|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
| **Ministerstwo Finansów** |  |  |
| *Właściciel* |  |  |
|  |  |  |
| <Szablon>  Projekt Infrastruktury Teleinformatycznej  Systemu (…) |  |  |
| *nazwa dokumentu* |  |  |
|  |  |  |
| PUESC…………… |  |  |
| *nazwa Projektu* |  |  |
|  |  |  |
| **30.03.2017r.**  **0.05** |  |  |
| *wersja* |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# SPIS TREŚCI

[1. SPIS TREŚCI 2](#_Toc465801839)

[2. Wstęp 4](#_Toc465801840)

[3. Słowniki 6](#_Toc465801841)

[3.1. Używane terminy i skróty technologiczne 6](#_Toc465801842)

[3.2. Terminy i skróty specyficzne dla Systemu 6](#_Toc465801843)

[3.3. Symbole graficzne 7](#_Toc465801844)

[3.4. Dane kontaktowe 9](#_Toc465801845)

[4. Wymagania formalne 10](#_Toc465801846)

[5. Rodzaje środowisk systemu 10](#_Toc465801847)

[6. Projekty poszczególnych środowisk 10](#_Toc465801848)

[6.1. Projekt środowiska (…) Systemu 10](#_Toc465801849)

[6.1.1. Klasa systemu 10](#_Toc465801850)

[6.1.2. Klasa bezpieczeństwa systemu 11](#_Toc465801851)

[*6.1.2.1.* Bezpieczeństwo w środowisku 11](#_Toc465801852)

[6.1.3. Uwierzytelnianie użytkowników i administratorów w środowisku 12](#_Toc465801853)

[6.1.4. Obciążenia połączeń sieciowych. 12](#_Toc465801854)

[6.1.5. Architektura Środowiska Systemu 13](#_Toc465801855)

[6.1.6. Platforma Środowiska Systemu 14](#_Toc465801856)

[6.1.6.1. Usługi dostępowe 14](#_Toc465801857)

[6.1.6.2. Usługi dostarczające bloki architektoniczne aplikacyjne 15](#_Toc465801858)

[6.1.6.3. Usługi dostarczające bloki architektoniczne bazodanowe 15](#_Toc465801859)

[6.1.6.4. Usługi dostarczające bloki architektoniczne OS 15](#_Toc465801860)

[6.1.6.5. Dodatkowe oprogramowanie wymagane w Środowisku Systemu 15](#_Toc465801861)

[6.1.7. Podstawowe informacje niezbędne do skonfigurowania infrastruktury komunikacyjnej warstwy dostępowej 16](#_Toc465801862)

[6.1.7.1. Adresacja IP środowiska Systemu 16](#_Toc465801863)

[6.1.7.2. Wymagania niezbędne do konfiguracji środowiska proxy i zewnętrznego Load Balancera 17](#_Toc465801864)

[6.1.7.2.1. Opis usług aplikacyjnych 17](#_Toc465801865)

[6.1.7.2.2. Lista przekierowań (redirect, rewrite) 17](#_Toc465801866)

[6.1.7.2.3. Określenie algorytmu balansowania ruchu na zewnętrznych Load Balancer’ach Cisco ACE30 17](#_Toc465801867)

[6.1.7.2.4. Definicja próbkowania dla każdej z usług aplikacyjnych 17](#_Toc465801868)

[6.1.7.2.5. Certyfikaty na potrzeby komunikacji HTTPS. 17](#_Toc465801869)

[6.1.7.2.6. Inne wymagania 17](#_Toc465801870)

[6.1.7.3. Wymagania dla warstwy aplikacyjnej (niezbędne do konfiguracji wewnętrznego Load Balancer’a) 17](#_Toc465801871)

[6.1.7.3.1. Opis usług aplikacyjnych 17](#_Toc465801872)

[6.1.7.3.2. Opis farm/klastrów serwerów 17](#_Toc465801873)

[6.1.7.3.3. Określenie algorytmu balansowania ruchu na wewnętrznych Load Balancer’ach Cisco ACE30 17](#_Toc465801874)

[6.1.7.3.4. Dla których usług aplikacyjnych/farm serwerów wymagane jest włączenie funkcjonalności session-persistance i jakie parametry muszą zostać użyte dla sesji sticky 17](#_Toc465801875)

[6.1.7.3.5. Inne wymagania 18](#_Toc465801876)

[6.1.7.3.6. Dane konieczne do przepuszczenia ruchu dla komunikacji między systemami oraz wewnątrz Systemu 19](#_Toc465801877)

[6.1.7.3.7. Dane konieczne do przepuszczenia ruchu dla użytkowników i administratorów: 19](#_Toc465801878)

[6.1.7.3.8. Dane konieczne do utworzenia wpisów w DNS dla usług udostępnianych przez środowisko systemu biznesowego 20](#_Toc465801879)

[6.1.7.4. Filtracja IPS w infrastrukturze CPD MF 21](#_Toc465801880)

[6.1.8. Wymagania środowiska dla systemu backupowego 22](#_Toc465801881)

[6.1.8.1. Wymagania na polityki tworzenia kopii bezpieczeństwa 22](#_Toc465801882)

[6.1.8.2. Zabezpieczane elementy środowiska 22](#_Toc465801883)

[7. Zestawienie bloków architektonicznych 23](#_Toc465801884)

[8. Procedura uzyskiwania dostępu do poszczególnych bloków architektonicznych w środowisku Usług Katalogowych. 24](#_Toc465801885)

[9. Grupy Zabezpieczeń 25](#_Toc465801886)

[9.1 Konta serwisowe 25](#_Toc465801887)

[9.2 Czynności serwisowe wymagające wyższych uprawnień 25](#_Toc465801888)

[Historia zmian 26](#_Toc465801889)

Tabele

[Tabela 1. Lista dokumentów powiązanych i/lub referencyjnych 5](#_Toc465801890)

[Tabela 2. Terminy i skróty specyficzne dla Systemu 6](#_Toc465801891)

[Tabela 3. Rodzaje środowisk Systemu 10](#_Toc465801892)

[Tabela 4. Parametry klasy systemów. 10](#_Toc465801893)

[Tabela 5. Mechanizmy i rozwiązania z zakresu bezpieczeństwa. 11](#_Toc465801894)

[Tabela 6. Mechanizmy uwierzytelniania i autoryzacji 12](#_Toc465801895)

[Tabela 7. Przewidywane obciążenia z podziałem na źródło ruchu 12](#_Toc465801896)

[Tabela 8. Przewidywane obciążenia połączeń sieciowych pomiędzy warstwami środowiska 12](#_Toc465801897)

[Tabela 9. Zestawienie usług dostępowych SMTP 14](#_Toc465801898)

[Tabela 10. Zestawienie usług dostępowych HTTP 14](#_Toc465801899)

[Tabela 11. Zestawienie aplikacyjnych bloków architektonicznych 15](#_Toc465801900)

[Tabela 12. Zestawienie bazodanowych bloków architektonicznych 15](#_Toc465801901)

[Tabela 13. Zestawienie bloków architektonicznych OS 15](#_Toc465801902)

[Tabela 14. Wykaz oprogramowania dodatkowego instalowanego na blokach OS 15](#_Toc465801903)

[Tabela 15. Reprezentacja logiczna adresacji IP środowiska Systemu 16](#_Toc465801904)

[**Tabela 16. Lista przekierowań dla konfiguracji PROXY.** 17](#_Toc465801905)

[Tabela 17. Dane dla komunikacji między systemami oraz wewnątrz Systemu 19](#_Toc465801906)

[Tabela18**.** Dane do przepuszczenia ruchu dla użytkowników i administratorów 19](#_Toc465801907)

[Tabela 19 Dane do utworzenia wpisu w DNS dla usługi – typ 1 20](#_Toc465801908)

[Tabela 20 Dane do utworzenia wpisu w DNS dla usługi - typ 2 20](#_Toc465801909)

[Tabela 21 Dane do utworzenia wpisu w DNS dla usługi - typ 3 20](#_Toc465801910)

[Tabela 22 Wykaz polityk backup’u 22](#_Toc465801911)

[Tabela 23 Wykaz backup’owanych elementów 22](#_Toc465801912)

[Tabela 24. Zbiorcze zestawienie usług dostępowych i usług - bloków architektonicznych dla wszystkich środowisk funkcjonujących w ramach Systemu. 23](#_Toc465801913)

[Tabela 25– Grupy zabezpieczeń 25](#_Toc465801914)

[Tabela 26– Konta Serwisowe 25](#_Toc465801915)

[Tabela 27– Wykaz bloków wymagających czynności z wyższymi uprawnieniami 25](#_Toc465801916)

**Zastrzeżenie poufności**

Niniejszy dokument stanowi własność Ministerstwa Finansów w tym Centrum Przetwarzania Danych Ministerstwa Finansów. Ministerstwo Finansów może udostępnić niniejszy dokument innym podmiotom prawnym i osobom fizycznym w związku z realizacją prac na rzecz resortu finansów. W takim przypadku podmiot prawny lub osoba fizyczna, która otrzymała niniejszy dokument jest zobowiązana do zachowania poufności w stosunku do wszelkich informacji technicznych, technologicznych, organizacyjnych i innych.

