Załącznik nr 1

**„ FORMULARZ OFERTY”**

##### **dla postępowania o udzielenie zamówienia publicznego** prowadzonego w trybie podstawowym na podstawie art. **275 pkt 1** ustawy **Pzp pn: Rozbudowa systemu ochrony urządzeń poprzez wdrożenie wyższej klasy rozwiązań technicznych w zakresie ochrony sieci w Urzędzie Gminy oraz wdrożenie zapory sieciowej UTM w 15 pozostałych jednostkach organizacyjnych Gminy**

|  |
| --- |
|  **Dane dotyczące Zamawiającego:** |
| **Gmina Mszana Dolna, 34-730 Mszana Dolna ul. Spadochroniarzy 6** |

|  |
| --- |
| **Dane dotyczące Wykonawcy\*:** |
| Zarejestrowana nazwa (firma) Wykonawcy: ..............................................................................................................................................................................................................................................................................NIP: .................................., REGON: ................................ Zarejestrowany adres (siedziba) Wykonawcy z numerem kodu pocztowego:ul. ......................................................, kod pocztowy: ......................, miejscowość: .......................................................powiat: .............................................., województwo: .................................................Dane kontaktowe Wykonawcy:telefon: .............................., e-mail: ............................@...............  |

\* w przypadku oferty składanej przez Konsorcjum, należy osobno podać dane dotyczące Lidera oraz Partnera Konsorcjum

**Zamówienie zamierzamy zrealizować** (należy zaznaczyć właściwy kwadrat):

1. [ ]  sami,
2. [ ]  jako konsorcjum w skład którego wchodzą:

LIDER: ..............................................................................................................................................................

PARTNER/RZY: ..............................................................................................................................................................

 *( nazwa firmy wiodącej – Lidera, oraz Partnera/ów/ Konsorcjum)*

**Uwaga:**

W przypadku złożenia oferty wspólnej (jako konsorcjum), do formularza oferty należy załączyć:

* wypełnione pełnomocnictwo do reprezentowania Wykonawców wspólnie ubiegających się o zamówienie,
* wypełnione oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia z którego wynika, jakie roboty budowlane wykonają poszczególni Wykonawcy.

I. **Inne informacje:**

1. Osobą uprawnioną do udzielania informacji na temat złożonej oferty jest: ………………………… tel. ………...……………, faks: ………, e-mail: ……………………….
2. Osoba/osoby przewidziana/ne do podpisania umowy:

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

1. Korespondencje związaną z prowadzonym postępowaniem przetargowym oraz ze złożoną przeze mnie ofertą przetargową proszę kierować na:

adres e-mail: ……………………………………@………………….

adres pocztowy *(ulica, kod pocztowy, miejscowość)*: …………………

**Pełnomocnik** w przypadku składania **oferty wspólnej:**

Nazwisko, imię..……………………………………………………………………………………………..…

Stanowisko…………………………………………………………………………………………

Adres e mail……………

**II. Oferta:**

W odpowiedzi na ogłoszenie oferuję wykonanie przedmiotu zamówienia w pełnym rzeczowym zakresie określonym w specyfikacji warunków zamówienia (SWZ), na zasadach określonych w *ustawie Prawo zamówień publicznych* *(Dz. U. z 2023r. poz. 1605 ze zm.)*, oraz zgodnie z poniższymi warunkami:

|  |
| --- |
|  CENA OFERTY(waga kryterium: 60%) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Wyszczególnienie** | CENA OFERTY[NETTO zł] | VAT**stawka [%]** **oraz kwota [zł]** | **CENA OFERTY [ BRUTTO zł ]** |
| Oferowana cena za realizację całości przedmiotu zamówienia | **………….. zł** | …. %…………. zł | …………. zł |

|  |
| --- |
| **Słownie Cena oferty (brutto):**  |

|  |
| --- |
| DODATKOWE KRYTERIUM OCENY OFERT:(waga kryterium: **40%**) |

|  |  |
| --- | --- |
| **Oferuję wstępne przygotowanie urządzenia do pracy zdalnej**  | …………(Tak lub Nie) |

