OPIS PRZEDMIOTU ZAMÓWIENIA - **PAKIET 1** (sprzęt serwerowy, zintegrowana ochrona antywirusowa, system ochrony i akceleracji aplikacji sieciowych, system ochrony w punkcie styku (UTM), wraz z niezbędnym oprogramowaniem)

„Rozwój e-usług medycznych w Szpitalu Specjalistycznym w Zabrzu Sp. z o.o.”

SZPITAL SPECJALISTYCZNY W ZABRZU SP. Z O.O.
UL. M. SKŁODOWSKIEJ CURIE 10, 41-800 ZABRZE

1. Założenia do realizacji projektu

Bezpośrednim celem realizacji projektu jest rozwój e-usług dostępnych dla pacjentów a także dostarczenie szybkich i zautomatyzowanych procesów pozwalających jednostce efektywniej wypełniać cele związane z ochroną i promocją zdrowia.

Projekt zakłada zakup licencji oprogramowania dla modułów e-usług, dostawy sprzętu i oprogramowania towarzyszącego, adaptacje oraz prace wdrożeniowe, które mają na celu uzyskanie w pełni funkcjonalnego rozwiązania pozwalającego na osiągnięcie zakładanych wskaźników.

2. Opis funkcjonalny planowanego do zakupu sprzętu

Przedstawione poniżej rozwiązania są rozwiązaniami, które należy traktować jako minimalne:

Serwer aplikacji (1szt.)

• Typu Rack, wysokość maksimum 3U wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack;

• Płyta główna wieloprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów min. 28-rdzeniowych; Minimum 24 gniazda pamięci RAM, obsługa minimum 3000GB pamięci RAM 2933 Mhz;

• Musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 1000GB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) – minimum 12 gniazd pamięci RAM musi umożliwiać wymienną instalację tego typu modułów;

• Sprzęt powinien pochodzić z autoryzowanego kanału dystrybucji właściwego dla terytorium Polski lub innego kraju UE.

• Procesor: dedykowany do serwerów, ze sprzętową obsługą wirtualizacji procesora oraz urządzeń wejścia/wyjścia osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 18000 punktów, wynik testu musi być opublikowany na stronie www.cpubenchmark.net. Pobór mocy TDP nie większy niż 135 W.

• Liczba procesorów – minimum 2.

• Minimum 3 złącza PCI Express generacji 3, w tym minimum 2 złącza o prędkości min. x16;

• Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera). Sloty razem z dołączonymi dyskami SSD 240 GB z możliwością spięcia w RAID 1

• Zainstalowane minimum 192 GB pamięci RAM typu Registered, min. 2933Mhz;

• Zainstalowany kontroler min. SAS 3.0 RAID 0,1,5,6,50.

• Zainstalowane minimum 4 dyski SAS SSD 3.0, 12 GB/s, o pojemności minimum 1,92 TB każdy, dyski Hotplug;

• Panel LCD na przodzie umożliwiający wyświetlenie między innymi adresu IP lub błędów

• Port na płycie głównej umożliwiający umieszczenie kart SD do 64 GB

• gwarancja serwera w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD). Gwarancja obejmuje pozostawienie dysków uszkodzonych w przypadku wymiany gwarancyjnej na cały okres serwisu serwera; Dostępność części zamiennych przez min. 5 lat od momentu zakupu serwera; W przypadku naprawy dłuższej niż 1 dzień roboczy gwarancja obejmuje dostarczenie urządzenia zamiennego o parametrach nie gorszych niż wskazane w niniejszej specyfikacji wraz z wykonaniem prac niezbędnych do prawidłowego działania e-usług.

• Wszystkie złącza PCI Express muszą być aktywne;

• Wbudowany moduł min. TPM 2.0;

• Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC lub równoważne;

• Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM;

• Wyposażony w nieulotną pamięć cache (nie dopuszcza się baterii z uwagi na ograniczoną żywotność);

• Minimum 8 wnęk dla dysków twardych Hotplug 2,5;

• Napęd z możliwością odczytu płyt DVD/CD;

• Dodatkowa osobna karta 2x min. 10Gbit/s SFP+;

• Dodatkowa osobna karta 2x min. 1 GBit/s RJ45

• Zintegrowana karta graficzna ze złączem VGA;

• Minimum 1x USB 3.0 i 1x USB dostępne z tyłu serwera;

• Dodatkowe złącze VGA dostępne z przodu serwera;

• Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;

