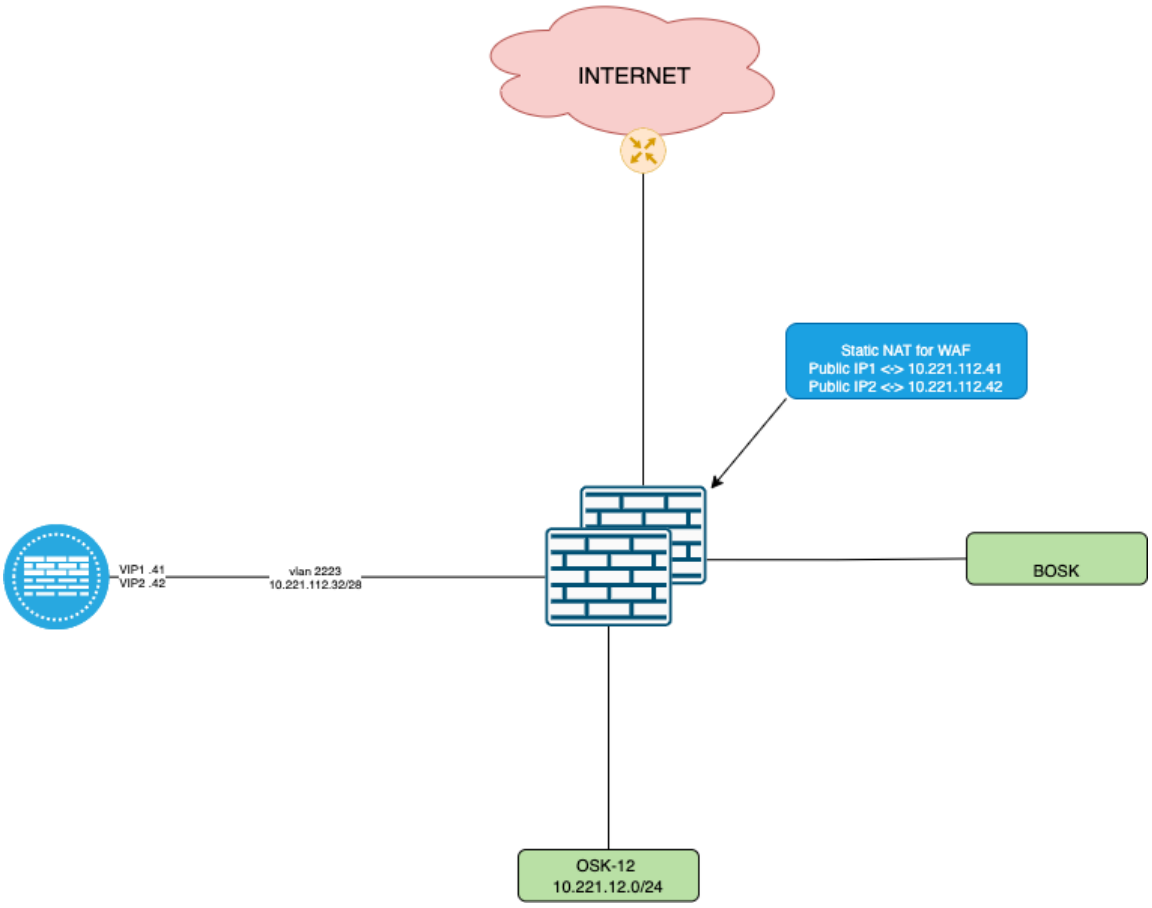


Topologia szczegółowa WAN

Kluczowym aspektem działania chmury komunikacyjnej eCareMed jest zachowanie spójnej adresacji IP w ramach całej struktury. Na potrzeby jednostek ŚUM zaalokowano następujące bloki adresowe:

Jednostka	KOD OSK	Adresacja DMZ	Adresacja OSK
UCK	OSK12	10.221.112.32/28	10.221.12.0/24
GCM	OSK13	10.221.113.32/28	10.221.13.0/24
NIO	OSK14	10.221.114.32/28	10.221.14.0/24
BCO	OSK15	10.221.115.32/28	10.221.15.0/24

Konfiguracja sieci po stronie jednostek ŚUM musi być tożsama z przyjętym modelem, który został wdrożony dla 11 jednostek będących objętych chmurą eCareMed. Niniejsze wynika z konieczności zachowania standaryzacji topologii sieci jak i należytego stopnia bezpieczeństwa poprzez segmentację poszczególnych obszarów jak i inspekcję ruchu pomiędzy nimi.
Poniższy schemat przedstawia topologię sieci LAN w ramach środowiska OSK.



