Załącznik nr 1 do wzoru umowy
Opis przedmiotu zamówienia
BDG-II-3820-23/10

Zawartość

MINIMALNE WYMAGANIA TECHNICZNE

I. Przedmiot zamówienia.

Przedmiotem zamówienia jest:

a) Stworzenie szczegółowego harmonogramu prac związanych z realizacją przedmiotu umowy z założeniem, iż cały projekt musi zostać zakończony w ciągu 35 dni roboczych od dnia podpisania umowy,
b) Audyt pod kątem migracji obecnie eksploatowanych przez Zamawiającego systemów IT (Active Directory, Exchange, ISA, BlackBerry)
c) Stworzenie środowiska laboratoryjnego (wirtualizacja),
d) Migracja domeny Active Directory 2003 do Active Directory 2008,
e) Migracja systemu pocztowego Exchange 2003 do Exchange 2010,
f) Migracja serwerów ISA 2006 do TMG,
g) Migracja środowiska BlackBerry Enterprise Server 4.1 do wersji 5.0 wraz z integracją z Exchange 2010,
h) Wdrożenie i skonfigurowanie System Center Operations Manager 2007,
i) Zapewnienie wsparcia powdrożeniowego,
j) Przeprowadzenie szkoleń administracyjnych.

Opracowanie określa parametry funkcjonalne i techniczne na poziomie obligatoryjnych wymagań minimalnych i koncepcji ogólnej, która jest niezbędna do przedstawienia przez Wykonawcę rozwiązania szczegółowego. Na etapie projektu Wykonawcy zostanie przedstawiony szczegółowy stan obecnej infrastruktury u Zamawiającego wraz z koniecznymi wyjaśnieniami.

II. Opis przedmiotu zamówienia – wymagania minimalne.

Wykonawca będzie zobowiązany do dostawy sprzętu oraz przygotowania nowego środowiska domeny AD 2008 i nowej organizacji Exchange 2010.

Na tym etapie Zamawiający oczekuje następujących produktów podlegających odbiorowi:

1. Dostawa i instalacja sprzętu:

1.1 Dostarczenie sprzętu zgodnie z załącznikiem nr 2 do umowy.

1.2 Wymagana instalacja wszystkich urządzeń w szafie RACK 19'' Zamawiającego. Zamawiający wymaga zapewnienia pełnego wyposażenia montażowego oraz konfigurację i uruchomienie

urządzeń oraz oprogramowania przy współpracy z administratorami Zamawiającego. Wymagane jest dostarczenie wszelkich kabli połączeniowych oraz elementów zapewniających instalację.

1.3 Wykonanie aktualizacji oprogramowania typu firmware oraz BIOS do najnowszych stabilnych wersji.

1.4 Przeprowadzenie testów poprawności działania dostarczonego sprzętu.

2. Przygotowanie domeny AD 2008 i aktualizacja domeny AD 2003

Wykonawca może przystąpić do aktualizacji systemów będących w posiadaniu Zamawiającego po przedstawieniu projektu technicznego, który musi zostać zaakceptowany przez Zamawiającego.

2.1 Aktualizacja domeny Windows 2003 do Windows 2008 – zadania:

Od oferentów wymagane jest przygotowanie i przeprowadzenie całego procesu migracji domeny, a w szczególności:

- ✓ Analiza domeny Windows 2003 pod kątem aktualizacji do Windows 2008.
- ✓ Przygotowanie projektu technicznego migracji do Windows 2008 z wykorzystaniem nowych funkcjonalności domeny Windows 2008:
    - Logicznej struktury Active Directory
    - Nazewnictwo obiektów w Active Directory
    - Struktura Lasu i Domeny AD
    - Poziom funkcjonalny domeny i lasu
    - Struktura jednostek organizacyjnych
        - ✓ Struktura jednostek organizacyjnych
        - ✓ Domyślne jednostki organizacyjne i kontenery
        - ✓ Specjalne jednostki organizacyjne
    - Obiekty zasad grupy (GPO)
        - ✓ Nazewnictwo Zasad Grupy
        - ✓ Zakres
        - ✓ Przypisywanie GPO
        - ✓ Kolejność wdrażania ustawień
        - ✓ Filtrowanie Zasad grupy
        - ✓ Zarządzanie obiektami Zasad grupy
        - ✓ Delegacja kontroli administracyjnej – na poziomie OU
    - Fizycznej struktury Active Directory
    - Lokalizacje i ilości kontrolerów domeny
    - Lokalizacja najbliższego kontrolera domeny
    - Wymiarowanie sprzętu pod DC
    - Standardowa konfiguracja kontrolera domeny
    - Rozmieszczenie wykazów globalnych
    - Rozmieszczenie wzorców operacji
    - Rozmieszczenie (GC) i (FSMO)
    - Topologia Replikacji, w szczególności:
        - Podsieci AD
        - Replikacja AD przez firewall
        - Szacunkowa objętość replikacji między lokacjami
        - Logowanie do domeny przez firewall
        - Lokacje (Sites)
        - Łącza lokacji (Sitelinks)
        - Topologia
        - Obiekty połączeniowe (Connections objects)
        - Serwery przyczółkowe (Bridgeheads Server)

- Usług sieciowych
- DNS
  - ✓ konfiguracja systemów korzystających z niego
  - ✓ Konfiguracja klientów DNS
  - ✓ Konfiguracja serwerów DNS
  - ✓ Opcje klienta DNS
  - ✓ Rejestracja Rekordów NS
  - ✓ Ogólne rekordy zasobowe SRV (Non-Site specyfic)
  - ✓ Site Coverage
- Synchronizacja czasu
- WINS
- DHCP
  - ✓ Standardowa konfiguracja zakresów DHCP
  - ✓ Rejestracja serwerów DHCP
- Bezpieczeństwa Active Directory
- Bezpieczeństwo fizyczne kontrolerów domeny
- Konfiguracja kontrolerów domeny
  - ✓ Lokalizacja plików bazy danych AD
  - ✓ Wybór uruchamianych usług
  - ✓ Zabezpieczenie przed atakiem na przestrzeń dyskową
- Zasad zabezpieczeń
- Default Domain Policy
  - Password Policy
  - Account Lockout Policy
  - Kerberos Policy
- Default Domain Controllers Policy
  - Audit Policy
  - User Rights Assignment
  - Ustawienia Security Options
  - Ustawienia Event Log
- PKI Policy
- Pozostałych zasad zabezpieczeń

- Inspekcja
- Zasady inspekcji (Audit Policy)
- Ustawienia inspekcji na istotnych obiektach Active Directory
  - ✓ Partycja Schematu (Schema Directory Partition)
  - ✓ Partycja konfiguracji (Configuration Directory Partition)
  - ✓ Partycja domeny (Domain Directory Partition)
  - ✓ Kontener zasad (Policies Container)

- ✓ Przed dokonaniem aktualizacji stworzenie wirtualnego środowiska laboratoryjnego Active Directory 2008 odzwierciedlającego środowisko produkcyjne.
- ✓ Instalacji i konfiguracji serwerów, systemów operacyjnych Windows 2008 R2, niezbędnych usług w celu uruchomienia systemów w roli kontrolerów domeny.
- ✓ Rekonfiguracja struktury fizycznej i logicznej Active Directory jeśli będzie to wymagane i stwierdzone podczas analizy.
- ✓ Zbudowanie koncepcji i scenariuszy aktualizacji uwzględniających wyniki prac laboratoryjnych i wymogi stawiane procesowi w ramach SIWZ.
- ✓ Przeorganizowanie usług DNS (wewnętrznych i zewnętrznych) i DHCP łącznie z przeniesieniem na inne serwery fizyczne lub wirtualne.
- ✓ Instalacja kontrolerów domeny w centrali na systemie Windows 2008 R2, oraz przeniesienie usług i adresacji z kontrolerów działających w centrali na systemie Windows 2003.
- ✓ Aktualizacja kontrolerów domeny w lokalizacjach Zamawiającego do systemu Windows Server 2008 x32.
- ✓ Podniesienie poziomu funkcjonalnego domeny i lasu.
- ✓ Migracja użytkowników, grup i komputerów do nowej wersji systemu.
- ✓ Aktualizacja protokołu replikacji kontrolerów domeny z FRS na DFS-R.

- ✓ Modyfikacja obiektów GPO tak aby były zgodne z najlepszymi praktykami i zaleceniami Microsoft dla domeny Windows 2008 – wykorzystanie nowych funkcjonalności oraz migracja z zasad zabezpieczeń przypisanych do lokalizacji.
- ✓ Instalacja, uruchomienie, konfiguracja sytemu monitoringu SCOM 2007 ze strukturą Active Directory.
- ✓ Instalacja, uruchomienie, konfiguracja systemu antywirusowego będącego w posiadaniu Zamawiającego z wykorzystaniem GPO.
- ✓ Ustawienie kopii zapasowych wszystkich kontrolerów domeny z wykorzystaniem oprogramowania będącego w posiadaniu Zamawiającego.