• Redundantne zasilacze hotplug o mocy maksimum 1100W o sprawności min. 94%;

• Redundantne wentylatory hotplug;

• Kable dla zasilaczy C13 o długości min. 4m każdy;

• Minimum dwie wkładki SFP + razem z Patchcordami min. 2m każdy;

• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania/rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca

ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera;

• Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;

- Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;

- Dostęp poprzez przeglądarkę Web (także SSL, SSH)

- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii

- Zarządzanie alarmami (zdarzenia poprzez SNMP)

- Możliwość przejęcia konsoli tekstowej

- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)

- Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych)

- Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 8Gbit/s oferowanych przez producenta serwera)

- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).

• Licencja Vmware ESXi posiadająca API umożliwiające wykonywanie kopii wirtualnych maszyn z poziomu Hypervisora lub równoważna;

Oferowane równoważne rozwiązanie ma pełnić rolę narzędzia pozwalającego na migrację maszyn wirtualnych klientów działających na Vmware ESXi oraz serwerach fizycznych z systemami MS Windows oraz umożliwiać wykonywania za pomocą innego oprogramowania kopii zapasowych maszyn wirtualnych z poziomu Hypervisora.

Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji; Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA;

• Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce;

• Ogólnopolska, telefoniczna linia techniczna (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;

• Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

• W ramach dostawy sprzętu Wykonawca zapewni również:

- Instalację sprzętu w miejscu wskazanym przez Zamawiającego.

- Uruchomienie, przetestowanie i wstępną konfigurację zgodnie z wytycznymi Zamawiającego.

- Szkolenie / instruktaż dla pracowników Zamawiającego z obsługi dostarczonego sprzętu w wymiarze 8h.

Rok produkcji co najmniej 2021

Macierz dyskowa (1szt.)

• Pojemność dyskowa min. 12 kieszeni, obsługujących: 3.5" SATA HDD lub 2.5" SATA HDD lub 2.5" SATA SSD

• Możliwość rozbudowy do 264 dysków poprzez dołożenie jednostek rozszerzających.

• Obudowa 19" 2U przygotowana do pracy w szafie rack. W zestawie szyny do montażu w szafie. Szyny powinny umożliwiać zainstalowanie urządzenia w stelażu szafy o głębokości maksymalnej 89cm.

• Minimum 2 kontrolery pamięci nie mniej niż 8GB na kontroler

• Procesor minimum 2 Core o taktowaniu minimum 2.2 GHz

• Karta sieciowa 4x1GbE Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę Link Aggregation.

• Karata sieciowa 2x10GbE Ethernet SFP+ wspierająca obsługę Link Aggregation. Dopuszcza się rozwiązanie 10GbE poprzez instalację karty PCI.

• Minimum 2 zasilacze Moc zasilacza nie mniejsza niż 580W każdy

• Dyski twarde minimum 6 x 1.92TB SSD SAS Read Intensive 12Gbps 512 2.5” Hot-plug.

• Obsługiwane dyski min.:

- NLSAS 7.2K 3.5” – 4TB, 8TB, 12TB, 12TB SED, 16TB

- NLSAS 7.2K 2.5” – 2TB, 2TB SED

- SAS 10K 2.5” – 1.2TB, 1.8TB, 2.4TB, 2.4TB SED

- SAS 15K 2.5” – 900GB, 900GB SED

- SAS SSD – 480GB, 960GB, 1.92TB, 1.92TB SED, 3.84TB

- SDD and HDD: FIPS-certified SEDs

• Możliwość rozbudowy o dodatkowe półki dyskowe, gdzie łączna pojemność będzie wynosić do minimum 3.1 PB.

• Obsługa minimum 1024 migawek

• Złącza wbudowane

• minimum 2szt USB 3.0

• minimum 2szt PCIe 2.0 x8, umożliwiające obsługę kart sieciowych lub karty rozszerzeń M.2 SATA SSD

• port konsoli RS232

• 2x port rozszerzeń do montażu dodatkowych półek dyskowych.

• Diody LED Zasilanie, Status, Stan każdego dysku, wskaźnik alarmu

• Możliwość pracy w trybie RAID 0, 1, 5, 6, 10 z funkcją rozbudowy i funkcją migracji poziomu RAID, RAID Hot Spare

• Obsługa SSD Cache do stworzenia pamięci „cache read/write” do obsługi wolumenów oraz jednostek LUN.

