

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup urządzeń do awaryjnego przywracania usług w podmiotach dotkniętych incydentami krytycznymi tzw. „Cyberkaretka”.

1. **Termin realizacji zamówienia:** 60 dni kalendarzowych.
2. **Zamówienie obejmuje:**
 - 2.1. Dostawę urządzeń opisanych szczegółowo w pkt. 3-9
 - 2.2. Zapewnienie gwarancji na dostarczone urządzenia i oprogramowanie opisane w pkt. 10
 - 2.3. Zamówienia podzielone jest na II części:
 - Część I: urządzenia sieciowe
 - Część II: sprzęt komputerowy i serwerowy

Część I: urządzenia sieciowe

3. Urządzenia typu Firewall - 6 sztuk.

- 3.1. Każde z urządzeń to Fortigate FG-400F lub model wyższy (wydajniejszy) lub urządzenia równoważne zapewniające funkcjonalność opisaną niżej w sekcji wymagania dla firewall równoważnego.
- 3.2. Każde z urządzeń musi być dostarczone z kompletem wymaganych licencji oraz możliwe do centralnego zarządzania przez posiadane przez Zamawiającego rozwiązanie FortiAnalyzer lub dostarczone rozwiązanie równoważne.
- 3.3. Każde z urządzeń musi być wyposażone w min:
 - 4 wkładki SFP+ 10GE RJ45,
 - 4 wkładki SFP+ 10GE SR,
 - okablowanie niezbędne do podłączenia urządzeń zewnętrznych,
 - wszelkie niezbędne komponenty potrzebne do zamontowania w szafach RACK (np. organizery) oraz podłączenia do sieci energetycznej,
 - dostarczone elementy tj. urządzenia firewall oraz wkładki SFP powinny być tego samego producenta.
- 3.4. Każde z urządzeń musi:

- spełniać wszystkie wymogi dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie,
- być fabrycznie nowe, kompletne, nieużywane i bez oznak używania, nierefabrykowane i nieregenerowane, nienaprawiane, nie podlegało ponownej obróbce,
- być wolne od jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwość jego prawidłowego użytkowania,
- dopuszczone do obrotu gospodarczego na terytorium Rzeczypospolitej Polskiej,
- być zgodne ze stosowanymi normami technicznymi,
- posiadać certyfikaty dopuszczające do stosowania w Unii Europejskiej,
- pochodzić z oryginalnego kanału dystrybucji Producenta na rynek polski,
- w dniu składania ofert nie może być przeznaczone przez Producenta do wycofania z produkcji lub sprzedaży.

3.5. Całość dostarczonego rozwiązania (sprzęt i oprogramowanie) musi być objęty serwisem gwarancyjnym producenta przez okres 60 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. Szczegóły wymagań dla gwarancji określono w pkt 10.

3.6. Wymagania dla firewall równoważnego:

- Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
- Wydajność każdego z urządzeń (minimalna):
 - Firewall: 70 Gbps, obsługa nie mniej niż 7 mln jednoczesnych sesji oraz 400 tys nowych połączeń na sekundę,
 - IPS: 12 Gbps,
 - NGFW (IPS, Application Control): 10 Gbps,
 - Thread Prevention: 9 Gbps.
- Wydajność szyfrowania VPN IPsec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 50 Gbps.
- System musi wspierać IPv4 oraz IPv6 w zakresie:
 - Firewall
 - Ochrony w warstwie aplikacji.
 - Protokołów routingu dynamicznego
- Tryby pracy

- System realizujący funkcję Firewall musi dawać możliwość pracy w każdym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
- Instancje systemu
 - W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 10 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:
 - Routingu,
 - Firewall'a,
 - IPSec VPN,
 - Antywirus,
 - IPS.Musi istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

- Redundancja

Urządzenia muszą umożliwiać łączenie w klaster Active-Active lub Active-Passive w ramach dostarczanych urządzeń. W obu trybach musi istnieć funkcja synchronizacji sesji firewall. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

- Monitoring

- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
- Monitoring stanu realizowanych połączeń VPN.

- Interfejsy

- System realizujący funkcję Firewall musi dysponować minimum:
 - 8 portami 10GE SFP+
 - 16 gniazdami Gigabit Ethernet RJ-45
- W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

- Dysk

- System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 400 GB.

- Zasilanie

- System musi być wyposażony w zasilanie AC 230V.

- Bezpieczeństwo

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:

- Kontrola dostępu - zaporę ogniową klasy Stateful Inspection,
- 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, np.: pobieranie, wysyłanie plików,
 - baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P,
 - Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur,
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
- Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS:
 - 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,
 - moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń..
- Ochrona przed atakami - Intrusion Prevention System:
 - ochrona przed atakami Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,
 - 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, długości parametrów URL, Cookies,
 - wykrywanie i blokowanie komunikacji C&C do sieci botnet.

- Kontrola stron WWW:
 - moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorii tematyczne,
 - w ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego programowania), phishing, spam, Dynamic DNS, proxy avoidance,
 - filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: hazard, pornografia małoletnich,
 - Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL,
 - system musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzić 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.
- Zarządzanie pasmem (QoS, Traffic shaping).
- Dwuskładnikowe uwierzytelnianie dla Administratorów.
- Analiza ruchu szyfrowanego protokołem SSL.
- Analiza ruchu szyfrowanego protokołem SSH.
- W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- Polityki
 - polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń,
 - możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików,
 - możliwość zbudowania min 10 tys. reguł firewall.
- Translacja

System musi zapewniać translację:

 - adresów NAT: źródłowego i docelowego,
 - translację PAT,
 - translację jeden do jeden oraz jeden do wielu,
 - dedykowany ALG (Application Layer Gateway) dla protokołu SIP.
- 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

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

 - routingu statycznego,
 - Policy Based Routingu,
 - protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
- WAN

System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
- Uwierzytelnianie

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,
- 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 dedykowaną platformą centralnego zarządzania i monitorowania. W ramach dostawy urządzeń należy dostarczyć również dedykowaną platformę centralnego zarządzania umożliwiającą centralne zarządzania politykami bezpieczeństwa na dostarczonych urządzeniach oraz budowanie wspólnej polityki bezpieczeństwa dla dostarczonych urządzeń,
 - komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów,
 - powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego 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,
 - system musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- Przesyłanie logów
 - system musi mieć możliwość logowania do centralnego systemu zarządzania (logowania i raportowania), w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej tego samego producenta,
 - w ramach przesyłania logów system 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 przesyłania logów do serwera SYSLOG.
- Serwisy i licencje

Powinny zostać dostarczone licencje lub subskrypcje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus, Web Filtering na okres 60 miesięcy.

- Wyposażenie

Urządzenie powinno być wyposażone w:

- 4 wkładki SFP+ 10GE RJ45,
- 4 wkładki SFP+ 10GE SR,
- dostarczone elementy tj. urządzenia firewall oraz wkładki SFP powinny być tego samego producenta,
- okablowanie niezbędne do podłączenia urządzeń zewnętrznych,
- wszelkie niezbędne komponenty potrzebne do zamontowania dostarczonych urządzeń w szafach RACK (np. organizery) oraz podłączenia do sieci energetycznej,
- maksymalna wysokość każdego z urządzeń 2U.

