

## Wymagania techniczne aplikacji LSI

Właściciel Dokumentu:	BLStream Sp. z o.o.
Data utworzenia	2008-04-18
Data ostatniego zapisu:	2008-06-23
Autorzy:	PKW, LRO

## Spis Treści

<b>1. Cel dokumentu.....</b>	<b>4</b>
<b>2. Informacje wstępne.....</b>	<b>4</b>
<b>3. Wymagania dot. oprogramowania.....</b>	<b>5</b>
3.1. Serwer HTTP.....	5
3.2. Serwer HTTPS.....	6
3.3. Serwer aplikacji.....	6
3.4. Serwer bazy danych.....	6
3.5. Serwer MTA.....	6
3.6. VPN.....	6
<b>4. Wymagania dot. Infrastruktury.....</b>	<b>9</b>
4.1. Serwis Beneficjenta.....	9
4.1.1. Konfiguracja zapory sieciowej dla SB.....	10
4.2. Baza Danych.....	11
4.2.1. Konfiguracja zapory sieciowej dla BD.....	12
4.3. Centra certyfikacyjne.....	13
4.3.1. BD CA.....	13
4.3.2. BD VPN CA.....	13
4.3.3. SB VPN CA.....	13
4.4. Kopie bezpieczeństwa.....	14
<b>5. Spełnienie wymogów.....</b>	<b>14</b>

## Rysunki

<b>Rysunek 1 Komponenty systemu LSI.....</b>	<b>5</b>
<b>Rysunek 2 Architektura Serwisu Beneficjenta.....</b>	<b>7</b>
<b>Rysunek 3 Architektura Bazy Danych.....</b>	<b>8</b>
<b>Rysunek 4 Infrastruktura systemu LSI.....</b>	<b>9</b>
<b>Rysunek 5 Serwis Beneficjenta.....</b>	<b>10</b>
<b>Rysunek 6 Baza Danych.....</b>	<b>12</b>

## Akronimy i skróty

BD	Baza Danych
CA	Centrum Certyfikacji
DMZ	Strefa zdemilitaryzowana – wydzielony na zaporze sieciowej obszar sieci komputerowej nie należący ani do sieci wewnętrznej ani do sieci zewnętrznej
ICMP	Internetowy protokół komunikatów kontrolnych
EJB	Standardowy zestaw interfejsów i modeli przesyłania komunikatów w języku programowania Java
ODBC	Standardowy zestaw interfejsów do komunikacji z systemem zarządzającym bazami danych
MTA	Agent przesyłania poczty elektronicznej
SB	Serwis Beneficjenta
VLAN	Sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej
VPN	Wirtualna Sieć Prywatna

## 1. Cel dokumentu

Niniejszy dokument ma na celu sprecyzować wymagania w stosunku do oprogramowania oraz elementów infrastruktury niezbędnych dla prawidłowego funkcjonowania aplikacji LSI.

## 2. Informacje wstępne

Aplikacja LSI składa się z dwóch komponentów:

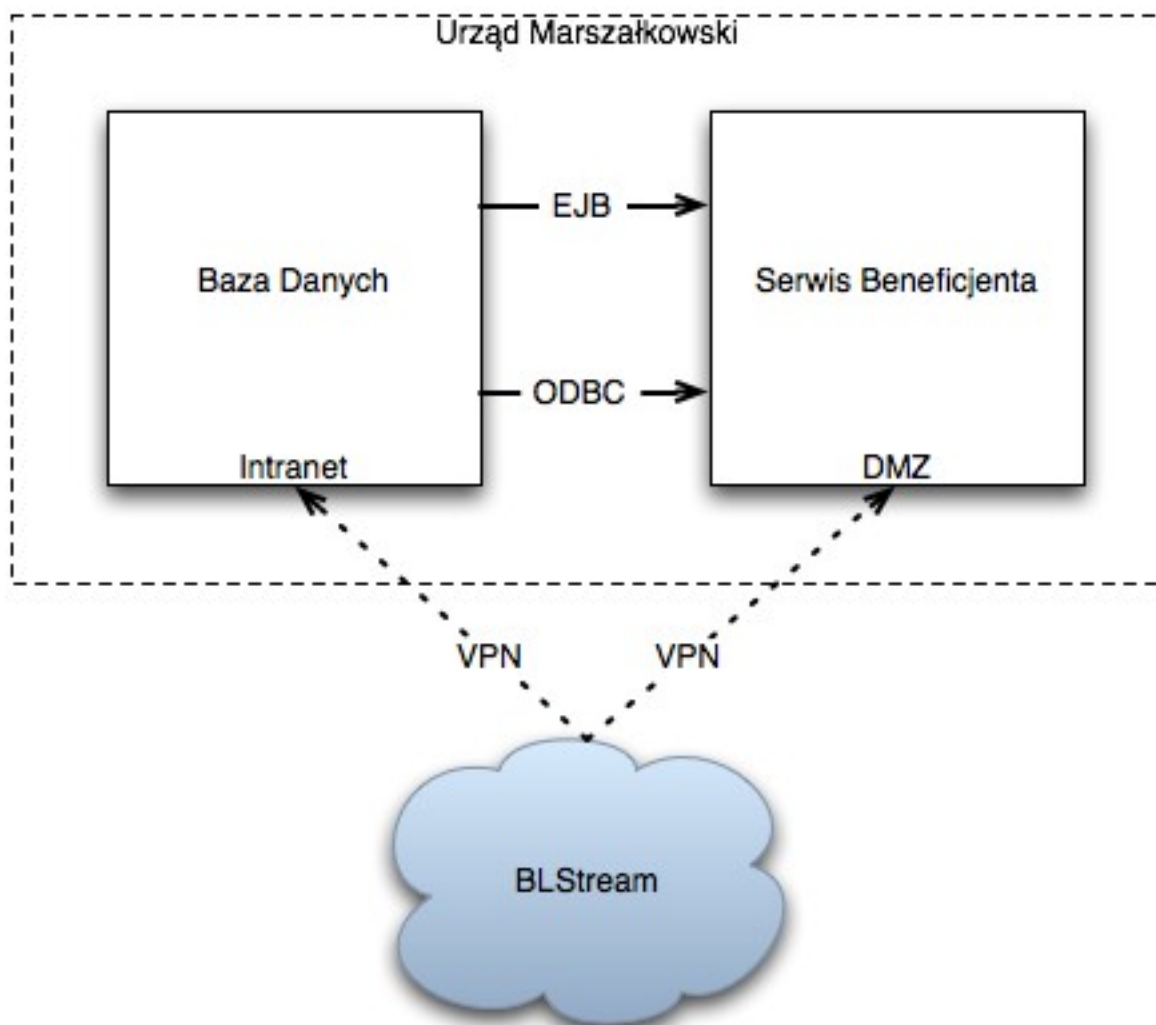
1. **Serwis Beneficjenta**, dalej nazywany SB, jest serwisem publicznym (dostępnym z sieci Internet), z którego mogą korzystać beneficjenci w celu składania wniosków.
2. **Baza Danych**, dalej nazywana BD, jest serwisem wewnętrznym (dostępnym tylko z sieci urzędu), z którego mogą korzystać pracownicy urzędu w celu obsługi wniosków beneficjentów.

Aplikacja jako całość jest hermetycznym systemem z bezpieczną infrastrukturą sieciową. Podstawowe części składowe infrastruktury to dwie podsieci: DMZ oraz Intranet.

1. **DMZ** jest tzw. strefą zdemilitaryzowaną, do której dostęp jest ograniczony za pomocą firewalla do niezbędnego minimum. Zarządzanie i utrzymanie przez pracowników BLStream musi być zapewnione przez bezpieczną sieć prywatną VPN.
2. **Intranet**, czyli wewnętrzna sieć urzędu, jest środowiskiem dla aplikacji BD. Dostęp tak samo musi być ograniczony do niezbędnego minimum. Z zewnątrz jedyny dostęp do BD jest realizowany poprzez osobny VPN, w celu zarządzania i utrzymywania usługi.

Komunikacja między dwoma podsieciami musi być ograniczona do minimum. Jedynie komunikaty do kolejki EJB oraz komunikaty do zarządzania bazą danych (ODBC) mogą być przekazywane z Intranetu do DMZ.

Poniższa ilustracja przedstawia poszczególne elementy systemu.



Rysunek 1 Komponenty systemu LSI

### 3. Wymagania dot. oprogramowania

Komponenty SB i BD mają następujące, częściowo wspólne wymagania dot. oprogramowania:

#### 3.1. Serwer HTTP

Zalecany oprogramowaniem jest Apache 2.