**Cena oferty została wyliczona na podstawie następującej tabeli elementów rozliczeniowych:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp.  | Nazwa przedmiotu zamówienia  | Producent i symbol oferowanego urządzenia | Ilość  | Cena jedn. netto | Cena jedn. brutto | Wartość netto | Wartość VAT, jeżeli dotyczy  | Wartość brutto  |
| 1 | Urządzenie typ 1: Urządzenie zapory sieciowej do transmisji danych cyfrowych (wymiana) w siedzibie Urzędu gminy |  | 15 |  |  |  |  |  |
| 2 | Urządzenie typ 2: Urządzenie zapory sieciowej do transmisji danych cyfrowych (zakup nowych urządzeń) w jednostkach oświatowych |  | 1 |  |  |  |  |  |
| Razem |  |  |  |

**III. Oświadczam że:**

Akceptuję Projekt umowy i zrealizuję zamówienie w terminie na warunkach i zasadach określonych przez Zamawiającego w SWZ.

Wszystkie informacje podane w załączonych do oferty dokumentach i oświadczeniach są aktualne, zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji;

Oświadczam/Oświadczamy, że wypełniłem/wypełniliśmy obowiązki

informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*

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).

\* 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).

**IV.W myśl *art. 225 ustawy pzp* informuję/my, że zgodnie z przepisami o podatku od towarów i usług wybór mojej/ naszej oferty (należy zaznaczyć właściwy kwadrat):**

1. [ ]  **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego.
2. [ ]  **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego w następującym zakresie:

|  |  |  |
| --- | --- | --- |
| Nazwa (rodzaj) towaru lub usług których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego | Wartość towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku | Stawka podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie. |
|  |  |  |
|  |  |  |

**V. Oświadczam/Oświadczamy\*,** że przy realizacji zamówienia objętego postępowaniem (należy zaznaczyć odpowiedni kwadrat):

1. [ ]  Nie zamierzam(-y) powierzyć podwykonawcom żadnej części zamówienia
2. [ ]  Zamierzam(-y) następujące części zamówienia powierzyć podwykonawcom:

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Nazwa/firma, adres podwykonawcy**(o ile jest znana na dzień składania oferty) | **Powierzane czynności**(należy wskazać/określić powierzany zakres) | **Uwagi** |
|  |  |  |  |

**Uwaga:**

W przypadku, gdy Wykonawca nie wypełni niniejszych danych lub zaznaczy „Nie zamierzam(-y) powierzyć podwykonawcom żadnej części zamówienia”, Zamawiający uzna, iż Wykonawca zamierza wykonać całość zamówienia bez udziału Podwykonawców.

**Oświadczam/Oświadczamy\*,** iż **w** **celu spełnienia warunku udziału** w niniejszym postępowaniu o udzielenie zamówienia, **polegam na** zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów udostępniających te zasoby zgodnie z przepisami *art. 118 ustawy pzp*. (należy zaznaczyć odpowiedni kwadrat):

1. [ ]  TAK
2. [ ]  NIE

**Uwaga:**

* W przypadku, gdy Wykonawca nie wypełni niniejszych danych lub zaznaczy **„NIE”,** Zamawiający uzna, iż Wykonawca **nie polega** na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów w celu spełnienia warunku udziału w niniejszym postępowaniu o udzielenie zamówienia.
* W przypadku, gdy Wykonawca zaznaczy **„TAK”,** do formularza oferty należy dołączyć zobowiązanie podmiotu udostępniającego Wykonawcy zasoby na potrzeby realizacji zamówienia - wg wzoru stanowiącego **załącznik** do SWZ.