- Każde z urządzeń musi

- spełniać wszystkie wymogi dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie,
- być fabrycznie nowe, kompletne, nieużywane i bez oznak używania, nierefabrykowane i nieregenerowane, nienaprawiane, nie podlegało ponownej obróbce,
- być wolne od jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwość jego prawidłowego użytkowania,
- dopuszczone do obrotu gospodarczego na terytorium Rzeczypospolitej Polskiej,
- być zgodne ze stosowanymi normami technicznymi,
- posiadać certyfikaty dopuszczające do stosowania w Unii Europejskiej,
- pochodzić z oryginalnego kanału dystrybucji Producenta na rynek polski,
- w dniu składania ofert nie może być przeznaczone przez Producenta do wycofania z produkcji lub sprzedaży.

- Gwarancja oraz wsparcie:

Całość dostarczonego rozwiązania (sprzęt i oprogramowanie) musi być objęty serwisem gwarancyjnym producenta przez okres 60 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. Szczegóły wymagań dla gwarancji określono w pkt 10.

- Szkolenia:

W przypadku rozwiązania równoważnego Wykonawca przeprowadzi szkolenia dla inżynierów Zamawiającego w następującym zakresie:

- szkolenie muszą zostać przeprowadzone dla 5-ciu pracowników Zamawiającego,
- szkolenia muszą umożliwiać przekazanie wiedzy umożliwiającej samodzielnie przez pracowników Zamawiającego: konfigurowania, zarządzanie, budowanie polityk bezpieczeństwa, zaawansowane funkcje bezpieczeństwa, ochrona przez zaawansowanymi atakami, VPN, zarządzania rolami/uprawnieniami, monitorowania, aktualizowanie oraz diagnozę i rozwiązywanie problemów dla dostarczonego rozwiązania oraz dobre praktyki i utwardzanie konfiguracji,
- szkolenie muszą zostać przeprowadzone przez certyfikowanego trenera producenta ofertowanego rozwiązania,
- szkolenia muszą zostać przeprowadzone w języku polskim,
- szkolenie muszą zostać w formie stacjonarnej w certyfikowany przez producenta ośrodku szkoleniowym na terenie Polski i muszą obejmować zarówno część teoretyczną oraz praktyczną na sprzęcie lub w środowisku symulacyjnym. Zamawiający dopuszcza też przeprowadzenie szkolenia w formie zdalnej,
- czas trwania szkolenia min 8 dni roboczych.

4. Urządzenia typu Switch zarządzalny - 6 sztuk.

łącznie 6 urządzeń: 2 w konfiguracji A oraz 4 w konfiguracji B, każde z urządzeń o wymaganiach opisanych niżej.

4.1. Każde z urządzeń musi:

- spełniać wszystkie wymogi dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie,
- być fabrycznie nowe, kompletne, nieużywane i bez oznak użytkowania, nierefabrykowane i nieregenerowane, nienaprawiane, nie podlegało ponownej obróbce,
- być wolne od jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwość jego prawidłowego użytkowania,
- dopuszczone do obrotu gospodarczego na terytorium Rzeczypospolitej Polskiej,
- być zgodne ze stosowanymi normami technicznymi,
- posiadać certyfikaty dopuszczające do stosowania w Unii Europejskiej,
- pochodzić z oryginalnego kanału dystrybucji Producenta na rynek polski,
- w dniu składania ofert nie może być przeznaczone przez Producenta do wycofania z produkcji lub sprzedaży.

4.2. Gwarancja oraz wsparcie

Całość dostarczonego rozwiązania (sprzęt i oprogramowanie) musi być objęty serwisem gwarancyjnym producenta przez okres 60 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. Szczegóły wymagań dla gwarancji określono w pkt 10.

4.3. Przełącznik w konfiguracji A (2 sztuki) posiada:

- 48 portów 100Mb/1GBaseT,
- 4 porty SFP+ 1/10/25 Gbps,
- 2 porty definiowane za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps.
- Parametry wydajnościowe:
 - Prędkość przełączania „wirespeed” dla każdego portu przełącznika,
 - Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3,
 - Obsługiwana łączna przepływność (pasmo) min. 600 Gbps,
 - Obsługiwana łączna przepustowość pakietowa przełącznika min. 250 mpps,
 - opóźnienie przełączania pakietów nie większe niż 3 μ s,
 - głębokość buforów min. 40 MB,
 - pamięć RAM min. 24 GB,
 - Pamięć SSD/FLASH 128GB.
- Przełącznik posiada następującą funkcjonalność warstwy L2:
 - Trunking IEEE 802.1Q VLAN,
 - Wsparcie dla 3900 sieci VLAN,
 - Funkcjonalność izolowania portów znajdujących się w tym samym VLAN,
 - Wsparcie sprzętowe dla minimum 90 tysięcy adresów MAC,
 - IEEE 802.1w Rapid Spanning Tree (RST),
 - IEEE 802.1s Multiple Spanning Tree (MST),
 - Wsparcie sprzętowe dla tunelowania QinQ,
 - Zabezpieczenie przeciwko incydentom w topologii Spanning Tree,
 - Internet Group Management Protocol (IGMP) Versions 2, 3,
 - Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach,
 - Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązkę,
 - Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów).
- Przełącznik posiada następującą funkcjonalność warstwy L3:

- Sprzętowe przełączanie pakietów w warstwie L3,
- Routing w oparciu o trasy statyczne,
- Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6,
- Policy Based Routing (PBR) dla IPv4,
- VRRP v3,
- Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol),
- Wsparcie sprzętowe dla minimum 700 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP,
- Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast),
- Wsparcie dla IGMPv3 oraz MSDP,
- Wsparcie sprzętowe dla minimum 32,000 tras multicastowych,
- Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking),
- Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP),
- Minimum 2000 wpisów dla ACL - access control list,
- Jeśli funkcjonalność powyższa wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.
- Przełącznik posiada sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
 - Layer 2 IEEE 802.1p (CoS),
 - Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4,
 - Kolejowanie na wyjściu w oparciu o CoS 802.1p,
 - Bezwzględne (strict-priority) kolejowanie na wyjściu,
 - Kolejowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający,
 - Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych,
 - Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych,
 - Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:

- Wejściowe ACL (standardowe oraz rozszerzone):
 - Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu,
 - Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP),
 - ACL oparte o VLAN-y (VACL),
 - ACL oparte o porty (PACL),
- DHCP Snooping,
- ARP Inspection,
- IP Source Guard,
- Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.
- Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
 - Port zarządzający 100/1000 Mbps,
 - Port konsoli CLI,
 - Zarządzanie In-band,
 - SSHv2,
 - Authentication, authorization, and accounting (AAA),
 - RADIUS,
 - TACACS+
 - Syslog,
 - SNMP v1, v2, v3,
 - RMON (przynajmniej grupy Events, Alarms),
 - sFlow lub netFlow,
 - IEEE 802.1ab LLDP,
 - Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
 - Role-Based Access Control RBAC,
 - Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing),
 - Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror),
 - Network Time Protocol (NTP),
 - Precision Time Protocol IEEE 1588,

