Załącznik nr 1 do SWZ

Znak postępowania PZ.271.22.2023

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

**Urządzenia UTM, przełączniki sieciowe i urządzenia Access Point**

**Dostawa urządzenia klasy UTM – w liczbie 1 sztuka.**

|  |
| --- |
| **Oferowany typ, model, producent: …………………………………………………………………………………………….** |
| **Wymagane minimalne parametry i właściwości** |
| Zamawiający wymaga, aby Wykonawca zaoferował sprzęt wyprodukowany nie wcześniej niż 6 miesięcy przed datą publikacji ogłoszenia o zamówieniu w Dzienniku Urzędowym Unii Europejskiej. |
| **Obudowa:** |
| do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn montażowych, lub półka montażowa. Podać sposób montażu: |
| **Porty:** |
| LAN: min 5 x 1GbE, |
| WAN: min 1x1GbE |
| Obsługa modułów min SFP/SFP+: 1/10GbE, SR, LR, ER (dostarczona min 1 wkładka 10Gbe zgodna z wkładkami dostarczonymi z urządzeniami switch) |
| Port konsolowy: minimum 1xRJ-45 |
| Port USB: minimum 1 port umożliwiający załadowanie konfiguracji dla przełącznika z pamięci flash USB |
| Urządzenie musi umożliwiać pełną rekonfigurację interfejsów wewnętrznych, wspierając m.in.:- Stworzenie wirtualnego switch z interfejsów,- Stworzenie interfejsów typu bridge,- Agregacji interfejsów m.in. za pomocą LACP. |
| **Wydajność urządzenia:** |
| Wymagane przepustowość urządzenia dla: Ruchu NGTP: min 450 MbPs |
| Wymagane przepustowość urządzenia dla ruchu: NGFW: min 800 Mbps, |
| Wymagane przepustowość urządzenia dla ruchu: IPS: min 900 Mbps |
| Wymagane przepustowość urządzenia dla ruchu: Ruchu Firewall: min 1000 Mbps, |
| Urządzenie musi monitorować minimum następujące parametry sieciowe:- Utrata pakietów,- Średnie opóźnienie,- Minimalne opóźnienie,- Maksymalne opóźnienie,- Jitter, |
| **Zarządzanie:** |
| Urządzenie musi posiadać interfejs WWW z poziomu, którego administrator może wykonać wszystkie czynności administracyjne. |
| Interfejs WWW musi umożliwiać zalogowanie się wielu administratorom jednocześnie. |
| Urządzenie musi posiadać możliwość ograniczenia dostępu administracyjnego tylko z konkretnych podsieci |
| Z poziomu interfejsu WWW administrator musi mieć możliwość szybkiego przeglądu stanu urządzenia widząc na panelu głównym minimum następujące informacje:- wersja oprogramowania układowego,- nazwa urządzenia,- adres sprzętowy urządzenia,- czas pracy urządzenia od ostatniego restartu,- status sieci internet,- status sieci wifi (o ile urządzenie jest wyposażone w moduł sieci WiFi),- ostatnio wykryte urządzenia w sieci wraz z alertami,- aktywność sieci zawierającą wykres ilości pakietów i ilości danych przepływających w czasie rzeczywistym przez urządzenie. |
| Jeśli urządzenie posiada moduł sieci bezprzewodowej to musi umożliwiać wyświetlenie aktywnych urządzeń podłączonych do sieci bezprzewodowej, wraz z informacjami o jakości sygnału dla pojedynczych urządzeń. |
| Możliwość wyświetlenia wszystkich aktywnych urządzeń pracujących w sieci, w postaci listy dostępnej |
| Możliwość wydruków wydruk raportów z aktywnością użytkowników |
| Możliwość przeglądu i wyszukiwania logów sieciowych  |
| Urządzenie musi umożliwiać przegląd i wyszukiwanie logów systemowych |
| Możliwość przeglądu i wyszukiwania logów sieciowych  |
| Możliwość przeglądu i wyszukiwanie logów systemowych |
| Możliwość wygenerowania plików diagnostycznych z działania systemu urządzenia |
| Urządzenie musi mieć możliwość na wyświetlenia:- stanu zasobów sprzętowych,- tablicy routingu,- stanu połączenia z usługami chmurowymi, |
| Urządzenie musi posiadać funkcję pozwalającą na zarządzenie urządzeniem z sieci internet, nawet jeśli znajduje się za NATem. Funkcja ta nie może wymagać od administratora uruchomienia tunelu VPN do sieci wewnętrznej. |
| Urządzenie musi posiadać funkcje pozwalające na wykonanie testów działania sieci dostępne bezpośrednio z interfejsu WWW. Wymagane są minimum narzędzia takie jak: - ping, - traceroute, - dns lookup, - tcpdump lub inne rozwiązania pozwalające na uzyskanie informacji jak we wskazanych komenach |
| **Bezpieczeństwo:** |
| Urządzenie musi mieć możliwość pracy zarówno w trybie monitorowania, jak i w trybie online. |
| Urządzenie musi posiadać predefiniowane profile pracy minimum:- Firewalla lub polityka firewall, - Kontroli aplikacji, - URL Filteringu, - IPS. |