Wykonawca zobowiązany jest do przygotowania i przekazania Zamawiającemu kompletu dokumentacji oraz przygotowania i przećwiczenia procedur operacyjnych po wdrożeniu systemu. Dokumentacja powinna składać się m.in. z:

- ✓ Dokumentacji projektowej:
  - Analizę bieżącego systemu w zakresie niezbędnym do aktualizacji,
  - Projekt techniczny – szczegółowa konfiguracja systemu docelowego,
  - Plan prac wdrożeniowych lub migracyjnych wraz z harmonogramem,
  - Scenariusze i procedury testowe.
- ✓ Dokumentacja powdrożeniowa:
  - Finalna konfiguracja systemu,
  - Szczegółowy harmonogram testów wraz z wnioskami po testach,
  - Napotkane problemy podczas wdrożenia i sposób ich rozwiązania,
  - W odrębnym punkcie wszystkie niestandardowe ustawienia systemu lub zastosowane obejścia czy też kruczki,
  - Wszystkie skrypty lub procesy automatyzujące pracę systemu wraz z celem, opisem działania i harmonogramem uruchomień.
- ✓ Procedury operacyjne:
  - Procedury sprawdzania dostępności systemu
  - Procedury backupu systemu
    - Backup systemu operacyjnego na kontrolerach domeny
      - ✓ szczegółowa procedura wykonywania kopii bezpieczeństwa,
      - ✓ szczegółowa procedura sprawdzania poprawności wykonania backupu
    - Sugerowany schemat i harmonogram backupu
  - Procedury odtworzenia poszczególnych elementów systemu:
    - Odtworzenie kontrolera domeny, który jest właścicielem jednej lub więcej roli FSMO
    - Odtworzenie kontrolera domeny, który nie jest właścicielem FSMO
    - Odtworzenie całego lasu Active Directory w przypadku katastrofy i awarii wszystkich kontrolerów domeny
    - Autorytatywne odtworzenie wskazanego obiektu
  - Szczegółowe procedury utrzymaniowe systemu dla administratorów. Poziom szczegółowości powinien umożliwiać zdiagnozowanie gdzie dokładnie jest problem, bez opisu wszystkich możliwych scenariuszy jego naprawy:
    - Odnosząc się do architektury rozwiązania, które elementy sieciowe, sprzętowe
      i aplikacyjne powinny działać do poprawnej pracy systemu – aplikacji,
    - Które usługi i na jakich serwerach mają być dostępne – jak to sprawdzić?,
    - Jakie są standardowe problemy z domeną/systemem i sposoby ich rozwiązania,
    - Schemat powiązań systemu z innymi systemami (wraz z infrastrukturą techniczną)
  - Spisy zawierający sugerowane utrzymaniowe czynności administracyjne dla danego systemu wraz z ich interwałami czasowymi, np.:
    - Częstotliwość kontroli poprawności backupu,
    - Opis zawartości logów (kody i opisy błędów pojawiających się w logach),
    - Lista elementów (serwisy, logi, liczniki wydajności) do monitorowania systemu oraz ich wartości progowe, ostrzegawcze, krytyczne.
  - Szczegółowe procedury monitorowania systemu
  - Szczegółowe procedury konfiguracji systemów operacyjnych Windows 2008 dla poszczególnych serwerów w Active Directory

- Szczegółowe procedury do GPO
- Procedury migracji domeny oraz jej elementów do wersji Windows Server 2008

3. Przygotowanie Exchange 2010 i migracja poczty z Exchange 2003

Wykonawca może przystąpić do aktualizacji systemów będących w posiadaniu Zamawiającego po przedstawieniu projektu technicznego, który musi zostać zaakceptowany przez Zamawiającego.

3.1 Migracja systemu pocztowego do Exchange 2010 - zadania

Od oferentów wymagane jest przygotowanie i przeprowadzenie całego procesu migracji Poczty elektronicznej, a w szczególności:

- ✓ Analiza obecnego systemu pod kątem migracji do Exchange 2010.
- ✓ Przygotowanie projektu technicznego migracji do systemu Exchange 2010 w konfiguracji klastrowej opartej o technologię DAG zapewniającą wysoką dostępność.
- ✓ Instalacji i konfiguracji serwerów, systemów operacyjnych Windows 2008 R2, niezbędnych usług, systemu MS Exchange 2010, systemu antywirusowego i anty spamowego dla Exchange.
- ✓ Przed dokonaniem migracji stworzenie wirtualnego środowiska laboratoryjnego do Exchange 2010 odzwierciedlającego środowisko produkcyjne.
- ✓ Zbudowanie koncepcji i scenariuszy migracji uwzględniających wyniki prac laboratoryjnych i wymogi stawiane procesowi w ramach SIWZ(musi zostać zaakceptowana przez zamawiającego).
- ✓ Zachowanie dotychczasowej zawartości GAL. Powstała organizacja Exchange 2010 musi zapewniać synchronizację GAL i wymianę poczty z inną organizacją Exchange 5.5 w wewnętrznej sieci resortowej (która nie jest objęta projektem). Sieć wewnętrzna resortowa nie posiada bezpośredniego styku (połączenia) z siecią objętą projektem. Wymiana poczty i replikacja musi odbywać się poprzez „przełącznik" realizujący rotacyjne (co 15 minut) połączenia serwerów pocztowych między podsieciami. Synchronizacja ma zostać wykonana za pomocą MIIS (GALSync).
- ✓ Zmigrowanie poczty użytkowników do nowej organizacji Exchange musi obsługiwać tą samą domenę SMTP (ms.gov.pl).
- ✓ Przygotowanie środowiska do instalacji systemu Exchange.
- ✓ Instalacja systemu Exchange 2010 zgodnie z założeniami koncepcji.
- ✓ Instalacja programu antywirusowego zgodnie z założeniami koncepcji.
- ✓ Instalacja, uruchomienie, dostrojenie sytemu monitoringu SCOM 2007 z strukturą Exchange.
- ✓ Przygotowanie, konfiguracja systemu Exchange 2010 do współpracy z systemem monitoringu Zamawiającego oraz zdefiniowanie i uruchomienie min. 10 wskaźników, które powinny być monitorowane.
- ✓ Przygotowanie i konfiguracja systemu Exchange 2010 do współpracy z systemem backupu Zamawiającego oraz uruchomienie zadań archiwizacji zgodnie z przyjętym harmonogramem.
- ✓ Przygotowanie serwerów mailbox i wpięcie w sieć SAN Zamawiającego.
- ✓ Przygotowanie dokumentacji oraz przygotowanie i przećwiczenie procedur operacyjnych po wdrożeniu systemu.
- ✓ Zachowanie obecnej funkcjonalności komunikacji nowo migrowanego systemu Exchange 2010 z systemem Exchange 5,5 innej domeny
- ✓ Zachowanie obecnej funkcjonalności komunikacji nowo migrowanego systemu Exchange 2010 z systemem BlackBerry.
- ✓ Instalacji i konfiguracji serwerów, systemów z Windows 2008 R2 i usług, systemu MS Exchange 2010, systemu antywirusowego Symantec dla Exchange.
- ✓ Przygotowanie systemów Exchange 2003 i Exchange 2010 do migracji danych.
- ✓ Przeniesienie skrzynek pocztowych użytkowników oraz folderów publicznych między serwerami Exchange 2003 i Exchange 2010.
- ✓ Wykonanie migracji pilotażowej minimum 50 skrzynek, po której nastąpi przeprowadzenie testów akceptacyjnych zakończonych podpisaniem protokołu odbierającego migrację pilotażową.
- ✓ Wykonanie migracji pozostałych zasobów systemu Exchange 2003 do systemu 2010.
- ✓ Wykonanie wszystkich niezbędnych prac umożliwiających bezpieczne wyłączenie systemu Exchange 2003 z systemu produkcyjnego.

Wykonawca zobowiązany jest do przygotowania i przekazania Zamawiającemu kompletu dokumentacji oraz przygotowania i przećwiczenia procedur operacyjnych po wdrożeniu systemu. Dokumentacja powinna składać się m.in. z:

- ✓ Dokumentacja projektowa:
  - Analiza bieżącego systemu pod kątem niezbędnym do migracji,
  - Projekt techniczny – docelowa konfiguracja systemu zawierająca między innymi:
  - Architektura organizacji Exchange, rozmieszczenie serwerów pocztowych z podziałem na role, skalowanie i konfiguracja sprzętowa, współpraca z AD, Usługi rozwiązywania nazw, konektory, certyfikaty, ustawienia antyspam wynikające z przeprowadzonego tuningu, konieczne do wykonania zmiany w obecnej infrastrukturze, konfiguracja sieciowa (adresacja, porty dla współpracy przez Firewall), itp.
  - Rozmieszczenie serwerów Exchange Server 2010 z podziałem na role
  - Skalowanie i konfiguracja sprzętowa
    - ✓ Wersje Exchange Server 2010
    - ✓ Procesor
    - ✓ Pamięć
    - ✓ Podsystem dyskowy
  - Współpraca z Active Directory
    - ✓ Wymagania Exchange 2010 względem Active Directory
    - ✓ Rozmieszczenie obiektów serwerów Exchange 2010 w strukturze logicznej Active Directory
    - ✓ Modyfikacje usługi Active Directory
  - Usługi rozwiązywania nazw
    - ✓ DNS Suffix
    - ✓ Konfiguracja klienta DNS serwerów Hub/CAS
    - ✓ Konfiguracja rozwiązywania nazw dla serwerów Mailbox
    - ✓ Konfiguracja rozwiązywania nazw dla serwerów edge Transport
    - ✓ Rekordy DNS w strefie wewnętrznej
    - ✓ Konfiguracja rekordów PTR
    - ✓ Rekordy DNS w strefie publicznej
  - Konfiguracja sieciowa
    - ✓ Adresacja IP systemów objętych rozwiązaniem
    - ✓ Porty i usługi – konfiguracja firewall
  - Konfiguracja redundantnych ról Exchange Server 2010 - Serwery Transportowe
    - ✓ Accepted Domains
    - ✓ Hub Transport server Role
    - ✓ Konfiguracja transport SMTP – konektory
    - ✓ Konfiguracja reguł transportowych
  - Konfiguracja redundantnych ról Exchange Server 2010 - Client Access Server
    - ✓ Outlook Anywhere

- ✓ Autodiscover Virtual Directory
- ✓ ActiveSync
- ✓ Offline Address Book Virtual Directory
- ✓ Outlook Web Access

➢ Konfiguracja Exchange Server 2010: Klaster Mailbox DAG

- ✓ Konfiguracja usługi Windows Clustering
- ✓ Dedykowna konfiguracja sieciowa dla klastra Mailbox
- ✓ Nazwy hostów stosowane dla klastra Windows oraz Mailbox
- ✓ Konfiguracja podsystemu dyskowego
- ✓ Rozmieszczenie baz w grupach magazynowych
- ✓ Parametry mechanizmu replikacji DAG

➢ Konfiguracja oprogramowania AV/AS

➢ Archiwizacja i odzyskiwanie po awarii

- ✓ Metody zabezpieczenia serwerów
- ✓ Metoda zabezpieczania serwerów CAS
- ✓ Metoda zabezpieczania serwerów Hub Transport
- ✓ Metoda zabezpieczania serwerów IIS
- ✓ Harmonogram archiwizacji dla serwerów w roli Mailbox

➢ Plan prac wdrożeniowych lub migracyjnych wraz z harmonogramem.