- Diagnostyka procesu BOOT,
- Ping,
- Traceroute.
- Narzędzia programowania i zarządzania przełącznikiem:
 - Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API,
 - Wbudowana powłoka bash do zarządzania systemem Linux przełącznika,
 - Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika,
 - Interfejs programistyczny REST API wraz z upublicznionym SDK,
 - Wsparcie dla NETCONF i zarządzania poprzez XML,
 - Wsparcie dla OpenStack Neutron plugin.
- Przełącznik musi być wyposażony w:
 - 2 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional),
 - 2 wkładki 10/25G SFP+ CSR,
 - Komplet 10 sztuk Patchcordów światłowodowych LC-LC OM4 MMF o długościach:
 - 2 sztuki: 50m,
 - 2 sztuki: 20m,
 - 2 sztuki: 10m,
 - 2 sztuki: 5m,
 - 2 sztuki: 2m.
 - 2 wkładki 10G SFP+ RJ45,
 - Okablowanie niezbędne do podłączenia urządzeń,
 - Komponenty potrzebne do zamontowania dostarczonych urządzeń w szafach rack (np. organizery) oraz podłączenia do sieci energetycznej.
- Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych lub połączeń zasilających urządzenia.
- Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rack 19".

4.4. Przełącznik w konfiguracji B (4 sztuki) posiada:

- 40 portów 100Mb/1GBaseT z obsługą PoE+ (IEEE 802.3at),
- 8 portów 100Mb/1G/2.5G/5G/10GBaseT z obsługą PoE+ (IEEE 802.3at),
- 4 porty SFP+ 10 Gbps.
- Parametry wydajnościowe:
 - Prędkość przełączania „wirespeed” dla każdego portu przełącznika,
 - Urządzenie sprzętowo przełącza pakiety w warstwie L2,
 - Obsługiwana łączna przepływność (pasmo) min. 160 Gbps,
 - Obsługiwana łączna przepustowość pakietowa przełącznika min. 100 mpps,
 - opóźnienie przełączania pakietów nie większe niż 5 μ s,
 - głębokość buforów min. 10 MB,
 - pamięć RAM min. 4 GB,
 - Pamięć SSD/FLASH min 4GB.
- Przełącznik posiada następującą funkcjonalność warstwy L2:
 - Trunking IEEE 802.1Q VLAN,
 - Wsparcie dla 3900 sieci VLAN,
 - Funkcjonalność izolowania portów znajdujących się w tym samym VLAN,
 - Wsparcie sprzętowe dla minimum 30 tysięcy adresów MAC,
 - IEEE 802.1w Rapid Spanning Tree (RST),
 - IEEE 802.1s Multiple Spanning Tree (MST),
 - Zabezpieczenie przeciwko incydentom w topologii Spanning Tree,
 - Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 2 interfejsów fizycznych w wiązkę,
 - Ramki Jumbo dla wszystkich portów (minimum 9000 bajtów).
- Przełącznik posiada następującą funkcjonalność warstwy L3:
 - Przełączanie pakietów w warstwie L3,
 - Routing w oparciu o trasy statyczne,
 - Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6,
 - Wsparcie sprzętowe dla minimum 2 tysięcy wpisów hosta w tablicy routingu IP,
 - Minimum 1000 wpisów dla ACL - access control list,
 - Jeśli funkcjonalność powyższa wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.

- Przełącznik posiada wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad i z wykorzystaniem klucza min 128 bit. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
 - Layer 2 IEEE 802.1p (CoS),
 - Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4
- Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
 - Wejściowe ACL (standardowe oraz rozszerzone):
 - Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu,
 - Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP),
 - ACL oparte o VLAN-y (VACL),
 - ACL oparte o porty (PACL),
 - DHCP Snooping,
 - ARP Inspection,
- Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
 - Port zarządzający 100/1000 Mbps,
 - Port konsoli CLI,
 - Zarządzanie In-band,
 - SSHv2,
 - Authentication, authorization, and accounting (AAA),
 - RADIUS,
 - TACACS+
 - Syslog,
 - SNMP v1, v2, v3,
 - RMON (przynajmniej grupy Events, Alarms),
 - sFlow lub netFlow,
 - IEEE 802.1ab LLDP,
 - Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
 - Role-Based Access Control RBAC,
 - Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing),

- Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror),
- Network Time Protocol (NTP),
- Precision Time Protocol IEEE 1588,
- Diagnostyka procesu BOOT,
- Ping,
- Traceroute.
- Narzędzia programowania i zarządzania przełącznikiem:
 - Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API,
 - Interfejs programistyczny REST API wraz z upublicznionym SDK,
 - Wsparcie dla NETCONF i zarządzania poprzez XML,
- Przełącznik musi być wyposażony w:
 - 2 wkładki 10G SFP+ CSR,
 - 2 wkładki 10G SFP+ RJ45,
 - Komplet 10 sztuk Patchcordów światłowodowych LC-LC OM4 MMF o długościach:
 - 2 sztuki: 20m,
 - 2 sztuki: 10m,
 - 2 sztuki: 5m,
 - 2 sztuki: 2m,
 - 2 sztuki: 1m.
 - Okablowanie niezbędne do podłączenia urządzeń,
 - Komponenty potrzebne do zamontowania dostarczonych urządzeń w szafach rack (np. organizery) oraz podłączenia do sieci energetycznej.
- Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych lub połączeń zasilających urządzenia.
- Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rack 19".

4.5. Szkolenia:

Zamawiający eksploatuje switchy firmy Cisco i posiada inżynierów do zarządzania taką platformą urządzeń, dlatego w przypadku zaoferowania urządzeń innej firmy Wykonawca przeprowadzi szkolenia dla inżynierów Zamawiającego w następującym zakresie:

- szkolenie muszą zostać przeprowadzone dla 5-ciu pracowników Zamawiającego,

- szkolenia muszą umożliwiać przekazanie wiedzy umożliwiającej samodzielnie przez pracowników Zamawiającego: konfigurowania, zarządzanie, budowanie polityk bezpieczeństwa, zaawansowane funkcje bezpieczeństwa, zarządzania rolami/uprawnieniami, monitorowania, aktualizowanie oraz diagnozę i rozwiązywanie problemów dla dostarczonego rozwiązania oraz dobre praktyki i utwardzanie konfiguracji,
- szkolenie muszą zostać przeprowadzone przez certyfikowanego trenera producenta ofertowanego rozwiązania,
- szkolenia muszą zostać przeprowadzone w języku polskim,
- szkolenie muszą zostać w formie stacjonarnej w certyfikowany przez producenta ośrodku szkoleniowym na terenie Polski i muszą obejmować zarówno część teoretyczną oraz praktyczną na sprzęcie lub w środowisku symulacyjnym. Zamawiający dopuszcza też przeprowadzenie szkolenia w formie zdalnej,
- czas trwania szkolenia min 5 dni roboczych.