Serwer HTTP jest wymagany jedynie do realizacji przekierowania całego ruchu na serwer HTTPS, który świadczy konkretne usługi.

### 3.2. Serwer HTTPS

Zalecany serwerem HTTPS jest Apache 2 z rozszerzeniem mod\_ssl.

Serwer HTTPS pełni rolę pośrednika między użytkownikami a serwerem aplikacji JBOSS, przy okazji zapewniając szyfrowanie transmisji.

W przypadku SB, ze względu na wrażliwość przesyłanych danych przez beneficjentów, serwer musi identyfikować się certyfikatem SSL wystawionym przez zaufany urząd certyfikacyjny (np. Thawte, Verisign, Certum).

W przypadku BD, serwer może się identyfikować certyfikatem wystawionym przez własne centrum certyfikacyjne.

### 3.3. Serwer aplikacji

Wymagany serwerem aplikacji jest JBOSS w wersji 4.2.2 + EJB + ODBC.

Serwer JBOSS nie może bezpośrednio świadczyć usług, więc ruch do aplikacji musi przechodzić przez proxy realizowane przez serwer HTTPS. EJB jest serwisem do przesyłania komunikatów między aplikacjami i za jego pomocą realizowana jest komunikacja między BD i SB. Dodatkowo połączenie ODBC zapewni możliwość generowania raportów bezpośrednio z bazy danych SB.

### 3.4. Serwer bazy danych

Wymagana jest najnowsza wersja PostgreSQL 8.3.1.

Serwer bazy danych służy do przechowywania danych wprowadzanych przez beneficjentów.