• Zgodność z systemami operacyjnymi OS min.: Windows 7 i 10, Mac OS X

• Wirtualizacja: VMware VSphere, Citrix, Hyper-V

• Protokoły sieciowe SMB, AFP, NFS, FTP, iSCSI, Telnet, SSH, SNMP, VPN

• Systemy plików:

- Wewnętrzny: Btrfs, ext4

- Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT

• Liczba folderów współdzielonych: min. 512

• Liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: min. 2048

• Możliwość połączenia w klaster high-availability

• Usługi:

- Integracja min. z Windows® AD, LDAP

- Obsługa zaawansowanych uprawnień dla pod folderów, Windows ACL.

- Stacja monitoringu, obsługa kamer ONVIF

- Serwer multimediów

• Bezpieczeństwo / zarządzanie- szyfrowanie wolumenów:

- skanowanie złych sektorów, S.M.A.R.T.,

- szyfrowana replikacja,

- automatyczne blokowanie adresów IP

- powiadomienia przez e-mail

- kopia zapasowa konfiguracji

- kopia na nośnik zewnętrzny,- logi systemowe (użytkownicy, alarmy, błędy, połączenia do plików),

- FTP przez SSL/TLS

- zarządzenie przez przeglądarkę HTTPS

- współpraca z zasilaczami awaryjnymi UPS

- przypisanie usługi sieciowej do konkretnego portu

- interfejs aplikacji www do zarządzania w języku polskim

• Pamięć masowa

- liczba iSCSI Target: min. 64

- liczba jednostek iSCSI LUN: 512

- obsługa klonowania/migawek jednostek iSCSI LUN

• Obudowa 19” W zestawie szyny do montażu w szafie.

• Minimum dwa kontrolery obsługujące technologie ULP (Unified LUN Presentation) oraz działające w trybie Active-Active.

• Minimum 12 zatok na dyski 3,5 cala

• Minimum 2 kontrolery pamięci nie mnie niż 8GB na kontroler

• Połączenie min. 10Gb iSCSI BaseT 8 Port Dual Controller

• Interfejs do zarządzania w HTML5

• Interfejs do zarządzania z odblokowanymi wszystkimi wbudowanymi licencjami

• Obsługa minimum 4 interfejsów FC i min. 4 interfejsów iSCSI

• Opcjonalnie możliwość za pomocą odpowiedniego pluginu zarządzania macierzą przez VMware vCenter

• Obsługa minimum 3-level tiering

• Pełna obsługa szyfrowania dysków oparta na AES-256

• Sprzęt powinien pochodzić z autoryzowanego kanału dystrybucji właściwego dla terytorium Polski lub innego kraju UE.

• gwarancja macierzy w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD). W przypadku naprawy dłuższej niż 1 dzień roboczy gwarancja obejmuje dostarczenie urządzenia zamiennego o parametrach nie gorszych niż wskazane w niniejszej specyfikacji wraz z wykonaniem prac niezbędnych do prawidłowego działania e-usług.

- Gwarancja obejmuje pozostawienie dysków uszkodzonych w przypadku wymiany gwarancyjnej na cały okres serwisu serwera;

- Dostępność części zamiennych przez min. 5 lat od momentu zakupu macierzy;

- Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanej macierzy – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta takowa licencja musi być uwzględniona w konfiguracji;

- Elementy, z których zbudowane są macierze muszą być produktami producenta tych macierzy lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA;

- Macierz musi być fabrycznie nowa i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce;

- Ogólnopolska, telefoniczna linia techniczna (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;

- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu macierzy w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

- Do macierzy dołączony przełącznik zarządzalny min. 10 GB/s RJ45 minimum 16 portowy wraz z okablowaniem umożliwiający połączenie macierzy z dostarczonym serwerem

• W ramach dostawy sprzętu Wykonawca zapewni również:

- Minimum dwie wkładki SFP + razem z Patchcordami min. 2m każdy;

- Minimum jeden przełącznik z minimum 4 portami 10GbE SFP +

- Instalację sprzętu w miejscu wskazanym przez Zamawiającego.

- Uruchomienie, przetestowanie i wstępną konfigurację zgodnie z wytycznymi Zamawiającego.

- Szkolenie / instruktaż dla pracowników Zamawiającego z obsługi dostarczonego sprzętu w wymiarze 8h.