# Wstęp

Niniejszy dokument należy wypełnić zgodnie z wytycznymi i przykładami zawartymi w tekście ukrytym.

Platforma sprzętowo-programowa jest udostępniania i konfigurowana etapowo na podstawie zaakceptowanego Projektu ITS.

**Etap 1 – udostępnienie wymaganych w Projekcie ITS bloków architektonicznych**

W celu uruchomienia procesu udostępnienia infrastruktury technicznej w CPD MF wymagane jest opracowanie i zaakceptowanie przez CPD MF Projektu ITS przynajmniej w zakresie poniższych rozdziałów (dla wszystkich środowisk systemu):

(2) Wstęp

(3) Słowniki

(4) Wymagania formalne

(5) Rodzaje środowisk systemu

(6) Projekty poszczególnych środowisk

(6.1.) Projekt środowiska (…) Systemu ***(rozdział powielony dla wszystkich środowisk systemu)***

(6.1.1.) Klasa systemu

(6.1.2.) Klasa bezpieczeństwa systemu

(6.1.3.) Uwierzytelnianie użytkowników i administratorów w środowisku

(6.1.4.) Obciążenia połączeń sieciowych

(6.1.5.) Architektura Środowiska Systemu

(6.1.6.) Platforma Środowiska Systemu

(6.1.6.1.) Usługi dostępowe

(6.1.6.2.) Usługi dostarczające bloki architektoniczne aplikacyjne

(6.1.6.3.) Usługi dostarczające bloki architektoniczne bazodanowe

(6.1.6.4.) Usługi dostarczające bloki architektoniczne OS

(6.1.6.5.) Dodatkowe oprogramowanie wymagane w Środowisku Systemu

(6.1.8.) Wymagania środowiska dla systemu backupowego

(6.1.8.1.) Wymagania na polityki tworzenia kopii bezpieczeństwa

(6.1.8.2.) Zabezpieczane elementy środowiska

(7.) Zestawienie bloków architektonicznych

(10.) Zakres zmian w stosunku do poprzedniej wersji dokumentu

**Etap 2 – konfiguracja udostępnionych bloków architektonicznych w tym usług dostępowych oraz katalogowych.**

W kolejnych krokach Projekt ITS powinien być sukcesywnie uzupełniany w poniższym zakresie (dla wszystkich środowisk systemu):

(6.1.7.) Podstawowe informacje niezbędne do skonfigurowania infrastruktury komunikacyjnej warstwy dostępowej

(6.1.7.1.) Adresacja IP środowiska Systemu ***(rozdział zostanie uzupełniony przez CPD MF)***

(6.1.7.2.) Wymagania niezbędne do konfiguracji środowiska proxy i zewnętrznego Load Balancera

(6.1.7.2.1.) Opis usług aplikacyjnych

(6.1.7.2.2.) Lista przekierowań (redirect, rewrite)

(6.1.7.2.3.) Określenie algorytmu balansowania ruchu na zewnętrznych Load Balancer’ach Cisco ACE30

(6.1.7.2.4.) Definicja próbkowania dla każdej z usług aplikacyjnych

(6.1.7.2.5.) Certyfikaty na potrzeby komunikacji HTTPS

(6.1.7.2.6.) Inne wymagania

(6.1.7.3.) Wymagania dla warstwy aplikacyjnej (niezbędne do konfiguracji wewnętrznego Load Balancer’a)

(6.1.7.3.1.) Opis usług aplikacyjnych

(6.1.7.3.2.) Opis farm/klastrów serwerów

(6.1.7.3.3.) Określenie algorytmu balansowania ruchu na wewnętrznych Load Balancer’ach Cisco ACE30

(6.1.7.3.4.) Dla których usług aplikacyjnych/farm serwerów wymagane jest włączenie funkcjonalności session-persistance i jakie parametry muszą zostać użyte dla sesji sticky

(6.1.7.3.5.) Inne wymagania

(6.1.7.3.6.) Dane konieczne do przepuszczenia ruchu dla komunikacji między systemami oraz wewnątrz Systemu

(6.1.7.3.7.) Dane konieczne do przepuszczenia ruchu dla użytkowników i administratorów

(6.1.7.3.8.) Dane konieczne do utworzenia wpisów w DNS dla usług udostępnianych przez środowisko systemu biznesowego

(6.1.7.4.) Filtracja IPS w infrastrukturze CPD MF

(9.) Grupy Zabezpieczeń

(9.1) Konta serwisowe

(9.2) Czynności serwisowe wymagające wyższych uprawnień

(10.) Zakres zmian w stosunku do poprzedniej wersji dokumentu

1. **Cel dokumentu**

Dokument opisuje wszystkie elementy infrastruktury teleinformatycznej Systemu (…) (dalej w tekście – Systemu) i ich parametry, niezbędne do umieszczenia go w Środowisku IT CPD MF.

1. **Odbiorcy dokumentu**

Dokument jest przeznaczony dla Klienta Usługi oraz CPD MF.

1. **Dokumenty powiązane/referencyjne**

| Lp. | Dokument (Tytuł) | Lokalizacja |
| --- | --- | --- |
| 1 | Katalog usług CPD MF | http://uslugi-it.cpd.mf.gov.pl |
| 2 | Bloki architektoniczne wspierające budowę systemów biznesowych |
| 3 | Standard określania klasy systemu informatycznego resortu finansów |
| 4 | Standard określania klasy bezpieczeństwa systemu informatycznego resortu finansów |
| 5 | Architektura referencyjna środowiska IT CPD |
| 6 | Procedura realizacji Wniosków o Usługę CPD MF |
| 7 | Słownik pojęć informatycznych |

Tabela 1. Lista dokumentów powiązanych i/lub referencyjnych

# Słowniki

## Używane terminy i skróty technologiczne

Patrz pkt 2.3 poz. 7.

## Terminy i skróty specyficzne dla Systemu

|  |  |
| --- | --- |
| Termin/skrót | Definicja |
|  |  |

Tabela 2. Terminy i skróty specyficzne dla Systemu

## Symbole graficzne

Elementy notacji UML Powiązania



Rysunek 1. Elementy notacji UML i powiązania wykorzystywane na diagramach



Rysunek 2. Symbole graficzne usług i bloków architektonicznych wykorzystywanych na diagramach

## Dane kontaktowe

W kontaktach miedzy CPD MF a Wykonawcą zawsze uwzględniany jest Kierownik Projektu lub wyznaczony przez niego przedstawiciel.