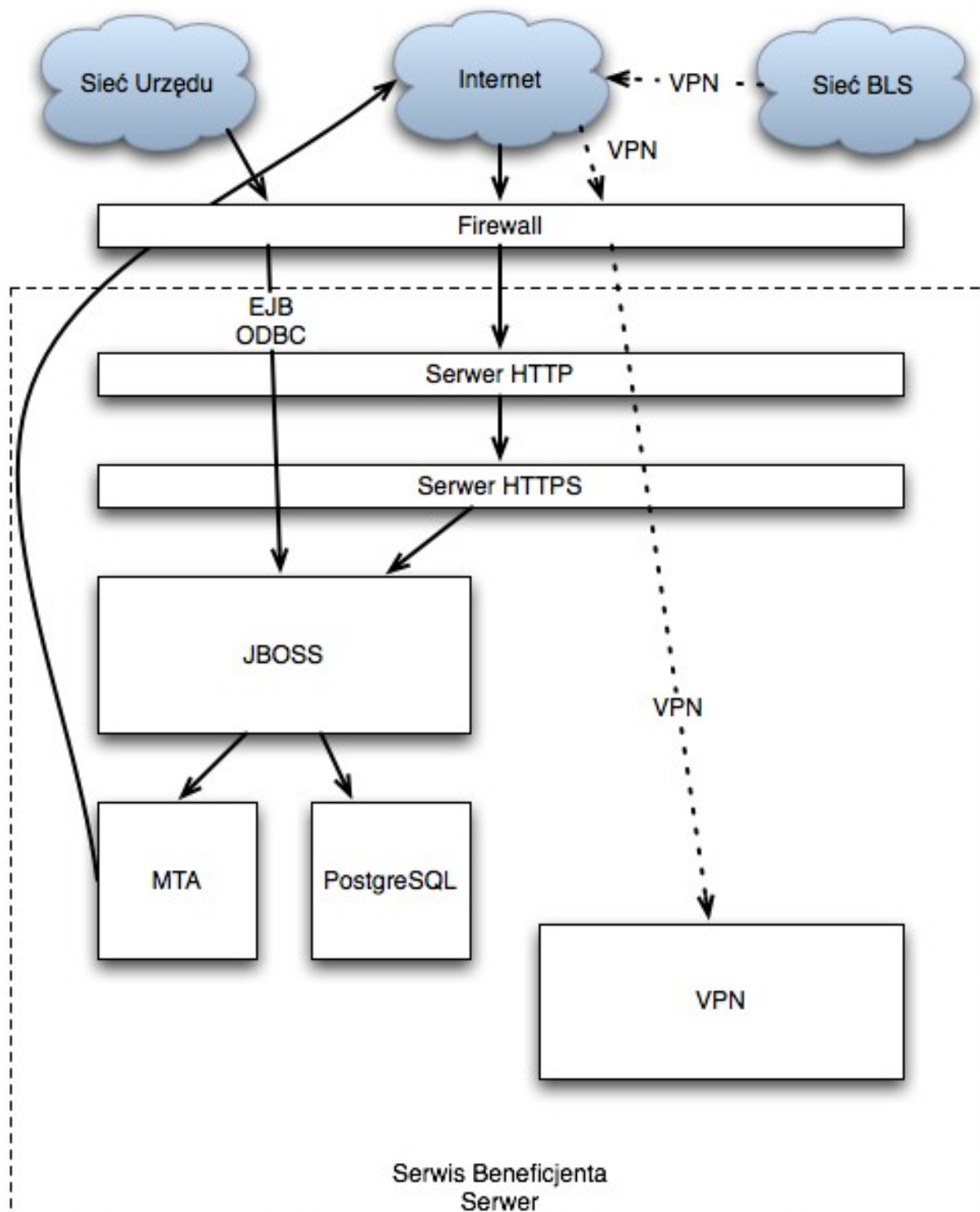
### 3.5. Serwer MTA

Zalecanymi MTA są Exim lub Postfix. MTA służy do wysyłania poczty e-mail bezpośrednio z aplikacji SB lub BD do beneficjentów (wymagane przy rejestracji beneficjenta).