**VI. Ponadto:**

1. **Oświadczam/Oświadczamy\***, że niniejsza oferta jest zgodna z przedmiotem zamówienia i treścią SWZ**.**
2. **Oświadczam/Oświadczamy\*,** że zapoznałem/zapoznaliśmy się z warunkami zawartymi w specyfikacji warunków zamówienia wraz z wszelkimi zmianami , uzupełnieniami i aktualizacjami oraz pozostałymi załączonymi dokumentami i przyjmuję/my je bez zastrzeżeń.
3. **Oświadczam/Oświadczamy\*,** że uwzględniłem/śmy zmiany i dodatkowe ustalenia wynikłe w trakcie procedury o udzielenie niniejszego zamówienia publicznego, stanowiące integralną część SWZ, wyszczególnionewe wszystkich przekazanych/ udostępnionych/ przez Zamawiającego pismach /dokumentach.
4. **Oświadczam/Oświadczamy\*,** że zdobyłem/śmy konieczne informacje niezbędne do przygotowania oferty.
5. **Oświadczam/Oświadczamy\***, że jestem/my związany/ni niniejszą ofertą przez okres co najmniej **30 dni**  licząc od daty składania ofert, tj. **do dnia**
6. **Oświadczam/Oświadczamy\***, że zobowiązuję/zobowiązujemy się do wypełnienia wymogów związanych z zatrudnieniem na podstawie umowy o pracę określnych w SWZ.
7. **Oświadczam/Oświadczamy\*,** że akceptuję/my wzór umowy stanowiący załącznik do SWZ i w przypadku wyboru mojej/naszej oferty, zobowiązuję/my się do jej podpisania w formie przedstawionej w SWZ (z uwzględnieniem zmian i dodatkowych ustaleń wynikłych w trakcie procedury o udzielenie niniejszego zamówienia publicznego) oraz w miejscu i terminie wyznaczonym przez Zamawiającego.
8. **Oświadczam/Oświadczamy\*,** że gwarantuję/my wykonanie przedmiotu umowy z należytą starannością z uwzględnieniem wszelkich wymaganych przepisów oraz przyjmujemy odpowiedzialność wynikającą z rodzaju wykonywanych usług/robót, przewidzianą w przepisach prawa cywilnego i prawa karnego.
9. **Oświadczam/Oświadczamy\*,** iż znana jest mi/nam treść *art. 297 §1 kodeksu karnego*: „Kto, w celu uzyskania dla siebie lub kogo innego, od banku lub jednostki organizacyjnej prowadzącej podobną działalność gospodarczą na podstawie ustawy albo od organu lub instytucji dysponujących środkami publicznymi - kredytu, pożyczki pieniężnej, poręczenia, gwarancji, akredytywy, dotacji, subwencji, potwierdzenia przez bank zobowiązania wynikającego z poręczenia lub z gwarancji lub podobnego świadczenia pieniężnego na określony cel gospodarczy, instrumentu płatniczego lub zamówienia publicznego, przedkłada podrobiony, przerobiony, poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania wymienionego wsparcia finansowego, instrumentu płatniczego lub zamówienia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

\* niepotrzebne skreślić

VII. **Wykonawca oświadcza iż jest\*** (należy zaznaczyć właściwy kwadrat)**:**

1. [ ]  Mikro przedsiębiorstwem
2. [ ]  Małym przedsiębiorstwem
3. [ ]  Średnim przedsiębiorstwem
4. [ ]  Dużym przedsiębiorstwem

 \* zaznaczyć właściwe - Por. zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych, średnich i dużych przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

Mikro przedsiębiorstwo: przedsiębiorstwo zatrudnia mniej niż 10 pracowników a jego roczny obrót nie przekracza (lub/i jego całkowity bilans roczny) 2 milionów EUR.

Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.

* Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które **zatrudniają mniej niż 250 osób** i których **roczny obrót nie przekracza 50 milionów EUR** **lub** **roczna suma bilansowa nie przekracza 43 milionów EUR.**
* Duże przedsiębiorstwo: jest to przedsiębiorstwo, które nie kwalifikuje się do żadnej z ww. kategorii przedsiębiorstw.

**VIII.Tajemnica przedsiębiorstwa.**

**Oświadczam/-my\*** że niniejsza oferta :

* nie zawiera informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu *art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 z późni. zm.)* \*
* zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu *art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 z późni. zm.).* Poniżej załączam stosowne uzasadnienie zastrzeżenia informacji stanowiących tajemnicę przedsiębiorstwa. \*

Wykaz zastrzeżonych dokumentów/informacji:

* ……………..