Rok produkcji co najmniej 2021

System operacyjny (2szt.) minimalne wymagania

Windows Server 2022 Standard 64bit 16 Core lub równoważny pozwalający na uruchomienie wymaganych baz danych dla systemu e-usług oraz Zintegrowanej ochrony antywirusowej ze skanerem podatności.

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

- Praca w roli serwera domeny Microsoft Active Directory.
- Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
- Zawarta możliwość uruchomienia roli serwera DNS.
- Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).
- Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
- Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
- Zawarta możliwość uruchomienia roli serwera stron WWW.
- Zawarta możliwość implementacji nieograniczonej licencyjnie liczby maszyn wirtualnych opartych o usługę Hyper-V
- W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych
- W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego, minimalnie przez okres 5 lat bez dodatkowych kosztów, licząc od dnia zawarcia umowy dostawy.
- Oprogramowanie wydane minimum po 2017 roku.
- Warunki licencjonowania systemu operacyjnego muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer.
- Liczba obsługiwanej pamięci RAM minimum 24 TB
- Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego
- System musi posiadać graficzny interfejs użytkownika
- Możliwość definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows 7, 8, 10, 11
- System musi posiadać wbudowaną obsługę zdalnego pulpitu zgodnie z protokołem RDP
- System musi posiadać możliwość instalacji roli umożliwiającej konfigurację serwera aktualizacji dla stacji roboczych z systemami Windows 7, 8, 10, 11
- System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS

• System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny.

Zintegrowana ochrona antywirusowa ze skanerem podatności

• System powinien pochodzić z autoryzowanego kanału dystrybucji właściwego dla terytorium Polski lub innego kraju UE.

Dostarczony system zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych aplikacji instalowanych na systemach Microsoft Windows Server 2012 posiadanych już przez zamawiającego lub nowszych.

• System zarzadzania aplikacjami klienckimi dla stacji roboczych dla systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 8 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit), Windows Server 2016, Windows Server 2008 R2 and Windows Server 2012, 2012 R2, Mac OS X v10.14, OS X v10.13, OS X v10.12, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze.

• System powinien umożliwiać automatyczne aktualizacje oprogramowania zabezpieczającego na aplikacji klienckich oraz musi zapewniać integracje z sieciowymi systemami bezpieczeństwa co najmniej z firewallem i rozwiązaniem typu Sandbox.

• Producent rozwiązania powinien dostarczać system ochrony dla stacji roboczych, który posiada następujące funkcje:

- antywirus,

- web filtering,

- firewall aplikacyjny,

- analiza podatności,

- szyfrowane tunele IPSec VPN oraz SSL VPN,

- mechanizmy uwierzytelniania dwuskładnikowego,

- AntiExploit,

- blokowanie dysków przenośnych typu USB,

- kwarantanna plików przesłanych do Sandbox.

• Konsola zarządzająca powinna umożliwiać konfigurowanie wszystkich funkcji klienckiego systemu zabezpieczeń. W szczególności wymagane jest, aby system zapewniał:

• integrację z systemami zarządzania tożsamością użytkowników AD,

• definiowanie różnych profil ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,

• zautomatyzowany proces zarządzania aplikacja kliencką,

• przygotowywanie paczek instalacyjnych w których administrator może określić komponenty dla ochrony stacji roboczych,

• możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,

• panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,

• patchowanie wykrytych podatności na stacjach roboczych,

• automatyczne wykrywanie stacji klienckich w grupach roboczych,

• logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora,

• generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C,

• definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego,

• zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN,

• automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji,

• możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi,

• możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie.

• możliwość tagowania komputerów należących do danych grup AD w celu łatwej weryfikacji źródła danych w systemie raportowania. Urządzenie Firewall musi rozpoznawać tagi i pozwalać na ich wykorzystanie do filtrowania w rejestrze zdarzeń.

• możliwość ustalania reguł dostępu do sieci/kwarantanny w oparciu o uruchomione aplikacje, m.in. oprogramowanie antywirusowe oraz aktualność jego sygnatur.

• Możliwość ustalenia wymaganych zabezpieczeń systemu Windows w oparciu o reguły: program Windows Defender jest włączony, szyfrowanie dysków funkcją Bitlocker jest włączone, funkcja Exploit Guard jest włączona, ochrona aplikacji jest włączona, zapora systemu Windows 10 jest włączona.

• Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działa system a także możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora.

• W ramach projektu wraz z konsolą centralnego zarządzania musi zostać dostarczona licencja na zarządzanie co najmniej 150 aplikacjami klienckimi dla stacji roboczych na okres 60 miesięcy.