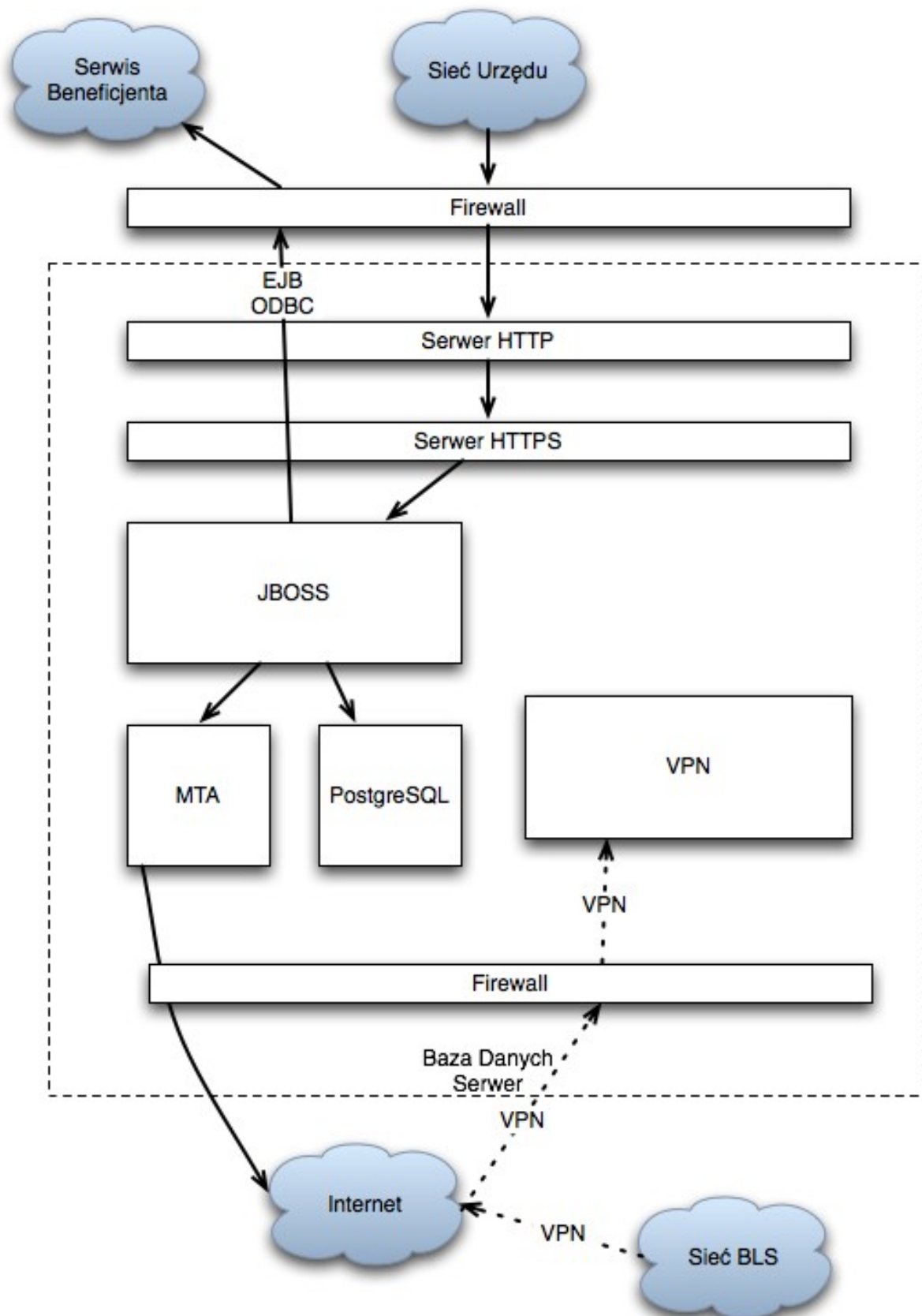
### 3.6. VPN

Zalecane programowanie realizujące VPN to OpenVPN 2.0.9 lub inne wspierające protokół IPsec oraz Certificate Based Authentication.

VPN realizuje bezpieczną, wirtualną sieć, która jest wymagana do utrzymywania aplikacji przez pracowników BLStream. Sieć VPN może być zabezpieczona certyfikatami SSL wystawionymi przez własne centrum certyfikacyjne, nie są konieczne certyfikaty wystawione przez zaufany urząd certyfikacyjny.



**Rysunek 2 Architektura Serwisu Beneficjenta**

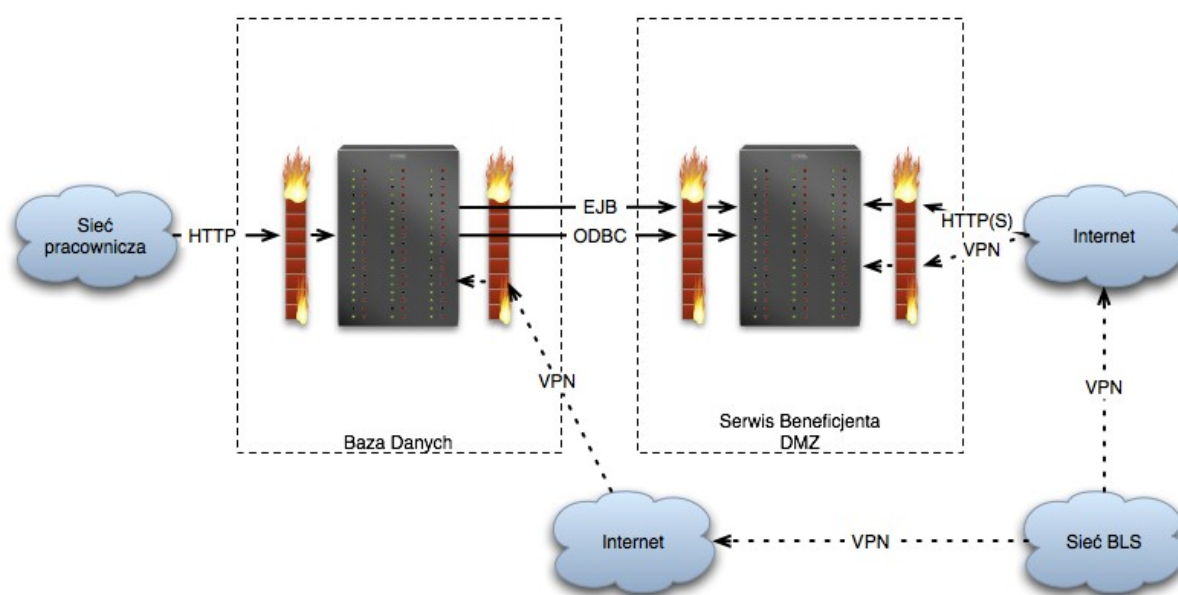


**Rysunek 3 Architektura Bazy Danych**



## 4. Wymagania dot. Infrastruktury

Ze względu na wrażliwość danych wprowadzanych i przetwarzanych w systemie LSI, wymagane są pewne środki bezpieczeństwa odnośnie infrastruktury. Środowisko dla systemu LSI musi być zamknięte na tyle na ile jest to możliwe. Ruch sieciowy do aplikacji SB, BD a także pomiędzy nimi musi być ograniczony do niezbędnego minimum przez zapory sieciowe oraz samą budowę infrastruktury, którą przedstawia poniższa ilustracja.