5. Urządzenie typu KVM over IP – 2 sztuki.

- 5.1. Urządzenie musi pozwalać na przekazywanie obrazu w rozdzielczości FullHD 1920x1080.
- 5.2. Urządzenie musi pozwalać na podłączenie co najmniej 4 serwerów.
- 5.3. Dostęp do urządzenia musi być szyfrowany.
- 5.4. Urządzenie musi pozwalać na jednoczesny dostęp co najmniej 2 użytkowników.
 - Urządzenie musi pozwalać na podłączenie do serwera poprzez hdmi oraz symulować klawiaturę oraz mysz. Zamawiający dopuszcza stosowanie adapterów o ile zostaną dołączone do zestawu.
- 5.5. Urządzenie musi być w obudowie typu RACK.

6. Urządzenie typu serial over ip – 2 sztuki.

- 6.1. Urządzenie musi pozwalać na podłączenie co najmniej 8 serwerów i/lub urządzeń sieciowych.
- 6.2. Dostęp do urządzenia musi być szyfrowany.
- 6.3. Urządzenie musi pozwalać na jednoczesny dostęp co najmniej 2 użytkowników.
- 6.4. Urządzenie musi pozwalać na podłączenie do portów konsolowych serwerów i urządzeń sieciowych.
 - Zamawiający dopuszcza stosowanie adapterów o ile zostaną dołączone do zestawu.
- 6.5. Urządzenie musi być w obudowie typu RACK lub dostarczone z adapterami pozwalającymi na montaż w szafie RACK.

7. Urządzenia typu Access Point - 20 sztuk.

- 7.1. 20 sztuk Access Point Cisco Meraki MR56 lub urządzenia równoważne zapewniające funkcjonalność opisaną niżej w sekcji wymagania dla Access Point równoważnego.
- 7.2. Każde z urządzeń musi być dostarczone z kompletem wymaganych licencji lub subskrypcji umożliwiających centralne zarządzanie przez portal chmurowy Meraki lub dostarczone rozwiązanie równoważne przez okres min 60 miesięcy.
- 7.3. Dostarczone licencje lub subskrypcje muszą rozszerzać obecnie wykorzystywany przez Zamawiającego portal zarządzania Meraki o możliwość zarządzania dostarczoną partią urządzeń lub w przypadku dostarczenia rozwiązania równoważnego umożliwić zbudowanie platformy do centralnego zarządzania dostarczonymi urządzeniami. Platforma zarządzania musi być tego samego producenta co dostarczone urządzenia.
- 7.4. Każde z urządzeń musi:
- spełniać wszystkie wymagania dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie,
 - być fabrycznie nowe, kompletne, nieużywane i bez oznak użytkowania, nierefabrykowane i nieregenerowane, nienaprawiane, nie podlegało ponownej obróbce,
 - być wolne od jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwość jego prawidłowego użytkowania,
 - dopuszczone do obrotu gospodarczego na terytorium Rzeczypospolitej Polskiej,
 - być zgodne ze stosowanymi normami technicznymi,
 - posiadać certyfikaty dopuszczające do stosowania w Unii Europejskiej,
 - pochodzić z oryginalnego kanału dystrybucji Producenta na rynek polski,
 - w dniu składania ofert nie może być przeznaczone przez Producenta do wycofania z produkcji lub sprzedaży.

7.5. Gwarancja:

Całość dostarczonego rozwiązania musi być objęty serwisem gwarancyjnym producenta przez okres 60 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. Szczegóły wymagań dla gwarancji określono w pkt 10.

7.6. **Wymagania dla Access Point równoważnego**

Niżej określone są wymagania minimalne:

- Punkt dostępowy zarządzany przez kontroler sieci bezprzewodowej dostępny w publicznej chmurze.
- Architektura radiowa i obsługa standardów:
 - zgodność ze standardami 802.11a/b/g/n oraz 802.11ac Wave 2 oraz 802.11ax,
 - moduł radiowy 802.11 b/g/n,
 - moduł radiowy 802.11 a/n/ac/ax ,

- dwuzakresowy moduł radiowy do zastosowań wIDS/wIPS,
- obsługa kanałów 20, 40, 80 MHz dla 802.11ac/ax oraz 20, 40 MHz dla 802.11n,
- obsługa 256-QAM dla pasma 2,4GHz oraz 5 GHz,
- obsługa MIMO co najmniej 4x4:4 dla pasma 2,4 oraz 8x8:8 dla pasma 5 GHz,
- obsługa prędkości PHY do co najmniej 4 Gbps dla 5 GHz,
- obsługa prędkości PHY do co najmniej 500 Mbps dla 2,4 GHz,
- łączna prędkość zagregowana nie mniejsza niż 5 Gbps,
- obsługa Maximal Ratio Combining,
- obsługa formowania wiązki (beamforming),
- obsługa agregacji ramek,
- obsługa SU-MIMO i MU-MIMO.
- Obsługa zakresów częstotliwości:
 - 2,412 – 2,484 GHz,
 - 5,150 – 5,250 GHz (UNII-1),
 - 5,250 – 5,350 GHz (UNII-2A),
 - 5,490 - 5,730 GHz (UNII-2C),
 - 5,735 - 5,825 GHz (UNII-3).
- Konfigurowalna moc nadajnika, pozwalająca na uzyskanie mocy:
 - dla pasma 2,4 GHz: do co najmniej 20 dBm,
 - dla pasma 5 GHz: do co najmniej 21 dBm.
- Moduł BLE (Bluetooth Low Energy):
 - praca jako beacon BLE (możliwość konfiguracji parametrów UUID, Major, Minor),
 - skanowanie sygnałów Bluetooth.
- Mechanizmy bezpieczeństwa:
 - WEP, WPA, WPA2-PSK, WPA2-Enterprise (802.1X),
 - szyfrowanie TKIP oraz AES,
 - tagowanie VLAN (IEEE 802.1q),
 - blokowanie ruchu między klientami bezprzewodowymi,
 - zintegrowany moduł wykrywania włamań, obcych AP i reagowania na nie (wIPS/wIDS):
 - skanowanie pasma 2,4 GHz oraz 5 GHz w czasie rzeczywistym,
 - detekcja obcych AP,
 - wykrywanie podłączenia obcego AP do sieci LAN,
 - klasyfikacja ataków w zależności od stopnia zagrożenia,
 - klasyfikacja ataków w oparciu o sygnatury bazujące na typie i profilu zachowania (podstawowe ataki co najmniej: spoofing, DoS, packet flood),
 - konfiguracja polityki reagowania na ataki,
 - prowadzenie logu zdarzeń.
- Mechanizmy QoS:
 - DSCP,

