# Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa sprzętu teleinformatycznego na potrzeby Zarządu Transportu Miejskiego w Poznaniu.

1. **Informacje ogólne dotyczące przedmiotu zamówienia:**

### Przedmiot zamówienia został podzielony na 3 Części (tj. zadania), których zakres przedmiotowy opisano poniżej. Zamawiający dopuszcza możliwość składania ofert częściowych, Wykonawca może złożyć tylko jedną ofertę na dowolną liczbę Części. Zamawiający nie wyraża zgody na złożenie oferty obejmującej jedynie wybrane pozycje w ramach jednej Części.

### Część 1 – sprzęt serwerowy

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis** | **Ilość** |
|  | Serwer | 2 serwery |

### Część 2 – sprzęt zabezpieczenia sieci

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis** | **Ilość** |
|  | Zapora ogniowa | 1 sztuka |

### Część 3 – sprzęt teleinformatyczny sieciowy

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis** | **Ilość** |
|  | Przełącznik sieciowy SAN | 2 sztuki |

**Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 1:**

**Wymagania technologiczne i funkcjonalne dla oferowanego serwera**

Zamawiający wymaga dostawy dwóch serwerów o identycznej konfiguracji, zgodnie z poniższymi warunkami technicznymi:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis** | **Minimalne wymagania techniczne** |
|  | Obudowa | * Obudowa ze wszystkimi komponentami umożliwiająca montaż w standardowej szafie typu rack. * Wysokość maksymalnie 2U. * Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack. |
|  | Płyta główna | Dwuprocesorowa, z możliwością instalacji procesorów minimum 64-rdzeniowych.  Możliwość instalacji minimum 8 złącz PCIe minimum 4 generacji. Serwer w ramach złącz PCIe musi potrafić obsługiwać minimum 2 karty pojedynczej szerokości GPU dla akceleracji maszyn wirtualnych.  Wbudowany kontroler NIC dwuportowy 1 GbE klasy LOM.  Możliwość integracji dedykowanej, wewnętrznej pamięci typu M.2 przeznaczonej dla systemu wirtualizacji (niezależne od dysków twardych) – musi istnieć możliwość instalacji dwóch pamięci pracujących jako macierz RAID1 (mirror). Pamięć ta musi być zgodna (poziom sterowników i HCL) z oprogramowaniem VMware vSphere 6.5 i nowszym. |
|  | Procesory | Zainstalowane dwa procesory, 16-rdzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECint\_rate2017 minimum 238 pkt (każdy CPU). Każdy procesor musi posiadać minimum 128 MB pamięci cache oraz wspierać pamięci typu DDR4 3200 MHz. Dodatkowo pojedynczy rdzeń procesora w trybie Turbo musi pracować z prędkością co najmniej 3300 MHz. |
|  | Pamięć RAM | Zainstalowane minimum 512 GB pamięci RAM typu DDR4 3200 MHz, klasy RDIMM z możliwością dalszej rozbudowy pamięci o dodatkowe 1536 GB wykorzystując kości o rozmiarze nie większym niż 64 GB RDIMM bez wymiany dostarczonych pamięci.  Wsparcie dla technologii zabezpieczania pamięci Advanced ECC.  32 gniazda pamięci RAM na płycie głównej, obsługa minimum 2TB pamięci RAM typu DDR4 dla klasy RDIMM. |
| **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:**  Serwer posiada 640 GB pamięci RAM typu DDR 3200 MHz, klasy RDIMM. |
|  | Dyski twarde | Minimum 4 wnęki dla dysków twardych 3,5 typu hot plug. |