\* jeżeli nie dotyczy należy usunąć bądź skreślić

**IX. Załączniki:**

Załącznikami do niniejszego formularza oferty są:

1. Oświadczenie dotyczące  przesłanek wykluczenia z postępowania, spełnienia warunków udziału w postępowaniu;
2. Pełnomocnictwo w przypadku podmiotów występujących wspólnie- (jeżeli dotyczy).\*
3. Zobowiązanie podmiotu udostępniającego zasoby - (jeżeli dotyczy).\*
4. Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia- (jeżeli dotyczy).\*
5. Pełnomocnictwo do reprezentowania Wykonawcy w przypadku podpisania oferty przez osoby nie wymienione w odpisie z właściwego rejestru (jeżeli dotyczy).\*

… …………………………………………………………

\* jeżeli nie dotyczy należy usunąć bądź skreślić

UWAGA:

1. Zamawiający zaleca przed podpisaniem, zapisanie niniejszego dokumentu w formacie .pdf
2. Formularz oferty musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania Wykonawcy, kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

# Załącznik nr 2a

**OŚWIADCZENIE O NIEPODLEGANIU WYKLUCZENIU I SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU[[1]](#footnote-1)**

*(składane* ***wraz z ofertą)***

|  |  |
| --- | --- |
| **Nazwa/Firma** |  |
| **Adres** |  |
| **dane rejestrowe:**(odpowiednio w zależności od formy działalności, należy podać przynajmniej jedną z wyszczególnionych informacji) | **NIP** | **REGON** | nr **KRS/CEiDG/PESEL** |
|  |  |  |

*(Nazwy (firmy) i dokładny adres wykonawcy/ lub odpowiednio wspólnika spółki cywilnej lub członka konsorcjum)*

## składane na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Rozbudowa systemu ochrony urządzeń poprzez wdrożenie wyższej klasy rozwiązań technicznych w zakresie ochrony sieci w Urzędzie Gminy oraz wdrożenie zapory sieciowej UTM w 15 pozostałych jednostkach organizacyjnych Gminy**

## **I. DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA**

Oświadczam, że **(*\*niepotrzebne skreślić)***:

**nie podlegam wykluczeniu z postępowania** na podstawie **art. 108 ust. 1** Ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t, j. Dz. U. z 2023 r. poz. 1605 z późni. zm.),\*

**zachodzi w stosunku do mnie podstawa wykluczenia z postępowania** (wskazać podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt. 1, 2 i 5 Ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych [t. j. Dz.U. z 2023 r. poz. 1605., dalej „Ustawa”] poprzez zaznaczenie odpowiedniego pola symbolem X w kolumnie nr 1 poniższej tabeli)\*.

Jednocześnie oświadczam, że w związku ze wskazaną okolicznością wykluczenia, na podstawie art. 110 ust. 2 Ustawy podjąłem środki naprawcze, w następującym zakresie(wskazać zakres podjętych środków naprawczych w kolumnie nr 3 poniższej tabeli)\*

|  |  |
| --- | --- |
| podstawa prawna wykluczenia wskazana w Ustawie | podjęte środki naprawcze |
| 1 | 2 | 3 |
|  | art. 108 ust. 1 pkt 1 |  |
|  | art. 108 ust. 1 pkt 2 |  |
|  | art. 108 ust. 1 pkt 5 |  |

UWAGA! Niewypełnienie tabeli cz. II pkt 2 nin. oświadczenia oznacza że nie dotyczy.

1. **nie podlegam 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 dnia 15.04.2022 r. poz. 835,) i nie jestem umieszczony na listach o których mowa w ww. ustawie;

**II. DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU:**

Oświadczam, że **spełniam warunki udziału w postępowaniu** określone przez zamawiającego w specyfikacji warunków zamówienia;

**III. INFORMACJE W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW \***

w celu potwierdzenia spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w rozdz. 8 SWZ w zakresie doświadczenia\*/osób skierowanych przez Wykonawcę do realizacji zamówienia, polegam na zdolnościach podmiotu/ów udostępniającego/ych zasoby:

|  |
| --- |
|  |

*(nazwa i adres podmiotu/ów udostępniającego/ych zasoby)*

którego/ych zobowiązanie/a do oddania niezbędnych zasobów oraz oświadczenie/a o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu składam wraz z ofertą.