Kontakt roboczy do wyznaczonego ze strony Projektu przedstawiciela i jego zastępcy w celu uszczegóławiania i wyjaśniania wymagań dotyczących niniejszego dokumentu.

|  |  |
| --- | --- |
| **Imię Nazwisko** |  |
| **Firma** |  |
| **e-mail** |  |
| **nr telefonu** |  |

Osoba zastępująca

|  |  |
| --- | --- |
| **Imię Nazwisko** |  |
| **Firma** |  |
| **e-mail** |  |
| **nr telefonu** |  |

Kontakt roboczy do wyznaczonego ze strony Wykonawcy przedstawiciela i jego zastępcy w celu uszczegóławiania i wyjaśniania wymagań dotyczących niniejszego dokumentu.

|  |  |
| --- | --- |
| **Imię Nazwisko** |  |
| **Firma** |  |
| **e-mail** |  |
| **nr telefonu** |  |

Osoba zastępująca

|  |  |
| --- | --- |
| **Imię Nazwisko** |  |
| **Firma** |  |
| **e-mail** |  |
| **nr telefonu** |  |

Kontakt roboczy do osób wyznaczonych ze strony CPD MF w celu uszczegóławiania i wyjaśniania wymagań dotyczących niniejszego dokumentu.

|  |  |
| --- | --- |
| **Imię Nazwisko** |  |
| **Firma** |  |
| **e-mail** |  |
| **nr telefonu** |  |

Osoba zastępująca

|  |  |
| --- | --- |
| **Imię Nazwisko** |  |
| **Firma** |  |
| **e-mail** |  |
| **nr telefonu** |  |

# Wymagania formalne

|  |  |
| --- | --- |
| Zagadnienie | Odpowiedź |
| Czy system przetwarza dane osobowe? |  |
| Czy wyznaczono ASI? |  |

# Rodzaje środowisk systemu

System funkcjonuje/będzie funkcjonować w oparciu o środowiska wymienione w poniższej tabeli.

* *Definicje poszczególnych środowisk oraz ich dopuszczalne nazwy znajdują się w dokumencie wymienionym pkt 2.3 poz. 7.*
* *Przykład wypełnienia tabeli:*

|  |  |  |
| --- | --- | --- |
| *Lp.* | *Rodzaj środowiska* | *Identyfikator* |
|  | *produkcyjne* | *pr* |

*Tabela 3 Rodzaje środowisk systemu*

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Rodzaj środowiska** | **Identyfikator** | **Lokalizacja** |
|  |  |  |  |

Tabela 3. Rodzaje środowisk Systemu

# Projekty poszczególnych środowisk

* *Należy wykonać projekty wszystkich środowisk systemu, zgodnie z zakresem przedstawionym poniżej w punkcie 5.1*

## Projekt środowiska (…) Systemu

* *Punkt 6.1 należy powielić dla wszystkich środowisk systemu wymienionych w punkcie 5 „Rodzaje środowisk Systemu” (specyfikację kolejnych środowisk umieścić w punktach 5.2. ... 5.x)*
* *W miejsce (…) należy wpisać odpowiedni rodzaj środowiska np. produkcyjne*

### Klasa systemu

Środowisko Systemu zostało zaklasyfikowane do Klasy (…)

|  |  |
| --- | --- |
| Wymagany Docelowy Czas Odtworzenia (RTO) [w godzinach] | … |
| Wymagany Docelowy Punkt Odtworzenia (RPO)[w godzinach] | … |
| Wymagana Dostępność środowiska [%] | … |

Tabela 4. Parametry klasy systemów.

Klasyfikacja została przeprowadzona zgodnie ze standardem wymienionym w pkt 2.3 poz. 3.

### Klasa bezpieczeństwa systemu

Środowisko Systemu zostało zaklasyfikowane do Klasy bezpieczeństwa (…)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **B3** | **B2** | **B1** | **BX** |  | **Klasa** |
| Ochrona kryptograficzna |  |  |  |  |  | **bezpieczeństwa** |
| Uwierzytelnianie i autoryzacja |  |  |  |  |  | **Środowiska** |
| Separacja zasobów |  |  |  |  |  | **Systemu** |
| Rejestrowanie, monitorowanie i audyt zdarzeń |  |  |  |  |  |  |
| Ochrona przed oprogramowaniem złośliwym |  |  |  |  |  |
| Zdalny dostęp |  |  |  |  |  |  |
| Bezpieczeństwo styku |  |  |  |  |  |  |

Tabela 5. Mechanizmy i rozwiązania z zakresu bezpieczeństwa.

Klasyfikacja została przeprowadzona zgodnie ze standardem wymienionym w pkt 2.3 poz. 4.

### Bezpieczeństwo w środowisku

* *Opis sposobu zapewnienia bezpieczeństwa w każdym z obszarów wymienionych w Tabeli 5.*

### Uwierzytelnianie użytkowników i administratorów w środowisku

* *Definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w pkt 2.3 poz. 7*
* *Przykład wypełnienia tabeli:*

|  |  |  |
| --- | --- | --- |
| *Lp.* | *Sposób uwierzytelniania i autoryzacji* | *Rodzaj mechanizmu* |
| *1* | *Użytkownik / hasło* | *Active Directory* |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Typ konta** | **Sposób uwierzytelniania i autoryzacji** | **Rodzaj mechanizmu** | **Protokół** | **Port** | **Szyfrowanie transmisji** | **Dostęp[ z innej podsieci/internetu]** | **Certyfikat [Serwera/Klienta]** | **Typ Certyfikatu** |
| 1 | Administrator |  |  |  |  |  |  |  | Samopodpisany |
| 2 | Użytkownik |  |  |  |  |  |  |  |  |
| 3 | Wykonawca |  |  |  |  |  |  |  |  |

*Tabela 6 Mechanizmy uwierzytelniania i autoryzacji*

Tabela . Mechanizmy uwierzytelniania i autoryzacji

### Obciążenia połączeń sieciowych.

* *Szacunkowy ruch sieciowy występujący pomiędzy poszczególnymi warstwami systemu, a także pomiędzy systemem a użytkownikami i innymi powiązanymi systemami.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Źródło** | **Obciążenia jednej sesji [Kb/s]** | **Liczba użytkowników** | **Liczba jednoczesnych sesji/sekundę** |
| 1. | Internet |  |  |  |
| 2. | WAN |  |  |  |
| 3. | LAN |  |  |  |

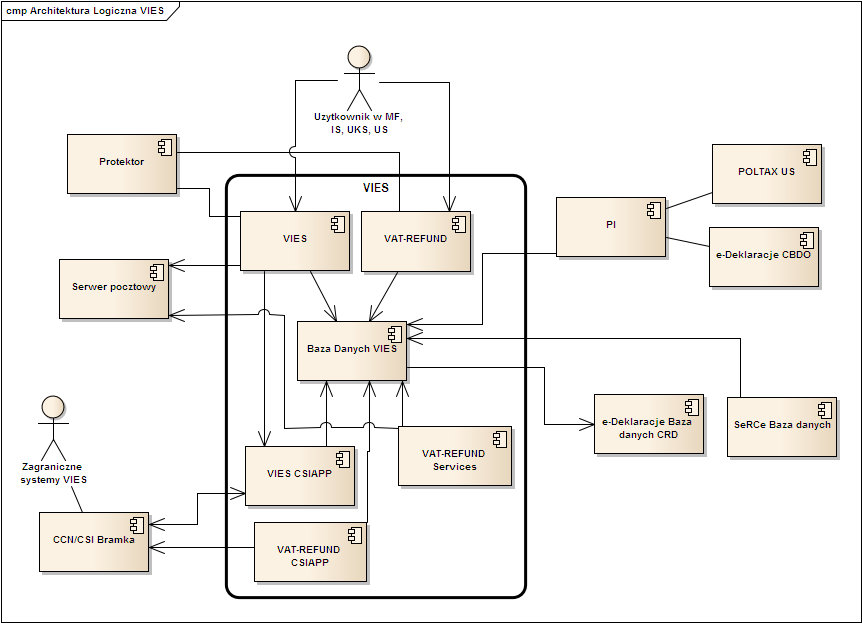
Tabela 7. Przewidywane obciążenia z podziałem na źródło ruchu

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Liczba sesji / całkowite obciążenie [szt./Mb/s]** | | |
| **Warstwa:** | **Proxy** | **Aplikacji** | **Bazy danych** |
| **Proxy** | **X** |  |  |
| **Aplikacji** |  |  |  |
| **Bazy danych** |  |  |  |