➢ Scenariusze i procedury testowe.

✓ Dokumentacja powdrożeniowa wg. której powinno być możliwe odtworzenie całego systemu zawierającej szczegółowy opis wraz z zrzutami obrazu.

➢ Finalna Konfiguracja

➢ Finalna konfiguracja systemu Poczty oraz systemów wraz z powiązanymi systemami

➢ Harmonogram testów wraz z wnioskami po testach

➢ Napotkane problemy podczas wdrożenia i sposób ich rozwiązania

➢ W odrębnym punkcie wszystkie niestandardowe ustawienia systemu lub zastosowane obejścia czy też kruczki,

➢ Wszystkie skrypty lub procesy automatyzujące pracę systemu wraz z celem, opisem działania i harmonogramem uruchomień.

✓ Procedury operacyjne:

➢ Procedury backupu systemu:

- Backup systemu operacyjnego na serwerach gdzie działa system,
- Backup samej aplikacji (binaria oraz pliki konfiguracyjne) i na jakich serwerach/urządzeniach się znajdują
- Backup danych danej aplikacji – systemu: pliki, foldery na systemach plików, lokalne oraz zdalne (np. udziały sieciowe), pliki baz danych oraz ich logi itd.,
- Szczegółowy schemat i harmonogram backupu, przewidywana ilość danych,
- Backup całego środowiska IT niezbędnego do uruchomienia aplikacji/systemu w razie totalnej katastrofy (należy wymienić systemy, od których zależy wdrażany system)

➢ Procedurę weryfikacji dostępności systemu z punktu widzenia administratora (lista może zostać dodefiniowana przez Zamawiającego na etapie wdrożenia). Poziom szczegółowości powinien umożliwiać diagnozowanie gdzie dokładnie jest problem, bez opisu wszystkich możliwych scenariuszy jego naprawy:

- Odnoszące się do architektury rozwiązania, które elementy sieciowe, sprzętowe i aplikacyjne powinny działać do poprawnej pracy systemu – aplikacji,
- Które usługi i na jakich serwerach mają być dostępne – jak to sprawdzić?,
- Gdzie szukać szczegółowych informacji o problemach w aplikacji (np. szczegółowe logi danej aplikacji),

        - Jakie są standardowe problemy z aplikacją/systemem i sposoby ich rozwiązania,
        - Określenie elementów krytycznych systemu (wraz z określeniem komponentów(np. file system, bazy danych, itp.)) – czyli jakie warunki muszą być spełnione, aby system mógł poprawnie realizować funkcje biznesowe,
        - Schemat powiązań systemu z innymi systemami (wraz z infrastrukturą techniczną)
    - Procedurę sprawdzania dostępności systemu z punktu widzenia klienta końcowego, (podręcznik dla helpdesku)
    - Procedury przełączenia systemu do centrum zapasowego:
        - Opis automatycznego przełączania,
        - Procedura ręcznego przepięcia systemu do centrum zapasowego. W procedurze ręcznego przełączania muszą być wymienione wszystkie niezbędne akcje dla administratora, krok po kroku, komenda po komendzie
- ✓ Procedurę odtworzenia poszczególnych elementów systemu w tym procedury disaster recovery dla poszczególnych scenariuszy:
    - awaria serwera hub/cas
    - awaria węzła klastra mailbox
    - awaria pojedynczej bazy Exchange
    - awaria pojedynczej skrzynki
    - awaria całego systemu
- ✓ Procedur dot. skalowania systemu:
    a) dodanie kolejnych serwerów i ich odpowiednich ról (procedury instalacyjne)
    b) szacunkowych wielkości przy których konieczna jest rozbudowa danego elementu systemu
- ✓ Procedury – zadania szczegółowe dla opiekunów Systemu
- ✓ Spis zawierający sugerowane utrzymaniowe czynności administracyjne dla danego systemu wraz z ich interwałami czasowymi, np.:
    - Częstotliwość kontroli poprawności backupu
    - Opis zawartości logów (kody i opisy błędów pojawiających się w logach),
    - Lista elementów (serwisy, logi, liczniki wydajności) do monitorowania systemu oraz ich wartości progowe, ostrzegawcze, krytyczne.
- ✓ Zaleceń operacyjnych, w tym procedura odnowienia certyfikatu.
- ✓ Zaleceń dot. monitorowania pracy systemu.

4. Migracja serwerów ISA 2006 do Threat Management Gateway

Wykonawca może przystąpić do aktualizacji systemów będących w posiadaniu Zamawiającego po przedstawieniu projektu technicznego, który musi zostać zaakceptowany przez Zamawiającego.

4.1 Wdrożenie Threat Management Gateway

Od oferentów wymagane jest przygotowanie i przeprowadzenie całego procesu wdrożenia Threat Management Gateway, a w szczególności:

- ✓ Analizy obecnego systemu firewall pod kątem migracji do TMG 2010.
- ✓ Przygotowania projektu technicznego wdrożenia/migracji do systemu Threat Management Gateway w konfiguracji klastrowej opartej o technologię NLB
- ✓ Instalacji i konfiguracji serwerów, systemów operacyjnych Windows 2008 R2 wraz z aktualizacjami systemu, niezbędnych usług, Threat Management Gateway.
- ✓ Przygotowania dokumentacji oraz przygotowanie i przećwiczenie procedur operacyjnych po wdrożeniu systemu.
- ✓ Przed dokonaniem migracji stworzenie wirtualnego środowiska laboratoryjnego TMG 2010 odzwierciedlającego środowisko produkcyjne.
- ✓ Instalacji systemu TMG zgodnie z założeniami koncepcji
- ✓ Instalacji programu AV/AS zgodnie z założeniami koncepcji

- ✓ Przygotowania, konfiguracji systemu TMG do współpracy z systemem monitoringu SCOM 2007 oraz zdefiniowanie i uruchomienie wskaźników, które powinny być monitorowane.
- ✓ Zaprojektowania, przygotowania i konfiguracji systemu TMG do współpracy z systemem backupu Zamawiającego oraz uruchomienie zadań archiwizacji zgodnie z przyjętym harmonogramem.
- ✓ Przygotowania dokumentacji oraz przygotowanie i przećwiczenie procedur operacyjnych po wdrożeniu systemu:
- ✓ Przygotowania systemów ISA 2006 i TMG 2010 do migracji danych.
- ✓ Rekonfiguracji serwerów ISA 2006 do współpracy z TMG
- ✓ Rekonfiguracji ruchu sieciowego w celu wykorzystania TMG
- ✓ Bezpiecznego usunięcia po wdrożeniu TMG serwera ISA 2006 z systemu produkcyjnego
- ✓ Przeniesienia wszystkich dotychczasowych funkcjonalności (np. ustawienia, reguły, stref itd) na serwery TMG oraz rozszerzenie o nowe zgodnie z najlepszymi praktykami Microsoft

Wykonawca zobowiązany jest do przygotowania i przekazania Zamawiającemu kompletu dokumentacji oraz przygotowania i przećwiczenia procedur operacyjnych po wdrożeniu systemu. Dokumentacja powinna składać się m.in. z:

- ✓ Dokumentacja projektowa:
  - Analiza techniczna bieżącego systemu w zakresie niezbędnym do wdrożenia,
  - Projekt techniczny – docelowa konfiguracja systemu (Architektura systemu, konfiguracja serwerów, konfiguracja reguł i stref, zasady i ustawienia monitorowania, parametry logicznego zabezpieczenia, odzyskiwanie po awarii)
    - ✓ Architektura systemu Threat Management Gateway i systemów wspomagających – opis ogólny i schematy rozwiązania
    - ✓ Koncepcja nowego systemu
      - Funkcjonalność systemu
      - Rozmieszczenie serwerów Threat Management Gateway
      - Adresacja serwera oraz trasy routingu
      - Ruch wychodzący z sieci wewnętrznej
      - Ruch wchodzący do sieci wewnętrznej
      - Ruch wychodzący z sieci zewnętrznej, kierowany do serwera Exchange
      - Dane konfiguracyjne – serwer PROXY
  - Role serwerów
    - ✓ Role serwera TMG Internal
    - ✓ Role serwera TMG External
  - Konfiguracja serwera znajdującego się w sieci wewnętrznej
    - ✓ Nazwa serwera i przynależność do domeny
    - ✓ Dyski twarde i podział na partycje
    - ✓ Zainstalowane usługi
    - ✓ Adresacja serwera i trasy routingu
    - ✓ Konfiguracja serwera TMG
    - ✓ Konfiguracja reguł
      - Reguły ruchu sieciowego
      - Reguły ruchu: obiekty
      - Reguły dostępowe
      - Wszystkie pozostałe niezbędne reguły
  - Konfiguracja serwera znajdującego się w sieci DMZ
    - ✓ Nazwa serwera i przynależność do domeny
    - ✓ Dyski twarde i podział na partycje
    - ✓ Zainstalowane usługi
    - ✓ Adresacja serwera i trasy routingu
    - ✓ Konfiguracja serwera TMG
    - ✓ Konfiguracja reguł