**IV. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam/y, 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.

**Wypełniony dokument musi być podpisany przez osobę umocowaną/ osobę upoważnioną do reprezentacji wykonawcy/wykonawców kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym (elektronicznym)**

# Załącznik Nr 2b

**OŚWIADCZENIE O NIEPODLEGANIU WYKLUCZENIU I SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU[[2]](#footnote-2)**

*(oświadczenie podmiotu udostępniającego Wykonawcy do dyspozycji niezbędne zasoby, składane* ***wraz z ofertą****)*

|  |  |
| --- | --- |
| **Nazwa/Firma/Imię i nazwisko** podmiotu, udostępniającego Wykonawcy niezbędne zasoby |  |
| **Adres** |  |
| **dane rejestrowe:**(odpowiednio w zależności od formy działalności, należy podać przynajmniej jedną z wyszczególnionych informacji) | **NIP** | **REGON** | nr **KRS/CEiDG/PESEL** |
|  |  |  |

W związku z zobowiązaniem się do oddania do dyspozycji na rzecz Wykonawcy:

|  |  |
| --- | --- |
| nazwa i adres wykonawcy, któremu zostaną udostępnione zasoby |  |

niezbędnych zasobów:

|  |  |
| --- | --- |
| należy wskazać udostępnione zasoby |  |

składane na potrzeby wykonania zamówienia publicznego pod nazwą: **Rozbudowa systemu ochrony urządzeń poprzez wdrożenie wyższej klasy rozwiązań technicznych w zakresie ochrony sieci w Urzędzie Gminy oraz wdrożenie zapory sieciowej UTM w 15 pozostałych jednostkach organizacyjnych Gminy**

**I. DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA**

Oświadczam, że:

1. **nie podlegam wykluczeniu z postępowania** na podstawie **art. 108 ust. 1 pkt 1-5 i 6** Ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t. j. Dz.U. z 2023 r. poz. 1605 z późni. zm.),
2. **nie podlegam 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 dnia 15.04.2022 r. poz. 835,) i nie jestem umieszczony na listach o których mowa w ww. ustawie;

**II. DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU:**

**Oświadczam, że spełniam warunki udziału w postępowaniu** określone przez zamawiającego w SWZ, w zakresie w jakim wykonawca powołuje się na udostępnione przeze mnie zasoby.

**III. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam/y, 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.

**Wypełniony dokument musi być podpisany przez osobę umocowaną/osobę upoważnioną do reprezentacji podmiotu oddającego Wykonawcy do dyspozycji zasoby kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym (elektronicznym)**

Załącznik nr 4

**Oświadczenie**

**Wykonawców wspólnie ubiegających się o udzielenie zamówienia**

**z art. 117 ust. 4 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych**

My, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego:

**Rozbudowa systemu ochrony urządzeń poprzez wdrożenie wyższej klasy rozwiązań technicznych w zakresie ochrony sieci w Urzędzie Gminy oraz wdrożenie zapory sieciowej UTM w 15 pozostałych jednostkach organizacyjnych Gminy**

Niniejszym oświadczamy, że Wykonawca/y:

Nazwa Wykonawcy : …………………………………………………………………….

 …………………………………………………………………………………………….

Adres Wykonawcy: ………………………………………………………………………

Wykonają dostawy/usługi w następującym zakresie:

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

 *(określić odpowiedni zakres dla wskazanego podmiotu)*

w następującym zakresie:

…………………………………………….…………………………………………………

(określić odpowiedni zakres dla wskazanego podmiotu)

………………………………………………….

 *Podpis elektroniczny*

Załącznik nr 5

**WYKAZ WYKONANYCH DOSTAW**

1. Nazwa Wykonawcy : …………………………………………………………………….

 …………………………………………………………………………………………….