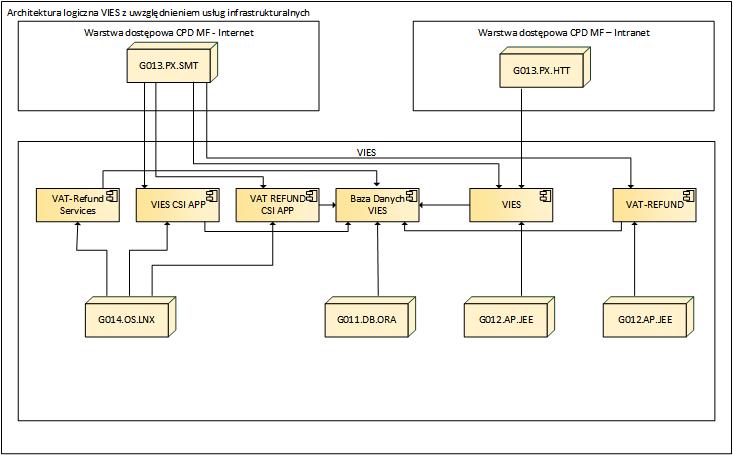
Tabela 8. Przewidywane obciążenia połączeń sieciowych pomiędzy warstwami środowiska

### Architektura Środowiska Systemu

* *Na rysunku należy przedstawić model logiczny środowiska w rozbiciu na komponenty Systemu, wykonany w narzędziu MS VISIO lub Enterprise Architect zgodnie z poniższym przykładem.*
* *Przykładowy model logiczny (komponentowy) przedstawiony na diagramach poniżej obrazuje relacje pomiędzy komponentami systemu oraz systemami i użytkownikami wewnętrznymi i zewnętrznymi.*

****

*Rysunek 3. Model logiczny środowiska Systemu*

**

*Rysunek 4. Model logiczny Systemu z* *uwzględnieniem usług infrastrukturalnych*

### Platforma Środowiska Systemu

#### Usługi dostępowe

Obciążenia związane z usługami dostępowymi (SMTP)

|  |  |  |
| --- | --- | --- |
| *Identyfikator obiektu* | *<system>.<środowisko>.<grupa>.<ID>* | *Unikalny identyfikator obiektu nadawany przez Wykonawcę. Sposób oznaczania identyfikatorów obiektów został opisany w dokumencie „Architektura referencyjna IT CPD MF”* |
| *Lista przekierowań* | *Lista postaci „Adres w warstwie dostępowej -> adres w warstwie aplikacyjnej”* | *Określa, jakie adresy w warstwie dostępowej SMTP są przekierowywane na jakie adresy w warstwie aplikacyjnej.* |
| *Liczba połączeń równoległych* | *n* | *Określa maksymalną liczbę równoległych połączeń SMTP do warstwy dostępowej.* |
| *Liczba wiadomości na godzinę/sekundę* | *n/h, m/s* | *Określa maksymalną liczbę wiadomości email przesyłanych w ciągu godziny/sekundy do systemu biznesowego.* |
| *Numer instancji Usługi* | *Numer instancji usługi dostępowej SMTP* | |

| **Lp.** | **Numer instancji Usługi** | **ID bloku korzystającego z Usługi** | **Lista przekierowań** | **Ilość połączeń równoległych** | **Liczba wiadomości na godzinę/sekundę** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

Tabela 9. Zestawienie usług dostępowych SMTP

Obciążenia związane z usługami dostępowymi (HTTP)

|  |  |  |
| --- | --- | --- |
| *Identyfikator obiektu* | *<system>.<środowisko>.<grupa>.<ID>* | *Unikalny identyfikator obiektu nadawany przez Wykonawcę. Sposób oznaczania identyfikatorów obiektów został opisany w dokumencie „Architektura referencyjna IT CPD MF”* |
| *Wejście bloku* | *Internet/Intranet MF* | *Określa sieć, z której ma być dostępna funkcjonalność systemu biznesowego.* |
| *Lista przekierowań* | *Lista postaci „Adres w warstwie dostępowej -> adres w warstwie aplikacyjnej”* | *Określa, jakie adresy w warstwie dostępowej HTTP są przekierowywane na jakie adresy w warstwie aplikacyjnej.* |
| *Liczba połączeń równoległych* | *n* | *Określa maksymalną liczbę równoległych połączeń HTTP do warstwy dostępowej.* |
| *Https* | *Tak/Nie* | *Określa czy dostęp ma być szyfrowany* |
| *Numer instancji Usługi* | *Numer instancji Usługi dostępowej HTTP* | |

| **Lp.** | **Numer instancji Usługi** | **ID**  **bloku korzystającego z Usługi** | **Wejście bloku** | **Lista przekierowań** | **Ilość połączeń równoległych** | **https**  **TAK/NIE** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |

Tabela 10. Zestawienie usług dostępowych HTTP

#### Usługi dostarczające bloki architektoniczne aplikacyjne

* *Definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w Katalogu Usług*

| **Lp.** | **Numer instancji Usługi** | **ID**  **bloku** | **CPU**  **[cCPU/**  **vCPU]** | **RAM [GB]** | **Przestrzeń dyskowa**  **[GB]** | **HA** | **Grupowanie** | **Krotność** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |

Tabela 11. Zestawienie aplikacyjnych bloków architektonicznych

#### Usługi dostarczające bloki architektoniczne bazodanowe

* *Definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w Katalogu Usług*

| **Lp.** | **Numer instancji Usługi** | **ID**  **bloku** | **CPU**  **[cCPU/**  **vCPU]** | **RAM [GB]** | **Przestrzeń**  **dyskowa**  **[GB]** | **HA** | **Grupowanie** | **Krotność** | **Backup** | **Opcje** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |

Tabela 12. Zestawienie bazodanowych bloków architektonicznych

#### Usługi dostarczające bloki architektoniczne OS

* *Definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w Katalogu Usług*

| **Lp.** | **Numer instancji Usługi** | **ID**  **bloku** | **CPU**  **[cCPU/**  **vCPU]** | **RAM [GB]** | **Przestrzeń dyskowa**  **[GB]** | **HA** | **Grupowanie** | **Krotność** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |

Tabela 13. Zestawienie bloków architektonicznych OS

#### Dodatkowe oprogramowanie wymagane w Środowisku Systemu

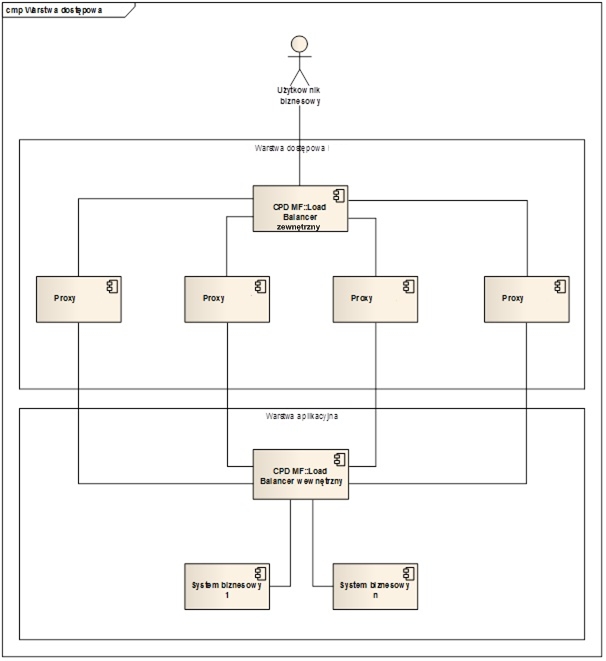
Tabela poniżej opisuje dodatkowe, tzn. niezapewniane przez bloki architektoniczne lub usługi, oprogramowanie wymagane do działania Środowiska Systemu.

*Definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w Katalogu Usług*

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Numer instancji Usługi** | **ID**  **bloku** | **Nazwa oprogramowania dodatkowego** |
|  |  |  |  |

Tabela 14. Wykaz oprogramowania dodatkowego instalowanego na blokach OS

### Podstawowe informacje niezbędne do skonfigurowania infrastruktury komunikacyjnej warstwy dostępowej

**

*Rysunek 5. Schemat warstwy dostępowej CPD MF*

#### Adresacja IP środowiska Systemu

*Należy wymienić wszystkie identyfikatory adresów IP używanych w środowisku Systemu. Adresację przydziela CPD MF.*

*Pozostałe pola w tabeli uzupełnia CPD MF na podstawie informacji zawartych w kolekcji Wniosków Złożonych o Usługi CPD MF.*

*Pola „Nazwa klastra” oraz „Identyfikator adresu IP klastra” wypełnić w przypadku, gdy blok jest częścią klastra*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Lp.* | *Hostname* | *Nazwa klastra* | *ID IP klastra* | *ID IP [ID obiektu].[Identyfikator IP]* | *Nazwa VLANu* | *VLNA ID* | *Adres IP* | *Maska* | *Brama domyślna* |
| *1* | *dbs-sql-059* | *brak* | *brak* | *zefir2.pr.db.01.ip1* | *R-Zefir2DB-pr* | *2430* | *1.1.1.144* | *255.255.255.0* | *1.1.1.1* |
| *2* | *dbs-sql-060* | *brak* | *brak* | *zefir2.pr.db.01.ip2* | *R-Zefir2DB-pr* | *2430* | *1.1.1.145* | *255.255.255.0* | *1.1.1.1* |
| *3* | *dbs-sql-061* | *vip.pr.db.01* | *zefir2.pr.db.01.vip1* | *zefir2.pr.db.01.vip1* | *R-Zefir2DB-pr* | *2430* | *1.1.1.146* | *255.255.255.0* | *1.1.1.1* |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Hostname** | **Nazwa klastra** | **ID IP klastra** | **ID IP** | **Nazwa VLANu** | **VLAN ID** | **Adres IP** | **Maska** | **Brama domyślna** |
|  |  |  |  |  |  |  |  |  |  |

Tabela 15. Reprezentacja logiczna adresacji IP środowiska Systemu

#### Wymagania niezbędne do konfiguracji środowiska proxy i zewnętrznego Load Balancera

##### Opis usług aplikacyjnych

*Nazwa usługi: Usługa dostępowa do aplikacji X*

*Protokół: HTTPS (między przeglądarką a zewnętrznym load balancerem)*

*Zasady komunikacji: IP vip.pr.lbzew.01 (10.121.8.175)*

*Port: tcp/443*

##### Lista przekierowań (redirect, rewrite)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***LP*** | ***HTTPS*** | ***HTTP*** | ***Port VIP  FrontEnd*** | ***Load Balancer FrontEnd*** | ***Port  PROXY*** | ***Serwery PROXY*** | ***Port VIP BackEnd*** | ***Load Balancer BackEnd*** | ***Port działania usługi na serwerach aplikacyjnych*** | ***Adresy Serwerów aplikacyjnych*** | *http przekierowania proxy* |
|  | *"Przyjazny" adres usługi* | ***(ruch wewnątrz po przejściu LB)***  *adres klastrowy aplikacji/ adres farmy aplikacyjnej* | *Port na którym wystawiona jest usługa dla użytkownika końcowego* | *Adres IP Load Balancer'a FrontEnd* | *Port  PROXY* | *Adresy IP Serwerów PROXY* | *Port na którym "nasłuchują" serwery PROXY w strefie BackEnd* | *Adres IP Load Balancer'a BackEnd* | *Port na którym wystawiona jest aplikacja na serwerach aplikacyjnych* | *Adresy Serwerów aplikacyjnych* |  |
|  | *https://e-deklaracje-pilot.mf.gov.pl/APP\_PU/* | *http://sap-jbo-064:8080/APP\_PU/* | *443* | *10.121.8.193* | *80* | *10.121.12.4-10.121.12.16* | *8080* | *10.121.19.222* | *8080* | *10.121.116.231* |  |

*Przykład wypełnienia tabeli*

*a) użycie instrukcji ProxyPass (pominięcie modułu mod\_rewrite) – mniejsze obciążenie serwerów proxy*

*b) użycie modułu mod\_rewrite – zaawansowane konfiguracje (przykładowo: wykorzystanie przekierowania – po wpisaniu w przeglądarce adresu przykładowadomena.mf.gov.pl zostaniemy przeniesieni do strony z logowaniem, która jest pod adresem: przykladowadomena.mf.gov.pl/secure/login.jsp, lub inny dowolny adres URL itp. Więcej informacji na stronie* [*http://httpd.apache.org/docs/2.2/rewrite/*](http://httpd.apache.org/docs/2.2/rewrite/)*)*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **LP** | **HTTPS** | **HTTP** | **Port VIP  FrontEnd** | **Load Balancer FrontEnd** | **Port**  **PROXY** | **Serwery PROXY** | **Port VIP BackEnd** | **Load Balancer BackEnd** | **Port działania usługi na serwerach aplikacyjnych** | **Adresy Serwerów aplikacyjnych** | **http przekierowania proxy** |
|  |  |  |  |  |  |  |  |  |  |  |  |

**Tabela 16. Lista przekierowań dla konfiguracji PROXY.**

##### Określenie algorytmu balansowania ruchu na zewnętrznych Load Balancer’ach Cisco ACE30

*Domyślnym ustawieniem jest algorytm Round Robin.*

##### Definicja próbkowania dla każdej z usług aplikacyjnych

*Domyślnym ustawieniem jest sprawdzanie dostępności hosta i portu pod którym usługa jest dostępna*

##### Certyfikaty na potrzeby komunikacji HTTPS.

*W przypadku potrzeby zapewnienia komunikacji HTTPS należy cyklicznie dostarczać wymagane certyfikaty dla systemów.*

*Obsługiwanymi formatami są pkcs12 oraz pem.*

*Należy wymienić nazwy dostarczanych certyfikatów.*

##### Inne wymagania

#### Wymagania dla warstwy aplikacyjnej (niezbędne do konfiguracji wewnętrznego Load Balancer’a)

##### Opis usług aplikacyjnych

*Nazwa usługi: Aplikacja X*

*Protokół: HTTP*

*zasady komunikacji IP vip.pr.lbwew.01 (10.121.19.171)*

*Port: tcp/80*

##### Opis farm/klastrów serwerów

*adresy IP, usługi – porty, identyfikatory bloków architektonicznych*

*lista wymaganych adresów VIP wraz z opisem celu ich przydzielenia oraz roli, jaką będą odgrywały w przepływach komunikacyjnych Systemu*

*Blok: vies.pr.ap.01*

*IP: 10.121.88.250-253*

##### Określenie algorytmu balansowania ruchu na wewnętrznych Load Balancer’ach Cisco ACE30

*Domyślnym ustawieniem jest algorytm Round Robin.*

##### Dla których usług aplikacyjnych/farm serwerów wymagane jest włączenie funkcjonalności session-persistance i jakie parametry muszą zostać użyte dla sesji sticky

##### Inne wymagania

##### Dane konieczne do przepuszczenia ruchu dla komunikacji między systemami oraz wewnątrz Systemu

*W poniższej tabeli należy określić ruch:*

* *Komponent aplikacyjny środowiska* ***(A)******Systemu (X)****🡪 Komponent aplikacyjny* ***Systemu (Y)*** *-*
* *Komponent aplikacyjny środowiska* ***(A)******Systemu (X)*** *🡪 Komponent aplikacyjny środowiska* ***(A) Systemu (X)***

*– np. przepływy między warstwą aplikacyjną a bazodanową*

* *Komponent aplikacyjny środowiska* ***(A) Systemu (X)*** *🡪 Komponent aplikacyjny środowiska* ***(B) Systemu (X)***

***Uwaga: Należy uwzględnić również ruch zwrotny.***

*W przypadku połączenia tymczasowego należy podać datę wygaśnięcia reguły, tzn. do kiedy reguła ma funkcjonować. Na przykład „tymczasowe - na czas migracji do 30.09.2015”.*