| Urządzenie musi umożliwiać ręczne definiowanie reguł działających na:- firewallu, - module kontroli aplikacji, - URL Filteringu, - module IPS, |
| Moduł Firewall |
| Moduł Kontrola aplikacji i URL Filtering |
| Moduł Rozpoznawania użytkowników |
| Moduł QoS |
| Moduł IPS |
| Moduł Anti-Virus |
| Moduł Anti-Bot |
| Moduł Emulacji zagrożeń |
| Moduł Antyspam |
| Moduł VPN Site-to-Site |
| Moduł VPN Client-to-Site |
| Urządzenie musi mieć możliwość monitorowania dostępu do internetu poprzez weryfikacje podanych przez administratora hostów.  |
| Urządzenie musi umożliwiać pełną rekonfigurację interfejsów wewnętrznych, wspierając m.in.:- Stworzenie wirtualnego switch z interfejsów,- Stworzenie interfejsów typu bridge,- Agregacji interfejsów m.in. za pomocą LACP. |  |
| Urządzenie musi mieć możliwość filtrowania urządzeń poprzez filtrowanie adresów MAC. |  |
| Urządzenie musi posiadać mechanizm DNS Proxy. |  |
| Urządzenie musi umożliwiać logowanie każdej sesji zezwolonej lub zablokowanej. |  |
| Urządzenie musi mieć możliwość inspekcji ruchu SSL. |  |
| Urządzenie musi mieć możliwość kategoryzowania stron HTTPS bez inspekcji ruchu SSL. |  |
| Urządzenie musi posiadać w interfejsie WWW listę, w której administrator może znaleźć wszystkie zainfekowane urządzenia w sieci. |  |
| **Inne wymagania:** |
| Urządzenie musi wspierać filtrowanie protokołów VoIP, oraz pozwalać na konfiguracje filtrowania tych urządzeń za pomocą prostego kreatora konfiguracji. |
| Urządzenie musi mieć możliwość integrowania się z usługami katalogowymi, minimum Microsoft Active Directory. |
| Urządzenie musi mieć możliwość synchronizacji czasu poprzez protokół NTP. |
| Urządzenie musi zapewniać możliwość uruchomienia usług serwera NTP dla innych urządzeń |
| Urządzenie musi umożliwiać na stworzenie tuneli VPN typu client-2-site minimum w formie:- dedykowane klienta VPN dostarczanego przez producenta rozwiązania,- mobilnego klient VPN dostarczanego przez producenta rozwiązania,- portalu SSL VPN,- klienta wbudowanego w system Windows, |
| **Warunki środowiskowe:** |
| Przystosowanie do pracy w temperaturze minimum w zakresie 0-35 stopni Celcjusza |
| Przystosowanie do pracy w wilgotności minimum w zakresie 10-90 procent wilgotności |
| **Gwarancja i serwis:** |
| Min. 3 lata gwarancji na miejscu lub w opcji „door-to-door”, z czasem reakcji NextBussinesDay od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez stronę internetową i/lub email oraz telefonicznie w godzinach 8-16.  |
| Ogólny czas naprawy wraz z transportem nie może przekroczyć 30 dni kalendarzowych. Nie później niż następnego dnia po przekroczeniu powyższego terminu (30 dni) wykonawca obowiązany jest dostarczyć nowy sprzęt w miejsce uszkodzonego. |
| Wykonawca zobowiązuje się zapewnić dostęp do najnowszych sterowników i uaktualnień na stronie własnej lub producenta |
| **Licencje i oprogramowanie:** |
| Dostarczone oprogramowanie do zarządzania Urządzeniem oraz wykonywaniem czynności administracyjnych (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |
| W przypadku gdy realizacji funkcjonalności w zakresie ochrony i monitorowania sieci WAN/LAN niezbędne są licencje i/lub subskrypcje dostarczone subskrypcje muszą obejmować co najmniej 3 letni okres od momentu ich aktywacji po instalacji urządzenia u Zamawiającego. |
| **Dostawa sprzętu:** |
| Wykonawca dostarcza sprzęt do siedziby Zamawiającego w oryginalnie zapakowanych i zaplombowanych opakowaniach w ustalonym z Zamawiającym terminie.Urządzenia po dostarczeniu podlegają przeglądowi i ocenie przez Zamawiającego w obecności przedstawiciela Wykonawcy w ustalonym z Zamawiającym terminie.Zgodnie z ustalonym z Zamawiającym harmonogramem Wykonawca:* rozmieszcza i podłącza sprzęt do wskazanych przez zamawiającego źródeł energii oraz punktów dostępowych sieci WAN/LAN znajdujących się w siedzibie Zamawiającego.
* dokonuje uruchomienia, instalacji, konfiguracji oraz aktywacji licencji (o ile jest to wymagane) niezbędnych do osiągnięcia funkcjonalności opisanej w OPZ .
 |
| **Oświadczenia:** |
| **Zamawiający wymaga a Wykonawca oświadcza, że oferowane urządzenia sieciowe spełniają poniższe wymogi i standardy:*** Są wyprodukowane z zachowaniem normy jakościowej ISO 9001 i/lub ISO 14001 lub równoważnych środków zapewnienia jakości;
* Posiadają deklarację zgodności CE;

