Załącznik 6.4. do SIWZ

SP.ZP.272.49.2018.II.FR

Opis Przedmiotu Zamówienia

Zadanie 4 – Dostawa i wdrożenie infrastruktury sieciowej – aktywnej i pasywnej dla Gminy Mietków

Zamówienie realizowane w ramach projektu pn**.** „Zwiększenie dostępności i jakości elektronicznych usług publicznych dla mieszkańców i podmiotów gospodarczych Powiatu Wrocławskiego oraz 8 Gmin: Czernicy, Długołęki, Jordanowa Śląskiego, Kątów Wrocławskich, Kobierzyc, Mietkowa, Siechnic i Żórawiny”. współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020; Oś Priorytetowa 2 Technologie Informacyjno - Komunikacyjne; Działanie 2.1 E-usługi publiczne, Poddziałanie 2.1.1 E-usługi publiczne – konkurs horyzontalny.

1. **Zestawienie zbiorcze sprzętu - Dostawa infrastruktury sieciowej – aktywnej i pasywnej**

Dostawa infrastruktury sieciowej – aktywnej i pasywnej		**Gmina Mietków**
L.p.	**Rodzaj sprzętu**	**Ilość sztuk**
1.	Switch zarządzalny	1
2.	Firewall	1

2. **Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia**

W zakresie realizacji niniejszych wymagań OPZ przewiduje się:

- Dostawę, instalację, konfigurację i uruchomienie zgodnie ze wskazaniem Zamawiającego urządzeń wymienionych w poz. 1 i 2 powyższej tabeli.

Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne". Wykonawca, który w ofercie powoła się na zastosowanie urządzeń równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

3. **Wymagania szczegółowe minimalne dla sprzętu ujętego w ramach niniejszego przedmiotu zamówienia**

1.1. Przełącznik sieciowy – switch – 1 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Wszystkie przełączniki powinny pochodzić z oficjalnego kanału dystrybucji producenta w Rzeczypospolitej Polskiej. Przełącznik musi być fabrycznie nowy.

L.P.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne**
1.	Obudowa	Obudowa wieżowa 1U umożliwiająca instalację w szafie 19"
2.	Zarządzanie	Telnet, SNMP v1/v2c/v3, Wiersz poleceń (CLI), Przeglądarka WWW
3.	Wejścia / Wyjścia	- RS-232 - min. 1 szt., - 48 portów GE w standardzie 10/100/1000BaseT - 4 porty 1000BaseX ze stykiem definiowanym przez SFP (niezależne od

		portów miedzianych, nie dopuszcza się tzw. portów Combo) - automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
4.	Obsługiwane standardy	IEEE 802.1 p, IEEE 802.1 x, IEEE 802.1 Q, IEEE 802.1 w, IEEE 802.1 s, IEEE 802.1 d, IEEE 802.3 x,IEEE 802.3 ad
5.	Rozmiar tablicy MAC	minimum 16000
6.	Obsługa VLAN	Tak. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN
7.	Pamięć	128 MB RAM / 32 MB Flash Przełącznik musi posiadać pamięć DUAL-Flash (możliwość uruchomienia z dwóch różnych wersji obrazu)
8.	Przepustowość	Wydajność przełączania co najmniej 104 Gbps oraz przepustowość 77,3 Mpps dla pakietów 64 bajtowych
10.	Materiał obudowy	metalowy
11.	Parametry i funkcje	Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2 i SNMPv3 Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) Obsługa Secure FTP Obsługa 802.3ad Link Aggregation Protocol (LACP) Obsługa Simple Network Time Protocol (SNTP) v4 Obsługa LLDP i LLDP-MED (automatyczna konfiguracja VLAN dla telefonów IP). Obsługa zabezpieczeń adresów MAC na portach Zabezpieczenia przed podszywaniem się pod serwer DHCP, (zdefiniowane na konkretny VLAN lub port(y)), Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting Możliwość autoryzacji użytkowników zgodna z 802.1x Możliwość autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, 2 Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) Obsługa list kontroli dostępu (ACL) Obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP (802.3ad)
11.	Gwarancja	Minimum 3 lata Gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający dostarczenie sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Dodatkowo przez pierwsze 90 dni wymagane jest zapewnienie wsparcia telefonicznego w trybie 24x7.

1.2. Firewall – 1 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowych. Integralność systemu musi być zapewniona także w przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

1. System powinien być zaprojektowany w taki sposób, aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii.

   W tym celu powinien zapewnić, co najmniej:

   1.1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.

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

   1.3. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.

   1.4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.

   1.5. System realizujący funkcję Firewall musi dysponować, co najmniej 10 portami Ethernet 10/100/1000 Base-TX

   1.6. Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. W zakresie Firewall'a obsługa nie mniej niż 1250 tys jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę

   1.7. Przepustowość Firewall'a: nie mniej niż 2,8Gbps (dla pakietów UDP 1518/512/64 bajtów)

   1.8. Wydajność szyfrowania 3DES: nie mniej niż 1750 Mbp

   1.9. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:

      1.9.1. kontrola dostępu - zapora ogniowa klasy Stateful Inspection

      1.9.2. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar

      1.9.3. poufność danych - IPSec VPN oraz SSL VPN

      1.9.4. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]

      1.9.5. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.

      1.9.6. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)

      1.9.7. kontrola pasma oraz ruchu [QoS, Traffic shaping]

      1.9.8. Kontrola aplikacji oraz rozpoznawanie ruchu P2P

      1.9.9. Ochrona przed wyciekiem poufnej informacji (DLP)

   1.10. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 140 Mbps

   1.11. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 1200 Mbps

1.12. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
  1.12.1. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
  1.12.2. Dostawca musi dostarczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem (dostępny dla Systemów Microsoft Windows 7 wzwyż, Systemy Android).
  1.12.3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
  1.12.4. Praca w topologii Hub and Spoke oraz Mesh
  1.12.5. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
  1.12.6. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
1.13. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
1.14. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
1.15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
1.16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
1.17. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
1.18. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
1.19. Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
1.20. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
1.21. Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam, Proxy avoidance). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
1.22. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
1.23. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
  1.23.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
  1.23.2. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
  1.23.3. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
  1.23.4. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.
1.24. Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty ICSA dla funkcjonalności Firewall, IPS, Antywirus

1.25. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Wymaga się, aby dostawa obejmowała również:

- W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 36 miesięcy.
- 36 miesięczny Serwis logistyczny na terenie Polski z dostawą urządzenia zastępczego na drugi dzień roboczy / 8x5xNBD gwarantujący udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy w Następnym Dniu Roboczym.

1.26. Gwarancja oraz wsparcie

1) Gwarancja: Dostarczone elementy systemu powinny być objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.

2) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5.

Oferent winien przedłożyć dokumenty:

- oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
- oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
- certyfikat ISO 9001 podmiotu serwisującego

3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca 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.

4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

2. Wymagania dotyczące gwarancji

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego.

Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie.

Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych innych niż określone w SIWZ. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.