- 802.1p,
- Advanced Power Save (U-APSD),
- IEEE 802.11e oraz WMM,
- priorytet dla ruchu głosowego,
- limitowanie ruchu per klient oraz per SSID,
- rozpoznawanie aplikacji w warstwie 7,
- limitowanie wybranego typu ruchu aplikacyjnego per klient oraz per SSID z możliwością markowania ruchu,
- mechanizm preferowania pasma 5 GHz dla klientów dwuzakresowych,
- mechanizm analizy widma częstotliwości z możliwością graficznej prezentacji pracujący w obu pasmach częstotliwości.
- Mechanizmy mobilności:
 - 802.11k oraz 802.11r,
 - Pairwise Master Key caching oraz Opportunistic Key Caching dla szybkiego roamingu L2.
- Obsługa dostępu gościnnego:
 - przekierowanie użytkowników danego SSID na portal logowania,
 - personalizacja wyglądu portalu logowania,
 - kreowanie i zarządzanie kontami gościnnymi przez interfejs webowy,
 - uwierzytelnianie do sieci za pośrednictwem: akceptacji portalu, możliwość uwierzytelniania SMSem, serwera LDAP, serwera RADIUS, kont z portalu Facebook,
 - obsługa Walled Garden (zdefiniowanie strefy sieciowej, do której gość ma dostęp przed zalogowaniem).
- Funkcje ogólne:
 - automatyczne budowanie sieci kratowej (formowanie połączeń do innych punktów dostępowych WiFi w oparciu o radio 2,4GHz lub 5 GHz bez podłączenia do sieci kablowej),
 - obsługa min. 15 SSID,
 - konfiguracja dostępności danego SSID w zależności od danego zakresu godzin w danym dniu tygodnia,
 - logowanie zdarzeń ,
 - logowanie zmian w konfiguracji,
 - eksport SYSLOG,
 - obsługa synchronizacji czasu (NTP lub podobny mechanizm).
- Uproszczona instalacja urządzenia, wymagająca co najwyżej:
 - podłączenia urządzenia do sieci Internet,
 - podania jego numeru seryjnego w module zarządzania i monitorowania infrastruktury sieciowej,
 - wskazania sieci / lokalizacji, która określa jego konfigurację.
- Parametry fizyczne, anteny, zasilanie:
 - masa poniżej 1 kg,
 - zabezpieczenie Kensington,
 - temperatura pracy: 0 – 40°C,
 - zintegrowane anteny dookólne o zysku co najmniej 5 dBi dla 2.4 GHz oraz 5,5 dBi dla 5 GHz,
 - diodowa sygnalizacja stanu urządzenia,

- obudowa niskoprofilowa (wysokość poniżej 5cm),
- zasilanie PoE (IEEE 802.3at) ,
- zużycie energii: nie więcej niż 30W.
- Interfejs przewodowy: RJ45 - 1 x 100/1000/2.5G Base-T Ethernet .
- Zgodność z dyrektywą RoHS.
- Niezbędne oprogramowanie do zarządzania urządzeniami wraz z niezbędnymi licencjami.
- Niezbędne wszelkie niezbędne komponenty potrzebne do zamontowania na suficie.
- Każde z urządzeń musi:
 - spełniać wszystkie wymagania dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie,
 - być fabrycznie nowe, kompletne, nieużywane i bez oznak użytkowania, nierefabrykowane i nieregenerowane, nienaprawiane, nie podlegało ponownej obróbce,
 - być wolne od jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwości jego prawidłowego użytkowania,
 - dopuszczone do obrotu gospodarczego na terytorium Rzeczypospolitej Polskiej,
 - być zgodne ze stosowanymi normami technicznymi,
 - posiadać certyfikaty dopuszczające do stosowania w Unii Europejskiej,
 - pochodzić z oryginalnego kanału dystrybucji Producenta na rynek polski,
 - w dniu składania ofert nie może być przeznaczone przez Producenta do wycofania z produkcji lub sprzedaży.
- Gwarancja:

Całość dostarczonego rozwiązania musi być objęty serwisem gwarancyjnym producenta przez okres 60 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. Szczegóły wymagań dla gwarancji określono w pkt 10.

7.7. Wymagania dla oprogramowania do zarządzania Access Point równoważnego

- System monitorowania, konfiguracji, utrzymania infrastruktury sieciowej pozwalający na zarządzanie punktami dostępowymi (wraz z niezbędną liczbą licencji na system pozwalający na scentralizowane zarządzanie punktami dostępowymi);
- System dostępny wraz z gwarancją, serwisem na okres nie krótszy niż 60 miesięcy oraz subskrypcją oprogramowania na okres 60 miesięcy dostępny w publicznej chmurze
- Funkcje ogólne:
 - zarządzanie przez graficzny interfejs webowy z wykorzystaniem HTTPS,
 - integracja z publicznie dostępnym serwisem mapowym (typu Google Maps) w celu graficznego rozmieszczenia położenia urządzeń i wizualizacji ich stanu,
 - wizualizacja topologii sieci:

- automatyczne rysowanie mapy topologii,
- wizualizacja stanu urządzeń,
- wizualizacja połączeń między urządzeniami,
- wizualizacja połączeń zablokowanych przez STP;
- podział zarządzanych urządzeń na logiczne podgrupy: np.: oddział, lokalizacja, itp.,
- monitoring i zarządzanie siecią z podziałem na podgrupy,
- możliwość przypisywania znaczników do różnych elementów w module, np.: podgrupa urządzeń, urządzenie, port urządzenia w celu łatwego wyszukiwania i konfiguracji danej grupy elementów o zadanym znaczniku,
- wbudowany mechanizm wyszukiwania ustawień, urządzeń, klientów,
- zautomatyzowany proces dodawania nowych urządzeń do systemu zarządzania, np.: poprzez wpisanie numeru seryjnego urządzenia,
- centralna administracja licencjami urządzeń,
- eksport zdarzeń do serwerów SYSLOG:
 - zarządzanie typem wysyłanych zdarzeń,
 - dla przełączników: log zdarzeń,
 - dla punktów dostępowych: log zdarzeń, URL, flow.
- Centralne zarządzanie oprogramowaniem na urządzeniach:
 - możliwość automatycznej aktualizacji po wprowadzeniu nowej wersji oprogramowania przez producenta,
 - możliwość wyboru daty aktualizacji,
 - możliwość modyfikacji daty aktualizacji dla danego typu lub konkretnych urządzeń.
- Narzędzia wspomagające diagnostykę problemów z urządzeniami:
 - dla punktu dostępowego: ping, traceroute, wyświetlenie tablicy ARP, test przepustowości,
 - dla przełącznika: ping, test kabla, wyświetlenie tablicy MAC, restart portu, test przepustowości.
- Narzędzie do przechwytywania ruchu do pliku w celu szczegółowej analizy z możliwością ignorowania pakietów broadcast, multicast oraz tworzeniem wyrażeń filtrujących (np.: po adresie IP, MAC, itp.).
- Monitoring podłączonych urządzeń/klientów za zadany okres: ostatnich godzin, ostatniego dnia, tygodnia, miesiąca z następującymi informacjami:
 - sposób podłączenia do sieci: przewodowo lub bezprzewodowo,
 - parametry IP: adres IPv4, IPv6, MAC, VLAN,
 - parametry urządzenia: typ/model urządzenia,

