

Pionki dn. 18.01.2021 r.

IR.271.12.2020

Wykonawcy
uczestniczący w postępowaniu
o udzielenie zamówienia

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na zakup licencji, wdrożenie i uruchomienie e-usług oraz zakup sprzętu komputerowego i szkolenia w ramach projektu pn.: „E-usługi dla mieszkańców Miasta Pionki”.

Wyjaśnienie i zmiana Treści Specyfikacji Istotnych Warunków Zamówienia

Zamawiający, tj. Gmina Miasto Pionki, działając na podstawie art. 38 ust. 1 i 4 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (tj. Dz.U. z 2019r. poz. 1843 z późn. zmianami), w wyniku otrzymanych pytań i wniosków, udziela następujących wyjaśnień i wprowadza zmiany dotyczące treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ):

Pytanie nr 1

W zakresie liczby urządzeń rejestrujących wejście/wyjścia dziecka. Czy w tabeli kolumna „ilość czytników do ewidencji dzieci” to liczba urządzeń jakie mają zostać dostarczone w zamówieniu?

Odpowiedź nr 1

Tak w kolumnie „Ilość czytników do ewidencji dzieci” znajduje się informacja o liczbie urządzeń, które należy dostarczyć w przypadku gdy system zaoferowany przez Wykonawcę wymaga urządzeń do monitorowania wejść/wyjść przy wejściu/wyjściu do/z placówki np. czytnik kart itp. W przypadku zastosowania innego rozwiązania np. nauczyciel zaznacza moment wejścia/wyjścia dziecka do/z sali dostarczenie tego typu urządzeń nie będzie konieczne.

Pytanie nr 2

W zakresie dostawy i wdrożenia systemu. Czy przedmiotem wdrożenia jest dostawa i wdrożenie zupełnie nowego systemu do E-ewidencja pobytu dziecka w przedszkolu/żłobku, czy aktualizacja istniejącego rozwiązania Stoperek?

Odpowiedź nr 2

Zamawiający dopuszcza uruchomienie i wdrożenie nowego systemu jak i aktualizację i wdrożenie obecnie używanego systemu.

Pytanie nr 3

Czy w poszczególnych oddziałach przedszkolnych nauczyciele dysponują urządzeniami niezbędnymi do wprowadzania np. ogłoszeń czy wiadomości dla rodziców? Jeżeli tak to czy w każdej grupie jest takie urządzenie?

Odpowiedź nr 3

Tak nauczyciele dysponują urządzeniami do wprowadzania ogłoszeń i informacji dla rodziców. Urządzenie jest dostępne w każdej grupie.

Pytanie nr 4

Czy zamawiający zgodzi się na zmianę zapisu „THD<2% dla obciążenia liniowego” na „THD<3% dla obciążenia liniowego” dla urządzeń UPS typ I typ II?

Odpowiedź nr 4

Tak dopuści.

Pytanie nr 5

Czy Zamawiający dopuści aby funkcja WOL (Wake-on-LAN) była dostępna tylko na portach 1 Gb/s dla „Urządzenie do archiwizacji”?

Odpowiedź nr 5

Tak dopuści.

W udzielonych wyjaśnieniach i wprowadzonych zmianach dotyczących treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ) z dnia 13.01.2021r. w pytaniach nr 34, 43 i 44 brakowało pytań do udzielonych odpowiedzi. Z tego powodu Zamawiający jeszcze raz odpowiada na te pytania, razem z zadanymi pytaniami:

Pytanie nr 34

Komputer przenośny typ II – 1 szt.

Czy Zamawiający dopuści nowsze rozwiązanie ze 1 złączem DisplayPort zamiast starego złącza HDMI oraz VGA lub dopuści adapter VGA?

Uzasadnienie pytania: od kilku lat nie ma laptopów 13.3” ze złączem VGA i w przypadku odmowy wnosimy o podanie min 2 różnych produktów spełniających zapis : „ nowy laptop 13,3” i wbudowane złącze VGA”.

Odpowiedź na pytanie nr 34

Zamawiający dopuszcza laptopa z wbudowanym portem HDMI oraz dołączonym adapterem umożliwiającym osiągnięcie portu VGA. Jednocześnie zamawiający dopuszcza zamiast portu HDMI, DisplayPort. Zapis otrzymuje brzmienie:

„Rodzaje wejść/wyjść: VGA (D-sub) (może być adapter) lub HDMI lub DisplayPort - 1 szt.”

