

Załącznik nr 3b do SWZ

Szczegółowy opis przedmiotu zamówienia – część II Sprzęt sieciowy

1. UTM – zakup i wdrożenie (2 sztuki)

Obszar	Wymagania
Wymagania ogólne systemu	System bezpieczeństwa realizuje wszystkie funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Elementy systemu mogą być realizowane jako komercyjne platformy sprzętowe lub aplikacje instalowane na platformach ogólnego przeznaczenia, przy czym w przypadku implementacji programowej muszą być zapewnione odpowiednie platformy sprzętowe wraz z zabezpieczonym systemem operacyjnym. System firewall umożliwia pracę w trybie routera z funkcją NAT, trybie transparentnym oraz trybie monitorowania ruchu na porcie SPAN. Rozwiązanie umożliwia budowę minimum dwóch niezależnych instancji logicznych lub fizycznych w zakresie routingu, firewalla, IPSec VPN, ochrony antywirusowej, IPS oraz kontroli aplikacji, z możliwością przypisania co najmniej siedmiu administratorów do poszczególnych instancji. System wspiera protokoły IPv4 i IPv6 dla funkcji firewall, ochrony w warstwie aplikacji oraz dynamicznych protokołów routingu.
Redundancja i dostępność	System realizujący funkcje firewall, IPSec, kontroli aplikacji oraz IPS umożliwia pracę w klastrze w trybie ActiveActive lub ActivePassive z synchronizacją sesji w obu trybach. Rozwiązanie zapewnia monitoring i wykrywanie awarii elementów sprzętowych, programowych oraz łączy sieciowych, a także monitorowanie stanu połączeń VPN. System umożliwia agregację łączy w sposób statyczny oraz z wykorzystaniem protokołu LACP oraz tworzenie interfejsów redundantnych.
Interfejsy i zasilanie	System firewall jest wyposażony w co najmniej osiem interfejsów Gigabit Ethernet RJ45 oraz posiada wolne sloty umożliwiające instalację minimum dwóch wkładek SFP+ 10 Gbps lub jest dostarczony z takimi wkładkami. Urządzenie posiada wbudowany port konsoli szeregową oraz port USB umożliwiający podłączenie modemu 3G/4G i instalację oprogramowania z nośnika USB. System umożliwia konfigurację co najmniej 200 interfejsów wirtualnych VLAN zgodnych ze standardem 802.1Q i jest wyposażony w zasilanie AC.
Wydajność	System firewall obsługuje minimum trzy miliony jednoczesnych połączeń oraz co najmniej 120 tysięcy nowych połączeń na sekundę. Przepustowość stateful firewall wynosi nie mniej niż 28 Gbps dla pakietów 512 B, natomiast przy włączonej kontroli aplikacji nie mniej niż 6,5 Gbps. Wydajność szyfrowania IPSec VPN z wykorzystaniem algorytmu AES128 wynosi minimum 25 Gbps. Wydajność skanowania ruchu w ramach IPS dla Enterprise Traffic Mix wynosi co najmniej 4 Gbps, przy jednoczesnym włączeniu IPS, kontroli aplikacji i antywirusa minimum 2 Gbps. Wydajność inspekcji ruchu SSL dla HTTP wynosi nie mniej niż 2,5 Gbps.
Funkcje bezpieczeństwa	System realizuje funkcje zapory ogniowej klasy Stateful Inspection, kontroli aplikacji, szyfrowanych połączeń IPSec VPN, ochrony przed malware, zapobiegania włamaniom (IPS), kontroli stron WWW, ochrony poczty elektronicznej przed spamem, zarządzania pasmem ruchu, ochrony przed wyciekiem danych (DLP) oraz uwierzytelniania dwuskładnikowego z wykorzystaniem tokenów sprzętowych lub programowych. System umożliwia inspekcję ruchu szyfrowanego SSL/TLS dla HTTP, SMTP, FTP i POP3, posiada funkcję lokalnego serwera DNS z filtrowaniem zapytań oraz zapewnia mechanizmy automatyzacji reakcji na zdarzenia bezpieczeństwa.
Polityki i firewall	Polityki firewall uwzględniają adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje, reakcje zabezpieczeń oraz rejestrowanie zdarzeń. System realizuje translację adresów NAT, w tym SNAT, DNAT, PAT, translację jedendojednego i jedendowielu oraz posiada dedykowany ALG dla protokołu SIP. Rozwiązanie umożliwia tworzenie stref bezpieczeństwa takich jak LAN, WAN i DMZ, korzystanie z zewnętrznych repozytoriów adresów IP i kategorii URL, filtrowanie ruchu na podstawie geolokalizacji, harmonogramowanie reguł oraz integrację z platformami SDN i środowiskami chmurowymi.
Połączenia VPN	System umożliwia zestawianie połączeń IPSec VPN z wykorzystaniem protokołów IKEv1 i IKEv2, obsługuje szyfrowanie AES128 i AES256 w trybie GCM oraz grupy DiffieHellman 19 i 20. Rozwiązanie wspiera topologie HubandSpoke oraz Mesh, połączenia Site-to-Site i Client-to-Site, monitorowanie tuneli, mechanizmy failover, routing dynamiczny i statyczny przez VPN, uwierzytelnianie kluczem współdzielonym lub certyfikatem, limity liczby tuneli oraz mechanizmy NATT, DPD, Xauth i split tunneling.
Routing i WAN	System obsługuje routing statyczny, Policy Based Routing oraz protokoły dynamicznego routingu RIP, OSPF, BGP i PIM. Umożliwia filtrowanie tras, wykorzystanie mechanizmu ECMP, obsługę BFD oraz monitorowanie dostępności adresów IP i automatyczne modyfikowanie tablic routingu w przypadku awarii.

