**Załącznik nr 2 do SWZ**

**Powiat Bytowski**

**ul. Ks. dr. Bolesława Domańskiego 2**

**77-100 Bytów**

**FORMULARZ OFERTOWY**

Ja/my niżej podpisani:

………………………………………………………………………………………………..

*(imię i nazwisko, stanowisko/podstawa reprezentacji)*

działając w imieniu i na rzecz:

………………………………………………………………………………………………..………………………………………………………………………………………………..

*(pełna nazwa Wykonawcy/Wykonawców w przypadku wspólnie ubiegających się o udzielenie zamówienia)*

Adres:…………………………………....

Województwo:……………………..……

Kraj:……………………………….……

Regon:……………………………..……

NIP:…………………………….………

Tel.:………………………………….….

Adres skrzynki ePUAP……………………

Adres e-mail:……………………………... *(na które Zamawiający ma przesłać korespondencję)*

Wadium wniesione w pieniądzu należy zwrócić na rachunek bankowy: ……………………………

Oświadczam, że rodzaj Wykonawcy to (informacja do celów statystycznych)\*:

*☐ mikroprzedsiębiorstwo*, *☐ małe przedsiębiorstwo*, *☐ średnie przedsiębiorstwo*, *☐ jednoosobowa działalność gospodarcza*, *☐ osoba fizyczna nieprowadząca działalności gospodarczej*, *☐ inny rodzaj*

Przystępując do postępowania o udzielenie zamówienia publicznego na **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD”**,Składamy ofertę na realizację przedmiotu zamówienia   
w zakresie określonym w Specyfikacji Warunków Zamówienia na następujących warunkach:

**cena netto** za realizacje całego zamówienia wynosi: …………………zł

(słownie złotych: ……………………………..)

Podatek VAT…..%, ……………………………..zł

**cena brutto** za realizacje całego zamówienia wynosi: …………………zł

(słownie złotych: ……………………………..)

**Oświadczamy, że oferujemy następujący termin wykonania zamówienia\*\*:………….. dni**

Oświadczamy, że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia oraz jej załącznikami i nie wnosimy do ich treści żadnych zastrzeżeń.

Oświadczamy, że uzyskaliśmy wszelkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty.

Informujemy, że zamierzamy/nie zamierzamy\* powierzyć wykonanie części zamówienia podwykonawcom. Zakres prac powierzonych podwykonawcy:

|  |  |  |
| --- | --- | --- |
| **Wykonawca powierzy podwykonawcom wykonanie następujących części zamówienia:** | | |
|  | Wskazanie części zamówienia, których wykonanie Wykonawca zamierza powierzyć podwykonawcy | Nazwy (firmy) podwykonawców, jeżeli są znani |
| L.p |  |  |
| 1. |  |  |
| 2. |  |  |
| 3. |  |  |
|  |  |  |

Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres wskazany w SWZ.

Oświadczamy, że zapoznaliśmy się z projektowanymi postanowieniami umowy, określonymi   
w **załączniku nr 6** do SWZ i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach w nich określonych.

Oświadczamy, że zapoznaliśmy się z klauzulą informacyjną zawartą w SWZ wynikającą z art.   
13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (t.j. Dz. U.   
z 2019 r. poz. 1781)

Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[[1]](#footnote-1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu[[2]](#footnote-2).

Oświadczamy, że sposób reprezentacji spółki/konsorcjum\* dla potrzeb niniejszego zamówienia jest następujący:

………………………………………………………………………………………………………………………………………………………………………………………………………………

Ofertę niniejszą składamy na ……… stronach.

Załącznikami do niniejszej oferty są:

………………………………………………

………………………………

Miejscowość i data …………………………………

*(podpis)*

**Informacja dla Wykonawcy:**

*Formularz oferty musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanych lub podpisem osobistym i przekazany Zamawiającemu wraz   
z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.*

**\* zakreślić właściwe**

**\*\* w wyznaczonym miejscu proszę wskazać deklarowany termin wykonania zamówienia**

**(UWAGA!!! W przypadku, gdy Wykonawca, nie zaznaczy w ofercie terminu wykonania zamówienia, Zamawiający do oceny oferty przyjmie 45 dni kalendarzowych i przyzna „0" punktów . W przypadku, gdy Wykonawca wskaże termin dłuższy niż 45 dni kalendarzowych, oferta zostanie odrzucona na podstawie art. 226 ust. 1 pkt 5.)**

