Zapytanie ofertowe

W związku z planowaniem udzielenia zamówienia publicznego, w odniesieniu, do którego nie stosuje się Ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych, Lubuski Oddział Wojewódzki Narodowego Funduszu Zdrowia w Zielonej Górze zwraca się z prośbą o przedstawienie oferty cenowej na: **Urządzenie brzegowe router - UTM**

Zamawiający:

Lubuski Oddział Wojewódzki Narodowego Funduszu Zdrowia
ul. Podgórna 9B
65-057 Zielona Góra

2. **Szczegółowy opis przedmiotu zamówienia:**
Przedmiotem zamówienia jest:
Urządzenie brzegowe router - UTM.

Opis minimalnych parametrów, które muszą spełnić zaoferowane zestawy zawiera **załącznik nr 2**.

Cena winna zawierać: podatek VAT.

3. **Wymagany termin realizacji oraz termin ważności oferty:**

- maksymalnie **60 dni licząc od dnia podpisania umowy,**
- 30 dni od upływu terminu składania ofert.

4. **Kryteria oceny ofert i ich znaczenie:**

Oferty będą oceniane wg kryterium:

a) C – **cena, waga 80 %**:

- liczba punktów będzie wyliczona wg wzoru:
$C = (C_N / C_{OB} \times 100) \times 80\ \%$, gdzie:

C_N - najniższa zaoferowana cena brutto

C_{OB} – cena brutto zaoferowana w ofercie badanej

- ocenie podlega całkowita cena brutto określona w formularzu ofertowym - załącznik nr 1 do zapytania ofertowego;

b) D – **termin dostawy, waga 20%**

Dodatkowe punkty za termin dostawy od dnia podpisania umowy, zostaną przyznane zgodnie z poniższym zestawieniem:

Do 21 dni – 20 punktów

Pomiędzy 22 a 40 dniem – 10 punktów

41 dni lub więcej – 0 punktów

- ocenie podlega termin dostawy w formularzu ofertowym - załącznik nr 1 do zapytania ofertowego;

Minimalny zaoferowany okres gwarancji nie może być krótszy niż 36 miesięcy.

Ogólna liczba punktów przyznana poszczególnym ofertom (L), obliczona zostanie zgodnie ze wzorem:

L = C + D

L – łączna ocena punktowa oferty we wszystkich kryteriach,
C – ocena oferty w kryterium cena,
D – ocena oferty w kryterium: termin dostawy.

Wybrana zostanie oferta, która spełni wszystkie wymogi formalne przez Zamawiającego oraz uzyska największą, sumaryczną ilość punktów (L) z poszczególnych kryteriów.

5. **Dokumenty, jakie Wykonawca winien załączyć do oferty.**
Zamawiający wymaga, aby oferta zawierała następujące dokumenty:
Dokumenty rejestrowe, pełnomocnictwa, uprawnienia do wykonywania określonej działalności, jeżeli ustawy nakładają obowiązek ich posiadania.

6. **Miejsce i termin składania ofert:**

Oferty należy składać w terminie **do dnia 28.05.2021 r. do godz. 16:00** osobiście w siedzibie Zamawiającego: w Zielonej Górze przy ul. Podgórnej 9b, **lub listownie** (liczy się data wpływu) na adres:
Lubuski Oddział Wojewódzki NFZ
ul. Podgórna 9b
65-057 Zielona Góra
Z dopiskiem: ***Oferta na dostawę 1szt. urządzenia brzegowego routera - UTM – Wydział Informatyki***.
Informacje o formalnościach

Zamawiający zastrzega sobie możliwość unieważnienia prowadzonej procedury wyboru Wykonawcy. W przypadku unieważnienia prowadzonego postępowania stronom nie przysługują żadne roszczenia w stosunku do Zamawiającego.
Niniejsze postępowanie prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach Zamawiającego.

7. Wszelkie pytania dotyczące zamówienia należy kierować na adres:
info@nfz-zielonagora.pl, lub telefonicznie: 68 3287 788 lub 68 3287 688.

Załączniki:

1. Formularz oferty cenowej
2. Szczegółowy opis przedmiotu zamówienia
3. Postanowienia umowne
4. Załącznik nr 4 klauzula informacyjna dla oferentów i kontrahentow

Załącznik nr 1

……. ……
(pieczęć Wykonawcy) (miejscowość, data)

Lubuski Oddział Wojewódzki
Narodowego Funduszu Zdrowia
ul. Podgórna 9b
65-057 Zielona Góra

OFERTA CENOWA

Odpowiadając na zapytanie ofertowe dotyczące zamówienia publicznego w odniesieniu, do którego nie stosuje się Ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych na: **dostawę 1 szt. urządzenia FortiGate 100F (lub równoważnego)** - Oferuję wykonanie przedmiotu zamówienia zgodnie z wymogami określonymi w zapytaniu ofertowym, zgodnie z poniższym wykazem:

Lp.	Typ sprzętu	Oferowany zestaw	Ilość szt.	Cena jednostkowa netto	Cena jednostkowa brutto	Wartość netto	Wartość brutto
1	2	3	4	5	6	7=4x5	8=4x6
1.	Urządzenie UTM	Producent…… Nazwa……. Model……..	1				

- oferuję wykonanie i dostarczenie przedmiotu zamówienia za łączną cenę:

Netto: ……. zł,

VAT: …….. zł,

Brutto: ……zł,

słownie ……zł;

W ww. cenie uwzględnione zostały wszystkie niezbędne koszty związane z realizacją zamówienia, zgodnie z opisem przedmiotu zamówienia.