        - Reguły ruchu sieciowego
        - Reguły ruchu: obiekty
        - Reguły dostępowe
        - Wszystkie pozostałe niezbędne reguły
    - Dodatkowe funkcjonalności
        - ✓ Inspekcja HTTPS
        - ✓ Kontrola pasma
        - ✓ Publikowanie aplikacji
        - ✓ Dostęp do sieci
        - ✓ Filtracja URL
        - ✓ Serwer proxy
    - Monitorowanie i system raportowania
        - ✓ Konfiguracja logowania
        - ✓ Konfiguracja raportowania
        - ✓ Konfiguracja alertów
        - ✓ Konfiguracja monitorowania połączeń
    - Zabezpieczenie serwerów
    - Archiwizacja i odzyskiwanie po awarii
        - ✓ Metody zabezpieczania serwerów
        - ✓ Harmonogram archiwizacji dla serwerów Threat Management Gateway
    - Plan prac wdrożeniowych i/lub migracyjnych wraz z harmonogramem.
    - Scenariusze i procedury testowe
    - Przygotowanie kompletu dokumentacji oraz przygotowanie i przećwiczenie procedur operacyjnych po wdrożeniu systemu

- ✓ Dokumentacja powdrożeniowa:
    - Finalna konfiguracja systemu,
    - Finalna konfiguracja systemu TMG oraz systemów wraz z powiązanymi systemami
    - Harmonogram testów wraz z wnioskami po testach
    - Napotkane problemy podczas wdrożenia i sposób ich rozwiązania
    - W odrębnym punkcie wszystkie niestandardowe ustawienia systemu lub zastosowanie obejścia czy też kruczki
    - Wszystkie skrypty lub procesy automatyzujące pracę systemu wraz z celem, opisem działania i harmonogramem uruchomień
    - Wnioski po testach produkcyjnych,
- ✓ Procedury operacyjne:
    - Procedury backupu systemu:
        - ✓ Backup systemu operacyjnego na serwerach gdzie działa system,
        - ✓ Backup samej aplikacji (binarna oraz pliki konfiguracyjne) i na jakich serwerach/urządzeniach się znajdują,
        - ✓ Backup danych danej aplikacji – systemu: pliki, foldery na systemach plików, lokalne oraz zdalne (np. udziały sieciowe), pliki baz danych oraz ich logi itd.,
        - ✓ Schemat i harmonogram backupu, przewidywana ilość danych
    - Procedurę sprawdzania dostępności systemu z punktu widzenia klienta końcowego (podręcznik dla HelpDesku),
    - Procedurę sprawdzania dostępności systemu z punktu widzenia administratora (zadania dzienne/tygodniowe/miesięczne). Poziom szczegółowości powinien umożliwiać zdiagnozowanie gdzie dokładnie jest problem, bez opisu wszystkich możliwych scenariuszy naprawy:
        - o Odnosząc się do architektury rozwiązania, które elementy sieciowe, sprzętowe i aplikacyjne powinny działać do poprawnej pracy systemu – aplikacji
        - o Które usługi i na jakich serwerach mają być dostępne – jak to sprawdzić?,
        - o Jakie są standardowe problemy za aplikacją/systemem i sposoby ich rozwiązania,
        - o Schemat powiązań systemu z innymi systemami (wraz z infrastrukturą techniczną)
    - Procedurę odtworzenia poszczególnych elementów systemu:
        - ✓ Jeżeli system składa się z więcej niż jednego serwera to musi być opisany proces odtwarzania każdego z nich. Procedura musi być tak szczegółowa, aby zawierała

wszystkie niezbędne polecenia – akcje niezbędne do poprawnego przywrócenia środowiska,
- ✓ Procedurę odtwarzania całego systemu w razie katastrofy jasno określającą kolejność odtwarzania poszczególnych elementów systemu.

- Spis zawierający utrzymaniowe czynności administracyjne dla danego systemu wraz z ich interwałami czasowymi, np.:
  - Częstotliwość kontroli poprawności backupu
  - Opis zawartości logów (kody i opisy błędów pojawiających się w logach),
  - Lista elementów (serwisy, logi, liczniki wydajności) do monitorowania systemu oraz ich wartości progowe, ostrzegawcze i krytyczne.

5. Migracja środowiska BlackBerry Enterprise Server 4.1 do wersji 5.0 wraz z integracją z Exchange 2010

Od Wykonawcy wymagane jest przygotowanie i przeprowadzenie całego procesu migracji środowiska BlackBerry i konfiguracji serwerów poczty, w szczególności:

- Analiza obecnego systemu BlackBerry pod kątem migracji do wersji 5.0 i współpracy z Exchange 2010.
- Opracowanie dokumentu - Szczegółowa Koncepcja migracji z wyspecyfikowaniem ścieżek migracji
- Przygotowanie projektu technicznego migracji do systemu BlackBerry 5.0 i współpracy z Exchange 2010.
- Przygotowanie kompletu dokumentacji oraz przygotowanie i przećwiczenie procedur operacyjnych po wdrożeniu systemu:
  - Dokumentacja projektowa powinna zawierać:
    - ✓ Analizę techniczną bieżącego systemu w zakresie niezbędnym do migracji,
    - ✓ Projekt techniczny - docelowa konfiguracja systemu
      - Architektura systemu BlackBerry , konfiguracja i sposób migracji systemu, schematy rozwiązania
      - Konfiguracja systemu poczty pod kątem współpracy z systemem BlackBerry
      - Skalowanie i konfiguracja sprzętowa
        - Procesor
        - o Pamięć
        - Podsystem dyskowy
      - Konfiguracja sieciowa
        - Adresacja IP systemów objętych rozwiązaniem
        - Porty i usługi - konfiguracja firewall
      - Backup i odzyskiwanie po awarii
    - ✓ Plan prac wdrożeniowych lub migracyjnych wraz z harmonogramem.
    - ✓ Scenariusze i procedury testowe.
  - Dokumentacja powdrożeniowa - poza finalną konfiguracją muszą być wymienione:
    - ✓ Harmonogram testów wraz z wnioskami po testach,
    - ✓ Napotkane problemy podczas wdrożenia i sposób ich rozwiązania,
    - ✓ W odrębnym punkcie wszystkie niestandardowe ustawienia systemu lub zastosowanie obejścia czy też kruczki

- Procedury backupu systemu:
  - ✓ Backup samej aplikacji (binaria oraz pliki konfiguracyjne) i na jakich serwerach/urządzeniach się znajdują,
  - ✓ Backup danych danej aplikacji - systemu: pliki, foldery na systemach plików, lokalne oraz zdalne (np. udziały sieciowe), pliki baz danych oraz ich logi itd.,
  - ✓ Schemat i harmonogram backupu, przewidywana ilość danych
- Procedurę odtworzenia poszczególnych elementów systemu:
  - ✓ Jeśli system składa się z więcej niż jednego serwera to musi być opisany proces odtwarzania każdego z nich. Procedura musi być tak szczegółowa, aby zawierała wszystkie niezbędne polecenia - akcje niezbędne do poprawnego przywrócenia środowiska,
  - ✓ Procedurę odtwarzania całego systemu w razie katastrofy jasno określającą kolejność odtwarzania poszczególnych elementów systemu.

6. Stworzenie środowiska laboratoryjnego (wirtualizacja).

- Odzwierciedlenie infrastruktury produkcyjnej Zamawiającego (zgodne z przedmiotem zamówienia) - na jego sprzęcie i oprogramowaniu (Hyper-V) w laboratorium
- Instalacja nowego środowiska objętego projektem
- Migracja odzwierciedlonego środowiska do przygotowanego nowego w laboratorium
- Testy przygotowanych procedur w środowisku laboratoryjnym
- Opracowanie szczegółowego harmonogramu z podziałem zadań (Zamawiający, Wykonawca) na podstawie przeprowadzonych prac w laboratorium

7. Szkolenia administracyjne

Warsztaty dla administratorów z zakresu instalacji, konfiguracji i obsługi w ilości po 16 godzin dla każdej z wdrożonych technologii, tj. Active Directory 2008, Exchange 2010, TMG, MS SCOM 2007, BlackBerry 5,0.

Szkolenia autoryzowane z AD 2008, Exchange 2010, TMG 2010 i MS SCOM 2007:

- MS-6419, MS-6421, MS-6422, MS-6423, MS-6425 przeprowadzone dla 6 pracowników Ministerstwa Sprawiedliwości,
- MS-10135 dla 2 pracowników Ministerstwa Sprawiedliwości
- MS-50020 dla 3 pracowników Ministerstwa Sprawiedliwości
- MS-50028 dla 2 pracowników Ministerstwa Sprawiedliwości

8. Wsparcie powdrożeniowe

- ✓ Nieodpłatne wsparcie serwisowe w usuwaniu pojawiających się problemów w domenie Active Directory 2008 i systemach ją przechowujących jak również z Exchange 2010, Microsoft TMG, MS SCOM 2007 przez okres 24 miesięcy od zakończenia prac wdrożeniowych środowiska produkcyjnego.

- ✓ Prowadzenie przez Wykonawcę bazy wiedzy występujących problemów z możliwymi ścieżkami ich rozwiązania i udostępnienie jej Zamawiającemu On-Line.
- ✓ Osoby świadczące wsparcie muszą legitymować się odpowiednimi certyfikatami inżynierskimi i odpowiednim doświadczeniem we wdrażaniu budowanych i podobnych rodzajem i skalą systemów (AD, Exchange, ISA/TMG, MS SCOM 2007).