Rok produkcji co najmniej 2021

System ochrony i akceleracji aplikacji sieciowych (2szt. HA)

System ochrony, podziału obciążenia dla ruchu przychodzącego i wychodzącego pracujący w warstwach 2,4,7 modelu OSI. Musi umożliwiać przeciwdziałanie atakom typu zero-day oraz zabezpieczać aplikację przed zagrożeniami wyszczególnionymi w OWASP top-10 niezależenie od kodu źródłowego aplikacji sieciowej lub jego ewentualnej aktualizacji lub modyfikacji.

Architektura systemu

• Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby system pracował w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.

• Powinna istnieć możliwość implementacji systemu w trybach: one-arm, reverse proxy, transparent proxy.

• W zakresie sieciowym wymagana jest obsługa IEEE 802.3ad link aggregation.

• Produkt nie powinien posiadać ograniczeń co do ilości obsługiwanych serwerów.

• Powinna istnieć możliwość zdefiniowania co najmniej 2 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.

Wymagane mechanizmy High Availability

• Pływające adresy IP oraz grupy dla Stateful failover. Failover jest anonsowany dla sąsiednich urządzeń sieciowych używając Gratuitous ARP.

• Wbudowane mechanizmy decyzji o failover w oparciu o: System Reboot, Interface monitoring failure, Heartbeat failure, IP monitoring failure.

• Synchronizacja konfiguracji po przeładowaniu urządzenia jak i w czasie pracy.

Parametry fizyczne systemu

• 2 porty Gigabit Ethernet RJ-45.

• Wbudowany port konsoli szeregowej.

• Powierzchnia dyskowa typu SSD - minimum 64 GB.

• Zasilanie z sieci 230V/50Hz.

• Obudowa urządzenia o wysokości do 2 U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Parametry wydajnościowe

• Przepustowość w warstwie 4 - min. 400 Mbps.

• Przepustowość w warstwie 7 - min. 200 Mbps.

• Ilość nowych połączeń SSL w ciągu sekundy - min. 50.

• Przepustowość w zakresie kompresji komunikacji - min. 400 Mbps.

Podstawowe funkcje systemu

• Podział obciążenia (loadbalancing) dla protokołów:

- dns
- ftp
- http
- https
- ip
- mysql
- DIAMETER
- radius
- rdp
- rtmp
- rtsp
- sip
- smtp
- tcp
- tcps
- turbohttp
- udp

• Mechanizmamy podziału obciążenia:

- Round Robin,
- Weighted Round Robin,
- Least Connection,

• Wsparcie dla mechanizmów server persistence:

- Source-IP
- Source-IP Hash
- Source-IP/Port Hash
- Hash Header
- Hash Request
- Persistent Cookie
- Rewrite Cookie

- Insert Cookie

- Hash Cookie

- Embedded Cookie

- RADIUS Attribute

- SSL Session ID

• Weryfikacja stanu pracy serwerów, co najmniej w oparciu o protokoły:

- dns

- ftp

- http

- https

- icmp

- imap4

- l2-detection

- mysql

- DIAMETER

- pop3

- radacct

- radius

- rtsp

- sip

- sip-tcp

- smtp

- snmp

- snmp-custom

• Content routing.

• Funkcja podmiany zawartości - content rewriting.

• Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”.

• Obsługa języków skryptowych, umożliwiających manipulowanie żądaniami i odpowiedziami w transakcjach, z funkcją debugowania działania skryptów.

• Podział obciążenia pomiędzy kilka łączy z funkcjami: health check oraz persistence, przy zastosowaniu metod: weighted round robin, least connections, least connection rate, least

throughput (inbound, outbound, total), spill-over throughput (inbound, outbound, total) oraz source-IP hash

• Wyjściowy multi-homing Link Load Balancing używając funkcji virtual tunnel (enkapsulacja GRE) przy wielu łączach wychodzących.

• Load balancing serwerów pomiędzy różnymi data center.

• Dynamic proximity bazujące na czasie round-trip używając ICMP i TCP.

• Global Load ballancing w oparciu o protokół DNS.

• Obsługa DNSSEC z możliwością definiowania list kontroli dostępu.

Wymagane funkcje w zakresie SSL-offload:

• Obsługa SSL Forward Proxy.

• Bezpieczne dostarczanie aplikacji przy wsparciu szyfrowania SSL.