*Instrukcja dotycząca wypełniania:*

1. *Dla pola „System źródłowy” oraz „System docelowy” należy podać obowiązującą nazwę systemu.*
2. *Dla każdego wiersza wypełnione muszą być wszystkie pola*
3. *VLAN ma być wpisany jako numer (VLAN ID), w przypadku adresu, który nie znajduje się w CPD MF w polu VLAN należy wpisać fizyczną lokalizację hosta.*
4. *Adres IP dla połączeń z/do "całego" Internetu należy wpisać 0.0.0.0/0.0.0.0. W przypadku serwerów dostępnych w Internecie zaleca się podanie "na sztywno" adresu IP (lub wszystkich adresów pod jakimi może występować), jednakże ("w drodze wyjątku") można także podać nazwę FQDN (która będzie rozwiązana przez DNS) można podać kilka adresów IP (źródłowych/docelowych) w ramach jednej reguły*
5. *Maska w formacie długim (np. 255.255.255.0), maska w przypadku pojedynczych hostów to 255.255.255.255*
6. *Porty zapis w formacie "nazwa protokół/port" - np. HTTP tcp/80, HTTPS tcp/443, DNS udp/53, SSH tcp/22, RDP tcp/3389, etc. można podać zakres portów - np. tcp/1234-1240, można podać kilka (zakresów) portów w ramach jednej reguły - każdy w nowej linii*
7. *Osoba odpowiedzialna/zgłaszająca i numer telefonu*
8. *W przypadku braku przynajmniej jednej z informacji (VLAN, adres i maska źródłowa oraz VLAN, adres, maska i porty docelowe, itd.) - reguła nie zostanie utworzona.*
9. *Jeżeli ruch nie zostanie zakwalifikowany do żadnej z reguł firewalla - będzie odrzucony i komunikacja nie będzie możliwa*
10. *Kolumny „VLAN”, „IP”, „maska” w przypadku systemów posadowionych w Ośrodkach Przetwarzania Danych Ministerstwa Finansów, wypełnia CPD MF.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *L.p.* |  | *Źródło* | | | | | | *Cel* | | | | | | *połączenie  (tymczasowe\*/ docelowe)* | *Komentarz – opis przepływu* | *Osoba odpowiedzialna lub zgłaszająca* |
| *VLAN* | *ID IP [ID obiektu].[Identyfikator IP]* | *IP* | *maska* | *porty* | *System źródłowy* | | *VLAN* | *ID IP wewnątrz systemu* | *IP systemu zewnętrznego* | *Maska systemu zewnętrznego* | *porty* | *System docelowy* |
| *1* | *R-Zefir2DB-te* | *zefir2.pr.db.01.ip1* | *10.10.123.100 10.10.123.101* | *255.255.255.0* | *tcp/443* | | *ZEFIR 2* | *R-Zefir2APP-te* | *pdr.pr.db.02.ip1* | *10.10.222.24 10.10.222.25 10.10.222.26 10.10.222.27* | *255.255.255.* | *tcp/135 tcp/5000-5500* | *ZEFIR 2* | *docelowe* |  |  |

*Tabela. 17 Dane dla komunikacji między systemami oraz wewnątrz Systemu*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L.p. | Źródło | | | | | | Cel | | | | | | połączenie  (tymczasowe\*/ docelowe) | Komentarz – opis przepływu | Osoba odpowiedzialna lub zgłaszająca |
| VLAN | ID IP | IP | maska | porty | System źródłowy | VLAN | ID IP | IP | maska | porty | System źródłowy |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Tabela 17. Dane dla komunikacji między systemami oraz wewnątrz Systemu

##### Dane konieczne do przepuszczenia ruchu dla użytkowników i administratorów:

*W celu umożliwienia dostępu do bloków architektonicznych należy wypełnić poniższą tabelę zgodnie z nagłówkami i opisem.*

*W przypadku połączenia tymczasowego należy podać datę wygaśnięcia reguły, tzn. do kiedy reguła ma funkcjonować. Na przykład „tymczasowe - na czas testów do 30.09.2013”.*

*Instrukcja dotycząca wypełniania:*

* + - 1. *Dla każdego wiersza powinny być wypełnione wszystkie pola*
      2. *Maska w formacie długim (np. 255.255.255.0), maska w przypadku pojedynczych hostów to 255.255.255.255*
      3. *Porty: zapis w formacie "nazwa protokół/port" - np. HTTP tcp/80, HTTPS tcp/443, DNS udp/53, SSH tcp/22, RDP tcp/3389, etc. można podać zakres portów - np. tcp/1234-1240, można podać kilka (zakresów) portów w ramach jednej reguły - każdy w nowej linii*
      4. *Osoba odpowiedzialna/zgłaszająca i numer telefonu*
      5. *Kolumny „VLAN”, „IP”, „maska” wypełnia CPD MF*

*W przypadku połączeń na potrzeby administracji systemami równolegle należy złożyć odpowiednie wnioski o zdalny dostęp do systemu z sieci WAN.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***L.p.*** | ***Źródło*** | | | ***Cel*** | | | | | | | ***połączenie  (tymczasowe\*/***  ***docelowe)*** | ***Cel połączenia*** | ***Osoba odpowiedzialna lub zgłaszająca*** |
| ***Lokalizacja*** | ***IP*** | ***maska*** | ***VLAN*** | *ID IP [ID obiektu].[Identyfikator IP]* | | ***IP*** | ***maska*** | ***porty*** | ***Nazwa systemu*** |
| *1* | *IC X* | *11.11.11.0* | *255.255.255.0* | *2080* | | *zefir2.pr.db.01.ip1* | *10.121.197.6* | *255.255.255.0* | *HTTP tcp/80,* | *SYSTEM\_X* | *docelowe* | *Administracja systemu dla sieci adminstratorów IC X* | *Jan Kowalski*  *(+48123456789)* |

*Tabela 18 Dane do przepuszczenia ruchu dla użytkowników i administratorów*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Źródło** | | | **Cel** | | | | | | **połączenie  (tymczasowe\*/**  **docelowe)** | **Cel połączenia** | **Osoba odpowiedzialna lub zgłaszająca** |
| **Lokalizacja** | **IP** | **maska** | **VLAN** | **ID IP** | **IP** | **maska** | **porty** | **Nazwa systemu** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

Tabela18**.** Dane do przepuszczenia ruchu dla użytkowników i administratorów

##### Dane konieczne do utworzenia wpisów w DNS dla usług udostępnianych przez środowisko systemu biznesowego

*W zależności od wymagań i sposobu publikacji systemu biznesowego przewiduje się trzy typy rejestracji w systemie DNS.*

*- A i PTR – rejestracja pojedynczego rekordu w strukturze DNS pozwalającego na powiązanie nazwy FQDN z adresem IP bloku, lub z adresem VIP Load Balancera; przy opcji PTR następuje zapisanie powiązania nazwy FQDN z adresem IP również w bazie danych adresów IP;*

*- CNAME – rejestracja pojedynczego rekordu w strukturze DNS pozwalającego na powiązanie nowej nazwy FQDN z istniejącą nazwą FQDN bloku architektonicznego.*

*- SUBDOMENA – pozwala na zgrupowanie jednego/wielu rekordów typu A/PTR i CNAME w postaci strefy np. trezor.mf.gov.pl, gdzie mf.gov.pl to podstawowa nazwa domeny MF.*

*Nazwa SUBDOMENY w zapisie FQDN musi być poprzedzona znakiem „-”: host-[subdomena].mf.gov.pl ze względu na stosowanie certyfikatów wildcard dla domeny MF.GOV.PL.*

*Rejestracja rekordów typu A i PTR odbywa się przy instalacji bloku architektonicznego*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Lp.* | *Nazwa domenowa (FQDN)* | *ID IP* | *PTR*  *[Tak/Nie]* | *ID bloku* |
| *1.* | *sms-win-015.mf.gov.pl* | *sms.os.pr.02.ip1* | *TAK* | *sms.os.pr.02* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa domenowa (FQDN)** | **ID IP** | **PTR**  **[Tak/Nie]** | **ID bloku** |
| 1. |  |  |  |  |

Tabela 19 Dane do utworzenia wpisu w DNS dla usługi – typ 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Lp.* | *Nazwa systemu* | *Alias name (CNAME)* | *Nazwa domenowa (FQDN)* | *ID IP* |
| *1* | *TREZOR* | *test-hyperion.mf.gov.pl* | *sap-lnx-145.mf.gov.pl* | *trezor.os.pr.01.ip1* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa systemu** | **Alias name (CNAME)** | **Nazwa domenowa (FQDN)** | **ID IP** |
|  |  |  |  |  |