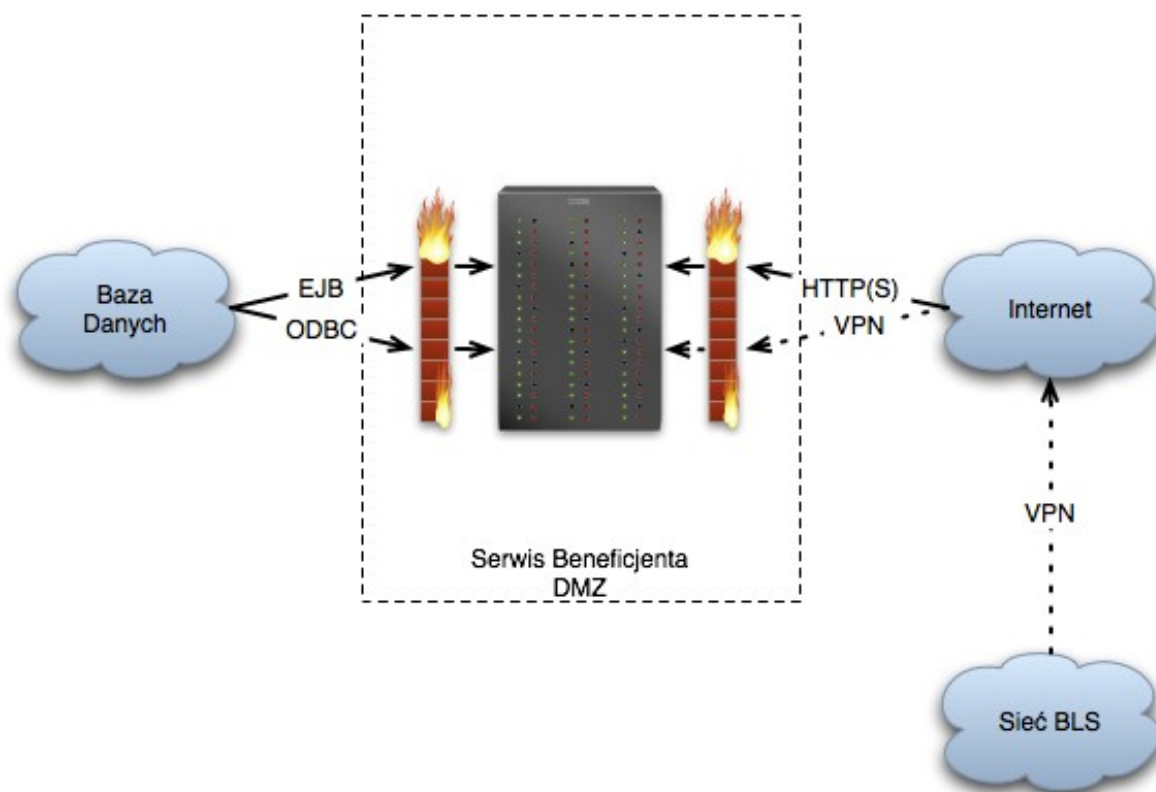


Rysunek 4 Infrastruktura systemu LSI

### 4.1. Serwis Beneficjenta

SB musi być zamknięty w osobnej strefie DMZ, czyli hermetycznie zamkniętej sieci. Serwer świadczący usługę SB musi być fizycznie odcięty od innych usług świadczonych przez Urząd, np. poprzez implementację wirtualnej sieci za pomocą VLAN, bądź wydzielonego na te potrzeby fizycznego dedykowanego okablowania strukturalnego wraz z dedykowanymi urządzeniami pasywnymi i aktywnymi.

Dostęp do DMZ SB musi być ograniczony za pomocą firewalla do niezbędnego minimum. Z jednej strony musi być zapewniony dostęp z sieci Internet, z drugiej zaś dostęp z serwera świadczącego usługę BD. Nie może przy tym być przepuszczany jakikolwiek ruch z sieci Internet do BD.



Rysunek 5 Serwis Beneficjenta

#### 4.1.1. Konfiguracja zapory sieciowej dla SB

Zapora sieciowa firewall powinna być tak skonfigurowana, aby umożliwić dostęp do SB tylko w następujący sposób:

- Z Internetu na port TCP/80.