Pytanie nr 43

Dotyczy: Część 1 - Switch typ II (10 Gb)

Opisany produkt jest produktem już aktualnie nie produkowanym oraz starej generacji prosimy o dopuszczenie urządzenia o specyfikacji:

Wymagane minimalne parametry techniczne	
1.	Przełącznik FC musi być wykonany w technologii FC 32 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8, 4 Gb/s z funkcją autonegocjacji prędkości.
2.	Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla 8 portów FC przełącznika.
3.	Przełącznik musi być dostarczony wraz z minimum 8 modułami SFP+ FC 16 Gb/s.
4.	Rodzaj obsługiwanych portów: D_Port (ClearLink Diagnostic Port), E_Port, F_Port, AE_Port,
5.	Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.
6.	Przełącznik FC musi posiadać wentylator.
7.	Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
8.	Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach.
9.	Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów.
10.	Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i

	na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
11.	Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, Konta użytkowników definiowane w środowisku RADIUS lub LDAP Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS Obsługa SNMP v3
12.	Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
13.	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC
14.	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)
15.	Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP
16.	Przełącznik musi posiadać wbudowany zasilacz. Maksymalny dopuszczalny pobór mocy przełącznika obsadzonego w 24 porty FC to 77W.
17.	Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.
18.	Przełącznik FC musi zapewniać sprzętową obsługę zoniingu na podstawie portów i adresów WWN
19.	Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP).
20.	Opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 900ns.
21.	Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.
22.	Szyby do montażu w szafie rack.
23.	Min. 36 miesięczna gwarancja (lub dłużej zgodnie ze złożoną ofertą) realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.

Odpowiedź na pytanie nr 43

Zamawiający nie wyraża zgody na zaproponowane przez Wykonawcę parametry. Wykonawca wszedł w rolę Zamawiającego i pod pozorem niedostępności sprzętu próbuje narzucić Zamawiającemu swoją specyfikację sprzętu i tym samym ograniczyć konkurencję.

Pytanie nr 44

Dotyczy: Część 1 - 2.3.7 Router UTM

Zamieszczony opis wskazuje na rozwiązania producentów, które są już wycofane z produkcji. Prosimy o dopuszczenie urządzenia o specyfikacji:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 10 interfejsami miedzianymi Ethernet 10/100/1000.
- Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1 Q.
- W zakresie Firewall'a obsługa nie mniej niż 500 tys jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę.

- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 200 GB do celów logowania i raportowania.
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System musi zostać dostarczony wraz z system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
 - Kontrola dostępu - zaporą ogniową klasy Stateful Inspection
 - Ochrona przed wirusami - antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
 - Poufność danych - IPSec VPN oraz SSL VPN
 - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
 - Kontrola stron Internetowych - Web Filter [WF]
 - Kontrola zawartości poczty - antyspam [AS] (dla protokołów SMTP, POP3)
 - Kontrola pasma oraz ruchu [QoS i Traffic shaping]
 - Kontrola aplikacji oraz rozpoznawanie ruchu P2P
 - Analiza ruchu szyfrowanego protokołem SSL
- Wydajność systemu Firewall min. 5 Gbps
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 800 Mbps
- Wydajność ochrony przed atakami (IPS) min 1.7 Gbps
- Wydajność VPN IPSec, nie mniej niż 1 Gbps
- W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
 - Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
 - Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
 - Praca w topologii Hub and Spoke oraz Mesh
 - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth
 - Obsługa ssl vpn w trybach portal oraz tunel
- Rozwiązanie musi zapewniać obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
- Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
- Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
- Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Baza filtra WWW pogrupowana w minimum 50 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
- Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
- System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
 - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
 - Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny

- W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
 - Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
 - Generowanie co najmniej 25 różnych typów raportów
- System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania
- System musi:
 - posiadać certyfikat Common Criteria EAL4+
 - posiadać certyfikat ICASA Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE
- Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Wymaga się, aby dostawa obejmowała również:
 - Minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
 - Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.