• Wparcie formatów certyfikatów: .cer, .pem, and .pfx (PKCS12).

• Backup i odtwarzanie certyfikatów oraz kluczy prywatnych na dysk lokalny lub serwer TFTP za pośrednictwem interfejsu GUI.

• Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.

• Możliwość generowania CSR (Certificate Signing Request), self-signed Certificate oraz klucza prywatnego dla okreslonego hosta.

• Możliwość dostosowania komunikatów błędów dla zdarzeń SSL.

• Przepisywanie nagłówka HTTP do HTTPS Host, Request URL, Referer oraz jego manipulację za pomocą skryptów.

• Wsparcie SSL end-to-end, jako SSL Server i/lub jako SSL Client.

• Weryfikacja certyfikatu klienta, CRL (HTTP, FTP, LDAP) przez http, SCEP oraz OSCP.

• Wspierane algorytmy, co najmniej: Elliptic Curve Diffie-Helman, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-RC4-SHA, ECDHE-RSA-DES-CBC3-SHA.

• Wsparcie rozszerzeń TLS SNI w połączeniach: client <-> ADC oraz ADC <-> server.

• Wspiercie wersji SSL/TLS dla serwerów wirtualnych oraz rzeczywistych: SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3.

Wymagane funkcje w zakresie akceleracji aplikacji:

• Optymalizacja wydajności przy użyciu TCP connection multiplexing oraz TCP buffering.

• Obsługa w czasie rzeczywistym tzw. Dynamic Web Content Compression w celu redukcji obciążenia serwerów z opcją wyboru typu kontentu oraz URI.

• Selektywna kompresja dla typów MIME, co najmniej: Text, HTML, XML, Java Scripts, CSS, Custom (images).

• Zaawansowany i wydajny Web cache bazujący na pamięci RAM.

• W zakresie HTTP cache'owanie obiektów statycznych oraz dynamicznych.

• Konfiguracja reguł w oparciu, o które działa cache. Powinny one uwzględniać co najmniej: max object size, TTL objects, refresh time interval.

• Statystyki dostępu do cache bazujące na IP lub http hosts.

• Obsługa Rate shaping oraz QoS dla: źródła, przenaczenia i usług.

Wymagane funkcje w zakresie bezpieczeństwa aplikacji:

• Ochrona przed atakami SYN flood oraz SYN Cookie.

• Stateful firewall dla IPv4 oraz IPv6.

• Funkcje Web Application Firewall z analizą w oparciu o sygnatury ochrony aplikacji web dostarczane przez producenta rozwiązania i aktualizowane zgodnie z harmonogramem.

• Mechanizmy analizy i ochrony dla: XSS/SQL injection, HTTP protocol constraints, URL protection, wykrywanie botów, Analiza XML oraz JSON.

• HTTP authentication.

• Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.

• Wsparcie Geo-IP dla ochrony przed DDoS.

• Limitowanie połączeń w oparciu o polityki.

Zarządzanie

• Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, SNMP v1, v2c, v3.

• Musi dostarczać w GUI informacji o zalogowanych administratorach.

• Możliwość aktualizacji oprogramowania, backupu i odtwarzania konfiguracji z poziomu GUI.

• Wsparcie dla REST API do integracji z innymi produktami.

• System musi posiadać co najmniej dwie partycje, na których przechowywane jest oprogramowania i konfiguracja.

Logowanie i Raportowanie

• System musi zapewniać lokalne logowanie oraz raportowanie.

• Możliwość logowania do wielu zewnętrznych serwerów syslog z możliwością określenia facility.

• Obsługa powiadomień o zdarzeniach systemowych mailem.

• Powiadomienia o zdarzeniach systemowych za pośrednictwem trapów SNMP, w tym co najmniej zużycie: CPU, RAM, Dysku.

Sygnatury, subskrypcje

• Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.

• Powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:

- Sygnatury ochrony dla aplikacji www.

- Bazy reputacyjne adresów IP.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku naprawy dłuższej niż 2 dni robocze gwarancja obejmuje dostarczenie urządzenia zamiennego o parametrach nie gorszych niż wskazane w niniejszej specyfikacji wraz z wykonaniem prac niezbędnych do prawidłowego działania e-usług. W ramach tego serwisu należy zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. System powinien pochodzić z autoryzowanego kanału dystrybucji właściwego dla terytorium Polski lub innego kraju UE.

• W ramach dostawy sprzętu Wykonawca zapewni również:

- Instalację sprzętu w miejscu wskazanym przez Zamawiającego.