9. Wymagania dodatkowe

- Należyta staranność
- System musi zapewnić wymagany poziom bezpieczeństwa
- System musi być zgodny z wewnętrznymi standardami i politykami Ministerstwa Sprawiedliwości
- System musi zapewnić wymaganą funkcjonalność.
- Budowany system, zarówno w fazie budowy jak i użytkowania, nie może zakłócić działania krytycznych aplikacji.
- System musi opierać się na ugruntowanych standardach tak, aby umożliwiać dalszy rozwój struktury w tym rozszerzenie funkcjonalności.
- Konfiguracja brzegowych urządzeń aktywnych do obsługi ruchu objętego projektem.
- Wszystkie procedury powinny być tak napisane aby umożliwiały krok po kroku ich wykonanie.
- Po ukończeniu migracji zostaje środowisko produkcyjne i laboratoryjne, które będzie wykorzystywane przez Zamawiającego do przeprowadzania testów przed dokonaniem istotnych zmian na środowisku produkcyjnym.
- Zadania zlecone Wykonawcy mogą zostać doprecyzowane przez Zamawiającego w trakcie procesu migracji aby została zachowana dotychczasowa funkcjonalność zarówno środowiska Active Directory, Exchange, ISA Server.
- Migracja do nowego środowiska domeny Active Directory, organizacji Exchange i TGM 2010 muszą być niezauważalne z punktu widzenia użytkownika co będzie się charakteryzowało:
  - Pojedynczym logowaniem do nowego i starego środowiska w czasie trwania migracji,
  - zachowaniem dotychczasowego profilu pocztowego i systemowego (profil logowania) migrowanemu użytkownikowi,
  - zachowaniem dotychczasowych uprawnień do zasobów sieciowych,
  - zachowaniem funkcjonalności dotychczasowych skryptów logowania,
  - zachowaniem dotychczasowych mapowań drukarek sieciowych,
  - zachowaniem dotychczasowej poczty migrowanego użytkownika,
  - zachowaniem dotychczasowej struktury i zawartości folderów publicznych Exchange 2003.
- Migracja WSUS do najnowszej stabilnej wersji, która obejmie:
  - Instalację i konfigurację środowiska WSUS
  - Przed instalacją i konfiguracją WSUS wymagane jest stworzenie środowiska laboratoryjnego odzwierciedlającego środowisko produkcyjne
  - Przygotowanie pełnej dokumentacji dla nowego środowiska WSUS składającej się z:
    - Dokumentacji projektowej:
      - Analiza techniczna bieżącego systemu w zakresie niezbędnym do wdrożenia
      - Projekt techniczny – docelowa konfiguracja systemu

- Skalowanie i konfiguracja sprzętowa
- Koncepcja nowej wersji systemu
  - Funkcjonalność systemu
  - Rozmieszczenie serwerów
- Projekt OU dla grup komputerów
- Projekt GPO dla zdefiniowanych grup komputerów
  - Dla stacji roboczych
  - Dla serwerów

✓ Dokumentacji powdrożeniowej:

- Finalna konfiguracja systemu,
- Finalna konfiguracja systemu WSUS oraz systemów wraz z powiązanymi systemami
- Harmonogram testów wraz z wnioskami po testach
- W odrębnym punkcie wszystkie niestandardowe ustawienia systemu lub zastosowanie obejścia czy też kruczki
- Wszystkie skrypty lub procesy automatyzujące pracę systemu wraz z celem, opisem działania i harmonogramem uruchomień
- Wnioski po testach produkcyjnych

✓ Procedur operacyjnych:

- Procedurę sprawdzania dostępności systemu z punktu widzenia klienta końcowego (podręcznik dla HelpDesku),
- Procedurę sprawdzania dostępności systemu z punktu widzenia administratora (zadania dzienne/tygodniowe/miesięczne). Poziom szczegółowości powinien umożliwiać zdiagnozowanie gdzie dokładnie jest problem, bez opisu wszystkich możliwych scenariuszy naprawy:
  - Odnosząc się do architektury rozwiązania, które elementy sieciowe, sprzętowe i aplikacyjne powinny działać do poprawnej pracy systemu – aplikacji
  - Które usługi i na jakich serwerach mają być dostępne – jak to sprawdzić?,
  - Jakie są standardowe problemy za aplikacją/systemem i sposoby ich rozwiązania,
  - Schemat powiązań systemu z innymi systemami (wraz z infrastrukturą techniczną)
- Spis zawierający utrzymaniowe czynności administracyjne dla danego systemu wraz z ich interwałami czasowymi, np.:
  - Opis zawartości logów (kody i opisy błędów pojawiających się w logach),
  - Lista elementów (serwisy, logi, liczniki wydajności) do monitorowania systemu oraz ich wartości progowe, ostrzegawcze i krytyczne.

- Wdrożenie System Center Operations Manager 2007, które obejmuje:
  - Instalację i konfigurację środowiska MS SCOM 2007
  - Objęcie monitoringiem 15 serwerów wskazanych przez Zamawiającego
  - Odzwierciedlenie w środowisku laboratorium.
  - Przygotowanie pełnej dokumentacji dla nowego środowiska MS SCOM 2007 składającej się z:

➢ Dokumentacji projektowej:

- Analiza techniczna bieżącego systemu w zakresie niezbędnym do wdrożenia
- Projekt techniczny – docelowa konfiguracja systemu MS SCOM 2007
  - Skalowanie i konfiguracja sprzętowa

- Procesor
- Pamięć
- Podsystem dyskowy

- Koncepcja systemu MS SCOM
  - Funkcjonalność systemu
  - Rozmieszczenie serwerów
- Konfiguracja systemu MS SCOM 2007 pod kątem współpracy z monitorowanymi systemami
- Konfiguracja sieciowa
  - Adresacja IP systemów objętych rozwiązaniem
  - Porty i usługi - konfiguracja firewall
- Backup i odzyskiwanie po awarii

- Plan prac wdrożeniowych wraz z harmonogramem.
- Scenariusze i procedury testowe.
- Procedura dodawania nowego serwera lub stacji roboczej do SCOM 2007 łącznie z konfiguracją i dostrojeniem.

✓ Dokumentacji powdrożeniowej:

- Finalna konfiguracja systemu,
- Finalna konfiguracja systemu MS SCOM 2007 oraz systemów wraz z powiązanymi systemami
- Harmonogram testów wraz z wnioskami po testach
- W odrębnym punkcie wszystkie niestandardowe ustawienia systemu lub zastosowanie obejścia czy też kruczki
- Wszystkie skrypty lub procesy automatyzujące pracę systemu wraz z celem, opisem działania i harmonogramem uruchomień
- Wnioski po testach produkcyjnych
- Napotkane problemy podczas wdrożenia i sposób ich rozwiązania,
- W odrębnym punkcie wszystkie niestandardowe ustawienia systemu lub zastosowanie obejścia czy też kruczki

✓ Procedur operacyjnych:

- Procedurę sprawdzania dostępności systemu z punktu widzenia klienta końcowego (podręcznik dla HelpDesku),
- Procedurę sprawdzania dostępności systemu z punktu widzenia administratora (zadania dzienne/tygodniowe/miesięczne). Poziom szczegółowości powinien umożliwiać zdiagnozowanie gdzie dokładnie jest problem, bez opisu wszystkich możliwych scenariuszy naprawy:
  - Odnosząc się do architektury rozwiązania, które elementy sieciowe, sprzętowe i aplikacyjne powinny działać do poprawnej pracy systemu – aplikacji
  - Które usługi i na jakich serwerach mają być dostępne – jak to sprawdzić?,
  - Jakie są standardowe problemy za aplikacją/systemem i sposoby ich rozwiązania,
  - Schemat powiązań systemu z innymi systemami (wraz z infrastrukturą techniczną)

- Spis zawierający utrzymaniowe czynności administracyjne dla danego systemu wraz z ich interwałami czasowymi, np.:
  - Opis zawartości logów (kody i opisy błędów pojawiających się w logach),
  - Lista elementów (serwisy, logi, liczniki wydajności) do monitorowania systemu oraz ich wartości progowe, ostrzegawcze i krytyczne.

✓ Procedury powdrożeniowe

- Procedury backupu systemu:
  - Backup samej aplikacji (binaria oraz pliki konfiguracyjne) i na jakich serwerach/urządzeniach się znajdują,
  - Backup danych danej aplikacji - systemu: pliki, foldery na systemach plików, lokalne oraz zdalne (np. udziały sieciowe), pliki baz danych oraz ich logi itd.,
  - Schemat i harmonogram backupu, przewidywana ilość danych
- Procedurę odtworzenia poszczególnych elementów systemu:
  - Procedurę odtwarzania całego systemu w razie katastrofy jasno określającą kolejność odtwarzania poszczególnych elementów systemu.

III. Koncepcja rozwiązania Exchange i Active Directory.

1. Organizacja Exchange 2003 w MS

Koncepcja rozwiązania zakłada rozbudowę istniejącej organizacji Exchange 2003 o nowe serwery pracujące pod kontrolą Exchange Server 2010. W związku z tym wszystkie zasoby związane z pocztą będą częścią istniejącej domeny Active Directory Ministerstwa Sprawiedliwości. W tej konfiguracji wszystkie serwery pocztowe są obsługiwane przez las MS, w którym również są utworzone konta użytkowników dla pracowników MS w ilości ok. 1300 szt. W lokalizacji Ujazdowskie znajdują się dwa serwery Exchange 2003 pracujące w trybie Front-end back-end. Separacją serwerów pocztowych zajmie się MS ISA 2006. Wszystkie serwery pocztowe pracują w ramach tej samej Organizacji. Klienci do obsługi poczty wykorzystują MAPI\SMTP z przechowywaniem poczty zarówno na serwerze jak i w plikach pst. W strukturze pocztowej zlokalizowano Foldery Publiczne synchronizowane w ramach Organizacji. Klienci do poczty dostają się za pomocą MS Outlook 2003 i 2007, OWA.