**Zamawiający wymaga a Wykonawca oświadcza, że w celu dokonania odbioru końcowego przez Zamawiającego Wykonawca złoży następujące dokumenty:*** Certyfikat ISO 9001:2000 producenta lub równoważny dokument zapewnienia jakości dla oferowanego urządzenia i/lub Certyfikat ISO 14001 producenta lub równoważny dokument zapewnienia ochrony środowiska.
 |

**Dostawa przełączników sieciowych – w liczbie 5 sztuk.**

|  |
| --- |
| **Oferowany typ, model, producent: …………………………………………………………………………………………….** |
| **Wymagane minimalne parametry i właściwości** | **Oferujemy produkt o następujących parametrach i właściwościach****(wykonawca wypełnia wpisując „tak” lub „nie” albo oferowane parametry):** |
| Zamawiający wymaga, aby Wykonawca zaoferował sprzęt wyprodukowany nie wcześniej niż 6 miesięcy przed datą publikacji ogłoszenia o zamówieniu w Dzienniku Urzędowym Unii Europejskiej. |
| **Obudowa:** |
| do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn montażowych,  |
| wyposażona w zintegrowany zasilacz |
| **Porty:** |
| minimum 48 porty 10/100/1000Mbps RJ45, (min. 190W POE) |
| minimum 4 porty SFP/SFP+ 1/10GbE  |
| Obsługa modułów SFP: 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX |
| Obsługa modułów SFP+: 10GbE, SR, LR, ER |
| minimum 1 port konsolowy RJ-45  |
| minimum 1 port USB umożliwiający załadowanie konfiguracji dla przełącznika z pamięci flash USB |
| Do każdego przełącznika należy dostarczyć:- 2 wkładki SFP, 2 wkładki SFP+ (dostarczone wkładki musza być kompatybilne z wkładkami z UTM)- 2 x patchcord 10Gbe (min 1m)- 2 x patchcord 1Gbe (min 1m)- 1 x kabel konsolowy |
| **Wydajność przełącznika:** |
| Switch fabric capacity min. 100Gbps |
| Forwarding rate min. 100Mpps |
| Pamięć procesora min. 512MB |
| Pamięć flash min. 128MB |
| Bufor pamięci dla pakietów minimum 1.5MB |
| **Funkcjonalność warstwy II:** |
| Obsługa minimum 512 wirtualnych sieci |
| Wsparcie dla agregacji LACP (802.3ad) |
| Obsługa min 8 grup LACP i 8 portów fizycznych per grupa |
| Obsługa technologii port mirroring oraz remote port mirroring |
| Obsługa funkcjonalnościi Voice vlan oraz Critical voice vlan (dostęp do vlan voice, w przypadku gdy niedostępny jest serwer Radius) |
| Obsługa Multicastów , w tym MLD snooping oraz IGMP Snooping. |
| **Funkcjonalność warstwy III:** |
| Obsługa minimum 256 wpisów routingu statycznego IPv4 |
| Obsługa minimum 256 wpisów routingu dynamicznego IPv4 |
| Obsługa protokołu RIP2 |
| **Inne funkcjonalności:** |
| Obsługa 802.1x z dynamicznym przydziałem list ACL, Mac Based Authentication Bypass oraz Captive Portal  |
| Obsługa list kontroli dostępu opartych o adresy MAC i IP  |
| Obsługa czasowych list kontroli dostępu |
| Obsługa protokołu co najmniej jednego z protokołów (NetFlow, SFlow, IPFIX, NSEL) |
| Obsługa kolejek QoS na portach fizycznych |
| **Zgodność z protokołami:** |
| 802.1AB LLDP, 802.1D Bridging, Spanning Tree, 802.1p Ethernet Priority (User Provisioning and Mapping), 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP, 802.1S Multiple Spanning Tree (MSTP), 802.1v Protocol-based VLANs, 802.1W Rapid Spanning Tree (RSTP), 802.1X Network Access Control, Auto VLAN, 802.2 Logical Link Control, 802.3ab Gigabit Ethernet (1000BASE-T), 802.3ac Frame Extensions for VLAN Tagging,802.3ad Link Aggregation with LACP802.3AX LAG Load Balancing, 802.3az Energy Efficient Ethernet (EEE), 802.3u Fast Ethernet (100BASE-TX) on Management Ports, 802.3x Flow Control, 802.3z Gigabit Ethernet (1000BASE-X),ANSI LLDP-MED (TIA-1057) |