**WYKAZ SPRZĘTU**

1. **UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv - 1 kpl.**

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| --- | --- | --- |
| **Typ** | **UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv, fabrycznie nowe.** | |
| System, k**onstrukcja** | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.  Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2.  Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)  Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active.  System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.  Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne).  Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19”.  Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).  Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.  Możliwość przeprowadzenia konfiguracji w trybie Zero Touch. |  |
| **Pamięć operacyjna RAM** | nie mniej niż 8 (GB) |  |
| **Przestrzeń do przechowywania logów i raportów** | nie mniej niż 120 GB |  |
| **Liczba fizycznych interfejsów 1000BASE-T** | nie mniej niż 8 |  |
| **Liczba fizycznych interfejsów 1000BASE-X** | nie mniej niż 2 |  |
| **Liczba fizycznych interfejsów 10GBASE-X** | nie mniej niż 4 |  |
| **Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q** | nie mniej niż 512 |  |
| **Wydajność Firewall** | nie mniej niż 30 000 Mbps |  |
| **Wydajność Firewall IMIX** | nie mniej niż 15 000 Mbps |  |
| **Wydajność IPS** | nie mniej niż 5 000 Mbps | …………………. |
| **Wydajność FW+IPS+AV** | nie mniej niż 1 000 Mbps |  |
| **Wydajność NGFW** | nie mniej niż 5 000 Mbps |  |
| **Liczba równoczesnych połączeń** | nie mniej niż 6 000 000 |  |
| **Liczba nowych połączeń na sekundę** | nie mniej niż 128 000 |  |
| **Wydajność IPsec VPN** | nie mniej niż 15 000 Mbps |  |
| **Wydajność dla inspekcji ruchu SSL/TLS** | nie mniej niż 2 000 Mbps |  |
| **Liczba równoczesnych połączeń SSL/TLS** | nie mniej niż 16 000 |  |
| **Liczba równoczesnych tuneli SSL VPN** | nie mniej niż 2 000 |  |
| **Liczba równoczesnych tuneli IPsec VPN** | nie mniej niż 2 000 |  |
| **Zarządzanie** | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.  Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).  Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.  Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.  Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.  Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.  System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.  System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.  Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).  System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.  System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).  Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.  System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).  Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.  System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika).  System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.  System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta  Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji.  Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. |  |
| **Zapora sieciowa** | Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.  System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.  Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.  Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.  Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.  System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).  System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika. |  |
| **Trasowanie ruchu** | Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing.  Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.  Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.  Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.  Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).  Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).  Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6. |  |
| **Translacja adresów i portów** | Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT.  Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT |  |
| **Kształtowanie pasma i jakość usług** | System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji.  Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.  System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.  Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.  Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet. |  |
| **Podstawowa ochrona przed atakami DoS i DDoS** | System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). |  |
| **Pozostałe** | Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.  Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).  System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.  System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP.  Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).  System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp.  Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).  Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).  Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych. |  |
| **Uwierzytelnianie i obsługa użytkowników** | Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.  Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników.  System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.  System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).  Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.  System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu. |  |
| **Koncentrator VPN** | System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.  System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).  System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.  Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.  Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.  Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.  Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.  Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN.  Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.  Urządzenie musi obsługiwać połączenia L2TP over IPsec. |  |
| **Logowanie i raportowanie** | System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym.  System powinien umożliwiać składowanie oraz archiwizację logów.  Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.  Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.  Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa  System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.  System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.  Rozwiązanie powinno umożliwiać wysyłanie raportów via email.  Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.  Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.  System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.  System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.  Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.  System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora. |  |
| **System prewencyjny i zaawansowanej ochrony** | Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur.  Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.  Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS.  Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.  System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet. |  |
| **Ochrona i kontrola web przed Malware** | Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.  Rozwiążanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.  Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.  System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.  Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.  Rozwiązanie musi przeprowadzać emulację skryptów Java.  Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta.  System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates) |  |
| **Ochrona i kontrola web - Inspecja ruchu SSL/TLS** | Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów.  Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.  Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.  Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).  Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.  Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. |  |
| **Filtr Web** | Filtrowanie stron web powinno być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron.  Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.  Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.  System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji. |  |
| **Ochrona i kontrola aplikacji** | Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji.  Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.  Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.  Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów.  Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.  Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN. |  |
| **Ochrona przed nieznanymi zagrożeniami** | Rozwiązanie klasy Sandbox do ochrony przez zadrożeniami typu Zero-Day.  Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.  Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.  Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf.  Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.  Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików.  System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS.  System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.  System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. |  |
| **Gwarancja** | Min. 2 lata gwarancji oraz wsparcia technicznego .  Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie.  Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.  Wsparcie i licencja na urządzenie, w tym na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące |  |
| **Wdrożenie, szkolenie** | Zamawiający wymaga podłączenia i zainstalowania we wskazanym miejscu UTM-a, Switch-y oraz AP. Zamawiający wymaga stworzenia przez Wykonawcę projektu segmentacji sieci oraz polityk bezpieczeństwa w myśl wytycznych Zamawiającego a opartych na wytycznych KRI i SZBI, CERT. Zamawiający po zaakceptowaniu projektów wymaga od Wykonawcy zaimplementowania i wdrożenia projektów na dostarczonych urządzeniach. Zamawiający wymaga szkolenia min. 8 godzin z wdrożonego rozwiązania w szczególności z zakresu polityk bezpieczeństwa, administracji i zarządzania. |  |

