Załącznik nr 1 do SWZ

**Opis przedmiotu zamówienia**

**Formularz specyfikacji technicznej urządzenia UTM oferowanego przez Wykonawcę**

**Minimalne parametry techniczne sprzętu komputerowego wymagane**

**przez Zamawiającego**

**Urządzenie UTM - 1 szt.**

**………………………………………………………..**

 (producent, model, numer katalogowy)

|  |  |  |
| --- | --- | --- |
|  | **UTM o minimalnych parametrach technicznych** | **UTM o parametrach technicznych oferowanych przez wykonawcę** |
| **OBSŁUGA SIECI** | Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. |  |
| **ZAPORA KORPORACYJNA (Firewall)** | Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. |  |
| Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. |  |
| Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). |  |
| Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. |  |
| Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. |  |
| Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. |  |
| Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. |  |
| Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. |  |
| Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. |  |
| Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). |  |
| System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe. |  |
| **INTRUSION PREVENTION SYSTEM (IPS)** | System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe |  |
| Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. |  |
| Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. |  |
| Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. |  |
| Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. |  |
| Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS |  |
| Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP |  |
| Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. |  |
| Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). |  |
| Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych. |  |
| **KSZTAŁTOWANIE PASMA (Traffic Shapping)** | Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. |  |
| Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP |  |
| Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). |  |
| Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. |  |
| **OCHRONA ANTYWIRUSOWA** | Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). |  |
| Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji |  |
| Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. |  |
| Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji. |  |
| **OCHRONA ANTYSPAM** | Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). |  |
| Ochrona antyspam ma działać w oparciu o: **a)** białe/czarne listy, **b)** DNS RBL, **c)** Skaner heurystyczny. |  |
| W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. |  |
| Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |  |
| **WIRTUALNE SIECI PRYWATNE (VPN)** | Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). |  |
| Urządzenie ma wspierać co najmniej następujące typy sieci VPN: **a)** PPTP VPN, **b)** IPSec VPN, **c)** SSL VPN. |  |
| SSL VPN ma działać co najmniej w trybach tunelu i portalu |  |
| Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. |  |
| Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) |  |
| Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). |  |
| Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. |  |
| Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. |  |
| **FILTR DOSTĘPU DO STRON WWW** | Urządzenie ma posiadać wbudowany filtr URL. |  |
| Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. |  |
| Administrator ma mieć możliwość dodawania własnych kategorii URL. |  |
| Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: **a)** blokowanie dostępu do adresu URL, **b)** zezwolenie na dostęp do adresu URL, **c)** blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. |  |
| Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. |  |
| Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych |  |
| Filtr URL musi uwzględniać komunikację po protokole HTTPS. |  |
| Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME |  |
| Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. |  |
| Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch |  |
| **UWIERZYTELNIANIE** | Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: **a)** lokalną bazę użytkowników (wewnętrzny LDAP), **b)** zewnętrzną bazę użytkowników (zewnętrzny LDAP), **c)** usługę katalogową Microsoft Active Directory. |  |
| Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. |  |
| Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: **a)** SSL, **b)** Radius, **c)** Kerberos. |  |
| Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy |  |
| Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. |  |
| Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. |  |
| Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). |  |
| Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. |  |
| **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** | Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing) |  |
| Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: **a)** równoważenie względem adresu źródłowego, **b)** równoważenie względem połączenia. |  |
| Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. |  |
| Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). |  |
| Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. |  |
| W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów) |  |
| Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. |  |
| **ROUTING (TRASOWANIE)** | Urządzenie ma umożliwiać statyczne trasowanie pakietów. |  |
| Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. |  |
| Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). |  |
| Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. |  |
| **ADMINISTRACJA URZĄDZENIEM** | Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. |  |
| Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. |  |
| Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. |  |
| Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. |  |
| Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis |  |
| Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) |  |
| Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania |  |
| Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. |  |
| Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. |  |
| Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. |  |
| Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. |  |
| Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ). |  |
| System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services) |  |
| Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. |  |
| Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. |  |
| Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). |  |
| Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX |  |
| Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: **a)** manualnego eksportu do pliku w dowolnym momencie czasu, **b)** automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu |  |
| Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. |  |
| Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. |  |
| **RAPORTOWANIE** | Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. |  |
| System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. |  |
| System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. |  |
| System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów |  |
| System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. |  |
| System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. |  |
| Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. |  |
| Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3 |  |
| Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH) |  |
| **POZOSTAŁE USŁUGI I FUNKCJE** | Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. |  |
| Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. |  |
| Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). |  |
| Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. |  |
| Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). |  |
| Urządzenie ma posiadać usługę DNS Proxy |  |
| Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). |  |
| Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. |  |
| Urządzenie musi mieć zaimplementowane Open API |  |
| Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. |  |
| Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia. |  |
| **GWARANCJA I SERWIS** | Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. |  |
| W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. |  |
| **PARAMETRY SPRZĘTOWE** | Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 Gb |  |
| Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy |  |
| Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16. |  |
| Liczba portów światłowodowych 10Gbps – min. 2 z możliwością rozszerzenia do 6. |  |
| . Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:**a)** Moduł z 8 interfejsami miedzianymi 10/100/1000Mbps**b)** Moduł z 4 interfejsami miedzianymi 10Gbps**c)** Moduł z 8 interfejsami światłowodowymi 1Gbps**d)** Moduł z 4 interfejsami światłowodowymi 10Gbps |  |
| Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. |  |
| Urządzenie ma być wyposażone w min. 2 różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45. |  |
| Przepustowość Firewall (1518 bajtów UDP) – minimum 18Gbps. |  |
| Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 10Gbps. |  |
| Przepustowość filtrowania Antywirusowego – minimum 3Gbps. |  |
| Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 4Gbps. |  |
| Liczba tuneli VPN IPSec – minimum 1 000 |  |
| Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300 |  |
| Liczba tuneli typu SSL VPN (tryb portalu) – minimum 300. |  |
| Obsługa interfejsów 802.11q (VLAN) – minimum 1336. |  |
| Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę. |  |
| Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. |  |
| Urządzenie musi być wyposażone w moduł TPM |  |
| Urządzenie nie ma limitu na liczbę użytkowników. |  |
| Liczba reguł filtrowania – minimum 32 768. |  |
| Liczba tras statycznego routingu – minimum 5 120. |  |
| Liczba tras dynamicznego routingu – minimum 10 000. |  |
| Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U |  |