|  | Nośniki dostarczone wraz z serwerem | Dwa dyski twarde talerzowe o pojemności minimum 2 TB, klasy SATA 6Gb/s, typu hot plug pracujące jako Mirror (RAID 1) i przeznaczone na instalację systemu operacyjnego VMware ESXi.  Realizacja trybu RAID 1 musi być wykonywana przez wbudowany w płytę główną sprzętowy kontroler RAID obsługujący następujące tryby RAID 0/1/10 z prędkością 12 Gbps.  Pozostałe wnęki wypełnione wyjmowanymi zaślepkami. |
|  | Kontrolery LAN | Minimum 2 porty 10GbE-T. Karta typu mezz. Zainstalowana bezpośrednio w płytę główną serwera. Musi wspierać funkcje wirtualizacji karty oraz SR-IOV. W pełni kompatybilna z systemem VMware vSphere 6.5 i nowsze. |
| **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:**  Serwer posiada minimum 2 porty 10Gb Ethernet na wkładki SFP+ (z wkładkami typu SR). |
|  | Kontrolery I/O | Minimum 2 porty typu FC 16 Gbps, z zainstalowanymi wkładkami SWL (multimode), SFP+, klasa marvell. |
|  | Porty | * Zintegrowana karta graficzna, * 1 x min. USB 3.0 zewnętrzne z tyłu obudowy, * 1 x min. USB 2.0 zewnętrzne z przodu obudowy, * 1 x VGA (DB15) zewnętrzne z tyłu.   Zamawiający nie dopuszcza aby zewnętrzne porty były rozszywane za pomocą specjalistycznych, niestandardowych kabli. |
|  | Zasilanie | Zainstalowane dwa redundantne zasilacze hot-plug o mocy minimalnej 1400W każdy (jednak nie większej niż 2400W). |
|  | Zarządzanie | Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 (klasa enterprise), o następujących 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). * Karta zarządzająca musi wspierać monitoring karty RAID (logiczne wolumeny, fizyczne dyski, grupy RAID) jeśli takowa jest zainstalowana w serwerze.   Jeśli wymagane są licencje dla wyżej opisanych funkcjonalności – należy je dostarczyć wraz z serwerem. |
| **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:**  Przekierowanie konsoli graficznej oraz możliwość montowania zdalnych napędów i ich obrazów bez konieczności wykorzystania technologii Java (wtyczki) po stronie przeglądarki internetowej Zamawiającego. |
|  | Wspierane systemy operacyjne | Minimum VMWare ESXi 6.7 – wymagana certyfikacja VMware. Zamawiający posiada odpowiednie licencje VMware – takowe nie muszą być dostarczane razem z serwerem. |
|  | Dodatkowe wyposażenie | Ramka zabezpieczająca chroniąca dyski twarde przed nieuprawnionym wyjęciem z wyświetlaczem LCD.  Zainstalowany układ TPM w wersji 2.0. |
|  | Gwarancja | Minimum 48 miesięcy gwarancji świadczonej przez producenta, bądź partnera serwisowego legitymującego się dokumentami potwierdzającymi posiadanie stosownej autoryzacji, obejmująca serwis sprzętowy oraz wsparcie dla nowych wersji oprogramowania.  Gwarancja liczona jest od daty podpisania bez uwag protokołu zdawczo-odbiorczego dostawy.  Standardowy czas przystąpienia do naprawy – następny dzień roboczy od zgłoszenia awarii (w godzinach pracy Zamawiającego).  Standardowy czas naprawy wynosi 1 dzień roboczy od dnia przystąpienia do naprawy.  Możliwość zgłaszania awarii bez ograniczenia czasowego (tryb 24x7).  Uszkodzone dyski pozostają własnością Zamawiającego przez cały okres gwarancji.  Pozostałe warunki gwarancji i serwisu zgodnie z treścią Umowy. |
| **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:**  **60 miesięcy** gwarancji świadczonej przez producenta, bądź partnera serwisowego legitymującego się dokumentami potwierdzającymi posiadanie stosownej autoryzacji, obejmująca serwis sprzętowy oraz wsparcie dla nowych wersji oprogramowania. |

**Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 2:**

**Wymagania technologiczne i funkcjonalne dla oferowanej zapory ogniowej Fortinet lub równoważny**

Zapora ogniowa firmy Fortinet, model FG-200E zgodny z numerem producenta **FG-200E-BDL-950-36** lub równoważny produkt spełniający poniższe warunki (dalej jako system):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis** | **Minimalne wymagania techniczne** |
|  | Wymagania ogólnie | Dostarczony system musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia.  W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów:   * routera z funkcją NAT, * transparentnym, * monitorowania na porcie SPAN.   W ramach dostarczonego systemu musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:   * rutingu, * firewalla, * IPSec VPN, * antywirus, * IPS, * kontroli aplikacji.   Powinna istnieć możliwość dedykowania co najmniej 10 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.  System musi umożliwiać zbudowanie systemu w postaci redundantnej.  Monitoring oraz 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. |
|  | Interfejsy i zasilanie | System musi dysponować minimum:   * 18 portami Gigabit Ethernet RJ-45. * 4 gniazdami SFP 1 Gbps.   System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo  USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  W ramach systemu powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.  System musi być wyposażony w zasilanie AC zgodnie ze standardem używanym w Polsce. |
|  | Parametry wydajnościowe | W zakresie Firewall’a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę.  Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B.  Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B.  Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.  Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 7.2 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 2.2 Gbps.  Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.  Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 820 Mbps. |
|  | Funkcje systemu bezpieczeństwa | W ramach dostarczonego 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, IMAP. * Zarządzanie pasmem (QoS, Traffic shaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego 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. |
|  | 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). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * 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. |
|  | Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.   System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
|  | Zarządzanie pasmem | System 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. |
|  | Kontrola antywirusowa | 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). |
|  | 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.  Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  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 2100 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 na przykład wysyłanie czy pobieranie 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 stron WWW | Moduł kontroli stron 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.  System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.  Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
|  | Uwierzytelnianie użytkowników w ramach sesji | System 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 dwu-składnikowego.  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 dwu-składnikowego 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 | Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  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 | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. * ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW. * ICSA dla funkcji IPSec VPN. * ICSA dla funkcji SSL VPN. |
|  | Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować na okres 36 miesięcy:   * kontrola aplikacji, * IPS, * antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), * analiza typu Sandbox, * antyspam, * filtrowanie stron WWW (web filtering), * bazy reputacyjne adresów IP/domen. |
|  | Warunki gwarancji | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie zgłoszonych usterek i awarii lub wymianie urządzenia w przypadku jego wadliwości, która uniemożliwia naprawę.  W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania. Wsparcie techniczne w trybie 8x5 (8 godzin x 5 dni w tygodniu). |
| **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:**  System jest objęty serwisem gwarancyjnym producenta przez okres **60 miesięcy**, polegającym na naprawie zgłoszonych usterek i awarii lub wymianie urządzenia w przypadku jego wadliwości, która uniemożliwia naprawę. W ramach tego serwisu producent zapewnia również dostęp do aktualizacji oprogramowania. Wsparcie techniczne w trybie 8x5 (8 godzin x 5 dni w tygodniu). |

**Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 3:**

**Wymagania technologiczne i funkcjonalne dla oferowanego przełącznika sieciowego SAN lub produkt równoważny**

Przełącznik sieciowy SAN firmy Brocade, model zgodny z numerem producenta **BR-G610-8-16G** wraz z dodatkowym pakietem 8 wkładek 16G typu SWL SFP+, zgodny z numerem producenta **X-SMED8PTPOD-16G.** Urządzenie zarządzalne 24-portowe posiadające optyczne porty FC, które mogą pracować z prędkością 32Gbps z użyciem właściwych wkładek SFP+.

Oferowany przełącznik musi mieć zainstalowane 16 wkładek typu SWL SFP+ pracujące z prędkością 16Gbps, wszystkie porty aktywne i gotowe do pracy jako zarządzalny przełącznik SAN dla 16 niezależnych hostów. Urządzenie musi mieć zainstalowaną właściwą licencję na korzystanie ze wszystkich 16 portów z wkładkami jednocześnie.

Oferowany przełącznik sieciowy musi pochodzić z oficjalnej dystrybucji producenta tego przełącznika na terytorium Polski w celu spełnienia warunków gwarancyjnych Producenta oraz objęty minimum 36-miesięczną Gwarancję Producenta.

**FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:**

Oferowany przełącznik jest objęty 60-miesięczną Gwarancję Producenta.

1. **Wymagania Zamawiającego dotyczące przedmiotu zamówienia:**

Zamawiający wymaga, aby dostarczony sprzęt był fabrycznie nowy, w oryginalnych, nieotwieranych opakowaniach oraz musi pochodzić z oficjalnej dystrybucji na terytorium Rzeczpospolitej Polski. Zamawiający nie dopuszcza dostarczenia produktów w nieoryginalnych opakowaniach, produktów tzw. „refurbished”, produktów nieposiadających ważnej gwarancji bez możliwości weryfikacji na stronie producenta produktu.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Wykonawca przekaże Zamawiającemu spis dostarczanego sprzętu wraz z numerami seryjnymi w formie papierowej i elektronicznej. Każdy z zamawianych elementów musi posiadać swój unikalny numer seryjny.