1. **Sprzętowy appliance zapewniający szyfrowany kanał komunikacji – 1 szt.**

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| **Typ systemu** | **Sprzętowy appliance zapewniający szyfrowany kanał komunikacji z nadrzędnym rozwiązaniem klasy UTM/NGFW zaproponowanym w obecnym postępowaniu, fabrycznie nowy.** | |
| **Porty** | min.: 1 porty 1 GbE/SFP WAN, 4 porty 1GbE LAN, 2 x port zasilania DC, 2 x USB 3.0, 1x Console (RJ-45 lub DB9) |  |
| **Rodzaj urządzenia** | switch zarządzalny z wbudowanym VPN z możliwością tunelowania ruchu w warstwie 2 z zaproponowanym urządzeniem UTM |  |
| **Przepustowość** | min. 250 Mb/s |  |
| **WIFI / GSM** | Możliwość rozbudowy urządzenia w zintegrowany modułu WIFI lub modułu GSM 3G/4G |  |
| **Moc pracy** | max. 9 W |  |
| **Zarządzanie i utrzymanie** | Rozwiązanie musi być w całości zarządzane przez nadrzędne rozwiązanie klasy UTM/NGFW.  Plik konfiguracyjny pobierany musi być automatycznie z serwera provisioningu lub z pamięci USB Flash.  Rozwiązanie cyklicznie sprawdzać powinno w/w lokalizacje pod kątem obecności nowej wersji konfiguracji.  Aktualizacja oprogramowania (firmware) realizowana z poziomu nadrzędnego urządzenia UTM/NGFW.  Urządzenie powinno pozwolić na zestawienie szyfrowanego kanału komunikacji z nadrzędnym UTM/NGFW (minimum AES-256).  Rozwiązanie po stronie interfejsu WAN winno działać jako klient DHCP z opcją późniejszej zmiany adresu na adres statyczny.  Urządzenie powinno obsługiwać modemy 3G/4G oferując przy tym mechanizm WAN Link Failover lub Load Balancing.  Interfesjy LAN urządzenia powinny działać jako kolejne interfejsy nadrzędnego rozwiązania klasy UTM/NGFW.  Filtrowanie ruchu realizowane być powinno na poziomie nadrzędnego urządzenia UTM/NGFW. |  |
| **Gwarancja i wsparcie** | Min. 2 lata gwarancji oraz wsparcia technicznego .  Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie.  Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. |  |
| **Dokumentacja, inne** | 1. Zgodność z normami: CE;  2. Produkt posiadający licencje uprawniające na dożywotnią możliwość korzystania z wszystkich funkcji produktu; |  |

1. **Przełącznik sieciowy zarządzalny 48-portowy - 5 szt.**

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| --- | --- | --- |
| **Typ** | **Przełącznik sieciowy typu core switch, fabrycznie nowy.** | |
| **Porty** | min.: 48 porty 1GbE 4 porty SFP+ 10GbE |  |
| **Rodzaj urządzenia** | switch zarządzalny |  |
| **Warstwa** | zarządzanie na poziomie warstwy 2 i 3 |  |
| **Minimalny rozmiar tablicy MAC** | 32000 |  |
| **Przepustowość** | min. 176Gb/s |  |
| **Pamięć robocza** | min. 512 MB |  |
| **Pamięć bufora** | min. 2 MB |  |
| **Moc pracy** | max. 60W |  |
| **Zarządzanie, zarządzanie zdalne z chmury** | Rozwiązanie powinno być zarządzane przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta. |  |
| **Typ obudowy** | RACK |  |
| **Ilość VLAN** | min 256 |  |
| **Gwarancja** | 1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące |  |
| **Dokumentacja, inne** | 1. Zgodność z normami: CE;  2. Zestaw mocowań do montażu w szafie RACK; |  |

1. **Przełącznik sieciowy zarządzalny 24-portowy - 3 szt.**

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| --- | --- | --- |
| **Typ** | **Przełącznik sieciowy typu core switch, fabrycznie nowy.** | |
| **Porty** | min.: 24 porty 1GbE, 4 porty SFP+ 10GbE |  |
| **Rodzaj urządzenia** | switch zarządzalny |  |
| **Warstwa** | zarządzanie na poziomie warstwy 2 i 3 |  |
| **Minimalny rozmiar tablicy MAC** | 16000 |  |
| **Przepustowość** | min. 128Gb/s |  |
| **Pamięć robocza** | min. 512 MB |  |
| **Pamięć bufora** | min. 1,5 MB |  |
| **Moc pracy** | max. 25W |  |
| **Zarządzanie, zarządzanie zdalne z chmury** | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta. |  |
| **Typ obudowy** | RACK |  |
| **Ilość VLAN** | min 256 |  |
| **Gwarancja** | 1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące |  |
| **Dokumentacja, inne** | 1. Zgodność z normami: CE;  2. Zestaw mocowań do montażu w szafie RACK; |  |