*(****podpis elektroniczny*** *osoby/osób upoważnionej do reprezentowania Wykonawcy)*

Załącznik nr 2 do SWZ

**FORMULARZ OFERTOWY**

**Dane dotyczące Wykonawcy**

|  |  |
| --- | --- |
| **Nazwa:*****(pełna nazwa Wykonawcy/Wykonawców, w przypadku wykonawców wspólnie ubiegających się o udzielenie* *zamówienia)*** |  |
| **Adres:** |  |
| **Województwo, w którym mieści się siedziba Wykonawcy:** |  |
| **Nr telefonu/faksu:** |  |
| **e-mail:** |  |
| **nr NIP:** |  |
| **nr REGON:** |  |

Odpowiadając na ogłoszenie o zamówieniu udzielanym w trybie podstawowym z możliwością negocjacji, którego przedmiotem jest **dostawa urządzenia UTM**, zobowiązujemy się wykonać przedmiot zamówienia zgodnie z opisem zawartym w SWZ, za wynagrodzenie:

cena netto.........................…………..zł

(słownie: ...................................................................................................................................)

podatek VAT……%..........................................................................zł

cena brutto.........................…………..zł

(słownie: ...................................................................................................................................)

**Kryterium pozacenowe:**

termin dostawy: **………. (wpisać ilość dni)**

1. Oświadczamy, że oferowana cena brutto obejmuje wszystkie koszty związane z realizacją zamówienia.
2. Oświadczamy, że zapoznaliśmy się z SWZ i nie wnosimy do niej żadnych zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty.
3. Uważamy się za związanych niniejszą ofertą do terminu związania ofertą wskazanego w SWZ.
4. Oświadczamy, że przedmiot zamówienia zamierzamy wykonać:

sami bez udziału podwykonawców \*/ z udziałem podwykonawców

W przypadku powierzenia części zamówienia podwykonawcom – Wykonawca wypełnia poniższe:

|  |  |  |
| --- | --- | --- |
| Wskazanie części zamówienia powierzanej podwykonawcy | Wartość lub procentowa część zamówienia, jaka zostanie powierzona podwykonawcy | Nazwa i adres firmypodwykonawcy |
|  |  |  |