Oferuję realizację przedmiotu zamówienia w terminie ….. dni kalendarzowych, od dnia podpisania umowy. (Termin dostawy stanowi jedno z kryteriów oceny ofert. W przypadku nie uzupełnienia powyższego punktu Zamawiający przyjmie, iż Wykonawca oferuje maksymalny 60-dniowy termin dostawy).

1. Prowadzę działalność gospodarcza na podstawie wpisu do …… numer ……
2. Oświadczam, że w stosunku do mnie: nie otwarto likwidacji, nie ogłoszono upadłości.
3. Oświadczam, iż termin ważności oferty wynosi 30 dni.

4. Udzielam gwarancji na okres ……(min. 36 miesięcy).
5. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na adres:

…….
nr telefonu: ……, nr fax: ……..…e-mail: ……
Załącznikami do niniejszej oferty są:
……..…..
……..…..

…….
(pieczęć i podpis Wykonawcy)

Załącznik nr 2

Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie urządzenia **FortiGate 100F** (lub równoważnego) wraz z usługą 3-letniego wsparcia technicznego w trybie 24x7xNBD oraz szkoleniem dwóch administratorów zamawiającego. W przypadku dostarczenia urządzenia równoważnego musi ono spełniać kryteria równoważności określone w punktach od 1 do 16.

Kryteria równoważności

1. Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa 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 oraz monitorowania na porcie SPAN.
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.

2. Redundancja, monitoring i wykrywanie awarii:
    1. 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.
    2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
    3. Monitoring stanu realizowanych połączeń VPN.
    4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

3. Interfejsy, Dysk, Zasilanie:
    1. System realizujący funkcję Firewall musi dysponować minimum:
        - 16 portami Gigabit Ethernet RJ-45.
        - 8 gniazdami SFP 1 Gbps.
        - 2 gniazdami SFP+ 10 Gbps.
    2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
    3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
    4. System musi być wyposażony w zasilanie AC.

4. Parametry wydajnościowe:
    1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
    2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
    3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
    4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
    5. 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 2.5 Gbps.
    6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

5. 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:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania 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.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

6. Polityki, Firewall:
    1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
    2. 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.
    3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
    4. 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).

7. Połączenia VPN:
    1. 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.
    2. 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.

8. Routing i obsługa łączy WAN:
   1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
      - Routingu statycznego.
      - Policy Based Routingu.
      - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

9. Zarządzanie pasmem:
   1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
   2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
   3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

10. Ochrona przed malware:
    1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
    2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
    3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
    4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
    5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

11. Ochrona przed atakami:
    1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
    2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
    3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
    5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
    6. Mechanizmy ochrony dla aplikacji Webowych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL injecton, trojany, exploity, roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, cookies.
    7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

12. Kontrola aplikacji:
    1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
    2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
    4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
    5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

13. Kontrola WWW:
    1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
    2. 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.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

14. Uwierzytelnianie użytkowników w ramach sesji:
    1. 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.
    2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
    3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

15. Zarządzanie:
    1. 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.
    2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
    3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
    4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
    5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
    6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
    7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

16. Logowanie:
    1. 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.
    2. 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.
    3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
    4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach dostawy powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- Kontrola 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 na okres 36 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Szkolenie

W ramach realizacji przedmiotu zamówienia Wykonawca zapewni dla dwóch pracowników Zamawiającego opłacony voucher ważny 1 rok na certyfikowane autoryzowane szkolenie w języku polskim (np. typu NSE4 - FortiGate I Security). W przypadku szkolenia stacjonarnego, zakwaterowanie, wyżywienie oraz dojazd pokrywa Zamawiający.

Rozszerzone wsparcie serwisowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu **w następnym dniu** od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres **36 miesięcy**.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.
3. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.
4. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
5. Wsparcie techniczne musi obejmować:
    1. dedykowane wsparcie telefoniczne zespołu certyfikowanych inżynierów,
    2. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu,
    3. doradztwo w zakresie konfiguracji,
    4. zdalna pomoc techniczna,
    5. pomoc w zakładaniu zgłoszeń serwisowych u producenta,
    6. pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą),
    7. przygotowanie urządzenia do zdalnej konfiguracji,
    8. zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika,
    9. rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań klienta,
    10. usługa upoważnia do maksymalnie 10 zdalnych zmian w konfiguracji w ciągu roku.
    11. dostęp do usługi świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres),

Oferent winien przedłożyć dokumenty:

1. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
2. Certyfikat ISO 9001 podmiotu serwisującego.