Tabela 20 Dane do utworzenia wpisu w DNS dla usługi - typ 2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *Lp.* | *Nazwa systemu* | *Nazwa SUBDOMENY w MF.GOV.PL* | *Nazwa domenowa (FQDN)\** | *ID IP dla rekordu A/PTR lub FQDN dla rekordu CNAME* | *Typ rekordu DNS*  *[A, CNAME]* | *PTR*  *[Tak/Nie]* |
| *1.* | *TREZOR* | *trezor* | *hyperion-trezor.mf.gov.pl* | *trezor.os.pr.01.ip1* | *A* | *TAK* |
| *2.* | *TREZOR-TE* | *trezor* | *test-hyperion-trezor.mf.gov.pl* | *sap-lnx-012.mf.gov.pl* | *CNAME* | *NIE* |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa systemu** | **Nazwa SUBDOMENY w MF.GOV.PL** | **Nazwa domenowa (FQDN)\*** | **ID IP dla rekordu A/PTR lub FQDN dla rekordu CNAME** | **Typ rekordu DNS**  **[A, CNAME]** | **PTR**  **[Tak/Nie]** |
|  |  |  |  |  |  |  |

Tabela 21 Dane do utworzenia wpisu w DNS dla usługi - typ 3

#### Filtracja IPS w infrastrukturze CPD MF

*Wszystkie strefy bezpieczeństwa w środowisku CPD MF są monitorowane przez systemy IDS/IPS (Intrusion Detection System/Intrusion Prevention System). Systemy IDS/IPS pracują jako dedykowane urządzenia oraz moduły IPS uruchomione na zaporach sieciowych w ścieżce Intranetowej.*

*Każde z urządzeń posiada możliwość dedykowanej konfiguracji dla prawidłowej inspekcji ruchu jak i umożliwia skorzystanie z szablonów polityk przygotowanych przez producenta, przypisanych zarówno do wagi zagrożeń (high, medium, low), rodzaju usług (np. smtp, dns), a także bardziej szczegółowo; do typu aplikacji (np. Apache, IIS). Poszczególne grupy i pojedyncze ataki mogą być blokowane, ignorowane i jednocześnie logowane.*

*Ze względu na specyfikę działania urządzeń IPS, ochrona została zaimplementowana na poziomie rekomendowanym przez producenta. Zostały uruchomione sygnatury wykrywania, w tym wszystkie dotyczące ataków skierowanych przeciwko aplikacjom webowym, typu: Command Execution, Malicious File Execution, CSRF, Information Disclosure, PathTraversal, Authentication, BufferOverflow, Brute Force, Directory Indexing, Miscellaneous Attacks. Zapewnia to podstawową ochronę przed popularnymi zagrożeniami sieciowymi, przy minimalnym ryzyku powstawania alertów false-positive.*

*Zdarzenia sieciowe są monitorowane na bieżąco, natomiast pojawiające się po raz pierwszy będą weryfikowane przez administratorów IPS u właściciela systemu, celem wyjaśnienia, czy dany atak wynika z podjętych działań produkcyjnych lub testowych, czy też faktycznie stanowi zagrożenie. W zależności od odpowiedzi, ataki te będą blokowane, lub ignorowane.*

***W celu rozszerzenia ochrony IPS o specyficzne sygnatury ataków, wymagane do ochrony Systemu, należy poniżej opisać niezbędne opcje (np. poszerzona inspekcja SQL, Apache, JBoss).***

Specyficzne sygnatury ataków:

### Wymagania środowiska dla systemu backupowego

#### Wymagania na polityki tworzenia kopii bezpieczeństwa

|  |  |  |
| --- | --- | --- |
| *Typ polityki* | *np. P.B.AP.JBO.K1* | *Określa rodzaj backupowanych danych np. system operacyjny / serwer aplikacyjny / baza danych / inne* |
| *Okno backup’owe* | *przedział czasowy* | *Określa przedział czasowy, w którym ma być wykonywany backup* |
| *Retencja /  liczba kopii* | *liczba dni /  liczba kopii* | *Określa czas przechowywania backupu w dniach oraz liczbę przechowywanych kopii* |
| *Rodzaj kopii* | *full | inc.| cumul.* | *Określa czy backup jest pełny, przyrostowy czy kumulacyjny* |
| *Typ kopii* | *Online / Offline/ Migawkowa* | *Określa metodę wykonania kopii zgodnie z dokumentem „System backupowy w CPD MF”* |
| *Inne parametry* | *tekst* | *Inne parametry dotyczące polityki backupu jak np. ochrona kryptograficzna, multipleksacja, zastosowanie równoległych strumieni, LAN, SAN, Proxy, itp.* |

* *Pozostałe definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w Katalogu Usług [1] lub w dokumencie Bloki* *architektoniczne wspierające budowę systemów biznesowych [2]*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr polityki | Typ  polityki | Okno backup’owe | Retencja /liczba kopii | Rodzaj kopii | Typ kopii | Inne parametry |
|  |  |  |  |  |  |  |

Tabela 22 Wykaz polityk backup’u

#### Zabezpieczane elementy środowiska

* *Definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w Katalogu Usług [1] lub w dokumencie Bloki* *architektoniczne wspierające budowę systemów biznesowych [2]*
* *Przykład wypełnienia tabeli*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Lp.* | *ID bloku* | *Backup automatyczny*  *(T/N)* | *Oczekiwany czas odtwarzania [min]* | *Nr polityki (patrz Tabela 22)* |
| *1* | *pdr.pr.ap.01* | *T* |  | *1* |
| *2* | *pdr.pr.db.01* | *T* |  | *3* |

*Tabela. 23 Wykaz backup’owanych elementów*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **ID**  **bloku** | **Backup automatyczny (T/N)** | **Oczekiwany czas odtwarzania [min]** | **Nr polityki**  **(patrz Tabela 22)** |
|  |  |  |  |  |

Tabela 23 Wykaz backup’owanych elementów

# Zestawienie bloków architektonicznych

* *Zestawienie wszystkich usług/bloków architektonicznych oraz usług dostępowych na wszystkich rodzajach środowisk funkcjonujących w ramach Systemu określonych w rozdziale 4.* Rodzaje środowisk systemu*.*
* *Definicje poszczególnych parametrów oraz ich dopuszczalne wartości znajdują się w Katalogu Usług [1].*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Usługi dostępowe** | | | | **Rodzaj środowiska**  **systemu** |
| Lp. | ID bloku korzystającego z Usługi | | Numer Instancji Usługi |
| 1 |  | |  |  |
| 2 |  | |  |  |
| 3 |  | |  |  |
| **Bloki architektoniczne typu PaaS - aplikacyjne** | | | | **Rodzaj środowiska**  **systemu** |
| Lp. | ID bloku | Hostname | Numer instancji Usługi |  |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| **Bloki architektoniczne typu PaaS - bazodanowe** | | | | **Rodzaj środowiska**  **systemu** |
| Lp. | ID bloku | hostname | Numer instancji Usługi |  |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| **Bloki architektoniczne typu PaaS – systemy operacyjne** | | | | **Rodzaj środowiska**  **systemu** |
| Lp. | ID bloku | Hostname | Numer Instancji Usługi |  |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

Tabela 24. Zbiorcze zestawienie usług dostępowych i usług - bloków architektonicznych dla wszystkich środowisk funkcjonujących w ramach Systemu.