1. Adres Wykonawcy: ………………………………………………………………………

Przystępując do udziału w postępowaniu o udzielenie zamówienia, pn. **Rozbudowa systemu ochrony urządzeń poprzez wdrożenie wyższej klasy rozwiązań technicznych w zakresie ochrony sieci w Urzędzie Gminy oraz wdrożenie zapory sieciowej UTM w 15 pozostałych jednostkach organizacyjnych Gminy**, w imieniu firmy którą reprezentuję

**OŚWIADCZAM(Y), ŻE:**

w okresie ostatnich 3 lat przed dniem wszczęcia postępowania o udzielenie zamówienia,
a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonałem (wykonaliśmy) następujące dostawy:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nazwa zamówienia, miejsce realizacji** | **Nazwa zamawiającego, adres, telefon, faks** | **Charakterystyka zamówienia** (zakres rzeczowy)  | **Okres realizacji**(dzień/miesiąc/rok) | **Wartość kontraktu wykonawcy**(kwota brutto w zł) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**W załączeniu przedkładam(-my) dokumenty potwierdzające należyte wykonanie dostawy wskazanej w tabeli powyżej.**

………………………………………………….

 *Podpis elektroniczny*

**Załącznik nr 6**

**Szczegółowy opis przedmiotu zamówienia**

**Przedmiot zamówienia obejmuje dostawę 16 szt. urządzeń do 16 lokalizacji Zamawiajacego.**

**Szczegółowy opis przedmiotu zamówienia:**

**Urządzenie typ 1: 15 szt.**

# Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
* 5 portami Gigabit Ethernet RJ-45.
1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# Polityki, Firewall

1. 2.       Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 3.       System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

# Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20 oraz 21.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Dynamiczne zestawianie 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.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
9. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
10. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
11. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo.
12. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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.
1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# Logowanie

1. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
3. Możliwość włączenia logowania per reguła w polityce firewall.
4. System zapewnia możliwość logowania do serwera SYSLOG.
5. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen **do 30.06.2026 r**.

# Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta **do 30.06.2026 r**., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
2. Wsparcie techniczne w ramach niniejszego zamówienia powinno być realizowane również przez autoryzowanego partnera producenta przez wykwalifikowaną biegłą w technologiach sieciowych oraz technologiach oferowanych w ramach zamówienia.

# Wdrożenie (dodatkowe kryterium oceny ofert).

W ramach dostawy należy urządzenie skonfigurować do pracy w środowisku docelowym. W ramach konfiguracji należy.

* rejestrację urządzeń na stronie producenta w imieniu zamawiającego
* podnieść oprogramowanie urządzenia do najwyższej stabilnej wersji rekomendowanej na oficjalnej stronie producenta urządzenia.
* skonfigurować port WAN oraz wszelkich niezbędnych parametrów wymaganych to aktywacji komunikacji LAN – WAN z wykorzystaniem parametrów dostarczonych przez zamawiającego.
* skonfigurować politykę odpowiedzialną za komunikację LAN – Internet najlepszymi praktykami uwzględniając wykorzystanie funkcji posiadanych w pakiecie licencyjnym oraz z uwzględnieniem potrzeb zamawiającego

**Urządzenie typ 2 – 1 szt.**

# Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
* 10 portami Gigabit Ethernet RJ-45.
1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# Polityki, Firewall

1. 2.       Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 3.       System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

# Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20 oraz 21.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Dynamiczne zestawianie 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.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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.
1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# Logowanie

1. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
3. Możliwość włączenia logowania per reguła w polityce firewall.
4. System zapewnia możliwość logowania do serwera SYSLOG.
5. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen **do 30.06.2026 r**.

# Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta **do 30.06.2026 r.,** polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
2. Wsparcie techniczne w ramach niniejszego zamówienia powinno być realizowane również przez autoryzowanego partnera producenta przez wykwalifikowaną biegłą w technologiach sieciowych oraz technologiach oferowanych w ramach zamówienia.

# Wdrożenie (dodatkowe kryterium oceny ofert).

W ramach dostawy należy urządzenie skonfigurować do pracy w środowisku docelowym. W ramach konfiguracji należy.