W organizacji znajdują się 4 obiekty typu „Storage group" oraz 11 obiektów typu „Store".

W systemie występuje jedna grupa administracyjna.

Na etapie Projektu Wykonawcy zostanie przedstawiony szczegółowy stan obecnej infrastruktury u Zamawiającego wraz z koniecznymi wyjaśnieniami.

2. Organizacja Active Directory 2003 w MS

Środowisko składa się z sześciu połączonych lokalizacji. Dwie z lokalizacji (Krasińskiego, Barska) posiada połączenia VPN z centralą realizowane za pomocą urządzeń Cisco. W każdej z tych lokalizacji znajduje się kontroler domeny 2003. Pozostałe lokalizacje (Czerniakowska, Ujazdowskie, Zwycięzców, Chopena) połączone są siecią LAN. Łącznie w tych lokalizacjach znajdują się trzy kontrolery domeny 2003. Każdy użytkownik struktury MS posiada konto domenowe i adres email. Loguje się ze stacji należącej do domeny 2003 za pomocą karty inteligentnej Aladdin eToken. Liczba komputerów w przybliżeniu równa się liczbie użytkowników.

Na etapie Projektu Wykonawcy zostanie przedstawiony szczegółowy stan obecnej infrastruktury u Zamawiającego wraz z koniecznymi wyjaśnieniami.

3. Konfiguracja Exchange 2010

Aktualnie wykorzystywane serwery Exchange 2003 nie zostaną uaktualnione do wersji Exchange 2010 tak, więc do czasu przeprowadzenia migracji tych serwerów lub ich usunięcia z organizacji, środowisko organizacji pocztowej MS będzie pracowało w koegzystencji.

4. Nowe środowisko Exchange 2010 i Active Directory 2008

Wykonawca będzie zobowiązany do przygotowania nowego środowiska domeny AD 2008 i nowej Organizacji Exchange 2010.

W celu realizacji założeń koncepcji sugeruje się wykorzystanie następujących serwerów:

- 4 serwery Microsoft Exchange Server 2010
- 2 serwery TMG
- 5 serwerów Domain Controler
- 2 serwery dla środowiska laboratoryjnego
- 1 serwer do SCOM 2007

Dla wszystkich serwerów, oprócz 2 kontrolerów domen, zostanie wykorzystany system operacyjny Microsoft Windows Server 2008 R2 64 bit. Szczegółowe informacje na temat wersji oraz edycji systemów zostały opisane w dalszej części dokumentu.

Logiczna i techniczna realizacja projektu będzie się opierać na jednej domenie logicznej: ms.gov.pl.

Organizacja Exchange 2010 zostanie wdrożona w oparciu o infrastrukturę Active Directory bazującą na kontrolerach pracujących pod kontrolą systemu Windows 2008 i Windows 2008 R2.

Struktura organizacji Exchange ma zapewnić bezpieczeństwo, redundancję oraz wysoką dostępność poczty korporacyjnej Ministerstwa Sprawiedliwości.

Sposób migracji musi zostać zrealizowany w sposób, który nie wpłynie na ciągłość pracy w godz. 8.15 – 16.15.

5. Bezpieczeństwo

Bezpieczeństwo serwerów oraz bezpieczny dostęp użytkowników do poczty firmowej zostanie zapewniony dzięki zastosowaniu serwerów Forefront Threat Management Gateway (TMG) 2010, oraz Intelligent Application Gateway 2007/ Forefront Unified Access Gateway 2010. Każde połączenie użytkownika do systemu poczty będzie realizowane w sposób bezpieczny z wykorzystaniem protokołu SSL. Tunel SSL będzie terminowany przez serwer TMG lub serwer IAG/UAG, który dokona uwierzytelnienia użytkownika i tylko w przypadku powodzenia tej operacji umożliwi połączenie z serwerem Exchange. Połączenie między serwerami TMG oraz IAG/UAG a serwerami Exchange również będzie realizowane z wykorzystaniem SSL.

6. Architektura rozwiązania

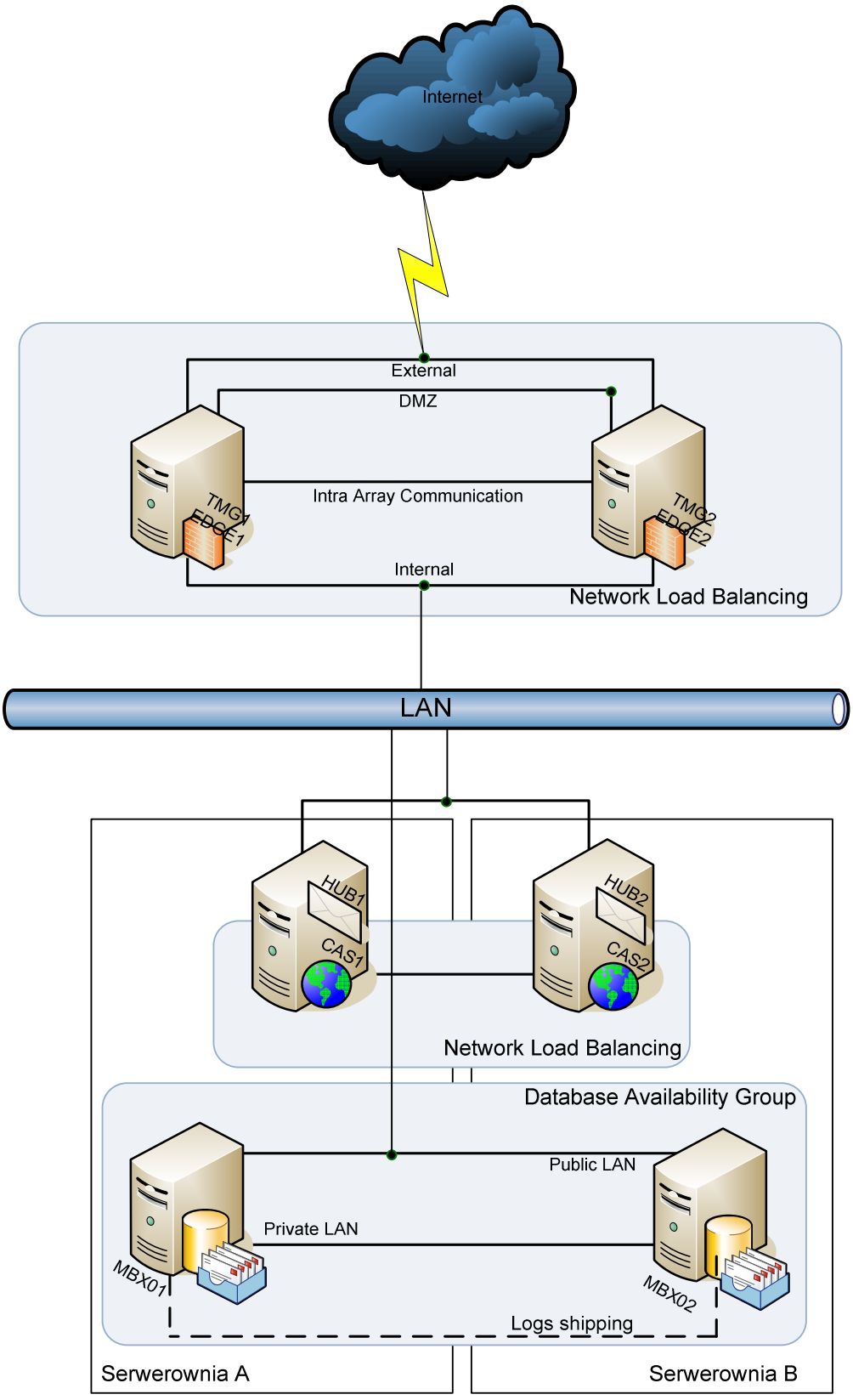
6.1 Rozmieszczenie usług

Koncepcja zakłada, rozbudowę organizacji pocztowej Exchange 2003 do wersji Exchange Server 2010 oraz Active Directory 2003 do wersji 2008 przez dodanie nowych serwerów, na których rozmieszczone zostaną poszczególne usługi. Wykorzystane zostaną następujące role serwerów Exchange Server 2010:

- **Edge Transport Server** –Zainstalowane zostaną dwa serwery Edge Transport, które odpowiedzialne będą za odbieranie i wysyłanie wiadomości SMTP do i z Internetu. Serwery będą dostarczały usługi skanowania antywirusowego i antyspamowego. Instalacja roli Edge Transport zostanie wykonana na tych samych serwerach, na których pracowało będzie oprogramowanie TMG. Dzięki takiej instalacji możliwe będzie pełne wykorzystanie wszystkich cech TMG oraz Exchange Server 2010 wspólnie tworzących mechanizm E-mail Protection.
- **Hub Transport Server** – Dwa serwery tego typu będą świadczyły usługi transportu wiadomości wewnątrz organizacji Exchange oraz przekazywanie wiadomości do i z serwerów Edge. Serwery zostaną zainstalowane w sieci LAN. Dla tego typu serwerów powinno zostać zainstalowane oprogramowanie Windows Server 2008 R2 Standard 64bit oraz Exchange Server 2010 Standard 64bit. Rola Hub Transport będzie współdzielona na serwerach z rolą Client Access Server.
- **Client Access Server** – Będą realizowały usługi dostępu klienckiego. Zostaną zainstalowane dwa tego typu serwery, które będą pracowały w klastrze Network Load Balancing. Dla tego typu serwerów powinno zostać zainstalowane oprogramowanie Windows Server 2008 R2 Standard 64bit oraz Exchange Server 2010 Standard 64bit. Rola Client Access Server będzie współdzielona na serwerach z rolą Hub Transport.
- **Mailbox Server** – Skrzynki pocztowe użytkowników obsługiwane będą przez dwa serwery w roli Mailbox, dla których zostanie skonfigurowany mechanizm Database Availability Group (DAG). Zalecane jest umieszczenie serwerów mailbox w różnych jednostkach fizycznych (dwie serwerownie).