SDWAN	Rozwiązanie umożliwia wykorzystanie dynamicznych protokołów routingu do równoważenia obciążenia łączy WAN oraz wspiera zarówno interfejsy fizyczne, jak i wirtualne, w tym VLAN oraz IPSec.
Zarządzanie pasmem	System firewall umożliwia zarządzanie pasmem poprzez definiowanie limitów maksymalnych i gwarantowanych, oznaczanie ruchu DSCP oraz przypisywanie priorytetów. Rozwiązanie pozwala na kontrolę pasma dla aplikacji, użytkowników niezależnie od adresów IP oraz dla wybranych kategorii URL.
Ochrona malware	przed Silnik antywirusowy skanuje ruch w obu kierunkach, w tym dla protokołów działających na niestandardowych portach, obsługuje protokoły HTTP, HTTPS, FTP, POP3, IMAP, SMTP i CIFS oraz umożliwia skanowanie archiwów zagnieżdżonych. System blokuje i rejestruje pliki nieskanowalne, posiada sygnatury dla urządzeń mobilnych, zapewnia automatyczne aktualizacje bazy sygnatur, współpracuje z platformą Sandbox, realizuje dezynfekcję plików PDF i Office oraz wykorzystuje mechanizmy sztucznej inteligencji.
Ochrona atakami	przed System IPS wykorzystuje analizę sygnaturową i anomalii, chroni aplikacje na niestandardowych portach, umożliwia definiowanie własnych sygnatur i wyjątków, zapewnia ochronę DoS i DDoS, mechanizmy ochrony aplikacji webowych, kontrolę nagłówków HTTP oraz wykrywanie komunikacji typu commandandcontrol. Ochrona IPS może być uruchamiana selektywnie dla wybranych zakresów ruchu.
Kontrola aplikacji	Funkcja kontroli aplikacji oparta jest o głęboką inspekcję pakietów i bazę co najmniej 2000 sygnatur. System umożliwia kontrolę aplikacji chmurowych w zakresie wykonywanych operacji, identyfikuje aplikacje wysokiego ryzyka, pozwala na definiowanie własnych sygnatur i wyjątków oraz blokowanie aplikacji działających na niestandardowych portach.
Kontrola WWW	Moduł kontroli WWW korzysta z bazy minimum 40 milionów adresów URL podzielonych na kategorie tematyczne, obejmuje kategorie istotne z punktu widzenia bezpieczeństwa i prawa, umożliwia definiowanie białych i czarnych list, obsługuje wyrażenia regularne, strony ostrzegawcze, funkcję Safe Search, komunikaty dla użytkowników oraz wyłączanie inspekcji SSL dla wybranych adresów i kategorii.
Uwierzytelnianie użytkowników	System umożliwia uwierzytelnianie użytkowników w oparciu o lokalne bazy danych, LDAP oraz zewnętrzne systemy RADIUS i RSA SecurID. Rozwiązanie wspiera uwierzytelnianie dwuskładnikowe, architekturę Single SignOn z Active Directory oraz protokół SAML dla ruchu HTTP.
Zarządzanie systemem	Elementy systemu mogą być zarządzane lokalnie poprzez HTTPS i SSH oraz współpracują z centralnymi platformami zarządzania i monitorowania przy użyciu szyfrowanych protokołów. System obsługuje SNMP, NetFlow i sFlow, posiada API z dokumentacją, narzędzia diagnostyczne, mechanizm zatwierdzania zmian, rolę administracyjną oraz możliwość ograniczenia dostępu administracyjnego według adresów IP.
Logowanie raportowanie	i System realizuje centralne logowanie do platformy chmurowej lub dedykowanego systemu logowania. Rejestrowany jest ruch dozwolony i blokowany, aktywność administratorów, wykorzystanie zasobów oraz stan systemu. Logowanie obejmuje wszystkie moduły bezpieczeństwa, umożliwia rejestrowanie per reguła oraz przysyłanie logów do wielu serwerów SYSLOG z wykorzystaniem TCP i szyfrowania SSL/TLS.
Testy	Wszystkie funkcje i parametry wydajnościowe systemu mogą być weryfikowane na podstawie publicznej dokumentacji producenta oraz wyników testów funkcjonalnych i wydajnościowych.
Gwarancja wsparcie	i System objęty jest 36miesięczną gwarancją producenta obejmującą naprawę lub wymianę sprzętu w trybie AHR, dostęp do aktualizacji oprogramowania oraz wsparcie techniczne 24x7. W okresie gwarancji dostępne są wszystkie funkcje bezpieczeństwa, w tym IPS, antywirus, kontrola aplikacji, sandbox, antyspam, web filtering oraz bazy reputacyjne.
Wymogi formalne	Zaleca się uzyskanie dokumentów potwierdzających spełnienie wymagań dotyczących produktów podwójnego zastosowania zgodnie z obowiązującymi przepisami prawa oraz oświadczenia producenta lub autoryzowanego dystrybutora potwierdzającego pochodzenie produktu z autoryzowanego kanału sprzedaży.