- Uruchomienie, przetestowanie i wstępną konfigurację zgodnie z wytycznymi Zamawiającego.

- Szkolenie / instruktaż dla pracowników Zamawiającego z obsługi dostarczonego sprzętu w wymiarze 8h.

Rok produkcji co najmniej 2021

Systemy ochrony w punkcie styku typu UTM (2szt. HA)

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

• Firewall.

• Ochrony w warstwie aplikacji.

• Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

• W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

• Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

• Monitoring stanu realizowanych połączeń VPN.

• System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Parametry fizyczne:

• minimum 10 portów Gigabit Ethernet RJ-45 w tym port DMZ

• wbudowany port konsoli szeregowej

• gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

• co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

• System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

• Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

• Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.

• Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.

• Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.

• Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

Serwisy i licencje

Powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, obejmujące: kontrolę aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku naprawy dłuższej niż 2 dni robocze gwarancja obejmuje dostarczenie urządzenia zamiennego o parametrach nie gorszych niż wskazane w niniejszej specyfikacji wraz z wykonaniem prac niezbędnych do prawidłowego działania e-usług. System powinien pochodzić z autoryzowanego kanału dystrybucji właściwego dla terytorium Polski lub

innego kraju UE. W ramach tego serwisu należy musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

• W ramach dostawy sprzętu Wykonawca zapewni również:

- Instalację sprzętu w miejscu wskazanym przez Zamawiającego.

- Uruchomienie, przetestowanie i wstępną konfigurację zgodnie z wytycznymi Zamawiającego.

- Szkolenie / instruktaż dla pracowników Zamawiającego z obsługi dostarczonego sprzętu w wymiarze 8h.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

• Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

• Kontrola Aplikacji.

• Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

• Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

• Ochrona przed atakami - Intrusion Prevention System.

• Kontrola stron WWW.

• Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

• Zarządzanie pasmem (QoS, Traffic shaping).

• Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

• Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Do urządzenia powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

• Analiza ruchu szyfrowanego protokołem SSL.

• Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

• Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

• System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

• Translację jeden do jeden oraz jeden do wielu.

• Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.

• W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

• Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).

- Microsoft Azure

- Cisco ACI.

- Google Cloud Platform (GCP).

- OpenStack.

- VMware vCenter (ESXi).

Połączenia VPN

System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

• Wsparcie dla IKE v1 oraz v2.

• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

• Mechanizm „Split tunneling” dla połączeń Client-to-Site.

System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

• Pracę w trybie Portal – gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

• Routingu statyczny.

• Policy Based Routing.

• Dynamiczny routing w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

• System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

• Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

• System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

• Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

• System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

• System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

• System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze.

• System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

• System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

• Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

• System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

• Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

• Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

• Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

• Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

• Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

• Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

• Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

• Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

• W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

• Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

• Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

• Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

• Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

• W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

• System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

• Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

• Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

• Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

• Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.

• System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

• System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

• Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

• W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

• Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

• Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Rozwiązanie systemowe musi posiadać certyfikacje:

• ICSA lub EAL4 dla funkcji Firewall.

Wdrożenie rozwiązań ochrony urządzeń

W ramach wdrożenia rozwiązań ochrony urządzeń Wykonawca zobowiązany jest do:

• Opracowania z Zamawiającym szczegółowej koncepcji wdrożenia dostarczanego sprzętu.

• Wykonawca zagwarantuje minimum 80h roboczych na wspólną pracę z Zamawiającym nad docelową koncepcją.

• Zainstalować, uruchomić, przetestować i skonfigurować zgodnie z wytycznymi Zamawiającego wszystkie dostarczone urządzenia i systemy, tj.:

a. Serwer (1szt.)

b. Macierz dyskowa (1szt.)

c. System operacyjny (2szt.)

d. Stacja robocza z monitorem (60szt.)

e. Laptop (11szt.)

f. Zintegrowana ochrona antywirusowa ze skanerem podatności

g. System ochrony i akceleracji aplikacji sieciowych (2szt. HA)

h. Systemy ochrony w punkcie styku typu UTM (2szt. HA)

• Wszystkie prace będą odbywać się w siedzibie Zamawiającego i z udziałem personelu Zamawiającego oraz zgodnie z obowiązującymi praktykami informatycznymi.