Za bezpieczeństwo dostępu do systemu pocztowego odpowiedzialny będzie dwuwęzłowych klaster Network Load Balancing serwerów Forefront TMG Enterprise.

Na Rysunku nr.1 przedstawiony został schemat rozmieszczenia usług dla rozwiązania opisanego w niniejszym dokumencie opartego o Exchange 2010.



Rysunek 1 Schemat rozmieszczenia usług

Wszystkie usługi zakładają redundancję. W celu osiągnięcia wysokiej wydajności i niezawodności zastosowane zostaną rozwiązania zapewniające równoważenie obciążenia i minimalizację prawdopodobieństwa wystąpienia awarii.Wybrano następujące rozwiązania zapewniające wysoką wydajność i nadmiarowość:

- **Network Load Balancing** – umożliwia połączenie w klaster NLB serwery pracujące pod kontrolą systemu Windows Server 2008 R2. Dzięki połączeniu serwerów w klaster NLB przychodzące połączenia sieciowe będą równomiernie rozdzielane między wszystkie węzły klastra. W przypadku awarii jednego z węzłów będzie on pomijany poprzez przekierowanie przychodzących połączeń do pozostałych serwerów, aż do czasu przywrócenia pełnej funkcjonalności. Klaster NLB może być rozbudowywany do 32 węzłów. Network Load Balancing zostanie wykorzystany dla serwerów pełniących rolę Client Access Server – szczegółowe informacje na temat serwerów CAS zostały umieszczone w dalszej części dokumentu.
- **Database Avaiability Group** – W celu zapewnienia ciągłości pracy serwera obsługującego skrzynki użytkowników (Exchange 2010 Maiblox Server Role) wykorzystany zostanie mechanizm DAG. Jest to mechanizm umożliwiający do tworzenia do 16 kopii baz danych na różnych serwerach Exchange 2010 w obrębie organizacji. Usługa Failover Cluster umożliwia przełączanie pojedynczych baz danych między poszczególnymi członkami grupy replikacyjnej DAG. W przypadku awarii całego serwera bądź jednej z baz danych wykorzystana zostanie jej kopia na drugim serwerze.
- **DNS Round Robin** - Algorytm Round Robin umożliwia równoważenie obciążenia dla usług, które nie mogą być elementem rozwiązań klastrowych. DNS Round Robin zostanie wykorzystany do równoważenia usług świadczonych przez serwery Exchange Server 2010 Edge Transport.

Dzięki zastosowaniu wymienionych powyżej rozwiązań cała struktura organizacji pocztowej powinna spełniać kryteria wysokiej dostępności i wydajności.

Rozmieszczenia usług dla rozwiązania opisanego w niniejszym dokumencie opartego o Active Directory 2008 będzie polegało na rozszerzeniu funkcjonalności występujących w AD 2008 oraz rozdzieleniu usług zainstalowanych w dotychczasowym środowisku na osobne serwery. Wszystko powinno zostać wykonane w oparciu o najlepsze praktyki Microsoft.

Na etapie Projektu Wykonawcy zostanie przedstawiony szczegółowy stan obecnej infrastruktury u Zamawiającego wraz z koniecznymi wyjaśnieniami.

6.2 Wykorzystane oprogramowanie

W Tabela 1 zawarte zostało podsumowanie informacji o oprogramowaniu niezbędnym do realizacji projektu. Oprogramowanie niezbędne do migracja środowiska znajduje się w posiadaniu Zamawiającego.

Tabela 1 Informacja zbiorcza o posiadanym oprogramowaniu

System operacyjny	Oprogramowanie aplikacyjne	Rola w systemie pocztowym	Ilość
Windows 2008 R2 Server 64-bit Standard Edition	Exchange Server 2010 Standard Edition, Forefront TMG Enterprise	TMG + Edge Transport Server, Client Access Server, Hub Transport Server	**4 szt**. (2x TMG +Edge Transport Server, 2x Client Access Server + Hub Transport Server)

Windows 2008 R2 Server 64-bit Enterprise Edition	Exchange Server 2010 Enterprise Edition	Mailbox Server	**2 szt.** (2x MailBox Server)
Windows 2008 R2 Server 64-bit Standard Edition	-	Domain Controler	**3 szt.**
Windows 2008 Server 32-bit Standard Edition	-	Domain Controler	**2 szt.**
Windows 2008 R2 Server 64-bit DataCenter	-	Serwer przeznaczony pod wirtualiazcję i środowisko laboratoryjne	**2 szt.**
Windows 2008 R2 Server 64-bit Standard Edition	SCOM 2007	System monitoringu AD I Exchange	**1 szt.**

7. Architektura organizacji pocztowej

7.1 Serwery transportowe

7.1.1 Połączenia SMTP przychodzące i wychodzące

W organizacji Exchange 2010 połączenia SMTP przychodzące oraz wychodzące będą obsługiwane przez serwery pełniące rolę Edge Transport (zainstalowane wspólnie z TMG). Jest to rola której podstawowym zadaniem jest zapewnienie bezpieczeństwa i higieny poczty elektronicznej. Głównymi zaletami zastosowania serwerów Edge są:

- Skanowanie poczty przychodzącej skanerami antywirusowymi oraz antyspamowymi (wbudowanymi oraz dodatkowymi firm trzecich).
- Przetwarzanie reguł transportowych z uwzględnieniem filtrowania wiadomości oraz ich przetwarzania.
- Dodatkowy punkt zabezpieczenia (serwery poza domeną)

Zainstalowane zostaną dwa serwery Exchange Server 2010 w roli Edge Transport. Oba serwery będą realizowały dwustronną komunikację SMTP z Internetem. Każdy z serwerów zostanie wyposażony w odpowiednie konektory zgodnie z następującymi kryteriami:

- **Konektory odbierające (Internet -> Edge)**- realizujące połączenia SMTP z Internetu zostaną skonfigurowane tak aby akceptowały połączenia anonimowe na standardowym porcie SMTP. Włączona zostanie obsługa protokołu TLS z wykorzystaniem certyfikatu typu wildcard. Każdy serwer Edge będzie posiadał jeden tego typu konektor.
- **Konektory wysyłające (Edge -> Internet)** – realizujące połączenia SMTP wychodzące do internetu zostaną skonfigurowane tak aby wykorzystywały uwierzytelnianie anonimowe i każdorazowo próbowały nawiązać bezpieczne połączenie SMTP z wykorzystaniem TLS. Parametr address space dla tego typu konektorów zostanie ustawiony na * (gwiazdka)
- **Konektory odbierające (Hub -> Edge)** – realizujące połączenia SMTP z wewnątrz organizacji. Dla konektorów tego typu zostaną wprowadzone restrykcje na adresy IP, które mogą nawiązywać

połączenie. Do listy dostępu dodane zostaną wyłącznie adresy IP serwerów Exchange Server 2010 Hub Transport. Wszystkie połączenia z tymi konektorami będą wykorzystywały TLS.

- **Konektory wysyłające (Edge -> Hub)** – służące do wysyłania wiadomości odebranych z Internetu do wewnątrz organizacji Exchange. Konektory te będą wykorzystywały TLS i łączyły się wyłącznie z serwerami HUB.

7.1.2 Exchange Server 2010 Hub Transport

Za realizację usług transportu wiadomości między użytkownikami wewnątrz organizacji Exchange Server 2010 odpowiedzialne są serwery Exchange Server 2010 Hub Transport. Dla zapewnienie nadmiarowości rozwiązania zostaną zainstalowane dwie instancje roli Exchange Server 2010 Hub Transport. Serwery te zostaną wyposażone w odpowiednie konektory, aby zapewnić komunikację ze środowiskiem Exchange 2003 a w konsekwencji z Exchange 5.5 oraz z serwerami Exchange Server 2010 Edge Transport. Komunikacja między serwerami transportowymi Exchange 2010, a więc rolami Hub Transport oraz Edge Transport odbywać będzie w ramach subskrypcji serwerów Edge obsługiwanej przez mechanizm synchronizacji EdgeSync. Mechanizm ten zapewnia synchronizację wybranych informacji zawartych w Active Directory do partycji aplikacyjnej Active Directory (Active Directory Application Mode) dzięki czemu serwery Exchange 2010 Edge Transport, które nie należą do domeny będą mogły weryfikować podczas skanowania AV i AS odbiorców oraz inne niezbędne atrybuty użytkowników organizacji.