2. Access point Wi-Fi (6 sztuk)

Lp. Wymaganie

1. Parametry fizyczne

- 1.1 Urządzenie przeznaczone do montażu wewnętrznego (sufitowego lub ściennego); zestaw montażowy dołączony w komplecie
- 1.2 Wymiary nie większe niż 175 × 175 × 40 mm
- 1.3 Waga urządzenia nie większa niż 0,45 kg
- 1.4 Maksymalne pobory mocy: 18 W
- 1.5 Zakres temperatury pracy: 0°C – 50°C

1.6 Wilgotność robocza: 5–90% bez kondensacji

2. Interfejsy i łączność

2.1 1 port Ethernet multigigabitowy 100M/1G/2,5G Base-T (RJ45) – port uplink główny

2.2 1 port Ethernet 10/100/1000 Base-T (RJ45) – port dodatkowy (np. na potrzeby zasilania PoE downstream lub redundancji)

2.3 Port konsoli szeregowej RS-232 (RJ45)

2.4 Port USB typ A

2.5 Zasilanie przez PoE zgodne z 802.3at (port 2,5G) lub zewnętrzny zasilacz AC

3. Parametry radiowe

3.1 Trzy niezależne radia Wi-Fi (tri-radio) + dedykowane radio BLE/Bluetooth/ZigBee

3.2 Standard bezprzewodowy: Wi-Fi 7 (IEEE 802.11be), obsługa pasm 2,4 GHz, 5 GHz oraz 6 GHz, z zachowaniem wstecznej kompatybilności z 802.11a/b/g/n/ac/ax; dostępność pasma 6 GHz zależna od lokalnych przepisów regulacyjnych (ETSI/CE)