- liczba przetransmitowanych danych (dla urządzeń obsługujących analizę aplikacyjną – z podziałem na aplikacje warstwy 7),
- dla urządzeń/klientów bezprzewodowych:
 - parametry radiowe połączenia: siła sygnału, kanał,
 - wspierane standardy radiowe,
 - maksymalna przepustowość,
 - wspierana ilość strumieni przestrzennych;
- dla urządzeń/klientów przewodowych:
 - numer portu i przełącznika, do którego podłączony jest klient.
- Ogólne parametry raportowania:
 - raporty z podziałem na logiczne podgrupy,
 - raporty z podziałem na logiczne podgrupy z wybranym tagiem,
 - raporty za okres ostatniego dnia, tygodnia, miesiąca, wybranego okresu,
 - wysyłanie raportów w formacie HTML lub tekstowym na zadany adres email.
- Raporty dotyczące sieci zawierające informacje za zadany okres:
 - wykorzystanie sieci (ilość przetransmitowanych danych) w postaci wykresu,
 - całkowita wartość ruchu z podziałem na ruch upstream oraz downstream,
 - lista klientów o największej ilości przetransmitowanych danych z podaną wartością,
 - lista najbardziej wykorzystywanych aplikacji w sieci z podaną wartością transmisji,
 - lista najczęściej spotykanych systemów operacyjnych w sieci z podaną wartością transmisji,
 - lista najczęściej spotykanych typów urządzeń klienckich z podaną wartością transmisji,
 - liczba klientów podłączonych do sieci z podziałem czasowym,
 - mapa rozmieszczenia urządzeń z ilością podłączonych klientów,
 - dla punktów dostępowych:
 - lista punktów dostępowych WiFi o największej transmisji danych z podaną wielkością transmisji,
 - lista SSID o największej transmisji danych z podziałem z podaną wartością transmisji.
- Dostęp administracyjny do modułu zarządzania:
 - blokowanie administratora po kilkukrotnych nieudanych próbach logowania,
 - ograniczanie możliwości zalogowania się do określonego zakresu adresów IP,
 - wyznaczanie administratorów do określonych logicznych podgrup urządzeń,

- wyznaczanie poziomu dostępu: tylko do odczytu, zarządzanie dostępem gościnnym, pełny dostęp do wprowadzania zmian,
- wysyłanie notyfikacji email w momencie wprowadzania zmian konfiguracyjnych,
- logowanie czasu, adresu IP oraz przybliżonej lokalizacji logującego się do modułu z możliwością weryfikacji tej informacji w logu wraz z informacją o wprowadzonych zmianach,
- wylogowywanie administratora po określonym czasie bezczynności,
- integracja SAML w celu uwierzytelniania administratorów za pośrednictwem zewnętrznego serwera uwierzytelniania.
- Alarmy dotyczące pracy sieci:
 - wysyłanie alarmów do administratorów lub do określonych adresów email,
 - wysyłanie trapów SNMP,
 - wysyłanie alarmów:
 - gdy nastąpi zmiana konfiguracji,
 - gdy urządzenie będzie nieosiągalne przez zadany okres czasu,
 - gdy zmieni się status głównego łącza,
 - gdy wyczerpie się pula adresów DHCP,
 - gdy pojawi się konflikt adresów IP,
 - gdy punkt dostępowy straci połączenie kablowe z siecią i podłączy się drogą bezprzewodową do innego punktu dostępowego.
- Mechanizmy dotyczące sieci bezprzewodowej:
 - wgranie map pomieszczeń z możliwością rozmieszczenia AP,
 - wyświetlanie rozmieszczenia AP oraz klientów (podłączonych oraz niepodłączonych) sieci bezprzewodowej na mapie pomieszczenia z zaznaczeniem miejsc o wysokiej i niskiej gęstości,
 - wizualizacja informacji o stanie spektrum radiowego w okolicy danego AP (chwilowa zajętość kanałów, histogram zajętości, interferencje),
 - zbieranie informacji o urządzeniach w zasięgu sieci radiowej z podziałem na urządzenia/klientów podłączonych do sieci, będących w jej zasięgu oraz przemieszczających się w jej zasięgu,
 - monitoring punktów dostępowych WiFi i wyświetlanie co najmniej następujących atrybutów: adres MAC, numer seryjny, uruchomione sieci SSID i VLAN, adres IP, DNS, transmisja danych oraz ilości klientów z ostatniego dnia,
 - narzędzia wspomagające diagnostykę problemów: ping, traceroute, wyświetlenie tablicy ARP, test przepustowości, mruganie diodami urządzenia,

- narzędzie do przechwytywania ruchu do pliku pcap w celu szczegółowej analizy z możliwością ignorowania pakietów broadcast, multicast oraz tworzeniem wyrażeń filtrujących (np. po adresie IP, MAC, itp.),
- monitoring urządzeń podłączających się do sieci w zakresie: parametrów radiowych połączenia (siła sygnału, kanał), atrybutów IP (adres IPv4, IPv6, MAC, VLAN), parametrach urządzenia (typ/model urządzenia, wspierane standardy radiowe, maksymalna przepustowość, wspierana ilość strumieni przestrzennych), ilości przetransmitowanych danych z podziałem na aplikacje,
- koordynacja funkcjonalności punktów dostępowych:
 - automatyczny dobór mocy nadawania na punktach dostępowych,
 - automatyczny dobór obsługiwanych kanałów na punktach dostępowych,
 - monitorowanie pasma radiowego pod kątem wykrywania interferencji, pomiaru poziomu zajętości i szumów w celu dynamicznej optymalizacji ustawień parametrów radiowych,
 - obsługa kanałów DFS,
 - zarządzanie mobilnością urządzeń,
 - zarządzanie budową sieci kratowej.
- Mechanizmy analityczne:
 - zbieranie i raportowanie informacji o urządzeniach Wi-Fi (z aktywnym sygnałem WiFi 802.11) w zasięgu sieci radiowej z podziałem na urządzenia/klientów podłączonych do sieci, będących w jej zasięgu oraz przemieszczających się w jej zasięgu,
 - zbieranie i raportowanie informacji o długości czasu przebywania urządzeń/klientów w zasięgu sieci radiowej,
 - zbieranie i raportowanie informacji o powtarzalności wizyt urządzeń/klientów,
 - możliwość raportowania w/w informacji dla różnych okresów czasu np. ostatni dzień, ostatni tydzień, ostatni miesiąc lub zadany okres czasu,
 - możliwość eksportu w/w statystyk / raportów w postaci pliku CSV,
 - możliwość tworzenia w/w statystyk niezależnie dla różnych obiektów (lokalizacji) jak również dla grup urządzeń bezprzewodowych,
 - API pozwalające na wysyłanie na zewnętrzny serwer informacji o lokalizacji klienckich urządzeń mobilnych połączonych i niepołączonych do sieci Wi-Fi znajdujących się w zasięgu działania sieci Wi-Fi. Format danych musi umożliwiać uzyskanie następujących informacji na temat danego urządzenia klienckiego Wi-Fi: adres MAC radiowego punktu dostępowego, który wykrył dane urządzenie klienckie, adres wykrytego urządzenia, adres IPv4 oraz IPv6 wykrytego urządzenia klienckiego, czas wykrycia w formacie UTC, nazwę SSID sieci dla urządzeń klienckich podłączonych do sieci Wi-Fi, zaobserwowane RSSI urządzenia klienckiego, producent i system operacyjny urządzenia klienckiego, współrzędne X (pionowa) i Y (pozioma) określające położenie urządzenia klienckiego.