| **Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa:** |
| 1212 Concise MIB Definitions, 1213 MIB-II, 1215 SNMP Traps, 1286 Bridge MIB, 1442 SMIv2, 1451 Manager-toManager MIB, 1492 TACACS+, 1493 Managed Objects for Bridges MIB, 1573 Evolution of Interfaces, 1612 DNS Resolver MIB Extensions, 1643 Ethernet-like MIB, 1757 RMON MIB, 1867 HTML/2.0 Forms with File Upload Extensions, 1901 Community-based SNMPv2, 1907 SNMPv2 MIB, ,2011 IP MIB,2012 TCP MIB , 2013 UDP MIB, 2096 IP Forwarding Table MIB, 2233 Interfaces Group using SMIv2, 2271 SNMP Framework MIB, 2295 Transport Content Negotiation, 2296 Remote Variant Selection, 2346 AES Ciphersuites for TLS, 2576 Coexistence Between NMPv1/v2/v3, 2578 SMIv2 , 2579 Textual Conventions for SMIv2, 2580 Conformance Statements for SMIv2, 2613 RMON MIB, 2618 RADIUS Authentication MIB, 2620 RADIUS Accounting MIB, 2665 Ethernet-like Interfaces MIB, 2674 Extended Bridge MIB, 2737 ENTITY MIB, 2818 HTTP over TLS, 2863 Interfaces MIB, 2865 RADIUS, 2866 RADIUS Accounting, 2868 RADIUS Attributes for Tunnel Prot.,2869 RADIUS Extensions, 3410 Internet Standard Mgmt. Framework, 3411 SNMP Management Framework, 3412 Message Processing and Dispatching, 3413 SNMP Applications, 3414 User-based security model, 3415 View-based control model, 3416 SNMPv2, 3418 SNMP MIB, 3580 802.1X with RADIUS, 3737 Registry of RMOM MIB, 4086 Randomness Requirements , 4113 UDP MIB, 4251 SSHv2 Protocol, 4252 SSHv2 Authentication, 4253 SSHv2 Transport, 4254 SSHv2 Connection Protocol, 4419 SSHv2 Transport Layer Protocol, 4521 LDAP Extensions, 4716 SECSH Public Key File Format, 6101 SSL |
| **Warunki środowiskowe:** |
| Przystosowanie do pracy w temperaturze minimum w zakresie 0-40 stopni Celcjusza |
| Przystosowanie do pracy w wilgotności minimum w zakresie 10-90 procent wilgotności |
| **Gwarancja i serwis:** |
| Min. 5 lata gwarancji na miejscu lub w opcji „door-to-door”, z czasem reakcji NextBussinesDay od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez stronę internetową i/lub email oraz telefonicznie w godzinach 8-16.  |
| Ogólny czas naprawy wraz z transportem nie może przekroczyć 30 dni kalendarzowych. Nie później niż następnego dnia po przekroczeniu powyższego terminu (30 dni) wykonawca obowiązany jest dostarczyć nowy sprzęt w miejsce uszkodzonego. |
| Wykonawca zobowiązuje się zapewnić dostęp do najnowszych sterowników i uaktualnień na stronie producenta sprzętu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu. |
| **Dostawa sprzętu:** |
| Wykonawca dostarcza sprzęt do siedziby Zamawiającego w oryginalnie zapakowanych i zaplombowanych opakowaniach w ustalonym z Zamawiającym terminie.Urządzenia po dostarczeniu podlegają przeglądowi i ocenie przez Zamawiającego w obecności przedstawiciela Wykonawcy w ustalonym z Zamawiającym terminie.Zgodnie z ustalonym z Zamawiającym harmonogramem Wykonawca:* rozmieszcza i podłącza sprzęt do wskazanych przez zamawiającego źródeł energii oraz punktów dostępowych sieci LAN znajdujących się w siedzibie Zamawiającego.
* dokonuje uruchomienia, instalacji, konfiguracji oraz aktywacji licencji (o ile jest to wymagane) niezbędnych do osiągnięcia funkcjonalności opisanej w OPZ .
 |
| **Oświadczenia:** |
| **Zamawiający wymaga a Wykonawca oświadcza, że oferowane urządzenia sieciowe spełniają poniższe wymogi i standardy:*** Są wyprodukowane z zachowaniem normy jakościowej ISO 9001 i/lub ISO 14001 lub równoważnych środków zapewnienia jakości;
* Posiadają deklarację zgodności CE;