3.3 Radio 1 (pasmo 2,4 GHz): konfiguracja 2x2 MU-MIMO, przepustowość do 688 Mbps, szerokość kanału 20/40 MHz

3.4 Radio 2 (pasmo 5 GHz): konfiguracja 2x2 MU-MIMO, przepustowość do 2 882 Mbps, szerokość kanału 20/40/80/160 MHz

3.5 Radio 3 (pasmo 5 GHz lub 6 GHz, konfigurowalne): konfiguracja 2x2; przepustowość do 5 765 Mbps w paśmie 6 GHz (HE320); umożliwia jednocześnie skanowanie wszystkich pasm 24/7 i obsługę klientów lub pracę w trybie dual-5G albo tri-band (2,4/5/6 GHz)

3.6 Anteny zewnętrzne; zysk: min. 4,5 dBi dla 2,4 GHz, min. 5,5 dBi dla 5 GHz, min. 5,5 dBi dla 6 GHz; antena BLE: min. 4,0 dBi

3.7 Obsługa OFDMA (UL i DL), DL-MU-MIMO, UL-MU-MIMO, BSS Coloring (Spatial Reuse), Target Wake Time (TWT), 1024-QAM

3.8 Maksymalna liczba jednocześnie obsługiwanych SSID: min. 16

3.9 Radio BLE/ZigBee umożliwiające wykrywanie urządzeń, obsługę iBeacon i aplikacji lokalizacyjnych

4. Bezpieczeństwo i uwierzytelnianie

4.1 Obsługa WPA, WPA2, WPA3 z uwierzytelnianiem 802.1X lub kluczem współdzielonym (PSK)

4.2 Obsługa metod EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/v1, EAP-SIM, EAP-AKA, EAP-FAST, EAP-GTC, w tym z możliwością przypisywania dynamicznego dostępu użytkownikom podpiętego serwera RADIUS

4.3 Obsługa Captive Portal (web portal) do uwierzytelniania użytkowników

4.4 Białe i czarne listy adresów MAC

4.5 Wykrywanie i neutralizacja nieautoryzowanych punktów dostępowych (WIPS/WIDS) — skanowanie 24/7 we wszystkich pasmach przez dedykowane radio skanujące bez przerywania obsługi klientów

4.6 Tryb analizatora widma (Spectrum Analyzer) oraz tryb przechwytywania pakietów (Packet Sniffer)

4.7 Ochrona sieci bezprzewodowej przez zintegrowane z kontrolerem funkcje: firewall, IPS, kontrola aplikacji, filtrowanie treści WWW

5. Zarządzanie i integracja z urządzeniem UTM/NGFW

5.1 Punkt dostępowy musi być zarządzany bezpośrednio przez wbudowany kontroler WLAN urządzenia UTM/NGFW (firewall nowej generacji) bez konieczności instalowania odrębnego oprogramowania kontrolera

5.2 Punkt dostępowy i urządzenie UTM/NGFW muszą pochodzić od tego samego producenta, zapewniając natywną integrację i wspólną platformę zarządzania bezpieczeństwem (single-pane-of-glass)

5.3 Z poziomu interfejsu zarządzającego urządzenia UTM/NGFW musi być możliwe: konfigurowanie profili SSID, zarządzanie pasmem radiowym, monitorowanie klientów Wi-Fi oraz egzekwowanie polityk bezpieczeństwa

5.4 Obsługa zero-touch deployment: punkt dostępowy po podłączeniu do sieci musi być automatycznie wykryty i wstępnie skonfigurowany przez kontroler UTM/NGFW bez ręcznej ingerencji administratora

5.5 Aktualizacja oprogramowania (firmware) punktu dostępowego musi być możliwa centralnie, z poziomu kontrolera UTM/NGFW

5.6 Integracja z modułem NAC (Network Access Control) kontrolera UTM/NGFW: możliwość automatycznej kwarantanny lub blokady urządzeń na podstawie polityki bezpieczeństwa

5.7 Ruch użytkowników sieci bezprzewodowej musi podlegać inspekcji przez mechanizmy UTM/NGFW (firewall, IPS, kontrola aplikacji, filtrowanie URL) – integracja na poziomie platformy, nie przez tunel VPN