• W trakcie wdrożenia rozwiązań ochrony urządzeń Wykonawca będzie świadczył na rzecz Zamawiającego usługi konsultacyjne w zakresie realizowanych prac. Konsultacje będą dostępne dla Zamawiającego w godzinach 8:00 – 16:00 w dni robocze od poniedziałku do piątku zgodnie z zapotrzebowaniem Zamawiającego.

• Wykonawca zagwarantuje minimum 40h roboczych konsultacji dla Zamawiającego.

• Opracowania dokumentacji powdrożeniowej w formacie DOC.

W ramach wdrożenia rozwiązań ochrony urządzeń Wykonawca zobowiązany jest do:

• Świadczenia na rzecz Zamawiającego serwisu infrastruktury krytycznej przez okres 36 miesięcy od daty zakończenia projektu.

• W ramach serwisu infrastruktury krytycznej Wykonawca będzie świadczył usługi wsparcia informatycznego w liczbie 20 godzin miesięcznie.

• Serwis świadczony będzie w godzinach 8:00 – 16:00 w dni robocze od poniedziałku do piątku na miejscu w siedzibie Zamawiającego lub zdalnie.

• Wykonawca zapewni następujące czasy reakcji:

a. 4h robocze dla awarii krytycznej.

b. 8h roboczych dla awarii standardowej

• Wszelkie zgłoszenia przekazane po godzinie 16:00 od poniedziałku do piątku będą traktowane jako przyjęte następnego dnia roboczego, do realizacji od godz. 8:00.

• Wykonawca zapewni dedykowany numer telefonu oraz adres e-mail, na który będą przesyłane zgłoszenia.

Informacje dodatkowe

Każdy z Dostawców i Wykonawców ma obowiązek zapoznać się ze wszystkimi pakietami Zamówienia (dotyczy wzajemnych relacji pomiędzy dostawą sprzętu, infrastruktury i oprogramowania).

Zakres obowiązków Wykonawcy obejmuje również czynności określone w § 3 umowy:

- Wypakowanie i utylizacja opakowań.
- Montaż w miejscu przeznaczenia używania (odpowiednie szafy RACK).
- Podłączenie do istniejącej infrastruktury sieci LAN i zasilania.
- Aktualizacja oprogramowania wewnętrznego.
- Prezentacja zasobów macierzowych do nowych hostów (środowisko wirtualne + systemy bazodanowe).

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji projektu.

W przypadku gdy wykonawca uzna, że dla potrzeb instalacji dostarczonych przez siebie rozwiązań informatycznych, wymagana będzie instalacja środowisk informatycznych lub/i licencji oprogramowania wykraczających poza udostępniane przez Zamawiającego, wykonawca musi dostarczyć we własnym zakresie bez dodatkowego wynagrodzenia wymagane dla dostarczonych rozwiązań: niezbędne środowiska informatyczne, dodatkowe oprogramowanie niezbędne do poprawnego funkcjonowania rozwiązań objętych niniejszym postępowaniem, licencje oprogramowania upoważniające do bezterminowego korzystania z dostarczonego oprogramowania, oraz wszelkie niezbędne komponenty.

Ilekroć mowa o integracji z posiadanym przez zamawiającego systemem HIS, wszędzie, gdzie to wymagane, Wykonawca zobowiązany będzie dostarczyć właściwe licencje integracyjne upoważniające do bezterminowego korzystania z dostarczonego oprogramowania.

Wytyczne do analizy przedwdrożeniowej

Wykonawca jest zobowiązany do przygotowania i dostarczenia w wyznaczonym przez Zamawiającego terminie analizy przedwdrożeniowej.

Analiza przedwdrożeniowa ma na celu opisać sposób wdrożenia wymaganych przez OPZ funkcjonalności tak aby spełniały one swoje funkcje (ujęte z punktu widzenia personelu medycznego Zamawiającego). Funkcjonalności ZSI mogą realizować te funkcje bezpośrednio lub pośrednio (wówczas należy wskazać sposób ich realizacji tzn., poprzez lub w ramach jakich funkcjonalności są one realizowane). Analiza przedwdrożeniowa musi obejmować również analizę integracji poszczególnych systemów Zamawiającego oraz sposób i terminy migracji danych z uwzględnieniem przewidywanych przerw w pracy poszczególnych systemów, tak aby Zamawiający mógł przygotować się do tych przerw i odpowiednio zaplanować pracę Szpitala w trakcie tych przerw. Wykonawca winien wskazać nie tylko konieczność zaplanowania przerwy, ale także określić szacowany termin i szacowany czas trwania przerwy.