**Zamawiający wymaga a Wykonawca oświadcza, że w celu dokonania odbioru końcowego przez Zamawiającego Wykonawca złoży następujące dokumenty:*** Certyfikat ISO 9001:2000 producenta lub równoważny dokument zapewnienia jakości dla oferowanego urządzenia i/lub Certyfikat ISO 14001 producenta lub równoważny dokument zapewnienia ochrony środowiska.
 |

**Dostawa punktów dostępowych (access point) – w liczbie 5 sztuk**

|  |
| --- |
| **Oferowany typ, model, producent: …………………………………………………………………………………………….** |
| **Wymagane minimalne parametry i właściwości** |
| Zamawiający wymaga, aby Wykonawca zaoferował sprzęt wyprodukowany nie wcześniej niż 6 miesięcy przed datą publikacji ogłoszenia o zamówieniu w Dzienniku Urzędowym Unii Europejskiej. |
| **Typ punktu dostępowego:** |
| Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków.  |
| Sposób montażu Acces Point: sufit, ściana |
| Acces Point Wyposażony w moduł radiowy, pracujący w paśmie 2.4GHz b/g/n/ax. |
| Acces Point Wyposażony w moduł radiowy, pracujący w paśmie 5GHz a/n/ac wave 2/ax |
| **SSID:** |
| Punkt dostępowy musi obsługiwać nie mniej niż 2 niezależnych SSID na każdym module radiowym |
| **Współpraca urządzeń:** |
| Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2  |
| **Wymagania sieciowe dla Access Point:** |
| Minimum 1 interfejs 100/1000BaseT z funkcją auto-sensing link oraz MDI/MDX z funkcją PoE/PoE+ ze wsparciem dla standardu 802.3az Energy Efficient Ethernet (EEE) |
| Punkt dostępowy musi posiadać minimum 2 wbudowane anteny pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 4.3 dBi dla 2,4GHz, 5.5 dBi dla 5 GHz |
| Prędkości transmisji: do 400 Mbps dla 802.11n, do 1000 Mbps dla 802.11ac, do 574 Mbps dla 802.11ax (2,4GHz), do 1200 Mbps dla 802.11ax (5GHz) |
| **Zasilanie:** |
| Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE oraz przy pomocy lokalnego zasilacza DC (zasilacz musi być dołączony) |
| **Licencje i oprogramowanie:** |
| Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |
| **Wymagania bezpieczeństwa:** |
| Terminowanie sesji użytkowników sieci bezprzewodowej - na punkcie dostępowym lub kontrolerze (o ile jest to wymagane – należy dostarczyć kontroler) |
| Możliwość wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia |
| Uwierzytelnienie oraz autoryzacja muszą być możliwe przy wykorzystaniu lokalnej bazy danych oraz zewnętrznych serwerach uwierzytelniających (Active Directory, LDAP) |
| Urzędzenie musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+, Radius Server, Microsoft Active Directory, Free Radius. |
| Metody szyfrowania i kontroli połączeń minimum w zakresie: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS |
| Obsługę szyfrowania AES-CCM, TKIP i WEP  |
| Obsługę minimum SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit |
| Typy uwierzytelnienia min : IEEE 802.1X 802.1X i MAC  |