5.8 Możliwość segmentacji ruchu bezprzewodowego przez przypisanie SSID do VLAN zarządzanych przez urządzenie UTM/NGFW

5.9 Obsługa trybu mesh między punktami dostępowymi, konfigurowanego i monitorowanego z poziomu kontrolera UTM/NGFW

5.10 Zarządzanie przez CLI (SSH) oraz GUI (HTTPS) dostępne bezpośrednio z interfejsu urządzenia UTM/NGFW

5.11 Obsługa protokołu SNMP (v1/v2c/v3) do monitorowania stanu punktu dostępowego

6. Normy i certyfikaty

6.1 Zgodność ze standardami IEEE: 802.11a/b/g/n/ac/ax (Wi-Fi 6E), 802.11e (QoS), 802.11h (DFS/TPC), 802.11i (bezpieczeństwo), 802.11k/r/v (roaming), 802.1X, 802.3at (PoE), 802.3az (EEE), 802.3bz (2,5GbE)

6.2 Certyfikacja CE (dyrektywa RED) lub równoważna wymagana dla rynku polskiego; dostępność pasma 6 GHz zgodna z obowiązującymi przepisami ETSI na terenie Polski

7. Gwarancja i wsparcie

7.1 Dożywotnia gwarancja sprzętowa producenta obejmująca wymianę wadliwego urządzenia

7.2 Serwis gwarancyjny realizowany na terenie Rzeczypospolitej Polskiej przez producenta lub wskazany przez niego autoryzowany podmiot; oferent zobowiązany do przedłożenia stosownego dokumentu

7.3 Oświadczenie producenta lub jego autoryzowanego dystrybutora potwierdzające posiadanie przez oferenta autoryzacji w zakresie sprzedaży i serwisu oferowanych rozwiązań

3. Przełącznik PoE pod WiFi 48 portów GbE (2 sztuki)

Parametr Opis i funkcjonalność

1. Parametry fizyczne platformy

1.1 Montaż w szafie rack 19", obudowa max 1U

1.2 Zasilanie 230V

1.3 MTBF > 10 lat

2. Interfejsy sieciowe – wymagania minimalne

2.1 48 portów GE, RJ-45

2.2 4 porty 10GE SFP+

2.3 24 porty PoE 802.3af/at, budżet mocy 370W (wersja PoE)

2.4 48 portów PoE 802.3af/at, budżet mocy 740W (wersja FPoE)

3. Zarządzanie

3.1 Port konsoli szeregowej RJ45

3.2 Zarządzanie przez CLI (SSH) oraz GUI przez przeglądarkę

3.3 Możliwość zarządzania przez kontroler przełączników z automatycznym wykrywaniem, centralną konfiguracją oraz będący jednocześnie konsolą NGFW

3.4 Kontroler musi automatycznie konfigurować Spanning Tree, tagowanie 802.1q oraz przejmować zarządzanie wykrytym przełącznikiem bez ingerencji administratora

3.5 Kontroler umożliwia aktualizację oprogramowania zarządzanych przełączników

3.6 Z poziomu kontrolera widoczny typ urządzeń wykrytych na porcie przełącznika (np. Linux, Windows)

3.7 Kontroler obsługuje automatyczną instalację wskazanego firmware po podłączeniu przełącznika; oprogramowanie przechowywane na kontrolerze