\* niepotrzebne skreślić

1. Zawarte w SWZ istotne postanowienia umowy zostały przez nas zaakceptowane i zobowiązujemy się w przypadku udzielenia nam zamówienia do podpisania umowy w miejscu i terminie określonym przez Zamawiającego.
2. Oświadczamy, że niniejsza oferta zawiera na stronach od ……. Do …….informacje stanowiące **tajemnicę przedsiębiorstwa** w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa stanowi **Załącznik nr….** Do oferty.
3. **Oświadczamy, że jesteśmy** (właściwe zaznaczyć):
* mikroprzedsiębiorstwem (zatrudniającym mniej niż 10 osób i roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów euro),
* małym przedsiębiorstwem (zatrudniającym mniej niż 50 osób i roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów euro),
* średnim przedsiębiorstwem (zatrudniającym mniej niż 250 osób i roczny obrót nie przekracza 50 milionów euro lub roczna suma bilansowa nie przekracza 43 milionów euro),
* dużym przedsiębiorstwem (zatrudniającym 250 lub więcej osób i roczny obrót przekracza 50 milionów euro lub roczna suma bilansowa przekracza 43 milionów euro)
1. Załącznikami do niniejszej oferty są:
	1. …..
	2. …..
	3. …..

10. Oświadczam/my, że wypełniłem/wypełniliśmy w imieniu Zamawiającego obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

…………….…. *(miejscowość),* dnia ……….……. r.

*(****podpis elektroniczny*** *osoby/osób upoważnionej do reprezentowania Wykonawcy)*

*Informacje dla wykonawcy:*

* + 1. *Formularz oferty musi być podpisany przez osobę lub osoby uprawnione do reprezentowania Wykonawcy
		i przedłożony wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.*
		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 następuje np. przez jego wykreślenie).*

Załącznik nr 3 do SWZ

**Wykonawca:**

*………………………………………….*

*………………………………………….*

*………………………………………….*

 *(pełna nazwa, adres)*

**Oświadczenie wykonawcy**

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych

w postępowaniu o udzielenie zamówienia publicznego prowadzonym **w trybie podstawowym z możliwością negocjacji, którego przedmiotem jest dostawa urządzenia UTM**

**DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA**

* + - 1. **OŚWIADCZENIE WYKONAWCY**
		1. Oświadczam/my, że nie podlegam/my wykluczeniu z postępowania na podstawie
		art. 108 ust. 1 Pzp.
1. Oświadczam/my, że zachodzą w stosunku do mnie/nas podstawy wykluczenia z postępowania na podstawie art. …………… ustawy Pzp (*podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 ustawy Pzp*).

Jednocześnie oświadczam/my, że w związku z ww. okolicznością, na podstawie art. 110 ust 2 ustawy Pzp podjąłem/ podjęliśmy następujące środki naprawcze:

**…………………………………………………………………………………………………………**

3. Oświadczam/my, że nie podlegam/my wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego Dz. U. z 2022 r., poz. 835).

* + - 1. **OŚWIADCZENIE WYKONAWCY DOTYCZĄCE PODWYKONAWCY/ÓW**
1. Oświadczam/my, że Podwykonawca/cy ………………………….. nie podlegaj/ją wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2. Oświadczam/my, że Podwykonawca/cy ………………………….. nie podlegaj/ją wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego Dz. U. z 2022 r., poz. 835).

  **III. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne
i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

…………….……. *(miejscowość),* dnia ………….……. r.

*(****podpis elektroniczny*** *osoby/osób upoważnionej do reprezentowania Wykonawcy)*

Załącznik nr 4 do SWZ

**Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia**

składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych w postępowaniu o udzielenie zamówienia publicznego prowadzonego **w trybie podstawowym z możliwością negocjacji, którego przedmiotem jest dostawa urządzenia UTM**

Oświadczam, że:

Wykonawca …………………………………………………………………………………..………

*(nazwa i adres Wykonawcy)*

zrealizuje zamówienie w zakresie:

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

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

Wykonawca …………………………………………………………………………………..………

*(nazwa i adres Wykonawcy)*

zrealizuje zamówienie w zakresie:

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

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

Wykonawca …………………………………………………………………………………..………

*(nazwa i adres Wykonawcy)*

zrealizuje zamówienie w zakresie:

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

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

 …………….……. *(miejscowość),* dnia …………………. r.

*(****podpis elektroniczny*** *osoby/osób upoważnionej do reprezentowania Wykonawcy)*