Odpowiedź na pytanie nr 44

Zamawiający nie wyraża zgody na zaproponowane przez Wykonawcę parametry. Wykonawca wszedł w rolę Zamawiającego i pod pozorem niedostępności sprzętu próbuje narzucić Zamawiającemu swoją specyfikację sprzętu i tym samym ograniczyć konkurencję.

W udzielonych wyjaśnieniach i wprowadzonych zmianach dotyczących treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ) z dnia 13.01.2021r. w pytaniach nr 32, 47 i 51 Zamawiający postanowił zmienić udzielone odpowiedzi. Z tego powodu Zamawiający jeszcze raz odpowiada na te pytania, razem z zadanymi pytaniami i zmienionymi odpowiedziami:

Pytanie nr 32

Komputer przenośny typ I – 2 szt.

Czy Zamawiający dopuści nowsze rozwiązanie ze złączem DisplayPort zamiast starego złącza HDMI lub VGA?

Zmieniona odpowiedź na pytanie nr 32

Zamawiający zmienia zapis na następujący: VGA (D-sub – może być adapter) lub HDMI lub Display Port - 1 szt.

Pytanie nr 47

Dotyczy: Część 2 – 3.4 Komputer przenośny typ II

A. **Zamawiający wymaga:** USB 2.0 - 1 szt. USB 3.0 - 2 szt.

Prosimy o dopuszczenie komputera z 2 portami USB 3.0 oraz jednym portem USB Typu-C.

B. **Zamawiający wymaga:** Rodzaje wejść/wyjść: VGA (D-sub) - 1 szt. HDMI - 1 szt.

Prosimy o dopuszczenie laptopa z wbudowanym portem HDMI oraz dołączonym adapterem umożliwiającym osiągnięcie portu VGA.

Zmieniona odpowiedź na pytanie nr 47

Ad A. Zamawiający dopuszcza komputer 2 portami USB 3.0 oraz jednym portem USB Typu-C.

Ad B. Zamawiający dopuszcza laptopa z wbudowanym portem HDMI oraz dołączonym adapterem umożliwiającym osiągnięcie portu VGA. Jednocześnie zamawiający dopuszcza zamiast portu HDMI, DisplayPort. Zapis otrzymuje brzmienie:

„Rodzaje wejść/wyjść: VGA (D-sub) (może być adapter) lub HDMI lub DisplayPort - 1 szt.”

Pytanie nr 51

Prosimy o wyjaśnienie regulacji dot. kar umownych w par. 10 ust. 2 pkt b) i c) bowiem w obu sytuacjach zamawiający uprawniony jest do naliczenia kar za opóźnienie w usunięciu wad na etapie gwarancji?

Prosimy o doprecyzowanie zapisów w tym zakresie tak aby było to jednoznaczne oraz możliwe do skalkulowania oferty ryzyko po stronie wykonawcy, wynikające z możliwości naliczenia kar przez Zamawiającego.

Zmieniona odpowiedź na pytanie nr 51

Zamawiający doprecyzowuje przywołane powyżej zapisy w związku z powyższym §10 ust. 2 lit. b) i c) otrzymują brzmienie:

„b) 0,2% kwoty wynagrodzenia brutto za realizację tego etapu w razie niewykonania, nienależytego wykonania lub zwłoki w usuwaniu wad i usterek zgłoszonych przez Zamawiającego, dotyczy usługi usunięcia Błędów oraz Awarii zaliczanych do Kategorii A, za każdy dzień zwłoki, licząc od następnego dnia po upływie terminu określonego dla wykonania tego obowiązku,

c) za zwłokę w usunięciu wad stwierdzonych przy odbiorze oraz w okresie gwarancji i rękojmi innych niż opisane w lit. b) – w wysokości 0,05% wynagrodzenia umownego brutto określonego § 7 ust. 1 za każdy dzień zwłoki,”

W związku z wprowadzonymi wyjaśnieniami i zmianami SIWZ termin składania ofert zostaje przesłuszony do dnia 03.02.2021 r. do godziny 10.00. Otwarcie ofert nastąpi 03.02.2021 r. o godzinie 12.00.

Proszę o uwzględnienie powyższych wyjaśnień i zmian w przygotowaniu ofert.

(-) *Burmistrz Miasta Pionki*

BURMISTRZ



Robert Kowalczyk