Topologia sieci LAN w ramach OSK

Powyższy schemat prezentuje topologię dla sieci (wraz z adresacją) dla jednostki OSK-12. Stanowi przykład rozwiązania, gdzie dla poszczególnych, pozostałych jednostek należy zastosować nadaną adresację zgodnie z wcześniej przedstawionym planem.
Widoczny w schemacie WAF realizujący funkcje bezpieczeństwa dla aplikacji wystawianych do sieci Internet, którego szczegółowe wymagania określone zostały w pkt. 2.
Ruch sieciowy pomiędzy środowiskiem BOSK a OSK podlegać musi inspekcji na firewallu. Definicje polityk muszą być wdrożone zgodnie z wytycznymi dostawcy oprogramowania eCareMed.
Połączenia pomiędzy komponentami systemu eCareMed (serwery OSK) w poszczególnych lokalizacjach muszą być zrealizowane zgodnie z wytycznymi dostawcy oprogramowania.
Połączenia do serwerów OSK ze strony sieci szpitala muszą ograniczać się wyłącznie do komunikacji BOSK-OSK.

4. Wymagania ogólne dla każdego szpitala

1. Dedykowane Projektowi łącze internetowe o minimalnym transferze danych 100/100 Mbit/s.
2. Posiadanie medycznego systemu komputerowego umożliwiającego prowadzenie dokumentacji w postaci elektronicznej i rozliczeń w pełnym zakresie działania (szpital,

poradnia, izba przyjęć, rehabilitacja, diagnostyka itp.).
3. Posiadanie archiwum PACS, wraz z systemem umożliwiającym integrację z systemem HIS
w zakresie przekazywania zdjęć w formacie DICOM oraz opisów z RIS. Integracja aparatury poprzez HL7.
4. Połączenie LIS z systemem HIS w zakresie zlecania badań oraz automatycznego odbioru wyników badań w postaci elektronicznej.
5. Posiadanie oprogramowania w zakresie EDM oraz macierzy dyskowej celem przechowywania REDM.
6. Posiadanie PIS oraz integracji z systemem HIS.
7. Posiadanie BOSK umożliwiającej komunikację z OSK poprzez HL7 CDA.
8. Posiadanie wydzielonej serwerowni spełniającej warunki bezpieczeństwa danych.
9. Posiadanie serwerów, macierzy, pozwalających na instalację systemów szpitalnych ZISIS: HIS, LIS, PIS, RIS, PACS, z BOSK oraz OSK. Założono wirtualizację środowiska.
10. Posiadanie systemu back-up, zabezpieczającego dane serwerów (maszyny wirtualne oraz obszary danych). Dane PACS archiwizowane na tasiemkach lub dodatkowej macierzy dyskowej.
11. Posiadanie jednolitej sieci wymiany informacji umożliwiającej stworzenie rozproszonej platformy sieciowej opartej o internet oraz zaawansowane rozwiązania typu „każdy z każdym” (fullmesh).
12. Posiadanie OSK komunikującego się z systemem P1, innymi OSK, z jednostkami zdrowia oraz pacjentem.
13. Posiadanie sieci komputerowej spełniającej warunki bezpieczeństwa danych.
14. Posiadanie wymaganej liczby stacji roboczych, tabletów itp.
15. Posiadanie infrastruktury umożliwiającej elektroniczne podpisywanie dokumentów: czytniki, podpisy elektroniczne (ZUS, podpis kwalifikowany, nowy dowód osobisty).
16. Posiadanie wymaganej liczby licencji oprogramowania (serwerowego, systemowego, biurowego, antywirusowego itp.)