1. **Przełącznik sieciowy zarządzalny 24-portowy PoE – 1 szt.**

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| --- | --- | --- |
| **Typ** | **Przełącznik sieciowy typu core switch, fabrycznie nowy.** | |
| **Porty** | min.: 24 porty 1GbE PoE, 4 porty SFP+ 10GbE |  |
| **Rodzaj urządzenia** | switch zarządzalny |  |
| **Warstwa** | zarządzanie na poziomie warstwy 2 i 3 |  |
| **Minimalny rozmiar tablicy MAC** | 16000 |  |
| **Przepustowość** | min. 128Gb/s |  |
| **Pamięć robocza** | min. 512 MB |  |
| **Pamięć bufora** | min. 1,5 MB |  |
| **PoE obciążenie portów w standardzie 802.3af/802.3at** | 24 porty (min. 15,4W) lub 13 protów (30W) |  |
| **Moc pracy** | max. 410W |  |
| **Zarządzanie, zarządzanie zdalne z chmury** | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta. |  |
| **Typ obudowy** | RACK |  |
| **Ilość VLAN** | min 256 |  |
| **Gwarancja** | 1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące |  |
| **Dokumentacja, inne** | 1. Zgodność z normami: CE;  2. Zestaw mocowań do montażu w szafie RACK; |  |

1. **Przełącznik sieciowy zarządzalny 8-portowy – 4 szt.**

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| --- | --- | --- |
| **Typ** | **Przełącznik sieciowy typu core switch, fabrycznie nowy.** | |
| **Porty** | min.: 8 porty 1GbE 2 porty SFP 1GbE |  |
| **Rodzaj urządzenia** | switch zarządzalny |  |
| **Warstwa** | zarządzanie na poziomie warstwy 2 i 3 |  |
| **Minimalny rozmiar tablicy MAC** | 8000 |  |
| **Przepustowość** | min. 20Gb/s |  |
| **Pamięć robocza** | min. 256 MB |  |
| **Pamięć bufora** | min. 512 KB |  |
| **Moc pracy** | max. 12W |  |
| **Zarządzanie, zarządzanie zdalne z chmury** | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta. |  |
| **Ilość VLAN** | min 256 |  |
| **Gwarancja** | 1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące |  |
| **Dokumentacja, inne** | 1. Zgodność z normami: CE;  2. Zestaw mocowań do montażu w szafie RACK; |  |

1. **Punkt dostępowy AP – 6 szt.**

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry sprzętu**  **oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| --- | --- | --- |
| **Typ** | **Punkt dostępowy AP, fabrycznie nowy** | |
| **Porty** | min.: 1GbE PoE+ (802.3at), gniazdo zasilania DC, port konsoli dostępu |  |
| **Rodzaj urządzenia** | Punkt dostępowy AP WIFI 6 |  |
| **Anteny wewnętrzne** | Min. 2x2:2 dual radio (1 x 2.4 GHz, 1 x 5 GHz) |  |
| **Obsługiwanie standardy 802.11** | b, n, g, ax, ac |  |
| **Szybkość transmisji danych 2,4 GHz** | min. 574 Mbps |  |
| **Szybkość transmisji danych 5 GHz** | min. 1,2 Gbps |  |
| **Uchwyt** | Dedykowany uchwyt producenta urządzenia do zamocowania na ścianie lub suficie |  |
| **Waga** | max. 0,9 kg |  |
| **Moc pracy** | max. 18W |  |
| **Zarządzanie, zarządzanie zdalne z chmury** | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta. |  |
| **Gwarancja** | 1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące |  |
| **Dodatkowe wymagania** | Zamawiający wymaga by Wykonawca wykonał przed dostarczeniem rozwiązania - projektu pokrycia i pojemności zasięgów WIFI z testami i pomiarami na obiekcie oraz miejscach wskazanych przez Zamawiającego. Przekazane mapy pokrycia sygnałem Zamawiającemu odbywa się w trakcie przekazania urządzeń. Zamawiający udostępni obiekt do dokonania wizji lokalnej wraz z pomiarami w uzgodnionym wcześniej terminie. |  |

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1). [↑](#footnote-ref-1)
2. W przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie) [↑](#footnote-ref-2)