# Procedura uzyskiwania dostępu do poszczególnych bloków architektonicznych w środowisku Usług Katalogowych.

*W celu uzyskania dostępu do bloków architektonicznych za pomocą Usług z Katalogu CPD MF należy - zgodnie z Procedurą realizacji Wniosków o Usługę CPD MF (http://uslugi-it.cpd.mf.gov.pl/) - złożyć odpowiedni Wniosek, załączając zgodny z niniejszym szablonem Projekt z wypełnionymi poszczególnymi tabelami.*

*W celu udzielania dostępu dla użytkowników końcowych Systemu należy - zgodnie z Procedurą realizacji Wniosków o Usługę CPD MF (http://uslugi-it.cpd.mf.gov.pl/) - złożyć odpowiedni Wniosek o usługę pozakatalogową,*

*Informacje ogólne*

*Dostęp do wszystkich bloków architektonicznych odbywa się poprzez konta domenowe mf.gov.pl. Dla wykonawców z firm zewnętrznych tworzone są konta imienne, natomiast dla użytkowników biznesowych (w tym członkowie zespołów projektowych) do czasu integracji domen z centralną domeną MF - konta testowe. Użytkownicy posiadający już konta w domenie mf.gov.pl wykorzystują swoje konta imienne, po uprzednim powiązaniu tych kont z określonymi Grupami Zabezpieczeń.*

*Konta użytkowników powiązane są z Grupami Zabezpieczeń, które określają dodatkowe parametry kont. Między innymi grupy te regulują dostęp do bloków architektonicznych oraz dostęp do określonych systemów biznesowych.*

*Na wszystkie konta użytkowników w domenie mf.gov.pl spływają domyślne polityki domenowe, oraz indywidualne powiązania tych kont z Grupami Zabezpieczeń.*

*W ramach domeny mf.gov.pl przewiduje się m.in. następujące rodzaje kont użytkowników:*

*konto imienne*

*konto serwisowe*

*konto serwisowe z wyższymi uprawnieniami*

*konta testowe*

*Na wszystkie bloki architektoniczne dołączone do domeny mf.gov.pl, bazujące na bloku B.OS.WIN spływają polityki domenowe, zgodnie z powiązanymi Grupami Zabezpieczeń. Polityki te narzucają następujące ustawienia:*

*ustawienia polityk FireWall na serwerach, zgodnie z opisem Bloków Architektonicznych*

*ustawienia suffix’ów DNS w konfiguracji TCP/IP*

*blokada przekierowania schowka, mapowania lokalnych dysków, drukarek w sesji RDP*

*blokada kopiowania plików przez udziały sieciowe*

*ustawienia centralnego serwera WSUS*

*zmiana nazwy domyślnego administratora lokalnego (konto lokalne: Administrator)*

*Wszelkie prace związane z administrowaniem systemem muszą być wykonywane z konta imiennego lub serwisowego. Instalacja jakiejkolwiek aplikacji/usługi na blokach architektonicznych bazujących na bloku B.OS.WIN, z systemowego konta lokalnego administratora (konto nieistniejące w domenie mf.gov.pl) jest niedopuszczalna i spowoduje utratę funkcjonowania aplikacji po spłynięciu na dany serwer polityk GPO.*

*Usługi tworzone w ramach instalacji aplikacji mogą pracować jedynie na wymienionych poniżej kontach:*

*Local System*

*Local Service*

*Network Service*

*Dedykowane konto serwisowe utworzone w domenie mf.gov.pl*

# Grupy Zabezpieczeń

*Dla potrzeb autoryzacji użytkowników w blokach architektonicznych, lub/i w określonych systemach biznesowych tworzone są w domenie mf.gov.pl określone Grupy Zabezpieczeń, do który dodawani są określeni użytkownicy.*

*Projektant systemu zobowiązany jest do wypełnienia Tabeli w celu utworzenia grup zabezpieczeń w domenie* ***mf.gov.pl****.*

*Przypisanie użytkowników do grup zabezpieczeń odbywa się na podstawie odpowiedniego Wniosku Złożonego zgodnie z obowiązującą Procedurą*

*Wszystkie grupy zabezpieczeń mają określony standard nazewnictwa. W przypadku grup grupujących konta osób mających związek z systemami biznesowymi stosuje się następujący standard nazewnictwa:*

***GG-[SYSTEM\_BIZNESOWY]\_[KOD\_ŚRODOWISKA]\_[ROLA\_UZYTKOWNIKÓW]***

*Np.:*

*GG-SERCE\_PR\_Standard\_Users - grupuje użytkowników standardowych systemu biznesowego SERCE pracującego jako system produkcyjny*

*lub:*

*GG-HRM\_PR\_Administrators - grupuje administratorów systemu biznesowego Hermes – wersja produkcyjna*

|  |  |  |  |
| --- | --- | --- | --- |
| *L.p.* | *System Biznesowy* | *Kod środowiska* | *Nazwa grupy użytkowników* |
| *1* | *TREZOR* | *pr* | *wg standardu (\*)* |

*Tabela nr 25 – Grupy Zabezpieczeń*

*(\*) Standard w domenie* ***mf.gov.pl*** *- GG-[SYSTEM\_BIZNESOWY]\_[KOD\_ŚRODOWISKA]\_[ROLA\_UZYTKOWNIKÓW]*

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **System Biznesowy** | **Kod środowiska** | **Nazwa Grupy Zabezpieczeń** |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Tabela 25– Grupy zabezpieczeń

# Konta serwisowe

* *Konta serwisowe w AD w mf.gov.pl tworzone są na wniosek zespołu projektowego przez CPD MF, a ich nazewnictwo jest zgodne z opisanym poniżej standardem. Zespół projektowy wnioskuje o określoną liczbę kont wypełniając odpowiednią tabelę.*
* *Stosuje się określony standard nazewnictwa kont serwisowych:* ***SVC-XXX-NNN****, gdzie:*

*XXX oznacza 3 literowy kod usługi/aplikacji/programu,*

*NNN oznacza numer kolejny konta w klasyfikacji*

* *Konta serwisowe posiadają włączony atrybut zapobiegający przedawnieniu i wygaśnięciu hasła*
* *Najwyższy dopuszczalny poziom uprawnień dla Konta serwisowego to Administrator Lokalny.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Lp.* | *Rola konta* | *Wymagane uprawnienia, parametry konta* | *Osoba odpowiedzialna po stronie Klienta* | *Nazwa Konta* | *Hasło (\*)* |
| *1* | *Konto dla MS SQL – dla usługi …dla zadania … dla systemu biznesowego …* |  | *Imię i nazwisko – email, telefon* | *wg schematu MF*  *SVC-XXX-NNN*   * *Ustala CPD MF* | *Uzupełnia SI CPD MF* |

*Tabela nr 26 – Konta Serwisowe*

*(\*) – CPD MF zakłada stosowne konta, uzupełnia i odsyła zaszyfrowany plik. Hasło do pliku jest przekazywane Wnioskodawcy telefonicznie.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Rola konta** | **Wymagane uprawnienia, parametry konta** | **Osoba odpowiedzialna po stronie Klienta** | **Nazwa Konta** | **Hasło (\*)** |
|  |  |  |  |  |  |

Tabela 26– Konta Serwisowe

# Czynności serwisowe wymagające wyższych uprawnień

*Należy wskazać osoby odpowiedzialne za realizację prac serwisowych wymagających wyższych uprawnień. Wymagane jest podanie uzasadnienia wykorzystania tego typu konta.*

***Hasło nie zostaje ujawnione Wnioskodawcy.***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Imię i Nazwisko osoby odpowiedzialnej za konfigurację po stronie Klienta* | *Telefon email* | *Hostname serwerów których konfiguracja będzie dotyczyć* | *ID IP* | *Termin obowiązywania* |
| *Jan Kowalski* | *+48 600600600* | *sap-win-021 sap-win-023* | *trezor.pr.os.01.ip2* | *01.01.2010* |
| *Uzasadnienie potrzeby prac serwisowych z wyższymi uprawnieniami:*  *<wypełnia Klient> - Wnioskuję o umożliwienie instalacji klastra dla roli FileServer na wskazanych hostach.* | | | | |

*Tabela nr 27 – Wykaz bloków wymagających czynności z wyższymi uprawnieniami*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Imię i Nazwisko osoby odpowiedzialnej za konfigurację po stronie Klienta** | **Telefon email** | **Hostname serwerów których konfiguracja będzie dotyczyć** | **ID IP** | **Termin obowiązywania** |
|  |  |  |  |  |
| *Uzasadnienie potrzeby prac serwisowych z wyższymi uprawnieniami:* | | | | |

Tabela 27– Wykaz bloków wymagających czynności z wyższymi uprawnieniami

**Historia zmian**

*Należy określić wszystkie zmiany w wymaganiach w stosunku do poprzedniej wersji.*

*W przypadku aktualizacji listy przepływów należy oznaczyć kolorem dodane wiersze w odpowiedniej tabeli.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nr wersji** | **Data** | **Opis** | **Działanie (\*)** | **Rozdziały(\*\*)** | **Autorzy** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*(\*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja*

*(\*\*) Rozdziały: numery rozdziałów lub W-Wszystkie*