| Możliwość wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia |
| Urządzenie (lub kontroler – dostarczany o ile jest to wymagane do zapewnienia funkcjonalności) musi umożliwiać stworzenie strony dla gości tzw. Captive Portal |
| Urządzenie (lub kontroler – dostarczany o ile jest to wymagane do zapewnienia funkcjonalności) musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji) |
| **Warunki środowiskowe:** |
| Przystosowanie do pracy w temperaturze minimum w zakresie 0-40 stopni Celcjusza |
| Przystosowanie do pracy w wilgotności minimum w zakresie 10-90 procent wilgotności |
| **Gwarancja i serwis:** |
| Min. 5 lata gwarancji na miejscu lub w opcji „door-to-door”, z czasem reakcji w następnym dniu roboczym od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez stronę internetową i/lub email oraz telefonicznie w godzinach 8-16.  |
| Ogólny czas naprawy wraz z transportem nie może przekroczyć 30 dni kalendarzowych. Nie później niż następnego dnia po przekroczeniu powyższego terminu (30 dni) wykonawca obowiązany jest dostarczyć nowy sprzęt w miejsce uszkodzonego. **Na czas naprawy gwarancyjnej wykonawca jest zobowiązany dostarczyć sprzęt zastępczy o równorzędnych parametrach.** |
| Wykonawca zobowiązuje się zapewnić dostęp do najnowszych sterowników i uaktualnień na stronie producenta sprzętu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu. |
| **Dostawa sprzętu:** |
| Wykonawca dostarcza sprzęt do siedziby Zamawiającego w oryginalnie zapakowanych i zaplombowanych opakowaniach w ustalonym z Zamawiającym terminie.Urządzenia po dostarczeniu podlegają przeglądowi i ocenie przez Zamawiającego w obecności przedstawiciela Wykonawcy w ustalonym z Zamawiającym terminie.Zgodnie z ustalonym z Zamawiającym harmonogramem Wykonawca:* instaluje i uruchamia urządzenia i (kontroler – o ile jest wymagany) w szafie rack wskazanej przez Zamawiającego.
* podłącza, konfiguruje oraz uruchamia urządzenia dostępowe i (kontroler – o ile jest wymagany). Rozmieszczenie urządzeń pozostaje w gestii Zamawiającego.
* dokonuje uruchomienia, instalacji, konfiguracji oraz aktywacji licencji (o ile jest to wymagane) niezbędnych do osiągnięcia funkcjonalności opisanej w OPZ .
 |
| **Oświadczenia:** |
| **Zamawiający wymaga a Wykonawca oświadcza, że oferowane urządzenia sieciowe spełniają poniższe wymogi i standardy:*** Są wyprodukowane z zachowaniem normy jakościowej ISO 9001 i/lub ISO 14001 lub równoważnych środków zapewnienia jakości;
* Posiadają deklarację zgodności CE;

**Zamawiający wymaga a Wykonawca oświadcza, że w celu dokonania odbioru końcowego przez Zamawiającego Wykonawca złoży następujące dokumenty:*** Certyfikat ISO 9001:2000 producenta lub równoważny dokument zapewnienia jakości dla oferowanego urządzeni i/lub Certyfikat ISO 14001 producenta lub równoważny dokument zapewnienia ochrony środowiska.
 |