4. Parametry wydajnościowe

4.1 Przepustowość min. 176 Gbps, min. 260 Mpps

4.2 Tablica MAC: min. 32 000 adresów

4.3 Opóźnienie poniżej 1 μ s

4.4 Bufor pakietów: min. 2 MB

4.5 Pamięć DRAM: min. 512 MB

4.6 Pamięć FLASH: min. 64 MB

5. Wymagane funkcje

5.1 Automatyczna negocjacja prędkości i duplexu

5.2 Obsługa 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP)

5.3 Agregacja portów zgodna z 802.3ad

5.4 Obsługa min. 4000 VLANów zgodna z 802.1Q

5.5 Routing statyczny (software'owy)

5.6 Port-mirroring

5.7 Kontrola dostępu 802.1x z uwierzytelnianiem RADIUS

5.8 Zarządzanie: Telnet/SSH, HTTP/HTTPS, SNMP v1-3, SNTp, LLDP (odbiór)

5.9 Zarządzanie przez GUI i CLI

5.10	Aktualizacja oprogramowania przez TFTP/FTP oraz GUI
5.11	Integracja z NGFW: Captive Portal, białe/czarne listy MAC, stateful firewall, routing statyczny i dynamiczny (min. OSPF)
6.	Moduły sieciowe
6.1	Moduły 1GE SFP transceiver SR/LR – XX szt.
6.2	Moduły 10GE SFP+ transceiver SR/LR – XX szt.
6.3	Moduły muszą być oficjalnie wspierane przez producenta urządzeń
7.	Gwarancja oraz wsparcie
7.1	Dożywotnia gwarancja producenta z wymianą wadliwego sprzętu (min. 5 lat od zakończenia produkcji)
7.2	Serwis gwarancyjny producenta przez XX miesięcy na terenie RP (naprawa lub wymiana); w razie braku centrum serwisowego w Polsce – dokument wskazujący autoryzowany podmiot serwisowy
7.3	Dokument importera potwierdzający zgodność z przepisami dot. produktów podwójnego zastosowania oraz posiadanie certyfikowanego wewnętrznego systemu kontroli eksportu
7.4	Oświadczenie producenta lub autoryzowanego dystrybutora o posiadaniu przez oferenta autoryzacji w zakresie sprzedaży i świadczenia usług

4. Organizacja realizacji zamówienia

- Komunikacja w ramach niniejszego zamówienia oraz podczas jego realizacji może odbywać się telefonicznie, poprzez komunikatory, ale wszelkie uzgodnienia w zakresie realizacji przedmiotu muszą być uzgadniane pomiędzy stronami pisemnie, w tym elektronicznie, poprzez wymianę informacji pocztą elektroniczną na wskazane adresy email.
- Realizacja przedmiotu zamówienia odbywać się będzie zdalnie oraz lokalnie w zakresie właściwym dla zadania. Realizacja zleconych zadań może wymagać w uzasadnionych przypadkach obecności Wykonawcy w siedzibie Zamawiających nawet jeżeli określono realizację zdalną wybranego zakresu, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania przedmiotu projektu.
- Wykonawca musi przekazywać w trakcie realizacji czynności przewidzianych niniejszym zamówieniem informacje o wszelkich wykrytych podatnościach, w celu umożliwienia Zamawiającemu podjęcia natychmiastowych działań naprawczych.
- Wykonawca każdorazowo, winien uzgadniać z Zamawiającym termin prowadzenia bardziej inwazyjnych czynności ze szczególnym uwzględnieniem: DoS, i prowadzić je dopiero po uzyskaniu pisemnej, w tym poprzez środki elektronicznej komunikacji, zgody osoby Zamawiającego. Wykonawca musi prowadzić prace, które umożliwią mu zakończenie w każdym momencie takich testów.
- Jakiegokolwiek czynności prowadzone przez Wykonawcę nie mogą spowodować przestoju w świadczeniu usług przez Zamawiającego. Gdyby jednak przeprowadzenie testów rodziło ryzyko przestoju w pracy, Wykonawca w porozumieniu z Zamawiającym Wykonawcą opracuje, zaakceptowany przez Zamawiającego, scenariusz alternatywny przeprowadzenia testów tak aby zminimalizować ryzyko problemów.
- Wykonawca może prowadzić prace po uprzednim uzgodnieniu ich zakresu z każdym z Zamawiających. Przez uzgodnienie należy rozumieć precyzyjne wskazanie daty oraz czasu rozpoczęcia a także zakończenia prac.
- Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
- Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w zapytaniu ofertowym i nie są z nimi sprzeczne.
- Zamawiający we współpracy z Wykonawcą ustalą harmonogram spotkań mających na celu weryfikację stanu projektu. Zakłada się minimalną częstotliwość spotkań raz w tygodniu.
- Wykonawca musi dostosować się do polityk bezpieczeństwa Zamawiającego.
- W niniejszym dokumencie opisano wymagania minimalne.

5. Wdrożenie

- Każdy z systemów stanowiący przedmiot dostawy winien zostać wdrożony w sposób umożliwiający prawidłowe funkcjonowanie bez negatywnego wpływu na środowisko Zamawiającego.
- W przypadku dostawy rozwiązania opierającego się o serwer Wykonawca wdroży je w całości na serwerze oraz w 20% na urządzeniach/użytkownikach objętych wdrożeniem.
- Wdrożenie ma odbywać się wraz z Zamawiającym co oznacza, że Wykonawca będzie prowadził prace bezpośrednio w obecności Zamawiającego.