Na porcie 80 jest uruchomiony serwer HTTP, którego jedynym zadaniem jest przekierowanie ruchu do serwera HTTPS.

- Z Internetu na port TCP/443.

Jest to ruch przeznaczony do serwera HTTPS, pośrednika do serwera JBOSS serwującego konkretną aplikację SB.

- Z Internetu z adresu 212.14.0.241 na port UDP/1194.

Standardowy port dla oprogramowania OpenVPN, umożliwiającego kontrolę nad serwerem przez pracowników BLStream. Dodatkowo ograniczamy ruch tylko dla adresu IP z sieci BLStream.

- Z Internetu ruch ICMP.

ICMP to protokół kontrolny, potrzebny do zapewnienia poprawnej komunikacji sieciowej.

- Z Internetu ruch powiązany (ESTABLISHED, RELATED).

Standardowa reguła przepuszczająca ruch powiązany z ustanowionymi już połączeniami.

- Z BD ruch na port TCP/2468 (EJB).

Wpuszczamy także komunikaty z serwera świadczącego usługi BD potrzebne do synchronizacji.

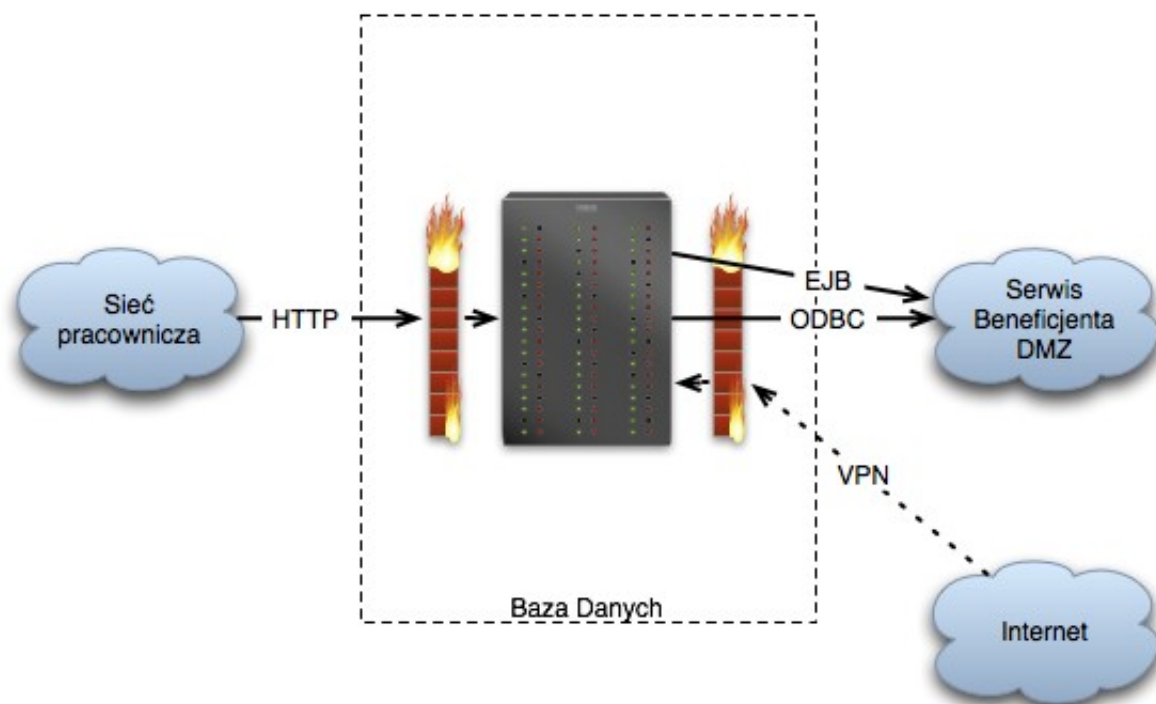
- Z BD ruch na port TCP/1433 (ODBC).

Zezwalamy na połączenia do bazy danych za pomocą mechanizmu ODBC, w celu generowania raportów.

Reszta ruchu sieciowego będzie blokowana.

## 4.2. Baza Danych

Serwer świadczący usługę BD musi być dostępny w sieci wewnętrznej Urzędu, lecz musi być odcięty od innych usług świadczonych przez Urząd. Musi być także odcięty od sieci Internet. Jedynie usługa VPN może być dostępna z zewnątrz, ale musi być ograniczona do adresu IP sieci BLStream. Ograniczenia dostępu będzie realizować firewall.