7.1.3 Dostęp użytkowników – Client Access Server

Dostęp użytkowników do poczty z Internetu będzie realizowany za pomocą serwerów pełniących rolę Client Access Server (CAS). Zainstalowane zostaną dwa serwery CAS. Wysoka wydajność i nadmiarowość będzie realizowana za pomocą dwuwęzłowego klastra Network Load Balancing. Takie rozwiązanie zapewni równoważenie obciążenia pomiędzy wszystkie serwery CAS oraz spójną przestrzeń nazewniczą, co nie jest bez znaczenia dla wygody pracy użytkowników. W przypadku, gdy jeden z serwerów CAS ulegnie awarii lub zostanie planowo wyłączony ruch dostępowy klientów będzie dynamicznie przełączany na działający serwer. Serwery CAS świadczyć będą następujące usługi:

- **Outlook Web Access** – Dostęp do poczty, kalendarzy, kontaktów z dowolnej przeglądarki na komputerze podłączonym do Internetu. Dostęp ten odbywa się przez bezpieczny protokół SSL.
- **Outlook Anywhere** – Jest to połączenie z programu Outlook 2010, 2007 lub 2003 wykorzystujące tunelowanie protokołu RPC wewnątrz protokołu HTTPS (RPC over HTTPS). Bezpieczeństwo połączenia zapewniane jest przez protokół SSL. Wykorzystanie Outlook Anywhere zapewnia wygodę dla użytkowników gdyż użytkownik niezależnie od tego czy korzysta z poczty podczas pracy w sieci LAN czy też w podróży przez dowolne łącze internetowe, posiada jedną konfigurację programu pocztowego i nie musi nawiązywać połączeń VPN w celu zapewnienia bezpieczeństwa komunikacji.
- **Exchange Active Sync** – Umożliwia bezpieczne połączenie z pocztą dla użytkowników urządzeń mobilnych z systemami Windows Mobile oraz pozostałymi, które obsługują Active Sync.
- **Autodiscover** – usługa umożliwiająca automatyczną konfigurację programu klienckiego MS Outlook
- **POP3S** – nie planuje się
- **IMAP4S** – nie planuje się

Każda z w/w metod dostępu do poczty będzie konfigurowalna per użytkownik tak, że administrator będzie mógł zabronić lub zezwolić na dostęp do poczty z wykorzystaniem wybranych metod. Niezależnie od metody dostępu

do poczty jest ona w pełni bezpieczna i szyfrowana za pomocą certyfikatów protokołu SSL z wykorzystaniem certyfikatów.

8. Architektura punktu dostępowego TMG 2010

8.1 Magazyn dla konfiguracji serwerów Microsoft Threat Management Gateway

Server TGM Enterprise Edition wymaga komponentu, który przechowuje konfigurację wszystkich serwerów TGM w przedsiębiorstwie. Taka architektura umożliwia centralne zarządzanie punktami dostępowymi w organizacji. Magazynem dla konfiguracji serwerów Microsoft Threat Management Gateway jest Active Directory Lightweight Directory Services (AD LDS). Lokalizacja magazynu zależy od wybranej macierzy Array dla TGM i może być skonfigurowany w trybie Standalone Array bądź macierzy zarządzanej poprzez **Enterprise Management Server (EMS).** W pierwszym przypadku jeden z serwerów TGM będących członkami macierzy dedykowany jest jako serwer zarządzający magazynem centralnym. Drugi przypadek zakłada istnienie dodatkowego serwera zarządzającego centralną konfiguracją serwerów TGM.

8.2 Serwery Microsoft Threat Management Gateway

Serwery TGM zostaną dołączone do wspólnej jednostki organizacyjnej, zwanej Array. Oba serwery będą miały adresy w sieci DMZ oraz sieci wewnętrznej. Taka adresacja umożliwi wykorzystanie mechanizmu NLB. Dodatkowo wszystkie serwery będą kierowały ruch na jedną bramę. Usługa NLB gwarantuje równoważenie obciążenia, odporność na uszkodzenia oraz pozwala na prace administracyjne bez wpływu na dostępność usług. Serwery TGM zostaną skonfigurowane poprzez aplikację wspólnej polityki przedsiębiorstwa (Enterprise Policy) oraz wspólnych reguł aplikowanych na poziomie jednostki organizacyjnej (Array). Charakter przepuszczanego ruchu zostanie uzgodniony z Zamawiającym.

8.3 Publikacja Microsoft Exchange

Do publikacji Microsoft Exchange zostanie wykorzystany Server TMG oraz IAG/UAG funkcjonujący w organizacji Ministerstwa Sprawiedliwości.

Bezpieczeństwo komunikacji, pomiędzy klientem, a usługami, będzie zapewnione przez zastosowanie kanałów SSL/TLS pomiędzy klientem a serwerem IAG/UAG/TMG oraz pomiędzy serwerem IAG/UAG/TMG i serwerem Exchange. Niezbędne certyfikaty zostaną przez Wykonawcę wygenerowane i zaimportowane

8.4 Dodatkowa funkcjonalność

Koncepcja zakłada stworzenie ułatwień w zakresie dostępu zdalnego. W tym celu odpowiedni proces nasłuchujący zostanie skonfigurowany tak, aby przekierowywał połączenia HTTP na HTTPS. Ścieżka URL, podawana przez użytkowników jako adres strony, poprzez którą mają dostęp do swojej poczty zostanie zachowana i będzie mogła mieć postać poczta.ms.gov.pl, logowanie za pomocą certyfikatu pocztat.ms.gov.pl lub intranet.ms.gov.pl a logowanie za pomocą OTP pocztao.ms.gov.pl lub intranet.ms.gov.pl

TMG Server zawiera mechanizmy, które umożliwiają uwierzytelnianie użytkowników za pomocą formularzy HTML (tzw. Form-Based Authentication). Dodatkową zaletą wykorzystania uwierzytelniania za pomocą

formularza jest fakt, iż TMG Server umożliwi użytkownikom zmianę hasła po zalogowaniu. W porozumieniu z Zamawiającym Wykonawca nałoży ograniczenia na długość sesji zestawianej ze zdalnych komputerów do usługi OWA, co znacząco powinno podnieść poziom bezpieczeństwa tej usługi.

9. Bezpieczeństwo

W celu podniesienie ogólnego poziomu bezpieczeństwa rekomenduje się wykonanie dodatkowych czynności. Dokładne czynności związane z podniesieniem bezpieczeństwa zostaną wykonane po szczegółowej analizie i zapoznaniu się ze środowiskiem Zamawiającego. Ogólne zagadnienia zostały opisane w niniejszym opracowaniu.

9.1 Hardening serwerów

Na wszystkich systemach przeprowadzony powinien być hardening konfiguracji. Systemy operacyjne i usługi powinny być zabezpieczone z wykorzystaniem zaleceń firmy Microsoft oraz zgodnie z dobrymi praktykami inżynierskimi. Zabezpieczenia systemów pracujących w domenie należy zaimplementować za pomocą polityk GPO. Serwery, które z racji pełnionej funkcji nie będą należały do domeny powinny zostać zabezpieczone wykorzystując narzędzie Security Configuration Wizard. Dodatkowo zaleca się wykonanie skanowania konfiguracji narzędziami Best Practice Analyzer w celu skonfrontowania zastosowanych ustawień z rekomendacjami Microsoft, dla każdej z zainstalowanych i wdrożonych ról posiadających narzędzie BPA.

9.2 Ochrona przed atakami typu DoS i Spoffing i inne zabezpieczenia

Mechanizm ochrony przed atakami typu Spoffing jest wbudowany w serwer TM i opiera się na prawidłowej definicji chronionych grup sieci. Wszystkie chronione sieci zostaną wprowadzone do konfiguracji TMG tak, aby serwery TMG mogły skutecznie chronić przed tego typu atakami.

Mechanizm ochrony przed atakami typu DoS są wbudowane w serwery TGM i zostaną aktywowane w trakcie konfiguracji. Dodatkowo w trakcie zabezpieczenia systemu operacyjnego zostanie dostosowana konfiguracji stosu TCP/IP tak, aby system był bardziej odporny na tego typu ataki.

Mechanizm inspekcji HTTPS jest wbudowany w serwer TMG i pozwala na skanowanie ruchu szyfrowanego poprzez SSL. Jeśli zaistnieje potrzeba zaufane źródła w porozumieniu z Zamawiającym zostaną wykluczone z takiej inspekcji.

Mechanizm Web-Anti-malware wbudowany z serwer TMG pozwala na skanowanie witryn WWW w poszukiwaniu wirusów, oprogramowania malware oraz innych zagrożeń.

9.3 Zabezpieczenia antywirusowe i antyspamowe

Zaleca się zastosowanie ochrony antywirusowej i antyspamowej. Pierwszy poziom ochrony będzie realizowany na poziomie filtru AS w Cisco ASA. Następne realizowane na poziomie serwerów Exchange Server 2010 Edge Transport, które będą skanowały całość poczty przychodzącej i wychodzącej. Ochrona realizowana zostanie poprzez ochronę AV i AS uruchomioną na serwerach Exchange Server 2010 Hub Transport i serwerach Exchange Server 2010 Mailbox poprzez instalację AV pozwalającego na skanowanie baz mailboxowych.

Do realizacji opisanych powyżej zadań wykorzystane zostanie oprogramowania będące w posiadaniu Zamawiającego dedykowane do Exchange. Ostateczny wybór oprogramowanie AV i AS nastąpi po wykonaniu analizy. Zamawiający posiada licencje na odpowiednie oprogramowanie dedykowane do współpracy z Exchange Server 2010.
Zastosowane zostanie oznaczanie wiadomości przeskanowanych. Wiadomości sprawdzone w trakcie transportu np: na serwerach z zainstalowaną rolą Edge Transport nie będą ponownie skanowane na serwerach z zainstalowaną rolą Hub Transport. Natomiast wiadomości przeskanowane na serwerze Hub Transport nie będą sprawdzane na serwerze Edge Transport.
Sugeruje się zaimplementownie polityk antyspamowych na serwerach skanujących (wszystkie warstwy), oraz wprowadzenie zabezpieczenia przed atakami ze znanych sieci wysyłających spam. Proponowane są następujące konfiguracje:

- Zmiana domyślnych ustawień i uprawnień dla SMTP
- Zmiana banerów SMTP
- Wykluczenie sieci z których rozsyłany jest spam

Proponowane jest wprowadzenie znaczenia przesyłanych wiadomości wybranym przez klienta ciągiem znaków w temacie wiadomości. Tylko wiadomości, które jednoznacznie zostaną zdefiniowane jako spam będą blokowane.