* rejestrację urządzeń na stronie producenta w imieniu zamawiającego
* podnieść oprogramowanie urządzenia do najwyższej stabilnej wersji rekomendowanej na oficjalnej stronie producenta urządzenia.
* skonfigurować port WAN oraz wszelkich niezbędnych parametrów wymaganych to aktywacji komunikacji LAN – WAN z wykorzystaniem parametrów dostarczonych przez zamawiającego.
* skonfigurować politykę odpowiedzialną za komunikację LAN – Internet najlepszymi praktykami uwzględniając wykorzystanie funkcji posiadanych w pakiecie licencyjnym oraz z uwzględnieniem potrzeb zamawiającego

**W przypadku składania ofert równoważnych Wykonawca ma obowiązek wykazać, że proponowane rozwiązania spełniają minimalne warunki równoważności, gwarantując uzyskanie niegorszych funkcjonalności od opisanych.**

**Zamawiający zwraca uwagę, że lokalizacje 16 adresów i miejsca dostawy i instalacji są różne, co Wykonawcy winni uwzględnić w składanych ofertach. Szczegóły realizacji ustalone zostaną po zawarciu umowy, z uwagi na konieczność uzgodnienia sposobu realizacji dostawy. Wykonawca akceptuje bez uwag te wytyczne.**

Załącznik nr 7

**Wykonawca/ Podmiot udostępniający zasoby:[[3]](#footnote-3)**

Niniejszym oświadczamy, że Wykonawca/y:

Nazwa Wykonawcy : …………………………………………………………………….

 …………………………………………………………………………………………….

Adres Wykonawcy: ………………………………………………………………………

**OŚWIADCZENIE**

**O AKTUALNOŚCI INFORMACJI ZAWARTYCH W OŚWIADCZENIU O BRAKU PODSTAW WYKLUCZENIA**

1. Na potrzeby postępowania o udzielenie zamówienia publicznego, oświadczam, że wszystkie informacje zawarte w złożonym przeze mnie wcześniej oświadczeniu o braku podstaw wykluczenia nadal są aktualne.

**2. Oświadczenie o przynależności do grupy kapitałowej[[4]](#footnote-4)**

[ ]  oświadczam, że Wykonawca, którego reprezentuję nie przynależy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jedn. Dz. U. z 2021 r., poz. 275 z późn. zm.) z innym wykonawcą, który złożył ofertę lub ofertę częściową w przedmiotowym postępowaniu\*

[ ]  oświadczam, że Wykonawca, którego reprezentuję przynależy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jedn. Dz. U. z 2021 r., poz. 275 z późn. zm.) wraz z wykonawcą, który złożył ofertę lub ofertę częściową w przedmiotowym postępowaniu tj. (podać nazwę i adres)\*:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ......................................................

Miejscowość, data

 Podpis elektroniczny

Informacja dla Wykonawcy:

Oświadczenie składa podmiot, na którego zdolnościach w celu potwierdzenia spełniania warunków udziału w postępowaniu powołuje się Wykonawca. Oświadczenie przekazuje Zamawiającemu wyłącznie ten Wykonawca, którego oferta zostanie najwyżej oceniona, na wezwanie Zamawiającego.\

1. *Oświadczenie składane na podstawie art. 125 ust. 1 Ustawy. W przypadku podmiotów występujących wspólnie (np. konsorcjum, spółka cywilna) oświadczenie powinien złożyć każdy podmiot (uczestnik konsorcjum, wspólnik spółki cywilnej).* [↑](#footnote-ref-1)
2. *Oświadczenie składane na podstawie art. 125 ust. 5 w związku z art. 125 ust. 1 Ustawy.*

*\* niepotrzebne skreślić* [↑](#footnote-ref-2)
3. Wypełnić właściwie [↑](#footnote-ref-3)
4. Należy zaznaczyć odpowiedni kwadrat. Wraz ze złożeniem oświadczenia o przynależności do tej samej grupy kapitałowej Wykonawca przedkłada dokumenty lub informacje potwierdzające przygotowanie oferty lub oferty częściowej niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej. [↑](#footnote-ref-4)