**Rysunek 6 Baza Danych**

#### 4.2.1. Konfiguracja zapory sieciowej dla BD

Zapora sieciowa firewall powinna być tak skonfigurowana, aby umożliwić dostęp do BD tylko w następujący sposób:

- Z Internetu z adresu 212.14.0.241 na port UDP/1194.

Standardowy port dla oprogramowania OpenVPN, umożliwiającego kontrolę nad serwerem przez pracowników BLStream. Dodatkowo ograniczamy ruch tylko dla adresu IP z sieci BLStream.

- Z Internetu ruch powiązany (ESTABLISHED, RELATED).

Standardowa reguła przepuszczająca ruch powiązany z ustanowionymi już połączeniami.

- Z sieci Urzędu na port TCP/80.

Na porcie 80 jest uruchomiony serwer HTTP, którego jedynym zadaniem jest przekierowanie ruchu do serwera HTTPS.

- Z sieci Urzędu na port TCP/443.

Jest to ruch przeznaczony do serwera HTTPS, pośrednika do serwera JBOSS serwującego

konkretną aplikację BD.

- Z sieci Urzędu ruch ICMP.

ICMP to protokół kontrolny, potrzebny do zapewnienia poprawnej komunikacji sieciowej.

- Z sieci Urzędu ruch powiązany (ESTABLISHED, RELATED).

Standardowa reguła przepuszczająca ruch powiązany z ustanowionymi już połączeniami.

Reszta ruchu sieciowego będzie blokowana.

### 4.3. Centra certyfikacyjne

Dla zapewnienia bezpiecznej transmisji danych wymagane są trzy własne centra certyfikacyjne (CA).

#### 4.3.1. BD CA

CA dla aplikacji BD, które wyda certyfikat SSL używany do transmisji danych wewnątrz Urzędu, między pracownikami a serwerem świadczącym usługę BD.

#### 4.3.2. BD VPN CA

Centrum, które wyda certyfikaty SSL używane w sieci VPN koniecznej do utrzymywania aplikacji BD, przez pracowników BLStream.

#### 4.3.3. SB VPN CA

Centrum, które wyda certyfikaty SSL używane w sieci VPN koniecznej do utrzymywania aplikacji SB, przez pracowników BLStream.

Bezpieczną transmisję danych między beneficjentami a aplikacją SB zapewnić będzie certyfikat SSL wydany przez zaufane centrum certyfikacyjne.

## 4.4. Kopie bezpieczeństwa

W sieci Intranet powinna być zapewniona usługa backupów on-site. Kopie bezpieczeństwa są wymagane do odtworzenia oryginalnych danych w przypadku ich utraty. Kopie bezpieczeństwa dzielimy na trzy grupy:

1. **Pełna:** całkowita kopia bezpieczeństwa wszystkich danych.
2. **Różnicowa:** Kopia bezpieczeństwa plików, które uległy zmianie od ostatniej pełnej kopii bezpieczeństwa.
3. **Przyrostowa:** Kopia bezpieczeństwa plików, które uległy zmianie od ostatniej pełnej kopii bezpieczeństwa, albo od ostatniej kopii różnicowej, albo od ostatniej kopii przyrostowej.

By zwiększyć poziom bezpieczeństwa, kopie powinny być wykonywane w dwóch niezależnych turach. Dzięki temu będą osobne dwie niezależne kopie bezpieczeństwa wszystkich danych.

Serwer zapewniający usługę kopii bezpieczeństwa powinien być dostępny zarówno z podsieci BD jak i ze strefy DMZ SB. Zalecane oprogramowanie do wykonywania automatycznych backupów to Bacula.

Oprócz usługi backupów on-site zalecana jest usługa kopii bezpieczeństwa off-site zapewniająca tygodniowe backupy.

## 5. Spełnienie wymogów

Na podstawie wypełnionych wymagań oraz audytów ze strony dostawcy, nastąpi autoryzacja środowiska klienta w celu wdrożenia produkcyjnego oraz zapewnienia usługi asysty technicznej ze strony dostawcy.

W przypadku braku autoryzacji, wdrożenie nastąpi wyłącznie na odpowiedzialność klienta i uniemożliwi prowadzenia prac ze strony dostawcy w celu świadczenia asysty technicznej.