Część II: sprzęt komputerowy i serwerowy

8. Laptop biznesowy – 6 sztuk.

- 8.1. Rozdzielczość ekranu: 1920 x 1080 lub wyższa.
- 8.2. Przekątna ekranu: min. 15,6 cali.
- 8.3. Matryca: matowa, jasność min. 500 nit.
- 8.4. Pamięć RAM: min. 32 GB DDR5, taktowanie 5600 MHz.
- 8.5. Pojemność dysku: min. 512 GB, Technologia dysku: SSD m.2 NVMe.
- 8.6. Karta graficzna: zintegrowana.
- 8.7. Komunikacja: min. karta sieciowa WLAN 802.11 AX (wbudowana), Bluetooth 5.3 lub nowszy (wbudowany), Ethernet 1Gb RJ45 (wbudowany).
- 8.8. Komputer powinien osiągać w teście wydajności dla testów PC Mark 10: Overall score - wynik min.: 7000.
- 8.9. Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę UL Laboratory i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowanie overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta.
- 8.10. Porty i złącza:
 - min 2 złącza Thunderbolt 4/USB4 lub nowsze, min 1 wspiera Power Delivery 3.0 i DisplayPort 2.1),
 - min. 2 złącza USB w tym przynajmniej jedno złącze USB Typ A. 3.2 lub nowsze (wbudowane),
 - złącze HDMI 1.4 lub nowsze - 1szt (wbudowane),
 - złącze słuchawkowe/mikrofonowe line-out/line-in, dopuszczalne złącze typu COMBO,
 - złącze Ethernet (Gigabit) – 1szt.
- 8.11. Wyposażenie/funkcje:
 - czytnik kart pamięci,
 - kamera internetowa min 3MP (wbudowana) z przesłoną mechaniczną zapewniającą prywatność oraz wsparciem rozpoznawania twarzy zgodna z Windows Hello for Business,
 - wbudowane głośniki stereo,
 - wbudowany mikrofon,
 - Touchpad,
 - moduł TPM 2.0,

- Bateria litowo-polimerowa lub litowo-jonowa, wspierająca szybkie ładowanie (80% baterii w 1h) o pojemności min 70Wh,
- Zasilacz z USB-C.

8.12. System operacyjny: Microsoft Windows 11 Pro.

8.13. Klawiatura (wbudowana): podświetlana, pełnowymiarowa, w układzie US-Qwerty, polskie znaki zgodne z układem MS Windows „polski programistyczny”.

8.14. Bios:

- Zgodny ze specyfikacją UEFI,
- Funkcje umożliwiające sprawdzenie wersji BIOS numeru seryjnego i dacie produkcji komputera, ID płyty głównej, informacja o baterii, wielkości i prędkości zainstalowanej pamięci RAM, informacje o zainstalowanym procesorze, informacje o zainstalowanych dyskach twardej, BIOS musi umożliwiać ustawienia hasła administratora oraz użytkownika
- Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych

8.15. Każde z urządzeń musi:

- spełniać wszystkie wymogi dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie,
- być fabrycznie nowe, kompletne, nieużywane i bez oznak używania, nierefabrykowane i nieregenerowane, nienaprawiane, nie podlegało ponownej obróbce,
- być wolne od jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwości jego prawidłowego użytkowania,
- dopuszczone do obrotu gospodarczego na terytorium Rzeczypospolitej Polskiej,
- być zgodne ze stosowanymi normami technicznymi,
- posiadać certyfikaty dopuszczające do stosowania w Unii Europejskiej,
- pochodzić z oryginalnego kanału dystrybucji Producenta na rynek polski,
- w dniu składania ofert nie może być przeznaczone przez Producenta do wycofania z produkcji lub sprzedaży.

8.16. Gwarancja:

Całość dostarczonego rozwiązania musi być objęty serwisem gwarancyjnym producenta przez okres 60 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. Szczegóły wymagań dla gwarancji określono w pkt 10.

9. Serwery RACK - 4 sztuki.

- Każdy z 4 dostarczonych serwerów w konfiguracji o wymaganiach minimalnych określonych niżej:
- 9.1. Procesory: min 2 procesory 32 rdzeniowe, każdy x86 - 64 bity taktowany częstotliwością bazową nie mniejszą niż 3,8 GHz, osiągający w testach SPECrate2017_int_base wynik minimum 800 punktów dla modelu oferowanego serwera, wyposażonego w dwa procesory. Wyniki dla oferowanego modelu serwera muszą być dostępne na stronie www.spec.org.
 - 9.2. Pamięć operacyjna: zainstalowane minimum 2048 GB pamięci RAM typu DDR5 Registered, min. 4800Mhz w kościach o pojemności min. 64 GB. Obsługa zabezpieczeń: korekcja błędów pamięci.
 - 9.3. Dyski twarde:
 - Zainstalowane 2 dyski Mixed Use min. 480GB SATA SSD Hot-Plug, DWPD (Disk Write Per Day) ≥ 3 działające redundantnie, służące do uruchamiania systemu lub 2 dyski m.2 zainstalowane na karcie BOSS o pojemności min. 240GB.
 - Zainstalowane 5 dysków Read Intensive min.10 TB NVMe SSD (spełniające wymagania VMware vSAN dla dysków capacity).
 - Zainstalowane 2 dyski Mixed Use 0,9TB NVMe SSD (spełniające wymagania VMWare vSAN dla dysków cache).
 - Serwer musi posiadać min 24 zatoki dyskowe 2,5" dostępne z przodu obudowy serwera.
 - Dostarczone dyski muszą być wspierane przez producenta oprogramowania BROADCOM dla produktu vSphere 8.0 (vSAN) i wyższych. Wyniki dla oferowanego modelu dysku muszą być dostępne na stronie <https://compatibilityguide.broadcom.com>
 - 9.4. Obudowa: Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez jego wyłączenia).
 - 9.5. Sloty rozszerzeń: Serwer musi posiadać minimum 8 gniazd PCI-Express generacji 5 z dostępem zewnętrznym, w tym min. 2 sloty x16 (szybkość slotu – bus width).
 - 9.6. Kontroler: Serwer musi być wyposażony w kontroler sprzętowy z min. 2 GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę min. 24 napędów dyskowych.
 - 9.7. Interfejsy sieciowe Ethernet:
 - Minimum 2 porty Ethernet SFP28 każdy 10/25 Gb/s wraz z wkładkami SFP-25G-SR. Karty muszą umożliwiać podział na wirtualne interfejsy za pomocą technologii NPAR.
 - Minimum 2 porty Ethernet SFP+ każdy 10 Gb/ wraz z wkładkami SFP+ RJ45.
 - Minimum 1 port Ethernet 1 Gb/s.
 - Wszystkie porty Ethernet muszą wspierać protokół LACP.
 - 9.8. Karta graficzna: zintegrowana.
 - 9.9. Porty:
 - min. 4 porty USB w tym jeden wewnątrz obudowy. Min 2 porty USB 3.0.
 - min. 1 port VGA wyprowadzony na zewnątrz obudowy.
 - liczba dostępnych złączy VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakiegokolwiek slot PCI Express serwera.
 - 9.10. Zasilacze: 2 redundantne zasilacze (1+1) typu HotPlug o mocy minimum 1600W każdy.
 - 9.11. Karta/moduł zarządzający: karta niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:

- monitorowanie podzespołów i stanu serwera: temperatura, stan zasilaczy, prędkość obrotowa wentylatorów, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty rozszerzeń,
- wsparcie dla agentów zarządzających oraz/lub możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP,
- dostęp do karty zarządzającej poprzez dedykowany port RJ45, dostępny z poziomu obudowy serwera,
- dostęp do karty zarządzającej możliwy w każdy z niżej wymienionych sposobów:
 - z poziomu przeglądarki webowej (GUI), wsparcie dla HTML 5,
 - z poziomu linii komend,
 - przez interfejs IPMI 2.0 (Intelligent Platform Management Interface).
- możliwość obsługi karty zarządzającej przez co najmniej dwóch administratorów jednocześnie,
- możliwość konfiguracji wysłania powiadomień poprzez wiadomość e-mail do administratora o awariach lub istotnych zdarzeniach systemowych,
- wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów,
- możliwość monitorowania zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji,
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping),
- zdalna aktualizacja oprogramowania (firmware),
- integracja z Microsoft Active Directory,
- wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API,
- możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP),
- możliwość zarządzania serwerami z jednej z posiadanych konsol, HPE iLO Advanced lub Integrated Dell Remote Access Controller m.in. do zarządzania grupami serwerów w posiadanej infrastrukturze IT

9.12. Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego w postaci innej konsoli zarządzającej, której zadaniem będzie zarządzanie obecnie użytkowanymi serwerami marki DELL i HPE oraz serwerami dostarczonymi w ramach realizacji niniejszego postępowania.

- Kompatybilność oferowanego rozwiązania w zakresie zarządzania obecnie użytkowanymi przez Zamawiającego serwerami musi zostać potwierdzona stosownym oświadczeniem ze strony producenta rozwiązania przy czym konsola nie może realizować mniejszej liczby funkcjonalności niż wymienione w punkcie 3.0.7 do 3.0.9
- Przed dokonaniem wyboru najkorzystniejszej oferty Zamawiający zastrzega sobie prawo do przeprowadzenia testów konsoli równoważnej w izolowanym środowisku, tożsamym pod względem funkcjonalnym z obecnie użytkowanym na koszt Wykonawcy, w siedzibie Zamawiającego. Testowaniu podlegać będzie m.in.: zgodność funkcjonalności konsoli z obecnie użytkowanymi konsolami HPE i DELL po ich poprawnym podłączeniu oraz weryfikacji funkcjonalności opisanych w punkcie wyżej.
- W przypadku zaoferowania rozwiązania równoważnego, Zamawiający wezwie Wykonawcę do przeprowadzenia testów w terminie wskazanym w wezwaniu. Testy przeprowadzone zostaną w ciągu 2 dni roboczych od dnia otrzymania wezwania, z udziałem wyznaczonego przedstawiciela Wykonawcy. Z przeprowadzonych testów sporządzony zostanie przez Zamawiającego protokół.

- Całość prac związanych z testowaniem konsoli równoważnej oraz jej wdrożeniem w infrastrukturze Zamawiającego musi być przeprowadzona na ryzyko i koszt Wykonawcy.
 - Uruchomienie nowej konsoli w obecnej infrastrukturze Zamawiającego nie może wpłynąć na dostępność biznesową systemów IT Zamawiającego.
 - Wykonawca musi również zapewnić minimum dwudniowy instruktaż dla pracowników Zamawiającego w liczbie przynajmniej 5 osób. Instruktaż musi uwzględnić przekazanie informacji na temat wszystkich funkcjonalności oferowanych przez konsolę.
 - Wykonawca musi również zapewnić niezbędne licencje na użytkowanie konsoli zarządzającej. Jeżeli licencje te są dystrybuowane w modelu subskrypcyjnym, Wykonawca ma obowiązek zapewnić licencje przez cały okres trwania gwarancji na dostarczane serwery.
- 9.13. Wsparcie dla systemów operacyjnych:
- VMware vSphere 8.0 i wyższe, konfiguracja serwera (w tym dyski) musi być wspierana przez VMware i certyfikowana dla oprogramowania vSAN zgodnie z matrycą umieszczoną na stronie producenta: <https://compatibilityguide.broadcom.com>
 - Microsoft Windows Server 2019 i wyższe
 - Red Hat Enterprise Linux (RHEL) 8 i wyższe
- 9.14. Ekologia: oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest umieszczenie oferowanego urządzenia w rejestrze internetowym www.epeat.net na poziomie min. Epeat bronze według normy wprowadzonej w 2019 roku.
- 9.15. Oferowane Urządzenia w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.

10. Usługi gwarancji i gwarancja jakości

- 10.1. Dostarczony sprzęt musi być nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą do Zamawiającego.
- 10.2. Dostarczone urządzenia oraz oprogramowanie muszą być objęte nie krótszą niż 60 miesięczną gwarancją od dnia podpisania Protokołu Odbioru wniosku o rozliczenie finansowe.
- 10.3. Zamawiający dopuszcza świadczenie serwisu gwarancyjnego bezpośrednio przez producenta lub partnera producenta przy wsparciu producenta uprawniającym do zgłaszania telefonicznego i mailowego w zakresie konfiguracji Sprzętu oraz aktualizacji oprogramowania, a w przypadku ujawnienia wad w okresie gwarancji Wykonawca zobowiązuje się w terminie nie dłuższym niż 10 dni roboczych od dnia zgłoszenia tego faktu przez Zamawiającego (reklamacja) do:
- usunięcia wad Sprzętu w siedzibie Zamawiającego lub, jeżeli usunięcie wady w siedzibie nie jest możliwe, usunięcia wady poza siedzibą Zamawiającego. W przypadku, gdy Wykonawca wykonuje naprawę poza siedzibą Zamawiającego, jest on zobowiązany na czas naprawy

udostępnić Zamawiającemu i dostarczyć na własny koszt sprzęt zastępczy o parametrach nie gorszych od sprzętu naprawianego. Koszty związane z dostarczeniem sprzętu zastępczego ponosi Wykonawca;

- wymiany Sprzętu na nowy, wolny od wad, przy czym Wykonawca jest zobowiązany do wymiany Sprzętu na nowy w przypadku ujawnienia wady tego samego Sprzętu po raz trzeci.

10.4. W obrębie gwarancji zawarte musi być również min:

- dostęp do aktualnych wersji oprogramowania, dokumentacji oprogramowania w serwisie producenta oraz wsparcie producenta w zakresie usuwania błędów oprogramowania,
- obsługa przyjmowania zgłoszeń gwarancyjnych w trybie 7x24 w języku polskim, poprzez ogólnopolską linię telefoniczną producenta lub partnera producenta,
- W przypadku uszkodzenia nośnika danych (dysku), uszkodzony nośnik pozostaje u Zamawiającego.